At-A-Glance

Cisco Identity Services Engine: Integration with SIEM and Threat Defense Platforms

Benefits

- **Decrease time to event classification:** Security information and event management and threat defense (SIEM/TD) platforms use Cisco ISE user, device-type, access-level, and posture information to expedite the classification of security events.
- **Improve SIEM analytic policies by differentiating users, groups, and devices:** SIEM/TD platforms use Cisco ISE user and device-type information to create analytic policies specific to users, groups, or devices. These can include, for example, users with access to highly sensitive data or mobile devices.

Overview

The Cisco® Identity Services Engine (ISE) integrates with leading security event and information management (SIEM) and threat defense (TD) platforms to bring together a networkwide view of security event analysis and relevant identity and device context.

Cisco ISE uses Cisco Platform Exchange Grid (pxGrid) technology to share contextual data with leading SIEM/TD partners. These integrated solutions give security analysts the ability to quickly and easily assess the significance of security events by correlating expanded context with the security alerts. Cisco pxGrid enables the SIEM/TD system management consoles to display contextual information pulled from Cisco ISE about a security event.

This data can include the identity and level of access of the users and the type of device they are using. Such information permits the analyst to more quickly determine where the event is coming from, whether it needs further investigation, and, if so, how urgently. Cisco ISE can then be used to take mitigation actions against those threats. These integrations with SIEM/TD platforms also allow for enhanced security monitoring, including mobility-aware security analytics. The enhanced capabilities from Cisco ISE and SIEM/TD integration streamline the process of threat detection, simplify execution of responses by IT, and greatly reduce the time to remediation of network security threats.

How the Solution Works

- Cisco ISE provides its user identity and device contextual information to SIEM/TD partner platforms.
- Cisco ISE contextual data is used to create new security analysis classes for high-risk user populations or devices, such as policies specific to mobile devices or users with access to highly sensitive information.

Benefits (Continued)

- **Decrease security risk from devices with security posture failures:** SIEM/TD platforms use Cisco ISE endpoint posture information to create analytic policies specific to endpoints that have a noncompliant posture status.
- **Improve visibility and analysis of Cisco ISE telemetry and event data:** Use SIEM/TD platforms to specifically analyze and provide alerts based on anomalies in Cisco ISE event data, such as excess authentication attempts.

- Cisco ISE contextual data is also appended to associated events in the SIEM/TD partner system to provide the additional context of the user, device, and access level. The information helps analysts to better decipher the significance of a security event.
- SIEM/TD partner users can then use Cisco ISE as a conduit for taking mitigation actions within the Cisco network infrastructure. Cisco ISE can undertake a quarantine or access-block action on users and devices based on policies defined by Cisco ISE for such actions.
- All of these functions can be logged and reported upon within the SIEM/TD partner platform, providing unified, network-wide security reporting.

Cisco ISE collects and delivers contextual data, including the following:

- **User:** User name, IP address, authentication status, location
- **User class:** Authorization group, guest, quarantined
- **Device:** Manufacturer, model, OS, OS version, MAC address, IP address, network connection method (wired or wireless), location
- **Posture:** Posture compliance status, antivirus installed, antivirus version, OS patch level, mobile device posture compliance status (through mobile device management, or MDM, ecosystem partners)

Supported SIEM and Threat Defense Partners

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

For More Information

Additional product information regarding each of the SIEM/TD partners may be found in the Cisco Marketplace Solutions Catalog at http://marketplace.cisco.com/catalog.

C45-728401-01 10/14