tenable network security

Outcome Based Security Monitoring in a Continuous Monitoring World

December 2012

Ron Gula
Chief Executive Officer / Chief Technology Officer

Introduction

Technology has advanced sufficiently enough such that vulnerability management can be performed in near real-time at large scale. Because of this, outcome based security monitoring for large enterprises is now possible with “big data” types of analytics.

At the recent 2012 ITSAC conference in Baltimore, John Streufert, the Director of the National Cyber Security Division of DHS, outlined five recommendations for achieving continuous monitoring. These were:

1) Scan daily, at least every 36 to 72 hours
2) Focus on attack readiness
3) Fix daily
4) Grade personally
5) Hold managers responsible

These recommendations are a key component of the government’s CyberScope program. CyberScope has been deployed across the US Federal Government, many state and local governments, and increasingly in private commercial, financial, manufacturing, energy and academic organizations. Although the CyberScope program mandates monthly reports, many organizations internally perform real-time or near daily security assessments.

Continuous monitoring brings the same level of effort and analysis to proactive security monitoring as with historically defensive strategies such as virus scanning and network intrusion detection. Rather than searching for attackers continuously, organizations that practice continuous monitoring react in real-time to new vulnerabilities and threats.

I agree with his points, but what I hadn’t fully realized until recently was that the majority of sizeable organizations performing vulnerability management today are still in the dark ages. Most organizations discover vulnerabilities at too slow of a rate to efficiently manage or react to them, and they don’t communicate what needs to be fixed very well. They are caught in a constant struggle of not having the right information and/or not having the right resources to mitigate security issues.

The high velocity nature of continuous monitoring creates the opportunity to make vulnerability management a “big data” problem. The data collected by numerous sensors can be leveraged to both model and measure large organizations in near real-time. This data helps drive better decisions, identify trends before they are problems, make better policies, and make asset owners more accountable for the systems they are managing. The data allows for true “outcome based” security measurements of different IT organizations, assets, or business units. The outcomes that executives and management can ask for can be tracked in real-time and not be constrained, modified or distorted by human intervention, politics or the lack of an ability to track this information.

In this whitepaper, we will discuss how Tenable’s solutions can help commercial and government organizations achieve these goals for their continuous monitoring programs. Tenable’s approach leverages distributed scanning, sniffing and log analysis to perform flexible, scalable and near real-time vulnerability detection for any size of network. More importantly, Tenable’s solution also includes advanced analytics, which score, alert, trend and visualize the vulnerability data by business unit, asset owner or technology platform. We will show how an organization of any size can set goals for their desired security outcomes and track how well each business unit performs to meet these goals.

Step 1 - Daily Scanning

For enterprise networks and even smaller SMB networks, it’s possible to perform vulnerability assessments daily if you deploy dedicated scanners, agents or sniffers. Historically, a vulnerability scanner was turned on once a month, a scan was performed, and a report was emailed to the IT group. However, today’s technology that leverages distributed scanning and network monitoring has progressed such that near instant assessments of even the largest networks can be performed.

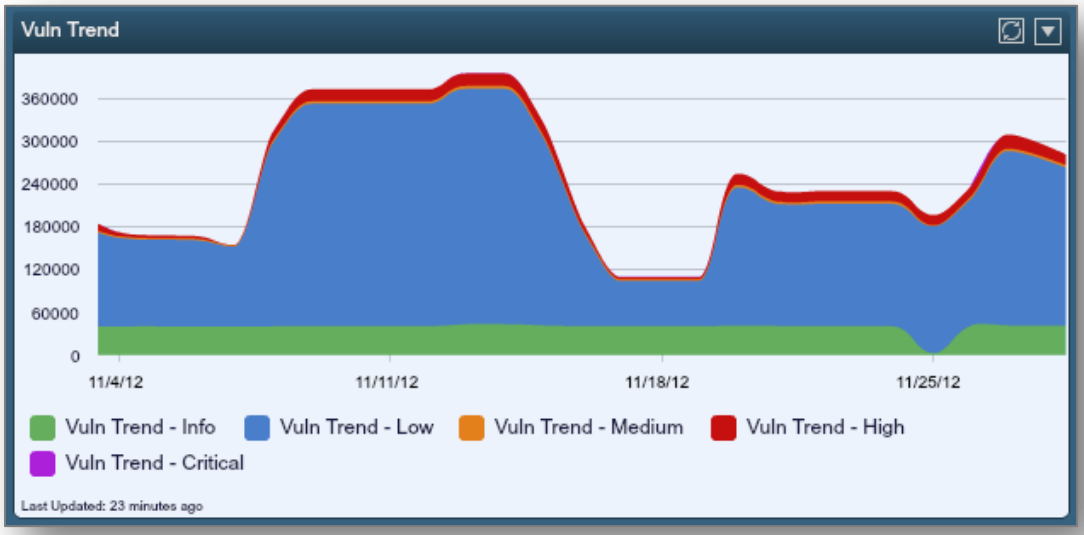
The threat of not scanning in real-time is very high. On any given week, Tenable’s Research team will ship 100 to 500 new Nessus and Passive Vulnerability Scanner plugins, which detect zero–days, disclosed vulnerabilities and out-of-cycle

emergency vendor patches. Waiting even once a month to perform a security assessment almost guarantees that your scans will identify critical security issues that need to be addressed. Since Tenable added malware and botnet detection into Nessus, a new trend our customers are finding is that unpatched and vulnerable systems now also have intruders on them.

To scan at scale and in near real-time, Tenable has many customers who deploy the SecurityCenter Continuous View solution. This solution allows an unlimited number of Nessus scanners as well as an unlimited number of Passive Vulnerability Scanner sniffers to be managed centrally by SecurityCenter. Discovery scans, real-time vulnerability sniffing and credentialed patch and configuration audits can all be managed from one spot. Organizations of any size can balance real-time vulnerability discovery and change detection with in-depth credentialed patch and configuration audits.

Tenable's products scale to extremely large networks. We've worked over the past ten years to optimize both credentialed scanning and un-credentialed scanning on networks of over 100,000 hosts in size. For active scanning, networks of this size will deploy between 10 and 100 Nessus scanners, depending on their topology and network access rules. For passive monitoring, PVS sensors are deployed on key choke points or alongside common applications and destinations such as virtual servers and email servers. Customers of this size organize and optimize their deployments to ensure scanning can be concluded in less than 24 hours.

Below is a screen shot of a SecurityCenter dashboard component that has graphed all vulnerabilities found from sniffing, scanning and credentialed patch auditing over a twenty-five day period for more than 15,000 hosts.



The data stream represents close to 40 billion tests performed by Tenable's SecurityCenter Continuous View (CV) solutions during this time frame. At its peak, there were more than 360,000 unique vulnerabilities reported.

Making sense of this data and trying to determine any impact to an organization's risk, compliance or attack profile would be difficult if it were not for the advanced filtering and "big data" analytics offered by SecurityCenter. For example, in the below screen shot, a dashboard was created for the same time frame which shows "new" vulnerabilities and vulnerabilities that were "Internet facing".

Being able to create queries, reports and dashboards that answer key business risk questions is critical to making sense of the vast amount of vulnerability data collected by Tenable's solutions.

The combination of active and passive analysis provides more actionable security data for any IPv4 or IPv6 network than any solution available on the market today. It also uniquely uncovers and audits all mobile devices that are in use on the network or are connected to your network. Support for analysis of IPv6 networks, which are measured in the trillions of potential IP addresses, is also provided by the SecurityCenter CV combination of active and passive discovery. Tenable also recently shipped the ability for Nessus to cross-reference vulnerability checks with enterprise patch management systems. We've encountered customers who thought that their patch management system was working flawlessly, when in fact there were entire classes of patches not being deployed.

Tenable has deployed SecurityCenter CV to many organizations, including large financial and large government networks. The Department of Defense standardized on leveraging Tenable's active and passive discovery for each of its four armed service branches. Organizations, such as SANS and Gartner, are also advocating passive network monitoring as a form of real-time network discovery and monitoring.

Without real-time discovery of new systems, new applications and new vulnerabilities, it is impossible to achieve the other four points outlined by Mr. Streufert because the data to drive the metrics isn't up to date. Tenable increases your confidence in making security decision, reduce time in identifying vulnerabilities, and in essence reduce operational overhead by allowing the administrator to tend to the highest risks in your organization.

Step 2 - Focus on Attack Readiness

Putting an organization on a footing of attack readiness is different than managing historical patching windows. During the past two decades, I've seen organizations move from not having any real sense of central security monitoring to one of "patch windows".

A patch window is a period of time that an organization gives an asset or business unit to apply patches. Today, many organizations have created dashboards and metrics reporting that is focused on applying patches at scale, but not necessarily focused on measuring an organization's real exposure to attacks. This gives organizations a false sense of security. Applying patches is still very important, but understanding how an asset can be exploited is even more crucial.

For example, consider the following dashboard created by SecurityCenter that graphs 25-day vulnerability trends for six different asset groups:

The green line represents any vulnerability with a CVSS score greater than 7 and the blue line represents any vulnerability with CVSS vulnerability older than 30 days. In general, there is improvement in both the reduction of older vulnerabilities and actual vulnerabilities for each asset. These types of graphs are very useful to compare vulnerabilities, and more importantly, attack readiness, from different business units.

Now consider the following new graph based on the same data in the previous example in which the number of exploitable vulnerabilities is graphed over time in yellow.

For Asset 2 and Asset 6, the number of exploitable vulnerabilities is actually higher or near the same as vulnerabilities with CVSS scores greater than 7.

Conventional and historical thinking says that it is unreasonable to expect all patches to be applied right away, so a patch window is given to allow IT managers a reasonable amount of time to fix any security issues. From an attacker's point of view though, it guarantees that any exploit disclosed today will work for some time on enterprise networks.

The "patch window" type of report does not consider the context of where a system is on a network. Is it behind a firewall? Is it an IT administrator's computer? Is it a sales person's laptop running in a hotel? Tracking whether a computer is patched or not is much simpler than tracking if a computer is something that can be directly attacked from the Internet, or something that could be used to leap-frog into an organization's critical systems.

Tenable's approach to understanding and visualizing attack readiness combines auditing for patches, auditing how well the system can resists an attack, and identifying systems that are exploitable or could be used to leap from into other systems. There are four steps of data collection and analysis by the SecurityCenter CV solution:

- Detect vulnerabilities, network trust and Internet access relationships in as near real-time as possible using sniffing and credentialed scans.
- Correlate each patched, scanned or sniffed vulnerability with any public exploits from popular penetration testing tools and products.
- Leverage attack paths and trust relationships to see which vulnerabilities are directly exploitable from the Internet, from Internet browsing or from internal privileged access.
- Associate these exploit paths on a per asset basis so they can be prioritized and mitigated with patching, firewall rules, proxies, etc.

Gathering vulnerabilities and correlating them to exploits is very useful. It allows us to see which assets are most likely exploitable by real server and client-side attacks. Tenable's approach of also including network trust and access information allows for automatic identification of trusted systems such as IT administrators, common servers accessed by many, and systems with both local network and Internet access.

With this information, SecurityCenter can be used to identify hosts in the following three classes:

1) Hosts that are directly exploitable from the Internet.

2) Internet browsing clients that have client-side exploitable software

3) Trusted systems which are accessed from hosts in category #1 or #2

Leveraging connectivity data from the PVS or from Nessus' netstat credentialed audits allows for the identification of which systems are clients and which systems are servers. Knowing these relationships allows for SecurityCenter users to understand which of their servers are being administered from vulnerable clients.

To learn more about this approach, please read the Tenable's "Predicting Attack Paths" paper, watch the webinar, or watch any of the YouTube videos featuring 3D attack path visualization.

Many of our customers have told us that they have to work very hard to obtain similar reports out of their GRC solutions – whether home grown or commercial – and don't get anywhere near the real-time capability needed to perform continuous monitoring. Tenable has worked with many organizations that have migrated from manual point scanning to centralized scanning and sniffing, and have had to completely rethink their compliance reporting because it didn't scale.

Step 3 - Fix Daily

The days of performing vulnerability scans once a quarter and sending a giant report to the IT groups are long gone. Also quickly approaching an end is "boutique vulnerability management", where the security group selects specific patches and asks the IT administrators to apply them. Because of the increased risk to IT assets, administrators are being asked to patch more often, sometimes approaching a daily patch rate.

Many years ago, there was no confidence in applying patches from leading vendors such as Microsoft, Adobe or Cisco. However, today we have almost a decade of patch application through hot updates, direct pushes from the vendor, and pushes of patches through patch management systems in an automated fashion, as well as easier ways to perform rollbacks. Because of this confidence, we see less emphasis on testing patches for an extended period of time to ensure they didn't break anything and more focus on pushing patches out quickly.

Tenable's approach to tracking daily fixes involves multiple technologies.

Passive monitoring can be used to track networks for which the security team may not have permission to scan, or only permission to scan with credentials to get missing patch status. When managed by SecurityCenter, passively obtained vulnerability data can be tracked for age of vulnerability, when it was first seen, when it was last seen, and if it recurred again. Active scanning with Nessus can provide exact vendor-agnostic patch information without deploying an agent on the scanned systems. SecurityCenter also keeps a history of which vulnerabilities have been fixed and can identify if a "fixed" vulnerability has come back again. This is important because unlike a new vulnerability that simply needs to be patched, a recurring vulnerability is one that results from a "broken" IT process. In these cases, the process needs to be fixed.

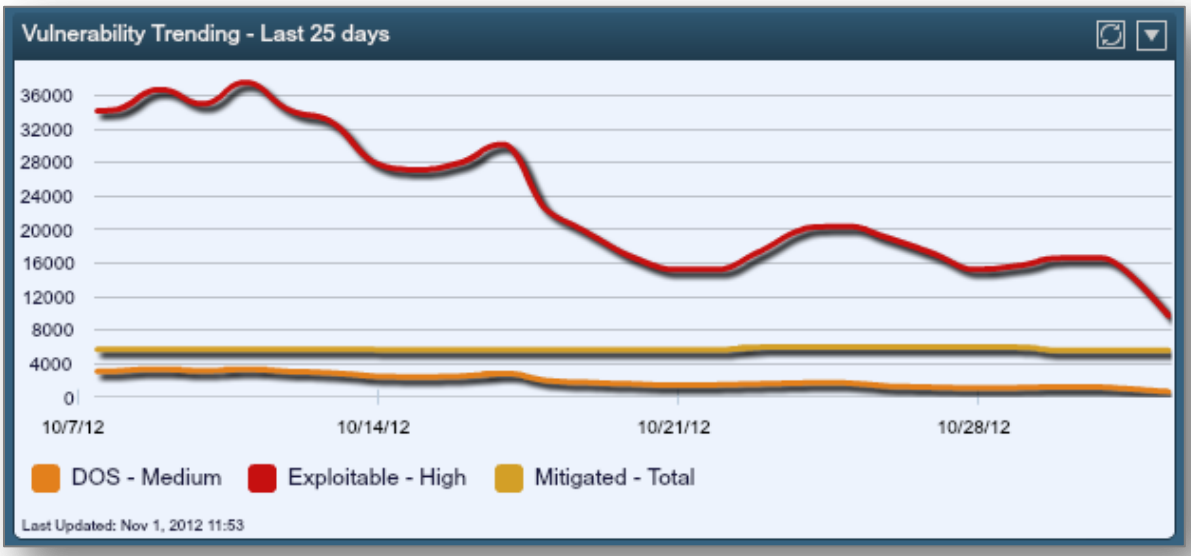
Finally, Tenable's Log Correlation Engine can be used to track vulnerabilities from log normalization. Logs can indicate patches being installed, software being removed and many other types of changes. The normalization scheme for the LCE is focused on making it easy to see this type of change and identify when systems have been modified.

Tenable's SecurityCenter also implements the concept of a default "cumulative" view. In the vulnerability scanning industry, the concept of working with individual scans is embedded into fifteen years of operational security, consultative engagements and annual audits. With continuous monitoring there is no individual scan. In fact, monolithic scans which used to try to do every type of test can be replaced with more efficient types of scans, especially when augmented by continuous passive discovery with distributed PVS sensors.

Another key aspect of the cumulative view in SecurityCenter is that everyone in the organization authorized to see vulnerability data for a host or asset gets to work with the latest data immediately. There is no extensive escalation or redaction process to distribute security findings. Once a system administrator is given access to the security of an asset, they will be working with the latest vulnerabilities. This has many advantages over manual scan distribution.

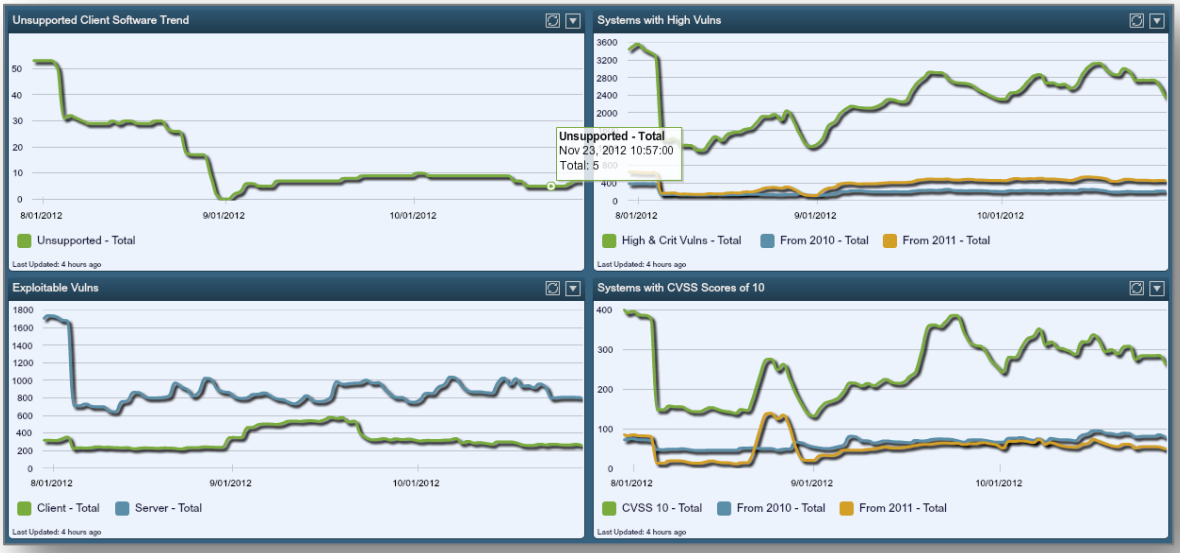
Depending on the size and complexity of your organization, all or some of these technologies can be leveraged to track what sort of security exposures exist on a daily basis. More importantly, if the goal is to patch on a daily basis, using this level of automation and tracking can audit daily progress and focus on where those efforts should be best spent.

As we've seen in the previous "Focus on Attack Readiness" section, daily vulnerability detection can help track daily patch administration. Progress, such as even one patch being applied at a time, can still be accounted for on large-scale networks. For example, passive detection of client-side security issues can be discovered at scale to produce trend charts such as this:



This trend line was produced completely through passive analysis. No interaction with target systems, their IT staff, or running scans was needed to show progress in tracking a daily reduction in the number of exploitable systems (shown in red).

It's also possible to graph a wide variety of daily changes on the network. Consider the following dashboard that shows occurrences of unsupported client software, client and server exploitable vulnerabilities, systems with critical vulnerabilities from 2012 (and also 2010 and 2011) over a six month period.



Being able to view this patching data in near real-time and a long term trend view allows organizations of any size to track their daily progress towards an enhanced security profile.

Step 4 - Grade Personally

Tenable's SecurityCenter offers many different methods to associate people with IT assets. Risk managers, IT administrators, asset owners and many other different types of both political and administrative "owners" can easily be associated with "assets". More importantly, when a person is associated with an asset, issues can be scored multiple ways to provide the organization with many different ways of measuring how good a person, or the group a person is managing, is doing at managing risk.

Each asset defined in SecurityCenter can be a list of IP addresses or DNS names. Combinations of network ranges can also be used. Lists can be composed by manually importing them from other systems; pulling them from LDAP (Active Directory) resources, and defining them based on passive or active scan results. Powerful rules can perform advanced processing on scan data to create lists based on details of the scans, such as creating lists of all IPv4 systems which have a port open, which have a certain domain name, which have unauthorized operating systems, and more..

Assets can also be grouped together, which is useful for identifying intersecting assets. For example, you could have an asset of "vulnerable Windows hosts" and then intersect that group with a list of organizational assets, such as a list of assets consisting of different Windows domains.

SecurityCenter also can create repositories of vulnerability data, which allows for mixing different types of vulnerability data. For example, if an asset on a DMZ had both an external scan and an internal patch audit, there would surely be different scan results. The external scan may not have access to login to perform a scan, and the scanned systems may also be protected by a firewall. The internal scan may identify missing patches that aren't relevant to the system's purpose, such as finding a missing MySQL patch on a system only running Apache web servers.

Finally, SecurityCenter can bring together multiple assets and multiple repositories into a construct called an "Organization". The Organization contains all of the users for a group, a separate scoring system, and specific types of scanning, vulnerability and log analysis resources.

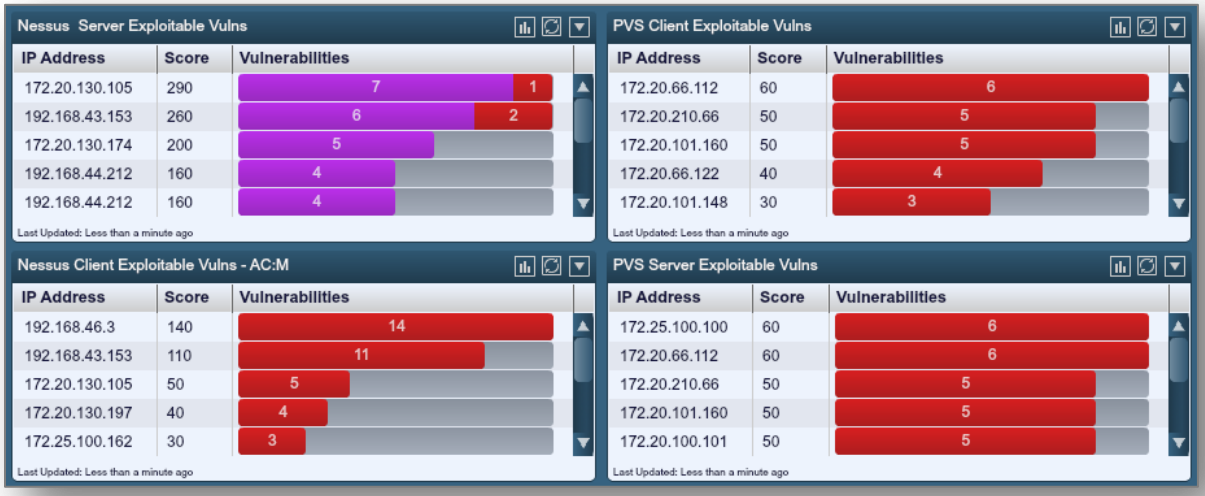
SecurityCenter also allows for the "accepting of risk" by a user or asset owner who can't fix a vulnerability. For example, a risk officer may be responsible for patching their systems, but also be required to run an anti-virus tool that has vulnerabilities but isn't scheduled to be patched for some time. The risk manager could "accept the risk" for this

vulnerability for which they have no control over. Having the ability to do this gives asset owners more comfort about having “their” vulnerabilities being tracked as long as only the vulnerabilities they can fix are counted.

On top of the advanced ways to associate users to IT assets, SecurityCenter has a wide variety of filtering methods that can be used to compute comparative scores for rankings assets, and thusly the people who manage them. There are over twenty types of filters in SecurityCenter including:

- Repository
- Partial Asset
- Severity
- Complete CVSS Score
- IP address & network range
- DNS name
- Port
- Public Exploit availability
- Vulnerability Publish Date
- Vulnerability Fix date
- Plugin family
- Plugin type (Active, Passive or Compliance)
- Date first observed in SecurityCenter
- Date most recently seen in SecurityCenter
- Bugtraq ID, CVE, IAVMIAVM and other references
- Microsoft patch KB reference
- Vulnerability Text Filter

For each of these filters, a dynamic score can be computed for each asset. SecurityCenter’s scoring system is designed to compare assets or IP addresses relative to each other. As assets or IP addresses are computed, their matching vulnerabilities for any query are weighed. For example, consider the following screen shot:



This dashboard attempts to score the IP addresses that are the most “exploitable”. We could have simply performed an IP summary for all vulnerabilities, which have an exploit available for them. This would have combined client-side exploits along with server-side exploits. Doing so would have provided a false sense of prioritization.

In addition, we created four different scoring mechanisms. The upper left has exploitable services as found by Nessus. The bottom left has exploitable client vulnerabilities as found by Nessus. The upper right has client-side exploits as found by the PVS, and the bottom right has server vulnerabilities as found by the PVS.

Tracking exploits by exploit vector keeps things extremely personal for system administrators. Administrators focused on securing key servers can further be focused and identify precisely when there are external risks to their systems. Administrators attempting to secure their user population while accessing the Internet or large Intranets can know immediately when they have serious client-side exploit vectors which need to be addressed.

Tracking and scoring by individual IP addresses can help make system administrators accountable for the security of their systems, but this does not scale for enterprise networks. Instead, SecurityCenter assets can use the same sort of analysis and scoring. Since assets can be associated with political groups, physical locations or clusters of systems managed by a single security officer, scoring them accordingly can provide relative comparison. For example, consider the following SecurityCenter dashboard that compares vulnerability data from five different geographical assets:

In each dashboard, any matching severities (low, medium, high and critical) are given weights and the cumulative score is computed based on the total number of each weighted severity count. In the upper left chart, Boston has the highest score when all vulnerabilities are considered. However, in the upper right the “San Fran” asset gets the highest score when only exploitable vulnerabilities are considered. In the lower left, “San Fran” also has the highest score when considering vulnerabilities that have been detected for more than 90 days. Finally, in the bottom right, only vulnerabilities that are accessible from the Internet are considered.

The same sort of filtering used to compute these relative scores can also be used to compute percentages and ratios. This allows per-system averages to be compared across assets that may have very different numbers and types of systems. The same data used to make the above screen shots was also used to drive the following chart that graphs numbers of systems, the percent with CVSS vulnerabilities greater than 7, percent with exploitable vulnerabilities and percent with vulnerabilities older than 90 days.

Being able to graph security and compliance results on a per-system basis is another way to keep things personal. It allows organizations to be compared on the average of their efforts rather than a cumulative score.

The data behind these tables can be modified with any of the numerous SecurityCenter filters. The weights for the severity levels can also be modified with logarithmic or cube scores if the default linear scoring isn’t desired.

The additional filtering allows organizations to keep things personal by creating dashboards and reports that are topical with news stories, corporate initiatives and reporting metrics. Tenable offers hundreds of pre-made dashboard and reports, which allows asset owners to be graded and tracked on the presence of very common IT audit items such as:

- USB device usage
- Unsupported software usage
- Default and vendor supplied passwords
- Authorized operating systems
- Mobile device and platform detection
- Correct configuration of OSes
- Correct anti-virus solution installed and up to date
- Wireless SSID
- Botnet and malware detection

- IPv6 configurations on IPv4IPv4 devices
- Outdated or vendor supplied SSL certificates
- Virtual, network and firewall security infrastructure audits
- Arbitrary compliance testing against PCI or government standards
- Modem detection
- Web Browser detection

The real-time nature of the vulnerability data collected by Tenable's solutions enables asset owners to be graded and tracked on a very personal level. We've shown that the level of tracking can be very discrete for focused analysis across an enterprise or can be very high level, yet still retain daily tracking, even at enterprise scale.

Step 5 – Hold Managers Accountable

The last component of Mr. Streufert's recommendations to achieve continuous monitoring is to hold managers accountable. It is very easy to imagine a system administrator who is responsible and thusly accountable for the security of the systems they manage. However, at scale, enterprise organizations often have difficulty in tracking who owns which systems and what "being secure" means. Enterprise networks are complex and often require exceptions to be made that further increase network complexity.

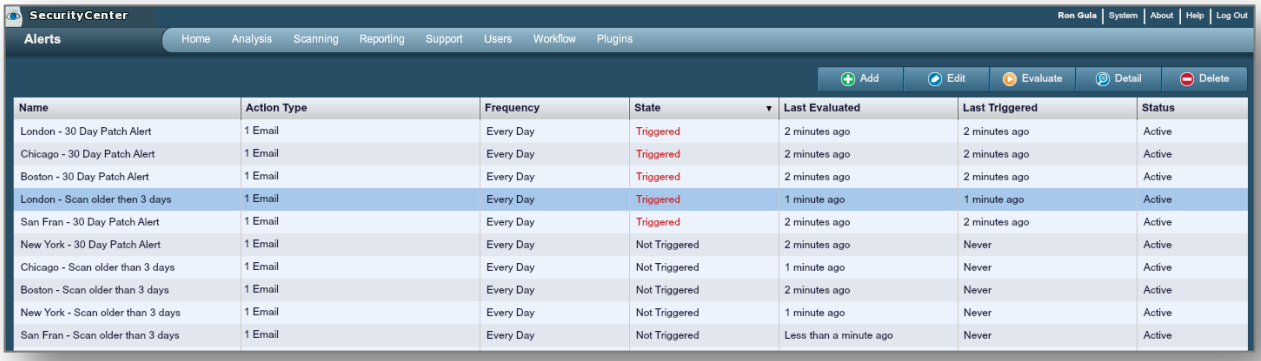
Tenable's solution allows for the simplification of security auditing at scale by leveraging "outcome based" auditing in real-time. Outcome based audits allow organizations to define their desired security posture and then track deviations against it. Outcomes can be defined within SecurityCenter with the same asset tagging and filtering we've shown in the previous four sections. More importantly, outcomes can be monitored in near real-time to inform asset owners and system administrators when they are out of compliance.

The days of an administrator receiving a vulnerability scan report, figuring out which patches to apply, and then re-scanning a system to ensure it is secure are nearing an end. There are simply too many vulnerabilities to patch and the threat of exposure to missing security patches is very high. Instead, with continuous monitoring, a solution from Tenable can help system administrators know when they are exploitable, when they are falling behind on patching, and when they are at risk from a corporate governance directive. The notification can come in real-time via secure email reports and predictive dashboards.

SecurityCenter includes an innovative alerting system which allows any user to create notifications, tickets, emails, scans and reports to be run when certain conditions are met. A condition is logically built around any query supported by SecurityCenter. There are many billions of combinations of filters and targets that could be used to monitor a network continuously. Several examples include:

- Counting the number of open perimeter ports and alerting if it changes
- Identifying the number of systems on a DMZ and alerting if a new system is discovered
- Emailing alerts if critical systems are discovered to be exploitable
- Creating alerts within patch windows, such as alerting on day 15 that a 20 day patch window is approaching
- Identifying when new vulnerabilities occur that have very old publish dates, signifying an unmanaged system being put into production
- Creating alerts if neither continuous passive vulnerability data nor recent credentialed patch audits have been performed in a timely manner.

Below is an example screen shot of the SecurityCenter's policy alerting screens.



Name	Action Type	Frequency	State	Last Evaluated	Last Triggered	Status
London - 30 Day Patch Alert	1 Email	Every Day	Triggered	2 minutes ago	2 minutes ago	Active
Chicago - 30 Day Patch Alert	1 Email	Every Day	Triggered	2 minutes ago	2 minutes ago	Active
Boston - 30 Day Patch Alert	1 Email	Every Day	Triggered	2 minutes ago	2 minutes ago	Active
London - Scan older then 3 days	1 Email	Every Day	Triggered	1 minute ago	1 minute ago	Active
San Fran - 30 Day Patch Alert	1 Email	Every Day	Triggered	2 minutes ago	2 minutes ago	Active
New York - 30 Day Patch Alert	1 Email	Every Day	Not Triggered	2 minutes ago	Never	Active
Chicago - Scan older than 3 days	1 Email	Every Day	Not Triggered	1 minute ago	Never	Active
Boston - Scan older than 3 days	1 Email	Every Day	Not Triggered	2 minutes ago	Never	Active
New York - Scan older than 3 days	1 Email	Every Day	Not Triggered	1 minute ago	Never	Active
San Fran - Scan older than 3 days	1 Email	Every Day	Not Triggered	Less than a minute ago	Never	Active

This uses the same geographical asset lists leveraged for the various dashboards and trend lines. The policy alerting allows an organization to use SecurityCenter to create alerts that will send notifications to asset owners and system administrators. The alerts can be extensively customized and even include full PDF reports. By default, text-based alerts include the basic information about why the alert was triggered, such as what is shown below:

London Has Late Scans

SecurityCenter

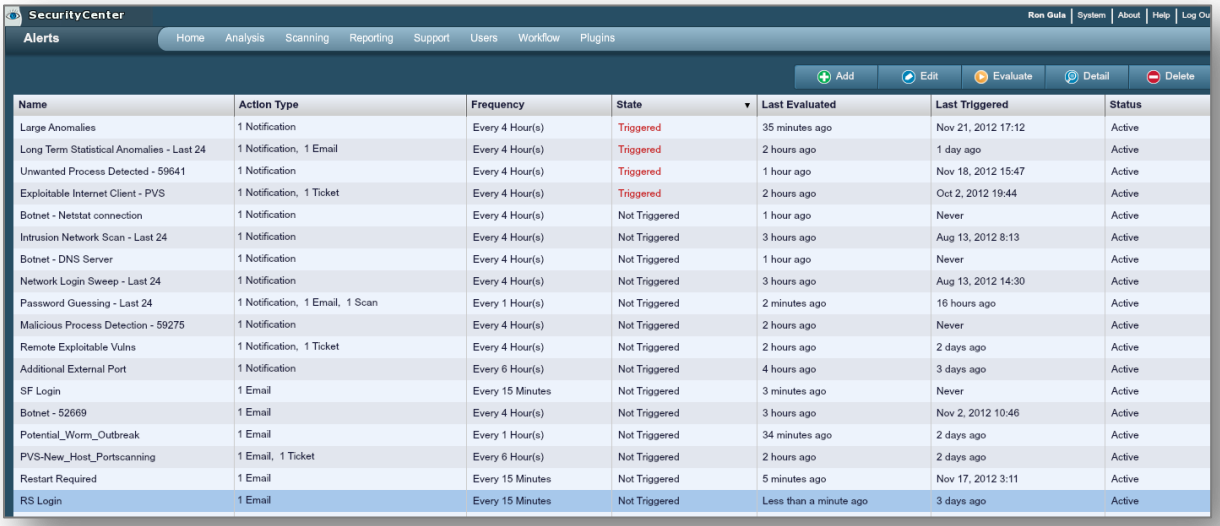
Sent: Thursday, November 29, 2012 5:46 PM

To: Ron Gula

Alert **'London - Scan older then 3 days'** (id #93) has triggered. **Alert Definition:** IP Count >= 1 **Calculated Value:** 3 Please visit your SecurityCenter (http://www.exampleSC4.com/sc4) for more information. This e-mail was automatically generated by SecurityCenter as a result of alert **'London - Scan older then 3 days'** owned by **Ron Gula [rgula]**. If you do not wish to receive this email, contact the alert owner.

For more complex communications, SecurityCenter's default and downloadable reports can be customized to deliver pertinent information to asset owners. For example, I've worked with customers who have used the operating system and application detection features of both Nessus and the Passive Vulnerability Scanner to detect "unauthorized" software and create a report that is emailed to asset owners whenever a detection occurs.

Alerts that are leveraged for high-level executive oversight and monitoring can also be complimented with tactical monitoring by asset owners. It is common for SecurityCenter users to create very high-level alerts for specific types of outcomes which are desired, such as all patches being applied within thirty days. At the same time, administrators, risk managers and IT auditors who are monitoring tactical systems much more closely can leverage SecurityCenter's policy alerting for close monitoring of system security. Next is an example screen shot of a much more detailed alert window for an administrator within the "Boston" business unit:



Name	Action Type	Frequency	State	Last Evaluated	Last Triggered	Status
Large Anomalies	1 Notification	Every 4 Hour(s)	Triggered	35 minutes ago	Nov 21, 2012 17:12	Active
Long Term Statistical Anomalies - Last 24	1 Notification, 1 Email	Every 4 Hour(s)	Triggered	2 hours ago	1 day ago	Active
Unwanted Process Detected - 59641	1 Notification	Every 4 Hour(s)	Triggered	1 hour ago	Nov 18, 2012 15:47	Active
Exploitable Internet Client - PVS	1 Notification, 1 Ticket	Every 4 Hour(s)	Triggered	2 hours ago	Oct 2, 2012 19:44	Active
Botnet - Netstat connection	1 Notification	Every 4 Hour(s)	Not Triggered	1 hour ago	Never	Active
Intrusion Network Scan - Last 24	1 Notification	Every 4 Hour(s)	Not Triggered	3 hours ago	Aug 13, 2012 8:13	Active
Botnet - DNS Server	1 Notification	Every 4 Hour(s)	Not Triggered	1 hour ago	Never	Active
Network Login Sweep - Last 24	1 Notification	Every 4 Hour(s)	Not Triggered	3 hours ago	Aug 13, 2012 14:30	Active
Password Guessing - Last 24	1 Notification, 1 Email, 1 Scan	Every 1 Hour(s)	Not Triggered	2 minutes ago	16 hours ago	Active
Malicious Process Detection - 59275	1 Notification	Every 4 Hour(s)	Not Triggered	2 hours ago	Never	Active
Remote Exploitable Vulns	1 Notification, 1 Ticket	Every 4 Hour(s)	Not Triggered	2 hours ago	2 days ago	Active
Additional External Port	1 Notification	Every 6 Hour(s)	Not Triggered	4 hours ago	3 days ago	Active
SF Login	1 Email	Every 15 Minutes	Not Triggered	3 minutes ago	Never	Active
Botnet - 52669	1 Email	Every 4 Hour(s)	Not Triggered	3 hours ago	Nov 2, 2012 10:46	Active
Potential_Worm_Outbreak	1 Email	Every 1 Hour(s)	Not Triggered	34 minutes ago	2 days ago	Active
PVS-New_Host_Portscanning	1 Email, 1 Ticket	Every 6 Hour(s)	Not Triggered	2 hours ago	2 days ago	Active
Restart Required	1 Email	Every 15 Minutes	Not Triggered	5 minutes ago	Nov 17, 2012 3:11	Active
RS Login	1 Email	Every 15 Minutes	Not Triggered	Less than a minute ago	3 days ago	Active

These notifications were much more tactical. Some organizations we've worked with leverage early non-compliance alerting internally, and generate alerts well ahead of what their groups are being measured against. For example, if scans should occur once a week, an internal IT group may scan every two days and then alert if there hasn't been a scan in three days.

Conclusion

Leveraging SecurityCenter CV to automate both the collection of vulnerability data and the analysis of the data from one console streamlines the entire vulnerability management process. It reduces the amount of time between updates and decreases the chance that executives and IT managers will make poor decisions based on old or incomplete data.

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/.

GLOBAL HEADQUARTERS

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