SecurityCenter Evaluation Guide

INTRODUCTION

The purpose of this document is to highlight the core features of SecurityCenter for users undergoing an evaluation. This document also serves as a checklist for the evaluation to help users determine the usefulness of the SecurityCenter within their network security infrastructure. SecurityCenter has many options, settings and functions that allow it to integrate with and perform security checks and intrusion management for a wide variety of enterprise networks. Another great place to start off with is the SecurityCenter documentation, located on the Tenable Support Portal.

DEPLOYMENT CONSIDERATIONS

1. **How many Nessus Scanners are you going to use?**

   Many customers typically deploy just one Nessus scanner on SecurityCenter for an evaluation. Additional scanners can be added on remote machines and remote networks. Multiple scanners greatly reduce the impact to the network infrastructure and decrease your scan time by several factors.

2. **How many IPs are going to be managed through SecurityCenter?**

   For testing purposes, please over estimate the number of IP addresses you have. If you have five "Class C" networks, please feel free to ask for a 1,275 active IP address demo license. This helps to get a more accurate determination of the number of IP addresses you will want to license.

3. **How many different networks are you going to break into separate "organizations"?**

   One of the best features of SecurityCenter is the ability to create multiple "organizations". An organization is a completely autonomous set of SecurityCenter users and IP addresses. For example, a University could have a unique SecurityCenter organization for each of its separate Schools of Health, Science and Engineering. For testing purposes, please feel free to place your entire network address range into one organization. However, when considering an operational deployment of the SecurityCenter, please keep in mind that several organization instances can be created and reported on as a unique entity. There is no additional cost in maintaining multiple organizations.

4. **What asset lists would you like to create?**

   SecurityCenter supports creation of both static and dynamic asset lists. Configuring your SecurityCenter with various assets lists allows you segregate what information users can view by limiting the users to only information about certain asset lists. It also facilitates scanning, reporting, analysis and trending. If you do not know what your assets are, you could simply create some static rules to configure the SecurityCenter with basic lists. If you have performed some scans, you could also use some of the pre-configured dynamic asset list templates that can create lists of discovered web servers, email clients and Windows operating systems.

5. **Who do you want to have accounts for on SecurityCenter and with what privileges?**

   SecurityCenter supports a model where all of its users exist within the security group or where all users are either part of security or part of IT or network engineering. These non-security users (referred to as end users) can have different access and scanning privileges. Tenable strongly encourages you to discuss SecurityCenter features with your IT department and get their input for how SecurityCenter will affect their daily tasks and performance.

6. **Are you going to use the recommendation and remediation workflow process to manage the vulnerability patching process?**

   SecurityCenter can help security groups issue recommendations for specific vulnerabilities. These recommendations can be sent for a vulnerable system, all systems with that vulnerability or to all particular assets (such as the Cisco routers on the New York network) with that vulnerability. As systems are patched, the SecurityCenter can track which administrators have mitigated their vulnerabilities or still have vulnerable systems. In addition, if multiple organizations are configured, the SecurityCenter will be able to show which business units of your company have been notified about a vulnerability, when they were notified and what they have done over time to mitigate it. This is a very powerful feature of the SecurityCenter and is useful to demonstrate in your testing.

7. **Are you going to use the IDS/VA correlation?**

   Many Tenable customers have the vulnerability assessment and management function performed by one group and intrusion detection performed by another. If this is the case, the LCE can still be used to pass through a feed of real-time IDS events and then pass back new alerts when a correlation between an IDS event and a vulnerability has occurred.

   In general, if the LCE is to be used as an IDS event aggregator, IDS/VA correlation is more or less automatic. Care should be taken to read the "LCE Administration and User Guide", which describes how to configure the LCE and a variety of supported NIDS devices to work together.

8. **Which IDS systems are you going to point to the LCE and how many?**

   For most customer implementations, the LCE will need to read IDS events via syslog or SNMP traps. This means that Snort sensors will need to send syslog messages to the LCE. Aggregated Snort syslog messages can also be sent to the LCE, but the LCE has no provision to read flat files and needs to accept the log messages "live". For other NIDS devices please refer to the "LCE Administration and User Guide".

9. **Are you going to use the Passive Vulnerability Scanner?**

   It is strongly recommended that anyone evaluating the SecurityCenter also consider using the Passive Vulnerability Scanner (PVS). The PVS can provide all of your vulnerability information without any active scanning. The PVS can feed its data into the SecurityCenter 24x7 so the SecurityCenter always has the latest vulnerability

information. For more information, please refer to "Passive Vulnarbility Scanner User Guide" located on the Tenable Support Portal.

VULNERABILITY SCANNING

1. **What scanning policies are you going to use? Have you created your own?**

   When performing a scan with the SecurityCenter, the performance and detection of vulnerabilities is highly influenced by the vulnerability policy in use. Tenable ships SecurityCenter with a number of policies that can be used to simply map your topology, run a patch audit with local security checks or perform a full vulnerability assessment. The more powerful feature that may not be apparent during testing is the ability to add your own custom vulnerability policies. These policies can be very useful for solving many of your specific business security issues such as finding unauthorized devices running a particular service or scanning for a recent worm outbreak.

2. **Are you going to schedule scans?**

   SecurityCenter can be used to perform a scan immediately, or schedule a scan to occur each day, each weekday, once a month and many other combinations. Different SecurityCenter users can each independently issue their own scanning schedules and results from scheduled scans can be automatically emailed to the system owners.

3. **Have you read through the list of scanning plugins available? Do you understand how the plugins work?**

   Tenable Network Security, Inc. is the author and manager of the Nessus vulnerability scanner and releases many new vulnerability checks called "plugins". When managing the SecurityCenter's vulnerability policies, plugins can be enabled or disabled depending on scan requirements. For example, to scan mail servers, enable the SMTP family of plugins.

VULNERABILITY MANAGEMENT CONSIDERATIONS

1. **Have you looked through all of the tools available when viewing vulnerabilities?**

   Some evaluation customers never discover some of the key features in SecurityCenter that could be very important to them. For example, SecurityCenter can produce an extremely robust topology map that is derived from the vulnerability scan. SecurityCenter has a number of tools that sort the vulnerabilities and provide the logic behind the reporting engine. We highly recommend that evaluators of SecurityCenter review the output of each tool.

2. **Have you marked any of the vulnerabilities as false positives?**

   Once vulnerabilities have been detected, SecurityCenter can be used to highlight one or more vulnerabilities as a false positive. A false positive can be issued so that the vulnerability will not appear in reports and the user interface. With a click of a button though, the vulnerability can be unmasked. When choosing which vulnerabilities are

false positives, asset information can also be applied. For example, this allows an Apache vulnerability to be labeled a false positive on all Cisco routers.

3. **Has your system admin logged in to see the list of tickets you have created for them?**

   Once a recommendation for a vulnerability is issued, the network administrators can be notified via email that they have a security hole that needs to be fixed and how they should fix it. When these users log into SecurityCenter, they can see all of their vulnerabilities and, with a click of the button, filter out any vulnerability that does not have a corresponding security recommendation.

4. **Have you patched vulnerabilities, run secondary scans and witnessed the remediation of the vulnerability?**

   SecurityCenter tracks vulnerability remediation actions by scanning for and observing that a vulnerability is no longer present. Each time a scan is completed, the scan is imported to the "cumulative" set of vulnerabilities. This is the most recent scan data and is both additive and subtractive. If a new vulnerability is discovered, it is added to the cumulative list of vulnerabilities. If an old vulnerability is tested for and not seen again, it is moved out of the cumulative database and into the "mitigated" database.

5. **Have you generated reports?**

   It is extremely easy to generate PDF and CSV reports from the SecurityCenter. Once a set of scan data has been created within SecurityCenter, it is highly recommended that the user generate one or more reports. These reports can contain enormous amounts of data and can also be filtered down to the tiniest detail. The reports are also hyper-linked, so it is very easy to send a document to someone and have them navigate the various reports and tables.

IDS EVENT ANALYSIS CONSIDERATION

1. **Have you witnessed the correlation?**

   If IDS events are being fed into the LCE, a simple selection of the event filter "Targeted IDS Events" checkbox will match on any IDS event that correlates with a known vulnerability. If there has not been any vulnerability scanning, correlation will not occur. Similarly, if IDS traffic is pretty light or filtered, there may not be any IDS events that correlate with a known vulnerability.

2. **Has it enabled you to cut down on the IDS events you need to analyze?**

   Knowing which IDS events target vulnerable systems also can help identify which signatures are generating too many false positive alerts.

3. **Has it enabled you to pinpoint the real intrusions that need immediate attenuation?**

   If the LCE is exposed to "live" IDS feeds and these events can be correlated against the set of "real" network vulnerabilities, the user can see what systems are being

targeted. Tenable has had experience with customers who were able to find real intrusion attempts during their testing of SecurityCenter that were otherwise hidden in the millions of events generated each day by their NIDS device.

4. **Have you distributed this information to system administrators that are responsible for these assets?**

SecurityCenter can also reach out to the systems administrators who are managing the systems that are determined to be under attack. These emails highlight that a server has a particular vulnerability and an attack has been detected for which there is a likely chance of compromise. These messages can be instantly communicated to each system administrator who has a system that has been compromised. Consider a worm outbreak in which an IDS sees one valid attack after another. Alerting each system administrator is inefficient, and there is no guarantee that each attack has succeeded. However, with SecurityCenter, only the system administrator for servers that are known to still be vulnerable to an attack will be notified.

ABOUT TENABLE NETWORK SECURITY

Tenable Network Security, the leader in Unified Security Monitoring, is the source of the Nessus vulnerability scanner and the creator of enterprise-class, agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure network security and FDCC, FISMA, SANS CAG and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit http://www.tenable.com/.

Tenable Network Security, Inc.
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410.872.0555
www.tenable.com