网络威胁情报共享 AWS

AWS 规范性指导

AWS 规范性指导: 网络威胁情报共享 AWS

Table of Contents

网络威胁情报共享 AWS

Amazon Web Services（贡献者）

2024 年 12 月（文件历史记录）

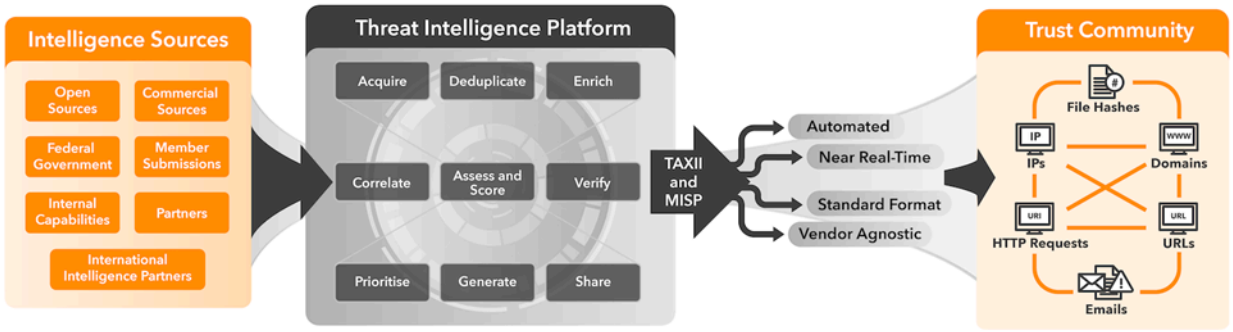
随着新风险的出现，保护关键云工作负载的最佳实践不断演变。随着需要保护的互联网连接资产数量的增加，与威胁行为者相关的安全事件的风险也随之增加。网络威胁情报 (CTI) 是对表明威胁行为者的意图、机会和能力的数据的收集和分析。它以证据为基础且具有可操作性，它为网络防御活动提供信息。它通常包括与行为者归因、战术技巧和程序、动机或目标有关的信息。

CTI 可以在组织内部、信任社区中的组织之间、与信息共享和分析中心 (ISAC) 或其他实体（例如政府机构）共享。政府机构的例子包括澳大利亚网络安全中心（ACSC）和美国网络安全和基础设施安全局（CISA）。

与所有形式的情报一样，威胁背景至关重要。CTI 共享为动态网络安全风险管理提供信息。这对于及时的网络安全防御、响应和恢复至关重要。这提高了网络安全能力的效率和有效性。威胁背景对于区分与不同目标相关的CTI能力要求也至关重要。例如，经验丰富的行为者可能瞄准特定的企业或政府，而商品行为者则使用现成的工具和技术对个人和组织进行广泛攻击。

安全规划、可观察性、威胁情报分析、安全控制自动化以及信任社区内的共享是威胁情报生命周期的关键部分。 AWS 帮助您自动执行手动安全任务，以更高的精度检测威胁，更快地做出响应，并生成可以共享的高质量威胁情报。您可以发现新的网络攻击，对其进行分析，生成 CTI，共享并应用它，所有这些都以旨在防止第二次攻击发生的速度进行。

本指南介绍如何在上部署威胁情报平台 AWS。信任社区提供CTI，平台将其摄取以识别可操作的情报，并自动执行环境中的保护和侦查控制。 AWS 下图显示了威胁情报的生命周期。CTI 从源头到达，然后威胁情报平台对其进行处理。通过使用可信自动交换情报信息 (TAXII) 协议或恶意软件信息共享平台 (MISP)，可与信任社区共享 CTI 以供采取行动。



威胁情报平台使用 CTI 在您的 AWS 环境中自动实施安全控制，或者在需要手动操作时通知您的安全团队。预防性控制是一种旨在防止事件发生的安全控制措施。例如，使用网络防火墙、DNS 解析器和其他入侵防御系统 (IPS) 自动生成已知不良 IP 地址或域名的屏蔽列表。侦探控件是一种安全控件，旨在在事件发生后进行检测、记录和发出警报。例如，持续监控恶意活动和在日志中搜索问题或事件的证据。

您可以在集中式安全可观察性工具中汇总任何发现，例如AWS Security Hub CSPM。然后，您可以与信任社区分享调查结果，共同构建全面的威胁画面。

CTI 共享的责任共担模型

责任AWS 共担模型定义了您如何分担云端安全性和合规性的责任。 AWS AWS 保护运行中提供的所有服务的基础架构 AWS Cloud，即云安全。您有责任保护您对这些服务的使用，例如您的数据和应用程序。这就是所谓的云端安全。

云的安全性

安全是重中之重 AWS。我们努力帮助防止安全问题对您的组织造成干扰。在我们努力保护我们的基础设施和您的数据时，我们会利用我们在全球范围的洞察力大规模和实时地收集大量安全情报，以帮助自动保护您。只要有可能 AWS ，其安全系统就会干扰最具影响力的威胁。通常，这项工作是在幕后进行的。

每天，我们都会在整个 AWS Cloud 基础设施中检测并成功阻止数百次网络攻击，否则这些攻击可能会造成破坏性且代价高昂。这些重要但基本上是看不见的胜利是通过全球传感器网络和一套相关的颠覆工具实现的。利用这些功能，我们可以使针对我们的网络和基础设施进行网络攻击变得更加困难和昂贵。

AWS 在所有云提供商中，公共网络占地面积最大。这为互联网上的某些活动提供了 AWS 无与伦比的实时见解。 MadPot是一个分布在全球的威胁传感器网络（称为蜜罐）。 MadPot 帮助 AWS 安全团队了解攻击者的策略和技巧。每当攻击者试图瞄准其中一个威胁传感器时，都会 AWS 收集和分析数据。

Sonaris 是另一种 AWS 用于分析网络流量的内部工具。它可以识别并阻止未经授权的访问大量账户和资源的尝试。在2023年5月至2024年4月期间，Sonaris拒绝了超过240亿次扫描存储在亚马逊简单存储服务（Amazon S3）中的客户数据的尝试。它还阻止了近2.6万亿次尝试发现亚马逊弹性计算云 (Amazon EC2) 上运行的易受攻击的工作负载。

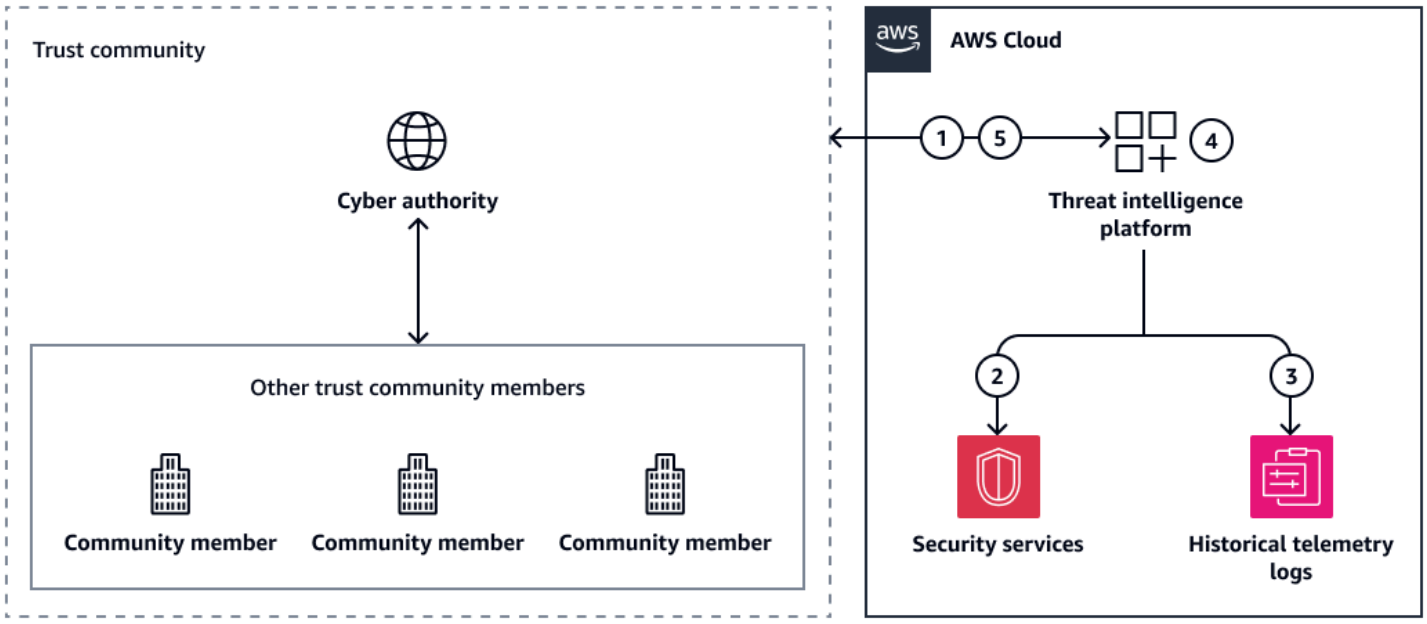
云中的安全性

本指南重点介绍网络威胁情报 (CTI) 的最佳实践。 AWS Cloud您负责生成本地化和情境化的 CTI。您可以控制数据的存储位置、保护方式以及谁有权访问数据。 AWS 无法查看您的日志、监控和审计数据，而这对于云中基于 CTI 的安全性至关重要。

结构化威胁信息表达 (STIX) 是一种用于交换 CTI 的开源语言和序列化格式。文件哈希、域 URLs、HTTP 请求和 IP 地址等指标是威胁拦截时需要共享的重要输出。但是，有效的行动依赖于其他情报，例如确定性评级和入侵集相关性。STIX 2.1 定义了 18 个 STIX 域对象，包括攻击模式、行动方案、威胁行为者、地理位置和恶意软件信息。它还引入了信心评级和关系等概念，这些概念可以帮助实体确定威胁情报平台收集的大量数据中的噪音信号。您可以检测、分析和共享有关 AWS 环境中威胁的这种详细程度。有关更多信息，请参阅本指南中的自动执行预防和侦查安全控制。

网络威胁情报架构已启用 AWS

下图描绘了使用威胁源将网络威胁情报 (CTI) 集成到您的环境中的通用架构。 AWS CTI 由您在中的威胁情报平台 AWS Cloud、选定的网络机构和其他信任社区成员共享。



它显示了以下工作流程：

1. 威胁情报平台从网络管理机构或其他信托社区成员那里获得可操作的 CTI。
2. 威胁情报平台责成 AWS 安全服务部门检测和防止事件。
3. 威胁情报平台接收来自的威胁情报 AWS 服务。
4. 如果事件发生，威胁情报平台将策划新的CTI。
5. 威胁情报平台与网络管理机构共享新的CTI。它还可以与其他信托社区成员共享 CTI。

有许多网络机构提供CTI提要。例子包括澳大利亚网络安全中心（ACSC）、英国国家网络安全中心提供的C onnect Inform Share Protect（CISP）计划以及新西兰政府通信安全局提供的无恶意软件网络（MFN）计划。许多 AWS 合作伙伴还提供 CTI 共享订阅源。

要开始使用 CTI 共享，我们建议您执行以下操作：

1. 部署威胁情报平台-部署一个平台，从多个来源以不同格式提取、聚合和组织威胁情报数据。

2. 摄取网络威胁情报-将您的威胁情报平台与一个或多个威胁源提供商集成。当您收到威胁源时，请使用您的威胁情报平台来处理新的 CTI，并识别与您环境中的安全操作相关的可操作情报。尽可能实现自动化，但在某些情况下，需要做出人性化决策。
3. 自动执行预防和侦测安全控制 — 将 CTI 部署到架构中提供预防和侦测控制的安全服务。这些服务通常被称为入侵防御系统 (IPS)。开启后 AWS，您可以使用服务 API 配置阻止列表，拒绝来自威胁源中提供的 IP 地址和域名的访问。
4. 通过可@@ 观察性机制获得可见性 — 当您的环境中进行安全操作时，您正在收集新的 CTI。例如，您可能会观察到威胁源中包含的威胁，或者可以观察到与入侵相关的入侵迹象（例如未修补漏洞）。集中威胁情报可提高整个环境的态势感知能力，因此您可以在一个系统中查看现有的 CTI 和新发现的 CTI。
5. 与您的信任社区共享 CTI — 要完成 CTI 共享生命周期，请生成自己的 CTI 并将其分享回您的信任社区。

以下视频《扩大与澳大利亚网络安全中心的网络威胁情报共享》更详细地讨论了这些步骤。尽管本视频讨论了澳大利亚网络安全中心的CTI共享功能，但无论您选择哪种威胁源或您所在的位置，步骤都是一样的。

部署威胁情报平台

威胁情报平台提取、汇总和组织来自多个来源和不同格式的威胁情报数据。它允许分析师查看从其信任社区收到的网络威胁情报 (CTI)，确定其优先顺序并采取行动。

OpenCTI 和 MISP 是常见的开源威胁情报平台。 AWS 合作伙伴还提供解决方案，网址为AWS Marketplace。在选择威胁情报平台时，您应该考虑安全团队的技能水平。MISP 既强大又复杂，而且 OpenCTI 具有更直观的用户界面。

选择威胁情报平台时，请考虑以下几点：

- 功能-该平台是否提供实时监控、威胁检测和分析等功能？
- 数据源 — 该平台是否使用各种来源，包括威胁源、暗网情报、社交媒体和开源情报？
- 数据质量 — 平台是否有确保信息准确可靠的流程？
- 可扩展性 — 该平台能否适应组织不断变化的需求，例如增长和不断演变的威胁？
- 集成 — 该平台能否与您现有的安全工具和基础架构集成？
- 用户体验 — 该平台是否易于浏览和使用？
- 定制 — 能否对平台进行定制以满足贵组织的特定需求？

- 成本 — 平台是否具有成本效益，包括许可成本和维护要求？

您可以在虚拟私有云 (VPC) 中部署威胁情报平台。您可以将其直接部署在亚马逊弹性计算云 (Amazon EC2) 实例上，也可以使用容器技术，例如亚马逊弹性容器服务 (Amazon ECS) 或。 AWS Fargate有关为现代应用程序开发选择合适的 AWS 容器服务的更多信息，请参阅选择 AWS 容器服务。

摄取网络威胁情报

摄取过程的第一步是将来自威胁源的网络威胁情报 (CTI) 数据转换为威胁情报平台可以摄取的格式。这被称为 CTI 转换。威胁源数据可以采用多种格式，例如结构化威胁信息表达 (STIX)。您必须将传入的数据重组为一种可预测且易于使用的格式，该格式适合您在环境中使用的安全产品。 AWS

为了最大限度地提高兼容性，我们建议您将数据转换为 JSON 格式。例如，AWS Step Functions可以使用 JSON 格式的数据，而自动化工作流程可以更轻松、更一致地使用这种格式。下一节 “自动化预防和侦查安全控制” 中提供了有关构建自动化工作流程的更多信息。

为了加快 CTI 数据的摄取，您可以自动进行数据转换。数据在摄取时会进行转换，然后直接传递到威胁情报平台。您可以使用 AWS Lambda 函数来完成转换，也可以通过 AWS 服务 诸如 AWS Step Functions 或 Amazon EventBridge 之类的方法编排流程。

提取 CTI 时，您可以选择提取和保留哪些属性。所需的确切详细信息量可能会因您的业务需求而异。但是，要更新防火墙和其他安全服务，我们建议使用以下最低限度属性：

- IP 地址和域名
- 威胁
- 在您的内部威胁列表中添加或删除

提取要使用的属性，然后将其格式化为结构化的 JSON 模板。

自动执行预防和侦查安全控制

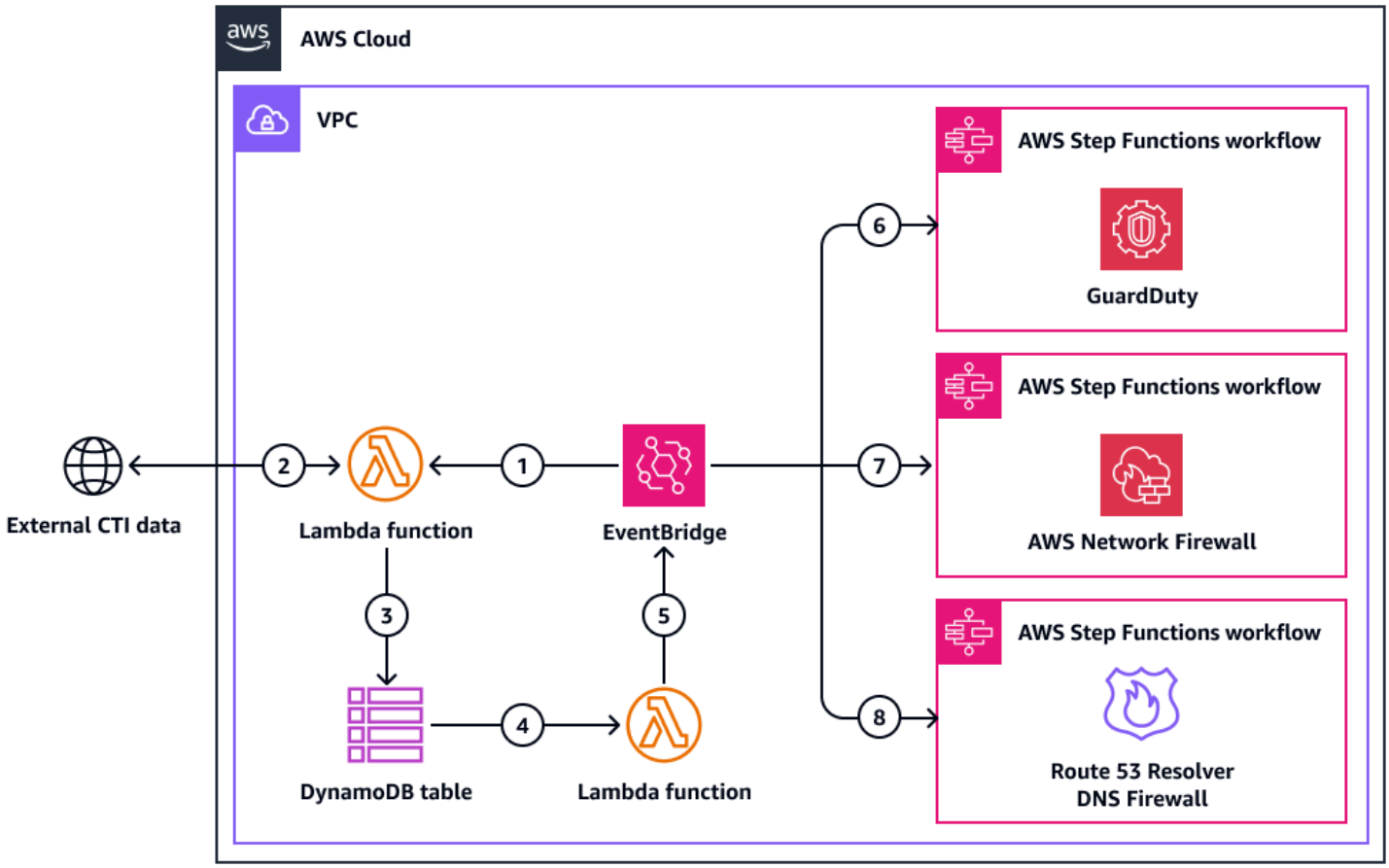
将网络威胁情报 (CTI) 导入威胁情报平台后，您可以自动执行根据数据进行配置更改的过程。威胁情报平台可帮助您管理网络威胁情报并观察您的环境。它们提供了构建、存储、组织和可视化有关网络威胁的技术和非技术信息的能力。它们可以帮助您建立威胁画面，并结合一系列情报来源来分析和跟踪威胁，例如高级持续威胁 (APT)。

自动化可以缩短从接收威胁情报到在环境中实施配置更改之间的时间。并非所有 CTI 回复都可以自动完成。但是，自动执行尽可能多的响应可以帮助您的安全团队更及时地确定其余CTI的优先级并对其进

行评估。每个组织都必须确定哪些类型的CTI响应可以自动化，哪些需要手动分析。根据组织背景（例如风险、资产和资源）做出此决定。例如，一些组织可能会选择自动屏蔽已知的恶意域或 IP 地址，但在屏蔽内部 IP 地址之前，他们可能需要分析师进行调查。

本节提供了如何在 Amazon GuardDuty 和 Amazon Route 53 Resolver DNS 防火墙中设置自动 CTI 响应的示例。AWS Network Firewall您可以相互独立地实现这些示例。让组织的安全要求和需求来指导您的决策。您可以 AWS 服务 通过AWS Step Functions工作流程（也称为状态机）自动更改配置。当AWS Lambda函数将 CTI 转换为 JSON 格式后，它会触发一个启动 Step Functions 工作流程的亚马逊 EventBridge事件。

下图显示了一个示例架构。Step Functions 工作流程会自动更新中的威胁列表 GuardDuty、Route 53 Resolver DNS Firewall 中的域列表以及 Network Firewall 中的规则组。



图中显示了以下工作流程：

1. EventBridge 活动按定期计划启动。此事件启动一个 AWS Lambda 函数。
2. Lambda 函数从外部威胁源中检索 CTI 数据。
3. Lambda 函数将检索到的 CTI 数据写入亚马逊 DynamoDB 表。

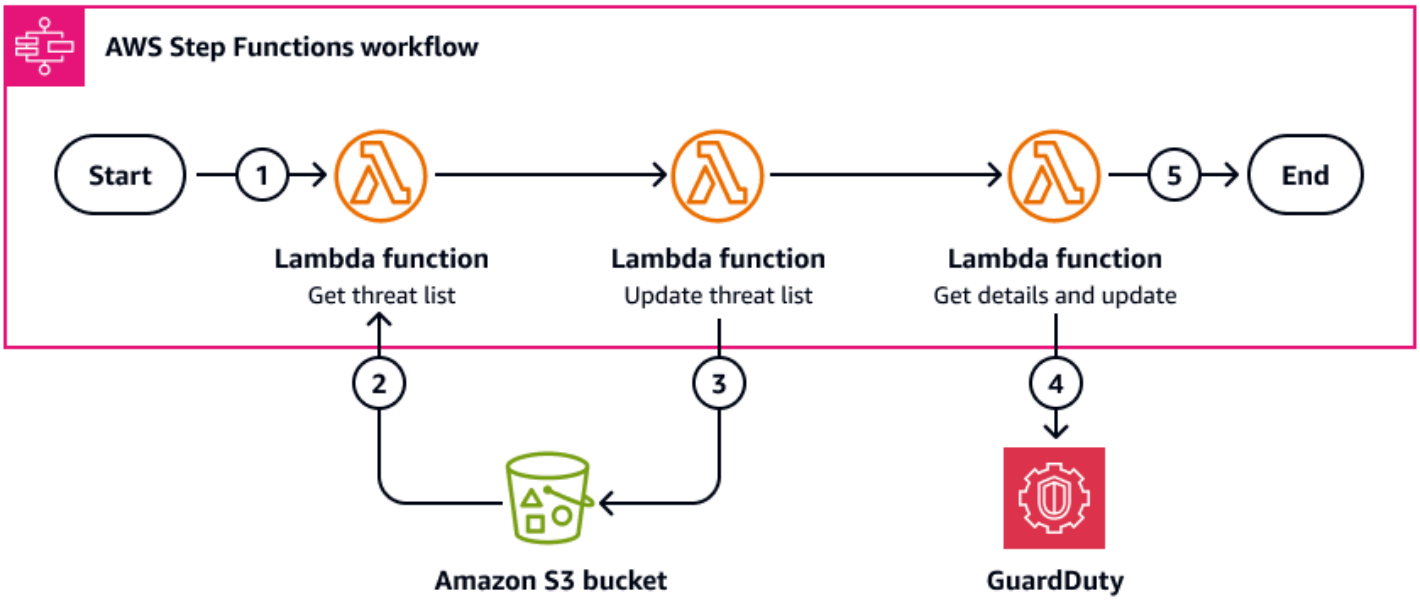
4. 向 DynamoDB 表写入数据会启动变更数据捕获流事件，该事件会启动 Lambda 函数。
5. 如果发生更改，Lambda 函数将在中启动一个新事件。 EventBridge如果未发生任何更改，则工作流程即告完成。
6. 如果 CTI 与 IP 地址记录相关，则 EventBridge 启动 Step Functions 工作流程，自动更新亚马逊 GuardDuty中的威胁列表。有关更多信息，请参阅本节 GuardDuty中的 Amazon。
7. 如果 CTI 与 IP 地址或域记录相关，则会 EventBridge 启动 Step Functions 工作流程，自动更新中的 AWS Network Firewall规则组。有关更多信息，请参阅此部分中的 AWS Network Firewall。
8. 如果 CTI 与域记录相关，则 EventBridge 启动 Step Functions 工作流程，自动更新 Amazon Route 53 Resolver DNS 防火墙中的域名列表。有关更多信息，请参阅本节中的 Amazon Route 53 Resolver DNS 防火墙。

Amazon GuardDuty

Amazon GuardDuty 是一项威胁检测服务，可持续监控您 AWS 账户 和工作负载中是否存在未经授权的活动，并提供详细的安全调查结果以供查看和补救。通过自动更新 CTI 源中的 GuardDuty 威胁列表，您可以深入了解可能正在访问您的工作负载的威胁。 GuardDuty 提高您的侦探控制能力。

> **Tip**
>
> GuardDuty 与原生集成。AWS Security Hub CSPMSecurity Hub CSPM 可全面了解您的安全状态， AWS 并帮助您根据安全行业标准和最佳实践检查您的环境。当你 GuardDuty 与 Security Hub CSPM 集成时，你的 GuardDuty 发现会自动发送到 Security Hub CSPM。然后，Security Hub CSPM 可以将这些发现纳入其对您的安全态势的分析中。有关更多信息，请参阅 GuardDuty 文档 AWS Security Hub CSPM中的与集成。在 Security Hub CSPM 中，您可以使用自动化来提高侦探和响应式安全控制能力。

下图显示了 Step Functions 工作流程如何使用威胁源中的 CTI 来更新中的 GuardDuty威胁列表。当 Lambda 函数完成将 CTI 转换为 JSON 格式时，它会触发一个启动工作 EventBridge 流程的事件。



图中显示以下步骤：

1. 如果 CTI 与 IP 地址记录相关，则 EventBridge 启动 Step Functions 工作流程。
2. Lambda 函数检索威胁列表，该列表作为对象存储在亚马逊简单存储服务 (Amazon S3) 存储桶中。
3. Lambda 函数使用 CTI 中的 IP 地址更改来更新威胁列表。它会将威胁列表作为对象的新版本保存到原始 Amazon S3 存储桶中。对象名称保持不变。
4. Lambda 函数使用 API 调用来检索 GuardDuty 探测器 ID 和威胁情报集 ID。它使用这些 ID GuardDuty 进行更新以引用新版本的威胁列表。

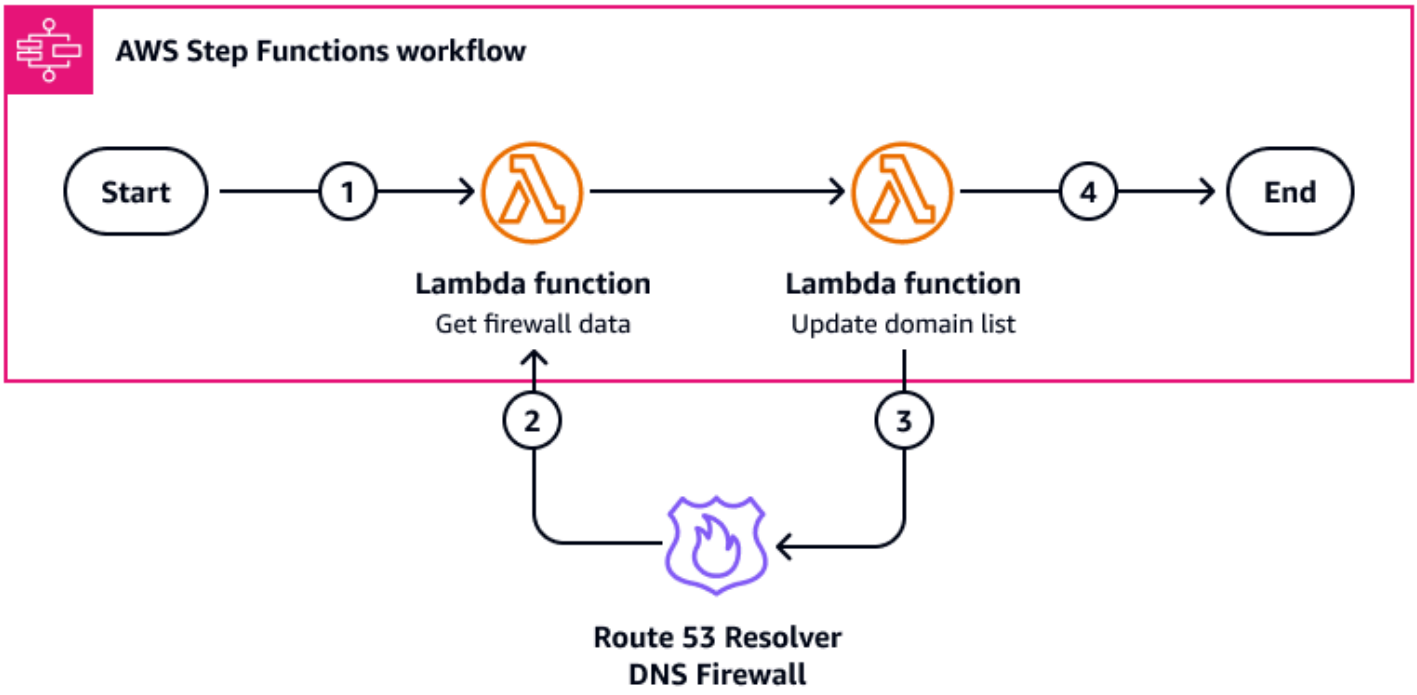
> **Note**
>
> 您无法检索特定的 GuardDuty 检测器和 IP 地址列表，因为它们是作为数组检索的。因此，我们建议目标中每个目标中只有一个 AWS 账户。如果您多于一个，则需要确保在此工作流程的最终 Lambda 函数中提取了正确的数据。

5. Step Functions 工作流程结束。

Amazon Route 53 Resolver 域名防火墙

Amazon Route 53 Resolver DNS 防火墙可帮助您筛选和监管虚拟私有云 (VPC) 的出站 DNS 流量。在 DNS 防火墙中，您可以创建一个规则组，用于屏蔽由 CTI 源标识的域地址。您可以将 Step Functions 工作流程配置为自动在此规则组中添加和删除域。

下图显示了 Step Functions 工作流程如何使用威胁源中的 CTI 来更新 Amazon Route 53 Resolver DNS 防火墙中的域名列表。当 Lambda 函数完成将 CTI 转换为 JSON 格式时，它会触发一个启动工作 EventBridge 流程的事件。



图中显示以下步骤：

1. 如果 CTI 与域名记录相关，则 EventBridge 启动 Step Functions 工作流程。
2. Lambda 函数检索防火墙的域列表数据。有关创建此 Lambda 函数的更多信息，请参阅文档中的 get_firewall_domain_ list。 适用于 Python (Boto3) 的 AWS SDK
3. Lambda 函数使用 CTI 和检索到的数据来更新域名列表。有关创建此 Lambda 函数的更多信息，请参阅 Boto3 文档中的 update_firewall_dom ains。Lambda 函数可以添加、删除或替换域。
4. Step Functions 工作流程结束。

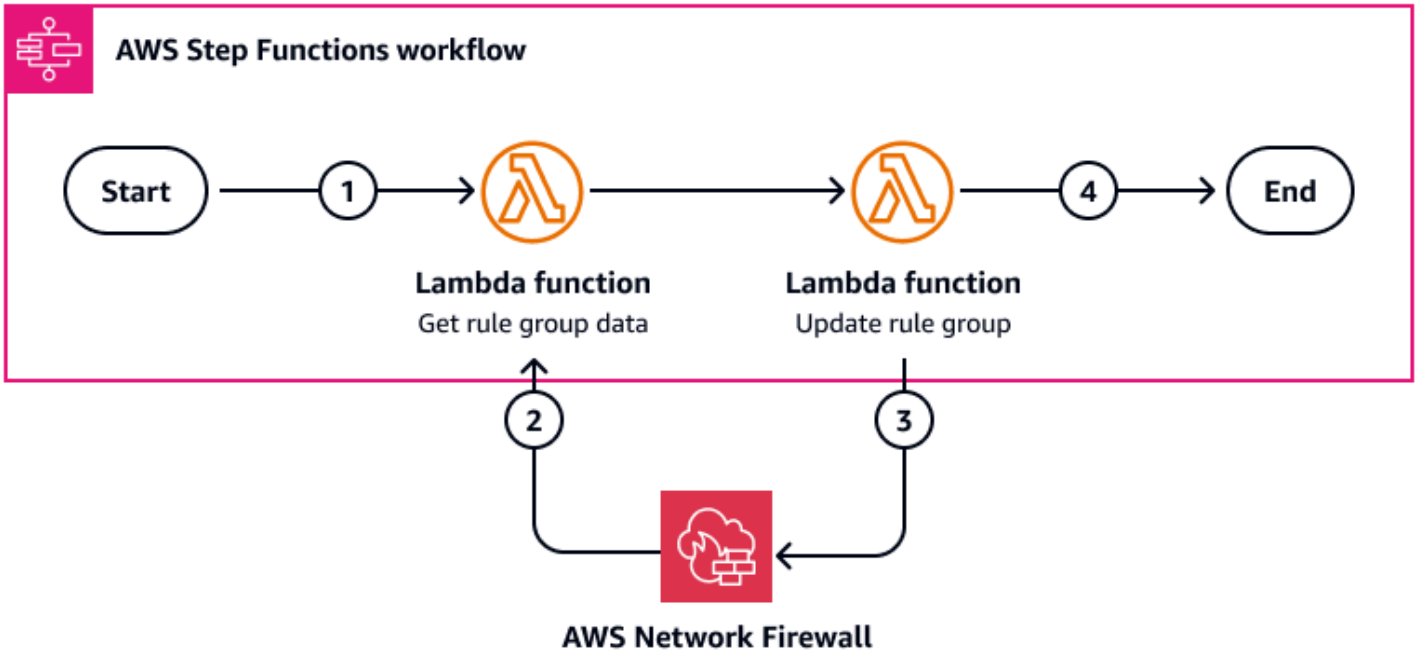
我们建议您遵循以下最佳实操：

- 我们建议您同时使用 Route 53 解析器 DNS 防火墙和。 AWS Network Firewall DNS 防火墙过滤 DNS 流量，Network Firewall 过滤所有其他流量。
- 我们建议您启用 DNS 防火墙的日志记录。您可以创建侦探控件，用于监控日志数据，并在受限域试图通过防火墙发送流量时提醒您。有关更多信息，请参阅使用 Amazon CloudWatch 监控 Route 53 解析器 DNS 防火墙规则组。

AWS Network Firewall

AWS Network Firewall是一项针对中 VPC 的状态托管网络防火墙以及入侵检测和防御服务。 AWS Cloud它可以过滤您的 VPC 周边的流量，帮助您阻止威胁。使用威胁情报源自动更新 Network Firewall 规则组可以帮助保护组织的云工作负载和数据免受恶意行为者的侵害。

下图显示了 Step Functions 工作流程如何使用威胁源中的 CTI 来更新 Network Firewall 中的一个或多个规则组。当 Lambda 函数完成将 CTI 转换为 JSON 格式时，它会触发一个启动工作 EventBridge 流程的事件。



图中显示以下步骤：

1. 如果 CTI 与 IP 地址或域记录相关，则会 EventBridge 启动 Step Functions 工作流程，自动更新 Network Firewall 中的规则组。
2. Lambda 函数从 Network Firewall 检索规则组数据。
3. Lambda 函数使用 CTI 来更新规则组。它添加或删除 IP 地址或域。
4. Step Functions 工作流程结束。

我们建议您遵循以下最佳实操：

- Network Firewall 可以有多个规则组。为域和 IP 地址创建单独的规则组。

- 我们建议您为 Network Firewall 启用日志记录。您可以创建侦探控件，用于监控日志数据，并在受限域或 IP 地址试图通过防火墙发送流量时提醒您。有关更多信息，请参阅记录来自的网络流量 AWS Network Firewall。
- 我们建议您同时使用 Route 53 解析器 DNS 防火墙和。 AWS Network Firewall DNS 防火墙过滤 DNS 流量，Network Firewall 过滤所有其他流量。

通过可观测性机制获得可见性

查看已发生的安全事件的能力与建立适当的安全控制措施同样重要。在 Framewor AWS Well-Architected k 的安全支柱中，检测最佳实践包括在标准化位置配置服务和应用程序日志以及捕获日志、发现结果和指标。要实施这些最佳实践，您必须记录有助于识别事件的信息，然后将这些信息处理成可供人类使用的格式，最好是在集中位置。

本指南建议您使用亚马逊简单存储服务 (Amazon S3) 来集中管理日志数据。Amazon S3 支持两者的日志存储 AWS Network Firewall 和 Amazon Route 53 Resolver DNS 防火墙。然后，您可以使用AWS Security Hub CSPM和 Amazon Security Lak e 将亚马逊 GuardDuty 调查结果和其他安全发现集中到一个位置。

记录网络流量

本指南的 “自动化预防和侦查安全控制” 部分介绍了使用 AWS Network Firewall 和 Amazon Route 53 Resolver DNS 防火墙自动响应网络威胁情报 (CTI)。我们建议您为这两项服务配置日志记录。您可以创建侦探控件，用于监控日志数据，并在受限域或 IP 地址试图通过防火墙发送流量时提醒您。

配置这些资源时，请考虑您的个人日志记录要求。例如，Network Firewall 的日志记录仅适用于您转发到状态规则引擎的流量。我们建议您遵循零信任模型，并将所有流量转发到有状态规则引擎。但是，如果您想降低成本，则可以排除组织信任的流量。

Network Firewall 和 DNS 防火墙都支持登录到 Amazon S3。有关为这些服务设置日志记录的更多信息，请参阅记录来自的网络流量 AWS Network Firewall和配置 DNS 防火墙的日志记录。对于这两项服务，您都可以通过配置对 Amazon S3 存储桶的日志记录 AWS 管理控制台。

将安全调查结果集中在 AWS

AWS Security Hub CSPM全面了解您的安全状态， AWS 并帮助您根据安全行业标准和最佳实践评估您的 AWS 环境。Security Hub CSPM 可以生成与您的安全控制相关的调查结果。它还可以接收来自其他 AWS 服务机构（例如亚马逊）的调查结果 GuardDuty。您可以使用 Security Hub CSPM 来集中

来自您 AWS 账户和支持的第三方产品的调查结果和数据。 AWS 服务有关集成的更多信息，请参阅 Security Hub CSPM 文档中的了解 Security Hub CSPM 中的集成。

Security Hub CSPM 还包括自动化功能，可帮助您对安全问题进行分类和修复。例如，当安全检查失败时，您可以使用自动化规则自动更新关键调查发现。您还可以使用与 Amazon 的集成 EventBridge 来启动对特定发现的自动响应。有关更多信息，请参阅 Sec urity Hub CSPM 文档中的自动修改 Security Hub CSPM 发现结果并对其采取行动。

如果您使用亚马逊 GuardDuty，我们建议您将其配置 GuardDuty 为将其调查结果发送到 Security Hub CSPM。然后，Security Hub CSPM 可以将这些发现纳入其对您的安全态势的分析中。有关更多信息，请参阅 GuardDuty 文档 AWS Security Hub CSPM中的与集成。

对于 Network Firewall 和 Route 53 Resolver DNS Firewall，您可以根据正在记录的网络流量创建自定义发现。Amazon Athena 是一种交互式查询服务，可帮助您使用标准 SQL 直接在 Amazon S3 中分析数据。您可以在 Athena 中构建查询，用于扫描 Amazon S3 中的日志并提取相关数据。有关说明，请参阅 Athena 文档中的入门。然后，您可以使用 AWS Lambda 函数将相关日志数据转换为AWS 安全调查结果格式 (ASFF)，并将结果发送到 Security Hub CSPM。以下是 Lambda 函数示例，该函数将来自网络防火墙的日志数据转换为 Security Hub CSPM 调查结果：

```
Import { SecurityHubClient, BatchImportFindingsCommand, GetFindingsCommand } from
 "@aws-sdk/client-securityhub";

Export const handler = async(event) => {
   const date = new Date().toISOString();

   const config = {
      Region: REGION
   };

   const input = {
      Findings: [
         {
            SchemaVersion: '2018-10-08',
            Id: ALERTLOGS3BUCKETID,
            ProductArn: FIREWALLMANAGERARN,
            GeneratorId: 'alertlogs-to-findings',
            AwsAccountId: ACCOUNTID,
            Types: 'Unusual Behaviours/Network Flow/Alert',
            CreatedAt: date,
            UpdatedAt: date,
            Severity: {
               Normalized: 80,
```

```
                Product: 8
            },
            Confidence: 100,
            Title: 'Alert Log to Findings',
            Description: 'Network Firewall Alert Log into Finding - add
               top level dynamic detail',
            Resources: [
               {
                  /*these are custom resources. Contain deeper details of your event
 here*/
                  firewallName: 'Example Name',
                  event: 'Example details here'
               }
            ]
         }
      ]
   };

   const client = new SecurityHubClient(config);
   const command = new BatchImportFindingsCommand(input);
   const response = await client.send(command);
   return { statusCode: 200, response };
};
```

您在提取信息并将其发送到 Security Hub CSPM 时所遵循的模式取决于您的个人业务需求。如果您需要定期发送数据，则可以使用 EventBridge 来启动该过程。如果您想在添加信息时收到提醒，则可以使用亚马逊简单通知服务 (Amazon SNS) Simple SNS SERVICE。有许多方法可以采用这种架构，因此必须进行适当的规划，以满足您的业务需求。

集成 AWS 安全数据与其他企业数据

Amazon Security Lake 可以自动从集成服务和第三方服务中收集与安全相关的日志 AWS 服务 和事件数据。它还可以通过可自定义的保留和复制设置帮助您管理数据的生命周期。Security Lake 会将摄取的数据转换为 Apache Parquet 格式和名为开放网络安全架构框架 (OCSF) 的标准开源架构。在 OCSF 的支持下，Security Lake 可以标准化 AWS 并合并来自各种企业安全数据源的安全数据。其他 AWS 服务 和第三方服务可以订阅存储在 Security Lake 中的数据，用于事件响应和安全数据分析。

您可以将 Security Lake 配置为接收来自 Security Hub CSPM 的调查结果。要激活此集成，您必须启用这两项服务，并将 Security Hub CSPM 作为源添加到 Security Lake 中。完成这些步骤后，Security Hub CSPM 开始将所有调查发现发送到 Security Lake。Security Lake 会自动标准化 Security Hub CSPM 的发现结果并将其转换为 OCSF。在 Security Lake 中，您可以添加一个或多个订阅用户来使用

Security Hub CSPM 调查发现。有关更多信息，请参阅 Security Lake 文档 AWS Security Hub CSPM 中的与集成。

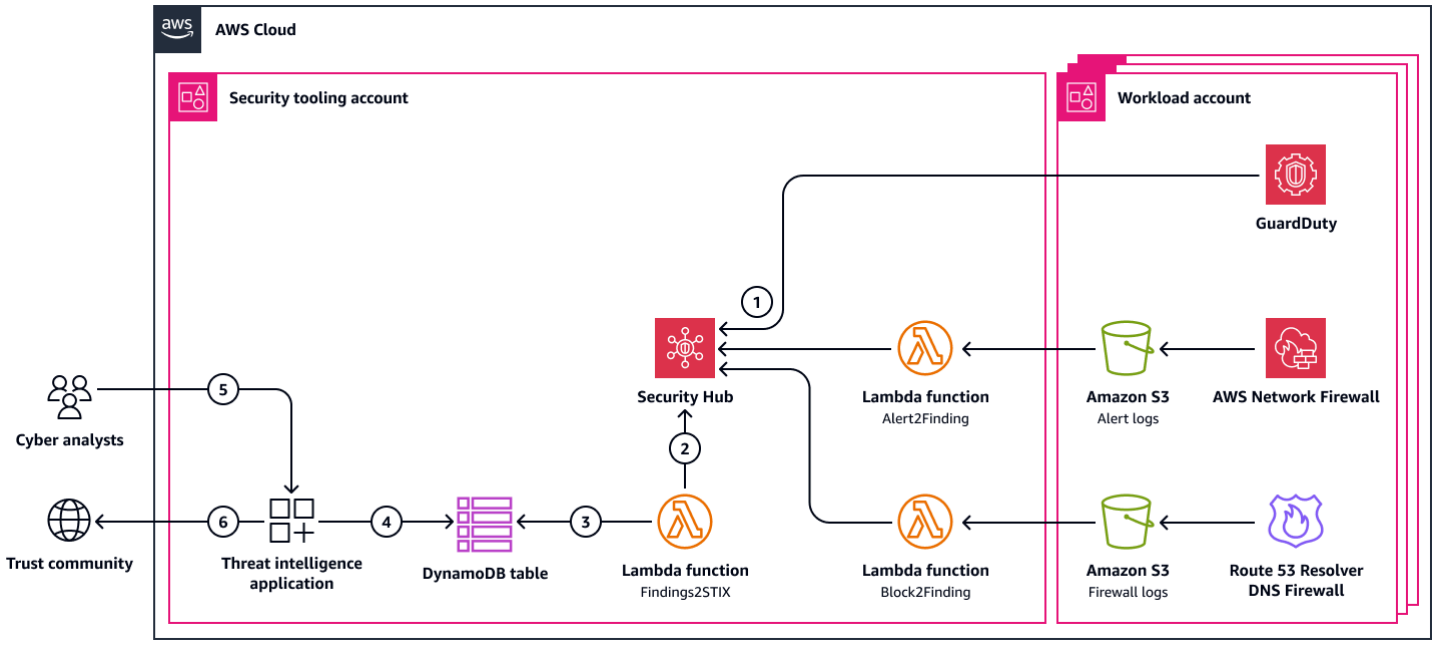
以下视频《re AWS : inForce 2024-网络威胁情报共享》 AWS讨论了如何使用 Security Hub CSPM 和 Security Lake 集成来共享 CTI。

与您的信任社区共享 CTI

您向其发送网络威胁情报 (CTI) 的社区通常与您接收网络威胁情报 (CTI) 的社区相同。但是，您可以选择分享给更多人。例如，您可以选择与您信任的政府或监管机构共享，例如您的国家网络安全中心或信息共享和分析中心 (ISAC)。目标是通过汇集多个组织的调查结果，快速传播和实施CTI。您的威胁情报平台管理 API 集成，以便与多个 Feed 共享。

向信托社区发送CTI是在实施预防和侦查控制的同时进行的。您可以使用日志来帮助识别安全事件。然后，您可以集中处理事件和调查结果，以便快速了解您的 AWS 账户安全状况。然后，您的安全团队（例如您的网络分析师）可以识别任何可能有价值的信息。由于您在中已经有了调查结果 AWS Security Hub CSPM，因此可以将这些发现转换为威胁源使用的格式，例如 JSON 或 STIX。然后，您将 CTI 发送给信息源提供商。他们的威胁情报平台会摄取、匿名化和验证您提供的 CTI。然后，您的CTI将与更广泛的社区共享。

下图显示了 AWS 服务 如何使用生成 CTI，然后与您的信任社区（包括网络管理机构和其他社区成员）共享。



此图显示了以下工作流程：

1. 调查结果是在中创建的 AWS Security Hub CSPM。
2. AWS Lambda 函数从 Security Hub CSPM 中检索发现的结果，并将其转换为可共享的格式，例如 JSON 或 STIX。
3. Lambda 函数将调查结果存储在亚马逊 DynamoDB 表中。
4. 在亚马逊弹性计算云 (Amazon EC2) 或亚马逊弹性容器服务 (Amazon ECS) 上运行的第三方威胁情报平台从 DynamoDB 表中检索调查结果。
5. 网络分析师在威胁情报平台中审查CTI。
6. 威胁情报平台将CTI发布给由其他CTI生产者和消费者组成的信任社区。

后续步骤和资源

考虑一下贵组织的资产、行业和威胁环境。这些因素应告知您选择加入以共享网络威胁情报的信任社区。世界各地的许多网络机构都提供威胁情报源。考虑所提供的内容，然后选择最适合您组织的用例的产品。使用本指南作为模块化方法，并相应地为您的组织量身定制。

我们建议您查看以下其他资源。这些资源可以帮助您在自己的 AWS 环境中构建或部署威胁情报平台，并帮助您设置网络威胁情报共享。

AWS 资源

- AWS 建筑中心
- AWS re: inForce 2024-网络威胁情报共享开启（视频） AWS
- AWS 2023 年澳新银行峰会：扩大与澳大利亚网络安全中心的网络威胁情报共享（视频）

AWS 服务 文档

- Amazon DynamoDB 文档
- 亚马逊 EventBridge 文档
- 亚马逊 GuardDuty 文档
- AWS Lambda 文档
- AWS Network Firewall 文档
- Amazon Route 53 Resolver DNS 防火墙文档
- AWS Security Hub CSPM 文档
- Amazon 安全湖文档
- 亚马逊简单存储服务 (Amazon S3) Semple Service 文档
- AWS Step Functions 文档

STIX 资源

- STIX 2.1 示例
- 恶意 URL 指示器

威胁情报平台

- OpenCTI
- MISP

贡献者

以下人员为本指南做出了贡献。

编写

- 杰西·莫迪尼，高级技术专家， AWS
- Alexa Donovan，助理解决方案架构师， AWS
- Steven Ryan，合作伙伴解决方案架构师， AWS
- 拜伦·波格森，安全解决方案架构师， AWS

正在审阅

- Brian Farnhill，高级软件开发工程师， AWS
- Marc Luescher，高级解决方案架构师， AWS
- Stefan Mijic，安全保障专家， AWS
- 公共部门解决方案架构师 Timothy Woodill AWS

技术写作

- Lilly AbouHarb，高级技术撰稿人， AWS

文档历史记录

下表介绍了本指南的一些重要更改。如果您希望收到有关未来更新的通知，可以订阅 RSS 源。

变更	说明	日期
初次发布	—	2024 年 12 月 12 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。