配置和监控取证事件

取证功能集可通过捕获实时取证事件和应用用户定义的规则来启用对可能的安全事件的监控和警报。具体而言，它可以实现：

- 定义规则以指定关注的取证事件
- 定义匹配取证事件的触发操作
- 搜索特定取证事件
- 可视化事件生成进程及其完整沿袭

警告 启用**取证**功能后，软件代理可能会消耗额外的主机资源，具体取决于代理配置。请参阅“软件代理配置”部分。

- 兼容性 ， 第 1 页
- 取证信号, on page 2
- 取证配置, on page 7
- 取证可视化, on page 20
- 取证事件中显示的字段, on page 23
- 取证分析 - 可搜索字段, on page 29
- 取证分析中的搜索词, on page 29
- 取证警报, on page 35
- 取证评分, on page 38
- 基于 PCR 的网络异常检测, on page 40
- 进程散列异常检测, on page 46

兼容性

除 Solaris 外，所有平台上的深度可视性代理都会报告取证取证信号。目前，AIX 仅支持少数取证信号。有关详细信息，请参阅“取证信号”部分。

取证信息通过 Linux 内核 API、审计和系统日志、Windows 内核 API、Windows 事件、AIX 审计系统等提供。一般来说，操作系统供应商会保证一个主要版本的兼容性。但是，不同平台和次版本的 API 可能会略有不同，因为操作系统供应商可能会回传功能和修复。因此，某些取证事件类型在某些平台上可能不可用。此外，代理不会尝试恢复或启用代理启动时已禁用的任何操作系统服务。

例如，有许多使用 Linux 审核框架的取证信号。如果启用取证，深度可视性代理将在代理启动后将 Cisco Secure Workload 审核规则插入系统中。规则插入会要求系统具有已安装的 augenrules 实用程序和 /etc/audit/rules.d 目录。如果不满足任何这些前提条件，则不会插入 Cisco Secure Workload 审核规则。因此，将不会报告包括文件访问和原始套接字创建在内的取证信号。

如果用户之前启用了取证并将其禁用，则代理会删除 Cisco Secure Workload 插入的审核规则。在 Red Hat 7.3 和 CentOS 7.3 上，我们观察到一个操作系统错误，可能会影响规则删除过程。代理通过以下方式来删除审核规则： 1. 删除 */etc/audit/rules.d/* 中的 taau.rules 2. 运行 *$service auditd restart*。操作系统会根据 */etc/audit/rules.d/* 中的 *audit.rules* 和 **.rules* 文件来重新生成规则集。然后，auditd 会将规则加载到系统中。

操作系统在 /etc/audit/rules.d/audit.rules 文件的开头添加 *-D*，以便在插入新规则集之前清除所有规则。但在 Red Hat 7.3 和 CentOS 7.3 计算机上，*/etc/audit/rules.d/audit.rules* 可能没有 *-D*。这是因为如果 */etc/audit/rules.d/audit.rules* 文件不存在，操作系统就会创建一个空文件，而且 */usr/share/doc/audit-<version>/* 子目录中的默认规则文件也不存在，例如，*/usr/share/doc/audit-2.8.4/rules/10-base-config.rules* 就是一个可能的默认规则位置。可以通过运行 *$rpm -qf -scripts /etc/audit/rules.d* 从 RPM 更新脚本中观察确切的操作系统行为

在 Linux 中，一些取证信号依赖于对 64 位系统调用的观察结果。当前版本不支持 32 位 Linux 系统调用。

根据兼容性矩阵，下面列出了代理上支持的操作系统 (OS)：

- Linux：所有版本均支持
- Windows：所有支持的版本
- AIX：在 AIX 7.2 和 Power8 或更高版本上支持
- Solaris：在 x86_64 和 SPARC 上支持

取证信号

必须启用**取证**功能，软件代理才能捕获和报告取证事件。该功能可以在软件代理配置中启用。有关详细信息，请参阅软件代理配置部分。

启用**取证**功能时，代理会报告以下取证事件。

信号	说明
权限提升	权限升级，例如使用 sudo 执行的命令。
用户登录	用户登录事件。
用户登录失败	用户登录失败尝试。

信号	说明
Shellcode	类似于 shellcode 尝试的可疑 shell 执行。
文件访问	对密码文件等敏感文件的访问。
用户帐户	添加或删除用户帐户。
未检测到的命令	代理未发现的新命令。用户可以使用命令异常评分根据范围来调整结果。有关详细信息，请参阅未检测到的命令 。
未检测到的库	代理未查看过之前加载的进程的新库。
原始套接字创建	创建原始套接字的进程。例如，端口敲击。
二进制文件已更改	对已知二进制文件的散列值或修改时间的更改。
库已更改	已知库的散列值或修改时间更改。
侧信道	侧信道攻击尝试 (Meltdown)。
跟踪用户登录	登录事件发生后派生或执行的后代进程。
跟踪进程	跟踪进程事件可根据进程属性（如二进制文件路径、命令字符串等）报告符合用户取证配置规则的进程。
网络异常	工作负载的网络流量异常，有关详细信息，请参阅基于 PCR 的网络异常检测。

Table 1: AIX 上支持的取证信号

信号	说明
权限提升	权限升级，例如使用 sudo 执行的命令。
原始套接字创建	创建原始套接字的进程。例如，端口敲击。
用户帐户	添加或删除用户帐户。

权限提升

当进程将其权限从低更改为高时，就会被视为权限升级。在 Linux 中，这意味着进程的用户 ID 已从非零变为了零。有些情况下是合规的，如更改普通用户的密码，以及其他特殊用途的二进制文件，如 sudo。此事件当前在 Windows 中不可用。Windows 中的权限升级通常是通过其他机制完成的，而不是改变进程本身的权限，即完整性级别。其他类型的取证事件（如未检测到的命令或二进制变化）也会涉及 Windows 上的权限升级。

用户登录

用户登录事件，包括 SSH、RDP 和其他类型的登录。只要出现，传感器就会捕获用户登录的人员、时间和方式。例如，对于 Linux 中的 SSH，传感器会报告用户名、身份验证类型（密码、公共）和源 IP。

用户登录失败

与上述用户登录事件类似，只要有类似信息，传感器就会报告失败的登录尝试。

Shellcode

Shellcode 事件在 Linux 和 Windows 中有着不同的解释。在 Linux 中，传感器可识别以交互式 shell 方式运行的进程，而无需登录会话或终端。（在登录会话之外运行交互式 shell 没有充分的理由。）在此版本中，对 shellcode 事件的检测存在限制，因为它假定攻击将利用系统中已有的 shell。如果攻击上传新的二进制文件，传感器会将这些二进制文件标记为未检测到的命令或二进制更改（如果它们替换现有的二进制文件）。在 Windows 中，与 PowerShell DLL 链接的每个进程都会被标记为 shellcode。用户可以创建规则以过滤掉合法的情况。

文件访问

文件访问事件会报告敏感文件（如密码文件）的访问情况。在此版本中，用户无法更改要监控的文件列表。在 Linux 中，传感器监控对 /etc/passwd 的写访问。Sensor 还会监控对 /etc/shadow 的读写访问。 在此版本中，Windows 不会触发此事件。

用户帐户

只要有可用信息，用户帐户事件就会报告本地用户帐户的创建情况。

未检测到的命令

未检测到的命令事件会报告传感器未检测到的命令。未检测到的命令定义为从父进程到子进程的未检测到的过渡/边缘。例如，假设 Web 服务器 (httpd) 正在执行名为 abc.sh 的 CGI 脚本，当传感器首次检测到该脚本时，它会将 abc.sh 报告为未检测到的命令。Web 服务器对 abc.sh 的后续执行不会导致取证事件，因为传感器之前已发现并报告过该事件。如果服务或进程从不执行任何二进制文件，则来自该服务/进程的未检测到的命令事件表示可能存在危害。请注意，传感器在重启后是无状态的，因此在传感器重启后，系统会再次报告之前看到的命令。

从 3.4 开始，对于 SaaS 集群，每个“未检测到的命令”事件都与一个命令异常评分相关联，评分范围为 0.0 到 1.0。评分越低，过渡越异常。命令转换，即元组（父命令行，命令行）会在下面具有相同元组的事件之间 交叉检查是否存在异常转换：

- 传感器所属的最窄范围。例如，在属于以下范围沿袭的工作负载 W 上观察到未检测到的命令事件：`Root Scope -> A -> B -> C and Root Scope -> D -> E`。然后，在范围 C 和 E 的所有工作

负载中交叉检查该命令（注意，C 和 E 可以重叠或不重叠）。事件的异常评分是关于这 2 个范围的事件异常评分的最大值。

- 正在运行的进程的执行路径。
- 父进程的执行路径。
- 正在运行的进程的二进制散列。

评分 1.0 表示已发现具有相同元组（最窄范围、执行路径、父执行路径、二进制散列）的相同命令转换。评分 0.0 表示从未在同一范围内的任何主机上观察到具有正在运行的进程的此类执行路径、父执行路径和二进制散列的此类命令转换。异常评分可用于抑制在同一范围内触发类似的未检测到的命令警报，并减少误报。有关如何使用此评分的示例，请参阅 默认 Cisco Secure Workload 规则。

Note 异常评分仅适用于版本 3.4 及更高版本的 SaaS 集群。

未检测到的库

未检测到的库事件报告传感器未检测到之前加载的进程的库。未检测到的库被定义为一对未检测到的二进制文件执行路径和库路径。例如，应用通常会加载相对稳定的库列表。可以访问机器的攻击者可能会重启应用和 LD_PRELOAD 恶意库。当传感器首次在此应用二进制文件执行路径中发现新加载的恶意库时，它会报告未发现的库事件。随后加载恶意库不会导致取证事件，因为传感器之前已经发现并报告过。合法的情况包括应用在升级后加载新库，或应用动态加载新库。请注意，传感器可能会在重启后再次报告以前看到的库。

请注意，这是一项试验性功能，在未来版本中可能会有所变化。

原始套接字创建

此版本仅支持 Linux 下的原始套接字创建事件。原始套接字通常用于监听或注入/欺骗流量。原始套接字有其合法用途，例如在 tcpdump 等诊断工具中，或在制作 ping 或 arp 等特殊 IP 数据包时。恶意用途包括用于避免目标/受害计算机进行日志记录的隐身扫描、恶意软件端口敲门等。Cisco Secure Workload 传感器还会创建原始套接字，用于收集流相关信息。（为了保持一致性，传感器不会抑制由自己的流信息收集触发的事件。）

二进制文件已更改

二进制文件更改事件会报告正在运行的进程的文件内容和二进制属性的更改。传感器会记录每个正在运行的进程的文件属性。如果一个进程在相同路径下运行二进制文件，但文件属性（ctime、mtime、大小或散列）不同，则传感器会将该进程标记为二进制文件更改。合法的案例包括应用升级。

库已更改

“库已更改”事件报告正在运行的进程的文件内容和库属性更改。传感器会记录已加载库的文件属性。如果一个进程在相同路径下加载了一个库，但文件属性（ctime、mtime、size 或 hash）不同，传感器就会标记该进程的库发生了变化。合法的案例包括库升级。

请注意，这是一项试验性功能，在未来版本中可能会有所变化。

侧信道

侧信道事件报告正在运行的软件利用侧信道漏洞。侧信道事件报告运行了利用侧信道漏洞的软件。此版本在选定的 Linux 平台上提供了一个侧信道检测功能：Meltdown。有关支持的计算机配置，请参阅下面的详细信息。这些是高级安全功能，因此默认情况下处于禁用状态。启用侧信道报告后，用户应该会看到 CPU 使用率提高。系统仍将遵循在 UI 中配置的 CPU 配额。如果传感器的取证收集子进程确定其 CPU 使用率过高且持续时间过长，则会将其关闭，并且父传感器进程将在稍许延迟后重启它。在旧内核或不支持的内核上启用此功能可能会导致系统不稳定。建议在类似的非生产环境中进行测试。

可以从 UI 中的代理配置页面打开/关闭此功能，并且可以在每个代理配置文件中打开/关闭这些功能。

崩溃是一种滥用 CPU 中的推测执行和缓存功能的侧信道攻击 (https://meltdownattack.com/)。它允许攻击者从非特权域读取特权域数据，例如，在没有 0 环权限的情况下从用户空间应用读取内核内存。崩溃检测当前支持 CentOS 7 和 Ubuntu 16.04。

跟踪用户登录

“跟踪用户登录”事件报告在用户登录事件进程（SSH、RDP 等）之后执行的后代进程（最多 4 个级别）。此跟踪用户登录事件下报告的进程用于审核目的，不一定具有任何安全事件。

跟踪进程

跟踪进程事件可根据进程属性（如二进制文件路径、命令字符串等）报告符合用户取证配置规则的进程。在此“跟踪进程”(Follow Process) 事件下报告的进程用于审核目的，不必具有任何安全事件。

示例 1：由 cmd.exe 或 powershell.exe 运行的报告进程

Event Type = Follow Process AND (Process Info - Exec Path contains cmd.exe OR Process Info - Exec Path contains powershell.exe)

示例 2：报告由 winword.exe、excel.exe 或 powerpnt.exe 创建的任何进程。

Event Type = Follow Process with_ancestor (Process Info - Exec Path contains winword.exe OR Process Info - Exec Path contains excel.exe OR Process Info - Exec Path contains powerpnt.exe)

注意：跟踪进程事件可以通过以下进程信号之一进行跟踪：

- 进程信息 - 执行路径
- 进程信息 - 命令字符串

- 进程信息 - 用户名
- 跟踪进程 - 父执行路径
- 跟踪进程 - 父命令字符串
- 跟踪进程 - 父用户名

取证配置

取证功能使用基于意图的配置。意图指定如何将取证配置文件应用于资产过滤器。取证配置文件由多个取证规则组成。意图中的配置文件按从上到下的顺序应用。

取证规则

Note 每个根范围的最大规则数为 100。

添加取证规则

本部分介绍如何添加新的取证规则。

准备工作

您必须在系统中以**站点管理员**、**客户支持**或系统**范围所有者**的身份登录。

Procedure

步骤 1 在左侧的导航栏中，点击**防御 (Defend)** > **取证规则 (Forensic Rules)**。

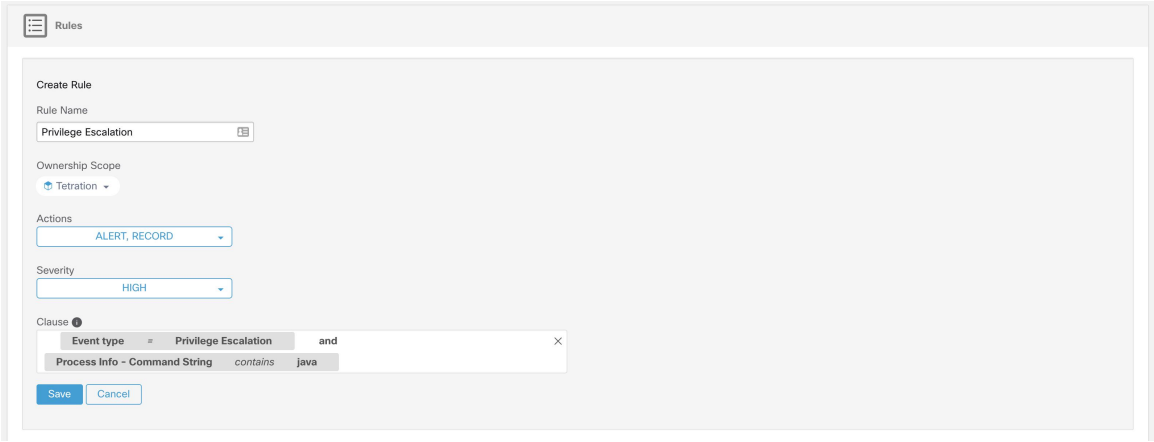
步骤 2 点击 **Create Rule**。

步骤 3 在以下字段中输入适当的值。

字段	说明
规则名称 (Rule Name)	为规则输入名称。名称不能为空。
所有权范围 (Ownership scope)	输入此规则的所有权范围。
操作 (Actions)	选择触发此规则时的操作。**记录**意味着匹配的安全事件会持续存在，以供进一步分析。**警报**操作意味着将匹配的安全事件发布到 Cisco Secure Workload 警报系统。

字段	说明
严重性 (Severity)	选择此规则的严重性级别：**LOW**、**MEDIUM**、**HIGH**、**CRITICAL** 或 **REQUIRES IMMEDIATE ACTION**
子句 (Clause)	输入规则子句。子句必须包含来自进程取证事件或工作负载事件的安全事件信号。如果一个子句同时包含进程信号和工作负载信号，则该子句无效。

Figure 1: 创建规则



步骤 4 点击**保存 (Save)**。

基本取证规则组成

取证规则必须仅包含**一个**取证事件类型（例如，**Event Type == Unseen Command**）。以下可选子句使用该事件的属性（例如，**Unseen Command - Parent Uptime**）。

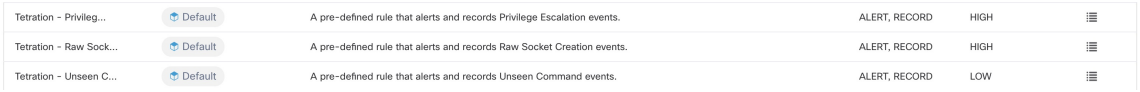
以下是使用**未检测到的命令**事件类型的示例。有关更多示例，请参阅默认规则和 MITRE 规则。

EventType = Unseen Command and Unseen Command - Parent Uptime (microseconds) >= 60000000.

默认 Cisco Secure Workload 规则

提供默认 Cisco Secure Workload 规则旨在帮助用户构建在其环境中有意义的规则。这些规则显示在取证配置页面中且不可编辑。这些规则在所有根范围内都可用。

Figure 2: 默认规则



Cisco Secure Workload 取证规则：

1. **名称** Cisco Secure Workload - 权限提升

   Clause EventType = Privilege Escalation and (ProcessInfo - ExecPath 不包含 **sudo and ProcessInfo - ExecPath** 不包含 **ping and Privilege Escalation Is = Type - Suid Binary)**

   说明。此规则可报告并非由 setuid 二进制文件生成的权限升级事件。为了可靠地过滤掉 setuid 二进制文件，它还会根据“ProcessInfo - ExecPath”来过滤掉 **sudo** 和 **ping**。Cisco Secure Workload 用户还可以通过定义自己的规则来过滤掉其他 setuid 二进制文件。

2. **名称** Tetration - 未检测到的命令

   Clause EventType = Unseen Command and Unseen Command - Parent Uptime (microseconds) >= 60000000 or ProcessInfo - ExecPath *contains* **/bash or ProcessInfo - ExecPath** *contains* **/sh or ProcessInfo - ExecPath** *contains* **/ksh or Parent - ExecPath** *contains* **httpd or Parent - ExecPath** *contains* **apache or Parent - ExecPath** *contains* **nginx or Parent - ExecPath** *contains* **haproxy**

   说明。此规则报告与以下条件之一匹配的未检测到的命令事件：此规则可报告符合以下条件之一的未察觉命令事件：

   a. 父进程处于活动状态的时间超过 **60,000,000** 微秒。

   b. Process ExecPath 包含某种类型的 shell，例如 **/bash**、**/sh** 和 **/ksh**。

   c. 进程父 ExecPath 包含某种类型的服务器应用，例如 **httpd**、**apache**、**nginx** 和 **haproxy**。

3. **名称** Tetration - 原始套接字

   Clause EventType = Raw Socket Creation and (Raw Socket - ExecPath *doesn’t contain* **ping and Raw Socket - ExecPath** *doesn’t contain* **iptables and Raw Socket - ExecPath** *doesn’t contain* **xtables-multi)**

   说明 此规则报告并非由 **ping** 和 **iptables** 生成的原始套接字创建事件。Cisco Secure Workload 用户还可以通过定义自己的规则来过滤掉其他二进制文件。

4. **名称** Tetration - 包含未检测到的命令的网络异常

   Clause EventType = Network Anomaly and Network Anomaly - Unseen Command Count > 3 and Network Anomaly - Non-seasonal Deviation > 0

   说明 此规则报告符合以下条件的网络异常事件：

   a. 在 15 分钟内，同一工作负载上有超过 3 个“未检测到的命令”事件。

   b. 规则属性大于 0（这也意味着它大于或等于 6.0，因为 6.0 是所有网络异常事件的最小报告偏差）。

5. **名称** Tetration - 异常未检测到的命令

   Clause EventType = Unseen Command and Unseen Command - Anomaly - Score < 0.6

   说明 此规则报告异常评分低于 0.6 的未检测到的命令事件。这意味着，只有命令与之前观察到的命令不相似的高度异常事件才会被报告。阈值 0.6 是根据 Cisco Secure Workload 对不同阈值下类似命令的试验确定的。有关评分的详细说明，请参阅未检测到的命令。

6. **名称** Tetration - smss 的异常父项

Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **smss.exe and (Follow Process - ParentExecPath** *doesn't contain* **smss.exe and Follow Process - ParentExecPath** *doesn't contain* **System)**

说明 此规则特定于 Windows。如果 smss.exe 的父进程与另一个 smss.exe 实例或系统进程不同，则此规则会发出警报。

7. **名称** Tetration - wininit 的异常父项

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **wininit.exe and Follow Process - ParentExecPath** *doesn't contain* **smss.exe**

   说明 此规则特定于 Windows。如果 wininit.exe 具有不同于 smss.exe 的父项，则此规则会发出警报。

8. **名称** Tetration - RuntimeBroker 的异常父项

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **RuntimeBroker.exe and Follow Process - ParentExecPath** *doesn't contain* **svchost.exe**

   说明 此规则特定于 Windows。如果 RuntimeBroker.exe 具有不同于 svchost.exe 的父项，则此规则会发出警报。

9. **名称** Tetration - services 的异常父项

   Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **services.exe and Follow Process - ParentExecPath** *doesn't contain* **wininit.exe**

   说明 此规则特定于 Windows。如果 services.exe 具有不同于 wininit.exe 的父项，则此规则会发出警报。

10. **名称** Tetration - lsaio 的异常父项

    Clause EventType = Follow Process and ProcessInfo - ExecPath *contains* **lsaio.exe and Follow Process - ParentExecPath** *doesn't contain* **wininit.exe**

    说明 此规则特定于 Windows。如果 lsaio.exe 的父项不同于 wininit.exe，则此规则会发出警报。

11. **名称** Tetration - lsass 的异常子项

    Clause (EventType = Follow Process and ProcessInfo - ExecPath *doesn't contain* **efsui.exe and ProcessInfo - ExecPath** *doesn't contain* **werfault.exe) with ancestor Process Info - ExecPath** *contains* **lsass.exe**

    说明 此规则特定于 Windows。如果 lsass.exe 具有任何并非 efsui.exe 或 werfault.exe 的后代，则此规则会发出警报。

默认 MITRE ATT&CK 规则

提供默认 MITRE ATT&CK 规则，以便向来自 MITRE ATT&CK 框架 (https://attack.mitre.org/) 的技术发出警报。与对抗行为有关的规则有 24 条，其中大部分都与 MITRE 的特定技术相对应。完整的规则列表如下。

1. **名称** 可疑的 MS Office 行为

Clause (Event type = Follow Process and (Process Info - Exec Path doesn’t contain **Windowssplwow64.exe) and (Process Info - Exec Path** *doesn’t contain* **chrome.exe) and (Process Info - Exec Path** *doesn’t contain* **msip.executionhost.exe) and (Process Info - Exec Path** *doesn’t contain* **msip.executionhost32.exe) and (Process Info - Exec Path** *doesn’t contain* **msosync.exe) and (Process Info - Exec Path** *doesn’t contain* **ofccccaupdate.exe) with ancestor (Process Info - Exec Path** *contains* **winword.exe or Process Info -Exec Path** *contains* **excel.exe or Process Info -Exec Path contains powerpnt.exe)**

说明 此规则在 Microsoft Office 进程 (WIN-WORD.exe/EXCEL.exe/POWERPNT.exe) 创建任何子进程时发出警报并进行记录。根据我们的研究，我们允许这些 MS Office 二进制文件创建一些已知的常见子进程，以减少误报的数量。

2. 名称 T1015 - 辅助功能 1

   Clause Event type = Follow Process (Process Info - Exec Path *contains* **cmd.exe or Process Info -Exec Path** *contains* **powershell.exe or Process Info - Exec Path** *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and (Follow Process - Parent Exec Path** *contains* **winlogon.exe or Follow Process - Parent Exec Path** *contains* **atbroker.exe or Follow Process - Parent Exec Path** *contains* **utilman.exe**)

   说明 此规则会在任何辅助功能二进制文件（屏幕键盘、放大镜、粘滞键等）被滥用并被欺骗打开 cmd/powershell/cscript/wscript 时发出警报，同时进行记录。辅助功能二进制文件的调用由 Winlogon、atBroker 或 utilman 进程控制，具体取决于调用它们的位置（从登录屏幕或用户登录后）。此规则可捕获辅助功能进程（winlogon.exe、utilman.exe 和 atBroker.exe）的可疑子进程（cmd.exe、powershell.exe、cscript.exe、wscript.exe）。将此与 **T1015 - 辅助功能 2** 配合使用，还可以捕获这四个可疑子进程的其他子进程**。

3. 名称 T1015 - 辅助功能 2

   Clause Event type = Follow Process with ancestor ((Process Info - Exec Path *contains* **cmd.exe or Process Info - Exec Path** *contains* **powershell.exe or Process Info - Exec Path** *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and (Follow Process - Parent Exec Path** *contains* **winlogon.exe or Follow Process - Parent Exec Path** *contains* **atbroker.exe or Follow Process - Parent Exec Path** *contains* **utilman.exe))**

   说明 此规则会在任何辅助功能二进制文件（屏幕键盘、放大镜、粘滞键等）被滥用并被欺骗打开 cmd.exe/powershell.exe/cscript.exe/wscript.exe 时发出警报，同时进行记录。 辅助功能二进制文件的调用由 Winlogon、atBroker 或 utilman 进程控制，具体取决于调用它们的位置（从登录屏幕或用户登录后）。此规则可捕获这些进程（winlogon、utilman 和 atBroker）的可疑子进程的子进程。应将此与 **T1015 - 辅助功能 1** 一起使用，该功能可提醒可疑子进程辅助功能二进制文件。

4. 名称 T1085 - rundll32

   Clause (Event type = Follow Process and Process Info Exec Path *does not contain* **msiexec.exe and Process Info Exec Path** *does not contain* **WindowsSystem32SystemPropertiesRemote.exe with ancestor (Process Info - Exec Path** *contains* **rundll32.exe and Follow Process - Parent Exec Path** *does not contain* **msiexec.exe and not (Process Info -command string** *contains* **Windowssystem32shell32.dll or (Process Info -command string** *contains* **Windowssyswow64shell32.dll or (Process Info -command string** *contains* **WindowsSystem32migrationWinInetPlugin.dll))**

说明 此规则可在 rundll32.exe 创建子进程时发出警报并记录。可以调用此二进制文件来执行任意二进制文件/dll，或者被 control.exe 用来安装恶意控制面板项目。但是，如果 msiexec.exe 是 rundll32.exe 的父项或后代项，则允许执行这些操作。我们还允许使用已知 dll 的一些常见 rundll32 命令。

5. 名称 T1118 - InstallUtil

   Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **installutil.exe**

   说明 此规则可在 InstallUtil.exe 创建子进程时发出警报并进行记录。

6. 名称 T1121 - Regsvcs/Regasm

   Clause Event type = Follow Process and (Process Info - Exec path *does not contain* **fondue.exe or Process Info - Exec path** *does not contain* **regasm.exe or Process Info - Exec path** *does not contain* **regsvr32.exe with ancestor (Process Info - Exec Path** *contains* **regasm.exe or Process Info - Exec Path** *contains* **regsvcs.exe)**

   说明 此规则可在 regsvcs.exe 或 regasm.exe 创建子进程时发出警报并记录。但是，如果 fondu.exe/regasm.exe/regsvr32.exe 是由 regasm.exe 或 regsvcs.exe 生成的，则我们允许这种情况，以减少误报的数量。

7. 名称 T1127 - 受信任的开发人员实用程序 - msbuild.exe

   Clause (Event type = Unseen Command with ancestor Process Info - Exec Path *contains* **MSBuild.exe) and (Process Info - Exec Path** *does not contain* **Tracker.exe) and (Process Info -Exec Path** *doesn’t contain* **csc.exe) and (Process Info - Exec Path** *does not contain* **Microsoft Visual Studio) and (Process Info - Exec Path** *does not contain* **al.exe) and (Process Info - Exec Path** *does not contain* **lc.exe) and (Process Info - Exec Path** *does not contain* **dotnet.exe) and (Process Info - Exec Path** *does not contain* **cvtres.exe) and (Process Info - Exec Path** *does not contain* **conhost.exe) and not (Event type = Unseen Command with ancestor (Process Info - Exec Path** *contains* **Tracker.exe or Process Info - Exec Path** *contains* csc.exe or Process Info - Exec Path *contains* **Microsoft Visual Studio or Process Info - Exec Path** *contains* **al.exe or Process Info - Exec Path** *contains* **lc.exe or Process Info - Exec Path** *contains* **dotnet.exe or Process Info - Exec Path** *contains* **cvtres.exe))**

   说明 如果 msbuild.exe 创建的子进程不属于其通常创建的子进程的允许列表，则此规则会发出警报并进行记录。此规则目前基于“未检测到的命令”，而不是“关注流程”规则，因为“关注流程”尚不支持允许进程子树。当前规则允许以下进程及其后代：Tracker.exe、csc.exe、“Microsoft Visual Studio”路径中的任何进程、al.exe、lc.exe、dotnet.exe 和 cvtres.exe。该规则还允许 conhost.exe。这些进程可以在 MSBuild.exe 的常规使用过程中看到（例如，通过 Visual Studio 编译项目）。MSBuild.exe 的所有其他子程序（非通常行为）都会收到警报。

8. 名称 T1127 - 受信任的开发人员实用程序 - rcsi.exe

   Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **rcsi.exe**

   说明 此规则可在 rcsi.exe 创建子进程时发出警报并进行记录。

9. 名称 T1127 - 受信任的开发人员实用程序 - tracker.exe

   Clause (Event type = Unseen Command with_ancestor Process Info - Exec Path *contains* **tracker.exe) and not (Event type = Unseen Command with_ancestor Process Info - Exec Path** *contains* **MSBuild.exe)**

说明 此规则可在 tracker.exe 创建子进程且跟踪器本身不是 MSBuild.exe 的后代时发出警报并进行记录。因此，通过 Visual Studio 对跟踪器的合法调用会获得批准，但会向其他调用发出警报。Tracker.exe 和以前的 MSBuild.exe 规则的一个限制是，如果攻击者使用 MSBuild 技术创建跟踪器，然后让跟踪器创建恶意子程序，那么这两条规则都不会发出警报，因为将MSBuild作为祖先的跟踪器被认为是合法的。

10. 名称 T1128 - Netsh 助手 Dll

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **netsh.exe**

    说明 此规则可在 netsh.exe 创建子进程时发出警报并进行记录。

11. 名称 T1136 - 创建帐户

    Clause Event type = User Account

    说明 此规则可在创建新用户时发出警报并进行记录。

12. 名称 T1138 - 应用补偿

    Clause Event type = Follow Process Info - Exec Path *contains* **sdbinst.exe**

    说明 此规则可在调用 sdbinst.exe 时发出警报并记录。

13. 名称 T1180 - 屏幕保护程序

    Clause Event type = Follow Process AND with ancestor Process Info - Exec Path *contains* **.scr**

    说明 如果创建的进程在执行路径中包含“.scr”，则此规则会发出警报并进行记录。

14. 名称 T1191 - CMTP

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **cmstp.exe**

    说明 此规则可在 cmstp.exe 创建子进程时发出警报并进行记录。

15. 名称 T1202 - 间接命令执行 - forfiles.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **forfiles.exe**

    说明 此规则可在 forfiles.exe 创建子进程时发出警报并记录。

16. 名称 T1202 - 间接命令执行 - pcalUA.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **pcalua.exe**

    说明 此规则可在 pcalUA.exe 创建子进程时发出警报并进行记录。

17. 名称 T1216 - 签名脚本代理执行 - pubprn.vbs

    Clause Event type = Follow Process with ancestor ((Process Info - Exec Path *contains* **cscript.exe or Process Info - Exec Path** *contains* **wscript.exe) and Process Info - Command String** *contains* **.vbs and Process Info - Command String** *contains* **script)**

    说明 如果使用 wscript.exe 或 cscript.exe 运行任何 vbs 脚本以创建新进程，且参数为“script”，则此规则会发出警报并进行记录。攻击者可利用这一技术执行带有指向恶意 sct 文件的脚本参数的 pubprn.vbs，然后执行代码。

18. 名称 T1218 - 签名二进制代理执行 - msiexec.exe

Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **msiexec.exe**

说明 此规则可在 msiexec.exe 创建子进程时发出警报并进行记录。

19. **名称** T1218 - 签名二进制代理执行 - odbcconf.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **odbcconf.exe**

    说明 此规则可在 odbcconf.exe 创建子进程时发出警报并记录。

20. **名称** T1218 - 签名二进制代理执行 - Register-CimProvider

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **Register-CimProvider.exe**

    说明 此规则可在 Register-CimProvider.exe 创建子进程时发出警报并进行记录。

21. **名称** T1220 - XSL 脚本处理 - msxsl.exe

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **msxsl.exe**

    说明 此规则可在 msxsl.exe 创建子进程时发出警报并进行记录。

22. **名称** T1220 - XSL 脚本处理 - wmic

    Clause Event type = Follow Process and (Process Info - Exec Path *contains* **wmic.exe and Process Info - Command String** *contains* **.xsl**)

    说明 此规则可在 wmic 使用 xsl 脚本时发出警报并进行记录。这可用于启动任意二进制文件。

23. **名称** T1223 - 已编译的 HTML 文件

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **hh.exe**

    说明 此规则可在 hh.exe 创建子进程时发出警报并记录。

24. **名称** T1003 - 凭证转储 - Lsass

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **procdump.exe and Process Info - Command String** *contains* **lsass**

    说明 此规则可在 procdump.exe 用于转储 lsass 进程的内存时发出警报并记录。

25. **名称** T1140 - 对文件或信息进行去混淆处理/解码

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **certutil.exe and (Process Info - Command String** *matches* **.*encode\s.* or Process Info - Command String** *matches* **.*decode\s.***

    说明 如果 certutil.exe 用于对文件进行编码或解码，则此规则会发出警报并进行记录。攻击者通常使用此技术来解码受害者计算机上的编码负载。

26. **Name** T1076 - 远程桌面协议

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **tscon.exe**

    说明 此规则可在执行 tscon.exe 时发出警报并进行记录。攻击者可以使用 tscon.exe 来劫持现有 RDP 会话。

27. **名称** T1197 - BITS 作业 - Powershell

Clause Event type = Follow Process and Process Info - Exec Path *contains* **powershell.exe and Process Info - Command String** *contains* **Start-BitsTransfer**

说明 此规则可在 powershell.exe 被用于运行 cmdlet Start- BitsTransfer 以复制/移动文件时发出警报并进行记录。

28. 名称 T1170 - MSHTA

    Clause Event type = Follow Process with ancestor Process Info - Exec Path *contains* **mshta.exe**

    说明 此规则可在使用 mshta.exe 运行生成子进程的恶意 HTA 脚本时发出警报并进行记录。

29. 名称 T1158 - 隐藏的文件和目录

    Clause Event type = Follow Process and (Process Info - Exec Path *contains* **attrib.exe and Process Info - Command String** *contains* **+h)**

    说明 此规则可在使用 attrib.exe 将文件/目录设置为隐藏时发出警报并记录。

30. 姓名 T1114 - 邮件收集

    Clause Event type = Follow Process (Process Info - Command String *matches* **.*.(ost|pst)(\s|"|’).* or Process Info - Command String** *matches* **.*.(ost|pst)$) Process Info - Exec Path** *doesn’ t contain* **outlook.exe**

    说明 此规则可在从 Outlook.exe 以外的任何其他进程访问邮件文件（.ost 和 .pst）时发出警报并进行记录。

31. 名称 T1070 - 删除主机上的指示器 - 事件日志

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **wevtutil.exe and Process Info - Command String** *matches* **.*\s(cl|clear-log)\s.***

    说明 此规则可在使用 wevtutil.exe 清除事件日志时发出警报并记录。

32. 名称 T1070 - 删除主机上的指示器 - USN

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **fsutil.exe and Process Info - Command String** *matches* **.*\susn\s.* and Process Info - Command String** *matches* **.*\sdeletejournal.***

    说明 此规则可在使用 fsutil.exe 删除 USN 日志时发出警报并记录。

33. 名称 T1053 - 计划任务

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **schtasks.exe and Process Info - Command String** *contains* **create**

    说明 此规则可在使用 schtasks.exe 创建新的计划任务时发出警报并记录。

34. 名称 T1003 - 凭证转储 - Vaultcmd

    Clause Event type = Follow Process and Process Info - Exec Path *contains* **vaultcmd.exe and Process Info - Command String** *matches* **.*\/list.***

    说明 此规则可在使用 vaultcmd.exe 访问 Windows 凭证保管库时发出警报并记录。

35. 名称 T1003 - 凭证转储 - 注册表

Clause Event type = Follow Process and Process Info - Exec Path *contains* **reg.exe and ((Process Info - Command String** *contains* **save or Process Info - Command String** *contains* **export) and (Process Info - Command String** *contains* **hklm or Process Info - Command String** *contains* **hkey_local_machine) and (Process Info - Command String** *contains* **sam or Process Info - Command String** *contains* **security or Process Info - Command String** *contains* **system))**

说明 此规则可在使用 reg.exe 转储某些注册表配置单元时发出警报并记录。

36. **名称** T1201 - 密码策略发现 1

Clause Event type = Follow Process and Process Info - Exec Path *contains* **change and Process Info - Command String** *contains* **-l**

说明 此规则可在使用更改实用程序列出 Linux 计算机上的密码策略（密码过期策略）时发出警报并进行记录。

37. **名称** T1081 - 文件中的凭证 - Linux

Clause Event type = Follow Process and (Process Info - Exec Path *contains* **cat or Process Info - Exec Path** *contains* **grep) and (Process Info - Command String** *contains* **.bash_history or Process Info - Command String** *contains* **.password or Process Info - Command String** *contains* **.passwd)**

说明 此规则可在尝试搜索存储在 Linux 计算机上的文件中的密码时发出警报并进行记录。

38. **名称** T1081 - 文件中的凭证 - Windows

Clause Event type = Follow Process and Process Info - Exec Path *contains* **findstr.exe and Process Info - Command String** *contains* **password**

说明 此规则可在尝试搜索 Windows 计算机上的文件中存储的密码时发出警报并进行记录。

39. **名称** T1089 - 禁用安全工具

Clause Event type = Follow Process and ((Process Info - Exec Path *contains* **fltmc.exe and Process Info - Command String** *contains* **unload sysmon) or (Process Info - Exec Path** *contains* **sysmon.exe and Process Info - Command String** *contains* **/u))**

说明 此规则可在尝试使用 fltmc.exe 或 sysmon.exe 卸载 sysmon 驱动程序时发出警报并记录

取证配置文件

添加配置文件

本部分介绍如何添加新的取证配置文件。

准备工作

您必须在系统中以**站点管理员**、**客户支持人员**或**范围所有者**身份登录。

Procedure

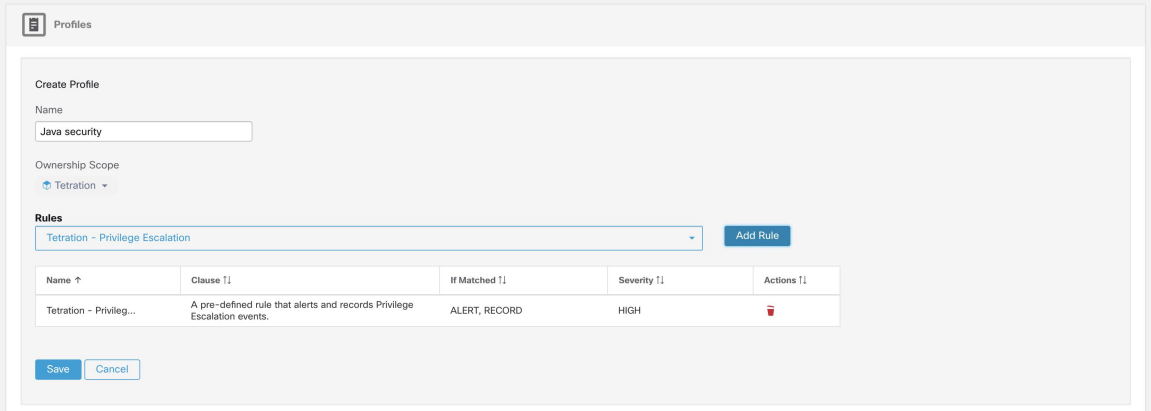
步骤 1 在左侧的导航栏中，点击**防御 (Defend)** > **取证规则 (Forensic Rules)**。

步骤 2 点击 **Create Profile**。

步骤 3 在以下字段中输入适当的值。

字段	说明
名称 (Name)	输入配置文件的名称。名称不能为空。
所有权范围 (Ownership scope)	输入此配置文件的所有权范围。
规则 (Rules)	将规则添加到此配置文件中。

Figure 3: 创建配置文件



步骤 4 点击**保存 (Save)**。

编辑配置文件

本部分介绍用户如何编辑取证配置文件。

准备工作

您必须在系统中以**站点管理员**、**客户支持**或系统**范围所有者**的身份登录。

Procedure

步骤 1 在左侧的导航栏中，点击**防御 (Defend)** > **取证规则 (Forensic Rules)**。

步骤 2 找到要编辑的配置文件，然后点击右侧列中的**铅笔**图标。

步骤 3 在以下字段中输入适当的值。

字段	说明
名称 (Name)	更新配置文件的名称。名称不能为空。
所有权范围 (Ownership scope)	更新此配置文件的所有权范围。
规则 (Rules)	在此配置文件中添加/删除规则。

步骤 4 点击**保存 (Save)**。

克隆配置文件

本部分介绍用户如何克隆取证配置文件。

Procedure

步骤 1 在左侧的导航栏中，点击**防御 (Defend)** > **取证规则 (Forensic Rules)**。

步骤 2 找到要克隆的配置文件，然后点击右侧列中的**克隆**图标。

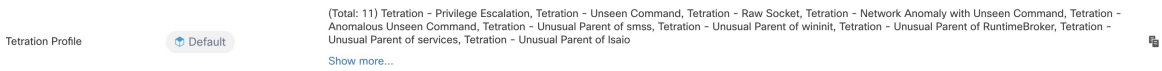
步骤 3 输入克隆配置文件的名称。

步骤 4 点击**保存 (Save)**。

默认配置文件 - Cisco Secure Workload 配置文件

Cisco Secure Workload 配置文件中包含 11 条默认取证规则，并且可以添加到意图。用户无法对其进行编辑，但可以对其进行克隆。克隆的默认取证配置文件可进行编辑。

Figure 4: 默认配置文件



默认配置文件 - MITRE ATT&CK 配置文件

MITRE ATT&CK 配置文件包含 39 条 MITRE ATT&CK 规则，并可添加到意图。用户无法对其进行编辑，但可以对其进行克隆。克隆的配置文件可进行编辑。MITRE ATT&CK 配置文件包括以下规则：

1. 可疑的 MS Office 行为
2. T1015 - 辅助功能 1
3. T1015 - 辅助功能 2
4. T1085 - rundll32
5. T1118 - InstallUtil
6. T1121 - Regsvcs/Regasm
7. T1127 - 值得信赖的开发人员实用程序 - msbuild.exe
8. T1127 - 值得信赖的开发人员实用程序 - rcsi.exe
9. T1127 - 值得信赖的开发人员实用程序 - tracker.exe
10. T1128 - Netsh 助手 DLL

11. T1136 - 创建帐户
12. T1138 - 应用补偿
13. T1180 - 屏幕保护程序
14. T1191 - CMSTP
15. T1202 - 间接命令执行 - forfiles.exe
16. T1202 - 间接命令执行 - pcalUA.exe
17. T1216 - 签名脚本代理执行 - pubprn.vbs
18. T1218 - 签名二进制代理执行 - msiexec.exe
19. T1218 - 签名二进制代理执行 - odbcconf.exe
20. T1218 - 签名二进制代理执行 - Register-CimProvider
21. T1220 - XSL 脚本处理 - msxsl.exe
22. T1220 - XSL 脚本处理 - wmic
23. T1223 - 已编译的 HTML 文件
24. T1003 - 凭证转储 - Lsass
25. T1140 - 对文件或信息进行去混淆处理/解码
26. T1076 - 远程桌面协议
27. T1197 - BITS 作业 - Powershell
28. T1170 - MSHTA
29. T1158 - 隐藏的文件和目录
30. T1114 - 邮件收集
31. T1070 - 主机上的指示灯删除 - 事件日志
32. T1070 - 主机上的指示灯删除 - USN
33. T1053 - 计划任务
34. T1003 - 凭证转储 - Vaultcmd
35. T1003 - 凭证转储 - 注册表
36. T1201 - 密码策略发现 1
37. T1081 - 文件中的凭证 - Linux
38. T1081 - 文件中的凭证 - Windows
39. T1089 - 禁用安全工具

变更日志 - 取证

站点管理员和在根范围上具有 SCOPE_OWNER 功能的用户可以通过点击图标来查看每个取证规则、配置文件和意图的更改日志，如下所示。

Figure 5: 变更日志

这些用户还可以通过点击相应表下方的**查看已删除规则/配置文件/意图 (View Deleted Rules/Profiles/Intents)** 链接来查看已删除规则、配置文件和意图的列表。

有关**变更日志**的详细信息，请参阅变更日志。根范围所有者只能查看属于其范围的实体的变更日志条目。

取证可视化

访问取证页面

本部分介绍如何访问取证页面。

准备工作

您必须在系统中以**站点管理员**、**客户支持人员**或**范围所有者**身份登录。

Procedure

步骤 1 点击左侧面板上的**安全 (Security)** 链接。

步骤 2 点击**取证 (Forensics)** 项目。系统将显示取证页面。

Figure 6: 安全取证

浏览取证事件

本部分介绍如何浏览匹配的取证事件。

准备工作

您必须在系统中以**站点管理员**、**客户支持人员**或**范围所有者**身份登录，然后导航至取证页面。

Procedure

步骤 1 在页面顶部的**时间范围选择器 (Time Range Picker)** 中选择特定范围。

步骤 2 从**严重性 (Severity)** 下拉列表中选择。

步骤 3 在**过滤器 (Filters)** 中，输入匹配取证事件的过滤器，然后点击 **过滤取证事件 (Filter Forensic Events)**。

步骤 4 系统将根据所选时间范围、严重性和过滤器来更新匹配取证事件表。

Note 取证事件在根范围级别下可见，在切换到子/子范围后将不可见。

检查取证事件

本部分介绍如何检查取证事件。

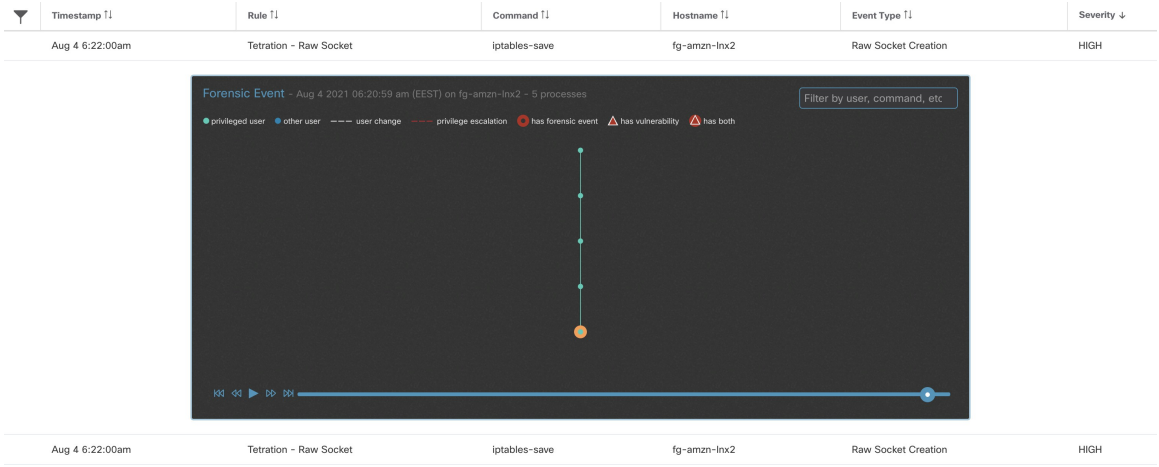
准备工作

您必须在系统中以**站点管理员**、**客户支持**或**范围所有者**（**根范围**）身份登录。

Procedure

步骤 1 点击要检查的事件。系统将显示**进程详细信息 (Process detail)** 窗格。

Figure 7: 取证事件表



步骤 2 在沿袭树上，点击要检查的进程以了解详细信息。

Figure 8: 取证过程详细信息

取证事件中显示的字段

每个取证事件都有几个可提供有用数据的字段。有几个字段是所有不同类型的取证事件所共有的，还有几个字段是特定取证事件所特有的。

以下是UI中所包含字段的列表。第一个表介绍了所有取证事件的通用字段，后面是一个表，介绍了随每个警报显示的进程信息，然后是包含每个调查事件的唯一字段的表。由于数据的存储和导出方式，某些字段可能会存在于多个表中。

通用字段

字段	说明
Bin attr ctime	更改了 Linux 中的时间/在二进制文件的 Windows 中创建时间
Bin attr hash	二进制文件的 Sha256 Hash
Bin attr mtime	二进制文件的修改时间
Bin attr name	文件系统上二进制文件的名称
Bin attr size	文件系统上二进制文件的大小
Bin exec path	二进制文件的完整路径
cmdline	执行的进程的完整命令行
Event time usec	观察到此事件的时间（以微秒为单位）

进程信息

字段	说明
进程 ID (Process ID)	进程的进程 ID
父进程 ID (Parent Process ID)	进程的父进程 ID
用户 (User)	执行进程的用户
执行路径 (Execution path)	与进程对应的二进制文件的完整路径。
开始时间 (Start time)	进程启动时间
完整命令 (Full command)	执行的进程的完整命令行

权限提升

字段	说明
父 cmdline (Parent cmdline)	进程父级的完整命令行
父 exe (Parent exe)	进程父级的完整路径
父正常运行时间（微秒）(Parent Uptime [microseconds])	自执行进程的进程父级以来的时间

字段	说明
父用户名 (Parent Username)	执行进程父级的用户
输入位图 suid 二进制文件 (Types bitmap suid binary)	指明二进制文件是否设置了 suid 位

用户登录

字段	说明
Auth type password	表示密码身份验证
Auth type pubkey	表示基于密钥的身份验证
Type login ssh	表示用户通过 ssh 登录
Type login win batch	表示 Windows 批量登录（类型 4，例如 schtasks）
Type login win cached	表示通过缓存的凭证登录（类型 11，CachedIntetractive）
Type login win interactive	表示交互式登录（类型 2，例如 RDP）
Type login win network cleartext	表示通过 ssh 登录（类型 8）
Type login win network	表示网络登录（类型 3，例如 Psexec）
Type login win new cred	表示使用新凭证（类型 9，例如 Runas 命令）
Type login win remote interactive	表示远程登录（类型 10，例如 RDP）
Type login win service	表示服务已由 SCM（类型 5）启动
Type login win unlock	表示工作站已解锁（类型 7）
Src IP	生成登录事件的源 IP
Src Port	生成登录事件的源端口
Username	与登录事件关联的用户名

用户登录失败

字段	说明
Auth type password	表示密码身份验证
Auth type pubkey	表示基于密钥的身份验证

字段	说明
Type login ssh	表示用户通过 ssh 登录
Type login win batch	表示 Windows 批量登录（类型 4，例如 schtasks）
Type login win cached	表示通过缓存的凭证登录（类型 11，CachedIntetractive）
Type login win interactive	表示交互式登录（类型 2，例如 RDP）
Type login win network cleartext	表示通过 ssh 登录（类型 8）
Type login win network	表示网络登录（类型 3，例如 Psexec）
Type login win new cred	表示使用新凭证（类型 9，例如 Runas 命令）
Type login win remote interactive	表示远程登录（类型 10，例如 RDP）
Type login win service	表示服务已由 SCM（类型 5）启动
Type login win unlock	表示工作站已解锁（类型 7）
Src IP	生成登录事件的源 IP
Src Port	生成登录事件的源端口
Username	与登录事件关联的用户名

Shellcode

字段	说明
信号源位图 cmd as sh no tty (Signal sources bitmap cmd as sh no tty)	表示 shell 进程没有与其关联的终端
信号源位图 Powershell (Signal sources bitmap powershell)	表示进程已加载 Powershell dll (System.Management.Autoration)

文件访问

字段	说明
File	已访问文件的完整路径
Perm read perm	表示文件具有读取权限
Perm read write perm	表示文件具有读写权限

字段	说明
Perm write perm	表示文件具有写入权限

用户帐户

字段	说明
Username	已创建的用户的用户名
Ops acct add	表示已添加新帐户

未检测到的命令

字段	说明
异常 - 评分 (Anomaly - Score)	评分（0至1.0）表示命令行以前出现的频率，评分越低，表示命令越异常
异常 - 相似性 - 高 (Anomaly - Similarity - High)	如果异常评分大于 0.8 且小于 1，则为 true
异常 - 相似性 - 中 (Anomaly - Similarity - Medium)	如果异常评分大于 0.6 且小于或等于 0.8，则为 true
异常 - 相似性 - 低 (Anomaly - Similarity - Low)	如果异常评分大于 0 且小于或等于 0.6，则为 true
异常 - 相似性 - 看到 (Anomaly - Similarity - Seen)	如果异常评分为 1，则为 true，即之前已看到相同的命令
异常 - 相似性 - 唯一 (Anomaly - Similarity - Unique)	如果异常评分为 0，则为 true，即之前从未见过该命令
父 cmdline (Parent cmdline)	父进程的完整命令行
父 exepath (Parent exepath)	父进程的二进制文件路径
父级正常运行时间 (Parent uptime)	自执行父进程以来的时间
父用户名 (Parent Username)	执行父进程的用户的用户名
传感器正常运行时间 (Sensor uptime)	传感器的正常运行时间

未检测到的库

字段	说明
库路径 (Lib Path)	之前未与进程关联的库文件的完整路径

原始套接字创建

字段	说明
可执行文件路径 (Exe Path)	创建原始套接字的进程的完整路径

库已更改

字段	说明
已更改名称的库 (Library changed name)	已更改的库的完整路径

侧信道

字段	说明
信号源位图崩溃 (Signal sources bitmap meltdown)	表示使用了崩溃漏洞

跟踪用户登录

字段	说明
用户名 (Username)	执行进程的用户名

跟踪进程

字段	说明
父 cmdline (Parent cmdline)	父进程的完整命令行
父 exepath (Parent exepath)	父进程的二进制文件路径
父级正常运行时间（毫秒）(Parent uptime usec)	自执行父进程以来的时间
父用户名 (Parent Username)	执行父进程的用户的用户名

字段	说明
自上次更改以来的时间（毫秒）(Time since last changed usec)	进程开始时间与其二进制文件更改时间之间经过的时间 (mtime)
用户名 (Username)	执行进程的用户的用户名

网络异常

有关详细信息，请参阅网络异常事件的取证规则，获取与网络异常事件关联的属性列表。

取证分析 - 可搜索字段

下表介绍“取证分析”(Forensics Analysis) 页面搜索栏上的可搜索字段。

其他字段

字段	说明
取证规则名称 (Forensic Rule Name)	由特定取证规则标记的事件
主机名 (Hostname)	来自特定主机名的事件
传感器 ID (Sensor ID)	来自特定传感器的事件
严重性 (Severity)	特定严重性的事件

取证分析中的搜索词

通用字段

这些字段是各种事件类型的通用字段。它们具有前缀“Event name - Event”，例如“Binary Changed - Binary Attribute - CTime (epoch nanoseconds)”

字段	说明
二进制属性 - CTime（纪元纳秒）(Binary Attribute - CTime [epoch nanoseconds])	更改了 Linux 中的时间/在二进制文件的 Windows 中创建时间
二进制属性 - 散列 (Binary Attribute - Hash)	二进制文件的 Sha256 Hash
二进制属性 - MTime（纪元纳秒）(Binary Attribute - MTime [epoch nanoseconds])	二进制文件的修改时间

字段	说明
二进制属性 - 文件名 (Binary Attribute - Filename)	文件系统上二进制文件的名称
二进制属性 - 大小（字节）(Binary Attribute - Size [bytes])	文件系统上二进制文件的大小
事件二进制文件路径 (Event Binary Path)	二进制文件的完整路径
命令行 (Command Line)	执行的进程的完整命令行

二进制文件已更改

除“通用字段”(Common Fields) 表中所述的搜索词外，没有其他搜索词。

文件访问

文件访问搜索词具有前缀“File Access -”，例如“File Access - Filename”

字段	说明
Filename	已访问文件的完整路径
Is = Permission - Read	表示文件具有读取权限
Is = Permission - ReadWrite	表示文件具有读写权限
Is = Permission - Write	表示文件具有写入权限

跟踪进程

跟踪进程搜索词具有前缀“Follow Process - “，例如“Follow Process - Parent Command Line”

字段	说明
父命令行 (Parent Command Line)	父进程的完整命令行
父执行路径 (Parent Exec Path)	父进程的二进制文件路径
父正常运行时间（微秒）(Parent Uptime [microseconds])	自执行父进程以来的时间
父用户名 (Parent Username)	执行父进程的用户的用户名
自上次文件更改以来的进程开始时间（微秒）(Process Start Time Since Last File Changed [microseconds])	从进程启动到最近一次（相应的）文件更改之间所经过的时间

字段	说明
用户名 (Username)	与所关注的进程相关联的用户名

跟踪用户登录

跟踪用户登录搜索词具有前缀“Follow User Logon -”，例如“Follow User Logon - Username”

字段	说明
用户名 (Username)	与进程关联的用户名

Ldap

Ldap 搜索词具有前缀“Ldap -”，例如“Ldap - Department”

字段	说明
部门 (Department)	与进程用户名关联的 AMS LDAP 用户部门（如果可用）
说明 (Description)	与进程用户名关联的 AMS LDAP 用户说明（如果可用）
用户名 (Username)	与进程关联的 AMS LDAP 用户名（如果可用）

库已更改

库已更改搜索词具有前缀“Library Changed -”，例如“Library Changed - Department”

字段	说明
库文件名 (Lib Filename)	已更改的库的完整路径

权限提升

权限升级搜索词具有前缀“Privilege Escalation -”，例如“Privilege Escalation - Parent Com- mand Line”

字段	说明
父命令行 (Parent Command Line)	进程父级的完整命令行
父执行路径 (Parent Exec Path)	进程父级的完整路径
Parent Uptime (microseconds)	自执行进程的进程父级以来的时间

字段	说明
父用户名 (Parent Username)	执行进程父级的用户
类型 - SUID 二进制文件 (Type - Suid Binary)	指明二进制文件是否设置了 suid 位

进程信息

进程信息搜索词带有前缀“Process Info - ”，例如“Process Info - Binary Hash”

字段	说明
二进制文件散列 (Binary Hash)	与进程关联的二进制文件的散列
令牌化的命令字符串 (Command String Tokenized)	进程的令牌化命令行
命令字符串 (Command String)	进程的完整命令行
执行路径 (Exec Path)	与进程对应的二进制文件的完整路径

原始套接字

原始套接字搜索词带有前缀“Raw Socket - ”，例如“Raw Socket - Exec Path”

字段	说明
执行路径 (Exec Path)	创建原始套接字的进程的完整路径

Shellcode

Shellcode 搜索词具有前缀“Shellcode - ”，例如“Shellcode - Source - Not From Login”

字段	说明
源 - 不是来自登录 (Source - Not From Login)	表示 shell 进程没有与其关联的终端
源 - Powershell (Source - Powershell)	表示进程已加载 Powershell dll (System.Management.Autoration)

侧信道

侧信道搜索词具有前缀“Shellcode - ”，例如“Shellcode - Source -Meltdown”

字段	说明
源 - 崩溃 (Source - Meltdown)	表示使用了崩溃漏洞

未检测到的命令

未检测到的命令搜索词具有前缀“Unseen Command - ”，例如“Unseen Command - Anomaly - Similarity - High”

字段	说明
异常 - 评分 (Anomaly - Score)	评分（0至1.0）表示命令行以前出现的频率，评分越低，表示命令越异常
异常 - 相似性 - 高 (Anomaly - Similarity - High)	如果异常评分大于 0.8 且小于 1，则为 true
异常 - 相似性 - 中 (Anomaly - Similarity - Medium)	如果异常评分大于 0.6 且小于或等于 0.8，则为 true
异常 - 相似性 - 低 (Anomaly - Similarity - Low)	如果异常评分大于 0 且小于或等于 0.6，则为 true
异常 - 相似性 - 看到 (Anomaly - Similarity - Seen)	如果异常评分为 1，则为 true，即之前已看到相同的命令
异常 - 相似性 - 唯一 (Anomaly - Similarity - Unique)	如果异常评分为 0，则为 true，即之前从未见过该命令
父 Cmdline (Parent Cmdline)	父进程的完整命令行
父 Exepath (Parent Exepath)	父进程的二进制文件路径
父级正常运行时间 (Parent Uptime)	自执行父进程以来的时间
父用户名 (Parent Username)	执行父进程的用户的用户名
传感器正常运行时间 (Sensor Uptime)	传感器的正常运行时间
异常 - 最新的类似命令 (Anomaly - Latest Similar Commands)	5 最近观察到的命令，这些命令类似于事件的命令

未检测到的库

未检测到的库搜索词具有前缀“Unseen Library - ”，例如“Unseen Library - Lib Filename”

字段	说明
库文件名 (Lib Filename)	之前未与进程关联的库文件的完整路径

用户帐户

用户帐户搜索词具有前缀“User Account - ”，例如“User Account - Account Name”

字段	说明
帐户名称 (Account Name)	已创建的用户的用户名
操作 - 添加帐户 (Operation - Add Account)	表示已添加新帐户

用户登录

用户登录搜索词具有前缀“User Logon - ”，例如“User Logon - Auth Type - Password”

字段	说明
Auth Type - Password	表示密码身份验证
Auth type - Pubkey	表示基于密钥的身份验证
Login Type - Login Via SSH	表示用户通过 ssh 登录
Login Type - Windows Login Batch	表示 Windows 批量登录（类型 4，例如 schtasks）
Login Type - Windows Login Cached	表示通过缓存的凭证登录（类型 11，CachedIntetractive）
Login Type - Windows Login Interactive	表示交互式登录（类型 2，例如 RDP）
Login Type - Windows Network Cleartext	表示通过 ssh 登录（类型 8）
Login Type - Windows Network	表示网络登录（类型 3，例如 Psexec）
Login Type - Windows Login New Credential	表示使用新凭证（类型 9，例如 Runas 命令）
Login Type - Windows Login Remote Interactive	表示远程登录（类型 10，例如 RDP）
Login Type - Windows Login Service	表示服务已由 SCM（类型 5）启动
Login Type - Windows Login Unlock	表示工作站已解锁（类型 7）
Source IP	生成登录事件的源 IP
Source Port	生成登录事件的源端口
Username	与登录事件关联的用户名

用户登录失败

User Logon Failed 搜索词具有前缀“User Logon Failed -”，例如“User Logon Failed - Auth Type - Password”

字段	说明
Auth Type - Password	表示密码身份验证
Auth type - Pubkey	表示基于密钥的身份验证
Login Type - Login Via SSH	表示用户通过 ssh 登录
Login Type - Windows Login Batch	表示 Windows 批量登录（类型 4，例如 schtasks）
Login Type - Windows Login Cached	表示通过缓存的凭证登录（类型 11，CachedIntetractive）
Login Type - Windows Login Interactive	表示交互式登录（类型 2，例如 RDP）
Login Type - Windows Network Cleartext	表示通过 ssh 登录（类型 8）
Login Type - Windows Network	表示网络登录（类型 3，例如 Psexec）
Login Type - Windows Login New Credential	表示使用新凭证（类型 9，例如 Runas 命令）
Login Type - Windows Login Remote Interactive	表示远程登录（类型 10，例如 RDP）
Login Type - Windows Login Service	表示服务已由 SCM（类型 5）启动
Login Type - Windows Login Unlock	表示工作站已解锁（类型 7）
Source IP	生成登录事件的源 IP
Source Port	生成登录事件的源端口
Username	与登录事件关联的用户名

取证警报

如果取证事件的匹配规则包含**警报**操作，则可以在 Cisco Secure Workload 警报系统中找到取证事件。

访问取证警报

本部分介绍如何访问取证警报。

准备工作

- 以**站点管理员**、**客户支持**或**范围所有者**身份登录系统。
- 打开**取证**警报源的警报。

Procedure

步骤 1 从导航窗格中选择**配置警报 (Configure Alerts)**。

步骤 2 随后将出现“警报”(Alerts) 页面。

检查警报详细信息

准备工作：

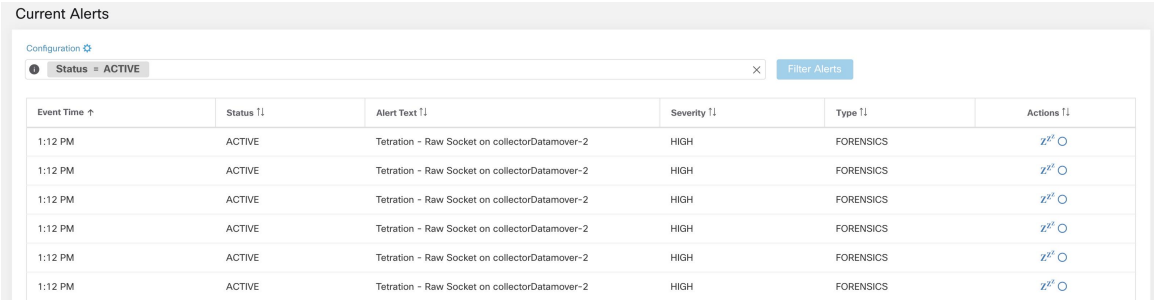
您必须在系统中以**站点管理员**、**客户支持人员**或**范围所有者**身份登录。

Procedure

步骤 1 在警报页面中，点击要检查的警报。

步骤 2 点击配置文件/规则，查看匹配的取证配置文件/规则的详细信息。如果在发出警报后更新匹配的配置文件/规则，则会出现一个警告指示器。

***Figure 9:*“取证警报”*(Forensic Alert)*页面**



此外，您可以暂停或包含/排除警报。有关详细信息，请参阅当前警报部分。

外部集成

取证警报可发送到系统日志等外部监控工具。取证警报将以 JSON 格式发送。JSON 字段定义在上面的“取证事件中显示的字段”部分中定义。

以下显示了一个 JSON Kafka 输出示例：

```
{
  "severity": "HIGH",
  "tenant_id": 0,
  "alert_time": 1595573847156,
  "alert_text": "Tetration - Anomalous Unseen Command on collectorDatamover-1",
  "key_id":
"d89f926cddc7577553eb8954e492528433b2d08e:5efcfdf5497d4f474f1707c2:5efcfdf6497d4f474f1707d6:20196:CMD_NOT_SEEN",
```

```
    "alert_id": "/Alerts/5efcfdf5497d4f474f1707c2/DataSource{location_type='TETRATION',
location_name='forensics', location_grain='MIN',
root_scope_id='5efcfdf5497d4f474f1707c2'}/db10d21631eebefc3b8d3aeaba5a0b1b45f4259e85b591763d7eaee9161ca076",

    "root_scope_id": "5efcfdf5497d4f474f1707c2",
    "type": "FORENSICS",
    "event_time": 1595573795135,
    "alert_details": "{\"Sensor
Id\":\"d89f926cddc7577553eb8954e492528433b2d08e\",\"Hostname\":\"collectorDatamover-1\",\"Process
 Id\":20196,\"scope_id\":\"5efcfdf5497d4f474f1707c2\",\"forensic\":{\"Unseen
Command\":\"true\",\"Unseen Command - Sensor Uptime (microseconds)\":\"34441125356\",\"Unseen
 Command - Parent Uptime (microseconds)\":\"35968418683\",\"Unseen Command - Parent
Username\":\"root\",\"Unseen Command - Parent Command Line\":\"svlogd -tt
/local/logs/tetration/efe/ \",\"Unseen Command - Parent Exec Path\":\"/sbin/svlogd\",\"Unseen
 Command - Anomaly - Score\":\"0\",\"Unseen Command - Anomaly - Similarity -
Unique\":\"true\",\"Process Info - Command String\":\"gzip \",\"Process Info - Exec
Path\":\"/bin/gzip\"},\"profile\":{\"id\":\"5efcfdf6497d4f474f1707e4\",\"name\":\"Tetration

Profile\",\"created_at\":1593638390,\"updated_at\":1593638390,\"root_app_scope_id\":\"5efcfdf5497d4f474f1707c2\"},\"rule\":{\"id\":\"5efcfdf6497d4f474f1707d6\",\"name\":\"Tetration
 - Anomalous Unseen
Command\",\"clause_chips\":\"[{\\\"type\\\":\\\"filter\\\",\\\"facet\\\":{\\\"field\\\":\\\"event_type\\\",\\\"title\\\":\\\"Event

type\\\",\\\"type\\\":\\\"STRING\\\"},\\\"operator\\\":{\\\"label\\\":\\\"\\u003d\\\",\\\"type\\\":\\\"eq\\\"},\\\"displayValue\\\":\\\"Unseen
 Command\\\",\\\"value\\\":\\\"Unseen
Command\\\"},{\\\"type\\\":\\\"filter\\\",\\\"facet\\\":{\\\"field\\\":\\\"forensic_event__cmd_not_seen_data__cmdline_anomaly_info_score\\\",\\\"title\\\":\\\"Unseen
 Command - Anomaly -
Score\\\",\\\"type\\\":\\\"NUMBER\\\"},\\\"operator\\\":{\\\"label\\\":\\\"\\u003e\\\",\\\"type\\\":\\\"gt\\\"},\\\"displayValue\\\":\\\"0\\\",\\\"value\\\":\\\"0\\\"}]\",\"created_at\":1593638390,\"updated_at\":1593638390,\"root_app_scope_id\":\"5efcfdf5497d4f474f1707c2\"}}"

  }
```


alert_details 中的值本身是一个转义的 JSON 字符串，其关于上述警报的内容如下所示：


```
  {
    "Sensor Id": "d89f926cddc7577553eb8954e492528433b2d08e",
    "Hostname": "collectorDatamover-1",
    "Process Id": 20196,
    "scope_id": "5efcfdf5497d4f474f1707c2",
    "forensic": {
      "Unseen Command": "true",
      "Unseen Command - Sensor Uptime (microseconds)": "34441125356",
      "Unseen Command - Parent Uptime (microseconds)": "35968418683",
      "Unseen Command - Parent Username": "root",
      "Unseen Command - Parent Command Line": "svlogd -tt /local/logs/tetration/efe/ ",
      "Unseen Command - Parent Exec Path": "/sbin/svlogd",
      "Unseen Command - Anomaly - Score": "0",
      "Unseen Command - Anomaly - Similarity - Unique": "true",
      "Process Info - Command String": "gzip ",
      "Process Info - Exec Path": "/bin/gzip"
    },
    "profile": {
      "id": "5efcfdf6497d4f474f1707e4",
      "name": "Tetration Profile",
      "created_at": 1593638390,
      "updated_at": 1593638390,
      "root_app_scope_id": "5efcfdf5497d4f474f1707c2"
    },
    "rule": {
      "id": "5efcfdf6497d4f474f1707d6",
      "name": "Tetration - Anomalous Unseen Command",
      "clause_chips":
"[{\"type\":\"filter\",\"facet\":{\"field\":\"event_type\",\"title\":\"Event
type\",\"type\":\"STRING\"},\"operator\":{\"label\":\"=\",\"type\":\"eq\"},\"displayValue\":\"Unseen
```

```
 Command\",\"value\":\"Unseen
Command\"},{\"type\":\"filter\",\"facet\":{\"field\":\"forensic_event__cmd_not_seen_data__cmdline_anomaly_info__score\",\"title\":\"Unseen
 Command - Anomaly -
Score\",\"type\":\"NUMBER\"},\"operator\":{\"label\":\"<\",\"type\":\"lt\"},\"displayValue\":\"0.6\",\"value\":\"0.6\"}]",

      "created_at": 1593638390,
      "updated_at": 1595539498,
      "root_app_scope_id": "5efcfdf5497d4f474f1707c2"
    }
 }
```


取证事件的详细信息包含在取证字段中。有关取证事件的属性列表，请参阅取证事件中显示的字段。这些属性也会在 UI 的警报详细信息中显示。

取证评分

何处查看取证评分

安全控制面板：

Figure 10: 安全控制面板中的“取证评分”***(Forensics Score)*** 部分

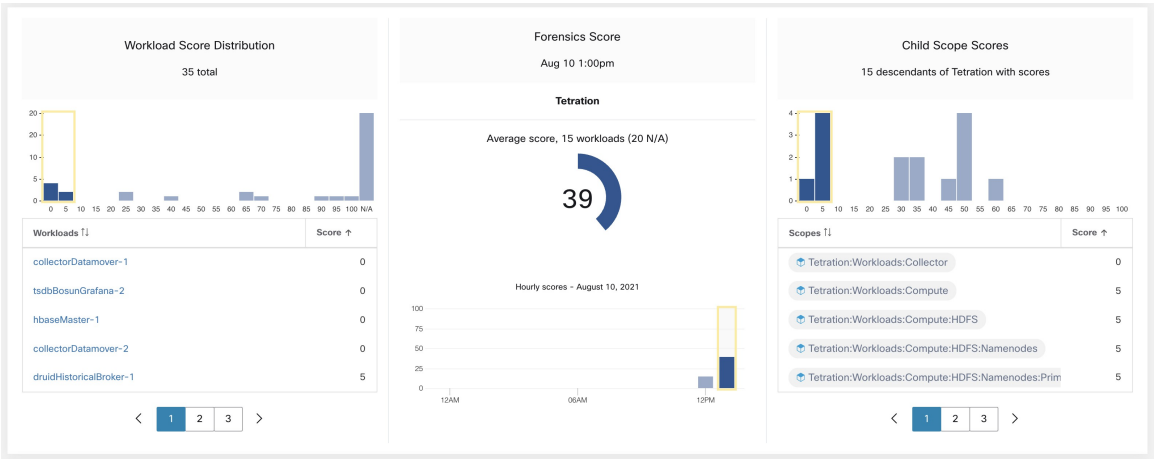
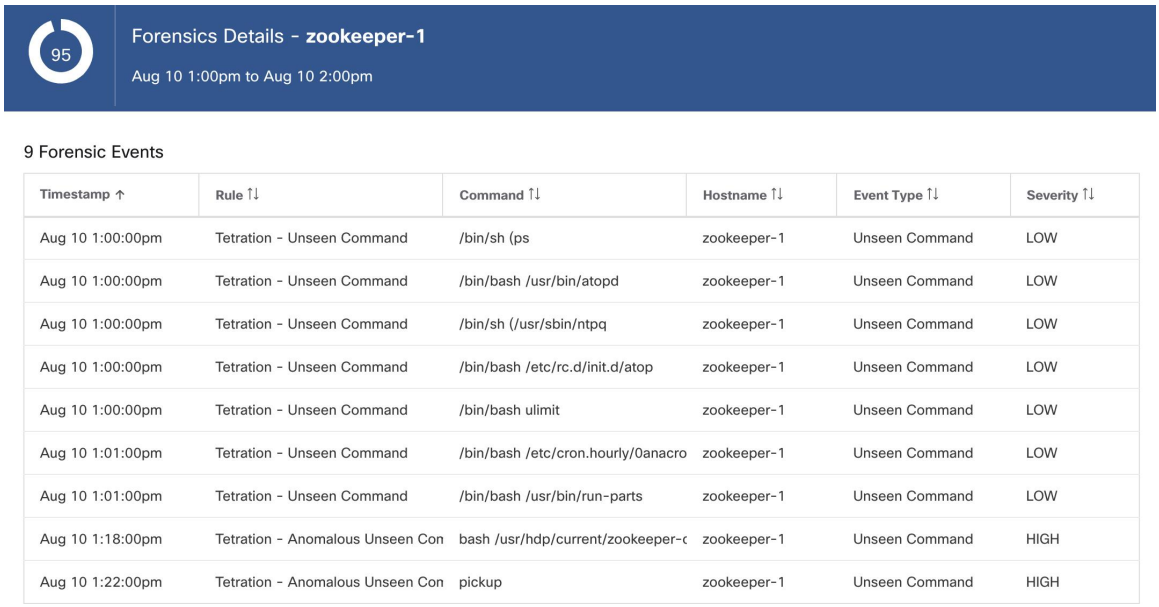


Figure 11: 安全控制面板中的“取证评分详细信息”***(Forensics Score Details)*** 部分



Timestamp ↑	Rule ↑↓	Command ↑↓	Hostname ↑↓	Event Type ↑↓	Severity ↑↓
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/sh (ps	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash /usr/bin/atopd	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/sh (/usr/sbin/ntpq	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash /etc/rc.d/init.d/atop	zookeeper-1	Unseen Command	LOW
Aug 10 1:00:00pm	Tetration - Unseen Command	/bin/bash ulimit	zookeeper-1	Unseen Command	LOW
Aug 10 1:01:00pm	Tetration - Unseen Command	/bin/bash /etc/cron.hourly/0anacro	zookeeper-1	Unseen Command	LOW
Aug 10 1:01:00pm	Tetration - Unseen Command	/bin/bash /usr/bin/run-parts	zookeeper-1	Unseen Command	LOW
Aug 10 1:18:00pm	Tetration - Anomalous Unseen Con	bash /usr/hdp/current/zookeeper-c	zookeeper-1	Unseen Command	HIGH
Aug 10 1:22:00pm	Tetration - Anomalous Unseen Con	pickup	zookeeper-1	Unseen Command	HIGH

如何计算取证评分

对于每个工作负载，我们都会计算取证评分。工作负载的取证评分源自基于为此范围启用的配置文件在该工作负载上观察到的取证事件。评分 100 表示未通过已启用配置文件中配置的规则观察到取证事件，评分 0 表示检测到需要立即操作的取证事件。范围的取证评分是该范围内的平均工作负载评分。特定小时的取证评分是该小时内所有评分的最小值。

- 严重性为需要立即执行操作的取证事件会将整个范围的评分降低到零。
- 严重性为“严重”的取证事件会降低工作负载的评分，权重为 10。
- 严重性为“高”的取证事件会降低工作负载的评分，权重为 5。
- 严重性为“中”的取证事件会降低工作负载的评分，权重为 3。
- 严重性为“低”的取证事件不会计入取证评分。对于信号质量仍在调整且可能存在噪声的新规则，建议采用此方法。

例如，工作负载具有 3 个取证事件，这些事件分别与 2 个严重性为严重 *(CRITICAL)* 的规则、1 个严重性为高 *(HIGH)* 的规则和 1 个严重性为低 *(LOW)* 的规则匹配。该工作负载的取证评分为：100 - 1 * 10 - 1 * 5 - 1 * 0 = 85。

对于未启用取证功能的工作负载，取证评分不适用。

如何提高取证评分

可以通过调整启用的取证规则来调整取证评分。创建干扰较小的规则将提供更准确的评分。采取行动并防止合法取证事件（作为入侵或其他不良活动证据的事件）是提高取证评分的另一个好方法。

警告

- 取证评分详细信息显示该小时内的所有取证事件。这意味着取证评分详细信息可能会显示取证事件，而不是用于计算取证评分的事件。
- 取证评分目前可用于深度可视性和执行传感器。

基于 PCR 的网络异常检测

网络异常功能根据生产者使用者比率 (PCR) 的概念检测流入或流出工作负载的异常大量数据。PCR 定义为：

```
Egress app byte count - Ingress app byte count
  PCR = ----------------------------------------------
        Egress app byte count + Ingress app byte count
```

PCR 的值范围为 [-1.0, 1.0]，其中：

- PCR = 1.0 表示工作负载仅向外发送数据。
- PCR = -1.0 表示工作负载仅接收数据。
- PCR = 0.0 表示工作负载的数据输入和数据输出量保持均衡。

与其他取证功能类似，您可以使用基于意图的配置来配置要记录和/或发出警报的网络异常事件。工作负载中检测到的网络异常事件每 5 分钟导出一次，而 5 分钟后将根据配置的规则进行匹配。因此，系统只会每 5 分钟在 UI 上观察到一次新的网络异常事件，从事件发生时起延迟最多 10 分钟。

Note 在 Cisco Secure Workload 软件的 3.2 和 3.1 版本中，网络异常检测称为数据泄漏检测。

网络异常事件的取证规则

有关如何添加取证规则，请参阅取证配置。

规则属性

本部分介绍用于定义网络异常相关规则的属性的详细信息。最简单的网络异常规则如下：

```
Event Type = Network Anomaly
```

网络异常事件中用于优化数据中心规则的其他属性：

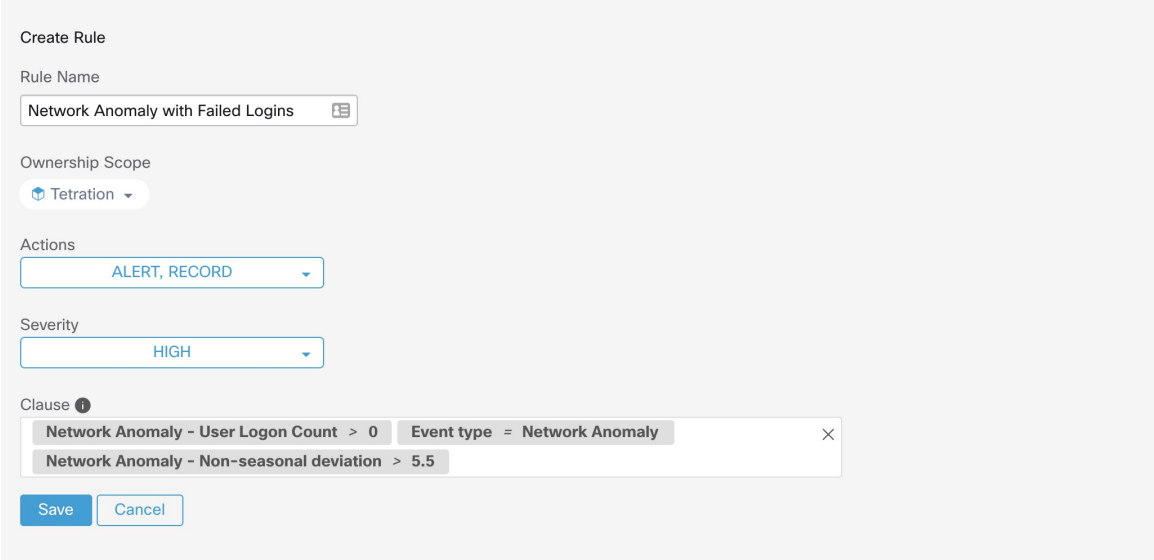
Table 2: 网络异常事件中的规则属性

属性	说明
Host Name	发出此事件的工作负载的主机名。

属性	说明
Timestamp (epoch milliseconds)	事件的时间戳（以毫秒为单位）。
PCR Deviation	PCR 与事件时间平均值的偏差，以历史标准偏差的倍数来表示。
Non-seasonal Deviation	这是删除季节性模式（例如，通过 Cron 作业删除）后的 PCR 偏差。非季节性偏差的值始终大于或等于 6.0。
PCR	生产者使用者比率。
EIR	出口入口比率，即总出口应用字节计数与入口应用字节计数之间的比率。
Egress App Byte Count	出口应用字节数，即流出工作负载的数据包内容（不包括标头）的总字节数。
Ingress App Byte Count	入口应用字节数，即流入工作负载的数据包内容（不包括标头）的总字节数。
Protocol	为其计算 PCR 时间序列的协议。目前，支持的协议包括 TCP、UDP 和 Aggregate。Aggregate PCR 是根据 TCP、UDP 和 ICMP 字节计数的总和计算得出的。
User Logon Count	大约过去 15 分钟内工作负载上的用户登录事件数。这是用户登录事件的计数，无论是否存在匹配的规则。要了解用户登录事件的详细信息，您必须定义规则来记录相关工作负载的事件，并在“取证分析”(Forensics Analysis) 页面上查看这些事件。
User Logon Failed Count	大约过去 15 分钟内工作负载上的用户登录失败事件数。这是用户登录失败事件的计数，无论是否存在匹配的规则。要了解“用户登录失败”事件的详细信息，您必须定义规则来记录相关工作负载的事件，并在“取证分析”(Forensics Analysis) 页面上查看这些事件。
Unseen Command Count	大约在过去 15 分钟内工作负载上的未检测到的命令事件数。这是未检测到的命令事件的计数，无论是否存在匹配的规则。要了解“未检测到的命令”事件的详细信息，必须定义规则来记录相关工作负载的事件，并在“取证分析”(Forensics Analysis) 页面上查看这些事件。
Date Time (UTC) - Year	事件时间的年份。

属性	说明
Date Time (UTC) - Month	事件时间的月份 (1, 2, . . .)。
Date Time (UTC) - Day	事件时间的日期 (1, 2, . . .)。
Date Time (UTC) - Hour	事件时间在一天中的小时数 (1, 2, . . . , 24)。
Date Time (UTC) - Minute	事件时间在一小时中的分钟数 (1, 2, . . . , 60)。
Date Time (UTC) - Second	事件时间在一分钟中的秒数 (1, 2, . . . , 60)。
Date Time (UTC) - Day of Week	事件时间的星期数（0-7，表示星期一至星期日）。

Figure 12: 定义网络异常事件的取证规则



以下是一些示例规则：

列表 7.10.1.1.1：仅检测 UDP 的网络异常。

```
Event Type = Network Anomaly AND Network Anomaly Is = Protocol - UDP
```

列表 7.10.1.1.2：在删除季节性模式后检测较大偏差（如已检测到），对于名称包含 *sensitiveDataServer* 的工作负载子集，出口应用字节数具有阈值。

```
Event Type = Network Anomaly AND Network Anomaly - Non-seasonal Deviation > 10.0)
AND Network Anomaly - Egress App Byte Count > 1000000
AND Network Anomaly - Host Name CONTAINS sensitiveDataServer
```

列表 7.10.1.1.3：在具有未检测到的命令事件的工作负载上检测网络异常事件，但网络异常事件发生在每天 7.30AM UTC 到 7.35AM UTC 之间。

```
Event Type = Network Anomaly AND Network Anomaly - Unseen Command Count > 0
```

```
   AND ( Network Anomaly - Date Time (UTC) - Hour != 7
   OR Network Anomaly - Date Time (UTC) - Minute < 30 OR Network Anomaly - Date Time (UTC)
- Minute > 35 )
```

规则操作

操作	说明
RECORD	匹配的事件会影响网络异常评分，可通过安全控制面板或“工作负载配置文件页面”(Workload Profile Page)/“网络异常”(Network Anomaly) 选项卡找到。
ALERT	匹配的事件显示在警报页面和所选的警报发布服务器中。

下一部分将详细介绍如何在 UI 中查找检测到的网络异常事件。

在何处查看网络异常事件

Note 网络异常事件目前不会显示在“取证分析”(Forensics Analysis) 页面上。您可以在以下页面中找到网络异常事件。

- **安全控制面板**：可以在安全控制面板的“网络异常”(Network Anomaly) 评分部分找到将规则与 **RECORD** 操作匹配的网络异常事件。如果有工作负载的评分不是最佳（小于 100），请点击工作负载名称，您可以查看该工作负载的 PCR 时间序列和网络异常事件。在网络异常事件表每一行的右侧，您都可以看到操作链接，这些链接可以帮助您搜索相应网络异常事件发生前后的流和其他取证事件。有关网络异常评分报告中的已知延迟，请参阅网络异常延迟。

Figure 13: 安全控制面板中的网络异常分数

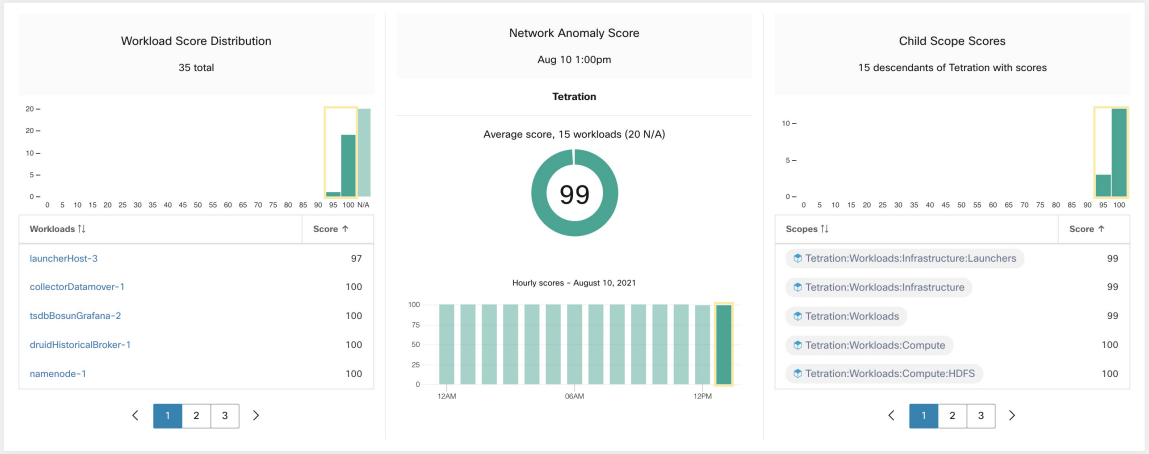
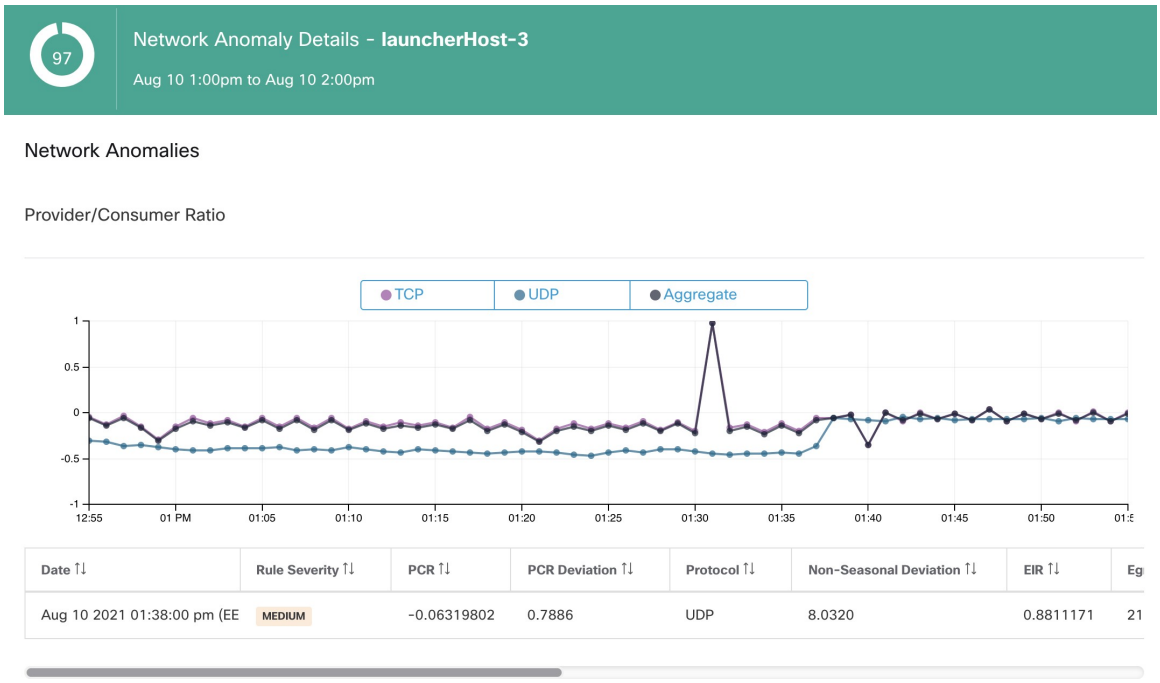
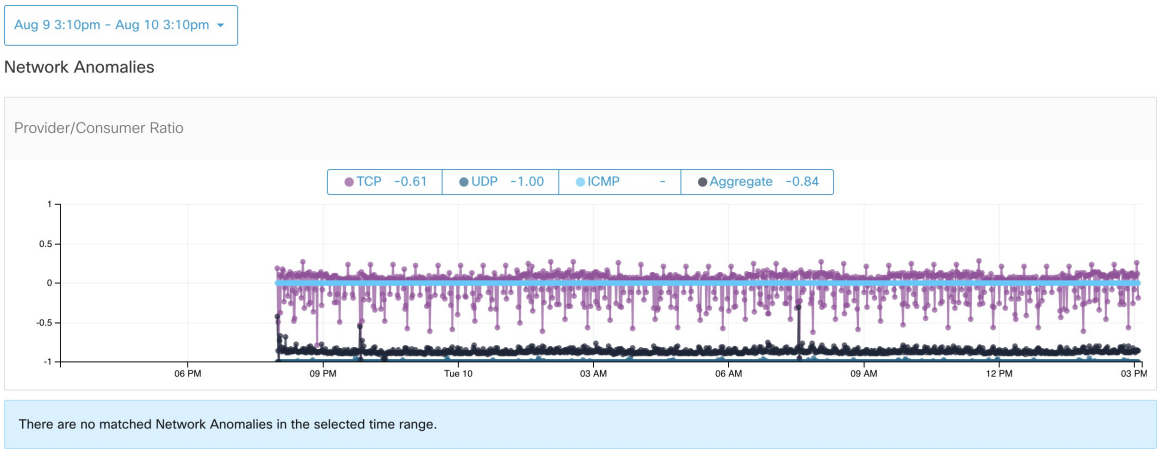


Figure 14: 安全控制面板中的网络异常评分按工作负载细分



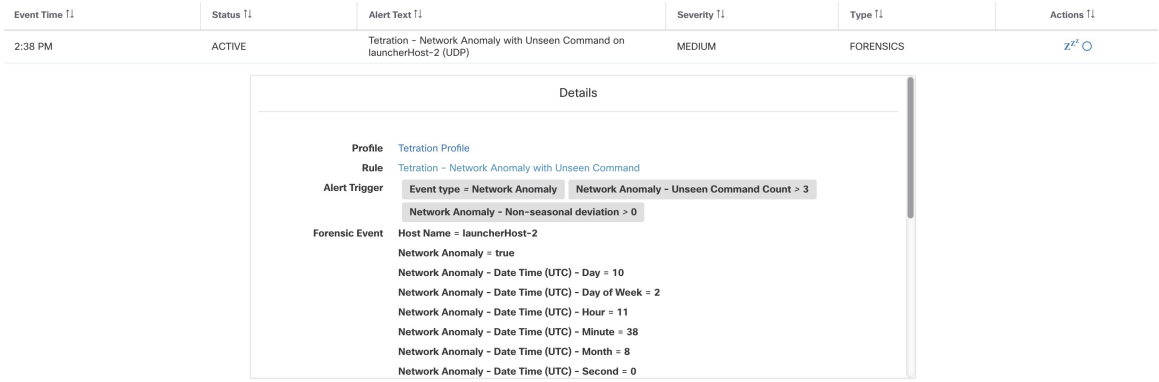
- 工作负载配置文件页面/网络异常选项卡：在此页面上，您可以查看PCR时间序列图以及将规则与 **RECORD** 操作匹配的网络异常事件。您在此页面上看到的内容类似于在安全控制面板中点击工作负载名称所看到的内容。

Figure 15: “工作负载配置文件” ***(Profile Page)*** 页面上的“网络异常” ***(Network Anomaly)*** 选项卡



- **警报**：如果为网络异常规则配置了**警报**操作，则匹配的事件将显示在警报页面上，也可通过警报发布服务器获取。

Figure 16: 网络异常警报



规则严重性和网络异常评分

网络异常评分的计算方法与取证评分类似。对于每个工作负载，我们都会计算网络异常评分。工作负载的网络异常评分是根据该范围启用的配置文件在该工作负载上观察到的网络异常事件得出的。100分表示没有通过启用的配置文件中的配置规则观察到网络异常事件。0分表示检测到网络异常事件，需要立即采取行动。

- 严重性为“需要立即采取行动”(REQUIRES IMMEDIATE ACTION) 的网络异常事件会将整个范围的评分降低到 0。
- 严重性为“严重”(CRITICAL) 的网络异常事件会降低工作负载的评分，影响为 10。
- 严重性为“高”(HIGH) 的网络异常事件会降低工作负载的评分，影响为 5。
- 严重性为“中”(MEDIUM) 的网络异常事件会降低工作负载的评分，影响为 3。
- 严重性为“低”(LOW) 的网络异常事件不会计入网络异常评分。对于信号质量仍在调整且可能存在噪声的新规则，建议采用此方法。

对于每个工作负载，每 5 分钟将汇总一次影响总评分，以计算该工作负载在这 5 分钟内的评分。

对于未启用网络异常的传感器类型的工作负载，则网络异常评分为 N/A。

PCR 数据和网络异常事件保留

PCR 数据和网络异常事件会保留 7 天。

网络异常延迟

安全控制面板中报告的网络异常评分有 5 分钟的延迟。例如，上午 10:00 至 10:59 小时的工作负载评分基于上午 9:55 至 10:54 期间发生的网络异常事件

警告

- 旧的数据泄漏事件保留为数据泄漏事件，而不是网络异常事件。
- 按协议进行网络异常检测是 3.3 中的一项新功能，而旧的数据泄漏事件中没有设置协议。

进程散列异常检测

顾名思义，此功能通过评估整个系统中进程二进制文件散列的一致性来检测进程散列异常。此功能的动机如下。假设您有一个 Apache 网络服务器场，这些服务器是从相同的设置配置中克隆出来的（例如，这些服务器是从相同的自动化脚本中部署的）。您可以预期，所有服务器上的 httpd 二进制文件的散列值都相同。如果不匹配，则为异常，可能值得作进一步的调查。

在形式上，我们将进程组定义为同一根范围内跨工作负载的一组进程，这些进程具有相同的可执行二进制文件路径、操作系统版本和软件包信息（如果适用）1。

Note 自 3.4 版本开始包含软件包信息；在以前的版本中，进程组是基于可执行二进制文件路径和仅操作系统版本的组合定义的。

在上面的示例中，如果所有 Apache Web 服务器在 CentOS 7.7 上且在同一根范围内运行 httpd 2.4.43，则相应的进程组是具有相同组合的进程集（跨所有服务器）：`/ usr/sbin/ httpd` 及 `CentOS-7.7` 的操作系统版本及 `httpd-2.4.43` 的软件包版本。预计同一进程组中所有二进制文件的散列均相同，如果检测到任何不匹配，就会出现异常。

除了检测异常进程散列之外，此功能还检测已上传的已标记文件散列列表中显示的进程散列。这样做的原因是，您可能有一个已知恶意软件散列的列表，并想知道是否运行了与其中任何一个散列相关的进程。

为了减少误报，我们使用 NIST 提供的美国国家软件参考库参考数据集 (RDS)，也称为 NIST RDS 数据集来作为“良性列表”；良性散列被视为“安全”（有关如何启用 NIST RDS 数据集，请参阅“分析威胁智能报告”部分）。此外，您还可以查看“文件散列”部分，以便从您自己的散列“良性列表”上传。

除了 NIST RDS 数据集，我们还精选了 Cisco Secure Workload **散列判定**服务。启用该服务后，如果出现任何已知的恶意软件散列，就会被检测为恶意散列。但是，如果散列已知且合法，则在异常分析中也会将其标记为良性。由于数据集庞大且更新快速，可用于批准或红色标记工作负载上运行的进程，因此 Cisco Secure Workload **散列**判定仅可通过 Cisco Secure Workload 云获得。要确保可从设备访问 Cisco Secure Workload **散列**判定服务，请参阅“自动威胁智能更新”。

此功能的输出是称为**进程散列评分的安全评分**。此评分每小时计算和输出。与所有其他安全评分一样，进程散列评分越高，效果越好。特别是对于进程散列：

- 散列评分 0 意味着散列被标记或恶意。
- 散列评分 100 表示散列是良性的，或者在工作负载之间是一致的（无不匹配）
- 散列评分（1-99）表示散列被视为异常（即，存在一些不匹配）

工作负载的进程散列评分是在该工作负载中观察到的所有散列的最小进程散列评分，0 表示系统中存在标记或恶意进程散列，100 表示系统中未观察到散列异常。

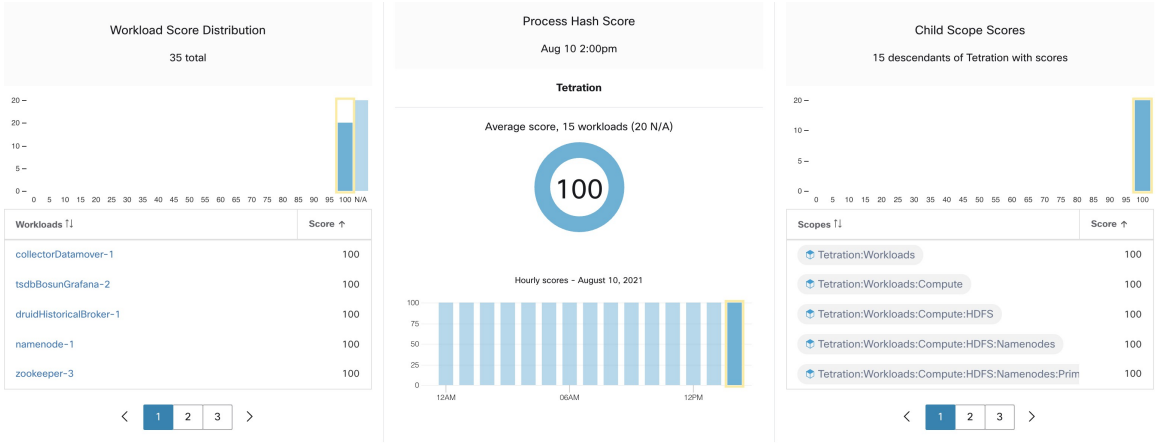
如何启用进程散列功能

默认情况下，在深度可视性代理和执行代理上启用进程散列功能；无需进行取证配置。如果您的系统中有此类代理，您应在系统启动后 2 小时内开始看到评分。

在何处查看进程散列评分

- 安全控制面板：

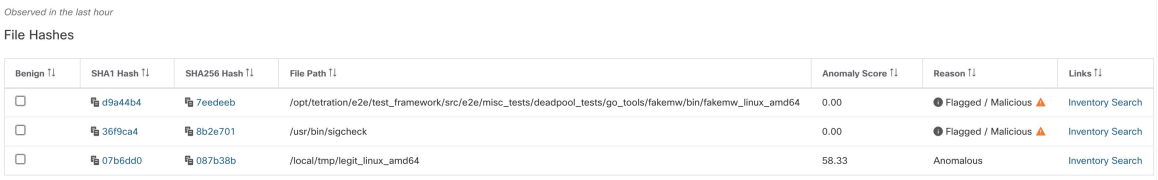
Figure 17: 安全控制面板中的“进程散列评分”***(Process Hash Score)*** 部分



安全控制面板中的“进程散列评分”(Process Hash Score) 部分

- 工作负载配置文件 **(Workload Profile)** 页面 / 文件散列 (File Hashes) 选项卡：

Figure 18: “工作负载配置文件”***(Workload Profile)*** 页面上的“文件散列”***(File Hashes)*** 选项卡



“工作负载配置文件”(Workload Profile) 页面中的“文件散列”(File Hashes) 选项卡

如何计算进程散列评分

对于每个进程散列，我们按如下方式计算评分：

1. 如果散列被标记或为恶意，则 `score = 0`

2. 否则，如果散列是良性的，则 `score = 100`
3. 否则，如果散列是异常，则 `score` 在 `[1, 99]` 范围内，越高越好。
4. 否则，`score = 100`

在(3)中计算评分的逻辑是，我们首先计算散列的少数评分（即1减去该散列在同一根范围下的工作负载填充中的填充比率），如果散列的少数评分高于0.5，则使用信息函数 `-log2(x)` 将其映射到范围 `[0.0, 1.0]`，然后将评分再次映射到范围 `[1.0, 99.0]`。让我们以上面的 Apache Web 服务器场为例，并考虑 `httpd` 的散列。以下是一些场景：

- 假设场中的1000台服务器中的 `httpd` 有两个散列值（`h1` 和 `h2`）：1台服务器中为 `h1`，其余999台服务器中为 `h2`。在这种情况下：
  - `population_ratio(h1) = 0.001, population_ratio(h2) = 0.999`. 然后：
  - `minority_score(h1) = 0.999, minority_score(h2) = 0.001`. 然后：
  - `score(h1) = -log2(0.999) * 98 + 1 = 1.14;`
  - 由于 `minority_score(h2) < 0.5, h2` 不被视为异常，因此 `score(h2) = 100`。
- 假设场中10台服务器中的 `httpd` 有两个散列值（`h1` 和 `h2`）：1台服务器中为 `h1`，其余9台服务器中为 `h2`。在这种情况下：
  - `population_ratio(h1) = 0.1, population_ratio(h2) = 0.9`. 然后：
  - `minority_score(h1) = 0.9, minority_score(h2) = 0.1`. 然后：
  - `score(h1) = -log2(0.9) * 98 + 1 = 15.90;`
  - 由于 `minority_score(h2) < 0.5, h2` 不被视为异常，因此 `score(h2) = 100`。
- 假设场中2台服务器中的 `httpd` 有两个散列值（`h1` 和 `h2`）：1台服务器中为 `h1`，另一台服务器中为 `h2`。在这种情况下：
  - `population_ratio(h1) = population_ratio(h2) = 0.5`. 然后：
  - `minority_score(h1) = minority_score(h2) = 0.5`. 然后：
  - `score(h1) = score(h2) = -log2(0.5) * 98 + 1 = 99.0`. 这是被视为异常的任何散列的最高评分。
- 假设 `httpd` 在所有服务器中只有一个散列值(`h1`)。在本例中，`minority_score(h1) = 0.0 < 0.5;` 因此，它不会被视为异常，并且 `score(h1) = 100`。

最后，工作负载的进程散列评分是在该工作负载中观察到的所有散列的最小进程散列评分。

有关 `-log2(x)` 信息功能的其他信息，请参阅此处。

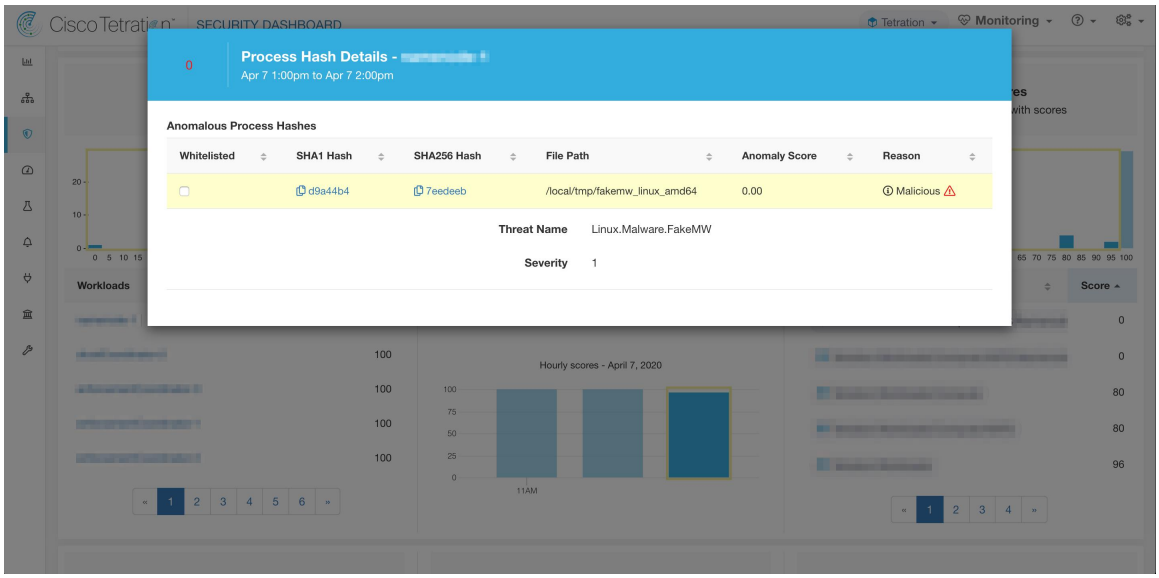
如何提高进程散列评分

如果某个工作负载的进程散列为 0，则表示该工作负载中出现了标记或恶意进程散列；防止此类进程再次运行可提高得分。如果进程散列小于 100，则表示系统中存在进程散列异常；这并非是恶意的，但值得进一步调查。仔细调查后，如果确定散列是安全的，则将其添加到良性列表也将提高评分。用户可以通过点击“文件散列/进程散列详细信息”(File Hashes / Process Hash Details) 页面中的良性复选框或通过 OpenAPI 上传良性列表，将异常散列标记为“良性”。

威胁信息详细信息

如前所述，如果启用 Cisco Secure Workload 散列判定服务，则任何已知的恶意软件散列在显示时都会被标记为恶意。在这种情况下，系统将提供恶意散列的更多威胁信息（通过我们的威胁智能平台收集）。目前，其他威胁数据包括威胁名称和严重性。威胁名称是威胁的名称，而严重性是一个介于 1-5 之间的值，表示威胁的严重程度，其中 1 表示最不严重，5 表示最严重。

Figure 19: 用户可以点击恶意散列行查看其威胁信息详细信息



警告

- 散列进程分析任务每小时运行一次，但在安全控制面板中显示预期评分/结果可能需要 2 个小时，具体取决于操作。例如：
  - 如果您上传了散列标记列表，并且该列表中的进程散列已显示出来，那么安全控制面板上可能需要 1 个小时才能反映出评分。
  - 如果从“已标记”(Flagged) 列表中删除散列，则可能需要 2 个小时才能清除，而评分也会反映在安全控制面板上。
- 保留：

  - 进程散列分析的详细结果会至少保留 7 天。

- “工作负载配置文件”(Workload Profile) 页面中的“文件散列”(File Hashes) 选项卡仅显示最近一小时内分析的进程散列详细信息。
- 以前版本的深度可视性和执行代理以及 AnyConnect 终端仅报告 SHA256 散列值。因此，这些代理不支持与 SHA1 散列标记/良性列表进行匹配。
- 会针对特定根范围计算进程散列评分。如果某一工作负载属于多个根权限，则该工作负载的进程散列评分是其所属所有根权限的最小评分。
- 为了进一步减少进程散列异常分析中的误报，我们还根据文件路径将所有 Cisco Secure Workload 代理二进制文件标记为良性。仅当这些散列值未出现在任何用户定义的散列列表中或未被 Cisco Secure Workload 散列判定服务标记时，才会使用此机制。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。