사용자 가이드

Amazon Security Lake

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Security Lake: 사용자 가이드

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 관련하여 고객에게 혼동을 일으킬 수 있는 방식이나 Amazon 브랜드 이미지를 떨어뜨리는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

Amazon Security Lake 란 무엇인가요? ... 1
- Security Lake 개요 ... 1
- Security Lake 특징 ... 2
- Security Lake ... 3
- 관련 서비스 ... 4

개념 및 용어 ... 6

시작 ... 7
- 설정 AWS 계정 ... 7
  - 에 가입 AWS 계정 ... 7
  - 관리자 액세스 권한이 있는 사용자 생성 ... 8
  - Security Lake를 활성화하는 데 사용할 계정을 식별하십시오. ... 9
- Security Lake 활성화 시 고려 사항 ... 9
- 콘솔 사용 ... 10
  - 1단계: 소스 구성 ... 10
  - 2단계: 스토리지 설정 및 롤업 리전 정의(선택 사항) ... 12
  - 3단계: 데이터 레이크 검토 및 생성 ... 13
  - 4단계: 자체 데이터 보기 및 쿼리 ... 13
  - 5단계: 구독자 생성 ... 13
- AWS CLI 또는 API 사용 ... 14
  - 1단계: IAM 역할 생성 ... 14
  - 2단계: Amazon Security Lake 활성화 ... 15
  - 3단계: 소스 구성 ... 16
  - 4단계: 스토리지 설정 및 롤업 리전 구성(선택 사항) ... 17
  - 5단계: 자체 데이터 보기 및 쿼리 ... 18
  - 6단계: 구독자 생성 ... 18

다중 계정 관리 ... 19
- 위임된 Security Lake 관리자를 위한 중요 고려 사항 ... 20
- 위임 관리자를 지정하는 데 필요한 IAM 권한 ... 21
- 위임된 Security Lake 관리자 지정 및 회원 계정 추가 ... 21
- 콘솔에서 새 계정 구성 편집 ... 23
- 위임된 Security Lake 관리자 제거 ... 24
- Security Lake의 신뢰할 수 있는 액세스 ... 25

리전 관리 ... 27
- 리전 상태 확인 ... 27

리전 설정 변경 28
롤업 리전 구성 29
데이터 복제를 위한 IAM 역할 30
AWS Glue 파티션을 등록하기 위한 IAM 역할 33
롤업 리전 추가 34
롤업 리전 업데이트 또는 제거 35
소스 관리 37
에서 데이터 수집 AWS 서비스 37
사전 조건: 권한 검증 38
소스 AWS 서비스 로 추가 39
소스 컬렉션 상태 가져오기 41
역할 권한 업데이트 41
소스 AWS 서비스 로 제거 43
CloudTrail 이벤트 로그 44
Amazon EKS 감사 로그 45
Route 53 Resolver 쿼리 로그 46
Security Hub 조사 결과 46
VPC 흐름 로그 47
AWS WAF 로그 48
소스 AWS 서비스 로 제거 43
사용자 지정 소스에서 데이터 수집 49
사용자 지정 소스 수집을 위한 파티셔닝 요구 사항 51
사용자 지정 소스를 추가하기 위한 사전 요구 사항 52
사용자 정의 소스 추가 55
사용자 지정 소스 삭제 59
구독자 관리 61
구독자 데이터 액세스 61
사전 조건 62
데이터에 액세스할 수 있는 구독자 만들기 65
데이터 구독자 업데이트 68
데이터 구독자 제거 70
구독자 쿼리 액세스 70
사전 조건 71
쿼리 액세스 권한이 있는 구독자 만들기 73
쿼리 액세스 권한이 있는 구독자 편집 76
Security Lake 쿼리 80

Security Lake 쿼리 소스 버전 1 80
로그 소스 테이블 81
데이터베이스 리전 82
파티션 날짜 82
CloudTrail 데이터에 대한 쿼리 84
Route 53 해석기 쿼리 로그에 대한 쿼리 86
Security Hub 조사 결과에 대한 쿼리 88
Amazon VPC 흐름 로그에 대한 쿼리 91
Security Lake 쿼리 소스 버전 2 95
로그 소스 테이블 81
데이터베이스 리전 82
파티션 날짜 82
Security Lake 관찰 파일 쿼리 99
CloudTrail 데이터에 대한 쿼리 100
Route 53 해석기 쿼리 로그에 대한 쿼리 102
Security Hub 조사 결과에 대한 쿼리 103
Amazon VPC 흐름 로그에 대한 쿼리 107
Amazon EKS 감사 로그에 대한 쿼리 110
AWS WAF v2 로그에 대한 쿼리 111
수명 주기 관리 114
보존 관리 114
Security Lake의 보존 설정에 대한 중요 고려 사항 114
Security Lake를 활성화할 때 보존 설정을 구성합니다. 115
보존 설정 업데이트 116
롤업 리전 117
개방형 사이버 보안 스키마 프레임워크 (OCSF) 118
OCSF란 무엇입니까? 118
OCSF 이벤트 클래스 118
OCSF 소스 식별 118
통합 122
AWS 서비스 통합 122
Amazon Bedrock 통합 124
Amazon Detective는 통합되었습니다. 124
Amazon OpenSearch Service 통합 125
Amazon OpenSearch Service Ingestion 파이프라인 통합 125
Amazon OpenSearch Service 제로 ETL 다이렉트 쿼리 통합 126

Amazon QuickSight 통합 127
Amazon SageMaker AI 통합 127
AWS AppFabric 통합 128
AWS Security Hub 통합 128
타사 통합 130
쿼리 통합 131
Accenture – MxDR 131
Aqua Security 131
Barracuda – Email Protection 132
Booz Allen Hamilton 132
Bosch Software and Digital Solutions – AIShield 132
ChaosSearch 132
Cisco Security – Secure Firewall 132
Claroty – xDome 133
CMD Solutions 133
Confluent – Amazon S3 Sink Connector 133
Contrast Security 133
Cribl – Search 134
Cribl – Stream 134
CrowdStrike – Falcon Data Replicator 134
CrowdStrike – Next Gen SIEM 134
CyberArk – Unified Identify Security Platform 135
Cyber Security Cloud – Cloud Fastener 135
DataBahn 135
Darktrace – Cyber AI Loop 135
Datadog 135
Deloitte – MXDR Cyber Analytics and AI Engine (CAE) 136
Devo 136
DXC – SecMon 136
Eviden— AIsaac (이전 명칭 Atos) 136
ExtraHop – Reveal(x) 360 137
Falcosidekick 137
Fortinet - Cloud Native Firewall 137
Gigamon – Application Metadata Intelligence 137
Hoop Cyber 137
HTCD – AI-First Cloud Security Platform 138

IBM – QRadar 138
Infosys 138
Insbuilt 138
Kyndryl – AIOps 139
Lacework – Polygraph 139
Laminar 139
MegazoneCloud 139
Monad 140
NETSCOUT – Omnis Cyber Intelligence 140
Netskope – CloudExchange 140
New Relic ONE 140
Okta – Workforce Identity Cloud 140
Orca – Cloud Security Platform 141
Palo Alto Networks – Prisma Cloud 141
Palo Alto Networks – XSOAR 141
Panther 141
Ping Identity – PingOne 142
PwC – Fusion center 142
Query.AI – Query Federated Search 142
Rapid7 – InsightIDR 142
RipJar – Labyrinth for Threat Investigations 142
Sailpoint 143
Securonix 143
SentinelOne 143
Sentra – Data Lifecyle Security Platform 143
SOC Prime 144
Splunk 144
Stellar Cyber 144
Sumo Logic 144
Swimlane – Turbine 145
Sysdig Secure 145
Talon 145
Tanium 145
TCS 146
Tego Cyber 146
Tines – No-code security automation 146

Torq – Enterprise Security Automation Platform 146
Trellix – XDR 147
Trend Micro – CloudOne 147
Uptycs – Uptycs XDR 147
Vectra AI – Vectra Detect for AWS 148
VMware Aria Automation for Secure Clouds 148
Wazuh 148
Wipro 148
Wiz – CNAPP 148
Zscaler – Zscaler Posture Control 149
보안 150
자격 증명 및 액세스 관리 151
대상 151
ID를 통한 인증 152
정책을 사용하여 액세스 관리 155
Security Lake와 IAM의 작동 방식 157
자격 증명 기반 정책 예제 165
AWS 관리형 정책 169
서비스 연결 역할 사용 192
데이터 보호 208
저장된 데이터 암호화 209
전송 중 암호화 212
서비스 개선을 위한 데이터 사용 거부 212
규정 준수 확인 212
Security Lake 보안 모범 사례 213
Security Lake 사용자에게 가능한 한 최소 권한 부여 213
요약 페이지를 봅니다. 214
Security Hub와 통합 214
삭제 AWS Lambda 214
Security Lake 이벤트 모니터링 214
복원성 215
인프라 보안 216
Security Lake의 구성 및 취약성 분석 216
VPC 엔드포인트(AWS PrivateLink) 216
Security Lake VPC 엔드포인트 고려 사항 217
Security Lake용 인터페이스 VPC 엔드포인트 생성 217

Security Lake에 대한 VPC 엔드포인트 정책 생성 217
공유 서브넷 218
모니터링 218
Amazon Security Lake에 대한 CloudWatch 지표 219
API 직접 호출 로깅 222
CloudTrail의 Security Lake 정보 222
Security Lake 로그 파일 항목 이해 223
리소스에 태그 지정 225
태그 지정 기본 사항 225
IAM 정책에서 태그 사용 226
리소스에 태그 추가 227
리소스에 대한 태그 편집 230
리소스에 대한 태그 검토 232
리소스에서 태그 제거 234
문제 해결 236
데이터 레이크 상태 문제 해결 236
Lake Formation 문제 해결 237
테이블을 찾을 수 없음 237
400 AccessDenied 237
SYNTAX_ERROR 238
호출자의 보안 주체 ARN을 Lake Formation에 추가하지 못함 238
Lake Formation을 사용하는 CreateSubscriber에서 새 RAM 리소스 공유 초대를 생성하지 않음 238
Amazon Athena에서 쿼리 문제 해결 239
쿼리해도 데이터 레이크의 새 객체가 반환되지 않습니다. 239
AWS Glue 테이블에 액세스할 수 없음 239
Organizations 문제 해결 240
액세스 거부 오류 240
IAM 문제 해결 240
Security Lake에서 작업을 수행할 권한이 없음 240
관리형 정책 이상으로 권한을 확장하고 싶습니다. 241
iam:PassRole을 수행하도록 인증되지 않음 241
내 외부의 사람이 내 Security Lake 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다. . 241
Security Lake 요금 결정 243
사용량 및 예상 비용 검토 244
지원되는 리전 및 엔드포인트 246

Security Lake 비활성화 247
문서 기록 249
..... ccliv

Amazon Security Lake 란 무엇인가요?

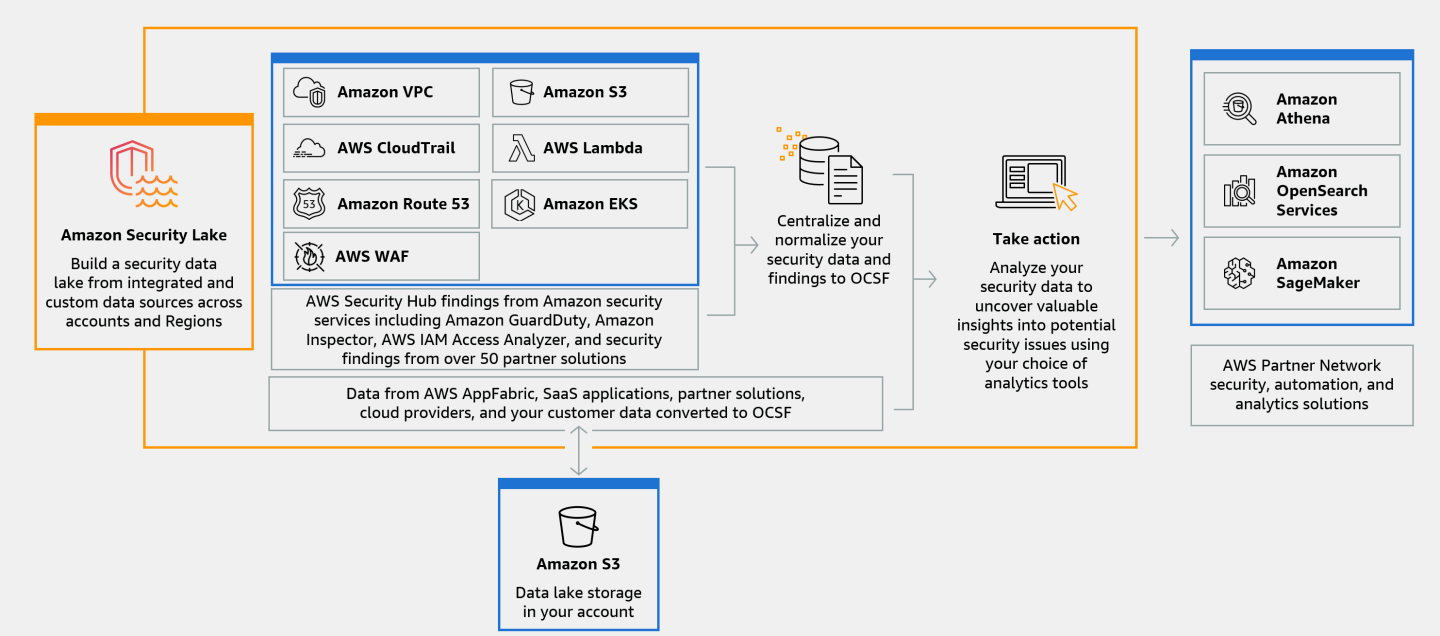
Amazon Security Lake는 완전 관리형 보안 데이터 레이크 서비스입니다. Security Lake를 사용하여 AWS 환경, SaaS 공급자, 온프레미스, 클라우드 소스 및 타사 소스의 보안 데이터를에 저장된 전용 데이터 레이크로 자동으로 중앙 집중화할 수 있습니다 AWS 계정. Security Lake를 사용하면 보안 데이터를 분석할 수 있으므로 조직 전체의 보안 상태를 더 완벽하게 이해할 수 있습니다. Security Lake를 사용하면 워크로드, 애플리케이션 및 데이터에 대한 보호도 개선할 수 있습니다.

데이터 레이크는 Amazon Simple Storage Service(S3) 버킷에서 지원되며, 데이터에 대한 소유권은 사용자에게 있습니다.

Security Lake는 통합 AWS 서비스 및 타사 서비스에서 보안 관련 로그 및 이벤트 데이터를 자동으로 수집합니다. 또한 사용자 지정 가능한 보존 및 복제 설정을 통해 데이터 수명 주기를 관리할 수 있습니다. Security Lake는 수집된 데이터를 Apache Parquet 형식과 개방형 사이버 보안 스키마 프레임워크(OCSF) 라는 표준 오픈 소스 스키마로 변환합니다. OCSF 지원을 통해 Security Lake는 및 광범위한 엔터프라이즈 보안 데이터 소스의 보안 데이터를 정규화 AWS 하고 결합합니다.

기타 AWS 서비스 및 타사 서비스는 인시던트 대응 및 보안 데이터 분석을 위해 Security Lake에 저장된 데이터를 구독할 수 있습니다.

Security Lake 개요



Security Lake 특징

다음은 Security Lake를 사용하여 보안 관련 로그 및 이벤트 데이터를 중앙 집중화, 관리 및 구독하는 데 도움이 되는 몇 가지 주요 방법입니다.

계정에서의 데이터 집계

Security Lake는 계정에 특별히 구축된 보안 데이터 레이크를 생성합니다. Security Lake는 계정 및 리전 전반의 클라우드, 온프레미스 및 사용자 지정 데이터 소스에서 로그 및 이벤트 데이터를 수집합니다. 데이터 레이크는 Amazon Simple Storage Service(S3) 버킷에서 지원되며, 데이터에 대한 소유권은 사용자에게 있습니다.

지원되는 다양한 로그 및 이벤트 소스

Security Lake는 온프레미스 및 타사 서비스를 포함한 여러 소스에서 보안 로그 AWS 서비스와 이벤트를 수집합니다. 소스에 상관없이 로그를 수집한 후에는 중앙에서 액세스하여 수명 주기를 관리할 수 있습니다. Security Lake에서 로그 및 이벤트를 수집하는 소스에 대한 자세한 내용은 Security Lake의 소스 관리을 참조하십시오.

데이터 변환 및 정규화

Security Lake는 기본적으로 지원되는 AWS 서비스 에서 들어오는 데이터를 자동으로 분할하여 스토리지 및 쿼리 효율이 높은 Parquet 형식으로 변환합니다. 또한 기본적으로 지원되는에서 Open Cybersecurity Schema Framework(OCSF) 오픈 소스 스키마 AWS 서비스 로 데이터를 변환합니다. 이렇게 하면 후처리 없이도 데이터가 다른 공급자 AWS 서비스 및 타사 공급자와 호환됩니다. Security Lake는 데이터를 정규화하므로 많은 보안 솔루션에서 이 데이터를 병렬로 사용할 수 있습니다.

구독자를 위한 다양한 수준의 액세스

구독자는 Security Lake에 저장된 데이터를 소비합니다. 구독자의 데이터 액세스 수준을 선택할 수 있습니다. 구독자는 사용자가 지정한 소스 및 AWS 리전의 데이터만 사용할 수 있습니다. 구독자는 새 객체가 데이터 레이크에 기록될 때 자동으로 알림을 받을 수 있습니다. 또는 구독자는 데이터 레이크의 데이터를 쿼리할 수 있습니다. Security Lake는 Security Lake와 구독자 간에 필요한 보안 인증을 자동으로 생성하고 교환합니다.

다중 계정 및 다중 리전 데이터 관리

Security Lake를 사용할 수 있는 모든 리전과 여러 AWS 계정을 중앙에서 활성화할 수 있습니다. Security Lake에서는 롤업 리전을 지정하여 여러 리전의 보안 로그 및 이벤트 데이터를 통합할 수도 있습니다. 이를 통해 데이터 레지던시 규정 준수 요구 사항을 준수할 수 있습니다.

구성 및 사용자 지정이 가능합니다.

Security Lake는 구성 및 사용자 지정이 가능한 서비스입니다. 로그 수집을 구성하려는 소스, 계정 및 리전을 지정할 수 있습니다. 데이터 레이크에 대한 구독자의 액세스 수준을 지정할 수도 있습니다.

데이터 수명 주기 관리 및 최적화

Security Lake는 자동 스토리지 계층화를 통해 사용자 지정 가능한 보존 설정과 스토리지 비용을 통해 데이터 수명 주기를 관리합니다. Security Lake는 들어오는 보안 데이터를 스토리지 및 쿼리에 효율적인 Apache Parquet 형식으로 자동으로 분할하고 변환합니다.

Security Lake

Security Lake를 사용할 수 있는 리전 목록은 Security Lake 리전 및 엔드포인트 섹션을 참조하세요. 리전에 대해 자세히 알아보려면 AWS 일반 참조의 AWS 서비스 엔드포인트를 참조하십시오.

각 리전에서 다음 방법 중 하나를 사용하여 Security Lake에 액세스할 수 있습니다.

AWS Management Console

AWS Management Console 는 AWS 리소스를 생성하고 관리하는 데 사용할 수 있는 브라우저 기반 인터페이스입니다. Security Lake 콘솔에서는 Security Lake 계정 및 리소스에 액세스할 수 있습니다. Security Lake 콘솔을 사용하여 대부분의 Security Lake 작업을 수행할 수 있습니다.

Security Lake

Security Lake 에 프로그래밍 방식으로 액세스하려면 Security Lake API를 사용하고 서비스로 직접 HTTPS 요청을 실행하십시오. 자세한 내용은 Security Lake API 참조를 참조하십시오.

AWS Command Line Interface (AWS CLI)

를 사용하면 시스템의 명령줄에서 명령을 실행하여 Security Lake 작업 및 AWS 작업을 수행할 AWS CLI수 있습니다. 명령줄을 사용하는 것이 콘솔을 사용하는 것보다 더 빠르고 편리할 수 있습니다. 작업을 수행하는 스크립트를 작성할 때도 명령줄 도구가 유용합니다. 설치 및 사용에 대한 자세한 내용은 섹션을 AWS CLI참조하세요AWS Command Line Interface.

AWS SDKs

AWS 는 Java, Go, Python, C++ 및 .NET과 같은 다양한 프로그래밍 언어 및 플랫폼을 위한 라이브러리 및 샘플 코드로 구성된 SDKs를 제공합니다. SDKs는 Security Lake 및 기타에 대한 편리하고 프로그래밍 방식의 액세스를 제공합니다 AWS 서비스. SDK는 요청에 암호화 방식으로 서명, 오류

관리 및 자동으로 요청 재시도와 같은 작업을 포함합니다. AWS SDKs 설치 및 사용에 대한 자세한 내용은 빌드 기반 도구를 AWS 참조하세요.

관련 서비스

다음은 Security Lake AWS 서비스 에서 사용하는 다른 방법입니다.

- Amazon EventBridge — Security Lake는 객체가 데이터 레이크에 기록되면 EventBridge를 사용하여 구독자에게 알립니다.
- AWS Glue – Security Lake는 AWS Glue 크롤러를 사용하여 AWS Glue Data Catalog 테이블을 생성하고 새로 작성된 데이터를 데이터 카탈로그로 전송합니다. 또한 Security Lake는 AWS Lake Formation 테이블의 파티션 메타데이터를 데이터 카탈로그에 저장합니다.
- AWS Lake Formation— Security Lake는 Security Lake에 데이터를 제공하는 각 소스에 대해 별도의 Lake Formation 테이블을 생성합니다. Lake Formation 테이블에는 스키마, 파티션, 데이터 위치 정보 등 각 원본의 데이터에 대한 정보가 들어 있습니다. 구독자는 Lake Formation 테이블을 쿼리하여 데이터를 사용할 수 있습니다.
- AWS Lambda— Security Lake는 Lambda 함수를 사용하여 원시 데이터에 대한 추출, 전환, 적재(ETL) 작업을 지원하고 AWS Glue의 소스 데이터에 대한 파티션을 등록합니다.
- Amazon S3 — Security Lake는 데이터를 Amazon S3 객체로 저장합니다. 스토리지 클래스 및 보존 설정은 Amazon S3 오퍼링을 기반으로 합니다. Security Lake는 Amazon S3 Select를 지원하지 않습니다.
- Amazon Simple Queue Service - Security Lake는 Amazon SQS를 사용하여 이벤트 기반 처리를 활성화하고 알림을 관리합니다.

Security Lake는 AWS 서비스다음과 함께 사용자 지정 소스에서 데이터를 수집합니다.

- AWS CloudTrail 관리 및 데이터 이벤트(S3, Lambda)
- Amazon Elastic Kubernetes Service(Amazon EKS) 감사 로그
- Amazon Route 53 Resolver 쿼리 로그
- AWS Security Hub 조사 결과
- Amazon Virtual Private Cloud(VPC) 흐름 로그
- AWS WAF v2 로그

이러한 소스에 대한 자세한 내용은 Security Lake AWS 서비스 에서 데이터 수집 섹션을 참조하세요. OCSF 스키마에서 데이터를 읽을 수 있는 구독자를 생성하여 보안 데이터 레이크의 Amazon S3 객체를 사용할 수 있습니다. 와 통합되는 Amazon Athena, Amazon Redshift 및 타사 구독 서비스를 사용하여 데이터를 쿼리할 수도 있습니다 AWS Glue.

개념 및 용어

이 섹션에서는 Amazon Security Lake를 사용하는 데 도움이 되는 주요 개념과 용어를 설명합니다.

기여 리전

롤업 리전에 데이터를 AWS 리전 제공하는 하나 이상의 입니다.

데이터 레이크

Amazon Simple Storage Service(S3) 에 저장되고 Security Lake에서 관리하는 영구 데이터 Security Lake는 AWS Glue 를 사용하여 새로 작성된 데이터를 데이터 카탈로그로 전송합니다. 또한 Security Lake는 데이터 레이크에 데이터를 제공하는 각 소스에 대한 AWS Lake Formation 테이블을 생성합니다. 데이터 레이크는 일반적으로 다음을 저장합니다.

- 정형 및 비정형 데이터
- 원시 데이터 및 변환된 데이터

Security Lake는 보안 관련 로그 및 이벤트를 수집하도록 설계된 데이터 레이크 서비스입니다.

개방형 사이버 보안 스키마 프레임워크 (OCSF)

보안 로그 및 이벤트를 위한 표준화된 오픈 소스 스키마입니다. 다양한 보안 도메인에서 AWS 및 기타 보안 업계 리더가 개발했습니다. Security Lake는에서 수집하는 로그와 이벤트를 OCSF 스키마 AWS 서비스 로 자동으로 변환합니다. 사용자 지정 소스는 로그와 이벤트를 Security Lake로 보내기 전에 OCSF로 변환합니다.

롤업 리전

하나 이상의 기여 리전의 보안 로그와 이벤트를 통합 AWS 리전 하는 입니다. 롤업 리전을 하나 이상 지정하면 리전 규정 준수 요구 사항을 준수하는 데 도움이 될 수 있습니다.

소스

OCSF의 특정 이벤트 클래스와 일치하는 단일 시스템에서 생성된 로그 및 이벤트 세트입니다. Security Lake는 소스에서 데이터 추출 출처는 다른 AWS 서비스 또는 타사 서비스일 수 있습니다. 타사 소스의 경우 데이터를 Security Lake로 보내기 전에 OCSF 스키마로 데이터를 변환해야 합니다.

구독자

Security Lake의 로그와 이벤트를 사용하는 서비스입니다. 구독자는 다른 서비스 AWS 서비스 또는 타사 서비스일 수 있습니다.

Amazon Security Lake 시작하기

이 섹션의 주제에서는 Security Lake 사용을 활성화하고 시작하는 방법을 설명합니다. 데이터 레이크 설정을 구성하고 로그 수집을 설정하는 방법을 알아봅니다. AWS Management Console 또는 프로그래밍 방식으로 Security Lake를 활성화하고 사용할 수 있습니다. 어떤 방법을 사용하든 먼저 AWS 계정 및 관리 사용자를 설정해야 합니다. 이후 단계는 액세스 방법에 따라 다릅니다.

Security Lake 콘솔은 시작하기 위한 간소화된 프로세스를 제공하며 데이터 레이크를 생성하는 데 필요한 모든 필수 AWS Identity and Access Management (IAM) 역할을 생성합니다.

프로그래밍 방식으로 Security Lake에 액세스하는 경우 데이터 레이크를 구성하려면 일부 AWS Identity and Access Management (IAM) 역할을 생성해야 합니다.

> **Important**
>
> Security Lake는 Security Lake를 활성화하기 전에 생성된 기존 AWS 원시 로그 소스 이벤트의 채우기를 지원하지 않습니다.

주제

- 설정 AWS 계정
- Security Lake 활성화 시 고려 사항
- 콘솔을 사용하여 Security Lake 활성화
- 프로그래밍 방식으로 Security Lake 활성화

설정 AWS 계정

Amazon Security Lake를 활성화하려면 먼저이 있어야 합니다 AWS 계정. 이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.

2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

   를 ID 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

Security Lake를 활성화하는 데 사용할 계정을 식별하십시오.

Security Lake는와 통합되어 조직의 여러 계정에서 로그 수집을 AWS Organizations 관리합니다. 조직에서 Security Lake를 사용하려면 Organizations 관리 계정을 사용하여 위임된 Security Lake 관리자를 지정해야 합니다. 그런 다음 위임된 관리자의 자격 증명을 사용하여 Security Lake를 활성화하고, 구성원 계정을 추가하고, 해당 구성원에 대해 Security Lake를 활성화해야 합니다. 자세한 내용은 Security Lake AWS Organizations 에서를 사용하여 여러 계정 관리 단원을 참조하십시오.

또는 조직에 속하지 않은 독립 실행형 계정에 대해 Organizations 통합 없이 Security Lake를 사용할 수도 있습니다.

Security Lake 활성화 시 고려 사항

Security Lake를 활성화하기 전에 다음 사항을 고려하십시오.

- Security Lake는 리전 간 관리 기능을 제공하므로 데이터 레이크를 생성하고 전체 AWS 리전에 걸쳐서 로그 수집을 구성할 수 있습니다. 지원되는 모든 리전에서 Security Lake를 활성화하려면 지원되는 모든 리전의 엔드포인트를 선택할 수 있습니다. 또한 롤업 리전을 추가하여 여러 리전의 데이터를 단일 리전으로 집계할 수 있습니다.
- 지원되는 모든 AWS 리전에서 Security Lake를 활성화하는 것이 좋습니다. 이렇게 하면 Security Lake는 사용자가 활발히 사용하지 않는 리전에서도 무단 또는 비정상적인 활동과 관련된 데이터를

수집할 수 있습니다. 지원되는 모든 리전에서 Security Lake가 활성화되지 않은 경우 여러 리전에서 사용하는 다른 서비스로부터 데이터를 수집하는 기능이 저하됩니다.

- 어느 리전에서든 Security Lake를 처음 활성화하면 계정에 대해 다음과 같은 서비스 연결 역할이 생성됩니다.
  - AWSServiceRoleForSecurityLake:이 역할에는 AWS 서비스 사용자를 대신하여 다른를 호출하고 보안 데이터 레이크를 운영할 수 있는 권한이 포함됩니다. Security Lake를 위임 Security Lake 관리자로 활성화하면 Security Lake가 조직의 각 구성원 계정에 서비스 연결 역할을 생성합니다.
  - AWSServiceRoleForSecurityLakeResourceManagement: Security Lake는이 역할을 사용하여 지속적인 모니터링 및 성능 개선을 수행하므로 지연 시간과 비용을 잠재적으로 줄일 수 있습니다. 이 서비스 연결 역할은 `resource-management.securitylake.amazonaws.com` 서비스에 해당 역할을 맡깁니다. 이 서비스 역할을 활성화하면 Lake Formation에 대한 액세스 권한도 부여됩니다.

    2025년 4월 17일 이전에 Security Lake를 활성화한 기존 계정에 미치는 영향에 대한 자세한 내용은 섹션을 참조하세요Update for existing accounts.

  서비스 연결 역할의 작동 방식에 대한 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 사용을 참조하세요.
- Security Lake는 Amazon S3 객체 잠금을 지원하지 않습니다. 데이터 레이크 버킷이 생성되면 S3 객체 잠금이 기본적으로 비활성화됩니다. 버킷에서 객체 잠금을 활성화하면 데이터 레이크로 정규화된 로그 데이터 전송이 중단됩니다.
- 리전에서 Security Lake를 다시 활성화하는 경우 이전 Security Lake 사용에서 리전의 해당 AWS Glue 데이터베이스를 삭제해야 합니다.

콘솔을 사용하여 Security Lake 활성화

이 자습서에서는를 통해 Security Lake를 활성화하고 구성하는 방법을 설명합니다 AWS Management Console. 의 일부로 AWS Management Console Security Lake 콘솔은 시작하기 위한 간소화된 프로세스를 제공하고 데이터 레이크를 생성하는 데 필요한 모든 필수 AWS Identity and Access Management (IAM) 역할을 생성합니다.

1단계: 소스 구성

Security Lake는 다양한 소스와 AWS 계정 및 AWS 리전전반에서 로그 및 이벤트 데이터를 수집합니다. 다음 지침에 따라 Security Lake에서 수집하려는 데이터를 식별하십시오. 기본적으로 지원되는

AWS 서비스 를 소스로 추가할 때만 이 지침을 사용할 수 있습니다. 사용자 지정 소스 추가에 대한 자세한 내용은 Security Lake의 사용자 지정 소스에서 데이터 수집 섹션을 참조하세요.

로그 소스 수집을 구성하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 리전을 선택합니다. 온보딩 중에 현재 리전 및 기타 리전에서 Security Lake를 활성화할 수 있습니다.
3. Get started를 선택합니다.
4. 로그 및 이벤트 소스 선택에서 소스 선택에 대한 다음 옵션 중 하나를 선택합니다.
   a. 수집 기본 AWS 소스 - 권장 옵션을 선택하면 CloudTrail - S3 데이터 이벤트 및 AWS WAF 가 기본적으로 수집에 포함되지 않습니다. 이는 두 소스 유형을 대량으로 수집하면 사용 비용에 상당한 영향을 미칠 수 있기 때문입니다. 이러한 소스를 수집하려면 먼저 특정 AWS 소스 수집 옵션을 선택한 다음 로그 및 이벤트 소스 목록에서 이러한 소스를 선택합니다.
   b. 특정 AWS 소스 수집 -이 옵션을 사용하면 수집하려는 로그 및 이벤트 소스를 하나 이상 선택할 수 있습니다.

> **Note**
> 계정에서 Security Lake를 처음 활성화하면 선택한 모든 로그 및 이벤트 소스가 15일 무료 평가판에 포함됩니다. 사용량 통계에 대한 자세한 내용은 사용량 및 예상 비용 검토 섹션을 참조하세요.

5. 버전에서 로그 및 이벤트 소스를 수집할 데이터 소스의 버전을 선택합니다. 버전에 대한 자세한 내용은 OCSF 소스 식별을 참조하십시오.

> **Important**
> 지정된 리전에서 AWS 로그 소스의 새 버전을 활성화하는 데 필요한 역할 권한이 없는 경우 Security Lake 관리자에게 문의하세요. 자세한 내용은 역할 권한 업데이트를 참조하세요.

6. 리전 선택의 경우 지원되는 모든 리전 또는 특정 리전의 로그 및 이벤트 소스를 수집할지 여부를 선택합니다. 특정 리전을 선택하는 경우 데이터를 수집할 리전을 선택합니다.
7. 계정 선택에서 다음 단계를 수행합니다.

1. Security Lake가 조직의 모든 계정 또는 특정 계정에서 데이터를 수집할지 여부를 선택합니다. Security Lake는이 구성 중에 선택한 설정으로 이러한 계정에 대해 활성화됩니다.
2. 새 조직 계정에 대해 Security Lake 자동 활성화 확인란이 기본적으로 선택되어 있습니다. 이러한 자동 활성화 설정은 조직에 가입할 AWS 계정 때에 적용됩니다. 언제든지 자동 활성화 설정을 편집할 수 있습니다.

> **Note**
>
> 자동 활성화 설정은 기존 계정이 아닌 조직에 가입한 계정에만 적용됩니다. 자세한 내용은 콘솔에서 새 계정 구성 편집 단원을 참조하십시오.

8. 서비스에 액세스하려면 새 IAM 역할을 생성하거나 Security Lake에 소스에서 데이터를 수집하여 데이터 레이크에 추가할 수 있는 권한을 부여하는 기존 IAM 역할을 사용하십시오. Security Lake를 활성화한 모든 리전에서 하나의 역할이 사용됩니다.
9. 다음을 선택합니다.

2단계: 스토리지 설정 및 롤업 리전 정의(선택 사항)

Security Lake에서 데이터를 저장할 Amazon S3 스토리지 클래스와 저장 기간을 지정할 수 있습니다. 또한 롤업 리전을 지정하여 여러 리전의 데이터를 통합할 수 있습니다. 이 단계는 선택적 단계입니다. 자세한 내용은 Security Lake의 수명 주기 관리 단원을 참조하십시오.

스토리지 및 롤업 설정을 구성하려면

1. 여러 기여 리전의 데이터를 롤업 리전으로 통합하려면 롤업 리전 선택에서 롤업 리전 추가를 선택합니다. 롤업 리전과 이에 기여할 리전을 지정합니다. 하나 이상의 롤업 리전을 설정할 수 있습니다.
2. 스토리지 클래스 선택에서 Amazon S3 스토리지 클래스를 선택합니다. 기본 스토리지 클래스는 S3 Standard입니다. 해당 기간 이후에 데이터를 다른 스토리지 클래스로 전환하려는 경우 보존 기간 (일)을 입력하고 이전 추가를 선택합니다. 보존 기간이 끝나면 객체가 만료되고 Amazon S3에서 객체를 삭제합니다. Amazon S3 스토리지 클래스 및 보유에 대한 자세한 내용은 보존 관리을 참조하십시오.
3. 첫 단계에서 롤업 리전을 선택한 경우 서비스 액세스를 위해 새 IAM 역할을 생성하거나 Security Lake에 여러 리전에 데이터를 복제할 수 있는 권한을 부여하는 기존 IAM 역할을 사용하십시오.

4. 다음을 선택합니다.

3단계: 데이터 레이크 검토 및 생성

Security Lake가 데이터를 수집하는 소스, 롤업 리전 및 보존 설정을 검토하십시오. 그런 다음 데이터 레이크를 생성하세요.

데이터 레이크를 검토하고 생성하려면

1. Security Lake를 활성화하는 동안 로그 및 이벤트 소스, 리전, 롤업 리전, 스토리지 클래스를 검토하세요.
2. 생성(Create)을 선택합니다.

데이터 레이크를 생성한 후에는 Security Lake 콘솔에 요약 페이지가 표시됩니다. 이 페이지에서는 리전 및 롤업 리전 수, 구독자에 대한 정보 및 문제에 대한 개요를 제공합니다.

문제 메뉴에는 Security Lake 서비스 또는 Amazon S3 버킷에 영향을 미치는 지난 14일간의 문제에 대한 요약이 표시됩니다. 각 문제에 대한 자세한 내용은 Security Lake 콘솔의 문제 페이지를 참조하십시오.

4단계: 자체 데이터 보기 및 쿼리

데이터 레이크를 생성한 후 Amazon Athena 또는 유사한 서비스를 사용하여 AWS Lake Formation 데이터베이스 및 테이블에서 데이터를 보고 쿼리할 수 있습니다. 콘솔을 사용하는 경우 Security Lake가 Security Lake를 활성화하는 데 사용하는 역할에 데이터베이스 보기 권한을 자동으로 부여합니다. 최소한 역할에는 데이터 분석가 권한이 있어야 합니다. 권한 수준에 대한 자세한 내용은 Lake Formation 페르소나 및 IAM 권한 참조를 참조하십시오. SELECT 권한 부여에 대한 지침은 AWS Lake Formation 개발자 안내서의 명명된 리소스 방법을 사용하여 데이터 카탈로그 권한 부여를 참조하십시오.

5단계: 구독자 생성

데이터 레이크를 생성한 후 구독자를 추가하여 데이터를 사용할 수 있습니다. 구독자는 Amazon S3 버킷의 객체에 직접 액세스하거나 데이터 레이크를 쿼리하여 데이터를 사용할 수 있습니다. 구독자에 대한 자세한 내용은 Security Lake의 구독자 관리을 참조하십시오.

프로그래밍 방식으로 Security Lake 활성화

이 자습서에서는 프로그래밍 방식으로 Security Lake 사용을 활성화하고 시작하는 방법을 설명합니다. Amazon Security Lake API를 사용하면 Security Lake 계정, 데이터 및 리소스에 포괄적이고 프로그래밍 방식으로 액세스할 수 있습니다. 또는 AWS 명령줄 도구, AWS Command Line Interface 또는 AWS PowerShell용 도구 또는 AWS SDKs를 사용하여 Security Lake에 액세스할 수 있습니다.

1단계: IAM 역할 생성

프로그래밍 방식으로 Security Lake에 액세스하는 경우 데이터 레이크를 구성하려면 일부 AWS Identity and Access Management (IAM) 역할을 생성해야 합니다.

> **Important**
>
> Security Lake 콘솔을 사용하여 Security Lake를 활성화하고 구성하는 경우 이러한 IAM 역할을 생성할 필요가 없습니다.

이러한 작업을 하나 이상 수행하려는 경우 IAM에서 역할을 생성해야 합니다(각 작업의 IAM 역할에 대한 자세한 내용을 보려면 링크 선택).

- 사용자 지정 소스 생성 - 사용자 지정 소스는 데이터를 Security Lake로 전송하는 기본적으로 지원되지 않는 AWS 서비스 입니다.
- 데이터 액세스 권한이 있는 구독자 생성 — 권한이 있는 구독자는 데이터 레이크에서 S3 객체에 직접 액세스할 수 있습니다.
- 쿼리 액세스 권한이 있는 구독자 생성 — 권한이 있는 구독자는 Amazon Athena와 같은 서비스를 사용하여 Security Lake에서 데이터를 쿼리할 수 있습니다.
- 롤업 리전 구성 — 롤업 리전은 여러 AWS 리전의 데이터를 통합합니다.

앞서 언급한 역할을 생성한 후 Security Lake를 활성화하는 데 사용하는 역할에 AmazonSecurityLakeAdministrator AWS 관리형 정책을 연결합니다. 이 정책은 보안 주체가 Security Lake에 온보딩하고 모든 Security Lake 작업에 액세스할 수 있도록 허용하는 관리 권한을 부여합니다.

AmazonSecurityLakeMetaStoreManager AWS 관리형 정책을 연결하여 Security Lake에서 데이터 레이크를 생성하거나 데이터를 쿼리합니다. 이 정책은 Security Lake가 소스에서 수신하는 원시 로그 및 이벤트 데이터에 대한 추출, 변환 및 로드(ETL) 작업을 지원하는 데 필요합니다.

2단계: Amazon Security Lake 활성화

프로그래밍 방식으로 Security Lake를 활성화하려면 Security Lake API의 CreateDataLake 작업을 사용합니다. 를 사용하는 경우 create-data-lake 명령을 AWS CLI실행합니다. 요청 시 `configurations` 객체의 `region` 필드를 사용하여 Security Lake를 활성화할 리전의 리전 코드를 지정하십시오. 리전 코드 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오.

예시 1

다음 예제 명령은 `us-east-1` 및 `us-east-2` 리전에서 Security Lake를 활성화합니다. 두 리전 모두에서이 데이터 레이크는 Amazon S3 관리형 키로 암호화됩니다. 객체는 365일 후에 만료되고 객체는 60일 후에 `ONEZONE_IA` S3 스토리지 클래스로 전환됩니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":[{"days":60,"storageClass":"ONEZONE_IA"}]}},
 {"encryptionConfiguration": {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}]' \
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

예시 2

다음 예제 명령은 `us-east-2` 리전에서 Security Lake를 활성화합니다. 이 데이터 레이크는 AWS Key Management Service ()에서 생성된 고객 관리형 키로 암호화됩니다AWS KMS. 객체는 500일 후에 만료되고 객체는 30일 후에 `GLACIER` S3 스토리지 클래스로 전환됩니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"1234abcd-12ab-34cd-56ef-1234567890ab"},"region":"us-
east-2","lifecycleConfiguration": {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"GLACIER"}]}}]' \
--meta-store-manager-role-arn "arn:aws:iam:us-east-1:123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

> **Note**
>
> Security Lake를 이미 활성화하고 리전 또는 소스의 구성 설정을 업데이트하려는 경우 UpdateDataLake 작업을 사용하거나를 사용하는 경우 AWS CLIupdate-data-lake 명령을 사용합니다. `CreateDataLake` 작업을 사용하지 마십시오.

3단계: 소스 구성

Security Lake는 다양한 소스와 AWS 계정 및 AWS 리전전반에서 로그 및 이벤트 데이터를 수집합니다. 다음 지침에 따라 Security Lake에서 수집하려는 데이터를 식별하십시오. 기본적으로 지원되는 AWS 서비스 를 소스로 추가할 때만 이 지침을 사용할 수 있습니다. 사용자 지정 소스 추가에 대한 자세한 내용은 Security Lake의 사용자 지정 소스에서 데이터 수집 섹션을 참조하세요.

프로그래밍 방식으로 컬렉션 소스를 하나 이상 정의하려면 Security Lake API의 CreateAwsLogSource 작업을 사용하십시오. 각 소스에 대해 `sourceName` 파라미터에 리전별로 고유한 값을 지정하십시오. 선택적으로 추가 파라미터를 사용하여 소스의 범위를 특정 계정 (`accounts`) 또는 특정 버전 (`sourceVersion`)으로 제한할 수 있습니다.

> **Note**
>
> 요청에 선택적 파라미터를 포함하지 않는 경우 Security Lake는 제외하는 파라미터에 따라 지정된 소스의 모든 계정 또는 모든 버전에 요청을 적용합니다. 예를 들어 조직의 Security Lake 위임 관리자인데 `accounts` 파라미터를 제외하면 Security Lake는 조직 내 모든 계정에 요청을 적용합니다. 마찬가지로 `sourceVersion` 파라미터를 제외하면 Security Lake는 요청을 지정된 소스의 모든 버전에 적용합니다.

요청에 Security Lake를 활성화하지 않은 리전이 지정된 경우 오류가 발생합니다. 이 오류를 해결하려면 Security Lake를 활성화한 리전만 `regions` 배열에 지정해야 합니다. 또는 리전에서 Security Lake를 활성화한 후 다시 요청을 제출할 수 있습니다.

계정에서 Security Lake를 처음 활성화하면 선택한 모든 로그 및 이벤트 소스가 15일 무료 평가판에 포함됩니다. 사용량 통계에 대한 자세한 내용은 사용량 및 예상 비용 검토 섹션을 참조하세요.

4단계: 스토리지 설정 및 롤업 리전 구성(선택 사항)

Security Lake에서 데이터를 저장할 Amazon S3 스토리지 클래스와 저장 기간을 지정할 수 있습니다. 또한 롤업 리전을 지정하여 여러 리전의 데이터를 통합할 수 있습니다. 이 단계는 선택적 단계입니다. 자세한 내용은 Security Lake의 수명 주기 관리 단원을 참조하십시오.

Security Lake를 활성화할 때 프로그래밍 방식으로 대상 목표를 정의하려면 Security Lake API의 CreateDataLake 작업을 사용합니다. Security Lake를 이미 활성화했고 대상 목표를 정의하려는 경우 UpdateDataLake 작업이 아닌 `CreateDataLake` 작업을 사용합니다.

어느 작업이든 지원되는 파라미터를 사용하여 원하는 구성 설정을 지정하십시오.

- 롤업 리전을 지정하려면 `region` 필드를 사용하여 롤업 리전에 데이터를 제공할 리전을 지정합니다. `replicationConfiguration` 객체의 `regions` 배열에서 각 롤업 리전의 리전 코드를 지정합니다. 리전 코드 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오.
- 데이터의 보존 설정을 지정하려면 `lifecycleConfiguration` 파라미터를 사용하세요.
  - `transitions`의 경우 특정 Amazon S3 스토리지 클래스 (`storageClass`)에 S3 객체를 저장할 총 일수 (`days`)를 지정합니다.
  - `expiration`의 경우, 객체를 생성한 후 임의의 스토리지 클래스를 사용하여 Amazon S3에 객체를 저장할 총 일수를 지정합니다. 이 보존 기간이 끝나면 객체가 만료되고 Amazon S3에서 객체를 삭제합니다.

  Security Lake는 지정된 보존 설정을 `configurations` 객체의 `region` 필드에 지정한 리전에 적용합니다.

예를 들어 다음 명령은를 롤업 리전`ap-northeast-2`으로 사용하여 데이터 레이크를 생성합니다. `us-east-1` 리전은 `ap-northeast-2` 리전에 데이터를 제공합니다. 또한이 예제에서는 데이터 레이크에 추가되는 객체에 대해 10일의 만료 기간을 설정합니다.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-2"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":10}}}]' \
--meta-store-manager-role-arn "arn:aws:iam::123456789012:role/service-role/
AmazonSecurityLakeMetaStoreManager"
```

이제 데이터 레이크를 생성했습니다. Security Lake API의 ListDataLakes 작업을 사용하여 각 리전에서 Security Lake 및 데이터 레이크 설정의 활성화를 확인합니다.

데이터 레이크 생성 시 문제나 오류가 발생하면 ListDataLakeExceptions 작업을 사용하여 예외 목록을 보고 CreateDataLakeExceptionSubscription 작업의 예외를 사용자에게 알릴 수 있습니다. 자세한 내용은 데이터 레이크 상태 문제 해결 단원을 참조하십시오.

5단계: 자체 데이터 보기 및 쿼리

데이터 레이크를 생성한 후 Amazon Athena 또는 유사한 서비스를 사용하여 AWS Lake Formation 데이터베이스 및 테이블에서 데이터를 보고 쿼리할 수 있습니다. 프로그래밍 방식으로 Security Lake를 활성화하면 데이터베이스 보기 권한이 자동으로 부여되지 않습니다. 의 데이터 레이크 관리자 계정은 관련 데이터베이스 및 테이블을 쿼리하는 데 사용할 IAM 역할에 SELECT 권한을 부여해야 AWS Lake Formation 합니다. 최소한 역할에는 데이터 분석가 권한이 있어야 합니다. 권한 수준에 대한 자세한 내용은 Lake Formation 페르소나 및 IAM 권한 참조를 참조하십시오. SELECT 권한 부여에 대한 지침은 AWS Lake Formation 개발자 안내서의 명명된 리소스 방법을 사용하여 데이터 카탈로그 권한 부여를 참조하십시오.

6단계: 구독자 생성

데이터 레이크를 생성한 후 구독자를 추가하여 데이터를 사용할 수 있습니다. 구독자는 Amazon S3 버킷의 객체에 직접 액세스하거나 데이터 레이크를 쿼리하여 데이터를 사용할 수 있습니다. 구독자에 대한 자세한 내용은 Security Lake의 구독자 관리을 참조하십시오.

Security Lake AWS Organizations 에서를 사용하여 여러 계정 관리

Amazon Security Lake를 사용하여 여러 개의 AWS 계정로부터 보안 로그와 이벤트를 수집할 수 있습니다. 여러 계정의 관리를 자동화하고 간소화하려면 Security Lake와 AWS Organizations통합하는 것이 좋습니다.

조직에서 조직을 만드는 데 사용하는 계정을 관리 계정이라고 합니다. Security Lake를 Organizations와 통합하려면 관리 계정에 조직의 위임된 Security Lake 관리자 계정을 지정해야 합니다.

위임된 Security Lake 관리자는 Security Lake를 활성화하고 멤버 계정에 대한 Security Lake 설정을 구성할 수 있습니다. 위임된 관리자는 Security Lake가 활성화된 모든 AWS 리전 의 조직 전체에서 로그와 이벤트를 수집할 수 있습니다(현재 사용 중인 리전 엔드포인트에 관계없이). 또한 위임된 관리자는 새 조직 계정의 로그 및 이벤트 데이터를 자동으로 수집하도록 Security Lake를 구성할 수 있습니다.

위임된 Security Lake 관리자는 연결된 멤버 계정의 로그 및 이벤트에 액세스할 수 있습니다. 따라서 연결된 멤버 계정이 소유한 데이터를 수집하도록 Security Lake를 구성할 수 있습니다. 연결된 멤버 계정이 소유한 데이터를 사용할 수 있는 권한을 구독자에게 부여할 수도 있습니다.

조직의 여러 계정에 대해 Security Lake를 사용하도록 설정하려면 먼저 조직 관리 계정이 조직의 위임된 Security Lake 관리자 계정을 지정해야 합니다. 그러면 위임된 관리자가 조직에 대해 Security Lake를 활성화하고 구성할 수 있습니다.

> **Important**
>
> Security Lake의 RegisterDataLakeDelegatedAdministrator API를 사용하여 조직에 대한 Security Lake 액세스를 허용하고 Organizations의 위임된 관리자를 등록합니다. Organizations의 API를 사용하여 위임된 관리자를 등록하는 경우 Organizations에 대한 서비스 연결 역할이 성공적으로 생성되지 않을 수 있습니다. 전체 기능을 보장하려면 Security Lake API를 사용합니다.

자세한 내용은 AWS Organizations 사용 설명서에서 조직 생성 및 관리를 참조하세요.

> **기존 Security Lake 계정의 경우**
>
> 2025년 4월 17일 이전에 Security Lake를 활성화한 경우를 활성화하는 것이 좋습니다리소스 관리를 위한 서비스 연결 역할(SLR) 권한. 이 SLR을 사용하면 지속적인 모니터링 및 성능 개선

을 계속 수행하여 지연 시간과 비용을 줄일 수 있습니다. 이 SLR과 연결된 권한에 대한 자세한 내용은 섹션을 참조하세요리소스 관리를 위한 서비스 연결 역할(SLR) 권한.
Security Lake 콘솔을 사용하는 경우를 활성화하라는 알림이 표시됩니다 AWSServiceRoleForSecurityLakeResourceManagement. 를 사용하는 경우 Security Lake 서비스 연결 역할 생성을 AWS CLI참조하세요.

위임된 Security Lake 관리자를 위한 중요 고려 사항

Security Lake에서 위임된 관리자의 행동 방식을 정의하는 다음 요소에 유의하세요.

위임된 관리자는 모든 리전에서 동일합니다.

위임된 관리자를 생성하면 Security Lake를 활성화한 모든 리전의 위임 관리자가 됩니다.

로그 아카이브 계정을 Security Lake의 위임 관리자로 설정하는 것이 좋습니다.

로그 아카이브 계정은 모든 보안 관련 로그를 수집하고 보관 AWS 계정 하는 전용 입니다. 이 계정에 대한 액세스는 일반적으로 규정 준수 조사를 위한 감사자 및 보안 팀과 같은 소수의 사용자로 제한됩니다. 컨텍스트 전환을 최소화하면서 보안 관련 로그와 이벤트를 볼 수 있도록 로그 아카이브 계정을 Security Lake의 위임 관리자로 설정하는 것이 좋습니다.

또한 최소한의 사용자만 로그 아카이브 계정에 직접 액세스할 수 있도록 하는 것이 좋습니다. 이 선택 그룹 외부에서 Security Lake가 수집하는 데이터에 액세스해야 하는 사용자는 해당 사용자를 Security Lake 구독자로 추가할 수 있습니다. 구독자 추가에 대한 자세한 내용은 Security Lake의 구독자 관리을 참조하십시오.

AWS Control Tower 서비스를 사용하지 않는 경우 로그 아카이브 계정이 없을 수 있습니다. 로그 아카이브 계정에 대한 자세한 내용은 AWS 보안 참조 아키텍처의 보안 OU — 로그 아카이브 계정을 참조하십시오.

조직의 위임 관리자는 한 명입니다.

각 조직에 위임된 Security Lake 관리자는 한 명만 둘 수 있습니다.

조직의 관리 계정은 위임된 관리자가 될 수 없습니다.

AWS 보안 모범 사례와 최소 권한 원칙에 따라 조직 관리 계정은 위임된 관리자가 될 수 없습니다.

위임된 관리자는 유효한 조직의 일원이어야 합니다.

> 조직을 삭제하면 위임된 관리자 계정으로 더 이상 Security Lake를 관리할 수 없습니다. 다른 조직의 위임 관리자를 지정하거나 조직에 속하지 않은 독립 실행형 계정으로 Security Lake를 사용해야 합니다.

위임 관리자를 지정하는 데 필요한 IAM 권한

위임된 Security Lake 관리자를 지정할 때는 Security Lake를 활성화하고 다음 정책 설명에 나열된 특정 AWS Organizations API 작업을 사용할 수 있는 권한이 있어야 합니다.

AWS Identity and Access Management (IAM) 정책의 끝에 다음 문을 추가하여 이러한 권한을 부여할 수 있습니다.

```
{
    "Sid": "Grant permissions to designate a delegated Security Lake administrator",
    "Effect": "Allow",
    "Action": [
        "securitylake:RegisterDataLakeDelegatedAdministrator",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListAccounts",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

위임된 Security Lake 관리자 지정 및 회원 계정 추가

액세스 방법을 선택하여 조직에 대해 위임된 Security Lake 관리자 계정을 지정할 수 있습니다. 조직의 관리 계정만 조직에 대해 위임된 관리자 계정을 지정할 수 있습니다. 조직 관리 계정은 해당 조직의 위임된 관리자 계정이 될 수 없습니다.

> **Note**
>
> - 조직 관리 계정은 Security Lake `RegisterDataLakeDelegatedAdministrator` 작업을 사용하여 위임된 Security Lake 관리자 계정을 지정해야 합니다. Organizations를 통해 위임된 Security Lake 관리자를 지정하는 것은 지원되지 않습니다.
> - 조직의 위임된 관리자를 변경하려면 먼저 현재 위임된 관리자를 제거해야 합니다. 그런 다음 위임된 관리자를 새로 지정할 수 있습니다.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.

   조직에 대한 관리 계정의 자격 증명을 사용하여 로그인합니다.

2. - Security Lake가 아직 활성화되지 않은 경우 시작하기를 선택한 다음 Security Lake 활성화 페이지에서 위임된 Security Lake 관리자를 지정합니다.
   - Security Lake가 이미 활성화된 경우 설정 페이지에서 위임된 Security Lake 관리자를 지정하십시오.
3. 다른 계정에 관리 위임에서 이미 다른 AWS 보안 서비스의 위임된 관리자 역할을 하는 계정을 선택합니다(권장). 또는 위임된 Security Lake 관리자로 지정하려는 계정의 12자리 AWS 계정 ID를 입력합니다.
4. 위임을 선택합니다. Security Lake가 아직 활성화되지 않은 경우 위임된 관리자를 지정하면 현재 리전의 해당 계정에 대해 Security Lake가 활성화됩니다.

API

위임된 관리자를 프로그래밍 방식으로 지정하려면 Security Lake API의 RegisterDataLakeDelegatedAdministrator 작업을 사용합니다. 조직 관리 계정에서 작업을 호출해야 합니다. 를 사용하는 경우 조직 관리 계정에서 register-data-lake-delegated-administrator 명령을 AWS CLI실행합니다. 요청에서 `accountId` 파라미터를 사용하여 조직의 위임된 관리자 계정으로 AWS 계정 지정할의 12자리 계정 ID를 지정합니다.

예를 들어 다음 AWS CLI 명령은 위임된 관리자를 지정합니다. 이 예제는 Linux, macOS 또는 Unix 용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake register-data-lake-delegated-administrator \
```

```
--account-id 123456789012
```

위임된 관리자는 새 조직 계정의 AWS 로그 및 이벤트 데이터 수집을 자동화하도록 선택할 수도 있습니다. 이 구성을 사용하면 계정이 조직에 추가될 때 새 계정에서 Security Lake가 자동으로 활성화됩니다 AWS Organizations. 위임된 관리자는 Security Lake API의 CreateDataLakeOrganizationConfiguration 작업을 사용하거나 AWS CLI를 사용하는 경우 create-data-lake-organization-configuration 명령을 실행하여이 구성을 활성화할 수 있습니다. 요청 시 새 계정에 대한 특정 구성 설정을 지정할 수도 있습니다.

예를 들어 다음 AWS CLI 명령은 새 조직 계정에서 Security Lake와 Amazon Route 53 해석기 쿼리 로그, AWS Security Hub 조사 결과 및 Amazon Virtual Private Cloud(Amazon VPC) 흐름 로그 모음을 자동으로 활성화합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake create-data-lake-organization-configuration \
--auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"ROUTE53"},{"sourceName":"SH_FINDINGS"},{"sourceName":"VPC_FLOW"}]}]'
```

조직 관리 계정이 위임된 관리자를 지정한 후 관리자는 조직에 대해 Security Lake를 활성화 및 구성할 수 있습니다. 여기에는 조직의 개별 계정에 대한 AWS 로그 및 이벤트 데이터를 수집하도록 Security Lake를 활성화하고 구성하는 작업이 포함됩니다. 자세한 내용은 Security Lake AWS 서비스 에서 데이터 수집 단원을 참조하십시오.

GetDataLakeOrganizationConfiguration 작업을 사용하여 새 멤버 계정에 대한 조직의 현재 구성에 대한 세부 정보를 가져올 수 있습니다.

새 조직 계정에 대한 자동 활성화 구성 편집

위임된 Security Lake 관리자는 조직에 가입할 때 계정에 대한 자동 활성화 설정을 보고 편집할 수 있습니다. Security Lake는 기존 계정이 아닌 새 계정에 대해서만 이러한 설정을 기반으로 데이터를 수집합니다.

다음 단계에 따라 새 조직 계정의 구성을 편집합니다.

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 Accounts(계정)를 선택합니다.
3. 계정 페이지에서 새 계정 구성 섹션을 확장합니다. 각 리전에서 수집하는 소스 Security Lake를 볼 수 있습니다.

4. 편집을 선택하여이 구성을 편집합니다.
5. 새 계정 구성 편집 페이지에서 다음 단계를 수행합니다.
   a. 리전 선택에서 데이터를 수집할 소스를 업데이트할 리전을 하나 이상 선택합니다. 그리고 다음을 선택합니다.
   b. 소스 선택에서 소스 선택에 대한 다음 옵션 중 하나를 선택합니다.
      i. 수집 기본 AWS 소스 - 권장 옵션을 선택하면 CloudTrail - S3 데이터 이벤트 AWS WAF 가 기본적으로 수집에 포함되지 않습니다. 이는 두 소스 유형을 대량으로 수집하면 사용 비용에 상당한 영향을 미칠 수 있기 때문입니다. 이러한 소스를 수집하려면 먼저 특정 AWS 소스 수집 옵션을 선택한 다음 로그 및 이벤트 소스 목록에서 이러한 소스를 선택합니다.
      ii. 특정 AWS 소스 수집 -이 옵션을 사용하면 수집하려는 로그 및 이벤트 소스를 하나 이상 선택할 수 있습니다.
      iii. 소스 수집 안 함 - 이전 단계에서 선택한 리전에서 소스를 수집하지 않으려면이 옵션을 선택합니다.
      iv. 다음을 선택합니다.

      > **Note**
      > 계정에서 Security Lake를 처음 활성화하면 선택한 모든 로그 및 이벤트 소스가 15일 무료 평가판에 포함됩니다. 사용량 통계에 대한 자세한 내용은 사용량 및 예상 비용 검토 섹션을 참조하세요.

   c. 변경 사항을 검토한 후 적용을 선택합니다.

      가 조직에 AWS 계정 가입하면 이러한 설정이 기본적으로 해당 계정에 적용됩니다.

위임된 Security Lake 관리자 제거

조직 관리 계정만 조직에 대해 위임된 Security Lake 관리자를 제거할 수 있습니다. 조직의 위임된 관리자를 변경하려면 현재 위임된 관리자를 제거한 다음 새로 위임된 관리자를 지정하십시오.

> **Important**
> 위임된 Security Lake 관리자를 제거하면 데이터 레이크가 삭제되고 조직 내 계정에 대한 Security Lake가 비활성화됩니다.

Security Lake 콘솔을 사용하여 위임된 관리자를 변경하거나 제거할 수 없습니다. 이러한 작업은 프로그래밍 방식으로만 수행할 수 있습니다.

프로그래밍 방식으로 위임된 관리자를 제거하려면 Security Lake API의 DeregisterDataLakeDelegatedAdministrator 작업을 사용합니다. 조직 관리 계정에서 작업을 호출해야 합니다. 를 사용하는 경우 조직 관리 계정에서 deregister-data-lake-delegated-administrator 명령을 AWS CLI실행합니다.

예를 들어 다음 AWS CLI 명령은 위임된 Security Lake 관리자를 제거합니다.

```
$ aws securitylake deregister-data-lake-delegated-administrator
```

위임된 관리자 지정을 유지하고 새 멤버 계정의 자동 구성 설정을 변경하려면 Security Lake API의 DeleteDataLakeOrganizationConfiguration 작업을 사용하거나를 사용하는 경우 AWS CLIdelete-data-lake-organization-configuration 명령을 사용합니다. 위임된 관리자만 조직에 대한 이러한 설정을 변경할 수 있습니다.

예를 들어 다음 AWS CLI 명령은 조직에 가입한 새 멤버 계정에서 Security Hub 조사 결과의 자동 수집을 중지합니다. 위임된 관리자가이 작업을 호출한 후에는 새 멤버 계정이 Security Hub 조사 결과를 데이터 레이크에 기여하지 않습니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake delete-data-lake-organization-configuration \
--auto-enable-new-account '[{"region":"us-east-1","sources":
[{"sourceName":"SH_FINDINGS"}]}]'
```

Security Lake의 신뢰할 수 있는 액세스

조직에 대해 Security Lake를 설정한 후 AWS Organizations 관리 계정은 Security Lake를 통해 신뢰할 수 있는 액세스를 활성화할 수 있습니다. 신뢰할 수 있는 액세스를 통해 Security Lake는 IAM 서비스 연결 역할을 생성하고 사용자를 대신해 조직과 그 계정의 작업을 수행합니다. 자세한 내용은 AWS Organizations 사용 설명서에서 다른 AWS 서비스와 함께 AWS Organizations 사용을 참조하세요.

조직 관리 계정의 사용자는 AWS Organizations에서 보안 레이크에 대한 신뢰할 수 있는 액세스를 비활성화할 수 있습니다. 신뢰할 수 있는 액세스를 비활성화하는 방법에 대한 지침은 AWS Organizations 사용 설명서의 신뢰할 수 있는 액세스를 활성화 또는 비활성화하는 방법을 참조하십시오.

위임된 관리자의 AWS 계정 가 일시 중지, 격리 또는 종료된 경우 신뢰할 수 있는 액세스를 비활성화하는 것이 좋습니다.

Security Lake의 리전 관리

Amazon Security Lake는 서비스를 활성화한 AWS 리전 에서 보안 로그 및 이벤트를 수집할 수 있습니다. 리전별로 데이터가 다른 Amazon S3 버킷에 저장됩니다. 리전별로 다른 데이터 레이크 구성 (예: 다른 소스 및 보존 설정)을 지정할 수 있습니다. 또한 하나 이상의 롤업 리전을 정의하여 여러 리전의 데이터를 통합할 수 있습니다.

리전 상태 확인

Security Lake는 여러 AWS 리전전체에서 데이터를 수집할 수 있습니다. 데이터 레이크의 상태를 추적하려면 각 리전이 현재 어떻게 구성되어 있는지 이해하는 것이 도움이 될 수 있습니다. 원하는 액세스 방법을 선택하고 다음 단계에 따라 해당 리전의 현재 상태를 확인하십시오.

Console

리전 상태를 확인하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 리전을 선택합니다. 현재 Security Lake가 활성화된 리전의 개요를 제공하는 리전 페이지가 나타납니다.
3. 리전을 선택한 다음 편집을 선택하여 해당 리전의 세부 정보를 확인합니다.

API

현재 리전에서 로그 수집 상태를 가져오려면 Security Lake API의 GetDataLakeSources 작업을 사용합니다. 를 사용하는 경우 get-data-lake-sources 명령을 AWS CLI실행합니다. `accounts` 파라미터의 경우 하나 이상의 AWS 계정 IDs 목록으로 지정합니다. 요청이 성공하면 Security Lake는 Security Lake가 데이터를 수집하는 AWS 소스와 각 소스의 상태를 포함하여 현재 리전의 해당 계정에 대한 스냅샷을 반환합니다. `accounts` 파라미터를 포함하지 않으면 응답에는 현재 리전에서 Security Lake가 구성된 모든 계정에 대한 로그 수집 상태가 포함됩니다.

예를 들어 다음 AWS CLI 명령은 현재 리전에서 지정된 계정의 로그 수집 상태를 검색합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake get-data-lake-sources \
--accounts "123456789012" "111122223333"
```

다음 AWS CLI 명령은 지정된 리전의 모든 계정 및 활성화된 소스에 대한 로그 수집 상태를 나열합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시 (\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake get-data-lake-sources \
--regions "us-east-1" \
--query 'dataLakeSources[].[account,sourceName]'
```

리전에 대해 Security Lake를 활성화했는지 확인하려면 ListDataLakes 작업을 사용합니다. 를 사용하는 경우 list-data-lakes 명령을 AWS CLI실행합니다. `regions` 파라미터에는 리전에 대한 리전 코드를 지정합니다 (예: 미국 동부 (버지니아 북부 리전용`us-east-1`). 리전 코드 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오. `ListDataLakes` 작업은 요청에서 지정한 각 리전의 데이터 레이크 구성 설정을 반환합니다. 리전을 지정하지 않으면 Security Lake는 Security Lake를 사용할 수 있는 각 리전에서 데이터 레이크의 상태 및 구성 설정을 반환합니다.

예를 들어 다음 AWS CLI 명령은 `eu-central-1` 리전에 있는 데이터 레이크의 상태 및 구성 설정을 보여줍니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake list-data-lakes \
--regions "us-east-1" "eu-central-1"
```

리전 설정 변경

원하는 방법을 선택하고 이 지침에 따라 하나 이상의 AWS 리전에서 데이터 레이크 설정을 업데이트하십시오.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 리전을 선택합니다.
3. 리전을 선택한 다음 편집을 선택합니다.
4. <리전>에서 모든 계정의 소스 재정의 확인란을 선택하여 여기에서 선택한 내용이 이 리전에 대한 이전 선택 사항보다 우선 적용되는지 확인하십시오.
5. 스토리지 클래스 선택에서 전환 추가를 선택하여 데이터에 새 스토리지 클래스를 추가합니다.

6. 태그의 경우 필요에 따라 리전에 태그를 할당하거나 편집할 수 있습니다. 태그는 특정 리전의 에 대한 데이터 레이크 구성을 포함하여 특정 유형의 AWS 리소스 AWS 계정 에 정의 및 할당할 수 있는 레이블입니다. 자세한 내용은 Security Lake 리소스에 태그 지정을 참조하십시오.
7. 리전을 롤업 리전으로 전환하려면 탐색 창에서 롤업 리전 (설정 아래)을 선택합니다. 그런 다음 Modify(수정)를 선택합니다. 롤업 리전 선택 섹션에서 롤업 리전 추가를 선택합니다. 기여 리전을 선택하고 Security Lake에 여러 리전에 걸쳐 데이터를 복제할 수 있는 권한을 부여합니다. 완료 시 저장을 선택하여 변경 사항을 저장합니다.

API

프로그래밍 방식으로 데이터 레이크의 리전 설정을 업데이트하려면 Security Lake API의 UpdateDataLake 작업을 사용합니다. 를 사용하는 경우 update-data-lake 명령을 AWS CLI실행합니다. `region` 파라미터에는 설정을 변경하려는 리전에 대한 리전 코드를 지정합니다(예: 미국 동부 (버지니아 북부) 리전에 대한 `us-east-1`). 리전 코드 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오.

추가 파라미터를 사용하여 변경하려는 각 설정에 대해 새 값을 지정합니다 (예: 암호화 키 (`encryptionConfiguration`) 및 보존 설정 (`lifecycleConfiguration`)).

예를 들어 다음 AWS CLI 명령은 `us-east-1` 리전의 데이터 만료 및 스토리지 클래스 전환 설정을 업데이트합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ update-data-lake \
--configurations '[{"region":"us-east-1","lifecycleConfiguration": {"expiration":
{"days":500},"transitions":[{"days":45,"storageClass":"ONEZONE_IA"}]}}]'
```

Security Lake에서 롤업 리전 구성

롤업 리전은 하나 이상의 기여 리전의 데이터를 통합합니다. 롤업 리전을 지정하면 리전 규정 준수 요구 사항을 준수하는 데 도움이 될 수 있습니다.

Amazon S3의 제한으로 인해 고객 관리형 키(CMK) 암호화된 리전 데이터 레이크에서 S3 관리형 암호화된(기본 암호화) 리전 데이터 레이크로의 복제는 지원되지 않습니다.

> **Important**
>
> 사용자 지정 소스를 생성한 경우 사용자 지정 소스 데이터가 대상에 올바르게 복제되도록 하기 위해 Security Lake는 사용자 지정 소스 수집 모범 사례에 설명된 모범 사례를 따를 것을 권장합니다. 페이지에 설명된 S3 파티션 데이터 경로 형식을 따르지 않는 데이터에서는 복제를 수행할 수 없습니다.

롤업 리전을 추가하기 전에 먼저 AWS Identity and Access Management (IAM) 에서 두 가지 역할을 생성해야 합니다.

- 데이터 복제를 위한 IAM 역할
- AWS Glue 파티션을 등록하기 위한 IAM 역할

> **Note**
>
> Security Lake 콘솔을 사용할 때 Security Lake는 사용자를 대신하여 이러한 IAM 역할을 생성하거나 기존 역할을 사용합니다. 그러나 Security Lake API 또는를 사용할 때는 이러한 역할을 생성해야 합니다 AWS CLI.

데이터 복제를 위한 IAM 역할

이 IAM 역할은 Amazon S3에 여러 리전에 걸쳐 소스 로그와 이벤트를 복제할 수 있는 권한을 부여합니다.

이러한 권한을 부여하려면 접두사 `SecurityLake`로 시작하는 IAM 역할을 생성하고 다음 샘플 정책을 역할에 연결해야 합니다. Security Lake에서 롤업 리전을 생성할 때 역할의 Amazon 리소스 이름 (ARN) 이 필요합니다. 이 정책에서 `sourceRegions`는 기여 `destinationRegions` 리전이며 롤업 리전입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadS3ReplicationSetting",
      "Action": [
        "s3:ListBucket",
        "s3:GetReplicationConfiguration",
```

```
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectRetention",
        "s3:GetObjectLegalHold"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-[[sourceRegions]]*",
        "arn:aws:s3:::aws-security-data-lake-[[sourceRegions]]*/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:ResourceAccount": [
            "{{bucketOwnerAccountId}}"
          ]
        }
      }
    },
    {
      "Sid": "AllowS3Replication",
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateDelete",
        "s3:ReplicateTags",
        "s3:GetObjectVersionTagging"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake-[[destinationRegions]]*/*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:ResourceAccount": [
            "{{bucketOwnerAccountId}}"
          ]
        }
      }
    }
  ]
}
```

다음 신뢰 정책을 역할에 첨부하여 Amazon S3가 역할을 맡을 수 있도록 허용합니다:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3ToAssume",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

AWS Key Management Service (AWS KMS)의 고객 관리형 키를 사용하여 Security Lake 데이터 레이크를 암호화하는 경우 데이터 복제 정책의 권한 외에도 다음 권한을 부여해야 합니다.

```
{
    "Action": [
        "kms:Decrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
                "s3.{sourceRegion1}.amazonaws.com",
                "s3.{sourceRegion2}.amazonaws.com"
                ],
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::aws-security-data-lake-{sourceRegion1}*",
                "arn:aws:s3:::aws-security-data-lake-{sourceRegion2}*"
            ]
        }
    },
    "Resource": [
        "{sourceRegion1KmsKeyArn}",
        "{sourceRegion2KmsKeyArn}"
    ]
},
{
    "Action": [
```

```
        "kms:Encrypt"
    ],
    "Effect": "Allow",
    "Condition": {
        "StringLike": {
            "kms:ViaService": [
            "s3.{destinationRegion1}.amazonaws.com",
            ],
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::aws-security-data-lake-{destinationRegion1}*",
            ]
        }
    },
    "Resource": [
            "{destinationRegionKmsKeyArn}"
    ]
}
```

복제 역할에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 권한 설정을 참조하세요.

AWS Glue 파티션을 등록하기 위한 IAM 역할

이 IAM 역할은 Security Lake에서 다른 리전에서 복제된 S3 객체에 대한 파티션을 등록하는 데 사용하는 AWS Glue 파티션 업데이터 AWS Lambda 함수에 대한 권한을 부여합니다. 이 역할을 생성하지 않으면 구독자는 해당 객체의 이벤트를 쿼리할 수 없습니다.

이러한 권한을 부여하려면 `AmazonSecurityLakeMetaStoreManager`라는 이름이 지정된 역할을 생성해야 합니다 (Security Lake에 온보딩하는 동안 이 역할을 이미 생성했을 수 있음). 샘플 정책을 포함하여 이 역할에 대한 자세한 내용은 1단계: IAM 역할 생성을 참조하십시오.

Lake Formation 콘솔에서는 다음 단계에 따라 데이터 레이크 관리자로서 `AmazonSecurityLakeMetaStoreManager` 권한도 부여해야 합니다.

1. Lake Formation 콘솔(https://console.aws.amazon.com/lakeformation/)을 엽니다.
2. 관리 사용자로 로그인
3. Welcome to Lake Formation 창이 나타나면 1단계에서 생성하거나 선택한 사용자를 선택한 다음 시작하기를 선택합니다.
4. Welcome to Lake Formation 창이 표시되지 않는 경우 다음 단계를 수행하여 Lake Formation 관리자를 구성하십시오.

1. 탐색 창의 권한 아래에서 관리 역할 및 작업을 선택합니다. 콘솔 페이지의 데이터 레이크 관리자 섹션에서 관리자 선택을 선택합니다.
2. 데이터 레이크 관리자 관리 대화 상자에서 IAM 사용자 및 역할에 대해 생성한 AmazonSecurityLakeMetaStoreManager IAM 역할을 선택한 다음 저장을 선택합니다.

데이터 레이크 관리자의 권한 변경에 대한 자세한 내용은 AWS Lake Formation 개발자 가이드의 데이터 레이크 관리자 생성을 참조하십시오.

롤업 리전 추가

원하는 액세스 방법을 선택하고 다음 단계에 따라 롤업 리전을 추가하세요.

> **Note**
> 리전은 여러 롤업 리전에 데이터를 제공할 수 있습니다. 하지만 롤업 리전은 다른 롤업 리전의 기여 리전이 될 수 없습니다.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창의 설정 아래에서 롤업 리전을 선택합니다.
3. 수정을 선택한 다음 롤업 리전 추가를 선택합니다.
4. 롤업 리전 및 기여 리전을 지정합니다. 여러 롤업 리전을 추가하려면 이 단계를 반복합니다.
5. 롤업 리전을 처음 추가하는 경우 서비스 액세스를 위해 새 IAM 역할을 생성하거나 Security Lake에 여러 리전에 걸쳐 데이터를 복제할 수 있는 권한을 부여하는 기존 IAM 역할을 사용하십시오.
6. 마쳤으면 저장을 선택합니다.

Security Lake에 온보딩할 때 롤업 리전을 추가할 수도 있습니다. 자세한 내용은 Amazon Security Lake 시작하기 단원을 참조하십시오.

API

프로그래밍 방식으로 롤업 리전을 추가하려면 Security Lake API의 UpdateDataLake 작업을 사용합니다. 를 사용하는 경우 update-data-lake 명령을 AWS CLI실행합니다. 요청 시 `region` 필드를 사용하여 롤업 리전에 데이터를 제공할 리전을 지정하십시오. `replicationConfiguration` 파

라미터 `regions` 배열에서 각 롤업 리전의 리전 코드를 지정합니다. 리전 코드 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오.

예를 들어 다음 명령은를 롤업 리전`ap-northeast-2`으로 설정합니다. `us-east-1` 리전은 `ap-northeast-2` 리전에 데이터를 제공합니다. 또한이 예제에서는 데이터 레이크에 추가된 객체에 대해 365일의 만료 기간을 설정합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-2"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":365}}}]'
```

Security Lake에 온보딩할 때 롤업 리전을 추가할 수도 있습니다. 이렇게 하려면 CreateDataLake 작업을 사용합니다(또는를 사용하는 경우 AWS CLIcreate-data-lake 명령). 온보딩 중 롤업 리전 구성에 대한 자세한 내용은 섹션을 참조하세요Amazon Security Lake 시작하기.

롤업 리전 업데이트 또는 제거

원하는 액세스 방법을 선택하고 다음 단계에 따라 Security Lake에서 롤업 리전을 업데이트하거나 제거하십시오.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창의 설정 아래에서 롤업 리전을 선택합니다.
3. 수정을 선택합니다.
4. 롤업 리전의 기여 리전을 변경하려면 롤업 리전 행에서 업데이트된 기여 리전을 지정하십시오.
5. 롤업 리전을 제거하려면 롤업 영역 행에서 제거를 선택합니다.
6. 마쳤으면 저장을 선택합니다.

API

프로그래밍 방식으로 롤업 리전을 구성하려면 Security Lake API의 UpdateDataLake 작업을 사용합니다. 를 사용하는 경우 update-data-lake 명령을 AWS CLI실행합니다. 요청 시 지원되는 파라미터를 사용하여 롤업 설정을 지정하십시오.

- 기여 리전을 추가하려면 `region` 필드를 사용하여 추가할 리전의 리전 코드를 지정합니다. `replicationConfiguration` 객체 `regions` 배열에서 데이터를 제공할 각 롤업 리전의 리전 코드를 지정합니다. 리전 코드 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오.
- 영향을 주는 리전을 제거하려면 `region` 필드를 사용하여 제거할 리전의 리전 코드를 지정합니다. 입력 파라미터에 대한 값을 지정합니다.

예를 들어 다음 명령은 `us-east-1` 및를 모두 기여 리전`us-east-2`으로 구성합니다. 두 리전 모두 `ap-northeast-3` 롤업 리전에 데이터를 제공합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","replicationConfiguration":
 {"regions": ["ap-northeast-3"],"roleArn":"arn:aws:iam::123456789012:role/service-
role/AmazonSecurityLakeS3ReplicationRole"},"lifecycleConfiguration": {"expiration":
{"days":365}}},
{"encryptionConfiguration": {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-
east-2","replicationConfiguration": {"regions": ["ap-
northeast-3"],"roleArn":"arn:aws:iam::123456789012:role/service-role/
AmazonSecurityLakeS3ReplicationRole"}, "lifecycleConfiguration": {"expiration":
{"days":500},"transitions":[{"days":60,"storageClass":"ONEZONE_IA"}]}}]'
```

Security Lake의 소스 관리

소스는 Security Lake의 Open Cybersecurity Schema Framework(OCSF) 스키마의 특정 이벤트 클래스와 일치하는 단일 시스템에서 생성된 로그 및 이벤트입니다. Amazon Security Lake는 기본적으로 지원되는 소스와 타사 사용자 지정 소스를 포함하여 다양한 소스에서 로그 AWS 서비스 와 이벤트를 수집할 수 있습니다.

Security Lake는 원시 소스 데이터의 추출, 전환, 적재(ETL) 작업을 실행하고 데이터를 Apache Parquet 형식과 스키마로 변환합니다. 처리 후 Security Lake는 데이터가 생성된의 Amazon Simple Storage Service(Amazon S3) 버킷 AWS 계정 에 소스 AWS 리전 데이터를 저장합니다. Security Lake는 사용자가 서비스를 활성화한 각 리전별로 여러 Amazon S3 버킷을 생성합니다. 각 소스는 S3 버킷에 별도의 접두사를 가져오고 Security Lake는 각 소스의 데이터를 별도의 AWS Lake Formation 테이블 세트로 구성합니다.

주제

- Security Lake AWS 서비스 에서 데이터 수집
- Security Lake의 사용자 지정 소스에서 데이터 수집

Security Lake AWS 서비스 에서 데이터 수집

Amazon Security Lake는 기본적으로 지원되는 AWS 서비스에서 로그 및 이벤트를 수집할 수 있습니다.

- AWS CloudTrail 관리 및 데이터 이벤트(S3, Lambda)
- Amazon Elastic Kubernetes Service(Amazon EKS) 감사 로그
- Amazon Route 53 Resolver 쿼리 로그
- AWS Security Hub 조사 결과
- Amazon Virtual Private Cloud(VPC) 흐름 로그
- AWS WAF v2 로그

Security Lake는 이 데이터를 Security Lake의 Open Cybersecurity Schema Framework(OCSF) 및 Apache Parquet 형식으로 자동 변환합니다.

> **Tip**
>
> 위의 서비스 중 하나 이상을 Security Lake의 로그 소스로 추가하려면 CloudTrail 관리 이벤트를 제외하고 이러한 서비스에서 로깅을 별도로 구성할 필요가 없습니다. 이러한 서비스에 로깅이 구성되어 있는 경우 Security Lake의 로그 소스로 추가하기 위해 로깅 구성을 변경할 필요가 없습니다. Security Lake는 독립적이고 복제된 이벤트 스트림을 통해 이러한 서비스에서 직접 데이터를 가져옵니다.

사전 조건: 권한 검증

Security Lake에서를 소스 AWS 서비스 로 추가하려면 필요한 권한이 있어야 합니다. 소스를 추가하는 데 사용하는 역할에 연결된 AWS Identity and Access Management (IAM) 정책에 다음 작업을 수행할 수 있는 권한이 있는지 확인합니다.

- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:GetDatabase`
- `glue:GetTable`
- `glue:UpdateTable`
- `iam:CreateServiceLinkedRole`
- `s3:GetObject`
- `s3:PutObject`

역할에 `S3:getObject` 및 `s3:PutObject` 권한에 대한 다음과 같은 조건과 리소스 범위가 있는 것이 좋습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUpdatingSecurityLakeS3Buckets",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
```

```
            ],
            "Resource": "arn:aws:s3:::aws-security-data-lake*",
              "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "${aws:PrincipalAccount}"
                }
            }
    }
    ]
}
```

이러한 작업을 통해에서 로그와 이벤트를 수집하여 올바른 AWS Glue 데이터베이스 AWS 서비스 와 테이블로 전송할 수 있습니다.

데이터 레이크의 서버 측 암호화에 AWS KMS 키를 사용하는 경우에 대한 권한도 필요합니다`kms:DescribeKey`.

소스 AWS 서비스 로 추가

를 소스 AWS 서비스 로 추가하면 Security Lake는 자동으로 보안 로그 및 이벤트를 수집하기 시작합니다. 이 지침에서는 Security Lake에서 기본적으로 지원되는를 소스 AWS 서비스 로 추가하는 방법을 설명합니다. 사용자 지정 소스 추가에 대한 지침은 Security Lake의 사용자 지정 소스에서 데이터 수집 단원을 참조하십시오.

Console

AWS 로그 소스를 추가하려면(콘솔)

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 소스를 선택합니다.
3. 데이터를 수집할 AWS 서비스 를 선택하고 구성을 선택합니다.
4. 소스 설정 섹션에서 소스를 활성화하고 데이터 수집에 사용할 데이터 소스 버전을 선택합니다. 기본적으로 최신 버전의 데이터 소스는 Security Lake에서 수집합니다.

> **Important**
> 지정된 리전에서 AWS 로그 소스의 새 버전을 활성화하는 데 필요한 역할 권한이 없는 경우 Security Lake 관리자에게 문의하십시오. 자세한 내용은 역할 권한 업데이트를 참조하세요.

구독자가 선택한 버전의 데이터 소스를 수집하려면 구독자 설정도 업데이트해야 합니다. 구독자를 편집하는 방법에 대한 자세한 내용은 Amazon Security Lake의 구독자 관리를 참조하세요.

선택적으로 최신 버전만 수집하고 데이터 수집에 사용된 모든 이전 소스 버전을 비활성화하도록 선택할 수 있습니다.

5. 리전 섹션에서 소스에 대한 데이터를 수집할 리전을 선택합니다. Security Lake는 선택한 리전의 모든 계정에서 소스에서 데이터를 수집합니다.
6. 활성화를 선택합니다.

API

AWS 로그 소스를 추가하려면(API)

를 프로그래밍 방식으로 소스 AWS 서비스 로 추가하려면 Security Lake API의 CreateAwsLogSource 작업을 사용합니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 create-aws-log-source 명령을 실행합니다. `sourceName` 및 `regions` 파라미터가 필요합니다. 선택적으로 소스의 범위를 특정 `accounts` 또는 특정 로 제한할 수 있습니다`sourceVersion`.

> **Important**
>
> 명령에 파라미터를 제공하지 않으면 Security Lake는 누락된 파라미터가 전체 세트를 참조한다고 가정합니다. 예를 들어 `accounts` 파라미터를 제공하지 않으면 조직의 전체 계정 집합에 명령이 적용됩니다.

다음 예시에서는 VPC 흐름 로그를 지정된 계정 및 리전의 소스로 추가합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

> **Note**
>
> Security Lake를 활성화하지 않은 리전에이 요청을 적용하면 오류가 발생합니다. 해당 리전에서 Security Lake를 활성화하거나 `regions` 파라미터를 사용하여 Security Lake를 활성화한 리전만 지정하여 오류를 해결할 수 있습니다.

```
$ aws securitylake create-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions=["us-east-2"],sourceVersion="2.0"
```

소스 컬렉션 상태 가져오기

액세스 방법을 선택하고 단계에 따라 현재 리전에서 로그 수집이 활성화된 계정 및 소스의 스냅샷을 가져옵니다.

Console

현재 리전에서 로그 수집 상태를 가져오려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 계정을 선택합니다.
3. 소스 열의 숫자 위에 커서를 놓으면 선택한 계정에 대해 활성화된 로그가 표시됩니다.

API

현재 리전에서 로그 수집 상태를 가져오려면 Security Lake API의 GetDataLakeSources 작업을 사용합니다. 를 사용하는 경우 get-data-lake-sources 명령을 AWS CLI실행합니다. `accounts` 파라미터의 경우 하나 이상의 AWS 계정 IDs으로 지정할 수 있습니다. 요청이 성공하면 Security Lake는 Security Lake가 데이터를 수집하는 AWS 소스와 각 소스의 상태를 포함하여 현재 리전의 해당 계정에 대한 스냅샷을 반환합니다. `accounts` 파라미터를 포함하지 않으면 응답에는 현재 리전에서 Security Lake가 구성된 모든 계정에 대한 로그 수집 상태가 포함됩니다.

예를 들어 다음 AWS CLI 명령은 현재 리전에서 지정된 계정의 로그 수집 상태를 검색합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake get-data-lake-sources \
--accounts "123456789012" "111122223333"
```

Security Lake에서 역할 권한 업데이트

새 AWS Lambda 버전의 데이터 소스에서 데이터를 수집하기 위해 새로운 함수와 Amazon Simple Queue Service(Amazon SQS) 대기열과 같은 필요한 역할 권한 또는 리소스가 없는 경우,

`AmazonSecurityLakeMetaStoreManagerV2` 역할 권한을 업데이트하고 소스의 데이터를 처리하기 위한 새 리소스 세트를 생성해야 합니다.

원하는 방법을 선택하고 지침에 따라 역할 권한을 업데이트하고 새 리소스를 생성하여 지정된 리전의 새 버전의 AWS 로그 소스에서 데이터를 처리합니다. 권한과 리소스가 향후 데이터 소스 릴리스에 자동으로 적용되므로 이는 일회성 작업입니다.

Console

역할 권한을 업데이트하려면(콘솔)

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.

   위임된 Security Lake 관리자의 자격 증명으로 로그인하십시오.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. 역할 권한 업데이트를 선택합니다.
4. 서비스 액세스 섹션에서 다음 중 하나를 수행합니다.
   - 새 서비스 역할 생성 및 사용 - Security Lake에서 생성한 AmazonSecurityLakeMetaStoreManagerV2 역할을 사용할 수 있습니다.
   - 기존 서비스 역할 사용 - 서비스 역할 이름 목록에서 기존 서비스 역할을 선택할 수 있습니다.
5. 적용을 선택합니다.

API

역할 권한을 업데이트하려면(API)

프로그래밍 방식으로 권한을 업데이트하려면 Security Lake API의 UpdateDataLake 작업을 사용합니다. 를 사용하여 권한을 업데이트하려면 update-data-lake 명령을 AWS CLI실행합니다.

역할 권한을 업데이트하려면 역할에 AmazonSecurityLakeMetastoreManager 정책을 연결해야 합니다.

AmazonSecurityLakeMetaStoreManager 역할 삭제

> **Important**
>
> 역할 권한을 로 업데이트한 후 이전 `AmazonSecurityLakeMetaStoreManager` 역할을 제거하기 전에 데이터 레이크가 올바르게 작동하는지

`AmazonSecurityLakeMetaStoreManagerV2`확인합니다. 역할을 제거하기 전에 최소 4시간을 기다리는 것이 좋습니다.

역할을 제거하기로 결정한 경우 먼저에서 `AmazonSecurityLakeMetaStoreManager` 역할을 삭제해야 합니다 AWS Lake Formation.

다음 단계에 따라 Lake Formation 콘솔에서 `AmazonSecurityLakeMetaStoreManager` 역할을 제거합니다.

1. 에 로그인 AWS Management Console하고 https://console.aws.amazon.com/lakeformation/ Lake Formation 콘솔을 엽니다.
2. Lake Formation 콘솔의 탐색 창에서 관리 역할 및 작업을 선택합니다.
3. 각 리전`AmazonSecurityLakeMetaStoreManager`에서를 제거합니다.

Security Lake에서 소스 AWS 서비스 로 제거

액세스 방법을 선택하고 다음 단계에 따라 Security Lake 소스 AWS 서비스 로 기본적으로 지원되는를 제거합니다. 하나 이상의 리전에 대한 소스를 제거할 수 있습니다. 소스를 제거하면 Security Lake는 지정된 리전 및 계정의 해당 소스에서 데이터 수집을 중단하고 구독자는 더 이상 원본의 새 데이터를 사용할 수 없습니다. 하지만 구독자는 Security Lake가 제거 전에 소스에서 수집한 데이터를 계속 사용할 수 있습니다. 소스로서 기본적으로 지원되는 AWS 서비스 를 제거할 때는 이 지침만 사용할 수 있습니다. 사용자 지정 소스 제거에 대한 자세한 내용은 Security Lake의 사용자 지정 소스에서 데이터 수집을 참조하십시오.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 소스를 선택합니다.
3. 소스를 선택하고 비활성화를 선택합니다.
4. 이 소스에서 데이터 수집을 중단하려는 리전 또는 리전들을 선택합니다. Security Lake는 선택한 리전의 모든 계정에서 소스로부터 데이터를 수집하는 것을 중단합니다.

API

를 소스 AWS 서비스 로 프로그래밍 방식으로 제거하려면 Security Lake API의 DeleteAwsLogSource 작업을 사용합니다. AWS Command Line Interface (AWS CLI)를 사용하는

경우 delete-aws-log-source 명령을 실행합니다. `sourceName` 및 `regions` 파라미터가 필요합니다. 선택적으로 제거 범위를 특정 `accounts` 또는 특정 로 제한할 수 있습니다`sourceVersion`.

> **Important**
>
> 명령에 파라미터를 제공하지 않으면 Security Lake는 누락된 파라미터가 전체 세트를 참조한다고 가정합니다. 예를 들어 `accounts` 파라미터를 제공하지 않으면 조직의 전체 계정 집합에 명령이 적용됩니다.

다음 예시에서는 지정된 계정 및 리전에서 VPC 흐름 로그를 소스로 제거합니다.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

다음 예시에서는 Route 53을 지정된 계정 및 리전의 소스로 제거합니다.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=ROUTE53,accounts='["123456789012"]',regions='["us-east-1", "us-
east-2"]',sourceVersion="2.0"
```

위의 예제는 Linux, macOS 또는 Unix용으로 포맷되어 있으며, 백슬래시(\) 줄 연속 문자를 사용하여 가독성을 개선합니다.

Security Lake의 CloudTrail 이벤트 로그

AWS CloudTrail 는 , AWS Management Console AWS SDKs, 명령줄 도구 및 특정 AWS 서비스를 사용하여 수행된 AWS API 호출을 포함하여 계정에 대한 API 호출 기록을 제공합니다. 또한, CloudTrail을 통해 CloudTrail을 지원하는 서비스에 대해 AWS API를 호출한 사용자와 계정, 호출이 이루어진 소스 IP 주소, 그리고 직접 호출이 발생한 시간을 파악할 수 있습니다. 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Security Lake는 S3 및 Lambda에 대한 CloudTrail 관리 이벤트 및 CloudTrail 데이터 이벤트와 관련된 로그를 수집할 수 있습니다. CloudTrail 관리 이벤트, S3 데이터 이벤트 및 Lambda 데이터 이벤트는 Security Lake의 세 가지 개별 소스입니다. 따라서 이들 중 하나를 수집된 로그 소스로 추가하면 `sourceName` 값이 달라집니다. 컨트롤 플레인 이벤트라고도 하는 관리 이벤트는의 리소스에서 수행되는 관리 작업에 대한 통찰력을 제공합니다 AWS 계정. 데이터 영역 작업이라고도 하는 CloudTrail 데

이터 이벤트는 AWS 계정의 리소스에서 또는 리소스 내에서 수행된 리소스 작업을 보여줍니다. 이러한 작업은 대량의 활동인 경우가 많습니다.

Security Lake에서 CloudTrail 관리 이벤트를 수집하려면 읽기 및 쓰기 CloudTrail 관리 이벤트를 수집하는 CloudTrail 다중 리전 추적 트레일이 하나 이상 있어야 합니다. 추적에 대한 로깅이 활성화되어 있어야 합니다. 다른 서비스에 로깅을 구성한 경우 Security Lake의 로그 소스로 추가하기 위해 로깅 구성을 변경할 필요가 없습니다. Security Lake는 독립적이고 복제된 이벤트 스트림을 통해 이러한 서비스에서 직접 데이터를 가져옵니다.

다중 리전 추적은 여러 리전의 로그 파일을 단일 AWS 계정에 대한 Amazon Simple Storage Service(S3) 버킷으로 전송합니다. 이미 CloudTrail 콘솔을 통해 관리되는 다중 리전 추적이 있거나 추가 작업이 필요하지 AWS Control Tower않습니다.

- CloudTrail을 통한 추적 생성 및 관리에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 조직을 위한 추적 생성을 참조하십시오.
- 를 통해 추적을 생성하고 관리하는 방법에 대한 자세한 내용은 AWS Control Tower 사용 설명서의 를 사용하여 AWS Control Tower 작업 로깅 AWS CloudTrail을 AWS Control Tower참조하세요.

CloudTrail 이벤트를 소스로 추가하면 Security Lake는 즉시 CloudTrail 이벤트 로그 수집을 시작합니다. 독립적이고 중복된 이벤트 스트림을 통해 CloudTrail에서 직접 CloudTrail 관리 및 데이터 이벤트를 사용합니다.

Security Lake는 CloudTrail 이벤트를 관리하거나 기존 CloudTrail 구성에 영향을 주지 않습니다. CloudTrail 이벤트의 액세스 및 보존을 직접 관리하려면 CloudTrail 서비스 콘솔 또는 API를 사용해야 합니다. 자세한 내용은AWS CloudTrail 사용 설명서에서 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

다음 목록은 Security Lake가 CloudTrail 이벤트를 OCSF로 정규화하는 방법에 대한 매핑 참조에 대한 GitHub 리포지토리 링크를 제공합니다.

CloudTrail 이벤트를 위한 GitHub OCSF 리포지토리

- 소스 버전 1(v1.0.0-rc.2)
- 소스 버전 2(v1.1.0)

Security Lake의 Amazon EKS 감사 로그

Amazon EKS 감사 로그를 소스로 추가하면 Security Lake는 Elastic Kubernetes Service(EKS) 클러스터에서 실행되는 Kubernetes 리소스에서 수행되는 활동에 대한 심층적인 정보를 수집하기 시작합니

다. EKS 감사 로그를 사용하면 Amazon Elastic Kubernetes Service 내의 EKS 클러스터에서 잠재적으로 의심스러운 활동을 감지할 수 있습니다.

Security Lake는 독립적이고 중복된 감사 로그 스트림을 통해 Amazon EKS 컨트롤 플레인 로깅 기능에서 직접 EKS 감사 로그 이벤트를 사용합니다. 이 프로세스는 추가 설정이 필요하지 않거나 기존 Amazon EKS 컨트롤 플레인 로깅 구성에 영향을 주지 않도록 설계되었습니다. 자세한 내용을 알아보려면 Amazon EKS 사용자 설명서의 Amazon EKS 클러스터 컨트롤 플레인 로깅을 참조하세요.

Amazon EKS 감사 로그는 OCSF v1.1.0에서만 지원됩니다. Security Lake가 EKS Audit Logs 이벤트를 OCSF로 정규화하는 방법에 대한 자세한 내용은 Amazon EKS Audit Logs 이벤트용 GitHub OCSF 리포지토리(v1.1.0)의 매핑 참조를 참조하세요.

Security Lake의 Route 53 해석기 쿼리 로그

Route 53 resolver 쿼리 로그는 Amazon Virtual Private Cloud(VPC)내의 리소스에서 만든 DNS 쿼리를 추적합니다. 이를 통해 애플리케이션 작동 방식을 이해하고 보안 위협을 찾아낼 수 있습니다.

Route 53 resolver 쿼리 로그를 Security Lake의 소스로 추가하면 Security Lake는 독립적이고 복제된 이벤트 스트림을 통해 Route 53에서 직접 resolver 쿼리 로그를 즉시 수집하기 시작합니다.

Security Lake는 Route 53 로그를 관리하거나 기존 Resolver 쿼리 로깅 구성에 영향을 주지 않습니다. Resolver 쿼리 로그를 관리하려면 Route 53 서비스 콘솔을 사용해야 합니다. Resolver 쿼리 로깅에 대한 자세한 내용은 Amazon Route 53 개발자 안내서의 Resolver 쿼리 로깅 구성 관리를 참조하세요.

다음 목록은 Security Lake가 Route 53 로그를 OCSF로 정규화하는 방법에 대한 매핑 참조에 대한 GitHub 리포지토리 링크를 제공합니다.

Route 53 로그용 GitHub OCSF 리포지토리

- 소스 버전 1(v1.0.0-rc.2)
- 소스 버전 2(v1.1.0)

Security Lake의 Security Hub 조사 결과

Security Hub 조사 결과는의 보안 태세를 이해하고 보안 업계 표준 AWS 및 모범 사례를 기준으로 환경을 확인할 수 있도록 도와줍니다. Security Hub는 다른 AWS 서비스타사 제품 통합과의 통합 및 Security Hub 제어에 대한 검사를 포함하여 다양한 소스에서 결과를 수집합니다. Security Hub는 AWS 결과를 Security Finding Format(ASFF)이라는 표준 형식으로 처리합니다.

Security Hub 조사 결과를 Security Lake의 소스로 추가하면 Security Lake는 즉시 독립적이고 복제된 이벤트 스트림을 통해 Security Hub에서 직접 결과를 수집하기 시작합니다. 또한 Security Lake는 조사 결과를 ASFF에서 Security Lake의 Open Cybersecurity Schema Framework(OCSF) (OCSF) 로 변환합니다.

Security Lake는 Security Hub 조사 결과를 관리하거나 Security Hub 설정에 영향을 주지 않습니다. Security Hub 조사 결과를 관리하려면 Security Hub 서비스 콘솔, API 또는를 사용해야 합니다 AWS CLI. 자세한 내용은 AWS Security Hub 사용 설명서의 조사 결과 AWS Security Hub를 참조하세요.

다음 목록은 Security Lake가 Security Hub 조사 결과를 OCSF로 정규화하는 방법에 대한 매핑 참조에 대한 GitHub 리포지토리 링크를 제공합니다.

Security Hub 조사 결과를 위한 GitHub OCSF 리포지토리

- 소스 버전 1(v1.0.0-rc.2)
- 소스 버전 2(v1.1.0)

Security Lake의 VPC 흐름 로그

Amazon VPC의 VPC 흐름 로그 기능은 환경 내 네트워크 인터페이스와 주고받는 IP 트래픽에 대한 정보를 캡처합니다.

Security Lake에서 VPC 흐름 로그를 소스로 추가하면 Security Lake는 즉시 VPC 흐름 로그를 수집하기 시작합니다. 독립적이고 중복된 흐름 로그 스트림을 통해 Amazon VPC에서 직접 VPC 흐름 로그를 사용합니다.

Security Lake는 VPC 흐름 로그를 관리하거나 Amazon VPC 구성에 영향을 주지 않습니다. 흐름 로그를 관리하려면 Amazon VPC 서비스 콘솔을 사용해야 합니다. 자세한 내용은 Amazon VPC 개발자 안내서의 흐름 로그로 작업을 참조하세요.

다음 목록은 Security Lake가 VPC 흐름 로그를 OCSF로 정규화하는 방법에 대한 매핑 참조에 대한 GitHub 리포지토리 링크를 제공합니다.

VPC 흐름 로그용 GitHub OCSF 리포지토리

- 소스 버전 1(v1.0.0-rc.2)
- 소스 버전 2(v1.1.0)

AWS WAF Security Lake의 로그

Security Lake에서를 로그 소스 AWS WAF 로 추가하면 Security Lake는 즉시 로그 수집을 시작합니다. AWS WAF 는 최종 사용자가 애플리케이션에 보내는 웹 요청을 모니터링하고 콘텐츠에 대한 액세스를 제어하는 데 사용할 수 있는 웹 애플리케이션 방화벽입니다. 로깅된 정보에는 리소스로부터 AWS 웹 요청을 AWS WAF 받은 시간, 요청에 대한 세부 정보, 요청이 일치하는 규칙에 대한 세부 정보가 포함됩니다.

Security Lake는 독립적인 중복 AWS WAF 로그 스트림을 AWS WAF 통해에서 직접 로그를 사용합니다. 이 프로세스는 추가 설정이 필요하지 않거나 기존 AWS WAF 구성에 영향을 주지 않도록 설계되었습니다. Security Lake 로그는 웹 액세스 제어 목록(웹 ACL) 구성에서 AWS WAF 허용하는 데이터만 검색합니다. Security Lake 계정의 웹 ACL에 대해 데이터 보호가 활성화된 경우 생성된 데이터는 웹 ACL 설정에 따라 수정되거나 해시됩니다. 를 사용하여 애플리케이션 리소스를 보호하는 AWS WAF 방법에 대한 자세한 내용은 AWS WAF 개발자 안내서의 AWS WAF 작동 방식을 참조하세요.

> **Important**
>
> Amazon CloudFront 배포를 리소스 유형으로 사용하는 경우 미국 동부(버지니아 북부)를 선택하여 Security Lake에서 글로벌 로그를 수집 AWS WAF해야 합니다.

AWS WAF 로그는 OCSF v1.1.0에서만 지원됩니다. Security Lake가 AWS WAF 로그 이벤트를 OCSF로 정규화하는 방법에 대한 자세한 내용은 AWS WAF 로그용 GitHub OCSF 리포지토리(v1.1.0)의 매핑 참조를 참조하세요.

소스 AWS 서비스 로 제거

액세스 방법을 선택하고 다음 단계에 따라 Security Lake 소스 AWS 서비스 로 기본적으로 지원되는를 제거합니다. 하나 이상의 리전에 대한 소스를 제거할 수 있습니다. 소스를 제거하면 Security Lake는 지정된 리전 및 계정의 해당 소스에서 데이터 수집을 중단하고 구독자는 더 이상 원본의 새 데이터를 사용할 수 없습니다. 하지만 구독자는 Security Lake가 제거 전에 소스에서 수집한 데이터를 계속 사용할 수 있습니다. 소스로서 기본적으로 지원되는 AWS 서비스 를 제거할 때는 이 지침만 사용할 수 있습니다. 사용자 지정 소스 제거에 대한 자세한 내용은 Security Lake의 사용자 지정 소스에서 데이터 수집을 참조하십시오.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 소스를 선택합니다.

3. 소스를 선택하고 비활성화를 선택합니다.
4. 이 소스에서 데이터 수집을 중단하려는 리전 또는 리전들을 선택합니다. Security Lake는 선택한 리전의 모든 계정에서 소스로부터 데이터를 수집하는 것을 중단합니다.

API

를 소스 AWS 서비스 로 프로그래밍 방식으로 제거하려면 Security Lake API의 DeleteAwsLogSource 작업을 사용합니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 delete-aws-log-source 명령을 실행합니다. `sourceName` 및 `regions` 파라미터가 필요합니다. 선택적으로 제거 범위를 특정 `accounts` 또는 특정 로 제한할 수 있습니다`sourceVersion`.

> **Important**
> 명령에 파라미터를 제공하지 않으면 Security Lake는 누락된 파라미터가 전체 세트를 참조한다고 가정합니다. 예를 들어 `accounts` 파라미터를 제공하지 않으면 조직의 전체 계정 집합에 명령이 적용됩니다.

다음 예시에서는 지정된 계정 및 리전에서 VPC 흐름 로그를 소스로 제거합니다.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=VPC_FLOW,accounts='["123456789012",
 "111122223333"]',regions='["us-east-1", "us-east-2"]',sourceVersion="2.0"
```

다음 예시에서는 Route 53을 지정된 계정 및 리전의 소스로 제거합니다.

```
$ aws securitylake delete-aws-log-source \
--sources sourceName=ROUTE53,accounts='["123456789012"]',regions='["us-east-1", "us-
east-2"]',sourceVersion="2.0"
```

위의 예제는 Linux, macOS 또는 Unix용으로 포맷되어 있으며, 백슬래시(\) 줄 연속 문자를 사용하여 가독성을 개선합니다.

Security Lake의 사용자 지정 소스에서 데이터 수집

Amazon Security Lake는 타사 사용자 지정 소스에서 로그와 이벤트를 수집할 수 있습니다. Security Lake 사용자 지정 소스는 보안 로그와 이벤트를 Amazon Security Lake로 전송하는 타사 서비스입니

다. 데이터를 전송하기 전에 사용자 지정 소스는 로그 및 이벤트를 OCSF(Open Cybersecurity Schema Framework)로 변환하고 파티셔닝, 파켓 파일 형식, 객체 크기 및 속도 요구 사항을 포함한 Security Lake의 소스 요구 사항을 충족해야 합니다.

Security Lake는 각 사용자 지정 소스에 대해 다음을 처리합니다.

- Amazon S3 버킷의 소스에 고유한 접두사를 제공합니다.
- 사용자 지정 소스가 데이터 레이크에 데이터를 쓸 수 있도록 허용하는 AWS Identity and Access Management (IAM)에서 역할을 생성합니다. 이 역할의 권한 경계는 라는 AWS 관리형 정책에 의해 설정됩니다`AmazonSecurityLakePermissionsBoundary`.
- 소스가 Security Lake에 쓰는 객체를 구성하는 AWS Lake Formation 테이블을 생성합니다.
- 소스 데이터를 분할할 AWS Glue 크롤러를 설정합니다. 크롤러는 테이블 AWS Glue Data Catalog 로를 채웁니다. 또한 새 소스 데이터를 자동으로 검색하고 스키마 정의를 추출합니다.

> **Note**
>
> 계정에 최대 50개의 사용자 지정 로그 소스를 추가할 수 있습니다.

Security Lake에 사용자 지정 소스를 추가하려면 다음 요구 사항을 충족해야 합니다. 이러한 요구 사항을 충족하지 못하면 성능에 영향을 줄 수 있으며 쿼리와 같은 분석 사용 사례에 영향을 줄 수 있습니다.

- 대상 - 사용자 지정 소스는 소스에 할당된 접두사 아래에 있는 S3 객체 세트로 Security Lake에 데이터를 쓸 수 있어야 합니다. 여러 범주의 데이터가 포함된 원본의 경우 고유한 OCSF (개방형 사이버 보안 스키마 프레임워크) 이벤트 클래스를 각각 별도의 원본으로 제공해야 합니다. Security Lake는 사용자 지정 소스가 S3 버킷의 지정된 위치에 쓸 수 있도록 허용하는 IAM 역할을 생성합니다.
- 형식 - 사용자 지정 소스에서 수집된 각 S3 객체는 Apache Parquet 파일 형식을 지정해야 합니다.
- 스키마 - Parquet 형식 객체 내의 각 레코드에 동일한 OCSF 이벤트 클래스를 적용해야 합니다. Security Lake는 Parquet 버전 1.x 및 2.x를 지원합니다. 데이터 페이지 크기는 1MB (비압축)로 제한해야 합니다. 행 그룹 크기는 256MB (압축)를 넘지 않아야 합니다. Parquet 객체 내의 압축의 경우 zstandard이 선호됩니다.
- 파티셔닝 - 객체는 리전, AWS 계정, eventDay로 파티셔닝해야 합니다. 객체에는 접두사가 붙어야 합니다`source location`/region=`region`/accountId=`accountID`/eventDay=`yyyyMMdd`/.
- 객체 크기 및 속도 - Security Lake로 전송된 파일은 5분에서 1일 사이의 이벤트 날짜 증분으로 전송되어야 합니다. 파일 크기가 256MB분 이상 파일을 보낼 수 있습니다. 객체 및 크기 요구 사항은 쿼

리 성능을 위한 Security Lake를 최적화하는 것입니다. 사용자 지정 소스 요구 사항을 따르지 않으면 Security Lake 성능에 영향을 미칠 수 있습니다.

- 정렬 - Parquet 형식의 각 객체 내에서 데이터 쿼리 비용을 줄이기 위해 레코드를 시간별로 정렬해야 합니다.

> **Note**
>
> OCSF 검증 도구를 사용하여 사용자 지정 소스가와 호환되는지 확인합니다OCSF Schema. 사용자 지정 소스의 경우 Security Lake는 OCSF 버전 1.3 이하를 지원합니다.

Security Lake에서 사용자 지정 소스를 수집하기 위한 파티셔닝 요구 사항

효율적인 데이터 처리 및 쿼리를 용이하게 하려면 Security Lake에 사용자 지정 소스를 추가할 때 파티셔닝 및 객체와 크기 요구 사항을 충족해야 합니다.

분할

객체는 소스 위치, AWS 리전, AWS 계정날짜별로 분할해야 합니다.

- 파티션 데이터 경로의 형식은 입니다.

  `/ext/`*`custom-source-name`*`/region=`*`region`*`/accountId=`*`accountID`*`/eventDay=`*`YYYYMMDD`*.

  버킷 이름 예시가 있는 샘플 파티션은 입니다`aws-security-data-lake-`*`us-west-2-lake-uid`*`/ext/`*`custom-source-name`*`/region=`*`us-west-2`*`/accountId=`*`123456789012`*`/eventDay=`*`20230428`*`/`.

다음 목록은 S3 경로 파티션에 사용되는 파라미터를 설명합니다.

- Security Lake가 사용자 지정 소스 데이터를 저장하는 Amazon S3 버킷의 이름입니다.
- `source-location`— S3 버킷에 있는 사용자 지정 소스의 접두사. Security Lake는 지정된 소스의 모든 S3 객체를 이 접두사 아래에 저장하며 접두사는 해당 소스에 고유합니다.
- `region` - 데이터가 업로드되는 AWS 리전 대상입니다. 예를 들어 `US East (N. Virginia)`를 사용하여 미국 동부(버지니아 북부) 리전의 Security Lake 버킷에 데이터를 업로드해야 합니다.
- `accountId` –소스 파티션의 레코드가 관련된 AWS 계정 ID입니다. 외부 계정과 관련된 레코드의 경우 `external` 또는와 같은 문자열을 사용하는 AWS것이 좋습니

다`external_externalAccountId`. 이 명명 대류를 채택하면 외부 계정 IDs의 명명이 다른 자격 증명 관리 시스템에서 유지 관리하는 AWS 계정 IDs 또는 외부 계정 IDs와 충돌하지 않도록 모호하지 않게 할 수 있습니다.

- `eventDay` - 레코드의 UTC 타임스탬프로, 8자 문자열() 형식의 시간으로 잘립니다`YYYYMMDD`. 레코드가 이벤트 타임스탬프에 다른 시간대를 지정하는 경우이 파티션 키의 타임스탬프를 UTC로 변환해야 합니다.

Security Lake에서 사용자 지정 소스를 추가하기 위한 사전 조건

사용자 지정 소스를 추가할 때 Security Lake는 원본이 데이터 레이크의 올바른 위치에 데이터를 쓸 수 있도록 허용하는 IAM 역할을 생성합니다. 역할의 이름은 형식을 따르며`AmazonSecurityLake-Provider-{name of the custom source}-{region}`, 여기서 `region`는 사용자 지정 소스를 추가하는 AWS 리전 입니다. Security Lake는 데이터 레이크에 대한 액세스를 허용하는 정책을 역할에 연결합니다. 고객 관리형 AWS KMS 키로 데이터 레이크를 암호화한 경우 Security Lake는 `kms:Decrypt` 및 `kms:GenerateDataKey` 권한을 사용하여 정책을 역할에 연결합니다. 이 역할의 권한 경계는 라는 AWS 관리형 정책에 의해 설정됩니다`AmazonSecurityLakePermissionsBoundary`.

주제

- 권한 확인
- Security Lake 버킷 위치에 대한 쓰기 액세스를 허용하는 IAM 역할 생성(API 및 AWS CLI전용 단계)

권한 확인

사용자 지정 소스를 추가하기 전에 다음 작업을 수행할 권한이 있는지 확인합니다.

권한을 확인하려면 IAM을 사용하여 IAM 자격 증명에 연결된 IAM 정책을 검토하십시오. 그런 다음 해당 정책의 정보를 사용자 지정 소스를 추가하기 위해 수행할 수 있어야 하는 다음 작업 목록과 비교하십시오.

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StopCrawlerSchedule`
- `iam:GetRole`

- `iam:PutRolePolicy`
- `iam:DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`
- `lakeformation:GrantPermissions`
- `s3:ListBucket`
- `s3:PutObject`

이러한 작업을 통해 사용자 지정 소스에서 로그와 이벤트를 수집하고 올바른 AWS Glue 데이터베이스와 테이블로 전송한 다음 Amazon S3에 저장할 수 있습니다.

데이터 레이크의 서버 측 암호화에 AWS KMS 키를 사용하는 경우 , `kms:DescribeKey`및 `kms:CreateGrant`에 대한 권한도 필요합니다`kms:GenerateDataKey`.

> **Important**
>
> Security Lake 콘솔을 사용하여 사용자 지정 소스를 추가하려면 다음 단계를 건너뛰고 로 진행할 수 있습니다Security Lake에 사용자 지정 소스 추가. Security Lake 콘솔은 간소화된 시작 프로세스를 제공하며, 필요한 모든 IAM 역할을 생성하거나 사용자 대신 기존 역할을 사용합니다. Security Lake API AWS CLI 를 사용하거나 사용자 지정 소스를 추가하려면 다음 단계를 진행하여 Security Lake 버킷 위치에 대한 쓰기 액세스를 허용하는 IAM 역할을 생성합니다.

Security Lake 버킷 위치에 대한 쓰기 액세스를 허용하는 IAM 역할 생성(API 및 AWS CLI전용 단계)

Security Lake API 또는 AWS CLI 를 사용하여 사용자 지정 소스를 추가하는 경우이 IAM 역할을 추가하여 사용자 지정 소스 데이터를 크롤링하고 데이터에서 파티션을 식별할 수 있는 AWS Glue 권한을 부여합니다. 이러한 파티션은 데이터를 구성하고 데이터 카탈로그에서 테이블을 생성 및 업데이트하는 데 필요합니다.

이 IAM 역할을 정의한 후에는 역할의 Amazon 리소스 이름(ARN)이 있어야 사용자 지정 소스를 추가할 수 있습니다.

`arn:aws:iam::aws:policy/service-role/AWSGlueServiceRole` AWS 관리형 정책을 연결해야 합니다.

필요한 권한을 부여하려면가 사용자 지정 소스에서 데이터 파일을 AWS Glue 크롤러 읽고 AWS Glue Data Catalog에서 테이블을 생성/업데이트할 수 있도록 역할에 다음 인라인 정책을 생성하고 포함해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3WriteRead",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::{{bucketName}}/*"
            ]
        }
    ]
}
```

외부 ID를 기반으로 역할을 수임할 수 있는를 AWS 계정 사용하여를 허용하려면 다음 신뢰 정책을 연결합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "glue.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

사용자 지정 소스를 추가하는 리전의 S3 버킷이 고객 관리형으로 암호화된 경우 역할 및 KMS 키 정책에 다음 정책도 연결 AWS KMS key해야 합니다.

```
{
```

```
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey"
        "kms:Decrypt"
    ],
    "Condition": {
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": [
                "arn:aws:s3:::{{name of S3 bucket created by Security Lake}"
            ]
        }
    },
    "Resource": [
        "{{ARN of customer managed key}}"
    ]
}
```

Security Lake에 사용자 지정 소스 추가

IAM 역할을 생성하여 AWS Glue 크롤러를 호출한 후 다음 단계에 따라 Security Lake에 사용자 지정 소스를 추가합니다.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 사용자 지정 소스를 생성할 리전을 선택합니다.
3. 탐색 창에서 사용자 지정 소스를 선택한 다음 사용자 지정 소스 만들기를 선택합니다.
4. 사용자 지정 소스 세부 정보 섹션에서 사용자 지정 소스의 전 세계적으로 고유한 이름을 입력합니다. 그런 다음 사용자 지정 소스가 Security Lake로 전송할 데이터 유형을 설명하는 OCSF 이벤트 클래스를 선택합니다.
5. AWS 계정 데이터 쓰기 권한이 있는 경우 데이터 레이크에 로그와 이벤트를 기록할 사용자 지정 소스의 AWS 계정 ID 및 외부 ID를 입력합니다.
6. 서비스 액세스의 경우 새 서비스 역할을 만들어 사용하거나 Security Lake에 AWS Glue를 간접 호출하는 권한을 부여하는 기존 서비스 역할을 사용하십시오.
7. 생성(Create)을 선택합니다.

API

프로그래밍 방식으로 사용자 지정 소스를 추가하려면 Security Lake API의 CreateCustomLogSource 작업을 사용하십시오. 사용자 지정 소스를 생성하려는 AWS 리전 에서 작업을 사용합니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 create-custom-log-source 명령을 실행합니다.

요청 시 지원되는 파라미터를 사용하여 사용자 지정 소스의 구성 설정을 지정하십시오.

- `sourceName` - 소스의 이름을 지정합니다. 이름은 리전 고유 값이어야 합니다.
- `eventClasses` - 하나 이상의 OCSF 이벤트 클래스를 지정하여 소스가 Security Lake로 전송할 데이터 유형을 설명합니다. Security Lake에서 소스로 지원되는 OCSF 이벤트 클래스 목록은 Open Cybersecurity Schema Framework(OCSF)를 참조하세요.
- `sourceVersion` - 선택적으로 로그 수집을 사용자 지정 소스 데이터의 특정 버전으로 제한하는 값을 지정합니다.
- `crawlerConfiguration` - 크롤러를 호출하기 위해 생성한 IAM 역할의 Amazon 리소스 이름(ARN)을 AWS Glue 지정합니다. IAM 역할을 생성하는 자세한 단계는 사용자 지정 소스를 추가하기 위한 사전 조건을 참조하세요.
- `providerIdentity` - 소스가 데이터 레이크에 로그와 이벤트를 쓰는 데 사용할 AWS 자격 증명과 외부 ID를 지정합니다.

다음 예시에서는 사용자 지정 소스를 지정된 리전의 지정된 로그 공급자 계정에 로그 소스로 추가합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake create-custom-log-source \
--source-name EXAMPLE_CUSTOM_SOURCE \
--event-classes '["DNS_ACTIVITY", "NETWORK_ACTIVITY"]' \
--configuration crawlerConfiguration={"roleArn=arn:aws:iam::XXX:role/service-role/
RoleName"},providerIdentity={"externalId=ExternalId,principal=principal"}  \
--region=[“ap-southeast-2”]
```

에서 사용자 지정 소스 데이터 업데이트 유지 AWS Glue

Security Lake에 사용자 지정 소스를 추가하면 Security Lake가 AWS Glue 크롤러를 생성합니다. 크롤러는 사용자 지정 소스에 연결하여 데이터 구조를 결정하고 AWS Glue 데이터 카탈로그를 테이블로 채웁니다.

크롤러를 수동으로 실행하여 사용자 지정 소스 스키마를 최신 상태로 유지하고 Athena 및 기타 쿼리 서비스에서 쿼리 기능을 유지하는 것이 좋습니다. 특히 사용자 지정 소스의 입력 데이터 집합에서 다음 변경 사항 중 하나가 발생하는 경우 크롤러를 실행해야 합니다.

- 데이터 세트에는 새 최상위 열이 하나 이상 있습니다.
- 데이터 세트의 열에는 `struct` 데이터 유형이 있는 열에 하나 이상의 새 필드가 있습니다.

크롤러 실행에 대한 지침은 AWS Glue 개발자 안내서의 AWS Glue 크롤러 예약을 참조하세요.

Security Lake는 계정의 기존 크롤러를 삭제하거나 업데이트할 수 없습니다. 사용자 지정 소스를 삭제하는 경우 나중에 같은 이름의 사용자 지정 소스를 만들 계획이라면 연결된 크롤러를 삭제하는 것이 좋습니다.

지원되는 OCSF 이벤트 클래스

Open Cybersecurity Schema Framework(OCSF) 이벤트 클래스는 사용자 지정 소스가 Security Lake로 전송할 데이터 유형을 설명합니다. 지원되는 이벤트 클래스 목록은 다음과 같습니다.

```
public enum OcsfEventClass {
    ACCOUNT_CHANGE,
    API_ACTIVITY,
    APPLICATION_LIFECYCLE,
    AUTHENTICATION,
    AUTHORIZE_SESSION,
    COMPLIANCE_FINDING,
    DATASTORE_ACTIVITY,
    DEVICE_CONFIG_STATE,
    DEVICE_CONFIG_STATE_CHANGE,
    DEVICE_INVENTORY_INFO,
    DHCP_ACTIVITY,
    DNS_ACTIVITY,
    DETECTION_FINDING,
    EMAIL_ACTIVITY,
    EMAIL_FILE_ACTIVITY,
    EMAIL_URL_ACTIVITY,
    ENTITY_MANAGEMENT,
    FILE_HOSTING_ACTIVITY,
    FILE_SYSTEM_ACTIVITY,
    FTP_ACTIVITY,
    GROUP_MANAGEMENT,
    HTTP_ACTIVITY,
    INCIDENT_FINDING,
```

```
    KERNEL_ACTIVITY,
    KERNEL_EXTENSION,
    MEMORY_ACTIVITY,
    MODULE_ACTIVITY,
    NETWORK_ACTIVITY,
    NETWORK_FILE_ACTIVITY,
    NTP_ACTIVITY,
    PATCH_STATE,
    PROCESS_ACTIVITY,
    RDP_ACTIVITY,
    REGISTRY_KEY_ACTIVITY,
    REGISTRY_VALUE_ACTIVITY,
    SCHEDULED_JOB_ACTIVITY,
    SCAN_ACTIVITY,
    SECURITY_FINDING,
    SMB_ACTIVITY,
    SSH_ACTIVITY,
    USER_ACCESS,
    USER_INVENTORY,
    VULNERABILITY_FINDING,
    WEB_RESOURCE_ACCESS_ACTIVITY,
    WEB_RESOURCES_ACTIVITY,
    WINDOWS_RESOURCE_ACTIVITY,
    // 1.3 OCSF event classes
    ADMIN_GROUP_QUERY,
    DATA_SECURITY_FINDING,
    EVENT_LOG_ACTIVITY,
    FILE_QUERY,
    FILE_REMEDIATION_ACTIVITY,
    FOLDER_QUERY,
    JOB_QUERY,
    KERNEL_OBJECT_QUERY,
    MODULE_QUERY,
    NETWORK_CONNECTION_QUERY,
    NETWORK_REMEDIATION_ACTIVITY,
    NETWORKS_QUERY,
    PERIPHERAL_DEVICE_QUERY,
    PROCESS_QUERY,
    PROCESS_REMEDIATION_ACTIVITY,
    REMEDIATION_ACTIVITY,
    SERVICE_QUERY,
    SOFTWARE_INVENTORY_INFO,
    TUNNEL_ACTIVITY,
    USER_QUERY,
```

```
    USER_SESSION_QUERY,
    // 1.3 OCSF event classes (Win extension)
    PREFETCH_QUERY,
    REGISTRY_KEY_QUERY,
    REGISTRY_VALUE_QUERY,
    WINDOWS_SERVICE_ACTIVITY
}
```

Security Lake에서 사용자 지정 소스 삭제

소스에서 Security Lake로 데이터를 더 이상 보내지 않으려면 사용자 지정 소스를 삭제하세요. 소스를 제거하면 Security Lake는 지정된 리전 및 계정의 해당 소스에서 데이터 수집을 중단하고 구독자는 더 이상 원본의 새 데이터를 사용할 수 없습니다. 하지만 구독자는 Security Lake가 제거 전에 소스에서 수집한 데이터를 계속 사용할 수 있습니다. 이러한 지침은 사용자 지정 소스를 제거하는 데만 사용할 수 있습니다. 기본적으로 지원되는 제거에 대한 자세한 내용은 섹션을 AWS 서비스참조하세요Security Lake AWS 서비스 에서 데이터 수집.

Security Lake에서 사용자 지정 소스를 삭제할 때는 Security Lake 콘솔 외부의 각 소스를 소스와 함께 비활성화해야 합니다. 통합을 비활성화하지 않으면 소스 통합이 Amazon S3로 로그를 계속 전송할 수 있습니다.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 사용자 지정 소스를 제거할 리전을 선택합니다.
3. 탐색 창에서 사용자 지정 소스를 선택합니다.
4. 제거할 사용자 지정 소스를 선택합니다.
5. 사용자 지정 소스 등록 취소를 선택한 다음 삭제를 선택하여 작업을 확인합니다.

API

프로그래밍 방식으로 사용자 지정 소스를 삭제하려면 Security Lake API의 DeleteCustomLogSource 작업을 사용하십시오. AWS Command Line Interface (AWS CLI)를 사용하는 경우 delete-custom-log-source 명령을 실행합니다. 사용자 지정 소스를 삭제하려는 AWS 리전 위치에서 작업을 사용하십시오.

요청 시 `sourceName` 파라미터를 사용하여 삭제할 사용자 지정 소스의 이름을 지정합니다. 또는 사용자 지정 소스의 이름을 지정하고 `sourceVersion` 파라미터를 사용하여 삭제 범위를 사용자 지정 소스의 특정 버전 데이터로만 제한할 수 있습니다.

다음 예시에서는 Security Lake에서 사용자 지정 로그 소스를 삭제합니다.

이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake delete-custom-log-source \
--source-name EXAMPLE_CUSTOM_SOURCE
```

Security Lake의 구독자 관리

Amazon Security Lake 구독자는 Security Lake의 로그와 이벤트를 사용합니다. 비용을 관리하고 최소 권한 액세스 모범 사례를 준수하려면 구독자에게 소스별로 데이터에 대한 액세스 권한을 제공해야 합니다. 소스에 대한 자세한 내용은 Security Lake의 소스 관리 섹션을 참조하세요.

Security Lake는 두 종류의 구독자 액세스를 지원합니다.

- 데이터 액세스 Amazon Security Lake의 소스 데이터에 대한 데이터 액세스 권한이 있는 구독자는 데이터가 S3 버킷에 기록될 때 소스의 새 객체에 대한 알림을 받습니다. 기본적으로 구독자는 자신이 제공하는 HTTPS 엔드포인트를 통해 새 객체에 대한 알림을 받습니다. Amazon Simple Queue Service(Amazon SQS) 대기열을 폴링하여 구독자에게 새 객체에 대한 알림을 받을 수도 있습니다.
- 쿼리 액세스 - 쿼리 액세스 권한이 있는 구독자는 Security Lake가 수집하는 데이터를 쿼리할 수 있습니다. 이러한 구독자는 Amazon Athena와 같은 서비스를 사용하여 S3 버킷의 AWS Lake Formation 테이블을 직접 쿼리합니다.

구독자는 구독자를 생성할 때 AWS 리전 선택한의 소스 데이터에만 액세스할 수 있습니다. 구독자에게 여러 리전의 데이터에 대한 액세스 권한을 부여하려면 구독자를 생성하는 리전을 롤업 리전으로 지정하고 다른 리전에서 해당 리전에 데이터를 제공하도록 할 수 있습니다. 롤업 리전 및 기여 리전에 대한 자세한 내용은 Security Lake의 리전 관리를 참조하십시오.

> **Important**
>
> Security Lake에서 구독자당 추가할 수 있는 최대 소스 수는 10개입니다. 소스와 사용자 지정 AWS 소스의 조합일 수 있습니다.

주제

- Security Lake 구독자의 데이터 액세스 관리
- 구독자를 위한 쿼리 액세스 관리

Security Lake 구독자의 데이터 액세스 관리

Amazon Security Lake의 원본 데이터에 대한 데이터 액세스 권한이 있는 구독자는 데이터가 S3 버킷에 기록될 때 원본의 새 객체에 대한 알림을 받습니다. 기본적으로 구독자는 자신이 제공하는 HTTPS

엔드포인트를 통해 새 객체에 대한 알림을 받습니다. Amazon Simple Queue Service(Amazon SQS) 대기열을 폴링하여 구독자에게 새 객체에 대한 알림을 받을 수도 있습니다.

객체가 Security Lake 데이터 레이크에 기록되면 구독자에게 소스의 새 Amazon S3 객체에 대한 알림이 전송됩니다. 구독자는 구독 엔드포인트를 통해 또는 Amazon Simple Queue Service (Amazon SQS) 대기열을 폴링하여 S3 객체에 직접 액세스하고 새 객체에 대한 알림을 받을 수 있습니다. 이 구독 유형은 CreateSubscriber API의 파라미터 `accessTypes`에서 `S3`로 식별됩니다.

주제

- Security Lake에서 데이터 액세스 권한이 있는 구독자를 생성하기 위한 사전 조건
- Security Lake에서 데이터 액세스 권한이 있는 구독자 생성
- Security Lake에서 데이터 구독자 업데이트
- Security Lake에서 데이터 구독자 제거

Security Lake에서 데이터 액세스 권한이 있는 구독자를 생성하기 위한 사전 조건

Security Lake에서 데이터 액세스 권한을 가진 구독자를 생성하려면 먼저 다음 사전 조건을 완료해야 합니다.

권한 확인

권한을 확인하려면 IAM을 사용하여 IAM ID에 연결된 IAM 정책을 검토하십시오. 그런 다음 해당 정책의 정보를 데이터 레이크에 새 데이터가 기록될 때 구독자에게 알려야 하는 다음 (권한) 조치 목록과 비교하십시오.

다음 작업을 수행할 수 있는 권한이 필요합니다.

- `iam:CreateRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `lakeformation:GrantPermissions`
- `lakeformation:ListPermissions`
- `lakeformation:RegisterResource`
- `lakeformation:RevokePermissions`

- `ram:GetResourceShareAssociations`
- `ram:GetResourceShares`
- `ram:UpdateResourceShare`

위의 목록 외에도 다음 작업을 수행할 수 있는 권한이 필요합니다.

- `events:CreateApiDestination`
- `events:CreateConnection`
- `events:DescribeRule`
- `events:ListApiDestinations`
- `events:ListConnections`
- `events:PutRule`
- `events:PutTargets`
- `s3:GetBucketNotification`
- `s3:PutBucketNotification`
- `sqs:CreateQueue`
- `sqs:DeleteQueue`
- `sqs:GetQueueAttributes`
- `sqs:GetQueueUrl`
- `sqs:SetQueueAttributes`

구독자의 외부 ID 가져오기

구독자를 생성하려면 구독자의 AWS 계정 ID 외에 외부 ID도 가져와야 합니다. 외부 ID는 구독자가 제공하는 고유 식별자입니다. Security Lake는 생성한 구독자 IAM 역할에 외부 ID를 추가합니다. 외부 ID는 Security Lake 콘솔에서 구독자를 생성할 때, API 또는 AWS CLI를 통해 사용합니다.

외부 IDs에 대한 자세한 내용은 IAM 사용 설명서의 AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요.

> **Important**
>
> Security Lake 콘솔을 사용하여 구독자를 추가하려는 경우 다음 단계를 건너뛰고 Security Lake에서 데이터 액세스 권한이 있는 구독자 생성 단원으로 진행하면 됩니다. Security Lake

콘솔은 간소화된 시작 프로세스를 제공하며, 필요한 모든 IAM 역할을 생성하거나 사용자 대신 기존 역할을 사용합니다.
Security Lake API를 사용하거나 구독자를 AWS CLI 추가하려면 다음 단계를 계속 진행하여 EventBridge API 대상을 호출하는 IAM 역할을 생성합니다.

EventBridge API 대상을 호출하는 IAM 역할 생성(API 및 AWS CLI전용 단계)

API 또는를 통해 Security Lake를 사용하는 경우 AWS Identity and Access Management (IAM)에서 API 대상을 호출하고 올바른 HTTPS 엔드포인트로 객체 알림을 보낼 수 있는 권한을 Amazon EventBridge에 부여하는 역할을 AWS CLI생성합니다.

IAM 역할을 정의한 후에는 역할의 Amazon 리소스 이름(ARN)이 있어야 구독자를 생성합니다. 구독자가 Amazon Simple Queue Service (Amazon SQS) 대기열에서 데이터를 폴링하거나 AWS Lake Formation에서 데이터를 직접 쿼리하는 경우에는 이 IAM 역할이 필요하지 않습니다. 이런 종류의 데이터 액세스 방법 (액세스 유형) 에 대한 자세한 정보는 구독자를 위한 쿼리 액세스 관리을 참조하십시오.

다음과 같은 정책을 IAM 역할에 연결합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowInvokeApiDestination",
            "Effect": "Allow",
            "Action": [
                "events:InvokeApiDestination"
            ],
            "Resource": [
                "arn:aws:events:{us-west-2}:{123456789012}:api-destination/
AmazonSecurityLake*/*"
            ]
        }
    ]
}
```

다음 신뢰 정책을 IAM 역할에 연결하여 EventBridge가 역할을 맡도록 허용하십시오.

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "AllowEventBridgeToAssume",
            "Effect": "Allow",
            "Principal": {
                "Service": "events.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Security Lake는 구독자가 데이터 레이크에서 데이터를 읽을 수 있도록 허용하는 IAM 역할을 자동으로 생성합니다 (또는 선호하는 알림 방법인 경우 Amazon SQS 대기열에서 이벤트를 폴링할 수 있음). 이 역할은 라는 AWS 관리형 정책으로 보호됩니다`AmazonSecurityLakePermissionsBoundary`.

Security Lake에서 데이터 액세스 권한이 있는 구독자 생성

다음 액세스 방법 중 하나를 선택하여 현재의 데이터에 액세스할 수 있는 구독자를 생성합니다 AWS 리전.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 구독자를 생성할 리전을 선택합니다.
3. 탐색 창에서 구독자를 선택합니다.
4. 구독자 페이지에서 구독자 생성을 선택합니다.
5. 구독자 세부 정보를 보려면 구독자 이름과 설명 (선택 사항)을 입력합니다.

   리전은 현재 선택한 대로 자동으로 채워 AWS 리전 지며 수정할 수 없습니다.
6. 로그 및 이벤트 소스의 경우 구독자에게 사용 권한이 부여된 소스를 선택합니다.
7. 데이터 액세스 방법에서 S3를 선택하여 구독자에 대한 데이터 액세스를 설정합니다.
8. 구독자 자격 증명에 구독자의 AWS 계정 ID와 외부 ID를 입력합니다.
9. (선택 사항) 알림 세부 정보에서 구독자가 객체 알림을 위해 폴링할 수 있는 Amazon SQS 대기열을 Security Lake에서 생성하도록 하려면 SQS 대기열을 선택하십시오. Security Lake가 EventBridge를 통해 HTTPS 엔드포인트로 알림을 보내도록 하려면 구독 엔드포인트를 선택하십시오.

   구독 엔드포인트를 선택하는 경우 다음 작업도 수행하십시오.

a. 구독 엔드포인트를 입력합니다. **`http://example.com`**등 유효한 엔드포인트 형식의 예는 다음과 같습니다. 선택적으로 HTTPS 키 이름과 HTTPS 키 값을 제공할 수도 있습니다.

b. 서비스 액세스의 경우 새 IAM 역할을 생성하거나 EventBridge에 API 대상을 간접적으로 호출하고 객체 알림을 올바른 엔드포인트로 전송할 수 있는 권한을 부여하는 기존 IAM 역할을 사용하세요.

   새 IAM 역할을 생성하는 방법에 대한 자세한 내용은 EventBridge API 대상을 간접 호출하기 위한 IAM 역할 생성을 참조하십시오.

10. (선택 사항) 태그에는 구독자에게 할당할 태그를 50개까지 입력합니다.

    태그는 정의하여 특정 유형의 AWS 리소스에 할당할 수 있는 레이블입니다. 각 태그는 필수 태그 키 및 선택적 태그 값으로 구성됩니다. 태그를 사용하면 다양한 방식으로 리소스를 식별, 분류 및 관리할 수 있습니다. 자세한 내용은 Security Lake 리소스에 태그 지정을 참조하십시오.

11. 생성(Create)을 선택합니다.

API

프로그래밍 방식으로 데이터에 액세스할 수 있는 구독자를 만들려면 Security Lake API의 CreateSubscriber 작업을 사용하십시오. AWS Command Line Interface (AWS CLI)를 사용하는 경우 create-subscriber 명령을 실행합니다.

요청에서 이러한 파라미터를 사용하여 구독자에 대해 다음 설정을 지정합니다.

- `sources`의 경우 구독자가 액세스할 수 있는 각 소스를 지정하십시오.
- 의 경우 구독자가 소스 데이터에 액세스하는 데 사용할 AWS 계정 ID와 외부 ID를 `subscriberIdentity`지정합니다.
- 에서 구독자의 이름을 `subscriber-name`지정합니다.
- `accessTypes`에서 `S3`를 지정합니다.

예시 1

다음 예제에서는 소스에 대해 지정된 구독자 자격 증명에 대해 현재 AWS 리전의 데이터에 액세스할 수 AWS 있는 구독자를 생성합니다.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \
--sources [{"awsLogSource": {"sourceName": VPC_FLOW, "sourceVersion": 2.0}}] \
```

```
--subscriber-name subscriber name \
--access-types S3
```

예시 2

다음 예시에서는 사용자 지정 소스에 대해 지정된 구독자 자격 증명에 대해 현재 AWS 리전의 데이터에 액세스할 수 있는 구독자를 생성합니다.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 1293456789123,"externalId": 123456789012} \
--sources [{"customLogSource": {"sourceName": custom-source-name,
 "sourceVersion": 2.0}}] \
--subscriber-name subscriber name
--access-types S3
```

위의 예제는 Linux, macOS 또는 Unix용으로 포맷되어 있으며, 백슬래시(\) 줄 연속 문자를 사용하여 가독성을 개선합니다.

(선택 사항) 구독자를 만든 후 CreateSubscriberNotification 작업을 사용하여 구독자가 액세스하도록 하려는 소스의 데이터 레이크에 새 데이터가 기록될 때 구독자에게 알리는 방법을 지정합니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 create-subscriber-notification 명령을 실행합니다.

- 기본 알림 방법(HTTPS 엔드포인트)을 재정의하고 Amazon SQS 대기열을 생성하려면 `sqsNotificationConfiguration` 파라미터 값을 지정하세요.
- HTTPS 엔드포인트를 통한 알림을 선호하는 경우 `httpsNotificationConfiguration` 파라미터 값을 지정하십시오.
- `targetRoleArn` 필드에는 EventBridge API 대상을 간접 호출하기 위해 생성한 IAM 역할의 ARN을 지정합니다.

```
$ aws securitylake create-subscriber-notification \
--subscriber-id "12345ab8-1a34-1c34-1bd4-12345ab9012" \
--configuration
 httpsNotificationConfiguration={"targetRoleArn"="arn:aws:iam::XXX:role/service-
role/RoleName", "endpoint"="https://account-management.$3.$2.securitylake.aws.dev/
v1/datalake"}
```

를 가져오려면 Security Lake API의 ListSubscribers 작업을 `subscriberID`사용합니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 list-subscriber 명령을 실행합니다.

```
$ aws securitylake list-subscribers
```

이후에 구독자의 알림 방법(Amazon SQS 대기열 또는 HTTPS 엔드포인트)을 변경하려면 UpdateSubscriberNotification 작업을 사용하거나를 사용하는 경우 update-subscriber-notification 명령을 AWS CLI실행합니다. Security Lake 콘솔을 사용하여 알림 방법을 변경할 수도 있습니다. 구독자 페이지에서 구독자를 선택한 다음 편집을 선택합니다.

샘플 객체 알림 메시지의 예

다음 예제에서는 `CreateSubscriberNotification` 작업에 대한 이벤트 알림을 JSON 구조 형식으로 보여줍니다.

```
{
  "source": "aws.s3",
  "time": "2021-11-12T00:00:00Z",
  "account": "123456789012",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket"
  ],
  "detail": {
    "bucket": {
      "name": "amzn-s3-demo-bucket"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b57f9512698f4b09e608f4f2a65852e5"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "securitylake.amazonaws.com"
  }
}
```

Security Lake에서 데이터 구독자 업데이트

구독자가 소비하는 소스를 변경하여 구독자를 업데이트할 수 있습니다. 구독자에게 태그를 할당하거나 편집할 수도 있습니다. 태그는 구독자를 포함하여 특정 유형의 AWS 리소스에 정의 및 할당할 수 있는 레이블입니다. 자세한 내용은 Security Lake 리소스에 태그 지정을 참조하십시오.

액세스 방법 중 하나를 선택하고 다음 단계에 따라 기존 구독의 새 소스를 정의하십시오.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 구독자를 선택합니다.
3. 구독자를 선택합니다.
4. 편집을 선택한 후 다음 중 하나를 수행하십시오.
   - 구독자의 소스를 업데이트하려면 로그 및 이벤트 소스 섹션에 새 설정을 입력합니다.
   - 구독자에게 태그를 할당하거나 편집하려면 태그 섹션에서 필요에 따라 태그를 변경합니다.
5. 마쳤으면 저장을 선택합니다.

API

구독자의 데이터 액세스 소스를 프로그래밍 방식으로 업데이트하려면 Security Lake API의 UpdateSubscriber 작업을 사용하십시오. AWS Command Line Interface (AWS CLI)를 사용하는 경우 update-subscriber 명령을 실행합니다. 요청 시 `sources` 파라미터를 사용하여 구독자가 액세스할 수 있는 각 소스를 지정하십시오.

```
$ aws securitylake update-subscriber --subscriber-id subscriber ID
```

특정 AWS 계정 또는 조직과 연결된 구독자 목록은 ListSubscribers 작업을 사용합니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 list-subscribers 명령을 실행합니다.

```
$ aws securitylake list-subscribers
```

특정 구독자의 현재 설정을 검토하려면 GetSubscriber 작업을 사용합니다. get-subscriber 명령을 실행합니다. 그런 다음 Security Lake는 구독자의 이름과 설명, 외부 ID 및 추가 정보를 반환합니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 get-subscriber 명령을 실행합니다.

구독자에 대한 알림 방법을 업데이트하려면 UpdateSubscriberNotification 알림 작업을 사용하십시오. AWS Command Line Interface (AWS CLI)를 사용하는 경우 update-subscriber-notification 명령을 실행합니다. 예를 들어 구독자를 위해 새 HTTPS 엔드포인트를 지정하거나 HTTPS 엔드포인트에서 Amazon SQS 대기열로 전환할 수 있습니다.

Security Lake에서 데이터 구독자 제거

구독자가 Security Lake의 데이터를 더 이상 사용하지 않도록 하려면 다음 단계에 따라 구독자를 제거할 수 있습니다.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 구독자를 선택합니다.
3. 제거할 구독자를 선택합니다.
4. 삭제(Delete)를 선택하고 작업을 확인합니다. 그러면 구독자 및 모든 관련 알림 설정이 삭제됩니다.

API

시나리오에 따라 다음 중 하나를 수행합니다.

- 구독자 및 모든 관련 알림 설정을 삭제하려면 Security Lake API의 DeleteSubscriber 작업을 사용하십시오. AWS Command Line Interface (AWS CLI)를 사용하는 경우 delete-subscriber 명령을 실행합니다.
- 구독자는 유지하되 구독자에 대한 향후 알림을 중지하려면 Security Lake API의 DeleteSubscriberNotification 작업을 사용하십시오. AWS Command Line Interface (AWS CLI)를 사용하는 경우 delete-subscriber-notification 명령을 실행합니다.

구독자를 위한 쿼리 액세스 관리

쿼리 액세스 권한이 있는 구독자는 Security Lake가 수집하는 데이터를 쿼리할 수 있습니다. 이러한 구독자는 Amazon Athena와 같은 서비스를 사용하여 S3 버킷의 AWS Lake Formation 테이블을 직접 쿼리합니다. Security Lake의 기본 쿼리 엔진은 Athena이지만 AWS Glue Data Catalog와 통합되는 Amazon Redshift Spectrum 및 Spark SQL과 같은 다른 서비스를 사용할 수도 있습니다.

구독자는 Amazon Athena와 같은 서비스를 사용하여 S3 버킷의 AWS Lake Formation 테이블에서 소스 데이터를 쿼리합니다. 이 구독 유형은 CreateSubscriber API의 파라미터 `accessTypes`에서 `LAKEFORMATION`로 식별됩니다.

> **Note**
>
> 이 섹션에서는 타사 구독자에게 쿼리 액세스 권한을 부여하는 방법을 설명합니다. 자체 데이터 레이크에 대해 쿼리 실행에 대한 자세한 내용은 4단계: 자체 데이터 보기 및 쿼리을 참조하세요.

주제

- Security Lake에서 쿼리 액세스 권한이 있는 구독자를 생성하기 위한 사전 조건
- Security Lake에서 쿼리 액세스 권한이 있는 구독자 생성
- Security Lake에서 쿼리 액세스 권한이 있는 구독자 편집

Security Lake에서 쿼리 액세스 권한이 있는 구독자를 생성하기 위한 사전 조건

Security Lake에서 데이터 액세스 권한을 가진 구독자를 생성하려면 먼저 다음 사전 조건을 완료해야 합니다.

권한 확인

쿼리 액세스 권한이 있는 구독자를 생성하기 전에 다음 작업 목록을 수행할 권한이 있는지 확인하십시오.

권한을 확인하려면 IAM을 사용하여 IAM ID에 연결된 IAM 정책을 검토하십시오. 그런 다음 해당 정책의 정보를 쿼리 액세스 권한이 있는 구독자를 생성하기 위해 수행할 수 있어야 하는 다음 작업 목록과 비교하세요.

- `glue:PutResourcePolicy`
- `glue:DeleteResourcePolicy`
- `iam:CreateRole`
- `iam:DeleteRolePolicy`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `lakeformation:GrantPermissions`

- `lakeformation:ListPermissions`
- `lakeformation:RegisterResource`
- `lakeformation:RevokePermissions`
- `ram:GetResourceShareAssociations`
- `ram:GetResourceShares`
- `ram:UpdateResourceShare`

> **Important**
>
> 권한을 확인한 후:
>
> - Security Lake 콘솔을 사용하여 쿼리 액세스 권한이 있는 구독자를 추가하려는 경우 다음 단계를 건너뛰고 Lake Formation 관리자 권한 부여로 진행하면 됩니다. Security Lake는 사용자를 대신하여 필요한 모든 IAM 역할을 생성하거나 기존 역할을 사용합니다.
> - Security Lake API 또는 CLI를 사용하여 쿼리 액세스 권한이 있는 구독자를 추가하려는 경우 다음 단계를 계속 진행하여 Security Lake 데이터를 쿼리하는 IAM 역할을 생성합니다.

Security Lake 데이터를 쿼리하는 IAM 역할 생성(API 및 AWS CLI전용 단계)

Security Lake API를 사용하거나 구독자에게 쿼리 액세스 권한을 부여 AWS CLI 하려면 라는 역할을 생성해야 합니다`AmazonSecurityLakeMetaStoreManager`. Security Lake는이 역할을 사용하여 AWS Glue 파티션을 등록하고 AWS Glue 테이블을 업데이트합니다. 필요한 IAM 역할을 생성하는 동안 이 역할을 이미 생성했을 수 있습니다.

Lake Formation 관리자 권한 부여

또한 Security Lake 콘솔에 액세스하고 구독자를 추가하는 데 사용하는 IAM 역할에 Lake Formation 관리자 권한을 추가해야 합니다.

다음 단계에 따라 Lake Formation 관리자에게 역할에 권한을 부여할 수 있습니다.

1. Lake Formation 콘솔(https://console.aws.amazon.com/lakeformation/)을 엽니다.
2. 관리 사용자로 로그인
3. Welcome to Lake Formation 창이 나타나면 1단계에서 생성하거나 선택한 사용자를 선택한 다음 시작하기를 선택합니다.

4. Welcome to Lake Formation 창이 표시되지 않는 경우 다음 단계를 수행하여 Lake Formation 관리자를 구성하십시오.

   1. 탐색 창의 권한에서 관리자 역할 및 작업을 선택합니다. 데이터 레이크 관리자 섹션에서 관리자 선택을 선택합니다.
   2. 데이터 레이크 관리자 관리 대화 상자의 IAM 사용자 및 역할에서 Security Lake 콘솔에 액세스할 때 사용하는 관리자 역할을 선택한 다음 저장을 선택합니다.

데이터 레이크 관리자의 권한 변경에 대한 자세한 내용은 AWS Lake Formation 개발자 가이드의 데이터 레이크 관리자 생성을 참조하십시오.

IAM 역할에는 구독자에게 액세스 권한을 부여하려는 데이터베이스 및 테이블에 대한 SELECT 권한이 있어야 합니다. 이 작업을 수행하는 방법에 대한 지침은 AWS Lake Formation 개발자 안내서의 명명된 리소스 방법을 사용하여 데이터 카탈로그 권한 부여를 참조하십시오.

Security Lake에서 쿼리 액세스 권한이 있는 구독자 생성

원하는 방법을 선택하여 현재에서 쿼리 액세스 권한이 있는 구독자를 생성합니다 AWS 리전. 구독자는 생성된 에서만 데이터를 쿼리 AWS 리전 할 수 있습니다. 구독자를 생성하려면 구독자의 AWS 계정 ID와 외부 ID가 있어야 합니다. 외부 ID는 구독자가 사용자에게 제공하는 고유 식별자입니다. 외부 IDs에 대한 자세한 내용은 IAM 사용 설명서의 AWS 리소스에 대한 액세스 권한을 타사에 부여할 때 외부 ID를 사용하는 방법을 참조하세요.

> **Note**
>
> Security Lake는 Lake Formation 계정 간 데이터 공유 버전 1을 지원하지 않습니다. Lake Formation 크로스 계정 데이터 공유를 버전 2 또는 버전 3으로 업데이트해야 합니다. AWS Lake Formation 콘솔 또는 AWS CLI를 통해 교차 계정 버전 설정을 업데이트하는 단계는 AWS Lake Formation 개발자 안내서의 새 버전 활성화를 참조하세요.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.

   위임된 관리자 계정에 로그인하기
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 구독자를 생성할 리전을 선택합니다.
3. 탐색 창에서 구독자를 선택합니다.

4. 구독자 페이지에서 구독자 생성을 선택합니다.
5. 구독자 세부 정보를 보려면 구독자 이름과 설명 (선택 사항)을 입력합니다.

   리전은 현재 선택한 대로 자동으로 채워 AWS 리전 지며 수정할 수 없습니다.
6. 로그 및 이벤트 소스의 경우 쿼리 결과를 반환할 때 Security Lake에 포함할 소스를 선택합니다.
7. 데이터 액세스 방법에서 Lake Formation을 선택하여 구독자에 대한 쿼리 액세스를 생성합니다.
8. 구독자 자격 증명에 구독자의 AWS 계정 ID와 외부 ID를 입력합니다.
9. (선택 사항) 태그에는 구독자에게 할당할 태그를 50개까지 입력합니다.

   태그는 정의하여 특정 유형의 AWS 리소스에 할당할 수 있는 레이블입니다. 각 태그는 필수 태그 키 및 선택적 태그 값으로 구성됩니다. 태그를 사용하면 다양한 방식으로 리소스를 식별, 분류 및 관리할 수 있습니다. 자세한 내용은 Security Lake 리소스에 태그 지정을 참조하십시오.
10. 생성(Create)을 선택합니다.

API

프로그래밍 방식으로 쿼리 액세스 권한이 있는 구독자를 만들려면 Security Lake API의 CreateSubscriber 작업을 사용하십시오. AWS Command Line Interface (AWS CLI)를 사용하는 경우 create-subscriber 명령을 실행합니다.

요청에서 이러한 파라미터를 사용하여 구독자에 대해 다음 설정을 지정합니다.

- `accessTypes`에서 `LAKEFORMATION`를 지정합니다.
- `sources`에 대해 쿼리 결과를 반환할 때 Security Lake에 포함하려는 각 소스를 지정하십시오.
- 의 경우 구독자가 소스 데이터를 쿼리하는 데 사용하는 AWS 자격 증명과 외부 ID를 `subscriberIdentity`지정합니다.

다음 예시에서는 지정된 구독자 자격 증명에 대해 현재 AWS 리전에 쿼리 액세스 권한이 있는 구독자를 생성합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake create-subscriber \
--subscriber-identity {"accountID": 129345678912,"externalId": 123456789012} \
--sources [{"awsLogSource": {"sourceName": VPC_FLOW, "sourceVersion": 2.0}}] \
--subscriber-name subscriber name \
```

```
--access-types LAKEFORMATION
```

계정 간 테이블 공유 설정 (구독자 단계)

Security Lake는 Lake Formation 크로스 계정 테이블 공유를 사용하여 구독자 쿼리 액세스를 지원합니다. Security Lake 콘솔, API 또는에서 쿼리 액세스 권한이 있는 구독자를 생성하면 AWS CLI Security Lake는 AWS Resource Access Manager ()에서 리소스 공유를 생성하여 구독자와 관련 Lake Formation 테이블에 대한 정보를 공유합니다AWS RAM.

쿼리 액세스 권한이 있는 구독자를 특정 유형으로 편집하면 Security Lake에서 새 리소스 공유를 생성합니다. 자세한 내용은 Security Lake에서 쿼리 액세스 권한이 있는 구독자 편집 단원을 참조하십시오.

구독자는 다음 단계에 따라 Lake Formation 테이블의 데이터를 사용해야 합니다.

1. 리소스 공유 수락 - 구독자는 구독자를 만들거나 편집할 때 생성되는 `resourceShareArn` 및 `resourceShareName`을 지닌 해당 리소스 공유를 수락해야 합니다. 다음 방법 중 한 가지를 선택하세요.
   - 콘솔 및의 경우에서 리소스 공유 초대 수락을 AWS CLI참조하세요. AWS RAM
   - API의 경우 GetResourceShareInvitations API를 간접 호출하십시오. `resourceShareArn` 및 `resourceShareName` 기준으로 필터링하여 올바른 리소스 공유를 찾아보세요. AcceptResourceShareInvitation API를 사용하여 초대를 수락합니다.

   리소스 공유 초대는 12시간 후에 만료되므로 12시간 이내에 초대를 확인하고 수락해야 합니다. 초대장이 만료되어도 초대장은 특정 `PENDING` 상태로 계속 표시되지만 수락해도 공유 리소스에 액세스할 수 있는 권한은 없습니다. 12시간이 지난 경우 Lake Formation 구독자를 삭제하고 구독자를 다시 생성하여 새 리소스 공유 초대장을 받으세요.
2. 공유 데이터베이스에 대한 리소스 링크 생성 - 구독자는 AWS Lake Formation (콘솔을 사용하는 경우) 또는 AWS Glue (API/AWS CLI를 사용하는 경우)에서 공유 Lake Formation 데이터베이스에 대한 리소스 링크를 생성해야 합니다. 이 리소스 링크는 구독자의 계정을 공유 데이터베이스로 가리킵니다. 다음 액세스 방법 중 한 가지를 선택하세요.
   - 콘솔 및의 경우 AWS Lake Formation 개발자 안내서의 공유 데이터 카탈로그 데이터베이스에 대한 리소스 링크 생성을 AWS CLI참조하세요. https://docs.aws.amazon.com/lake-formation/latest/dg/create-resource-link-database.html
   - 구독자는 CreateDatabase API로 고유한 데이터베이스를 만들어 리소스 링크 테이블을 저장하는 것도 좋습니다.
3. 공유 테이블 쿼리 — Amazon Athena와 같은 서비스는 테이블을 직접 참조할 수 있으며 Security Lake가 수집하는 새 데이터를 자동으로 쿼리할 수 있습니다. 쿼리는 구독자의에서 실행 AWS 계정

되며 쿼리로 인해 발생한 비용은 구독자에게 청구됩니다. 자신의 Security Lake 계정에 있는 리소스에 대한 읽기 액세스를 제어할 수 있습니다.

계정 간 권한 부여에 대한 자세한 내용은 AWS Lake Formation 개발자 안내서의 Lake Formation에서의 계정 간 데이터 공유를 참조하십시오.

Security Lake에서 쿼리 액세스 권한이 있는 구독자 편집

Security Lake는 쿼리 액세스 권한이 있는 구독자를 편집할 수 있도록 지원합니다. 구독자의 이름, 설명, 외부 ID, 보안 주체(AWS 계정 ID) 및 구독자가 사용할 수 있는 로그 소스를 편집할 수 있습니다. 원하는 방법을 선택하고 단계에 따라 현재 AWS 리전내 쿼리 액세스 권한이 있는 구독자를 편집하십시오.

> **Note**
>
> Security Lake는 Lake Formation 계정 간 데이터 공유 버전 1을 지원하지 않습니다. Lake Formation 크로스 계정 데이터 공유를 버전 2 또는 버전 3으로 업데이트해야 합니다. AWS Lake Formation 콘솔 또는 AWS CLI를 통해 교차 계정 버전 설정을 업데이트하는 단계는 AWS Lake Formation 개발자 안내서의 새 버전 활성화를 참조하세요.

Console

편집하려는 세부 정보에 따라 해당 작업에 대해 제공된 단계만 따르십시오.

구독자 이름을 편집하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.

   위임된 관리자 계정에 로그인하기
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 구독자 세부 정보를 편집할 리전을 선택합니다.
3. 탐색 창에서 구독자를 선택합니다.
4. 구독자 페이지에서 라디오 버튼을 사용하여 편집하려는 구독자를 선택합니다. 선택한 구독자의 데이터 액세스 방법은 LAKEFORMATION이어야 합니다.
5. 편집을 선택합니다.
6. 새 구독자 이름을 입력하고 저장을 선택합니다.

구독자 설명을 편집하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.

   위임된 관리자 계정에 로그인하기
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 구독자를 편집할 리전을 선택합니다.
3. 탐색 창에서 구독자를 선택합니다.
4. 구독자 페이지에서 라디오 버튼을 사용하여 편집하려는 구독자를 선택합니다. 선택한 구독자의 데이터 액세스 방법은 LAKEFORMATION이어야 합니다.
5. 편집을 선택합니다.
6. 구독자에 대한 새 설명을 입력하고 저장을 선택합니다.

외부 ID를 편집하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.

   위임된 관리자 계정에 로그인하기
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 구독자 세부 정보를 편집할 리전을 선택합니다.
3. 탐색 창에서 구독자를 선택합니다.
4. 구독자 페이지에서 라디오 버튼을 사용하여 편집하려는 구독자를 선택합니다. 선택한 구독자의 데이터 액세스 방법은 LAKEFORMATION이어야 합니다.
5. 편집을 선택합니다.
6. 구독자가 제공한 새 외부 ID를 입력하고 저장을 선택합니다.

   새 외부 ID를 저장하면 이전 AWS RAM 리소스 공유가 자동으로 제거되고 구독자에 대한 새 리소스 공유가 생성됩니다.
7. 구독자는 계정 간 테이블 공유 설정 (구독자 단계)의 1단계에 따라 새 리소스 공유를 수락해야 합니다. 구독자 세부 정보에 표시되는 Amazon 리소스 이름(ARN) 이 Lake Formation 콘솔과 동일한지 확인하십시오. 공유 테이블에 대한 리소스 링크는 그대로 유지되므로 구독자는 새 리소스 링크를 생성할 필요가 없습니다.

보안 주체(AWS 계정 ID)를 편집하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.

위임된 관리자 계정에 로그인하기

2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 구독자 세부 정보를 편집할 리전을 선택합니다.
3. 탐색 창에서 구독자를 선택합니다.
4. 구독자 페이지에서 라디오 버튼을 사용하여 편집하려는 구독자를 선택합니다. 선택한 구독자의 데이터 액세스 방법은 LAKEFORMATION이어야 합니다.
5. 편집을 선택합니다.
6. 구독자의 새 AWS 계정 ID를 입력하고 저장을 선택합니다.

   새 계정 ID를 저장하면 이전 보안 주체가 로그 및 이벤트 소스를 사용할 수 없도록 이전 AWS RAM 리소스 공유가 자동으로 제거됩니다. Security Lake는 새 리소스 공유를 생성합니다.
7. 구독자는 새 보안 주체의 자격 증명을 사용하여 새 리소스 공유를 수락하고 공유 테이블에 대한 리소스 링크를 생성해야 합니다. 이렇게 하면 새 보안 주체가 공유 리소스에 액세스할 수 있습니다. 지침은 계정 간 테이블 공유 설정 (구독자 단계)의 1 및 2단계를 참조하십시오. 구독자 세부 정보에 표시되는 ARN이 Lake Formation 콘솔에 표시되는 ARN과 동일한지 확인하십시오.

로그 및 이벤트 소스를 편집하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.

   위임된 관리자 계정에 로그인하기
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 구독자 세부 정보를 편집할 리전을 선택합니다.
3. 탐색 창에서 구독자를 선택합니다.
4. 구독자 페이지에서 라디오 버튼을 사용하여 편집하려는 구독자를 선택합니다. 선택한 구독자의 데이터 액세스 방법은 LAKEFORMATION이어야 합니다.
5. 편집을 선택합니다.
6. 기존 소스를 선택 취소하거나 추가하려는 소스를 선택합니다. 소스를 선택 취소하면 사용자가 추가 조치를 취하지 않아도 됩니다. 소스를 추가하도록 선택하면 새 리소스 공유 초대가 생성되지 않습니다. 하지만 Security Lake는 추가된 소스를 기반으로 공유 Lake Formation 테이블을 업데이트합니다. 구독자는 업데이트된 공유 테이블에 대한 리소스 링

크를 생성해야 소스 데이터를 쿼리할 수 있습니다. 지침은 계정 간 테이블 공유 설정 (구독자 단계)의 2단계를 참조하십시오.

7. 저장(Save)을 선택합니다.

API

쿼리 액세스 권한이 있는 구독자를 프로그래밍 방식으로 편집하려면 Security Lake API의 UpdateSubscriber 작업을 사용하십시오. AWS Command Line Interface (AWS CLI)를 사용하는 경우 update-subscriber 명령을 실행합니다. 요청 시 지원되는 파라미터를 사용하여 구독자에 대해 다음 설정을 지정하십시오.

- `subscriberName`의 경우 새 구독자 이름을 지정합니다.
- `subscriberDescription`의 경우 새 설명을 지정합니다.
- 의 경우 구독자가 소스 데이터를 쿼리하는 데 사용할 보안 주체(AWS 계정 ID) 및 외부 ID를 `subscriberIdentity`지정합니다. 주체 ID와 외부 ID를 모두 제공해야 합니다. 이러한 값 중 하나를 동일하게 유지하려면 현재 값을 전달하십시오.
  - 외부 ID만 업데이트 - 이 작업을 수행하면 이전 AWS RAM 리소스 공유가 제거되고 구독자를 위한 새 리소스 공유가 생성됩니다. 구독자는 계정 간 테이블 공유 설정 (구독자 단계)의 1단계에 따라 새 리소스 공유를 수락해야 합니다. 공유 테이블에 대한 리소스 링크는 그대로 유지되므로 구독자는 새 리소스 링크를 생성할 필요가 없습니다.
  - 보안 주체만 업데이트 -이 작업은 이전 보안 주체가 로그 및 이벤트 소스를 사용할 수 없도록 이전 AWS RAM 리소스 공유를 제거합니다. Security Lake는 새 리소스 공유를 생성합니다. 구독자는 새 보안 주체의 자격 증명을 사용하여 새 리소스 공유를 수락하고 공유 테이블에 대한 리소스 링크를 생성해야 합니다. 이렇게 하면 새 보안 주체가 공유 리소스에 액세스할 수 있습니다. 지침은 계정 간 테이블 공유 설정 (구독자 단계)의 1 및 2단계를 참조하십시오.

  외부 ID 및 보안 주체를 업데이트하려면 계정 간 테이블 공유 설정 (구독자 단계)의 1단계와 2단계를 따르세요.
- `sources`의 경우, 기존 소스를 제거하거나 추가하려는 소스를 지정하십시오. 소스를 삭제하면 추가 조치가 필요하지 않습니다. 소스를 추가하면 새 리소스 공유 초대가 생성되지 않습니다. 하지만 Security Lake는 추가된 소스를 기반으로 공유 Lake Formation 테이블을 업데이트합니다. 구독자는 업데이트된 공유 테이블에 대한 리소스 링크를 생성해야 소스 데이터를 쿼리할 수 있습니다. 지침은 계정 간 테이블 공유 설정 (구독자 단계)의 2단계를 참조하십시오.

Security Lake 쿼리

Security Lake가 AWS Lake Formation 데이터베이스 및 테이블에 저장하는 데이터를 쿼리할 수 있습니다. Security Lake 콘솔, API 또는 AWS CLI에서 타사 구독자를 생성할 수도 있습니다. 타사 구독자는 지정한 소스에서 Lake Formation 데이터를 쿼리할 수도 있습니다.

Lake Formation 데이터 레이크 관리자는 데이터를 쿼리하는 IAM ID에 관련 데이터베이스 및 테이블에 대한 `SELECT` 권한을 부여해야 합니다. 또한 Security Lake에서 구독자를 생성해야 데이터를 쿼리할 수 있습니다. 쿼리 액세스 권한이 있는 구독자를 만드는 방법에 대한 자세한 내용은 구독자를 위한 쿼리 액세스 관리를 참조하십시오.

보존 설정을 사용하여 데이터 쿼리

> Amazon S3 수명 주기 설정은 데이터가 보관되는 기간에 영향을 미치며, 이는 쿼리할 수 있는 시간에 영향을 미칩니다. Security Lake에서 보존 설정을 구성한 경우 쿼리에 시간 기반 필터를 포함하여 결과 집합이 만료되지 않은 데이터 파일로 범위가 지정되도록 해야 합니다. Security Lake의 데이터 보존에 대한 자세한 내용은 섹션을 참조하세요수명 주기 관리.

다음 섹션의 쿼리 예제에는이 모범 사례를 보여주기 `time_dt`위해 `eventDay` 또는와 같은 시간 기반 필터가 포함되어 있습니다.

주제

- AWS 소스 버전 1(OCSF 1.0.0-rc.2)에 대한 Security Lake 쿼리
- AWS 소스 버전 2(OCSF 1.1.0)에 대한 Security Lake 쿼리

AWS 소스 버전 1(OCSF 1.0.0-rc.2)에 대한 Security Lake 쿼리

다음 섹션에서는 Security Lake에서 데이터를 쿼리하는 방법에 대한 지침을 제공하며 AWS 소스 버전 1에서 기본적으로 지원되는 AWS 소스에 대한 몇 가지 쿼리 예제를 포함합니다. 이러한 쿼리는 특정의 데이터를 검색하도록 설계되었습니다 AWS 리전. 이 예시에서는 us-east-1 (미국 동부 (버지니아 북부))을 사용합니다. 또한 예제 쿼리는 최대 25개의 레코드를 반환하는 `LIMIT 25` 파라미터를 사용합니다. 이 파라미터를 생략하거나 원하는 대로 조정할 수 있습니다. 더 많은 예를 보려면 Amazon Security Lake OCSF 쿼리 GitHub 디렉터리를 참조하십시오.

다음 쿼리에는 `eventDay`를 사용하여 쿼리가 구성된 보존 설정 내에 있는지 확인하는 시간 기반 필터가 포함됩니다. 자세한 내용은 Querying data with retention settings 단원을 참조하십시오.

예를 들어 60일보다 오래된 데이터가 만료된 경우 쿼리에는 만료된 데이터에 액세스하지 못하도록 하는 시간 제약이 포함되어야 합니다. 60일의 보존 기간 동안 쿼리에 다음 절을 포함시킵니다.

```
...
WHERE eventDay BETWEEN cast(date_format(current_date - INTERVAL '59' day, '%Y%m%d') AS
 varchar)
                   AND cast(date_format(current_date, '%Y%m%d') AS varchar)
...
```

이 절은 Amazon S3와 Apache Iceberg 간의 데이터 또는 시간 중복을 방지하기 위해 59일(60일 아님)을 사용합니다.

로그 소스 테이블

Security Lake 데이터를 쿼리할 때는 데이터가 있는 Lake Formation 테이블의 이름을 포함해야 합니다.

```
SELECT *
   FROM
 amazon_security_lake_glue_db_DB_Region.amazon_security_lake_table_DB_Region_SECURITY_LAKE_TABL
   WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
   LIMIT 25
```

로그 소스 테이블의 일반적인 값은 다음과 같습니다.

- `cloud_trail_mgmt_1_0` - AWS CloudTrail 관리 이벤트
- `lambda_execution_1_0`— Lambda에 대한 CloudTrail 데이터 이벤트
- `s3_data_1_0`— S3에 대한 CloudTrail 데이터 이벤트
- `route53_1_0` – Amazon Route 53 Resolver 쿼리 로그
- `sh_findings_1_0` – AWS Security Hub 조사 결과
- `vpc_flow_1_0` – Amazon Virtual Private Cloud(VPC) 흐름 로그

예: 미국 동부 1 리전의 표 **`sh_findings_1_0`**에 있는 모든 Security Hub 조사 결과

```
SELECT *
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
   LIMIT 25
```

데이터베이스 리전

Security Lake 데이터를 쿼리할 때는 데이터를 쿼리하려는 데이터베이스 리전의 이름을 포함해야 합니다. 현재 Security Lake를 사용할 수 있는 데이터베이스 리전의 전체 목록은 Amazon Security Lake 엔드포인트를 참조하십시오.

예: 소스 IP의 AWS CloudTrail 활동 나열

다음 예시는 *us-east-1* DB_Region의 *cloud_trail_mgmt_1_0* 테이블에 *20230301* (2023년 3월 1일) 이후에 기록된 소스 IP *192.0.2.1*의 모든 CloudTrail 활동을 나열합니다.

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > '20230301' AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

파티션 날짜

데이터를 분할하면 각 쿼리가 스캔하는 데이터의 양을 제한하여 성능을 향상시키고 비용을 절감할 수 있습니다. Security Lake는 `eventDay`, `region` 및 `accountid` 파라미터를 통해 파티셔닝을 구현합니다. `eventDay` 파티션은 형식 `YYYYMMDD`을 사용합니다.

다음은 `eventDay` 파티션을 사용한 예제 쿼리입니다.

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
```

```
    WHERE eventDay > '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
```

eventDay에 대한 공통값은 다음과 같습니다.

최근 1년 동안 발생한 이벤트

```
> cast(date_format(current_timestamp - INTERVAL '1' year, '%Y%m%d%H') as varchar)
```

지난 1개월 동안 발생한 이벤트

```
> cast(date_format(current_timestamp - INTERVAL '1' month, '%Y%m%d%H') as varchar)
```

지난 30일 동안 발생한 이벤트

```
> cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d%H') as varchar)
```

지난 12시간 동안 발생한 이벤트

```
> cast(date_format(current_timestamp - INTERVAL '12' hour, '%Y%m%d%H') as varchar)
```

지난 5분간 발생한 이벤트

```
> cast(date_format(current_timestamp - INTERVAL '5' minute, '%Y%m%d%H') as varchar)
```

7~14일 전에 발생한 이벤트

```
BETWEEN cast(date_format(current_timestamp - INTERVAL '14' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar)
```

특정 날짜 또는 이후에 발생하는 이벤트

```
>= '20230301'
```

예: 2023년 3월 1일 또는 이후 소스 IP **192.0.2.1**의 모든 CloudTrail 활동 목록이 표 **cloud_trail_mgmt_1_0**에 나와 있습니다.

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay >= '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

예: 최근 30일 동안 소스 IP **192.0.2.1**의 모든 CloudTrail 활동이 표 **cloud_trail_mgmt_1_0**에 나열되어 있습니다.

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

CloudTrail 데이터에 대한 Security Lake 쿼리 예제

AWS CloudTrail 는에서 사용자 활동 및 API 사용량을 추적합니다 AWS 서비스. 구독자는 CloudTrail 데이터를 쿼리하여 다음 유형의 정보를 학습할 수 있습니다.

다음은 AWS 소스 버전 1에 대한 CloudTrail 데이터의 몇 가지 예제 쿼리입니다.

지난 7일 AWS 서비스 동안에 대한 무단 시도

```
SELECT
      time,
      api.service.name,
      api.operation,
      api.response.error,
      api.response.message,
      unmapped['responseElements'],
      cloud.region,
      actor.user.uuid,
```

```
      src_endpoint.ip,
      http_request.user_agent
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND api.response.error in (
        'Client.UnauthorizedOperation',
        'Client.InvalidPermission.NotFound',
        'Client.OperationNotPermitted',
        'AccessDenied')
    ORDER BY time desc
    LIMIT 25
```

최근 7일간 소스 IP **192.0.2.1**의 모든 CloudTrail 활동 목록

```
SELECT
      api.request.uid,
      time,
      api.service.name,
      api.operation,
      cloud.region,
      actor.user.uuid,
      src_endpoint.ip,
      http_request.user_agent
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '127.0.0.1.'
    ORDER BY time desc
    LIMIT 25
```

지난 7일간의 모든 IAM 활동 목록

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
```

```
      AND api.service.name = 'iam.amazonaws.com'
    ORDER BY time desc
    LIMIT 25
```

지난 7일 동안 자격 증명 **AIDACKCEVSQ6C2EXAMPLE**이 사용된 인스턴스

```
SELECT
      actor.user.uid,
      actor.user.uuid,
      actor.user.account_uid,
      cloud.region
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND actor.user.credential_uid = 'AIDACKCEVSQ6C2EXAMPLE'
      LIMIT 25
```

지난 7일간 실패한 CloudTrail 레코드 목록

```
SELECT
      actor.user.uid,
      actor.user.uuid,
      actor.user.account_uid,
      cloud.region
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE status='failed' and eventDay BETWEEN cast(date_format(current_timestamp -
 INTERVAL '7' day, '%Y%m%d%H') as varchar) and cast(date_format(current_timestamp -
 INTERVAL '0' day, '%Y%m%d%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

Route 53 해석기 쿼리 로그에 대한 Security Lake 쿼리 예제

Amazon Route 53 Resolver 쿼리 로그는 아마존 VPC 내 리소스에서 만든 DNS 쿼리를 추적합니다. 구독자는 Route 53 Resolver 쿼리 로그를 쿼리하여 다음 유형의 정보를 학습할 수 있습니다.

다음은 AWS 소스 버전 1에 대한 Route 53 해석기 쿼리 로그의 몇 가지 예제 쿼리입니다.

최근 7일간 CloudTrail에서 발생한 DNS 쿼리 목록

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

지난 7일 동안 **s3.amazonaws.com**와 일치하는 DNS 쿼리 목록

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
      answers
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE query.hostname LIKE 's3.amazonaws.com.' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    ORDER BY time DESC
    LIMIT 25
```

지난 7일 동안 해결되지 않은 DNS 쿼리 목록

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
```

```
      answers
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    WHERE cardinality(answers) = 0 and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

지난 7일 동안 **192.0.2.1**에 해결된 DNS 쿼리 목록

```
SELECT
      time,
      src_endpoint.instance_uid,
      src_endpoint.ip,
      src_endpoint.port,
      query.hostname,
      rcode,
      answer.rdata
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_route53_1_0
    CROSS JOIN UNNEST(answers) as st(answer)
    WHERE answer.rdata='192.0.2.1' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

Security Hub 조사 결과에 대한 Security Lake 쿼리 예제

Security Hub는에서 보안 상태를 포괄적으로 볼 수 있게 해 AWS 주며 보안 업계 표준 및 모범 사례를 기준으로 환경을 확인하는 데 도움이 됩니다. Security Hub는 보안 검사 조사 결과를 생성하고 타사 서비스로부터 조사 결과를 수신합니다.

Security Hub 조사 결과에 대한 몇 가지 예제 쿼리는 다음과 같습니다.

지난 7일간의 심각도가 **MEDIUM**이상인 새로운 조사 결과

```
SELECT
      time,
      finding,
      severity
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0_fi
```

```
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND severity_id >= 3
      AND state_id = 1
    ORDER BY time DESC
    LIMIT 25
```

지난 7일간의 중복된 조사 결과

```
SELECT
    finding.uid,
    MAX(time) AS time,
    ARBITRARY(region) AS region,
    ARBITRARY(accountid) AS accountid,
    ARBITRARY(finding) AS finding,
    ARBITRARY(vulnerabilities) AS vulnerabilities
FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d
%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H')
 as varchar)
GROUP BY finding.uid
LIMIT 25
```

지난 7일간의 모든 정보 외 조사 결과

```
SELECT
      time,
      finding.title,
      finding,
      severity
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE severity != 'Informational' and eventDay BETWEEN
 cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m%d%H') as varchar) and
 cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d%H') as varchar)
    LIMIT 25
```

리소스가 Amazon S3 버킷인 경우 조사 결과 (시간 제한 없음)

```
SELECT *
```

```
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE any_match(resources, element -> element.type = 'amzn-s3-demo-bucket')
   LIMIT 25
```

CVSS (Common Vulnerability Scoring System) 점수가 **1** (시간 제한 없음) 보다 높은 조사 결과

```
SELECT *
   FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
   WHERE any_match(vulnerabilities, element -> element.cve.cvss.base_score > 1.0)
   LIMIT 25
```

일반적인 취약성 및 노출도 (CVE) **CVE-0000-0000**와 일치하는 조사 결과 (시간 제한 없음)

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE any_match(vulnerabilities, element -> element.cve.uid = 'CVE-0000-0000')
    LIMIT 25
```

지난 7일 동안 Security Hub에서 조사 결과를 전송한 제품 수

```
SELECT
      metadata.product.feature.name,
      count(*)
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    GROUP BY metadata.product.feature.name
    ORDER BY metadata.product.feature.name DESC
    LIMIT 25
```

지난 7일간의 조사 결과에 포함된 리소스 유형 수

```
SELECT
      count(*),
      resource.type
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
```

```
        CROSS JOIN UNNEST(resources) as st(resource)
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    GROUP BY resource.type
    LIMIT 25
```

지난 7일간의 조사 결과에서 나온 취약한 패키지

```
SELECT
      vulnerability
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0,
    UNNEST(vulnerabilities) as t(vulnerability)
    WHERE vulnerabilities is not null
    LIMIT 25
```

지난 7일 동안 변경된 조사 결과

```
SELECT
    finding.uid,
    finding.created_time,
    finding.first_seen_time,
    finding.last_seen_time,
    finding.modified_time,
    finding.title,
    state
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_sh_findings_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    LIMIT 25
```

Amazon VPC 흐름 로그에 대한 Security Lake 쿼리 예제

Amazon Virtual Private Cloud(VPC)는 VPC의 네트워크 인터페이스에서 양쪽에서 이동하는 IP 트래픽에 대한 세부 정보를 제공합니다.

다음은 AWS 소스 버전 1에 대한 Amazon VPC 흐름 로그의 몇 가지 예제 쿼리입니다.

지난 7일 AWS 리전 동안 특정의 트래픽

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND region in ('us-east-1','us-east-2','us-west-2')
    LIMIT 25
```

최근 7일간 소스 IP **192.0.2.1** 및 소스 포트 **22**의 활동 목록

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND src_endpoint.ip = '192.0.2.1'
      AND src_endpoint.port = 22
    LIMIT 25
```

지난 7일간의 고유 대상 IP 주소 수

```
SELECT
    COUNT(DISTINCT dst_endpoint.ip)
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
    LIMIT 25
```

지난 7일 동안의 198.51.100.0/24에서 발생한 트래픽

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
```

```
    AND split_part(src_endpoint.ip,'.', 1)='198'AND split_part(src_endpoint.ip,'.',
 2)='51'
    LIMIT 25
```

지난 7일간의 모든 HTTPS 트래픽

```
SELECT
      dst_endpoint.ip as dst,
      src_endpoint.ip as src,
      traffic.packets
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND dst_endpoint.port = 443
    GROUP BY
      dst_endpoint.ip,
      traffic.packets,
      src_endpoint.ip
    ORDER BY traffic.packets DESC
    LIMIT 25
```

지난 7일 동안 포트 **443**로 향하는 연결의 패킷 수를 기준으로 정렬합니다.

```
SELECT
      traffic.packets,
      dst_endpoint.ip
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND dst_endpoint.port = 443
    GROUP BY
      traffic.packets,
      dst_endpoint.ip
    ORDER BY traffic.packets DESC
    LIMIT 25
```

지난 7일간의 IP **192.0.2.1** 및 **192.0.2.2** 간 모든 트래픽

```
SELECT
      start_time,
      end_time,
      src_endpoint.interface_uid,
      connection_info.direction,
      src_endpoint.ip,
      dst_endpoint.ip,
      src_endpoint.port,
      dst_endpoint.port,
      traffic.packets,
      traffic.bytes
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND(
        src_endpoint.ip = '192.0.2.1'
        AND dst_endpoint.ip = '192.0.2.2')
      OR (
        src_endpoint.ip = '192.0.2.2'
        AND dst_endpoint.ip = '192.0.2.1')
    ORDER BY start_time ASC
    LIMIT 25
```

지난 7일간의 모든 인바운드 트래픽

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND connection_info.direction = 'ingress'
    LIMIT 25
```

지난 7일간의 모든 아웃바운드 트래픽

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
```

```
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND connection_info.direction = 'egress'
    LIMIT 25
```

지난 7일간 거부된 모든 트래픽

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_vpc_flow_1_0
    WHERE eventDay BETWEEN cast(date_format(current_timestamp - INTERVAL '7' day, '%Y%m
%d%H') as varchar) and cast(date_format(current_timestamp - INTERVAL '0' day, '%Y%m%d
%H') as varchar)
      AND type_uid = 400105
    LIMIT 25
```

AWS 소스 버전 2(OCSF 1.1.0)에 대한 Security Lake 쿼리

다음 섹션에서는 Security Lake에서 데이터를 쿼리하는 방법에 대한 지침을 제공하며 AWS 소스 버전 2에서 기본적으로 지원되는 AWS 소스에 대한 몇 가지 쿼리 예제를 포함합니다. 이러한 쿼리는 특정의 데이터를 검색하도록 설계되었습니다 AWS 리전. 이 예시에서는 us-east-1 (미국 동부 (버지니아 북부))을 사용합니다. 또한 예제 쿼리는 최대 25개의 레코드를 반환하는 `LIMIT 25` 파라미터를 사용합니다. 이 파라미터를 생략하거나 원하는 대로 조정할 수 있습니다. 더 많은 예를 보려면 Amazon Security Lake OCSF 쿼리 GitHub 디렉터리를 참조하십시오.

Security Lake가 AWS Lake Formation 데이터베이스 및 테이블에 저장하는 데이터를 쿼리할 수 있습니다. Security Lake 콘솔, API 또는 AWS CLI에서 타사 구독자를 생성할 수도 있습니다. 타사 구독자는 지정한 소스에서 Lake Formation 데이터를 쿼리할 수도 있습니다.

Lake Formation 데이터 레이크 관리자는 데이터를 쿼리하는 IAM ID에 관련 데이터베이스 및 테이블에 대한 `SELECT` 권한을 부여해야 합니다. 또한 Security Lake에서 구독자를 생성해야 데이터를 쿼리할 수 있습니다. 쿼리 액세스 권한이 있는 구독자를 만드는 방법에 대한 자세한 내용은 구독자를 위한 쿼리 액세스 관리를 참조하십시오.

다음 쿼리에는 `eventDay`를 사용하여 쿼리가 구성된 보존 설정 내에 있는지 확인하는 시간 기반 필터가 포함됩니다. 자세한 내용은 Querying data with retention settings 단원을 참조하십시오.

예를 들어 60일보다 오래된 데이터가 만료된 경우 쿼리에는 만료된 데이터에 액세스하지 못하도록 하는 시간 제약이 포함되어야 합니다. 60일 보존 기간 동안 쿼리에 다음 절을 포함시킵니다.

```
...
WHERE time_dt > DATE_ADD('day', -59, CURRENT_TIMESTAMP)
...
```

이 절은 Amazon S3와 Apache Iceberg 간의 데이터 또는 시간 중복을 방지하기 위해 59일(60일 아님)을 사용합니다.

로그 소스 테이블

Security Lake 데이터를 쿼리할 때는 데이터가 있는 Lake Formation 테이블의 이름을 포함해야 합니다.

```
SELECT *
FROM
 "amazon_security_lake_glue_db_DB_Region"."amazon_security_lake_table_DB_Region_SECURITY_LAKE_T
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

로그 소스 테이블의 일반적인 값은 다음과 같습니다.

- `cloud_trail_mgmt_2_0` – AWS CloudTrail 관리 이벤트
- `lambda_execution_2_0`— Lambda에 대한 CloudTrail 데이터 이벤트
- `s3_data_2_0`— S3에 대한 CloudTrail 데이터 이벤트
- `route53_2_0` – Amazon Route 53 Resolver 쿼리 로그
- `sh_findings_2_0` – AWS Security Hub 조사 결과
- `vpc_flow_2_0` – Amazon Virtual Private Cloud(VPC) 흐름 로그
- `eks_audit_2_0` - Amazon Elastic Kubernetes Service(Amazon EKS) 감사 로그
- `waf_2_0` – AWS WAF v2 로그

예: 미국 동부 1 리전의 표 **`sh_findings_2_0`**에 있는 모든 Security Hub 조사 결과

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

데이터베이스 리전

Security Lake 데이터를 쿼리할 때는 데이터를 쿼리하려는 데이터베이스 리전의 이름을 포함해야 합니다. 현재 Security Lake를 사용할 수 있는 데이터베이스 리전의 전체 목록은 Amazon Security Lake 엔드포인트를 참조하십시오.

예: 소스 IP에서 Amazon Virtual Private Cloud 활동 나열

다음 예제에서는 *us-west-2# vpc_flow_2_0 #### 3# 1#(2023# 3# 1#) ### ### ## IP 192.*0.2.1의 모든 Amazon VPC 활동을 나열합니다DB_Region. *20230301*

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
    WHERE time_dt > TIMESTAMP '2023-03-01'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time_dt desc
LIMIT 25
```

파티션 날짜

데이터를 분할하면 각 쿼리가 스캔하는 데이터의 양을 제한하여 성능을 향상시키고 비용을 절감할 수 있습니다. 파티션은 Security Lake 1.0과 비교하여 Security Lake 2.0에서 약간 다르게 작동합니다. Security Lake는 이제 `time_dt`, `region`및를 통해 파티셔닝을 구현합니다`accountid`. 반면 Security Lake 1.0은 , `eventDay` `region`및 `accountid` 파라미터를 통해 파티셔닝을 구현했습니다.

쿼리`time_dt`는 S3에서 날짜 파티션을 자동으로 생성하며 Athena의 모든 시간 기반 필드와 마찬가지로 쿼리할 수 있습니다.

다음은 2023년 3월 1일 이후 파티션을 `time_dt` 사용하여 로그를 쿼리하는 예제 쿼리입니다.

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt > TIMESTAMP '2023-03-01'
AND src_endpoint.ip = '192.0.2.1'
ORDER BY time desc
LIMIT 25
```

`time_dt`에 대한 공통값은 다음과 같습니다.

최근 1년 동안 발생한 이벤트

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '1' YEAR
```

지난 1개월 동안 발생한 이벤트

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '1' MONTH
```

지난 30일 동안 발생한 이벤트

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '30' DAY
```

지난 12시간 동안 발생한 이벤트

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '12' HOUR
```

지난 5분간 발생한 이벤트

```
WHERE time_dt > CURRENT_TIMESTAMP - INTERVAL '5' MINUTE
```

7~14일 전에 발생한 이벤트

```
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '14' DAY AND
CURRENT_TIMESTAMP - INTERVAL '7' DAY
```

특정 날짜 또는 이후에 발생하는 이벤트

```
WHERE time_dt >= TIMESTAMP '2023-03-01'
```

예: 2023년 3월 1일 또는 이후 소스 IP **192.0.2.1**의 모든 CloudTrail 활동 목록이 표 **cloud_trail_mgmt_1_0**에 나와 있습니다.

```
SELECT *
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay >= '20230301'
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

예: 최근 30일 동안 소스 IP **192.0.2.1**의 모든 CloudTrail 활동이 표 **cloud_trail_mgmt_1_0**에 나열되어 있습니다.

```
SELECT *
```

```
    FROM
 amazon_security_lake_glue_db_us_east_1.amazon_security_lake_table_us_east_1_cloud_trail_mgmt_1
    WHERE eventDay > cast(date_format(current_timestamp - INTERVAL '30' day, '%Y%m%d
%H') as varchar)
    AND src_endpoint.ip = '192.0.2.1'
    ORDER BY time desc
    LIMIT 25
```

Security Lake 관찰 파일 쿼리

Observables는 이제 Security Lake 2.0에서 사용할 수 있는 새로운 기능입니다. 관찰 가능한 객체는 이벤트의 여러 위치에서 발견된 관련 정보를 포함하는 피벗 요소입니다. 관찰 가능한 쿼리를 통해 사용자는 데이터 세트 전체에서의 높은 수준의 보안 인사이트를 도출할 수 있습니다.

관찰 가능한 내에서 특정 요소를 쿼리하여 데이터 세트를 특정 사용자 이름, 리소스 UIDs, IPs, 해시 및 기타 IOC 유형 정보와 같은 항목으로 제한할 수 있습니다.

다음은 관찰 가능한 배열을 사용하여 IP 값 '172.01.02.03'가 포함된 VPC 흐름 및 Route53 테이블에서 로그를 쿼리하는 예제 쿼리입니다.

```
WITH a AS
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0",
    UNNEST(observables) AS t(observable)
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip'),
b as
    (SELECT
    time_dt,
    observable.name,
    observable.value
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
    UNNEST(observables) AS t(observable)
    WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND observable.value='172.01.02.03'
    AND observable.name='src_endpoint.ip')
```

```
SELECT * FROM a
LEFT JOIN b ON a.value=b.value and a.name=b.name
LIMIT 25
```

CloudTrail 데이터에 대한 Security Lake 쿼리 예제

AWS CloudTrail 는에서 사용자 활동 및 API 사용량을 추적합니다 AWS 서비스. 구독자는 CloudTrail 데이터를 쿼리하여 다음 유형의 정보를 학습할 수 있습니다.

다음은 AWS 소스 버전 2의 CloudTrail 데이터에 대한 몇 가지 쿼리 예제입니다.

지난 7일 AWS 서비스 동안에 대한 무단 시도

```
SELECT
    time_dt,
    api.service.name,
    api.operation,
    api.response.error,
    api.response.message,
    api.response.data,
    cloud.region,
    actor.user.uid,
    src_endpoint.ip,
    http_request.user_agent
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND api.response.error in (
    'Client.UnauthorizedOperation',
    'Client.InvalidPermission.NotFound',
    'Client.OperationNotPermitted',
    'AccessDenied')
ORDER BY time desc
LIMIT 25
```

최근 7일간 소스 IP **192.0.2.1**의 모든 CloudTrail 활동 목록

```
SELECT
    api.request.uid,
    time_dt,
    api.service.name,
    api.operation,
    cloud.region,
```

```
    actor.user.uid,
    src_endpoint.ip,
    http_request.user_agent
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '192.0.2.1.'
ORDER BY time desc
LIMIT 25
```

지난 7일간의 모든 IAM 활동 목록

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND api.service.name = 'iam.amazonaws.com'
ORDER BY time desc
LIMIT 25
```

지난 7일 동안 자격 증명 **AIDACKCEVSQ6C2EXAMPLE**이 사용된 인스턴스

```
SELECT
      actor.user.uid,
      actor.user.uid_alt,
      actor.user.account.uid,
      cloud.region
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND actor.user.credential_uid = 'AIDACKCEVSQ6C2EXAMPLE'
LIMIT 25
```

지난 7일간 실패한 CloudTrail 레코드 목록

```
SELECT
      actor.user.uid,
      actor.user.uid_alt,
      actor.user.account.uid,
      cloud.region
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_cloud_trail_mgm
```

```
WHERE status='failed' and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND
 CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

Route 53 Resolver 쿼리 로그의 쿼리 예제

Amazon Route 53 Resolver 쿼리 로그는 아마존 VPC 내 리소스에서 만든 DNS 쿼리를 추적합니다. 구독자는 Route 53 Resolver 쿼리 로그를 쿼리하여 다음 유형의 정보를 학습할 수 있습니다.

다음은 AWS 소스 버전 2의 Route 53 reesolver 쿼리 로그에 대한 몇 가지 예제 쿼리입니다.

최근 7일간 CloudTrail에서 발생한 DNS 쿼리 목록

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
LIMIT 25
```

지난 7일 동안 **s3.amazonaws.com**와 일치하는 DNS 쿼리 목록

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE query.hostname LIKE 's3.amazonaws.com.' and time_dt BETWEEN CURRENT_TIMESTAMP -
 INTERVAL '7' DAY AND CURRENT_TIMESTAMP
ORDER BY time DESC
```

```
LIMIT 25
```

지난 7일 동안 해결되지 않은 DNS 쿼리 목록

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0"
WHERE cardinality(answers) = 0 and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY
 AND CURRENT_TIMESTAMP
LIMIT 25
```

지난 7일 동안 **192.0.2.1**에 해결된 DNS 쿼리 목록

```
SELECT
    time_dt,
    src_endpoint.instance_uid,
    src_endpoint.ip,
    src_endpoint.port,
    query.hostname,
    rcode,
    answer.rdata
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_route53_2_0",
UNNEST(answers) as st(answer)
WHERE answer.rdata='192.0.2.1'
AND time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Security Hub 조사 결과에 대한 Security Lake 쿼리 예제

Security Hub는에서 보안 상태를 포괄적으로 볼 수 있게 해 AWS 주며 보안 업계 표준 및 모범 사례를 기준으로 환경을 확인하는 데 도움이 됩니다. Security Hub는 보안 검사 조사 결과를 생성하고 타사 서비스로부터 조사 결과를 수신합니다.

다음은 AWS 소스 버전 2의 Security Hub 조사 결과에 대한 몇 가지 쿼리 예제입니다.

지난 7일간의 심각도가 **MEDIUM**이상인 새로운 조사 결과

```
SELECT
    time_dt,
    finding_info,
    severity_id,
    status
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
    AND severity_id >= 3
    AND status = 'New'
ORDER BY time DESC
LIMIT 25
```

지난 7일간의 중복된 조사 결과

```
SELECT
    finding_info.uid,
    MAX(time_dt) AS time,
    ARBITRARY(region) AS region,
    ARBITRARY(accountid) AS accountid,
    ARBITRARY(finding_info) AS finding,
    ARBITRARY(vulnerabilities) AS vulnerabilities
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY finding_info.uid
LIMIT 25
```

지난 7일간의 모든 정보 외 조사 결과

```
SELECT
    time_dt,
    finding_info.title,
    finding_info,
    severity
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE severity != 'Informational' and time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7'
 DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

리소스가 Amazon S3 버킷인 경우 조사 결과 (시간 제한 없음)

```
SELECT *
   FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE any_match(resources, element -> element.type = 'amzn-s3-demo-bucket')
LIMIT 25
```

CVSS (Common Vulnerability Scoring System) 점수가 **1** (시간 제한 없음) 보다 높은 조사 결과

```
SELECT
    DISTINCT finding_info.uid
    time_dt,
    metadata,
    finding_info,
    vulnerabilities,
    resource
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
UNNEST(vulnerabilities) AS t(vulnerability),
UNNEST(vulnerability.cve.cvss) AS t(cvs)
WHERE cvs.base_score > 1.0
AND vulnerabilities is NOT NULL
LIMIT 25
```

일반적인 취약성 및 노출도 (CVE) **CVE-0000-0000**와 일치하는 조사 결과 (시간 제한 없음)

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE any_match(vulnerabilities, element -> element.cve.uid = 'CVE-0000-0000')
LIMIT 25
```

지난 7일 동안 Security Hub에서 조사 결과를 전송한 제품 수

```
SELECT
    metadata.product.name,
    count(*)
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
```

```
GROUP BY metadata.product.name
ORDER BY metadata.product.name DESC
LIMIT 25
```

지난 7일간의 조사 결과에 포함된 리소스 유형 수

```
SELECT
    count(*) AS "Total",
    resource.type
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
GROUP BY resource.type
ORDER BY count(*) DESC
LIMIT 25
```

지난 7일간의 조사 결과에서 나온 취약한 패키지

```
SELECT
    vulnerabilities
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND vulnerabilities is NOT NULL
LIMIT 25
```

지난 7일 동안 변경된 조사 결과

```
SELECT
    status,
    finding_info.title,
    finding_info.created_time_dt,
    finding_info,
    finding_info.uid,
    finding_info.first_seen_time_dt,
    finding_info.last_seen_time_dt,
    finding_info.modified_time_dt
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_sh_findings_2_0
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

Amazon VPC 흐름 로그에 대한 Security Lake 쿼리 예제

Amazon Virtual Private Cloud(VPC)는 VPC의 네트워크 인터페이스에서 양쪽에서 이동하는 IP 트래픽에 대한 세부 정보를 제공합니다.

다음은 AWS 소스 버전 2의 Amazon VPC 흐름 로그에 대한 몇 가지 예제 쿼리입니다.

지난 7일 AWS 리전 동안 특정의 트래픽

```
SELECT *
    FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND region in ('us-east-1','us-east-2','us-west-2')
LIMIT 25
```

최근 7일간 소스 IP **192.0.2.1** 및 소스 포트 **22**의 활동 목록

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '192.0.2.1'
AND src_endpoint.port = 22
LIMIT 25
```

지난 7일간의 고유 대상 IP 주소 수

```
SELECT
    COUNT(DISTINCT dst_endpoint.ip) AS "Total"
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
LIMIT 25
```

지난 7일 동안의 198.51.100.0/24에서 발생한 트래픽

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
```

```
AND split_part(src_endpoint.ip,'.', 1)='198'AND split_part(src_endpoint.ip,'.', 2)='51'
LIMIT 25
```

지난 7일간의 모든 HTTPS 트래픽

```
SELECT
    dst_endpoint.ip as dst,
    src_endpoint.ip as src,
    traffic.packets
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    dst_endpoint.ip,
    traffic.packets,
    src_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

지난 7일 동안 포트 **443**로 향하는 연결의 패킷 수를 기준으로 정렬합니다.

```
SELECT
    traffic.packets,
    dst_endpoint.ip
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND dst_endpoint.port = 443
GROUP BY
    traffic.packets,
    dst_endpoint.ip
ORDER BY traffic.packets DESC
LIMIT 25
```

지난 7일간의 IP **192.0.2.1** 및 **192.0.2.2** 간 모든 트래픽

```
SELECT
    start_time_dt,
    end_time_dt,
    src_endpoint.interface_uid,
    connection_info.direction,
```

```
    src_endpoint.ip,
    dst_endpoint.ip,
    src_endpoint.port,
    dst_endpoint.port,
    traffic.packets,
    traffic.bytes
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND(
    src_endpoint.ip = '192.0.2.1'
AND dst_endpoint.ip = '192.0.2.2')
OR (
    src_endpoint.ip = '192.0.2.2'
AND dst_endpoint.ip = '192.0.2.1')
ORDER BY start_time_dt ASC
LIMIT 25
```

지난 7일간의 모든 인바운드 트래픽

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Inbound'
LIMIT 25
```

지난 7일간의 모든 아웃바운드 트래픽

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND connection_info.direction = 'Outbound'
LIMIT 25
```

지난 7일간 거부된 모든 트래픽

```
SELECT *
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_vpc_flow_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
```

```
AND action = 'Denied'
LIMIT 25
```

Amazon EKS 감사 로그에 대한 Security Lake 쿼리 예제

Amazon EKS 로그 추적 컨트롤 플레인 활동은 Amazon EKS 컨트롤 플레인에서 계정의 CloudWatch Logs로 직접 감사 및 진단 로그를 제공합니다. 이러한 로그를 통해 클러스터를 쉽게 보호하고 실행할 수 있습니다. 구독자는 EKS 로그를 쿼리하여 다음 유형의 정보를 알아볼 수 있습니다.

다음은 AWS 소스 버전 2의 Amazon EKS 감사 로그에 대한 몇 가지 예제 쿼리입니다.

지난 7일 동안 특정 URL에 대한 요청

```
SELECT
    time_dt,
    actor.user.name,
    http_request.url.path,
    activity_name
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND activity_name = 'get'
and http_request.url.path = '/apis/coordination.k8s.io/v1/'
LIMIT 25
```

지난 7일 동안 '10.0.97.167'에서 요청 업데이트

```
SELECT
    activity_name,
    time_dt,
    api.request,
    http_request.url.path,
    src_endpoint.ip,
    resources
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '10.0.97.167'
AND activity_name = 'Update'
LIMIT 25
```

지난 7일 동안 리소스 'kube-controller-manager'와 연결된 요청 및 응답

```
SELECT
    activity_name,
    time_dt,
    api.request,
    api.response,
    resource.name
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_eks_audit_2_0",
UNNEST(resources) AS t(resource)
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND resource.name = 'kube-controller-manager'
LIMIT 25
```

AWS WAF v2 로그에 대한 Security Lake 쿼리 예제

AWS WAF 는 최종 사용자가 애플리케이션에 보내는 웹 요청을 모니터링하고 콘텐츠에 대한 액세스를 제어하는 데 사용할 수 있는 웹 애플리케이션 방화벽입니다.

다음은 AWS 소스 버전 2의 AWS WAF v2 로그에 대한 몇 가지 예제 쿼리입니다.

지난 7일 동안 특정 소스 IP의 요청 게시

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    http_request.http_headers
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND src_endpoint.ip = '100.123.123.123'
AND activity_name = 'Post'
LIMIT 25
```

지난 7일 동안 방화벽 유형 MANAGED_RULE_GROUP과 일치하는 요청

```
SELECT
    time_dt,
    activity_name,
```

```
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    firewall_rule.uid,
    firewall_rule.type,
    firewall_rule.condition,
    firewall_rule.match_location,
    firewall_rule.match_details,
    firewall_rule.rate_limit
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND firewall_rule.type = 'MANAGED_RULE_GROUP'
LIMIT 25
```

지난 7일 동안 방화벽 규칙의 REGEX와 일치하는 요청

```
SELECT
    time_dt,
    activity_name,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    firewall_rule.uid,
    firewall_rule.type,
    firewall_rule.condition,
    firewall_rule.match_location,
    firewall_rule.match_details,
    firewall_rule.rate_limit
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND firewall_rule.condition = 'REGEX'
LIMIT 25
```

지난 7일 동안 AWS WAF 규칙을 트리거한 AWS 자격 증명에 대한 요청 가져오기 거부

```
SELECT
    time_dt,
    activity_name,
    action,
```

```
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method,
    firewall_rule.uid,
    firewall_rule.type
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY AND CURRENT_TIMESTAMP
AND http_request.url.path = '/.aws/credentials'
AND action = 'Denied'
LIMIT 25
```

지난 7일 동안 국가별로 그룹화된 AWS 자격 증명에 대한 요청 가져오기

```
SELECT count(*) as Total,
    src_endpoint.location.country AS Country,
    activity_name,
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method
FROM
 "amazon_security_lake_glue_db_us_east_1"."amazon_security_lake_table_us_east_1_waf_2_0"
WHERE time_dt BETWEEN CURRENT_TIMESTAMP - INTERVAL '7' DAY
    AND CURRENT_TIMESTAMP
    AND activity_name = 'Get'
    AND http_request.url.path = '/.aws/credentials'
GROUP BY src_endpoint.location.country,
    activity_name,
    action,
    src_endpoint.ip,
    http_request.url.path,
    http_request.url.hostname,
    http_request.http_method
```

Security Lake의 수명 주기 관리

Security Lake를 사용자 지정하여 원하는 시간 AWS 리전 동안 원하는에 데이터를 저장할 수 있습니다. 수명 주기 관리를 통해 다양한 규정 준수 요구 사항을 준수할 수 있습니다.

보존 관리

데이터를 비용 효율적으로 저장하도록 관리하려면 Security Lake의 수명 주기 설정을 사용하여 데이터에 대한 보존을 구성할 수 있습니다. 이러한 보존 설정을 사용하면 원하는 Amazon S3 스토리지 클래스와 Amazon S3 객체가 다른 스토리지 클래스로 전환되어 만료되기 전에 해당 스토리지 클래스에 머무르는 기간을 지정할 수 있습니다.

> **Warning**
>
> Security Lake 콘솔, API 또는 CLI를 통해 보존 설정을 관리하는 것이 좋습니다. 이는 Amazon S3 서비스에서 Amazon S3 수명 주기 설정을 직접 수정하면 메타데이터가 삭제되어 데이터에 액세스할 수 없기 때문입니다.

Security Lake의 보존 설정에 대한 중요 고려 사항

Security Lake에서 데이터 보존을 관리할 때 다음 고려 사항을 검토하세요.

- Security Lake는 Amazon S3 객체 잠금을 지원하지 않습니다. 데이터 레이크 버킷이 생성되면 S3 객체 잠금이 기본적으로 비활성화됩니다. 기본 보존 모드로 S3 객체 잠금을 활성화하면 정규화된 로그 데이터가 데이터 레이크로 전달되지 않습니다.
- 기본 Amazon S3 스토리지 클래스는 S3 Standard입니다. 보존 설정을 구성하지 않으면 Security Lake는 Amazon S3 수명 주기 구성에 기본 설정을 사용합니다. S3 Standard 스토리지 클래스를 사용하여 데이터를 무기한 저장합니다.
- Security Lake에서는 리전 수준에서 보존 설정을 지정합니다. 예를 들어 데이터 레이크에 기록된 후 S30일이 지나면 S3 Standard-IA 스토리지 클래스로 전환 AWS 리전 하도록 특정의 모든 S3 객체를 구성할 수 있습니다. S3
- 보존 설정은 S3 버킷에 저장된 데이터에만 적용되지만 Apache Iceberg 메타데이터는 보존 정책에서 제외됩니다.

Security Lake를 활성화할 때 보존 설정을 구성합니다.

Security Lake에 온보딩할 때 다음 지침에 따라 하나 이상의 리전에 대한 보존 설정을 구성하십시오.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 2단계: 온보딩 워크플로의 대상 목표 정의에 도달하면 스토리지 클래스 선택에서 전환 추가를 선택합니다. 그런 다음 S3 객체를 전환하려는 Amazon S3 스토리지 클래스를 선택합니다. (목록에 없는 기본 스토리지 클래스는 S3 Standard입니다.) 또한 해당 스토리지 클래스의 보존 기간 (일) 을 지정하십시오. 해당 기간 이후에 객체를 다른 스토리지 클래스로 전환하려면 전환 추가를 선택하고 후속 스토리지 클래스 및 보존 기간에 대한 설정을 입력합니다.
3. S3 객체 만료 시기를 지정하려면 전환 추가를 선택합니다. 그런 다음 스토리지 클래스의 경우 만료를 선택합니다. 보존 기간에는 객체 생성 후 임의의 스토리지 클래스를 사용하여 Amazon S3에 객체를 저장할 총 일수를 입력합니다. 이 기간이 끝나면 객체가 만료되고 Amazon S3에서 객체를 삭제합니다.
4. 마쳤으면 다음을 선택합니다.

변경 사항은 이전 온보딩 단계에서 Security Lake를 활성화한 모든 리전에 적용됩니다.

API

Security Lake에 온보딩할 때 프로그래밍 방식으로 보존 설정을 구성하려면 Security Lake API의 CreateDataLake 작업을 사용합니다. AWS CLI을(를) 사용하는 경우, create-data-lake 명령을 실행합니다. 다음과 같이 `lifecycleConfiguration` 파라미터에 원하는 보존 설정을 지정합니다.

- `transitions`의 경우 특정 Amazon S3 스토리지 클래스 (`storageClass`)에 S3 객체를 저장할 총 일수 (`days`)를 지정합니다.
- `expiration`의 경우, 객체를 생성한 후 임의의 스토리지 클래스를 사용하여 Amazon S3에 객체를 저장할 총 일수를 지정합니다. 이 기간이 끝나면 객체가 만료되고 Amazon S3에서 객체를 삭제합니다.

Security Lake는 `configurations`객체의 `region` 필드에 지정하는 리전에 설정을 적용합니다.

예를 들어 다음 명령은 `us-east-1` 리전에서 Security Lake를 활성화합니다. 이 리전에서는 객체가 365일 후에 만료되고 객체가 60일 후에 `ONEZONE_IA` S3 스토리지 클래스로 전환됩니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake create-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":365},"transitions":
[{"days":60,"storageClass":"ONEZONE_IA"}]}}]' \
--meta-store-manager-role-arn "arn:aws:securitylake:ap-
northeast-2:123456789012:data-lake/default"
```

보존 설정 업데이트

Security Lake를 활성화한 후 다음 지침에 따라 하나 이상의 지역에 대한 보존 설정을 업데이트하십시오.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창에서 리전을 선택합니다.
3. 리전을 선택한 다음 편집을 선택합니다.
4. 스토리지 클래스 선택 섹션에서 원하는 설정을 입력합니다. 스토리지 클래스의 경우, S3 개체를 전환할 Amazon S3 스토리지 클래스를 선택합니다. (목록에 없는 기본 스토리지 클래스는 S3 Standard입니다.) 보관 기간에는 해당 스토리지 클래스에 객체를 저장할 일수를 입력합니다. 여러 전환을 지정할 수 있습니다.

   S3 객체 만료 시기도 지정하려면 스토리지 클래스에 대해 Expire를 선택합니다. 그런 다음, 보관 기간에 객체 생성 후 임의의 스토리지 클래스를 사용하여 Amazon S3에 객체를 저장할 총 일수를 입력합니다. 이 기간이 끝나면 객체가 만료되고 Amazon S3에서 객체를 삭제합니다.
5. 마쳤으면 저장을 선택합니다.

API

보존 설정을 프로그래밍 방식으로 업데이트하려면 Security Lake API의 UpdateDataLake 작업을 사용합니다. 를 사용하는 경우 update-data-lake 명령을 AWS CLI실행합니다. 요청에서 `lifecycleConfiguration` 파라미터를 사용하여 새 설정을 지정합니다.

- 전환 설정을 변경하려면 `transitions` 파라미터를 사용하여 특정 Amazon S3 스토리지 클래스(`storageClass`)에 S3 객체를 저장할 각각의 새 기간을 일 (`days`) 단위로 지정합니다.

- 전체 보존 기간을 변경하려면 `expiration` 파라미터를 사용하여 객체 생성 후 스토리지 클래스를 사용하여 S3 객체를 저장할 총 일수를 지정합니다. 이 보존 기간이 끝나면 객체가 만료되고 Amazon S3에서 객체를 삭제합니다.

Security Lake는 `configurations` 객체의 `region` 필드에 지정한 리전에 설정을 적용합니다.

Security Lake API의 `UpdateDataLake` 작업은 지정된 항목 또는 레코드가 없는 경우 삽입을 수행하는 "upsert" 작업으로 작동하고, 이미 있는 경우 업데이트로 작동합니다. Security Lake는 AWS 암호화 솔루션을 사용하여 저장된 데이터를 안전하게 저장합니다.

현재 KMS를 사용하는 업데이트 호출에 포함된 리전`encryptionConfiguration`에서 키를 생략하면 해당 리전의 KMS 키가 그대로 유지되지만 키를 지정하면 동일한 리전에서 키가 재설정됩니다.

예를 들어 다음 AWS CLI 명령은 `us-east-1` 리전의 데이터 만료 설정 및 스토리지 전환 설정을 업데이트합니다. 이 리전에서는 객체가 500일 후에 만료되고 객체가 30일 후에 `ONEZONE_IA` S3 스토리지 클래스로 전환됩니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake update-data-lake \
--configurations '[{"encryptionConfiguration":
 {"kmsKeyId":"S3_MANAGED_KEY"},"region":"us-east-1","lifecycleConfiguration":
 {"expiration":{"days":500},"transitions":
[{"days":30,"storageClass":"ONEZONE_IA"}]}}]' \
--meta-store-manager-role-arn "arn:aws:securitylake:ap-
northeast-2:123456789012:data-lake/default"
```

롤업 리전

롤업 리전은 하나 이상의 기여 리전의 데이터를 통합합니다. 이렇게 하면 리전별 데이터 규제 요구 사항을 준수할 수 있습니다.

롤업 리전 구성에 대한 지침은 섹션을 참조하세요Security Lake에서 롤업 리전 구성.

Security Lake의 Open Cybersecurity Schema Framework(OCSF)

OCSF란 무엇입니까?

Open Cybersecurity Schema Framework(OCSF)는 사이버 보안 업계의 AWS 및 주요 파트너가 공동으로 수행하는 오픈 소스 작업입니다. OCSF는 일반적인 보안 이벤트에 대한 표준 스키마를 제공하고, 스키마 진화를 촉진하기 위한 버전 관리 기준을 정의하며, 보안 로그 생성자와 소비자를 위한 자체 거버넌스 프로세스를 포함합니다. OCSF의 공개 소스 코드는 GitHub에서 호스팅됩니다.

Security Lake는 기본적으로 지원되는에서 OCSF 스키마 AWS 서비스 로 오는 로그와 이벤트를 자동으로 변환합니다. OCSF로 변환한 후 Security Lake는 데이터를의 Amazon Simple Storage Service(Amazon S3) 버킷(1개당 버킷 1개 AWS 리전)에 저장합니다 AWS 계정. 사용자 지정 소스에서 Security Lake에 기록되는 로그 및 이벤트는 OCSF 스키마와 Apache Parquet 형식을 준수해야 합니다. 구독자는 로그 및 이벤트를 일반 Parquet 레코드로 취급하거나 OCSF 스키마 이벤트 클래스를 적용하여 레코드에 포함된 정보를 더 정확하게 해석할 수 있습니다.

OCSF 이벤트 클래스

지정된 Security Lake 소스의 로그 및 이벤트는 OCSF에 정의된 특정 이벤트 클래스와 일치합니다. OCSF의 이벤트 클래스 예로는 DNS 활동, SSH 활동 및 인증이 있습니다. 특정 소스와 일치하는 이벤트 클래스를 지정할 수 있습니다.

OCSF 소스 식별

OCSF는 다양한 필드를 사용하여 특정 로그 또는 이벤트 집합이 발생한 위치를 확인하는 데 도움을 줍니다. Security Lake에서 소스로 AWS 서비스 기본적으로 지원되는에 대한 관련 필드의 값입니다.

The OCSF source identification for AWS log sources (Version 1) are listed in the following table.

소스	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.version
CloudTrail Management Events	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
CloudTrail 관리 이벤트	CloudTrail	AWS	Management	API Activity,Autation 또는 Account Change	1.0.0-rc.2
CloudTrail S3 데이터 이벤트	CloudTrail	AWS	Data	API Activity	1.0.0-rc.2
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.0.0-rc.2
Security Hub	Security Hub	AWS	Security Hub ProductName 값과 일치합니다.	Security Finding	1.0.0-rc.2
VPC 흐름 로그	Amazon VPC	AWS	Flowlogs	Network Activity	1.0.0-rc.2

The OCSF source identification for AWS log sources (Version 2) are listed in the following table.

소스	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.version
CloudTrail Management Events	CloudTrail	AWS	Data	API Activity	1.1.0
CloudTrail 관리 이벤트	CloudTrail	AWS	Management	API Activity,Autation 또는 Account Change	1.1.0
CloudTrail S3 데이터 이벤트	CloudTrail	AWS	Data	API Activity	1.1.0
Route 53	Route 53	AWS	Resolver Query Logs	DNS Activity	1.1.0
Security Hub	AWS 보안 조사 결과 형식(ASFF) ProductName 값과 일치	AWS 보안 조사 결과 형식(ASFF) CompanyName 값과 일치	ASFF의 featureName 값과 일치 ProductFields	Vulnerability Finding, Compliance Finding, or Detection Finding	1.1.0
VPC 흐름 로그	Amazon VPC	AWS	Flowlogs	Network Activity	1.1.0
EKS 감사 로그	Amazon EKS	AWS	Elastic Kubernetes Service	API Activity	1.1.0

소스	metadata.product.name	metadata.product.vendor_name	metadata.product.feature.name	class_name	metadata.version
AWS WAF v2 로그	`AWS WAF`	`AWS`	–	`HTTP Activity`	`1.1.0`

Security Lake와 통합

Amazon Security Lake는 다른 AWS 서비스 및 타사 제품과 통합됩니다. 통합을 통해 Security Lake에 데이터를 소스로 전송하거나 구독자로 Security Lake의 데이터를 사용할 수 있습니다. 다음 주제에서는 Security Lake와 통합되는 AWS 서비스 및 타사 제품에 대해 설명합니다.

주제

- AWS 서비스 Security Lake와의 통합
- Security Lake와의 타사 통합

AWS 서비스 Security Lake와의 통합

Amazon Security Lake는 다른와 통합됩니다 AWS 서비스. 서비스는 소스 통합, 구독자 통합 또는 둘 다로 운영될 수 있습니다.

소스 통합에는 다음과 같은 속성이 있습니다.

- Security Lake로 데이터 전송
- 데이터가 Security Lake의 Open Cybersecurity Schema Framework(OCSF) 스키마에 도착함
- 데이터가 Apache Parquet 형식으로 도착함

구독자 통합은 다음 방법 중 하나로 Security Lake 데이터에 액세스할 수 있습니다.

- HTTPS 엔드포인트를 통해 Security Lake에서 소스 데이터 읽기
- Amazon Simple Queue Service(Amazon SQS)를 통해 Security Lake에서 소스 데이터 읽기
- 를 사용하여 소스 데이터를 직접 쿼리 AWS Lake Formation

다음 표에는 Security Lake에서 지원하는 AWS 서비스 통합 목록이 나와 있습니다.

AWS 서비스	통합 유형	설명	통합의 작동 방식
Amazon Bedrock	구독자	AI 기반 인사이트를 생성하여 Security Lake 데이터를 분석합니다.	Amazon Bedrock 통합

AWS 서비스	통합 유형	설명	통합의 작동 방식
Amazon Detective	구독자	Security Lake를 쿼리하여 보안 조사 결과 또는 의심스러운 활동의 근본 원인을 분석, 조사 및 신속하게 식별합니다.	Amazon Detective는 통합되었습니다.
Amazon OpenSearch Service	구독자	OpenSearch Service 수집을 사용하여 Security Lake 데이터에서 보안 인사이트를 생성합니다.	Amazon OpenSearch Service 통합
Amazon OpenSearch Service 수집 파이프라인	구독자, 소스	로그, 지표 및 추적 데이터를 OpenSearch Service 및 Security Lake로 스트리밍합니다.	Amazon OpenSearch Service Ingestion 파이프라인 통합
Amazon OpenSearch Service 제로 ETL	구독자(쿼리)	제로 ETL을 사용하여 Security Lake에서 데이터를 쿼리합니다.	Amazon OpenSearch Service 제로 ETL 다이렉트 쿼리 통합
Amazon QuickSight	구독자	QuickSight를 사용하여 Security Lake에서 로그를 시각화, 탐색 및 해석합니다.	Amazon QuickSight 통합
Amazon SageMaker AI	구독자	AI 기반 인사이트를 생성하여 Security Lake 데이터를 분석합니다.	Amazon SageMaker AI 통합

AWS 서비스	통합 유형	설명	통합의 작동 방식
AWS AppFabric	소스	서비스형 소프트웨어(SaaS) 애플리케이션 로그를 Security Lake 표준 형식으로 수집하고 정규화합니다.	AWS AppFabric 통합
AWS Security Hub	소스	Security Hub의 보안 조사 결과를 Security Lake 표준 형식으로 중앙 집중화하고 저장합니다.	AWS Security Hub 통합

Amazon Bedrock과 통합

Amazon Bedrock은 통합 API를 통해 주요 AI 스타트업 및 Amazon의 고성능 파운데이션 모델(FMs)을 사용할 수 있도록 하는 완전관리형 서비스입니다. Amazon Bedrock의 서버리스 환경을 사용하면 인프라를 관리할 필요 없이 AWS 도구를 사용하여 파운데이션 모델을 빠르고 비공개로 사용자 지정하고 쉽고 안전하게 통합하고 애플리케이션에 배포할 수 있습니다.

생성형 AI

Amazon Bedrock의 생성형 AI 기능과 SageMaker AI Studio의 자연어 입력을 사용하여 Security Lake의 데이터를 분석하고 조직의 위험을 줄이고 보안 태세를 강화할 수 있습니다. 적절한 데이터 소스를 자동으로 식별하고, SQL 쿼리를 생성 및 호출하고, 조사에서 데이터를 시각화하여 조사를 수행하는 데 필요한 시간을 줄일 수 있습니다. 자세한 내용은 Amazon SageMaker AI Studio 및 Amazon Bedrock을 사용하여 Amazon Security Lake에 대한 AI 기반 인사이트 생성을 참조하세요.

Amazon Detective와 통합

통합 유형: 구독자

Amazon Detective는 사용자가 보안 조사 결과 또는 의심스러운 활동의 근본 원인을 분석 및 조사하고 신속하게 식별하는 데 도움이 됩니다. Detective는 AWS 리소스에서 로그 데이터를 자동으로 수집합니다. 그런 다음 기계 학습, 통계 분석 및 그래프 이론을 사용하여 더 빠르고 효율적으로 보안 조사를 수행할 수 있도록 시각화를 생성합니다. Detective의 사전 구축된 데이터 집계, 요약 및 컨텍스트는 가능한 보안 문제의 특성과 범위를 신속하게 분석하고 확인하는 데 도움이 됩니다.

Security Lake와 Detective를 통합하면 Detective에서 Security Lake에 저장된 원시 로그 데이터를 쿼리할 수 있습니다. 자세한 내용은 Amazon Security Lake와의 통합을 참조하세요.

Amazon OpenSearch Service와 통합

통합 유형: 구독자

Amazon OpenSearch Service는에서 OpenSearch Service 클러스터를 쉽게 배포, 운영 및 확장할 수 있는 관리형 서비스입니다 AWS 클라우드. OpenSearch Service Ingestion을 사용하여 OpenSearch Service 클러스터로 데이터를 수집하면 시간에 민감한 보안 조사에 대한 인사이트를 더 빠르게 도출할 수 있습니다. 보안 인시던트에 신속하게 대응하여 비즈니스에 중요한 데이터와 시스템을 보호할 수 있습니다.

OpenSearch Service 대시보드

OpenSearch Service를 Security Lake와 통합한 후 서버리스 OpenSearch Service Ingestion을 통해 다양한 소스의 보안 데이터를 OpenSearch Service로 보내도록 Security Lake를 구성할 수 있습니다. 보안 데이터를 처리하도록 OpenSearch Service 수집을 구성하는 방법에 대한 자세한 내용은 Amazon OpenSearch Service Ingestion을 사용하여 Amazon Security Lake 데이터에서 보안 인사이트 생성을 참조하세요.

OpenSearch Service Ingestion이 OpenSearch Service 도메인에 데이터 쓰기를 시작한 후 사전 구축된 대시보드를 사용하여 데이터를 시각화하려면 대시보드로 이동하여 설치된 대시보드 중 하나를 선택합니다.

Amazon OpenSearch Service Ingestion 파이프라인과 통합

통합 유형:구독자, 소스

Amazon OpenSearch Service Ingestion은 로그, 지표 및 추적 데이터를 OpenSearch Service 및 Security Lake로 스트리밍하는 완전 관리형 서버리스 데이터 수집기입니다.

OpenSearch Ingestion 파이프라인을 사용하여 Security Lake로 데이터 전송

> OpenSearch Ingestion에서 Amazon Simple Storage Service(Amazon S3) 싱크 플러그인을 사용하여 지원되는 모든 소스에서 Security Lake로 데이터를 전송할 수 있습니다. Security Lake는 AWS 환경, 온프레미스 환경 및 SaaS 공급자의 보안 데이터를 특별히 구축된 데이터 레이크로 자동으로 중앙 집중화합니다. 자세한 내용은 Amazon Security Lake를 싱크로 사용하여 OpenSearch Ingestion 파이프라인 사용을 참조하세요.

OpenSearch Ingestion 파이프라인을 사용하여 Security Lake에서 OpenSearch로 데이터 전송

Amazon S3 소스 플러그인을 사용하여 OpenSearch Ingestion 파이프라인에 데이터를 수집할 수 있습니다. 자세한 내용은 Amazon Security Lake를 소스로 사용하여 OpenSearch Ingestion 파이프라인 사용을 참조하세요.

Amazon OpenSearch Service 제로 ETL 직접 쿼리와 통합

통합 유형: 구독자(쿼리)

OpenSearch Service 다이렉트 쿼리를 사용하여 Amazon Security Lake의 데이터를 분석할 수 있습니다. OpenSearch Service는 수집 파이프라인 구축 또는 분석 도구 간 전환의 마찰 없이 OpenSearch SQL 또는 OpenSearch Piped Processing Language(PPL)를 사용하여 Security Lake에서 데이터를 직접 쿼리하는 방법으로 제로 ETL 통합을 제공합니다. 이 접근 방식을 사용하면 데이터 이동 또는 복제가 필요하지 않으므로 OpenSearch Service Dashboards의 Discover 환경을 사용하여 데이터가 저장된 위치를 분석할 수 있습니다. 유휴 데이터 쿼리에서 대시보드를 사용한 능동적 모니터링으로 전환하려는 경우 쿼리 결과에 인덱싱된 뷰를 빌드하여 OpenSearch Service 인덱스로 수집할 수 있습니다. 직접 쿼리에 대한 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 직접 쿼리 작업을 참조하세요.

OpenSearch Service는 OpenSearch Serverless 컬렉션을 사용하여 Security Lake에서 데이터를 직접 쿼리하고 인덱싱된 뷰를 저장합니다. 이렇게 하려면 Security Lake 데이터에 OpenSearch 제로 ETL 기능을 사용할 수 있는 데이터 소스를 생성합니다. 데이터 소스를 생성할 때 Security Lake에 저장된 데이터를 직접 검색하고, 인사이트를 얻고, 분석할 수 있습니다. 온디맨드 인덱싱을 사용하여 일부 Security Lake 데이터 세트에서 쿼리 성능을 가속화하고 고급 OpenSearch 분석을 사용할 수 있습니다.

- OpenSearch Service 데이터 소스 통합 생성에 대한 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 Amazon Security Lake 데이터 소스 통합 생성을 참조하세요. OpenSearch
- OpenSearch Service에서 Security Lake 데이터 소스를 구성하는 방법에 대한 자세한 내용은 Amazon OpenSearch Service 개발자 안내서의 OpenSearch OpenSearch Service Dashboards에서 Security Lake 데이터 소스 구성을 참조하세요.

Security Lake에서 OpenSearch Service를 사용하는 방법에 대한 자세한 내용은 다음 리소스를 참조하세요.

- Amazon OpenSearch Service 및 Amazon Security Lake 통합을 도입하여 보안 분석 간소화
- Amazon Security Lake를 사용하는 OpenSearch Service의 제로 ETL 소개

Amazon Security Lake를 사용하는 OpenSearch Service의 제로 ETL 소개

Amazon QuickSight와 통합

통합 유형: 구독자

Amazon QuickSight는 클라우드 규모의 비즈니스 인텔리전스(BI) 서비스로, 어디에서 작업하든 함께 작업하는 사람들에게 easy-to-understand 인사이트를 제공하는 데 사용할 수 있습니다. QuickSight는 클라우드의 데이터에 연결하고 다양한 소스의 데이터를 결합합니다. QuickSight는 의사 결정자에게 대화형의 시각적 환경에서 정보를 탐색하고 해석할 수 있는 기회를 제공합니다. 네트워크에 있는 모든 장치와 모바일 장치에서 대시보드에 안전하게 액세스할 수 있습니다.

Amazon QuickSight 대시보드

Amazon QuickSight에서 Amazon Security Lake 데이터를 시각화하려면 Security Lake와 관련하여 필요한 AWS 객체를 생성하고 기본 데이터 소스, 데이터 세트, 분석, 대시보드 및 사용자 그룹을 Amazon QuickSight에 배포합니다. 자세한 지침은 Amazon QuickSight와의 통합을 참조하세요.

Amazon QuickSight를 사용하여 Security Lake 데이터를 시각화하는 방법에 대한 자세한 내용은 다음 리소스를 참조하세요.

Amazon QuickSight를 사용하여 Security Lake 데이터 시각화: 2024 Amazon QuickSight 학습 시리즈

Security Lake를 사용하여 AWS WAF 웹 ACL 로그 운영

Amazon SageMaker AI와 통합

통합 유형: 구독자

Amazon SageMaker AI는 완전 관리형 기계 학습(ML) 서비스입니다. Security Lake를 사용하면 데이터 과학자와 개발자가 ML 모델을 빠르고 자신 있게 구축, 훈련 및 프로덕션 지원 호스팅 환경에 배포할 수 있습니다. 여러 통합 개발 환경(IDEs)에서 SageMaker AI ML 도구를 사용할 수 있도록 ML 워크플로를 실행하기 위한 UI 환경을 제공합니다.

SageMaker AI 인사이트

SageMaker AI Studio를 사용하여 Security Lake에 대한 기계 학습 인사이트를 생성할 수 있습니다. 이 Studio는 데이터 과학자가 기계 학습 모델을 준비, 구축, 훈련 및 배포할 수 있는 도구를 제공하는 기

계 학습용 웹 통합 개발 환경(IDE)입니다. 이 솔루션을 사용하면 Security Lake의 AWS Security Hub 조사 결과에 초점을 맞춘 기본 Python 노트북 세트를 빠르게 배포할 수 있으며, Security Lake의 다른 AWS 소스 또는 사용자 지정 데이터 소스를 통합하도록 확장할 수도 있습니다. 자세한 내용은 Amazon SageMaker AI를 사용하여 Amazon Security Lake 데이터에 대한 기계 학습 인사이트 생성을 참조하세요.

와 통합 AWS AppFabric

통합 유형: 소스

AWS AppFabric는 조직 전체에서 서비스형 소프트웨어(SaaS) 애플리케이션을 연결하는 코드 없는 서비스이므로 IT 및 보안 애플리케이션은 표준 스키마와 중앙 리포지토리를 사용합니다.

Security Lake가 AppFabric 조사 결과를 수신하는 방법

Amazon Kinesis Data Firehose를 대상으로 선택하고 OCSF 스키마 및 Apache Parquet 형식의 데이터를 Security Lake로 전송하도록 Kinesis Data Firehose를 구성하여 AppFabric 감사 로그 데이터를 Security Lake로 보낼 수 있습니다.

사전 조건

AppFabric 감사 로그를 Security Lake로 보내려면 먼저 OCSF 정규화된 감사 로그를 Kinesis Data Firehose 스트림으로 출력해야 합니다. 그런 다음 출력을 Security Lake Amazon S3 버킷으로 전송하도록 Kinesis Data Firehose를 구성할 수 있습니다. 자세한 정보는 Amazon Kinesis 개발자 안내서에서 대상에 대한 Amazon S3 선택하기를 참조하십시오.

AppFabric 조사 결과를 Security Lake로 전송하기

위의 사전 요구 사항을 완료한 후 AppFabric 감사 로그를 Security Lake로 보내려면 두 서비스를 모두 활성화하고 AppFabric을 Security Lake에서 사용자 지정 소스로 추가해야 합니다. 사용자 지정 소스 추가에 대한 지침은 Security Lake의 사용자 지정 소스에서 데이터 수집 단원을 참조하십시오.

Security Lake에서 AppFabric 로그 수신 중단하기

AppFabric 감사 로그 수신을 중지하려면 Security Lake 콘솔, Security Lake API 또는를 사용하여 AppFabric AWS CLI 을 사용자 지정 소스로 삭제할 수 있습니다. 지침은 Security Lake에서 사용자 지정 소스 삭제 섹션을 참조하세요.

와 통합 AWS Security Hub

통합 유형: 소스

AWS Security Hub는의 보안 상태에 대한 포괄적인 보기를 AWS 제공하고 보안 업계 표준 및 모범 사례를 기준으로 환경을 지원합니다. Security Hub는 전체 AWS 계정, 서비스 및 지원되는 타사 파트너 제품에서 보안 데이터를 수집하고 보안 추세를 분석하고 우선순위가 가장 높은 보안 문제를 식별하는 데 도움이 됩니다.

Security Hub를 활성화하고 Security Hub 조사 결과를 Security Lake의 소스로 추가하면 Security Hub는 새로운 조사 결과 및 기존 조사 결과에 대한 업데이트를 Security Lake로 보내기 시작합니다.

Security Lake가 Security Hub 조사 결과를 받는 방법

Security Hub의 경우 보안 문제를 조사 결과와 같이 추적합니다. 일부 결과는 다른 AWS 서비스 또는 타사 파트너가 감지한 문제에서 비롯됩니다. Security Hub는 또한 규칙에 대해 자동화되고 지속적인 보안 검사를 실행하여 자체 조사 결과를 생성합니다. 규칙은 보안 제어로 표시됩니다.

Security Hub의 모든 결과는 표준 JSON 형식을 사용합니다. 이를 AWS Security Finding Format(ASFF)이라고 합니다.

Security Lake는 Security Hub 조사 결과를 받아 Security Lake의 Open Cybersecurity Schema Framework(OCSF)로 변환합니다.

Security Hub 조사 결과를 Security Lake에 전송하기

Security Hub 조사 결과를 Security Lake로 보내려면 두 서비스를 모두 활성화하고 Security Hub 결과를 Security Lake에 소스로 추가해야 합니다. AWS 소스 추가에 대한 지침은 섹션을 참조하세요소스 AWS 서비스 로 추가.

Security Hub가 제어 조사 결과를 생성하여 Security Lake로 보내도록 하려면 관련 보안 표준을 활성화하고 AWS Config에 리소스 기록을 지역별 기준으로 설정해야 합니다. 자세한 내용은 AWS Security Hub 사용 설명서에서 활성화 및 구성 AWS Config 단원을 참조하십시오.

Security Lake에서 Security Hub 조사 결과 수신 중지하기

Security Hub 조사 결과 수신을 중지하려면 사용 AWS Security Hub 설명서의 다음 주제 AWS CLI 에서 Security Hub 콘솔, Security Hub API 또는를 사용할 수 있습니다.

- 통합에서 결과의 흐름 사용 중지 및 사용 설정(콘솔)
- 통합에서 결과 흐름 비활성화(Security Hub API, AWS CLI)

Security Lake와의 타사 통합

Amazon Security Lake는 여러 타사 공급자와 통합됩니다. 공급자는 소스 통합, 구독자 통합 또는 서비스 통합을 제공할 수 있습니다. 공급자는 하나 이상의 통합 유형을 제공할 수 있습니다.

소스 통합에는 다음과 같은 속성이 있습니다.

- Security Lake로 데이터 전송
- 데이터가 Apache Parquet 형식으로 도착함
- 데이터가 Security Lake의 Open Cybersecurity Schema Framework(OCSF) 스키마에 도착함

구독자 통합에는 다음과 같은 속성이 있습니다.

- HTTPS 엔드포인트 또는 Amazon Simple Queue Service(Amazon SQS) 대기열에서 또는에서 소스 데이터를 직접 쿼리하여 Security Lake에서 소스 데이터 읽기 AWS Lake Formation
- Apache Parquet 형식으로 데이터 읽기 가능
- OCSF 스키마에서 데이터 읽기 가능

서비스 통합은 조직에서 Security Lake 및 기타 AWS 서비스 를 구현하는 데 도움이 될 수 있습니다. 또한 보고, 분석 및 기타 사용 사례에 대한 지원을 제공할 수도 있습니다.

특정 파트너 공급자를 검색하려면 파트너 솔루션 파인더를 참조하십시오. 타사 제품을 구매하려면 AWS Marketplace를 참조하십시오.

파트너 통합으로 추가하거나 Security Lake 파트너가 되도록 요청하려면 `<securitylake-partners@amazon.com>`으로 이메일을 보내세요.

조사 결과를 보내는 타사 통합을 사용하는 경우 Security Lake용 Security Hub 통합이 활성화된 경우 Security Lake에서 해당 조사 결과를 검토할 수도 AWS Security Hub있습니다. 통합 활성화에 대한 자세한 내용은 와 통합 AWS Security Hub 단원을 참조하십시오. 결과를 Security Hub로 보내는 타사 통합 목록은 AWS Security Hub 사용 설명서에서 사용 가능한 타사 파트너 제품 통합을 참조하십시오.

구독자를 설정하기 전에 구독자의 OCSF 로그 지원을 확인합니다. 최신 세부 정보는 구독자 설명서를 참조하세요.

쿼리 통합

Security Lake가 AWS Lake Formation 데이터베이스 및 테이블에 저장하는 데이터를 쿼리할 수 있습니다. Security Lake 콘솔, API 또는에서 타사 구독자를 생성할 수도 있습니다 AWS Command Line Interface.

Lake Formation 데이터 레이크 관리자는 데이터를 쿼리하는 IAM ID에 관련 데이터베이스 및 테이블에 대한 SELECT 권한을 부여해야 합니다. 데이터를 쿼리하기 전에 Security Lake에서 구독자를 생성해야 합니다. 쿼리 액세스 권한이 있는 구독자를 만드는 방법에 대한 자세한 내용은 구독자를 위한 쿼리 액세스 관리를 참조하십시오.

다음 타사 파트너에 대해 Security Lake와의 쿼리 통합을 구성할 수 있습니다.

- Cribl – Search
- IBM – QRadar
- Palo Alto Networks – XSOAR
- Query.AI – Query Federated Search
- SOC Prime
- Splunk – Federated Analytics
- Tego Cyber

Accenture – MxDR

통합 유형: 구독자, 서비스

Accenture's MxDR과 Security Lake의 통합은 로그 및 이벤트의 실시간 데이터 모으기, 관리형 이상 탐지, 위협 추적 및 보안 작업을 제공합니다. 이는 분석 및 관리형 탐지 및 대응 (MDR)을 지원합니다.

서비스 통합으로서 Accenture는 조직에 Security Lake를 구현하는 데도 도움이 될 수 있습니다.

통합 설명서

Aqua Security

통합 유형: 소스

감사 이벤트를 Security Lake로 전송하기 위한 사용자 지정 소스로 Aqua Security를 추가할 수 있습니다. 감사 이벤트는 OCSF 스키마와 Parquet 형식으로 변환됩니다.

통합 설명서

Barracuda – Email Protection

통합 유형: 소스

새로운 피싱 이메일 공격이 탐지되면 Barracuda Email Protection은 Security Lake에 이벤트를 보낼 수 있습니다. 데이터 레이크의 다른 보안 데이터와 함께 이러한 이벤트를 수신할 수 있습니다.

통합 설명서

Booz Allen Hamilton

통합 유형: 서비스

서비스 통합으로서, Booz Allen Hamilton은 데이터와 분석을 Security Lake 서비스와 융합하여 사이버 보안에 대한 데이터 기반 접근 방식을 사용합니다.

파트너 링크

Bosch Software and Digital Solutions – AIShield

통합 유형: 소스

AIShield 로 구동되는 Bosch는 Security Lake와의 통합을 통해 AI 자산에 대한 자동화된 취약성 분석 및 엔드포인트 보호를 제공합니다.

통합 설명서

ChaosSearch

통합 유형: 구독자

ChaosSearch는 Elasticsearch 및 SQL과 같은 개방형 API를 사용하거나 기본적으로 포함된 Kibana 및 Superset UI를 통해 사용자에게 다중 모델 데이터 액세스를 제공합니다. 보존 제한 없이 ChaosSearch에서 Security Lake 데이터를 사용하여 모니터링, 경고 및 위협 추적을 수행할 수 있습니다. 이를 통해 오늘날의 복잡한 보안 환경과 지속적인 위협에 대응할 수 있습니다.

통합 문서

Cisco Security – Secure Firewall

통합 유형: 소스

Security Lake와 Cisco Secure Firewall을 통합하면 방화벽 로그를 구조적이고 확장 가능한 방식으로 저장할 수 있습니다. Cisco의 eNcore 클라이언트는 방화벽 관리 센터에서 방화벽 로그를 스트리밍하고 OCSF 스키마로 스키마를 변환한 다음 Security Lake에 저장합니다.

통합 설명서

Claroty – xDome

통합 유형: 소스

Claroty xDome은 네트워크 내에서 탐지된 알림을 최소한의 구성으로 Security Lake로 전송합니다. 유연하고 신속한 배포 옵션을 통해 네트워크 내에서 IoT, IIoT 및 BMS 자산으로 구성된 확장된 사물 인터넷 (XIoT) 자산을 xDome이 보호하는 동시에 위협의 초기 지표를 자동으로 탐지할 수 있습니다.

통합 설명서

CMD Solutions

통합 유형: 서비스

CMD Solutions는 설계, 자동화 및 지속적인 보증 프로세스를 통해 보안을 초기에 지속적으로 통합하여 기업이 민첩성을 높일 수 있도록 지원합니다. 서비스 통합으로서 CMD Solutions는 조직에 Security Lake를 구현하는 데 도움이 될 수 있습니다.

파트너 링크

Confluent – Amazon S3 Sink Connector

통합 유형: 소스

Confluent는 완전히 관리되고 사전 구축된 커넥터를 사용하여 데이터 통합을 자동으로 연결, 구성 및 조정합니다. Confluent S3 Sink Connector를 통해 원시 데이터를 가져와 네이티브 파켓 형식으로 대규모로 Security Lake에 저장할 수 있습니다.

통합 설명서

Contrast Security

통합 유형: 소스

통합을 위한 파트너 제품:Contrast Assess

Contrast Security Assess는 웹 앱, API 및 마이크로서비스에서 실시간으로 취약성을 탐지할 수 있도록 도와주는 IAST 도구입니다. Assess는 Security Lake와 통합되어 모든 워크로드에 대한 중앙 집중식 가시성을 제공합니다.

통합 설명서

Cribl – Search

통합 유형: 구독자

Cribl Search를 사용하여 Security Lake 데이터를 검색할 수 있습니다.

통합 설명서

Cribl – Stream

통합 유형: 소스

Cribl이 지원하는 모든 타사 소스의 데이터를 OCSF 스키마의 Security Lake로 보내는 데 Cribl Stream을 사용할 수 있습니다.

통합 설명서

CrowdStrike – Falcon Data Replicator

통합 유형: 소스

이 통합은 연속 스트리밍 기반으로 CrowdStrike Falcon Data Replicator에서 데이터를 가져와 OCSF 스키마로 변환한 다음 Security Lake로 전송합니다.

통합 설명서

CrowdStrike – Next Gen SIEM

통합 유형: 구독자

네이티브 OCSF 스키마 파서가 포함된 CrowdStrike Falcon Next-Gen SIEM 데이터 커넥터를 사용하여 Security Lake 데이터의 수집을 간소화합니다.는 위반을 방지하기 위해 하나의 통합 플랫폼에서 비교할 수 없는 보안 깊이와 범위를 결합하여 위협 탐지, 조사 및 대응을 Falcon NG SIEM 혁신합니다.

통합 설명서

CyberArk – Unified Identify Security Platform

통합 유형: 소스

CyberArk Audit Adapter AWS Lambda 함수인는에서 보안 이벤트를 수집하고 OCSF 스키마의 Security Lake로 데이터를 CyberArk Identity Security Platform 전송합니다.

통합 설명서

Cyber Security Cloud – Cloud Fastener

통합 유형: 구독자

CloudFastener는 Security Lake를 활용하여 클라우드 환경에서 보안 데이터를 더 쉽게 통합할 수 있습니다.

통합 설명서

DataBahn

통합 유형: 소스

Security Data Fabric을 사용하여 Security Lake에서 DataBahn's 보안 데이터를 중앙 집중화합니다.

통합 설명서 (DataBahn 포털에 로그인하여 설명서 검토)

Darktrace – Cyber AI Loop

통합 유형: 소스

Security Lake와 Darktrace의 통합은 Darktrace 자체 학습의 힘을 Security Lake에 제공합니다. Cyber AI Loop에서 얻은 통찰력을 조직의 보안 스택의 다른 데이터 스트림 및 요소와 상호 연관시킬 수 있습니다. 통합 로그 Darktrace는 침해를 보안 조사 결과로 모델링합니다.

통합 설명서 (Darktrace 포털에 로그인하여 설명서 검토)

Datadog

통합 유형: 구독자

Datadog Cloud SIEM은 Security Lake의 데이터를 포함하여 클라우드 환경에 대한 실시간 위협을 탐지하고 DevOps 및 보안 팀을 하나의 플랫폼으로 통합합니다.

통합 설명서

Deloitte – MXDR Cyber Analytics and AI Engine (CAE)

통합 유형: 구독자, 서비스

Deloitte MXDR CAE는 표준화된 보안 데이터를 신속하게 저장, 분석 및 시각화하는 데 도움이 됩니다. 맞춤형 분석, AI 및 ML 기능으로 구성된 CAE 제품군은 Security Lake의 OCSF 형식 데이터에 대해 실행되는 모델을 기반으로 실행 가능한 통찰력을 자동으로 제공합니다.

서비스 통합으로 Deloitte는 조직에 Security Lake를 구현하는 데도 도움이 될 수 있습니다.

통합 설명서

Devo

통합 유형: 구독자

용 Devo 수집기는 Security Lake에서 수집을 AWS 지원합니다. 이 통합을 통해 위협 탐지, 조사, 사고 대응과 같은 다양한 보안 사용 사례를 분석하고 해결할 수 있습니다.

통합 문서

DXC – SecMon

통합 유형: 구독자, 서비스

DXC SecMon은 Security Lake에서 보안 이벤트를 수집하고 모니터링하여 잠재적 보안 위협을 탐지하고 경고합니다. 이를 통해 조직은 보안 상태를 더 잘 이해하고 위협을 사전에 식별하여 대응할 수 있습니다.

서비스 통합으로서 DXC는 조직에 Security Lake를 구현하는 데도 도움이 될 수 있습니다.

통합 설명서

Eviden— AIsaac (이전 명칭 Atos)

통합 유형: 구독자

이 AIsaac MDR 플랫폼은 Security Lake의 OCSF 스키마에 수집된 VPC 흐름 로그를 사용하고 AI 모델을 활용하여 위협을 탐지합니다.

통합 설명서

ExtraHop – Reveal(x) 360

통합 유형: 소스

ExtraHop Reveal(x) 360의 IOC 탐지를 비롯한 네트워크 데이터를 OCSF 스키마의 Security Lake로 통합하여 워크로드 및 애플리케이션 보안을 강화할 수 있습니다.

통합 설명서

Falcosidekick

통합 유형: 소스

Falcosidekick은 Falco 이벤트를 수집하여 Security Lake로 전송합니다. 이 통합은 OCSF 스키마를 사용하여 보안 이벤트를 내보냅니다.

통합 설명서

Fortinet - Cloud Native Firewall

통합 유형: 소스

에서 FortiGate CNF 인스턴스 AWS를 생성할 때 Amazon Security Lake를 로그 출력 대상으로 지정할 수 있습니다.

통합 설명서

Gigamon – Application Metadata Intelligence

통합 유형: 소스

Gigamon Application Metadata Intelligence (AMI)는 중요한 메타데이터 속성으로 관찰성, SIEM 및 네트워크 성능 모니터링 도구를 강화합니다. 이를 통해 애플리케이션에 대한 심층적인 가시성을 제공하여 성능 병목 현상, 품질 문제 및 잠재적 네트워크 보안 위험을 정확히 찾아낼 수 있습니다.

통합 문서

Hoop Cyber

통합 유형: 서비스

Hoop Cyber FastStart는 데이터 소스 평가, 우선 순위 지정, 데이터 소스 온보딩이 포함되며 고객이 Security Lake를 통해 제공되는 기존 도구 및 통합을 사용하여 데이터를 쿼리할 수 있도록 도와줍니다.

파트너 링크

HTCD – AI-First Cloud Security Platform

통합 유형: 구독자

즉각적인 규정 준수 자동화, 보안 조사 결과의 우선순위 지정 및 맞춤형 패치를 확보합니다. HTCD는 Security Lake를 쿼리하여 자연어 쿼리 및 AI 기반 인사이트로 위협을 발견하는 데 도움이 될 수 있습니다.

통합 설명서

IBM – QRadar

통합 유형: 구독자

IBM Security QRadar SIEM with UAX는 Security Lake를 하이브리드 클라우드 전반에서 위협을 식별하고 방지하는 분석 플랫폼과 통합합니다. 이 통합은 데이터 액세스와 쿼리 액세스를 모두 지원합니다.

사용 AWS CloudTrail 로그에 대한 통합 설명서

쿼리에 Amazon Athena를 사용하는 방법에 대한 통합 설명서

Infosys

통합 유형: 서비스

Infosys는 조직의 요구 사항에 맞게 Security Lake 구현을 사용자 지정할 수 있도록 지원하고 사용자 지정 통찰력을 제공합니다.

파트너 링크

Insbuilt

통합 유형: 서비스

Insbuilt는 클라우드 컨설팅 서비스를 전문으로 하며 조직에 Security Lake를 구현하는 방법을 이해하는 데 도움을 줄 수 있습니다.

파트너 링크

Kyndryl – AIOps

통합 유형: 구독자, 서비스

Kyndryl은 Security Lake와 통합되어 사이버 데이터, 위협 인텔리전스 및 AI 기반 분석의 상호 운용성을 제공합니다. 데이터 액세스 구독자인 Kyndryl는 분석 목적으로 Security Lake에서 AWS CloudTrail 관리 이벤트를 수집합니다.

서비스 통합으로서 Kyndryl는 조직에 Security Lake를 구현하는 데도 도움이 될 수 있습니다.

통합 설명서

Lacework – Polygraph

통합 유형: 소스

Lacework Polygraph® Data Platform는 Security Lake와 데이터 소스로 통합되며 AWS 환경 전반의 취약성, 잘못된 구성 및 알려진 위협과 알려지지 않은 위협에 대한 보안 조사 결과를 제공합니다.

통합 설명서

Laminar

통합 유형: 소스

Laminar는 데이터 보안 이벤트를 OCSF 스키마 내 Security Lake에 전송하여 사고 대응 및 조사와 같은 추가 분석 사용 사례에 사용할 수 있도록 합니다.

통합 설명서

MegazoneCloud

통합 유형: 서비스

MegazoneCloud는 클라우드 컨설팅 서비스를 전문으로 하며 조직에 Security Lake를 구현하는 방법을 이해하는 데 도움을 줄 수 있습니다. Security Lake를 통합 ISV 솔루션과 연결하여 맞춤형 작업을 구축하고 고객 요구와 관련된 맞춤형 통찰력을 구축합니다.

통합 문서

Monad

통합 유형: 소스

Monad는 데이터를 OCSF 스키마로 자동 변환하여 Security Lake 데이터 레이크로 전송합니다.

통합 설명서

NETSCOUT – Omnis Cyber Intelligence

통합 유형: 소스

Security Lake와 통합하면 NETSCOUT은 사이버 위협, 보안 위험, 공격 표면 변경 등 기업에서 발생하는 상황에 대한 보안 탐지 결과 및 상세한 보안 인사이트를 제공하는 맞춤형 소스가 됩니다. 이러한 결과는 NETSCOUT CyberStreams 및 Omnis Cyber Intelligence를 통해 고객 계정에서 생성된 다음 OCSF 스키마를 통해 Security Lake에 전송됩니다. 수집된 데이터는 형식, 스키마, 파티셔닝 및 성능 관련 측면을 포함하여 Security Lake 소스에 대한 기타 요구 사항 및 모범 사례도 충족합니다.

통합 설명서

Netskope – CloudExchange

통합 유형: 소스

Netskope는 Security Lake와 보안 관련 로그 및 위협 정보를 공유하여 보안 태세를 강화하는 데 도움이 됩니다. Netskope 조사 결과는 CloudExchange 플러그인을 사용하여 Security Lake로 전송되며, 로컬 데이터 센터 내에서 AWS 또는 로컬 데이터 센터에서 도커 기반 환경으로 시작할 수 있습니다.

통합 설명서

New Relic ONE

통합 유형: 구독자

New Relic ONE은 Lambda 기반 구독자 애플리케이션입니다. 계정에 배포되고 Amazon SQS에서 트리거되며 New Relic 라이선스 키를 사용하여 데이터를 New Relic에 전송합니다.

통합 설명서

Okta – Workforce Identity Cloud

통합 유형: 소스

Okta는 Amazon EventBridge 통합을 통해 OCSF 스키마의 보안 레이크에 ID 로그를 전송합니다. OCSF 스키마 내 Okta System Logs는 보안 및 데이터 과학자 팀이 오픈 소스 표준에 따라 보안 이벤트를 쿼리하는 데 도움이 됩니다. Okta에서 표준화된 OCSF 로그를 생성하면 감사 활동을 수행하고 일관된 스키마에 따라 인증, 권한 부여, 계정 변경 및 엔터티 변경과 관련된 보고서를 생성할 수 있습니다.

통합 설명서

AWS CloudFormation Security Lake에서 사용자 지정 소스Okta로 추가할 템플릿

Orca – Cloud Security Platform

통합 유형: 소스

용 Orca 에이전트리스 클라우드 보안 플랫폼은 OCSF 스키마에서 클라우드 감지 및 응답(CDR) 이벤트를 전송하여 Security Lake와 AWS 통합됩니다.

통합 설명서 (Orca 포털에 로그인하여 설명서 검토)

Palo Alto Networks – Prisma Cloud

통합 유형: 소스

Palo Alto Networks Prisma Cloud는 클라우드 네이티브 환경의 VM 전반에서 취약성 탐지 데이터를 집계하여 Security Lake로 보냅니다.

통합 설명서

Palo Alto Networks – XSOAR

통합 유형: 구독자

Palo Alto Networks XSOAR는 XSOAR 및 Security Lake와의 구독자 통합을 구축했습니다.

통합 설명서

Panther

통합 유형: 구독자

Panther는 검색 및 탐지에 사용할 Security Lake 로그 수집을 지원합니다.

통합 설명서

Ping Identity – PingOne

통합 유형: 소스

PingOne은 계정 변경 알림을 OCSF 스키마 및 Parquet 형식으로 Security Lake에 전송하여 계정 변경 사항을 발견하고 조치를 취할 수 있도록 합니다.

통합 설명서

PwC – Fusion center

통합 유형: 구독자, 서비스

PwC는 지식과 전문 지식을 제공하여 고객이 개별 요구에 맞는 융합 센터를 구현할 수 있도록 지원합니다. Amazon Security Lake를 기반으로 구축된 퓨전 센터는 다양한 소스의 데이터를 결합하여 중앙에서 거의 실시간으로 볼 수 있는 기능을 제공합니다.

통합 설명서

Query.AI – Query Federated Search

통합 유형: 구독자

Query Federated Search는 Amazon Athena를 통해 모든 Security Lake 테이블을 직접 쿼리하여 OCSF 스키마의 다양한 관찰 가능, 이벤트 및 객체에 대한 인시던트 대응, 조사, 위협 추적 및 일반 검색을 지원할 수 있습니다.

통합 설명서

Rapid7 – InsightIDR

통합 유형: 구독자

Rapid7 SIEM/XDR 솔루션인 InsightIDR은 Security Lake의 로그를 수집하여 위협을 탐지하고 의심스러운 활동을 조사할 수 있습니다.

통합 문서

RipJar – Labyrinth for Threat Investigations

통합 유형: 구독자

Labyrinth for Threat Investigations는 세분화된 보안, 조정 가능한 워크플로 및 보고를 통해 데이터 융합을 기반으로 대규모 위협 탐색을 위한 전사적 접근 방식을 제공합니다.

통합 문서

Sailpoint

통합 유형: 소스

통합을 위한 파트너 제품: SailPoint IdentityNow

이 통합을 통해 고객은 SailPoint IdentityNow에서 이벤트 데이터를 변환할 수 있습니다. 통합은 IdentityNow 사용자 활동 및 거버넌스 이벤트를 Security Lake로 가져와 보안 사고 및 이벤트 모니터링 제품의 통찰력을 향상시키는 자동화된 프로세스를 제공하기 위한 것입니다.

통합 문서

Securonix

통합 유형: 구독자

Securonix Next-Gen SIEM은 Security Lake와 통합되어 보안 팀이 데이터를 더 빠르게 수집하고 탐지 및 대응 기능을 확장할 수 있도록 지원합니다.

통합 문서

SentinelOne

통합 유형: 구독자

SentinelOne Singularity™ XDR 플랫폼은 Amazon Elastic Compute Cloud(Amazon EC2), Amazon Elastic Container Service(Amazon ECS) 및 Amazon Elastic Kubernetes Service(Amazon EKS)를 비롯한 온프레미스 및 퍼블릭 클라우드 인프라에서 실행되는 엔드포인트, 자격 증명 및 클라우드 워크로드로 실시간 탐지 및 대응을 확대합니다.

통합 설명서 (SentinelOne 포털에 로그인하여 설명서 검토)

Sentra – Data Lifecyle Security Platform

통합 유형: 소스

Sentra는 계정에 Sentra 스캔 인프라를 배포한 후 조사 결과를 가져와 SaaS에 수집합니다. 이러한 조사 결과는 쿼리를 위해 OCSF 스키마의 Security Lake에 Sentra를 저장하고 나중에 스트리밍하는 메타데이터입니다.

통합 설명서

SOC Prime

통합 유형: 구독자

SOC Prime은 Amazon OpenSearch Service 및 Amazon Athena를 통해 Security Lake와 통합되어 제로 트러스트 마일스톤을 기반으로 스마트 데이터 오케스트레이션 및 위협 헌팅을 촉진합니다. SOC Prime은 보안 팀이 엄청난 양의 경고 없이 위협의 가시성을 높이고 인시던트를 조사할 수 있도록 지원합니다. OCSF 스키마의 Athena 및 OpenSearch Service로 자동 변환할 수 있는 재사용 가능한 규칙 및 쿼리를 사용하여 개발 시간을 절약할 수 있습니다.

통합 설명서

Splunk

통합 유형: 구독자

Amazon Web Services용 Splunk AWS 추가 기능(AWS)은 Security Lake에서 수집을 지원합니다. 이 통합을 통해 Security Lake에서 OCSF 스키마의 데이터를 구독하여 위협 탐지, 조사 및 대응을 가속화할 수 있습니다.

통합 설명서

Stellar Cyber

통합 유형: 구독자

Stellar Cyber는 Security Lake의 로그를 사용하고 해당 레코드를 Stellar Cyber 데이터 레이크에 추가합니다. 이 커넥터는 OCSF 스키마를 사용합니다.

통합 설명서

Sumo Logic

통합 유형: 구독자

Sumo Logic는 Security Lake의 데이터를 사용하며, 전체 AWS, 온프레미스 및 하이브리드 클라우드 환경에서 광범위한 가시성을 제공합니다. Sumo Logic은 보안 팀에 모든 보안 도구 전반에 대한 포괄적인 가시성, 자동화 및 위협 모니터링을 제공합니다.

통합 문서

Swimlane – Turbine

통합 유형: 구독자

Swimlane은 Security Lake에서 OCSF 스키마로 데이터를 수집하고 로우 코드 플레이북 및 사례 관리를 통해 데이터를 전송하여 위협 탐지, 조사 및 사고 대응을 가속화합니다.

통합 설명서 (Swimlane 포털에 로그인하여 설명서 검토)

Sysdig Secure

통합 유형: 소스

Sysdig Secure's 클라우드 네이티브 애플리케이션 보호 플랫폼(CNAPP)은 Security Lake에 보안 이벤트를 전송하여 감독을 극대화하고, 조사를 간소화하고, 규정 준수를 간소화합니다.

통합 설명서

Talon

통합 유형: 소스

통합을 위한 파트너 제품: Talon 엔터프라이즈 브라우저

안전하고 격리된 브라우저 기반 엔드포인트 환경인 Talon's Enterprise Browser는 Talon 액세스, 데이터 보호, SaaS 조치 및 보안 이벤트를 Security Lake로 전송하여 탐지, 포렌식 및 조사를 위해 이벤트를 상호 연관시킬 수 있는 가시성과 옵션을 제공합니다.

통합 설명서 (Talon 포털에 로그인하여 설명서 검토)

Tanium

통합 유형: 소스

Tanium Unified Cloud Endpoint Detection, Management, and Security 플랫폼은 인벤토리 데이터를 OCSF 스키마 내 Security Lake에 제공합니다.

통합 설명서

TCS

통합 유형: 서비스

TCS AWS Business Unit은 혁신, 경험 및 재능을 제공합니다. 이러한 통합은 10년에 걸친 공동 가치 창출, 심층적인 업계 지식, 기술 전문성 및 제공 지혜에 의해 뒷받침됩니다. 서비스 통합으로서 TCS는 조직에 Security Lake를 구현하는 데 도움이 될 수 있습니다.

통합 설명서

Tego Cyber

통합 유형: 구독자

Tego Cyber를 Security Lake와 통합하여 잠재적 보안 위협을 신속하게 탐지하고 조사할 수 있습니다. Tego Cyber는 광범위한 기간 및 로그 소스에서 다양한 위협 지표를 상호 연관시켜 숨겨진 위협을 찾아냅니다. 이 플랫폼은 상황에 맞는 위협 인텔리전스를 통해 위협 탐지 및 조사에서 정확성을 높이고 유용한 인사이트를 제공합니다.

통합 설명서

Tines – No-code security automation

통합 유형: 구독자

Tines No-code security automation은 Security Lake에서 중앙 집중화된 보안 데이터를 활용하여 보다 정확한 결정을 내릴 수 있도록 도와줍니다.

통합 문서

Torq – Enterprise Security Automation Platform

통합 유형: 소스, 구독자

Torq는 사용자 지정 소스 및 구독자로서 Security Lake와 원활하게 통합됩니다. Torq는 코드가 필요 없는 간단한 플랫폼으로 엔터프라이즈 규모의 자동화 및 오케스트레이션을 구현할 수 있도록 지원합니다.

통합 문서

Trellix – XDR

통합 유형: 소스, 구독자

개방형 XDR 플랫폼으로서 Trellix XDR은 Security Lake 통합을 지원합니다. Trellix XDR은 보안 분석 사용 사례에 OCSF 스키마의 데이터를 활용할 수 있습니다. Trellix XDR의 1,000개 이상의 보안 이벤트 소스로 Security Lake 데이터 레이크를 보강할 수도 있습니다. 이를 통해 AWS 환경에 대한 탐지 및 대응 기능을 확장할 수 있습니다. 수집된 데이터는 다른 보안 위험과 상호 연관되어 적시에 위험에 대응하는 데 필요한 플레이북을 제공합니다.

통합 문서

Trend Micro – CloudOne

통합 유형: 소스

Trend Micro CloudOne Workload Security는 Amazon Elastic Compute Cloud (EC2) 인스턴스에서 Security Lake와 상호 다음 정보를 보냅니다.

- DNS 쿼리 활동
- 파일 활동
- 네트워크 활동
- 프로세스 활동
- 레지스트리 값 활동
- 사용자 계정 활동

통합 문서

Uptycs – Uptycs XDR

통합 유형: 소스

Uptycs는 온프레미스 및 클라우드 자산에서 OCSF 스키마의 풍부한 데이터를 Security Lake로 보냅니다. 데이터에는 엔드포인트 및 클라우드 워크로드의 행동 위협 탐지, 이상 탐지, 정책 위반, 위험한 정책, 잘못된 구성 및 취약성이 포함됩니다.

통합 문서

Vectra AI – Vectra Detect for AWS

통합 유형: 소스

를 사용하면 전용 AWS CloudFormation 템플릿을 사용하여 사용자 지정 소스로 Security Lake에 충실도가 높은 알림을 보낼 Vectra Detect for AWS수 있습니다.

통합 설명서

VMware Aria Automation for Secure Clouds

통합 유형: 소스

이 통합을 통해 클라우드 구성 오류를 탐지하고 이를 Security Lake로 전송하여 고급 분석을 수행할 수 있습니다.

통합 설명서

Wazuh

통합 유형: 구독자

Wazuh는 사용자 데이터를 안전하게 처리하고, 각 소스에 대한 쿼리 액세스를 제공하고, 쿼리 비용을 최적화하는 것을 목표로 합니다.

통합 문서

Wipro

통합 유형: 소스, 서비스

이 통합을 통해 Wipro Cloud Application Risk Governance (CARG) 플랫폼에서 데이터를 수집하여 기업 전체의 클라우드 애플리케이션 및 규정 준수 상태를 통합적으로 파악할 수 있습니다.

서비스 통합으로서 Wipro는 조직에 Security Lake를 구현하는 데도 도움이 될 수 있습니다.

통합 설명서

Wiz – CNAPP

통합 유형: 소스

Security Lake와 Wiz 간의 통합은 확장 가능하고 표준화된 보안 데이터 교환을 위해 설계된 오픈 소스 표준인 OCSF 스키마를 활용하여 단일 보안 데이터 레이크에서 클라우드 보안 데이터 수집을 용이하게 합니다.

통합 설명서 (Wiz 포털에 로그인하여 설명서 검토)

Zscaler – Zscaler Posture Control

통합 유형: 소스

클라우드 네이티브 애플리케이션 보호 플랫폼인 Zscaler Posture Control™이 보안 조사 결과를 OCSF 스키마로 Security Lake에 전송합니다.

통합 문서

Security Lake의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon Security Lake에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Security Lake 사용 시 책임 분담 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 항목에서는 보안 및 규정 준수 목표를 충족하도록 Security Lake를 구성하는 방법을 보여줍니다. 또한 Security Lake 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- Security Lake의 자격 증명 및 액세스 관리
- Amazon Security Lake의 데이터 보호
- Amazon Security Lake 규정 준수 검증
- Security Lake 보안 모범 사례
- Amazon Security Lake의 복원성
- Amazon Security Lake의 인프라 보안
- Security Lake의 구성 및 취약성 분석
- Amazon Security Lake 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)
- Amazon Security Lake 모니터링

Security Lake의 자격 증명 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와주는 입니다. IAM 관리자는 누가 ACM 리소스를 사용하도록 인증되고 (로그인됨) 권한이 부여되는지 (권한 있음)를 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- Security Lake와 IAM의 작동 방식
- Security Lake에 대한 자격 증명 기반 정책 예제
- AWS Security Lake에 대한 관리형 정책
- Security Lake에 서비스 연결 역할 사용

대상

사용 방법 AWS Identity and Access Management (IAM)은 Security Lake에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 - Security Lake 서비스를 사용하여 작업을 수행하는 경우 필요한 자격 증명과 권한을 관리자가 제공합니다. 더 많은 Security Lake 기능을 사용하여 작업을 수행하게 되면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Security Lake의 기능에 액세스할 수 없는 경우 Amazon Security Lake 자격 증명 및 액세스 문제 해결 단원을 참조하세요.

서비스 관리자 - 회사에서 Security Lake 리소스를 책임지고 있는 경우 에 대한 전체 액세스 권한을 가지고 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Security Lake 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해하세요. 회사가 Security Lake에서 IAM을 사용하는 방법에 대해 자세히 알아보려면 Security Lake와 IAM의 작동 방식 단원을 참조하세요.

IAM 관리자 - IAM 관리자라면 Security Lake에 대한 액세스 권한 관리 정책 작성 방법을 자세히 알고 싶을 것입니다. IAM에서 사용할 수 있는 Security Lake 자격 증명 기반 정책 예제를 보려면 Security Lake에 대한 자격 증명 기반 정책 예제 단원을 참조하세요.

ID를 통한 인증

인증은 AWS 자격 증명으로에 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 다중 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 테루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자가 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액

세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 자격 증명 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페

더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 (역할을 프록시로 사용하는 대신) 정책을 리소스에 직접 연결할 AWS 서비스 수 있습니다. 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.
- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그

램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의

경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.
- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.

- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 가 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Security Lake와 IAM의 작동 방식

IAM을 사용하여 에 대한 액세스를 관리하기 전에 Security Lake와 함께 사용할 수 있는 IAM 기능을 알아보세요.

Amazon Security Lake에서 사용할 수 있는 IAM 기능

IAM 기능	Security Lake 지원
ID 기반 정책	예
리소스 기반 정책	예
정책 작업	예
정책 리소스	예
정책 조건 키	예
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
보안 주체 권한	예
서비스 역할	아니요

IAM 기능	Security Lake 지원
서비스 링크 역할	예

Security Lake 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

Security Lake에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Security Lake는 자격 증명 기반 정책을 지원합니다. 자세한 내용은 Security Lake에 대한 자격 증명 기반 정책 예제 단원을 참조하십시오.

Security Lake 내 리소스 기반 정책

리소스 기반 정책 지원: 예

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 위탁자로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 경우 신뢰할 수 AWS 계정있는 계정의 IAM 관리자는 보안 주체 엔터티(사용자 또는 역할)에게 리소스에 액세스할 수 있는

권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 위탁자에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

Security Lake 서비스는 데이터가 저장된 Amazon S3 버킷에 대한 리소스 기반 정책을 생성합니다. 사용자는 이러한 리소스 기반 정책을 S3 버킷에 연결하지 않습니다. Security Lake가 사용자를 대신하여 이러한 정책을 자동으로 생성합니다.

Amazon 리소스 이름(ARN)이 `arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}`인 S3 버킷이 그 예제입니다. 이 예제에서 `region`는 Security Lake를 활성화한 특정 AWS 리전 이고 `bucket-identifier`는 Security Lake가 버킷에 할당하는 리전 고유 영숫자 문자열입니다. Security Lake는 해당 리전의 데이터를 저장하기 위해 S3 버킷을 생성합니다. 리소스 정책은 버킷에서 작업을 수행할 수 있는 보안 주체를 정의합니다. 다음은 Security Lake가 버킷에 연결하는 샘플 리소스 기반 정책 (버킷 정책)입니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": [
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}"
            ],
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "false"
                }
            }
        },
        {
            "Sid": "PutSecurityLakeObject",
            "Effect": "Allow",
            "Principal": {
                "Service": "securitylake.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
```

```
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}/*",
                "arn:aws:s3:::aws-security-data-lake-{region}-{bucket-identifier}"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "{DA-AccountID}",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:securitylake:us-east-1:{DA-AccountID}:*"
                }
            }
        }
    ]
}
```

리소스 기반 정책에 대해 자세히 알아보려면 IAM 사용 설명서의 자격 증명 기반 정책 및 리소스 기반 정책을 참조하세요.

Security Lake의 정책 조치

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Security Lake 작업 목록을 보려면 서비스 권한 부여 참조에서 Amazon Security Lake에서 정의한 작업을 참조하세요.

Security Lake의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
securitylake
```

예를 들어 특정 구독자에 대한 정보에 액세스할 수 있는 권한을 사용자에게 부여하려면 해당 사용자에게 할당된 정책에 해당 `securitylake:GetSubscriber` 작업을 포함시키십시오. 정책 문에는

`Action` 또는 `NotAction` 요소가 포함되어야 합니다. Security Lake는 이 서비스로 수행할 수 있는 작업을 설명하는 고유한 작업 세트를 정의합니다.

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "securitylake:action1",
      "securitylake:action2"
]
```

Security Lake 자격 증명 기반 정책의 예를 보려면 Security Lake에 대한 자격 증명 기반 정책 예제 단원을 참조하세요.

Security Lake의 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Security Lake는 구독자 및 AWS 계정 특정의 데이터 레이크 구성과 같은 리소스 유형을 정의합니다 AWS 리전. ARN을 사용하여 정책에서 이러한 유형의 리소스를 지정할 수 있습니다.

Security Lake 리소스 유형 및 해당 ARN 구문 목록을 보려면 서비스 승인 참조의 Amazon Security Lake에서 정의한 리소스 유형을 참조하세요. 각 리소스 유형으로 지정할 수 있는 작업을 알아보려면 서비스 승인 참조의 Amazon Security Lake에서 정의한 작업 섹션을 참조하세요.

Security Lake 자격 증명 기반 정책의 예를 보려면 Security Lake에 대한 자격 증명 기반 정책 예제 단원을 참조하세요.

Security Lake에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇을 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Security Lake 조건 키 목록을 보려면 서비스 승인 참조의 Amazon Security Lake에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 서비스 승인 참조의 Amazon Security Lake에서 정의한 작업을 참조하세요. 조건 키를 사용하는 정책의 예는 Security Lake에 대한 자격 증명 기반 정책 예제을 참조하세요.

Security Lake의 액세스 제어 목록 (ACL)

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 위탁자(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Security Lake는 ACL을 지원하지 않습니다. 즉, 보안 레이크 리소스에 ACL을 연결할 수 없습니다.

Security Lake의 ABAC(속성 기반 액세스 제어)

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할)와 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

구독자인 Security Lake 리소스와에 대한 데이터 레이크 구성에 개별 태그를 연결할 수 AWS 계정 있습니다 AWS 리전. 또한 정책 `Condition` 요소에 태그 정보를 제공하여 이러한 유형의 리소스에 대한 액세스를 제어할 수 있습니다. Security Lake 리소스 태깅에 대한 자세한 내용은 Security Lake 리소스에 태그 지정 단원을 참조하세요. 리소스의 태그를 기반으로 리소스에 대한 액세스를 제한하는 ID 기반 정책의 예는 Security Lake에 대한 자격 증명 기반 정책 예제 단원을 참조하세요.

Security Lake에 대한 임시 보안 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인할 때 일부 AWS 서비스 는 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 비롯한 자세한 내용은 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는를 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신에 임시 자격 증명을 동적으로 생성하는 access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

Security Lake에서 임시 자격 증명 사용을 지원합니다.

Security Lake에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

일부 Security Lake 작업에는 다른 AWS 서비스작업의 추가 종속 작업에 대한 권한이 필요합니다. 작업 목록을 보려면 서비스 권한 부여 참조에서 Amazon Security Lake에서 정의한 작업을 참조하세요.

Security Lake의 서비스 역할

서비스 역할 지원: 아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.

Security Lake는 서비스 역할을 맡거나 사용하지 않습니다. 그러나 Security Lake를 사용할 때 Amazon EventBridge AWS Lambda및 Amazon S3와 같은 관련 서비스가 서비스 역할을 수임합니다. Security Lake는 사용자를 대신하여 작업을 수행하기 위해 서비스 연결 역할을 사용합니다.

> **Warning**
> 서비스 역할에 대한 권한을 변경하면 Security Lake 사용 시 운영 문제가 발생할 수 있습니다. Security Lake에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

Security Lake의 서비스 연결 역할

서비스 링크 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Security Lake는 `AWSServiceRoleForAmazonSecurityLake`이라는 IAM 서비스 연결 역할을 사용합니다. Security Lake 서비스 연결 역할은 고객을 대신하여 보안 데이터 레이크 서비스를 운영할 수 있는 권한을 부여합니다. 서비스 연결 역할은 Security Lake에 직접 연결된 IAM 역할입니다. Security Lake에서 사전 정의하며 Security Lake가 AWS 서비스 사용자를 대신하여 다른를 호출하는 데 필요한 모든 권한을 포함합니다. Security Lake는 Security Lake를 사용할 수 AWS 리전 있는 모든에서이 서비스 연결 역할을 사용합니다.

Security Lake 서비스 연결 역할을 생성 또는 관리하는 방법에 대한 자세한 내용은 Security Lake에 서비스 연결 역할 사용을 참조하세요.

Security Lake에 대한 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 Security Lake 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 Security Lake에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조에서 Amazon Security Lake에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Security Lake 콘솔 사용
- 예: 사용자가 자신이 권한을 볼 수 있도록 허용
- 예: 조직 관리 계정에서 위임된 관리자를 지정하고 제거하도록 허용
- 예: 사용자가 태그를 기반으로 구독자를 검토할 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Security Lake 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. 조건을 사용하여 AWS 서비스와 같은 특정를 통해 사용되는 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Security Lake 콘솔 사용

Amazon Security Lake 콘솔에 액세스하려면 최소한의 권한 집합이 있어야 합니다. 이러한 권한을 통해의 Security Lake 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API에만 호출하는 사용자에 대해 최소 콘솔 권한을 허용할 필요는 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 Security Lake 콘솔을 사용할 수 있도록 하려면 콘솔 액세스를 제공하는 IAM 정책을 생성하십시오. 자세한 내용은 사용 설명서에서 IAM 자격 증명를 참조하세요.

사용자 또는 역할이 Security Lake 콘솔을 사용할 수 있도록 허용하는 정책을 생성하는 경우, 해당 사용자 또는 역할이 콘솔에서 액세스해야 하는 리소스에 대한 적절한 조치가 정책에 포함되어 있는지 확인하세요. 그렇지 않으면 콘솔에서 해당 리소스로 이동하거나 해당 리소스에 대한 세부 정보를 표시할 수 없습니다.

예를 들어 콘솔을 사용하여 사용자 지정 소스를 추가하려면 사용자가 다음 작업을 수행할 수 있어야 합니다.

- `glue:CreateCrawler`
- `glue:CreateDatabase`
- `glue:CreateTable`
- `glue:StartCrawlerSchedule`
- `iam:GetRole`
- `iam:PutRolePolicy`
- `iam:DeleteRolePolicy`
- `iam:PassRole`
- `lakeformation:RegisterResource`
- `lakeformation:GrantPermissions`
- `s3:ListBucket`
- `s3:PutObject`

예: 사용자가 자신이 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함되어 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
```

```
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

예: 조직 관리 계정에서 위임된 관리자를 지정하고 제거하도록 허용

이 예에서는 AWS Organizations 관리 계정의 사용자가 조직의 위임된 Security Lake 관리자를 지정하고 제거하도록 허용하는 정책을 생성하는 방법을 보여줍니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "securitylake:RegisterDataLakeDelegatedAdministrator",
                "securitylake:DeregisterDataLakeDelegatedAdministrator"
            ],
            "Resource": "arn:aws:securitylake:*:*:*"
        }
    ]
}
```

예: 사용자가 태그를 기반으로 구독자를 검토할 수 있도록 허용

자격 증명 기반 정책의 조건을 사용하여 태그를 기반으로 Security Lake 리소스에 대한 액세스를 제어할 수 있습니다. 이 예제는 Security Lake 콘솔 또는 Security Lake API를 사용하여 사용자가 구독자를 검토하도록 허용하는 정책을 생성하는 방법을 보여줍니다. 하지만 구독자에 대한 `Owner` 태그가 해당 사용자의 사용자 이름 값을 가지고 있는 경우에만 권한이 부여됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReviewSubscriberDetailsIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:GetSubscriber",
            "Resource": "arn:aws:securitylake:*:*:subscriber/*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        },
        {
            "Sid": "ListSubscribersIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:ListSubscribers",
            "Resource": "*",
            "Condition": {
                "StringEquals": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

이 예시에서는 사용자 이름 `richard-roe`을 가진 사용자가 개별 구독자의 세부 정보를 검토하려는 경우 구독자에게 `Owner=richard-roe` 또는 `owner=richard-roe` 태그를 지정해야 합니다. 그렇지 않으면 사용자는 액세스가 거부됩니다. 조건 키 이름은 대소문자를 구분하지 않기 때문에 조건 태그 키 `Owner`는 `Owner` 및 `owner` 모두와 일치합니다. 조건 키 사용에 대한 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요. Security Lake 리소스 태깅에 대한 자세한 내용은 Security Lake 리소스에 태그 지정을 참조하세요.

AWS Security Lake에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 AWS 관리형 정책에 정의된 권한을 AWS 업데이트하면 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS 는 새 AWS 서비스 가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AWS 관리형 정책: AmazonSecurityLakeMetastoreManager

Amazon Security Lake는 AWS Lambda 함수를 사용하여 데이터 레이크의 메타데이터를 관리합니다. Security Lake는이 함수를 사용하여 데이터 및 데이터 파일이 포함된 Amazon Simple Storage Service(Amazon S3) 파티션을 AWS Glue 데이터 카탈로그 테이블로 인덱싱할 수 있습니다. 이 관리형 정책에는 Lambda 함수가 S3 파티션 및 데이터 파일을 AWS Glue 테이블로 인덱싱할 수 있는 모든 권한이 포함되어 있습니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `logs` - 보안 주체가 Lambda 함수의 출력을 Amazon CloudWatch Logs에 로깅할 수 있도록 허용합니다.
- `glue` - 보안 주체가 AWS Glue 데이터 카탈로그 테이블에 대한 특정 쓰기 작업을 수행할 수 있도록 허용합니다. 또한 AWS Glue 크롤러가 데이터에서 파티션을 식별할 수 있습니다.
- `sqs` - 보안 주체가 데이터 레이크에 객체가 추가되거나 업데이트될 때 이벤트 알림을 보내는 Amazon SQS 대기열에 대한 특정 읽기 및 쓰기 작업을 수행할 수 있도록 허용합니다.
- `s3` - 보안 주체가 데이터가 포함된 Amazon S3 버킷에 대해 특정 읽기 및 쓰기 작업을 수행할 수 있도록 허용합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowWriteLambdaLogs",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:CreateLogGroup"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLake*",
        "arn:aws:logs:*:*:/aws/lambda/AmazonSecurityLake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowGlueManage",
      "Effect": "Allow",
      "Action": [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:UpdateTable"
      ],
      "Resource": [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowToReadFromSqs",
```

```
      "Effect": "Allow",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:DeleteMessage",
        "sqs:GetQueueAttributes"
      ],
      "Resource": [
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowMetaDataReadWrite",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowMetaDataCleanup",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition": {
        "StringEquals": {
```

```
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

AWS 관리형 정책: AmazonSecurityLakePermissionsBoundary

Amazon Security Lake는 타사 사용자 지정 소스가 데이터 레이크에 데이터를 기록하고 타사 사용자 지정 구독자가 데이터 레이크의 데이터를 사용하도록 IAM 역할을 생성하고, 이러한 역할을 생성할 때 이 정책을 사용하여 권한의 경계를 정의합니다. 따라서 이 정책을 사용하기 위해 별도의 조치를 취할 필요가 없습니다. 데이터 레이크가 고객 관리형 AWS KMS 키로 암호화`kms:Decrypt`되고 `kms:GenerateDataKey` 권한이 추가되는 경우.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowActionsForSecurityLake",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsForSecurityLake",
      "Effect": "Deny",
```

```
      "NotAction": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation",
        "kms:Decrypt",
        "kms:GenerateDataKey",
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:ListQueues"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeBucket",
      "Effect": "Deny",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "NotResource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ]
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeSQS",
      "Effect": "Deny",
      "Action": [
        "sqs:ReceiveMessage",
        "sqs:ChangeMessageVisibility",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
```

```
        "sqs:ListQueues"
      ],
      "NotResource": "arn:aws:sqs:*:*:AmazonSecurityLake*"
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSS3SQS",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotLike": {
          "kms:ViaService": [
            "s3.*.amazonaws.com",
            "sqs.*.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSForS3",
      "Effect": "Deny",
      "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "kms:EncryptionContext:aws:s3:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:s3:arn": [
            "arn:aws:s3:::aws-security-data-lake*"
          ]
        }
      }
    },
    {
      "Sid": "DenyActionsNotOnSecurityLakeKMSForS3SQS",
      "Effect": "Deny",
      "Action": [
```

```
        "kms:Decrypt",
        "kms:GenerateDataKey"
      ],
      "Resource": "*",
      "Condition": {
        "Null": {
          "kms:EncryptionContext:aws:sqs:arn": "false"
        },
        "StringNotLikeIfExists": {
          "kms:EncryptionContext:aws:sqs:arn": [
            "arn:aws:sqs:*:*:AmazonSecurityLake*"
          ]
        }
      }
    }
  ]
}
```

AWS 관리형 정책: AmazonSecurityLakeAdministrator

보안 주체가 계정에 대해 Amazon Security Lake를 활성화하기 전에 보안 주체에 `AmazonSecurityLakeAdministrator` 정책을 연결할 수 있습니다. 이 정책은 보안 주체에게 모든 Security Lake에 대한 전체 액세스를 허용하는 관리 권한을 부여합니다. 그러면 주체가 Security Lake에 온보딩한 다음 Security Lake에서 소스 및 구독자를 구성할 수 있습니다.

이 정책에는 Security Lake 관리자가 Security Lake를 통해 다른 AWS 서비스에서 수행할 수 있는 작업이 포함됩니다.

이 `AmazonSecurityLakeAdministrator` 정책은 Security Lake가 Amazon S3 리전 간 복제를 관리하고,에서 새 데이터 파티션을 등록하고 AWS Glue, 사용자 지정 소스에 추가된 데이터에 대해 Glue 크롤러를 실행하거나, HTTPS 엔드포인트 구독자에게 새 데이터를 알리는 데 필요한 유틸리티 역할 생성을 지원하지 않습니다. Amazon Security Lake 시작하기에 설명된 대로 이러한 역할을 미리 생성할 수 있습니다.

`AmazonSecurityLakeAdministrator` 관리형 정책 외에도 Security Lake에는 온보딩 및 구성 기능을 위한 `lakeformation:PutDataLakeSettings` 권한이 필요합니다. `PutDataLakeSettings`은 IAM 보안 주체를 계정의 모든 리전의 Lake Formation 리소스에 대한 관리자로 설정할 수 있습니다. 이 역할에는 `iam:CreateRole permission`뿐만 아니라 `AmazonSecurityLakeAdministrator` 정책도 첨부되어 있어야 합니다.

Lake Formation 관리자는 Lake Formation 콘솔에 대한 전체 액세스 권한을 가지며 초기 데이터 구성 및 액세스 권한을 제어할 수 있습니다. Security Lake는 Security Lake를 활성화하는 주체와 `AmazonSecurityLakeMetaStoreManager` 역할(또는 기타 지정된 역할)을 Lake Formation 관리자로 할당하여 이들이 테이블을 생성하고, 테이블 스키마를 업데이트하고, 새 파티션을 등록하고, 테이블에 대한 권한을 구성할 수 있도록 합니다. Security Lake 관리자 사용자 또는 역할에 대한 정책에 다음 권한을 포함해야 합니다.

> **Note**
>
> Lake Formation 기반 구독자 액세스 권한을 부여할 수 있는 충분한 권한을 제공하려면 Security Lake에서 다음 `glue:PutResourcePolicy` 권한을 추가하는 것이 좋습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPutLakeFormationSettings",
      "Effect": "Allow",
      "Action": "lakeformation:PutDatalakeSettings",
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowGlueActions",
      "Effect": "Allow",
      "Action": ["glue:PutResourcePolicy", "glue:DeleteResourcePolicy"],
      "Resource": [
        "arn:aws:glue:*:*:catalog",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
```

```
    }
  ]
}
```

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `securitylake` - 보안 주체가 모든 Security Lake에 대한 모든 권한을 허용합니다.
- `organizations` - 보안 주체가 조직에서 AWS 조직의 계정에 대한 정보를 검색할 수 있습니다. 계정이 조직에 속한 경우 이러한 권한을 통해 Security Lake 콘솔에 계정 이름과 계정 번호를 표시할 수 있습니다.
- `iam` - 보안 주체가 Security Lake Amazon EventBridge, AWS Lake Formation및에 대한 서비스 연결 역할을 해당 서비스를 활성화할 때 필요한 단계로 생성할 수 있도록 허용합니다. 또한 구독자 및 사용자 지정 소스 역할에 대한 정책을 만들고 편집할 수 있으며, 이러한 역할의 권한은 `AmazonSecurityLakePermissionsBoundary` 정책에서 허용하는 한도로 제한됩니다.
- `ram` - 보안 주체가 Security Lake 소스 구독자의 Lake Formation기반 쿼리 액세스를 구성할 수 있습니다.
- `s3` - 보안 주체가 Security Lake 버킷을 생성 및 관리하고 해당 버킷의 내용을 읽을 수 있습니다.
- `lambda` - 보안 주체가 AWS 소스 전송 및 리전 간 복제 후 테이블 파티션을 업데이트 AWS Glue 하는 데 Lambda 사용되는를 관리할 수 있습니다.
- `glue`— 보안 주체가 Security Lake에 사용되는 데이터베이스 및 테이블을 생성 및 관리할 수 있습니다.
- `lakeformation` - 보안 주체가 Security Lake 테이블에 대한 Lake Formation 권한을 관리할 수 있도록 허용합니다.
- `events`— 보안 주체가 Security Lake 소스의 새 데이터를 구독자에게 알리는 데 사용되는 규칙을 관리할 수 있습니다.
- `sqs` - 보안 주체가 Security Lake 소스의 새 데이터를 구독자에게 알리는 데 사용되는 Amazon SQS 대기열을 생성하고 관리할 수 있습니다.
- kms— 보안 주체가 고객 관리 키를 사용하여 데이터를 기록할 수 있는 액세스 권한을 Security Lake에 부여할 수 있습니다.
- `secretsmanager` - 보안 주체가 HTTPS 엔드포인트를 통해 Security Lake 소스의 새 데이터를 구독자에게 알리는 데 사용되는 암호를 관리할 수 있습니다.

```
{
"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowActionsWithAnyResource",
    "Effect": "Allow",
    "Action": [
      "securitylake:*",
      "organizations:DescribeOrganization",
      "organizations:ListDelegatedServicesForAccount",
      "organizations:ListAccounts",
      "iam:ListRoles",
      "ram:GetResourceShareAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AllowActionsWithAnyResourceViaSecurityLake",
    "Effect": "Allow",
    "Action": [
      "glue:CreateCrawler",
      "glue:StopCrawlerSchedule",
      "lambda:CreateEventSourceMapping",
      "lakeformation:GrantPermissions",
      "lakeformation:ListPermissions",
      "lakeformation:RegisterResource",
      "lakeformation:RevokePermissions",
      "lakeformation:GetDatalakeSettings",
      "events:ListConnections",
      "events:ListApiDestinations",
      "iam:GetRole",
      "iam:ListAttachedRolePolicies",
      "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowManagingSecurityLakeS3Buckets",
```

```
    "Effect": "Allow",
    "Action": [
      "s3:CreateBucket",
      "s3:PutBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:PutBucketNotification",
      "s3:PutBucketTagging",
      "s3:PutEncryptionConfiguration",
      "s3:PutBucketVersioning",
      "s3:PutReplicationConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:ListBucket",
      "s3:PutObject",
      "s3:GetBucketNotification"
    ],
    "Resource": "arn:aws:s3:::aws-security-data-lake*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowLambdaCreateFunction",
    "Effect": "Allow",
    "Action": [
      "lambda:CreateFunction"
    ],
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowLambdaAddPermission",
    "Effect": "Allow",
    "Action": [
      "lambda:AddPermission"
    ],
```

```
    "Resource": [
      "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
      "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
      "StringEquals": {
        "lambda:Principal": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowGlueActions",
    "Effect": "Allow",
    "Action": [
      "glue:CreateDatabase",
      "glue:GetDatabase",
      "glue:CreateTable",
      "glue:GetTable"
    ],
    "Resource": [
      "arn:aws:glue:*:*:catalog",
      "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
      "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
    ],
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowEventBridgeActions",
    "Effect": "Allow",
    "Action": [
      "events:PutTargets",
      "events:PutRule",
      "events:DescribeRule",
      "events:CreateApiDestination",
      "events:CreateConnection",
      "events:UpdateConnection",
      "events:UpdateApiDestination",
```

```
        "events:DeleteConnection",
        "events:DeleteApiDestination",
        "events:ListTargetsByRule",
        "events:RemoveTargets",
        "events:DeleteRule"
      ],
      "Resource": [
        "arn:aws:events:*:*:rule/AmazonSecurityLake*",
        "arn:aws:events:*:*:rule/SecurityLake*",
        "arn:aws:events:*:*:api-destination/AmazonSecurityLake*",
        "arn:aws:events:*:*:connection/AmazonSecurityLake*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowSQSActions",
      "Effect": "Allow",
      "Action": [
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "sqs:GetQueueURL",
        "sqs:AddPermission",
        "sqs:GetQueueAttributes",
        "sqs:DeleteQueue"
      ],
      "Resource": [
        "arn:aws:sqs:*:*:SecurityLake*",
        "arn:aws:sqs:*:*:AmazonSecurityLake*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowKmsCmkGrantForSecurityLake",
      "Effect": "Allow",
      "Action": "kms:CreateGrant",
      "Resource": "arn:aws:kms:*:*:key/*",
```

```
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      },
      "StringLike": {
        "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": [
          "GenerateDataKey",
          "RetireGrant",
          "Decrypt"
        ]
      }
    }
  },
  {
    "Sid": "AllowEnablingQueryBasedSubscribers",
    "Effect": "Allow",
    "Action": [
      "ram:CreateResourceShare",
      "ram:AssociateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "StringLikeIfExists": {
        "ram:ResourceArn": [
          "arn:aws:glue:*:*:catalog",
          "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
          "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*"
        ]
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowConfiguringQueryBasedSubscribers",
    "Effect": "Allow",
    "Action": [
      "ram:UpdateResourceShare",
      "ram:GetResourceShares",
      "ram:DisassociateResourceShare",
```

```
      "ram:DeleteResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "ram:ResourceShareName": "LakeFormation*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowConfiguringCredentialsForSubscriberNotification",
    "Effect": "Allow",
    "Action": [
      "secretsmanager:CreateSecret",
      "secretsmanager:GetSecretValue",
      "secretsmanager:PutSecretValue"
    ],
    "Resource": "arn:aws:secretsmanager:*:*:secret:events!connection/
AmazonSecurityLake-*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForUpdatingGluePartitionsSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
      "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "lambda.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
```

```
    },
    {
      "Sid": "AllowPassRoleForUpdatingGluePartitionsLambdaArn",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManager",
        "arn:aws:iam::*:role/service-role/AmazonSecurityLakeMetaStoreManagerV2"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "lambda.amazonaws.com"
        },
        "StringLike": {
          "iam:AssociatedResourceARN": [
            "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
            "arn:aws:lambda:*:*:function:AmazonSecurityLake*"
          ]
        },
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": "securitylake.amazonaws.com"
        }
      }
    },
    {
      "Sid": "AllowPassRoleForCrossRegionReplicationSecLakeArn",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "s3.amazonaws.com"
        },
        "StringLike": {
          "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
        }
      }
    },
    {
      "Sid": "AllowPassRoleForCrossRegionReplicationS3Arn",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::*:role/service-role/AmazonSecurityLakeS3ReplicationRole",
      "Condition": {
```

```
      "StringEquals": {
        "iam:PassedToService": "s3.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:s3:::aws-security-data-lake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerSecLakeArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "glue.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:data-lake/default"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForCustomSourceCrawlerGlueArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeCustomDataGlueCrawler*",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "glue.amazonaws.com"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForSubscriberNotificationSecLakeArn",
    "Effect": "Allow",
```

```
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "events.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:securitylake:*:*:subscriber/*"
      }
    }
  },
  {
    "Sid": "AllowPassRoleForSubscriberNotificationEventsArn",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam::*:role/service-role/
AmazonSecurityLakeSubscriberEventBridge",
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "events.amazonaws.com"
      },
      "StringLike": {
        "iam:AssociatedResourceARN": "arn:aws:events:*:*:rule/AmazonSecurityLake*"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowOnboardingToSecurityLakeDependencies",
    "Effect": "Allow",
    "Action": "iam:CreateServiceLinkedRole",
    "Resource": [
      "arn:aws:iam::*:role/aws-service-role/securitylake.amazonaws.com/
AWSServiceRoleForSecurityLake",
      "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
      "arn:aws:iam::*:role/aws-service-role/apidestinations.events.amazonaws.com/
AWSServiceRoleForAmazonEventBridgeApiDestinations"
    ],
    "Condition": {
      "StringLike": {
```

```
        "iam:AWSServiceName": [
          "securitylake.amazonaws.com",
          "lakeformation.amazonaws.com",
          "apidestinations.events.amazonaws.com"
        ]
      }
    }
  },
  {
    "Sid": "AllowRolePolicyActionsforSubscibersandSources",
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:PutRolePolicy",
      "iam:DeleteRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
      "StringEquals": {
        "iam:PermissionsBoundary": "arn:aws:iam::aws:policy/
AmazonSecurityLakePermissionsBoundary"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowRegisterS3LocationInLakeFormation",
    "Effect": "Allow",
    "Action": [
      "iam:PutRolePolicy",
      "iam:GetRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/lakeformation.amazonaws.com/
AWSServiceRoleForLakeFormationDataAccess",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "AllowIAMActionsByResource",
```

```
    "Effect": "Allow",
    "Action": [
      "iam:ListRolePolicies",
      "iam:DeleteRole"
    ],
    "Resource": "arn:aws:iam::*:role/AmazonSecurityLake*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "securitylake.amazonaws.com"
      }
    }
  },
  {
    "Sid": "S3ReadAccessToSecurityLakes",
    "Effect": "Allow",
    "Action": [
      "s3:Get*",
      "s3:List*"
    ],
    "Resource": "arn:aws:s3:::aws-security-data-lake-*"
  },
  {
    "Sid": "S3ReadAccessToSecurityLakeMetastoreObject",
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::security-lake-meta-store-manager-*"
  },
  {
    "Sid": "S3ResourcelessReadOnly",
    "Effect": "Allow",
    "Action": [
      "s3:GetAccountPublicAccessBlock",
      "s3:ListAccessPoints",
      "s3:ListAllMyBuckets"
    ],
    "Resource": "*"
  }
]
}
```

AWS 관리형 정책: SecurityLakeServiceLinkedRole

Security Lake는 라는 서비스 연결 역할을 `AWSServiceRoleForSecurityLake` 사용하여 보안 데이터 레이크를 생성하고 운영합니다.

`SecurityLakeServiceLinkedRole` 관리형 IAM 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Security Lake에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 Security Lake에 대한 서비스 연결 역할 권한을 참조하세요.

AWS 관리형 정책: SecurityLakeResourceManagementServiceRolePolicy

Security Lake는 라는 서비스 연결 역할을 사용하여 지속적인 모니터링 및 성능 개선을 `AWSServiceRoleForSecurityLakeResourceManagement` 수행하여 지연 시간과 비용을 줄일 수 있습니다.

`SecurityLakeResourceManagementServiceRolePolicy` 관리형 IAM 정책을 IAM 엔터티에 연결할 수 없습니다. 이 정책은 Security Lake에서 사용자를 대신하여 작업을 수행할 수 있도록 서비스 연결 역할에 연결됩니다. 자세한 내용은 리소스 관리에 대한 서비스 연결 역할 권한을 참조하세요.

AWS 관리형 정책: AWS GlueServiceRole

`AWS GlueServiceRole` 관리형 정책은 AWS Glue 크롤러를 호출하고가 사용자 지정 소스 데이터를 크롤링하고 파티션 메타데이터를 식별할 AWS Glue 수 있도록 허용합니다. 이 메타데이터는 Data Catalog에 테이블을 생성 및 업데이트하는 데 필요합니다.

자세한 내용은 Security Lake의 사용자 지정 소스에서 데이터 수집 단원을 참조하십시오.

AWS 관리형 정책에 대한 Security Lake 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후 Security Lake의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받으려면 Security Lake 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
Amazon Security Lake의 서비스 연결 역할 - 새 서비스 연결 역할	새 서비스 연결 역할을 추가했습니다`AWSServiceRoleForSecurityLa`	2024년 11월 14일

변경 사항	설명	날짜
	keResourceManageme nt . 이 서비스 연결 역할은 Security Lake에 지속적인 모니터링 및 성능 개선을 수행할 수 있는 권한을 제공하여 지연 시간과 비용을 줄일 수 있습니다.	
Amazon Security Lake의 서비스 연결 역할 - 기존 서비스 연결 역할 권한 업데이트	SecurityLakeServic eLinkedRole 정책의 AWS 관리형 정책에 AWS WAF 작업을 추가했습니다. 추가 작업을 통해 Security Lake는 Security Lake에서 AWS WAF 로그 소스로 활성화되면 로그를 수집할 수 있습니다.	2024년 5월 22일
AmazonSecurityLake PermissionsBoundary -기존 정책 업데이트	Security Lake가 정책에 SID 작업을 추가했습니다.	2024년 5월 13일
AmazonSecurityLake MetastoreManager -기존 정책 업데이트	Security Lake는 데이터 레이크에서 메타데이터를 삭제할 수 있는 메타데이터 정리 작업을 추가하도록 정책을 업데이트했습니다.	2024년 3월 27일
AmazonSecurityLakeAdministrator -기존 정책 업데이트	Security Lake는 새 AmazonSecurityLake MetastoreManagerV2 역할에 iam:PassRole 대해를 허용하도록 정책을 업데이트하고 Security Lake가 데이터 레이크 구성 요소를 배포하거나 업데이트하도록 허용합니다.	2024년 2월 23일

변경 사항	설명	날짜
AmazonSecurityLake MetastoreManager - 새 정책	Security Lake는 Security Lake가 데이터 레이크의 메타데이터를 관리할 수 있는 권한을 부여하는 새로운 관리형 정책을 추가했습니다.	2024년 1월 23일
AmazonSecurityLakeAdministrator - 새 정책	Security Lake는 보안 주체에게 모든 Security Lake 작업에 대한 전체 액세스 권한을 부여하는 새로운 관리형 정책을 추가했습니다.	2023년 5월 30일
Security Lake에 변경 내용 추적	Security Lake는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2022년 11월 29일

Security Lake에 서비스 연결 역할 사용

Security Lake는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Security Lake에 직접 연결된 IAM 역할입니다. Security Lake에서 사전 정의한 것으로, Security Lake가 사용자를 대신하여 다른 AWS 서비스 를 직접 호출하고 보안 데이터 레이크 서비스를 운영하는 데 필요한 모든 권한이 포함되어 있습니다. Security Lake는 Security Lake를 사용할 수 AWS 리전 있는 모든에서이 서비스 연결 역할을 사용합니다.

이 서비스 연결 역할을 사용하면 Security Lake를 설정할 때 필요한 권한을 수동으로 추가할 필요가 없습니다. Security Lake는 이 서비스 연결 역할의 권한을 정의하며, 달리 정의되지 않는 한 Security Lake만이 이 역할을 맡을 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요. 먼저 관련 리소스를 삭제해야만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 부주의로 삭제할 수 없기 때문에 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 다른 서비스에 대한 자세한 내용은 AWS IAM으로 작업하는 서비스를 참조하고 서비스 연결 역할 열에서 Yes가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

주제

- Security Lake에 대한 서비스 연결 역할(SLR) 권한
- 리소스 관리를 위한 서비스 연결 역할(SLR) 권한

Security Lake에 대한 서비스 연결 역할(SLR) 권한

Security Lake에서는 `AWSServiceRoleForSecurityLake`인 서비스 연결 역할을 사용합니다. 이 서비스 연결 역할은 `securitylake.amazonaws.com` 서비스에 해당 역할을 맡깁니다. Amazon Security Lake의 AWS 관리형 정책에 대한 자세한 내용은 AWS Amazon Security Lake의 정책 관리를 참조하세요.

라는 AWS 관리형 정책인 역할에 대한 권한 정책을 `SecurityLakeServiceLinkedRole`통해 Security Lake는 보안 데이터 레이크를 생성하고 운영할 수 있습니다. 또한 Security Lake는 지정된 리소스에서 다음과 같은 작업을 수행할 수 있습니다.

- AWS Organizations 작업을 사용하여 연결된 계정에 대한 정보 검색
- Amazon Elastic Compute Cloud(Amazon EC2)를 사용하여 Amazon VPC 흐름 로그에 대한 정보를 검색할 수 있습니다.
- AWS CloudTrail 작업을 사용하여 서비스 연결 역할에 대한 정보 검색
- Security Lake에서 AWS WAF 로그 소스로 활성화된 경우 AWS WAF 작업을 사용하여 로그 수집
- `LogDelivery` 작업을 사용하여 AWS WAF 로그 전송 구독을 생성하거나 삭제합니다.

역할은 다음의 권한 정책으로 구성됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Sid": "OrganizationsPolicies",
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:DescribeOrganization"
            ],
            "Resource": [
```

```
                "*"
            ]
        },
        {
            "Sid": "DescribeOrgAccounts",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeAccount"
            ],
            "Resource": [
                "arn:aws:organizations::*:account/o-*/*"
            ]
        },
        {
            "Sid": "AllowManagementOfServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:CreateServiceLinkedChannel",
                "cloudtrail:DeleteServiceLinkedChannel",
                "cloudtrail:GetServiceLinkedChannel",
                "cloudtrail:UpdateServiceLinkedChannel"
            ],
            "Resource": "arn:aws:cloudtrail:*:*:channel/aws-service-channel/security-
lake/*"
        },
        {
            "Sid": "AllowListServiceLinkedChannel",
            "Effect": "Allow",
            "Action": [
                "cloudtrail:ListServiceLinkedChannels"
            ],
            "Resource": "*"
        },
        {
            "Sid": "DescribeAnyVpc",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ListDelegatedAdmins",
            "Effect": "Allow",
```

```
            "Action": [
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "securitylake.amazonaws.com"
                }
            }
        },
        {
            "Sid": "AllowWafLoggingConfiguration",
            "Effect": "Allow",
            "Action": [
                "wafv2:PutLoggingConfiguration",
                "wafv2:GetLoggingConfiguration",
                "wafv2:ListLoggingConfigurations",
                "wafv2:DeleteLoggingConfiguration"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "wafv2:LogScope": "SecurityLake"
                }
            }
        },
        {
            "Sid": "AllowPutLoggingConfiguration",
            "Effect": "Allow",
            "Action": [
                "wafv2:PutLoggingConfiguration"
            ],
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "wafv2:LogDestinationResource": "arn:aws:s3:::aws-waf-logs-
security-lake-*"
                }
            }
        },
        {
            "Sid": "ListWebACLs",
            "Effect": "Allow",
            "Action": [
```

```
                "wafv2:ListWebACLs"
            ],
            "Resource": "*"
        },
        {
            "Sid": "LogDelivery",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogDelivery",
                "logs:DeleteLogDelivery"
            ],
            "Resource": "*",
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:CalledVia": [
                        "wafv2.amazonaws.com"
                    ]
                }
            }
        }

    ]
}
```

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Security Lake 서비스 연결 역할 생성

Security Lake의 `AWSServiceRoleForSecurityLake` 서비스 연결 역할을 수동으로 생성할 필요가 없습니다. 에 대해 Security Lake를 활성화하면 AWS 계정 Security Lake가 자동으로 서비스 연결 역할을 생성합니다.

Security Lake 서비스 연결 역할 편집

Security Lake는 `AWSServiceRoleForSecurityLake` 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할이 생성된 후에는 여러 엔터티가 역할을 참조할 수 있으므로, 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Security Lake 서비스 연결 역할 삭제

Security Lake에서는 서비스 연결 역할을 삭제할 수 없습니다. 대신 IAM 콘솔, API 또는에서 서비스 연결 역할을 삭제할 수 있습니다 AWS CLI. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

서비스 연결 역할을 삭제하려면 먼저 해당 역할에 활성 섹션이 없는지 확인하고 `AWSServiceRoleForSecurityLake`가 사용 중인 모든 리소스를 제거해야 합니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Security Lake가 `AWSServiceRoleForSecurityLake` 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

`AWSServiceRoleForSecurityLake` 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 계정의 Security Lake를 활성화하여 다시 생성할 수 있습니다. Security Lake를 다시 활성화하면 Security Lake는 서비스 연결 역할을 다시 생성합니다.

Security Lake 서비스 연결 역할에 AWS 리전 지원됩니다.

Security Lake는 Security Lake를 사용할 수 AWS 리전 있는 모든에서 `AWSServiceRoleForSecurityLake` 서비스 연결 역할 사용을 지원합니다. Security Lake를 사용할 수 있는 리전 목록은 Security Lake 리전 및 엔드포인트 섹션을 참조하세요.

리소스 관리를 위한 서비스 연결 역할(SLR) 권한

Security Lake는 라는 서비스 연결 역할을 `AWSServiceRoleForSecurityLakeResourceManagement` 사용하여 지속적인 모니터링 및 성능 개선을 수행하여 지연 시간과 비용을 줄일 수 있습니다. 이 서비스 연결 역할은 `resource-management.securitylake.amazonaws.com` 서비스에 해당 역할을 맡깁니다. 또한 `AWSServiceRoleForSecurityLakeResourceManagement`를 활성화하면 Lake Formation에 대한 액세스 권한이 부여되고 보안 개선을 위해 모든 리전에서 Security Lake 관리형 S3 버킷이 Lake Formation에 자동으로 등록됩니다.

라는 AWS 관리형 정책인 역할에 대한 권한 정책은 데이터 레이크의 메타데이터 관리를 포함하여 Security Lake에서 생성한 리소스를 관리할 수 있는 액세스를 `SecurityLakeResourceManagementServiceRolePolicy`허용합니다. Amazon Security Lake의 AWS 관리형 정책에 대한 자세한 내용은 AWS Amazon Security Lake의 관리형 정책을 참조하세요.

이 서비스 연결 역할을 통해 Security Lake는 Security Lake에서 계정에 배포한 리소스(S3 버킷, AWS Glue 테이블, Amazon SQS 대기열, Metastore Manager(MSM) Lambda 함수 및 EventBridge 규칙)의 상태를 모니터링할 수 있습니다. Security Lake가이 서비스 연결 역할로 수행할 수 있는 작업의 몇 가지 예는 다음과 같습니다.

- Apache Iceberg 매니페스트 파일 압축으로 쿼리 성능이 향상되고 Lambda MSM 처리 시간과 비용이 절감됩니다.
- Amazon SQS의 상태를 모니터링하여 수집 문제를 감지합니다.
- 메타데이터 파일을 제외하도록 리전 간 데이터 복제를 최적화합니다.

> **Note**
>
> `AWSServiceRoleForSecurityLakeResourceManagement` 서비스 연결 역할을 설치하지 않으면 Security Lake는 계속 작동하지만 Security Lake가 계정의 리소스를 모니터링하고 최적화할 수 있도록이 서비스 연결 역할을 수락하는 것이 좋습니다.

권한 세부 정보

역할은 다음의 권한 정책으로 구성됩니다.

- `events` - 보안 주체가 로그 소스 및 로그 구독자에 필요한 EventBridge 규칙을 관리할 수 있도록 허용합니다.
- `lambda` - 보안 주체가 AWS 소스 전송 및 리전 간 복제 후 AWS Glue 테이블 파티션을 업데이트하는 데 사용되는 Lambda를 관리할 수 있도록 허용합니다.
- `glue` - 보안 주체가 AWS Glue 데이터 카탈로그 테이블에 대한 특정 쓰기 작업을 수행할 수 있도록 허용합니다. 또한 AWS Glue 크롤러가 데이터의 파티션을 식별하고 Security Lake가 Apache Iceberg 테이블에 대한 Apache Iceberg 메타데이터를 관리할 수 있습니다.
- `s3` - 보안 주체가 로그 데이터 및 Glue 테이블 메타데이터가 포함된 Security Lake 버킷에서 특정 읽기 및 쓰기 작업을 수행할 수 있도록 허용합니다.
- `logs` - 보안 주체가 Lambda 함수의 출력을 CloudWatch Logs에 로깅할 수 있는 읽기 액세스를 허용합니다.
- `sqs` - 보안 주체가 데이터 레이크에 객체가 추가되거나 업데이트될 때 이벤트 알림을 수신하는 Amazon SQS 대기열에 대해 특정 읽기 및 쓰기 작업을 수행할 수 있도록 허용합니다.

- `lakeformation` - 보안 주체가 Lake Formation 설정을 읽고 잘못된 구성을 모니터링할 수 있습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadEventBridgeRules",
      "Effect": "Allow",
      "Action": [
        "events:ListRules"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ManageSecurityLakeEventRules",
      "Effect": "Allow",
      "Action": [
        "events:PutRule"
      ],
      "Resource": "arn:aws:events:*:*:rule/AmazonSecurityLake-*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ManageSecurityLakeLambdaConfigurations",
      "Effect": "Allow",
      "Action": [
        "lambda:GetEventSourceMapping",
        "lambda:GetFunction",
        "lambda:PutFunctionConcurrency",
        "lambda:GetProvisionedConcurrencyConfig",
        "lambda:GetFunctionConcurrency",
        "lambda:GetRuntimeManagementConfig",
```

```
        "lambda:PutProvisionedConcurrencyConfig",
        "lambda:PublishVersion",
        "lambda:DeleteFunctionConcurrency",
        "lambda:DeleteEventSourceMapping",
        "lambda:GetAlias",
        "lambda:GetPolicy",
        "lambda:GetFunctionConfiguration",
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource": [
        "arn:aws:lambda:*:*:function:SecurityLake_Glue_Partition_Updater_Lambda*",
        "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowListLambdaEventSourceMappings",
      "Effect": "Allow",
      "Action": [
        "lambda:ListEventSourceMappings"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowUpdateLambdaEventSourceMapping",
      "Effect": "Allow",
      "Action": [
        "lambda:UpdateEventSourceMapping"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        },
        "StringLike": {
```

```
          "lambda:FunctionArn":
 "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*"
        }
      }
    },
    {
      "Sid": "AllowUpdateLambdaConfigs",
      "Effect": "Allow",
      "Action": [
        "lambda:UpdateFunctionConfiguration"
      ],
      "Resource": "arn:aws:lambda:*:*:function:AmazonSecurityLakeMetastoreManager-*-*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ManageSecurityLakeGlueResources",
      "Effect": "Allow",
      "Action": [
        "glue:CreatePartition",
        "glue:BatchCreatePartition",
        "glue:GetTable",
        "glue:GetTables",
        "glue:UpdateTable",
        "glue:GetDatabase"
      ],
      "Resource": [
        "arn:aws:glue:*:*:table/amazon_security_lake_glue_db*/*",
        "arn:aws:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:aws:glue:*:*:catalog"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowDataLakeConfigurationManagement",
      "Effect": "Allow",
      "Action": [
```

```
        "s3:ListBucket",
        "s3:PutObject",
        "s3:GetObjectAttributes",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:GetEncryptionConfiguration",
        "s3:GetReplicationConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowMetaDataCompactionAndManagement",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:RestoreObject"
      ],
      "Resource": [
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.avro",
        "arn:aws:s3:::aws-security-data-lake*/metadata/*.metadata.json"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ReadSecurityLakeLambdaLogs",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:StartQuery",
        "logs:GetLogEvents",
```

```
        "logs:GetQueryResults",
        "logs:GetLogRecord"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/lambda/AmazonSecurityLakeMetastoreManager-*-*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "ManageSecurityLakeSQSQueue",
      "Effect": "Allow",
      "Action": [
        "sqs:StartMessageMoveTask",
        "sqs:DeleteMessage",
        "sqs:GetQueueUrl",
        "sqs:ListDeadLetterSourceQueues",
        "sqs:ChangeMessageVisibility",
        "sqs:ListMessageMoveTasks",
        "sqs:ReceiveMessage",
        "sqs:SendMessage",
        "sqs:GetQueueAttributes",
        "sqs:SetQueueAttributes"
      ],
      "Resource": [
        "arn:aws:sqs:*:*:SecurityLake_*",
        "arn:aws:sqs:*:*:AmazonSecurityLakeManager-*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "AllowDataLakeManagement",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GetDataLakeSettings",
        "lakeformation:ListPermissions"
      ],
```

```
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
      }
    }
  ]
}
```

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 링크 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한을 참조하세요.

Security Lake 서비스 연결 역할 생성

Security Lake 콘솔 또는를 사용하여 Security Lake에 대한 `AWSServiceRoleForSecurityLakeResourceManagement` 서비스 연결 역할을 생성할 수 있습니다 AWS CLI.

서비스 연결 역할을 생성하려면 IAM 사용자 또는 IAM 역할에 다음 권한을 부여해야 합니다. IAM 역할은 모든 Security Lake 지원 리전의 Lake Formation 관리자여야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLakeFormationActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "lakeformation:GrantPermissions",
        "lakeformation:ListPermissions",
        "lakeformation:ListResources",
        "lakeformation:RegisterResource",
        "lakeformation:RevokePermissions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIamActionsViaSecurityLakeConsole",
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole",
        "iam:GetPolicyVersion",
```

```
        "iam:GetRole",
        "iam:PutRolePolicy"
      ],
      "Resource": [
        "arn:*:iam::*:role/aws-service-role/resource-
management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement",
        "arn:*:iam::*:role/*AWSServiceRoleForLakeFormationDataAccess",
        "arn:*:iam::aws:policy/service-role/AWSGlueServiceRole",
        "arn:*:iam::aws:policy/service-role/AmazonSecurityLakeMetastoreManager",
        "arn:*:iam::aws:policy/aws-service-role/
SecurityLakeResourceManagementServiceRolePolicy"
      ],
      "Condition": {
        "StringLikeIfExists": {
          "iam:AWSServiceName": [
            "securitylake.amazonaws.com",
            "resource-management.securitylake.amazonaws.com",
            "lakeformation.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowGlueActionsViaConsole",
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:*:glue:*:*:catalog",
        "arn:*:glue:*:*:database/amazon_security_lake_glue_db*",
        "arn:*:glue:*:*:table/amazon_security_lake_glue_db*/*"
      ]
    }
  ]
}
```

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 요약 페이지의 정보 표시줄에서 서비스 연결 역할 활성화를 클릭하여 새 서비스 연결 역할을 수락합니다.

서비스 연결 역할을 활성화한 후에는 나중에 Security Lake를 사용하기 위해이 프로세스를 반복할 필요가 없습니다.

CLI

프로그래밍 방식으로 `AWSServiceRoleForSecurityLakeResourceManagement` 서비스 연결 역할을 생성하려면 다음 CLI 명령을 사용합니다.

```
$ aws iam create-service-linked-role
--aws-service-name resource-management.securitylake.amazonaws.com
```

를 사용하여 `AWSServiceRoleForSecurityLakeResourceManagement` 서비스 연결 역할을 생성할 때 테이블 메타데이터를 관리하고 데이터에 액세스하려면 Security Lake Glue 데이터베이스의 모든 테이블에 Lake Formation 테이블 수준 권한(ALTER, DESCRIBE)도 부여해야 AWS CLI합니다. 리전의 Glue 테이블이 이전 Security Lake 활성화의 S3 버킷을 참조하는 경우 Security Lake가이 상황을 해결할 수 있도록 서비스 연결 역할에 대한 DATA_LOCATION_ACCESS 권한을 일시적으로 허용해야 합니다.

또한 계정의 `AWSServiceRoleForSecurityLakeResourceManagement` 서비스 연결 역할에 Lake Formation 권한을 부여해야 합니다.

다음 예제에서는 Lake Formation에 지정된 리전의 서비스 연결 역할에 권한을 부여하는 방법을 보여줍니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws lakeformation grant-permissions --region {region} --principal
 DataLakePrincipalIdentifier={AWSServiceRoleForSecurityLakeResourceManagement ARN} \
--permissions ALTER DESCRIBE --resource '{ "Table": { "DatabaseName":
 "amazon_security_lake_glue_db_{region}", "TableWildcard": {} } }'
```

다음 예제에서는 역할 ARN의 모양을 보여줍니다. 리전과 일치하도록 역할 ARN을 편집해야 합니다.

`"AWS": "arn:[partition]:iam::[accountid]:role/aws-service-role/resource-management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement"`

CreateServiceLinkedRole API 호출을 사용할 수도 있습니다. 요청에서를 `AWSServiceName`로 지정합니다`resource-management.securitylake.amazonaws.com`.

`AWSServiceRoleForSecurityLakeResourceManagement` 역할을 활성화한 후 암호화에 AWS KMS 고객 관리형 키(CMK)를 사용하는 경우 서비스 연결 역할이 CMK가 있는 리전의 S3 버킷에 암호화된 객체를 AWS 쓰도록 허용해야 합니다. AWS KMS 콘솔에서 CMK가 있는 AWS 리전의 KMS 키에 다음 정책을 추가합니다. KMS 키 정책을 변경하는 방법에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 에서 키 정책을 AWS KMS 참조하세요.

```
{
    "Sid": "Allow SLR",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:[partition]:iam::[accountid]:role/aws-service-role/resource-
management.securitylake.amazonaws.com/AWSServiceRoleForSecurityLakeResourceManagement"
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey*"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::[regional-datalake-s3-
bucket-name]"
        },
        "StringLike": {
            "kms:ViaService": "s3.[region].amazonaws.com"
        }
    }
},
```

Security Lake 서비스 연결 역할 편집

Security Lake는 `AWSServiceRoleForSecurityLakeResourceManagement` 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할이 생성된 후에는 여러 엔터티가 역할을 참조할 수 있으므로, 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Security Lake 서비스 연결 역할 삭제

Security Lake에서는 서비스 연결 역할을 삭제할 수 없습니다. 대신 IAM 콘솔, API 또는에서 서비스 연결 역할을 삭제할 수 있습니다 AWS CLI. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제를 참조하십시오.

서비스 연결 역할을 삭제하려면 먼저 해당 역할에 활성 섹션이 없는지 확인하고 `AWSServiceRoleForSecurityLakeResourceManagement`가 사용 중인 모든 리소스를 제거해야 합니다.

> **Note**
>
> 리소스를 삭제하려 할 때 Security Lake가 `AWSServiceRoleForSecurityLakeResourceManagement` 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

`AWSServiceRoleForSecurityLakeResourceManagement` 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 계정의 Security Lake를 활성화하여 다시 생성할 수 있습니다. Security Lake를 다시 활성화하면 Security Lake는 서비스 연결 역할을 다시 생성합니다.

Security Lake 서비스 연결 역할에 AWS 리전 지원됩니다.

Security Lake는 Security Lake를 사용할 수 AWS 리전 있는 모든에서 `AWSServiceRoleForSecurityLakeResourceManagement` 서비스 연결 역할 사용을 지원합니다. Security Lake를 사용할 수 있는 리전 목록은 Security Lake 리전 및 엔드포인트을 참조하세요.

Amazon Security Lake의 데이터 보호

AWS 공동 책임 모델 Amazon Security Lake의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.

- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내부의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Security Lake 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

저장된 데이터 암호화

Amazon Security Lake는 AWS 암호화 솔루션을 사용하여 저장 데이터를 안전하게 저장합니다. 원시 보안 로그 및 이벤트 데이터는 Security Lake가 관리하는 계정의 소스별 다중 테넌트 Amazon Simple Storage Service(Amazon S3) 버킷에 저장됩니다. 각 로그 소스에는 자체 멀티 테넌트 버킷이 있습니다. Security Lake는 AWS Key Management Service ()에서 AWS 소유한 키를 사용하여이 원시 데이터를 암호화합니다AWS KMS. AWS 소유 키는 AWS 서비스가 소유한 AWS KMS 키 모음으로,이 경우 Security Lake는 여러 AWS 계정에서 사용할 수 있도록 관리하고 있습니다.

Security Lake는 원시 로그 및 이벤트 데이터에서 추출, 전환, 적재(ETL) 작업을 실행합니다.

ETL 작업이 완료되면 Security Lake는 계정에 단일 테넌트 S3 버킷을 생성합니다(Security Lake를 활성화 AWS 리전 한 각 버킷에 대해 버킷 하나). 데이터는 Security Lake가 단일 테넌트 S3 버킷으로 데이터를 안정적으로 전송할 수 있을 때까지 일시적으로만 다중 테넌트 S3 버킷에 저장됩니다. 싱글 테넌트 버킷에는 Security Lake에 로그 및 이벤트 데이터를 버킷에 쓸 수 있는 권한을 부여하는 리소스 기반 정책이 포함되어 있습니다. S3 버킷의 데이터를 암호화하려면 S3-managed형 암호화 키 또는 고객 관리형 키(발신)를 선택할 수 있습니다 AWS KMS. 두 옵션 모두 대칭 암호화를 사용합니다.

KMS 키를 사용하여 데이터를 암호화합니다.

기본적으로 Security Lake가 S3 버킷에 제공하는 데이터는 Amazon S3가 관리하는 암호화 키(SSE-S3)를 사용하는 서버 측 암호화를 사용하여 암호화됩니다. 직접 관리하는 보안 계층을 제공하려면 대신 Security Lake 데이터에 대한 AWS KMS 키를 사용한 서버 측 암호화(SSE-KMS)를 사용할 수 있습니다.

SSE-KMS는 Security Lake 콘솔에서 지원되지 않습니다. Security Lake API 또는 CLI와 함께 SSE-KMS를 사용하려면 먼저 KMS 키를 만들거나 기존 키를 사용해야 합니다. 키에 정책을 연결합니다. 이 키는 Security Lake 데이터를 암호화하고 암호화를 해제할 수 있는 사용자를 결정합니다.

고객 관리형 키를 사용하여 S3 버킷에 기록된 데이터를 암호화하는 경우 다중 지역 키를 선택할 수 없습니다. 고객 관리형 키의 경우 Security Lake는 `CreateGrant` 요청을 AWS KMS에 전송하여 사용자를 대신하여 권한을 생성합니다. 의 권한 부여 AWS KMS 는 Security Lake에 고객 계정의 KMS 키에 대한 액세스 권한을 부여하는 데 사용됩니다.

Security Lake는 다음 내부 작업에 대해 고객 관리형 키를 사용할 수 있는 권한이 필요합니다.

- AWS KMS 에 `GenerateDataKey` 요청을 보내 고객 관리형 키로 암호화된 데이터 키를 생성합니다.
- 에 `RetireGrant` 요청을 보냅니다 AWS KMS. 데이터 레이크를 업데이트하면 이 작업을 통해 ETL 처리를 위해 AWS KMS 키에 추가된 권한을 사용 중지할 수 있습니다.

Security Lake에는 `Decrypt` 권한이 필요하지 않습니다. 키에 대한 권한이 부여된 사용자가 Security Lake 데이터를 읽는 경우 S3는 암호화를 관리하고 권한이 부여된 사용자는 암호화되지 않은 양식에서 데이터를 읽을 수 있습니다. 하지만 구독자는 소스 데이터를 사용할 수 있는 `Decrypt` 권한이 필요합니다. 이러한 구독자 권한에 대한 자세한 내용은 Security Lake 구독자의 데이터 액세스 관리 을 참조하십시오.

기존 KMS 키를 사용하여 Security Lake 데이터를 암호화하려면 KMS 키의 키 정책을 수정해야 합니다. 키 정책은 Lake Formation 데이터 레이크 위치와 연결된 IAM 역할이 KMS 키를 사용하여 데이터를 복호화하도록 허용해야 합니다. KMS 키의 키 정책을 변경하는 방법에 대한 지침은 AWS Key Management Service 개발자 안내서의 키 정책 변경을 참조하세요.

KMS 키는 권한 부여 요청을 수락하여 키 정책을 생성하거나 적절한 권한이 있는 기존 키 정책을 사용할 때 Security Lake가 키에 액세스하도록 허용할 수 있습니다. 키 정책 생성에 대한 지침은 AWS Key Management Service 개발자 안내서의 키 정책 생성을 참조하세요.

다음 키 정책을 KMS 키에 연결합니다.

```
{
  "Sid": "Allow use of the key",
  "Effect": "Allow",
  "Principal": {"AWS": "arn:aws:iam::111122223333:role/ExampleRole"},
  "Action": [
    "kms:CreateGrant",
    "kms:DescribeKey",
    "kms:GenerateDataKey"
  ],
  "Resource": "*"
}
```

고객 관리형 키를 사용할 때 필요한 IAM 권한

Security Lake를 사용하기 위해 생성해야 하는 IAM 역할에 대한 개요는 시작하기: 사전 요구 사항 섹션을 참조하십시오.

사용자 지정 소스 또는 구독자를 추가하면 Security Lake가 계정에 IAM 역할을 생성합니다. 이러한 역할은 다른 IAM ID와 공유하기 위한 것입니다. 이를 통해 사용자 지정 소스는 데이터 레이크에 데이터를 쓰고 구독자는 데이터 레이크의 데이터를 사용할 수 있습니다. 라는 AWS 관리형 정책은 이러한 역할에 대한 권한 경계를 `AmazonSecurityLakePermissionsBoundary` 설정합니다.

Amazon SQS 대기열 암호화

데이터 레이크를 생성하면 Security Lake가 위임된 Security Lake 관리자 계정에 암호화되지 않은 Amazon Simple Queue Service(Amazon SQS) 대기열 두 개를 생성합니다. 데이터를 보호하려면 이러한 대기열을 암호화해야 합니다. Amazon Simple Queue Service에서 제공하는 기본 서버 측 암호화(SSE)만으로는 충분하지 않습니다. 대기열을 암호화하려면 AWS Key Management Service (AWS KMS)에서 고객 관리형 키를 생성하고 Amazon S3 서비스 보안 주체에게 암호화된 대기열로 작업할 수 있는 권한을 부여해야 합니다. 이러한 권한 부여에 대한 지침은 AWS 지식 센터의 Amazon S3 이벤트 알림이 서버 측 암호화를 사용하는 Amazon SQS 대기열로 전송되지 않는 이유는 무엇입니까?를 참조하세요.

Security Lake는 AWS Lambda 를 사용하여 데이터에 대한 추출, 전송 및 로드(ETL) 작업을 지원하므로 Lambda에 Amazon SQS 대기열의 메시지를 관리할 수 있는 권한도 부여해야 합니다. 자세한 내용은 AWS Lambda 개발자 가이드의 실행 역할 권한을 참조하세요.

전송 중 암호화

Security Lake는 AWS 서비스 간에 전송 중인 모든 데이터를 암호화합니다. Security Lake는 전송 계층 보안(TLS) 1.2 암호화 프로토콜을 사용하여 모든 네트워크 간 데이터를 자동으로 암호화하여 서비스에서 전송되는 데이터를 보호합니다. Security Lake API로 전송되는 직접 HTTPS 요청은 AWS 서명 버전 4 알고리즘을 사용하여 서명되어 보안 연결을 설정합니다.

서비스 개선을 위한 데이터 사용 거부

옵트아웃 AWS Organizations 정책을 사용하여 Security Lake 및 기타 AWS 보안 서비스를 개발하고 개선하는 데 데이터를 사용하지 않도록 선택할 수 있습니다. Security Lake에서 현재 그러한 데이터를 수집하지 않더라도 옵트아웃을 선택할 수 있습니다. 옵트아웃 방법에 대한 자세한 내용은 AWS Organizations 사용 설명서의 AI 서비스 옵트아웃 정책을 참조하십시오.

현재 Security Lake는 사용자를 대신하여 처리하는 보안 데이터 또는 사용자가 이 서비스에서 생성한 보안 데이터 레이크에 업로드한 보안 데이터를 수집하지 않습니다. Security Lake 서비스와 다른 AWS 보안 서비스의 기능을 개발하고 개선하기 위해 Security Lake는 타사 데이터 소스에서 업로드한 데이터를 포함하여 향후 이러한 데이터를 수집할 수 있습니다. Security Lake에서 이러한 데이터를 수집하려는 경우 이 페이지를 업데이트하고 해당 데이터의 작동 방식을 설명합니다. 언제라도 옵트아웃할 수 있는 기회는 여전히 있습니다.

> **Note**
>
> 옵트아웃 정책을 사용하려면에서 AWS 계정을 중앙에서 관리해야 합니다 AWS Organizations. AWS 계정에 대한 조직을 아직 생성하지 않은 경우 AWS Organizations 사용 설명서의 조직 생성 및 관리를 참조하세요.

옵트아웃은 다음과 같은 효과가 있습니다.

- Security Lake는 사용자가 옵트아웃하기 전에 수집 및 저장한 데이터를 삭제합니다 (있는 경우).
- 옵트아웃하면 Security Lake는 더 이상 이 데이터를 수집하거나 저장하지 않습니다.

Amazon Security Lake 규정 준수 검증

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 규정 준수 AWS 서비스 프로그램 범위규정 준수 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모든 AWS 서비스 가 HIPAA에 적합한 것은 아닙니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 업계 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(NIST), 결제 카드 산업 보안 표준 위원회(PCI), 국제표준화기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 이를 AWS 서비스 통해 내 보안 상태를 포괄적으로 확인할 수 있습니다 AWS. Security Hub는 보안 컨트롤을 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty - 의심스러운 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

Security Lake 보안 모범 사례

Amazon Security Lake로 작업할 때 다음 모범 사례를 참조하십시오.

Security Lake 사용자에게 가능한 한 최소 권한 부여

AWS Identity and Access Management (IAM) 사용자, 사용자 그룹 및 역할에 대한 최소 액세스 정책 권한 세트를 부여하여 최소 권한 원칙을 따릅니다. 예를 들어 IAM 사용자가 Security Lake의 로그 소

스 목록을 볼 수는 있지만 소스 또는 구독자를 생성하지 못하도록 허용할 수 있습니다. 자세한 내용은 Security Lake에 대한 자격 증명 기반 정책 예제 단원을 참조하세요.

AWS CloudTrail 를 사용하여 Security Lake에서 API 사용량을 추적할 수도 있습니다. CloudTrail은 Security Lake에서 사용자, 그룹, 또는 역할이 수행한 API 작업 기록을 제공합니다. 자세한 내용은 CloudTrail을 사용하여 Security Lake API 호출 로깅 단원을 참조하십시오.

요약 페이지를 봅니다.

Security Lake 콘솔의 요약 페이지는 Security Lake 서비스 및 데이터가 저장된 Amazon S3 버킷에 영향을 미친 지난 14일간의 문제에 대한 개요를 제공합니다. 이러한 문제를 추가로 조사하여 발생 가능한 보안 관련 영향을 완화하는 데 도움을 받을 수 있습니다.

Security Hub와 통합

Security Lake 및 AWS Security Hub 를 통합하여 Security Lake에서 Security Hub 조사 결과를 수신합니다. Security Hub는 다양한 AWS 서비스 타사 통합에서 결과를 생성합니다. Security Hub 조사 결과를 받으면 규정 준수 태세와 AWS 보안 모범 사례를 충족하는지 여부에 대한 개요를 확인할 수 있습니다.

자세한 내용은 와 통합 AWS Security Hub 단원을 참조하십시오.

삭제 AWS Lambda

AWS Lambda 함수를 삭제할 때 먼저 비활성화하지 않는 것이 좋습니다. 삭제하기 전에 Lambda 함수를 비활성화하면 데이터 쿼리 기능이 방해를 받고 다른 기능에 잠재적으로 영향을 미칠 수 있습니다. Lambda 함수를 비활성화하지 않고 직접 삭제하는 것이 가장 좋습니다. Lambda 함수 삭제에 대한 자세한 내용은 AWS Lambda 개발자 안내서를 참조하세요.

Security Lake 이벤트 모니터링

Amazon CloudWatch 지표를 사용하여 Security Lake를 모니터링할 수 있습니다. CloudWatch는 Security Lake의 원시 데이터를 1분마다 수집하여 지표로 처리합니다. 지표가 지정된 임계값과 일치할 경우 알림을 시작하도록 경보를 설정할 수 있습니다.

자세한 내용은 Amazon Security Lake에 대한 CloudWatch 지표 단원을 참조하십시오.

Amazon Security Lake의 복원성

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결된 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공합니다. 이러한 가용 영역은 응용 프로그램과 데이터베이스를 설계하고 운영하는 효과적인 방법을 제공합니다. 가용 영역은 기존의 단일 또는 복수 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

Security Lake의 가용성은 리전 가용성과 관련이 있습니다. 여러 가용 영역에 분산하면 서비스가 단일 가용 영역의 장애를 견딜 수 있습니다.

Security Lake 데이터 영역의 가용성은 리전 가용성과 관련이 없습니다. 하지만 Security Lake 컨트롤 플레인의 가용성은 미국 동부 (버지니아 북부) 리전 가용성과 밀접하게 연관되어 있습니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 외에도 Amazon Simple Storage Service(Amazon S3)에서 데이터를 지원하는 Security Lake는 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 제공합니다.

수명 주기 구성

수명 주기 구성은 Amazon S3가 객체 그룹에 적용되는 작업을 정의하는 일련의 규칙입니다. 수명 주기 구성 규칙을 사용하면 Amazon S3가 객체를 더 저렴한 스토리지 클래스로 전환하거나 보관하거나 삭제하도록 유도할 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 스토리지 수명 주기 관리를 참조하세요.

버전 관리

버전 관리는 동일 버킷 내에 여러 개의 객체 변형을 보유하는 것을 의미합니다. 버전 관리를 사용하면 Amazon S3 버킷에 저장된 모든 버전의 모든 객체를 보존, 검색 및 복원할 수 있습니다. 버전 관리는 의도치 않은 사용자 작업 및 애플리케이션 장애로부터 복구하는 데 도움이 됩니다. 자세한 내용은 Amazon S3 사용자 설명에서 S3 버킷에서 버전 관리 사용을 참조하세요.

스토리지 클래스

Amazon S3는 워크로드 요구 사항에 따라 선택할 수 있는 다양한 스토리지 클래스를 제공합니다. S3 Standard-IA 및 S3 One Zone-IA 스토리지 클래스는 한 달에 한 번 정도 액세스하며 밀리초 단위의 액세스가 필요한 데이터용으로 설계되었습니다. S3 Glacier Instant Retrieval 스토리지 클래스는 분기에 한 번 정도 액세스하며 밀리초 단위의 액세스가 필요한 수명이 긴 아카이브 데이터용으로 설계되었습니다. 백업과 같이 즉각적인 액세스가 필요하지 않은 아카이브 데이터의 경우 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스를 사용할 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 Storage Classes 사용을 참조하세요.

Amazon Security Lake의 인프라 보안

관리형 서비스인 Amazon Security Lake는 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 Security Pillar AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Security Lake에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 자격 증명을 생성하여 요청에 서명할 수 있습니다.

Security Lake의 구성 및 취약성 분석

구성 및 IT 제어는 AWS 와 고객 간의 공동 책임입니다. 자세한 내용은 AWS 공동 책임 모델을 참조하세요.

Amazon Security Lake 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)

인터페이스 VPC 엔드포인트를 생성하여 VPC와 Amazon Security Lake 간에 프라이빗 연결을 설정할 수 있습니다. 인터페이스 엔드포인트는 인터넷 게이트웨이AWS PrivateLink, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 Security Lake APIs에 비공개로 액세스할 수 있는 기술인 로 구동됩니다. VPC의 인스턴스는 Security Lake APIs. VPC와 Security Lake 간의 트래픽은 Amazon 네트워크를 벗어나지 않습니다.

각 인터페이스 엔드포인트는 서브넷에서 하나 이상의 탄력적 네트워크 인터페이스로 표현됩니다.

자세한 내용은 AWS PrivateLink 설명서의 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하십시오.

Security Lake VPC 엔드포인트 고려 사항

Security Lake용 인터페이스 VPC 엔드포인트를 설정하기 전에 AWS PrivateLink 가이드의 인터페이스 엔드포인트 속성 및 제한 사항을 검토해야 합니다.

Security Lake는 VPC에서 모든 API 작업을 호출할 수 있도록 지원합니다.

Security Lake는 FIPS가 있는 다음 리전에서만 FIPS VPC 엔드포인트를 지원합니다.

- 미국 동부(버지니아 북부)
- 미국 동부(오하이오)
- 미국 서부(캘리포니아 북부)
- 미국 서부(오리건)

Security Lake용 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 Security Lake 서비스에 대한 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트 생성을 참조하세요.

다음 서비스 이름을 사용하여 Security Lake용 VPC 엔드포인트를 생성합니다.

- com.amazonaws.*region*.securitylake
- com.amazonaws.*region*.securitylake-fips(FIPS 엔드포인트)

엔드포인트에 대해 프라이빗 DNS를 활성화하는 경우 리전의 기본 DNS 이름을 사용하여 Security Lake에 API 요청을 할 수 있습니다. 예: `securitylake.us-east-1.amazonaws.com`.

자세한 내용은 AWS PrivateLink 설명서의 인터페이스 엔드포인트를 통해 서비스 액세스를 참조하십시오.

Security Lake에 대한 VPC 엔드포인트 정책 생성

Security Lake에 대한 액세스를 제어하는 엔드포인트 정책을 VPC 엔드포인트에 연결할 수 있습니다. 이 정책은 다음 정보를 지정합니다.

- 작업을 수행할 수 있는 위탁자.
- 수행할 수 있는 작업.

- 작업을 수행할 수 있는 리소스.

자세한 내용은 AWS PrivateLink 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하십시오.

예: Security Lake 작업에 대한 VPC 엔드포인트 정책

다음은 Security Lake에 대한 엔드포인트 정책의 예입니다. 엔드포인트에 연결되면이 정책은 모든 리소스의 모든 보안 주체에 대해 나열된 Security Lake 작업에 대한 액세스 권한을 부여합니다.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "securitylake:ListDataLakes",
            "securitylake:ListLogSources",
            "securitylake:ListSubscribers"
         ],
         "Resource":"*"
      }
   ]
}
```

공유 서브넷

공유하는 서브넷의 VPC 엔드포인트는 생성, 설명, 수정 또는 삭제할 수 없습니다. 그러나 공유하는 서브넷의 VPC 엔드포인트를 사용할 수는 있습니다. VPC 공유에 관한 자세한 내용은 Amazon VPC 사용 설명서의 다른 계정과 VPC 공유를 참조하십시오.

Amazon Security Lake 모니터링

Security Lake는 사용자 AWS CloudTrail, 역할 또는 다른 사용자가 Security Lake에서 수행한 작업에 대한 레코드를 제공하는 서비스인와 통합됩니다 AWS 서비스. 여기에는 Security Lake 콘솔의 작업과 Security Lake API 작업에 대한 프로그래밍 방식 직접 호출이 포함됩니다. CloudTrail에서 수집한 정보를 사용하여 Security Lake에 대해 어떤 요청이 수행되었는지 확인할 수 있습니다. 각 요청에 대해 요청이 이루어진 시기, 요청이 이루어진 IP 주소, 요청한 사람 및 추가 세부 정보를 식별할 수 있습니다. 자세한 내용은 CloudTrail을 사용하여 Security Lake API 호출 로깅 단원을 참조하십시오.

Security Lake 및 Amazon CloudWatch가 통합되어 Security Lake 및 로그에 대한 지표를 수집, 확인 및 분석할 수 있습니다. Security Lake 데이터 레이크에 대한 CloudWatch의 지표는 자동으로 수집되어 1분 간격으로 CloudWatch에 푸시됩니다. Security Lake 지표에 대해 지정된 임계값에 도달하면 알림을 전송하도록 경보를 설정할 수도 있습니다. Security Lake가 CloudWatch에 전송하는 모든 지표 목록은 Security Lake 지표 및 차원에서 확인하세요.

Amazon Security Lake에 대한 CloudWatch 지표

원시 데이터를 수집하여 읽기 가능하며 실시간에 가까운 지표로 처리하는 Amazon CloudWatch를 통해 Security Lake를 모니터링할 수 있습니다. 이러한 통계는 15개월간 보관되므로 기록 정보에 액세스하고 데이터 레이크의 데이터를 전체적으로 더 잘 파악할 수 있습니다. 특정 임곗값을 주시하다가 해당 임곗값이 충족될 때 알림을 전송하거나 조치를 취하도록 경보를 설정할 수도 있습니다.

주제

- Security Lake 지표 및 차원
- Security Lake에 대한 CloudWatch 지표 보기
- Security Lake 지표에 대한 CloudWatch 경보 설정

Security Lake 지표 및 차원

`AWS/SecurityLake` 네임스페이스에는 다음과 같은 지표가 포함됩니다.

지표	설명
`ProcessedSize`	현재 데이터 레이크에 저장된 기본적으로 지원되는의 데이터 볼륨 AWS 서비스 입니다. 단위: 바이트

다음 차원에 사용할 수 있는 Security Lake 지표는 다음과 같습니다.

차원	설명
`Account`	특정 AWS 계정항목에 대한 지표 `Processed Size` 이 차원은 CloudWatch에서 `Per-Accou`

차원	설명
	nt Source Version Metrics 볼 때만 사용할 수 있습니다.
Region	특정 항목 AWS 리전에 대한 지표 Processed Size
Source	ProcessedSize 특정 AWS 로그 소스에 대한 지표입니다.
SourceVersion	ProcessedSize AWS 로그 소스의 특정 버전에 대한 지표입니다.

특정 AWS 계정 (Per-Account Source Version Metrics) 또는 조직의 모든 계정()에 대한 지표를 볼 수 있습니다Per-Source Version Metrics.

Security Lake에 대한 CloudWatch 지표 보기

CloudWatch 콘솔, CloudWatch의 자체 명령줄 인터페이스(CLI)를 사용하거나 프로그래밍 방식으로 CloudWatch API를 사용하여 Security Lake에 대한 지표를 모니터링할 수 있습니다. 원하는 방법을 선택하고 단계에 따라 Security Lake 지표에 액세스하십시오.

CloudWatch console

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 탐색 창에서 지표(Metrics), 모든 지표(All metrics)를 선택합니다.
3. 찾아보기 탭에서 Security Lake를 선택합니다.
4. 계정별 소스 버전 지표 또는 소스별 버전 지표를 선택합니다.
5. 지표를 선택하면 자세히 볼 수 있습니다. 다음을 선택할 수도 있습니다.
   - 지표를 정렬하려면 열 머리글을 사용합니다.
   - 지표를 그래프로 표시하려면 지표 이름을 선택하고 그래프 옵션을 선택합니다.
   - 지표로 필터링하려면 지표 이름을 선택한 후 검색에 추가를 선택합니다.

CloudWatch API

CloudWatch API를 사용하여 Security Lake 지표에 액세스하려면 `GetMetricStatistics` 작업을 사용합니다.

AWS CLI

를 사용하여 Security Lake 지표에 액세스하려면 `get-metric-statistics` 명령을 AWS CLI실행합니다.

지표를 사용한 모니터링에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 지표 사용을 참조하세요.

Security Lake 지표에 대한 CloudWatch 경보 설정

CloudWatch에서는 지표에 대한 임계값에 도달한 경우에도 경보를 설정할 수 있습니다. 예를 들어 ProcessedSize 지표에 대한 경보를 설정하여 특정 소스의 데이터 볼륨이 특정 임계값을 초과할 때 알림을 받을 수 있습니다.

알림에 대한 구체적인 지침은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 경보 사용을 참조하십시오.

CloudTrail을 사용하여 Security Lake API 호출 로깅

Amazon Security Lake는 Security Lake의 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Security Lake에 대한 API 직접 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Security Lake 콘솔에서의 직접 호출과 Security Lake API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 Security Lake에 대한 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Security Lake에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Security Lake 정보

CloudTrail은 계정을 생성할 AWS 계정 때에서 활성화됩니다. Security Lake에서 활동이 발생하면 해당 활동이 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. 에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다 AWS 계정. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Security Lake에 대한 이벤트를 AWS 계정포함하여에서 이벤트를 지속적으로 기록하려면 추적을 생성합니다. trail은 추적을 사용하여 사용자가 지정한 Amazon S3 버킷으로 이벤트의 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션의 모든 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

Security Lake 작업은 CloudTrail에서 로깅되고 Security Lake API 참조에 기록됩니다. 예를 들어 `UpdateDataLake`, `ListLogSources` 및 `CreateSubscriber` 작업을 직접적으로 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 대한 정보가 포함됩니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청을 했는지 여부입니다.

자세한 내용은 CloudTrail userIdentity 요소를 참조하십시오.

Security Lake 로그 파일 항목 이해

CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 Security Lake `GetSubscriber` 작업에 대한 CloudTrail 로그 항목을 표시합니다.

```
{
   "eventVersion": "1.08",
   "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE:user",
      "arn": "arn:aws:sts::123456789012:assumed-role/Admin/user",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "sessionContext": {
         "sessionIssuer": {
            "type": "Role",
            "principalId": "AIDACKCEVSQ6C2EXAMPLE",
            "arn": "arn:aws:iam::123456789012:role/Admin",
            "accountId": "123456789012",
            "userName": "Admin"
         },
         "webIdFederationData": {
         },
         "attributes": {
            "creationDate": "2023-05-30T13:27:19Z",
            "mfaAuthenticated": "false"
         }
```

```
        }
    },
    "eventTime": "2023-05-30T17:29:17Z",
    "eventSource": "securitylake.amazonaws.com",
    "eventName": "GetSubscriber",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "198.51.100.1",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "subscriberId": "30ed17a3-0cac-4997-a41f-f5a6bexample"
    },
    "responseElements": null,
    "requestID": "d01f0f32-9ec6-4579-af50-e9f14example",
    "eventID": "9c1bff41-0f48-4ee6-921c-ebfd8example",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

Security Lake 리소스에 태그 지정

태그는 특정 유형의 Amazon Security Lake AWS 리소스를 포함하여 리소스를 정의하고 리소스에 할당할 수 있는 선택적 레이블입니다. 태그를 사용하면 용도, 소유자, 환경 또는 기타 기준과 같은 다양한 방법으로 리소스를 분류하고 관리하는 데 도움이 됩니다. 예를 들어 태그를 사용하여 정책을 적용하고, 비용을 할당하고, 리소스를 구분하거나, 특정 규정 준수 요구 사항 또는 워크플로를 지원하는 리소스를 식별할 수 있습니다.

구독자 및 개별의 데이터 레이크 구성과 같은 유형의 Security Lake 리소스 AWS 계정 에 태그를 할당할 수 있습니다 AWS 리전.

주제

- 태그 지정 기본 사항
- IAM 정책에서 태그 사용
- Amazon Security Lake 리소스에 태그 추가
- Amazon Security Lake 리소스에 대한 태그 편집
- Amazon Security Lake 리소스에서 태그 제거

태그 지정 기본 사항

리소스는 최대 50개의 태그를 가질 수 있습니다. 각 태그는 사용자가 정의하는 필수 태그 키와 선택적 태그 값으로 구성됩니다. 태그 키는 더 구체적인 태그 값에 대해 카테고리와 같은 역할을 하는 일반적인 레이블입니다. 태그 값은 태그 키에 대한 설명자 역할을 합니다.

예를 들어 여러 환경의 보안 데이터를 분석하기 위해 구독자를 추가하는 경우 (클라우드 데이터용 구독자 세트 하나와 온프레미스 데이터용 구독자 세트 하나) 해당 구독자에게 `Environment` 태그 키를 할당할 수 있습니다. 연결된 태그 값은의 데이터를 분석하는 `Cloud` 구독자 AWS 서비스및 다른 구독자의 태그 값일 `On-Premises` 수 있습니다.

Amazon Security Lake 리소스에 태그를 정의하고 할당할 때 다음 사항에 유의합니다.

- 각 리소스는 최대 50개의 태그를 보유할 수 있습니다.
- 각 리소스에 대해 각 태그 키는 고유하며 하나의 태그 값만 가질 수 있습니다.
- 태그 키와 값은 대소문자를 구분합니다. 모범적으로는 태그를 대문자로 사용하는 전략을 세우고 이러한 전략을 모든 리소스 유형에 대해 일관되게 구현하는 것이 좋습니다.

- 태그 키는 최대 128개의 UTF-8 문자를 포함할 수 있습니다. 태그 값은 최대 256개의 UTF-8 문자를 포함할 수 있습니다. 문자는 문자, 숫자, 공백 또는 _ . : / = + - @ 기호일 수 있습니다.
- `aws:` 접두사는에서 사용하도록 예약되어 있습니다 AWS. 정의한 태그 키나 값에는 이를 사용할 수 없습니다. 또는 이 접두사를 사용하는 태그 키 또는 값을 변경하거나 제거할 수 없습니다. 이 접두사를 사용하는 태그는 리소스당 50개의 할당량에 포함되지 않습니다.
- 할당하는 모든 태그는 에서만 사용할 수 AWS 계정 있으며 할당하는 AWS 리전 에서만 사용할 수 있습니다.
- Security Lake를 사용하여 리소스에 태그를 할당하는 경우 해당 태그는 해당 AWS 리전의 Security Lake에 직접 저장된 리소스에만 적용됩니다. Security Lake가 다른 AWS 서비스에서 생성, 사용 또는 유지 관리하는 관련 지원 리소스에는 적용되지 않습니다. 예를 들어 데이터 레이크에 태그를 할당하면 지정된 지역의 Security Lake에 있는 데이터 레이크 구성에만 태그가 적용됩니다. 로그 및 이벤트 데이터를 저장하는 Amazon Simple Storage Service(S3) 버킷에는 적용되지 않습니다. 또한 연결된 리소스에 태그를 할당하려면 리소스를 AWS 서비스 저장하는 AWS Resource Groups 또는를 사용할 수 있습니다. 예를 들어 SAmazon S3S3를 사용할 수 있습니다. 관련 리소스에 태그를 할당하면 데이터 레이크를 지원하는 리소스를 식별하는 데 도움이 될 수 있습니다.
- 리소스를 삭제하면, 리소스에 할당된 태그 또한 삭제됩니다.

추가 제한 사항, 팁 및 모범 사례는 AWS 리소스 태그 지정 사용 설명서의 리소스 태그 지정을 참조하세요. AWS

> **Important**
>
> 기밀 또는 기타 유형의 민감한 데이터를 태그에 저장하지 마세요. 를 AWS 서비스포함하여 많은에서 태그에 액세스할 수 있습니다 AWS 결제 및 비용 관리. 태그는 민감한 데이터에 사용하기 위한 것이 아닙니다.

Security Lake 리소스에 태그를 추가하고 관리하려면 Security Lake 콘솔 또는 Security Lake API를 사용할 수 있습니다.

IAM 정책에서 태그 사용

리소스에 태그를 지정한 후 AWS Identity and Access Management (IAM)정책에서 태그 기반의 리소스 수준 권한을 정의할 수 있습니다. 이러한 방식으로 태그를 사용하면에서 리소스를 생성하고 태그를 지정할 수 있는 권한이 AWS 계정 있는 사용자 및 역할과 태그를 더 일반적으로 추가, 편집 및 제거할 수

있는 권한이 있는 사용자 및 역할에 대한 세분화된 제어를 구현할 수 있습니다. 태그를 기반으로 액세스를 제어하려면 IAM 정책의 조건 요소에서 태그 관련 조건 키를 사용할 수 있습니다.

예를 들어, 사용자가 이름이 리소스의 `Owner` 태그 값인 모든 Amazon Security Lake 리소스에 대한 전체 액세스 권한을 갖도록 허용하는 정책을 생성할 수 있습니다.

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "ModifyResourceIfOwner",
            "Effect": "Allow",
            "Action": "securitylake:*",
            "Resource": "*",
            "Condition": {
                "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
            }
        }
    ]
}
```

태그 기반의 리소스 수준 권한을 정의하면 권한이 즉시 적용됩니다. 즉, 리소스를 생성하자마자 더 안전하게 보호할 수 있으며 새로운 리소스에 태그 사용 적용을 빠르게 시작할 수 있습니다. 리소스 수준 권한을 사용하여 새로운 및 기존 리소스와 연결할 수 있는 태그 키와 값을 제어할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 태그를 사용하여 AWS 리소스에 대한 액세스 제어를 참조하세요.

Amazon Security Lake 리소스에 태그 추가

Amazon Security Lake 리소스에 태그를 추가하려면 Security Lake 콘솔 또는 Security Lake API를 사용할 수 있습니다.

> **Important**
>
> 리소스에 태그를 추가하면 리소스에 대한 액세스에 영향을 줄 수 있습니다. 리소스에 태그를 추가하기 전에 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 AWS Identity and Access Management (IAM) 정책을 검토합니다.

Console

에 대해 Security Lake를 활성화 AWS 리전 하거나 구독자를 생성하면 Security Lake 콘솔은 리소스에 태그를 추가하는 옵션, 즉 리전 또는 구독자의 데이터 레이크 구성을 제공합니다. 리소스를 생성할 때 콘솔의 지침에 따라 리소스에 태그를 추가하십시오.

Security Lake 콘솔을 사용하여 기존 리소스에 하나 이상의 태그를 추가하려면 다음 단계를 따르세요.

리소스에 태그를 추가합니다.

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 태그를 추가하고 싶은 리소스 유형에 따라 다음 중 하나를 수행합니다.
   - 데이터 레이크 구성의 경우 탐색 창에서 리전을 선택합니다. 그런 다음 리전 테이블에서 리전을 선택합니다.
   - 구독자의 경우 탐색 창에서 구독자를 선택합니다. 그런 다음 내 구독자 테이블에서 구독자를 선택합니다.

     구독자가 표에 표시되지 않는 경우 페이지의 오른쪽 상단에 있는 AWS 리전 선택기를 사용하여 구독자를 생성한 리전을 선택합니다. 표에는 현재 리전의 기존 구독자만 나열됩니다.
3. 편집을 선택합니다.
4. 태그 섹션을 확장합니다. 이 섹션에는 현재 리소스에 할당된 태그가 모두 나열됩니다.
5. 태그 섹션에서 새로운 태그 추가를 선택합니다.
6. 키 상자에 리소스에 추가할 태그의 태그 키를 입력합니다. 그런 다음, 값 상자에 태그 값을 입력합니다(선택 사항).

   태그 키에는 최대 128자를 사용할 수 있습니다. 태그 값에는 최대 256자를 사용할 수 있습니다. 문자는 문자, 숫자, 공백 또는 _ . : / = + - @ 기호일 수 있습니다.
7. 리소스에 다른 태그를 추가하려면 새 태그 추가를 선택한 다음 이전 단계를 반복합니다. 리소스에 최대 50개의 태그를 할당할 수 있습니다.
8. 태그 추가가 완료되면 저장을 선택합니다.

API

리소스를 만들고 프로그래밍 방식으로 하나 이상의 태그를 추가하려면 만들려는 리소스 유형에 맞는 `Create` 작업을 사용하십시오.

- 데이터 레이크 구성 - CreateDataLake 작업을 사용하거나 AWS Command Line Interface (AWS CLI)를 사용하는 경우 create-data-lake 명령을 실행합니다.
- 구독자 - CreateSubscriber 작업을 사용하거나, AWS CLI를 사용하는 경우 create-subscriber 명령을 실행합니다.

요청에서 `tags` 파라미터를 사용하여 리소스에 추가할 각 태그의 태그 키(`key`)와 선택적 태그 값(`value`)을 지정합니다. `tags` 파라미터는 객체 배열을 지정합니다. 각 객체는 태그 키 및 연결된 태그 값을 지정합니다.

기존 리소스에 태그를 하나 이상 추가하려면 Security Lake API의 TagResource 작업을 사용하거나를 사용하는 경우 tag-resource 명령을 AWS CLI실행합니다. 요청에서 태그를 추가하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. `tags` 파라미터를 사용하여 추가할 각 태그의 태그 키(`key`)와 선택적 태그 값(`value`)을 지정합니다. `Create` 작업 및 명령의 경우와 마찬가지로 `tags` 파라미터는 개체의 배열, 각 태그 키당 하나의 개체 및 관련 태그 값을 지정합니다.

예를 들어 다음 AWS CLI 명령은 지정된 구독자에게 `Environment` 태그 값이 있는 `Cloud` 태그 키를 추가합니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud
```

위치:

- `resource-arn`은 태그를 추가할 구독자의 ARN을 지정합니다.
- *`Environment`*는 구독자에 추가할 태그의 태그 키입니다.
- *`Cloud`*는 지정된 태그 키(*`Environment`*)의 태그 값입니다.

다음 예제에서 명령은 구독자에 여러 태그를 추가합니다.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=Cloud key=CostCenter,value=12345 key=Owner,value=jane-
doe
```

tags 배열의 각 개체에는 key 및 value 인수가 모두 필요합니다. 그러나 value 인수 값은 빈 문자열일 수도 있습니다. 태그 값을 태그 키와 연결하지 않으려면 value 인수 값을 지정하지 마세요. 예를 들어 다음 명령은 연결된 태그 값이 없는 Owner 태그 키를 추가합니다.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

태깅 작업이 성공하면 Security Lake는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Lake는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

Amazon Security Lake 리소스에 대한 태그 편집

Amazon Security Lake 리소스의 태그 (태그 키 또는 태그 값)를 편집하려면 Security Lake 콘솔 또는 Security Lake API를 사용할 수 있습니다.

> **Important**
> 리소스의 태그를 편집하면 리소스 액세스에 영향을 미칠 수 있습니다. 리소스에 대한 태그 키 또는 값을 편집하기 전에 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 AWS Identity and Access Management (IAM) 정책을 검토합니다.

Console

Security Lake 콘솔을 사용하여 리소스의 태그를 편집하려면 다음 단계를 따르세요.

리소스에 대한 태그를 편집하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 태그를 편집할 리소스의 유형에 따라 다음 중 하나를 수행합니다.
   - 데이터 레이크 구성의 경우 탐색 창에서 리전을 선택합니다. 그런 다음 리전 테이블에서 리전을 선택합니다.
   - 구독자의 경우 탐색 창에서 구독자를 선택합니다. 그런 다음 내 구독자 테이블에서 구독자를 선택합니다.

구독자가 표에 표시되지 않는 경우 페이지의 오른쪽 상단에 있는 AWS 리전 선택기를 사용하여 구독자를 생성한 리전을 선택합니다. 표에는 현재 리전의 기존 구독자만 나열됩니다.

3. 편집을 선택합니다.
4. 태그 섹션을 확장합니다. 태그 섹션에는 현재 리소스에 할당된 모든 태그가 나열됩니다.
5. 다음을 수행합니다.

   - 기존 태그 키에 태그 값을 추가하려면 태그 키 옆의 값 상자에 값을 입력합니다.
   - 기존 태그 키를 변경하려면 태그 옆에 있는 제거를 선택합니다. 그런 다음 Add new tag(새 태그 추가)를 선택합니다. 표시되는 키 상자에 새 태그 키를 입력합니다. 값 상자에 연결된 태그 값을 입력합니다(선택 사항).
   - 기존 태그 값을 변경하려면 값이 포함된 값 상자에서 X를 선택합니다. 그런 다음, 값 상자에 새 태그 값을 입력합니다.
   - 기존 태그 값을 제거하려면 값이 포함된 값 상자에서 X를 선택합니다.
   - 기존 태그(태그 키 및 태그 값 모두)를 제거하려면 태그 옆의 제거를 선택합니다.

   리소스는 최대 50개의 태그를 가질 수 있습니다. 태그 키에는 최대 128자를 사용할 수 있습니다. 태그 값에는 최대 256자를 사용할 수 있습니다. 문자는 문자, 숫자, 공백 또는 _ . : / = + - @ 기호일 수 있습니다.
6. 태그 편집을 완료하면 저장을 선택합니다.

API

프로그래밍 방식으로 리소스의 태그를 편집하면 기존 태그를 새 값으로 덮어쓰게 됩니다. 따라서 태그를 편집하는 가장 좋은 방법은 태그 키를 편집할지, 태그 값을 편집할지 또는 둘 다를 편집할지에 따라 달라집니다. 태그 키를 편집하려면 현재 태그를 제거하고 새 태그를 추가합니다.

태그 키와 연결된 태그 값만 편집하거나 제거하려면 Security Lake API의 TagResource 작업을 사용하여 기존 값을 덮어씁니다. AWS Command Line Interface (AWS CLI)를 사용하는 경우 tag-resource 명령을 실행하십시오. 요청에서 태그 값을 편집 또는 제거하려는 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

태그 값을 편집하려면 `tags` 파라미터를 사용하여 태그 값을 변경하려는 태그 키를 지정합니다. 또한 키에 새 태그 값을 지정합니다. 예를 들어 다음 AWS CLI 명령은 지정된 구독자에게 할당된 태그 키`CloudOn-Premises`의 `Environment` 태그 값을에서 로 변경합니다. 이 예제는 Linux, macOS 또는 Unix용으로 포맷되었으며 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Environment,value=On-Premises
```

위치:

- `resource-arn`은 구독자의 ARN을 지정합니다.
- *`Environment`*는 변경할 태그 값과 연결된 태그 키입니다.
- *`On-Premises`*는 지정된 태그 키(*`Environment`*)에 사용할 새로운 태그 값입니다.

태그 키에서 태그 값을 제거하려면 `tags` 파라미터에 키 `value` 인수 값을 지정하지 마세요. 예시:

```
$ aws securitylake tag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tags key=Owner,value=
```

작업이 성공하면 Security Lake는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Lake는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

Amazon Security Lake 리소스에 대한 태그 검토

Security Lake 콘솔 또는 Security Lake API를 사용하여 Amazon Security Lake 리소스의 태그 (태그 키와 태그 값 모두)를 검토할 수 있습니다.

Console

다음 단계에 따라 Security Lake 콘솔을 사용하여 리소스 태그를 검토합니다.

리소스에 대한 태그를 검토하려면

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 태그를 검토하려는 리소스의 유형에 따라 다음 중 하나를 수행합니다.
   - 데이터 레이크 구성의 경우 탐색 창에서 리전을 선택합니다. 리전 테이블에서 리전을 선택한 다음 편집을 선택합니다. 태그 섹션을 확장합니다.

- 구독자의 경우 탐색 창에서 구독자를 선택합니다. 그런 다음 내 구독자 테이블에서 구독자 이름을 선택합니다.

  구독자가 표에 표시되지 않는 경우 페이지의 오른쪽 상단에 있는 AWS 리전 선택기를 사용하여 구독자를 생성한 리전을 선택합니다. 표에는 현재 리전의 기존 구독자만 나열됩니다.

태그 섹션에는 현재 리소스에 할당된 모든 태그가 나열됩니다.

API

프로그래밍 방식으로 기존 리소스의 태그를 검색하고 검토하려면 Security Lake API의 ListTagsForResource 작업을 사용하십시오. 요청에서 `resourceArn` 파라미터를 사용하여 리소스의 Amazon 리소스 이름(ARN)을 지정합니다.

AWS Command Line Interface (AWS CLI)를 사용하는 경우 list-tags-for-resource 명령을 실행하고 `resource-arn` 파라미터를 사용하여 리소스의 ARN을 지정합니다. 예시:

```
$ aws securitylake list-tags-for-resource --resource-arn arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab
```

앞의 예에서 *arn:aws:securitylake:us-east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab*는 기존 구독자의 ARN입니다.

작업이 성공하면 Security Lake 가 `tags` 배열을 반환합니다. 배열의 각 객체는 현재 리소스에 할당된 태그 (태그 키와 태그 값 모두)를 지정합니다. 예제:

```
{
    "tags": [
        {
            "key": "Environment",
            "value": "Cloud"
        },
        {
            "key": "CostCenter",
            "value": "12345"
        },
        {
            "key": "Owner",
            "value": ""
        }
```

```
    ]
}
```

여기서 `Environment`, `CostCenter`, `Owner`는 리소스에 할당된 태그 키입니다. `Cloud`는 `Environment` 태그 키에 연결된 태그 값입니다. `12345`는 `CostCenter` 태그 키에 연결된 태그 값입니다. `Owner` 태그 키에 연결된 태그 값이 없습니다.

Amazon Security Lake 리소스에서 태그 제거

Amazon Security Lake 리소스에서 태그를 제거하려면 Security Lake 콘솔 또는 Security Lake API를 사용할 수 있습니다.

> **Important**
> 리소스에서 태그를 제거하면 리소스에 대한 액세스에 영향을 줄 수 있습니다. 태그를 제거하기 전에 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있는 AWS Identity and Access Management (IAM) 정책을 검토합니다.

Console

Security Lake 콘솔을 사용하여 리소스에서 하나 이상의 태그를 삭제하려면 다음 단계를 따르세요.

리소스에서 태그를 제거합니다.

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 태그를 제거하고 싶은 리소스 유형에 따라 다음 중 하나를 수행합니다.
   - 데이터 레이크 구성의 경우 탐색 창에서 리전을 선택합니다. 그런 다음 리전 테이블에서 리전을 선택합니다.
   - 구독자의 경우 탐색 창에서 구독자를 선택합니다. 그런 다음 내 구독자 테이블에서 구독자를 선택합니다.

     구독자가 표에 표시되지 않는 경우 페이지의 오른쪽 상단에 있는 AWS 리전 선택기를 사용하여 구독자를 생성한 리전을 선택합니다. 표에는 현재 리전의 기존 구독자만 나열됩니다.
3. 편집을 선택합니다.
4. 태그 섹션을 확장합니다. 태그 섹션에는 현재 리소스에 할당된 모든 태그가 나열됩니다.
5. 다음을 수행합니다.

- 태그의 태그 값만 제거하려면 제거할 값이 포함된 값 상자에서 X를 선택합니다.
- 태그의 태그 키와 태그 값(한 쌍)을 모두 제거하려면 제거할 태그 옆의 제거를 선택합니다.

6. 리소스에서 추가 태그를 제거하려면 제거할 각 추가 태그에 대해 이전 단계를 반복합니다.
7. 태그 제거를 마쳤으면 저장을 선택합니다.

API

프로그래밍 방식으로 리소스에서 하나 이상의 태그를 삭제하려면 Security Lake API의 UntagResource 작업을 사용합니다. 요청에서 `resourceArn` 파라미터를 사용하여 태그를 제거할 리소스의 Amazon 리소스 이름(ARN)을 지정합니다. `tagKeys`파라미터를 사용하여 제거할 태그의 태그 키를 지정합니다. 여러 태그를 제거하려면 제거할 각 태그의 `tagKeys` 파라미터와 인수를 앰퍼샌드(&)로 구분하여 추가합니다—예제: `tagKeys=`*`key1`*`&tagKeys=`*`key2`*. 리소스에서 특정 태그 값(태그 키 제외)만 제거하려면 태그를 제거하는 대신 태그를 편집하세요.

AWS Command Line Interface (AWS CLI)를 사용하는 경우 untag-resource 명령을 실행하여 리소스에서 하나 이상의 태그를 제거합니다. `resource-arn` 파라미터에는 태그를 제거할 리소스의 ARN을 지정합니다. `tag-keys`파라미터를 사용하여 제거할 태그의 태그 키를 지정합니다. 예를 들어 다음 명령은 지정된 구독자에서 `Environment` 태그 (태그 키와 태그 값 모두)를 제거합니다.

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment
```

여기서 `resource-arn`은 태그를 제거할 구독자의 ARN을 지정하고, *`Environment`*는 제거할 태그의 태그 키입니다.

리소스에서 여러 태그를 제거하려면, 각 추가 키를 `tag-keys` 파라미터의 인수로 추가합니다. 예제:

```
$ aws securitylake untag-resource \
--resource-arn arn:aws:securitylake:us-
east-1:123456789012:subscriber/1234abcd-12ab-34cd-56ef-1234567890ab \
--tag-keys Environment Owner
```

작업이 성공하면 Security Lake는 빈 HTTP 200 응답을 반환합니다. 그렇지 않으면 Security Lake는 작업이 실패한 이유를 나타내는 HTTP 4xx 또는 500 응답을 반환합니다.

Security Lake 문제 해결

Amazon Security Lake 작업 시 문제가 발생하면 다음 문제 해결 리소스를 사용합니다.

다음 주제에서는 데이터 레이크 상태, Lake Formation, Amazon Athena에서의 쿼리 및 IAM과 관련하여 발생할 수 있는 오류 AWS Organizations 및 문제에 대한 문제 해결 조언을 제공합니다. 여기에 나열되지 않은 문제가 발견되면이 페이지의 `Feedback` 버튼을 사용하여 보고할 수 있습니다.

Security Lake 사용 시 문제가 발생하면 다음 주제를 참조하세요.

주제

- 데이터 레이크 상태 문제 해결
- Lake Formation 문제 해결
- Amazon Athena에서 쿼리 문제 해결
- Organizations 문제 해결
- Amazon Security Lake 자격 증명 및 액세스 문제 해결

데이터 레이크 상태 문제 해결

Security Lake 콘솔의 문제 페이지에는 데이터 레이크에 영향을 미치는 문제에 대한 요약이 표시됩니다. 예를 들어 조직에 대한 CloudTrail 추적을 생성하지 않은 경우 Security Lake는 AWS CloudTrail 관리 이벤트에 대한 로그 수집을 활성화할 수 없습니다. 문제 페이지에서는 지난 14일 동안 발생한 문제를 다룹니다. 각 문제에 대한 설명과 제안된 문제 해결 단계를 볼 수 있습니다.

프로그래밍 방식으로 문제 요약에 액세스하려면 Security Lake API의 ListDataLakeExceptions 작업을 사용할 수 있습니다. 를 사용하는 경우 list-data-lake-exceptions 명령을 AWS CLI실행합니다. `regions` 파라미터의 경우 미국 동부(버지니아 북부) 리전`us-east-1`과 같은 하나 이상의 리전 코드를 지정하여 해당 리전에 영향을 미치는 문제를 확인할 수 있습니다. `regions` 파라미터를 포함하지 않으면 모든 리전에 영향을 미치는 문제가 반환됩니다. 리전 코드 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오.

예를 들어 다음 AWS CLI 명령은 `us-east-1` 및 `eu-west-3` 리전에 영향을 미치는 문제를 나열합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake list-data-lake-exceptions \
```

```
--regions "us-east-1" "eu-west-3"
```

Security Lake 사용자에게 문제 또는 오류를 알리려면 Security Lake API의 CreateDataLakeExceptionSubscription 작업을 사용합니다. 사용자는 이메일, Amazon Simple Queue Service(Amazon SQS) 대기열로 전송, AWS Lambda 함수로 전송 또는 지원되는 다른 프로토콜을 통해 알림을 받을 수 있습니다.

예를 들어 다음 AWS CLI 명령은 SMS 전송을 통해 Security Lake 예외 알림을 지정된 계정으로 전송합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake create-data-lake-exception-subscription \
--notification-endpoint "123456789012" \
--exception-time-to-live 30 \
--subscription-protocol "sms"
```

예외 구독에 대한 세부 정보를 보려면 GetDataLakeExceptionSubscription 작업을 사용할 수 있습니다. 예외 구독을 업데이트하려면 UpdateDataLakeExceptionSubscription 작업을 사용할 수 있습니다. 예외 구독 및 중지 알림을 삭제하려면 DeleteDataLakeExceptionSubscription 작업을 사용할 수 있습니다.

Lake Formation 문제 해결

다음 정보를 사용하여 Security Lake 및 AWS Lake Formation 데이터베이스 또는 테이블 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다. Lake Formation 문제 해결 항목에 대한 자세한 내용은 AWS Lake Formation 개발자 안내서의 문제 해결 섹션을 참조하십시오.

테이블을 찾을 수 없음

구독자를 만들려고 할 때 이 오류가 발생할 수 있습니다.

이 오류를 해결하려면 해당 리전에 소스를 이미 추가했는지 확인하세요. Security Lake 서비스가 프리뷰 릴리즈일 때 소스를 추가한 경우 구독자를 생성하기 전에 소스를 다시 추가해야 합니다. 소스 추가에 대한 자세한 내용은 Security Lake의 소스 관리을 참조하십시오.

400 AccessDenied

사용자 지정 소스를 추가하고 `CreateCustomLogSource` API를 직접 호출할 때 이 오류가 발생할 수 있습니다.

오류를 해결하려면 Lake Formation 권한을 검토하십시오. API를 직접 호출하는 IAM 역할에는 Security Lake 데이터베이스에 대한 테이블 생성 권한이 있어야 합니다. 자세한 내용은 AWS Lake Formation 개발자 가이드에서 Lake Formation 콘솔 및 명명된 리소스 방법을 사용하여 데이터베이스 권한 부여 방법을 참조하세요.

SYNTAX_ERROR: 행 1:8: 열이 없는 관계에서는 선택*을 사용할 수 없습니다.

Lake Formation에서 처음으로 소스 테이블을 쿼리할 때 이 오류가 발생할 수 있습니다.

오류를 해결하려면에 로그인할 때 사용 중인 IAM 역할에 SELECT 권한을 부여합니다 AWS 계정. SELECT 권한을 부여하는 방법에 대한 지침은 AWS Lake Formation 개발자 안내서의 Lake Formation 콘솔 및 명명된 리소스 방법을 사용하여 테이블 권한 부여를 참조하십시오.

Security Lake가 발신자의 기본 ARN을 Lake Formation 데이터 레이크 관리자에 추가하지 못했습니다. 현재 데이터 레이크 관리자는 더 이상 존재하지 않는 잘못된 보안 주체를 포함할 수 있습니다.

Security Lake를 활성화하거나를 로그 소스 AWS 서비스 로 추가할 때이 오류가 발생할 수 있습니다.

에러를 해결하려면 다음 단계를 따릅니다.

1. Lake Formation 콘솔(https://console.aws.amazon.com/lakeformation/)을 엽니다.
2. 관리 사용자로 로그인
3. 탐색 창의 권한에서 관리자 역할 및 작업을 선택합니다.
4. 데이터 레이크 관리자 섹션에서 관리자 선택을 선택합니다.
5. IAM에서 찾을 수 없음이라는 레이블이 붙은 보안 주체를 지운 다음 저장을 선택합니다.
6. Security Lake 작업을 다시 시도해 보십시오.

Lake Formation을 사용한 Security Lake CreateSubscriber가 수락을 위한 새 RAM 리소스 공유 초대를 생성하지 않았습니다.

Security Lake에서 Lake Formation 구독자를 생성하기 전에 Lake Formation 버전 2 또는 버전 3 크로스 계정 데이터 공유를 통해 리소스를 공유한 경우 이 오류가 표시될 수 있습니다. 이는 Lake Formation 버전 2 및 버전 3 교차 계정 공유가 여러 교차 계정 권한 부여를 하나의 AWS RAM 리소스 공유로 매핑하여 AWS RAM 리소스 공유 수를 최적화하기 때문입니다.

리소스 공유 이름에 구독자를 생성할 때 지정한 외부 ID가 있고 리소스 공유 ARN이 `CreateSubscriber` 응답의 ARN과 일치하는지 확인하세요.

Amazon Athena에서 쿼리 문제 해결

다음 정보를 사용하여 Athena를 사용하여 Security Lake S3 버킷에 저장된 객체를 쿼리하기 위해 Athena를 사용할 때 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다. Athena 문제 해결 항목에 대한 자세한 내용은 Amazon Athena 사용 설명서의 Athena에서의 문제 해결 섹션을 참조하십시오.

쿼리해도 데이터 레이크의 새 객체가 반환되지 않습니다.

Athena 쿼리는 Security Lake의 S3 버킷에 해당 객체가 포함되어 있더라도 데이터 레이크의 새 객체를 반환하지 않을 수 있습니다. Security Lake를 비활성화했다가 다시 활성화한 경우 이 문제가 발생할 수 있습니다. 따라서 AWS Glue 파티션이 새 객체를 제대로 등록하지 못할 수 있습니다.

에러를 해결하려면 다음 단계를 따릅니다.

1. https://console.aws.amazon.com/lambda/ AWS Lambda 콘솔을 엽니다.
2. 탐색 표시줄의 리전 선택기에서 Security Lake가 활성화되었지만 Athena 쿼리가 결과를 반환하지 않는 리전을 선택합니다.
3. 탐색 창에서 함수를 선택하고 소스 버전에 따라 다음 목록에서 함수를 선택합니다.
   - `Source version 1 (OCSF 1.0.0-rc.2)` – SecurityLake_Glue_Partition_Updater_Lambda_***"region>*** 함수.
   - `Source version 2 (OCSF 1.1.0)` – AmazonSecurityLakeMetastoreManager_***"region>*** 함수.
4. 구성 탭에서 트리거를 선택합니다.
5. 함수 옆에 있는 옵션을 선택하고 편집을 선택합니다.
6. 트리거 활성화를 선택하고 저장을 선택합니다. 그러면 기능 상태가 활성화됨으로 바뀝니다.

AWS Glue 테이블에 액세스할 수 없음

쿼리 액세스 구독자는 Security Lake 데이터가 포함된 AWS Glue 테이블에 액세스하지 못할 수 있습니다.

먼저 계정 간 테이블 공유 설정 (구독자 단계)에 설명된 단계를 따르십시오.

구독자에게 여전히 액세스 권한이 없는 경우 다음 단계를 따르세요.

1. https://console.aws.amazon.com/glue/ AWS Glue 콘솔을 엽니다.
2. 탐색 창에서 데이터 카탈로그 및 카탈로그 설정을 선택합니다.
3. 구독자에게 리소스 기반 정책을 사용하여 AWS Glue 테이블에 액세스할 수 있는 권한을 부여합니다. 리소스 기반 정책에 대한 자세한 내용은AWS Glue 개발자 설명서의 AWS Glue에 대한 리소스 기반 정책 예시를 참조하세요.

Organizations 문제 해결

다음 정보를 사용하여 AWS Organizations및 Security Lake에서 발생할 수 있는 공통적인 문제를 진단하고 수정할 수 있습니다. Organizations 문제 해결 항목에 대한 자세한 내용은 AWS Organizations 사용 설명서의 문제 해결 섹션을 참조하십시오.

CreateDataLake 작업을 직접 호출하는 동안 액세스 거부 오류가 발생했습니다. 사용자 계정은 조직의 위임된 관리자 계정이거나 독립 실행형 계정이어야 합니다.

위임된 관리자 계정이 속한 조직을 삭제한 다음 Security Lake 콘솔 또는 CreateDataLake API를 사용하여 해당 계정을 사용하여 Security Lake를 설정하려고 하면 이 오류가 발생할 수 있습니다.

오류를 해결하려면 다른 조직의 위임된 관리자 계정이나 독립형 계정을 사용하십시오.

Amazon Security Lake 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Security Lake 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

Security Lake에서 작업을 수행할 권한이 없음

에서 작업을 수행할 권한이 없다고 AWS Management Console 알려주는 경우 관리자에게 문의하여 지원을 받아야 합니다. 관리자는 로그인 보안 인증 정보를 제공한 사람입니다.

다음 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`subscriber`*에 대한 세부 정보를 보려고 하지만 가상 `SecurityLake:`*`GetSubscriber`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 YOURSERVICEPREFIX:GetWidget on resource: my-example-widget
```

이 경우 Mateo는 `SecurityLake:GetSubscriber` 작업을 사용하여 `subscriber` 정보에 액세스하도록 허용하는 정책을 업데이트하라고 관리자에게 요청합니다.

관리형 정책 이상으로 권한을 확장하고 싶습니다.

구독자 또는 사용자 지정 로그 소스 APIs가 생성한 모든 IAM 역할은 `AmazonSecurityLakePermissionsBoundary` 관리형 정책의 적용을 받습니다. 관리형 정책 이상으로 권한을 확장하려면 역할의 권한 경계에서 관리형 정책을 제거할 수 있습니다. 그러나 dataLakes 및 구독자에 대한 Security Lake APIs를 변경하는 것과 상호 작용할 때는 IAM이 IAM 역할을 변경하기 위해 권한 경계를 연결해야 합니다.

iam:PassRole을 수행하도록 인증되지 않음

`iam:PassRole` 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Security Lake에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 `marymajor`라는 IAM 사용자가 콘솔을 사용하여 Security Lake에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 `iam:PassRole` 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 Security Lake 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Security Lake가 이러한 기능을 지원하는지 여부를 알아보려면 Security Lake와 IAM의 작동 방식을 참조하십시오.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유 AWS 계정 한 다른의 IAM 사용자에게 액세스 권한 제공을 참조하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Security Lake 요금 결정 방법

Amazon Security Lake 요금은 데이터 모으기와 데이터 변환이라는 두 가지 기준을 기반으로 합니다. 또한 Security Lake는 다른 AWS 서비스 와 협력하여 데이터를 저장하고 공유하므로 이러한 활동에 대해 별도의 요금이 부과될 수 있습니다.

Security Lake AWS 리전 에서 지원하는의 AWS 계정 에서 로그 컬렉션을 처음 켜면 해당 계정이 Security Lake의 15일 무료 평가판에 자동으로 등록됩니다. 무료 평가판 기간 동안에는 여전히 다른 서비스에서 요금이 부과될 수 있습니다.

Security Lake 요금의 방법론을 이해하려면 Amazon Security Lake 요금--> 비디오를 시청하세요.

데이터 모으기

이러한 비용은 수집된 AWS CloudTrail 로그 및 기타 AWS 서비스 로그와 이벤트(Amazon Route 53 해석기 쿼리 로그, AWS Security Hub 조사 결과 및 Amazon VPC 흐름 로그)의 볼륨에서 파생됩니다.

데이터 변환

이러한 비용은 Security Lake가 Security Lake의 Open Cybersecurity Schema Framework(OCSF) 스키마로 정규화하고 Apache Parquet 형식으로 변환하는 AWS 서비스 로그 및 이벤트의 볼륨에서 파생됩니다.

관련 서비스 비용

다음은 보안 데이터 레이크에 데이터를 저장하고 공유하기 AWS 서비스 위해 다른에서 발생할 수 있는 몇 가지 비용입니다.

- Amazon S3 — 이러한 비용은 Security Lake 계정에서 Amazon S3 버킷을 유지 관리하고, 여기에 데이터를 저장하고, 보안 및 액세스 제어를 위해 버킷을 평가 및 모니터링할 때 발생합니다. 자세한 내용은 Amazon S3 요금을 참조하십시오.
- Amazon SQS — 이러한 비용은 메시지 전송을 위한 Amazon SQS 대기열을 생성할 때 발생합니다. 자세한 내용은 Amazon SQS 요금을 참조하세요.
- Amazon EventBridge — 이러한 비용은 Amazon EventBridge가 구독 엔드포인트로 객체 알림을 전송할 때 발생합니다. 자세한 내용은 Amazon EventBridge 요금을 참조하세요.
- AWS Glue - 월별 비용은 기가바이트당 AWS 서비스에서 수집된 로그 및 이벤트 데이터의 양에 따라 결정됩니다. 데이터는 Amazon Simple Storage Service에 저장되며 표준 Amazon S3 요금이 적용됩니다. Security Lake는 사용자를 대신하여 다른 AWS 서비스도 오케스트레이션합니

다. 사용된 AWS 서비스와 보안 데이터 레이크의 일부로 설정된 리소스에 대해 별도의 요금이 부과됩니다. AWS Glue, Amazon EventBridge, AWS Lambda, Amazon SQS 및 Amazon Simple Notification Service에 대한 요금을 참조하세요. Security Lake에서 데이터를 쿼리하고 쿼리 결과를 저장하여 발생하는 비용은 사용자가 부담합니다.

구독자가 Security Lake에서 데이터를 쿼리하고 쿼리 결과를 저장하여 발생하는 비용은 구독자의 책임입니다.

비용 및 보조 서비스의 전체 목록은 Security Lake 요금을 참조하세요.

Security Lake 사용량 및 예상 비용 검토

Amazon Security Lake 콘솔의 사용량 페이지에서는 현재 Security Lake 사용량은 물론 향후 사용량 및 예상 비용을 검토할 수 있습니다. 현재 15일 무료 평가판에 참여 중인 경우 평가 기간 동안의 사용량을 통해 무료 평가판 종료 후 Security Lake를 사용하는 데 드는 비용을 추정할 수 있습니다. Security Lake 요금에 대한 개요는 Security Lake 요금 결정 방법을 참조하십시오. 자세한 정보 및 비용 예시는 Amazon Security Lake 요금을 참조하십시오.

Security Lake의 예상 사용 비용은 미국 달러로 보고되며 현재 AWS 리전에만 적용됩니다. 비용에는 조직의 모든 계정에서 Security Lake를 사용하는 비용이 포함되며, 여기에는 개방형 사이버 보안 스키마 프레임워크 (OCSF) 및 Apache Parquet 형식으로의 전환이 포함됩니다. 하지만 Amazon Simple Storage Service(S3) 및 AWS Glue와 같은 Security Lake와 함께 작동하는 다른 서비스에 대한 비용은 예측 비용에 포함되지 않습니다.

사용량 페이지에서 사용량 및 비용 데이터를 볼 기간을 선택합니다. 기본 기간은 지난 1일입니다. 예상 비용을 보려면 최소 1일 이상의 Security Lake를 사용해야 합니다.

페이지 상단에는 모든 계정의 예상 비용이 표시됩니다. 선택한 기간 동안의 실제 사용량을 기준으로 향후 30일 AWS 리전 동안 현재 Security Lake에서 예상한 비용입니다. 실제 사용량과 예상 비용에는 조직의 모든 계정이 반영됩니다.

페이지의 나머지 부분에서는 사용량 및 비용 데이터를 다음과 같이 두 개의 테이블로 나눕니다.

- 소스별 사용량 및 비용 - 데이터 소스별로 분류된 현재 Security Lake 사용량과 선택한 기간 동안의 실제 사용량을 기준으로 향후 30일 동안의 예상 사용량 및 비용입니다. 실제 사용량, 예상 사용량 및 예상 비용은 조직의 모든 계정을 반영합니다. 소스를 선택하면 해당 소스에서 로그와 이벤트를 생성한 계정을 보여주는 분할 패널이 열립니다. 각 계정의 분할 패널에는 해당 소스의 실제 사용량과 예상 사용량 및 비용이 모두 포함됩니다.

- 계정별 사용량 및 비용 — 계정별로 분류된 현재 Security Lake 사용량과 선택한 기간 동안의 실제 사용량을 기준으로 향후 30일 동안의 예상 사용량 및 비용을 나타냅니다. 계정을 선택하면 해당 계정 사용에 기여한 소스를 보여주는 분할 패널이 열립니다. 각 기여 소스에 대해 분할 패널에는 실제 사용량과 예상 사용량 및 비용이 모두 포함됩니다.

Security Lake에 특정 소스를 추가하지 않은 경우에도 지원되는 모든 AWS 데이터 소스가 이전 테이블에 표시됩니다. 무료 평가판에 참여하는 경우 모든 AWS 소스를 추가하여 전체 로그 및 이벤트 세트에 대한 비용 견적을 얻는 것이 좋습니다. AWS 소스 추가에 대한 지침은 섹션을 참조하세요Security Lake AWS 서비스 에서 데이터 수집. 사용자 지정 소스는 사용량 또는 비용 계산에 포함되지 않습니다.

다음 단계에 따라 Security Lake 콘솔에서 사용량 및 비용 데이터를 검토하십시오.

Security Lake 사용량 및 예상 비용을 검토하려면 (콘솔)

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 페이지 오른쪽 상단의 AWS 리전 선택기를 사용하여 사용량과 비용을 검토할 리전을 선택합니다.
3. 탐색 창에서 설정을 선택한 다음 사용량을 선택합니다.
4. 사용 및 비용 데이터를 보려는 기간을 선택합니다. 기본값은 지난 1일입니다.
5. 데이터 소스별 또는 계정별 탭을 선택하여 사용량과 비용을 자세히 검토할 수 있습니다.

Security Lake 리전 및 엔드포인트

Security Lake에 지원되는 리전 및 서비스 엔드포인트 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오.

모든 지원되는 AWS 리전의 Security Lake 기능을 활성화하는 것이 좋습니다. 이를 통해 Security Lake를 사용하여 적극적으로 사용하지 않는 리전에서도 무단 또는 비정상적인 활동을 탐지하고 조사할 수 있습니다.

Security Lake 비활성화

Amazon Security Lake를 비활성화하면 Security Lake는 AWS 소스에서 로그 및 이벤트 수집을 중단합니다. 기존 Security Lake 설정과 사용자 AWS 계정 내에서 생성된 리소스는 그대로 유지됩니다. 또한 AWS Lake Formation 테이블 및 AWS CloudTrail 로그의 민감한 데이터와 AWS 서비스같이에 저장하거나 다른에 게시한 데이터는 계속 사용할 수 있습니다. Amazon Simple Storage Service(S3) 버킷에 저장된 데이터는 Amazon S3 스토리지 수명 주기에 따라 계속 사용할 수 있습니다.

Security Lake 콘솔의 설정 페이지에서 Security Lake를 비활성화 AWS 리전 하면 Security Lake가 현재 활성화된 모든의 AWS 로그 및 이벤트 수집이 중지됩니다. 콘솔의 리전 페이지를 사용하여 특정 리전의 로그 수집을 중지할 수 있습니다. Security Lake API 및는 요청에 지정한 리전에서 로그 수집 AWS CLI 을 중지합니다.

AWS Organizations 와의 통합을 사용하고 계정이 여러 Security Lake 계정을 중앙에서 관리하는 조직의 일부인 경우 위임된 Security Lake 관리자만 자체 및 멤버 계정에 대해 Security Lake를 비활성화할 수 있습니다. 하지만 조직을 탈퇴하면 구성원 계정에 대한 로그 수집은 중지됩니다.

조직에 대해 Security Lake를 비활성화한 경우 이 페이지에 제공된 비활성화 지침을 따르면 위임된 관리자 지정이 유지됩니다. Security Lake를 다시 활성화하기 전에 위임된 관리자를 다시 지정할 필요는 없습니다.

사용자 지정 소스의 경우 Security Lake를 비활성화할 때 Security Lake 콘솔 외부의 각 소스를 비활성화해야 합니다. 통합을 비활성화하지 않으면 소스 통합이 Amazon S3로 로그를 계속 전송하게 됩니다. 또한 구독자 통합을 비활성화해야 합니다. 그러지 않으면 구독자가 Security Lake의 데이터를 계속 사용할 수 있습니다. 사용자 지정 소스 또는 구독자 통합을 제거하는 방법에 대한 자세한 내용은 해당 제공자의 설명서를 참조하세요.

> **Important**
>
> 쿼리가 제대로 작동하려면 Security Lake를 다시 활성화하기 전에 AWS Glue 데이터베이스를 삭제해야 합니다.

Security Lake를 다시 활성화하면 새 데이터 레이크 Amazon S3 버킷이 생성되고이 새 S3 버킷에서 데이터가 수집됩니다. 이전에 AWS Glue 테이블을 삭제한 경우 새 AWS Glue 테이블 세트가 생성됩니다.

Security Lake를 비활성화하기 전에 수집된 모든 데이터는 이전 Amazon S3 버킷에 유지됩니다. 이전 데이터를 쿼리하려면 Amazon S3 Sync 명령을 사용하여 새 버킷으로 이동해야 합니다. 자세한 내용은 명령 참조의 동기화 AWS CLI 명령을 참조하세요.

이 주제에서는 Security Lake 콘솔, Security Lake API 또는를 사용하여 Security Lake를 비활성화하는 방법을 설명합니다 AWS CLI.

Console

1. Security Lake 콘솔(https://console.aws.amazon.com/securitylake/)을 엽니다.
2. 탐색 창의 설정 아래에서 일반을 선택합니다.
3. Security Lake 비활성화를 선택합니다.
4. 확인 메시지가 나타나면 **`Disable`**을 입력한 다음 비활성화를 선택합니다.

API

프로그래밍 방식으로 Security Lake를 비활성화하려면 Security Lake API의 DeleteDataLake 작업을 사용합니다. 를 사용하는 경우 delete-date-lake 명령을 AWS CLI실행합니다. 요청에서 `regions` 목록을 사용하여 Security Lake를 비활성화하려는 각 리전의 리전 코드를 지정합니다. 리전 코드 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하십시오.

를 사용하는 Security Lake 배포의 경우 조직의 위임된 Security Lake 관리자 AWS Organizations만 조직의 계정에 대해 Security Lake를 비활성화할 수 있습니다.

예를 들어 다음 AWS CLI 명령은 `ap-northeast-1` 및 `eu-central-1` 리전에서 Security Lake를 비활성화합니다. 이 예제는 Linux, macOS 또는 Unix용으로 형식이 지정되며, 가독성을 높이기 위해 백슬래시(\) 줄 연속 문자를 사용합니다.

```
$ aws securitylake delete-data-lake \
--regions "ap-northeast-1" "eu-central-1"
```

Amazon Security Lake 사용 설명서에 대한 문서 기록

다음 표에서는 Amazon Security Lake의 최신 릴리스 이후 이 설명서에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

최종 설명서 업데이트: 2025년 4월 24일

변경 사항	설명	날짜
업데이트된 기능 - 서비스 연결 역할	이제 Security Lake는 데이터 레이크 생성 중에 AWSServiceRoleForSecurityLakeResourceManagement SLR을 자동으로 생성합니다. 자세한 내용은 고려 사항 단원을 참조하세요.	2025년 4월 24일
상당히 재작성된 주제 - AWS 통합	Security Lake와 특정의 통합을 지정하는 콘텐츠를 업데이트했습니다 AWS 서비스. 자세한 내용은 AWS 서비스 통합을 참조하세요.	2025년 3월 31일
업데이트된 기능 - 여러 계정 관리	Security Lake 콘솔은 이제 조직에 가입할 때 계정에 대한 자동 활성화 구성 관리를 지원합니다. 자세한 내용은 콘솔에서 새 계정 구성 편집을 참조하세요.	2025년 3월 10일
업데이트된 기능 - AWS WAF 로그의 데이터 보호	Security Lake 계정에 대한 웹 ACL에서 활성화된 경우 데이터 보호에 대한 지원이 추가되었습니다. 자세한 내용은 AWS WAF Security Lake의 로그를 참조하세요.	2025년 2월 17일
새로운 기능 - VPC 엔드포인트에 대한 지원 추가	Security Lake는 이제 AWS PrivateLink 와 통합되어 VPC	2025년 2월 4일

	엔드포인트를 지원합니다. AWS PrivateLink 통합에 대한 자세한 내용은 Amazon Security Lake 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)를 참조하세요.	
새로운 특성	Security Lake는 이제 Security Lake의 데이터를 분석하기 위한 OpenSearch Service 다이렉트 쿼리를 지원합니다. 자세한 내용은 OpenSearch Service와의 통합을 참조하세요.	2024년 12월 1일
새 서비스 연결 역할	새 서비스 연결 역할을 추가했습니다`AWSServiceRoleForSecurityLakeResourceManagement`. 이 서비스 연결 역할은 Security Lake에 지속적인 모니터링 및 성능 개선을 수행할 수 있는 권한을 제공하여 지연 시간과 비용을 줄일 수 있습니다.	2024년 11월 14일
리전별 가용성	이제 Security Lake를 AWS GovCloud(미국 동부) 및 AWS GovCloud(미국 서부)에서 사용할 수 있습니다 AWS 리전. 현재 Security Lake를 사용할 수 있는 리전의 전체 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하세요.	2024년 6월 10일

기존 관리형 정책 업데이트	`SecurityLakeServiceLinkedRole` 정책의 AWS 관리형 정책에 AWS WAF 작업을 추가했습니다. 추가 작업을 통해 Security Lake는 Security Lake에서 AWS WAF 로그 소스로 활성화된 로그를 수집할 수 있습니다.	2024년 5월 22일
새 AWS 로그 소스	Security Lake에서 AWS WAF 로그를 AWS 로그 소스로 추가했습니다. AWS WAF 를 사용하면 최종 사용자가 애플리케이션에 보내는 웹 요청을 모니터링할 수 있습니다.	2024년 5월 22일
기존 관리형 정책 업데이트	`AmazonSecurityLakePermissionsBoundary` 정책에 SID 작업을 추가했습니다.	2024년 5월 13일
기존 관리형 정책 업데이트	데이터 레이크에서 메타데이터를 삭제할 수 있는 메타데이터 정리 작업을 추가하도록 AmazonSecurityLakeMetastoreManager 정책을 업데이트했습니다.	2024년 3월 27일
새 소스 버전	역할 권한을 업데이트하여 새 데이터 소스 버전에서 데이터를 수집합니다.	2024년 2월 29일

새 AWS 로그 소스	Security Lake는 EKS 감사 로그를 AWS 로그 소스로 추가했습니다. EKS 감사 로그는 Amazon Elastic Kubernetes Service 내의 EKS 클러스터에서 잠재적으로 의심스러운 활동을 탐지하는 데 도움이 됩니다.	2024년 2월 29일
기존 관리형 정책 업데이트	새 `AmazonSecurityLakeMetastoreManagerV2` 역할에 `iam:PassRole` 대해를 허용하고 Security Lake가 데이터 레이크 구성 요소를 배포하거나 업데이트하도록 정책을 업데이트했습니다.	2024년 2월 23일
새 관리형 정책	새 AWS 관리형 정책인 `AmazonSecurityLakeMetastoreManager` 정책을 추가했습니다. 이 정책은 Security Lake가 데이터 레이크의 메타데이터를 관리할 수 있는 권한을 부여합니다.	2024년 1월 23일
리전별 가용성	이제 AWS 리전아시아 태평양(오사카), 캐나다(중부), 유럽(파리) 및 유럽(스톡홀름)에서 Security Lake를 사용할 수 있습니다. 현재 Security Lake를 사용할 수 있는 리전의 전체 목록은 AWS 일반 참조의 Amazon Security Lake 엔드포인트를 참조하세요.	2023년 10월 26일

새로운 기능	이제 쿼리 액세스 권한이 있는 구독자의 특정 설정을 편집할 수 있습니다. 자신의 AWS 계정에 Security Lake 리소스에 태그를 할당할 수도 있습니다.	2023년 7월 20일
새 관리형 정책	Security Lake는 새로운 AWS 관리형 정책인 `AmazonSecurityLakeAdministrator` 정책을 추가했습니다. 이 정책은 모든 Security Lake 작업에 대한 전체 액세스를 허용하는 관리 권한을 부여합니다.	2023년 5월 30일
정식 출시	Security Lake가 일반 공개되었습니다.	2023년 5월 30일
새로운 특성	Security Lake는 이제 Amazon CloudWatch에 지표를 전송합니다.	2023년 5월 4일
리전별 가용성	이제 AWS 리전아시아 태평양(싱가포르), 유럽(런던) 및 남아메리카(상파울루)에서 Security Lake를 사용할 수 있습니다.	2023년 3월 22일
새로운 특성	이제 Security Lake 콘솔을 사용하여 Security Lake 사용을 활성화하고 시작할 때 Security Lake가 사용자를 대신하여 AWS Identity and Access Management (IAM) 역할을 생성합니다.	2023년 2월 15일
최초 릴리스	Amazon Security Lake 사용 설명서의 최초 릴리스입니다.	2022년 11월 29일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.