At-a-Glance

Cisco Identity Services Engine with Integrated Security Information and Event Management and Threat Defense Platforms

Benefits

- Decrease time to event classification by using Cisco® Identity Services Engine (ISE) contextual information to expedite the classification of security events.
- Improve SIEM analytic policies by differentiating users, groups, and devices using contextual information to create analytic policies specific to users, groups, or devices.
- Decrease security risk from devices with security posture failures by using 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 by analyzing and providing alerts based on anomalies in Cisco ISE event data, such as excessive authentication attempts.

Gain Visibility into Network Threats and Remediate

Cisco® Identity Services Engine (ISE) integrates with leading security event and information management (SIEM) and threat defense (TD) platforms to bring together a network wide 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 and TD partner solutions. The combination of these integrated technologies gives security analysts the ability to quickly and easily assess the significance of security events by correlating expanded context with the security alerts. Cisco ISE enables the SIEM and TD system management consoles to display contextual information pulled from the engine about each security event.

The data can include the identity and level of access of each user and the type of device used. This information permits the analyst to more quickly determine where the event is coming from, whether it needs further investigation, and, if so, how urgent is the threat. Cisco ISE can then be used to take mitigation actions. Cisco ISE integrations with SIEM and TD platforms also allow for enhanced security monitoring, including mobility-aware security analytics. The enhanced capabilities from Cisco ISE with SIEM and 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.

Next Steps

To learn more about the Cisco Identity Services Engine, visit http://www.cisco.com/go/ISE.

For additional information regarding Identity Services Engine SIEM/TD partners, visit http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html.

How Cisco ISE Integrations with SIEM and TD Solutions Works

The Identity Services Engine provides its user identity and device contextual information to SIEM and TD partner platforms. Then:

- 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.
- Appended to associated events in the SIEM and TD partner solutions to provide the additional context of the user, device, and access level. The information helps analysts better decipher the significance of a security event.
- Take mitigation actions within the Cisco network infrastructure. ISE can undertake a quarantine action on users and devices.
- Log and report within the SIEM and TD products, providing unified, network-wide security reporting.

Some of the main attributes of the Identity Services Engine available for use SEIM and TD for user- and device-related context are:

- **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 (MDM) ecosystem partners

C45-732858-02 05/17