概览

好处

- **缩短事件分类时间：**安全信息和事件管理及威胁防御 (SIEM/TD) 平台使用 Cisco ISE 用户、设备类型、访问权限级别和状态信息来加快安全事件的分类速度。
- **通过区分用户、组和设备改进 SIEM 分析策略：**SIEM/TD 平台使用 Cisco ISE 用户和设备类型信息来创建专门针对用户、组或设备的分析策略。例如，具有访问高度敏感数据或移动设备的权限的用户。

思科身份服务引擎：与 SIEM 和威胁防御平台全面集成

概述

思科® 身份服务引擎 (ISE) 与领先的安全事件和信息管理 (SIEM) 平台以及威胁防御 (TD) 平台相集成，将安全事件分析及相关身份和设备情景融合为一个涵盖整个网络的视图。

Cisco ISE 使用思科平台交换网格 (pxGrid) 技术与领先的 SIEM/TD 合作伙伴共享情景数据。这些集成的解决方案支持安全分析师将更大范围的情景与安全警报相关联，从而快速轻松地评估安全事件的重大影响。借助 Cisco pxGrid 技术，SIEM/TD 系统管理控制台可以显示从 Cisco ISE 提取的有关安全事件的情景信息。

此类数据可包括用户的身份和访问级别以及他们所使用设备的类型。分析师可通过此类信息更快地确定事件发生的源头，是否需要进一步调查，如果需要，其紧急程度如何。然后，就可以使用 Cisco ISE 来对这些威胁采取相应的防范措施。这些解决方案与 SIEM/TD 平台实现集成后，还可以增强安全监视功能，包括移动感知的安全分析。通过 Cisco ISE 和 SIEM/TD 集成实现的增强功能，可简化威胁检测流程和 IT 执行响应的过程，并且大幅缩短修复网络安全威胁所需的时间。

解决方案如何发挥作用

- Cisco ISE 将其用户身份和设备情景信息提供给 SIEM/TD 合作伙伴平台。
- Cisco ISE 情景数据可用于为高风险用户群或设备创建新的安全分析类别，例如专门针对可访问高度敏感信息的移动设备或用户的策略。
- Cisco ISE 情景数据也可以附加到 SIEM/TD 合作伙伴系统中的关联事件，提供有关用户、设备和访问权限级别的更多情景信息。这些信息有助于分析师解读安全事件的重要意义。
- SIEM/TD 合作伙伴用户然后可以将 Cisco ISE 作为管道，在思科网络基础设施中采用相应的预防措施。Cisco ISE 可以根据自身针对隔离或访问阻止操作定义的策略对用户和设备采取此类操作。
- 所有这些功能都可以在 SIEM/TD 合作伙伴平台中进行记录和报告，从而提供涵盖整个网络的统一安全报告。

好处（续）

- **降低具有安全状态故障的设备带来的安全风险：**SIEM/TD 平台使用 Cisco ISE 终端状态信息创建专门针对具有不符合状态的终端的分析策略。
- **改进 Cisco ISE 遥测和事件数据的可视性和分析：**使用 SIEM/TD 平台来根据 Cisco ISE 事件数据的异常情况（例如超过身份验证尝试次数）进行具体分析并提供警报。

Cisco ISE 将收集和提供包括以下内容在内的情景数据：

- **用户：**用户名、IP 地址、身份验证状态、位置
- **用户类别：**授权组、访客、被隔离
- **设备：**制造商、型号、操作系统、操作系统版本、MAC 地址、IP 地址、网络连接方式（有线或无线）、位置
- **状态：**状态合规性情况、安装的病毒防护程序、病毒防护程序版本、操作系统补丁级别、移动设备状态合规性情况（通过移动设备管理 [MDM]、生态系统合作伙伴了解）

支持的 SIEM 和威胁防御合作伙伴

- **Cisco ISE 版本 1.2：**HP (ArcSight)、IBM (QRadar)、Lancope、LogRhythm、Splunk、Symantec、Tibco (LogLogic)
- **Cisco ISE 版本 1.3：**HP (ArcSight)、IBM (QRadar)、Lancope、LogRhythm、Splunk、Symantec、Tibco (LogLogic)、NetIQ

更多详情

有关每个 SIEM/TD 合作伙伴的其他产品信息，请参阅思科市场解决方案目录，地址：http://marketplace.cisco.com/catalog。