AWS 技术指南

AWS 安全事件响应指南

AWS 安全事件响应指南: AWS 技术指南

Table of Contents

AWS 安全事件响应指南

发布日期：2020 年 11 月 23 日（文档修订）

本指南概述了在客户的 AWS 云环境中应对安全事件的基础知识。它重点概述了云安全和事件响应概念，并确定了可供响应安全问题的客户使用的云功能、服务和机制。

本白皮书面向担任技术角色的人员，假定您熟悉信息安全的一般原则，对当前本地环境中的事件响应有基本的了解，并且对云服务有一定的了解。

引言

AWS 将安全性视为头等大事。作为 AWS 客户，您将从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中受益。AWS 云采用责任共担模式。AWS 负责管理云的安全性。您负责云中的安全性。这意味着您可以保持对选择实施的安全性的控制。您可以使用数百种工具和服务来帮助您实现自己的安全目标。这些功能可帮助您建立安全基准，以满足您在云中运行的应用程序的目标。

如果确实出现偏离基准的情况（例如由于配置错误），您可能需要作出响应并进行调查。要成功做到这一点，您必须了解 AWS 环境内安全事件响应的基本概念，以及在出现安全问题之前准备、教育和培训云团队时需要考虑的问题。重要的是要知道您可以使用哪些控制和功能，以便查看用于解决潜在问题的话题示例，并确定可用于实现自动化和提高响应速度的修复方法。

由于安全事件响应可能是一个复杂的话题，我们建议您从小处着手，开发运行手册，利用基本功能，并创建一个初始的事件响应机制库，以便进行迭代和改进。这项初始工作应该让您的法律部门以及不涉及安全问题的团队参与进来，以便您能够更好地了解事件响应（IR）以及您所做的选择对企业目标的影响。

主题

开始前的准备工作

除了本文档之外，我们还建议您查看安全、身份和合规性的最佳实践以及 AWS Cloud Adoption Framework（CAF）的安全视角白皮书。AWS CAF 提供指导，支持在组织迁移到云的不同部分之间进行协调。CAF 指导分为与实施基于云的 IT 系统相关的几个重点领域，我们称之为视角。安全视角描述了如何在多个工作流中实施安全计划，其中一个工作流侧重于事件响应。本文档详细介绍了我们在帮助客户评估和实施该工作流中的成功机制方面的一些经验。

AWS CAF 安全视角

安全视角包括四个组成部分：

- 指导性控制机制旨在围绕运营环境构建治理、风险和合规模型。
- 预防性控制机制旨在保护您的工作负载并减少威胁和漏洞。

- 检测性控制机制可使您在 AWS 中的部署运营变得可见、透明。
- 响应性控制机制旨在纠正可能偏离安全基准的行为。

尽管通常是在响应性控制组成部分下查看 IR，但这些组件相互依赖并受其他组件影响。例如，指导性和预防性安全控制机制可帮助建立基准，因此您可以监控和调查任何偏离此基准的情况。此方法不仅消除了噪音，而且还有助于防御性安全设计。

事件响应的基础

组织中的所有 AWS 用户都应基本了解安全事件响应流程，安全人员必须深入了解如何应对安全问题。在处理安全事件之前，经验和教育对于云事件响应计划至关重要。在云端成功实施事件响应计划的基础是培训、准备、模拟和迭代。

要了解其中的每一个方面，请考虑以下说明：

- 培训您的安全运营和事件响应员工，以使他们了解云技术以及您的组织如何使用这些技术。
- 让您的事件响应团队做好准备，以便启用检测性功能并确保对必要的工具和云服务拥有适当的访问权限，从而可以在云中检测和响应事件。此外，还应通过人工和自动化的方式准备必要的运行手册，以确保可靠且一致的响应。与其他团队合作，以确立预期的基准操作，并利用这些知识来发现与那些正常操作的偏差。
- 模拟您的云环境内的预期和意外安全事件，以了解您的准备工作的有效性。
- 迭代您的模拟结果，以提高您的响应能力、缩短价值实现时间并进一步降低风险。

培训

主题

责任共担

AWS 和您共同承担安全性和合规性的责任。此责任共担模式可以帮助您减轻一些操作负担，因为 AWS 会操作、管理并控制各个组件，从主机操作系统和虚拟化层到运行各种服务的设施的物理安全，均由 AWS 保障。

您负责管理来宾操作系统（包括更新和安全补丁）和应用程序软件，以及配置 AWS 提供的安全控制措施，例如安全组、网络访问控制列表以及身份和访问管理。您应慎重考虑使用哪些服务，因为您所承担的责任会因选择的服务、服务与 IT 环境的集成以及适用法律法规而异。图 2 显示了适用于基础设施服务（例如 Amazon Elastic Compute Cloud（Amazon EC2））的责任共担模式的典型表示形式。它将大部分责任分为两类：云的安全性（由 AWS 管理）和云中的安全性（由客户管理）。责任会发生变化，具体取决于使用的服务。对于抽象化服务（例如 Amazon S3 和 Amazon DynamoDB），AWS 运营基础设施层、操作系统和平台，而客户通过访问端点来存储和检索数据。客户负责管理其数据（包括加密选项），对其资产进行分类，以及使用 IAM 工具应用适当的权限。

但是，随着容器和其他服务的增加，责任共担模式发生了变化，这些服务将运营模式移交给服务提供商。随着我们向运营模式的左侧移动，从 IaaS 和数据中心转向 PaaS，服务提供商的责任也随之增加。迁移至图左侧时，客户在云中的责任更少，操作更轻松。请注意下图以及在云中操作或运行能力的差异。随着您在云中的责任共担发生变化，事件响应或取证的选项也会发生变化。作为客户，在规划事件响应时，您还需要确保围绕运营模型中的能力进行规划，并在您选择的模型中发生可能的交互之前对其进行规划。规划和了解这些权衡并将其与您的治理需求相匹配，这是事件响应的关键步骤。

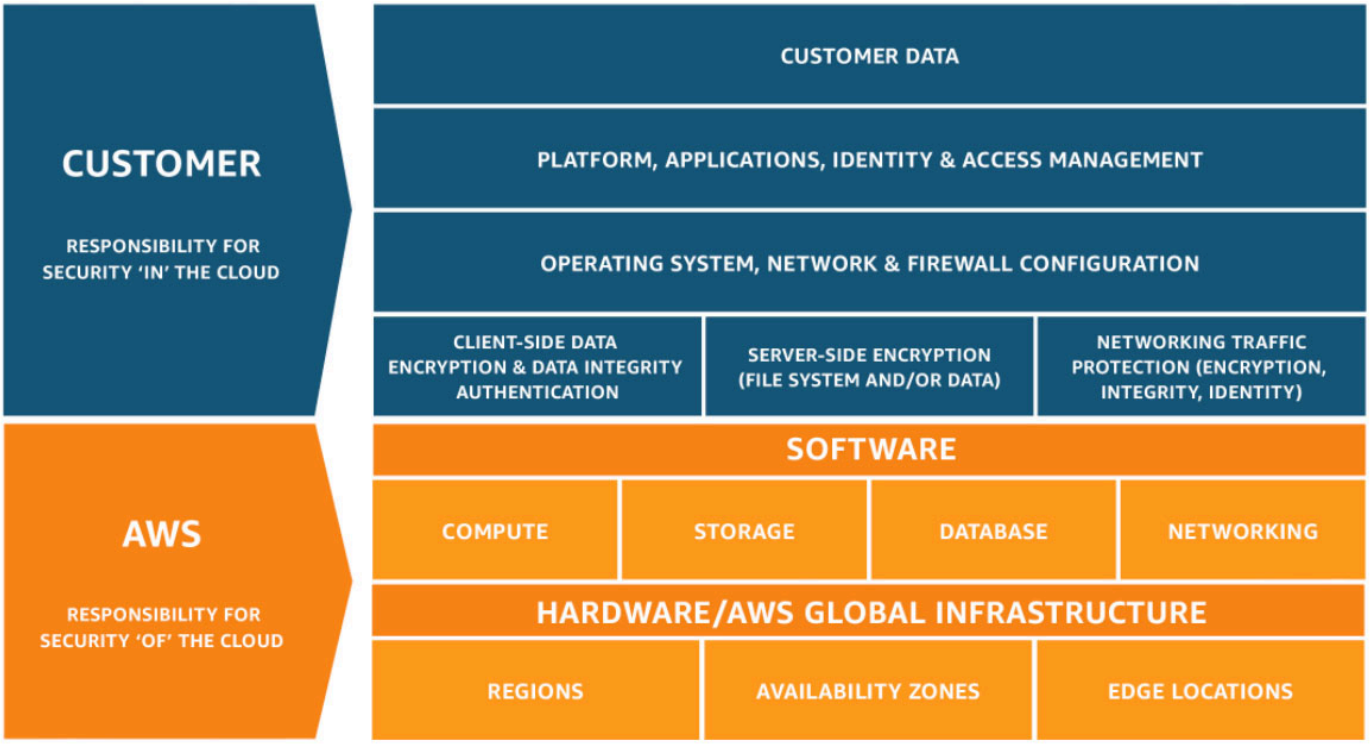
CUSTOMER
RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD
CUSTOMER DATA
PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)
AWS
RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD
SOFTWARE
COMPUTE
STORAGE
DATABASE
NETWORKING
HARDWARE/AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

图 1：责任共担模式

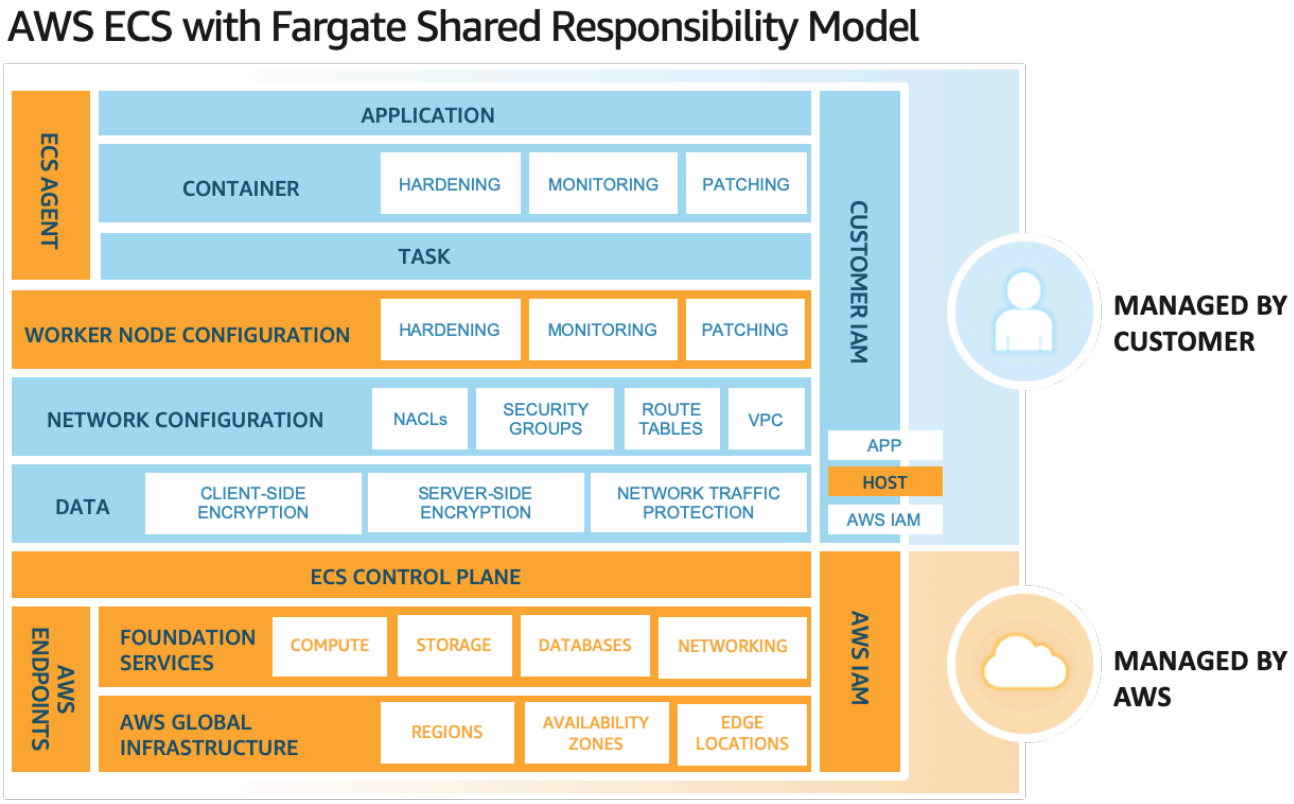

图 2：具有 AWS Fargate 类型责任共担模式的 Amazon Elastic Container Service（Amazon ECS）

除了您与 AWS 的直接关系之外，可能还有其他实体在您的特定责任模式中承担责任。例如，您可能有内部组织单位负责运营的某些方面。您可能还有合作伙伴或其他第三方来开发、管理或运营您的部分云技术。

创建与您的运营模式相匹配的适合事件响应和取证运行手册，这一点非常重要。您的成功取决于您对您需要为所选运营模式创建或购买的工具类型的了解。您的组织对可用工具的了解越深入，您为满足企业监管风险与合规性（GRC）模式的需求所做的准备就越充分。

云中的事件响应

云响应的设计目标

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那些流程和机制）依然有效，但我们建议您考虑这些与云环境中的安全事件响应相关的特定设计目标：

- 制定响应目标 – 与您的利益攸关方、法律顾问和组织领导合作，确定事件响应目标。一些常见目标包括抑制和缓解问题、恢复受影响的资源、保留数据以供取证和确定归属。
- 利用云进行响应 – 在发生事件和遇到数据时，实施您的响应模式。
- 了解您拥有和需要的证据 – 将日志、快照和其他证据复制到中央安全云账户中，以保留这些证据。使用标签、元数据和保留策略实施机制。例如，您可以出于调查目的，选择使用 Linux dd 命令或相应的 Windows 命令为数据制作一个完整的副本。
- 使用重新部署机制 – 如果安全异常可归因于配置错误，那么可能只需使用适当的配置重新部署资源以消除差异即可完成修复。如果可能，请确保您的响应机制能够安全地在未知状态下多次发挥作用。
- 尽可能自动化 – 当您发现问题或事件反复发生时，构建一些能够以编程方式确定并响应常见情况的机制。对于特殊事件、新事件和敏感事件，进行人为响应。
- 选择可扩展的解决方案 – 尽量让您的组织所用方法的可扩展性与云计算能力相匹配，并缩短检测与响应之间的时间差。
- 了解并改进您的流程 – 当您发现流程、工具或员工存在差距时，制定相应规划来弥补这些差距。模拟是找到差距和改进流程的安全方法。

NIST 设计目标提醒您检查架构，以确定它是否能够执行事件响应和威胁检测。在规划云实施时，请考虑响应事件或取证事件。在某些情况下，这意味着您可能为这些响应任务专门设置了多个组织、客户和工具。这些工具和功能应通过部署管道提供给事件响应者，并且不应是静态的，因为这样会导致更大的风险。

云安全事件

主题

事件域

在客户的责任范围内，安全事件可能发生在三个领域：服务、基础设施和应用程序。领域之间的差异与您在响应时使用的工具有关。以下面的领域为例：

- 服务领域 – 服务领域中的事件会影响客户的 AWS 账户、IAM 权限、资源元数据、计费等方面。服务领域事件包括您专门使用 AWS API 机制响应的事件，或者具有与您的配置或资源权限相关的根本原因的事件，以及可能具有相关的面向服务的日志记录的事件。

- 基础设施领域 – 基础设施领域中的事件包括数据或网络相关活动，例如流向 VPC 内 Amazon EC2 实例的流量、Amazon EC2 实例上的流程和数据，以及其他方面，例如容器或其他未来服务。对基础设施领域事件的响应通常涉及检索、恢复或获取用于取证的事件相关数据。可能包括与实例操作系统的交互，在某些情况下，还可能涉及 AWS API 机制。
- 应用程序领域 – 应用程序领域中的事件发生在应用程序代码或部署到服务或基础设施的软件中。此领域应包含在您的云威胁检测和响应运行手册中，并且可能包含与基础设施领域中的响应类似的响应。借助适当且经过深思熟虑的应用架构，您可以使用云工具通过自动取证、恢复和部署来管理此领域。

在这些领域中，您必须考虑可能对您的账户、资源或数据采取行动的参与者。无论是内部还是外部，使用风险框架来确定您的组织面临的具体风险并做好相应的准备。

在服务领域，您致力于完全通过 AWS API 来实现自己的目标。例如，处理来自 Amazon S3 存储桶的数据泄露事件涉及 API 调用，以便检索存储桶的策略、分析 S3 访问日志，以及可能查看 AWS CloudTrail 日志。在本示例中，您的调查不太可能涉及数据取证工具或网络流量分析工具。

在基础设施领域，您可以在工作站的操作系统中使用 AWS API 和熟悉的数字取证/事件响应（DFIR）软件的组合，例如您为 IR 工作准备的 Amazon EC2 实例。基础设施领域事件可能涉及分析网络数据包捕获、Amazon Elastic Block Store（Amazon EBS）卷上的磁盘数据块或从实例获取的易失性内存。

云安全事件的指标

有许多安全事件可能未归类为事故，但仍应谨慎地对它们进行调查。要检测您的 AWS 云环境中的安全相关事件，您可以使用这些机制。以下示例均为可能的指标，并非详尽无遗，但可作为参考：

- 日志和监控器 – 查看 AWS 日志（例如 Amazon CloudTrail、Amazon S3 访问日志和 VPC 流日志）和安全监控服务（例如 Amazon GuardDuty、Amazon Detective、AWS Security Hub 和 Amazon Macie）。此外，还可以使用 Amazon Route 53 运行状况检查和 Amazon CloudWatch 警报等监控。同样，使用 Windows 事件、Linux 系统日志以及您可以在应用程序中生成的其他特定于应用程序的日志，然后使用 CloudWatch 代理记录到 Amazon CloudWatch。
- 计费活动 – 计费活动的突然变化可能表示发生了安全事件。
- 威胁情报 – 如果您订阅了第三方威胁情报源，则可以将该信息与其他日志记录和监控工具关联起来，以识别潜在的事件指标。
- 合作伙伴工具 – AWS 合作伙伴网络（APN）中的合作伙伴提供数百种业界领先的产品，可帮助您实现安全目标。有关更多信息，请参阅安全合作伙伴解决方案和AWS Marketplace 中的安全解决方案。

- AWS Outreach – 如果我们发现滥用或恶意活动，AWS Support 可能会与您联系。有关更多信息，请参阅 AWS 对滥用和损害的回应部分。
- 一次性联系 – 由于可能是您的客户、开发人员或组织中的其他员工发现了异常情况，因此需要有一种广为人知的方法来联系您的安全团队，这非常重要。热门选择包括工单系统、联系电子邮件地址和 Web 表单。如果您的组织为公众服务，您可能还需要面向公众的安全联系机制。

AWS 为自动化和检测提供的其中一个工具是 AWS Security Hub。Security Hub 让您可以在一个位置全面了解各个 AWS 账户的高优先级安全警报和合规性状态，从而更好地了解这些指标。AWS Security Hub 不是安全信息和事件管理（SIEM）软件，它不存储日志数据，而是汇总、整理来自多个 AWS 服务的安全警报或调查结果并确定其优先级。Security Hub 还使您能够创建来自多个来源的自定义洞察。这样，安全运营团队就可以在事件发生时作出选择并深入了解更多信息。Security Hub 根据 AWS 最佳实践以及您组织所遵循的行业标准，自动进行合规性检查，从而持续监控您的环境。

此外，您还可以在 Amazon Detective 或 Amazon Athena 中对安全性与合规性进行调查，或通过使用 Amazon CloudWatch Events 或 Event Bus 规则将这些安全性和合规性调查结果发送至工单、聊天、SIEM、安全编排自动化和响应（SOAR）以及事件管理工具，或者发送到自定义修复行动手册，从而对这些调查结果采取措施。基于事件的自动化使您可以自动响应发生的事件。与本地环境相比，这种方法改变了安全性以及您在云中处理事件的方式。

了解云功能

AWS 提供了各种安全功能，您可以使用这些功能来调查各个领域的安全事件。例如，AWS 提供了许多日志记录机制，例如 AWS CloudTrail 日志、Amazon CloudWatch Logs、Amazon S3 访问日志等。您应该考虑正在使用的服务，并确保已启用与这些服务相关的日志。AWS 还提供集中式日志记录解决方案，可帮助您了解如何集中和存储常见类型的云日志。启用这些日志记录源后，您必须决定如何分析它们，例如使用 Amazon Athena 查询 Amazon S3 存储桶中保存的日志。

此外，还有许多 APN 合作伙伴产品可以简化分析这些日志的过程，例如 APN 安全能力计划中说明的那些产品。还有几种 AWS 服务可以帮助您获得有关这些数据的宝贵洞察，例如 Amazon GuardDuty（威胁检测服务）和 AWS Security Hub，它们让您可以全面了解各个 AWS 账户的高优先级安全警报和合规性状态。此外，Amazon Detective 还会从您的 AWS 资源收集日志数据，并使用机器学习、统计分析和图论来帮助您确定发生潜在安全问题或可疑活动的根本原因。有关在调查期间可以利用的其他云功能的更多信息，请参阅附录 A：云功能定义。

主题

- 数据隐私
- AWS 对滥用和损害的回应

数据隐私

我们知道客户非常关心隐私和数据安全，因此我们实施了负责任且完善的技术和物理控制，旨在阻止对客户内容进行未经授权的访问或披露。维护客户信任是一项持续的承诺。您可以在我们的数据隐私常见问题页面上了解有关 AWS 数据隐私承诺的更多信息。

这些有意识、自我强加的控制限制了 AWS 协助在客户环境中作出响应的能力。因此，在 AWS 云中取得成功的关键在于专注于在责任共担模式中理解和构建能力。尽管在事件发生之前在 AWS 账户中启用日志记录和监控功能非常重要，但事件响应还有其他方面对于计划取得成功至关重要。

加州消费者数据隐私

2018 年《加州消费者隐私法案》（CCPA）授予 “消费者对企业持有的与消费者相关的个人信息的各种权利”，这些权利受 CCPA 约束。有关与受 CCPA 约束的客户相关的 AWS 隐私和数据安全政策的信息，请参阅为加利福尼亚州消费者隐私法案做准备白皮书以获取指导。

一般数据保护条例

《一般数据保护条例》（GDPR）是一项欧洲隐私法（2016 年 4 月 27 日颁布的欧洲议会和理事会 2016/679 号条例），于 2018 年 5 月 25 日开始强制实施。GDPR 取代了欧盟数据保护指令（指令 95/46/EC），在每个欧盟成员国应用具有约束力的单一数据保护法，从而协调整个欧盟（EU）的数据保护法。有关与 GDPR 相关的 AWS 合规性的信息，请参阅了解 AWS 上的 GDPR 指导白皮书。

AWS 对滥用和损害的回应

滥用活动是对 AWS 客户的实例或其他资源观察到的行为，这些行为具有恶意、会发起进攻、违反法律或可能对其他互联网站点造成损害。AWS 与您合作检测和处理针对您的 AWS 资源的可疑和恶意活动。您的资源中的非预期或可疑行为可能表示您的 AWS 资源已经受到损害，这可能对您的企业构成潜在风险。请记住，您的 AWS 账户中有备选联系方式。无论是出于安全性还是计费目的，在添加联系人时，请务必遵循最佳实践。尽管您的根账户电子邮件是 AWS 通信的主要目标，但 AWS 也会向辅助电子邮件地址传达安全问题和计费问题。添加仅发送给一个人的电子邮件地址，这意味着您向 AWS 账户中添加了单点故障。请确保您已向联系人添加了至少一个通讯组列表。

AWS 使用以下机制检测您资源中的滥用活动：

- AWS 内部事件监控。
- 针对 AWS 网络地址空间的外部安全信息。
- 针对 AWS 资源的互联网滥用投诉。

尽管 AWS 滥用响应团队会积极地监控并关闭在 AWS 中运行的未经授权的活动，但大多数滥用投诉都与在 AWS 中经营合法业务的客户有关系。以下是非故意滥用活动常见原因的一些示例：

- 遭盗用的资源 – 未安装修补程序的 Amazon EC2 实例受到感染而成为僵尸网络代理。
- 非故意滥用 – 过度激进的 Web 爬网程序可能会被某些互联网站点归类为拒绝服务攻击。
- 次要滥用 – 使用 AWS 客户所提供服务的终端用户可能在公有 Amazon S3 存储桶中发布恶意软件文件。
- 错误投诉 – 有时，互联网用户会错误地将合法活动报告为滥用行为。

AWS 尽全力与 AWS 客户合作，共同防止、检测和减少滥用，防范以后再出现滥用。我们建议您查看 AWS 可接受使用政策，该政策描述了禁止使用 Amazon Web Services 及其附属公司提供的 Web 服务的情况。为支持及时响应 AWS 的滥用通知，请确保您的 AWS 账户联系信息准确无误。当您收到 AWS 滥用警告时，您的安全与运营人员应立即对事件展开调查。拖延可能会延长声誉影响以及对自己和他人造成的法律影响。更重要的是，受牵涉的滥用资源可能被恶意用户损害，忽视这种损害可能会加大对您业务造成的破坏。

准备 – 人员

使用自动化流程，组织将有更多的时间专注于能够提高其云环境和应用程序安全性的措施。自动化事件响应还能够让人员关联事件、练习模拟、设计新的响应程序、执行研究、开发新技能以及测试或构建新的工具。尽管提高了自动化程度，但安全组织中的分析师和响应者仍有许多工作要做。同质化团队会制造盲点，因此必须建立一个多元化的团队，在复杂的不稳定环境中提供不同的思维体系、文化视角以及工作和生活体验。在为事件做计划时，我们能做的最有影响力的事情之一就是确保我们的团队和响应计划具有多元性。一个由具有不同观点的人员组成的团队有可能找出可能没有被发现的盲点，并找出原本可能没有想到的解决方案。

主题

定义角色和职责

在处理新事件或大规模事件时，事件响应的技能和机制最为重要。这些事件取决于您的团队制定的书面标准和您的团队已经进行过的实践。由于我们无法预测或整理事件的所有潜在方向，因此我们依靠自动化来完成简单、重复的任务，例如收集实例内存或诊断日志，然后让人类做出艰难的决定。处理不明确的安全事件需要跨组织的纪律性、偏向于采取果断行动以及交付结果的能力。在事件发生期间，组织结构中应该有许多人可负责、可审计、可咨询或随时了解最新进展，例如来自人力资源（HR）、管理团队和法务部门的代表。考虑这些角色和职责，以及是否必须有第三方参与。请注意，在许多地区，都有当地法律规定可以做什么和不能做什么。尽管为事件建立可负责、可审计、可咨询和知情（RACI）图表似乎有些官僚主义，但这样做可以实现快速而直接的沟通，清晰地勾勒出事件不同阶段的领导层。

值得信赖的合作伙伴可能会参与调查或响应，他们会提供额外的专业知识和有价值的审查。当您自己的团队不具备这些技能时，可能需要聘请外部人员以寻求协助。如果雇用了外部人员，请确保该方对您的团队成员进行培训。当这些外部各方与您的内部开发人员和运营者合作时，他们可以扩展团队成员的技能，而新的专业知识对未来的 IR 计划很有价值。

在事件发生期间，关键的是将受影响应用程序和资源的所有者和开发人员考虑在内，因为他们是可以提供信息和上下文的主题专家（SME）。在依靠开发人员和应用程序所有者的专业知识进行事件响应之前，请务必与开发人员和应用程序所有者进行练习并与他们建立关系。应用程序所有者或 SME 可能需

要在环境不熟悉、具有意想不到的复杂性或响应者无法访问的情况下采取行动。应用程序 SME 应该练习并适应与 IR 团队的合作。

提供培训

为了降低依赖性并缩短响应时间，请确保您的安全团队和响应者接受有关云服务的培训，并有机会亲身体验组织使用的特定云平台。其中一些培训来自于流程开始时进行的团队建设和运行手册创建。通过在形成运行手册的初始步骤中让尽可能多的人员参与进来，您可以更好地了解内部团队。随着这些团队开始在桌面练习中遵循这些运行手册，这种培训变得更加真实。

AWS 和其他第三方还提供在线安全研讨会（AWS 安全研讨会），您可以下载并完成这些研讨会。通过提供额外的培训，以使您的员工学习编程技能、开发流程（包括版本控制系统和部署实践）和基础设施自动化，您的组织将会受益良多。

AWS 通过数字培训、课堂培训、APN 合作伙伴和认证提供了许多培训选项和学习路径。要了解更多信息，请参阅 AWS 培训和认证。

定义响应机制

您的响应机制取决于您的监管、风险与合规性（GRC）模型。理想情况下，在计划事件响应之前构建 GRC 模型。如果您还没有开始构建 GRC，那么这是建立良好的事件响应机制不可或缺的第一步。当您与其他团队（例如法律顾问、领导、业务利益攸关方等）一起考虑云中的事件响应方法时，您必须了解自己拥有什么和需要什么。确定利益攸关方和相关联系人，并确保您有适当的访问权限来执行必要的响应。

云可以通过服务 API 为您提供更好的可见性和更多功能，而您的 GRC 模型向您展示了如何在响应中使用这些 API。确定团队的 AWS 账号、Virtual Private Cloud（VPC）的 IP 范围、相应的网络图、日志、数据位置和数据分类。准备 – 技术 部分中包括了其中许多技术流程。然后，开始记录事件响应程序（通常称为程序或运行手册），这些程序定义了调查和修复事件的步骤。

营造一种具有接受性和适应性的安全文化

在 AWS，我们了解到，当安全团队成为其业务和开发人员的协作推动者时，我们的客户和我们自己的内部团队才能取得最大的成功，他们培养一种文化，确保所有利益攸关方进行合作并逐步升级以保持敏捷、响应迅速的安全状况。尽管改善组织的安全文化不是本白皮书的主题，但如果非安全人员认为安全团队乐于接受，您可以从他们那里获得相关情报。当您的安全团队开放且可访问时，在领导层的支持下，他们更有可能获得更多、及时的通知、合作以及对安全事件的响应。

在某些组织中，工作人员可能会害怕在报告安全问题时遭到报复。有时他们根本不知道如何报告问题。在其他情况下，他们可能不想浪费时间，或者在将某件事报告为安全事件但后来发现不是问题时可能会感到尴尬。从领导团队开始，重要的是要提倡一种接受的文化，并邀请每个人都参与到维护组织安全中来。为所有人提供清晰的渠道，让他们在认为可能存在潜在风险或威胁时开立严重程度较高的工单。以热切和开放的心态接受这些通知，但更重要的是，向非安全人员明确表示欢迎这些通知。强调您宁愿收到过多的潜在问题通知，也不愿根本接收不到任何通知。比起让研究人员在公开文章中指出问题，让开发人员说出他或她自己的错误要好得多。

这些通知为在压力下进行响应式调查提供了宝贵的机会。在您制定响应程序时，它们可以作为重要的反馈循环。

预测响应

由于无法预测所有潜在事件，因此您必须继续依靠人工分析。花时间认真培训员工并为组织做好准备，帮助您预测意想不到的情况；但是，您的组织不必单独准备。与值得信赖的安全合作伙伴合作以识别意外安全事件，使组织受益于额外的可见性和洞察。

合作伙伴和响应窗口

每个组织的云之旅都是独一无二的。但是，其他组织已经遇到过一些值得信赖的安全合作伙伴可以提请您注意的模式和做法。我们建议您寻找外部 AWS 安全 APN 合作伙伴，他们应当能够为您带来外部专业知识和不同的视角，以增强您的响应能力。您的可靠安全合作伙伴可以帮助您发现您可能并不熟悉的潜在风险或威胁。

1955 年，Joseph Luft 和 Harrington Ingham 创建了乔哈里视窗，这是一个将特质映射到类别的练习。该视窗被描绘为由四个象限组成的网格，类似于下图。

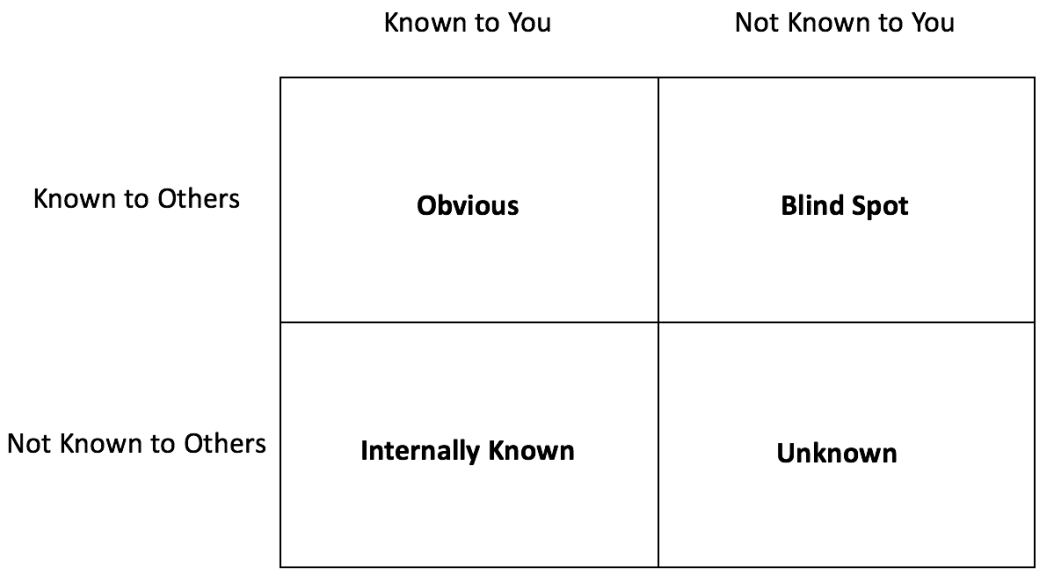

图 3：为事件响应修改乔哈里视窗

尽管乔哈里视窗不是为信息安全而设计，但我们可以调整该概念，将其用作简单的心智模型，以考虑评估组织威胁的困难度。在我们修改后的概念中，四个象限是：

- 显而易见 – 您的团队和您的 APN 合作伙伴都知道的风险。
- 内部已知 – 您的团队熟悉但您的 APN 合作伙伴不熟悉的风险。这可能意味着您有内部专业知识或系统知识。
- 盲点 – 您的 APN 合作伙伴熟悉但您的团队不熟悉的风险。
- 未知 – 您或您的 APN 合作伙伴都不熟悉的风险。

尽管此示意图很简单，但它代表了拥有值得信赖的 APN 合作伙伴可以实现的价值。最关键的是，可能有一些您不知道的盲点项，但具备适当专业知识的 APN 合作伙伴可以提请您注意这些事项。尽管你们可能都熟悉显而易见象限中的这些风险，但您的 APN 合作伙伴可以推荐您不熟悉的控制措施和解决方案。此外，尽管您可能会提请您的 APN 合作伙伴注意内部已知象限中的这些风险，但您的 APN 合作伙伴可能还可以确定优化的控制措施来降低该风险。在衡量自己的改进情况时，请联系您的 APN 合作伙伴以提供专家建议。

未知风险

如果您一直专注于定制警报、通过自动化改进事件响应程序以及改进安全防御，那么您可能会想知道接下来要改进什么。您可能对未知风险感到好奇，如图 3 中的未知类别所示。您可以通过以下方法降低未知风险：

- 定义安全断言 – 您可以断言哪些事实？ 在您的环境中绝对应该存在哪些安全原语？ 明确定义这些原语使您可以逆向搜索。这在云之旅的早期阶段更容易做到，而不是在以后尝试对安全断言进行逆向工程。
- 教育、沟通和研究 – 在员工中培养云安全专家，或让专家合作伙伴协助仔细检查您的环境。挑战您的假设，警惕微妙的推理。在流程中创建反馈循环，并为工程团队提供与安全团队沟通的机制。您还可以扩展监控相关安全邮件列表和信息安全披露的方法。
- 减少攻击面 – 提高防御能力，规避风险，让自己有更多时间抵御未知攻击。阻止攻击者和减慢攻击者的速度，并迫使他们发出噪音。
- 威胁情报 – 订阅世界各地的当前和相关威胁、风险和指标的持续馈送。
- 警报 – 生成通知，提醒您注意异常、恶意或代价高昂的活动。例如，您可为在不使用的区域或服务中发生的活动创建通知。
- 机器学习 – 使用机器学习来识别特定组织或个人角色的复杂异常。为了帮助您识别异常行为，您还可以分析网络、用户和系统的正常特征。

当您考虑盲点和未知的未知数时，威胁情报成为主要话题。乔哈里视窗显示了如何对您知道和不知道的内容进行分类，而威胁情报显示如何解释您还不知道的内容。威胁情报是一门学科，可以帮助公司了解威胁模型的各个角落，以发现贵公司可能还不知道存在的威胁。

通常，威胁情报包括：

1. 发现新的威胁。
2. 定义新模式。
3. 定义新的自动化采集技术。
4. 重复这些过程。

尽管这种做法可能会有所帮助，但威胁情报团队的照护和维护可能会使许多企业（甚至是大型企业）负担过重。最后，问题变成了匹配威胁模型、规模和风险逆境的问题。考虑这些问题：

- 您的威胁模型是否与企业所处的标准垂直行业有足够的显著差异？
- 您的风险偏好是否足够低，导致需要这样的团队？

- 为您的企业组建一支团队在财务上是否可行？
- 您的风险状况是否足以吸引合理的人才加入您的事业？

如果您对这些问题中的任何一个的回答是否，您很可能应该找一个威胁情报合作伙伴。这项服务由许多大型知名公司提供，具有竞争力。

AWS 为您提供了自行管理这些问题的工具和服务。使用机器学习识别恶意模式是一个经过充分研究的研究领域，其模式由客户、AWS 专业服务、APN 合作伙伴以及通过 Amazon GuardDuty 和 Amazon Macie 等 AWS 服务来实施。其中一些模式已在 AWS re:Invent 会议上进行了讨论。有关更多信息，请参阅本白皮书的媒体部分。

客户还在扩展其传统上以业务为中心的数据湖，以便在开发安全数据湖时利用类似的架构模式。安全运营团队还将传统日志记录和监控工具（例如 Amazon OpenSearch Service 和 OpenSearch Dashboards）的使用扩展到大数据架构。

这些客户从 AWS CloudTrail 事件日志、VPC 流日志、Amazon CloudFront 访问日志、数据库日志和应用程序日志中收集内部数据，然后将这些数据与公有数据和威胁情报相结合。有了这些宝贵的数据，客户已经扩展到将数据科学和数据工程技能纳入其安全运营团队，以便利用 AWS 上的 Amazon EMR、Amazon Kinesis Data Analytics、Amazon Redshift、Amazon QuickSight、AWS Glue、Amazon SageMaker 和 Apache MXNet 等工具来构建用于识别和预测其业务特有的异常情况的自定义解决方案。

最后，请参阅安全合作伙伴解决方案，了解 APN 合作伙伴提供的数百种业界领先的产品，这些产品与本地环境中的现有控件等效、相同或相集成。这些产品对现有 AWS 服务起到补充作用，使您能够在云和本地部署环境中部署全面的安全架构，进而实现更为无缝的体验。

准备 – 技术

主题

准备对 AWS 账户的访问权限

在事件发生期间，您的事件响应团队必须能够访问事件所涉及的环境和资源。确保您的团队拥有适当的访问权限，以便能够在事件发生之前履行他们的职责。为此，您必须了解您的团队成员所需的访问级别（例如他们可能采取哪些类型的操作），还必须提前预置访问权限。这种访问权限来自您公司的监管、风险管理和合规性（GRC）政策。在事件发生之前应该对您的团队成员的身份验证和授权进行记录和测试，以确保他们能够及时响应而不会出现延迟。为了正确响应事件，准备工作的一部分应该是审查 AWS 账户的布置方式以及如何允许和组织跨账户角色。

在此阶段，您必须与开发人员、架构师、合作伙伴、监管团队和合规性团队密切合作，以了解响应者所需的访问权限级别。确定并与您的组织的云架构师讨论 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，例如：

- 联合 – 用户在身份提供商的 AWS 账户中担任 IAM 角色。
- 跨账户访问 – 用户在多个 AWS 账户中担任 IAM 角色。
- 身份验证 – 用户作为在单个 AWS 账户中创建的 AWS IAM 用户进行身份验证。

这些选项定义了针对 AWS 进行身份验证的技术选择，以及您在响应期间如何获得访问权限，但有些组织可能会依赖另一个团队或合作伙伴来协助响应。为了响应安全事件而创建的用户账户通常是特权，目的是提供足够的访问权限。因此，应限制使用这些用户账户，而且不应使用这些账户来执行日常活动。

在创建新的访问机制之前，请与您的云团队合作，了解如何组织和管理您的 AWS 账户。许多客户使用 AWS Organizations 来帮助集中管理账单、在其 AWS 账户之间共享资源以及控制访问、合规性和安全性。Organizations 的核心功能是可以利用它来将服务控制策略应用于账户组，从而使您能够大规模进行策略管理。有关大规模实施治理机制的更多信息，请参阅 AWS 大规模治理。了解您的组织如何组织和管理您的 AWS 账户之后，请考虑以下通用响应模式，以帮助确定哪些方法适合您的组织。

主题

- 间接访问权限
- 直接访问权限
- 替代访问权限
- 自动化访问
- 托管式服务访问

间接访问权限

如果您使用间接访问权限，您的账户所有者或应用程序团队需要在作为安全专家的事件响应团队的战术指导下，在其 AWS 账户中执行授权修复。通过这种方法执行任务时速度较慢且更复杂，但是当响应者不熟悉账户或云环境时，它可能会成功。

直接访问权限

要向事件响应者提供直接访问权限，请将安全工程师或事件响应者可以在安全事件期间担任的 AWS IAM 角色部署到 AWS 账户中。如果事件影响到您的正常身份验证过程，事件响应者可通过正常的联合过程或特殊的紧急过程进行身份验证。您授予事件响应 IAM 角色的权限取决于您预计响应者要执行的操作。

替代访问权限

如果您认为安全事件正在影响您的安全、身份或通信系统，则可能需要寻求替代机制和访问权限来调查和修复影响。通过使用专门构建的新 AWS 账户，您的响应者可以在安全的替代基础设施中进行协作和工作。

例如，响应者可以利用在云中启动的新基础设施，例如使用 Amazon WorkSpaces 的远程工作站和 Amazon WorkMail 提供的电子邮件服务。您必须准备适当的访问控制（使用 IAM 策略）来委派访问权限，以便您安全的替代 AWS 账户能够获得受影响的 AWS 账户的权限。

委托适当的访问权限后，您可以使用受影响账户中的 AWS API 共享相关数据（例如日志和卷快照），以便在隔离环境中执行调查工作。有关此跨账户访问的更多信息，请参阅教程：使用 IAM 角色委派跨 AWS 账户的访问权限。

自动化访问

迁移到使用自动化来响应安全事件时，您必须专门为要使用的自动化资源（例如 Amazon EC2 实例或 AWS Lambda 函数）创建 IAM 角色。然后，这些资源可以担任 IAM 角色并继承分配给该角色的权

限。您无需创建和分发 AWS 凭证，而是向 AWS Lambda 函数或 Amazon EC2 实例委派权限。AWS 资源会自动接收一组临时凭证，并使用它们签署 API 请求。

您还可以考虑一种安全的方法，让您的自动化或工具在您的 Amazon EC2 实例的操作系统中进行身份验证和执行。尽管有许多工具可以执行此自动化，但请考虑使用 AWS Systems Manager Run Command，它可以使用安装在 Amazon EC2 实例操作系统中的代理，安全地远程管理实例。

默认情况下，AWS Systems Manager Agent（SSM Agent）安装在某些 Amazon EC2 Amazon Machine Images（AMI）上，例如 Microsoft Windows Server 和 Amazon Linux。但是，您可能需要在其他版本的 Linux 和混合实例上手动安装代理。无论您是使用 Run Command 还是其他工具，在收到要调查的第一个安全相关警报之前，请先完成所有先决条件设置和配置。

托管式服务访问

您的组织可能已经与代表您管理服务和解决方案的信息技术提供商建立了合作伙伴关系。这些合作伙伴在支持组织的安全方面共担责任，重要的是在发生异常情况之前清楚地了解这种关系。无论您已经与 AWS 托管式服务提供商（MSP）合作伙伴、AWS Managed Services，还是托管式安全服务合作伙伴合作，都必须确定每个合作伙伴与您的云环境相关的责任、提供商对您的云服务已经拥有什么访问权限、他们需要什么访问权限，以及当您需要帮助时可以获得的联系人或上报路径。最后，您应该与合作伙伴一起练习，以确保您的响应计划可预测并取得成功。

准备流程

预置和测试适当的访问权限后，您的事件响应团队必须定义并准备调查和修复所需的相关流程。此阶段需要大量精力，因为您必须充分规划对云环境中的安全事件的适当响应。

与内部云服务团队和合作伙伴密切合作，以确定可确保实施这些流程的必要任务。相互协作或分配响应活动任务，并确保必要的账户配置已经就绪。我们建议您提前准备流程和先决条件配置，以便为您的组织提供以下响应能力。

主题

- 事件即将发生时启动资源
- 隔离资源
- 启动取证工作站

决策树

有时，不同的条件可能需要不同的操作或步骤。例如，您可以根据 AWS 账户的类型（开发账户与生产账户）、资源标签、这些资源的 AWS Config 规则合规性状态或其他输入采取不同的操作。

为了支持您创建和记录这些决策，我们建议您与其他团队和利益攸关方一起起草决策树。与流程图类似，决策树是一种可以用来支持决策的工具，有助于指导您根据潜在条件和输入（包括概率）确定最佳行动和结果。

使用替代账户

尽管可能需要对受影响账户中的事件作出响应，但最好是调查受影响账户以外的数据。有些客户有一个创建独立、隔离的 AWS 账户环境的流程，使用模板来预先配置他们必须预置的资源。这些模板通过服务（例如 AWS CloudFormation 或 Terraform）进行部署，该服务提供了一种简单的方法来创建相关 AWS 资源的集合，并以有序且可预测的方式对其进行预置。

使用模板化机制预先配置这些账户，这有助于消除事件初始阶段的人为交互，并确保以可重复和可预测的方式准备环境和资源，并可通过审计进行验证。此外，这种机制还提高了在取证环境中维护数据安全和遏制数据的能力。

此方法要求您与云服务和架构师团队合作，确定可用于调查的适当 AWS 账户流程。例如，您的云服务团队可以使用 AWS Organizations 生成新账户，并协助您使用模板化或脚本化方法预先配置这些账户。

当您需要使大型组织远离潜在威胁时，这种分段方法是最佳选择。这种分段使用的是新的、在很大程度上没有关联的 AWS 账户，意味着来自组织且在多账户文档中被标记为安全组织单位（OU）的用户能够进入账户，执行所需的取证活动，并有可能在需要时将账户作为一个整体移交给法律实体。这种取证和归因方法需要进行大量的审查和规划，并且应符合企业的 GRC 政策。尽管这项工作并不容易，但在建立庞大的客户基础之前完成这项工作要容易得多。

查看或复制数据

响应者需要访问日志或其他证据才能进行分析，并且必须确保他们能够查看或复制数据。响应者的 IAM 权限策略至少应提供只读访问权限，以便他们可以进行调查。要启用适当的访问权限，您可以考虑使用一些预先构建的 AWS 托管策略，例如 SecurityAudit 或 ViewOnlyAccess。

例如，响应者可能希望将数据（如 AWS CloudTrail 日志）从一个账户中的 Amazon S3 存储桶复制到另一个账户中的 Amazon S3 存储桶，制作一个时间点副本。例如，ReadOnlyAccess 托管策略提供的权限使响应者可以执行这些操作。要了解如何使用 AWS 命令行界面（CLI）执行此操作，请参阅如何将所有对象从一个 Amazon S3 存储桶复制到另一个存储桶？。

共享 Amazon EBS 快照

许多客户使用 Amazon Elastic Block Store（Amazon EBS）快照作为涉及其 Amazon EC2 实例的安全事件调查的一部分。Amazon EBS 卷的快照是增量备份。有关 Amazon EBS 增量快照的更多信息，请参阅 Amazon EBS 快照。

要对单独的隔离账户中的 Amazon EBS 卷进行调查，您必须修改快照的权限，以便与其他指定的 AWS 账户共享该快照。您已授权的用户可以使用您共享的快照作为基础来创建自己的 EBS 卷，同时您的原始快照不受影响。有关更多信息，请参阅共享 Amazon EBS 快照。

如果快照已加密，则还必须共享用于加密快照的自定义 AWS Key Management Service（AWS KMS）客户管理密钥（CMK）。您可以在创建自定义 CMK 时或以后的某个时间向自定义 CMK 应用跨账户权限。快照受限于创建快照的区域，但您可以将快照复制到另一个区域，以便与该区域共享快照。有关更多信息，请参阅复制 Amazon EBS 快照。

共享 Amazon CloudWatch Logs

Amazon CloudWatch Logs 中记录的日志（例如 Amazon VPC 流日志）可通过 CloudWatch Logs 订阅与另一个账户（例如您的集中式安全账户）共享。例如，可以从集中的 Amazon Kinesis 流中读取日志事件数据，以执行自定义处理和分析。当您从多个账户收集日志记录数据时，自定义处理特别有用。理想情况下，应该在与安全相关的事件发生之前，在云之旅的早期创建此配置。有关更多信息，请参阅使用订阅跨账户共享日志数据。

使用不可变存储

将日志和其他证据复制到替代账户时，请确保复制的数据受到保护。除了保护次要证据外，还必须在源位置保护数据的完整性。这些机制称为不可变存储，通过防止数据被篡改或删除来保护数据的完整性。

使用 Amazon S3 的原生功能，您可以配置 Amazon S3 存储桶来保护数据的完整性。例如，通过使用 S3 对象锁定，您可以在固定的时间段内或无限期地阻止删除或覆盖对象。限制数据写入或读取方式的其他方法是使用 S3 存储桶策略管理访问权限、配置 S3 版本控制和启用 MFA 删除。这种类型的配置对于存储调查日志和证据非常有用，通常称为一次写入，多次读取（WORM）。您还可以使用带有 AWS Key Management Service（AWS KMS）的服务器端加密，并确认只有适当的 IAM 主体才有权解密数据，从而保护数据。

此外，如果您希望在完成调查后将数据安全地保存在长期存储中，请考虑使用对象生命周期策略将数据从 Amazon S3 移动到 Amazon S3 Glacier。Amazon S3 Glacier 是一款安全、持久且成本极低的云存储服务，适用于数据归档和长期备份。它旨在提供 99.999999999% 的耐用性，并提供全面的安全性和合规性功能。

此外，您可以使用 Amazon S3 Glacier 文件库锁定来保护 Amazon S3 Glacier 中的数据，从而使您可以使用文件库锁定策略轻松部署和实施单个 Amazon S3 Glacier 文件库的合规性控制。您可以在一个文件库锁定策略中指定类似 WORM 这样的安全控制，并且可以锁定该策略以防止将来进行编辑。策略在锁定之后便无法更改。Amazon S3 Glacier 可以执行文件库锁定策略中设定的控制，以便帮助您实现合规性目标，例如用于数据留存。您可以使用 AWS Identity and Access Management（IAM）策略语言，在文件库锁定策略中部署各种合规性控制。

事件即将发生时启动资源

对于刚开始使用云的响应者，尝试在现有工具所在的场所进行云调查会很吸引人。根据我们的经验，使用云技术响应事件的 AWS 客户可以获得更好的结果 – 可以自动实现隔离、更轻松地制作副本、更快地准备好分析证据，并且可以更快地完成分析。

最佳实践是在数据所在的云端执行调查和取证，而不是在调查之前尝试将数据传输到数据中心。您几乎可以在世界上任何地方使用云的安全计算和存储功能来执行安全响应操作。许多客户选择预先建立一个单独的 AWS 账户，准备进行调查，但在某些情况下，您可能会选择在同一 AWS 账户中执行分析。如果您的组织出于合规性和法律原因而需要保留记录，那么谨慎的做法是为长期存储和法律活动维护单独的账户。

最佳实践是在发生事件的同一 AWS 区域执行调查，而不是将数据复制到其他区域。我们之所以推荐这种做法，主要是因为在区域之间传输数据需要额外的时间。对于您运营所在的每个 AWS 区域，请确保您的事件响应流程和响应者都遵守相关的数据隐私法。如果您确实需要在区域之间移动数据，请考虑在不同司法管辖区之间移动数据的法律影响。一般而言，最佳实践是将数据保留在同一国家的管辖区内。

如果您认为安全事件正在影响您的安全、身份或通信系统，则可能需要寻求替代机制和访问权限来调查和修复影响。AWS 使您能够快速启动可用于安全的替代工作环境的新基础设施。例如，在调查情况的潜在严重性时，您可能希望使用法律顾问、公共关系和安全团队所需的安全工具创建一个新的 AWS 账户，以便进行沟通和继续工作。诸如 AWS WorkSpaces（用于虚拟桌面）、AWS WorkMail（用于电子邮件）和 Amazon Chime（用于通信）之类的服务可以为您的响应团队、领导层和其他参与者提供他们进行沟通、调查和修复问题所需的能力和连接性。

隔离资源

在调查过程中，为了对安全异常情况作出响应，您可能需要隔离资源。隔离资源的目的是限制潜在影响、防止受影响资源进一步传播、限制数据的意外泄露，以及防止进一步的未经授权访问。

与任何响应一样，可能需要考虑业务、法规、法律或其他因素。确保根据预期和意外的后果权衡您的预期行动。如果您的云团队使用资源标签，则这些标签可以帮助您确定资源的重要性或要联系的所有者。

启动取证工作站

您的一些事件响应活动可能需要分析磁盘映像、文件系统、RAM 转储或者事件中涉及的其他构件。许多客户构建了一个自定义的取证工作站，他们可以使用该工作站挂载任何受影响的数据卷的副本（称为 EBS 快照）。为此，请按照以下基本步骤操作：

1. 选择可以用作取证工作站的基本 Amazon Machine Image（AMI）（例如 Linux 或 Microsoft Windows）。
2. 从该基本 AMI 启动 Amazon EC2 实例。
3. 强化操作系统、删除不需要的软件包并配置相关的审计和日志记录机制。
4. 安装您首选的开源或私有工具包套件，以及您需要的任何供应商软件和软件包。
5. 停止 Amazon EC2 实例，然后从已停止的实例创建新的 AMI。
6. 创建每周或每月的流程，使用最新的软件补丁更新和重建 AMI。

使用 AMI 预置取证系统后，您的事件响应团队可以使用此模板创建新的 AMI，以便为每次调查启动新的取证工作站。可以预先配置作为 Amazon EC2 实例启动 AMI 的流程，以简化部署过程。例如，您可以在文本文件中创建所需取证基础设施资源的模板，然后使用 AWS CloudFormation 将其部署到您的 AWS 账户中。

当您的资源可以通过模板快速部署时，训练有素的取证专家能够为每次调查使用新的取证工作站，而不是重复使用基础设施。通过此过程，您可以确保没有来自其他取证检验的交叉污染。

实例类型和位置

Amazon EC2 提供了针对不同使用案例进行优化的多种实例类型以供选择。实例类型由 CPU、内存、存储和网络容量组成不同的组合，可让您灵活地为您的应用程序选择适当的资源组合。许多实例类型包括多种实例大小，从而使您能够根据目标工作负载的要求扩展资源。对于事件响应实例，请遵循您公司为运行生产实例的网络的位置和分段制定的 GRC 策略。

AWS 增强联网使用单个根 I/O 虚拟化（SR-IOV）为支持的实例类型提供高性能的联网功能。SR-IOV 是一种设备虚拟化方法，与传统虚拟化网络接口相比，它不仅能提高 I/O 性能，还能降低 CPU 使用率。增强联网可以提高带宽，提高每秒数据包数 (PPS) 性能，并不断降低实例间的延迟。使用增强联网不收取任何额外费用。有关哪些实例类型支持 10Gbps 或 25Gbps 网络速度以及其他高级功能的信息，请参阅 Amazon EC2 实例类型。

云提供商支持

主题

AWS Managed Services

AWS Managed Services（AWS）可持续管理您的 AWS 基础设施，让您可以专注于应用程序。AWS 利用最佳实践来维护您的基础设施，帮助您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。

作为基础设施运营商，AMS 负责部署一套安全检测控制措施，并使用全天候模式对警报提供全天候的一线响应。触发警报时，AMS 会遵循一套标准的自动和手动运行手册，以确保响应的一致性。在 AMS 客户加入时与他们分享这些运行手册，以便他们可以与 AMS 一起制定和协调响应。AMS 建议与客户联合执行安全响应模拟，以便在实际事件发生之前开发运营力量。

AWS Support

AWS Support 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，为成功部署和正常实施 AWS 解决方案提供支持。所有支持计划均提供全天候客户服务、AWS 文档服务、白皮书服务和支持论坛服务。如果您需要可帮助规划、部署和优化 AWS 环境的技术支持服务和更多资源，您可以选择一项最适合您的 AWS 用例的支持计划。

对于影响您的 AWS 资源的问题，您应该将 AWS Management Console 中的支持中心视为获得支持的中心联系点。对 AWS Support 的访问由 IAM 控制。有关获取 AWS 支持功能的更多信息，请参阅访问支持。

此外，如果您需要报告滥用 Amazon EC2 的情况，请联系 AWS 滥用问题团队。

DDoS 响应支持

拒绝服务（DoS）攻击会使您的网站或应用程序无法为终端用户提供服务。攻击者会运用多种耗用网络带宽或其他资源的手段来中断终端用户的合法访问。最简单的 DoS 攻击形式是攻击者本人从单一来源对目标实施攻击。

在分布式拒绝服务（DDoS）攻击形式中，攻击者将借助多个来源（可能遭到一组协作者的盗用或控制）发动对目标的攻击。在 DDoS 攻击中，每个协作者或遭到盗用的主机均参与攻击活动，从而生成海量的数据包或请求来“淹没”预定目标。

AWS 为客户提供 AWS Shield，它提供托管的 DDoS 保护服务，可保护在 AWS 上运行的 Web 应用程序。AWS Shield 为您提供始终在线的检测和自动内联缓解措施，可更大限度减少应用程序停机时间和延迟，因此无需联系 AWS Support 即可享有 DDoS 保护。AWS Shield 有两个层级：Standard 和 Advanced。

所有 AWS 客户都可从 AWS Shield Standard 的自动防护功能中获益。AWS Shield Standard 可以抵御以您的网站或应用程序为目标的最为常见、经常发生的网络和传输层 DDoS 攻击。如果将 AWS Shield Standard 与 Amazon CloudFront 和 Amazon Route 53 结合使用，您会获得全面的可用性保护，以应对所有已知的基础设施（第 3 层和第 4 层）攻击。

对于以在 Amazon Elastic Compute Cloud（Amazon EC2）、Elastic Load Balancing（ELB）、Amazon CloudFront 和 Amazon Route 53 资源上运行的 Web 应用程序为目标的攻击，如果想要获得更高级别的防护，您可以使用 AWS Shield Advanced。此外，利用 AWS Shield Advanced，您还可以全天候联系 AWS DDoS 响应团队（DRT）。有关 AWS Shield Standard 和 AWS Shield Advanced 的更多信息，请参阅 AWS Shield。

模拟

主题

安全事件响应模拟

安全事件响应模拟（SIRS）是内部事件，可提供结构化机会，使您能够在逼真的场景中练习您的事件响应计划和程序。SIRS 事件主要涉及做好准备，并以迭代方式提高您的响应能力。客户发现从执行 SIRS 活动中获得价值的一些原因包括：

- 验证准备情况。
- 从模拟中学习以及开展员工培训，建立信心。
- 履行合规或合同义务。
- 生成资格鉴定构件。
- 保持敏捷性，集中精力实现增量改进。
- 提高速度和改进工具。
- 优化沟通和上报。
- 适应罕见和意外的情况。

由于这些原因，通过参与 SIRS 活动而获得的价值能够让组织有效地应对压力重重的事件。开展既逼真又有益的 SIRS 活动可能是一项非常困难的练习。尽管对可处理常见事件的流程或自动化进行测试能够实现一些优势，但只有参与创造性的 SIRS 活动以测试您应对意外情况的能力时，这些测试才能体现价值。

模拟步骤

无论您是设计自己的 SIRS，还是有值得信赖的合作伙伴来完成准备工作，模拟通常都遵循以下步骤：

1. 找出重要问题 – 定义应引起响应的触发条件。
2. 识别熟练的安全工程师 – 模拟需要构建者和测试者。

3. 构建逼真的模型系统 – 模拟必须逼真且适当。如果不逼真，参与者可能不重视这项练习。如果模拟太少，那么练习可能被认为微不足道。从简单的练习开始，然后努力完成完整的事件。
4. 构建和测试场景元素 – 可能需要构建相关的模拟材料，例如日志记录构件、电子邮件通知和警报以及潜在的运行手册。
5. 邀请其他安全人员和跨组织参与者 – 邀请所有需要培训和参与的人员。如果您的总法律顾问、高管和公共关系部门参与了模拟，您也应该邀请他们。
6. 运行模拟 – 选择您的员工是否应该期待 SIRS 事件，或者模拟是否应保持未通知状态。
7. 庆祝、衡量、改进和重复 – 模拟存在压力因素，因此重要的是要对参与者所作的努力进行鼓励和庆祝。鼓励之后，我们就有机会衡量、改进和迭代下一次模拟。AWS 建议您养成完成这些活动的习惯。

> **Important**
>
> 如果您正在计划安全事件响应模拟（SIRS），请参阅渗透测试并查看其他模拟事件部分，了解有关如何进行的最新信息。

模拟示例

安全模拟必须逼真，这样才能提供预期的价值。当您或您的合作伙伴努力创建自己的模拟时，请始终将过去的真实事件视为潜在模拟练习的有价值来源。以下是 AWS 客户发现可用于初始模拟的几个示例：

- 未经授权更改网络配置或资源。
- 由于开发人员配置错误而导致错误地公开凭证。
- 由于开发人员配置错误而导致错误地公开敏感内容。
- 隔离正在与可疑恶意 IP 地址通信的 Web 服务器。

除了有价值的体验式学习之外，执行 SIRS 活动还会产生诸如经验教训之类的输出，您可以将其用作计划的下一个过程（迭代）的输入。

迭代

上一节定义了 SIRS 活动的一些益处。其中一项优势是通过渐进式改进获得敏捷性。模拟应产生有价值的结果，您可以利用这些结果来改善安全响应。它们为组织提供了反馈循环，说明哪些结果有效，哪些结果无效。有了这些信息，您就可以逐步创建新程序或更新现有程序，以改善您的响应。

主题

运行手册

当检测到安全异常时，响应计划最重要的就是要将事件控制下来，然后将情况扭转回到之前已知的良好状态。例如，如果是由于安全配置错误而发生异常，那么可能只需使用适当的配置重新部署资源以消除差异即可完成修复。为此，您需要提前计划并定义自己的安全响应程序，这些程序通常称为运行手册。

运行手册以文档形式记录组织执行一项任务或一系列任务的程序。此文档通常存储在内部数字系统或打印出来。您当前可能有事件响应运行手册，或者可能需要创建它们以符合安全保障框架。但是，当您手动遵循书面的运行手册时，您会增加犯错的可能性。相反，我们建议自动执行所有可重复的任务。自动化使您的响应团队从常见任务中解放出来，让他们可以执行更重要的任务，例如关联事件、通过模拟来实践、设计新的响应程序、进行研究、开发新技能以及测试或构建新工具。但是，在将任务分解为可编程逻辑并逐步实现适当的自动化之前，您必须从编写运行手册开始。

创建运行手册

要为云创建运行手册，我们建议您首先关注当前生成的警报。如果生成警报，请务必对其进行调查。首先，为您执行的手动流程定义说明。随后，测试这些流程并在运行手册模式中进行迭代，以改进您的响应的核心逻辑。确定异常以及这些场景的备用解决方案。例如，在开发环境中，您可能希望终止错误配置的 Amazon EC2 实例。但如果相同的事件发生在生产环境中，您不应终止实例，而应停止实例并向利益攸关方核实关键数据不会丢失，以及是否可以接受终止。

确定最佳解决方案后，您可以将此逻辑解构到基于代码的解决方案中，很多响应者可以将此逻辑用作工具来自动进行响应，因此消除了响应者的分歧或猜测。这加快了响应的生命周期。下一个目标是允许通过警报或事件本身调用此代码，而不是由人类响应者执行代码，从而实现完全自动化。

入门

如果您不确定从哪里开始，可以考虑从 AWS Trusted Advisor、AWS Security Hub 的基础安全最佳实践和 AWS Config 规则（包括 AWS Config 规则 Github 存储库）生成的警报开始。然后，重点关注由服务生成的事件，这些事件将描述您所关心的系统。

Amazon GuardDuty 和 Access Analyzer 描述了应用程序将在 AWS 中使用的许多域，这就是为什么通常建议使用这些域；但是，Amazon Inspector 和 Amazon Macie 对那些存在数据和端点问题的域有特定的用途。有关 Amazon GuardDuty 调查结果的信息，请参阅 Amazon GuardDuty 用户指南。Amazon Access Analyzer 用户指南中提供了 Access Analyzer 调查结果。Amazon Macie 用户指南中提供了 Macie 调查结果。Amazon Inspector 用户指南中提供了 Amazon Inspector 调查结果。借助 Security Hub，您可以将这些调查结果统一到一个地方，并以低延迟的方式对它们作出反应，所以我们建议将其作为修复的中心位置。

当调查结果或警报发生任何变化（包括新生成的警报和对现有警报的更新）时，上述所有服务都会通过 Amazon CloudWatch Events 发送通知。您可以设置 Amazon CloudWatch Events 规则来触发 AWS Lambda 函数以执行事件驱动型响应。而能够构建自定义洞察并从应用程序域中添加自己的发现，这也为使用 Security Hub 增加了重要理由。想要了解更多信息，请参阅事件驱动型响应部分。

自动化

自动化是一个力量倍增器，这意味着它可以扩大响应者的工作量，以适应组织的速度。从手动流程转向自动化流程，使您能够将更多时间用于提高 AWS 云环境的安全性。

主题

自动执行事件响应

要自动执行安全工程和运营功能，您可以使用 AWS 提供的一整套 API 和工具。您可以完全自动执行身份管理、网络安全、数据保护和监控功能。构建安全自动化时，您让自己的系统监控、审核和启动响应，而不必安排人员监控您的安全状况并对事件作出人为响应。

如果您的事件响应团队继续以同样的方式响应警报，警报可能会让他们应接不暇。随着时间的推移，团队对警报的敏感性可能会下降，并可能在处理正常情况时犯错或者错过异常警报。利用一些功能自动处理重复和正常的警报，并将敏感、特殊的事件交由人员来处理，这样有助于避免疲于应对警报。

您可以通过编程方式自动执行此流程中的步骤，从而改进手动流程。为事件定义修复模式之后，您可以将此模式分解为可执行的逻辑，并编写代码以执行此逻辑。随后，响应者即可执行此代码以修复问题。随着时间的推移，您可以自动化越来越多的步骤，并最终自动处理各类常见事件。

但是，您的目标应该是进一步缩短检测性机制和响应性机制之间的时间差。从历史上看，此时间差可能会持续几个小时、几天或甚至几个月。SANS 在 2016 年进行的一项事件响应调查发现，21% 的受访者表示他们进行检测所花的时间为两到七天，只有 29% 的受访者能够在同一时间范围内修复事件。在云中，您可以通过构建事件驱动型响应能力，将响应时间差距缩短到几秒钟。

主题

用于自动响应的选项

务必确保在企业实施和组织结构之间取得平衡。图 4 用雷达图说明了 AWS 实施中每个自动响应选项的技术属性差异。在图表中，技术属性从图表中心移得越远，相应自动化响应的该技术属性就越强。例如，AWS Lambda 提供更快的速度，且所需的技术技能集更少。AWS Fargate 提供更大的灵活性，且需要更少的维护和技术技能组合。表 1 概述了这些自动化选项，并提供了每个选项的技术属性摘要。

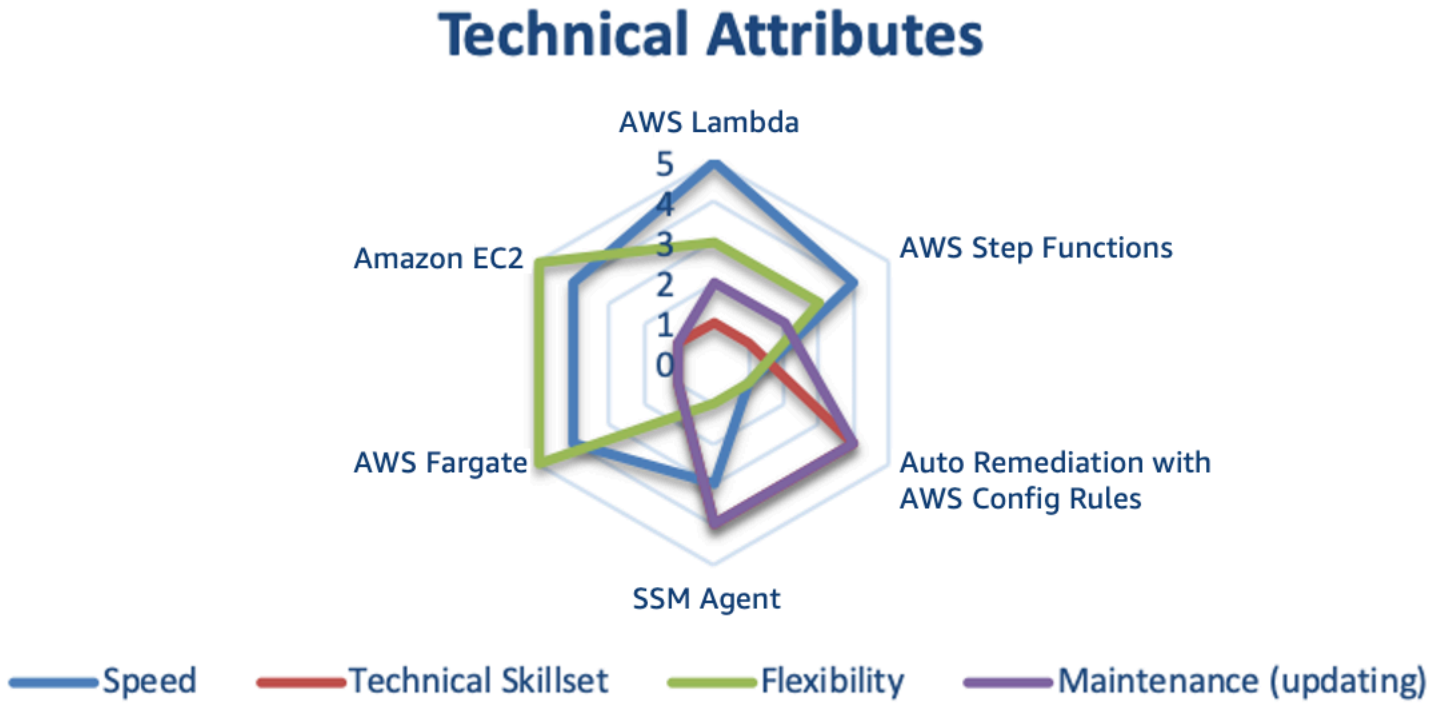

图 4：不同自动响应方法的技术属性差异

表 1：自动响应的选项

AWS 服务或功能	说明	属性摘要*
AWS Lambda	系统仅使用 AWS Lambda，使用您所在组织的企业语言。	速度 灵活性 维护 技能组合
AWS Step Functions	系统使用 AWS Step Functions、Lambda 和 SSM Agent。	速度 灵活性 维护 技能组合
使用 AWS Config 规则 自动修复	评估环境并将其推回到已批准规范的一组 AWS Config 规则和自动修复。	维护和技能组合 速度和灵活性
SSM Agent	一组自动化规则和文档，用于审查环境和内部系统的多个部分并进行更正。	维护和技能组合 速度 灵活性
AWS Fargate	AWS Fargate 系统使用开源阶跃函数代码以及来自 Amazon CloudWatch 和其他系统的事件，从而推动检测和修复。	灵活性 速度 维护和技能组合
Amazon EC2	在完整实例上运行的系统，与 AWS Fargate 选项类似。	灵活性 速度 维护

AWS 服务或功能	说明	属性摘要*
		技能组合

* 每项服务或功能的属性按降序列出。例如，AWS Lambda 提供更快的速度，且所需的技术技能集更少。AWS Fargate 提供更大的灵活性，且需要更少的维护和技术技能组合。

在您的 AWS 环境中考虑这些自动化选项时，还需要考虑集中化和扫描周期（每秒事件数 [EPS]）。

集中化是指推动组织的所有检测和修复工作的中央账户。这种方法似乎是开箱即用的最佳选择，也是当前的最佳实践。但在某些情况下，不能采用这种方法，并且要求您根据处理下属账户的方式了解何时采用此方法。我们建议您利用 AWS Organizations 中的多账户框架或 AWS Control Tower 中的安全工具账户方法，从而开始使用。

表 2：集中化的利弊

	集中化	去中心化
优点	简单的配置管理 无法取消或修改响应	简单的架构 更快的初始设置
缺点	架构的复杂性增加 载入/停用账户和资源	要管理更多资源 难以维护软件基准

对这些实施的成本进行比较也可能促使您的企业作出决定以确定最佳选项。每秒事件数（EPS）是您用来最好地估算成本的指标。最后，使用集中化或去中心化方法可能会更容易和更便宜，但是我们无法审查您将如何具体评估账户中的成本。在将这些事件发送到要响应的中央账户时，请务必考虑 EPS。EPS 越多，将这些事件发送到集中化账户的成本就越高。

扫描方法中的成本比较

通过检测异常的扫描方法和两次验证之间的时间范围进一步确定成本。对于扫描方法，您可以选择基于事件或定期扫描审查。表 3 显示了这两种方法的优缺点。

表 3：不同扫描方法的优缺点

	基于事件	定期扫描
优点	从事件到响应的时间更短 查询额外 API 调用的需求有限	给定时间点的全貌
缺点	有关资源的状态上下文有限 触发的事件可能是针对不容易获得的资源	针对大型账户的服务限制 可能由于大量 API 调用而受到限制

在许多情况下，在完全成熟的组织中，结合使用这两种扫描方法很可能是最佳选择。AWS Security Hub 和 AWS 基础安全最佳实践标准提供了两种扫描方法的组合。

图 5 提供了一个雷达图，说明了每种自动化方法的每秒事件数（EPS）成本比较。例如，Amazon EC2 和 AWS Fargate 运行 0-10 EPS 的成本最高，而 AWS Lambda 和 AWS Step Functions 运行 76 个以上 EPS 的成本最高。

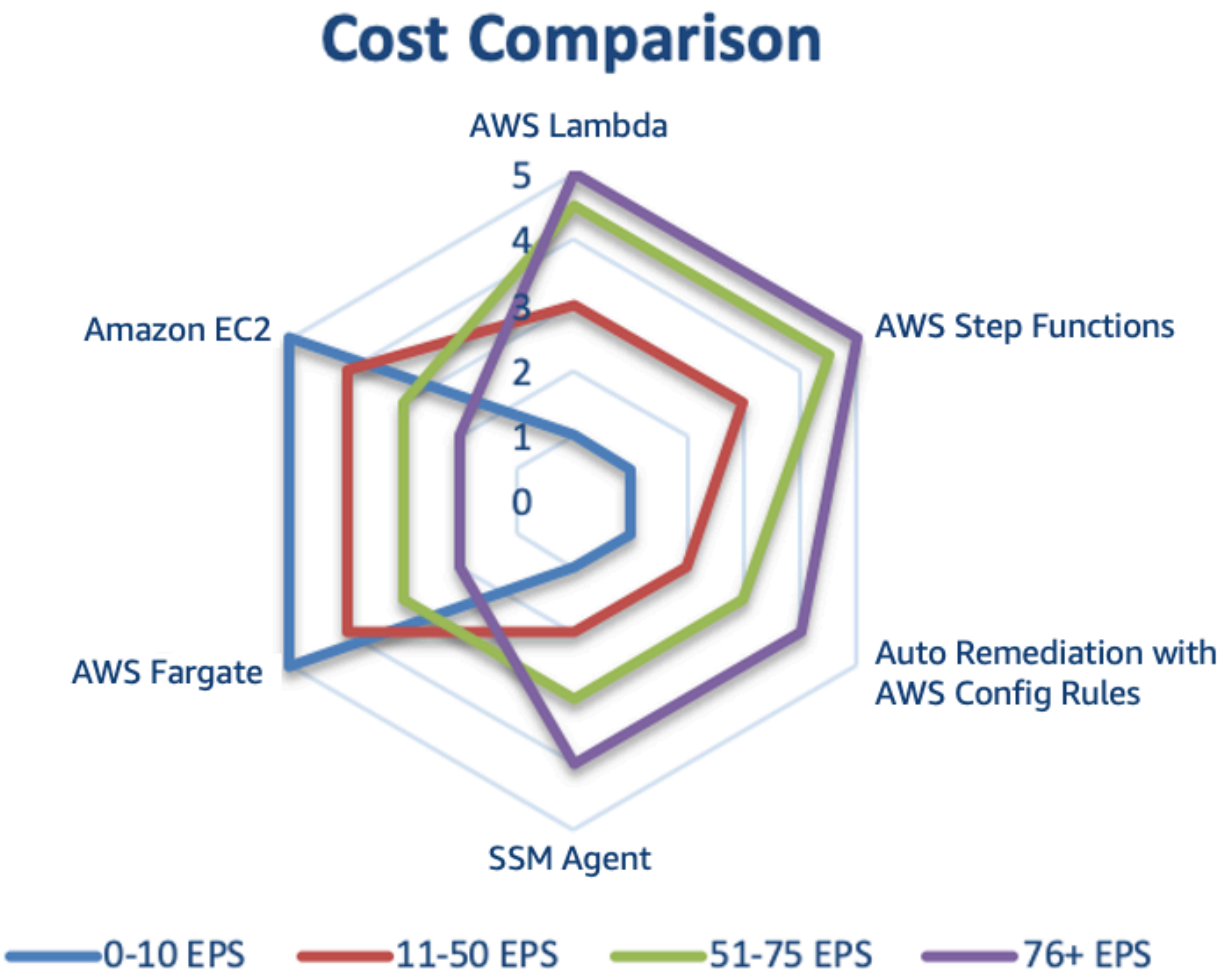

图 5：自动化选项扫描方法的成本比较（每秒事件数 [EPS]）

事件驱动型响应

使用事件驱动型响应系统，检测性机制会触发一个响应机制，以自动修复事件。您可以使用由事件驱动的响应能力，以缩短检测机制与响应机制之间的价值实现时间。要创建这个由事件驱动的架构，您可以使用 AWS Lambda，这是一项无服务器计算服务，可运行您的代码以响应事件并为您自动管理底层计算资源。

例如，假设您有一个 AWS 账户并为其启用了 AWS CloudTrail 服务。如果 AWS CloudTrail 曾经禁用过（通过 `cloudtrail:StopLogging` API），则响应程序是再次启用该服务，并调查禁用 AWS CloudTrail 日志记录的用户。您可以通过编程方式（通过 `cloudtrail:StartLogging` API）再次启用日志记录，而不是在 AWS Management Console 中手动执行这些步骤。如果您使用代码实现此功能，则您的响应目标是尽快执行此任务，并通知响应者已执行响应。

您可以将逻辑分解为简单的代码，以便在 AWS Lambda 函数中运行来执行这些任务。然后，您可以使用 Amazon CloudWatch Events 监控特定 `cloudtrail:StopLogging` 事件，并在事件发生时调用该函数。当 Amazon CloudWatch Events 调用此 AWS Lambda 响应程序函数时，您可以向其传递特定事件的详细信息，包括禁用 AWS CloudTrail 的主体的信息、禁用时间、受影响的特定资源以及其他相关信息。您可以使用此信息来丰富日志中的发现结果，然后生成仅包含响应分析师所需的特定值的通知或警报。

理想情况下，事件驱动型响应的目标是让 Lambda 响应程序函数执行响应任务，然后使用任何相关的上下文信息通知响应者已成功处理异常。然后，由人工响应者决定如何确定其发生原因以及如何防止将来再次发生。此反馈循环可进一步提高云环境的安全性。要实现这一目标，您必须营造一种文化，使您的安全团队能够与开发和运营团队更紧密地合作。

事件响应示例

主题

服务领域事件

服务领域事件通常仅通过 AWS API 进行处理。

身份

AWS 为我们的云服务提供 API，数以百万计的客户使用这些服务来构建新的应用程序并推动实现业务成果。可以通过多种方法调用这些 API，例如通过软件开发工具包（SDK）、AWS CLI 和 AWS Management Console。要通过这些方法与 AWS 交互，IAM 服务可帮助您安全地控制对 AWS 资源的访问。您可以使用 IAM 来控制谁通过了身份验证（准许登录）并获得授权（拥有权限），可以在账户级别使用资源。有关可通过 IAM 使用的 AWS 服务的列表，请参阅使用 IAM 的 AWS 服务。

当您首次创建 AWS 账户时，最初使用的是一个对账户中所有 AWS 服务和资源有完全访问权限的单点登录（SSO）身份。此身份称为 AWS 账户根用户，可以通过使用您用于创建账户的电子邮件地址和密码进行登录来访问该身份。强烈建议您不要使用根用户执行日常任务，尤其是不要使用根用户执行管理任务。我们建议您遵循最佳实践，仅使用根用户创建第一个 IAM 用户，安全地存储根用户凭证，仅使用它们执行一些账户和服务管理任务。有关更多信息，请参阅创建单独的 IAM 用户。

尽管这些 API 为数百万客户提供了价值，但如果错误的人获得您的 IAM 账户或根凭证，其中一些 API 可能会被滥用。例如，您可以使用 API 在您的账户中启用日志记录，例如 AWS CloudTrail。但是，如果攻击者获得了您的凭证，他们也可以使用 API 禁用这些日志。您可以通过配置遵循最低权限模式的适当 IAM 权限以及适当保护您的 IAM 凭证，从而防止此类滥用。有关更多信息，请参阅 AWS Identity and Access Management 用户指南中的 IAM 最佳实践。如果确实发生了此类事件，则可以通过多种检测控制来识别您的 AWS CloudTrail 日志记录是否已被禁用，包括 AWS CloudTrail、AWS Config、AWS Trusted Advisor、Amazon GuardDuty 和 AWS CloudWatch Events。

资源

其他会被滥用或配置错误的功能因组织而异，具体取决于每个客户在云中的运营方式。例如，一些组织打算让某些数据或应用程序可供公开访问，而另一些组织则将其应用程序和数据保留在内部并保密。并

非所有安全事件本质上都是恶意的；有些事件可能是因无意或错误配置而引起的。考虑哪些 API 或功能对组织影响很大，以及您是否经常使用这些 API 或功能。

您可以利用工具和服务识别许多安全配置错误。例如，AWS Trusted Advisor 提供了许多针对最佳实践的检查。APN 合作伙伴也提供了数百种业界领先的产品，这些产品与您的本地环境中的现有控制措施等效、相同或相集成。其中许多产品和解决方案已通过 AWS 合作伙伴能力计划的资格预审。我们建议您访问 APN 安全能力计划的配置和漏洞分析部分，浏览这些解决方案并确定它们是否可以满足您的要求。

基础设施领域事件

基础设施领域通常包括应用程序的数据或与网络相关的活动，例如流向 VPC 内的 Amazon EC2 实例的流量以及在 Amazon EC2 实例操作系统中运行的进程。

例如，假设您的监控解决方案报告，Amazon EC2 实例上存在潜在的安全异常。以下操作是解决此问题的常见步骤：

1. 在对环境进行任何更改之前，从 Amazon EC2 实例捕获元数据。
2. 通过为实例启用终止保护，保护 Amazon EC2 实例免遭意外终止。
3. 通过切换 VPC 安全组来隔离 Amazon EC2 实例。但请了解 VPC 连接跟踪和其他遏制技术。
4. 将 Amazon EC2 实例与任何 AWS Auto Scaling 组分离。
5. 从任何相关的 Elastic Load Balancing 服务中取消注册 Amazon EC2 实例。
6. 对连接至 EC2 实例的 Amazon EBS 数据卷拍摄快照，用于保留和后续调查。
7. 将 Amazon EC2 实例标记为已隔离以进行调查，并添加任何相关元数据，例如与调查相关的故障单。

您可以使用 AWS API、AWS 软件开发工具包、AWS CLI 和 AWS Management Console 执行上述所有步骤。要使用这些方法与 AWS 交互，IAM 服务可帮助您安全地控制对 AWS 资源的访问。您可以使用 IAM 来控制谁通过了身份验证并获得授权，可以在账户级别使用资源。IAM 服务为您提供身份验证和授权，以便您执行这些操作并与服务域进行交互。

Amazon EBS 卷的快照是 EBS 数据卷的时间点、数据块级副本，它以异步方式生成，可能需要一些时间才能完成，但这是未来数据的增量。您可以根据这些副本创建新的 EBS 卷，并将它们装载到取证 EC2 实例，以便取证调查人员离线进行深入分析。下图显示了结果的简化版本，并未描述所有网络组件（例如子网、路由表和网络访问控制列表）。

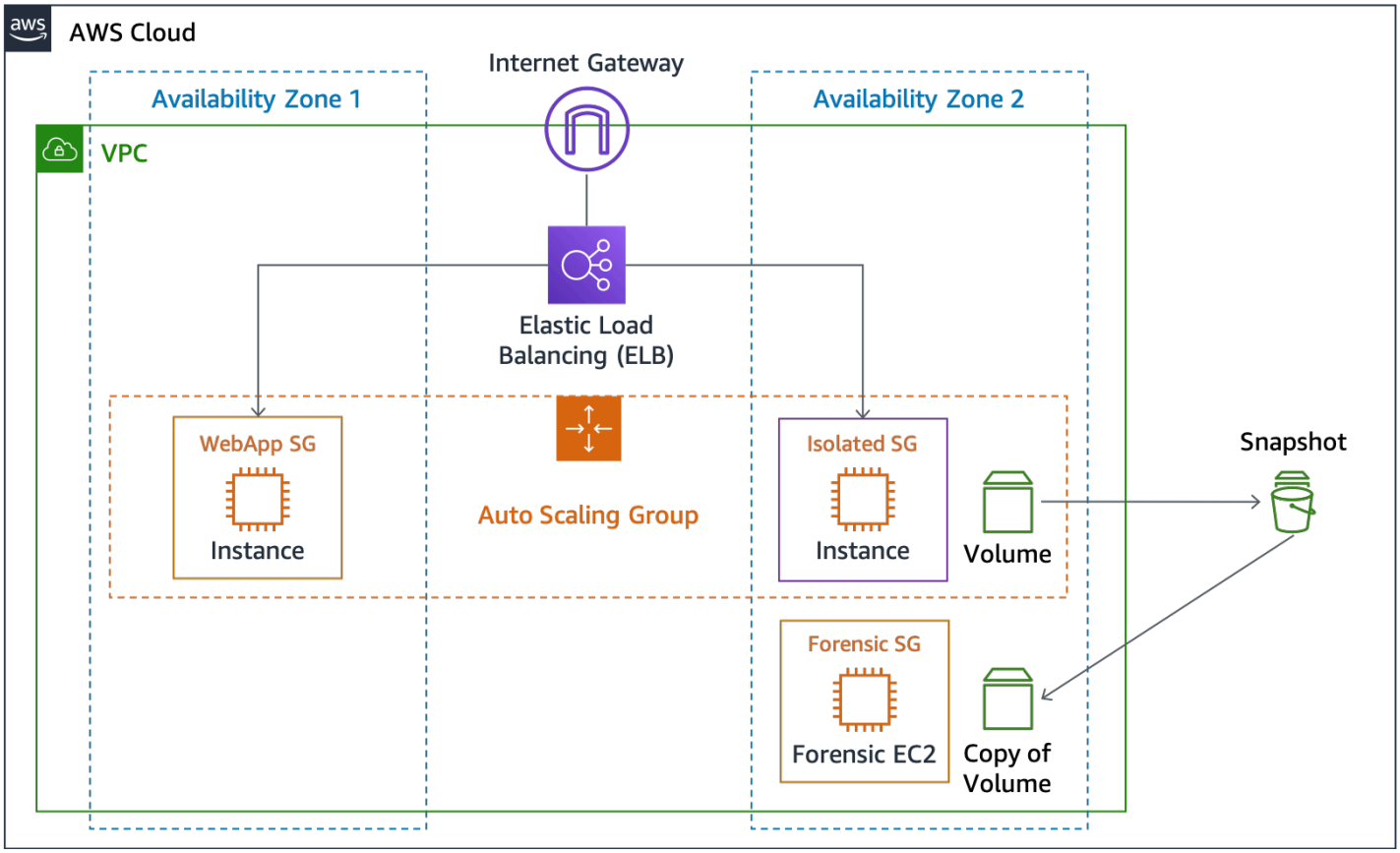

图 6：EC2 实例隔离和快照

主题

- 调查决定
- 捕获易失性数据
- 使用 AWS Systems Manager
- 自动执行捕获

调查决定

此时，您可以在离线调查（立即关闭实例）或在线调查（使实例保持运行）之间进行选择。离线调查的一个优势是，实例关闭后，它将不再影响现有环境。此外，您可以根据 EBS 快照创建受影响实例的副本，然后在隔离的 AWS 账户中检查该实例，该账户具有专为调查而设计的隔离环境。但是，如果在线调查使您有可能从主机操作系统捕获短暂易逝的证据（例如内存或网络流量），则可以选择不立即关闭实例。

捕获易失性数据

尽管您可能不会选择执行在线调查，但重要的是要了解从实例捕获易失性数据的必要机制。在线调查需要与 Amazon EC2 实例上运行的操作系统进行交互。在这种情况下，为了在 Amazon EC2 实例上执行任务，您需要的不仅仅是 AWS IAM 服务。尽管您可以使用标准方法（例如 Linux 安全外壳（SSH）或 Microsoft Windows 远程桌面（RDP））直接向计算机进行身份验证，但手动与操作系统交互并不是最佳实践。我们建议您以编程方式使用自动化工具在主机上执行任务。

使用 AWS Systems Manager

AWS Systems Manager Run Command 帮助您在远程安全地执行按需更改，在目标实例上运行 Linux Shell 脚本和 Windows PowerShell 命令。尽管您可以通过 AWS IAM 服务中的权限调用 Run Command，但您必须先将 Amazon EC2 实例激活为托管实例，在您的计算机上安装 SSM Agent（如果默认情况下未安装），然后配置 AWS IAM 权限。如果您想要使用 Run Command 执行自动化或响应活动，请确保在执行调查之前完成先决条件活动。

AWS Systems Manager（包括 Run Command）与 AWS CloudTrail 集成，后者是一种服务，可捕获由 Systems Manager 自身或代表其发出的 API 调用，并将日志文件传送到您指定的 Amazon S3 存储桶。通过使用 AWS CloudTrail 收集的信息，您可以确定发出了什么请求、发出请求的源 IP 地址、何人发出请求以及发出请求的时间等。CloudTrail 创建所有 Systems Manager API 操作的日志，包括使用 Run Command 执行命令或创建 Systems Manager 文档的 API 请求。

您可以使用 AWS Systems Manager Run Command 服务调用执行 Linux Shell 脚本和 Windows PowerShell 命令的 SSM Agent。这些脚本可以加载和执行特定的工具，以便从主机捕获其他数据，例如 Linux Memory Extractor（LiME）内核模块。然后，您可以将内存捕获传输到 VPC 网络中的取证 Amazon EC2 实例，或传输到 Amazon S3 存储桶以进行持久存储。

自动执行捕获

调用 SSM Agent 的一种方法是，当使用特定标签对实例进行标记时，通过 Amazon CloudWatch Events 将 Run Command 作为目标。例如，如果您将 `Response=Isolate+MemoryCapture` 标签应用于受影响的实例，则可以将 Amazon CloudWatch Events 配置为触发两个操作：

- 执行隔离活动的 Lambda 函数
- 执行 shell 命令以通过 SSM Agent 导出 Linux 内存的 Run Command

这种标签驱动的响应是事件驱动型响应的另一种方法。

总结

在继续云之旅的过程中，请务必考虑上述 AWS 环境的基本安全事件响应概念。您可以结合使用可用的控制、云功能和修复选项，以帮助您增强云环境的安全性。您还可以从小处着手，然后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已做好充分的准备。

其他资源

如需更多信息，请参阅：

- AWS Well-Architected
- AWS Cloud Adoption Framework 页面
- AWS 集中式日志记录解决方案
- 使用 AWS Glue 和 Amazon QuickSight 可视化 AWS CloudTrail 日志
- 如何在 Amazon EC2 实例上监控基于主机的入侵检测系统提醒
- 使用 Amazon CloudWatch 存储和监控操作系统与应用程序日志文件
- Amazon S3 中的 Identity and Access Management
- 使用版本控制（Amazon S3）
- 使用 MFA 删除
- 使用具有 AWS KMS 托管密钥的服务器端加密（SSE-KMS）保护数据
- 使用 AWS 控制台和 CLI 的事件响应
- 为加利福尼亚州消费者隐私法案做准备

媒体

- AWS re:Invent 2014（SEC402）：云中的入侵检测
- AWS re:Invent 2014（SEC404）：云中的事件响应
- AWS re:Invent 2015（SEC308）：争论云中的安全事件
- AWS re:Invent 2015（SEC316）：通过安全事件响应模拟强化您的架构
- AWS re:Invent 2016（SEC313）：自动执行从想法到代码，再到执行的安全事件响应
- AWS re:Invent 2017（SID302）：利用自动化和 Alexa 扩充您的安全团队
- AWS re:Invent 2016（SAC316）：安全自动化：减少保护应用程序安全所花的时间
- AWS re:Invent 2016（SAC304）：预测性安全性：使用大数据强化防御
- AWS re:Invent 2017（SID325）：Amazon Macie：通过机器学习为安全性和合规性工作负载带来的数据可见性
- 2018 年 AWS 伦敦峰会：在 AWS 中实现事件响应和取证自动化

第三方工具

以下第三方工具链接为外部链接，未得到 AWS 的认可。对于这些工具或页面，AWS 不提供任何形式的保证或声明。

- AWS_IR – Python 可安装的命令行实用程序，用于缓解主机和密钥损害。
- MargaritaShotgun – 远程内存获取工具。
- ThreatPrep – Python 模块，用于评估有关事件处理就绪情况的 AWS 账户最佳实践。
- ThreatResponse Web – 基于 Web 的分析平台，可与 AWS_IR 命令行工具配合使用。
- GRR 快速响应 – 用于事件响应的远程实时取证。
- Linux 写入阻止程序 – 用于启用 Linux 软件写入阻止的内核补丁和用户空间工具。

行业参考文献

- NIST SP 800-61R2：计算机安全事件处理指南

文档修订

要获得有关此白皮书更新的通知，请订阅 RSS 源。

更新-历史记录-更改	更新-历史记录-描述	更新-历史记录-日期
次要更新	通篇进行了错误修复和多处细微更改。	2021 年 6 月 2 日
次要更新	更正了失效的链接。	2021 年 3 月 5 日
更新了白皮书	更正了失效的链接和大量文本更改，以提高可读性。	2020 年 11 月 23 日
次要更新	修复了“使用 AWS 控制台和 CLI 的事件响应”的链接	2020 年 6 月 30 日
更新了白皮书	更新了新的安全服务、威胁情报、容器责任共担、自动化和 CCPA。添加了附录以及示例决策树和运行手册。	2020 年 6 月 11 日
初次发布	白皮书首次发布	2019 年 6 月 1 日

附录 A：云功能定义

AWS 提供了超过 150 项云服务和数千项功能。这其中有很多提供了本机检测、预防和响应功能，而其他一些服务和功能可用于构建自定义安全解决方案。本节介绍了与云中的事件响应最相关的一部分服务。

主题

日志记录和事件

AWS CloudTrail – AWS CloudTrail 是一项服务，支持对 AWS 账户进行监管、合规性检查、操作审计和风险审计。借助 CloudTrail，您可以跨 AWS 基础设施记录、持续监控和保留与操作相关的账户活动。CloudTrail 可提供 AWS 账户活动的事件历史记录，包括通过 AWS Management Console、AWS 软件开发工具包、命令行工具和其他 AWS 服务执行的操作。事件历史记录简化了安全分析、资源更改跟踪和故障排除。

在安全和事故调查中，经验证的日志文件非常重要。要确定在 CloudTrail 交付后日志文件是否被修改、删除或未进行更改，您可以使用 CloudTrail 日志文件完整性验证。该功能是使用业界标准算法构建的：哈希采用 SHA-256，数字签名采用带 RSA 的 SHA-256。这样，要修改、删除或伪造 CloudTrail 日志文件而不被检测到在计算上是不可行的。

默认情况下，CloudTrail 传送到存储桶的日志文件通过 Amazon 服务器端加密进行加密。您可以选择对 CloudTrail 日志文件使用 AWS Key Management Service（AWS KMS）托管密钥（SSE-KMS）。

Amazon CloudWatch Events – Amazon CloudWatch Events 提供近乎实时的系统事件流，描述 AWS 资源中的变化或 AWS CloudTrail 何时发布 API 调用。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。CloudWatch Events 会在发生操作更改时感知到这些更改。CloudWatch Events 可以对这些操作更改作出响应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（例如 Amazon GuardDuty）会以 CloudWatch Events 形式生成输出。

AWS Config – AWS Config 服务可以帮助您评估、审计和评价您的 AWS 资源配置。Config 持续监控和记录您的 AWS 资源配置，并支持您自动依据配置需求评估记录的配置。借助 Config，您可以手动或自动查看 AWS 资源之间的配置和关系更改。您可以查看详细的资源配置历史记录，并判断您的配置在整体上是否符合内部指南中所指定的配置要求。如此一来，您将能够简化合规性审计、安全性分析、变更管理和操作故障排除。

Amazon S3 访问日志 – 如果您将敏感信息存储在 Amazon S3 存储桶中，则可以启用 S3 访问日志来记录对该数据的每次上传、下载和修改。此日志与记录存储桶本身更改（例如更改访问策略和生命周期策略）的 CloudTrail 日志是分开的，也是 CloudTrail 日志的补充。

Amazon CloudWatch Logs – 您可以使用 Amazon CloudWatch Logs，借助 CloudWatch Logs 代理从 Amazon Elastic Compute Cloud（Amazon EC2）实例监控、存储和访问您的日志文件（例如操作系统、应用程序和自定义日志文件）。此外，Amazon CloudWatch Logs 可以捕获来自 AWS CloudTrail、Amazon Route 53 DNS 查询、VPC 流日志、Lambda 函数和其他来源的日志。然后，您可以从 CloudWatch Logs 检索关联的日志数据。

Amazon VPC 流日志 – 使用 VPC 流日志，您可以捕获有关传入和传出 VPC 中网络接口的 IP 流量的信息。创建流日志后，您可以在 Amazon CloudWatch Logs 中查看和检索其数据。VPC 流日志可帮助您处理多种任务。例如，您可以使用流日志排查特定流量未到达实例的原因，从而帮助您诊断限制过于严格的安全组规则。您还可以使用流日志作为安全工具来监控到达您的实例的流量。

AWS WAF 日志 – AWS WAF 现在支持完整记录该服务检测到的所有 Web 请求。您可以将这些日志存储在 Amazon S3 中，以满足合规性与审计需求，以及将它们用于调试和额外取证。这些日志可以帮助您了解为什么会触发某些规则和阻止某些 Web 请求。您还可以将这些日志与 SIEM 和日志分析工具集成。

其他 AWS 日志 – 随着创新的推进，我们几乎每天都在继续为客户部署新的特性和功能，这意味着有数十种 AWS 服务提供日志记录和监控功能。有关各项 AWS 服务提供的特性的信息，请参阅该服务的 AWS 文档。

可见性和警报

AWS Security Hub – AWS Security Hub 使您可以全面了解各 AWS 账户的高优先级安全警报和合规性状态。借助 Security Hub，您可以设置单个位置，对来自多个 AWS 服务（如 Amazon GuardDuty、Amazon Inspector 和 Amazon Macie），以及来自 AWS 合作伙伴解决方案的安全警报或检测结果进行聚合、组织和设置优先级。您的检测结果可在具有可操作图形和表格的集成控制面板上进行直观汇总。您还可以使用自动合规性检查（基于您的组织遵循的 AWS 最佳实践和行业标准），持续监控您的环境。

Amazon GuardDuty – Amazon GuardDuty 是一种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，从而帮助您保护您的 AWS 账户和工作负载。该服务会监控异常 API 调用或可能未授权部署之类的表明潜在账户损失的活动。GuardDuty 还会检测可能受损的实例或攻击者的侦测。

GuardDuty 通过集成的威胁情报源识别可疑的攻击者，并使用机器学习来检测账户和工作负载活动中的异常情况。如果检测到潜在威胁，该服务会向 GuardDuty 控制台和 AWS CloudWatch Events 提供详细的安全警报。这使得警报具有可操作性，并且易于集成到现有的事件管理和工作流系统中。

Amazon Macie – Amazon Macie 是一种支持 AI 技术的安全服务，可以帮助您通过自动发现、分类和保护存储在 AWS 中的敏感数据来防止数据丢失。Amazon Macie 使用机器学习来识别敏感数据（例如，个人身份信息（PII）或知识产权）、赋予商业价值以及提供此数据的存储位置信息及其在组织中的使用方式信息。Amazon Macie 可持续监控数据访问活动异常，并在检测到未经授权的访问或意外数据泄漏风险时发出警报。

AWS Config 规则 – AWS Config 规则代表某个资源的首选配置，其评估依据是 AWS Config 记录的相关资源的配置更改。您可以在控制面板上查看针对资源配置评估规则的结果。使用 Config 规则，您可以从配置角度评估整体合规性和风险状态、查看一段时间内的合规性趋势，以及查明哪些配置更改导致资源不符合规则。

AWS Trusted Advisor – AWS Trusted Advisor 是一种在线资源，可通过优化您的 AWS 环境来帮助您降低成本、提高性能和改进安全性。Trusted Advisor 可提供实时指导，帮助您按照以下 AWS 最佳实践预置资源。全套 Trusted Advisor 检查（包括 CloudWatch Events 集成）面向商业和企业支持计划客户提供。

Amazon CloudWatch – Amazon CloudWatch 是一项针对 AWS 云资源和在 AWS 上运行的应用程序的监控服务。您可以使用 Amazon CloudWatch 来收集和跟踪各项指标、收集和监控日志文件、设置警报以及自动应对 AWS 资源的更改。Amazon CloudWatch 可以监控各种 AWS 资源，例如 Amazon EC2 实例、Amazon DynamoDB 表、Amazon RDS 数据库实例、应用程序和服务生成的自定义指标以及应用程序生成的所有日志文件。您可通过使用 Amazon CloudWatch 全面地了解资源使用率、应用程序性能和运行状况。使用这些分析结果，您可以相应地作出反应，保证应用程序顺畅运行。

AWS Inspector – Amazon Inspector 是一项自动安全评估服务，有助于提高在 AWS 上部署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相较于最佳实践的偏差。执行评估后，Amazon Inspector 会生成按严重程度确定优先级的安全检验详细列表。这些评估结果可直接接受审核，也可作为通过 Amazon Inspector 控制台或 API 提供的详细评估报告的一部分接受审核。

Amazon Detective – Amazon Detective 是一项安全服务，它会自动从您的 AWS 资源中收集日志数据，并使用机器学习、统计分析和图论来构建一组关联的数据，使您能够轻松地进行更快、更有效的安全调查。Amazon Detective 可以分析来自多个数据源（例如 Virtual Private Cloud（VPC）流日

志、AWS CloudTrail 和 Amazon GuardDuty）的数万亿个事件，并自动创建资源、用户及其不同时间交互情况的统一交互式视图。使用这种统一视图，您可以集中直观呈现所有详细信息和上下文，确定检测结果的基本原因，深入研究相关历史活动，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 在高可用性计算基础设施上运行代码，为您执行计算资源的所有管理工作。这包括服务器和操作系统维护、容量调配和弹性伸缩、代码和安全补丁部署以及代码监控和日志记录。您只需要提供代码。

AWS Step Functions – 使用 AWS Step Functions，通过可视化工作流程轻松协调分布式应用程序和微服务的组件。Step Functions 提供一个图形控制台，使您可以按照一系列步骤排列应用程序的组件，并以可视化方式呈现这些组件。这可以简化多步骤应用程序的构建和运行。Step Functions 可以自动触发和跟踪各个步骤，并在出现错误时重试，以便您的应用程序按照预期顺序执行。

Step Functions 可记录每个步骤的状态，因此在出现错误时，您能够迅速诊断并调试问题。无需编写代码即可更改和添加步骤，因此您可以轻松改进应用程序并加快创新。AWS Step Functions 是 AWS 无服务器平台的一部分，通过它，可以轻松为无服务器应用程序编排 AWS Lambda 功能。在使用 Amazon EC2 和 Amazon ECS 等计算资源编排微服务时，您也可以使用 Step Functions。

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，并使您可以在 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，并对资源组采取操作。Systems Manager 可以使您的实例处于其定义的状态，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 S3 – Amazon S3 是专为从任意位置存储和检索任意数量的数据而构建的对象存储。它旨在提供 99.999999999% 的持久性，并存储每个行业的市场领导者使用的数百万个应用程序的数据。Amazon S3 提供全面的安全性，旨在满足您的监管要求。它为客户提供了用于管理数据的灵活方法，以实现成本优化、访问控制和合规性。Amazon S3 提供就地查询功能，使您可以在 Amazon S3 中直接对静态数据进行强大的分析。Amazon S3 是最受支持的可用云存储服务，可与最大的第三方解决方案社群、系统集成商合作伙伴和其他 AWS 服务集成。

Amazon S3 Glacier – Amazon S3 Glacier 是一款安全、持久且成本极低的云存储服务，适用于数据归档和长期备份。它旨在提供 99.999999999% 的持久性，提供全面的安全性，并满足您的监管要求。Amazon S3 Glacier 提供就地查询功能，使您可以针对静态归档数据直接运行强大的分析。为了保持成本低廉，同时满足各种数据检索需求，Amazon S3 Glacier 提供三种访问归档的选项，其各自的检索时间从数分钟到数小时不等。

自定义

上述服务和功能列表并不详尽。AWS 仍在不断添加新的功能。有关更多信息，我们建议您查看 AWS 的新增功能和 AWS 云安全页面。除了 AWS 作为原生云服务提供的安全服务之外，您可能有兴趣在 AWS 服务基础上构建自己的功能。

尽管我们建议在账户中启用一组基本安全服务（例如，AWS CloudTrail、Amazon GuardDuty 和 Amazon Macie），但您可能最终希望扩展这些功能，以便从日志资产中获取更多价值。有许多可用的合作伙伴工具，例如我们的 APN 安全能力计划中列出的那些工具。您可能还希望编写自己的查询来搜索日志。借助 AWS 提供的大量托管式服务，这项工作从未如此轻松。还有许多其他 AWS 服务可以帮助您进行调查，这些服务不在本白皮书的讨论范围之内，例如 Amazon Athena、Amazon OpenSearch Service、Amazon QuickSight、Amazon Machine Learning 和 Amazon EMR。

附录 B：示例代码

示例 AWS CloudTrail 事件

以下示例显示，一位名为 `Alice` 的 IAM 用户使用 AWS CLI，通过使用 `ec2-stop-instances` 来调用 Amazon EC2 `StopInstancesaction`。

```
{"Records": [{
    "eventVersion": "1.0",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:user/Alice",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID",
        "userName": "Alice"
    },
    "eventTime": "2014-03-06T21:01:59Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "StopInstances",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "205.251.233.176",
    "userAgent": "ec2-api-tools 1.6.12.2",
    "requestParameters": {
        "instancesSet": {"items": [{"instanceId": "i-ebeaf9e2"}]},
        "force": false
    },
    "responseElements": {"instancesSet": {"items": [{
        "instanceId": "i-ebeaf9e2",
        "currentState": {
            "code": 64,
            "name": "stopping"
        },
        "previousState": {
            "code": 16,
            "name": "running"
        }
    }]}}
}]}
```

示例 AWS CloudWatch Events

以下 Amazon CloudWatch Events 示例显示，发现名为 `jane-roe-test` 的 AWS IAM 用户在 `www.github.com` 上公开暴露，并可能会被未经授权的用户滥用。

```
{
  "check-name": "Exposed Access Keys",
  "check-item-detail": {
    "Case ID": "02648f3b-e18f-4019-8d68-ce25efe080ff",
    "Usage (USD per Day)": "0",
    "User Name (IAM or Root)": "jane-roe-test",
    "Deadline": "1440453299248",
    "Access Key ID": "AKIAIOSFODNN7EXAMPLE",
    "Time Updated": "1440021299248",
    "Fraud Type": "Exposed",
    "Location": "www.github.com"
  },
  "status": "ERROR",
  "resource_id": "",
  "uuid": "cce6d28f-e44b-4e61-aba1-5b4af96a0f59"
}
```

示例基础设施域 CLI 活动

以下 AWS CLI 命令显示了响应基础设施域内事件的示例。此示例使用 AWS API 执行本白皮书中描述的许多初始事件响应活动。

```
# Anomaly detected on IP X.X.X.X. Capture that instance's metadata
> aws ec2 describe-instances --filters "Name=ip-address,Values=X.X.X.X"
```

```
# Protect that instance from accidental termination
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --attribute
 disableApiTermination --value true
```

```
# Switch the EC2 instance's Security Group to a restricted Security Group
> aws ec2 modify-instance-attribute --instance-id i-abcd1234 --groups sg-a1b2c3d4
```

```
# Detach from the Auto Scaling Group
```

```
> aws autoscaling detach-instances --instance-ids i-abcd1234 --auto-scaling-group-name
 web-asg
```

```
# Deregister the instance from the Elastic Load Balancer
> aws elb deregister-instances-from-load-balancer --instances i-abcd1234 --load-
balancer-name web-load-balancer
```

```
# Create an EBS snapshot
> aws ec2 create-snapshot --volume vol-12xxxx78 --description "ResponderName-Date-
REFERENCE-ID"
```

```
# Create a new EC2 instance from the Forensic Workstation AMI
> aws ec2 run-instances --image-id ami-4n6x4n6x --count 1 --instance-type c4.8xlarge --
key-name forensicPublicKey --security-group-ids sg-1a2b3c4d --subnet-id subnet-6e7f819e
```

```
# Create a new EBS volume copy from the EBS snapshot
> aws ec2 create-volume --region us-east-1 --availability-zone us-east-1a --snapshot-id
 snap-abcd1234 --volume-type io1 --iops 10000
```

```
# Attach the volume to the forensic workstation
> aws ec2 attach-volume --volume-id vol-1234abcd --instance-id i-new4n6x --device /dev/
sdf
```

```
# Create a security group rule to allow the new Forensic Workstation to communicate to
 the contaminated instance.
> aws ec2 authorize-security-group-ingress --group-id sg-a1b2c3d4 --protocol tcp --port
 0-65535 --source-group sg-1a2b3c4d
```

```
# Tag the contaminated instance with the ticket or reference ID
> aws ec2 create-tags -resources i-abcd1234 -tags
 Key=Environment,Value=Quarantine:REFERENCE-ID
```

附录 C：示例运行手册

下面的示例运行手册表示较大运行手册的一个条目。此运行手册是非官方的，仅作为示例提供。 在制作运行手册时，每种情景都可能演变成具有不同的起点和妥协指标的更大项目，但都有类似的结果或需要采取的行动。意识到这种变化还可以使其他情况得到更好或更有见地的回应。

事件响应运行手册 – Root 使用情况

目标

本运行手册的目的是提供有关如何管理 Root AWS 账户使用情况的具体指导。本运行手册不能替代深入的事件响应策略。本运行手册重点介绍事件响应生命周期：

- 建立控制。
- 确定影响。
- 根据需要恢复。
- 调查根本原因。
- 改进。

下面列出了妥协指标（IOC）、初始步骤（止血）以及执行这些步骤所需的详细 CLI 命令。

假设

- 已配置并安装了 CLI。
- 报告程序已经到位。
- Trusted Advisor 处于活动状态。
- Security Hub 处于活动状态。

妥协指标

- 账户出现异常的活动。
  - 创建 IAM 用户。
  - CloudTrail 已关闭。
  - CloudWatch 已关闭。

  - SNS 已暂停。
  - Step Functions 已暂停。
- 启动新的或意外的 AMI。
- 账户中联系人的更改。

修复步骤 – 建立控制

有关可能被盗用账户调用下面列出的特定任务的 AWS 文档。有关可能被盗用账户的文档可在以下网址找到：发现我的 AWS 账户中存在未经授权的活动时该怎么办？

1. 请尽快联系 AWS Support 和 TAM。
2. 更改和轮换 Root 密码，然后添加与 Root 关联的 MFA 设备。
3. 轮换密码、访问密钥/私有密钥和与修复步骤相关的 CLI 命令。
4. 查看 Root 用户执行的操作。
5. 打开这些操作的运行手册。
6. 关闭事件。
7. 查看事件并了解发生了什么。
8. 修复基本问题，实施改进，并根据需要更新运行手册。

进一步的操作项目 – 确定影响

查看创建的项目和变异的调用。可能已创建一些项目以允许将来访问。需要关注的一些事项：

- IAM 跨账户角色。
- IAM 用户。
- S3 存储桶。
- EC2 实例。
- [根据您的应用程序和基础设施，此列表会有所不同。]

声明

客户负责对本文档中的信息进行独立评估判断。本文档：(a) 仅供参考；(b) 代表当前提供的 AWS 产品和实践，如有更改，恕不另行通知；并且 (c) AWS 及其附属机构、供应商或许可方不做任何承诺或保证。AWS 产品或服务“按原样”提供，不提供任何形式的保证、陈述或条件，无论是明示还是暗示。AWS 对其客户的责任和义务由 AWS 协议决定，本文档与 AWS 和客户之间签订的任何协议无关，亦不影响任何此类协议。