AWS 安全事件响应 用户指南

版本 April 29, 2026

AWS 安全事件响应 用户指南:

Table of Contents

什么是 AWS 安全事件响应？

AWS 安全事件响应可帮助您快速做好安全准备、及时响应事件，并获取恢复指导，从而有效应对安全事件。这些安全事件包括账户劫持、数据泄露和勒索软件攻击。

AWS 安全事件响应 会对威胁调查发现进行分级，升级安全事件，并管理需要您立即关注的案例。此外，您还可获得安全事件响应工程师的支持，由其负责调查受影响的资源。

> **Note**
>
> 无法保证受影响资源一定能被恢复。建议为可能影响业务需求的资源建立并维护备份。

AWS 安全事件响应与其他 AWS 检测和响应服务协同工作，指导您完成从检测到恢复的整个事件生命周期。

内容

支持的配置

AWS 安全事件响应支持以下语言及区域配置：

- 语言：AWS 安全事件响应提供专业的英语支持。日语支持仅在日本标准时间的工作时间内提供，且存在限制：
-
  > **Note**
  >
  > 日语支持仅限于日本标准时间工作日（周一至周五 09:00-17:00；节假日除外）
- 支持的 AWS 区域：

  AWS 安全事件响应在部分 AWS 区域 区域提供服务。在这些支持的区域中，您可以创建会员资格、创建和查看案例以及访问控制面板。
  - 美国东部（俄亥俄州）
  - 美国西部（俄勒冈州）
  - 美国东部（弗吉尼亚）

- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（米兰）
- 欧洲地区（巴黎）
- 欧洲（西班牙）
- 欧洲地区（斯德哥尔摩）
- 欧洲（苏黎世）
- 亚太地区（香港）
- 亚太地区（海得拉巴）
- 亚太地区（雅加达）
- 亚太地区（墨尔本）
- 亚太地区（孟买）
- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 加拿大（中部）
- 中东（巴林）
- 中东（阿联酋）：
- 南美洲（圣保罗）
- 非洲（开普敦）

在启用监控与调查功能时，AWS 安全事件响应会监控所有活跃的商业 AWS 区域中 Amazon GuardDuty 的调查发现。作为安全最佳实践，AWS 建议在所有支持的 AWS 区域启用 GuardDuty。即使在未主动部署资源的AWS 区域，该配置也能让 GuardDuty 生成关于未经授权或异常活动的调查发现。如此，您可以全面提升安全防护水平，在整个 AWS 环境中保持完整的威胁检测覆盖范围。

> **Note**
>
> Amazon GuardDuty 会报告已配置区域的调查发现。如果选择不在特定区域启用该服务，则无法获取相关警报。

功能概述

监控与调查

AWS 安全事件响应会快速检查来自 Amazon GuardDuty 及与 AWS Security Hub CSPM 集成的第三方的安全威胁警报，有效减少您团队需要分析的工作量。该服务会根据您的环境配置隐藏规则，降低需要分级和调查的威胁警报数量。

简化事件响应

在数分钟内协同相关人员、第三方服务及工具，规模化执行事件响应流程。

自助式安全解决方案

AWS 安全事件响应提供 API 接口，支持您集成并构建定制化的安全解决方案。

可视化控制面板

监控和评估事件响应准备状态。

安全防护水平

获取 AWS 最佳实践和经过验证的安全评估工具，实现快速事件响应调查。

快速协助服务

联系安全事件响应工程师以调查、遏制安全事件，以及获取有关安全事件恢复方式的指导。

准备与就绪状态管理

通过配置事件响应团队实现高效通知机制：根据预设权限策略，自动向指定人员或群组发送警报通知。

概念和术语

掌握以下术语和概念对了解 AWS 安全事件响应服务及其工作原理来说很重要。

范围：AWS 安全事件响应符合美国国家标准与技术研究院（NIST）800-61《计算机安全事件处理指南》，提供了与行业最佳实践相关的统一安全事件管理方法。

分析：对安全事件进行详细调查和检查，了解安全事件的范围、影响和根本原因。

AWS 安全事件响应服务门户：自助服务门户，供您启动和管理安全事件案例。通过工单系统、自动通知以及与服务团队的直接接洽，实现持续的沟通和报告。

沟通：在事件响应过程中，AWS 安全事件响应团队与客户之间正在进行的对话和信息共享。

遏制、根除和恢复：防止其他未经授权的活动（遏制）、删除未经授权的资源和原始漏洞（消除）、恢复资源，从而恢复正常业务运营。

持续改进：AWS 安全事件响应会整合从先前接洽中吸取的反馈和经验教训，增强自身检测能力、调查流程和补救措施。AWS 安全事件响应还会随时了解最新的安全威胁和最佳实践，从而应对不断变化的安全挑战。

网络安全事件：利用信息系统或网络对系统、网络或其中包含的信息产生不利影响的行为。

网络安全事故：违反计算机安全政策、可接受使用政策或标准安全惯例的行为，或即将发生此类违规的威胁。

安全事件响应工程师：在活跃安全事件期间提供支持的一组人员。对于由 AWS 支持的案例，请联系安全事件响应工程师。

事件响应工作流程：遵循 NIST 800-61 标准，用于端到端管理安全事故所涉及的明确定义的步骤和活动序列。

调查工具：用于审查账户和资源运营状况的 AWS 安全事件响应工具和与服务相关角色。

经验教训：对安全事故响应的评审和记录，以识别改进领域并为未来的事故响应规划提供依据。

监控和调查：AWS 安全事件响应会快速审查来自 Amazon GuardDuty 的安全警报，将您团队需要分析的最重要的警报放在最前面。它会根据您环境的具体情况配置抑制规则，防止出现不必要的警报。

准备工作：为使组织做好有效响应和管理安全事件而开展的活动，例如制定事件响应计划和测试程序。

报告和沟通：用于在整个事件响应过程中让您随时了解情况的流程，包括自动通知、呼叫桥接和调查产物的交付。AWS 安全事件响应在 AWS 管理控制台中提供了一个集中的控制面板，用于管理您的所有 AWS 安全事件响应工作。

响应者生成的情报：妥协指标；战术、技术和程序；以及 AWS 调查观察到的相关模式。

安全事件专业知识：在 AWS 云环境中有效响应和管理安全事件所需的专业知识和技能。

责任共担模式：AWS 与客户之间的安全责任划分，其中 AWS 负责云的安全性，客户负责云中的安全性。

威胁情报：包含未经授权活动详细信息的内部和外部数据源，可帮助识别和响应不断变化的安全威胁。

工单系统：专门的案例管理平台，您可以在其中注册和管理安全事件案例、添加附件以及跟踪事件响应生命周期。

分类：对安全事件进行初步评估和优先排序，以确定适当的响应和后续步骤。

工作流程：用于端到端管理安全事件所涉及的已定义步骤和活动序列。

开始使用

AWS 安全事件响应 入门

内容

信息载入指南

AWS 安全事件响应 可帮助您做好准备、应对安全事件和从安全事件恢复，例如账户盗用、数据泄露和勒索软件攻击。该服务会对来自 Amazon GuardDuty 和 AWS Security Hub CSPM 的调查发现进行分级处理，升级安全事件，并管理需要您关注的案例。您还可以联系 AWS 安全事件响应团队（SIRT），其负责调查受影响的资源并在整个事件生命周期内提供指导。

有关该服务的完整概述，请参阅 什么是 AWS 安全事件响应？

为入门做好准备

我们建议在实施 AWS 安全事件响应 时使用概念验证（POC）方法。部署之前，请与您的内部团队和 AWS 客户团队一起完成下面的准备步骤。

- 确定关键利益相关者：确定贵组织的事件响应决策者。他们参与策略更新和流程变更对于成功推出至关重要。
- 验证调查发现来源：确认所有安全调查发现来源均已正确配置和部署。GuardDuty 和 Security Hub CSPM 是该服务的自动分级技术的关键输入。
- 确定账户范围：决定 AWS 安全事件响应 将覆盖整个 AWS 组织还是特定的组织单元（OU）。尽早定义此范围可以使实施和扩展变得更加简单。
- 制定升级协议：更新现有升级程序以包括 AWS 安全事件响应。将更新后的协议传达给所有利益相关者和响应人员。

- 收集联系人和关键信息：尽早收集客户元数据可确保顺畅的入门体验，并在需要时从 AWS SIRT 及时进行外联。有关所需信息，请参阅 附录 A：联系人和关键信息。

载入先决条件

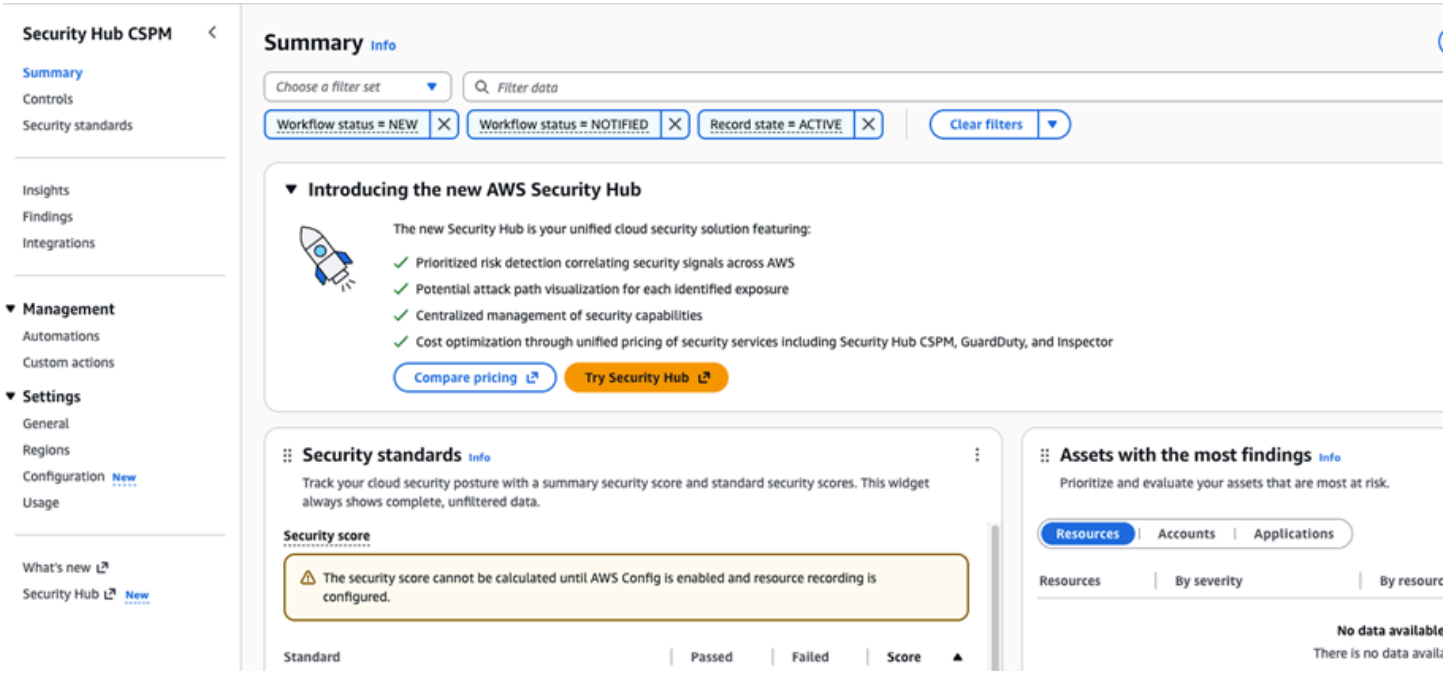
唯一必需的先决条件是启用 AWS Organizations 并启用所有功能。仅整合账单并不足够。

虽然不是必需的，但我们强烈建议在所有账户和活动的 AWS 区域启用 Amazon GuardDuty 和 AWS Security Hub CSPM，以从 AWS 安全事件响应 获得最大价值。

- GuardDuty 和 AWS 安全事件响应
- GuardDuty 最佳实践

第三方 EDR 集成

Security Hub CSPM 可以摄取来自第三方端点检测和响应（EDR）供应商的调查发现。摄取后，这些调查发现将由 AWS 安全事件响应 自动分级，以便主动创建案例。要设置第三方 EDR 集成，请按照 Security Hub CSPM 集成文档中的步骤进行操作。



> **Note**
>
> 无需启用 Security Hub CSPM 标准或控件。只需要供应商集成，AWS 安全事件响应 即可摄取第三方调查发现。

定价：前 1 万个 Security Hub CSPM 调查发现是免费的。之后，每个调查发现的成本为 0.00003 美元。有关更多信息，请参阅 Security Hub CSPM 定价。

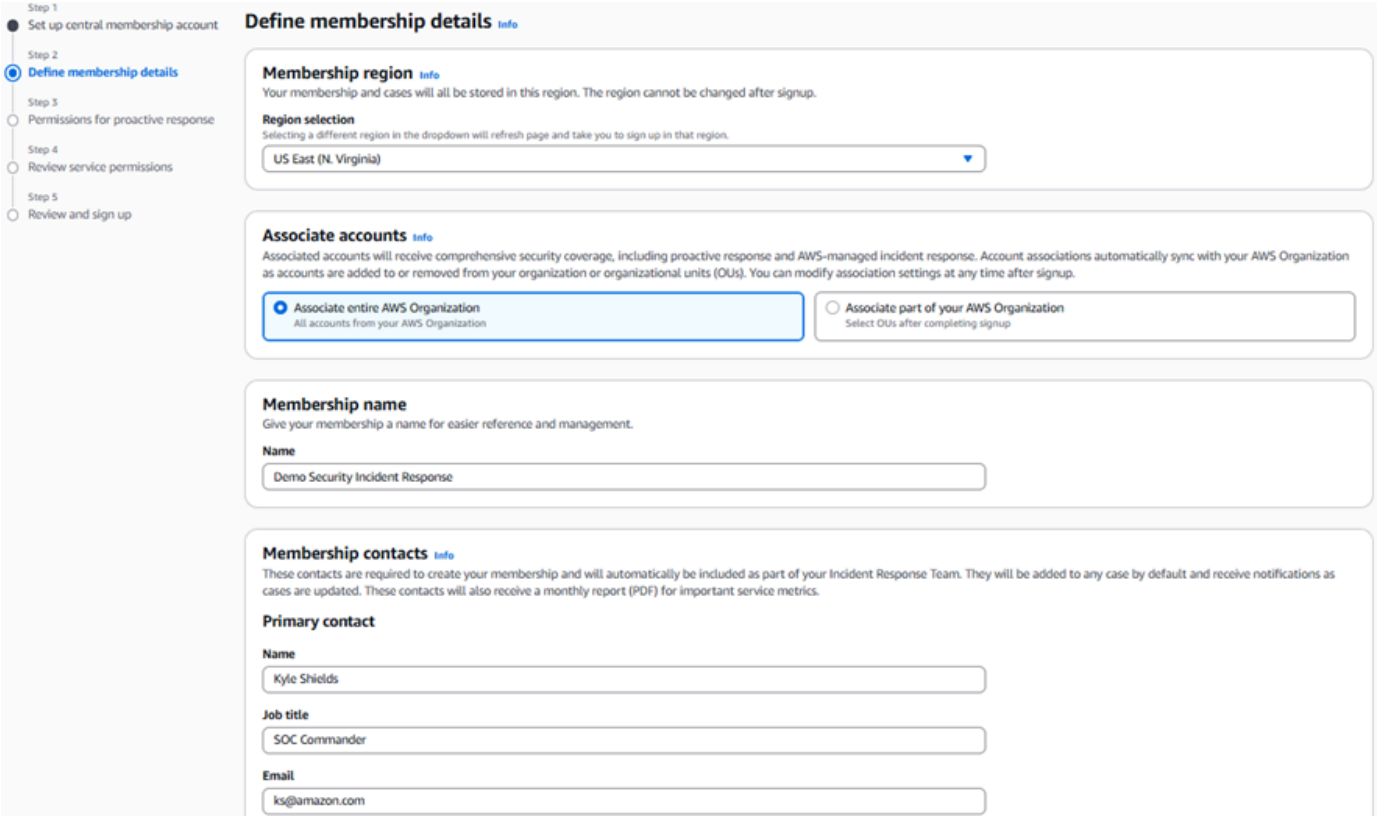
步骤 1：启用 AWS 安全事件响应

每个 AWS 组织的入门流程大约需要 10 到 15 分钟。有关演练，请参阅服务文档中的入门视频。

启用 AWS 安全事件响应

1. 使用管理账户登录到 AWS 管理控制台。
2. 打开 AWS 安全事件响应 控制台，然后选择注册。

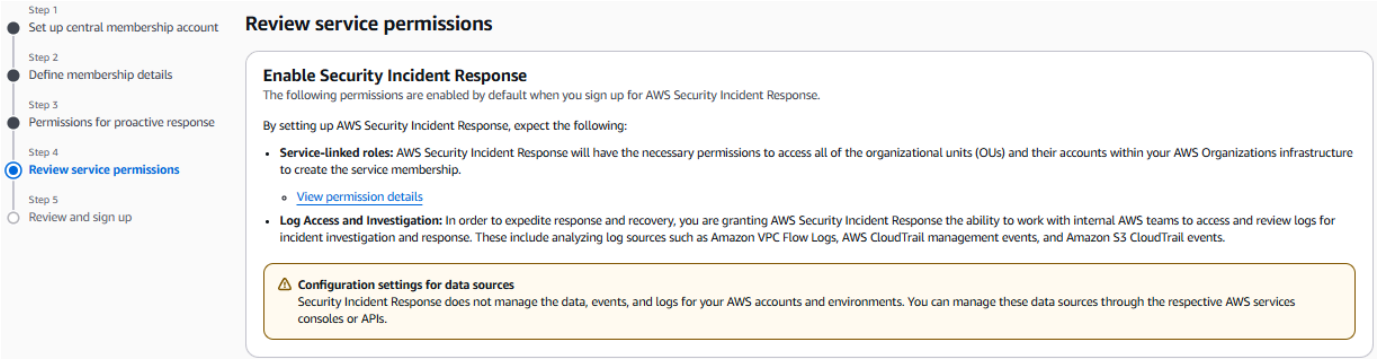
3. 指定安全工具账户作为委派管理员。
   - 有关指导，请参阅《AWS 规范性指导》中的安全参考架构和委派管理员。

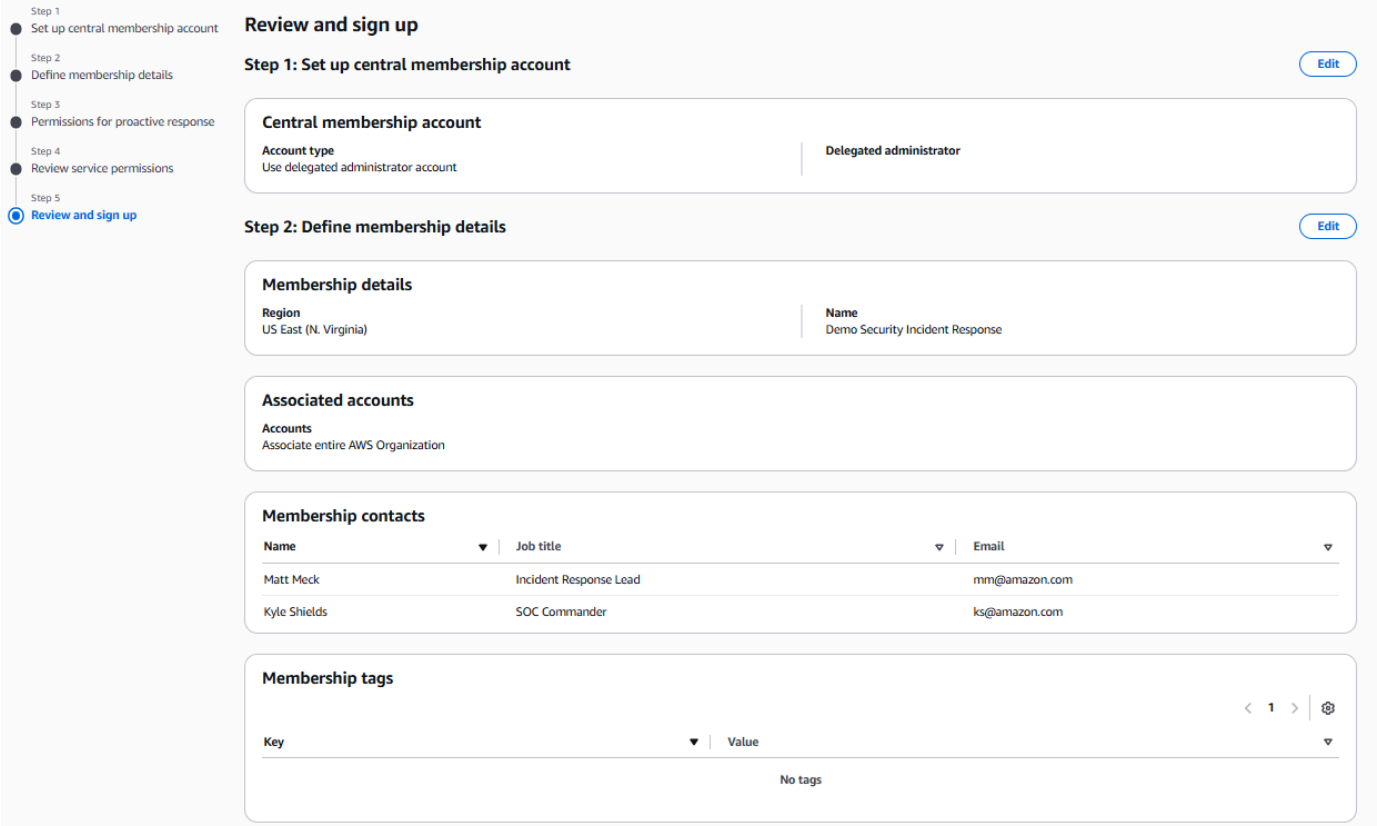


4. 登录委托管理员账户。
5. 输入会员资格详细信息并关联相关账户。
6. 对于账户范围，选择为整个 AWS 组织还是特定 OU 启用 AWS 安全事件响应。您可以在 OU 级别选择覆盖，但不能在个人账户级别选择覆盖。
7. 对于主动响应，确认该设置已启用。默认情况下，主动响应处于开启状态并创建了一个服务相关角色，允许 AWS SIRT 摄取 GuardTuty 调查发现，并在检测到威胁时创建主动调查案例。有关更多信息，请参阅主动响应。

> **Important**
>
> 服务相关角色不会自动部署到管理账户。您必须手动配置它才能实现全面覆盖。有关说明，请参阅设置主动响应和警报分级工作流程。

8. （可选）选择预授权 AWS SIRT，以在活动事件期间代表您执行遏制操作。支持的遏制操作包括遭盗用的 S3 存储桶、EC2 实例和 IAM 主体的运行手册。如果跳过此步骤，SIRT 将在调查期间提供手动指导。有关更多信息，请参阅遏制操作。
9. 查看服务权限和入门配置，然后选择注册。



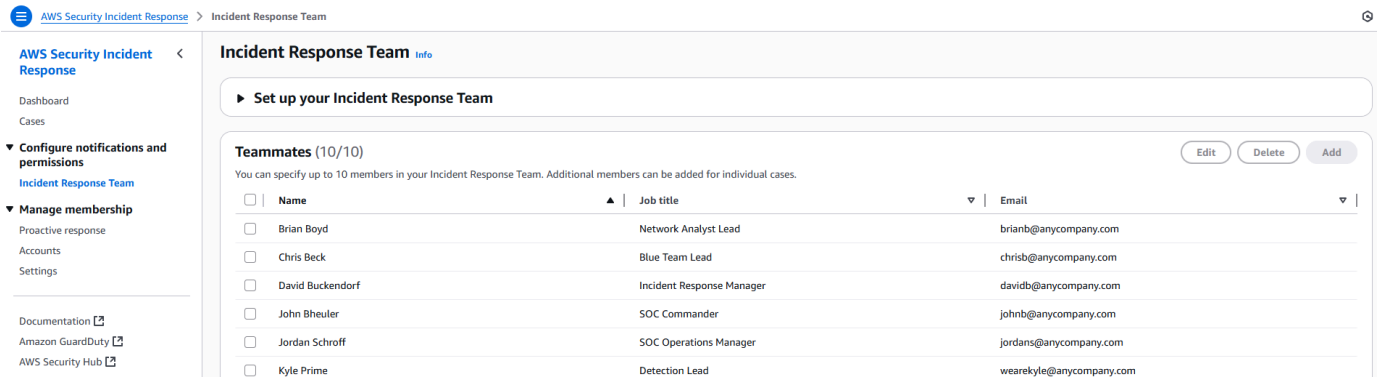


步骤 2：配置事件响应团队

完成部署后，请配置事件响应团队，以确保在安全事件期间进行适当的通知和上报。

配置事件响应团队

1. 打开 AWS 安全事件响应 控制台。
2. 在左侧导航窗格中，选择事件响应团队。
3. 最多可添加 10 名团队成员。针对每个成员提供其姓名、职务和电子邮件地址。



团队可以包括组织领导层、法律顾问、托管检测和响应（MDR）合作伙伴、云工程师以及在安全事件期间需要通知的其他利益相关者。

步骤 3：了解案例类型和管理

AWS 安全事件响应提供两种类型的案例来管理安全事件：检测到威胁时自动创建的主动案例，以及需要 AWS SIRT 帮助时创建的被动案例。您还可以向合作伙伴、法律团队或主题专家等外部各方公开案例信息。

本节将讨论以下主题：

- 主动案例
- 被动案例
- 观察程序

主动案例

自动分级功能会持续审查大量警报，以过滤掉噪音并专注于严重的高影响威胁。检测到潜在威胁后，系统会将调查发现上报给 AWS SIRT 响应人员进行调查。如果确认调查发现是真正的威胁，则会在案例管理门户中创建主动案例，并自动通知所有已配置的利益相关者。

除了启用 GuardDuty 和将第三方安全解决方案与 Security Hub CSPM 集成之外，主动案例不需要手动配置。该服务还与人工智能调查代理集成，其会关联来自多个来源的数据以加快调查速度。此功能当前可用于 AWS 支持的被动案例。

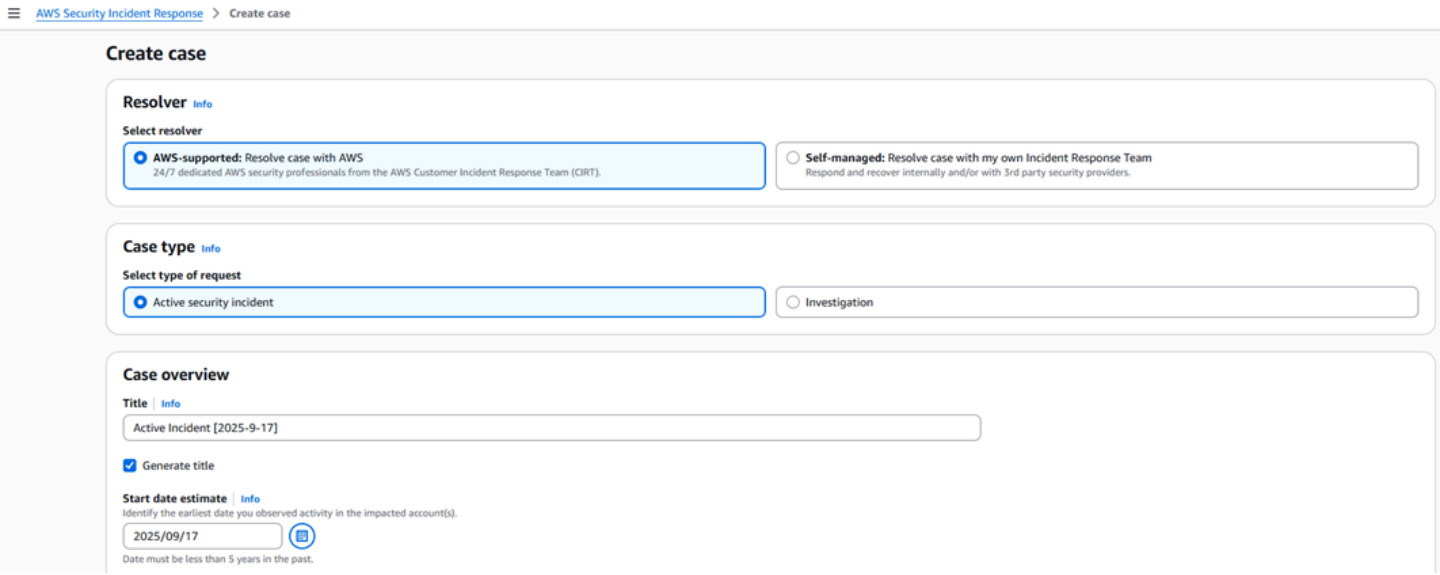
被动案例

AWS 安全事件响应 提供了一个基于订阅的案例管理门户，组织可以在其中直接与 AWS SIRT 合作。AWSSIRT 以 15 分钟服务级别目标（SLO）协助处理安全调查和活动事件。可创建的被动案例数量没有限制。

创建案例

1. 打开 AWS 安全事件响应 控制台。
2. 选择案例，然后选择创建案例。
3. 选择案例类型：
   - AWS 支持：直接上报给 AWS SIRT 进行调查和获取指导（15 分钟 SLO）。
   - 自我管理：保留在组织内部，用于跟踪和记录。
4. 填写所有相关字段。请尽可能提供详细信息，以便进行高效调查。

两种案例类型使用相同的数据字段。您可以通过选择案例右上角的从 AWS 获取帮助来随时将自我管理的案例上报给 AWS SIRT。



有关详细说明，请参阅创建案例。

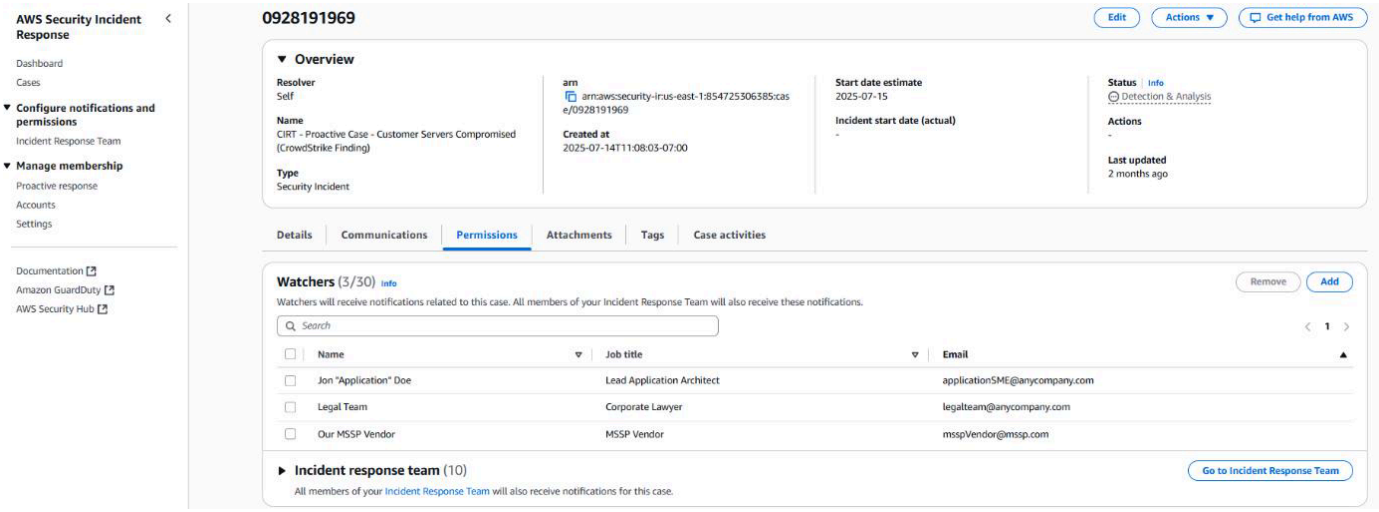
观察程序

您可以使用观察程序或 IAM 策略向外部各方公开案例信息。这些选项允许在调查中包括合作伙伴、风险和合规团队、法律顾问或主题专家。观察程序会接收特定案例的所有更新的通知。IAM 策略提供具有最低权限的直接控制台访问。

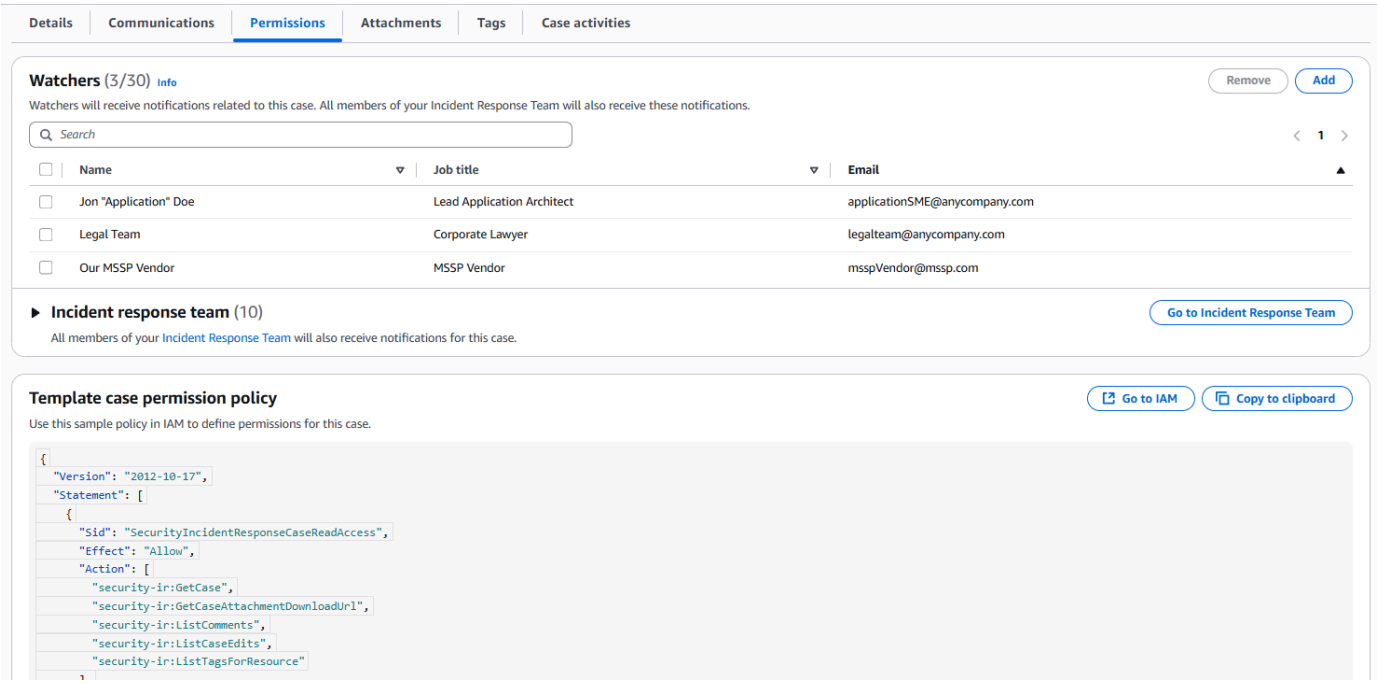
向案例添加观察程序

1. 打开 AWS 安全事件响应 控制台，然后选择案例。
2. 打开要共享的案例。

3. 选择权限选项卡，然后选择添加。



4. 复制预填充的 IAM 策略，并将其应用于合适的 IAM 角色或用户。



> **Note**
>
> 每个案例都包含预填充的、针对该特定案例的 IAM 策略。这样可以确保第三方 MDR 合作伙伴和调查团队获得最低权限访问权限。

步骤 4：与现有工具集成

AWS 安全事件响应与您现有的安全工具和工作流集成，以简化事件响应操作。您可以配置来自 GuardDuty 的自动调查发现摄取，使用 EventBridge 设置事件驱动的工作流，连接到 Jira 和 ServiceNow 等 ITSM 平台，以及与 SIEM 和 MDR 提供商协作。

本节将讨论以下主题：

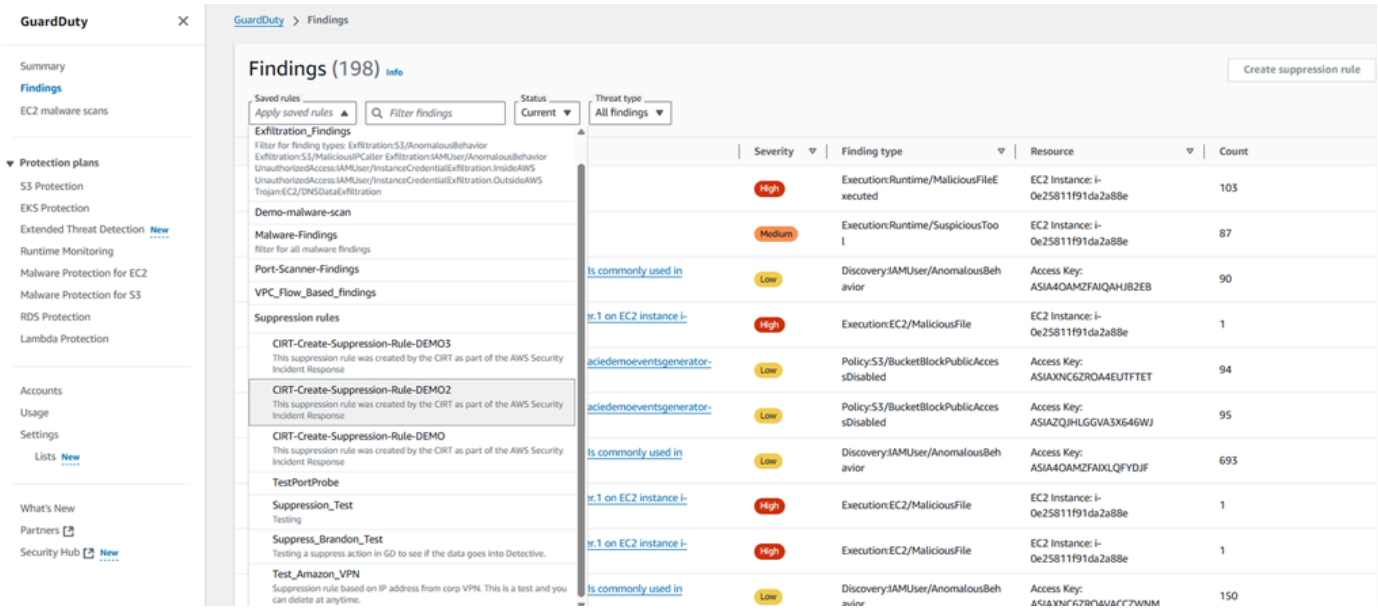
- GuardDuty 调查发现和隐藏规则
- Amazon EventBridge
- Jira、Slack 和 ServiceNow 集成
- SIEM 和外部工具

GuardDuty 调查发现和隐藏规则

AWS 安全事件响应 自动摄取、分级和响应来自第三方集成的 GuardDuty 调查发现和 Security Hub CSPM 调查发现。自动分级技术将分析作为检测和分析的附加层进行处理。该服务可以在上报误报调查发现后在 GuardDuty 中创建自动存档规则。响应人员将在实施该规则之前始终与您讨论此事。

查看 GuardDuty 抑制规则

1. 打开 GuardDuty 控制台。



2. 选择调查发现。
3. 在导航窗格中，选择抑制规则。抑制规则页面会显示您账户的所有抑制规则的列表。
4. 要查看或更改规则的设置，请选择该规则，然后从操作菜单中选择更新抑制规则。

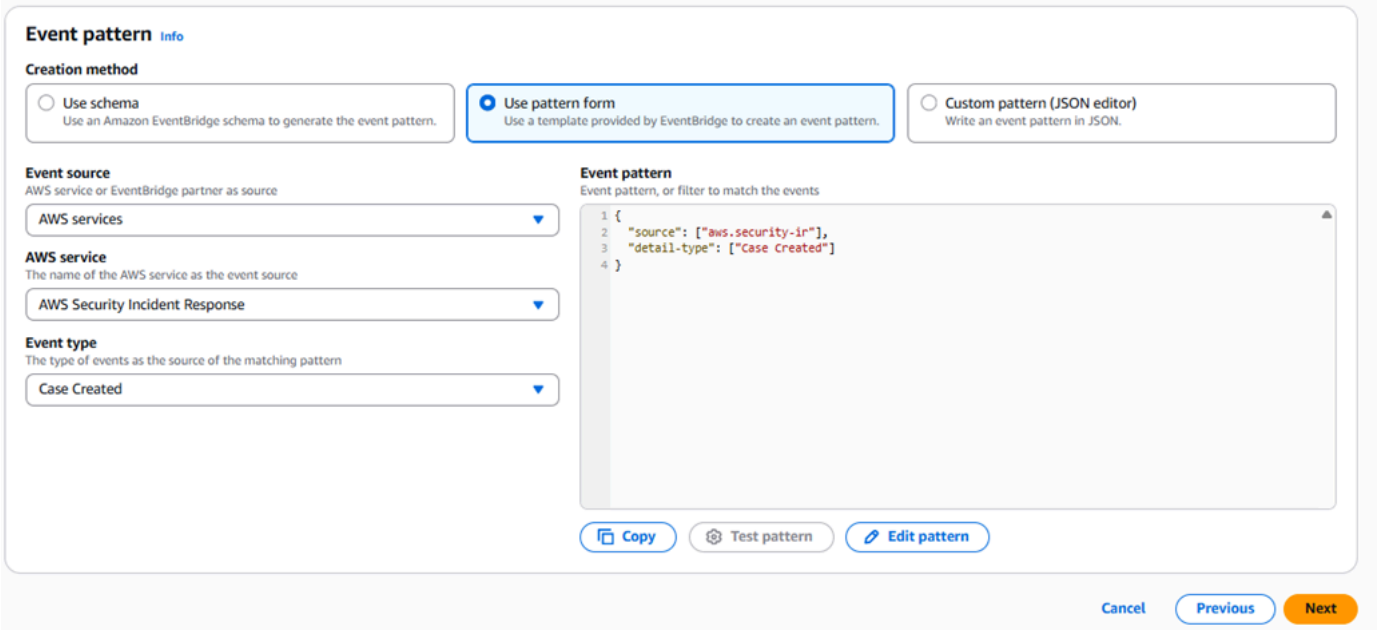
> **Note**
>
> 使用 SIEM 技术的组织会发现，随着时间推移，GuardDuty 调查发现量减少，AWS 安全事件响应 和 SIEM 性能都有所提升。

Amazon EventBridge

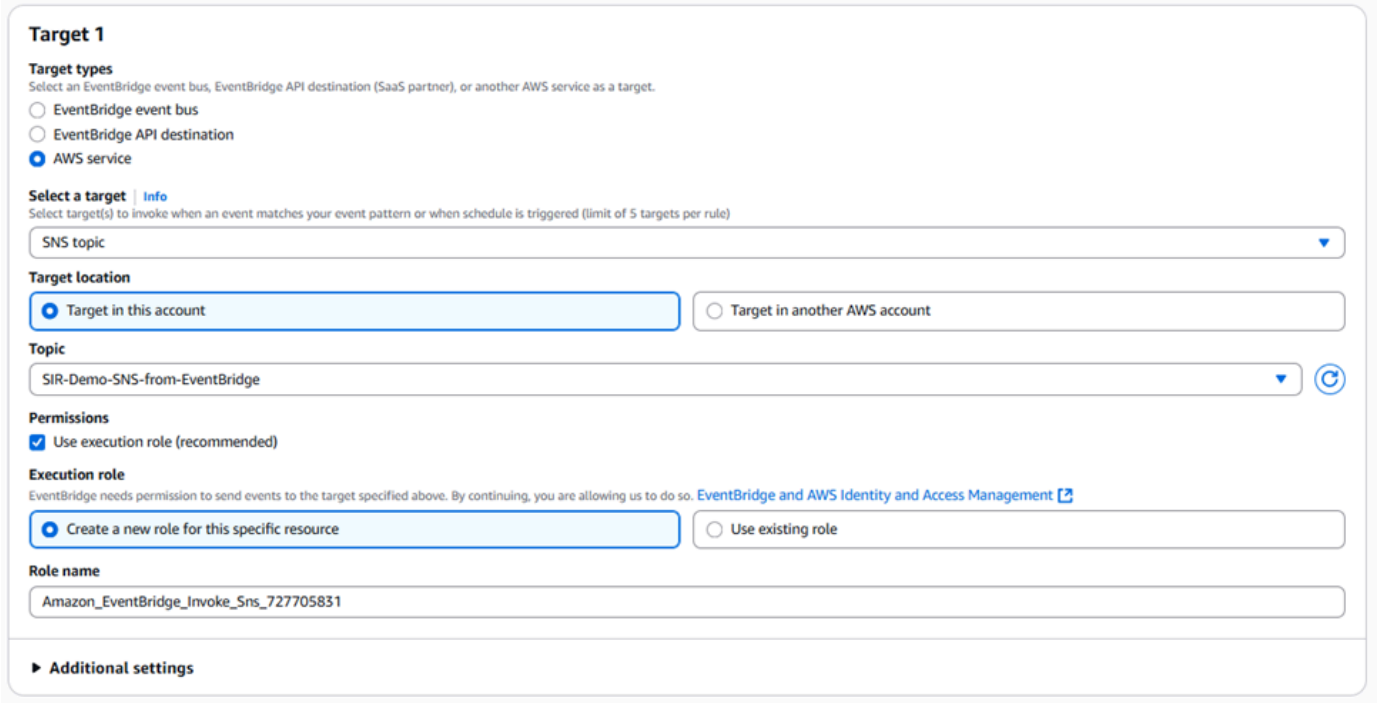
Amazon EventBridge 为 AWS 安全事件响应 启用事件驱动的工作流。您可以将案例活动配置为触发下游 AWS 服务（Amazon Simple Notification Service、AWS Lambda、Amazon Simple Queue Service、AWS Step Functions）或外部工具（例如 Jira、ServiceNow、Slack 和 PagerDuty）。

为 AWS 安全事件响应 配置 EventBridge 规则

1. 登录AWS 安全事件响应的委派管理员账户。
2. 打开 EventBridge 控制台。
3. 在导航窗格中的总线下，选择规则。
4. 选择创建规则，填写规则详细信息，然后选择下一步。
5. 在 AWS 服务下，从下拉列表中选择 AWS 安全事件响应。
6. 对于事件类型，选择要匹配的事件或 API 调用。您可以手动编辑模式以包含多个事件。
7. 选择下一步。

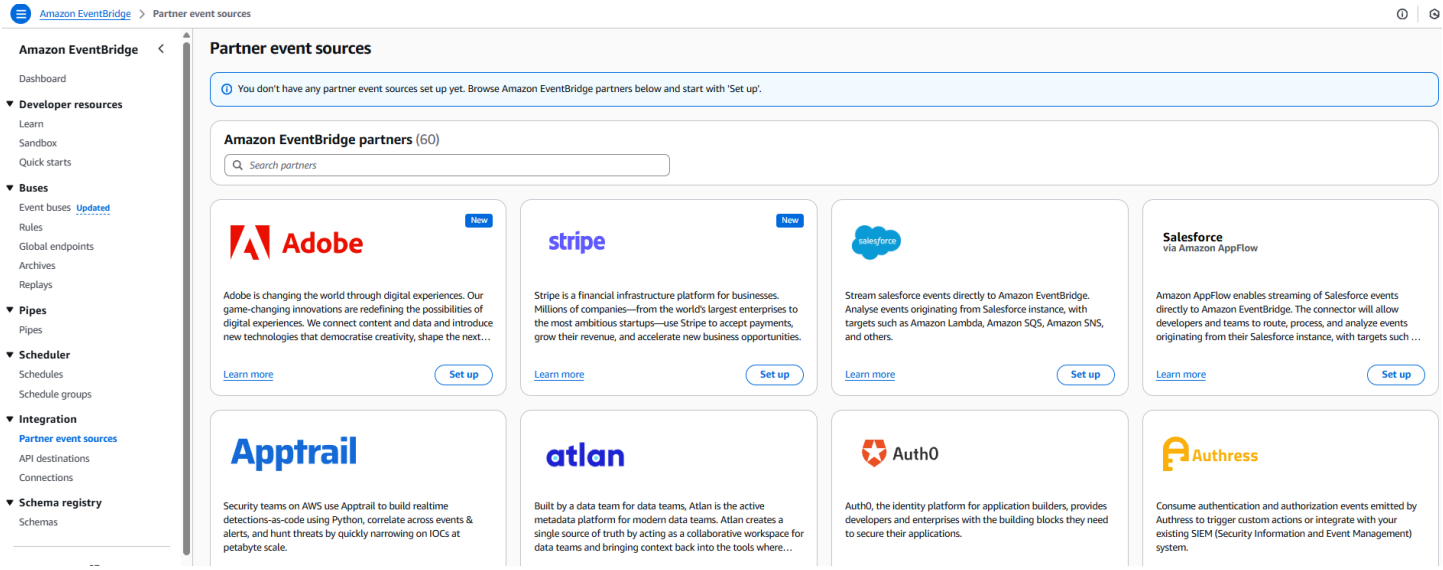


8. 为您的事件选择一个或多个目标，例如 Amazon SNS、AWS Lambda、SSM 文档或 Step Functions。如有需要，请配置跨账户目标。



9. 查看并创建规则。

要使用预构建的合作伙伴集成，请在 EventBridge 控制台中勾选合作伙伴事件来源。可用的合作伙伴包括 Atlassian（Jira）、Datadog、New Relic、PagerDuty、Symantec 和 Zendesk。



Jira、Slack 和 ServiceNow 集成

AWS 提供完全开发的解决方案，实现与 Jira、Slack 和 ServiceNow 的双向集成。这些集成使 AWS 安全事件响应 案例与 ITSM 或 ChatOps 平台保持同步，一个系统中的更新会自动反映在另一个系统中。

集成的优势

将 AWS 安全事件响应与现有 ITSM 平台集成，可通过集中处理事件跟踪和响应工作流来简化安全运营。借助这些预先构建的解决方案，您的安全团队无需自定义开发，即可跨 AWS 原生事件管理系统以及整个企业的事件管理系统随时掌握各种安全事件。利用 EventBridge 实现事件驱动的自动化功能，可在不同的平台之间无缝掌握动态，有助确保无论安全事件来自何处，都能持续进行跟踪。通过这种统一的方法，可减少安全分析师切换上下文的操作，缩短响应时间，并在整个事件响应生命周期中提供全面的审计跟踪记录。

有关部署说明，请参阅 AWS sample solutions for Jira, Slack, and ServiceNow。

SIEM 和外部工具

AWS 安全事件响应不会直接从 SIEM 摄取调查发现。但是，当您创建 AWS 支持的案例时，AWS SIRT 响应人员会与您的团队并行分析和调查 SIEM 调查发现。SIRT 有助于跨混合云和多云环境识别关联，并协助跨提供商确定威胁行为者活动的范围。

AWS SIRT 还直接与 MDR 提供商和第三方调查团队合作，帮助在事件发生之前制定有效的协调流程。

附录 A：联系人和关键信息

部署之前，请填写下表并将其提供给您的 AWS 客户团队。此信息使 AWS SIRT 能够在安全事件期间快速联系到合适的人员。

IR 和 SOC 人员联系方式

条目	IR | SOC 人员：职务、姓名、电子邮件	主要/备用上报联系人	内部已知 CIDR 范围	外部已知 CIDR 范围	其他云服务提供商	有效的 AWS 区域	DNS 服务器 IP（如果不是 Amaz Route 53 Resol	VPN | 远程访问解决方案和 IP	关键应用程序名称 | 账号	常用的非常用端口	EDR | AV | 使用的漏洞管理工具	IDP | 位置
1	SOC 负责人，Joh Smith，j ith@exa le.com	主	10.0.0 16	5.5.60 20（A	Azure	us-east-1、us-east-2	不适用	Direct Connect 公有 VIF 116.32.8 7	Nginx Web 服务器（示例关键服务器）| 1234567 0	8080	CrowdSt ke Falcon	Entra、Azu re

要提交此信息，请完成下面的步骤：

1. 使用您的环境信息填写前面的元数据表。
2. 创建包含以下详细信息的 AWS 支持 案例：
   - 案例类型：技术
   - 服务：安全事件响应
   - 类别：其他
3. 将填好的元数据表附加到案例中。

RACI 矩阵

以下 RACI 矩阵定义了整个安全事件响应实施过程中的角色和责任。RACI 代表执行（Responsible，R）、负责（Accountable，A）、咨询（Consulted，C）和知情（Informed，I）。

活动	Customer	AWS 客户团队	SIR 团队
信息载入前			
确定关键利益相关者	R		我
核实调查发现来源	R	C	我
[第三方 EDR 集成] Security Hub CSPM	R	C	我
GuardDuty 验证/运行状况检查	C	R	我
确定账户范围	R		
制定升级方案	R	我	C
启用 AWS Organizations	R	C	
将账户与 AWS Organizations 关联	R	我	
选择委托管理员/安全工具账户	R	我	
信息载入			
设置会员资格详细信息	R	我	
演练（设置主动响应和警报分级工作流；将服务相关角色部署到管理账户；授权遏制措施）	R	C	我
部署后配置			
检查运营集成能力	R	C	我
提交安全事件响应被动案例	R		

活动	Customer	AWS 客户团队	SIR 团队
配置 Amazon EventBridge 集成	R	C	C
连接第三方工具（Jira、ServiceNow、PagerDuty、Teams 等）	R	我	C
服务深入分析和演示	A	R	C

RACI 定义：

- 执行（R）：执行工作以完成任务的一方
- 负责（A）：对任务的正确完成最终负责的一方
- 咨询（C）：向其征求意见的一方，沟通方向为双向
- 知情（I）：向其通报事件进展的一方，沟通方向为单向

选择一个会员账户

会员账户是用于配置账户详细信息、为事件响应团队添加和删除详细信息，以及可以在其中创建和管理所有活动和历史安全事件的 AWS 账户。建议将 AWS 安全事件响应成员账户与您为 Amazon GuardDuty 和 AWS Security Hub CSPM 等服务启用的账户保持一致。

可通过两种方式来使用 AWS Organizations 选择 AWS 安全事件响应成员账户。您可以在组织管理账户或组织委托管理员账户中创建会员资格。

使用委托管理员账户：AWS 安全事件响应管理任务和案例管理在委托管理员账户中执行。建议使用您为其他 AWS 安全与合规服务设置的相同委派管理员。提供 12 位数的委托管理员账户 ID，然后登录该账户继续操作。

> **Important**
>
> 如果在设置过程中使用委托管理员账户，AWS 安全事件响应无法在您的 AWS Organizations 管理账户中自动创建所需的分类服务相关角色。请完成下面的步骤以在您的 AWS Organizations 管理账户中手动创建此角色。
>
> 创建服务相关角色（控制台）
>
> 1. 登录您的 AWS Organizations 管理账户。

2. 使用您偏好的方法访问 AWS CloudShell 控制台或通过 AWS Command Line Interface 访问账户。
3. 使用 `aws iam create-service-linked-role --aws-service-name "triage.security-ir.amazonaws.com" --no-cli-pager` CLI 命令。
4. （可选）要验证命令是否有效，请运行命令 `aws iam get-role --role-name AWSServiceRoleForSecurityIncidentResponse_Triage`。

使用当前登录的账户：选择此账户意味着当前账户将被指定为您 AWS 安全事件响应会员资格的中央会员账户。贵组织内的个人需要通过此账户访问该服务，才能创建、访问和管理处于活动状态的案例和已解决的案例。

确保您有权管理 AWS 安全事件响应。

有关添加权限的具体步骤，请参阅添加和删除 IAM 身份权限。

请参阅 AWS 安全事件响应托管策略。

要验证 IAM 权限，您可以按照以下步骤操作：

- 查看 IAM 策略：审查附加到用户、群组或角色的 IAM 策略，确保此策略授予了必要的权限。为此，您可以导航到 https://console.aws.amazon.com/iam/，选择 `Users` 选项，选择特定用户，然后转到他们摘要页面上的 `Permissions` 选项卡，查看所有附加策略列表；您可以展开每个策略行查看其详细信息。
- 测试权限：尝试执行验证权限所需的操作。例如，如果您需要访问案例，请尝试 `ListCases`。如果您没有必要的权限，则会收到错误消息。
- 使用 AWS CLI 或 SDK：您可以使用首选编程语言的 AWS Command Line Interface 或 AWS SDK 来测试权限。例如，使用 AWS Command Line Interface，您可以运行 `aws sts get-caller-identity` 命令来验证您当前用户的权限。
- 查看 AWS CloudTrail 日志：审查 CloudTrail 日志，查看是否记录了您尝试执行的操作。这可以帮助您识别任何权限问题。
- 使用 IAM 策略模拟器：IAM 策略模拟器工具，可以让您测试 IAM 策略并查看它们对您权限的影响。

> **Note**
>
> 具体步骤可能会有所不同，具体取决于 AWS 服务和您尝试执行的操作。

设置会员资格详细信息

- 选择存储了会员资格和案例的 AWS 区域。

> **Warning**
>
> 在初始会员资格注册后，就无法更改默认 AWS 区域。

- 选择您是想您的成员关系覆盖整个 AWS Organizations，还是通过组织单元（OU）覆盖 AWS Organizations 的一部分。
- 您可以选择为此成员提供一个名称。
- 在成员创建工作流中，必须提供一个主要联系人和一个辅助联系人。这些联系人会自动加入您的事件响应团队。单个会员资格必须至少有两个联系人，这可确保事件响应团队中至少有两个联系人。
- 为您的会员资格定义可选标签。标签可帮助您跟踪 AWS 成本和搜索资源。

将账户与 AWS Organizations 关联

如果您在设置期间选择关联整个 AWS Organizations，则您的成员关系会覆盖组织中的所有成员账户。在组织中添加或删除账户时，关联的账户将自动更新。

如果您在设置期间选择关联 AWS Organizations 的一部分，并且将成员关系限制为特定的组织单元（OU），则您的成员关系会覆盖所选 OU 下的所有账户。这包括所选 OU 的子 OU 下的账户。在这些 OU 中添加或移除账户时，关联的账户将自动更新。

要详细了解涉及组织单元的最佳实践，请参阅 Organizing Your AWS environment Using multiple accounts。

设置主动响应和警报分级工作流程

AWS 安全事件响应会监控和调查由 Amazon GuardDuty 和 Security Hub CSPM 集成生成的威胁警报。要使用此功能，必须启用 Amazon GuardDuty。AWS 安全事件响应会通过服务自动化对低优先级警报进行分类，以便您的团队可以专注于最关键的问题。有关如何将 AWS 安全事件响应与 Amazon GuardDuty、AWS Security Hub CSPM 结合使用的更多信息，请查看用户指南检测和分析章节。

如果您遇到信息载入问题，请创建 AWS 支持 案例以获得更多帮助。请务必提供详细信息，包括 AWS 账户 ID 和您在设置过程中看到的任何错误。

> **Note**
>
> 如果您对 Amazon GuardDuty 抑制规则、警报分级配置或主动响应工作流有疑问，可以使用调查与咨询案例类型创建 AWS 支持的案例，从而咨询AWS 安全事件响应团队。有关更多信息，请参阅 创建 AWS 托管案例。

此功能可让 AWS 安全事件响应 监控和调查组织中所有范围内账户以及处于活动状态且受支持的 AWS 区域的调查发现。为便于使用此功能，AWS 安全事件响应 会自动在您 AWS Organizations 内的所有覆盖的成员账户中创建服务相关角色。但是，对于管理账户，您必须手动创建服务相关角色才能启用监控。

AWS 安全事件响应无法在管理账户中创建服务相关角色。您必须在管理账户中手动创建此角色。有关更多信息，请参阅选择一个会员账户中的重要说明。

了解主动响应的自动存档行为

启用主动响应和警报分级后，AWS 安全事件响应 会自动监控来自 Amazon GuardDuty 和 Security Hub CSPM 的安全调查发现并进行分级。作为这一自动分级工作流的一部分，系统会根据以下标准将调查发现自动存档：

自动存档行为：

- 无害调查发现：当自动分级过程确定某项调查发现是无害的（不是真正的安全威胁）时，AWS 安全事件响应会自动在 Amazon GuardDuty 中将该调查发现存档，并创建隐藏规则来防止类似的调查发现在未来生成警报。
- 隐藏规则：服务会针对符合您环境中已知无害模式（例如符合预期的 IP 地址、IAM 实体和正常运行行为）的调查发现，在 Amazon GuardDuty 和 Security Hub CSPM 中创建隐藏和自动存档规则。
- 减少警报量：随着时间推移，服务会了解您的环境并自动存档无害的调查发现，因此使用 SIEM 技术的组织所看到的 Amazon GuardDuty 调查发现数量将会显著减少。这有助 AWS 安全事件响应 服务和您的 SIEM 提高效率。

查看已存档调查发现：

您可以查看自动存档的调查发现以及由 AWS 安全事件响应创建的抑制规则：

1. 导航到 Amazon GuardDuty 控制台
2. 选择调查发现

3. 选择调查发现筛选条件中的已存档
4. 选择每条规则旁边的向下箭头，查看隐藏规则

重要注意事项：

- 已存档调查发现将在 Amazon GuardDuty 中保留 90 天，您可以在此期间随时查看
- 您可以随时通过 Amazon GuardDuty 控制台修改或删除隐藏规则
- 自动分级流程会不断适应您的环境，随着时间推移逐渐提高准确性和减少误报

遏制：发生安全事件时，AWS 安全事件响应可以执行遏制措施，快速缓解影响，例如隔离受影响的主机或轮换凭证。安全事件响应默认不会启用遏制功能。要执行这些遏制操作，您必须先授予此服务必要的权限。这可以通过部署 AWS CloudFormation StackSet 来完成，该堆栈集会创建所需的角色。

用户任务

内容

安全事件响应控制面板

在 AWS 安全事件响应控制台中，控制面板会提供事件响应团队、主动响应状态以及为期四周的滚动案例数量等内容的概览。

事件响应团队

选择查看事件响应团队，以获取事件响应团队成员的详细信息。

我的案例

控制面板中我的案例板块会显示在指定时间段内已开启和已关闭的 AWS 托管案例数量，以及分配给您的自主管理案例数量。此外，该板块还会以小时为单位显示已关闭案例的平均解决时长。

管理我的事件响应团队

您的事件响应团队包含参与事件响应流程的相关人员。您最多可以配置十名相关人员作为团队成员。

内部相关人员示例：事件响应团队成员、安全分析师、应用程序负责人、安全领导团队。

外部相关人员示例：希望纳入事件响应流程的独立软件供应商（ISV）、托管服务提供商（MSP）。

> **Note**
>
> 配置事件响应团队并不会自动授予成员对服务资源（如成员资格和案例）的访问权限。您可以使用 AWS 安全事件响应提供的 AWS 托管策略，授予对资源的读写访问权限。点击此处，了解详情。

事件响应团队成员（在成员级别指定）会被自动添加到所有案例。创建好案例后，您仍可随时添加或删除单个团队成员。

发生通信偏好中列出的事件时，事件响应团队会收到电子邮件通知。

通信偏好

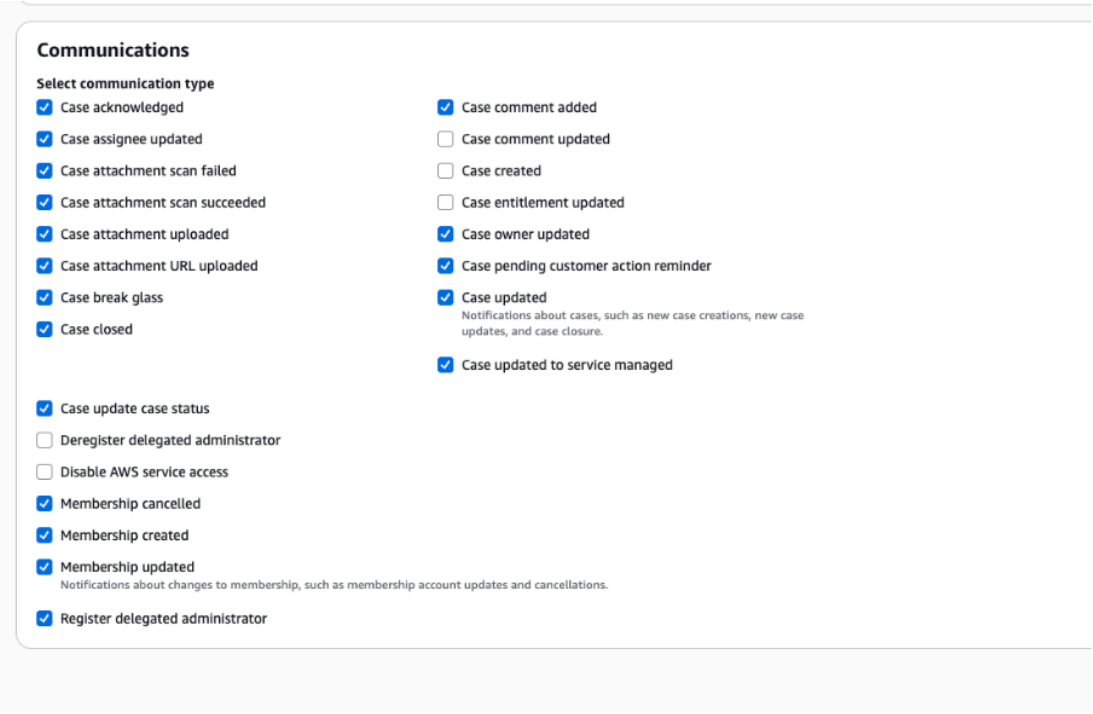
配置通信首选项，以控制您接收通知以及与安全事件响应系统交互的方式。

管理团队通信首选项

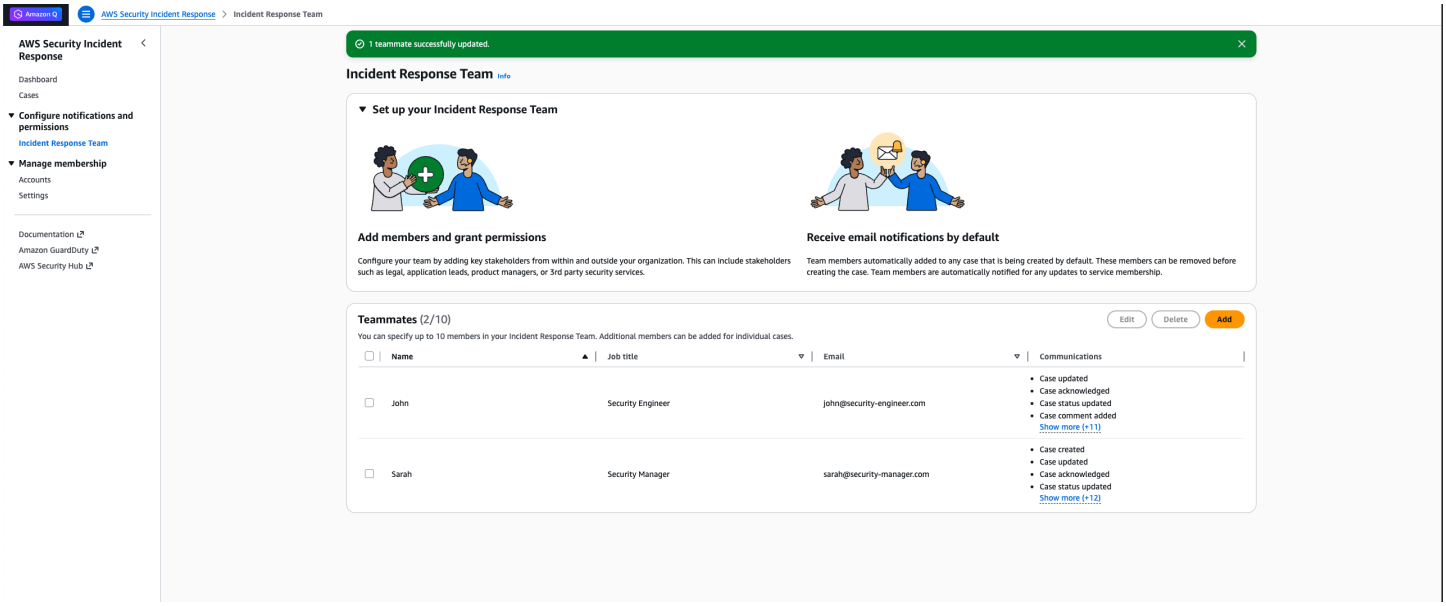
您可以从控制面板页面为事件响应团队中的个人配置通信首选项。

可按照以下步骤管理团队成员的通信设置：

1. 从控制面板导航到事件响应团队页面
2. 请执行以下操作之一：
   - 要更新现有团队成员：选择要修改其通信偏好的团队成员，然后选择编辑
   - 要添加新的团队成员，请执行以下操作：选择添加
3. 您将在此表单底部看到“通信”
   a. 勾选要接收的通信的复选框
   b. 清除不想接收的通信的复选框



4. 保存您的更改



默认通信设置

默认情况下，事件响应团队成员将启用所有通信。可以随时按照上述步骤修改这些设置。

通信选项

通信首选项控制您与事件响应团队交互的方式，以及在安全事件期间向您发送通知的方式。

> **Note**
>
> 这些首选项适用于安全事件响应系统内的所有未来通信。可以随时重复上述步骤来修改这些设置。

AWS Organizations 账户关联

启用 AWS 安全事件响应 时，您可以选择整个组织或特定组织单元（OU）。如果选择了特定 OU，则您的会员资格将仅覆盖属于这些选定 OU 的账户。如果选择了整个组织，则您的会员资格将覆盖组织内的所有账户。

如需了解更多详情，请参阅使用 AWS Organizations 管理 AWS 安全事件响应账户。

管理成员覆盖范围

您可以随时更改成员覆盖范围选项，包括从全组织覆盖切换到特定的 OU。

更新 OU 关联

要管理成员覆盖范围，请执行以下操作：

1. 导航到“账户关联设置”页面
2. 选择添加 OU，以选择要关联到成员的 OU
3. 选择要关联到成员的 OU
4. 单击更新关联，以在该成员上保存 OU 关联

更新关联后，您可以返回到同一页面，移除要与您的成员取消关联的任何 OU。即使您最初选择的是整个组织，也同样可以拥有这种灵活性——您可以事后更新成员以仅涵盖特定的 OU，而无需取消和重新启用服务。

如需了解更多信息，请参阅使用组织单元（OU）管理成员。

重要注意事项

直接位于根目录下的账户：选择特定的 OU 作为成员时，直接位于组织根目录下的账户（不属于任何 OU）将不会关联到您的成员。要将这些账户纳入成员覆盖范围，您必须先将其添加到某个 OU，然后将该 OU 关联到成员。

> **Note**
>
> 我们正在不断改进 OU 关联的用户体验，确保过程更加直观、易懂。

监控与调查

AWS 安全事件响应会审查来自 Amazon GuardDuty 和 AWS Security Hub CSPM 的安全警报并进行分级，然后根据您的环境配置隐藏规则来阻止不必要的警报。AWS 安全事件响应工程（SIRE）团队会调查调查发现并快速升级，指导您的团队及时遏制潜在问题。您也可以选择授权 AWS 安全事件响应代表自己执行遏制措施。

AWS 安全事件响应会遵循 NIST 800-61r2 Computer Security event Handling Guide 的安全事件响应标准。通过采用这一行业标准，AWS 安全事件响应提供一致的安全事件管理方法，并在您的 AWS 环境中遵循安全事件防护和响应的最佳实践。

当 AWS 安全事件响应检测到安全警报或您请求安全协助时，AWS SIRE 会进行调查。该团队会收集日志事件和服务数据（如 GuardDuty 警报），对这些数据进行分级和分析，执行修复和遏制措施，并提供事件后分析报告。

内容

准备

AWS 安全事件响应团队会在整个安全事件响应生命周期中全程参与调查，并与您保持密切协作。建议在安全事件发生前就完成该团队的组建，并分配好必要的访问权限。

检测与分析

报告事件

您可通过 AWS 安全事件响应门户上报安全事件。发生安全事件时，切勿延误。AWS 安全事件响应采用自动化与人工结合的方式调查安全事件、分析日志并识别异常模式。您对自身环境的深入理解与积极配合会显著加速分析进程。

启用支持的检测数据源

> **Note**
>
> AWS 安全事件响应费用不包含与支持的检测数据源相关的使用费用，以及其他 AWS 服务的使用费用。如需了解费用详情，请参阅各功能或服务的定价页面。

Amazon GuardDuty

如需在整个组织内启用 GuardDuty，请参阅《Amazon GuardDuty User Guide》中的“`Setting up GuardDuty`”部分。

强烈建议在所有受支持的 AWS 区域启用 GuardDuty。这样，GuardDuty 就可以生成有关未经授权或异常活动的调查发现，甚至在您未主动使用的区域也是如此。有关更多信息，请参阅 Amazon GuardDuty Regions and endpoints。

启用 GuardDuty 可为 AWS 安全事件响应提供关键威胁检测数据，显著增强其在 AWS 环境中识别和响应潜在安全问题的能力。

AWS Security Hub CSPM

AWS Security Hub CSPM 可以从多个 AWS 服务和受支持的第三方安全解决方案摄取安全调查发现。这些集成可以帮助 AWS 安全事件响应监控和调查来自其他检测工具的调查发现。

要启用 Security Hub CSPM 与 Organizations 的集成，请参阅 AWS Security Hub CSPM 用户指南。

Security Hub CSPM 提供了多种启用集成的方式。对于第三方产品集成，您可能需要从 AWS Marketplace 中购买集成，然后配置该集成。集成信息提供了用于完成这些任务的链接。详细了解如何启用 AWS Security Hub CSPM 集成。

当以下工具与 AWS Security Hub CSPM 集成时，AWS 安全事件响应会监控和调查来自这些工具的调查发现：

- CrowdStrike – CrowdStrike Falcon
- Lacework – Lacework
- Trend Micro – Cloud One

启用这些集成可显著提升 AWS 安全事件响应的监控和调查能力范围及效果。

检测

通过主动响应，AWS 安全事件响应会通过在加入期间部署到您账户的 Amazon EventBridge 规则从 Amazon GuardDuty 和 AWS Security Hub CSPM 中摄取调查发现。

对于在自动分级期间确定为无害或与预期活动相关的 Amazon GuardDuty 调查发现，AWS 安全事件响应 会自动将其存档。您可以在 Amazon GuardDuty 控制台中选择调查发现“状态”筛选条件中的“已存档”，从而查看已存档的调查发现。有关更多信息，请参阅《Amazon GuardDuty 用户指南》中的 Viewing generated findings in GuardDuty console。

对于在自动分级期间确定为无害或与预期活动相关的 Amazon GuardDuty 调查发现，AWS 安全事件响应 会自动将其存档。这种存档仅适用于经过分级且结果为“存档”的调查发现。即使调查已经结束，当前正在调查的调查发现仍然可在 Amazon GuardDuty 控制台中看到。您可以在 Amazon GuardDuty 控制台中选择调查发现“状态”筛选条件中的已存档，从而查看已存档的调查发现。有关使用已存档调查发现的更多信息，请参阅《Amazon GuardDuty 用户指南》中的 Working with findings。

当 AWS Security Hub CSPM 摄取安全调查发现时，系统会更新每个调查发现，添加一条指示已开始自动化分级的注释。工作流状态将从“新”变为“已通知”，这会将该调查发现从默认的 AWS Security Hub CSPM 调查发现视图中移除。如果分级后确定某个调查发现是无害或与预期活动相关联，则系统会向该调查发现添加一条注释，并将工作流状态更新为“已隐藏”。

分析：自动化分级

AWS 安全事件响应 会自动对安全调查发现进行分级。在确定检测到的活动是否属于预期行为时，分级过程会分析来自多个来源的数据，包括调查发现有效载荷、AWS 服务元数据、AWS 日志记录和监控

数据（例如 AWS CloudTrail 和 VPC 流日志）、AWS 威胁情报以及邀请您提供有关您的 AWS 和本地环境的上下文等。

如果自动分级确定检测到的活动是预期行为，则系统不会执行进一步的调查操作。

分析：事件响应安全调查

AWS 安全事件响应工程是一支可随时为用户提供支持的全球性团队，由拥有 AWS 和安全事件响应专业知识的安全专业人员组成。如果自动分级无法确定该活动是否是预期行为，则 AWS 安全事件响应工程将参与安全调查。如果事件是从 Security Hub 摄取的，则会在相关调查发现中发布一条注释，表明 AWS 安全事件响应工程正在进行调查。

AWS 安全事件响应工程通过分析额外的服务元数据和威胁情报、查看根据您环境中的历史调查发现和调查得出的见解，并运用事件响应专业知识，来进行切实的安全调查。根据您的遏制偏好（请参阅“遏制”），AWS 安全事件响应工程可能会通过 AWS 安全事件响应控制台中的安全事件响应案例与贵组织的事件响应团队联系，核实检测到的活动是否是预期行为以及对 AWS 生成案例的授权响应。

作为安全调查的一部分，AWS 安全事件响应还可以使用 EC2 Triage 从 Amazon Elastic Compute Cloud 实例收集调查信息。启用此功能后，AWS 安全事件响应响应人员可以对 Amazon EC2 实例执行 AWS Systems Manager Run Command，以收集调查数据、检查正在运行的进程并分析系统状态，而无需直接访问实例。

EC2 Triage 支持以下操作系统：

Linux

- Amazon Linux 2、Amazon Linux 2023
- Ubuntu 18.04、20.04、22.04、24.04
- Red Hat Enterprise Linux（RHEL）7.x、8.x、9.x
- CentOS 7.x、8.x
- SUSE Linux Enterprise Server（SLES）12.x、15.x
- Debian 10、11、12

Windows

- Windows Server 2012 R2
- Windows Server 2016、2019、2022

要使用 EC2 Triage，您必须将带有 EC2 Triage 的遏制 CloudFormation 模板部署到您的账户。有关更多信息，请参阅 使用 CloudFormation StackSets。目标 Amazon EC2 实例必须安装并运行 SSM

Agent，并且必须处于联机状态并由 AWS Systems Manager 管理。有关设置信息，请参阅 Setting up Systems Manager for Amazon EC2 instances。

沟通

AWS 安全事件响应通过安全事件响应案例与事件响应团队接触互动，让您在安全调查期间随时了解情况。多名 AWS 安全事件响应工程成员可能会为一项调查提供支持。沟通内容可能包括：确认或通知安全调查的创建；建立通话桥梁；分析日志文件等构件；请求确认预期活动；以及共享调查结果。

当 AWS 安全事件响应与您的事件响应团队主动联系时，会在您的 AWS 安全事件响应成员账户中创建一个案例，用于集中管理所有组织账户的沟通。这些案例的标题中带有用于标识发起者为 AWS 安全事件响应的“[Proactive case]”前缀。通过积极参与并及时回复这些沟通，您的事件响应团队可以 AWS 安全事件响应 协助完成以下工作：

- 确保快速响应真实安全事件。
- 了解您的环境和预期行为。
- 逐步减少检测误报情况。

AWS 安全事件响应的有效性会随着协作不断提升，从而打造更有效监控和安全的 AWS 环境。

更新调查发现

AWS 安全事件响应根据调查发现的来源和分级结果，对其进行不同的管理。

服务优化

如果您的账户服务配额允许，则 AWS 安全事件响应 会尝试部署一条 Amazon GuardDuty 隐藏规则 或 AWS Security Hub CSPM 自动化规则。这些规则会隐藏与已知获授权活动类型和来源（例如，源 IP 地址、ASN、身份主体或资源）匹配的未来调查发现。AWS Security Hub CSPM 规则的部署优先级为 10，从而让您能够在需要时使用自定义规则覆盖这些自动化。

通过这种方式，AWS 安全事件响应 可以根据 AWS 环境中的预期行为优化检测来源。有关这些规则集的修改将会通知您的事件响应团队，并可按要求回滚更改。

人工智能调查代理

概述

由人工智能驱动的调查代理与客户和 AWS 安全事件响应工程师协同工作，加快安全调查。当客户创建由 AWS 支持的案例时，该代理会在安全事件响应工程师参与的同时自动激活，从而将解决问题的时间从几天缩短到几小时。

在客户升级期间，安全事件响应案例可以由客户创建，也可以由 AWS 安全事件响应主动创建。创建由 AWS 支持的新案例时，系统会自动触发调查代理。您可以通过控制台、API 或 Amazon EventBridge 集成来管理所有案例。

主要优势

- 并行调查：代理与响应人员同时工作，实现人工智能驱动的自动化与人类专业知识的结合。
- 自动采集证据：通过自动查询 AWS CloudTrail、IAM、Amazon EC2 和 Cost Explorer 成本管理服务，消除手动日志分析的需要。
- 自然语言界面：可用通俗易懂的语言描述安全问题，无需有关 AWS 日志格式的专业知识。
- 更快响应：几分钟之内即可在“调查”选项卡中查看调查摘要。
- 完全可审计：所有代理操作均在 AWS CloudTrail 中于 `AWSServiceRoleForSupport` 角色下记录。

> **Important**
>
> 此功能仅适用于由 AWS 支持的案例。客户自行管理的案例不包括人工智能调查功能。

工作原理

人工智能调查代理在分析由 AWS 支持的安全案例时遵循结构化的工作流：

调查工作流

1. 创建案例：客户在安全事件响应控制台中创建一个由 AWS 支持的案例并提供有关安全问题的描述。
2. 并行激活
   - 安全事件响应工程师参与处理该案例。
   - 人工智能代理同时启动其调查工作流。
3. 背景问题（可选）：代理可以询问澄清性的问题来收集具体细节：
   - 受影响的 AWS 账户 ID
   - 涉及的 IAM 主体（用户、角色、访问密钥）
   - 具体的资源标识符（S3 存储桶、EC2 实例、ARN）
   - 可疑活动的时间线
4. 证据采集：代理自动查询 AWS 数据来源：

- AWS CloudTrail：与事件相关的 API 调用与活动
- IAM：用户和角色权限、策略更改和新身份创建
- Amazon EC2 实例 API：有关计算资源（如涉及）的信息
- Cost Explorer 成本管理服务：异常资源消耗的成本和使用情况指标

5. 分析和关联：代理将跨服务的证据关联起来，识别模式并确定事件发生的时间线。
6. 生成摘要：代理将在几分钟之内在“调查”选项卡中显示一份全面的调查摘要。

> **Note**
>
> 所有字段都是可选字段。如果在 10 分钟内未提供答案，则将自动启动调查。对于某些案例，如果已经有足够充分的信息，则代理可能会完全跳过可选问题。

访问调查结果

查看人工智能分析：

1. 在安全事件响应控制台中导航到您的案例。
2. 选择调查选项卡。
3. 查看调查摘要，包括调查发现、时间线和背景。

人工智能调查代理摘要会作为备注在案例的沟通部分发布，便于结合其他案例更新查看。

数据访问与权限

人工智能调查代理使用 `AWSServiceRoleForSupport` 服务相关角色来访问 AWS 资源。该角色提供了证据采集所需的只读权限：

代理执行的所有操作均在 AWS CloudTrail 记录，以便客户能够准确审计在调查期间访问的数据。在 AWS CloudTrail 日志中，这些操作均归于 `AWSServiceRoleForSupport`。

先决条件

在使用人工智能驱动的调查功能前，请确保您已满足下列条件：

必需的设置

- 已启用 AWS 安全事件响应：必须已通过 AWS Organizations 管理账户启用该服务。

- 由 AWS 支持的案例类型：人工智能调查仅适用于由 AWS 支持的案例（不适用于客户自行管理的案例）。
- AWSServiceRoleForSupport：此服务相关角色会自动创建，为调查代理提供所需的权限。

所需权限

要创建由 AWS 支持的案例并访问调查结果，该 IAM 主体需要具有以下权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "security-ir:CreateCase",
                "security-ir:GetCase",
                "security-ir:ListCases",
                "security-ir:UpdateCase"
            ],
            "Resource": "*"
        }
    ]
}
```

使用调查代理

创建由 AWS 支持的案例时，人工智能调查代理会自动激活。

监控人工智能调查进度

1. 在 AWS 安全事件响应 控制台中打开您的案例。
2. 选择调查选项卡。
3. 查看调查状态（正在进行或已完成）。
4. 完成后，查看综合调查摘要，其中包括调查结果、时间线和建议。

负责任的人工智能披露

调查摘要是使用 AWS 生成式人工智能功能生成的。您负责根据自己的具体背景评估人工智能生成的建议，实施恰当的监督机制，独立验证调查发现，并确保对所有安全决策实施人工监督。

客户数据的使用

人工智能调查代理不使用客户数据进行模型训练，也不会与第三方共享客户数据。

遏制

AWS 安全事件响应会与您协同遏制安全事件。您可以将该服务配置为在您的账户中主动执行遏制措施，以响应安全调查发现。您可以自行执行遏制措施，也可以使用支持的遏制措施中所述的 SSM 文档，与第三方合作伙伴协同执行遏制措施。

> **Important**
>
> 默认情况下，AWS 安全事件响应不会启用遏制功能。
> 需要完成两个步骤才能启用主动遏制功能：
>
> 1. 使用 IAM 角色向服务授予必要的权限。您可以为每个账户分别创建这些角色，也可使用 AWS CloudFormation 堆栈集为整个组织创建这些角色（这些堆栈集将会创建所需角色）。
> 2. 为每个账户或整个组织定义遏制首选项，以授权主动执行遏制措施。账户级别的首选项会取代组织级别的首选项。这可以通过创建 AWS Support 案例（技术：安全事件响应服务/其他）来完成。可用的遏制首选项如下：
>   - 需要审批（默认）：除非针对具体案例获得显式授权，否则不对任何资源执行主动遏制。
>   - 遏制已确认：主动遏制已确认泄露的资源。
>   - 遏制疑似：根据 AWS 安全事件响应工程所执行的分析，主动遏制泄漏可能性高的资源。

遏制决策

遏制的核心在于决策，例如：判断是否关闭系统、从网络隔离资源、禁用访问权限或终止会话等。如果已经预先确定了遏制事件的策略和程序，则这些决策将会更加容易。AWS安全事件响应会提供遏制策略，告知潜在影响，并仅在您确认同意相关风险后指导您实施解决方案。

支持的遏制措施

AWS 安全事件响应可代表您执行支持的遏制措施，以便加速响应，缩短威胁行为者在您环境中可能造成破坏的时间窗口。该功能可快速解决已识别的威胁，最大程度降低潜在影响，提升整体安全防护水平。根据分析的资源类型，有不同的遏制选项可供使用。支持的遏制措施详见以下子章节。

EC2 实例遏制

`AWSSupport-ContainEC2Instance` 自动化遏制方案将对 EC2 实例执行可逆的网络遏制，在保持实例完整运行的同时阻断所有新网络活动，防止实例与 VPC 内外资源通信。

> **Important**
>
> 值得注意的是，修改安全组规则不会中断现有已建立的连接，新安全组和该 SSM 文档只会有效阻断后续流量。如需了解更多信息，请参阅服务技术指南的源遏制部分。

IAM 访问遏制

`AWSSupport-ContainIAMPrincipal` 自动化遏制方案将对 IAM 用户或角色执行可逆的网络遏制，在 IAM 中保留该用户/角色的同时，阻止其与您账户中的资源进行通信。

S3 存储桶遏制

`AWSSupport-ContainS3Resource` 自动化遏制方案将对 S3 存储桶执行可逆的遏制，在保留存储桶内所有对象的同时，通过修改访问策略来隔离 Amazon S3 存储桶或对象。

制定遏制策略

AWS 安全事件响应建议根据风险承受能力，为每类主要事件制定相应的遏制策略。请明确记录决策标准，以便事件发生时参考。需考虑的标准包括：

- 资源潜在损害程度
- 证据保存与合规要求
- 服务不可用性（如网络连接、向外部提供的服务）
- 实施策略所需的时间与资源
- 策略有效性（如部分遏制与完全遏制）
- 解决方案持久性（如可逆与不可逆操作）
- 解决方案的持续时间（如应急变通方案、临时变通方案、永久解决方案）

执行可降低风险的安全控制措施，为制定和实施更有效的遏制策略争取时间。

阶段式遏制方法

AWS 安全事件响应建议采用分阶段方案实现高效遏制，根据资源类型制定短期与长期策略。

遏制策略决策流程

AWS 安全事件响应是否能识别安全事件的范围？

- 是：标记所有相关资源（用户、系统、资源）。
- 否：对已识别资源执行下一步，同时继续调查。

资源是否能被隔离？

- 是：立即隔离受影响资源。
- 否：协同系统负责人确定替代遏制方案。

所有受影响的资源是否都已与未受影响的资源隔离开来？

- 是：进入下一阶段。
- 否：继续执行隔离，完成短期遏制，防止事件升级。

系统备份

是否已为受影响的系统创建备份以用于进一步的分析？

取证副本是否已加密并安全存储？

- 是：进入下一阶段。
- 否：立即加密取证映像并安全存储，防止意外使用、损坏或篡改。

提交遏制偏好

要为您的账户或组织配置遏制偏好，请创建 AWS 支持 案例。

在支持案例中，请指定以下信息：

配置完成后，AWS 安全事件响应 将在活跃安全事件期间执行授权的遏制措施，以帮助保护您的环境。

- 您的 AWS Organizations ID 或应授权遏制措施的特定账户 ID
- 您的偏好遏制选项。

> **Note**
>
> 只有在配置了适当的偏好且部署所需的 AWS CloudFormation 堆栈集以授予必要权限之后，AWS 安全事件响应 才会执行遏制措施。

根除

在根除阶段，必须全面识别并处理所有受影响的账户、资源及实例（包括删除恶意软件、清除遭入侵的用户账户、修复已发现的漏洞），以便在整个环境中实施统一的修复措施。

最佳实践是采用分阶段根除与恢复方案，并优先处理关键修复步骤。早期阶段旨在通过高价值变更快速（数日至数周内）提升整体安全性，预防未来发生安全事件。后期阶段则侧重于长期变更（例如基础设施改造）和持续优化工作来尽力保障企业安全。每个案例都具有独特性，AWS 安全事件响应工程师会协助您评估需采取的必要措施。

请考虑以下事项：

- 能否通过系统重装并应用补丁或其他防护措施来消除或降低攻击风险？
- 能否以全新实例替换受感染系统，在终止污染项目的同时建立洁净基准？
- 是否已清除所有恶意软件及未授权使用痕迹，并针对进一步攻击对受影响系统进行强化？
- 是否需要对受影响资源进行取证？

恢复

AWS 安全事件响应将提供系统恢复指导，包括：恢复正常运行、确认功能完整性，以及修复漏洞以防事件重现。但 AWS 安全事件响应不会直接参与系统恢复操作。关键考虑因素包括：

- 受影响系统是否已针对同类攻击完成补丁安装并强化防护？
- 将系统恢复至生产环境的合理时间安排为何？
- 将使用哪些工具来测试、监控及验证已恢复的系统？

事件后报告

AWS 安全事件响应将在双方团队完成安全处置工作后，提供事件摘要报告。

每月底，AWS 安全事件响应将通过电子邮件向每位客户的主要联系人发送月度报告。报告将采用 PDF 格式，且包含下述指标。每个 AWS Organizations 的客户都会收到一份报告。

案例指标

- 新建案例
  - 维度名称：类型

  - 维度值：AWS 托管 | 自主管理
  - 单位：个
  - 说明：新建案例数量统计。
- 已关闭案例
  - 维度名称：类型
  - 维度值：AWS 托管、自主管理
  - 单位：个
  - 说明：已关闭案例总数统计。
- 未关闭案例
  - 维度名称：类型
  - 维度值：AWS 托管 | 自主管理
  - 单位：个
  - 说明：未关闭案例数量统计。

分级指标

- 接收到的调查发现
  - 单位：个
  - 说明：需分级处理的调查发现数量。
- 已归档的调查发现
  - 单位：个
  - 说明：经处理后无需人工调查而归档的调查发现数量。
- 人工调查的调查发现
  - 单位：个
  - 说明：经过人工调查的调查发现数量。
- 已归档调查
  - 单位：个
  - 说明：判定为误报并归档的人工调查案例数量。
- 已升级的调查
  - 单位：个
  - 说明：确认为安全事件并升级处理的人工调查案例数量。

案例

AWS 安全事件响应支持创建两种类型的案例：AWS 托管案例、自主管理案例。

创建 AWS 托管案例

您可通过控制台、API 或 AWS Command Line Interface为 AWS 安全事件响应创建由 AWS 支持的案例。由 AWS 支持的案例将由安全事件响应工程师为您提供支持。

Important

演示/模拟案例将在 90 天后关闭。

Note

AWS 安全事件响应工程师将在 15 分钟内响应您的案例。响应时间指 AWS 安全事件响应工程师发出首次响应的时间。我们会尽一切合理努力在此时间范围内响应您的初次请求。该响应时效不适用于后续响应。

Note

您不仅可以为活跃安全事件和调查创建由 AWS 支持的案例，还可以创建此类案例来咨询 AWS 安全事件响应的功能。这包括有关 GuardDuty 隐藏规则、警报分级配置、主动响应工作流以及有关安全态势的一般指导的问题。对于此类目的，请选择调查与查询案例类型。

何时联系 AWS 安全事件响应

您可以根据自己的需求出于各种目的联系 AWS 安全事件响应。下表介绍了各种不同的场景以及每种场景的相应联系方式。

场景	何时使用	响应时间	案例类型
活跃安全事件	您遇到了紧急安全事件，需要立即获得事件响应支持和服务	15 分钟（第一次响应）	活跃安全事件

场景	何时使用	响应时间	案例类型
调查	您怀疑出现了安全事件，需要获得有关日志分析和事件响应调查二次确认方面的支持	15 分钟（第一次响应）	调查与咨询
咨询与指导	您有涉及 Amazon GuardDuty 调查发现、隐藏规则、警报分级配置、主动响应工作流或与 AWS 安全事件响应 功能相关的一般安全态势等方面的问题	15 分钟（第一次响应）	调查与咨询
信息载入问题	您在 AWS 安全事件响应的信息载入过程中遇到了技术问题	因支持计划而异	AWS 支持 案例

对于所有由 AWS 支持的案例（活跃安全事件以及调查与咨询），AWS 安全事件响应工程师将在 15 分钟内进行第一次响应。该响应时效仅适用于第一次联系，不适用于后续响应。

以下示例演示控制台操作流程。

1. 通过 AWS 管理控制台登录 AWS 安全事件响应。
2. 选择创建案例
3. 选择通过 AWS 解决案例
4. 选择请求类型：
   a. 活跃安全事件：用于紧急事件响应支持服务。
   b. 调查与咨询：用于疑似的安全事件，AWS 安全事件响应工程师在日志分析和事件响应调查二次确认等方面提供支持。您还可以使用此类下来咨询涉及 Amazon GuardDuty 调查发现、隐藏规则、警报分级配置、主动响应工作流或与 AWS 安全事件响应功能相关的一般安全态势等方面的问题。
5. 将预估开始日期设置为事件最早出现迹象的日期，例如：首次出现异常行为或收到首个相关安全警报的日期。
6. 为案例定义标题
7. 请提供案例的详细描述。 以下内容将帮助事件响应人员更快解决问题：
   a. 发生了什么？
   b. 是谁发现并报告的该事件？

c. 哪些对象受到该案例影响？

d. 目前已知的影响范围？

e. 该案例的紧急程度？

f. 添加一个或多个属于案例范围内的 AWS 账户 ID。

8. 添加案例详细信息（选填）：

a. 从下拉列表中选择受影响的主要服务。

b. 从下拉列表中选择受影响的主要区域。

c. 添加一个或多个在该案例中确定的威胁行为者 IP 地址。

9. 为案例添加其他事件响应人员，以便接收通知。要添加响应人员，请执行以下操作：

a. 添加电子邮件地址。

b. 添加姓名（选填）。

c. 选择新增添加其他响应人员。

d. 要删除响应人员，选择对应人员的删除选项。

e. 选择添加，可将所列出的所有人员添加到案例中。

i. 您可以选择多人，然后选择删除，即可批量删除所选人员。

10.将标签添加到案例（可选）。

a. 要添加标签，请执行以下操作：

b. 选择添加新标签。

c. 对于键，输入标签的名称。

d. 对于值，输入标签的值。

e. 要删除标签，请为该标签选择删除选项。

由 AWS 支持等案例创建后，AWS 安全事件响应工程师和您的事件响应团队会立即收到通知。

创建由 AWS 支持的案例并启用人工智能调查

1. 从 console.aws.amazon.com/ 打开 AWS 安全事件响应控制台。
2. 从导航窗格中选择案例。
3. 选择创建工单。
4. 对于案例类型，选择由 AWS 支持的案例。
5. 提供案例详情，包括标题、事件开始日期和受影响的 AWS 账户 ID。
6. 在描述安全事件部分中，提供对事件的详尽描述。

7. 提供有关受影响 AWS 服务、区域和其他相关细节的更多信息。
8. 选择创建工单。

案例创建后，安全事件响应工程师和人工智能代理开始同时工作。

回答人工智能澄清性问题（可选）

1. 在您的案例中导航至调查选项卡。
2. 查看人工智能代理提出的任何澄清性问题。
3. 回答问题，或者选择跳过（如果您不想回答）。
4. 选择提交以继续。所有字段都是可选字段。

负责任的人工智能披露

调查摘要是使用 AWS 生成式人工智能功能生成的。您负责根据自己的具体背景评估人工智能生成的建议，实施恰当的监督机制，独立验证调查发现，并确保对所有安全决策实施人工监督。

创建自主管理案例

您可通过控制台、API 或 AWS Command Line Interface为 AWS 安全事件响应创建自主管理案例。此类案例不需要 AWS 安全事件响应工程师参与。以下示例演示控制台操作流程。

1. 通过位于 https://console.aws.amazon.com/security-ir/ 的 AWS 管理控制台 登录 AWS 安全事件响应。
2. 选择创建案例。
3. 选择通过自有事件响应团队解决案例。
4. 将预估开始日期设置为事件最早出现迹象的日期，例如：首次出现异常行为或收到首个相关安全警报的日期。
5. 为案例定义标题。建议选择生成标题选项，按提示纳入日期信息。
6. 输入案例涉及的 AWS 账户 ID。要添加账户 ID，请执行以下操作：
   a. 输入 12 位数账户 ID，然后选择添加账户。
   b. 要删除账户，选择案例中需删除账户旁的删除选项。
7. 请提供案例的详细描述。
   a. 以下内容将帮助事件响应人员更快解决问题：
      i. 发生了什么？

ii. 是谁发现并报告的该事件？

iii. 哪些对象受到该案例影响？

iv. 目前已知的影响范围？

v. 该案例的紧急程度？

8. 添加案例详细信息（选填）：
   a. 从下拉列表中选择受影响的主要服务。
   b. 从下拉列表中选择受影响的主要区域。
   c. 添加一个或多个在该案例中确定的威胁行为者 IP 地址。
9. 为案例添加其他事件响应人员，以便接收通知。要添加响应人员，请执行以下操作：
   a. 添加电子邮件地址。
   b. 添加姓名（选填）。
   c. 选择新增添加其他响应人员。
   d. 要删除响应人员，选择对应人员的删除选项。
   e. 选择添加，可将所列出的所有人员添加到案例中。您可以选择多人，然后选择删除，即可批量删除所选人员。
10. 将标签添加到案例（可选）。要添加标签，请执行以下操作：
   a. 选择添加新标签。
   b. 对于键，输入标签的名称。
   c. 对于值，输入标签的值。
   d. 要删除标签，请为该标签选择删除选项。

案例创建后，系统会通过电子邮件通知事件响应团队。

与 AWS 安全事件响应工程师协同工作

在您创建安全事件案例后，AWS 安全事件响应工程师将开始处理您的事件。本节介绍了调查期间预计将出现的情况以及如何与我们的团队进行有效协作。

AWS 安全事件响应工程师预计将执行的工作

当您创建由 AWS 支持的案例时，系统将为您的事件指派一名安全事件响应工程师。为您指定的响应人员将执行以下工作：

- 检查您在案例中提供的初步信息

- 分析相关的 AWS 服务日志和安全调查发现
- 确定安全事件的范围和影响
- 根据您的情况制定调查和响应计划

响应时限：AWS 安全事件响应工程师确认新案例的服务等级目标（SLO）为 15 分钟内。初始评估时限可能因案例的严重程度和复杂性而异。如果 AWS 安全事件响应工程师在 5 个工作日内没有收到您的回复或重要信息，则将关闭该案例。

调查工作流

AWS 安全事件响应工程师遵循与 NIST 800-61r2 框架一致的结构化事件响应流程。在调查期间，预计将会出现以下阶段：

1. 初步分级：安全事件响应工程师审查您的案例详情并确认事件范围
2. 调查：安全事件响应工程师分析日志，识别泄漏指标并确定根本原因
3. 遏制：安全事件响应工程师建议可限制事件影响的措施
4. 根除和恢复：安全事件响应工程师协助您消除威胁并恢复正常运行
5. 事后审查：安全事件响应工程师提供调查发现，以及旨在防止未来发生事件的建议

在这些阶段，安全事件响应工程师会通过案例更新随时向您通报情况，并且可能会要求您提供更多信息或采取行动。

信息安全事件响应工程师可能提出要求

为有效地调查您的事件，AWS 安全事件响应工程师可能会要求您提供下列信息：

- 时间线详情：您首次检测到事件的时间以及引发该事件的任何相关事件
- 受影响的资源：涉及的特定 AWS 账户 ID、服务、区域和资源 ARN
- 访问信息：有关谁有权访问受影响资源的详细信息以及任何最近的访问权限变更
- 业务背景：受影响资源的使用方式以及对业务的潜在影响
- 日志和证据：可能有助于调查的其他日志、屏幕截图或构件
- 授权：批准代表您执行特定的遏制或补救措施

您的安全事件响应工程师将解释为什么需要各条信息以及这些信息对调查有何帮助。

沟通最佳实践

有效的沟通可以加快事件的解决。与 AWS 安全事件响应工程师协作时，请遵循以下最佳实践：

- 及时响应安全事件响应工程师要求提供的信息
- 即使您不确定其相关性，也应提供完整的信息
- 如果您不理解任何建议或需要澄清，请随时提问
- 根据事件的任何新进展或变化更新案例
- 在您的团队中指定一名主要联系人，负责与安全事件响应工程师进行协调

> **Important**
>
> 如果对于提供关键信息的请求，AWS 安全事件响应工程师在 5 个工作日内未收到回复，我们会关闭案例。如果有新信息可用，您可以重新创建案例。

您在调查期间的角色

虽然调查由 AWS 安全事件响应工程师主管，但您的参与也至关重要。您负责采取以下措施：

- 及时响应有关提供信息的请求
- 在您的 AWS 环境中实施建议的遏制和弥补措施
- 授权安全事件响应工程师代表您采取措施（如果您启用了主动响应）
- 根据需要与内部团队（安全、法律、合规）进行协调
- 做出有关事件响应优先级和权衡的商业决策

AWS 安全事件响应工程师提供专业知识和建议，您自己的 AWS 资源始终由您控制，相关响应措施也由您最终决定。

关闭案例

发生下列情况时，AWS 安全事件响应工程师会关闭案例：

- 事件已得到遏制和补救
- 已将所有调查发现提供给您
- 不再需要 安全事件响应工程师提供任何进一步的协助

- 您要求关闭案例

在关闭案例之前，安全事件响应工程师将会向您提供一份摘要，说明相关调查发现、所执行的措施以及可改善安全状况的建议。

如果您在案例关闭后需要其他帮助，可以创建新案例或联系 AWS 支持。

响应 AWS 生成的案例

当账户或资源可能受到影响需要而采取行动或给予关注时，AWS 安全事件响应可能会主动创建外发通知或案例。只有当您在订阅中启用了主动响应和警报分级工作流时，才会触发此功能。

这些通知会在 AWS 安全事件响应中显示为带 "[Proactive case]" 前缀的安全事件响应案例。要查看和管理这些案例，请完成以下步骤：

- 在 https://console.aws.amazon.com/security-ir/ 上打开安全事件响应控制台
- 选择案例。
- 您会看到所有案例，包括带 "[Proactive case]" 前缀的案例。

您可以根据需要更新、解决、重新打开这些案例。您可以通过这些案例直接与 AWS 安全事件响应团队沟通，确保潜在安全问题得到高效处理。

管理案例

内容

更改案例状态

案例可能的状态如下：

- 已提交：这是案例的初始状态，表示已收到请求但尚未开始处理。
- 检测与分析：此状态表示事件响应人员已开始处理案例。此阶段包括包括数据收集、事件分级及分析数据进行论证。
- 遏制、根除与恢复：此状态表示事件响应人员已识别需要额外处置的可疑活动。响应人员将提供业务风险分析建议和后续行动方案。若已启用服务的可选功能，AWS 事件响应人员会征求您的授权，以便在受影响账户中通过 SSM 文档执行遏制措施。
- 事件后活动：该状态表示主要安全事件已得到控制。当前重点是让业务恢复正常运营。若案例由 AWS 托管解决，则会提供事件摘要和根本原因分析。
- 已关闭：这是工作流程的最终状态。案例处于“已关闭”状态，表示处置已完成。已关闭案例无法重新开启，因此务必确保已完成所有操作，再切换到该状态。

对于自主管理案例，选择操作/更新状态即可更改状态。对于由 AWS 支持的案例，该状态将由 AWS 安全事件响应工程师设置。

变更解决方

对于自主管理案例，您的事件响应团队可向 AWS 请求协助。选择获取 AWS 协助即可将案例解决方变更为 AWS。转为 AWS 托管案例后，状态会变更为已提交。现有的案例历史记录将可由 AWS 安全事件响应工程师查阅。一旦请求 AWS 协助，案例不可再转回自主管理模式。

待执行事项

负责该案例的 AWS 安全事件响应工程师可能会要求您的内部团队采取行动。

案例创建后出现的待执行事项包括：

- 请求为事件响应人员授予案例访问权限
- 请求提供更多关于案例的信息

准备关闭时的待执行事项：

- 请求查看案例报告
- 请求关闭案例

编辑案例

选择编辑即可更改案例详情。

对于 AWS 托管案例和自主管理案例：

创建案例后，您可以更改案例的下列详情：

- 标题
- 说明

仅适用于 AWS 托管案例：

您可以更改其他字段：

- 请求类型：
  - 活跃安全事件：用于紧急事件响应支持服务。
  - 调查：可让您获取有关疑似安全事件的支持，AWS 安全事件响应工程师可在日志深度分析和安全事件二次确认等方面提供支持。
- 预计开始日期：如果获取到早于当前设定日期的案例相关迹象，请修改此字段。建议在描述字段补充新发现迹象的详细信息，或在沟通标签页中添加评论说明。

通信

AWS 安全事件响应工程师可在处理案例时添加备注，以记录自己的工作内容。不同的 AWS 安全事件响应工程师可能会同时处理同一案例。这些人在通信日志中统一标记为 AWS 响应人员。

权限

“权限”选项卡列出了所有会收到案例变更通知的人员。在案例关闭之前，您都可以在列表中添加或删除人员。

> **Note**
>
> 单个案例最多支持添加 30 名相关人员。需额外配置权限才可授予这些相关人员案例级别的访问权限。

在控制台中授予对案例的访问权限

要通过 AWS 管理控制台管理控制台授予案例访问权限，请复制 IAM 权限策略模板，并将之添加到用户或角色。

将 IAM 策略附加到用户或角色：

1. 复制 IAM 权限策略。
2. 通过 https://console.aws.amazon.com/iam/ 打开 IAM。
3. 在导航窗格中，选择用户或角色。
4. 选择用户或角色打开详细信息页面。
5. 在“权限”选项卡中，请选择添加权限。
6. 选择附加策略。
7. 选择相应的 AWS 安全事件响应托管策略。
8. 选择添加策略。

附件

事件响应人员可为案例添加附件，协助其他响应人员调查自主管理案例。

> **Note**
>
> 若选择 AWS 托管案例，AWS 便无法查看附件内容。AWS 托管案例的所有详细信息都必须通过案例评论来提供，或由您使用自选通讯技术进行屏幕共享来提供。

点击上传从本机选择文件添加到案例。

> **Note**
>
> 所有已上传附件都会在案例处于 `Closed` 状态七天后自动删除。

标签

标签是一种可选标记，您可将其分配给案例来存储相应资源的元数据。每个标签都是由一个密钥和一个可选值组成的。标签可用来搜索、分配成本以及对资源进行权限认证。

要添加标签，请执行以下操作：

1. 选择添加新标签。
2. 对于键，输入标签的名称。
3. 对于值，输入标签的值。

要删除标签，请为该标签选择删除选项。

案例活动

审计跟踪记录功能提供所有案例活动的详细时间序记录。这些记录在事后分析中至关重要，能帮助识别潜在改进点。案例审计跟踪记录会记录任何案例变更的时间、用户、操作及详情。

关闭案例

对于 AWS 托管案例，在案例详细信息页面选择关闭案例，即可随时永久关闭处于任何状态的案例。通常情况下，案例会先进入准备关闭状态，再被永久关闭。若在非准备关闭状态下提前关闭案例，即表示要求 AWS 安全事件响应工程师停止处理该由 AWS 支持的案例。

如果您的事件响应团队为响应方，请在案例详细信息页面选择操作/关闭案例。

> **Note**
>
> “准备关闭”状态表示案例可以永久关闭，且无需进一步处理。

永久关闭后，案例无法重新开启，所有信息将转为只读模式。为防止意外关闭，系统会要求您确认是否要关闭案例。

使用 CloudFormation StackSets

有关如何使用服务管理权限创建堆栈集的具体说明，请参阅 AWS CloudFormation 用户指南中的使用服务管理权限创建 CloudFormation 堆栈集。

AWS 安全事件响应提供了两个 CloudFormation 模板。这两个模板创建两个相同的 AWS Identity and Access Management 角色：`AWSSecurityIncidentResponseContainment` 和 `AWSSecurityIncidentResponseContainmentExecution`。带有 EC2 Triage 的遏制模板向 `AWSSecurityIncidentResponseContainment` 添加 `AWSSecurityIncidentResponseInvestigationPolicy`，其授予 EC2 Triage 的额外权限。选择符合您的安全要求的模板：

- 仅遏制：创建遏制操作所需的最低权限。
- 带有 EC2 Triage 的遏制：包括所有遏制权限以及 EC2 Triage 的额外权限。此模板允许AWS 安全事件响应在安全调查期间对 Amazon Elastic Compute Cloud 实例执行 AWS Systems Manager Run Command。

有关 EC2 Triage 的更多信息，请参阅 检测与分析。

CloudFormation 模板

以下模板为AWS 安全事件响应遏制操作创建了必要的 IAM 角色。请选择最适合您的安全要求的模板。

内容

仅遏制

此模板创建了遏制操作所需的最低角色。如果不需要 EC2 Triage 功能，请使用此模板。

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for production SIR containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
```

```
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainEC2Instance',
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainS3Resource',
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainIAMPrincipal',
                        !Sub 'arn:${AWS::Partition}:ssm:*:${AWS::AccountId}:automation-
execution/*',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
                      ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
 'ssm:ListCommandInvocations'],
                    'Resource': '*',
                  },
                  {
                    'Effect': 'Allow',
                    'Action': ['iam:PassRole'],
                    'Resource': !GetAtt
 AWSSecurityIncidentResponseContainmentExecution.Arn,
                    'Condition': { 'StringEquals': { 'iam:PassedToService':
 'ssm.amazonaws.com' } },
                  },
                ],
            }
```

```
  AWSSecurityIncidentResponseContainmentExecution:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
'Action': 'sts:AssumeRole' }],
        }
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Sid': 'AllowIAMContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'iam:AttachRolePolicy',
                        'iam:AttachUserPolicy',
                        'iam:DeactivateMFADevice',
                        'iam:DeleteLoginProfile',
                        'iam:DeleteRolePolicy',
                        'iam:DeleteUserPolicy',
                        'iam:GetLoginProfile',
                        'iam:GetPolicy',
                        'iam:GetRole',
                        'iam:GetRolePolicy',
                        'iam:GetUser',
                        'iam:GetUserPolicy',
                        'iam:ListAccessKeys',
                        'iam:ListAttachedRolePolicies',
                        'iam:ListAttachedUserPolicies',
                        'iam:ListMfaDevices',
                        'iam:ListPolicies',
                        'iam:ListRolePolicies',
                        'iam:ListUserPolicies',
```

```
                'iam:ListVirtualMFADevices',
                'iam:PutRolePolicy',
                'iam:PutUserPolicy',
                'iam:TagMFADevice',
                'iam:TagPolicy',
                'iam:TagRole',
                'iam:TagUser',
                'iam:UntagMFADevice',
                'iam:UntagPolicy',
                'iam:UntagRole',
                'iam:UntagUser',
                'iam:UpdateAccessKey',
                'identitystore:CreateGroupMembership',
                'identitystore:DeleteGroupMembership',
                'identitystore:IsMemberInGroups',
                'identitystore:ListUsers',
                'identitystore:ListGroups',
                'identitystore:ListGroupMemberships',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowOrgListAccounts',
            'Effect': 'Allow',
            'Action': 'organizations:ListAccounts',
            'Resource': '*',
          },
          {
            'Sid': 'AllowSSOContainment',
            'Effect': 'Allow',
            'Action':
              [
                'sso:CreateAccountAssignment',
                'sso:DeleteAccountAssignment',
                'sso:DeleteInlinePolicyFromPermissionSet',
                'sso:GetInlinePolicyForPermissionSet',
                'sso:ListAccountAssignments',
                'sso:ListInstances',
                'sso:ListPermissionSets',
                'sso:ListPermissionSetsProvisionedToAccount',
                'sso:PutInlinePolicyToPermissionSet',
                'sso:TagResource',
                'sso:UntagResource',
              ],
```

```
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowSSORead',
                    'Effect': 'Allow',
                    'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Read',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:GetAccountPublicAccessBlock',
                        's3:GetBucketAcl',
                        's3:GetBucketLocation',
                        's3:GetBucketOwnershipControls',
                        's3:GetBucketPolicy',
                        's3:GetBucketPolicyStatus',
                        's3:GetBucketPublicAccessBlock',
                        's3:GetBucketTagging',
                        's3:GetEncryptionConfiguration',
                        's3:GetObject',
                        's3:GetObjectAcl',
                        's3:GetObjectTagging',
                        's3:GetReplicationConfiguration',
                        's3:ListBucket',
                        's3express:GetBucketPolicy',
                      ],
                    'Resource': '*',
                  },
                  {
                    'Sid': 'AllowS3Write',
                    'Effect': 'Allow',
                    'Action':
                      [
                        's3:CreateBucket',
                        's3:DeleteBucketPolicy',
                        's3:DeleteObjectTagging',
                        's3:PutAccountPublicAccessBlock',
                        's3:PutBucketACL',
                        's3:PutBucketOwnershipControls',
                        's3:PutBucketPolicy',
```

```
                    's3:PutBucketPublicAccessBlock',
                    's3:PutBucketTagging',
                    's3:PutBucketVersioning',
                    's3:PutObject',
                    's3:PutObjectAcl',
                    's3express:CreateSession',
                    's3express:DeleteBucketPolicy',
                    's3express:PutBucketPolicy',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowAutoScalingWrite',
                'Effect': 'Allow',
                'Action':
                  [
                    'autoscaling:CreateOrUpdateTags',
                    'autoscaling:DeleteTags',
                    'autoscaling:DescribeAutoScalingGroups',
                    'autoscaling:DescribeAutoScalingInstances',
                    'autoscaling:DescribeTags',
                    'autoscaling:EnterStandby',
                    'autoscaling:ExitStandby',
                    'autoscaling:UpdateAutoScalingGroup',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowEC2Containment',
                'Effect': 'Allow',
                'Action':
                  [
                    'ec2:AuthorizeSecurityGroupEgress',
                    'ec2:AuthorizeSecurityGroupIngress',
                    'ec2:CopyImage',
                    'ec2:CreateImage',
                    'ec2:CreateSecurityGroup',
                    'ec2:CreateSnapshot',
                    'ec2:CreateTags',
                    'ec2:DeleteSecurityGroup',
                    'ec2:DeleteTags',
                    'ec2:DescribeImages',
                    'ec2:DescribeInstances',
                    'ec2:DescribeSecurityGroups',
```

```
                    'ec2:DescribeSnapshots',
                    'ec2:DescribeTags',
                    'ec2:ModifyNetworkInterfaceAttribute',
                    'ec2:RevokeSecurityGroupEgress',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowKMSActions',
                'Effect': 'Allow',
                'Action':
                  [
                    'kms:CreateGrant',
                    'kms:DescribeKey',
                    'kms:GenerateDataKeyWithoutPlaintext',
                    'kms:ReEncryptFrom',
                    'kms:ReEncryptTo',
                  ],
                'Resource': '*',
              },
              {
                'Sid': 'AllowSSMActions',
                'Effect': 'Allow',
                'Action': ['ssm:DescribeAutomationExecutions'],
                'Resource': '*',
              },
            ],
        }
```

带有 EC2 Triage 的遏制

此模板创建了具有 EC2 Triage 功能额外权限的遏制角色。如果需要 AWS 安全事件响应 在安全调查期间对 Amazon EC2 实例执行 Systems Manager Run Command，请使用此模板。

```
AWSTemplateFormatVersion: '2010-09-09'
Description: 'Template for AWS Security Incident Response containment roles'

Resources:
  AWSSecurityIncidentResponseContainment:
    Type: 'AWS::IAM::Role'
    Properties:
      RoleName: AWSSecurityIncidentResponseContainment
      AssumeRolePolicyDocument:
```

```
        {
          'Version': '2012-10-17',
          'Statement':
            [
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:AssumeRole',
                'Condition': { 'StringEquals': { 'sts:ExternalId': !Sub
 '${AWS::AccountId}' } },
              },
              {
                'Effect': 'Allow',
                'Principal': { 'Service': 'containment.security-ir.amazonaws.com' },
                'Action': 'sts:TagSession',
              },
            ],
        }
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Effect': 'Allow',
                    'Action': ['ssm:StartAutomationExecution'],
                    'Resource':
                      [
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainEC2Instance',
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainS3Resource',
                        !Sub 'arn:${AWS::Partition}:ssm:*::document/AWSSupport-
ContainIAMPrincipal',
                        !Sub 'arn:${AWS::Partition}:ssm:*:${AWS::AccountId}:automation-
execution/*',
                      ],
                  },
                  {
                    'Effect': 'Allow',
                    'Action':
```

```
                    ['ssm:DescribeInstanceInformation', 'ssm:GetAutomationExecution',
'ssm:ListCommandInvocations'],
                  'Resource': '*',
                },
                {
                  'Effect': 'Allow',
                  'Action': ['iam:PassRole'],
                  'Resource': !GetAtt
AWSSecurityIncidentResponseContainmentExecution.Arn,
                  'Condition': { 'StringEquals': { 'iam:PassedToService':
'ssm.amazonaws.com' } },
                },
              ],
          }
      - PolicyName: AWSSecurityIncidentResponseInvestigationPolicy
        PolicyDocument:
          {
            'Version': '2012-10-17',
            'Statement':
              [
                {
                  'Effect': 'Allow',
                  'Action': [
                    'ec2:DescribeInstanceStatus',
                    'ec2:DescribeInstances',
                    'ec2:DescribeRouteTables',
                    'ec2:DescribeSecurityGroupRules',
                    'iam:GetInstanceProfile',
                    'ssm:DescribeInstanceInformation',
                    'ssm:GetCommandInvocation'
                  ],
                  'Resource': '*'
                },
                {
                  'Effect': 'Allow',
                  'Action': [
                    'ssm:SendCommand'
                  ],
                  'Resource': '*'
                }
              ]
            }
 AWSSecurityIncidentResponseContainmentExecution:
   Type: 'AWS::IAM::Role'
```

```
    Properties:
      RoleName: AWSSecurityIncidentResponseContainmentExecution
      AssumeRolePolicyDocument:
        {
          'Version': '2012-10-17',
          'Statement':
            [{ 'Effect': 'Allow', 'Principal': { 'Service': 'ssm.amazonaws.com' },
 'Action': 'sts:AssumeRole' }],
        }
      ManagedPolicyArns:
        - !Sub arn:${AWS::Partition}:iam::aws:policy/SecurityAudit
      Policies:
        - PolicyName: AWSSecurityIncidentResponseContainmentExecutionPolicy
          PolicyDocument:
            {
              'Version': '2012-10-17',
              'Statement':
                [
                  {
                    'Sid': 'AllowIAMContainment',
                    'Effect': 'Allow',
                    'Action':
                      [
                        'iam:AttachRolePolicy',
                        'iam:AttachUserPolicy',
                        'iam:DeactivateMFADevice',
                        'iam:DeleteLoginProfile',
                        'iam:DeleteRolePolicy',
                        'iam:DeleteUserPolicy',
                        'iam:GetLoginProfile',
                        'iam:GetPolicy',
                        'iam:GetRole',
                        'iam:GetRolePolicy',
                        'iam:GetUser',
                        'iam:GetUserPolicy',
                        'iam:ListAccessKeys',
                        'iam:ListAttachedRolePolicies',
                        'iam:ListAttachedUserPolicies',
                        'iam:ListMfaDevices',
                        'iam:ListPolicies',
                        'iam:ListRolePolicies',
                        'iam:ListUserPolicies',
                        'iam:ListVirtualMFADevices',
                        'iam:PutRolePolicy',
```

```
                'iam:PutUserPolicy',
                'iam:TagMFADevice',
                'iam:TagPolicy',
                'iam:TagRole',
                'iam:TagUser',
                'iam:UntagMFADevice',
                'iam:UntagPolicy',
                'iam:UntagRole',
                'iam:UntagUser',
                'iam:UpdateAccessKey',
                'identitystore:CreateGroupMembership',
                'identitystore:DeleteGroupMembership',
                'identitystore:IsMemberInGroups',
                'identitystore:ListUsers',
                'identitystore:ListGroups',
                'identitystore:ListGroupMemberships',
              ],
            'Resource': '*',
          },
          {
            'Sid': 'AllowOrgListAccounts',
            'Effect': 'Allow',
            'Action': 'organizations:ListAccounts',
            'Resource': '*',
          },
          {
            'Sid': 'AllowSSOContainment',
            'Effect': 'Allow',
            'Action':
              [
                'sso:CreateAccountAssignment',
                'sso:DeleteAccountAssignment',
                'sso:DeleteInlinePolicyFromPermissionSet',
                'sso:GetInlinePolicyForPermissionSet',
                'sso:ListAccountAssignments',
                'sso:ListInstances',
                'sso:ListPermissionSets',
                'sso:ListPermissionSetsProvisionedToAccount',
                'sso:PutInlinePolicyToPermissionSet',
                'sso:TagResource',
                'sso:UntagResource',
              ],
            'Resource': '*',
          },
```

```
                {
                  'Sid': 'AllowSSORead',
                  'Effect': 'Allow',
                  'Action': ['sso-directory:SearchUsers', 'sso-
directory:DescribeUser'],
                  'Resource': '*',
                },
                {
                  'Sid': 'AllowS3Read',
                  'Effect': 'Allow',
                  'Action':
                    [
                      's3:GetAccountPublicAccessBlock',
                      's3:GetBucketAcl',
                      's3:GetBucketLocation',
                      's3:GetBucketOwnershipControls',
                      's3:GetBucketPolicy',
                      's3:GetBucketPolicyStatus',
                      's3:GetBucketPublicAccessBlock',
                      's3:GetBucketTagging',
                      's3:GetEncryptionConfiguration',
                      's3:GetObject',
                      's3:GetObjectAcl',
                      's3:GetObjectTagging',
                      's3:GetReplicationConfiguration',
                      's3:ListBucket',
                      's3express:GetBucketPolicy',
                    ],
                  'Resource': '*',
                },
                {
                  'Sid': 'AllowS3Write',
                  'Effect': 'Allow',
                  'Action':
                    [
                      's3:CreateBucket',
                      's3:DeleteBucketPolicy',
                      's3:DeleteObjectTagging',
                      's3:PutAccountPublicAccessBlock',
                      's3:PutBucketACL',
                      's3:PutBucketOwnershipControls',
                      's3:PutBucketPolicy',
                      's3:PutBucketPublicAccessBlock',
                      's3:PutBucketTagging',
```

```
                'Resource': '*',
            },
            {
                'Sid': 'AllowAutoScalingWrite',
                'Effect': 'Allow',
                'Action':
                    [
                        'autoscaling:CreateOrUpdateTags',
                        'autoscaling:DeleteTags',
                        'autoscaling:DescribeAutoScalingGroups',
                        'autoscaling:DescribeAutoScalingInstances',
                        'autoscaling:DescribeTags',
                        'autoscaling:EnterStandby',
                        'autoscaling:ExitStandby',
                        'autoscaling:UpdateAutoScalingGroup',
                    ],
                'Resource': '*',
            },
            {
                'Sid': 'AllowEC2Containment',
                'Effect': 'Allow',
                'Action':
                    [
                        'ec2:AuthorizeSecurityGroupEgress',
                        'ec2:AuthorizeSecurityGroupIngress',
                        'ec2:CopyImage',
                        'ec2:CreateImage',
                        'ec2:CreateSecurityGroup',
                        'ec2:CreateSnapshot',
                        'ec2:CreateTags',
                        'ec2:DeleteSecurityGroup',
                        'ec2:DeleteTags',
                        'ec2:DescribeImages',
                        'ec2:DescribeInstances',
                        'ec2:DescribeSecurityGroups',
                        'ec2:DescribeSnapshots',
                        'ec2:DescribeTags',
```

```
                    'ec2:ModifyNetworkInterfaceAttribute',
                    'ec2:RevokeSecurityGroupEgress',
                ],
                'Resource': '*',
            },
            {
                'Sid': 'AllowKMSActions',
                'Effect': 'Allow',
                'Action':
                [
                    'kms:CreateGrant',
                    'kms:DescribeKey',
                    'kms:GenerateDataKeyWithoutPlaintext',
                    'kms:ReEncryptFrom',
                    'kms:ReEncryptTo',
                ],
                'Resource': '*',
            },
            {
                'Sid': 'AllowSSMActions',
                'Effect': 'Allow',
                'Action': ['ssm:DescribeAutomationExecutions'],
                'Resource': '*',
            },
        ],
    }
```

取消会员资格

拥有 AWS 安全事件响应 服务 CancelMembership 权限的角色，可通过控制台、API 或 AWS Command Line Interface取消会员资格。

> **Important**
>
> 取消成员资格后，您将无法查看历史案例数据。当您取消某个成员资格时，您的成员资格将被立即删除，并且您将不再能够查看有关该成员资格的案例。所有处于 `Active` 或 `ready to close` 状态的资源或调查都将在成员资格取消时终止。

当您取消会员资格时：

您的成员资格将被删除，并且您将无法进一步访问有关该成员资格的案例。

> **Important**
>
> 如果重新订阅服务，系统会创建新的成员资格，原成员资格下的案例资源仅可在取消前下载方可访问。

成员资格取消后，系统会通过电子邮件通知该成员资格事件响应团队的所有人。

> **Important**
>
> 如果使用委派管理员账户创建成员资格，并通过 AWS Organizations API 删除该账户的委派管理员身份，则相关成员资格会立即终止。

为 AWS 安全事件响应 资源添加标签

标签是您或 AWS 为 AWS 资源分配的元数据标记。每个标签均包含一个键和一个值。对于您分配的标签，需要定义键和值。例如，您可以将键定义为 `stage`，将一个资源的值定义为 `test`。

标签可帮助您：

- 标识和整理您的 AWS 资源。许多 AWS 服务都支持添加标签，因此，您可以将同一标签分配给来自不同服务的资源，以表明这些资源相互之间存在关系。
- 跟踪您的 AWS 成本。您可以在 AWS Billing 控制面板上激活这些标签。AWS 使用标签对您的成本进行分类，并向您提供每月成本分配报告。有关更多信息，请参阅《AWS Billing User Guide》中的 Use cost allocation tags。
- 控制对 AWS 资源的访问。有关更多信息，请参阅《IAM 用户指南》https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html中的使用标签控制访问。

有关标记，请参阅 AWS 安全事件响应 API 参考。

结合使用 AWS CloudShell 和 AWS 安全事件响应

AWS CloudShell 是一个已经事先完成身份验证的浏览器式 Shell，您可以直接从 AWS 管理控制台启动它。您可以使用自己惯用的 Shell（Bash、PowerShell 或 Z Shell），在 AWS 服务（包括 AWS 安全事件响应）中运行 AWS CLI 命令。您无需下载或安装命令行工具，即可完成此操作。

您可以 从 AWS 管理控制台 启动 AWS CloudShell，用于登录控制台的 AWS 凭证将在新的 Shell 会话中自动可用。通过对 AWS CloudShell 用户进行这种预身份验证，您可在使用 AWS CLI 版本 2（在 Shell 的计算环境中预装）与安全事件响应等 AWS 服务进行交互时跳过凭证配置步骤。

内容

获取 AWS CloudShell 的 IAM 权限

使用 AWS Identity and Access Management 提供的访问管理资源，管理员可以向 IAM 用户授予权限，使其能够访问 AWS CloudShell 并使用环境的功能。

管理员要向用户授予访问权限，最快捷的方法是通过 AWS 托管式策略。AWS 托管式策略是由 AWS 创建和管理的独立策略。可以将以下适用于 CloudShell 的 AWS 托管式策略附加到 IAM 身份：

- `AWSCloudShellFullAccess`：授予使用 AWS CloudShell 的权限，并具有对所有功能的完全访问权限。

如果要限制 IAM 用户可以使用 AWS CloudShell 执行的操作范围，则可以 `AWSCloudShellFullAccess` 托管式策略为模板创建使用的定义策略。要详细了解如何限制用户可在 CloudShell 中使用的操作，请参阅《AWS CloudShell 用户指南》中的 Managing AWS CloudShell access and usage with IAM policies。

> **Note**
>
> 您的 IAM 身份还需要一个策略来授予对安全事件响应进行调用的权限。

使用 AWS CloudShell 与安全事件响应进行交互

在 AWS 管理控制台启动 AWS CloudShell 后，您可以立即开始使用命令行界面与安全事件响应进行交互。

> **Note**
>
> 在 AWS CloudShell 中使用 AWS Command Line Interface 时，无需下载或安装任何其他资源。此外，由于已经在 Shell 中进行了身份验证，因此在进行调用之前无需配置凭证。

结合使用 AWS CloudShell 和安全事件响应

1. 从 AWS 管理控制台选择导航栏提供的下列可用选项，从而启动 CloudShell：
   - 选择 CloudShell 图标。
   - 首先在搜索框中键入“cloudshell”，然后选择 CloudShell 选项。
2. 使用标准 AWS Command Line Interface 与 AWS 安全事件响应进行交互。有关可用 CLI 命令的完整参考，请参阅 AWS 安全事件响应 AWS CLI 命令参考。

使用 AWS CloudTrail 记录 AWS 安全事件响应 API 调用

AWS 安全事件响应与 AWS CloudTrail 集成，后者可提供用户、角色或 AWS 服务在安全事件响应中所执行操作的记录。CloudTrail 会将安全事件响应的所有 API 调用作为事件捕获。捕获的调用包括来自安全事件响应控制台的调用以及对安全事件响应 API 操作的代码调用。如果您创建跟踪记录，可以将 CloudTrail 事件持续传送到 Amazon S3 存储桶（包括安全事件响应的事件）。如果您不配置跟踪，则仍可在 CloudTrail 控制台中的事件历史记录中查看最新事件。使用 CloudTrail 收集的信息，您可以确定向安全事件响应发出了什么请求、发出请求的 IP 地址、请求方、请求时间以及其他详细信息。

要了解有关 CloudTrail 的更多信息，请参阅 AWS CloudTrail 用户指南。

CloudTrail 中的安全事件响应信息

在您创建 AWS 账户时，将在该账户上启用 CloudTrail。安全事件响应中发生活动时，该活动将记录在 CloudTrail 事件中，并与其他 AWS 服务事件一同保存在事件历史记录中。您可以在 AWS 账户 中查看、搜索和下载最新事件。有关更多信息，请参阅使用 CloudTrail 事件历史记录查看事件。

要持续记录您的 AWS 账户 过去 90 天的事件，请创建跟踪或 CloudTrail Lake 事件数据存储。

CloudTrail 跟踪

通过跟踪记录，CloudTrail 可将日志文件传送至 Simple Storage Service (Amazon S3) 存储桶。使用 AWS 管理控制台 创建的所有跟踪均具有多区域属性。您可以通过使用 AWS CLI 创建单区域或多区域跟踪。建议创建多区域跟踪，因为您可记录您账户中的所有 AWS 区域 的活动。如果您创建单区域跟踪，则只能查看跟踪的 AWS 区域 中记录的事件。有关跟踪的更多信息，请参阅《AWS CloudTrail 用户指南》中的为您的 AWS 账户 创建跟踪和为组织创建跟踪。

通过创建跟踪，您可以从 CloudTrail 免费向您的 Amazon S3 存储桶传送一份正在进行的管理事件的副本，但会收取 Amazon S3 存储费用。有关 CloudTrail 定价的更多信息，请参阅 AWS CloudTrail 定价。有关 Amazon S3 定价的信息，请参阅 Amazon S3 定价。

CloudTrail Lake 事件数据存储

CloudTrail Lake 允许您对事件运行基于 SQL 的查询。CloudTrail Lake 可将基于行的 JSON 格式的现有事件转换为 Apache ORC 格式。ORC 是一种针对快速检索数据进行优化的列式存储格式。事件将被聚合到事件数据存储中，它是基于您通过应用高级事件选择器选择的条件的不可变的事件集合。应用于事件数据存储的选择器用于控制哪些事件持续存在并可供您查询。有关 CloudTrail Lake 的更多信息，请参阅《AWS CloudTrail 用户指南》中的使用 AWS CloudTrail Lake。

CloudTrail Lake 事件数据存储和查询会产生费用。创建事件数据存储时，您可以选择要用于事件数据存储的定价选项。定价选项决定了摄取和存储事件的成本，以及事件数据存储的默认和最长保留期。有关 CloudTrail 定价的更多信息，请参阅 AWS CloudTrail 定价。

CloudTrail 会记录所有的安全事件响应操作，《AWS Security Incident Response API Reference》中介绍了这些操作。例如，对 `CreateMembership`、`CreateCase` 和 `UpdateCase` 操作的调用会在 CloudTrail 日志文件中生成条目。

每个事件或日志条目都包含有关生成请求的人员信息。身份信息可帮助您确定以下内容：

- 请求是使用根用户凭证还是 AWS Identity and Access Management（IAM）用户凭证发出的。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解安全事件响应日志文件条目

跟踪是一种配置，可用于将事件作为日志文件传送到您指定的 Amazon S3 存储桶。CloudTrail 日志文件包含一个或多个日记账条目。一个事件表示来自任何源的一个请求，包括有关所请求的操作、操作的日期和时间、请求参数等方面的信息。CloudTrail 日志文件不是公用 API 调用的有序堆栈跟踪，因此它们不会按任何特定顺序显示。

以下示例是演示 CreateCase 操作的 CloudTrail 日志条目。


```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA00000000000000000:user",
        "arn": "arn:aws:sts::123412341234:assumed-role/Admin/user",
        "accountId": "123412341234",
        "accessKeyId": "****",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA00000000000000000",
                "arn": "arn:aws:iam::123412341234:role/Admin",
                "accountId": "123412341234",
                "userName": "Admin"
```

```
            },
            "attributes": {
                "creationDate": "2024-10-13T06:32:53Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2024-10-13T06:40:45Z",
    "eventSource": "security-ir.amazonaws.com",
    "eventName": "CreateCase",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "1.2.3.4",
    "userAgent": "aws-cli/2.17.23 md/awscrt#0.20.11 ua/2.0 os/macos#23.6.0 md/
arch#x86_64 lang/python#3.11.9 md/pyimpl#CPython cfg/retry-mode#standard md/
installer#exe md/prompt#off md/command#security-ir.create-case",
    "requestParameters": {
        "impactedServices": [
            "Amazon GuardDuty"
        ],
        "impactedAccounts": [],
        "clientToken": "testToken112345679",
        "resolverType": "Self",
        "description": "***",
        "engagementType": "Investigation",
        "watchers": [
            {
                "email": "***",
                "name": "***",
                "jobTitle": "***"
            }
        ],
        "membershipId": "m-r1abcdabcd",
        "title": "***",
        "impactedAwsRegions": [
            {
                "region": "ap-southeast-1"
            }
        ],
        "reportedIncidentStartDate": 1711553521,
        "threatActorIpAddresses": [
            {
                "ipAddress": "***",
                "userAgent": "browser"
            }
```

```
        ]
    },
    "responseElements": {
        "caseId": "0000000001"
    },
    "requestID": "2db4b08d-94a9-457a-9474-5892e6c8191f",
    "eventID": "b3fa3990-db82-43be-b120-c81262cc2f19",
    "readOnly": false,
    "resources": [
        {
            "accountId": "123412341234",
            "type": "AWS::SecurityResponder::Case",
            "ARN": "arn:aws:security-ir:us-east-1:123412341234:case/*"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "123412341234",
    "eventCategory": "Management"
}
```

使用 AWS Organizations 管理 AWS 安全事件响应账户

AWS 安全事件响应 已与 AWS Organizations 集成。只有组织的 AWS Organizations 管理账户可以指定某个账户作为 AWS 安全事件响应的委托管理员账户。此操作会启用 AWS 安全事件响应作为 AWS Organizations 中的可信服务。有关如何授予这些权限的信息，请参阅 Using AWS Organizations with other AWS services。

以下章节将介绍安全事件响应委托管理员账户可以执行的各种任务。

内容

将 AWS 安全事件响应与 AWS Organizations 结合使用的注意事项和建议

以下注意事项和建议有助您了解安全事件响应委托管理员账户在 AWS 安全事件响应中的工作原理：

AWS 安全事件响应委托管理员账户。

> 您可以将某个成员账户指定为安全事件响应委托管理员账户。例如，假设您在*#########*区域指定了一个成员账户 *111122223333*，则无法在*#######*区域指定另一个成员账户 *555555555555*。但您必须在所有其他区域将同一账户作为安全事件响应委托管理员账户。

您可以在特定 AWS 区域 中设置安全事件响应委托管理员账户。

> 在初始设置期间，您可以在一个 AWS 区域 中指定委托的安全事件响应管理员账户。尽管设置是区域性的，但 AWS 安全事件响应 在所有支持的 AWS 区域 中提供组织范围的覆盖。从所有支持的 AWS 区域 中提取来自 Amazon GuardDuty 和 AWS Security Hub CSPM 的安全调查发现，并且在您激活订阅的区域中集中管理案例。必须通过 AWS Organizations 添加安全事件响应委托管理员账户和成员账户。

不建议将组织的管理账户设置为安全事件响应委托管理员账户。

组织的管理账户可以是委托的安全事件响应管理员账户。但是，AWS 安全最佳实践遵循最低权限原则，不建议使用此配置。

从实时订阅中删除安全事件响应委托管理员账户会立即取消订阅。

如果您删除安全事件响应委托管理员账户，AWS 安全事件响应 将删除与该安全事件响应委托管理员账户关联的所有成员账户。将不再为所有成员账户启用 AWS 安全事件响应。

启用 AWS 账户管理的可信访问权限

启用 AWS 安全事件响应的可信访问权限可让管理账户的委托管理员修改 AWS Organizations 中每个成员账户的特定信息和元数据（例如，主要联系人或备用联系人详细信息）。

请按照以下步骤在组织中启用 AWS 安全事件响应的可信访问权限。

最小权限

要执行这些任务，您必须满足以下要求：

- 只能从组织的管理账户执行此操作。
- 您的组织必须已启用所有功能。

Console

启用 AWS 安全事件响应的可信访问权限

1. 登录 AWS Organizations 控制台。您必须以 IAM 用户的身份登录，担任 IAM 角色；或在组织的管理账户中以根用户的身份登录（不推荐）。
2. 在导航窗格中，选择服务。
3. 在服务列表中选择 AWS 安全事件响应。
4. 选择 Enable trusted access (启用可信访问)。
5. 在为 AWS 安全事件响应 启用可信访问对话框中，键入启用进行确认，然后选择启用可信访问。

API/CLI

启用 AWS 账户管理的可信访问权限

运行以下命令后，就可以使用组织管理账户中的凭证调用账户管理 API 操作，这些操作使用 `--accountId` 参数来引用组织中的成员账户。

- AWS CLI：enable-aws-service-access

  以下示例在调用账户的组织中启用了 AWS 安全事件响应的可信访问权限。

```
$ aws organizations enable-aws-service-access \
                                        --service-principal security-
ir.amazonaws.com
```

  如果成功，此命令不会产生任何输出。

指定安全事件响应委托管理员账户所需的权限

您可以选择使用 AWS Organizations 委托管理员来设置 AWS 安全事件响应会员资格。有关如何授予这些权限的信息，请参阅 Using AWS Organizations with other AWS services。

> **Note**
>
> AWS 安全事件响应会在使用控制台进行设置和管理时，自动启用 AWS Organizations 信任关系。如果您使用 CLI/SDK，则必须使用 EnableAWSServiceAccess API 手动启用此功能才能信任 `security-ir.amazonaws.com`。

作为 AWS Organizations 管理员，在为组织指定安全事件响应委托管理员账户之前，请先验证您是否可以执行以下 AWS 安全事件响应操作：`security-ir:CreateMembership` 和 `security-ir:UpdateMembership`。这些操作可让您使用 AWS 安全事件响应为组织指定安全事件响应委托管理员账户。此外还必须确保您有权执行 AWS Organizations 操作，这将有助您检索有关组织的信息。

要授予这些权限，请在您的账户的 AWS Identity and Access Management (IAM) 策略中包括以下语句：

```
        {
```

```
            "Sid": "PermissionsForSIRAdmin",
            "Effect": "Allow",
            "Action": [
                "security-ir:CreateMembership",
                "security-ir:UpdateMembership",
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
```

如果要将您的 AWS Organizations 管理账户指定为安全事件响应委托管理员账户，您的账户还需要执行以下 IAM 操作：`CreateServiceLinkedRole`。请先查看将 AWS 安全事件响应与 AWS Organizations 结合使用的注意事项和建议，然后再继续添加权限。

要继续将 AWS Organizations 管理账户指定为安全事件响应委托管理员账户，请将以下语句添加到 IAM 策略中并将 *111122223333* 替换为 AWS Organizations 管理账户的 AWS 账户 ID：

```
        {
         "Sid": "PermissionsToEnableSecurityIncidentResponse"
         "Effect": "Allow",
         "Action": [
          "iam:CreateServiceLinkedRole"
         ],
         "Resource": "arn:aws:iam::111122223333:role/aws-service-role/security-
ir.amazonaws.com/AWSServiceRoleForSecurityIncidentResponse",
         "Condition": {
          "StringLike": {
           "iam:AWSServiceName": "security-ir.amazonaws.com"
          }
         }
        }
```

指定 AWS 安全事件响应委托管理员账户

本节介绍了在 AWS 安全事件响应组织中指定委托管理员的步骤。

作为 AWS 组织的管理员，请务必通读有关安全事件响应委托管理员账户工作原理的注意事项和建议。在继续操作之前，请确保您拥有指定安全事件响应委托管理员账户所需的权限。

选择一种您偏好的访问方法，为组织指定安全事件响应委托管理员账户。只有管理账户才能执行此步骤。

Console

1. 在 https://console.aws.amazon.com/security-ir/ 上打开安全事件响应控制台

   若要登录，请使用 AWS Organizations 组织的管理账户凭证。
2. 使用页面右上角的 AWS 区域选择器，选择您要在其中为组织指定安全事件响应委托管理员账户的区域。
3. 按照设置向导创建您的会员资格，包括委托管理员账户。

API/CLI

- 使用组织管理 AWS 账户的凭证运行 CreateMembership。
  - 或者，您可以使用 AWS Command Line Interface 来执行此操作。以下 AWS CLI 命令会指定安全事件响应委托管理员账户。以下是可用于配置会员资格的字符串选项：

```
                                        {
                                          "customerAccountId": "stringstring",
                                          "membershipName": "stringstring",
                                          "customerType": "Standalone",
                                          "organizationMetadata": {
                                            "organizationId": "string",
                                            "managementAccountId":
"stringstring",
                                            "delegatedAdministrators": [
                                              "stringstring"
                                            ]
                                          },
                                          "membershipAccountsConfigurations":
{
                                            "autoEnableAllAccounts": true,
```

```
      "organizationalUnits": [
        "string"
      ]
    },
    "incidentResponseTeam": [
      {
        "name": "string",
        "jobTitle": "stringstring",
        "email": "stringstring"
      }
    ],
    "internalIdentifier": "string",
    "membershipId": "stringstring",
    "optInFeatures": [
      {
        "featureName": "RuleForwarding",
        "isEnabled": true
      }
    ]
}
```

如果未为安全事件响应委托管理员账户启用 AWS 安全事件响应，该账户将无法执行任何操作。如果尚未启用，请确保为新指定的安全事件响应委托管理员账户启用 AWS 安全事件响应。

使用 AWS 安全事件响应 的组织单元（OU）管理会员资格

AWS 安全事件响应 支持单独组织单元（OU）的会员资格覆盖。您随时可以更新您的会员资格，使其覆盖特定的 OU。所选 OU 中的所有账户，包括子 OU 下的账户，都将受您的会员资格覆盖。

更新您的会员资格关联时，一次最多可以为 5 个 OU 应用更新。如果您希望对 5 个以上的 OU 进行更改，请每 5 个 OU 分成一批完成关联更改，直到所有更新都完成。

Console

1. 在 https://console.aws.amazon.com/security-ir/ 上打开安全事件响应控制台

   若要登录，请使用 AWS Organizations 组织的管理账户凭证。
2. 导航到管理会员资格 > 账户
3. 单击更新关联

4. 选择选择组织单元（OU）
5. 选择添加 OU 或删除 OU
6. 最多选择 5 个您要更新的 OU。您不能同时添加和删除 OU。

> **Note**
>
> 选定 OU 下的所有账户和子 OU 都将关联。

7. 单击更新关联
8.

> **Note**
>
> 如果要对超过 5 个 OU 进行更改，请重复步骤 5 和 6，直到所有 OU 都已关联。

要了解有关在 AWS 组织内进行 OU 更改的更多信息，请参阅使用 AWS Organizations 管理组织单元（OU）。

向 AWS 安全事件响应添加成员

AWS Organizations 与 AWS 安全事件响应会员资格之间是一对一的关系。在您的组织或组织单元（OU）中添加（或删除）账户后，您的 AWS 安全事件响应 会员资格覆盖的账户中就会反映出这些更改。

要将账户添加到您的会员资格，请按照使用 AWS Organizations 管理组织中的账户中的选项之一进行操作。

您也可以随时向您的会员资格添加其他 OU，请参阅使用组织单元（OU）管理会员资格。

从 AWS 安全事件响应中删除成员

要从您的会员资格中删除账户，您可以从组织中删除成员账户，将账户移出选定的 OU，或者从您的会员资格中删除 OU。

要从您的会员资格中删除某个账户，请按照从组织中删除成员账户的步骤进行操作。

要将账户移出 OU，请按照使用 AWS Organizations 将账户移动到某个组织单元（OU）或者在根和 OU 之间移动的程序进行操作。

要从您的会员资格中删除 OU，请按照使用组织单元（OU）管理会员资格的程序进行操作。

Amazon EventBridge

使用 Amazon EventBridge 可以响应、监控和协调与 AWS 安全事件响应案例和会员资格相关的事件。您可以通过规则（适用于扇出场景，一个或多个目标）或管道（适用于具有增强型筛选、富集和转换功能的点对点集成）来路由这些事件。

您可以在安全事件响应和第三方工具之间创建集成，也可以使用生成式人工智能和其他 AWS 工具聚合数据进行分析。例如，当安全事件响应主动创建案例时，您可以使用 EventBridge 自动化来触发系统以通知利益相关者。此外，如果您管理多个 AWS 环境，则可以使用 Amazon EventBridge 集成来监控 AWS 安全事件响应会员资格，以确保所有环境都维持强大的安全态势。

有关更多信息，请参阅 What is Amazon EventBridge?

> **Note**
>
> 有关 AWS 安全事件响应与 Amazon EventBridge 集成（包括 ITSM 集成）的最新更新，请参阅“AWS 新增内容”页面上的 AWS 安全事件响应现在支持 ITSM 集成。

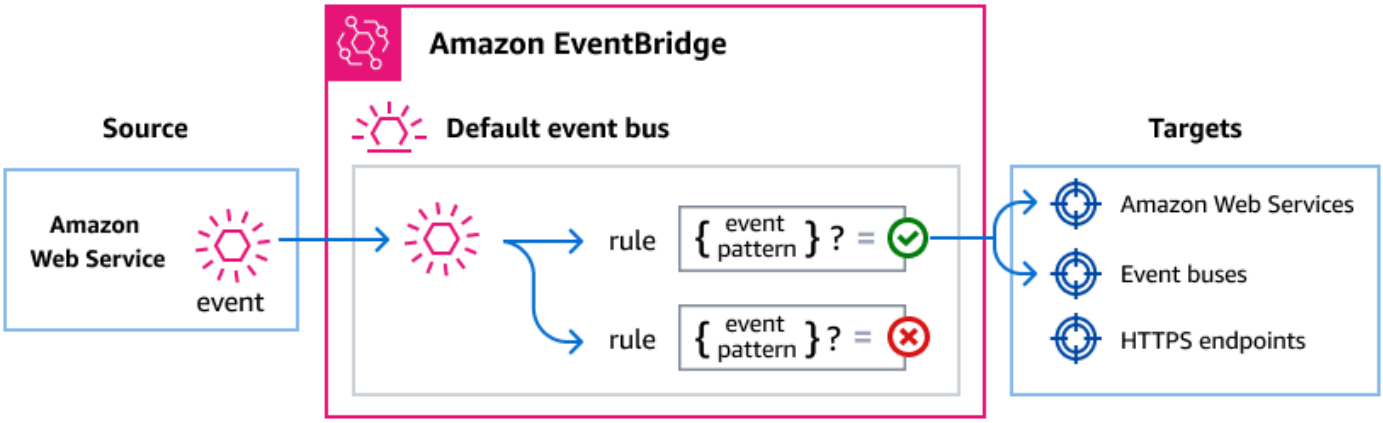
内容

使用 Amazon EventBridge 管理安全事件响应事件

Amazon EventBridge 是一项无服务器服务，使用事件将应用程序组件连接在一起，可让您更轻松地构建可扩展的事件驱动型应用程序。事件驱动型架构是一种构建松耦合软件系统的风格，这些系统通过发出和响应事件来协同工作。事件代表资源或环境中的变化。

下面将介绍操作方式：

与许多 AWS 服务一样，安全事件响应会生成事件并将其发送到 EventBridge 的默认事件总线。（默认事件总线会在您的 AWS 账户中自动预置。）事件总线是接收事件并将其传送到零个或多个目的地或目标的路由器。为事件总线指定的规则会在事件到达时进行评估。每条规则都会检查事件是否与规则的事件模式相匹配。如果事件确实匹配，事件总线会将事件发送到指定的目标。



使用 EventBridge 规则传送安全事件响应事件

要让 EventBridge 默认事件总线将安全事件响应事件发送到目标，必须创建规则。每条规则都包含一个事件模式，EventBridge 将其与在事件总线上接收到的每个事件进行匹配。如果事件数据与指定的事件模式匹配，EventBridge 会将该事件传送给规则的目标。

有关创建事件总线规则的全面说明，请参阅《Amazon EventBridge User Guide》中的 Creating rules that react to events。

创建与安全事件响应事件相匹配的事件模式

每个事件模式是一个 JSON 对象，其中包含：

- 标识发送事件的服务的 `source` 属性。对于安全事件响应事件，来源是 `"aws.security-ir"`。
- （可选）：包含要匹配的事件类型数组的 `detail-type` 属性。
- （可选）：包含要匹配的其他事件数据的 `detail` 属性。

例如，以下事件模式与特定 AWS 账户的所有 `Case Updated by AWS ###### Service` 事件相匹配：

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
```

```
    "time": "2023-05-12T03:45:00Z",
    "region": "us-west-2",
    "resources": [
      "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
    ],
    "detail": {
      "caseId": "1234567890",
      "updatedBy": "security-ir.amazonaws.com"
    }
  }
```

有关写入事件模式的更多信息，请参阅《EventBridge 用户指南》中的 Event patterns。

安全事件响应事件详细信息参考

来自 AWS 服务的所有事件都有一组公共字段，其中包含有关事件的元数据，例如作为事件来源的 AWS 服务、事件的生成时间、事件发生的账户和区域。有关这些常规字段的定义，请参阅《Amazon EventBridge User Guide》中的 Event structure reference。

此外，每个事件都有一个 `detail` 字段，其中包该特定事件专有的数据。下面的引用内容定义了各种安全事件响应事件的详细信息字段。

在使用 EventBridge 选择和管理安全事件响应事件时，请记住以下几点：

- 安全事件响应中所有事件的 `source` 字段均设置为 `"aws.security-ir"`。
- `detail-type` 字段指定事件类型。

  例如 `"Case Updated"`。
- `detail` 字段包含该特定事件专有的数据。

有关如何构造使规则能够与安全事件响应事件匹配的事件模式的信息，请参阅《Amazon EventBridge User Guide》中的 Event patterns。

有关事件以及 EventBridge 如何处理事件的更多信息，请参阅《Amazon EventBridge 用户指南》中的 EventBridge 事件。

常用字段：所有 AWS 安全事件响应事件都包含这些标准的 Amazon EventBridge 字段

- version：EventBridge 事件格式版本
- id：事件的唯一标识符

- detail-type：人类可读的事件类型描述
- source：对于安全事件响应事件，始终是“aws.security-ir”
- account：发生事件的 AWS 账户 ID
- time：事件发生时的 ISO 8601 时间戳
- region：资源所在的 AWS 区域
- resources：包含受影响资源 ARN 的数组

详细信息字段：`detail` 对象包含特定于安全事件响应的信息

- caseId：案例的唯一标识符（仅限案例事件）
- membershipId：会员资格的唯一标识符（仅限会员事件）
- updatedBy：执行了更新的人员（仅限案例和评论更新事件）
- createdBy：创建了实体的人员（仅限案例和评论创建事件）

操作人员值：`updatedBy` 和 `createdBy` 字段可能包含

- AWS Responder：AWS 安全响应者执行的操作
- *`security-ir.amazonaws.com`*：服务自动执行的操作
- Account ID：客户执行的操作（例如，“111122223333”）

资源 ARN 值：AWS 安全事件响应资源会使用以下 ARN 格式

- Cases：`arn:aws:security-ir:{region}:{account-id}:case/{case-id}`
- Memberships：`arn:aws:security-ir:{region}:{account-id}:membership/{membership-id}`

案例事件

AWS 响应者创建的案例

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
```

```
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

服务创建的案例

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

客户创建的案例

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Created",
  "source": "aws.security-ir",
```

```
  "account": "111122223333",
  "time": "2023-05-12T00:00:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

AWS 响应者更新的案例

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T01:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "AWS Responder"
  }
}
```

AWS 客户更新的案例

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
```

```
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

AWS 安全事件响应服务更新的案例

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T03:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

已关闭的案例

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Closed",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-15T14:22:00Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890"
  }
}
```

案例评论事件

AWS 响应者创建的案例评论

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T04:30:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "AWS Responder"
  }
}
```

客户创建的案例评论

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
```

```
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "111122223333"
  }
}
```

AWS 安全事件响应服务创建的案例评论

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Created",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:15:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "createdBy": "security-ir.amazonaws.com"
  }
}
```

客户更新的案例评论

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
```

```
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "111122223333"
  }
}
```

AWS 安全事件响应服务更新的案例评论

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
  ],
  "detail": {
    "caseId": "1234567890",
    "updatedBy": "security-ir.amazonaws.com"
  }
}
```

AWS 响应者创建的案例评论

```
{
  "version": "0",
  "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "detail-type": "Case Comment Updated",
  "source": "aws.security-ir",
  "account": "111122223333",
  "time": "2023-05-12T02:45:00Z",
  "region": "us-west-2",
  "resources": [
```

```
            "arn:aws:security-ir:us-west-2:111122223333:case/1234567890"
          ],
          "detail": {
            "caseId": "1234567890",
            "updatedBy": "AWS Responder"
          }
        }
```

会员资格事件

创建的会员资格

```
        {
          "version": "0",
          "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
          "detail-type": "Membership Created",
          "source": "aws.security-ir",
          "account": "111122223333",
          "time": "2023-04-01T10:00:00Z",
          "region": "us-west-2",
          "resources": [
            "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
          ],
          "detail": {
            "membershipId": "m-1234567890abcdef0"
          }
        }
```

更新的会员资格

```
        {
          "version": "0",
          "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
          "detail-type": "Membership Updated",
          "source": "aws.security-ir",
          "account": "111122223333",
          "time": "2023-04-15T16:30:00Z",
          "region": "us-west-2",
```

```
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

取消的会员资格

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Closed",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-06-30T23:59:59Z",
              "region": "us-west-2",
              "resources": [
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-1234567890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

终结的会员资格

```
            {
              "version": "0",
              "id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
              "detail-type": "Membership Terminated",
              "source": "aws.security-ir",
              "account": "111122223333",
              "time": "2023-07-01T00:00:00Z",
              "region": "us-west-2",
              "resources": [
```

```
                "arn:aws:security-ir:us-west-2:111122223333:membership/
m-123456s7890abcdef0"
              ],
              "detail": {
                "membershipId": "m-1234567890abcdef0"
              }
            }
```

使用 AWS 安全事件响应 事件

您可以创建 EventBridge 规则来匹配这些事件并触发自动操作。下面是一些使用使用案例：

匹配所有 AWS 安全事件响应事件：

```
        {
          "source": ["aws.security-ir"]
        }
```

仅匹配案例事件：

```
        {
          "source": ["aws.security-ir"],
          "detail-type": [
            "Case Created",
            "Case Updated",
            "Case Closed",
            "Case Comment Added",
            "Case Comment Updated"
          ]
        }
```

匹配 AWS 响应者更新的案例：

```
        {
          "source": ["aws.security-ir"],
```

```
    "detail-type": ["Case Updated"],
    "detail": {
      "updatedBy": ["AWS Responder"]
    }
  }
```

匹配特定案例的事件：

```
  {
    "source": ["aws.security-ir"],
    "detail": {
      "caseId": ["1234567890"]
    }
  }
```

教程：针对 **Membership Updated** 事件发送 Amazon Simple Notification Service 警报

在本教程中，您将学会如何配置 Amazon EventBridge 事件规则，以便只捕获订阅已转为 `Membership Updated` 状态的事件。

先决条件

本教程假定您的会员资格中拥有有效的订阅和活动的 AWS 账户。

主题

- 教程：创建并订阅 Amazon SNS 主题
- 教程：注册事件规则
- 教程：测试您的规则
- 替代规则：安全事件响应案例更新

教程：创建并订阅 Amazon SNS 主题

在本教程中，您配置一个 Amazon SNS 主题来充当新事件规则的事件目标。

创建 Amazon SNS 主题

1. 通过 https://console.aws.amazon.com/sns/v3/home 打开 Amazon SNS 控制台。
2. 依次选择 Topics (主题) 和 Create topic (创建主题)。
3. 对于类型，选择标准。
4. 对于名称，输入 **`MembershipUpdated`** 并选择创建主题。
5. 在 MembershipUpdated 屏幕上，选择创建订阅。
6. 对于协议，选择电子邮件。
7. 对于端点，输入您当前有权访问的电子邮件地址，然后选择 创建订阅。
8. 检查您的电子邮件账户，并等待接收订阅确认电子邮件。在收到此电子邮件后，选择 确认订阅。

教程：注册事件规则

接下来，注册一个仅捕获 `Membership Updated` 事件的事件规则。

注册您的 EventBridge 规则

1. 打开位于 https://console.aws.amazon.com/events/ 的 Amazon EventBridge 控制台。
2. 在导航窗格中，选择规则。
3. 选择创建规则。
4. 为规则输入名称和描述。

> **Note**
>
> 规则不能与同一区域中的另一个规则和同一事件总线上的名称相同。

5. 对于事件总线，请选择要与此规则关联的事件总线。如果您希望此规则对来自您自己的账户的匹配事件触发，请选择 AWS默认事件总线。当您账户中的某个 AWS 服务发出一个事件时，它始终会发送到您账户的默认事件总线。

> **Note**
>
> 这应该在您创建 AWS 安全事件响应会员资格的 AWS Organizations 或委托管理员账户中进行设置。

6. 对于规则类型，选择具有事件模式的规则。

7. 选择下一步。
8. 对于事件源，选择其他。
9. 对于事件模式，选择 自定义模式（JSON 编辑器）。
10. 在文本区域中粘贴以下事件模式。

```
{
  "source": ["aws.security-ir"],
  "detail-type": ["Membership Updated"]
}
```

此代码定义了一个与服务会员资格更新或修改事件匹配的 EventBridge 规则。有关事件模式的更多信息，请参阅 Amazon EventBridge 用户指南 中的 事件和事件模式。

11. 选择下一步。
12. 对于目标类型，选择AWS 服务。
13. 在选择目标中，选择 SNS 主题；在主题中，选择 MembershipUpdated。
14. （可选）对于 Additional settings（其他设置），执行以下操作：

    a. 对于 Maximum age of event（事件的最大时长），输入一分钟（00:01）与 24 小时（24:00）之间的值。

    b. 对于重试尝试，输入 0 到 185 之间的数字。

    c. 对于死信队列，选择是否使用标准 Amazon SQS 队列作为死信队列。如果与此规则匹配的事件未成功传递到目标，EventBridge 会将这些事件发送到死信队列。请执行以下操作之一：

    - 选择无不使用死信队列。
    - 选择在当前 AWS 账户中选择一个 Amazon SQS 队列用作死信队列，然后从下拉列表中选择要使用的队列。
    - 选择在其他 Amazon SQS 队列中选择其他队列 AWS 帐户作为死信队列，然后输入要使用的队列的 ARN。您必须将基于资源的策略附加到队列，以授予 EventBridge 向其发送消息的权限。有关更多信息，请参阅 Amazon EventBridge 用户指南中的授予死信队列的权限。

15. 选择下一步。
16. （可选）为规则输入一个或多个标签。有关更多信息，请参阅《Amazon EventBridge 用户指南》中的 Amazon EventBridge 标签。
17. 选择下一步。

18. 查看规则详细信息并选择创建规则。

教程：测试您的规则

要测试规则，需要向 AWS 安全事件响应会员资格提交更新。如果您的规则配置正确，您将在几分钟内收到包含事件文本的电子邮件消息。

替代规则：安全事件响应案例更新

要创建监控所有案例更新的事件规则，请重复教程中的步骤，并进行以下更改：

1. 在教程：创建并订阅 Amazon SNS 主题中，使用 *CaseUpdates* 作为主题名称。
2. 在 教程：注册事件规则 中，在 JSON 编辑器中使用以下模式：

```
{
  "source": ["aws.security-ir"],
  "detail-type": [
    "Case Created",
    "Case Updated",
    "Case Closed",
    "Case Comment Created",
    "Case Comment Updated"
  ]
}
```

故障排除

如果遇到与执行 AWS 安全事件响应特有的操作相关的问题，请参阅本部分的主题。

错误（ERROR）是指示操作故障的状态标识，表示部分或全部操作出现异常。另外，当任务中出现问题但任务仍然完成时，您也会收到警告提示。

内容

事务

未从正确的上下文发起请求。

调用 AWS 安全事件响应 API 的所有请求必须源自服务委托管理员账户或成员账户中的 IAM 主体。确保当前操作的 IAM 主体位于正确的 AWS 账户中，且该账户需已设置为贵组织 AWS 安全事件响应委托管理员账户或成员账户。

错误

AccessDeniedException

您没有足够的访问权限，无法执行该操作。

请与您的 AWS 管理员协作，确保自己具备在 AWS 安全事件响应应委托管理员账户或成员账户中担任 IAM 角色的权限。同时，请检查该角色是否关联允许请求操作的 IAM 策略。有关更多信息，请参阅 AWS 安全事件响应 IAM。

ConflictException

该请求导致系统状态不一致。

请检查您指定的所有案例附件文件名或默认响应团队成员是否具有唯一性。另请检查 AWS 安全事件响应会员资格是否尚未被配置。在 https://console.aws.amazon.com/security-ir/ 上打开安全事件响应控制台，导航到 `Membership Details`。

InternalServerException

请求处理过程中发生意外错误。请过几分钟再试。如果问题仍然存在，请向 支持 提交案例。

ResourceNotFoundException

请求引用的资源不存在。

您请求中指定的一个或多个资源不存在。请检查提供的所有资源 ARN 或 ID 是否正确，包括：AWS Organizations ID、账户 ID、IAM 角色、成员资格、案例、响应团队成员、案例响应人、案例附件、案例评论。

ThrottlingException

由于请求限制而导致请求被拒绝。

您的 IAM 主体在特定时间段内对该 API 功能的请求过于频繁。请稍等片刻，然后重试。如果问题仍然存在，建议采用指数回退重试机制。

ValidationException

输入未能满足 AWS 服务指定的约束条件。

您请求中的一个或多个数据字段未通过验证和/或逻辑组合要求。请检查所有资源 ARN 是否完整，文本值是否符合《AWS 安全事件响应 API 参考指南》中的大小和格式限制。也要检查是否允许任何值更新。例如，案例类型无法从 AWS 托管更改为自主管理。

支持

如需进一步协助，请联系 支持 Center 进行故障排查。请准备好以下信息：

- 您所使用的 AWS 区域
- 会员资格的 AWS 账户 账户 ID
- 您的来源内容（如果适用且可用）
- 可能帮助您排除所遇到问题的任何其他详细信息

安全性

主题

AWS 安全事件响应 中的数据保护

AWS 责任共担模型适用于 AWS 安全事件响应服务的数据保护。如该模式中所述，AWS 负责保护运行 AWS 云所提供服务的基础设施。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用 AWS 服务的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，AWS 最佳安全实践规定，您应保护 AWS 账户凭证并使用 AWS Identity Center 或 AWS Identity and Access Management（IAM）设置单独的用户。这样，每个用户只能获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与 AWS 资源进行通信。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用 AWS CloudTrail 设置 API 和用户活动日志记录。

- 使用 AWS 加密解决方案以及 AWS 服务中的所有默认安全控制。
- 此服务目前不支持 FIPS 140-3。

切勿将机密信息或敏感信息（如电子邮件地址）放入标签或自由格式文本字段（如名称字段）中。这包括使用控制台、API、AWS Command Line Interface 或 AWS SDK 处理 AWS 支持 或其他 AWS 服务时。在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，强烈建议您不要在 URL 中包含凭证信息来验证对该服务器的请求。

主题

数据加密

AWS 安全事件响应使用静态加密和传输中加密计数保护数据。所有数据均采用行业标准加密协议进行加密，以帮助您满足安全和合规性要求。

主题

静态加密

使用透明的服务器端加密，加密静态数据。这样可以帮助减少在保护敏感数据时涉及的操作负担和复杂性。通过静态加密，您可以构建符合加密合规性和法规要求的安全敏感型应用程序。

传输中加密

AWS 安全事件响应 收集和访问的数据仅通过受传输层安全性协议（TLS）保护的通道进行。

密钥管理

AWS 安全事件响应会实现与 AWS KMS 的集成，为案例和附件数据提供静态加密。

AWS 安全事件响应 不支持客户管理的密钥。

数据收集和使用

AWS 安全事件响应处理三类不同的数据，每类数据的收集方法、存储模式和区域行为都不同。了解这些类别对于评估安全事件响应如何符合您的合规性要求至关重要。

主题

案例调查数据

当您创建安全事件案例时，安全事件响应会从您的 AWS 环境收集日志和元数据以支持调查。此案例特定数据包括 API 日志、VPC 流日志、Amazon Route 53 DNS 查询、Amazon S3 访问事件、资源元数据（名称、标签和配置详细信息）以及案例信息（如评论和调查笔记）。

> **Important**
>
> 安全事件响应会收集有关您环境的活动模式和资源配置的信息。它不会收集 Amazon S3 存储桶、数据库记录或应用程序数据的实际内容。安全事件响应收集“谁在何时做了什么”，而不是底层数据本身。

此案例调查数据是针对特定事件按需收集的，并与您的案例保持关联。安全事件响应默认保留此数据 90 天，以便您能够查看调查历史记录、支持正在进行调查或后续调查，并满足审计和合规性文档要求。如果需要在 90 天期限到期之前删除数据，请联系 AWS 支持 申请提前删除。

安全调查发现数据

安全事件响应会跨已启用这些服务的所有受支持的 AWS 区域持续从 Amazon GuardDuty 和 AWS Security Hub CSPM 摄取安全调查发现元数据。此调查发现数据包括资源标识符、调查发现类型、严重性级别、受影响的资源和检测时间戳。与案例调查数据不同，系统会自动持续摄取调查发现数据，以使安全事件响应能够关联整个 AWS 环境中的威胁。

调查发现数据不包括生成调查发现的详细日志或原始数据，仅包括有关检测到的内容、检测位置和检测严重性的元数据。此元数据使安全事件响应能够识别模式、跨区域关联相关的安全事件并提供全面的威胁分析。

调查代理处理

由 Amazon Bedrock 提供支持的安全事件响应调查代理处理来自您的案例调查数据和调查发现数据的元数据，以生成见解、识别模式并建议响应操作。作为代理分析工作流的一部分，此处理在 Amazon Bedrock 的全球区域进行。

> **Important**
>
> 调查代理暂时处理元数据，不会将这些数据永久存储在 Amazon Bedrock 的全球区域。元数据仅用于生成调查见解，在处理完成后不会保留。

了解元数据敏感度

虽然安全事件响应不会收集您的应用程序数据，但它跨三个类别收集的元数据可能会泄露有关您的环境以及可能有关您的用户的敏感信息。考虑以下示例：

- 资源名称（例如 `patient-database-prod` 或 `financial-records-2026`）表示资源的用途和敏感性。
- `user12345.internal.app.com` 等 DNS 查询可能包含用户标识符或内部系统信息。
- API 调用模式可以揭示业务流程和操作工作流。

受监管行业的组织应评估此元数据是否符合其合规要求，即使它本身不是受监管的数据。

数据驻留和区域行为

安全事件响应中的三类数据具有不同的存储位置和区域移动模式。对于有数据驻留要求的组织而言，了解这些模式至关重要。

主题

案例调查数据存储和移动

案例调查数据仍保留在您创建安全事件案例的 AWS 区域。当您在特定区域创建案例时，为该调查收集的所有日志、元数据和案例信息都存储在该区域中。此数据不会移动到其他区域。

对于标准 AWS 区域（默认可用的区域），案例调查数据在整个调查生命周期和 90 天保留期内都保留在创建案例的区域中。

对于 AWS 选择加入区域，例如中东（巴林）、非洲（开普敦）或亚太地区（香港），案例调查数据也保留在创建案例的区域中。但是，如果在选择加入区域启用了安全事件响应，则该区域的所有案例数据都会自动复制到美国东部（弗吉尼亚州北部）区域（us-east-1），以便集中进行案例管理和分析。

> **Important**
>
> 如果在选择加入区域开展业务，则案例调查数据会自动流向 us-east-1。对数据驻留有严格要求的组织必须评估此跨区域复制是否符合其合规义务。数据永远不会在不同的选择加入区域之间流动，非选择加入区域的数据也永远不会复制到选择加入区域。

安全调查发现数据存储和移动

无论调查发现来自何处，安全调查发现元数据都会遍历区域。安全事件响应会跨已启用这些服务的区域从 Amazon GuardDuty 和 AWS Security Hub CSPM 摄取调查发现，并跨区域关联此元数据，以识别分布式威胁和攻击模式。

对于标准 AWS 区域，可以访问所有区域的调查发现元数据以进行关联和分析。此跨区域移动使安全事件响应能够检测到跨越多个区域的威胁，例如攻击者跨您的基础设施横向移动。

对于 AWS 选择加入区域，调查发现元数据遵循与案例调查数据相同的复制模式。来自选择加入区域的调查发现会复制到商业 AWS 区域（AWS GovCloud (US) 区域和中国地区以外的区域），以便与其他区域的调查发现一起集中进行分析。

调查发现元数据仅包括资源标识符、调查发现类型和严重性信息，不包括生成调查发现的详细日志或原始数据。此元数据能够实现威胁关联，同时最大限度地减少跨区域边界的数据量。

调查代理处理位置

无论案例或调查发现数据来自哪个区域，安全事件响应调查代理都会在 Amazon Bedrock 的全球区域处理元数据。此处理是暂时的，代理会分析元数据以生成见解和建议，但不会将元数据永久存储在 Amazon Bedrock 基础设施中。

代理完成其分析后，生成的见解和建议将与案例调查数据一起存储在创建案例的区域。分析完成后，用于处理的元数据不会保留在 Amazon Bedrock 全球区域。

区域可用性

有关哪些区域支持安全事件响应的信息，请参阅 AWS Regional Services。

数据访问与权限

两个组可以访问您的AWS 安全事件响应数据：

- 您的授权用户：您授予安全事件响应权限的 IAM 用户和角色。
- AWS 事件响应人员：调查您的案例的 AWS 员工和经过审查的承包商。

主题

AWS 事件响应人员访问

AWS 将安全事件响应作为“跟随太阳”服务运营，通过位于美洲、欧洲和亚太地区的事件响应人员提供全天候服务。当您创建安全事件案例时，为您的案例分配的响应人员可能位于这些区域中的任何一个。所有 AWS 事件响应人员在获得客户数据访问权限之前，都要接受背景调查并完成安全培训。

> **Important**
>
> 处理您案例的事件响应人员的地理位置可能会因您创建案例的时间和响应人员可用性而有所不同。对谁可以访问其数据有要求的组织应评估此全球访问模式是否符合其策略。

访问日志记录和可审计性

对安全事件响应数据的每次访问都会被记录下来。您可以审核谁访问了您的数据、访问了哪些数据以及访问的发生时间。这些审计日志支持您的合规性和安全监控要求。

使用 IAM 控制访问

您可以通过 IAM 策略控制您 AWS 账户中的哪些用户和角色可以访问安全事件响应。有关为安全事件响应配置 IAM 权限的信息，请参阅 身份和访问管理。

互联网络流量隐私

服务与本地客户端和应用之间的流量

私有网络和 AWS 之间有两种连接方式：

- AWS Site-to-Site VPN 连接。有关更多信息，请参阅 AWS Site-to-Site VPN 用户指南的 什么是 AWS Site-to-Site VPN？。
- Direct Connect 连接。有关更多信息，请参阅 Direct Connect 用户指南的 什么是 Direct Connect？。

通过网络访问 AWS 安全事件响应 是通过 AWS 发布的 API 进行的。客户端必须支持传输层安全性协议（TLS）1.2。我们建议使用 TLS 1.3。客户端还必须支持具有完全向前保密（PFS）的密码套件，例如 Ephemeral Diffie-Hellman（DHE）或 Elliptic Curve Diffie-Hellman Ephemeral（ECDHE）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。此外，必须使用与 IAM 主体关联的访问密钥 ID 和秘密访问密钥签名请求，或者可以使用 AWS Security Token Service（STS）生成临时安全证书来签名请求。

同一区域中 AWS 资源之间的流量

AWS 安全事件响应的 Amazon Virtual Private Cloud（Amazon VPC）端点是 VPC 内的逻辑实体，仅允许连接到 AWS 安全事件响应。Amazon VPC 会将请求路由到 AWS 安全事件响应并将响应路由回 VPC。有关更多信息，请参阅《Amazon VPC 用户指南》中的 VPC 端点。有关可以用于控制 VPC 端点访问的示例策略，请参阅使用 IAM 策略控制对 DynamoDB 的访问。

> **Note**
>
> 不能通过 AWS Site-to-Site VPN 或 Direct Connect 访问 Amazon VPC 端点。

身份和访问管理

AWS Identity and Access Management（IAM）是一项 AWS 服务，可帮助管理员控制对 AWS 资源的访问。IAM 管理员控制经过身份验证（登录）和经过授权（具有权限）的主体来使用 AWS 安全事件响应资源。IAM 是一项可以免费使用的 AWS 服务。

主题

- 使用身份进行身份验证
- AWS 安全事件响应 如何与 IAM 协同工作

受众

使用 AWS Identity and Access Management（IAM）的方式因您可以在 AWS 安全事件响应 中执行的操作而异。

安全管理员

建议这些用户使用 AWSSecurityIncidentResponseFullAccess 托管策略来确保拥有对会员资格和案例资源的读写权限。

案例观察者

这些人员不具有对所有案例的授权访问权限，只能访问您明确授予权限的个别案例。

事件响应团队成员

团队成员可以获得正式会员资格和案例访问权限。建议不要让所有个人都对服务会员资格有授权操作，但所有人都应有权访问通过该服务创建和管理的所有案例。有关更多信息，请参阅 AWS 安全事件响应托管策略。

使用身份进行身份验证

身份验证是您使用身份凭证登录 AWS 的方法。您必须作为 AWS 账户根用户、IAM 用户或通过代入 IAM 角色进行身份验证（登录到 AWS）。

您可以使用通过身份源提供的凭证以联合身份登录到 AWS。AWSIAM Identity Center（IAM Identity Center）用户、您公司的单点登录身份验证以及您的 Google 或 Facebook 凭证都是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当您使用联合身份验证访问 AWS 时，您就是在间接代入角色。

根据您的用户类型，您可以登录 AWS 管理控制台或 AWS 访问门户。有关登录到 AWS 的更多信息，请参阅《AWS Sign-In User Guide》中的 How to sign in to your AWS account。

如果您以编程方式访问 AWS，则 AWS 将提供软件开发工具包（SDK）和命令行界面（CLI），以便使用您的凭证以加密方式签署您的请求。如果您不使用 AWS 工具，则必须自行对请求签名。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的签署 AWS API 请求。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如，AWS 建议您使用多重身份验证（MFA）来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center User Guide》中的 Multi-factor authentication 和《IAM 用户指南》中的在 AWS 中使用多重身份验证（MFA）。

AWS 账户根用户

在创建 AWS 账户时，您首先需要使用一个对账户中所有 AWS 服务和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。切勿使用根用户执行日常任务，您需要采取措施保护根用户凭证。仅使用根用户凭证来执行仅限根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求真人用户（包括需要管理员访问权限的用户）结合使用联合身份验证和身份提供程序，以使用临时凭证来访问 AWS 服务。

联合身份是来自企业用户目录、Web 身份提供程序、AWS Identity Service 的用户，或任何使用通过身份源提供的凭证来访问 AWS 服务的用户。当联合身份访问 AWS 账户时，他们会代入角色，而角色会提供临时凭证。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和组，也可以连接并同步到您自己的身份源中的一组用户和组以跨所有 AWS 账户和应用程序使用。有关 IAM Identity Center 的信息，请参阅《AWS IAM Identity Center User Guide》中的 What is IAM Identity Center?。

IAM 用户和组

IAM 用户是 AWS 账户内对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用案例需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的使用案例，应在需要时更新访问密钥。

IAM 组是一种指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可能具有一个名为 IAMAdmins 的组，并为该组授予权限以管理 IAM 资源。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的何时创建 IAM 用户（而不是角色）。

IAM 角色

IAM 角色是 AWS 账户中具有特定权限的身份。它类似于 IAM 用户，但与特定人员不关联。您可以通过切换角色，在 AWS 管理控制台中暂时代入 IAM 角色。可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关联合身份验证的角色的信息，请参阅《IAM 用户指南》中的为第三方身份提供者创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的更多信息，请参阅《AWS IAM Identity Center User Guide》中的 Permission sets。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户访问：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 – 某些 AWS 服务使用其它 AWS 服务中的功能。例如，当您在某个服务中进行调用时，该服务通常会在 Amazon EC2 中运行应用程序或在 Simple Storage Service（Amazon S3）中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 服务角色：服务角色是服务代表您在账户中执行操作而代入的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的创建向 AWS 服务委派权限的角色。
  - 服务相关角色 – 服务相关角色是与 AWS 服务关联的一种服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。IAM 管理员可以查看但不能编辑服务关联角色的权限。

- 在 Amazon EC2 上运行的应用程序：您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时凭证。这优先于在 EC2 实例中存储访问密钥。要将 AWS 角色分配给 EC2 实例并使其对该实例的所有应用程序可用，需要创建一个附加到实例的实例配置文件。实例配置文件包含角色，并使 EC2 实例上运行的程序能够获得临时凭证。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM 角色为 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用 IAM 角色还是 IAM 用户，请参阅IAM 用户指南中的何时创建 IAM 角色（而不是用户）。

AWS 安全事件响应 如何与 IAM 协同工作

AWS Identity and Access Management（IAM）是一种 AWS 服务，可以帮助管理员安全地控制对 AWS 资源的访问。IAM 管理员控制谁可以通过身份验证（登录）和授权（具有权限）来使用 AWS 安全事件响应 资源。IAM 是一项可以免费使用的 AWS 服务。

可以与 AWS 安全事件响应 搭配使用的 IAM 功能	
IAM 功能	服务是否支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是（全球）
ACL	否
ABAC（策略中的标签）	是
临时凭证	是
转发访问会话（FAS）	是
服务角色	否
服务关联角色	是

主题

适用于 AWS 安全事件响应 的基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

主题

基于身份的策略示例

默认情况下，用户和角色没有创建或修改 AWS 安全事件响应 资源的权限。它们也无法使用 AWS 管理控制台、AWS 命令行界面（AWS CLI）或 AWS API 执行任务。IAM 管理员可以创建 IAM 策略，授予用户对所需资源执行操作的权限。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅 IAM 用户指南中的 创建 IAM 策略。

有关 AWS 安全事件响应定义的操作和资源类型的详细信息（包括每种资源类型的 ARN 格式），请参阅《Service Authorization Reference》中的 Actions, resources, and condition keys for AWS 安全事件响应。

策略最佳实践

基于身份的策略确定某个人是否可以创建、访问或删除您账户中的 AWS 安全事件响应 资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

AWS 托管式策略及转向最低权限许可入门：要开始向用户和工作负载授予权限，请使用 AWS 托管式策略来为许多常见使用场景授予权限。您可以在 AWS 账户中找到这些策略。我们建议通过定义特定于您的使用案例的 AWS 客户管理型策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略或工作职能的 AWS 托管策略。

应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。

使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果通过特定 AWS 服务（例如 AWS CloudFormation）使用服务操作，您还可以使用条件来授予对服务操作的访问权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。

使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性：IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM Acess Analyzer 策略验证。

需要多重身份验证（MFA）– 如果您所处的场景要求您的 AWS 账户中有 IAM 用户或根用户，请启用 MFA 来提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的配置受 MFA 保护的 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实操。

使用 AWS 安全事件响应 控制台

要访问 https://console.aws.amazon.com/security-ir/，您必须具有一组最低权限。这些权限必须允许您列出和查看有关您的 AWS 账户中的 AWS 安全事件响应 资源的详细信息。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于只需要调用 AWS CLI 或 AWS API 的用户，您无需为其提供最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

附加 AWS 安全事件响应访问或只读 AWS 托管策略，可确保用户和角色可以使用服务控制台。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包含通过控制台或者使用 AWS CLI 或 AWS API 以编程方式完成此操作所需的权限。

基于资源的策略

AWS 安全事件响应中基于资源的策略

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。主体可以包括账户、用户、角色、联合用户或 AWS 服务。

有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

策略操作

适用于 AWS 安全事件响应的策略操作

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Action 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 AWS 安全事件响应操作的列表，请参阅《Service Authorization Reference》中 AWS 安全事件响应定义的操作。

AWS 安全事件响应 中的策略操作在操作前使用以下前缀：

AWS 安全事件响应 -identity

要在单个语句中指定多项操作，请使用逗号将它们隔开。

"Action": ["AWS 安全事件响应 -identity:action1", "AWS 安全事件响应 -identity:action2"]

AWS 安全事件响应的策略资源

支持策略资源：是。管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 Resource 元素指定要向其应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

"Resource": "*"

AWS 安全事件响应 的策略条件键

支持特定于服务的策略条件键：否

管理员可以使用 AWS JSON 策略来指定谁有权访问什么内容。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 Condition 元素（或 Condition 块）中，您可以指定语句生效的条件。条件元素为可选元素。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 Condition 元素，或在单个 Condition 元素中指定多个键，则 AWS 会使用 AND 逻辑运算评估条件。如果您为单个条件键指定多个值，则 AWS 会使用 OR 逻辑运算来评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件键和特定于服务的条件键。要查看所有 AWS 全局条件键，请参阅《IAM 用户指南》中的 AWS 全局条件上下文键。

AWS 安全事件响应 中的访问控制列表（ACL）

支持 ACL：否

访问控制列表（ACL）控制哪些主体（账户成员、用户或角色）有权访问资源。ACL 与基于资源的策略类似，但它们不使用 JSON 策略文档格式。

用于 AWS 安全事件响应的基于属性的访问权限控制（ABAC）

支持 ABAC（策略中的标签）：是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在 AWS 中，这些属性称为标签。您可以将标签附加到 IAM 实体（用户或角色）以及 AWS 资源。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `AWS:ResourceTag/key-name`、`AWS:RequestTag/key-name` 或 `AWS:TagKeys` 条件键在策略的条件元素中提供标签信息。如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。有关 ABAC 的更多信息,请参阅《IAM 用户指南》中的什么是 ABAC？。要查看设置 ABAC 步骤的教程，请参阅《AWS Identity and Access Management 用户指南》中的使用基于属性的访问权限控制（ABAC）。

将临时凭证用于 AWS 安全事件响应

支持临时凭证：是

AWS 服务在您使用临时凭证登录时无法正常工作。有关更多信息，包括哪些 AWS 服务与临时凭证配合使用，请参阅《AWS Identity and Access Management 用户指南》中的使用 IAM 的 AWS 服务。如果您不使用用户名和密码而用其他方法登录到 AWS 管理控制台，可使用临时凭证。例如，当您使用贵公司的单点登录（SSO）链接访问 AWS 时，该过程将自动创建临时凭证。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的切换到角色（控制台）。

您可以使用 AWS CLI 或者 AWS API 手动创建临时凭证。之后，您可以使用这些临时凭证访问 AWS。AWS 建议您动态生成临时凭证，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

AWS 安全事件响应 的转发访问会话

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在 AWS 中执行操作时，您将被视为主体。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用主体调用 AWS 服务的权限，结合请求的 AWS 服务，向下游服务发出请求。只有在服务收到需要与其它 AWS 服务或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

排除 AWS 安全事件响应 身份和访问问题

使用以下信息可帮助您诊断和修复您在结合使用 AWS 安全事件响应和 IAM 时可能遇到的常见问题。

主题

- 我无权执行操作
- 我无权执行 iam:PassRole
- 我希望允许我的 AWS 账户之外的人员访问我的 AWS 安全事件响应 资源

我无权执行操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 mateojackson IAM 用户尝试使用控制台查看有关虚构 my-example-widget 资源的详细信息，但不拥有虚构 AWS 安全事件响应 GetWidget 权限时，会发生以下示例错误。

User: arn:AWS:iam::123456789012:user/mateojackson is not authorized to perform: AWS 安全事件响应 :GetWidget on resource: my-example-widget

在此情况下，必须更新 mateojackson 用户的策略，以允许使用 AWS 安全事件响应 :GetWidget 操作来访问 my-example-widget 资源。

如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

我无权执行 **`iam:PassRole`** 如果您收到一个错误，指明您无权执行 `iam:PassRole` 操作，则必须更新策略以允许您将角色传递给 AWS 安全事件响应。

有些 AWS 服务允许您将现有角色传递到该服务，而不是创建新服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为 marymajor 的 IAM 用户尝试使用控制台在 AWS 安全事件响应中执行操作时，会发生以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

User: arn:AWS:iam::123456789012:user/marymajor is not authorized to perform: `iam:PassRole`

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。如果您需要帮助，请联系 AWS 管理员。您的管理员是提供登录凭证的人。

我希望允许我的 AWS 账户之外的人员访问我的 AWS 安全事件响应 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以担任角色。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon 的 AWS 安全事件响应是否支持这些功能，请参阅“AWS 安全事件响应如何使用 IAM”。
- 要了解如何为您拥有的 AWS 账户中的资源提供访问权限，请参阅 IAM 用户指南中的为您拥有的另一个 AWS 账户中的 IAM 用户提供访问权限。
- 要了解如何为第三方 AWS 账户提供您的资源的访问权限，请参阅IAM 用户指南中的 为第三方拥有的 AWS 账户提供访问权限。
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

使用服务角色

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅 IAM 用户指南中的创建向AWS服务委派权限的角色。

使用服务关联角色

AWS 安全事件响应 的服务相关角色

主题

- AWS SLR：AWSServiceRoleForSecurityIncidentResponse
- AWS SLR：AWSServiceRoleForSecurityIncidentResponse_Triage
- AWS 安全事件响应 服务相关角色的受支持区域

支持服务关联角色：是

服务相关角色是一种与AWS服务相关的服务角色。服务可以代入代表您执行操作的角色。服务相关角色显示在您的 AWS 账户中，并由该服务拥有。AWS Identity and Access Management 管理员可以查看但不能编辑服务相关角色的权限。

服务相关角色使 AWS 安全事件响应 的设置更轻松，因为您不必手动添加必要的权限。AWS 安全事件响应 定义其服务相关角色的权限，除非另行定义，否则仅 AWS 安全事件响应 可以担任其角色。定义的权限包括信任策略和权限策略，以及不能附加到任何其他 IAM 实体的权限策略。

有关支持服务相关角色的其他服务的信息，请参阅使用 IAM 的 AWS 服务，并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务关联角色文档。

AWS SLR：AWSServiceRoleForSecurityIncidentResponse

AWS 安全事件响应 使用名为 AWSServiceRoleForSecurityIncidentResponse 的服务相关角色（SLR）（AWS 安全事件响应策略，用于识别订阅的账户、创建案例和标记相关资源）。

权限

AWSServiceRoleForSecurityIncidentResponse 服务相关角色信任以下服务来代入该角色：

- `triage.security-ir.amazonaws.com`

附加到此角色的是名为 AWSSecurityIncidentResponseServiceRolePolicy 的 AWS 托管策略。该服务会使用该角色对以下资源执行操作：

- AWS Organizations：允许该服务查找用于该服务的会员资格账户。
- CreateCase：允许该服务代表会员资格账户创建服务案例。
- ListCases：允许服务的人工智能代理出于安全调查目的查看案例。
- UpdateCase：允许服务的人工智能代理更新案例元数据。
- CreateCaseComment：允许服务的人工智能代理将其结果发布为案例备注。
- ListComments：允许服务的人工智能代理查看执行自动调查所需的案例备注。
- TagResource：允许服务标签资源配置为该服务的一部分。

管理角色

您无需手动创建服务关联角色。当您在 AWS 管理控制台、AWS CLI、或 AWS API 中加入 AWS 安全事件响应时，该服务会为您创建服务相关角色。

> **Note**
>
> 如果您使用委托管理员账户创建了会员资格，则需要在 AWS Organizations 管理账户中手动创建服务相关角色。

如果您删除该服务关联角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您加入该服务时，该服务会再次为您创建服务相关角色。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

AWS SLR：AWSServiceRoleForSecurityIncidentResponse_Triage

AWS 安全事件响应会使用名为 AWSServiceRoleForSecurityIncidentResponse_Triage 的服务相关角色（SLR）（AWS 安全事件响应策略，用于持续监控环境中是否存在安全威胁，调整安全服务以减少警报噪音，并收集信息以调查潜在事件。）

权限

AWSServiceRoleForSecurityIncidentResponse_Triage 服务相关角色信任以下服务来代入角色：

- `triage.security-ir.amazonaws.com`

附加到此策略的是名为 AWSSecurityIncidentResponseTriageServiceRolePolicy 的 AWS 托管策略。该服务会使用该角色对以下资源执行操作：

- 事件：允许该服务创建 Amazon EventBridge 托管规则。此规则是您的 AWS 账户所需的基础设施，用于将事件从账户传送到该服务。此操作可在由 `triage.security-ir.amazonaws.com` 管理的任何 AWS 资源上执行。
- Amazon GuardDuty：允许该服务调整安全服务以减少警报噪音，收集信息以调查潜在事件，以及启动 GuardDuty 恶意软件扫描。
- AWS Security Hub CSPM：允许该服务列出已启用的标准和产品集成，列出组织成员和管理员帐户，调整安全服务以减少警报噪音，以及收集信息以调查潜在事件。
- AWS Identity and Access Management：允许服务检索 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 服务相关角色的角色信息，以验证是否已配置 GuardDuty MalwareProtection。

- AWS 安全事件响应：允许服务创建和更新案例并标记资源，仅限于标有 `SecurityIncidentResponseManaged=true` 的资源。允许该服务读取成员资格信息（GetMembership、ListMemberships）。

管理角色

您无需手动创建服务关联角色。当您在 AWS 管理控制台、AWS CLI、或 AWS API 中加入 AWS 安全事件响应时，该服务会为您创建服务相关角色。

如果您删除该服务关联角色，然后需要再次创建，您可以使用相同流程在账户中重新创建此角色。当您加入该服务时，该服务会再次为您创建服务相关角色。

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务关联角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

AWS 安全事件响应 服务相关角色的受支持区域

AWS 安全事件响应 支持在服务可用的所有区域中使用服务相关角色。

- 美国东部（俄亥俄州）
- 美国西部（俄勒冈州）
- 美国东部（弗吉尼亚）
- 欧洲地区（法兰克福）
- 欧洲地区（爱尔兰）
- 欧洲地区（伦敦）
- 欧洲地区（米兰）
- 欧洲地区（巴黎）
- 欧洲（西班牙）
- 欧洲地区（斯德哥尔摩）
- 欧洲（苏黎世）
- 亚太地区（香港）
- 亚太地区（海得拉巴）
- 亚太地区（雅加达）
- 亚太地区（墨尔本）
- 亚太地区（孟买）

- 亚太地区（首尔）
- 亚太地区（新加坡）
- 亚太地区（悉尼）
- 亚太地区（东京）
- 加拿大（中部）
- 中东（巴林）
- 中东（阿联酋）：
- 南美洲（圣保罗）
- 非洲（开普敦）

AWS 托管式策略

AWS 托管式策略是由 AWS 创建和管理的独立策略。AWS 托管式策略旨在为许多常见使用案例提供权限，以便您可以开始为用户、组和角色分配权限。

要向用户、组和角色添加权限，与自己编写策略相比，使用 AWS 托管式策略更简单。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管式策略。这些策略涵盖常见使用案例，可在您的 AWS 账户中使用。有关 AWS 托管式策略的更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略。

AWS 服务负责维护和更新关联的 AWS 托管策略。您无法更改 AWS 托管式策略中的权限。服务偶尔会向 AWS 托管式策略添加额外权限以支持新特征。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管式策略中删除权限，因此策略更新不会破坏您的现有权限。

此外，AWS 还支持跨多种服务的工作职能的托管式策略。例如，ReadOnlyAccess AWS 托管式策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动新特征时，AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的 AWS 托管式策略。

主题

- AWS 托管策略：AWSSecurityIncidentResponseServiceRolePolicy
- AWS 托管策略：AWSSecurityIncidentResponseFullAccess
- AWS 托管策略：AWSSecurityIncidentResponseReadOnlyAccess
- AWS 托管策略：AWSSecurityIncidentResponseCaseFullAccess

- AWS 托管策略：AWSSecurityIncidentResponseTriageServiceRolePolicy
- AWS 安全事件响应 SLR 和托管策略更新

AWS 托管策略：AWSSecurityIncidentResponseServiceRolePolicy

AWS 安全事件响应会使用 AWSSecurityIncidentResponseServiceRolePolicy AWS 托管策略。此 AWS 托管策略会附加到 AWSServiceRoleForSecurityIncidentResponse 服务相关角色。此策略向 AWS 安全事件响应 提供识别订阅账户、创建案例、更新案例、创建案例备注、列出案例、列出案例备注以及标记相关资源的访问权限。

> **Important**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。AWS 安全事件响应会使用标签来为您提供管理服务。标签不适合用于私有或敏感数据

权限详细信息

该服务会使用此策略对以下资源执行操作：

- AWS Organizations：允许该服务查找用于该服务的会员资格账户。
- CreateCase：允许该服务代表会员资格账户创建服务案例。
- ListCases：允许服务的人工智能代理出于安全调查目的查看案例。
- UpdateCase：允许服务的人工智能代理更新案例元数据。
- CreateCaseComment：允许服务的人工智能代理将其结果发布为案例备注。
- ListComments：允许服务的人工智能代理查看执行自动调查所需的案例备注。
- TagResource：允许服务标签资源配置为该服务的一部分。

要查看此策略相关的权限，您可以参阅 AWS 托管策略中的 AWSSecurityIncidentResponseServiceRolePolicy。

AWS 托管策略：AWSSecurityIncidentResponseFullAccess

AWS 安全事件响应会使用 AWSSecurityIncidentResponseAdmin AWS 托管策略。此策略会授予对服务资源的完全访问权限以及对 AWS 服务相关资源的访问权限。您可以将此策略与 IAM 主体结合使用，以快速添加 AWS 安全事件响应权限。

> **Important**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。AWS 安全事件响应会使用标签来为您提供管理服务。标签不适合用于私有或敏感数据

权限详细信息

该服务会使用此策略对以下资源执行操作：

- IAM 主体只读访问权限：授予服务用户对现有 AWS 安全事件响应资源执行只读操作的权限。
- IAM 主体写入访问权限：授予服务用户更新、修改、删除和创建 AWS 安全事件响应资源的权限。

要查看此策略相关的权限，请参阅 AWS 托管策略中的 AWSSecurityIncidentResponseFullAccess。

AWS 托管策略：AWSSecurityIncidentResponseReadOnlyAccess

AWS 安全事件响应会使用 AWSSecurityIncidentResponseReadOnlyAccess AWS 托管策略。此策略会授予对服务案例资源的只读访问权限。您可以将此策略与 IAM 主体结合使用，以快速添加 AWS 安全事件响应权限。

> **Important**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。AWS 安全事件响应会使用标签来为您提供管理服务。标签不适合用于私有或敏感数据

权限详细信息

该服务会使用此策略对以下资源执行操作：

- IAM 主体只读访问权限：授予服务用户对现有 AWS 安全事件响应资源执行只读操作的权限。

要查看此策略相关的权限，请参阅 AWS 托管策略中的 AWSSecurityIncidentResponseReadOnlyAccess。

AWS 托管策略：AWSSecurityIncidentResponseCaseFullAccess

AWS 安全事件响应会使用 AWSSecurityIncidentResponseCaseFullAccess AWS 托管策略。此策略会授予对服务案例资源的完全访问权限。您可以将此策略与 IAM 主体结合使用，以快速添加 AWS 安全事件响应权限。

> **Important**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。AWS 安全事件响应会使用标签来为您提供管理服务。标签不适合用于私有或敏感数据

权限详细信息

该服务会使用此策略对以下资源执行操作：

- IAM 主体案例只读访问权限：授予服务用户对现有 AWS 安全事件响应案例执行只读操作的权限。
- IAM 主体案例写入访问权限：授予服务用户更新、修改、删除和创建 AWS 安全事件响应案例的权限。

要查看此策略相关的权限，请参阅 AWS 托管策略中的 AWSSecurityIncidentResponseCaseFullAccess。

AWS 托管策略：AWSSecurityIncidentResponseTriageServiceRolePolicy

AWS 安全事件响应会使用 AWSSecurityIncidentResponseTriageServiceRolePolicy AWS 托管策略。此 AWS 托管策略会附加到 AWSServiceRoleForSecurityIncidentResponse_Triage 服务相关角色。

此策略提供对 AWS 安全事件响应的访问权限，以持续监控环境中是否存在安全威胁，调整安全服务以减少警报噪音，以及收集信息以调查潜在事件。您不能将此策略附加到您的 IAM 实体。

> **Important**
>
> 请勿在标签中存储个人身份信息（PII）或其他机密或敏感信息。AWS 安全事件响应会使用标签来为您提供管理服务。标签不适合用于私有或敏感数据

权限详细信息

该服务会使用此策略对以下资源执行操作：

- 事件：允许该服务创建 Amazon EventBridge 托管规则。此规则是您的 AWS 账户所需的基础设施，用于将事件从账户传送到该服务。此操作可在由 `triage.security-ir.amazonaws.com` 管理的任何 AWS 资源上执行。
- Amazon GuardDuty：允许该服务调整安全服务以减少警报噪音，收集信息以调查潜在事件，以及启动 GuardDuty 恶意软件扫描。
- AWS Security Hub CSPM：允许该服务列出已启用的标准和产品集成，列出组织成员和管理员帐户，调整安全服务以减少警报噪音，以及收集信息以调查潜在事件。
- AWS Identity and Access Management：允许服务检索 `AWSServiceRoleForAmazonGuardDutyMalwareProtection` 服务相关角色的角色信息，以验证是否已配置 GuardDuty MalwareProtection。
- AWS 安全事件响应：允许服务创建和更新案例并标记资源，仅限于标有 `SecurityIncidentResponseManaged=true` 的资源。允许该服务读取成员资格信息（GetMembership、ListMemberships）。

要查看此策略相关的权限，请参阅 AWS 托管策略中的 AWSSecurityIncidentResponseTriageServiceRolePolicy。

AWS 安全事件响应 SLR 和托管策略更新

由于此服务开始跟踪这些更改，您可以查看 AWS 安全事件响应 SLR 和托管策略更新的详细信息。

更改	描述	日期
已更新：AWSSecurityIncidentResponseReadOnlyAccess	该策略现在包括 `security-ir:ListInvestigations` 操作。	2026 年 4 月 22 日
已更新：AWSSecurityIncidentResponseFullAccess	该策略现在使用 `security-ir:*` ，而不是列出显式 `security-ir` 操作。添加了八个新的 AWS Organizations 权限（`organizations:ListAWSServiceAccessForOrganization` 、`organizations:ListRoots` 、`organizations:List`	2026 年 4 月 22 日

更改	描述	日期
	OrganizationalUnitsForParent 、organizations:ListAccountsForParent 、organizations:ListChildren 、organizations:DescribeOrganizationalUnit 、organizations:ListAccounts 和 organizations:DescribeAccount ），以便在更新关联时支持控制台的账户选择器。已删除 MFA 条件。	
已更新：AWSSecurityIncidentResponseCaseFullAccess	该策略现在包括两项新操作：security-ir:ListInvestigations 和 security-ir:SendFeedback 。已删除 MFA 条件。	2026 年 4 月 22 日
已更新：AWSSecurityIncidentResponseTriageServiceRolePolicy	现在，该政策允许该服务修改标有 SecurityIncidentResponseManaged=true 的 GuardDuty 筛选条件，以更新检测器配置和启动 GuardDuty 恶意软件扫描。它允许该服务创建和管理自动根据 Security Hub CSPM 调查发现采取行动的规则，以及了解组织结构。	2026 年 3 月 27 日
更新了 – AWSSecurityIncidentResponseServiceRolePolicy	此策略现在会在以下资源上执行操作： ListCases：允许服务的人工智能代理出于安全调查目的查看案例 UpdateCase：允许服务的人工智能代理更新案例元数据。 CreateCaseComment：允许服务的人工智能代理将其结果发布为案例备注 ListComments：允许服务的人工智能代理查看执行自动调查所需的案例备注	2025 年 11 月

更改	描述	日期
更新了 – AWSSecurityIncidentResponseServiceRolePolicy	该政策现在包括以下两个新操作 "organizations:DescribeAccount" 、"organizations:ListDelegatedAdministrators" 和一个新条件： `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	2025 年 11 月
SLR 更新，增加了获得支持服务权利的权限。	AWSSecurityIncidentResponseTriageServiceRolePolicy 已更新，添加了 security-ir:GetMembership、security-ir:ListMemberships、security-ir:UpdateCase、guardduty:ListFilters、guardduty:UpdateFilter、guardduty:DeleteFilter，以及 guardduty:GetAdministratorAccount 权限。添加的 guardduty:GetAdministratorAccount 权限有助于在委托账户中实现 GuardDuty 自动存档筛选条件管理。	2025 年 6 月 2 日
新增 SLR：AWSServiceRoleForSecurityIncidentResponse 新增托管策略：AWSSecurityIncidentResponseServiceRolePolicy。	新增服务相关角色和附加策略，允许服务访问 AWS Organizations 账户来识别会员资格。	2024 年 12 月 1 日

更改	描述	日期
新增 SLR：AWSServiceRoleForSecurityIncidentResponse_Triage 新增托管策略：AWSSecurityIncidentResponseTriageServiceRolePolicy	新增服务相关角色和附加策略，允许服务访问 AWS Organizations 账户来对安全事件进行分类。	2024 年 12 月 1 日
新增托管策略：AWSSecurityIncidentResponseFullAccess	AWS 安全事件响应添加一个新的附加到 IAM 主体的 SLR，用于执行服务的读取和写入操作。	2024 年 12 月 1 日
新增托管策略角色：AWSSecurityIncidentResponseReadOnlyAccess	AWS 安全事件响应添加新的附加到 IAM 主体的 SLR 用于执行读取操作	2024 年 12 月 1 日
新增托管策略角色：AWSSecurityIncidentResponseCaseFullAccess	AWS 安全事件响应添加一个新的附加到 IAM 主体的 SLR，用于执行服务案例的读取和写入操作。	2024 年 12 月 1 日
开启更改跟踪。	开启了 AWS 安全事件响应 SLR 和托管策略更改跟踪	2024 年 12 月 1 日

事件响应

安全性和合规性是 AWS 与客户共同承担的责任。这种共担模式可以减轻客户的运营负担，因为 AWS 负责运营、管理和控制从主机操作系统和虚拟化层组件，乃至服务运行所在物理设施的安全性。而客户负责管理来宾操作系统（包括更新和安全补丁）、其他关联应用程序软件以及 AWS 提供的安全组防火墙的配置。有关更多信息，请参阅 AWS 责任共担模式。

通过建立符合云端运行应用程序目标的安全基准，您可以检测出可以响应的偏差。由于安全事件响应是一个复杂的主题，因此建议您查看以下资源，以便更好地了解事件响应和您的选择对企业目标的影响：《AWS Security Best Practices》白皮书、《Security Perspective of the AWS Cloud Adoption Framework（CAF）》白皮书。

合规性验证

作为多个 AWS 合规性计划的一部分，第三方审计员将评估 AWS 服务的安全性和合规性。其中包括 SOC、PCI、FedRAMP、HIPAA 及其它。

有关特定合规性计划范围内的 AWS 服务的列表，请参阅合规性计划范围内的 AWS 服务。有关一般信息，请参阅 AWS 合规性计划。

您可以使用 AWS Artifact 下载第三方审计报告。有关更多信息，请参阅下载 AWS Artifact 中的报告。

您在使用AWS服务时的合规性责任由您数据的敏感性、贵公司的合规性目标以及适用的法律法规决定。AWS提供以下资源来帮助满足合规性：

- 安全性与合规性快速入门指南：这些部署指南介绍了架构注意事项，提供了在 AWS 上部署基于安全性和合规性的基准环境的步骤。
- 《Architecting for HIPAA Security and Compliance》白皮书：此白皮书介绍公司如何使用 AWS 创建符合 HIPAA 标准的应用程序。
- AWS 合规性资源：业务手册和指南集合，按行业和/或地点分别提供。
- 《AWS Config Developer Guide》中的 Evaluating resources with AWS Config Rules：AWS Config 会评估您的资源配置对内部实践、行业指南和法规的遵循情况。
- AWS Security Hub – 该 AWS 服务向您提供 AWS 中安全状态的全面视图。Security Hub 通过安全控制措施评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty – 该 AWS 服务通过监控您的环境中是否存在可疑和恶意活动，来检测您的 AWS 账户、工作负载、容器和数据面临的潜在威胁。GuardDuty 可以通过满足某些合规性框架规定的入侵检测要求，来协助您满足各种合规性要求，如 PCI DSS。

- AWS 审计管理器 – 此 AWS 服务可帮助您持续审计 AWS 使用情况，以简化您管理风险和符合法规及行业标准的方式。

合规性责任共担

您使用AWS 安全事件响应的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供安全事件响应工具来帮助您调查和响应安全事件。您负责执行以下操作：

- 确定安全事件响应是否符合您的合规性要求。
- 根据您的策略配置安全事件响应。
- 确保您对安全事件响应的使用符合适用法规。

元数据作为受监管数据

虽然安全事件响应不会收集您的应用程序数据，但它收集的元数据可能符合您的合规性要求。组织应评估以下内容：

- 资源名称和标识符是否构成受监管数据。
- DNS 查询日志是否包含个人信息。
- API 调用模式是否会泄露受保护的业务信息。

请咨询您的法律和合规团队，以确定根据您适用的法规应如何对安全事件响应元数据进行分类。

AWS 安全事件响应中的日志记录和监控

监控是维护 AWS 安全事件响应和其他 AWS 解决方案的可靠性、可用性和性能的重要部分。AWS 安全事件响应目前支持以下 AWS 服务来监控您的组织及其内部发生的活动。

AWS CloudTrail：借助 CloudTrail，您可以捕获来自 AWS 安全事件响应控制台的 API 调用。例如，在用户进行身份验证时，CloudTrail 会记录请求中的 IP 地址、发出请求的人以及发出请求的时间等详细信息。

Amazon CloudWatch 指标 – 利用 CloudWatch 指标，您可以几乎实时地监控和报告，并在发生事件时采取自动措施。例如，您可以基于提供的指标创建 CloudWatch 控制面板来监控 AWS 安全事件响应使用情况，也可以基于提供的指标创建 CloudWatch 警报，以便在超过设定的阈值时接收通知。

该服务的命名空间是 AWS/Usage/ServiceName。可用的指标名称是 ActiveManagedCases 和 SelfManagedCases。

根据 AWS 服务条款，AWS 安全事件响应响应团队将有权访问您的 CloudTrail、VPC、DNS 和 S3 日志数据历史记录。当 AWS 安全事件响应服务门户中有案例开启时，可以在活动安全事件期间使用这些数据。

恢复能力

AWS 全球基础设施围绕 AWS 区域和可用区构建。区域提供多个在物理上独立且隔离的可用区，这些可用区通过延迟低、吞吐量高且冗余性高的网络连接在一起。利用可用区，您可以设计和操作在可用区之间无中断地自动实现故障转移的应用程序和数据库。与传统的单个或多个数据中心基础设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关 AWS 区域和可用区的更多信息，请参阅 AWS 全球基础设施。

基础结构安全性

AWS 安全事件响应由 AWS 全球网络安全服务提供保护。有关 AWS 安全服务以及 AWS 如何保护基础设施的信息，请参阅 AWS 云安全性。要按照基础结构安全最佳实践设计您的 AWS 环境，请参阅《安全性支柱 AWS Well-Architected Framework》中的 基础结构保护。

您可以使用 AWS 发布的 API 调用通过网络访问。AWS 安全事件响应客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证，对请求进行签名。

配置和漏洞分析

您负责管理服务包含角色和相关的 CloudFormation 堆栈集。

AWS 负责处理来宾操作系统（OS）和数据库补丁、防火墙配置以及灾难恢复等基本安全任务。这些流程已通过相应第三方审核和认证。有关更多详细信息，请参阅以下 AWS 资源：

- 责任共担模式
- 安全性、身份和合规性最佳实践

防止跨服务混淆代理

混淆代理问题是一个安全性问题，即不具有某操作执行权限的实体可能会迫使具有更高权限的实体执行该操作。在 AWS 中，跨服务模拟可能会导致混淆代理问题。一个服务（呼叫服务）调用另一项服务（所谓的服务）时，可能会发生跨服务模拟。可以操纵调用服务，使用其权限以在其他情况下该服务不应有访问权限的方式对另一个客户的资源进行操作。为防止这种情况，AWS 提供可帮助您保护所有服务的数据的工具，而这些服务中的服务主体有权限访问账户中的资源。

我们建议在资源策略中使用 AWS:SourceArn 和 AWS:SourceAccount 全局条件上下文键，以限制 Amazon Connect 为其他服务提供的资源访问权限。如果使用两个全局条件上下文键，在同一策略语句中使用时，AWS:SourceAccount 值和 AWS:SourceArn 值中的账户必须使用相同的账户 ID。

防止混淆代理问题的最有效方法是使用您想要允许的资源的准确 Amazon 资源名称 (ARN)。如果您不知道资源的完整 ARN，或者您正在指定多个资源，请针对 ARN 未知部分使用带有通配符 (*) 的 AWS:SourceArn 全局上下文条件键。例如，arn:AWS:servicename::region-name::您的 AWS 账户 ID:*。

有关说明如何防范出现混淆代理问题的代入角色策略的示例，请参阅混淆代理问题防范策略。

服务配额

AWS 安全事件响应

《AWS通用参考指南》包含最新的 AWS 安全事件响应 端点和配额。

AWS 安全事件响应 技术指南

内容

摘要

本指南概述了在客户 Amazon Web Services（AWS）云环境中响应安全事件的基础知识。它概述了云安全和事件响应概念，并确定了响应安全问题的客户可以使用的云功能、服务和机制。

本指南面向担任技术角色的用户，假定您熟悉信息安全的一般原则、对当前本地环境中的安全事件响应有基本了解，并且对云服务有一定了解。

您的架构是否良好？

当您在云端构建系统时，AWS Well-Architected Framework 可帮助您了解所做决策的利弊。利用此框架的六个支柱，您可以了解到设计和运行可靠、安全、高效、经济有效且可持续的系统的架构最佳实践。您可以使用 AWS Well-Architected Tool 控制台中免费提供的 AWS Well-Architected Tool，回答与每个支柱相关的一组问题，即可根据这些最佳实践检查自己的工作负载。

有关云架构的更多专家指导和最佳实践（参考架构部署、图表和白皮书），请参阅 AWS 架构中心。

简介

安全是 AWS 的重中之重。AWS 客户受益于专为满足大多数安全敏感型组织的要求而打造的数据中心和网络架构。AWS 采用责任共担模式：AWS 负责云的安全，客户则负责云中的安全。这意味着您可以完全控制自身的安全实施，例如使用多种工具和服务助您实现安全目标。这些功能可以帮助您为在 AWS 云 中运行的应用程序建立安全基准。

如果偏离基准，例如由于配置错误或外部因素变化，则需做出响应并进行调查。要成功做到这一点，您需要了解 AWS 环境中安全事件响应的基本概念，并了解在安全问题发生之前做好准备以及向云团队传授知识并开展培训的相关要求。您需要了解可以使用的控制措施和功能，查看用于解决潜在问题的主题示例，并掌握利用自动化提高响应速度与一致性的补救方法。此外，您还应了解相关的合规性规定和法规，因为这些规定和法规与制定安全事件响应计划以满足上述要求相关。

安全事件响应可能较为复杂，因此我们建议您采用迭代方法：从核心安全服务开始，构建基础的检测和响应能力，而后制定行动手册以创建初始的事件响应机制库，并在此基础上进行迭代和改进。

开始前的准备工作

在开始了解 AWS 中的安全事件响应之前，请先熟悉 AWS 安全和事件响应的相关标准和框架。这些基础知识将有助于您理解本指南中介绍的概念和最佳实践。

AWS 安全标准和框架

首先，我们建议您查看《安全、身份与合规性的最佳实践 – AWS Well-Architected Framework》以及《AWS Cloud Adoption Framework（AWS CAF）概览》白皮书中的“安全视角”。

AWS CAF 会提供指南，促进向云迁移的组织中不同部门之间的协调。AWS CAF 指南分为几个重点领域（称为视角），这些领域与构建基于云的 IT 系统有关。安全视角描述了如何跨工作流实施安全计划，其中之一便是事件响应。本文档是我们与客户合作的经验成果，旨在帮助他们建立有效的安全事件响应计划与高效的安全事件响应能力。

行业事件响应标准和框架

本白皮书遵循美国国家标准与技术研究院（NIST）制定的《计算机安全事件处理指南 SP 800-61 r3》中的事件响应标准和最佳实践。阅读并理解 NIST 提出的概念是有益的先决条件。本白皮书将把该 NIST 指南中的概念和最佳实践应用于 AWS 技术。但是，本地事件场景不在本指南的讨论范围内。

AWS 事件响应概述

首先，了解云中的安全运营和事件响应有何不同至关重要。要构建 AWS 中的有效事件响应能力，需要了解其与传统本地响应的差异，以及这些差异对事件响应计划的影响。本节将详细介绍这些差异以及 AWS 事件响应的核心设计原则。

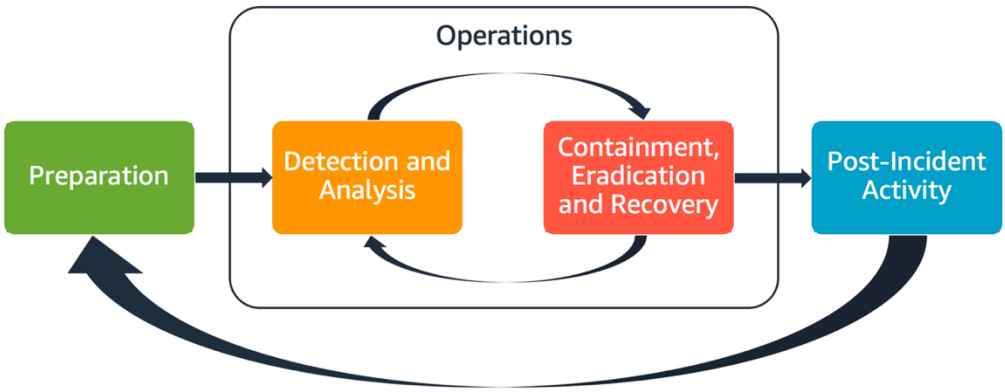
AWS 事件响应的各个方面

组织内的所有 AWS 用户都应对安全事件响应流程有基本的了解，并且安全人员应了解如何响应安全问题。教育、培训和经验对于成功的云事件响应计划至关重要，最好在处理可能发生的安全事件之前提前实施。云中成功的事件响应计划的基础在于准备工作、操作和事件后活动。

要了解其中的各个方面，请考虑以下描述：

- 准备工作：让事件响应团队做好准备，以便在 AWS 中检测和响应事件，方法是启用检测性控制措施，并确保对必要的工具和云服务拥有适当的访问权限。此外，还应通过人工和自动化的方式准备必要的行动手册，以确保可靠且一致的响应。
- 操作：按照 NIST 的事件响应阶段（检测、分析、遏制、根除和恢复）对安全事件和潜在事件采取相应操作。
- 事件后活动：对安全事件和模拟的结果进行迭代，以提高响应的有效性，从响应和调查中获得更多价值，并进一步降低风险。您必须从事件中吸取经验教训，并对改进活动占有很大的所有权。

本指南将探讨这些方面并逐一进行详细介绍。下图显示了这些方面的流程，与前面提到的 NIST 事件响应生命周期一致，但操作包括检测、分析、遏制、根除和恢复。



AWS 事件响应的各个方面

AWS 事件响应原则和设计目标

尽管事件响应的一般流程和机制（例如《NIST SP 800-61 计算机安全事件处理指南》中定义的流程和机制）依然有效，但我们建议您评估这些与云环境中的安全事件响应相关的特定设计目标：

- 建立响应目标：与利益相关者、法律顾问和组织领导合作，以确定事件响应目标。一些共同的目标包括遏制和缓解问题、恢复受影响的资源、保留数据为便取证、恢复已知安全运营，以及最终从事件中吸取教训。
- 利用云进行响应：在云中（即事件和数据的发生地）实施响应模式。
- 了解所拥有和需要的证据：通过复制日志、资源、快照和其他证据并将其存储在一个集中的响应专用云账户中来保存这些内容。使用标签、元数据和保留策略实施机制。您需要了解自己使用了哪些服务，然后确定调查这些服务的要求。为了帮助您了解自己的环境，您还可以使用标记（本文档后面的the section called “制定和实施标记策略”一节将对此进行介绍）。
- 使用重新部署机制：如果安全异常可归因于一个配置错误，那么可能只需使用适当的配置重新部署资源来删除差异，即可完成修复。如果发现可能存在漏洞，请核实您重新部署时是否包括成功且经过验证的根本原因缓解措施。
- 尽可能自动化：当问题出现或事件重复发生时，建立机制，以程序化方式对常见事件进行分类和响应。对于自动化程度不足的独特、复杂或敏感事件，使用人工响应。
- 选择可扩展的解决方案：尽量让组织采用方法的可扩展性与云计算能力相匹配。实施可在您环境中扩展的检测和响应机制，有效地缩短检测与响应之间的时间差。
- 了解并改进流程：主动找出流程、工具或人员的不足，并实施计划来弥补这些不足。模拟是找出不足并改进流程的妥善方法。有关如何对流程进行迭代的详细信息，请参阅本文档的the section called “事件后活动”一节。

这些设计目标会提醒您审查架构实施情况，确定是否同时具备事件响应能力和威胁检测能力。在规划云端实施时，应考虑如何应对事件，最好使用具备司法有效性的响应方法。在某些情况下，这意味着您可能需要专门为这些响应任务设置多个组织、账户和工具。这些工具和功能应通过部署管道提供给事件响应者。它们不应该是静态的，因为这会导致更大的风险。

云安全事件域

要进行有效准备并响应 AWS 环境中的安全事件，您需要了解常见的云安全事件类型。在客户责任范围内，有三个可能发生安全事件的域：服务域、基础设施域和应用程序域。不同的域需要不同的知识、工具和响应流程。请考虑以下域：

- 服务域：服务域中的事件可能会影响您的 AWS 账户、AWS Identity and Access Management（IAM）权限、资源元数据、账单或其他方面。服务域事件是指仅使用 AWS API 机制

进行响应的事件，或者是其根本原因与配置或资源权限相关，且可能包含相关的服务导向型日志记录的事件。

- 基础设施域：基础设施域中的事件包括与数据或网络相关的活动，例如 Amazon Elastic Compute Cloud（Amazon EC2）实例上的进程和数据、虚拟私有云（VPC）内流向 Amazon EC2 实例的流量，以及容器或其他未来服务等其他方面。对基础设施域事件的响应通常需要获取与事件相关的数据，以进行取证分析。这可能包括与实例操作系统进行交互，并且在不同情况下，还可能涉及与 AWS API 机制交互。在基础设施域中，可在来宾操作系统（例如专门用于执行取证分析和调查的 Amazon EC2 实例）中组合使用 AWS API 和数字取证/事件响应（DFIR）工具。基础设施域事件可能涉及分析网络数据包捕获、Amazon Elastic Block Store（Amazon EBS）卷上的磁盘块或从实例获取的易失性存储器。
- 应用程序域：应用程序域中的事件通常发生在应用程序代码或部署到服务或基础设施的软件中。该域应包含在您的云威胁检测和响应行动手册中，并且还可能包含基础设施域中的类似响应。您可以借助适当且周密的应用程序架构，使用云工具，通过自动获取、恢复和部署来管理该域。

在这些域中，请考虑可能对 AWS 账户、资源或数据执行操作的行为者。无论是内部行为者还是外部行为者，都应使用风险框架来确定组织面临的具体风险，并做好相应的准备。此外，您还应该开发威胁模型，这有助于您规划事件响应和构建周密架构。

AWS 中事件响应的主要差异

无论是在本地还是在云中，事件响应都是网络安全战略不可或缺的一部分。最低权限和深度防御等安全原则旨在保护本地数据与云中数据的机密性、完整性和可用性。随之诞生的，是支持这些安全原则的几种事件响应模式，包括日志保留、来自威胁建模的警报选择、行动手册制定以及安全信息和事件管理（SIEM）集成。当客户开始在云中架构和设计这些模式时，差异便开始显现。以下是 AWS 中事件响应的主要差异。

差异 #1：安全性的责任共担

安全性和合规性是 AWS 与客户共同承担的责任。这种责任共担模式可以减轻客户的运营负担，因为 AWS 会运营、管理和控制从主机操作系统和虚拟化层组件，一直到服务运营所在物理设施的安全性。有关责任共担模式的更多详细信息，请参阅责任共担模式文档。

随着您在云中的共担责任发生变化，事件响应选项也会随之改变。规划并了解这些权衡取舍，使其与您的治理需求相匹配，是事件响应的关键一步。

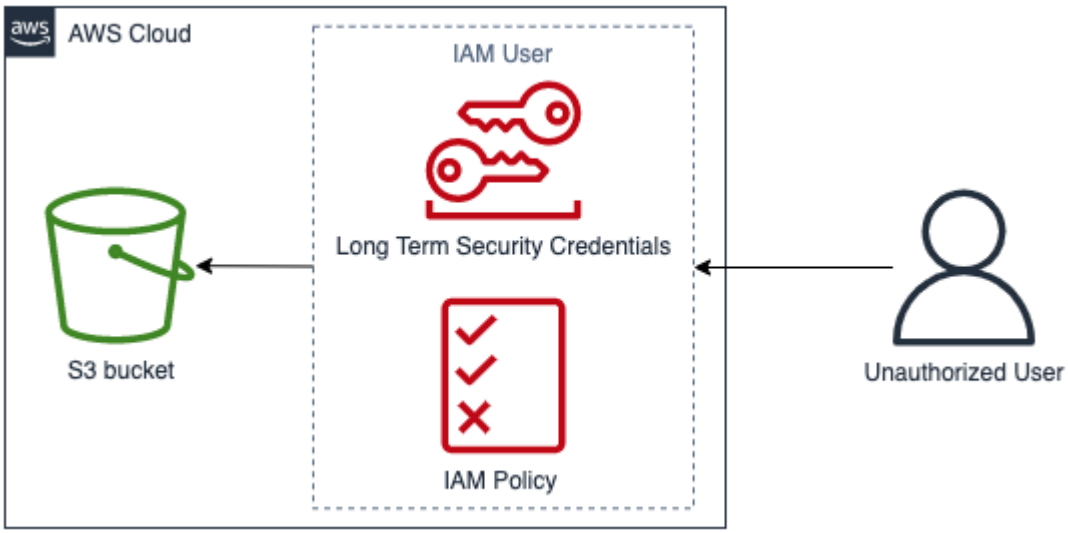
除了与您直接相关的 AWS 外，可能还有其他实体在特定责任模式中承担责任。例如，可能有内部组织单元，负责您运营的某些方面。此外，您也可能与开发、管理或运营部分云技术的其他各方有关系。

制定并测试与运营模式相匹配的适当事件响应计划和相应的行动手册至关重要。

差异 #2：云服务域

由于云服务中存在安全责任差异，因此需要一个新的安全事件域：服务域（该域已在之前的事件域一节中进行说明）。服务域包括客户的 AWS 账户、IAM 权限、资源元数据、账单及其他方面。由于您的响应方式不同，该域在事件响应方面亦有所不同。服务域内的响应通常通过查看和发出 API 调用实现，并非基于主机和基于网络的传统响应。在服务域中，您不会与受影响资源的操作系统进行交互。

下图显示了服务域中基于架构反模式的安全事件示例。在此事件中，未经授权的用户将获取 IAM 用户的长期安全凭证。IAM 用户拥有 IAM 策略，该策略允许其从 Amazon Simple Storage Service（Amazon S3）存储桶检索对象。要响应此安全事件，可以使用 AWS API 来分析 AWS 日志（例如 AWS CloudTrail 和 Amazon S3 访问日志）。您还可以使用 AWS API 来遏制事件并从中恢复。



服务域示例

差异 #3：用于预置基础设施的 API

另一个差异源于云按需自助服务的特性。主要设施客户通过 RESTful API 与 AWS 云 交互，这些 API 经由全球诸多地理位置可用的公有和私有端点提供。客户可以使用 AWS 凭证访问这些 API。与本地访问控制措施不同，这些凭证不一定受网络或 Microsoft Active Directory 域的约束。与之相反，这些凭证与 AWS 账户内的 IAM 主体相关联。这些 API 端点可以在企业网络之外进行访问，在对预期网络或地理位置之外使用凭证的事件进行响应时，理解这一点非常重要。

由于 AWS 基于 API 的特性，响应安全事件的一个重要日志源是 AWS CloudTrail，它会跟踪 AWS 账户中发出的管理 API 调用，您可以在其中找到有关 API 调用源位置的信息。

差异 #4：云的动态特性

云是动态的；支持您快速创建和删除资源。借助自动扩展，您可以根据流量增加情况启动和终止资源。由于基础设施生命周期短且变化快速，您正在调查的资源可能已不复存在或已被修改。理解 AWS 资源的短暂性以及如何跟踪 AWS 资源的创建和删除对于事件分析至关重要。您可以使用 AWS Config 来跟踪 AWS 资源的配置历史记录。

差异 #5：数据访问

云中的数据访问也有所不同。您无法通过接入服务器收集安全调查所需的数据。数据将通过线路和 API 调用进行收集。您需要实践并了解如何通过 API 执行数据收集，以便为这种转变做好准备，并确保进行了适当存储以实现有效收集和访问。

差异 #6：自动化的重要性

为了让客户充分意识到云采用的优势，其运营策略必须采用自动化。基础设施即代码（IaC）是一种高效的自动化环境模式，在这种环境中，AWS 服务通过代码（由原生 IaC 服务如 AWS CloudFormation 或第三方解决方案提供支持）进行部署、配置、重新配置和销毁。这可提供高度自动化的事件响应实施方式，有助于避免人为错误，尤其是在处理证据时。尽管本地环境也采用自动化，但在 AWS 云 中，自动化不可或缺，而且可以更轻松地实现。

应对差异

要应对这些差异，请按照下一节概述的步骤进行操作，以确保涉及人员、进程和技术的事件响应计划准备充分。

准备

要想及时、有效地应对事件，为事件做好准备至关重要。“准备工作”涉及三个领域：

- 人员：要让员工做好应对安全事件的准备，需要确定事件响应的利益相关者，并对他们进行事件响应和云技术方面的培训。
- 进程：为安全事件做好进程准备，包括记录架构、制定全面的事件响应计划，以及创建行动手册，以便对安全事件做出一致响应。
- 技术：为安全事件做好技术准备，包括设置访问权限、汇总和监控必要的日志、实施有效的警报机制，以及培养响应和调查能力。

对有效的事件响应而言，每个领域都同等重要。没有这三项，任何事件响应计划都不完整或无效。您需要在人员、流程和技术方面做好准备，并将其紧密集成，以便为应对事件做好准备。

People

要响应安全事件，您需要确定支持安全事件响应的利益相关者。此外，确保他们接受过 AWS 技术及 AWS 环境方面的相关培训，这对于实现有效响应至关重要。

定义角色和职责

处理安全事件需要在整个组织中落实纪律要求和行动意愿。在您的组织结构中，发生事件时，负责、追责、咨询或者告知信息等各个环节会涉及到不同的人员，例如人力资源（HR）、高管团队和法律部门的代表。请考虑这些角色和职责，以及是否必须有第三方参与。请注意，许多地区的当地法律都规定了，哪些事能做，哪些事不能做。尽管为安全响应计划建立一个负责、问责、咨询和知情（RACI）的图表可能显得过于繁文缛节，但这样做有利于快速直接地进行沟通，并清楚地概述在事件不同阶段负责的领导层。

在事件发生期间，让受影响应用程序和资源的负责人和开发人员参与进来非常关键，因为这些人员是主题专家（SME），可以提供信息和背景情况来协助衡量影响。您应该先练习并与开发人员和应用程序负责人建立关系，然后才能依靠他们的专业知识进行事件响应。应用程序负责人或 SME，如云管理员或工程师，可能需要在不熟悉环境、面临复杂情况或响应人员没有访问权限的情况下采取行动。

最后，值得信赖的关系可以参与到调查或响应中，因为他们可以提供额外的专业知识和宝贵的审查工作。当您自己的团队缺乏具备这些技能的人员时，您可能需要聘请外部人员寻求帮助。

培训事件响应人员

对事件响应人员进行有关其组织所使用技术的培训，对于其能否充分响应安全事件至关重要。如果相关人员不了解底层技术，响应时间可能会延长。除了传统的事件响应概念外，了解 AWS 服务及其 AWS 环境同样重要。用于培训事件响应人员的传统机制有很多，例如在线培训和课堂培训。但是，您还应该考虑将开展 GameDay 活动或进行模拟作为其中一种培训机制。有关如何进行模拟的详细信息，请参阅本文档的the section called “定期进行模拟”一节。

了解 AWS 云 技术

要减少依赖性并缩短响应时间，请确保您的安全团队和响应人员接受过云服务相关培训，并且有机会在组织所使用的特定云环境中进行实操演练。事件响应人员要想高效工作，了解 AWS 基础知识、IAM、AWS Organizations、AWS 日志记录与监控服务以及 AWS 安全服务至关重要。

AWS 提供在线安全讲习会（请参阅 AWS Security Workshops），您可以通过其获得有关 AWS 安全与监控服务的实操经验。AWS 还提供多种培训选项和学习路径，包括数字培训、课堂培训、AWS 培训合作伙伴和认证。要了解更多信息，请参阅 AWS 培训和认证。

AWS 提供免费培训和基于订阅的培训，支持多个角色和重点领域。请访问 AWS Skillbuilder 了解更多信息。

了解 AWS 环境

除了了解 AWS 服务、其使用案例及其集成方式外，了解组织 AWS 环境的实际架构以及所实施的操作流程也同样重要。通常情况下，此类内部知识没有文档记录，且仅由少数领域专家掌握，这可能会产生依赖项、阻碍创新并减慢响应时间。

为避免产生这些依赖性并缩短响应时间，应记录有关 AWS 环境的内部知识，形成文档，便于安全分析师访问和理解。要了解完整云足迹，需要安全利益相关者与相关云管理员进行协作。针对事件响应流程进行准备的一部分内容包括记录并集中管理架构图（本白皮书中的the section called “记录并集中管理架构图”一节将对此进行介绍）。然而，从人员角度来看，重要的是分析师能够访问并理解与 AWS 环境相关的架构图和操作流程。

了解 AWS 响应团队和支持

支持

支持 包含一系列计划，这些计划旨在让您能够运用各种工具和专业知识来为成功部署和正常实施 AWS 解决方案提供支持。如果您需要技术支持及更多资源来规划、部署和优化 AWS 环境，则可以选择最符合 AWS 使用案例的支持计划。

考虑将支持中心（在 AWS 管理控制台中，需要登录）作为中心联系点，为影响您 AWS 资源的问题获取支持。对 支持 的访问由 IAM 控制。有关获取对 AWS 支持功能的访问权限的更多信息，请参阅 Getting started with 支持。

此外，如果您需要举报滥用行为，请联系 AWS 信任与安全团队。

安全事件响应工程师

安全事件响应工程师是一支专业的 AWS 全球团队，全天候向客户提供支持，协助客户解决根据 AWS 责任共担模式应由客户一方负责的安全事件。

安全事件响应工程师为您提供的支持，是就 AWS 上出现的安全事件提供分级和恢复方面的协助。他们将使用 AWS 服务日志来协助分析根本原因，并为您提供恢复建议。他们还将提供安全建议和最佳实践，从而让您以后能够避免出现安全事件。

AWS 客户可以通过 AWS 支持案例与安全事件响应工程师互动。

- 所有客户：

1. 账户和计费
2. 服务：账户
3. 类别：安全
4. 严重性：一般问题

- 使用开发人员版 支持 计划的客户：
  1. 账户和计费
  2. 服务：账户
  3. 类别：安全
  4. 严重性：重要问题

- 使用 Business 版 支持 计划的客户：
  1. 账户和计费
  2. 服务：账户
  3. 类别：安全
  4. 严重性：影响业务的紧急问题

- 使用 Enterprise 版 支持 计划的客户：
  1. 账户和计费
  2. 服务：账户
  3. 类别：安全
  4. 严重性：关键业务风险问题

- 使用 AWS 安全事件响应订阅的客户：在 https://console.aws.amazon.com/security-ir/ 上打开安全事件响应控制台

DDoS 响应支持

AWS 提供 AWS Shield，这是一项托管的分布式阻断服务（DDoS）保护服务，可保护在 AWS 上运行的 Web 应用程序。AWS Shield 提供不间断检测和自动化内嵌缓解措施，可以最大限度地减少应用程序停机时间和延迟，因此无需与 支持 交流即可从 DDoS 保护中受益。AWS Shield 提供两个等级：Shield Standard 和 Shield Advanced。要了解这两个级别之间的区别，请参阅《Shield 功能文档》。

AWS Managed Services（AMS）

AWS Managed Services（AMS）可持续管理您的 AWS 基础设施，让您可以专注于应用程序。AMS 实施最佳实践来维护您的基础设施，让您能够降低运营开销和风险。AMS 可以自动执行常见活动 (例如更改请求、监控、补丁管理、安全性和备份服务)，并可以提供全生命周期服务来预置、运行和支持您的基础设施。

AMS 负责部署一套安全检测性控制措施，并每天提供对警报的第一线响应。启动警报后，AMS 遵循一组标准的自动和手动行动手册，验证是否有一致的响应。这些行动手册在功能部署期间与 AMS 客户共享，这样客户就能够开发并与 AMS 协调响应措施。

流程

要想成功实现可扩展的事件响应计划，制定全面且明确定义的事件响应流程是关键。在发生安全事件时，明确的步骤和工作流程有助于您及时做出响应。您可能已经有事故响应流程。无论您当前的状态如何，定期更新、迭代和测试事件响应流程都很重要。

制定并测试事件响应计划

为事件响应制定的第一个文档是事件响应计划。事件响应计划旨在为您的事件响应计划和战略奠定基础。事件响应计划是一份高级文档，通常包括以下部分：

- 事件响应团队概述：概述事件响应团队的目标和职能
- 角色和职责：列出事件响应利益相关者，并详细说明他们在发生事件时的角色
- 沟通计划：详细介绍联系人信息，以及在事件发生期间如何进行沟通

  此时的最佳实践是采用带外通信，作为事件沟通的后备。AWS Wickr 就是一个提供安全的带外通信渠道的应用程序示例。
- 事件响应阶段和应采取的行动：列举事件响应的各个阶段（例如，检测、分析、根除、遏制和恢复），包括在这些阶段中要采取的高级别操作
- 事件严重性和优先级定义：详细说明如何对事件的严重性进行分类，如何确定事件的优先级，然后详细说明严重性定义对上报程序有何影响

尽管这些内容部分在各种规模和行业的公司中很常见，但每个组织的事件响应计划都是独一无二的。您将需要制定最适合贵组织的事件响应计划。

记录并集中管理架构图

为了快速准确地响应安全事件，您需要了解系统和网络的架构方式。了解这些内部架构模式不仅对事件响应至关重要，而且对于验证遵循最佳实践构建这些模式的应用程序之间的一致性也同样重要。您还应确保本文档保持最新，并根据新的架构模式定期更新。您应建立文档和内部存储库，详细说明以下项目：

- AWS 账户结构：需要了解：
  - 您有多少个 AWS 账户？
  - 这些 AWS 账户是如何组织的？
  - AWS 账户的业务负责人是谁？
  - 您是否使用服务控制策略（SCP）？ 如果是，通过 SCP 实施了哪些组织护栏？
  - 您是否限制了可使用的区域和服务？
  - 业务部门和环境（开发/测试/生产）之间存在哪些差异？
- AWS 服务模式
  - 您使用了哪些 AWS 服务？
  - 使用最广泛的 AWS 服务有哪些？
- 架构模式
  - 您使用了哪些云架构？
- AWS 身份验证模式
  - 您的开发人员通常如何向 AWS 进行身份验证？
  - 您使用的是 IAM 角色还是用户（或两者兼而有之）？ 您的 AWS 身份验证是否连接到身份提供者（IdP）？
  - 如何将 IAM 角色或用户映射到员工或系统？
  - 当某人不再获得授权时，如何撤销其访问权限？
- AWS 授权模式
  - 您的开发人员使用了哪些 IAM 策略？
  - 您是否使用了基于资源的策略？
- 日志记录和监控
  - 您使用了哪些日志源？它们存储在何处？
  - 您是否聚合 AWS CloudTrail 日志？ 如果是，它们存储在何处？
  - 如何查询 CloudTrail 日志？
  - 您是否启用了 Amazon GuardDuty？

  - 如何访问 GuardDuty 调查发现（例如控制台、工单系统、SIEM）？
  - 调查发现或事件是否聚合在 SIEM 中？
  - 是否会自动创建工单？
  - 进行日志调查分析时，使用了哪些工具？
- 网络拓扑
  - 网络上的设备、端点和连接在物理上或逻辑上是如何排列的？
  - 您的网络如何与 AWS 连接？
  - 不同环境之间的网络流量是如何过滤的？
- 外部基础设施
  - 面向外部的应用程序是如何部署的？
  - 哪些 AWS 资源可以公开访问？
  - 哪些 AWS 账户包含面向外部的基础设施？
  - 部署了哪些 DDoS 或外部过滤措施？

记录内部技术图表和流程能够减轻事件响应分析师的工作负担，帮助他们快速获得必要的机构知识以响应安全事件。全面记录内部技术流程不仅可以简化安全调查，还可以根据流程的合理性和评估进行调整。

制定事件响应行动手册

准备事件响应流程的关键环节是制定行动手册。事件响应行动手册提供了一系列规范性指南和步骤，供发生安全事件时遵循。清晰的结构和步骤可简化响应，减少发生人为错误的可能性。

应针对哪些事件场景创建行动手册

应针对以下事件场景创建行动手册：

- 预期事件：应针对预期的事件创建行动手册。这包括拒绝服务（DoS）、勒索软件和凭证泄露等威胁。
- 已知的安全调查发现或警报：应针对已知的安全调查发现和警报（如 GuardDuty 调查发现）创建行动手册。您可能会收到一个 GuardDuty 调查发现，然后想：“现在怎么办？”为防止错误处理 GuardDuty 调查发现或忽略调查发现，应针对每个可能的 GuardDuty 调查发现创建行动手册。有关补救细节和指导的信息可在 GuardDuty 文档中找到。需要注意的是，默认情况下并不会启用 GuardDuty，而且需要付费。有关 Guarduty 的更多信息，请参阅附录 A：云功能定义 – the section called “可见性和警报”。

行动手册应包含的内容

行动手册应包含安全分析师需要完成的技术步骤，以便充分调查和应对潜在的安全事件。

行动手册中应包括的项目有：

- 行动手册概述：本行动手册针对哪些风险或事件场景？ 本行动手册的目标是什么？
- 先决条件：此事件场景需要哪些日志和检测机制？ 预期的通知是什么？
- 利益相关者信息：涉及哪些人员？其联系人信息是什么？ 每个利益相关方的责任是什么？
- 响应步骤：在事件响应的各个阶段，应采取哪些战术性措施？ 分析师应该进行哪些查询？ 应该运行什么代码才能达到预期的结果？
  - 检测：如何检测事件？
  - 分析：如何确定影响范围？
  - 遏制：如何隔离事件来限制其影响范围？
  - 根除：如何从环境中消除威胁？
  - 恢复：受影响的系统或资源将如何恢复生产？
- 期望结果：运行查询和代码后，行动手册的期望结果是什么？

为确保每个行动手册中的信息一致，创建一个行动手册模板供其他安全行动手册参考会很有帮助。先前列出的某些项目，例如利益相关者信息，可以在多个行动手册中共享。在这种情况下，您可以为这些信息创建集中管理的文档，并在行动手册中引用，然后在行动手册中明确列举出差异。如此一来，您无需在所有单独的行动手册中更新相同的信息。通过创建模板并识别行动手册中的通用或共享信息，您可以简化并加速行动手册的制定过程。最后，行动手册可能会随着时间推移而演变；您确认步骤一致后，这便构成了自动化的需求基础。

示例行动手册

有关大量示例行动手册，请参阅附录 B 中的the section called “行动手册资源”。此处的示例可用于指导您创建哪些行动手册以及行动手册应包含哪些内容。然而，至关重要的是，所制定的行动手册应涵盖与您的业务最相关的风险。您需要确认行动手册中的步骤和工作流程是否包含相关技术和流程。

定期进行模拟

随着组织不断发展壮大，威胁形势也会不断变化，因此，必须持续评估组织的事件响应能力。模拟便是可用于执行这种评估的一种方法。模拟过程使用现实世界中的安全事件场景，旨在模仿威胁主体采取的战术、技术和程序（TTP），让组织通过响应现实中可能发生的模拟网络事件，来练习和评估自己的事件响应能力。

模拟有多种好处，包括：

- 检验网络准备情况，有助于事件响应人员树立信心。
- 测试工具和工作流程的准确性和有效性。
- 完善沟通和上报环节，使之与您的事件响应计划相吻合。
- 提供机会来应对不太常见的攻击载体。

模拟类型

模拟主要分为三种类型：

- 桌面演练：桌面演练模拟方法严格来说是一种基于讨论的研讨会，让各个事件响应利益相关者参与进来，练习角色和职责，以及练习使用既定的沟通工具和行动手册。通常是用一整天的时间在虚拟场地和/或实地中协调完成演练。由于桌面演练以讨论为基础的特性，因而其侧重于流程、人员和协作。在讨论中，技术是必不可少的一部分，但事件响应工具或脚本的实际使用通常不包括在桌面演练中。
- 紫队演练：紫队演练可提高事件响应人员（蓝队）和模拟威胁行为者（红队）之间的协作能力。蓝队通常由安全运营中心（SOC）的成员组成，但也可以包括在实际网络事件中会参与进来的其他利益相关者。红队通常由渗透测试团队或接受过攻击安全培训的关键利益相关者组成。在设计场景时，红队会与演练协调员相互协作，以确保场景的准确性与可行性。在紫队演练中，主要的关注点是支持事件响应工作的检测机制、工具和标准操作程序（SOP）。
- 红队演练：在红队演练中，进攻方（红队）模拟进行攻击，以在预定范围内实现特定目标或一系列目标。防御方（蓝队）不一定知道演练的范围和持续时间，如此，可以更真实地评估他们应对真实事件的能力。由于红队的演练可能是侵入性测试，因此务必谨慎行事，并实施控制措施，以确保该演练不会对环境造成实际破坏。

> **Note**
>
> AWS 要求客户在进行紫队或红队演练之前，先查看渗透测试网站上提供的渗透测试策略。

表 1 总结了这几类模拟的一些主要差异。值得注意的是，这些定义通常视为宽泛定义，可根据组织需求进行自定义。

表 1 – 模拟类型

	桌面演练	紫队演练	红队演练
总结	此类演练基于文档，专注于一个特定的安全事件场景。可以是高级别的，也可以是技术性的，并通过一系列书面预设场景推动演练进程。	相较于桌面演练，此类演练更贴近现实。紫队演练期间，协调员需要与参与者协作，以提升演练参与度，并在必要时提供培训。	此类演练通常提供更高级别的模拟形式。具有高度的隐蔽性，参与者可能并不知晓演练的所有细节。
所需资源	所需技术资源较少	需要多方利益相关者参与，且需要高水平的技术资源	需要多方利益相关者参与，且需要高水平的技术资源
复杂性	低	中	高

请考虑定期协调开展网络模拟。对于参与者和整个组织而言，每种演练类型都可以带来独特的好处，因此您可以选择从不太复杂的模拟类型（例如桌面演练）入手，然后再慢慢过渡到较为复杂的模拟类型（红队演练）。您应根据自身的安全成熟度、资源和期望结果选择模拟类型。由于红队演练的复杂性和成本，一些客户可能不会选择进行红队演练。

演练生命周期

无论您选择哪种模拟类型，模拟通常都遵循以下步骤：

1. 定义核心演练要素：定义模拟场景和模拟要达成的目标。这两者都应该得到领导层的认同。
2. 确定关键利益相关者：演练至少需要演练协调员和参与者。根据具体的场景，可能会涉及其他利益相关方，例如法务、通信或行政等领域的领导层。
3. 构建和测试场景：如果有特定要素不可行，则可能需要在构建时重新定义该场景。本阶段的期望结果是最终确定的场景。
4. 协调开展模拟：采用的模拟类型决定了所需的协调工作（书面讨论场景对比高技术含量的模拟场景）。协调员应根据演练目标调整其协调战术，并应尽可能让所有演练参与者都参与进来，以实现最大利益。
5. 撰写事后报告（AAR）：确定哪些方面进展较为顺利、哪些方面需要改进以及可能存在的差距。AAR 应衡量模拟的有效性，并记录团队对模拟事件的响应情况，以便在将来的模拟中可以不断跟踪进度。

Technology

如果您在安全事件发生之前开发并采用适当的技术，事件响应人员将能够及时进行调查、了解范围并采取行动。

创建 AWS 账户结构

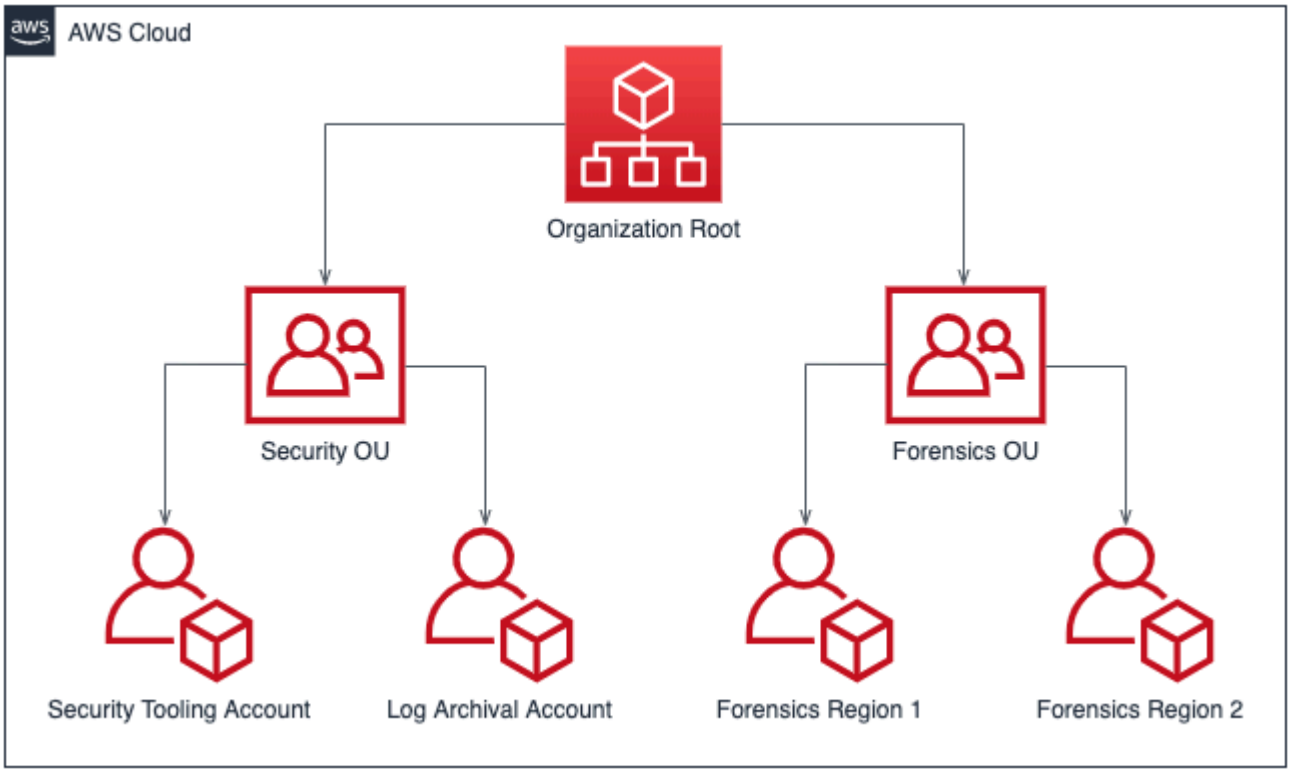
AWS Organizations 有助于您随着 AWS 资源的增长和扩展，集中管理和监管 AWS 环境。AWS 组织会整合您的 AWS 账户，这样您就能够将这些账户作为一个单元进行管理。您可以使用组织单元 (OU)，将账户分组到一起，作为一个单元管理。

对于事件响应，拥有一个支持事件响应功能的 AWS 账户结构（包括安全组织单元和取证组织单元）会很有帮助。在安全 OU 中，您应该拥有以下账户：

- 日志存档：将日志聚合到日志存档 AWS 账户中。
- 安全工具：将安全服务集中在安全工具 AWS 账户中。此账户以安全服务的委托管理员身份运行。

在取证 OU 中，您可以选择实施单一取证账户，也可以为您运营的每个区域实施账户，具体取决于哪种账户最适合您的业务和运营模式。以根据区域创建账户方法为例，如果您只在美国东部（弗吉尼亚州北部）(us-east-1) 和美国西部（俄勒冈州）(us-west-2) 运营，那么您将在取证组织单元中拥有两个账户：一个用于 us-east-1，另一个用于 us-west-2。由于预置新账户需要时间，因此必须在事件发生前创建和分析取证账户，以便响应人员能够做好准备，有效地使用这些账户进行响应。

下图显示了一个账户结构示例，其中包括一个取证 OU，涵盖了根据每个区域创建的取证账户：



用于响应事件而根据区域创建的账户结构

制定和实施标记策略

要获取围绕 AWS 资源的业务场景和相关内部利益相关方的背景信息，可能很困难。要做到这一点，可以采用标签的形式，标签为 AWS 资源分配元数据，并由用户定义的键和值组成。您可以创建标签，按照用途、所有者、环境、处理的数据类型以及您选择的其他标准对资源进行分类。

采用一致的标记策略可以让您快速识别和辨别 AWS 资源的背景信息，从而加快响应速度。标签还可以充当启动自动响应的机制。有关要标记内容的更多信息，请参阅文档 AWS 资源标记方法。首先，您需要定义要在组织内实施的标签。之后，实施并强制执行这一标记策略。有关实施和强制执行的详细信息，请参阅 AWS 博客《Implement AWS resource tagging strategy using AWS Tag Policies and Service Control Policies (SCPs)》。

更新 AWS 账户联系人信息

对于每个 AWS 账户，提供准确且最新的联系人信息至关重要，这样才能确保正确的利益相关者收到来自 AWS 的安全性、账单和运营等主题的重要通知。对于每个 AWS 账户，需设置一位主要联系人以及多位负责安全性、账单和运营的备用联系人。有关这些联系人之间的区别，请参阅《AWS Account Management Reference Guide》。

有关管理备用联系人的详细信息，请参阅有关添加、更改或删除备用联系人的 AWS 文档。如果您的团队负责处理账单、运营和安全性相关问题，使用电子邮件通讯组列表是一种最佳实践。电子邮件通讯组列表可以消除对某一成员的依赖，避免因其不在办公室或离开公司而造成工作停滞。您还应确保电子邮件和账户联系人信息（包括电话号码）得到充分保护，以避免根账户密码重置和多重身份验证（MFA）重置。

对于使用 AWS Organizations 的客户，组织管理员可以使用管理账户或委托管理员账户，集中管理成员账户的备用联系人，而无需每个 AWS 账户的凭证。但是，您还需确保新创建的账户提供了准确的联系人信息。请参阅博客文章《Automatically update alternate contacts for newly created AWS 账户》。

准备 AWS 账户访问权限

在事件发生期间，事件响应团队必须有权访问事件中涉及的环境和资源。在事件发生之前，确保团队具有履行其职责的适当访问权限。为此，您应了解团队成员所需的访问级别（例如，他们可能采取哪些行动），且应提前预置最低访问权限。

要实施和配置此访问权限，您应与组织的云架构师确定并讨论 AWS 账户策略和云身份策略，以了解配置了哪些身份验证和授权方法。由于这些凭证的特权性质，在实施过程中，您应考虑使用审批流程，或从保管库或保险箱中检索凭证。实施后，您应在事件发生之前尽早记录并测试团队成员的访问权限，确保他们能够立即做出响应。

最后，专门创建用于响应安全事件的用户通常具有特权，以便提供足够的访问权限。因此，应当限制并监控这些凭证的使用，不得将其用于日常活动。

了解威胁形势

开发威胁模型

通过开发威胁模型，组织能够先于未经授权的用户识别威胁并制定缓解措施。有多种威胁建模策略和方法可供选择；请参阅博客文章《How to approach threat modeling》。对于事件响应，威胁模型有助于识别威胁行为者在事件发生期间可能使用的攻击向量。理解您需要防御的对象对于及时响应至关重要。您也可以使用 AWS Partner 进行威胁建模。要查找 AWS 合作伙伴，请使用 AWS Partner Network。

整合和利用网络威胁情报

网络威胁情报是指关于威胁行为者意图、机会及能力的数据和分析。获取和利用威胁情报有助于尽早检测到事件并更好地了解威胁行为者的行为。网络威胁情报包括静态指标，例如 IP 地址或恶意软件的文件哈希值。它还包括高级别信息，例如行为模式和意图。您可以从多家网络安全供应商和开源存储库收集威胁情报。

要为 AWS 环境整合并最大限度地利用威胁情报，您可以使用一些开箱即用功能，并整合自己的威胁情报列表。Amazon GuardDuty 使用 AWS 内部及第三方威胁情报源。其他 AWS 服务，例如 DNS 防火墙和 AWS WAF 规则，也接收来自 AWS 高级威胁情报组的输入。部分 GuardDuty 调查发现映射到 MITRE ATT&CK 框架，该框架可提供有关攻击者策略和技术的实际观察信息。

选择并设置用于分析和报警的日志

在安全调查期间，您需要能够查看相关日志，以便记录并了解事件的来龙去脉和时间线。生成警报时也需要日志，因为日志可以指示某些相关操作已经发生。选择、启用、存储、设置查询和检索机制以及设置警报至关重要。本节将回顾上述每个操作。有关更多详细信息，请参阅 AWS 博客文章《Logging strategies for security incident response》。

选择并启用日志源

进行安全调查之前，您需要捕获相关日志，以便以回溯方式重建 AWS 账户中的活动。选择并启用与其 AWS 账户工作负载相关的日志源。

AWS CloudTrail 是一项日志记录服务，可跟踪针对 AWS 账户捕获 AWS 服务活动所进行的 API 调用。它在默认情况下启用，管理事件保留 90 天，可以使用 AWS 管理控制台、AWS CLI 或 AWS SDK 通过 CloudTrail 事件历史记录工具检索这些事件。为了更长久地保留和了解数据事件，您需要创建 CloudTrail 跟踪并将其与 Amazon S3 存储桶关联，也可以选择与 CloudWatch 日志组关联。或者，您可以创建 CloudTrail Lake，这可保留 CloudTrail 日志最多七年，并提供基于 SQL 的查询工具。

AWS 建议使用 VPC 的客户分别使用 VPC 流日志和 Amazon Route 53 Resolver 查询日志启用网络流量和 DNS 日志，并将其流式传输到 Amazon S3 存储桶或 CloudWatch 日志组。您可以为 VPC、子网或网络接口创建 VPC 流日志。对于 VPC 流日志，您可以选择启用流日志的方式和位置，以降低成本。

AWS CloudTrail 日志、VPC 流日志和 Route 53 解析器查询日志是支持 AWS 中安全调查的基本日志记录三要素。

AWS 服务可以生成基本日志记录三要素未捕获到的日志，如弹性负载均衡日志、AWS WAF 日志、AWS Config 记录器日志、Amazon GuardDuty 调查发现、Amazon Elastic Kubernetes Service（Amazon EKS）审计日志，以及 Amazon EC2 实例操作系统和应用程序日志。有关日志记录和监控选项的完整列表，请参阅the section called “附录 A：云功能定义”。

选择日志存储

日志存储的选择通常与您使用的查询工具、保留能力、熟悉程度和成本有关。启用 AWS 服务日志时，需要提供存储工具；通常是 Amazon S3 存储桶或 CloudWatch 日志组。

Amazon S3 存储桶提供持久且经济高效的存储，并具有可选的生命周期策略。可以使用 Amazon Athena 等服务本地查询存储在 Amazon S3 存储桶中的日志。CloudWatch 日志组通过 CloudWatch Logs Insights 提供持久存储和内置查询工具。

确定适当的日志保留

使用 S3 存储桶或 CloudWatch 日志组存储日志时，必须为每个日志源建立足够的生命周期，以优化存储和检索成本。客户通常可以查询三个月到一年的日志，日志保留期最多七年。可用性和保留时长的选择应与您的安全要求以及法律法规和业务授权的综合因素相一致。

选择和实施日志查询机制

在 AWS 中，可以用来查询日志的主要服务包括 CloudWatch Logs Insights（用于查询存储在 CloudWatch 日志组中的数据）和 Amazon Athena 和 Amazon OpenSearch Service（用于查询存储在 Amazon S3 中的数据）。您还可以使用第三方查询工具，如安全信息和事件管理（SIEM）。

选择日志查询工具的过程中，应考虑安全运营的人员、流程和技术方面。选择一款能够满足运营、业务和安全要求并可长期使用和维护的工具。请记住，当要扫描的日志数量保持在工具的限制范围内时，日志查询工具的工作状态最佳。由于成本或技术限制，客户拥有多款查询工具的情况并不罕见。例如，客户可能会使用第三方 SIEM 对过去 90 天的数据执行查询，但由于 SIEM 的日志提取成本较高，会使用 Athena 来执行 90 天以上的查询。无论采用何种实施方式，都要验证您的方法能够尽可能地减少充分提高运营效率所需的工具数量，尤其在安全事件调查期间。

使用日志发出警报

AWS 通过 Amazon GuardDuty、AWS Security Hub CSPM 和 AWS Config 安全服务，自身就能提供警报功能。您也可以使用自定义警报生成引擎来处理这些服务未涵盖的安全警报或与环境相关的特定警报。本文档的the section called “检测”一节介绍了如何构建这些警报和检测。

构建取证能力

在发生安全事件之前，可以考虑构建取证能力来支持安全事件调查工作。NIST 发布的《Guide to Integrating Forensic Techniques into Incident Response》提供了此类指导。

AWS 取证

传统本地取证的概念适用于 AWS。博客文章《Forensic investigation environment strategies in the AWS 云》提供了关键信息，便于您开始将取证专业知识迁移到 AWS。

设置好取证的环境和 AWS 账户结构后，需要确定在以下四个阶段有效执行可靠取证方法所需的技术：

- 收集：收集相关的 AWS 日志，例如 AWS CloudTrail、AWS Config、VPC 流日志和主机级日志。收集受影响的 AWS 资源的快照、备份和内存转储。
- 检查：通过提取和评测相关信息来检查收集到的数据。
- 分析：分析收集到的数据，以便了解事件并从中得出结论。
- 报告：提供分析阶段得出的信息。

捕获备份和快照

为关键系统和数据库建立备份对于从安全事件中恢复和取证至关重要。有了备份，您就能够将系统恢复到以前的安全状态。在 AWS 上，您可以创建各种资源的快照。快照为您提供这些资源的时间点备份。有许多 AWS 服务能够在备份和恢复方面为您提供支持。有关这些服务以及备份和恢复方法的详细信息，请参阅 Backup and Recovery Prescriptive Guidance。有关更多详细信息，请参阅博客文章《Use backups to recover from security incidents》。

特别是遇到勒索软件等情况时，妥善保护备份至关重要。有关保护备份的指导，请参阅博客文章《Top 10 security best practices for securing backups in AWS》。除了确保备份安全外，您还应当定期测试备份和还原流程，从而确保现有的技术和流程按预期运行。

AWS 上的取证自动化功能

在安全事件发生期间，您的事件响应团队必须能够快速收集和分析证据，同时保持事件相关时间段的准确性。对于事件响应团队来说，在云环境中手动收集相关证据既具有挑战性又很耗时，尤其是在存在大量实例和账户的情况下。此外，手动收集容易出现人为错误。出于这些原因，客户应该开发和实现取证自动化功能。

AWS 提供了大量用于取证的自动化资源，这些资源已整合到附录的the section called “取证资源”中。这些资源是我们开发并由客户实施的取证模式示例。虽然这些资源可能是有用的参考架构，但可以考虑根据您的环境、要求、工具和取证流程对资源进行修改，或者创建新的取证自动化模式。

准备项目总结

要实现及时有效的事件响应，为响应安全事件做好充分准备至关重要。事件响应准备涉及人员、流程和技术。就响应准备而言，这三个领域都同等重要。因此，您应该针对这三个领域准备和完善事件响应计划。

表 2 总结了本节中详述的准备项目。

表 2 – 事件响应准备项目

域：	准备项目	操作项
人员	定义角色和职责。	• 确定相关的事件响应利益相关者。 • 为事件制定责任、问责、咨询和知情（RACI）图表。
人员	对事件响应人员进行 AWS 培训。	• 对事件响应利益相关者进行 AWS 基础培训。 • 对事件响应利益相关者进行 AWS 安全和监控服务相关培训。 • 对事件响应利益相关者进行 AWS 环境及其架构方式相关培训。
人员	了解 AWS 支持选项。	• 了解 AWS 支持、安全事件响应工程师、DDoS 响应团队（DRT）与 AMS 之间的差异。 • 了解在活跃安全事件期间进行分级以及在必要时联系安全事件响应工程师的升级路径。
流程	制定事件响应计划。	• 创建高级别文档，用于定义您的事件响应计划和策略。 • 事件响应计划应当包含 RACI、沟通计划、事件定义和事件响应阶段。
流程	记录并集中管理架构图。	• 记录有关 AWS 环境配置的详细信息，涵盖账户结构、服务使用情况、IAM 模式以及 AWS 配置的其他核心功能。

域：	准备项目	操作项
		• 绘制云架构的架构图。
流程	制定事件响应行动手册。	• 创建用于行动手册结构的模板。 • 编写用于预期安全事件的行动手册。 • 编写用于 GuardDuty 调查发现等已知安全警报的行动手册。
流程	定期进行模拟。	• 确定定期进行事件模拟的频率。 • 利用输出和经验教训对事件响应计划进行迭代。
技术	规划 AWS 账户结构。	• 规划账户结构，确定如何按 AWS 账户划分工作负载。 • 创建安全组织单元，其中包含安全工具和日志存档账户。 • 创建取证组织单元，其中包含您的每个运营所在区域的取证账户。
技术	制定和实施标记策略，帮助响应人员确定调查发现的所有权和背景情况。	• 规划标记策略以及您希望与 AWS 资源关联的标记内容。 • 实施并执行标记策略。
技术	更新 AWS 账户联系人信息。	• 确认 AWS 账户是否列出了联系人信息。 • 创建用于联系人信息的电子邮件通讯组列表，以消除单点故障。 • 保护与 AWS 账户信息关联的电子邮件账户。

域：	准备项目	操作项
技术	准备 AWS 账户访问权限。	• 定义事件响应人员响应事件所需的访问权限。 • 实施、测试和监控访问权限。
技术	了解威胁形势。	• 开发针对环境和应用程序的威胁模型。 • 整合并利用网络威胁情报。
技术	选择并设置日志。	• 识别并启用调查日志。 • 选择日志存储。 • 标识和实施日志保留。 • 开发检索和查询日志及构件的机制。 • 使用日志发出警报。
技术	开发取证能力。	• 识别取证收集所需的构件。 • 收集和保护关键系统备份。 • 定义针对已识别日志及构件的分析机制。 • 实现取证分析自动化。

建议采用迭代方法进行事件响应准备。所有这些准备项目皆无法一蹴而就；您应该制定计划，从小处着手，随着时间的推移不断提升事件响应能力。

操作

“操作”是执行事件响应的核心。这是响应和修复安全事件的操作发生的地方。“操作”包括以下五个阶段：检测、分析、遏制、根除和恢复。表 3 提供了这些阶段和目标的描述。

表 3 – 操作阶段

阶段	目标
检测	识别潜在的安全事件。
分析	确定安全事件是否为意外事件，并评估事件的影响范围。
遏制	尽量减小和限制安全事件的影响范围。
根除	移除与安全事件相关的未经授权的资源或构件。实施可消除安全事件的缓解措施。
恢复	将系统恢复到已知安全状态并监控这些系统，确认威胁不会再次出现。

在应对和处理安全事件时，应将这些阶段作为指导，以便有效且可靠地进行响应。采取的实际操作会因事件而异。例如，涉及勒索软件的事件要遵循的响应步骤与涉及公共 Amazon S3 存储桶的事件不同。此外，这些阶段不一定按顺序发生。在遏制和根除之后，您可能需要重新分析，了解操作是否有效。

检测

警报是检测阶段的主要组成部分。它会根据需要关注的 AWS 账户威胁活动生成通知，以启动事件响应流程。

确保警报准确性颇具挑战性；因为通常无法完全确定事件是否已经发生、正在进行还是将在未来发生。原因如下：

- 检测机制基于基准偏差、已知模式以及来自内部或外部实体的通知。
- 由于技术和人员（分别指安全事件的手段和行为者）的不可预测性，基准会随着时间的推移而变化。新型或经过修改的威胁行为者战术、技术和程序（TTP）会导致新的恶意模式出现。
- 对人员、技术和流程的更改不会立即纳入事件响应流程。部分变更是在调查过程中发现的。

警报源

您应考虑使用以下源来定义警报：

- 调查发现：AWS 服务，例如 Amazon GuardDuty、AWS Security Hub CSPM、Amazon Macie、Amazon Inspector、AWS Config、IAM Access Analyzer 和网络访问分析器等，可以生成用于制作警报的调查发现。
- 日志：存储在 Amazon S3 存储桶和 CloudWatch 日志组中的 AWS 服务、基础设施和应用程序日志，在经过解析和关联之后，可以生成警报。
- 账单活动：如果账单活动突然发生变化，则表示发生了安全事件。请按照文档创建账单警报以监控 AWS 预估费用进行监控。
- 网络威胁情报：如果您订阅了第三方网络威胁情报源，则可将该信息与其他日志记录和监控工具关联起来，以确定事件的潜在指标。
- 合作伙伴工具：AWS Partner Network（APN）中的合作伙伴可提供助您实现安全目标的顶级产品。对于事件响应，具备端点检测与响应（EDR）或 SIEM 的合作伙伴产品可助您实现事件响应目标。有关更多信息，请参阅安全能力合作伙伴和AWS Marketplace 中的安全解决方案。
- AWS 信任和安全：如果我们发现滥用或恶意活动，支持 可能会联系客户。
- 一次性联系渠道：由于注意到异常情况的可能是客户、开发人员或组织中的其他员工，因此确立一种广为人知的安全团队联系方式至关重要。常见选择包括工单系统、联系人电子邮件地址和网页表单。如果组织与公众协同合作，则可能还需要一个面向公众的安全联系机制。

有关调查阶段可以使用的云功能的更多信息，请参阅本文档中的the section called “附录 A：云功能定义”一节。

检测属于安全控制措施工程的一部分

检测机制是制定安全控制措施不可或缺的一部分。定义指令性控制措施和预防性控制措施时，应同时设立相关的检测性控制措施和响应性控制措施。例如，某组织设立了与 AWS 账户根用户相关的指令性控制措施，该控制措施仅应用于明确定义的特定活动。组织将其与通过 AWS 组织的服务控制策略（SCP）实施的预防性控制措施相关联。如果根用户活动超出预期基准，通过 EventBridge 规则和 SNS 主题实施的检测性控制措施将向安全运营中心（SOC）发出警报。响应性控制措施则要求 SOC 选择适当的行动手册、执行分析，并持续工作直至事件解决。

安全控制措施最好通过对 AWS 中运行的工作负载进行威胁建模来定义。检测性控制措施的严重程度需要查看特定工作负载的业务影响分析（BIA），据此确定。检测性控制措施生成的警报不会按接收顺序处理，而会根据其初始严重程度进行处理，以便在分析期间进行调整。虽然设定的初始严重程度有助于排列优先顺序，但发生警报的具体环境决定了真正的严重程度。例如，组织将 Amazon GuardDuty 用作检测性控制措施的组成部分，用于保护属于工作负载的 EC2 实例。此时，将生成调查发现 `Impact:EC2/SuspiciousDomainRequest.Reputation`，告知您工作负载中列出的 Amazon EC2 实例正在查询疑似恶意的域名。默认情况下，此警报会设置为低严重性，但随着分析阶段的深入，确定未经授权的行为者部署了数百个 `p4d.24xlarge` 类型 EC2 实例，导致组织运营成本

激增。在这种情况下，事件响应团队决定将此警报的严重程度调整为高，从而提升紧迫感并加快进一步的行动。请注意，GuardDuty 调查发现的严重性无法更改。

实施检测性控制措施

了解检测性控制措施的实施方式至关重要，因为这有助于确定警报将如何用于特定事件。检测性技术控制措施主要有两种实施方式：

- 行为检测依赖于通常称为机器学习（ML）或人工智能（AI）的数学模型。检测基于推断进行；因此，警报不一定反映实际事件。
- 基于规则的检测是确定性的；客户可以设定需要发出警报的确切活动参数，结果是确定的。

现代检测系统 [例如入侵检测系统（IDS）] 的实现通常同时包含这两种机制。以下是使用 GuardDuty 进行基于规则的检测和行为检测的一些示例。

- 调查发现 `Exfiltration:IAMUser/AnomalousBehavior` 生成后，将通知您，“在您的账户中观察到异常的 API 请求。” 当您进一步查阅文档时，将提示您“机器学习模型会评估您账户中的所有 API 请求，并识别与攻击者所用技术相关的异常事件”，这表明该调查发现具有行为检测的特性。
- 对于调查发现 `Impact:S3/MaliciousIPCaller`，GuardDuty 会分析 CloudTrail 中来自 Amazon S3 服务的 API 调用，将 `SourceIPAddress` 日志元素与包含威胁情报源的公有 IP 地址表进行比对。发现直接匹配的条目后，便会生成调查发现。

我们建议混合使用行为警报和规则警报，因为针对威胁模型中的每项活动发出基于规则的警报并非总是可行。

基于人员的检测

至此，我们讨论的都是基于技术的检测。另一个重要的检测源来自客户组织内部或外部的人员。内部人员可定义为员工或承包商，外部人员则包括安全研究人员、执法机构、新闻媒体和社交媒体等实体。

尽管基于技术的检测可以进行系统性配置，但基于人员的检测形式多种多样，包括电子邮件、工单、邮件、新闻文章、电话以及面对面交流。基于技术的检测通知有望近乎实时地发送，但对于基于人员的检测，则没有明确的时间预期。安全文化必须接纳、促进并充分发挥基于人员的检测机制的作用，以实现深度防御的安全方法。

摘要

在检测方面，将基于规则的警报与行为驱动的警报结合使用非常重要。此外，应构建相应机制，便于内部人员和外部人员就安全问题提交工单。工作人员可能是安全事件最宝贵的来源之一，因此制定供工作

人员上报疑虑的流程至关重要。您应利用针对环境的威胁模型来着手构建检测机制。威胁模型将帮助您基于与环境最相关的威胁来生成警报。最后，您可以借助 MITRE ATT&CK 等框架来了解威胁行为者的战术、技术和程序（TTP）。MITRE ATT&CK 框架可作为一种通用语言，促进您对各种检测机制的理解。

分析

日志、查询功能与威胁情报是分析阶段所需的一些支持性组成部分。检测阶段使用的许多相同日志同样适用于分析，但需要接入并配置查询工具。

验证警报、限定警报范围并评估其影响

在分析阶段，将执行全面的日志分析，旨在验证警报、定义范围并评估潜在入侵的影响。

- 警报验证是分析阶段的入口点。事件响应人员将查找来自各种源的日志条目，并直接联系受影响工作负载的所有者。
- 下一步是限定范围，在此过程中会清点所有涉及的资源，并在利益相关者一致认为不太可能是误报后，调整警报的严重性。
- 最后，影响分析会详细说明实际的业务中断情况。

确定受影响的工作负载组件后，便可将范围限定结果与相关工作负载的恢复点目标（RPO）和恢复时间目标（RTO）相关联，同时考虑调整警报严重性，这将启动资源分配以及后续的所有活动。并非所有事件都会直接中断支持业务流程的工作负载运营。敏感数据泄露、知识产权盗窃或资源劫持（例如用于加密货币挖矿）等事件可能不会立即停止或削弱业务流程，但可能在后期导致严重后果。

完善安全日志与调查发现

利用威胁情报和组织背景进行完善

在分析过程中，需要对值得关注的可观测对象进行完善，以提升警报的背景关联性。如“准备”一节所述，整合并利用网络威胁情报有助于更深入地了解安全调查发现。威胁情报服务可用于为公有 IP 地址、域名和文件哈希值分配信誉和属性所有权。这些工具既提供付费服务，也提供免费服务。

采用 Amazon Athena 作为日志查询工具的客户，可以利用 AWS Glue 作业的优势，将威胁情报信息加载为表格。威胁情报表可用于 SQL 查询，以关联 IP 地址和域名等日志元素，为待分析数据提供丰富视图。

AWS 不会向客户直接提供威胁情报，但 Amazon GuardDuty 等服务会利用威胁情报进行完善并生成调查发现。您也可以根据自己的威胁情报，将自定义威胁列表上传到 GuardDuty。

利用自动化进行完善

自动化是 AWS 云 治理不可或缺的一部分，可应用于事件响应生命周期的各个阶段。

在检测阶段，基于规则的自动化会匹配日志中威胁模型的关注模式，并采取相应的操作，例如发送通知。分析阶段可利用检测机制，将警报正文转发给能够查询日志和完善可观测对象以进行事件背景关联的引擎。

警报正文的基本形式由资源和身份组成。例如，您可以自动查询 CloudTrail，以了解警报正文的身份或资源在警报生成前后执行的 AWS API 活动，进而提供更多见解，例如已识别 API 活动的 `eventSource`、`eventName`、`SourceIPAddress` 和 `userAgent` 等等。通过执行这些自动化查询，响应人员可在分类期间节省时间，并获取更多背景情况，有助于做出更明智的决策。

请参阅博客文章《How to enrich AWS Security Hub findings with account metadata》，了解有关如何利用自动化功能完善安全调查发现并简化分析的示例。

收集和分析取证证据

如本文档the section called “准备”一节所述，取证是在事件响应期间收集和分析构件的过程。在 AWS 上，它不仅适用于基础架构域资源，例如网络流量数据包捕获、操作系统内存转储，也适用于服务域资源，例如 AWS CloudTrail 日志。

取证过程具有以下基本特征：

- 一致性：严格遵循所记录的确切步骤，没有偏差。
- 可重复性：对同一个构件重复执行操作时，会产生完全相同的结果。
- 惯用性：会公开记录并被广泛采用。

维护事件响应期间所收集构件的监管链至关重要。除了将构件存储在只读存储库外，使用自动化并生成此收集过程的自动文档也会有所帮助。应仅对所收集构件的精确副本进行分析，以保持完整性。

收集相关构件

牢记这些特性，基于相关警报以及对其影响范围的评估，需要收集与进一步调查和分析相关的数据。可能与调查相关的各类数据及其来源包括：服务/控制面板日志（CloudTrail、Amazon S3 数据事件、VPC 流日志）、数据（Amazon S3 元数据和对象）以及资源（数据库、Amazon EC2 实例）。

可收集服务/控制面板日志以进行本地分析，或者理想情况下，使用 AWS 原生服务直接查询（如适用）。可直接查询数据（包括元数据）以获取相关信息或获取源对象；例如，使用 AWS CLI 以获取 Amazon S3 存储桶和对象元数据，并直接获取源对象。必须按照与资源类型及预期分析方法相符的方

式收集资源。例如，可通过以下方式收集数据库：创建运行数据库的系统的副本/快照、创建整个数据库本身的副本/快照，或查询并提取数据库中与调查相关的特定数据和日志。

对于 Amazon EC2 实例，应收集一组特定数据，同时应遵循特定的收集顺序，以获取和保留最多数据以供分析和调查。

具体而言，从 Amazon EC2 实例获取和保留最多数据的响应顺序如下：

1. 获取实例元数据：获取与调查和数据查询相关的实例元数据（实例 ID、类型、IP 地址、VPC/子网 ID、区域、亚马逊机器映像（AMI）ID、附加的安全组、启动时间）。
2. 启用实例保护和标签：启用实例保护，例如终止保护、将关闭行为设为停止（如果设为终止）、禁用附加 EBS 卷的“终止时删除”属性，以及应用适当的标签以用于视觉标记和可能的响应自动化（例如，在应用名称为 `Status`、值为 `Quarantine` 的标签时，执行数据取证获取并隔离实例）。
3. 获取磁盘（EBS 快照）：获取附加 EBS 卷的 EBS 快照。每个快照包含将数据（拍摄快照时的数据）还原到新 EBS 卷所需的信息。如果您使用的是实例存储卷，请参阅执行实时响应/构件收集的步骤。
4. 获取内存：由于 EBS 快照只能捕获已写入 Amazon EBS 卷的数据（可能会排除应用程序或操作系统存储或缓存在内存中的数据），因此必须使用合适的第三方开源或商业工具获取系统内存映像，这样才能获取系统中的可用数据。
5. （可选）执行实时响应/构件收集：仅在无法通过其他方式获取磁盘或内存，或存在有效的业务或操作原因时，才能通过系统上的实时响应执行针对性数据收集（磁盘/内存/日志）。执行此操作将修改重要的系统数据和构件。
6. 停用实例：将实例与自动扩缩组分离、从负载均衡器注销实例，并调整或应用具有最低权限或无权限的预构建实例配置文件。
7. 隔离或遏制实例：通过终止和阻止当前及未来与该实例的双向连接，验证实例是否已与环境中的其他系统和资源有效隔离。有关详细信息，请参阅本文档的the section called “遏制”一节。
8. 响应人员选择：根据具体情况和目标，选择下列选项之一：
   - 停用并关闭系统（建议）。

     获取可用证据后关闭系统，以确保缓解措施是否最有效，防止实例将来可能会对环境造成的影响。
   - 在配备监控工具的隔离环境中继续运行实例。

     尽管不建议将其作为标准方法，但如果存在需要对实例进行持续观测的情况（例如需要其他数据或指标以对实例进行全面调查和分析时），可以考虑关闭实例，创建实例的 AMI，然后在已预置为完全隔离且配备检测工具（例如 VPC 流日志或 VPC Traffic Mirroring）的沙盒环境中，使用专用的取证账户重新启动该实例，以便近乎持续地监控该实例。

> **Note**
>
> 必须在执行实时响应活动、系统隔离或关闭之前捕获内存，这样才能捕获可用的易失性（且宝贵的）数据。

编写叙述

在分析和调查期间，需记录所采取的操作、执行的分析以及确定的信息，以供后续阶段使用，并生成最终报告。这些叙述应当简洁准确，确认包含相关信息以验证对事件的有效理解，并维护准确的时间线。与核心事件响应团队之外的人员交流时，这些叙述也很有帮助。示例如下：

> 市场销售部门于 2022 年 3 月 15 日收到一封勒索信函，要求支付加密货币，否则将公开发布潜在敏感数据。SOC 发现，属于市场销售部门的 Amazon RDS 数据库在 2022 年 2 月 20 日处于公开访问状态。SOC 查询了 RDS 访问日志，发现有人通过属于网站开发人员之一的 Major Mary 的凭证 *mm03434*，于 2022 年 2 月 20 日使用了 IP 地址 198.51.100.23。SOC 进一步查询了 VPC 流日志，发现约 256 MB 数据在同一天（时间戳 2022-02-20T15:50+00Z）外流至同一 IP 地址。SOC 通过开源威胁情报确定，该凭证目前在公共存储库 *https[:]//example[.]com/majormary/rds-utils* 中以纯文本形式提供。

遏制

就事件响应而言，遏制的一种定义是：在处理安全事件期间，为最大限度地缩小安全事件的范围并控制环境中未经授权使用的影响，所采取的策略执行或实现过程。

遏制策略取决于众多因素，不同组织在遏制战术的应用、时机和目的方面可能各不相同。《NIST SP 800-61 计算机安全事件处理指南》概述了确定适当遏制策略的几个标准，其中包括：

- 资源可能遭受损害甚至被窃取
- 需要保留证据
- 服务可用性（网络连接、向外部提供的服务）
- 实施策略所需的时间与资源
- 策略有效性（部分遏制或完全遏制）
- 解决方案持续时间（应急方案需在四小时内删除，临时方案需在两周内删除，以及永久方案）

然而，对于 AWS 上的服务，基本的遏制步骤可归纳为三类：

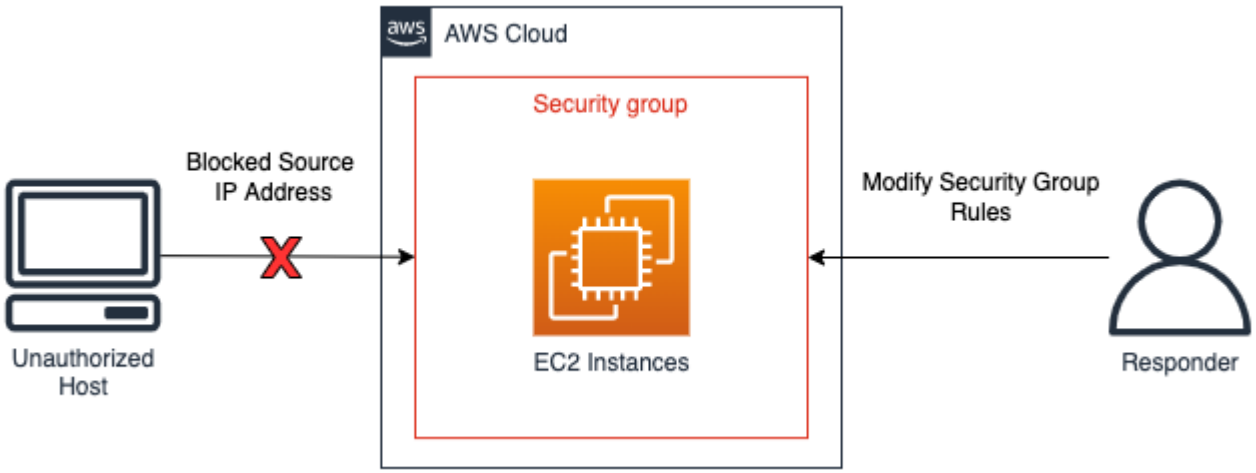
- 源遏制：使用筛选和路由功能，阻止来自特定源的访问。
- 技术与访问遏制：删除访问权限，阻止对受影响资源的未经授权的访问。
- 目标遏制：使用筛选和路由功能，阻止对目标资源的访问。

源容器

源遏制是指在环境中应用筛选和路由功能，阻止来自特定源 IP 地址或网络范围的资源访问。此处重点介绍了使用 AWS 服务进行源遏制的示例：

- 安全组：创建隔离安全组并将其应用于 Amazon EC2 实例，或从现有安全组中删除规则，有助于遏制流向 Amazon EC2 实例或 AWS 资源的未经授权的流量。请务必注意，更改安全组不会中断现有的已跟踪连接，新安全组只会有效阻止未来的流量（有关已跟踪和未跟踪连接的更多信息，请参阅 Incident Response Playbook 和安全组连接跟踪）。
- 策略：可配置 Amazon S3 存储桶策略，以阻止或允许来自 IP 地址、网络范围或 VPC 端点的流量。策略能够屏蔽可疑地址并阻止对 Amazon S3 存储桶进行访问。有关存储桶策略的更多信息，请参阅使用 Amazon S3 控制台添加存储桶策略。
- AWS WAF：可在 AWS WAF 上配置 Web 访问控制列表（Web ACL），以便对资源所响应的 Web 请求进行精细控制。可将 IP 地址或网络范围添加到 AWS WAF 上配置的 IP 集中，并对该 IP 集应用匹配条件（如“阻止”）。如果原始流量的 IP 地址或网络范围与 IP 集规则中配置的 IP 地址或网络范围相匹配，则这将阻止资源的 Web 请求。

如下图的源遏制示例所示，事件响应分析师修改了 Amazon EC2 实例的安全组，以限制仅允许特定 IP 地址的新连接。如前文安全组要点所述，更改安全组不会中断现有的已跟踪连接。



源遏制示例

> **Note**
>
> 安全组和网络 ACL 不会筛选发往 Amazon Route 53 的流量。在遏制 EC2 实例时，如果想阻止其联系外部主机，请确保同时显式阻止 DNS 通信。

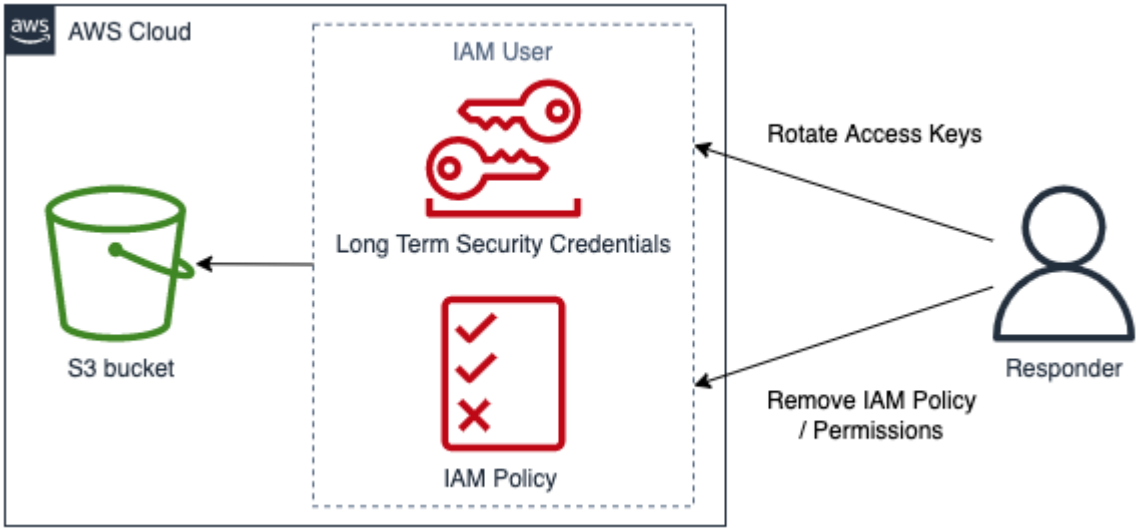
技术与访问遏制

通过限制功能和 IAM 主体对资源的访问权限，防止未经授权使用资源。这包括限制有权访问资源的 IAM 主体的权限；也包括撤销临时安全凭证。此处重点介绍了使用 AWS 服务进行技术与访问遏制的示例：

- 限制权限：分配给 IAM 主体的权限应遵循最低权限原则。但是，在活跃的安全事件期间，可能需要进一步限制特定 IAM 主体对目标资源的访问。在这种情况下，可以删除需遏制的 IAM 主体对资源的访问权限，以实现访问遏制。这是通过 IAM 服务完成的，可使用 AWS 管理控制台、AWS CLI 或 AWS SDK 进行操作。
- 撤销密钥：IAM 主体使用 IAM 访问密钥来访问或管理资源。这些是长期静态凭证，用于签署对 AWS CLI 或 AWS API 的编程请求，以前缀 AKIA 开头（有关更多信息，请参阅 IAM 标识符中的了解唯一 ID 前缀部分）。如果 IAM 访问密钥已遭泄露，可停用或删除该访问密钥以遏制 IAM 主体访问。请务必记住以下事项：
  - 可以重新激活已停用的访问密钥。
  - 访问密钥一经删除，将无法恢复。
  - 在给定的任何时间，IAM 主体最多可拥有两个访问密钥。
  - 密钥停用或删除后，使用该访问密钥的用户或应用程序将失去访问权限。
- 撤销临时安全凭证：组织可使用临时安全凭证来控制对 AWS 资源的访问权限，此类凭证以前缀 ASIA 开头（有关更多信息，请参阅 IAM 标识符中的了解唯一 ID 前缀部分）。临时凭证通常由 IAM 角色使用，因其生命周期有限，因此无需轮换或显式撤销。若在临时安全凭证到期前发生了涉及该凭证的安全事件，则可能需要更改现有临时安全凭证的有效权限。这可借助 AWS 管理控制台 中的 IAM 服务完成。临时安全凭证也可签发给 IAM 用户（与 IAM 角色相对）；然而，截至本文撰写时，尚无法在 AWS 管理控制台 中撤销 IAM 用户的临时安全凭证。如果发生某位用户的 IAM 访问密钥被创建临时安全凭证但未经授权的用户泄露的安全事件，可通过两种方法撤销临时安全凭证：
  - 将内联策略附加到 IAM 用户，根据安全令牌签发时间阻止访问（有关更多详细信息，请参阅禁用临时安全凭证的权限中的拒绝访问在特定时间之前签发的临时安全凭证部分）。
  - 删除访问密钥遭泄露的 IAM 用户。如有必要，可重新创建用户。

- AWS WAF：未经授权的用户所用的某些技术包括常见的恶意流量模式，例如包含 SQL 注入和跨站脚本攻击（XSS）的请求。可配置 AWS WAF，利用 AWS WAF 内置的规则语句匹配和拒绝使用这些技术的流量。

如下图技术与访问遏制示例所示，事件响应人员正在轮换访问密钥或删除 IAM 策略以阻止 IAM 用户访问 Amazon S3 存储桶。



技术与访问遏制示例

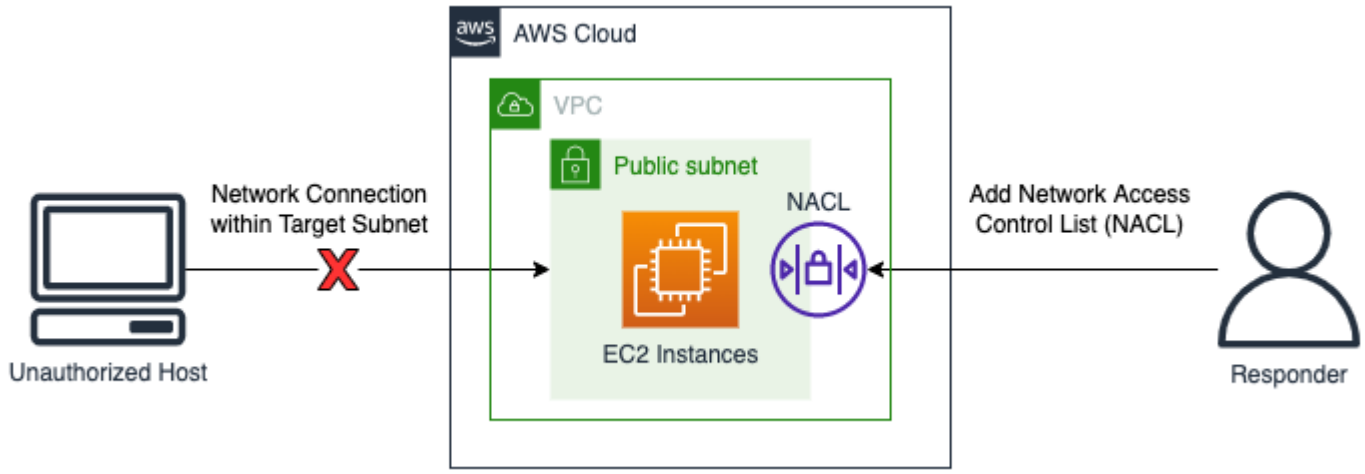
目标遏制

目标遏制是指在环境中应用筛选和路由功能，阻止对目标主机或资源的访问。在某些情况下，目标遏制还涉及某种形式的弹性，以确保对合法资源进行复制以保障可用性；应将资源与这些形式的弹性分离，以实现隔离和遏制。使用 AWS 服务进行目标遏制的示例包括：

- 网络 ACL：可在包含 AWS 资源的子网上配置的网络 ACL，还可以添加拒绝规则。这些拒绝规则可用于阻止对特定 AWS 资源的访问；但应用网络访问控制列表将影响子网上的所有资源，而不仅仅是正被未经授权访问的资源。网络 ACL 中列出的规则按自上而下的顺序进行处理，因此应将现有网络 ACL 中的首条规则配置为拒绝未经授权的流量流向目标资源和子网。或者，可以创建一个全新的网络 ACL，仅包含一条入站和出站流量的拒绝规则，并将其与包含目标资源的子网相关联，从而通过这个新的网络 ACL 阻止对子网的访问。
- 关闭：完全关闭资源可以有效遏制未经授权使用所造成的影响。但关闭资源也会阻止业务所需的合法访问，并妨碍获取易失性取证数据，因此这应是一个审慎的决定，并需根据组织的安全策略进行判断。

- 隔离 VPC：隔离 VPC 可用于有效遏制资源，同时允许访问合法流量 [例如需要访问互联网或外部管理控制台的防病毒（AV）或 EDR 解决方案]。在安全事件发生之前，可预置隔离 VPC，以允许有效的 IP 地址和端口。而在活跃的安全事件期间，可将目标资源立即移至该隔离 VPC，从而在遏制资源的同时，允许其在事件响应后续阶段发送和接收合法流量。使用隔离 VPC 的一个重要方面是，EC2 实例等资源需要先关闭，然后在新的隔离 VPC 中重新启动才能使用。现有 EC2 实例无法移至其他 VPC 或其他可用区。为此，请按照如何将我的 Amazon EC2 实例移动到其他子网、可用区或 VPC？中概述的步骤操作。
- 自动扩缩组和负载均衡器：作为目标遏制程序的一部分，应分离并取消注册附加到 自动扩缩组和负载均衡器的 AWS 资源。可使用 AWS 管理控制台、AWS CLI 和 AWS SDK，分离并取消注册 AWS 资源。

如下图目标遏制示例所示，事件响应分析师向子网添加了网络 ACL，以阻止来自未经授权的主机的网络连接请求。



目标遏制示例

摘要

遏制是事件响应流程中的一个步骤，可以手动完成，也可以自动执行。总体遏制策略应与组织的安全策略和业务需求保持一致，并确保在根除和恢复阶段之前尽可能有效地减轻负面影响。

根除

就安全事件响应而言，根除是指清除可疑或未经授权的资源，以使账户恢复到已知安全状态。根除策略取决于多种因素，而这些因素取决于组织的业务需求。

《NIST SP 800-61 计算机安全事件处理指南》提供了几个根除步骤：

1. 识别并缓解所有被利用的漏洞。
2. 清除恶意软件、不当材料及其他组件。
3. 如果发现更多受影响的主机（例如，新的恶意软件感染），则重复检测和分析步骤以识别所有其他受影响的主机，然后为其遏制和根除事件。

对于 AWS 资源，可通过可用日志或自动化工具（例如 CloudWatch Logs 和 Amazon GuardDuty）来检测和分析事件，进一步完善根除工作。应基于这些事件确定应当采取的补救措施，以将环境正确恢复到已知安全状态。

根除的第一步是确定 AWS 账户内哪些资源受到了影响。这可通过分析可用的日志数据来源、资源和自动化工具来实现。

- 识别账户中 IAM 身份采取的未经授权的操作。
- 识别对账户进行的未经授权的访问或更改。
- 识别创建的未经授权的资源或 IAM 用户。
- 识别存在未经授权的更改的系统或资源。

确定资源列表后，应对每项资源进行评估，以确定删除或恢复资源会产生的业务影响。例如，如果 Web 服务器托管业务应用程序，删除它会导致停机，那么在删除受影响的服务器之前，应考虑从经验证的安全备份中恢复资源，或者从纯净 AMI 重新启动系统。

完成业务影响分析后，应基于日志分析中的事件，进入账户并执行适当的补救措施，例如：

- 轮换或删除密钥：此步骤可使行为者无法继续在账户中执行活动。
- 轮换可能未经授权的 IAM 用户凭证。
- 删除无法识别或未经授权的资源。

> **Important**
>
> 如果出于调查需要必须保留资源，请考虑将这些资源备份。例如，如果出于监管、合规或法律原因必须保留 Amazon EC2 实例，请在删除该实例前创建 Amazon EBS 快照。

- 对于恶意软件感染，可能需要联系 AWS Partner 或其他供应商。AWS 不提供用于恶意软件分析或删除的原生工具。但是，如果您使用的是适用于 Amazon EBS 的 GuardDuty 恶意软件模块，则提供的调查发现可能会包含相关建议。

在根除确定的受影响资源后，AWS 会建议您对账户进行安全审查。这可以借助 AWS Config 规则、Prowler 和 ScoutSuite 等开源解决方案，或通过其他供应商来完成。还应考虑对面向公众（互联网）的资源执行漏洞扫描，以评估残余风险。

根除是事件响应流程中的一个步骤，可以手动完成，也可以自动执行，具体取决于事件和受影响的资源。总体策略应与组织的安全策略和业务需求保持一致，并确保在删除不当资源或配置后减轻负面影响。

恢复

恢复是指将系统恢复到已知安全状态的流程，在此期间，需要在恢复之前确认备份是否安全或未受事件影响，然后进行测试以确认系统在恢复后正常运行，以及解决与安全事件相关的漏洞。

恢复顺序取决于组织的要求。作为恢复流程的一部分，需要进行业务影响分析，至少确定：

- 业务或依赖项的优先级
- 恢复计划
- 身份验证和授权

《NIST SP 800-61 计算机安全事件处理指南》提供了几个系统恢复步骤，包括：

- 从纯净备份恢复系统。
  - 在将备份恢复到系统之前，需确认是否对备份进行评估，排除感染情况，防止安全事件卷土重来。

    作为灾难恢复测试的一部分，应定期评估备份，以确认备份机制是否正常运行以及数据完整性是否符合恢复点目标。
  - 如果可能，请使用在根本原因分析中确定的第一个事件时间戳之前的备份。
- 从头开始重建系统，包括使用自动化工具从可信来源重新部署（有时需要在新 AWS 账户中进行）。
- 将受损文件替换为纯净版本。

  执行此操作时应格外小心。必须完全确定要恢复的文件处于已知安全状态，且未受事件影响
- 安装补丁。
- 更改密码。
  - 这包括可能已被滥用的 IAM 主体的密码。
  - 如果可能，建议采用适用于 IAM 主体和联合身份验证的角色，作为最低权限策略的一部分。
- 加强网络周边安全（防火墙规则集、周边路由器访问控制列表）。

资源恢复后，必须总结经验教训，以更新事件响应策略、程序和指南。

总之，必须实施恢复已知安全运营的恢复流程。恢复可能需要很长时间，并且需要密切结合遏制策略，以平衡业务影响和再次感染的风险。恢复程序应当包括恢复资源和服务、IAM 主体的步骤，以及对账户进行安全审查以评估残余风险的步骤。

结论

每个运营阶段都有其独特的目标、技术、方法和策略。表 4 总结了这些阶段以及本节涵盖的一些技术和方法。

表 4 – 运营阶段：目标、技术和方法

阶段	目标	技术和方法
检测	识别潜在的安全事件。	• 用于检测的安全控制措施 • 行为检测和基于规则的检测 • 基于人员的检测
分析	确定安全事件是否为意外事件，并评估事件的影响范围。	• 验证警报和限定警报范围 • 查询 日志 • 威胁情报 • 自动化
遏制	尽量减小和限制安全事件的影响。	• 源容器 • 技术与访问遏制 • 目标遏制
根除	移除与安全事件相关的未经授权的资源或构件。	• 轮换或删除已泄露或未经授权的凭证 • 删除未经授权的资源 • 清除恶意软件 • 安全扫描
恢复	将系统恢复到已知安全状态并监控这些系统，以确保威胁不会再次出现。	• 从备份恢复系统 • 从头开始重建系统 • 将受损文件替换为纯净版本

事件后活动

威胁形势在不断变化，您的组织必须具备同样的动态性，才能有效保护自己的环境。持续改进的关键在于对事件和模拟的结果进行迭代，以提高有效检测、响应和调查潜在安全事件的能力，从而减少潜在漏洞，缩短响应时间，最终恢复安全运营。以下机制有助于验证您的组织是否已经准备就绪，可以利用最新的功能和知识有效应对任何情形。

建立从事件中吸取经验教训的框架

实施经验教训总结框架和方法不仅有助于提高事件响应能力，还有助于防止事件再次发生。通过从每次事件中吸取教训，您可以避免重复同样的错误、泄露或错误配置，这不仅可以改善您的安全态势，还可以最大限度地减少因可预防的情况而损失的时间。

重要的是要实现一个经验教训总结框架，大体上确立并实现以下几点：

- 何时总结经验教训？
- 总结经验教训的过程涉及什么？
- 如何总结经验教训？
- 谁参与了这个过程，具体情况如何？
- 如何确定需要改进的领域？
- 如何确保有效跟踪和实施改进措施？

除了这些列出的大体上的成果外，重要的是要确保提出正确的问题，以便从流程中获得最大价值（可以带来切实可行的改进的信息）。请考虑以下问题，以便于您启动经验教训讨论：

- 发生了什么事件？
- 何时首次发现该事件？
- 是如何发现的？
- 哪些系统针对该活动发出了警报？
- 涉及哪些系统、服务和数据？
- 具体发生了什么？
- 哪些地方做得好？
- 哪些地方做得不好？
- 哪些流程或程序出现问题或未能扩展以应对事件？
- 以下方面有哪些地方有待改进：

- 人员
  - 需要联系的人是否真的可以联系上，联系名单是否是最新名单？
  - 相应人员是否缺少有效应对和调查事件所需的培训或能力？
  - 相应的资源是否已就绪并随时可用？
- 流程
  - 是否遵循了流程和程序？
  - 是否针对这种事件记录并提供了流程和程序？
  - 是否缺少必要的流程和程序？
  - 响应人员是否能够及时获得所需的信息来处理问题？
- 技术
  - 现有警报系统是否能有效识别活动并发出警报？
  - 现有警报是否需要改进，或者是否需要针对这种事件设置新的警报？
  - 现有工具是否允许对事件进行有效调查（搜索/分析）？
- 怎样才能更快地识别这种事件？
- 如何防止这种事件再次发生？
- 谁是改进计划的负责人，如何检验改进计划的执行情况？
- 实施和测试额外监控/预防性控制机制/流程的时间表是怎样的？

此列表并非详尽无遗；旨在作为一个起点，确定组织和业务需求是什么，以及如何分析这些需求，以便最有效地从事件中吸取经验教训，并不断改进您的安全态势。最重要的是，该列表开始将经验教训作为事件响应流程、文档和利益相关方期望的标准组成部分。

设立成功指标

指标对于有效衡量、评估和提高事件响应能力至关重要。没有指标，就没有参考，无法准确衡量甚至确定组织表现的好坏。事件响应有几个常见指标，对于希望建立卓越运营期望和相关基准的组织而言，是很好的入手点。

平均检测时间

平均检测时间是指发现潜在安全事件所需的平均时间。具体而言，这是从首次出现漏洞指标，到初步识别或生成警报之间的时间。

您可以使用此指标来跟踪检测和警报系统的有效性。有效的检测和警报机制是确保潜在安全事件不会在环境中持续存在的关键。

平均检测时间越长，就越需要建立更多或更有效的警报和机制来识别和发现潜在安全事件。平均检测时间越短，表明检测和警报机制运行得越好。

平均确认时间

平均确认时间是指确认潜在安全事件并确定其处理优先级所需的平均时间。具体而言，这是从生成警报，到 SOC 成员或事件响应人员识别警报并确定其优先级以进行处理之间的时间。

您可以使用此指标来跟踪团队处理警报和确定其优先级的效率。如果团队无法有效识别警报并确定其优先级，响应将会延迟甚至无效。

平均确认时间越长，就越需要确保团队拥有充足资源并且接受了适当培训，能够快速确认潜在安全事件并确定其优先级以进行响应。平均确认时间越短，表明团队的安全警报响应能力越强，因为这说明他们准备充分且能有效确定警报优先级。

平均响应时间

平均响应时间是指开始对潜在安全事件做出初始响应所需的平均时间。具体而言，这是从首次发出警报或发现潜在安全事件，到采取首个响应行动之间的时间。这与平均确认时间类似，不同之处在于其衡量的是具体的响应行动（例如，获取系统数据、遏制系统），而不仅仅是对情况的简单识别或确认。

您可以使用此指标来跟踪您在响应安全事件方面的准备情况。如前所述，充分准备是有效响应的关键。请参阅本文档的the section called “准备”一节。

平均响应时间越长，就越需要确保团队接受过充分的响应培训，从而使响应流程得到有效记录和运用。平均响应时间越短，表明团队越擅长针对已识别的警报确定适当的响应措施，并执行必要的响应行动以启动恢复安全运营的进程。

平均遏制时间

平均遏制时间是指遏制潜在安全事件所需的平均时间。具体而言，这是从首次发出警报或发现潜在安全事件，到完成有效阻止攻击者或受损系统造成进一步危害的响应行动之间的时间。

您可以使用此指标来跟踪团队在缓解或遏制潜在安全事件方面的能力。如果无法快速有效地遏制潜在安全事件，将增加其影响范围，并可能导致进一步危害。

平均遏制时间越长，就越需要积累知识和提升能力，以便快速有效地缓解和遏制遇到的安全事件。平均遏制时间越短，表明团队越擅长理解和采取必要措施来缓解和遏制已确定的威胁，从而减少其影响范围，并降低业务风险。

平均恢复时间

平均恢复时间是指从潜在安全事件完全恢复安全运营所需的平均时间。具体而言，这是从首次发出警报或发现潜在安全事件，到业务恢复正常、安全运营且不再受事件影响之间的时间。

您可以使用此指标来跟踪团队在安全事件发生后使系统、账户和环境恢复安全运营的有效性。无法迅速或有效地恢复安全运营，不仅会影响安全性，还会增加对业务及其运营造成的影响及相关成本。

平均恢复时间越长，就越需要让团队和环境做好准备，建立适当的机制（例如，失效转移流程以及用于重新部署安全纯净系统的 CI/CD 管道），以最大限度地减少安全事件对运营和业务的影响。平均恢复时间越短，表明团队在最大限度减少安全事件对运营和业务影响方面越有效。

攻击者驻留时间

攻击者驻留时间是指未经授权的用户访问系统或环境的平均时间。这与平均遏制时间类似，不同之处在于其时间范围始于攻击者首次获得系统或环境访问权限的时间，该时间可能早于首次发出警报或发现潜在安全事件的时间。

您可以使用此指标来跟踪多个系统与机制的协同工作情况，以缩短攻击者或威胁影响环境的时间、访问权限及机会。缩短攻击者驻留时间应是团队和业务的首要任务。

攻击者驻留时间越长，就越需要确定事件响应流程中哪些部分需要改进，以确保团队能够最大限度地减少威胁或攻击对环境的影响范围。攻击者驻留时间越短，表明团队在最大限度减少威胁或攻击者在环境中的时间和机会方面做得越好，最终降低了运营风险和对业务的影响。

指标汇总

通过建立和跟踪事件响应指标，您可以有效地衡量、评估和提高事件响应能力。为此，本节重点介绍了一些常见的事件响应指标。表 5 将这些指标进行了汇总。

表 5 – 事件响应指标

指标	说明
平均检测时间	发现潜在安全事件所需的平均时间
平均确认时间	确认潜在安全事件（并确定其优先级）所需的平均时间
平均响应时间	开始对潜在安全事件做出初始响应所需的平均时间

指标	说明
平均遏制时间	遏制潜在安全事件所需的平均时间
平均恢复时间	从潜在安全事件完全恢复安全运营所需的平均时间
攻击者驻留时间	攻击者访问系统或环境的平均时间

使用漏洞指标（IOC）

漏洞指标（IOC）是在网络、系统或环境中观察到的一种构件，它可以（以高置信度）识别恶意活动或安全事件。IOC 能够以多种形式存在，包括 IP 地址、域、网络级构件（例如 TCP 标志或有效载荷）、系统或主机级构件（例如可执行文件、文件名和哈希值、日志文件条目或注册表条目等）。IOC 也可以是项目或活动的组合，例如系统中存在的特定项目或构件（某个文件或一组文件及注册表项）、按特定顺序执行的操作（从特定 IP 登录系统后执行特定异常命令）、或网络活动（进出特定域的异常入站或出站流量），这些组合能够指示特定的威胁、攻击或攻击者手法。

在迭代改进事件响应计划的过程中，应实施一个框架来收集、管理和利用 IOC，以此作为持续构建和改进检测与警报的机制，同时提高调查速度和有效性。首先，您可以将收集与管理 IOC 纳入事件响应流程的分析和调查阶段。通过主动识别、收集和存储 IOC，并将其作为流程的标准部分，您可以构建数据存储库（作为更全面的威胁情报计划的一部分），该存储库反过来又可以用于改进现有的检测和警报、构建额外的检测和警报、识别某个构件之前出现的位置和时间、构建和参考涉及匹配 IOC 的既往调查方式的文档等等。

继续教育和培训

教育和培训是不断发展、持续改进的，应当有目的地规划并坚持。有多种机制可用于确认团队是否保持着与不断发展的技术状态以及威胁形势相称的认知、知识和能力。

一种机制是将继续教育作为团队目标和运营的标准组成部分。如“准备”一节所述，必须对事件响应人员和利益相关者进行有效培训，使其掌握在 AWS 中检测、响应和调查事件的能力。然而，教育不是一个可以“一蹴而就”的工程。必须持续开展教育，以确认团队始终了解新的技术进步、更新和改进（这些信息可用于提高响应的有效性和效率），以及可用于改进调查和分析的数据新增或更新内容。

另一种机制是确保定期进行模拟（例如每季度一次），并侧重于实现特定的业务成果。请参阅本文档的the section called “定期进行模拟”一节。

尽管进行初始桌面演练是建立改进初始基准的好办法，但是对于实现持续改进以及确保得到对当前运营状态最新的精确反映而言，持续测试才是关键。针对最新、最关键的安全情况以及最重要或最新的响应能力进行测试，并将总结的经验教训重新纳入教育、运营和流程/程序中，将确保您能够持续改进整个响应流程和计划。

结论

在继续云之旅的过程中，考虑适用于 AWS 环境的基本安全事件响应概念至关重要。您可以结合使用可用控制措施、云功能及修复选项，以提高云环境的安全性。您也可以从小处着手，在采用可提高响应速度的自动化功能时进行迭代，以便在发生安全事件时做好更充分的准备。

贡献者

本文档的当前及过往贡献者包括：

- Anna McAbee，Amazon Web Services 高级安全解决方案架构师
- Freddy Kasprzykowski，Amazon Web Services 高级安全顾问
- Jason Hurst，Amazon Web Services 高级安全工程师
- Jonathon Poling，Amazon Web Services 首席安全顾问
- Josh Du Lac，Amazon Web Services 安全解决方案架构高级经理
- Paco Hope，Amazon Web Services 首席安全工程师
- Ryan Tick，Amazon Web Services 高级安全工程师
- Steve de Vera，Amazon Web Services 高级安全工程师

附录 A：云功能定义

AWS 提供 200 多种云服务和数千种功能。其中许多功能可提供本机检测、预防和响应功能，而其他功能则可用于构建自定义安全解决方案。本节包含与云中事件响应最相关的部分服务。

主题

- 未来与自定义安全功能

日志记录和事件

AWS CloudTrail：AWS CloudTrail 服务支持对 AWS 账户进行治理、合规、运营审计和风险审计。借助 CloudTrail，您可以记录、持续监控和保留与跨 AWS 服务操作相关的账户活动。CloudTrail 提供 AWS 账户活动的事件历史记录，包括通过 AWS 管理控制台、AWS SDK、命令行工具和其他 AWS 服务执行的操作。该事件历史记录简化了安全分析、资源变更跟踪和故障排除工作。CloudTrail 记录了两种不同类型的 AWS API 操作：

- CloudTrail 管理事件（也称为控制面板操作）会显示对 AWS 账户内的资源执行的管理操作。这包括创建 Amazon S3 存储桶和设置日志记录等操作。
- CloudTrail 数据事件（也称为数据面板操作）显示在 AWS 账户内的资源上或资源内执行的资源操作。这些操作通常是大规模活动。这包括 Amazon S3 对象级 API 活动（例如 `GetObject`、`DeleteObject` 和 `PutObject` API 操作）以及 Lambda 函数调用活动等操作。

AWS Config：AWS Config 服务使客户能够评测、审计和评估 AWS Config 资源的配置。AWS 可以持续监控和记录客户的 AWS 资源配置，并让其能够依据配置需求自动评估记录的配置。借助 AWS Config，客户可以手动或自动查看配置更改以及 AWS 资源之间的关系、详细的资源配置历史记录，并判断配置在整体上是否符合客户指南中所指定的配置要求。这可以简化合规性审核、安全性分析、变更管理和操作故障排除。

Amazon EventBridge：Amazon EventBridge 可提供近乎实时的系统事件流，这些系统事件描述了 AWS 资源中的更改，或者 AWS CloudTrail 发布 API 调用的时间。通过使用可快速设置的简单规则，您可以匹配事件并将事件路由到一个或多个目标函数或流。EventBridge 可在发生操作更改时感知到这些更改。EventBridge 可以响应这些操作更改并在必要时采取纠正措施，方式是发送消息以响应环境、激活函数、进行更改并捕获状态信息。一些安全服务（如 Amazon GuardDuty），以 EventBridge 事件的形式生成输出。许多安全服务还提供向 Amazon S3 发送输出的选项。

Amazon S3 访问日志：如果敏感信息存储在 Amazon S3 存储桶中，客户可以启用 Amazon S3 访问日志来记录相关数据的每次上传、下载和修改。该日志独立于 CloudTrail 日志（并作额外补充），CloudTrail 日志可用于记录存储桶本身的更改（例如更改访问策略和生命周期策略）。需要注意的是，访问日志记录会以最大努力进行传输。针对已正确配置了日志记录的存储桶的大多数请求会导致传输一条日志记录。因此不能保证服务器日志记录的完整性和即时性。

Amazon CloudWatch Logs：客户可以通过 Amazon CloudWatch Logs 代理监控、存储和访问来自 Amazon EC2 实例上运行的操作系统、应用程序和其他来源的日志文件。CloudWatch Logs 可以作

为 AWS CloudTrail、Route 53 DNS 查询、VPC 流日志、Lambda 函数等的目的地。客户随后可以从 CloudWatch Logs 中检索关联的日志数据。

Amazon VPC 流日志：VPC 流日志使客户能够捕获有关在 VPC 中传入和传出网络接口的 IP 流量的信息。启用流日志后，可以将其流式传输到 Amazon CloudWatch Logs 和 Amazon S3。VPC 流日志可帮助客户完成诸多任务，例如排查特定流量无法到达实例的原因、诊断过于严格的安全组规则，以及将其用作监控 EC2 实例流量的安全工具。使用最新版本的 VPC 流日志记录可获取最全面的字段信息。

AWS WAF 日志：AWS WAF 支持完整记录该服务检查的所有 Web 请求。客户可将其存储在 Amazon S3 中，以满足合规和审计要求，以及用于调试和取证。这些日志可帮助客户确定规则触发和 Web 请求被阻止的根本原因。日志可与第三方 SIEM 和日志分析工具集成。

Route 53 Resolver 查询日志：Route 53 Resolver 查询日志便于您记录 Amazon Virtual Private Cloud（Amazon VPC）内资源发出的所有 DNS 查询。无论是 Amazon EC2 实例、AWS Lambda 函数还是容器，只要其位于 Amazon VPC 中且发出 DNS 查询，此功能都会将其记录下来；之后您就能够探索并更好地理解应用程序的运行情况。

其他 AWS 日志：AWS 将持续为客户发布包含新日志记录和监控功能的服务特性与功能。有关每项 AWS 服务可用功能的信息，请参阅我们的公共文档。

可见性和警报

AWS 安全事件响应— AWS 安全事件响应 是一项综合服务，通过将自动化功能与专业人力支持相结合，帮助组织在整个生命周期中处理安全事件。该服务利用自动监控和调查功能来腾出组织资源，同时保持警惕的安全监督，当安全事件发生时，它有助于加快利益相关者之间的沟通和协调，从而加快响应时间。该服务支持多种使用案例，包括安全事件的准备和模拟、对活动事件的响应以及简化的事后报告和分析，确保组织有能力应对每个阶段的安全挑战。

AWS Security Hub CSPM：AWS Security Hub CSPM 可为客户提供跨 AWS 账户的高优先级安全警报与合规状态的全面视图。Security Hub CSPM 可以聚合、组织来自 AWS 服务（例如 Amazon GuardDuty、Amazon Inspector、Amazon Macie）和 AWS Partner解决方案的威胁调查发现并确定优先级。通过包含可操作图表和表格的集成控制面板，对调查发现进行直观汇总。您还可以基于 AWS 最佳实践及组织所遵循的行业标准，使用自动化合规性检查对环境进行持续监控。

Amazon GuardDuty：Amazon GuardDuty 是一项托管的威胁检测服务，可以持续监控恶意或未经授权的行为，从而帮助客户保护 AWS 账户和工作负载。Amazon GuardDuty 可以监控异常的 API 调用或可能未经授权的部署等活动，这些活动表明 Amazon EC2 实例、Amazon S3 存储桶的账户或资源可能遭到破坏或者有恶意行为者正在进行侦察。

GuardDuty 通过集成的威胁情报源识别可疑的不良行为者，利用机器学习检测账户和工作负载活动中的异常情况。检测到潜在威胁后，该服务便会向 GuardDuty 控制台和 CloudWatch Events 发送详细的安全警报。这样一来，警报将具有可操作性，并且能轻松集成到现有的事件管理和工作流程系统中。

GuardDuty 还提供两个附加组件，用于监控特定服务的威胁：用于保护 Amazon S3 的 Amazon GuardDuty 以及用于保护 Amazon EKS 的 Amazon GuardDuty。Amazon S3 防护使 GuardDuty 能够监控对象级 API 操作，以识别 Amazon S3 存储桶中数据的潜在安全风险。Kubernetes 保护有助于 GuardDuty 检测 Amazon EKS 中 Kubernetes 集群的可疑活动和潜在漏洞。

Amazon Macie：Amazon Macie 是一项人工智能驱动的安全服务，通过自动发现、分类和保护存储在 AWS 中的敏感数据来防止数据丢失。Macie 利用机器学习（ML）来识别敏感数据，例如个人身份信息（PII）或知识产权，为其分配业务价值，并提供关于这些数据存储位置及其在组织中使用情况的见解。Amazon Macie 会持续监控数据访问活动是否存在异常情况，并在检测到未经授权的访问或无意的数据泄露风险时发出警报。

AWS Config 规则：AWS Config 规则代表资源的首选配置，会根据 AWS Config 记录的相关资源配置更改进行评估。您可以在控制面板上查看针对资源配置评估规则的结果。借助 AWS Config 规则，您可以从配置角度评估总体合规性和风险状态，查看一段时间内的合规性趋势，并找出哪些配置更改导致资源违反规则。

AWS Trusted Advisor：AWS Trusted Advisor 是一种在线资源，可通过优化 AWS 环境来帮助您降低成本、提高性能和增强安全性。Trusted Advisor 可提供实时指南，帮助您按照 AWS 最佳实践预置资源。全套 Trusted Advisor 检查（包括 CloudWatch Events 集成）可供商业和企业支持计划的客户使用。

Amazon CloudWatch：Amazon CloudWatch 是一项针对 AWS 云 资源以及您在 AWS 运行的应用程序的监控服务。您可以使用 CloudWatch 收集和跟踪指标、收集和监控日志文件、设置警报并自动对 AWS 资源中的更改做出反应。CloudWatch 可以监控 AWS 资源，例如 Amazon EC2 实例、Amazon DynamoDB 表和 Amazon RDS 数据库实例，以及您的应用程序和服务生成的自定义指标以及您的应用程序生成的任何日志文件。您可以通过使用 Amazon CloudWatch 全面地了解资源利用率、应用程序性能和运行状况。使用这些分析结果，您可以及时做出相应反应，保证应用程序顺畅运行。

Amazon Inspector：Amazon Inspector 是一项自动安全评估服务，有助于提高部署在 AWS 上的应用程序的安全性与合规性。Amazon Inspector 会自动评估应用程序的漏洞以及偏离最佳实践的情况。执行评估后，Amazon Inspector 将生成按严重性级别优先排序的安全调查发现详细列表。这些调查发现可以直接查看，也可以作为详细评估报告的一部分进行查看，报告则可通过 Amazon Inspector 控制台或 API 获取。

Amazon Detective：Amazon Detective 是一项安全服务，可自动从 AWS 资源收集日志数据，并利用机器学习、统计分析和图形理论构建一组关联数据，以帮助您更快、更高效地进行安全调

查。Detective 可分析来自多个数据来源（例如 VPC 流日志、CloudTrail 和 GuardDuty）的数万亿个事件，并自动创建统一的交互式视图，供您了解资源、用户及此类行为随时间推移的相互作用。借助此统一视图，在一个位置就能查看所有细节和背景情况，以确定调查发现的根本原因，深入探究相关的历史活动，并快速确定根本原因。

自动化

AWS Lambda：AWS Lambda 是一项无服务器计算服务，可运行代码来响应事件并为您自动管理底层计算资源。您可以使用 Lambda 通过自定义逻辑扩展其他 AWS 服务，或创建您自己的按 AWS 规模、性能和安全性运行的后端服务。Lambda 会在可用性高的计算基础设施上运行您的代码，并为您执行计算资源的管理工作。这包括服务器和操作系统维护、容量预置、自动扩展、代码和安全补丁部署以及代码监控和日志记录。您只需提供代码即可。

AWS Step Functions：AWS Step Functions 让您通过可视工作流程，轻松协调分布式应用程序和微服务的组件。Step Functions 提供图形控制台，您可以排列应用程序的组件，并将其直观地展示为一系列步骤。这样就可以轻松构建和运行多步骤应用程序。Step Functions 可以自动开始和跟踪各个步骤，并在出现错误时重试，因此您的应用程序能够按照预期顺序运行。

Step Functions 会记录每个步骤的状态，这样在出现错误时，您就能够迅速诊断并调试问题。您无需编写代码即可更改和添加步骤，因而可以更快地改进应用程序并进行创新。AWS Step Functions 是 AWS Serverless 的一部分，可以轻松编排无服务器应用程序中的 AWS Lambda 函数。您还可以使用 Step Functions，借助 Amazon EC2 和 Amazon ECS 等计算资源进行微服务编排。

AWS Systems Manager：AWS Systems Manager 让您能够查看和控制 AWS 上的基础设施。Systems Manager 可以提供一个统一的用户界面，供您查看多种 AWS 服务的运行数据，并且便于您在 AWS 资源上自动执行操作任务。借助 Systems Manager，您可以按应用程序对资源进行分组，查看用于监控和故障排除的操作数据，并对资源组执行操作。Systems Manager 可以使实例保持预先设定状态，执行按需更改（例如更新应用程序或运行 shell 脚本），以及执行其他自动化和修补任务。

安全存储

Amazon Simple Storage Service：Amazon S3 是一种对象存储，旨在从任何地方存储和检索任意数量的数据。它可提供 99.999999999% 的持久性，并为各行各业市场领导者所使用的数百万个应用程序存储数据。Amazon S3 可提供全面的安全保护，旨在帮助您满足监管要求。它为客户提供了灵活的数据管理方法，可实现成本优化、访问控制和合规性。此外，Amazon S3 可提供就地查询功能，便于您直接对 Amazon S3 中的静态数据进行强大的分析。Amazon S3 是一项得到广泛支持的云存储服务，集成了由第三方解决方案、系统集成商合作伙伴和其他 AWS 服务组成的其中一个最大社区。

Amazon Glacier：Amazon Glacier 是一项安全、持久且成本极低的云存储服务，适用于数据存档和长期备份。它可提供 99.999999999% 的持久性以及全面的安全保护，旨在帮助您满足监管要求。Amazon Glacier 可提供就地查询功能，便于您直接静态存档数据进行强大的分析。为了降低成本同时满足不同的检索需求，Amazon Glacier 提供了三种存档访问选项，用时从几分钟到几小时不等。

未来与自定义安全功能

上述服务和功能并非详尽列表。AWS 正在不断添加新功能。有关更多信息，我们建议您查看 AWS 的新功能 与 AWS 云安全性页面。除了 AWS 作为原生云服务提供的安全服务外，您可能还有兴趣基于 AWS 服务构建自己的安全功能。

尽管我们建议在账户中启用一组基本的安全服务（如 AWS CloudTrail、Amazon GuardDuty 和 Amazon Macie），但您最终可能希望扩展这些功能，以从日志资产中获得更多价值。有多款合作伙伴工具可供选择，例如 APN 安全能力计划中列出的工具。您可能还想编写自己的查询来搜索日志。没问题，借助 AWS 提供的大量托管服务，这将变得前所未有的简单。许多其他 AWS 服务也可帮助您进行调查，但这些服务不在本文的讨论范围之内，例如 Amazon Athena、Amazon OpenSearch Service、Amazon Quick、Amazon Machine Learning 和 Amazon EMR。

附录 B：AWS 事件响应资源

AWS 会发布资源以帮助客户构建事件响应能力。有关大多数示例代码和程序，请参阅 AWS 外部 GitHub 公共存储库。以下是一些可以提供如何执行事件响应示例的资源。

行动手册资源

- 事件响应行动手册框架：一个示例框架，供客户在使用 AWS 服务时创建、制定和集成安全行动手册，为潜在的攻击场景做好准备。
- 事件响应行动手册样本：该行动手册涵盖了 AWS 客户面临的常见场景。
- AWS 宣布开放五场公开讲习会。

取证资源

- 自动事件响应和取证框架：一种提供标准数字取证流程的框架和解决方案，涉及以下阶段：遏制、采集、检查和分析。它利用 AWS Λ 函数，以自动化、可重复的方式触发事件响应流程。它可提供分割账户，以操作自动化步骤、存储工件和创建取证环境。
- 适用于 Amazon EC2 的自动取证编排工具：此实施指南提供了一种自助服务解决方案，用于在检测到潜在安全问题时捕获和检查来自 EC2 实例及附加卷的数据，以进行取证分析。此外，还提供用于部署解决方案的 AWS CloudFormation 模板。

- 如何在 AWS 中自动实施取证磁盘收集：此 AWS 博客文章详细介绍了如何设置自动化工作流程以捕获磁盘证据用于分析，从而确定潜在安全事件的范围和影响。此外，还提供用于部署解决方案的 AWS CloudFormation 模板。

版权声明

文档历史记录

下表介绍了自 2026 年 1 月 1 日以来对 AWS 安全事件响应文档的重要补充。如需有关此文档的更新通知，您可以订阅 RSS 源。

变更	说明	日期
添加了 EC2 Triage 支持的操作系统	添加了 EC2 Triage 功能支持的操作系统列表，包括 Linux 发行版（Amazon Linux 2、Amazon Linux 2023、Ubuntu、RHEL、CentOS、SLES 和 Debian）和 Windows Server 版本。	2026 年 4 月 29 日
更新了 AWSSecurityIncidentResponseReadOnlyAccess 的策略描述	更新了策略以添加 `security-ir:ListInvestigations` 操作。	2026 年 4 月 22 日
更新了 AWSSecurityIncidentResponseFullAccess 的策略描述	更新了策略以添加 AWS Organizations 权限，并删除了 MFA 条件。	2026 年 4 月 22 日
更新了 AWSSecurityIncidentResponseCaseFullAccess 的策略描述	更新了策略以添加 `security-ir:ListInvestigations` 和 `security-ir:SendFeedback` 操作，并删除了 MFA 条件。	2026 年 4 月 22 日
用于 AWS 安全事件响应的 EC2 Triage 功能	添加了 EC2 Triage 功能，使 AWS 安全事件响应能够在安全调查期间使用 AWS Systems Manager Run Command 从 Amazon Elastic Compute Cloud 实例收集调查信息。更	2026 年 4 月 20 日

	新了“检测和分析”页面，以记录 EC2 Triage 先决条件和功能。	
用于 AWS 安全事件响应的 EC2 Triage 功能	更新了 CloudFormation StackSets 文档以提供两个模板选项：“仅遏制”和“带有 EC2 Triage 的遏制”。“带有 EC2 Triage 的遏制”模板包括从 Amazon EC2 实例收集调查数据的额外权限。	2026 年 4 月 20 日
受监管客户的数据收集、区域行为和合规性指导	添加了有关数据收集和使用、数据驻留和区域行为以及数据访问和权限的新章节。扩展了合规性验证部分，为受监管行业的客户提供了责任共担和元数据分类指导。	2026 年 4 月 17 日
更新了入门指南	使用新的分步结构更新了入门指南，包括事件响应团队的准备步骤、先决条件和简化的配置工作流、案例类型和工具集成。	2026 年 4 月 7 日
更新了 AWS 安全事件响应分类服务角色策略的策略描述	更新了 AWS 安全事件响应分类服务角色策略的策略描述，以反映允许该服务改进服务调整并收集信息以调查潜在事件的更改。	2026 年 3 月 27 日
提交元数据	添加了通过 AWS 支持 案例提交元数据的说明。	2026 年 3 月 27 日
提交遏制偏好	添加了通过 AWS 支持 案例提交遏制偏好的说明。	2026 年 3 月 27 日
遏制堆栈集模板	更新了遏制堆栈集 CloudFormation 模板。	2026 年 3 月 27 日

阐明了委派管理员账户的 AWS 区域 注意事项	阐明如下事实：虽然您于初始设置期间在一个 AWS 区域 中指定委托的 AWS 安全事件响应管理员账户，但该服务在所有支持的 AWS 区域 中提供组织范围的覆盖。	2026 年 3 月 20 日
定义遏制措施偏好	更新了遏制措施偏好部分以匹配当前选项。	2026 年 3 月 19 日
主动响应和警报分级	删除有关主动响应和警报分级工作流属于可选功能的表述。	2026 年 3 月 3 日
响应时限	更新了响应时限，将案例确认的 SLO 指定为 15 分钟，案例关闭前的客户响应时限为 5 个工作日。	2026 年 2 月 24 日
沟通最佳实践	更新了案例关闭时限，规定客户响应关键信息请求的时限为 5 个工作日。	2026 年 2 月 24 日
在“使用 AWS CloudShell 与安全事件响应进行交互”部分增加了 AWS CLI 参考	添加了指向“AWS 安全事件响应的 AWS Command Line Interface 参考”链接。	2026 年 2 月 24 日
RACI 矩阵	将 RACI 矩阵中的“授权 CIRT 遏制措施”更新为“授权遏制措施”。	2026 年 2 月 13 日
遏制偏好	将遏制偏好选项从“无遏制措施”、“经批准后遏制”和“自动遏制”更新为“需要审批”、“遏制已确认”和“遏制疑似”，并修改了描述。	2026 年 2 月 13 日
安全事件响应部署后	添加了指向“AWS 安全事件响应：新集成与 OU 级别订阅”演示的链接。	2026 年 2 月 4 日

监控与调查	在此页面的介绍及子章节中添加了修改后的内容。	2026 年 2 月 4 日
检测与分析	在此页面的介绍及子章节中添加了修改后的内容。	2026 年 2 月 4 日
遏制	在此页面中添加了修改后的内容。	2026 年 2 月 4 日
人工智能调查代理	在此页面中增加了客户数据的使用免责声明。免责声明：人工智能调查代理不使用客户数据进行模型训练，也不会与第三方共享客户数据。	2026 年 2 月 4 日

更改	描述	日期
取消会员资格	更新了取消成员资格页面，说明成员资格和服务将在取消后立即终止，而不是在账单周期结束时才终止。	2025 年 11 月 20 日
AWS 托管式策略	在服务提供的操作列表中增加了“更新案例”、“创建案例备注”、“列出案例”、“列出案例备注”等操作。	2025 年 11 月 19 日
使用服务关联角色	在服务提供的操作列表中增加了“更新案例”、“创建案例备注”、“列出案例”、“列出案例备注”等操作。	2025 年 11 月 19 日
通信首选项	创建并更新了为新功能文档添加了“通信首选项”部分。	2025 年 11 月 12 日
信息载入指南新增内容与更新	创建并更新了添加了信息载入指南，包括以下部分	2025 年 11 月 12 日

更改	描述	日期
	增加了启用安全事件响应章节。 增加了授权安全事件响应工程师执行威胁遏制措施章节。 增加了安全事件响应部署后章节。 添加了更新事件响应团队部分。 添加了 GuardDuty 调查发现和禁止规则部分。 添加了 Amazon EventBridge 部分。 添加了集成和外部工具工作流程部分。 添加了外部工具工作流程部分。 添加了附录 A：联系人部分。	

更改	描述	日期
合规和账单语言更新	更新了已删除AWS任何框架均未涵盖安全事件响应AWS的声明。HITRUST 现在涵盖了安全事件响应，将来还会有更多内容。 更新了可见性和控制以添加AWS安全事件响应 更新了取消会员资格，以明确服务账单周期。 在入门中添加了一段视频，为开始使用 AWS 安全事件响应的典型任务提供了额外的背景信息。	2025 年 8 月 15 日
更新了 – AWSSecurityIncidentResponseServiceRolePolicy	该政策现在包括以下两个新操作 "organizations:DescribeAccount" 、"organizations:ListDelegatedAdministrators" 和一个新条件： `"Condition": { "StringEquals": { "aws:ResourceAccount": "${aws:PrincipalAccount}" } }`	待定

更改	描述	日期
功能更新：订阅特定组织单元（OU）或整个 AWS 组织	用户界面中的帮助面板已更新，以反映订阅特定组织单元（OU）或整个 AWS 组织的更新。 创建用于管理组织单元（OU）成员资格的新页面 与 AWS Organizations 相关的页面已更新，以反映新的 OU 管理功能。	2025 年 8 月 7 日
更新了服务限额	服务配额页面已更新，引导用户查看《AWS 一般参考指南》中的 AWS 安全事件响应端点和配额	2025 年 8 月 7 日
用户反馈更新	为该服务添加了 AWS 安全事件响应案例的超链接 更新以反映《安全技术指南》的《计算机安全事件处理指南》SP 800-61 r3	2025 年 8 月 7 日
添加 Amazon EventBridge 与 AWS 安全事件响应集成的页面。	新的内容章节，介绍 Amazon EventBridge 如何集成到 AWS 安全事件响应中。	2025 年 6 月 26 日

更改	描述	日期
SLR 更新，增加了获得支持服务权利的权限。	AWSSecurityIncidentResponseTriageServiceRolePolicy 已更新，添加了 security-ir:GetMembership、security-ir:ListMemberships、security-ir:UpdateCase、guardduty:ListFilters、guarduty:UpdateFilter、guardduty:DeleteFilter，以及 guardduty:GetAdministratorAccount 权限。添加的 guardduty:GetAdministratorAccount 权限有助于在委托账户中实现 GuardDuty 自动存档筛选条件管理。	2025 年 6 月 2 日
资源更新。	更新了 https://docs.aws.amazon.com/security-ir/latest/userguide/appendix-b-incident-response-resources.html#playbook-resources 以反映可供客户参加的活动讲习会。	2025 年 5 月 23 日
服务现在支持日语。	更新了支持的配置，以识别日语支持（日本当地时间）。全球都支持英语。	2025 年 5 月 13 日

更改	描述	日期
内容更新和客户反馈。	在 https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html 中添加了说明，以反映在设置过程中使用委托管理员账户时需完成的额外任务。 更新了服务生成的案例和检测和分析功能的客户使用体验。 更新了账户取消详情，以便更清晰地说明取消会员资格的计费影响。	2025 年 5 月 9 日
添加三个新的支持区域。	在 https://docs.aws.amazon.com/security-ir/latest/userguide/supported-configs.html 中添加了三个新区域。孟买、巴黎和圣保罗。	2025 年 5 月 7 日
更新：根据客户评论对文档进行了更新。	多个页面上的拼写和语法错误都已更正。 更新了 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/organizations_permissions.html 以准确反映 security-ir 是服务前缀。 在 https://docs.aws.amazon.com/security-ir/latest/userguide/source-containment.html 中添加了一条关于 Route53 和 DNS 的说明。	2025 年 2 月 7 日

更改	描述	日期
更新：根据客户评论对文档进行了更新。	更新了 https://docs.aws.amazon.com/security-ir/latest/userguide/setup-monitoring-and-investigation-workflows.html 中的 StackSet 模板。 将 triage.security-ir.com 条目更正为 triage.security-ir.amazonaws.com 在 https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html 中添加了对 AWSSupport-ContainEC2Reversible 的跟踪连接说明。 修复了 https://docs.aws.amazon.com/security-ir/latest/userguide/managing-associated-accounts.html 中的失效链接。 在 https://docs.aws.amazon.com/security-ir/latest/userguide/select-a-membership-account.html 中添加了会员账户定义。 在 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/using-service-linked-roles.html 中添加了针对 AWS Organizations 管理账户的澄清说明。	2024 年 12 月 20 日

更改	描述	日期
更新：根据客户评论对文档进行了更新。	删除了文中多个重复的 AWS AWS。 修复了 https://docs.aws.amazon.com/security-ir/latest/userguide/sir_tagging.html 和 https://docs.aws.amazon.com/security-ir/latest/userguide/service-name-info-in-cloudtrail.html 中的失效链接。 https://docs.aws.amazon.com/security-ir/latest/userguide/contain.html 更新。删除了第一段中的 >。将 AWSSupport-ContainEC2Reversible 替换为 AWSSupport-ContainEC2Instance。将 AWSSupport-ContainIAMReversible 替换为 AWSSupport-ContainIAMPrincipal。将 AWSSupport-ContainS3Reversible 替换为 AWSSupport-ContainS3Resource。 更新了 https://docs.aws.amazon.com/en_us/security-ir/latest/userguide/issues.html 中的格式 在告诉客户通过支持票证联系安全事件响应时，https://docs.aws.amazon.com/security-ir/latest/userguide/understand-response-teams-and-	2024 年 12 月 10 日

更改	描述	日期
	support.html 现在提供了若干可在支持表单中选择的选项。 删除了 https://docs.aws.amazon.com/security-ir/latest/userguide/logging-and-events.html 中的 CloudWatch Events，将其替换为 EventBridge。 更新了 https://docs.aws.amazon.com/security-ir/latest/userguide/technique-access-containment.html 中的语法。 删除了 https://docs.aws.amazon.com/security-ir/latest/userguide/security-incident-response-guide.html 中的发布日期，替换为此表中的更新日期。	
更新：AWS 托管策略和服务相关角色。	托管策略和服务相关角色更新。	2024 年 12 月 1 日
服务启动	re:Invent 2024 服务发布的初始文档	2024 年 12 月 1 日