Cisco Secure Cloud Analytics

警报和观察结果参考指南

目录

警报和观察结果参考简介

以下内容概述了 Cisco Secure Cloud Analytics (以前称为 Stealthwatch 云) 中可用的警报和观察结果类型。

风险通告和观察结果

Cisco Secure Cloud Analytics 使用动态实体建模来跟踪网络状态。在 Cisco Secure Cloud Analytics环境中，实体是指可以随时间推移进行跟踪的对象，例如网络上的主机或终端，或是 AWS 部署中的 Lambda 函数。动态实体建模根据实体传输的流量及其在网络上执行的活动，收集实体的相关信息。

根据此信息，Cisco Secure Cloud Analytics 可确定：

- 实体的角色，即实体通常执行的操作的描述符。例如，如果实体发送通常与邮件服务器关联的流量，Cisco Secure Cloud Analytics 会为该实体分配邮件服务器角色。角色/实体关系可以是多对一，因为实体可以履行多种角色。
- 对实体的观察结果，即有关实体在网络上的行为的事实，例如与外部 IP 地址建立的心跳连接、与监视列表中实体的交互或与另一个实体建立的远程访问会话。观察结果本身并不具有超出其所代表的事实的意义。一个典型的客户可能有数千个观察结果和若干个风险通告。

Cisco Secure Cloud Analytics 根据角色、观察结果和其他威胁情报的组合生成风险通告，这些风险通告是可操作项目，代表系统标识的可能的恶意行为。

在 Cisco Secure Cloud Analytics Web 网页门户 UI 中打开警报时，您可以查看导致系统生成该警报的支持性观察结果。您还可以从这些观察结果中查看有关所涉实体的其他背景信息，包括它们传输的流量以及外部威胁情报(如果可用)。

指南概述

本指南列出了 Cisco Secure Cloud Analytics 可以生成的警报和观察结果类型。

警报前提条件 提供按基准要求排序的警报表，以及基本生成前提条件。

在 警报说明 列表中的每个警报：

- 警报类型
- 生成的任何前提条件
- 关联的观察结果
- 简要说明，以及为什么这可能表示恶意行为

在 观察结果说明 中列出的每种观察结果类型：

- 观察结果类型
- 生成的任何前提条件
- 关联警报
- 简要说明

警报前提条件和 MITRE ATT&CK 映射

ISE 用户异常

无效的 MAC 地址

ISE 越狱设备

ISE 会话已启动观察结果

ISE 可疑活动观察结果

下表概述了生成给定警报类型所需的历史记录天数，是否可以通过 Cisco Secure Cloud Analytics 专用网络监控（此前称为 Stealthwatch 云专用网络监控）或 Cisco Secure Cloud Analytics 公共云监控（此前称为 Stealthwatch 云公共云监控）生成该警报类型，是否有任何额外的生成限制或前提条件（例如，需要 AWS 集成）。还列出了与风险通告类型关联的任何 MITRE ATT&CK 策略或技术（如果适用）。

风险通告	专用网络监控	公共云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
ISE 用户异常	要求 思科身份服务引擎 (ISE)	要求 思科身份服务引擎 (ISE)	36 天	初始访问	有效账户
异常用户	是	是	36 天	持久性	有效账户
放大攻击	是	是	0 天	影响	网络拒绝服务
异常 AWS 工作空间	否	仅 AWS	14 天		
异常 Mac 工作站	是	是	14 天		
异常 Windows 工作站	是	是	14 天		
参与率丢弃	是	是	14 天	影响	终端拒绝服务
AWS API 监视列表 IP 击中	否	仅 AWS	0 天	发现	云服务发现
AWS 配置规则违规	否	仅 AWS	0 天	持久性	账户操纵
AWS 控制台登录失败	否	仅 AWS	0 天	凭证访问	暴力攻击
AWS 检测器已修改	否	仅 AWS	0 天	防御规避	损害防御

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
AWS 域接管	否	仅 AWS	0 天	资源开发	危害基础设施
AWS EC2 启动脚本已修改	否	仅 AWS	0 天	持久性	启动或登录初始化脚本
AWS ECS 凭证访问	否	仅 AWS	0 天	持久性	植入物内部图像
已创建 AWS IAM Anywhere 信任锚点	否	仅 AWS	0 天	持久性	账户操纵
AWS IAM 用户接管	否	仅 AWS	0 天	持久性	账户操纵
AWS Inspector 评估结果	否	仅 AWS	0 天	持久性	账户操纵
AWS Lambda 调用尖峰	否	仅 AWS	14 天	影响	资源劫持
AWS Lambda 持久性	否	仅 AWS	0 天	持久性	事件触发执行
已删除 AWS 日志记录	否	仅 AWS	0 天	防御规避	损害防御
AWS 日志记录受损	否	仅 AWS	0 天	防御规避	损害防御
AWS 多因素身份验证更改	否	仅 AWS	0 天	持久性	账户操纵
AWS 重复 API 故障	否	仅 AWS	3 天	发现	云服务发现
使用的 AWS 根账户	否	仅 AWS	0 天	持久性	有效账户
已删除 AWS 安全组	否	仅 AWS	0 天	影响	账户访问权限已删除
AWS 快照泄露	否	仅 AWS	0 天	渗漏	将数据传输到云账户
Azure 活动日志 IP 监视列表命中	否	仅 Azure	0 天	发现	云服务发现

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
Azure 活动日志监视列表命中	否	仅 Azure	0 天	持久性	事件触发执行
Azure 顾问监视列表	否	仅 Azure	0 天	持久性	事件触发执行
Azure 缺乏保护的服务	否	仅 Azure	0 天	侦测	收集受害主机信息
已删除 Azure 防火墙	否	仅 Azure	0 天	防御规避	损害防御
Azure 函数调用尖峰	否	仅 Azure	14 天	影响	资源劫持
已删除 Azure Key Vault	否	仅 Azure	0 天	影响	账户访问权限删除
已删除 Azure 网络安全组	否	仅 Azure	0 天	防御规避	损害防御
Azure OAuth 绕行	否	仅 Azure	0 天	初始访问	有效账户
Azure 许可安全组	否	仅 Azure	0 天	初始访问	外部远程服务
Azure 许可存储帐户	否	仅 Azure	0 天	持久性	账户操纵
已删除 Azure 资源组	否	仅 Azure	0 天	影响	数据损坏
Azure 安全事件	否	仅 Azure	0 天	持久性	事件触发执行
Azure 将数据传输到云账户	否	仅 Azure	0 天	渗漏	通过 Web 服务进行的泄露
未使用位置的 Azure 虚拟机	否	仅 Azure	0 天	影响	资源劫持
CloudTrail 监视列表命中	否	仅 AWS	0 天	持久性	事件触发执行
已确认的威胁监视列表命中	需要 安全分析和日志记录 (SaaS)、增强型 NetFlow 或 DNS 日志	需要 安全分析和日志记录 (SaaS)、增强型 NetFlow 或 DNS 日志	0 天	命令和控制	应用层协议
国家/地区集偏差	是	是	36 天	初始访问	有效账户

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
严重性云安全评估监控列表命中	否	是	0 天		
DNS 滥用	是	是	0 天	渗漏	通过替代协议渗漏
域生成算法成功查找	需要 DNS 日志	否	0 天	命令和控制	动态分辨率
垃圾邮件警报	是	是	36 天	渗漏	通过替代协议渗漏
紧急配置文件	是	是	14 天	渗漏	通过替代协议渗漏
Empire 命令和控制	是	是	1 天	命令和控制	非应用层协议
异常域控制器	是	是	7 天	权限提升	滥用海拔控制机制
访问尝试次数过多(外部)	是	是	0 天	凭证访问	暴力攻击
网络打印机连接过多	是	是	0 天	影响	终端拒绝服务
GCP 云函数调用尖峰	否	仅 GCP	14 天	影响	资源劫持
GCP Stackdriver Logging 监视列表命中	否	仅 GCP	0 天	持久性	事件触发执行
地理位置异常的 AWS API 使用情况	否	仅 AWS	14 天	发现	云服务发现
地理位置异常的 Azure API 使用情况	否	仅 Azure	14 天	发现	云服务发现
地理位置异常的远程访问	是	是	14 天	初始访问	外部远程服务
心跳连接计数	是	是	1 天	命令和控制	非应用层协议
高带宽单向	是	是	0 天	渗漏	自动渗漏

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
流量					
高严重性云安全评估监视列表命中	否	是	0 天		
ICMP 滥用	是	是	0 天	渗漏	通过替代协议渗漏
IDS 紧急配置文件	要求 Cisco Security Analytics and Logging (SaaS) 或 IDS	要求 安全分析和日志记录 (SaaS) 或 IDS	14 天	影响	终端拒绝服务
IDS 通知尖峰	要求 安全分析和日志记录 (SaaS) 或 IDS	要求 安全分析和日志记录 (SaaS) 或 IDS	1 天	影响	终端拒绝服务
入站端口扫描程序	是	是	1 天	发现	网络服务扫描
内部连接峰值	是	是	0 天	发现	网络服务扫描
内部连接监视列表命中	是	是	0 天	持久性	事件触发执行
内部端口扫描程序	是	是	7 天	发现	网络服务扫描
无效的 MAC 地址	要求 思科身份服务引擎 (ISE)	要求 思科身份服务引擎 (ISE)	0 天	威胁横向运动	伪装
ISE 越狱设备	要求 思科身份服务引擎 (ISE)	要求 思科身份服务引擎 (ISE)	0 天	初始访问	偷渡式入侵
来自可疑进程的 LDAP 连接	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	0 天	凭证访问	有效账户
LDAP 连接峰值	是	是	9 天	发现	网络服务扫描
低严重性云安全评估监视列表命中	否	是	0 天		
检测到恶意	需要过渡到思科	需要过渡到思科	0 天	执行	伪装

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
进程	XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)			
恶意软件激增	要求 安全分析和日志记录 (SaaS)	要求 安全分析和日志记录 (SaaS)	1 天	执行	用户执行
中严重性级别的云安全评估监控列表命中	否	是	0 天		
已执行的 Metasploit	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	0 天	执行	用户执行
Meterpreter 命令和控制成功	是	是	1 天	命令和控制	非应用层协议
缺少相扑逻辑日志	需要 Sumo Logic	否	0 天	影响	数据操纵
NetBIOS 连接峰值	是	是	7 天	发现	网络服务发现
网络群体峰值	是	是	36 天	影响	网络拒绝服务
网络打印机连接过多	是	是	0 天	命令和控制	Web 服务
添加了新的 AWS Lambda 调用权限	否	仅 AWS	0 天	持久性	事件触发执行
新 AWS 区域	否	仅 AWS	0 天	防御规避	未使用/不受支持的云区域
新的 AWS Route53 目标	否	仅 AWS	0 天	持久性	账户操纵
新外部连接	是	是	35 天	集合	自动收集
新内部设备	是	是	21 天	初始访问	添加硬件
新 IP 扫描程序	是	是	7 天	发现	网络服务发现
新的长会话	是	是	2 天	渗漏	通过替代

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
(地理)					协议渗漏
新远程访问	是	是	36 天	初始访问	外部远程服务
新 SNMP 扫描	是	是	7 天	发现	网络服务发现
新异常 DNS 解析器	是	是	7 天	命令和控制	应用层协议
非服务端口扫描程序	是	是	9 天	发现	网络服务扫描
出站 LDAP 连接尖峰	是	是	0 天	侦测	主动扫描
出站 SMB 连接峰值	是	是	0 天	侦测	主动扫描
出站流量尖峰	是	是	14 天	渗漏	自动渗漏
已创建许可 Amazon Elastic Kubernetes 服务集群	否	仅 AWS	0 天	发现	容器和资源发现
许可 AWS S3 访问控制列表	否	仅 AWS	0 天	集合	来自云存储对象的数据
已创建许可的 AWS 安全组	否	仅 AWS	0 天	持久性	账户操纵
持久性远程控制连接	是	是	7 天	初始访问	外部远程服务
端口 8888：来自多个源的连接	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	0 天	命令与控制	自动渗漏
潜在数据泄露	是	是	0 天	渗漏	自动渗漏
潜在数据库泄露	是	是	7 天	渗漏	通过替代协议渗漏
潜在的持久性尝试	需要过渡到思科 XDR 和思科 AnyConnect 安全	需要过渡到思科 XDR 和思科 AnyConnect 安全	0 天	持久性	事件触发执行

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
	移动客户端网络可视性模块 (NVM)	移动客户端网络可视性模块 (NVM)			
潜在的系统进程模拟	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	0 天	防御规避	伪装
潜在有害的隐藏文件扩展名	需要 安全分析和日志记录 (SaaS) 或 增强型 NetFlow	需要 安全分析和日志记录 (SaaS) 或 增强型 NetFlow	0 天	执行	用户执行
潜在易受攻击的远程控制协议	需要增强型 NetFlow	需要增强型 NetFlow	1 天	防御规避	防御规避漏洞攻击
协议伪造	是	是	1 天	命令和控制	非标准端口
协议违规(地理)	是	是	0 天	命令和控制	应用层协议
已创建公共 Amazon Route 53 托管区域	否	仅 AWS	0 天	资源开发	建立账户
面向公众的 IP 监视列表匹配	是	是	0 天	侦测	收集受害网络信息
远程访问(地理)	是	是	0 天	初始访问	有效账户
重复的 Umbrella Sinkhole 通信	是	是	0 天	命令和控制	应用层协议
重复的监视列表通信	是	是	0 天	命令和控制	应用层协议
角色违规	是	是	0 天	持久性	创建或修改系统进程
已配置 S3 存储桶生命周期	否	仅 AWS	0 天	影响	数据损坏
SMB 连接异常值	是	是	36 天	侦测	收集受害网络信息
SMB 连接峰	是	是	7 天	发现	网络服务

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
值					发现
SMB|RDP：与多个目标的连接	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络可视性模块 (NVM)	1 天	威胁横向运动	远程服务
失效 AWS 访问密钥	否	仅 AWS	30 天	集合	来自云存储对象的数据
静态设备连接偏差	是	是	1 天	初始访问	外部远程服务
静态设备偏差	是	是	35 天	影响	资源劫持
疑似僵尸网络交互	是	是	1 天	命令和控制	应用层协议
疑似加密货币活动	是	是	0 天	影响	资源劫持
可疑恶意 URL	需要 安全分析和日志记录 (SaaS) 或 增强型 NetFlow	需要 安全分析和日志记录 (SaaS) 或 增强型 NetFlow	0 天	初始访问	偷渡式入侵
可疑网络钓鱼域	需要 安全分析和日志记录 (SaaS)、增强型 NetFlow 或 DNS 日志	需要 安全分析和日志记录 (SaaS)、增强型 NetFlow 或 DNS 日志	0 天	初始访问	偷渡式入侵
疑似端口滥用(外部)	是	是	1 天	发现	网络服务扫描
疑似远程访问工具心跳	是	是	0 天	命令和控制	非应用层协议
疑似 Zerologon RPC 漏洞攻击尝试	是	是	0 天	权限提升	权限提升漏洞攻击
可疑的 DNS Over HTTPS 活动	是	是	7 天	防御规避	损害防御
可疑的域查找失败	需要 DNS 日志	否	0 天	命令和控制	动态分辨率
可疑进程路径	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络	需要过渡到思科 XDR 和思科 AnyConnect 安全移动客户端网络	0 天	防御规避	伪装

风险通告	专用网络监控	公共 云监控	历史记录	MITRE ATT&CK 策略	MITRE ATT&CK 技术
	可视性模块 (NVM)	可视性模块 (NVM)			
可疑 SMB 活动	是	是	14 天	威胁横向运动	远程服务
可疑用户代理	要求 安全分析和日志记录 (SaaS)	要求 安全分析和日志记录 (SaaS)	0 天	初始访问	漏洞攻击面向公众的应用
Talos 情报监视列表命中	是	是	0 天	命令和控制	应用层协议
TrickBot 锚点 DNS 隧道	否	仅 AWS	14 天	命令和控制	应用层协议
未使用的 AWS 资源	否	仅 AWS	14 天	影响	服务停止
异常 DNS 连接	是	是	1 天	命令和控制	应用层协议
异常外部服务器	是	是	14 天	命令和控制	应用层协议
来自新外部服务器的异常文件扩展名	要求 安全分析和日志记录 (SaaS)	要求 安全分析和日志记录 (SaaS)	1 天	命令与控制	应用层协议
异常大的 EC2 实例	否	仅 AWS	0 天	影响	资源劫持
用户监视列表命中	是	是	0 天	命令和控制	Web 服务
易受攻击的传输安全协议	需要增强型 NetFlow	需要增强型 NetFlow	1 天	防御规避	防御规避漏洞攻击
监视列表命中	是	是	0 天	命令和控制	Web 服务
蠕虫传播	是	是	9 天	威胁横向运动	远程服务漏洞攻击

警报说明

异常 ISE 用户

描述：有一个用户是过去唯一从特定设备进行身份验证的用户。最近在同一设备上进行了身份验证的另一个用户，但该用户通常仅从不同的设备进行身份验证。默认情况下，此警报处于禁用状态。如果需要，请确保启用此警报。

前提条件：此警报需要 36 天的历史记录，以建立与实体建立会话的一般预期用户。此警报需要 ISE 集成用户数据属性。

关联观察结果：ISE 会话开始的观察结果

后续步骤：参考与此警报关联的支持观察结果，以确定在终端上进行身份验证的用户和时间。查看 ISE 会话日志，以验证与观察结果关联的用户和终端类型。联系用户并确定他们在做什么。如果他们的操作不正常，请执行其他调查。如果用户未自行登录，或实体无法识别，则假定用户凭证已被盗取。在具有虚拟桌面基础设施 (VDI) 的环境中预计会出现检测到的场景。

异常用户

描述：在通常不会看到此用户会话的实体上创建了用户会话。新用户会话可能表示恶意活动或尚未建立常规重复会话的预期用户。

前提条件：此警报需要 36 天的历史记录，以建立与实体建立会话的一般预期用户。此警报需要满足以下条件之一：

- AWS 集成。
- ISE 集成用户数据属性。
- Sumo Logic

关联观察结果：ISE会话打开的观察结果

后续步骤：参考与此警报关联的支持观察结果，以确定登录实体的用户账户和时间。联系用户并确定他们在做什么。如果他们的操作不正常，请执行其他调查。如果用户未自行登录，或者实体未被识别或来自您不信任的外部网络，请更新阻止列表和防火墙规则，以防止恶意攻击者访问您的网络。确定用户对实体执行的操作，并在可能的情况下补救任何负面影响。如果用户窃取了数据，请确定发送了哪些数据，并遵循组织的数据丢失准则。

放大攻击

说明：此实体发送的流量包含一个配置文件，该配置文件表明参与放大攻击。放大攻击会尝试使用大量数据包响应某个请求，以达到淹没服务器的目的，其中通常涉及欺骗性的 IP 地址，以允许多个实体发送流量来响应请求。参与放大攻击可能表示某个实体已感染僵尸网络恶意软件，并在无意中发送这些数据包。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：流量放大观察结果

后续步骤：参考风险通告和支持性观察结果中的实体信息，确定是否有外部实体负责传播恶意软件。如果有，请更新防火墙规则，以阻止来自该外部实体和任何其他实体（如果是分布式拒绝服务 (DDoS) 攻击）的流量。

如果发送放大攻击的实体在您的网络内部，则将该实体以及任何其他实体（如果是 DDoS 攻击）从您的网络隔离出来。检查实体中是否有恶意软件；如果有，请删除。

异常 AWS 工作空间

说明：AWS 虚拟工作空间使用新的异常行为配置文件（例如，主机通过 BitTorrent 连接到许多实体）。这可能表示存在恶意软件或滥用行为。

前提条件：此风险通告需要 14 天的历史记录，才能确定实体的正常活动级别。

关联观察结果：异常配置文件观察结果

后续步骤：参考支持性观察结果，确定实体的角色并确定异常行为是否存在正当的业务原因。例如，如果某个实体使用 BitTorrent 连接到其他实体，它可能是测试实体或某种可能的防火墙规则测试或其他安全测试。如果异常行为没有正当原因，请检查实体，确定实体是否按预期运行，以及是否没有恶意软件。

异常 Mac 工作站

说明：Apple Mac 工作站使用新的异常行为配置文件（例如，主机通过 BitTorrent 连接到许多实体）。此警报可能表示存在恶意软件或滥用行为。

前提条件：此风险通告需要 14 天的历史记录，才能确定实体的正常活动级别。

关联观察结果：异常配置文件观察结果

后续步骤：参考支持性观察结果，确定实体的角色并确定异常行为是否存在正当的业务原因。例如，如果某个实体使用 BitTorrent 连接到其他实体，它可能是测试实体或某种可能的防火墙规则测试或其他安全测试。如果异常行为没有正当原因，请检查实体，确定实体是否按预期运行，以及是否没有恶意软件。

异常 Windows 工作站

说明：Windows 工作站使用新的异常行为配置文件（例如，主机通过 BitTorrent 连接到许多实体）。此警报可能表示存在恶意软件或滥用行为。

前提条件：此风险通告需要 14 天的历史记录，才能确定实体的正常活动级别。

关联观察结果：异常配置文件观察结果

后续步骤：参考支持性观察结果，确定实体的角色并确定异常行为是否存在正当的业务原因。例如，如果某个实体使用 BitTorrent 连接到其他实体，它可能是测试实体或某种可能的防火墙规则测试或其他安全测试。如果异常行为没有正当原因，请检查实体，确定实体是否按预期运行，以及是否没有恶意软件。

参与率丢弃

描述：此实体通常在一天的大部分时间都处于活动状态，但其活动会在多个配置文件（例如，SSH 服务器、FTP 服务器）中丢弃。此类行为可能表示实体的计划停机或维护，但也可能表示影响实体运行能力的恶意软件，或以某种方式影响实体的其他恶意行为。

前提条件：此风险通告需要 14 天的历史记录，才能确定实体的正常活动级别。

关联观察结果：历史异常值观察结果

后续步骤：参考支持性观察结果，查看实体的角色并确定活动丢弃是否存在正当的业务原因。如果活动丢弃没有正当原因，请检查实体，确定实体是否按预期运行，以及是否没有恶意软件。

AWS API 监视列表 IP 命中

描述：已从监视列表中的 IP 访问 AWS API。如果 Cisco Secure Cloud Analytics 监视列表中的实体访问了 AWS 部署中的 API，则可能表示存在恶意访问资源的尝试，应进行进一步调查。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS API 监视列表访问观察结果

后续步骤：研究访问 AWS API 的实体以及该实体调用的 API 函数。确定访问是否导致了恶意活动，恶意活动是否正在进行，并补救活动。检查您的 AWS 安全设置，并确保您已采取适当的预防措施来防止未经授权的访问。如果此访问是恶意的，请更新防火墙规则以阻止该实体。

AWS 配置规则违规

描述：违反了 AWS Config 规则。如果配置更改违反了 AWS 配置规则，则应检查更改并更新配置以符合配置规则。

前提条件：此风险通告需要 0 天的历史记录。此观察结果需要 AWS 集成、用于将配置更改传输到 SNS 主题的 AWS 配置、用于发送配置更改的 SQS 队列，以及用于检索消息的 Cisco Secure Cloud Analytics 中其他配置。

关联观察结果：AWS 配置合规性观察结果

后续步骤：参考警报和支持观察结果，以确定哪个 AWS 资源是配置更改和配置规则违规的来源。检查配置更改在业务过程中是否符合预期和正常，例如在不更新 AWS Config 规则的情况下进行必要的更新。如果发生意外更改，请恢复更改并查看日志，以确定实施更改的用户或会话。

AWS 控制台登录失败

描述：用户多次尝试登录 AWS 控制台均失败。如果用户反复登录 AWS 控制台失败，则可能表示有未经授权的用户尝试获取访问权限，或者用户忘记了凭证。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 IAM 日志。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：确定与失败登录关联的用户账户。参考支持观察结果，以确定登录是否发生在您的网络上已识别的实体。如果登录来自您不认识的实体，请进一步研究这是否是恶意实体，并在等待调查结果出来之前重置或锁定用户的凭证。更新阻止列表和防火墙规则，以禁止恶意实体访问您的网络。

如果您识别出提交登录请求的实体，请联系用户并确定他们是否忘记了凭证。如果他们忘记了凭证，请重置凭证。如果他们没有忘记自己的凭证，而其他人正在尝试以该人的身份登录，请重置或锁定该用户的凭证，并尝试识别您网络上的恶意攻击者。断开实体与网络的连接，并确定其是否感染了恶意软件，或者恶意攻击者是否通过恶意软件获得了远程访问权限。

AWS 检测器已修改

描述：AWS GuardDuty 检测器已被删除或禁用。此警报可能表示尝试避免检测恶意活动。

前提条件：此风险通告需要 0 天的历史记录。此警报需要启用 AWS 集成和 GuardDuty。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：重新启用 GuardDuty 检测器以重新启用 GuardDuty。查看日志以确定 GuardDuty 检测器的删除或禁用方式。更新防火墙规则和安全设置，以防止由于恶意行为而导致的访问。

AWS 域接管

描述：已尝试将使用 AWS Route53 注册的域转移到另一个 AWS 账户。可能表示尝试劫持域，然后可以在未来的攻击中使用或劫持域以获取赎金。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：确保此操作由授权人员根据适用程序有目的地执行，并且不会造成安全风险。如果这似乎不是合法的访问密钥创建，请查看创建访问密钥的用户或角色的 CloudTrail 日志，并考虑轮换用于发出请求的凭证，并立即禁用已创建的访问密钥。

AWS EC2 启动脚本已修改

描述：AWS EC2 实例启动脚本已修改。此警报可能表示恶意攻击者试图建立持久性或执行恶意代码。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：确认启动脚本是否已被合法用户修改为有效活动。如果不是，请查看启动脚本及其执行的操作。检查 IAM 用户执行的其他操作，并轮换用户的凭证，因为它们可能被视为已被入侵。

AWS ECS 凭证访问

描述：ECS 任务定义已使用容器命令注册，该命令将从 AWS 实例元数据服务获取凭证。此警报可能表示攻击者正在尝试获取服务凭证。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：确保此操作由授权人员根据适用程序有目的地执行，并且不会造成安全风险。如果这似乎不是合法访问，请查看其凭证被访问的用户或角色的 CloudTrail 日志，并考虑轮换用于发出请求的凭证。

已创建 AWS IAM Anywhere 信任锚点

描述：已创建新的 IAM Roles Anywhere 信任锚。这可能是合法活动，但也可能表示攻击者尝试从 AWS 外部建立对账户的持久访问。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：使用关联的观察结果验证新创建的信任锚的合法性。如果不合法，请禁用新的信任锚并查看创建信任锚的用户的 CloudTrail 日志，以查看他们是否执行了其他可疑活动。

AWS IAM 用户接管

描述：如果您正在监控 AWS CloudTrail 日志，此警报表示用户已为其他用户创建凭证。这可能表示攻击者正在尝试在环境中建立额外的持久性。默认情况下，此警报处于禁用状态。如果需要，请确保启用此警报。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：使用关联的观察结果验证新创建的用户凭证的合法性。如果不合法，请禁用新用户，然后查看创建凭证的用户的 CloudTrail 日志，以查看他们是否执行了其他可疑活动。

AWS Inspector 评估结果

描述：AWS Inspector 报告实体的严重性为高。高严重性检查结果表示您应尽快补救的重要安全和合规性调查结果。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并启用检查器。

关联观察结果：Amazon Inspector 发现观察结果

后续步骤：检查 AWS Inspector 中的调查结果，并采取必要的措施来纠正调查结果。

AWS Lambda 调用高峰

描述：Lambda 函数被调用了记录的次数。Lambda 函数活动激增可能是由于非恶意行为(例如 Lambda 配置错误)造成的。也可能是恶意行为导致的，例如恶意攻击者反复调用该函数以占用资源。

前提条件：此警报需要 14 天的历史记录，以建立 Lambda 函数运行频率的指标。此警报还需要 AWS 集成，并且至少需要 AWS 中的一个 Lambda 函数。

关联观察结果：AWS Lambda 指标异常值观察结果

后续步骤：如果 Lambda 函数调用次数导致网络出现问题，请暂时禁用 Lambda 函数，等待调查结果。

查看调用 AWS Lambda 函数所需的条件，以及多次触发 Lambda 函数的原因。更正条件以确保这种情况不会再次发生。如果外部恶意实体导致 Lambda 函数触发，请更新阻止列表和防火墙规则，以禁止此实体访问您的网络。如果这会暴露 Lambda 函数中的缺陷，请更新 Lambda 函数逻辑。

AWS Lambda 持久性

描述：已创建新的 AWS Lambda 函数并将其与新的 CloudWatch 事件关联。这可能表示尝试通过向新创建的资源添加后门来实现持久性。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，Cisco Secure Cloud Analytics 允许在 AWS 中读取 CloudTrail 日志和至少一个 Lambda 函数。

关联观察结果：AWS Lambda 指标异常值观察结果

后续步骤：验证触发 Lambda 函数的操作和执行的代码。触发 Lambda 的事件模式可以在 `PutRule` 事件的请求中找到，函数名称包含在 `CreateFunction` 事件的请求中。查看随附的观察结果，并确保授权人员根据适用的程序有目的地执行此操作，并且不会造成安全风险。如果不是，请恢复操作并验证所使用的凭证是否未受到危害。

已删除 AWS 日志记录

描述：AWS VPC 流日志或 CloudTrail 日志已删除。此警报可能表示尝试删除恶意活动的历史记录。

前提条件：此风险通告需要 0 天的历史记录。此警报需要启用 AWS 集成和 VPC 流日志记录或 CloudTrail 日志记录。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：确定删除日志信息的用户或进程，并确定用户或进程在删除日志时可能采取的任何其他操作。如果恶意行为导致进一步访问，请更新防火墙规则和安全设置。

AWS 日志记录受损

描述：AWS CloudTrail 或 VPC 流日志收集受损。停止收集新日志，删除现有日志，或者 S3 存储桶生命周期策略在创建和存储日志后不久将其删除。这可能表示威胁发起者试图隐藏其他恶意行为并利用 AWS CloudTrail 事件观察结果。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：确定检测到的活动是否合法。如果需要，请采取措施来撤销 AWS VPC 流日志、CloudTrail、S3 生命周期或事件选择器更改。

AWS 多因素身份验证更改

描述：多因素身份验证已从用户账户中删除。删除多因素身份验证违反了安全最佳实践。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

相关观察结果：AWS CloudTrail 事件观察结果、AWS 多因素身份验证更改观察结果

后续步骤：根据组织的安全要求，根据需要禁用帐户。确定删除多因素身份验证的人员及其原因。如果由于用户丢失多因素身份验证设备而将其删除，请更换该设备并重置多因素身份验证。

如果恶意攻击者删除了多因素身份验证，请禁用账户并重置凭证。更新阻止列表和防火墙规则，以禁止此实体访问您的网络。

AWS 重复 API 故障

描述：用户执行了多个 API 调用，导致权限不足而失败。这可能表明攻击者正在尝试发现/枚举有关其环境的信息、建立持久性或升级权限。

前提条件：此风险通告需要 3 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：检查用户和 API 调用的关联 CloudTrail 观察结果。如果调用不是合法用户操作的结果，则假定用户已受到攻击。使用 CloudTrail 日志调查此用户最近的活动，并采取必要的操作来隔离用户，以防止任何进一步的操作。尝试确定初始访问的方法并查看 IAM 委托人以获取不必要的权限。

使用的 AWS 根账户

描述：已使用 AWS 根账户执行操作。AWS 建议的最佳实践是仅将执行任务所需的权限委派给用户创建的账户，并且在不必要时不要使用根账户。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果、AWS 根账户使用的观察结果

后续步骤：确定用户或角色是否应具有根级别权限。如果不是，请更新配置以减少 AWS 根账户的风险。

已删除 AWS 安全组

已删除 AWS 安全组

描述：已删除 AWS VPC 安全组或 ElastiCache 安全组。这可能表示有人试图损害合法功能。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：验证这是否是合法行为。否则，请调查此 IAM 委托人的其他未经授权的活动的历史记录。

AWS 快照泄露

描述：EC2 快照已修改为可由其他账户访问。此警报可能表示攻击者正在尝试窃取数据。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：确保此操作由授权人员根据适用程序有目的地执行，并且不会造成安全风险。

Azure 活动日志 IP 监视列表命中

描述：Azure 活动日志报告了由与用户定义的或集成的监视列表匹配的 IP 地址发起的事件。这可能表示未经授权的用户已获得对 Azure 的访问权限。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 活动日志。

关联观察结果：Azure 异常活动观察结果

后续步骤：验证监视列表条目是否正确。引用 IP 地址的支持观察结果，并确定行为是否为恶意行为。如果是恶意行为，则对活动进行补救。检查您的 Azure 安全设置，并确保您已采取适当的预防措施来防止未经授权的访问。如果此访问是恶意的，请更新防火墙规则以阻止 IP 地址。

Azure 活动日志监视列表命中

描述：Azure 活动日志报告了用户提供的监视列表中的事件。如果 Cisco Secure Cloud Analytics 监视列表中的某个实体访问了您的 Azure 部署，则可能表示存在恶意访问资源的尝试，应进行进一步调查。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 活动日志。

关联观察结果：Azure 异常活动观察结果

后续步骤：验证监视列表条目是否正确。引用实体流量量变曲线的支持观察结果，并确定该行为是否为恶意行为。如果是恶意行为，则对活动进行补救。检查您的 Azure 安全设置，并确保您已采取适当的预防措施来防止未经授权的访问。如果此访问是恶意的，请更新防火墙规则以阻止该实体。

Azure 顾问监视列表

描述：检测到针对监视列表中的建议类型的 Azure 顾问建议。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 顾问。

关联观察结果：Azure 顾问建议观察结果

后续步骤：查看关联的 Azure 顾问建议，并根据建议采取行动。

Azure 缺乏保护的服务

描述：向互联网公开诸如控制面板或数据库之类的开放服务。此警报可能表示无意中暴露了敏感数据。默认情况下，此警报处于启用状态。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成。

关联观察结果：Azure 暴露的服务观察结果

后续步骤：检查 Azure 中服务的权限，并将其限制为仅授权用户、域或 IP。

已删除 Azure 防火墙

描述：Azure 防火墙已删除。此警报可能表示攻击者正在尝试破坏网络防御，主要针对已成功删除的防火墙。成功删除 Azure 防火墙，可能表示有人尝试损害网络防御。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 活动日志。

关联观察结果：Azure 异常活动观察结果

后续步骤：确保此操作由授权人员根据适用程序有目的地执行，并且不会造成安全漏洞。

Azure 函数调用高峰

描述：Azure 函数被调用了记录的次数。此警报可能表示存在操作问题或拒绝服务攻击。

前提条件：此风险通告需要 14 天的历史记录。此警报需要 Azure 集成。

关联观察结果：Azure 函数指标异常值观察结果

后续步骤：如果 Azure 函数调用次数导致网络出现问题，请暂时禁用 Azure 函数，等待调查结果。查看调用 Azure 函数所需的条件，以及多次触发 Azure 函数的原因。更正条件以确保这种情况不会再次发生。如果外部恶意实体导致 Azure 功能触发，请更新阻止列表和防火墙规则，以禁止此实体访问您的网络。如果这会暴露 Azure 函数中的缺陷，请更新 Azure 函数逻辑。

已删除 Azure Key Vault

描述：密钥保管库已删除。此警报可能表示尝试通过删除密钥来中断服务可用性。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 活动日志。

关联观察结果：Azure 异常活动观察结果

后续步骤：确保此操作由授权人员根据适用程序有目的地执行，并且不会造成安全风险。

已删除 Azure 网络安全组

描述：Azure 网络安全组已删除。此警报可能表示攻击者正在尝试破坏网络防御。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 活动日志。

关联观察结果：Azure 异常活动观察结果

后续步骤：确保此操作由授权人员根据适用程序有目的地执行，并且不会造成安全漏洞。

Azure OAuth 绕行

描述：检测到修改 kubeconfig 文件的操作。kubeconfig 文件（也由 kubectl 使用）包含有关 Kubernetes 集群的详细信息，包括其位置和凭证。攻击者可以使用 listClusterAdminCredential 操作从受攻击的客户端访问此文件。然后，他们可以使用它来访问集群。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 活动日志。

关联观察结果：Azure 异常活动观察结果

后续步骤：检查所采取操作的详细信息，以确定这是合法的还是恶意的，并在需要时采取补救措施。

Azure 许可安全组

描述：Azure 安全中心将网络安全组识别为过于宽松。如果入站规则允许从“任何”或“互联网”范围进行访问，或者允许的端口范围过于宽松，就会发生这种情况。强化这些规则有助于防止攻击者轻易地将您的资源作为攻击目标。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和至少一个网络安全组。

关联观察结果：Azure 许可安全组观察结果

后续步骤：检查 Azure 中的网络安全组权限，并将权限限制为仅授权用户或域。根据需要限制端口范围。

Azure 许可存储帐户

描述：Azure 安全中心将存储帐户识别为具有不受限制的防火墙设置。这可能导致未经授权访问存储的数据。建议配置网络规则，以便只有来自允许的网络或 IP 地址范围的应用才能访问存储帐户。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和至少一个存储帐户。

关联观察结果：Azure 许可存储设置观察结果

后续步骤：检查 Azure 中的存储帐户权限，并将权限限制为仅授权用户或域。根据需要限制端口范围。

已删除 Azure 资源组

描述：资源组已删除。此警报可能表示有人尝试销毁数据。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 活动日志。

关联观察结果：Azure 异常活动观察结果

后续步骤：确保此操作由授权人员根据适用程序有目的地执行，并且不会造成安全风险。

Azure 安全事件

描述：Azure 安全中心报告了中或高严重性事件。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成、Azure 安全中心、标准层和 Azure 活动日志。

关联观察结果：Azure 安全事件观察结果

后续步骤：查看支持性观察结果，以确定严重性为中或高的事件。登录 Azure 安全中心并查看事件。根据需要进行补救。

Azure 将数据传输到云账户

描述：已为虚拟机创建可公开访问的快照。此警报可能表示有数据泄露尝试。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成和 Azure 活动日志。

关联观察结果：Azure 异常活动观察结果

后续步骤：确保此操作由授权人员根据适用程序有目的地执行，并且不会造成安全风险。

未使用位置的 Azure 虚拟机

描述：已在以前未使用的位置创建 Azure 虚拟机。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Azure 集成，并授予 Cisco Secure Cloud Analytics “监控读者”角色查看 Azure 订用的权限。

关联观察结果：未使用位置的 Azure VM 观察结果

后续步骤：查看支持观察结果，以确定虚拟机及其位置。如果创建的虚拟机可能是恶意的，请关闭虚拟机。根据需要进行补救。

CloudTrail 监视列表命中

描述：AWS CloudTrail 报告了用户提供的监视列表中的事件。您可以自定义 CloudTrail 监视列表，以关注您的 AWS 账户的事件，并在系统生成这些警报时执行其他研究。

前提条件：此警报需要 AWS 集成，允许 Cisco Secure Cloud Analytics读取 CloudTrail 日志，并在 Cisco Secure Cloud Analytics Web UI 中配置 AWS CloudTrail 监视列表。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：引用报告的事件和警报的支持观察结果。确定行为是否为恶意行为，是否需要进一步调查。

已确认的威胁监视列表命中

描述：此实体与与已知威胁关联的外部资源进行了交互。此警报是 加密流量分析 功能的一部分。使用基于增强型 NetFlow 的威胁情报可以进一步洞察网络威胁。

前提条件：此风险通告需要 0 天的历史记录。支持 已确认威胁指标匹配 - 域观察结果、已确认威胁指标匹配 - 主机名观察结果和 已确认威胁指标匹配 - URL 观察结果 需要以下一项或多项：

- 安全分析和日志记录 (SaaS) 通过思科防御协调器和 Secure Firewall 设备。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。
- 增强型 NetFlow。有关详细信息，请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。
- 来自 SPAN 或镜像端口的 DNS 日志。

关联观察结果：已确认威胁指标匹配 - 主机名观察结果、已确认威胁指标匹配 - IP 观察结果、已确认威胁指标匹配 - 域观察结果、已确认威胁指标匹配 - URL 观察结果

后续步骤：参考已知威胁类型（域名、主机名、IP 地址或恶意 URL）的警报和支持观察结果。根据已知威胁，根据需要进行补救。更新您的防火墙规则，以防止访问或来自已知威胁。

国家/地区集偏差

说明：此实体已明显偏离通常与其通信的国家/地区集。默认情况下，此警报处于启用状态。

前提条件：此风险通告需要 36 天的历史记录，才能确定与实体通信的正常国家/地区集。

关联观察结果：国家/地区集偏差观察结果

后续步骤：参考支持性观察结果，找到与该实体建立了连接的实体及其地理位置。确定该实体建立这些连接的原因，并在问题归因于恶意行为的情况下予以修复。根据需要更新国家/地区监视列表，以包括所有与恶意行为有关的国家/地区。

严重性云安全评估监控列表命中

描述：在 Cisco Secure Cloud Analytics监控的云环境中发现了云安全评估监视列表中的一个或多个严重合规性故障。此警报可能表示环境不符合最佳实践。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 或 Azure 集成。

关联观察结果：合规性判定摘要观察结果、新合规性资源失败观察结果

后续步骤：点击警报中观察结果的 ID，了解有关合规性失败和补救后续步骤的详细信息，以解决失败问题。

DNS 滥用

描述：此实体一直在发送异常大的 DNS 数据包。这可能是为了将数据传输伪装成 DNS 流量。例如，恶意软件可能导致实体将敏感信息发送到受攻击者控制的远程服务器。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：异常数据包大小观察结果

后续步骤：参考支持观察结果，以确定实体将 DNS 数据包发送到哪个 DNS 服务器。如果 DNS 服务器是合法的，请将其添加到子网配置中的 VPN 子网，以减少误报的数量。对实体发送大型 DNS 数据包的原因进行进一步研究。如果 DNS 服务器不合法，请查看实体的日志并确定实体发送 DNS 数据包的原因，以及它是否是恶意行为。补救任何恶意行为。根据需要更新防火墙规则，以防止进一步的恶意行为。

域生成算法成功查找

描述：此实体已成功将算法生成的域（例如 rgkte-hdvj.cc）解析为 IP 地址。这可能表示恶意软件感染或尝试在生成的域中使用命令和控制服务器创建僵尸网络或其他僵尸网络活动。

前提条件：此警报需要 0 天的历史记录。此警报需要来自 SPAN 或镜像端口的 DNS 日志。

关联观察结果：域生成算法成功观察结果

后续步骤：引用支持观察结果中列出的域，并确定域查找是良性还是恶意。如果是恶意软件，请确定生成查找的软件。查看 域生成算法成功观察结果 并确定其他实体是否进行了可疑调用。

垃圾邮件警报

描述：此实体与外部邮件服务器的连接异常增加。这可能表示存在恶意行为，例如僵尸网络恶意软件或试图窃取数据的恶意软件、发送和接收垃圾邮件的恶意软件或某些其他类型的危害。

前提条件：此风险通告需要 36 天的历史记录，才能建立实体模型及预期流量配置文件。

关联观察结果：外部邮件客户端连接观察结果、历史异常值观察结果、新配置文件观察结果

后续步骤：参考支持性观察结果并确定外部邮件服务器是否符合预期和合法性。如果是这种情况，请确定实体增加了这些服务器的流量的原因。否则，请确定恶意行为的原因。隔离受影响的实体并删除所有恶意软件。确保网络上的其他实体不会受到类似的影响。

紧急配置文件

说明：某个高度敏感的实体具有符合新配置文件的流量。例如，某个开始接受 FTP 连接的实体可能正在暴露敏感数据。

前提条件：此风险通告需要 14 天的历史记录，才能建立实体模型并确定预期流量配置文件。

关联观察结果：新配置文件观察结果

后续步骤：参考支持性观察结果中实体的新流量配置文件，看它是否符合预期，特别是要考虑到之前的配置文件或角色。例如，如果某个实体已从 FTP 服务器重新定位为邮件服务器，这种行为上的转变是可以预计到的。如果不符合预期，请调查实体流量发生变化的原因，以及它是否为恶意流量。

Empire 命令和控制

说明：某个实体建立了新的周期性连接，这些连接似乎是 Empire PowerShell 命令和控制通道的一部分。此警报可能表示设备受到攻击。

前提条件：此风险通告需要 1 天的历史记录，才能建立实体模型并确定预期流量配置文件。

关联观察结果：心跳观察结果

后续步骤：在支持性观察结果中查看实体流量，确定与其建立心跳连接的实体，并确定流量是预期流量还是恶意流量。如果是恶意流量，请确定网络上的其他实体是否也受到类似影响。隔离这些实体并删除所有恶意软件。更新阻止列表和防火墙规则，以禁止命令和控制服务器访问您的网络。

异常域控制器

说明：此实体被标识为偏离其正常行为的域控制器。这可能表示存在滥用行为。例如，如果实体正在建立许多出站连接，则可能是数据泄露、僵尸网络恶意软件或可能是恶意 DNS 请求重定向的迹象。

前提条件：此风险通告需要 7 天的历史记录，才能确定正常实体流量配置文件。

关联观察结果：异常域控制器观察结果、新外部服务器观察结果、新高吞吐量连接观察结果、新配置文件观察结果

后续步骤：从风险通告和支持性观察结果中，查看实体的流量配置文件以及与其他实体的连接，确定其发送的流量类型，以及它是否具有恶意性质。确定是否已从您的网络中窃取数据；如果是，请确定数据类型以及针对这种情况的最佳修复方式。

访问尝试次数过多(外部)

说明：某个外部实体多次尝试访问此实体，且均失败。例如，如果某个远程实体反复尝试使用 SSH 或 Telnet 访问内部服务器，将触发此风险通告。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：多次访问失败观察结果

后续步骤：参考支持性观察结果，确保外部实体的行为异常且不符合预期。如果其行为正常且符合预期，请确定用户或计算机登录一直失败的原因，例如凭证已更改，但未向用户或计算机提供更新后的凭证。如果外部实体未知，请更新防火墙或安全组规则，以限制对远程控制协议的访问。如果此实体可能是恶意的，请更新阻止列表和防火墙规则，以禁止该实体访问您的网络。

网络打印机连接过多

说明：此实体向网络打印机发起的连接过多。此行为可能表示拒绝服务攻击，或尝试通过打印文档窃取数据。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：网络打印机连接过多观察结果

后续步骤：参考支持性观察结果，确定实体如何与网络打印机通信。如果通信是恶意的，请隔离实体并删除恶意软件。检查打印机作业队列，确定它们正在执行哪些操作。如果打印机的任务是打印机密文档，请清除队列。如果打印机的任务是将机密信息传输到外部实体，请断开打印机的互联网访问。根据需要从打印机中删除所有恶意软件。

GCP 云函数调用高峰

描述：GCP 云 函数被调用了记录的次数。

前提条件：此警报需要 14 天的历史记录，以确定函数的调用频率。此警报需要与 GCP 集成。

关联观察结果：GCP 云函数指标异常值观察结果

后续步骤：查看 GCP 云功能和预期代码。确定函数是否已损坏，或者是否有其他环境因素导致函数改变行为。如果调用高峰是良性的，思科建议暂停警报。

GCP Stackdriver Logging 监视列表命中

描述：Google 云平台 (GCP) Stackdriver Logs 报告了用户提供的监视列表中的事件。

前提条件：此风险通告需要 0 天的历史记录。此警报还需要与 GCP 集成并授予 Cisco Secure Cloud Analytics 访问 Stackdriver Logs 的权限。

关联观察结果：GCP 监视列表活动观察结果

后续步骤：查看支持观察结果，以确定生成事件的监视列表条目。根据需要进行补救。登录 GCP 并根据需要更新监视列表。

地理位置异常的 AWS API 使用情况

说明：在某个国家/地区，某个通常不访问 API 的远程主机已访问 AWS API。例如，从异常的外部 IP 访问云控制台会触发此警报。来自意外地理位置的用户访问 AWS API 可能表示恶意行为。

前提条件：此警报需要 14 天的历史记录，以便为访问部署中的 AWS API 的 IP 地址建立正常的地理位置。此警报也需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：参考支持性观察结果，确定实体采取的操作以及采取该操作的原因。如果该实体是预期的，但从另一个国家/地区访问互联网，请确认用户身份未受到危害，然后在该实体正在旅行的时间段内暂停警报。如果用户的身份被盗取，请立即禁用该用户账户。

地理位置异常的 Azure API 使用情况

说明：在某个国家/地区，某个通常不访问 API 的远程主机已访问 Azure API。例如，从异常的外部 IP 创建 IAM 角色会触发此警报。来自意外地理位置的用户访问 Azure API 可能表示恶意行为。

前提条件:此警报需要 14 天的历史记录,以便为访问部署中的 Azure API 的 IP 地址建立正常的地理位置。此警报需要 Azure 集成。

关联观察结果: Azure 异常活动观察结果

后续步骤: 参考支持性观察结果,确定实体采取的操作以及采取该操作的原因。如果实体是预期访问,则关闭警报(如果这是一次性访问),或者如果异常访问预期会持续一段时间,则暂停警报。如果访问是恶意的,请更新防火墙或安全组规则以阻止进一步访问,并确定对系统执行的操作。补救措施。

地理位置异常的远程访问

说明: 在某个国家/地区,某个通常不访问本地网络的远程主机已访问此实体。例如,如果某个本地服务器接受来自外部源的 SSH 连接,则将触发此风险通告。从异常地理位置进行的远程访问可能表示恶意访问。

前提条件:此风险通告需要 14 天的历史记录,才能建立足够的流量历史记录,并根据地理位置确定流量是否正常。

关联观察结果: 远程访问观察结果

后续步骤:参考支持性观察结果,确定实体采取的操作以及采取该操作的原因。如果实体符合预期,但从预期之外的另一个国家/地区访问互联网,请更新防火墙设置以允许此流量通过。如果这是恶意行为,请修复该操作,并更新阻止列表和防火墙规则,以禁止实体访问您的网络。

心跳连接计数

说明: 此实体已与许多远程实体建立新的周期性连接,这可能表示存在未经授权的 P2P 流量或僵尸网络活动。

前提条件:此风险通告需要 1 天的历史记录才能建立流量模型。

关联观察结果: 心跳观察结果

后续步骤:参考支持性观察结果,确定与受影响实体建立心跳连接的实体,并确认它们不是预期实体。了解周期性连接的用途,并更新防火墙和阻止列表规则以防止进一步访问。

高带宽单向流量

说明: 此实体已开始向新的远程主机发送大量数据。这可能表示存在滥用行为或配置错误。例如,恶意软件可能通过指示主机向易受攻击的服务发送大量数据,使受感染主机攻击网站。

前提条件: 此警报需要 0 天的历史记录。

关联观察结果: 新的高吞吐量连接观察结果

后续步骤:参考有关流量详细信息的支持性观察结果,确定实体发送大量流量的原因。如果允许流量,则暂停此主机的警报。如果这些流量未得到允许,请调查主机上负责发送恶意流量的软件。

高严重性云安全评估监视列表命中

描述：在 Cisco Secure Cloud Analytics监控的云环境中发现了云安全评估监视列表中的一个或多个高严重合规性故障。此警报可能表示环境不符合最佳实践。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 或 Azure 集成。

关联观察结果：合规性判定摘要观察结果、新合规性资源失败观察结果

后续步骤：点击警报中观察结果的 ID，了解有关合规性失败和补救后续步骤的详细信息，以解决失败问题。

ICMP 滥用

描述：设备向新的外部服务器发送异常大的 ICMP 数据包。此警报可能表示攻击者使用 ICMP 协议作为隐蔽的通信通道来窃取数据。

前提条件：此风险通告需要 0 天的历史记录。

关联观察结果：异常数据包大小观察结果、新外部服务器观察结果

后续步骤：参考支持观察结果，以确定实体将 ICMP 数据包发送到哪个外部服务器。查看实体的日志并确定实体发送 ICMP 数据包的原因，以及它是否是恶意行为。补救任何恶意行为。为防止将来可能发生的 ICMP 隧道泄露尝试，请更新防火墙规则以禁止外部 ICMP 流量。

IDS 紧急配置文件

描述：此实体在被 IDS 标记为可疑的同时显示出一种新的流量类型。

前提条件：此警报需要 14 天的历史记录，以建立足以确定实体何时开始传输不同流量类型的实体模型。此警报需要满足以下条件之一：

- 安全分析和日志记录 (SaaS) 通过思科防御协调器和 Secure Firewall 设备。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。
- Suricata IDS

关联观察结果：入侵检测系统通知观察结果、新配置文件观察结果

后续步骤：在支持观察结果中引用配置文件详细信息，并确定新的流量配置文件是否为恶意。如果是恶意软件，则隔离主机并删除违规软件。如果不合法，请为主机暂停此警报。

IDS 通知高峰

描述：此实体触发了 IDS 观察结果的突然增加。

前提条件：此警报需要 1 天的历史记录，才能建立正常 IDS 报告行为。此警报还需要满足以下条件之一：

- 安全分析和日志记录 (SaaS) 通过思科防御协调器和 Secure Firewall 设备。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_

Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

- Suricata IDS
- Zeek IDS

关联观察结果：入侵检测系统通知观察结果

后续步骤：参考支持性观察结果，以确定触发多个通知的原因。查看并纠正 IDS 通知。确定其他实体是否可能受到影响。根据需要更新防火墙和阻止列表规则。

入站端口扫描程序

说明：某个外部实体已通过端口扫描此实体。如果外部实体正在扫描网络内部的实体，它可能是在扫描未修补的漏洞或以其他方式渗透网络中的实体。

前提条件：此风险通告需要 1 天的历史记录，才能建立实体模型并确定正常行为。

关联观察结果：外部端口扫描程序观察结果

后续步骤：参考支持性观察结果，识别通过端口扫描内部实体的外部实体。确定这是由于计划内的渗透测试或其他预期行为而在执行扫描活动，还是一种恶意行为。如果是预期流量，则更新 IP 扫描程序和允许列表规则，以允许该流量通过。如果不是预期流量，则予以阻止。根据需要更新防火墙规则，包括端口访问。

内部连接峰值

说明：此实体的内部连接突然增加，这表明存在扫描活动。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：记录指标异常值观察结果

后续步骤：参考支持性观察结果，确定实体建立多个连接的原因。确定这是由于渗透测试或其他允许的目的而在执行扫描活动，还是一种恶意行为。根据需要修复此行为。

内部连接监视列表命中

描述：观察到两个不应通信的 IP 地址正在交换数据。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：内部连接监视列表观察结果

后续步骤：参考支持性观察结果，确定匹配的监视列表规则并分析流详细信息。如果允许此连接，请更新监视列表规则以允许此连接。

仅当用户输入分段规则时，系统才会生成此警报。

内部端口扫描程序

说明：此实体已在网络内部的实体上开始进行端口扫描。如果某个内部实体正在扫描网络内部的实体，这有可能是网络安全团队正在进行渗透测试，也有可能是网络上某个实体的恶意行为。

前提条件：此风险通告需要 7 天的历史记录，才能建立实体模型并确定正常的实体行为。

关联观察结果：内部端口扫描程序观察结果、端口扫描程序观察结果

后续步骤：参考支持性观察结果，了解扫描活动的类型。扫描活动通常与正在搜索数据或其他主机以使其受感染的受攻击主机有关。要获取更多背景信息，请搜索与系统大约在同一时间记录的实体相关的观察结果（例如监视列表交互）。这可能会提供有关该行为的其他信息。

无效 MAC 地址

描述：使用思科 ISE 遥测检测到具有未注册 Mac 地址的组织唯一标识符 (OUI) 的设备。这并不总是恶意的，但它可能表示有人试图绕过 Mac 访问控制（Mac 过滤），实施“中间人攻击”技术或损害其他防御功能。

前提条件：此风险通告需要 0 天的历史记录，才能建立实体模型并确定正常的实体行为。

关联观察结果：ISE 会话开始的观察结果

后续步骤：验证设备的类型，找到设备并确定 MAC 地址设置不正确的原因。如果不是故意更改 Mac 地址，请隔离设备并进一步调查。

ISE 越狱设备

描述：思科身份服务引擎 (ISE) 检测到已越狱的设备。此类设备应被视为不安全，因为它们更容易受到威胁。这不一定表示孤立的活动威胁，但可能会增加组织风险的漏洞。默认情况下，此警报处于禁用状态。如果需要，请确保启用此警报。

前提条件：此警报需要与 ISE集成。此风险通告需要 0 天的历史记录。

关联观察结果：ISE 会话开始的观察结果

后续步骤：越狱设备可以运行来自官方应用商店以外的未经授权来源的恶意软件。如果设备是公司所有，则将其与公司网络隔离并验证移动设备的策略。如果设备是专用设备，请验证其在移动设备管理系统中注册的原因，并将其与企业网络隔离。如果越狱是故意的，请与设备所有者联系。如果所有者不知道这一点，则可能表明移动设备中存在漏洞。建议在移动设备上重新安装操作系统。

来自可疑进程的 LDAP 连接

描述：检测到设备正在运行非标准 LDAP 进程。这可能表示存在凭证盗窃尝试。默认情况下，此警报处于禁用状态。如果需要，请确保启用此警报。

前提条件：此警报需要与 NVM 集成。此风险通告需要 0 天的历史记录。

关联观察结果：可疑终端活动观察结果

后续步骤：调查已执行的流程，并验证其使用是否符合业务需求。

LDAP 连接峰值

说明：设备尝试访问数量异常多的内部 LDAP 服务器。此风险通告可能表示存在恶意软件或滥用行为。

前提条件：此风险通告需要 9 天的历史记录，才能确定正常行为。

关联观察结果：IP 扫描程序观察结果

后续步骤：参考支持性观察结果，确定实体与多个 LDAP 服务器建立连接的原因，实体采取的操作类型，以及这是否是恶意行为。如果数据已泄露，请按照组织的准则处理数据泄露。根据需要隔离实体，以删除恶意软件。

低严重性云安全评估监视列表命中

描述：在 Cisco Secure Cloud Analytics监控的云环境中发现了云安全评估监视列表中的一个或多个低严重合规性故障。此警报可能表示环境不符合最佳实践。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 或 Azure 集成。

关联观察结果：合规性判定摘要观察结果、新合规性资源失败观察结果

后续步骤：点击警报中观察结果的 ID，了解有关合规性失败和补救后续步骤的详细信息，以解决失败问题。

检测到恶意进程

描述：正在运行的进程具有与已知恶意散列值列表中的一个匹配的散列值。

前提条件：此警报需要与 NVM 集成。此风险通告需要 0 天的历史记录。

关联观察结果：可疑终端活动观察结果

后续步骤：隔离终端并进行调查，以确定是否运行了恶意可执行文件。

恶意软件激增

描述：此实体触发了 IDS 观察结果的突然增加。

前提条件：此警报需要 1 天的历史记录，才能建立正常 IDS 报告行为。此警报还需要通过思科防御协调器将 安全分析和日志记录 (SaaS) 与 Secure Firewall 设备集成。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联观察结果：恶意软件事件观察结果

后续步骤：参考支持性观察结果，以确定触发多个恶意软件事件的原因。查看并修复恶意软件事件。确定其他实体是否可能受到影响。根据需要更新防火墙和阻止列表规则。

中严重性级别的云安全评估监控列表命中

描述：在 Cisco Secure Cloud Analytics监控的云环境中发现了云安全评估监视列表中的一个或多个中级严重合规性故障。此警报可能表示环境不符合最佳实践。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 或 Azure 集成。

关联观察结果：合规性判定摘要观察结果、新合规性资源失败观察结果

后续步骤：点击警报中观察结果的 ID，了解有关合规性失败和补救后续步骤的详细信息，以解决失败问题。

执行的可疑进程

描述：通过终端遥测在终端中检测到攻击性工具 Metasploit 的执行。

前提条件：此警报需要与 NVM 集成。此风险通告需要 0 天的历史记录。

关联观察结果：可疑终端活动观察结果

后续步骤：隔离终端并调查在终端上执行的漏洞攻击和负载。

Meterpreter 命令和控制成功

说明：设备建立了新的周期性连接，这些连接似乎是 Meterpreter 命令和控制通道的一部分。此警报可能表示设备受到攻击。

前提条件：此警报需要 1 天的历史记录，才能建立正常行为。

关联观察结果：心跳观察结果

后续步骤：在支持性观察结果中查看实体流量，确定与其建立心跳连接的实体，并确定流量是预期流量还是恶意流量。如果是恶意流量，请确定网络上的其他实体是否也受到类似影响。隔离这些实体并删除所有恶意软件。更新阻止列表和防火墙规则，以禁止命令和控制服务器访问您的网络。

缺少相扑逻辑日志

描述：在您的 Sumo Logic 数据库中找不到具有此角色的实体的一个或多个日志。这可能意味着您的一个 Sumo Logic 收集器配置错误或缺失。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 Sumo Logic 集成。

关联观察结果：Sumo Logic 日志观察结果

后续步骤：检查您的 Sumo Logic 收集器并检查其配置。如果无法从网络中检测到您的一个 Sumo Logic 收集器，请重新部署或验证其连接。

NetBIOS 连接峰值

说明：源尝试使用 NetBIOS 访问大量主机。这可能表示存在恶意软件或滥用行为。

前提条件：此风险通告需要 7 天的历史记录，才能建立实体流量模型并确定正常的流量行为。

关联观察结果：IP 扫描程序观察结果

后续步骤：参考支持性观察结果，确定主机并分析流量传输详细信息。NetBIOS 不是一种常用协议，因此任何连接峰值事件都有可能是恶意的。如果检测到此类事件，请查看哪些应用正在使用 NetBIOS，以及该流量是否合法。如果合法，请为主机暂停此风险通告。

网络群体峰值

说明：观察到在网络上通信的 IP 地址达到创记录的数量。这可能表示存在源地址欺骗行为或扫描活动。

前提条件：此风险通告需要 36 天的历史记录，以获得足够的天数来计算正在网络上通信的实体总数。

关联观察结果：群体峰值观察结果

后续步骤：参考与该风险通告相关的支持性观察结果，确定 IP 地址是否为合法实体。如果不合法，请查找欺骗性地址的来源，根据需要进行修复。

网络打印机连接过多

说明：此打印机发起的连接过多。这可能表示存在恶意行为，例如僵尸网络恶意软件感染。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：网络打印机连接过多观察结果

后续步骤：查看已建立的连接以及与打印机建立连接的实体。参考支持性观察结果，了解打印机建立的连接类型。如果这些连接指示打印机受到攻击，请隔离打印机，考虑删除并重新安装操作系统。

添加了新的 AWS Lambda 调用权限

描述：添加了从其他 AWS 服务、账户或组织调用 AWS Lambda 函数的新权限。从外部账户或组织访问可能是在尝试在您的 AWS 环境中实施后门。这可能是合法活动，但也可能表示攻击者尝试从 AWS 外部建立对账户的持久访问。

前提条件：此警报需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：使用关联的观察结果验证新创建的基于 Lambda 资源的策略的合法性。查看 CloudTrail 事件的响应字段，该字段将列出新权限。主体字段指向允许调用函数的 AWS 服务或账户。如果不合法，请撤销这些权限，并查看 CloudTrail 日志搜索创建这些权限的用户，以查看他们是否执行了其他可疑活动。

新 AWS 区域

描述：在以前未使用的区域中检测到 AWS 资源。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS CloudTrail 事件观察结果

后续步骤：找到 AWS 资源并确定它是否适用于您的 AWS 部署。如果 AWS 资源不是预期的，请根据需要进行补救。参考 AWS CloudTrail 事件观察结果，查看有关资源和配置的创建者的更多详细信息。

新的 AWS Route53 目标

描述：新的 AWS Route53 资源记录分配给之前未与 Route53 资源记录关联的实体。此风险通告需要 0 天的历史记录。新的 Route53 资源记录可能表示该实体尝试恶意重定

向流量。

前提条件:此风险通告需要 0 天的历史记录。此警报需要 AWS 集成,并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果: AWS CloudTrail 事件观察结果

后续步骤:参考警报和支持观察结果以收集有关实体的信息,然后确定它是否适用于您的网络。查看 AWS 中的日志,以确定实体表现出的行为。如果这是预期的实体,请更新您的配置以允许该实体。

新外部连接

描述:在基准期内,实体从未与组织外部进行双向通信,然后才第一次如此,这是行为偏差。

前提条件:此风险通告需要 35 天的历史记录,才能建立流量模型并确定预期的流量行为。

关联观察结果: 新外部连接观察结果

后续步骤:参考支持性观察结果和流量详细信息,确定流量是否合法或可疑。一些非常静态的实体偶尔会调用外部 IP(例如,检查软件更新的打印机)。在这种情况下,请暂停警报或将该外部 IP 范围添加到 VPN 子网。

新内部设备

说明:回溯期内未出现的新实体出现在受限子网范围内。

前提条件:此风险通告需要 21 天的历史记录,以了解网络上通常会出现哪些实体。此风险通告还需要在"子网配置"页面上选择**新内部设备**。

关联观察结果: 新内部设备观察结果

后续步骤:参考支持性观察结果,确定此实体是否为预期实体,它对您的网络而言是一个新实体。如果是预期实体,并且不是恶意的,则关闭风险通告;未来的新实体将继续生成风险通告。如果是可疑实体,则通过访问本地交换机确定 Mac 地址。

新 IP 扫描程序

说明:此实体已开始扫描本地 IP 网络。这可能表示,例如,攻击者正在进行侦测。

前提条件:此风险通告需要 7 天的历史记录,才能建立实体流量模型并确定正常的流量行为。

关联观察结果: IP 扫描程序观察结果

后续步骤:参考支持性观察结果,调查外部实体扫描网络的原因。确定这是由于渗透测试或其他预期行为而在执行扫描活动,还是一种恶意行为。如果是预期流量,则更新 IP 扫描程序和防火墙规则,以允许该流量通过。如果有可能是恶意流量,则搜索该实体或拥有该计算机的用户的关联观察结果,以确定导致该扫描活动的软件。

新的长会话(地理)

说明:此实体已与列入监视列表国家的主机建立长期连接。这些连接可能表明这些国家/地区的用户存在恶意行为。

前提条件:此警报需要 2 天的历史记录,以确定哪些连接已建立较长时间。您可以在 Cisco Secure Cloud Analytics Web 门户 UI 中配置添加到"国家/地区监视列表"的国家/地区。

关联观察结果:长时间会话观察结果

后续步骤:参考支持性观察结果,了解流量传输详细信息。通过从 IP 地址菜单中选择 **Talos 情报** 和 **滥用 IPDB**,调查外部 IP 地址的信誉。如果外部 IP 显示为恶意,请调查主机或使用安全组或防火墙规则阻止流量。

新远程访问

说明:在最近的历史记录中,第一次从远程主机访问了(例如,通过 SSH)此实体。此远程访问可能表示存在恶意行为,尤其是在预计该实体不接受来自外部实体的连接的情况下。

前提条件:此风险通告需要 36 天的历史记录,才能建立足够的流量历史记录和实体模型。

关联观察结果:远程访问观察结果

后续步骤:参考支持性观察结果,确定外部实体访问该实体的原因,以及访问形式是否合法。此外,还要(基于观察结果)确定在此次访问之前,此外部实体或其他外部实体是否曾多次尝试访问源实体。根据此信息更新防火墙和阻止列表规则。

新 SNMP 扫描

说明:此实体尝试使用 SNMP 访问大量主机。这可能表示恶意软件对网络进行了侦测。当恶意攻击者执行 SNMP 扫描时,可能会导致收集有关您的网络的信息或恶意实体配置更新。

前提条件:此风险通告需要 7 天的历史记录,才能建立实体流量模型并确定正常的流量行为。

关联观察结果:IP 扫描程序观察结果

后续步骤:参考支持性观察结果,确定此实体是否意在通过 SNMP 跟踪网络实体,以及此行为是否是恶意行为。如果该活动不是计划内的渗透测试或其他预期行为的一部分,则隔离该实体并修复问题。确定是否有任何实体受到影响(例如配置更新或安全设置受损),并修复所有问题。如果实体执行 SNMP 扫描是一种预期行为,则将该实体添加到扫描程序监视列表或暂停警报。

新异常 DNS 解析器

说明:此实体访问了一个不常用的 DNS 解析器。这可能表示配置错误或存在恶意软件。例如,攻击者可以使 DNS 解析器将热门网站重定向到提供其他恶意软件的域。

前提条件:此风险通告需要 7 天的历史记录,才能确定实体角色并为正常流量建模。

关联观察结果：异常 DNS 解析器观察结果

后续步骤：验证实体的配置，确保其配置了正确的 DNS 设置。如果配置正确，请确定正在执行 DNS 查找的软件。如果该流量被认为是恶意流量，则阻止外部 IP 地址。如果该流量是预期的，则暂停警报。

非服务端口扫描程序

说明：设备已开始扫描未与通用服务关联的端口上的本地网络。此警报可能表示攻击者正在网络内部扫描漏洞。

前提条件：此风险通告需要 9 天的历史记录，才能建立实体模型并确定正常行为。

关联观察结果：IP 扫描程序观察结果

后续步骤：参考支持性观察结果，调查外部实体扫描网络的原因。确定这是由于渗透测试或其他预期行为而在执行扫描活动，还是一种恶意行为。如果是预期流量，则更新 IP 扫描程序和防火墙规则，以允许该流量通过。如果有可能是恶意流量，则搜索该实体或拥有该计算机的用户的关联观察结果，以确定导致该扫描活动的软件。

出站 LDAP 连接峰值

说明：设备正在使用 LDAP 端口与大量外部主机通信。此风险通告可能表示存在受感染的主机或内部发起的端口扫描。

前提条件：此风险通告需要 0 天的历史记录。

关联观察结果：IP 扫描程序观察结果

后续步骤：参考支持性观察结果，确定源实体正在向哪些实体发送流量、流量类型，以及这是对实体角色或职责的更新，还是意外情况。如果这是意外情况，请修复问题。更新防火墙和阻止列表规则以阻止此访问。

出站 SMB 连接峰值

说明：此实体正在使用 SMB 端口与大量外部主机通信。这可能表示可能受感染的主机、外部发起的滥用（例如，欺骗攻击）或内部发起的端口扫描。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：IP 扫描程序观察结果

后续步骤：参考支持性观察结果，确定源实体正在向哪些实体发送流量、流量类型，以及这是对实体角色或职责的更新，还是意外情况。如果这是意外情况，请修复问题。更新防火墙和阻止列表规则以阻止此访问。

出站流量尖峰

描述：源开始向外部目标发送比以前更多的流量。以前从未出现过的大流量高峰可能表示存在恶意行为，例如数据泄露。即使此行为不是恶意的，也可能需要进行调查。

前提条件：此警报需要 14 天的历史记录，以建立具有足够信息的实体模型，以显示此实体发送的正常流量级别。

关联观察结果：历史异常值观察结果、记录指标异常值观察结果、记录配置文件异常值观察结果、新的大型连接(外部)观察结果

后续步骤：参考支持观察结果以确定流量的性质及其发送位置(例如，大型 Dropbox 上传)。如果流量可疑，请联系用户或计算机所有者，以确定流量被移至外部的原因。根据需要在边界阻止流量。

已创建许可 Amazon Elastic Kubernetes 服务集群

描述：已创建允许从任何主机访问的新 Amazon Elastic Kubernetes 服务集群。此警报可能表示敏感资源或数据存在风险。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：检查 Amazon Elastic Kubernetes 服务集群设置和网络安全设置，并在不影响业务需求的情况下尽可能限制访问。

许可 AWS S3 访问控制列表

描述：已创建允许对 S3 存储桶进行许可访问的新 ACL。这可能是配置错误，并可能导致对存储的数据进行未经授权的访问。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：检查访问控制列表并确定 S3 存储桶访问权限是否受到适当限制。如果配置错误，请更正条目。

已创建许可的 AWS 安全组

描述：已创建新的 AWS 安全组，允许从不安全端口上的任何主机进行访问。具有不安全端口的 VPC 安全组构成安全问题，应保护这些端口。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：使用 AWS 控制台或 AWS 可视化页面检查 AWS 安全组设置，然后根据需要限制访问。

持久性远程控制连接

说明：此实体正在通过远程桌面或 SSH 等远程控制协议接收来自新主机的持久连接。这可能表示防火墙规则或 ACL 过于宽松。

前提条件：此风险通告需要 7 天的历史记录，才能建立流量模型并确定正常的流量行为。

关联观察结果：新外部服务器观察结果、持久性外部服务器观察结果

后续步骤:调整防火墙或安全组规则,以防止恶意尝试重复访问该实体。通过检查 远程访问观察结果 或本地实体,确认该实体未遭到入侵。

端口 8888:从多个源连接

描述:多台设备将文件传输到在延迟端口上提供服务的主机。这可能表示存在前过滤尝试。

此警报仅在设备和主机为内部时适用,主要是在多个内部设备将文件传输到在延迟端口上提供服务的内部主机时。这可能表示存在泄露企图。默认情况下,此警报处于禁用状态。如果需要,请确保启用此警报。

前提条件:此警报需要与 NVM 集成。此风险通告需要 0 天的历史记录。

关联观察结果: 可疑终端活动观察结果

后续步骤:验证端口上的主机是否为合法服务器。

潜在数据泄露

说明: 此实体从一个不常与之通信的内部实体下载了大量数据。此后不久,该实体向外部实体上传了相近数量的数据。这可能表示未经授权的信息传输或其他恶意行为。默认情况下,此警报处于启用状态。

前提条件: 此警报需要 0 天的历史记录。

关联观察结果: 潜在数据转发观察结果

后续步骤:参考支持性观察结果来确定流量大小和客户端实体,以确定该行为是否是正常业务过程(例如新的计划备份)中的预期行为。如果是恶意行为,请确定传输的内容。遵循组织的数据泄露准则。

潜在数据库泄露

说明: 从数据库服务器向客户端传输了统计上数量异常的数据。这可能表示未经授权的信息传输或其他恶意行为。

前提条件:此风险通告需要 7 天的历史记录,以确定哪些实体通常用作数据库,以及它们的正常流量配置文件是什么。

关联观察结果: 新的高吞吐量连接观察结果

后续步骤:检查客户端实体,确定该行为是否是正常业务过程(例如新的计划备份)中的预期行为。如果是恶意行为,请确定传输的内容。遵循组织的数据泄露准则。

潜在的持久性尝试

描述:检测到设备应用了已知的持久性机制,例如建立用于网络访问的后台进程或从网络共享运行应用。默认情况下,此警报处于禁用状态。如果需要,请确保启用此警报。

前提条件:此警报需要与 NVM 集成。此风险通告需要 0 天的历史记录。

关联观察结果: 可疑终端活动观察结果

后续步骤: 调查已执行的流程,并验证其使用是否符合业务需求。

潜在的系统进程模拟

描述:执行了一个名称看起来像普通进程的进程,表明存在进程模拟。

前提条件:此警报需要与 NVM 集成。此风险通告需要 0 天的历史记录。

关联观察结果: 可疑终端活动观察结果

后续步骤: 验证它是否是已知的合法进程。否则,请隔离终端并验证是否已运行恶意可执行文件。

潜在有害的隐藏文件扩展名

描述: 此实体遇到具有潜在有害隐藏扩展名的文件。具有潜在有害扩展名的隐藏文件可能构成恶意软件。

前提条件:此风险通告需要 0 天的历史记录。此警报需要以下一项或多项:

- 安全分析和日志记录 (SaaS) 通过思科防御协调器和 Firepower 设备。有关详细信息,请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。
- 增强型 NetFlow。有关详细信息,请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。

关联观察结果: 多个文件拓展观察结果

后续步骤: 参考支持观察结果,以确定文件是否为恶意软件,或文件具有隐藏扩展名的原因。了解文件在网络上的传输位置,以及哪些实体可能受到恶意软件的感染。隔离受影响的实体并从中清除恶意软件。

潜在易受攻击的远程控制协议

描述: 使用较早版本的远程控制应用(例如 OpenSSH) 观察到此实体。它可能存在已知安全漏洞的风险。

前提条件:此风险通告需要 1 天的历史记录,建立使用远程控制应用的模型。此警报需要增强型 NetFlow。有关详细信息,请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。

关联观察结果: 不安全的传输协议观察结果

后续步骤: 参考支持性观察结果,以确定实体正在使用的应用,其建立的连接以及与哪个实体的连接。如果您的组织允许远程控制应用,请将应用更新到最新版本,并更新实体的安全设置以符合您组织的使用策略。如果您的组织不允许远程控制应用,请确定是由授权还是未授权的个人安装的,然后删除该应用。

协议伪造

说明: 观察到此实体在非标准端口上运行可能受限的服务(例如 SSH)。这可能表示规避安全控制措施。

前提条件:此风险通告需要 1 天的历史记录才能建立实体模型并查看哪些实体使用可能受限的服务。

关联观察结果：不安全的传输协议观察结果

后续步骤：参考支持性观察结果，确定实体为何使用异常协议/端口组合进行通信。如果认为存在安全风险，请更新防火墙和阻止列表规则，以防止使用此协议/端口组合进行进一步访问。

协议违规(地理)

说明：此实体尝试通过非法协议/端口组合(例如，端口 22 上的 UDP)与列入监视列表的国家/地区的主机通信。

前提条件：此风险通告需要 0 天的历史记录。您必须为国家/地区监视列表配置至少一个国家/地区。

关联观察结果：不良协议观察结果

后续步骤：参考支持性观察结果，确定实体为何使用异常协议/端口组合与列入监视列表的国家/地区的实体通信。确定通信中传输的内容。如果认为这是恶意的，请更新防火墙和阻止列表规则，以防止使用此协议/端口组合以及此地理位置进行进一步访问，除非出于业务原因允许这样做。

已创建公共 Amazon Route 53 托管区域

描述：已创建公共 Amazon Route 53 托管区域。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：如果您没有创建公共托管区域，这可能是恶意尝试将用户从 AWS 托管的资源重定向到非预期的外部资源。检查 AWS Cloudtrail 事件观察结果 以调查新区域。

面向公众的 IP 监视列表匹配

描述：在监视列表中发现了您的网络中面向公众的 IP(通过域名显式或隐式)。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：面向公众的 IP 监视列表匹配观察结果

后续步骤：参考支持性观察结果，并检查受影响的实体和日志信息。确定导致实体被添加到威胁情报监视列表的恶意软件或活动，并采取补救措施。

远程访问(地理)

说明：已从远程主机访问此实体，该主机位于列入监视列表的国家 。

前提条件：此警报需要 0 天的历史记录。此风险通告要求为国家/地区监视列表配置至少一个国家/地区。

关联观察结果：远程访问观察结果

后续步骤：参考支持性观察结果，以识别外部实体，以及外部实体如何与您的内部实体交互。确定该行为是否是恶意行为，是否泄露了任何数据，以及对内部实体采取的操作。如果需要，请添加额外的防火墙或安全组规则，以防止后续访问。

重复的 Umbrella Sinkhole 通信

说明：设备已与 Cisco Umbrella Sinkhole 建立周期性连接。此警报可能表示设备已被入侵。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：心跳观察结果、Umbrella Sinkhole 命中观察结果、

后续步骤：参考支持性观察结果，并检查受影响的实体和日志信息。确定实体与 Sinkhole 建立周期性通信的原因，并修复这种情况。

重复的监视列表通信

说明：此实体已与列入监视列表的 IP 建立周期性连接。这可能表示您的网络中存在恶意软件或受攻击的实体。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：监视列表交互观察结果、心跳观察结果

后续步骤：参考支持性观察结果，并检查受影响的实体和日志信息。确定实体建立周期性通信的原因，并修复这种情况。如有必要，请联系维护给定监视列表的组织，以获取有关如何修复这种情况的建议，或确保实体不再感染恶意软件。

角色违规

说明：此实体被标识为具有特定角色（例如，用户实体），但系统观察到它正以该角色的非典型方式（例如，SSH 服务器）运行。如果实体更改角色，则可能表示存在恶意行为，例如恶意软件更改了实体的运行方式。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：角色违规观察结果

后续步骤：参考支持性观察结果，确定新角色行为是否是预期行为以及正常业务过程的一部分。如果不是，请隔离该实体。如果是预期行为，则暂停风险通告。

已配置 S3 存储桶生命周期

描述：已创建新的 S3 存储桶生命周期配置，用于安排同时永久删除存储桶中的所有文件。此警报可能表示数据被破坏。

前提条件：此风险通告需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：AWS Cloudtrail 事件观察结果

后续步骤：查看随附的观察结果，并确保授权人员根据适用的程序有目的地执行此操作，并且不会造成安全风险。如果不是，请恢复操作并验证所使用的凭证是否未受到危害。

SMB 连接异常值

描述：设备与异常大的一组 SMB 对等体交换了异常大的 SMB 流量。此警报可能表示网络侦查活动。

前提条件：此风险通告需要 36 天的历史记录，才能建立实体流量模型并确定正常的流量行为。

关联观察结果：历史异常值观察结果

后续步骤：参考支持性观察结果，确定实体与多个 SMB 服务器建立连接的原因，实体采取的操作类型，以及这是否是恶意行为。

SMB 连接峰值

说明：此实体尝试访问数量异常多的 SMB 服务器。这可能表示存在恶意软件或滥用行为。SMB 主要用于文件共享，但也可用于访问网络打印机或浏览网络上的其他主机，这可能表示存在数据泄露或网络资源滥用行为。

前提条件：此风险通告需要 9 天的历史记录，才能建立实体流量模型并确定正常的流量行为。

关联观察结果：IP 扫描程序观察结果

后续步骤：参考支持性观察结果，确定实体与多个 SMB 服务器建立连接的原因，实体采取的操作类型，以及这是否是恶意行为。如果数据已泄露，请按照组织的准则处理数据泄露。根据需要隔离实体，以删除恶意软件。

SMB|RDP：与多个目标的连接

描述：主机已使用 SMB 将文件传输到多个目标主机，并使用 RDP 连接到这些主机。这可能表示横向移动。

前提条件：此警报需要与 NVM 集成。此风险通告需要 1 天的历史记录。

关联观察结果：可疑终端活动观察结果

后续步骤：验证此类终端的内部连接是否正常。

失效 AWS 访问密钥

描述：AWS IAM 访问密钥超出可配置的期限。这违反了最佳实践。

前提条件：此风险通告需要 30 天的历史记录。此警报还需要 AWS 集成。

关联观察结果：AWS 架构合规性观察结果

后续步骤：验证 IAM 用户账户是否仍应具有访问权限。调整 IAM 策略，确保更频繁地轮换密钥。

静态设备连接偏差

描述：设备在网络上通常是静态的 - 它与相同的设备通信，每个设备具有类似的流量模式。最近，此设备偏离了其规范，包括与新的外部主机通信。此警报可能表示误用或危害。

前提条件:此风险通告需要 1 天的历史记录,才能建立实体模型并确定正常流量和行为。

关联观察结果: 历史异常值观察结果 和 新的外部连接观察结果

后续步骤:参考支持性观察结果,了解扫描实体的正常通信。确定偏差是良性还是恶意行为。补救任何恶意行为。

静态设备偏差

描述: 此实体在网络上通常是静态的,在相同的端口上通信或与相同的实体通信,每天的流量模式类似。此实体最近偏离了其规范,这可能是滥用的迹象。默认情况下,此警报处于启用状态。

前提条件:此风险通告需要 35 天的历史记录,才能建立实体模型并确定正常流量和行为。

关联观察结果: 历史异常值观察结果、静态连接集偏差观察结果、静态端口集偏差观察结果

后续步骤:参考支持性观察结果,了解扫描实体的正常通信。确定偏差是良性还是恶意行为。补救任何恶意行为。

疑似僵尸网络交互

说明: 此实体与僵尸网络关联的 IP 地址交换流量,或尝试解析僵尸网络关联的域名。

前提条件:此警报需要 1 天的历史记录才能建立实体模型。

关联观察结果: 监视列表交互观察结果

后续步骤: 隔离实体,并删除所有恶意软件。更新阻止列表和防火墙规则,以禁止僵尸网络实体访问您的网络。参考支持性观察结果,根据实体可能已建立的通信确定网络上是否有任何其他实体也受到感染,并根据需要进行修复。

疑似加密货币活动

说明: 根据 Talos 情报和其他来源,源与多个已知正在运行加密货币节点的地址交换了大量流量。此行为可能表示实体正在用于挖掘加密货币。

前提条件: 此警报需要 0 天的历史记录。

关联观察结果: 监视列表交互观察结果

后续步骤: 隔离实体,并删除所有加密货币挖掘软件(无论是恶意软件还是由用户安装的软件)。

可疑恶意 URL

描述: 实体与可疑的恶意 URL 通信。这可能表示对实体的恶意访问或危害。

前提条件: 此风险通告需要 0 天的历史记录。此警报需要满足以下条件之一:

- 安全分析和日志记录 (SaaS) 通过思科防御协调器和 Firepower 设备。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。
- 增强型 NetFlow。有关详细信息，请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。

关联观察结果：可疑的恶意 URL 观察结果

后续步骤：参考支持性观察结果，确定实体访问的 URL。确定实体是否受到攻击，如果实体受到感染，则从实体中删除恶意软件。更新阻止列表和防火墙规则以禁止访问 URL。

可疑网络钓鱼域

描述：实体对可疑的网络钓鱼域执行了成功的 DNS 查找。

前提条件：此风险通告需要 0 天的历史记录。此警报需要满足以下条件之一：

- 安全分析和日志记录 (SaaS) 通过思科防御协调器和 Firepower 设备。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。
- 增强型 NetFlow。有关详细信息，请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。
- 来自 SPAN 或镜像端口的 DNS 日志。

关联观察结果：疑似网络钓鱼域观察结果

后续步骤：参考支持性观察结果，以确定实体及其连接的域。确定这是否由恶意软件或恶意行为而导致，并修复问题。根据需要更新防火墙和阻止列表规则。

查看实体的活动，并确定它与计划内的渗透测试一致，还是与恶意行为一致。确定恶意行为的来源，并修复问题。根据需要更新防火墙和阻止列表规则。

疑似端口滥用(外部)

说明：此实体正在与异常端口范围内的外部主机通信。这可能表示外部发起的滥用(例如，欺骗攻击)或内部发起的端口扫描。

前提条件：此警报需要 1 天的历史记录才能建立实体模型。

关联观察结果：端口扫描程序观察结果、外部端口扫描程序观察结果

后续步骤：参考支持性观察结果以查看实体的活动，并确定它与计划内的渗透测试一致，还是与恶意行为一致。确定恶意行为的来源，并修复问题。根据需要更新防火墙和阻止列表规则。

疑似远程访问工具心跳

说明：在此设备上发现了签名与远程访问工具(例如 RevengeRAT)匹配的流量。此警报可能表示设备受到攻击。

前提条件：此风险通告需要 0 天的历史记录。

关联观察结果：可疑网络活动观察结果

后续步骤：确保此设备应用了最新的安全更新，并调查设备是否存在受攻击迹象。

疑似 Zerologon RPC 漏洞攻击尝试

说明：在此设备上发现了签名与 Zerologon RPC 漏洞攻击匹配的流量。此风险通告使用可疑网络活动观察结果，可能表示设备成为了漏洞攻击的目标。

前提条件：此风险通告需要 0 天的历史记录。

关联观察结果：可疑网络活动观察结果

后续步骤：确保此设备应用了最新的安全更新。遵循 CVE-2020-1472中的缓解步骤。

可疑的 DNS Over HTTPS 活动

描述：发现内部服务器通过 HTTPS 服务器与已知 DNS 交换流量。此警报可能表示有人企图规避基于 DNS 的安全措施。

前提条件：此风险通告需要 7 天的历史记录。

关联观察结果：监视列表交互观察结果

后续步骤：查看支持观察结果，以验证是否有意使用 DNS over HTTPS，以及它是否属于恶意行为。补救任何恶意行为。

可疑的域查找失败

描述：此实体尝试将多个通过算法生成的域（例如 rgkte-hdvj.cc）解析为一个 IP 地址。这可能表示存在恶意软件感染或尝试在生成的域中使用命令和控制服务器创建僵尸网络。

前提条件：此警报需要 0 天的历史记录。此警报需要来自 SPAN 或镜像端口的 DNS 日志。

关联观察结果：域生成算法观察结果

后续步骤：参考支持观察结果并确定实体是否感染了恶意软件或域查找的原因。根据需要删除违规软件。检查网络上可能表现出类似行为的其他实体，并进行修复。

可疑进程路径

描述：在终端上从不应包含可执行文件的目录执行进程。

前提条件：此警报需要与 NVM 集成。此风险通告需要 0 天的历史记录。

关联观察结果：可疑终端活动观察结果

后续步骤：隔离终端并调查是否在非标准目录中下载并执行了可执行文件。

可疑 SMB 活动

说明：多个新 SMB 服务器已与常见 SMB 对等体通信。这可能表示存在恶意软件或滥用行为。

前提条件：此风险通告需要 14 天的历史记录。

关联观察结果：可疑 SMB 活动观察结果

后续步骤：参考支持性观察结果，检查实体的流量配置文件，以确定是否有进一步的证据表明存在僵尸网络活动或其他恶意行为。检查网络上可能表现出类似行为的其他实体，并进行修复。

可疑用户代理

描述：发现设备与使用可疑用户代理字符串的设备通信。此警报可能表示恶意软件（例如，Log4J 漏洞攻击）或滥用。

前提条件：此警报需要 0 天的历史记录。此警报需要防火墙通过思科防御协调器与 安全分析和日志记录 (SaaS) 集成提供用户代理数据。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联观察结果：异常用户代理观察结果

后续步骤：参考支持性观察结果，确定用户代理字符串是否会影响服务器（如 Log4J），实体采取的操作类型，以及这是否是恶意行为。如果数据已泄露，请按照组织的准则处理数据泄露。根据需要隔离实体，以删除恶意软件。

Talos 情报监视列表命中

说明：此实体与 Cisco Talos IP 阻止列表上的多个地址交换了大量流量。

前提条件：此警报需要 0 天的历史记录。

关联观察结果：监视列表交互观察结果

后续步骤：隔离实体，并删除所有恶意软件。通过从菜单中选择 **Talos 情报**来调查外部 IP 地址，以查看流量指示的内容并采取适当的修复操作。

TrickBot 锚点 DNS 隧道

描述：设备查找与 AnchorDNS 使用的算法（TrickBot 恶意软件使用的隧道方法）匹配的域。此警报可能表示存在恶意软件感染或僵尸网络活动。

前提条件：此风险通告需要 0 天的历史记录。此警报需要来自 SPAN 或镜像端口的 DNS 日志。

关联观察结果：TrickBot 锚点 DNS 隧道活动观察结果

后续步骤：隔离实体，并删除所有恶意软件。更新阻止列表和防火墙规则，以禁止任何僵尸网络实体访问您的网络。参考支持性观察结果，根据实体可能已建立的通信确定网络上是否有任何其他实体也受到感染，并根据需要进行修复。

未使用的 AWS 资源

描述：此 AWS 资源最近未发现任何活动。这可能是预期行为，因为资源不再相关。

前提条件：此风险通告需要 0 天的历史记录。

关联观察结果：未使用的 AWS 资源观察结果

后续步骤：确定您是否需要此 AWS 资源，或者是否可以将其删除。如果它应该在运行或以其他方式表现出活动，请检查 AWS 资源并确定其处于非活动状态的原因。根据需要进行补救。

异常 DNS 连接

说明：此实体访问了异常的 DNS 解析器，然后与远程实体建立了周期性连接。此行为可能表示流量的恶意重定向或实体上的恶意软件感染。

前提条件：此警报需要 1 天的历史记录才能建立实体模型。

关联观察结果：异常 DNS 解析器观察结果、心跳观察结果

后续步骤：参考支持性观察结果，确定此行为是否是恶意行为，并删除存在的恶意软件。更新阻止列表和防火墙规则以禁止访问。

异常外部服务器

说明：此实体已反复与具有可疑流量配置文件的新外部服务器通信。这可能表示，例如，某个新软件正在充当外部实体（如系统日志或 TeamViewer）的服务器。

前提条件：此警报需要 14 天的历史记录，才能建立正常流量模式并确定预期的外部实体流量。

关联观察结果：新外部服务器观察结果、持久性外部服务器观察结果

后续步骤：参考支持性观察结果，检查实体的流量配置文件，以确定流量的性质以及是否允许该流量通过。隔离实体并删除违规软件。确定网络上的其他实体是否表现出类似行为，并修复该行为。

来自新外部服务器的异常文件扩展名

描述：实体和新的外部服务器之间交换了最近未发现的新文件扩展名。这可能表示恶意软件尝试与其命令和控制中心通信。

前提条件：此警报需要 1 天的历史记录才能建立实体模型。此警报需要防火墙通过思科防御协调器与 安全分析和日志记录 (SaaS) 集成提供 URL 数据。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联观察结果：新外部服务器观察结果、新文件扩展观察结果

后续步骤：参考支持观察结果，以确定与哪个外部服务器交换了具有此新扩展名的文件。查看实体的日志并确定实体交换此文件的原因，以及它是否属于恶意行为。补救任何恶意行为。

异常大的 EC2 实例

描述：已创建异常大的 EC2 实例。此警报可能表示攻击者已部署大型 ec2 实例以进行资源劫持。

前提条件：此警报需要 0 天的历史记录。此警报需要 AWS 集成，并允许 Cisco Secure Cloud Analytics 读取 CloudTrail 日志。

关联观察结果：异常 EC2 实例观察结果

后续步骤:检查有问题的新设备,并确定它们是否已合法部署。

用户监视列表命中

描述:此实体与用户提供的监视列表中的 IP 地址交换了流量,或尝试解析用户提供的监视列表中的域名。

前提条件:此警报需要 0 天的历史记录。

关联观察结果:监视列表查找观察结果、监视列表交互观察结果

后续步骤:参考支持性观察结果,检查实体的流量配置文件,以确定行为是否为恶意行为。根据需要更新防火墙和阻止列表规则。

易受攻击的传输安全协议

描述:观察到此实体使用不安全的 SSL/TLS 协议版本。

前提条件:此警报需要 1 天的历史记录才能建立实体模型。此警报需要增强型 NetFlow。有关详细信息,请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。

关联观察结果:不安全的传输协议观察结果

后续步骤:参考支持观察结果并查看使用不安全传输协议的应用。如果是本地应用,请将其更新为安全版本。如果它在您的网络外部,请确定应用是否存在安全风险,并根据需要使用防火墙规则阻止访问。

监视列表命中

描述:此实体与监视列表中的 IP 地址交换了流量,或尝试解析监视列表中的域名。Cisco Secure Cloud Analytics 引擎包括多个内置监视列表。

前提条件:此警报需要 0 天的历史记录。

关联观察结果:监视列表查找观察结果、监视列表交互观察结果

后续步骤:参考支持性观察结果,检查实体的流量配置文件,以确定行为是否为恶意行为。根据需要更新防火墙和阻止列表规则。

蠕虫传播

说明:先前扫描的设备开始扫描本地 IP 网络。此警报可能表示蠕虫正在网络内部传播。

前提条件:此风险通告需要 9 天的历史记录,才能确定正常行为。

关联观察结果:蠕虫传播观察结果

后续步骤:参考支持性观察结果,调查内部实体扫描网络的原因。确定这是由于渗透测试或其他预期行为而在执行扫描活动,还是一种恶意行为。如果是预期流量,则更新 IP 扫描程序和防火墙规则,以允许该流量通过。如果有可能是恶意流量,则搜索该实体或拥有该计算机的用户的关联观察结果,以确定导致该扫描活动的软件。

观察结果说明

Amazon GuardDuty DNS 请求结果观察结果

描述：Amazon GuardDuty 报告了可疑的 DNS 请求。

先决条件：此观察结果需要 AWS 集成并启用 GuardDuty。

Amazon GuardDuty 网络连接结果观察

描述：Amazon GuardDuty 报告了可疑的网络连接。

先决条件：此观察结果需要 AWS 集成并启用 GuardDuty。

Amazon Inspector 发现观察结果

描述：报告了 AWS 资源的调查结果。

先决条件：此观察结果需要 AWS 集成并启用检查器。

关联警报：AWS Inspector 调查结果警报

异常配置文件观察结果

说明：一个或多个实体首次使用与网络中常见行为不同的配置文件(例如，数量异常多的实体首次使用该配置文件发送异常流量)。

前提条件：无。

关联警报：异常 AWS 工作空间警报、异常 Mac 工作站、异常 Windows 工作站警报

异常用户代理观察结果

描述：向设备发送了包含异常用户代理字符串的流量。这可能表明存在尝试的 Log4J 漏洞攻击或其他恶意活动。

先决条件：此观察结果需要通过思科防御协调器与 安全分析和日志记录 (SaaS) 集成。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联风险通告：可疑的用户代理警报

AWS API 监视列表访问观察结果

描述：已从监视列表中的 IP 访问 AWS API。可能需要检查来自监视列表上的实体的 API 访问，以确定是否存在恶意行为。

先决条件：此观察结果需要 AWS 集成并启用 CloudTrail。

关联警报：AWS API 监视列表 IP 命中警报

AWS 架构合规性观察结果

描述：检测到可能违反 AWS“架构良好”准则的 AWS 资源。

先决条件：此观察结果需要 AWS 集成。

关联警报：过时的 AWS 访问密钥警报

AWS CloudTrail 事件观察结果

描述：为实体报告的 AWS CloudTrail 事件。

先决条件：此观察结果需要 AWS 集成并启用 CloudTrail。

关联警报：AWS 控制台登录失败警报、AWS 检测器修改警报、AWS EC2 启动脚本修改警报、AWS ECS 凭证访问警报、AWS IAM Anywhere 信任锚点创建警报、AWS 日志记录已删除警报、AWS 重复 API 失败警报、使用的 AWS 根账户警报、AWS 快照泄露警报、AWS 临时令牌持久性警报、地理位置异常的 AWS API 使用警报、新 AWS Lambda 调用权限添加的警报、新 AWS 区域警报、新 AWS Route53 目标警报、许可的 Amazon Elastic Kubernetes 服务集群创建警报、许可的 AWS S3 访问控制列表警报、许可的 AWS 安全组创建警报、公共 Amazon Route 53 托管区域创建警报、S3 存储桶生命周期配置警报

AWS 配置合规性观察结果

描述：为 AWS 资源报告配置合规性。

先决条件：此观察结果需要 AWS 集成、用于将配置更改传输到 SNS 主题的 AWS 配置、用于发送配置更改的 SQS 队列，以及用于检索消息的 Cisco Secure Cloud Analytics 中其他配置。

关联警报：角色违规风险通告

AWS 配置更新观察结果

描述：已为 AWS 资源报告更新的配置。

先决条件：此观察结果需要 AWS 集成、用于将配置更改传输到 SNS 主题的 AWS 配置、用于发送配置更改的 SQS 队列，以及用于检索消息的 Cisco Secure Cloud Analytics 中其他配置。

关联警报：角色违规风险通告

AWS Lambda 指标异常值观察结果

描述：AWS Lambda 函数的其中一个指标存在异常活动，例如调用次数。

先决条件：此观察结果需要 AWS 集成和至少一个 Lambda 函数。

关联警报：AWS Lambda 调用高峰警报、AWS Lambda 持久性警报

AWS 多因素身份验证更改观察结果

描述：多因素身份验证已从用户账户中删除。

先决条件：此观察结果需要 AWS 集成并启用 CloudTrail。

关联警报：AWS 多因素身份验证更改警报

AWS 新用户操作观察结果

描述：CloudTrail 记录了 AWS 用户第一次执行操作。

先决条件：此观察结果需要 AWS 集成并启用 CloudTrail。

使用的 AWS 根账户观察结果

描述：已使用 AWS 根账户执行操作。

先决条件：此观察结果需要 AWS 集成并启用 CloudTrail。

关联警报：AWS 根账户已用警报

Azure Advisor 建议观察结果

描述：Azure 顾问为 Azure 资源管理器 (ARM) 资源生成了建议。

先决条件：此观察结果需要 Azure 集成和至少一个网络安全组或存储帐户。

关联警报：Azure 顾问监视列表警报

Azure 公开服务观察结果

描述：设备具有公开暴露的服务，攻击者可能会使用该服务收集有关基础设施的信息或获取对数据的访问权限。

先决条件：此观察结果需要 Azure 集成。

关联警报：Azure 暴露的服务警报

Azure 函数指标异常值观察结果

描述：Azure Functions 的其中一个指标出现异常活动。

先决条件：此观察结果需要 Azure 集成。

关联警报：Azure 函数调用高峰警报

Azure 许可安全组观察结果

描述：与网络安全组相关的安全规则设置了过多权限，允许访问整个互联网（例如 *、0.0.0.0、:0/0），而不是更保守的允许 IP 地址的明确列表

先决条件：此观察结果需要 Azure 集成和至少一个网络安全组或。

关联警报：Azure 许可安全组警报

Azure 许可存储设置观察结果

描述：Azure 存储设置过于宽松。

前提条件：此观察结果需要 Azure 集成和至少一个存储帐户。

关联警报：Azure 许可存储帐户警报

Azure 安全事件观察

描述：已生成 Azure 安全中心警报。

前提条件：此观察结果需要 Azure 集成、Azure 安全中心、标准层和 Azure 活动日志

关联警报：Azure 安全事件警报

Azure 异常活动观察结果

描述：在 Azure 活动日志中检测到异常活动。

前提条件：此观察结果需要 Azure 集成和 Azure 活动日志。

关联警报：Azure 活动日志 IP 监视列表命中、Azure 活动日志监视列表命中警报、Azure 防火墙删除警报、Azure 密钥保管库删除警报、Azure 网络安全组删除警报、Azure OAuth 绕行警报、Azure 资源组删除警报、Azure 数据传输到云账户警报、地理位置异常 Azure API 使用警报

未使用位置观察中的 Azure VM

描述：已生成 Azure 安全中心警报。

前提条件：此观察结果需要 Azure 集成，并授予 Cisco Secure Cloud Analytics “监控读者”角色查看 Azure 订用的权限。

关联警报：未使用位置警报中的 Azure 虚拟机

不良协议观察结果

说明：实体在标准端口上使用非标准协议(例如，在端口 22 上使用 UDP)。

前提条件：无

关联风险通告：协议违规(地理)风险通告

集群更改观察结果

描述：实体的配置文件集与该实体最近未关联的其他实体的配置文件集类似。

前提条件：无。

合规性判定摘要观察结果

描述：检测到违反合规性框架建议的云资源。

前提条件：此观察结果需要与云提供商集成以进行云安全状态管理。

关联警报：严重性级别云安全评估监视列表命中警报、高严重性云安全评估监视列表命中警报、低严重性云安全评估监视列表命中警报、中严重性云安全评估监视列表命中警报

已确认威胁指标匹配 - 域观察结果

描述：某个实体解析了列为已知威胁的 IOC 的域。

前提条件：此观察结果需要通过思科防御协调器与安全分析和日志记录 (SaaS) 集成。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联警报：已确认的威胁监视列表命中警报

已确认威胁指标匹配 - 主机名观察结果

描述：与列为已知威胁的 IOC 的主机名交互的实体。此观察结果使用来自增强型 NetFlow 的信息。

前提条件：此观察结果需要增强型 NetFlow。有关详细信息，请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。

关联警报：已确认的威胁监视列表命中警报

已确认威胁指标匹配 - IP 观察结果

描述：与列为已知威胁的 IOC 的 IP 地址通信的实体。

前提条件：无。

关联警报：已确认的威胁监视列表命中警报

已确认威胁指标匹配 - URL 观察结果

描述：与列为已知威胁的 IOC 的 URL 交互的实体。此观察结果使用来自增强型 NetFlow 的信息。

前提条件：此观察结果需要满足以下条件之一：

- 增强型 NetFlow。有关详细信息，请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。
- 安全分析和日志记录 (SaaS) 通过思科防御协调器。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联警报：已确认的威胁监视列表命中警报

国家/地区集偏差观察结果

说明：实体与一组不同于以往的国家/地区通信。

前提条件：无。

关联风险通告：国家/地区集偏差风险警报

域生成算法观察结果

描述：实体尝试联系算法生成的域（例如，qhjvd-hdvj.cc）。

前提条件：无。

关联警报：可疑域查找失败警报

域生成算法成功观察结果

描述：实体已成功将算法生成的域(例如 rgkte-hdvj.cc)解析为 IP 地址。

前提条件：无。

关联警报：域生成算法成功查找警报

通过下载观察结果驱动

描述：实体在外部主机初始访问后从远程主机下载了大量数据，这可能表示无意中下载了恶意负载。

前提条件：无。

关联警报：无。

异常域控制器观察结果

说明：域控制器实体与异常外部端口通信。

前提条件：无。

关联风险通告：异常域控制器风险通告

网络打印机连接过多观察结果

说明：实体向网络打印机发起的连接过多。

前提条件：无。

关联风险通告：网络打印机连接过多风险通告

外部邮件客户端连接观察结果

说明：实体开始与很多外部邮件服务器通信。

前提条件：无。

相关警报：垃圾邮件警报

外部端口扫描程序观察结果

说明：本地网络上的实体扫描了远程 IP 地址或被远程 IP 地址扫描。

前提条件：无。

关联风险通告：入站端口扫描程序风险通告、疑似端口滥用(外部)风险通告

GCP 云函数指标异常值观察结果

描述：GCP 云函数的其中一个指标出现异常活动。

前提条件：此观察结果需要与 Google 云平台 (GCP) 集成。

关联警报：GCP 函数调用高峰警报

GCP 监视列表活动观察结果

描述：在 GCP Stackdriver 日志中检测到监视列表活动。

前提条件：此观察结果需要与 Google 云平台 (GCP) 集成，并具有访问 Stackdriver Logs 的 Cisco Secure Cloud Analytics 权限。

相关警报：GCP Stackdriver Logging 监视列表命中警报

地理监视列表观察结果

描述：与列入观察名单的地理区域通信的实体。在调查地理监视列表观察结果时，除了国家/地区代码外，您现在还可以按国家/地区名称过滤观察结果列表。在“观察”>“所选观察结果”页面中向下透视或直接调查“地理观察列表”后，请使用此过滤器。

前提条件：无。

心跳观察结果

说明：实体与远程主机保持心跳连接。

前提条件：无。

关联警报：Empire 命令和控制警报、心跳连接计数警报、Meterpreter 命令和控制成功警报、重复的 Umbrella Sinkhole 通信警报、重复的观察列表通信警报、异常 DNS 连接警报

历史异常值观察结果

描述：源的其中一个指标与其历史基准有显着偏差。此观察结果可能是预期的或有意的，但也可能表示恶意行为。

前提条件：无。

关联警报：出勤丢弃警报、垃圾邮件警报、出站流量高峰警报、SMB 连接异常警报、静态设备连接偏差警报、静态设备偏差警报

不安全的传输协议观察结果

描述：具有 加密流量分析 功能的网络资源使用不安全的传输协议观察到源。

前提条件：此观察结果需要增强型 NetFlow。有关详细信息，请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。

关联警报：潜在易受攻击的远程控制协议警报、协议伪造警报、易受攻击的传输安全协议警报

内部连接监视列表观察结果

描述：检测到两个内部 IP 终端之间禁止通信。

前提条件：无。

关联警报：内部连接监视列表警报

内部端口扫描程序观察结果

说明：实体扫描了大量端口。

前提条件：无。

关联警报：内部端口扫描程序风险通告

入侵检测系统通知观察结果

描述：IDS 看到与可疑签名匹配的流量。

前提条件：此观察结果需要满足以下条件之一：

- 安全分析和日志记录 (SaaS) 通过思科防御协调器。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。
- Suricata IDS
- Zeek IDS

关联风险通告：IDS 紧急配置文件警报、IDS 通知尖峰警报

IP 扫描程序观察结果

说明：某个实体扫描了大量实体。

前提条件：无。

关联警报：LDAP 连接峰值警报、NetBIOS 连接峰值警报、新 IP 扫描程序警报、新 SNMP 扫描警报、非服务端口扫描程序警报、出站 LDAP 峰值警报、出站 SMB 峰值警报、SMB 连接峰值警报

ISE 会话已启动观察结果

描述：已在 思科身份服务引擎 (ISE)上创建新的用户会话。

先决条件：此观察结果需要 思科身份服务引擎 (ISE)集成。

关联警报：异常 ISE 用户警报

ISE 可疑活动观察结果

描述：在思科 ISE 上检测到可疑活动。

先决条件：此观察结果需要 思科身份服务引擎 (ISE)集成。

长会话观察

描述：实体与外部 IP 地址保持长期会话。

前提条件：无。

关联警报：新的长时间会话(地理)警报

恶意软件事件观察

描述：从实体检测到恶意软件活动

前提条件：此观察结果需要通过思科防御协调器与 安全分析和日志记录 (SaaS) 集成。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联警报：恶意软件高峰警报

多次访问失败观察结果

说明：实体多次尝试访问应用（例如，FTP、SSH、RDP）失败。

前提条件：无。

关联警报：访问尝试次数过多（外部）风险通告

多个文件扩展名观察结果

描述：此实体交换了具有多个扩展名的文件。

先决条件：此观察结果需要通过思科防御协调器与 安全分析和日志记录 (SaaS) 集成。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联警报：可能有害的隐藏文件扩展名警报

网络打印机连接过多观察结果

说明：网络打印机向其他实体发起的连接过多。

前提条件：无。

关联警报：网络打印机连接过多风险通告

新的合规性资源失败观察结果

描述：检测到在前一天合规时违反合规性框架建议的云资源。

前提条件：此观察结果需要与云提供商集成以进行云安全状态管理。

关联警报：严重性级别云安全评估监视列表命中警报、高严重性云安全评估监视列表命中警报、低严重性云安全评估监视列表命中警报、中严重性云安全评估监视列表命中警报

新外部连接观察结果

描述：与外部实体通信的通常可预测的本地实体。

前提条件：无。

关联警报：新外部连接警报、静态设备连接偏差警报

新外部服务器观察结果

说明：实体开始与外部服务器通信。

前提条件：无。

关联警报：异常域控制器警报、ICMP 滥用警报、持久性远程控制连接警报、异常外部服务器警报、来自新外部服务器的异常文件扩展名

新文件扩展名观察结果

描述：已交换新的文件扩展名。

前提条件：此观察结果需要通过思科防御协调器与 安全分析和日志记录 (SaaS) 集成。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联警报：潜在有害的隐藏文件扩展名警报、来自新外部服务器的异常文件扩展名警报

新的高吞吐量连接观察结果

说明：实体与新主机交换了大量流量。

前提条件：无。

关联警报：异常域控制器警报、高带宽单向流量警报、潜在数据库泄露警报

新内部连接观察结果

描述：与新内部实体通信的通常可预测的本地实体。

前提条件：无。

新内部设备观察结果

说明：回溯期内未出现的新实体出现在网络上。

前提条件：无。

关联风险通告：新内部设备风险通告

新大型连接(外部)观察结果

描述：实体与外部主机交换了异常大量的数据。

前提条件：无。

关联风险通告：出站流量峰值风险通告

新大型连接(内部)观察结果

描述：实体与内部主机交换了异常大量的数据。

前提条件：无。

新配置文件观察结果

说明：实体与最近不匹配的配置文件标记(例如 FTP 服务器)匹配。

前提条件：无。

关联警报：垃圾邮件警报、紧急配置文件警报、异常域控制器警报

持久性外部服务器观察结果

说明：此实体与同一外部服务器(FTP、SSH 等)定期通信。

前提条件：无。

关联风险通告：持久性远程控制连接警报、异常外部服务器警报

群体峰值观察结果

说明：观察到在本地网络上通信的 IP 地址达到创记录的数量。

前提条件：无。

关联风险通告：网络群体峰值风险通告

端口扫描程序观察结果

说明：实体扫描了大量端口。

前提条件：无。

关联风险通告：内部端口扫描程序风险通告、疑似端口滥用(外部)风险通告

潜在数据转发观察结果

说明：在内部数据源到此实体之间(“下载”)，以及此实体到外部数据接收器之间(“上传”)，检测到大小相似且时间接近的数据传输。

前提条件：无。

关联警报：潜在数据泄露风险通告

公共 Amazon Route 53 托管区域创建的观察结果

描述：已创建公共 Amazon Route 53 托管区域。

前提条件：此观察结果需要 AWS 集成并启用 CloudTrail。

面向公众的 IP 监视列表匹配观察结果

描述：在监视列表中发现了您的网络中面向公众的 IP(通过域名显式或隐式)。

前提条件：无。

关联警报：面向公众的 IP 监视列表匹配警报

公共 IP 服务观察结果

描述：设备使用了可能被恶意软件使用的 IP 服务。

前提条件：此观察结果需要通过思科防御协调器与安全分析和日志记录 (SaaS) 集成。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。

关联警报：公共 IP 服务警报

快速登录观察

描述：用户在短时间内登录了许多实体。

前提条件：无。

记录指标异常值观察结果

说明：实体发送或接收的流量达到创记录的数量。

前提条件：无。

关联警报：内部连接峰值警报、出站流量峰值警报

记录分析文件异常值观察结果

描述：发送或接收与已知配置文件匹配的流量的实体(例如 Facebook 客户端)。

前提条件：无。

关联风险通告：出站流量峰值风险通告

远程访问观察结果

说明：从远程源访问了实体。

前提条件：无。

关联警报：地理位置异常的远程访问警报、新远程访问警报、远程访问(地理)警报

角色违规观察结果

说明：实体具有不符合其角色的新流量(例如，FTP 服务器在端口 80 上通信)。

前提条件：无。

关联警报：角色违规警报

扫描结果观察结果

描述：活动扫描程序(例如，nmap)发现了实体行为。

前提条件：无。

会话已关闭的观察结果

描述：用户会话已关闭。

前提条件：此观察结果需要 OSSEC、Sumo Logic 或 Active Directory 部署。

会话打开的观察结果

描述：用户会话已打开。

前提条件：无。

关联警报：异常用户警报

静态连接集偏差观察结果

描述：实体通常与一组静态(内部/外部)实体通信，但最近开始/停止与新/正常实体通信。

前提条件：无。

关联警报：静态设备偏差警报

静态端口集偏差观察结果

描述：实体通常使用一组静态(本地/已连接)端口进行(内部/外部)通信，但最近添加/丢弃了端口。

前提条件：无。

关联警报：静态设备偏差警报

Sumo Logic 日志观察结果观察结果

描述：某个实体可能会参与由 Sumo Logic 托管的日志。

前提条件：此观察结果需要 Sumo Logic 部署。

关联警报：缺少 Sumo 逻辑日志警报

可疑恶意 URL 观察结果

描述：主机与可疑的恶意 URL 通信。

前提条件：此观察结果需要满足以下条件之一：

- 安全分析和日志记录 (SaaS) 通过思科防御协调器。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。
- 增强型 NetFlow。有关详细信息，请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。

关联警报：疑似恶意 URL 警报

可疑网络钓鱼域观察结果

描述：主机与可疑的网络钓鱼域通信。

前提条件：此观察结果需要满足以下条件之一：

- 安全分析和日志记录 (SaaS) 通过思科防御协调器。有关详细信息，请参阅 https://docs.defenseorchestrator.com/Configuration_Guides/Monitoring_and_Reporting/Cisco_Security_Analytics_and_Logging 。
- 增强型 NetFlow。有关详细信息，请参阅 Cisco Secure Cloud Analytics增强型 NetFlow 配置指南 。
- 来自 SPAN 或镜像端口的 DNS 日志。

关联警报：疑似网络钓鱼域警报

可疑终端活动观察结果

说明：检测到与已知攻击者的战术、技术和程序相关的可疑终端活动。

前提条件：无。

关联警报：来自可疑进程警报的 LDAP 连接、检测到恶意进程警报、已执行 Metasploit 警报、端口 8888：来自多个源的连接警报、潜在持久性尝试警报、潜在系统进程模拟警报、SMB|RDP：连接到多个目标警报和 可疑进程路径警报

可疑网络活动观察结果

说明：检测到与已知攻击者的战术、技术和程序相关的可疑活动。

前提条件：无。

关联警报：疑似远程访问工具心跳警报、疑似 Zerologon RPC 攻击尝试警报

可疑 SMB 活动观察结果

说明：多个实体首次使用 SMB 协议执行了异常活动。

前提条件：无。

关联警报：可疑 SMB 活动风险通告

流量放大观察结果

说明：实体的出站和入站流量与其使用的配置文件关联的典型比率不匹配。这可能表示参与了放大攻击。放大攻击会尝试使用大量数据包响应某个请求，以达到淹没服务器的目的，其中涉及欺骗性的 IP 地址或其他标识信息。参与放大攻击也可能表示某个实体已感染僵尸网络恶意软件，并在无意中发送这些数据包。

前提条件：无。

关联警报：放大攻击警报

TrickBot 锚点DNS 隧道活动观察

描述：设备使用 TrickBot Anchor_DNS 隧道方法与 C&C 服务器通信。

前提条件：无。

关联警报：TrickBot 锚点DNS 隧道警报

Umbrella Sinkhole 命中观察结果

说明：设备与已知的 Cisco Umbrella Sinkhole 通信。

前提条件：无。

关联警报：重复的 Umbrella Sinkhole 通信风险通告

未使用的 AWS 资源观察结果

描述：未发现 AWS 资源的近期活动。

前提条件：此观察结果需要 AWS 集成。

关联警报：未使用的 AWS 资源警报

异常 DNS 解析器观察结果

说明：实体与异常 DNS 解析器通信。

前提条件：无。

关联警报：新异常 DNS 解析器警报、异常 DNS 连接警报

观察到异常的 EC2 实例

描述：已创建类型和大小异常的新 EC2 实例。

前提条件：此观察结果需要 AWS 集成并启用 CloudTrail。

关联警报：异常大的 EC2 实例警报

观察到的数据包大小异常

描述：实体发送或接收的数据包对于给定配置文件而言大小异常。

前提条件：无。

相关警报：DNS 滥用警报、ICMP 滥用警报

监视列表交互观察结果

说明：实体通过域名与监视列表中的 IP 地址显式或隐式通信。

前提条件：无。

关联警报：重复的监视列表通信警报、可疑的僵尸网络交互警报、疑似加密货币活动警报、可疑的 DNS over HTTPS 活动警报、DNSTalos 情报监视列表命中警报、异常外部服务器警报、用户监视列表命中警报、监视列表命中警报

监视列表查找观察结果

描述：实体查找列入监视列表的域。

前提条件：无。

关联警报：用户监视列表命中警报、监视列表命中警报

蠕虫传播观察结果

说明：先前扫描的设备开始扫描本地 IP 网络。

前提条件：无。

关联风险通告：蠕虫传播警报

更多资源

有关 Cisco Secure Cloud Analytics的详细信息，请参阅以下资源：

- https://www.cisco.com/c/en/us/products/security/stealthwatch-cloud/index.html 用于总体概述
- https://www.cisco.com/c/en/us/products/security/stealthwatch/stealthwatch-cloud-free-offer.html 以注册长达 60 天的免费试用
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/tsd-products-support-series-home.html 用于文档资源
- https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-guides-list.html 用于了解安装和配置指南，包括 Cisco Secure Cloud Analytics 初始部署指南

联系支持人员

如果需要技术支持人员，请执行以下操作之一：

- 联系您当地的思科合作伙伴
- 联系思科支持
- 通过以下网址反映问题：http://www.cisco.com/c/en/us/support/index.html
- 通过以下邮箱反映问题：tac@cisco.com
- 美国支持电话：1-800-553-2447
- 全球支持电话：https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html
- 对于 Cisco Secure Cloud Analytics 免费试用客户，请通过电子邮件提交支持案例：swatchc-support@cisco.com

更改历史记录

修订	修订日期	说明
1.0	2020 年 4 月 3 日	初始版本。
1.1	2020 年 9 月 4 日	添加了以下警报和观察结果： • 异常 AWS 工作空间警报 • 异常 Mac 工作站警报 • Empire 命令和控制警报 • 恶意软件高峰警报 • 异常配置文件观察结果 更新了以下警报和观察结果： • 垃圾邮件警报 • 历史异常值观察结果 • 新配置文件观察结果 还添加了有关 安全分析和日志记录 (SaaS) 并更正拼写错误的其他信息。
2.0	2021 年 10 月 25 日	已更名，并添加了以下警报和观察结果： • AWS 检测器已修改警报 • AWS 日志记录已删除警报 • AWS 临时令牌持久性警报 • Azure 顾问监视列表警报 • 非服务端口扫描程序警报 • 公共 IP 服务查找警报 • 静态设备连接偏差警报 • 疑似 Zerologon RPC 漏洞攻击尝试警报 • TrickBot 锚点DNS 隧道警报 • 使用公共 IP 查找服务观察结果的设备 • Azure 许可安全组观察结果 • Azure 许可存储设置观察结果 • 合规性判定摘要观察结果 • 新的合规性资源故障观察结果

		• TrickBot 锚点DNS 隧道活动观察结果
2.1	2022 年 5 月 10 日	更新了警报的 MITRE ATT&CK 战术或技术，并添加了以下警报： • AWS EC2 启动脚本已修改 • AWS ECS 凭证访问 • AWS IMDS 生成的凭证 • AWS Lambda 持久性 • AWS 快照泄露 • Azure 缺乏保护的服务 • 已删除 Azure 防火墙 • Azure 函数调用高峰 • 已删除 Azure Key Vault • 已删除 Azure 网络安全组 • Azure OAuth 绕行 • 已删除 Azure 资源组 • Azure 将数据传输到云账户 • 严重性云安全评估监控列表命中 • 高严重性云安全评估监视列表命中 • ICMP 滥用 • LDAP 连接峰值 • 低严重性云安全评估监视列表命中 • 中严重性级别的云安全评估监控列表命中 • Meterpreter 命令和控制成功 • 出站 LDAP 峰值 • 已创建许可 Amazon Elastic Kubernetes 服务集群 • 重复的 Umbrella Sinkhole 通信 • 已配置 S3 存储桶生命周期 • SMB 连接异常值 • 可疑的 DNS Over HTTPS 活动

		• 疑似远程访问工具心跳 • 可疑用户代理 • 来自新外部服务器的异常文件扩展名 • 蠕虫传播 已添加以下观察结果： • 异常用户代理观察结果 • Azure 公开服务观察结果 • Azure 函数指标异常值观察结果 • 新文件扩展名观察结果 • 公共 IP 服务观察结果 • Umbrella Sinkhole 命中观察结果 • 蠕虫传播观察结果 已删除以下警报： • AWS IMDS 生成的凭证 • 潜在勒索软件活动 • 快速登录
2.2	2022 年 8 月 2 日	已添加联系支持人员
2.3	2022 年 9 月 14 日	已添加 ISE 会话已启动观察结果 删除了公共 IP 服务警报。
2.4	2022 年 11 月 1 日	已添加以下警报： • 已创建 AWS IAM Anywhere 信任锚点 • 已添加新的 AWS Lambda 调用权限 • 异常大的 EC2 实例 已添加以下观察结果： • 观察到异常的 EC2 实例 已更新警报的 MITRE ATT&CK 战术或技术。 已更新警报的遥测要求。
2.5	2023 年 1 月 17 日	已添加以下警报：

		• AWS 重复 API 故障
2.6	2023 年 2 月 13 日	已添加以下警报和观察结果： • ISE 用户异常警报 • ISE 可疑活动观察结果
3.0	2023 年 8 月 29 日	已添加以下警报： • AWS IAM 用户接管 • AWS 日志记录受损 • 已删除 AWS 安全组 • 无效的 MAC 地址 • ISE 越狱设备 • 来自可疑进程的 LDAP 连接 • 检测到恶意进程 • 已执行的 Metasploit • 端口 8888：从多个源连接 • 潜在的持久性尝试 • 潜在的系统进程模拟 • SMB|RDP：与多个目标的连接 • 可疑进程路径 已更新以下警报： • Azure 缺乏保护的服务 • 已删除 Azure 防火墙 • 潜在数据泄露

版权信息