At-a-Glance

Benefits

- **Increase the accuracy and effectiveness** of vulnerability assessment platforms.
- **Decrease response time and complexity** when responding to vulnerability events.
- **Enhance security analysis** through deeper visibility into network vulnerabilities.

Cisco Identity Services Engine Integration with Vulnerability Assessment Platforms

Audit OSs, Endpoints, and Apps for Threats

Network environments have become increasingly complex with the multitude of devices that are constantly being given access. This new network complexity has highlighted management issues related to security such as the limited analysis capabilities of traditional solutions, and the inability of many solutions to comply with industry security requirements. It was once sufficient to analyze network vulnerabilities using broad identifiers such as an IP address. However, the increase in mobile traffic and devices, bring-your-own-device (BYOD) initiatives, software as a service (SaaS), and virtualization have contributed to the need for deeper network security visibility and more fine-grained analysis. Vulnerability assessment tools enable the audit of operating systems, servers, network devices, databases, and web applications for known or potential vulnerability threats.

Cisco® Identity Services Engine (ISE) shares accurate contextual data, such as user identity, user privilege levels, endpoint device type, and endpoint security posture through the engine's Cisco Platform Exchange Grid (pxGrid) technology, with vulnerability assessment platforms. Together, they deliver in-depth network vulnerability visibility along with relevant identity and device context. The integration of these leading-edge security solutions gives security analysts the ability to assess the significance of a vulnerability event by correlating the context of the event within a vulnerability management platform console. This creates a detailed picture of the risks each vulnerability represents and the ability to take immediate action on the most egregious ones.

How Cisco Identity Services Engine Integration with Vulnerability Assessment Platforms Works

- Provides user identity and device/contextual information to vulnerability assessment platforms.
- Generates a complete view of vulnerability event, identity, and device data. The information is used to rate the severity of vulnerabilities, which then allows vulnerability events and responses to be prioritized.

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 Vulnerability Assessment partners, visit http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html.

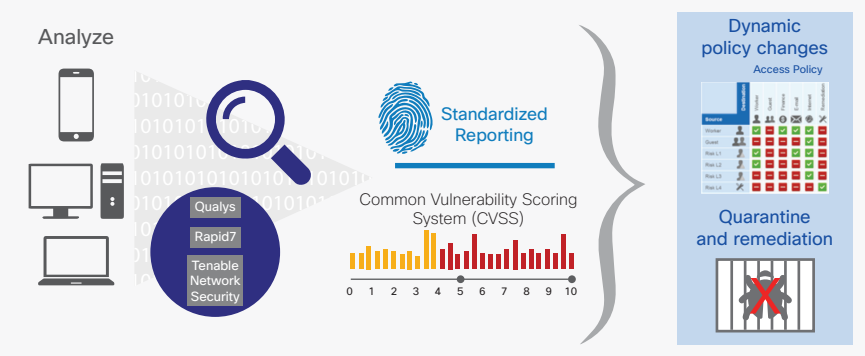
- Take mitigation actions within the Cisco network infrastructure. The engine can undertake a quarantine or block access to specific users and devices based on policies defined by the engine for such actions.
- Log and report upon within the vulnerability assessment platform, providing unified, network-wide security reporting.

Some of the main Identity Services Engine attributes available for use by vulnerability assessment platforms 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

Introducing Threat-centric NAC

You can also enable intelligent, automated policy updates based on vulnerability data, ensuring that your policies are always up to date based on the latest vulnerability levels. Cisco ISE uses standard Common Vulnerability Scoring System (CVSS) scores to assign a 1-10 score to each vulnerability, helping you investigate the most important items. Threat-centric NAC is an advanced use case for the Cisco ISE Rapid Threat Containment solution.



C45-733044-02 05/17