Cisco ISE: SIEM and Threat Defense Ecosystem Integration

Overview

The complexity of network environments has driven the need for increased granularity in security monitoring, threat analysis, and compliance assessment. With the advent of mobility, "bring your own device" (BYOD) policies, software as a service (SaaS), and virtualization, it is no longer sufficient to analyze security activity associated solely with a broad identifier like an IP address. Today's diverse networks require effective security event visibility and integration with accurate contextual data such as user identity, user privilege levels, endpoint device type, and endpoint security posture to provide a meaningful picture of security events on the network and their significance.

The Cisco® Identity Services Engine (ISE) integrates with leading security event and information management and threat defense (SIEM/TD) platforms to bring together a networkwide view of security events supplemented with relevant identity and device context. This integration provides security analysts the context they need to quickly assess the significance of security events by being able to answer questions like "who is this security event associated with and what level of access do they have on the network" and "what type of device is it coming from" all within the SIEM/TD system.

Providing ISE user and device context to SIEM/TD platforms also enables a new suite of security monitoring capabilities such as mobility-aware analytics. SIEM/TD platforms may utilize Cisco ISE to take remediation actions in the Cisco network infrastructure. This suite of capabilities helps IT organizations increase the speed of threat detection and simplifies threat response.

Solution Highlights and Components

This solution is composed of Cisco ISE with an Advanced Feature License and a SIEM or threat defense platform from one of our integration partners (see list at end of this document). Integration with Cisco ISE enables SIEM/TD partners to supplement their networkwide security event visibility with information about user identity, network authorization levels, endpoint device identification, and security posture. This provides a composite, "single pane of glass" view of a security event from the SIEM/TD partner console. Partners are also able to take remediation actions via ISE; the solution provides complete visibility, contextual assessment, and remediation capabilities from the SIEM/TD partner platform.

ISE integration with SIEM/TD partners is accomplished through the following:

- Cisco ISE provides its user identity and device information to SIEM/TD partner platforms.
- This contextual data is used to create new security analysis classes for high-risk user populations or devices. A common application is to create analytic policies specific to mobile devices or users with access to highly sensitive information.
- 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, enabling analysts to better understand the significance of a security event.
- ISE contextual data can itself be a source of security insight. SIEM platforms can trend ISE data to discover abnormal or suspicious activity.
- SIEM/TD partners may utilize ISE as a conduit for taking mitigation actions within the Cisco network infrastructure. SIEM/TD platforms can instruct ISE to undertake quarantine or access-block actions on users and/or device based on ISE policies that have been defined for such actions.
- All of these functions can be logged and reported on within the SIEM/TD partner platform, providing unified, networkwide security reporting.

Some of the key ISE attributes collected by SIEM/TD partner platforms for user- and device-related context are:

- User: User name, IP address, authentication status, location
- User class: Authorization group, guest, quarantine status
- 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 (via MDM ecosystem partners)

Common Use Cases

- Decrease time to event classification – SIEM/TD platform utilizes ISE user, device type, access level, and posture information to answer common questions needed expedite the classification of and response to a security event.
- Scrutinize mobile and device network activity – SIEM/TD platform utilizes ISE device-type information to create security analytic policies specific to mobile devices. This enables a comprehensive view of the security status associated with the mobility environment.
- Differentiate privileges of users and groups – SIEM/TD platform utilizes ISE user information to create security analytic policies for specific users or groups, such as populations with access to highly sensitive data or less trusted populations (guests, for example).
- Scrutinize devices with security posture failures – SIEM/TD platform utilizes ISE endpoint posture information to create security analytic policies specific to endpoints that have a noncompliant posture status. These devices typically represent a higher security risk on the network.
- Visualize and analyze ISE telemetry and event data – Utilize the SIEM platform to specifically analyze and alert on anomalies in ISE event data, such as excess authentication attempts. This data may be presented visually to provide a security-specific dashboard related to ISE telemetry.

Benefits

- Increased effectiveness of SIEM and threat defense deployments
- Decreased time to detect, assess, and respond to security events
- Complete user/device visibility and control

Supported SIEM/TD Partners

As of Cisco ISE Release 1.2:

- HP (ArcSight), IBM (QRadar), Lancope, LogRhythm, Splunk, Symantec, Tibco (LogLogic)

For More Information

Additional product information regarding each of the SIEM/TD partners is available on the Cisco Developer Network Marketplace at http://marketplace.cisco.com/catalog.

Feature & Release Summary

	HP (ArcSight)	IBM (QRadar)	Lancope	LogRhythm	Splunk	Symantec	Tibco (LogLogic)
ISE Release Version	1.1 and 1.2	1.1 and 1.2	1.1 and 1.2	1.1 and 1.2	1.1 and 1.2	1.1 and 1.2	1.1 and 1.2
SIEM/TD Partner Release Version	ESM 5.x, 6.x; SmartConnector 6.0.7.xxxx	IBM Security QRadar SIEM v7.0 and v7.1	6.2 or later	6.0	5.0	4.8	5.4.0
SIEM Partner Integration Release Date	Q4R1 (Nov 2013)	Released	Released	Released	Jul 2013	Sept 2013	Released
Link to Partner Collateral on Cisco Developer Network Site	http://marketplace.cisco.com/catalog/companies/HP	http://marketplace.cisco.com/catalog/companies/IBM	http://marketplace.cisco.com/catalog/companies/Lancope	http://marketplace.cisco.com/catalog/companies/LogRhythm	http://marketplace.cisco.com/catalog/companies/Splunk	http://marketplace.cisco.com/catalog/companies/Symantec	http://marketplace.cisco.com/catalog/companies/Tibco
Correlation of ISE Context Data within SIEM/TD Analytics							
Device-Type	YES	YES	YES	YES	YES	YES	YES
Username/Identity	YES	YES	YES	YES	YES	YES	YES
Endpoint Security Posture Status	YES	YES	YES	YES	YES	YES	YES
User Network Privilege Level (Authorization Group)	YES	YES	YES	YES	YES	YES	YES
Authentication Status/Attempts	YES	YES	YES	YES	YES	YES	YES
Ability to Conjoin all ISE Context Data Above	YES	YES	YES	YES	YES	YES	YES
Use-Cases Supported							
Scrutinize Specific Device-Types (e.g. Mobile)	YES	YES	YES	YES	YES	YES	YES
Scrutinize Specific User-Types (e.g. Guest, Sensitive Users)	YES	YES	YES	YES	YES	YES	YES
Scrutinize Specific Classes of Users (e.g. IT Admins)	YES	YES	YES	YES	YES	YES	YES
Scrutinize Users/Devices with Posture Failures	YES	YES	YES	YES	YES	YES	LSP27 (Q4 2013)
Ability to Conjoin all Use-Cases Above	YES	YES	YES	YES	YES	YES	LSP27 (Q4 2013)
Visualization of ISE Context Data	YES	YES	YES	YES	YES	YES	TIBCO Iris 2.0.0 (Q1 2014)
Ability to Generate ISE-Specific Dashboard	YES	YES	YES	YES	YES	YES	TIBCO Iris 2.0.0 (Q1 2014)
Detect Anomolous Patterns in ISE Context Data	YES	YES	YES	YES	YES	YES	TIBCO Iris 3.0.0 (Q3 2014)
Long-Term Storage & Reporting on ISE Context Data	YES	YES	YES	YES	YES	YES	YES
Execute Network Actions from Partner Platform							
Block Network Access	YES	NO	2H13	YES	YES	NO	NO
Quarantine	YES	NO	2H13	YES	YES	NO	NO
ISE Context Data Collected							
See: http://www.cisco.com/en/US/docs/security/ise/1.0/user_guide/ise10_logging.html							

C45-728401-00 06/13