

Products

PRODUCTS & SERVICES TO SECURE YOUR ENTERPRISE

VULNERABILITY MANAGEMENT

Security Center 3.0

Tenable Network Security

www.tenablesecurity.com

Price: Starts at \$15,750, plus \$3,150 for annual maintenance for a 500-host license

Vulnerability management is a complex, dynamic and absolutely essential security process. Tenable Network Security's Security Center 3.0 is the company's most comprehensive solution yet, helping organizations throughout the VM life cycle from asset discovery to remediation.

Tenable, which is closely identified with its popular Nessus VA scanner (the newest version is no longer open source), has developed an asset-centric management tool, allowing an admin to manage, analyze and respond to vulnerability data from one Web console.

In addition to Nessus, Security Center brings an impressive array of VM tools to bear, employing a passive scanner, log correlation engine and the capability to read data directly from many popular IDS/IPS products, including those from Snort, Cisco Systems, Enterasys, ISS, McAfee, TippingPoint, NFR Security, Juniper Networks and Forti-net. The combination of active and passive scans gives admins an accurate assessment of what's on their network, and what's vulnerable. Security Center can also import an organization's existing asset lists from other sources.

This asset and vulnerability information is helpful in assessing the actual risk presented by threats detected through the corroborating evidence gathered from intrusion detection feeds and log correlation.

Through the Web-based management interface, admins can configure the console, update plug-ins, and add the Nessus, passive IDS sensors and log correlation engines. The interface is also used to create and manage the hierarchy of assets, users and managers.

Asset-centric structuring allows the delegation of responsibility for assets and networks to individuals. Within an enterprise, the admin defines all of the assets and networks (assets can also



Tenable Network Security's Security Center 3.0 covers the vulnerability management life cycle from asset discovery to remediation.



be created dynamically from scan data), and identifies and assigns specific assets to each security manager.

The Nessus active scanner is one of the most comprehensive available, with thousands of checks. The passive vulnerability scanner adds detection of vulnerabilities that are not possible with any active scanner. It sniffs traffic and can identify things such as out-of-date Web browsers and e-mail clients, and will discover services running on nonstandard ports. It also has the advantage of being "always on," constantly scanning for changes and new assets.

The log correlation engine allows analysis from network devices such as firewalls, routers and servers—basically as a SIM/SEM tool. It provides data that can be used in incident response and detects impending and ongoing attacks.

All the data is collected and displayed within the console, where you can drill down in a vulnerability to see all the hosts with the issue and view the IP to see the data for that host. The data also provides relevant information, such as mitigation solutions and external resources like CVE numbers. The proprietary ticketing system is also controlled through this interface, so you can open and track remediation orders.

The Passive Vulnerability scanner and Log Correlation Engine are purchased separately, but Security Center is still a strong tool with just the Nessus scanner. The complete package, however, will give your organization one of the more comprehensive VM solutions available. ▶

—BRENT HUSTON

Test Notes

- ↑ Deep correlation capabilities
- ↑ Active and passive scanning
- ↑ Admin delegation
- ↑ IDS/IPS support

Reprinted with permission from Information Security Magazine, July 2006.

© 2006 TechTarget. All Rights Reserved. FosteReprints: 1-866-879-9144