



# Tenable Product Evaluations Application: HIPAA

January 23, 2009  
*(Revision 6)*

David Breslin – Director of Sales Engineering

## Table of Contents

Table Of Contents	2
Introduction	3
Scope	3
Executive Summary	3
HIPAA Security Rule	3
HIPAA Security Rule: Administrative Safeguards	4
Security Management Process: Risk Analysis And Risk Management	4
Security Management Process: Information System Activity Review	10
Security Awareness And Training: Protection From Malicious Software	11
Security Awareness And Training: Log-In Monitoring	12
Security Incident Procedures: Response And Reporting	13
Contingency Plan: Applications And Data Criticality Analysis	14
Evaluation	15
HIPAA Security Rule: Physical Safeguards	16
Workstation Use	16
HIPAA Security Rule: Technical Safeguards	18
Access Control: Automatic Logoff	18
Audit Controls	21
HIPAA Security Rule: Additional Considerations	22
About Tenable Network Security	23

## Introduction

Purchasers of security compliance solutions require a time efficient evaluation period to maximize the use of their resources. This document highlights features of Tenable products that apply to the standards and implementation specifications of the HIPAA Security Rule. Tenable maintains dedicated regionalized sales teams to assist in technical and non-technical issues during an evaluation period. If you wish to start an evaluation please contact Tenable sales by phone, 877-448-0489, or by email, [sales@tenablesecurity.com](mailto:sales@tenablesecurity.com), and ask to be introduced to a sales manager.

## Scope

This paper highlights the sections, standards and implementation specifications within the HIPAA Security Rule that Tenable products can help in building security and workflow based software processes in support of compliance standards within the overall HIPAA Security Rule. In addition, the paper will highlight areas of functionality to explore during an evaluation. The purpose of this paper is not to be a supplement to an organization's documented adherence to the HIPAA Security Rule. The HIPAA Security Rule includes recommendations for formalized processes and plans for the protection of EPHI which cannot be satisfied by computer software or hardware alone. This paper is not a replacement for legal counsel or experienced Security and HIPAA compliance professionals.

## Executive Summary

Some of the standards and implementation specifications within the HIPAA Security Rule can be satisfied by developing processes based around implementing security based software.

Tenable's executive management team consists of respected IT Security visionaries, Ron Gula, Renaud Deraison and Marcus Ranum. Each one has authored leading security tools, appliances and software. For more information on their backgrounds, please visit <http://www.tenablesecurity.com/about/index.php?view=management>.

Some of Tenable's customers do not choose to implement the full Tenable product suite for their specific and customized compliance needs. However, Tenable's Security Center (SC) management console, when combined with Tenable's Nessus vulnerability scanner, Passive Vulnerability Scanner (PVS), Log Correlation Engine (LCE) and third party security appliances like NIDS systems and firewalls, brings compelling results to the consumers of the data that very few competing vendors can deliver. Data is core to information systems, whether security based or not. Many corporations have been facing the ongoing challenge of data islands and are now faced with ongoing data warehousing projects to consolidate those data islands. Using the entire Tenable product suite reduces the risk of requiring security based data islands to be brought together in future projects requiring further funding.

This paper provides a framework, based on the HIPAA Security Rule, for your evaluation of our products to help you understand how your organization can meet HIPAA compliance at a very detailed level during a formal evaluation. Tenable has a dedicated Sales Engineering team to assist organizations in evaluating our products. This paper is not a replacement for seeking legal and/or professional advice on meeting or exceeding HIPAA compliance standards.

Tenable recommends a blended approach that includes active (Nessus) and passive (PVS) scanning for automated technical risk discovery via the Security Center. For those areas of your infrastructure that are so high risk that generating network traffic could be destructive, PVS can be solely deployed as a best effort in managing an ongoing risk management and assessment plan passively. Throughout this paper the evaluation tips refer to a laboratory setting purposely, an area where machines or devices are not performing live critical functions so there is a low risk of accidents when performing active vulnerability scanning.

## HIPAA Security Rule

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical and physical safeguards for covered entities to use to assure the confidentiality, integrity and availability of electronic protected health information (EPHI). Each safeguard category consists of standards and implementation specifications.

This paper is divided into the HIPAA Security Rule Administrative, Technical and Physical Safeguard categories and their respective standards and implementation specifications which should be considered when evaluating Tenable products for assistance in complying with the rule.

All covered entities were to be in compliance with the Security Rule no later than April 20, 2005, except small health plans which had to comply no later than April 20, 2006.

## HIPAA Security Rule: Administrative Safeguards

Administrative Safeguards are summarized in the HIPAA Security Rule as “administrative actions, and policies and procedures, to manage the selection, development, implementation and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity’s workforce in relation to the protection of that information.”

## Security Management Process: Risk Analysis and Risk Management

For the Risk Analysis and Risk Management implementation specifications a good source of information is CMS’s paper entitled “Basics of Risk Analysis and Risk Management”. Many of the points made in the paper can be applied to an evaluation of Tenable products as validation of requirements. The following CMS points are highlighted in bold text with evaluation comments, tips and sample Tenable product screen captures.

### **Risk analysis and risk management are the foundation of a covered entity’s Security Rule compliance efforts.**

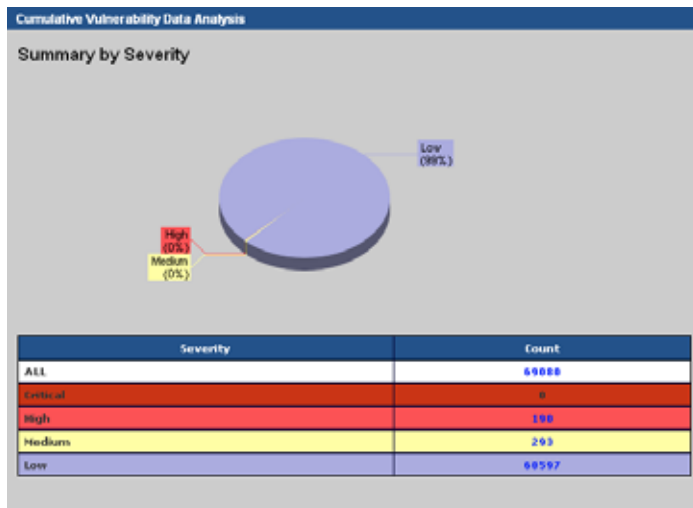
Tenable’s core product, Security Center (first released as the Lightning Console), was initially conceived from the need to collect, manage and interrogate technical vulnerability data and Network Intrusion Detection System (NIDS) alerts produced by many popular third party NIDS vendors. Analyzing vulnerability data can form an ongoing strategy for reviewing technical risks and NIDS alerts can be included in a strategy for the ongoing monitoring of technical threats.

### **Risk analysis and risk management are not one-time activities.**

Security Center consists of automated and manually initiated processes in support of ongoing technical vulnerability discovery. For the passive discovery of technical vulnerabilities, Security Center will automatically poll Tenable’s Passive Vulnerability Scanners for current and new vulnerability data 24/7. For the active discovery of technical vulnerabilities using Tenable’s active vulnerability scanner, Nessus, scanning can be scheduled daily, hourly, weekly or using far more complex periodic intervals or simply on demand. Third party NIDS can be configured to send their alerts to either Security Center and/or LCE, which will be correlated 24/7 within either Tenable product. Security Center’s collection of current vulnerabilities, the cumulative database, is actually a current “state” of vulnerabilities.

A common misconception by customers that have used the Nessus scanner in a standalone mode is to look for individual scan results in Security Center so they can perform change (delta) analysis. The cumulative database is a current snapshot. To perform queries in the GUI or via reporting for newly discovered vulnerabilities through both active and passive scanning, please use the “discovered” and “observed” filters. To view those vulnerabilities that are no longer detected and are therefore not present, users can use the “patched and mitigated vulnerability” database view.

EVALUATION TIP: Within a lab environment, configure Security Center with both a Tenable PVS sensor and a Nessus scanner. The PVS sensor should be configured at a convenient network choke point created using either a network tap or a network device span port for maximum evaluation effectiveness. Also for maximum evaluation effectiveness, configure hosts with missing patches for scanning. For example, try using Windows hosts with no service packs or updates applied and/or Linux hosts with no package updates applied. Configure a NIDS sensor also off the network choke point, alongside the PVS sensor and have it send its alerts via the syslog network protocol to your Security Center and LCE installations. There are free NIDS solutions available via the Internet if you require them. The Bro Intrusion Protection System (<http://www.bro-ids.org/>) is a good example. Configure Security Center and the LCE for receiving the alerts from your NIDS software. PVS, when running and configured with Security Center, will immediately begin to detect vulnerabilities by monitoring network traffic between the hosts in your lab (in other words it is an ongoing process and not a one-time activity). Configure scheduled scans of your lab with your Nessus scanner which will put in place ongoing active vulnerability scanning. Some of your active vulnerability scanning may or may not trigger NIDS alerts for review in Security Center and/or LCE. If you need help in running a controlled exploit or threat within your lab to trigger NIDS alerts please contact your assigned Tenable sales engineer.



Security Center Cumulative View of Vulnerabilities Summary

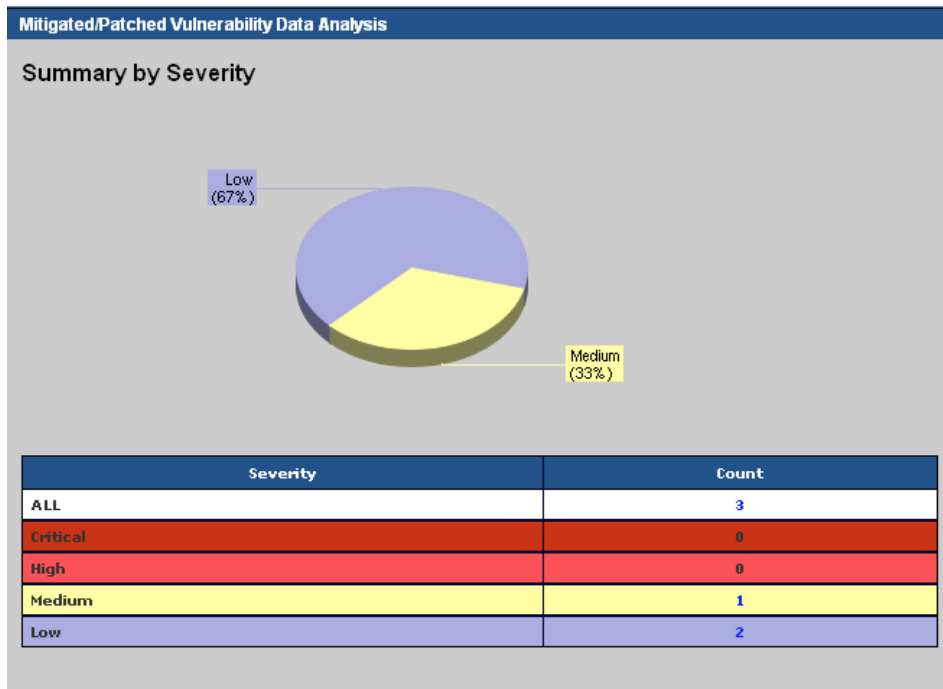
IDS Log Data Analysis		
Event	Count	24 Hour Plot
TELNET:BINARY	8758	▲
SMB:NAME-WILDCARD	4926	▲
ICMP:3-RETRIEVER	4619	▲
NT:NULL	4588	▲
NT:NULL-INBOUND	2283	▲
HTTP:INVALID-MESSAGE	1493	▲
WEB:MULTI-REQ	1147	▲
SNMP:PUBLIC	938	▲
ICMP-LARGE	888	▲
NETBIOS	843	▲
DNS:ANY-UDP	632	▲
ORACLE:UNION-BYPASS-LEFT	630	▲
NT:NULL-OUTBOUND	539	▲
CVE:CAN-2005-0568+DC:2001848+SMTP:EXCHAN	340	▲
TELNET:BINARY+TELNET:BAD_CMD	292	▲
TELNET:BAD_CMD	239	▲
SSH:VERSION-2	141	▲
CVE:2006-0006+DC:2002882	132	▲
MS:LSADS-UUID+MS:LSASS-ACCESS	111	▲
ICMP:ISS	69	▲
MS:MSDELL-HTTP-OVERFLOW	68	▲
ICMP-LARGE+ICMP:SCAN	61	▲
DOS:DNSF	40	▲
TEL:ANTI-SNIFF	33	▲
ICMP:CYBERCOP	23	▲

Security Center NIDS Alerts Summary

**The Security Rule does not prescribe a specific risk analysis or risk management methodology.**

Security Center supports a repetitive active and/or passive scan model to validate ongoing remediation efforts within a risk management plan and also to report new vulnerabilities.

EVALUATION TIP: If you have been scanning a host in your lab environment that was not patched, either Windows or Linux, then use Security Center and produce a report of vulnerabilities for the host. Also use the Security Center GUI and the cumulative database and its filters to display vulnerabilities for the host. Now, also apply all the latest patches and service packs, if applicable. Wait for Nessus to scan the host again and/or wait for the duration you set up to purge PVS vulnerability data in Security Center to be exceeded and run the same report as before and use the same GUI query. Any previously discovered vulnerabilities which were fixed due to successfully patching the host will not be reported and can be found for the host in the Security Center GUI using the patched and mitigated vulnerability database.



Security Center Patched and Mitigated View of Vulnerabilities Summary

Although only federal agencies are required to follow federal guidelines like the NIST 800 series, non-federal covered entities may find their content valuable when performing compliance activities.

Tenable's products are developed to satisfy a wide range of security compliance standards either developed internally within an organization or by an external organization. Nessus is a next generation closed source vulnerability scanner and its origins in open source helped greatly to define the ability to automate vulnerability discovery in the IT security industry. Tenable has been leading the effort on passive vulnerability discovery and although bringing a product to market a couple of years ago many compliance advisory bodies have simply failed to keep up with advancements and to include this technology in recommendations. This happened despite the fear in many organizations of running active vulnerability scanners within their infrastructure and believing there were no other alternative automated technologies to support vulnerability discovery within risk management/remediation plans.

**A covered entity must identify where the EPHI is stored, received, maintained or transmitted.**

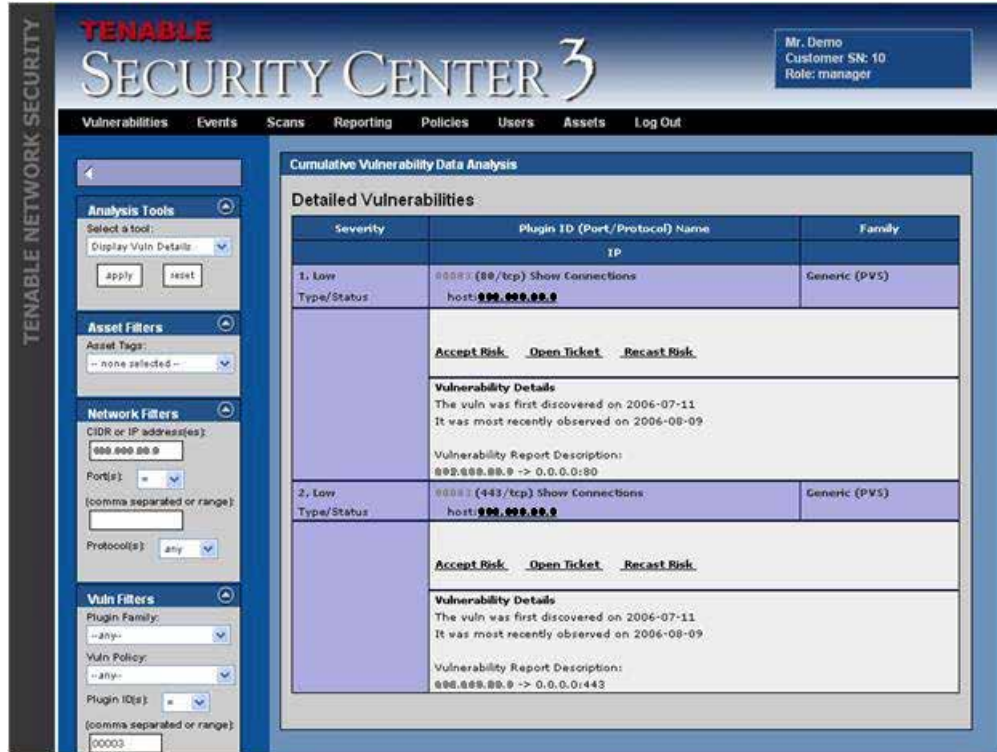
Security Center is a Tenable next generation product with the concept of asset tagging and discovery embedded into its heart. In general, being able to label and/or discover interacting devices and hosts, a HIPAA EDI transaction processor host or client credit card database for example, will greatly help in the areas of assigned risk and remediation prioritization (and also incident response).

EVALUATION TIP: Configure the Tenable Network Monitor (TNM) to use your network choke point and forward connection data to your LCE. If your lab is firewalled then forward the firewall events via the syslog network protocol to your LCE also. Periodically review connection data between hosts in your lab and externally using Security Center and its query engine to LCE. Look for correlation between firewall events and TNM events. If you configured a NIDS sensor in your lab and it has been forwarding alerts to LCE, also look for correlation by host, IP, across TNM, firewall and NIDS alerts. If you have the evaluation time, look at LCE and its scripting language called Tenable Application Scripting Language (TASL), and build a custom TASL script that will raise an alert to Security Center if a host in your lab has a conversation with another host as observed by either your NIDS, TNM or Firewall or all within a given time period. Then test it by installing your TASL script and configuring Security Center to consider LCE as an IDS source. If you need help contact your Tenable Sales Engineer.



Security Center querying LCE for host IP connections

EVALUATION TIP: Ensure in PVS that “show-connections” is enabled. Allow PVS to collect vulnerability data in your lab for a while and then review plugin 00003 in Security Center for hosts within your lab. Plugin 00003 shows what the network relationship is between hosts and devices, in other words, what has been observed talking to what. With this kind of data we can ask questions like “should your HIPAA EDI transaction processor be talked to from a host external to your organization and should that conversation be allowed through your firewall?”



Security Center showing PVS connection data for a host

Sources of information to identify technical vulnerabilities may include assessments of information systems, information system security testing or publicly available vulnerability lists and advisories.

Tenable’s dedicated Research Team ensures links to popular sources of vulnerability lists and advisories are maintained for vulnerabilities for review in Security Center either via reporting or using the GUI to drill down. In fact, the Nessus index or plugin id used in Security Center is public, popular and used by other security vendors.

EVALUATION TIP: Review the Nessus publicly accessible website at <http://www.nessus.org/> for information on plugins. In addition, look at the detail of vulnerabilities reported in Security Center and look for external links to perform further research on vulnerabilities and in many cases what to do to fix the vulnerability and reduce risk. Do not forget to also review PVS plugins in Security Center.

SHOW VULNERABILITY CHECKS	
Family:	Windows <input type="button" value="Search"/>
Plugin:	SMB shares access <input type="button" value="View"/>
[NEW SCAN][VIEW NASL SOURCE]	
<p>CVE-1999-0519</p> <p>CVE-1999-0520</p> <p>Synopsis :</p> <p>It is possible to access a network share.</p> <p>Description :</p> <p>The remote has one or many Windows shares that can be accessed through the Network with the given credentials. Depending on the share rights, it may allow an attacker to read/write confidential data.</p> <p>Solution :</p> <p>To restrict access under Windows, open the explorer, do a right click on each shares, go to the 'sharing' tab, and click on 'permissions'</p> <p>Risk factor :</p> <p>None</p> <p>This script is Copyright (C) 2005 Tenable Network Security</p>	

Security Center Nessus 3 plugin detail for a discovered vulnerability with CVE references

The output of the security testing may be a report identifying technical vulnerabilities that exist within the organization.

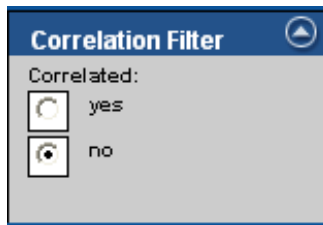
Security Center has extensive reporting capabilities for such requirements. For users participating in risk analysis and risk management who are unable to access Security Center directly, detailed reports can be generated on demand or scheduled and automatically emailed if necessary.

EVALUATION TIP: Schedule a vulnerability summary report in Security Center to run early tomorrow morning and then review tomorrow.

“Likelihood of occurrence” is the probability that a threat will trigger or exploit a specific vulnerability.

To help in risk analysis calculations Security Center vulnerabilities are ranked as either low, medium or high. They are also given a score of 1, 3 or 10 respectively. In real-time, regardless of scoring and probability, Security Center can correlate NIDS alerts to identified vulnerabilities in the cumulative database and be configured to alert via email this correlation. The correlation technology might be considered as a tool for prioritization of NIDS alerts, the detected exploitation of vulnerability attempts in conjunction with developing a risk level matrix as outlined in the CMS paper.

EVALUATION TIP: If you have been running exploits or technical threats in your lab that successfully compromise a host, your NIDS sensor detected the exploits or threats, and Security Center has listed vulnerabilities or risks, then try the correlated filter in the GUI IDS View in Security Center. If you have the resources to run correlated exploits or threats, then configure Security Center to syslog correlated alerts to LCE and use a Security Center GUI query to LCE to find the correlated alerts.



Correlation Filter in Security Center's Analyze IDS Events View

IP	Score	Total	Critical	High	Medium	Low
■■■■■■■■■■	54	43	0	1	1	41
■■■■■■■■■■	46	42	0	0	2	40
■■■■■■■■■	158	42	0	12	4	26
■■■■■■■■■■	39	37	0	0	1	36
■■■■■■■■■■	59	37	0	2	2	33
■■■■■■■■■■	39	37	0	0	1	36
■■■■■■■■■■	58	36	0	2	2	32
■■■■■■■■■■	35	35	0	0	0	35
■■■■■■■■■■	57	35	0	2	2	31
■■■■■■■■■■	34	34	0	0	0	34
■■■■■■■■■■	36	34	0	0	1	33
■■■■■■■■■■	34	34	0	0	0	34
■■■■■■■■■■	56	34	0	2	2	30
■■■■■■■■■■	36	34	0	0	1	33
■■■■■■■■■■	36	34	0	0	1	33
■■■■■■■■■■	56	34	0	2	2	30
■■■■■■■■■■	56	34	0	2	2	30
■■■■■■■■■■	32	32	0	0	0	32
■■■■■■■■■■	34	32	0	0	1	31
■■■■■■■■■■	31	31	0	0	0	31
■■■■■■■■■■	30	30	0	0	0	30
■■■■■■■■■■	30	30	0	0	0	30
■■■■■■■■■■	32	30	0	0	1	29
■■■■■■■■■■	32	30	0	0	1	29
■■■■■■■■■■	44	29	0	1	3	25

Technical threat or risk scoring supported in Security Center



The purpose of a risk management plan is to provide structure for the covered entity’s evaluation, prioritization and implementation of risk-reducing security measures.

For technical vulnerabilities Security Center was developed not only to support their automated discovery with Nessus and PVS and to store NIDS alerts or technical threats, it also contains a workflow and GUI supporting evaluation, prioritization and implementation. Ticketing, a simple or complex SC user model and asset list management can support the mitigation, assignment and tracking of remediation work.

EVALUATION TIP: Try opening tickets for discovered vulnerabilities. Create end users using the Primary Security Manager that are responsible for assets within certain asset lists. Become familiar with how tickets can be viewed and responded to by only those users that have the appropriate asset lists assigned to them. Security Center can support a simple user model or complex user model of Security Personnel and Asset Administrators. Use the Accept Risk option so a vulnerability is no longer reported within the cumulative database. Recast a vulnerability to “critical”, therefore giving it a very high score of 40 and bringing focus to the vulnerability in reporting.

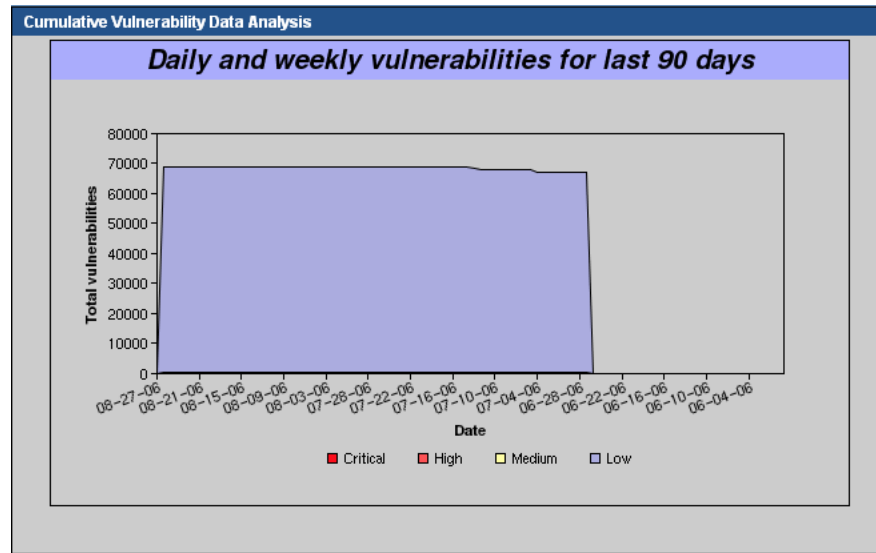
Cumulative Vulnerability Data Analysis		
Detailed Vulnerabilities		
Severity	Plugin ID (Port/Protocol) Name	Family
	IP	
1. Medium Type/Status	02183 (80/tcp) OpenSSL denial of service host:000.000.00.0	Web Servers (PVS)
	CVE: <a href="#">CVE-2004-0112</a> Bugtraq: <a href="#">9899</a> <a href="#">Accept Risk</a> <a href="#">Open Ticket</a> <a href="#">Recast Risk</a>	
	<b>Vulnerability Details</b> The vuln was first discovered on 2006-07-11 It was most recently observed on 2006-08-09  Vulnerability Report Description: Synopsis : The remote host is vulnerable to a Denial of Service (DoS) attack The remote host is using a version of OpenSSL which is older than 0.9.6m or 0.9.7d There are several bug in this version of OpenSSL which may allow an attacker to cause a denial of service against the remote host. . IAVA Reference : 2004-b-0006  CVSS Base Score : 5 AV:R/AC:L/Au:NR/C:N/I:N/A:C/B:A Solution : Upgrade to version 0.9.6m (0.9.7d) or newer	

*Vulnerability with links for ticket creation, severity recasting and risk acceptance*

For the risk management plan to be successful, key members of the covered entity’s workforce, including senior management and other key decision makers, must be involved. The outputs of the risk analysis process will provide these key workforce members with the information needed to make risk prioritization and mitigation decisions.

There are many ways with reporting and its filters to indicate the success of remediation efforts for technical vulnerabilities discovered using Security Center. The least sophisticated may be using GUI and Reporting filters and a 90 day trend showing high, medium and low vulnerabilities daily for 90 days as captured in the Cumulative database. Dependent on new vulnerability discovery and successful remediation of current vulnerabilities, the trend line should slope down in height over time.

EVALUATION TIP: Use the “trending tool” in Browse Cumulative Vulnerabilities and the Vulnerability Summary to review a 90 day trend graph. Produce the graph for a particular host or asset list.



Security Center 90 Day Trend Graph

## Security Management Process: Information System Activity Review

In CMS's paper entitled "Security Standards: Administrative Safeguards", there are a few points to gear the evaluation mostly of LCE, its supporting agents and Security Center for consideration of complying with some of the requirements within the Information System Activity Review standard.

### Implement procedures to regularly review records of information system activity, such as audit logs, access reports and security incident tracking reports.

A great deal of Information System activity can be determined from logs generated by all sorts of devices and hosts. The problem is the sheer volume of data that logging can produce and the large number of devices and hosts producing logs. Tenable's LCE has a technology that overcomes these short comings. It is called normalization. Common elements are parsed from logs with perhaps the most important of all being the IP address of the host or device producing the log. And a unique index number and name is given to this new "normalized" record generated by parsing common elements from the original log record. LCE allows organizations to build their own rules for normalization normally generated by custom built software applications like perhaps a payment processor or web application. It should be noted however that by changing a filter in Security Center, the original log record can always be displayed underneath the normalized record. Tenable's LCE in most cases also deals with the problem of centralizing log data by using the very well established syslog network protocol which was specifically designed for sending logs over networks. Many network devices like firewalls, VPNs and switches can be configured to forward their logs to LCE eliminating the need to log on to every device to check its log data making the process of implementing a plan to "regularly review records" more humanly possible. For hosts that do not natively support the syslog protocol for sending logs over a network for collation at a central server Tenable provides several clients that can monitor file logs and directories and send new records to LCE encrypted over using raw TCP.

**EVALUATION TIP:** Install the TNM at a convenient choke point in your lab and have it forward TCP and UDP system activity to LCE. Configure a Windows host with the LCE client for Windows to forward the Windows event logs to LCE. If your lab network has CISCO devices that are publishing network traffic information with the CISCO NetFlow protocol then configure the Tenable NetFlow Monitor (TFM) to forward NetFlow events to LCE. Check your access to Tenable software and see if there are any other agents you might be interested in running, OPSEC and RDEP for example. If you have a firewall in the lab or VPN device configure them to syslog their logs to LCE. Allow your configuration to sit for a while and then review your lab's network and host activity as captured in LCE and by its sensors and via the syslog network traffic to it.

Log Data Analysis	
Summary by Event	
Count	Event
139349	TNM-TCP_Session_Started
133151	TNM-UDP_Activity
120878	TNM-TCP_Session_Timedout
18468	TNM-TCP_Session_Completed
10670	TNM-ICMP_Activity
3192	Microsoft_Close_TCP
2097	SSH-Illegal_User
1777	Microsoft_Open-Inbound_TCP
1592	NeVO-Internal_PortScanning
1300	Microsoft_Open_TCP
872	Windows-Successful_Logoff
862	Microsoft_Opened_UDP
859	Microsoft_Close_UDP
833	Windows-Successful_Network_Login
771	Snort-TCP_Portswep
239	Snort-HTTP_Inspect
127	Statistics-Long_Term_Abuse
122	SSH-PAM_Session_Opened
116	Statistics-Anomaly
110	Microsoft_Drop_TCP
99	SSH-Failed_Password
67	Statistics-Medium_Anomaly
64	Statistics-Internal_Connection_Spike
59	Windows-Special_Privilege_New_Logon
41	Windows-Account_Used_For_Login

*Normalized events in LCE from multiple sources*

**The information system activity review enables covered entities to determine if any EPHI is used or disclosed in an inappropriate manner.**

There can be no fully automated replacement for skilled staff members that could distinguish good and bad information system activity in a very complex environment and be correct 100% all of the time. However, with LCE and multiple sources of host and network based log activity, experienced staff have a much better chance of distinguishing good and bad behavior, a best effort. If you feed in NIDS alerts to LCE, you can observe the network connections sensitive hosts, perhaps those known to handle EPHI and make any of those connections sub categorize into known as acting suspiciously, carrying threats that require further investigation. LCE also comes with a free statistical anomalies daemon which can be switched on or left off and can be adjusted for sensitivity. Its basic premise is to learn what regular behavior is by looking at normalized event data stored in LCE and then compare that to current activity. Statistical deviations will cause the daemon to produce its own events in LCE. These events could also be used to trigger NIDS alerts and effectively turn LCE into an intrusion detection system of its own as a value add to its normalization capabilities.

**EVALUATION TIP:** Consider one of your hosts a very sensitive host, perhaps a HIPAA EDI transaction processor. Use LCE and the TNM to review what connections are regular connections for the host to make or receive, basically what IPs does the host talk too and what IPs talk to the host. Now create a TASL script that will consider any new connection, an IP never observed talking to or being talked to by your emulated sensitive host, as suspicious and warranting a NIDS alert to be sent to LCE. Cause a new connection to be made to your emulated HIPAA EDI transaction processor host from an IP never observed before as having network conversations and observe the alert the TASL script raises and is seen in Security Center. This is a very one dimensional example and experienced Security and Network staff members will have more elaborate and robust techniques for using TASL scripting.

## Security Awareness and Training: Protection from Malicious Software

The Protection from malicious software standard is about implementing procedures for guarding against, detecting and reporting malicious software. There are many technologies that use various methods to perform this task. Tenable does not produce comprehensive solutions for rootkit detection, software or hardware firewalls and desktop agents for virus and worm detection. However if you deploy such technologies and they are automated, a NIDS sensor for example, forward their output to Security Center and LCE to centralize and normalize information on sources and destinations of malicious activity.

EVALUATION TIP: Tenable has produced a series of TASL scripts that can be installed with your LCE. Research these TASL scripts for their usefulness in your HIPAA compliance efforts, for example, the crowd surge TASL script which looks for the kind of malicious activity a botnet would produce and might be missed by a NIDS deployment.

## Security Awareness and Training: Log-In Monitoring

The Log-in monitoring policy is about implementing procedures for monitoring log-in attempts and reporting discrepancies. LCE can be used to receive and process logs that highlight failed or successful log-ins. Its scripting language, TASL, can be used to automatically alert on unusual patterns of activity, for example, 100 failed log-in attempts within 1 minute at the same workstation.

EVALUATION TIP: Have the Windows events logs feed into LCE by installing and configuring the Windows LCE client on a lab host. Log-in and log-out a couple of times using different userids and passwords, perhaps even use bad passwords and bad userids. Use Security Center and query your LCE for the successful and unsuccessful log-in attempts. Write a simple TASL script to send an alert to your Security Center console if there are 3 failed log-in attempts with in 1 minute and test your script by purposely failing log-in 3 times within 1 minute. If you have access to a brute force login tool, use it against your lab host and adjust the sensitivity of your TASL script to highlight its use on your host.

---

```
# Copyright Tenable Network Security 2006
#
# TASL:      SC3_Brute_Force_Login_Attempt.tasl
# NAME:      Threshold alert for SC 3 login failures
# ALERT:     Brute_Force_Login_Attempt
# PRM FILE:  tenable_sc3_logs.prm
# REQUIRES:  SC 3 Apache log
#
# SYNOPSIS:
#
#
#
# LAST UPDATED:
# June 3, 2006

BAD_LOGIN   = 3421;

obj = object();
obj.filter.ip.src.add("0.0.0.0/0");
obj.callback.add("myCallback");
obj.filter.event.id.add(BAD_LOGIN);

function myCallback(obj)
{
  lightning_ip = obj.lightning_ip();
  local_var count, last60;
  last60 = unixtime() - 60;
  count = obj.event.count.get(id:BAD_LOGIN,
                             src:obj.event.src(),
                             newer_than:last60);

  if ( count >= 100 )
  {
    # log a correlated IDS event to Security Center 3 and raise a correlated event in LCE
    message = 'Brute_Force_Login_Attempt - ' + count + ' login failures in last minute';
    obj.log(src:obj.event.src(), dst:obj.event.dst(), msg:message, lightning:lightning_ip);

    # Don't report this host again for 1 min
    obj.filter.ip.src.remove.until(ip:obj.event.src(), until:unixtime () + 60);
  }
}
}
```

*Sample TASL script for brute force password attack detection against a Security Center console*

Log Data Analysis		
Time	Source	Type
08-24-2006 17:20:36	###.##.###.### Syslog	user-activity
	Security,08/18/2006,09:16:09 AM,Security,528,Success Audit,None,N/A,SEWINDOWSBOX,IP:###.##.###.###,Successful Logon: User Name: Administrator Domain: SE Logon ID: (0x0,0x2C96C5) Logon Type: 10 Logon Process: User32 Authentication Package: Negotiate Workstation Name: SEWINDOWSBOX Logon GUID: {47a28f0b-7986-571e-400c-b485d940b933} Caller User Name: SEWINDOWSBOX\$ Caller Domain: SE Caller Logon ID: (0x0,0x3E7) Caller Process ID: 1316 Transited Services: - Source Network Address: ###.##.###.### Source Port: 2312	
08-24-2006 17:20:37	###.##.###.###	user-activity
	Security,08/18/2006,10:29:11 AM,Security,528,Success Audit,None,N/A,SEWINDOWSBOX,IP:###.##.###.###,Successful Logon: User Name: administrator Domain: SE Logon ID: (0x0,0x2F5E78) Logon Type: 10 Logon Process: User32 Authentication Package: Negotiate Workstation Name: SEWINDOWSBOX Logon GUID: {77d5f03e-f351-d827-44fe-f479a32d4675} Caller User Name: SEWINDOWSBOX\$ Caller Domain: SE Caller Logon ID: (0x0,0x3E7) Caller Process ID: 3648 Transited Services: - Source Network Address: ###.##.###.### Source Port: 1139	
08-24-2006 17:20:39	###.##.###.###	user-activity
	Security,08/18/2006,13:55:42 PM,Security,528,Success Audit,None,N/A,SEWINDOWSBOX,IP:###.##.###.###,Successful Logon: User Name: Administrator Domain: SE Logon ID: (0x0,0x31ECBB) Logon Type: 10 Logon Process: User32 Authentication Package: Negotiate Workstation Name: SEWINDOWSBOX Logon GUID: {6a54ac93-0c9a-6811-c170-1600650653cf} Caller User Name: SEWINDOWSBOX\$ Caller Domain: SE Caller Logon ID: (0x0,0x3E7) Caller Process ID: 3592 Transited Services: - Source Network Address: ###.##.###.### Source Port: 1371	
08-24-2006 17:20:41	###.##.###.###	user-activity
	Security,08/18/2006,16:41:33 PM,Security,528,Success Audit,None,N/A,SEWINDOWSBOX,IP:###.##.###.###,Successful Logon: User Name: LOCAL SERVICE Domain: NT AUTHORITY Logon ID: (0x0,0x3E5) Logon Type: 5 Logon Process: Advapi Authentication Package: Negotiate Workstation Name: Logon GUID: - Caller User Name: SEWINDOWSBOX\$ Caller Domain: SE Caller Logon ID: (0x0,0x3E7) Caller Process ID: 536 Transited Services: - Source Network Address: - Source Port: -	

Visually analyzing Windows Log-In Events normalized in LCE

### Security Incident Procedures: Response and Reporting

It is vital that an organization identify a security incident early and respond quickly for the ongoing protection of EPHI. Please review all the Tenable products for incorporation into policies and procedures to comply with this standard. If a host was compromised, consider actively scanning it with Nessus and determining if patch levels were adequate. Also consider using LCE to review the activity of a compromised host leading up to and after a compromise. For implementing procedures to avoid a compromise can you learn from a real situation, for example, was the network and host activity you have stored in LCE leading up to a compromise adequate enough to have had an early warning? Can you build a TASL script to act as an early warning for next time? Can you build a report that would achieve the same thing? If a patch was missing on a host that helped a compromise situation, consider an audit using your Tenable products to detect similar hosts with the same missing patch and put them high in your ongoing risk management process and perhaps assign them their own dynamic asset list so you can very easily monitor progress towards patch application.

EVALUATION TIP: With your lab detected vulnerabilities, use Security Center to build a dynamic asset list of all hosts detected as requiring the same patch upgrade to some piece of software, perhaps SSH or web browser. Run a report focused on that asset list using the report filters. Create an end user account for a desktop administrator and assign them the asset list.

**ADD NEW USER**

USER ACCOUNT INFORMATION	CONTACT INFORMATION	USER MANAGED ASSET LISTS
<p><b>Account Type:</b>  <input style="width: 100%;" type="text" value="End User"/></p> <p><b>Web Account:</b>  <input style="width: 100%;" type="text" value="misterdadmin"/></p> <p><b>Password:</b>  <input style="width: 100%;" type="password" value="*****"/></p> <p><b>Password (confirm):</b>  <input style="width: 100%;" type="password" value="*****"/></p> <p style="text-align: center;"><input type="button" value="Submit"/></p>	<p><b>Name:</b>  <input style="width: 100%;" type="text" value="mister admin"/></p> <p><b>Title:</b>  <input style="width: 100%;" type="text" value="Desktop Admin"/></p> <p><b>Organization:</b>  <input style="width: 100%;" type="text" value="XYZ Corp"/></p> <p><b>Phone # 1:</b>  <input style="width: 100%;" type="text"/></p> <p><b>Phone # 2:</b>  <input style="width: 100%;" type="text"/></p> <p><b>Email:</b>  <input style="width: 100%;" type="text"/></p> <p><input type="checkbox"/> <b>Email user their account info</b></p> <p><input type="checkbox"/> <b>Include password in email</b></p> <p><input type="checkbox"/> <b>User cannot launch scans</b></p>	<div style="border: 1px solid gray; padding: 5px;"> <p>Customer Ranges</p> <p>Potential Web Servers</p> <p style="background-color: #0056b3; color: white;">Vulnerable Firefox Browsers</p> <p>Windows</p> </div>

*Creating Desktop Administrator Account for managing vulnerable browser hosts*

### Contingency Plan: Applications and Data Criticality Analysis

In the CMS paper entitled “Security Standards: Administrative Safeguards” the following is stated about the applications and data criticality analysis standard: “The implementation specification requires covered entities to identify their software applications (data applications that store, maintain or transmit EPHI) and determine how important each is to patient care or business needs, in order to prioritize for data backup, disaster recovery and/or emergency operations plan.”

A first step in prioritizing the importance of applications and the hosts they run on might be building inventory lists. In large organizations this can be a resource intensive task, especially if their environments are relatively dynamic, for example, new workstations added to contact centers relatively frequently. The dynamic asset discovery built into Security Center may help reduce resource hours in building and maintaining asset inventory lists for hosts, devices and applications.

EVALUATION TIP: Create dynamic asset lists for the hosts scanned either passively or actively within your lab. Perhaps have one asset list that has all Windows platform identified hosts. Perhaps another dynamic asset list for detected email servers. Build a static asset list of the lab subnet and label it “lab subnet”.

AVAILABLE ASSET LISTS			
ASSET LIST	TYPE	CREDENTIALS	SIZE
All Assets demo	Dynamic	Not Set	78 bytes
Apache 1_3 Web Server	Dynamic	Not Set	849 bytes
Apache 2_0 Web Server	Dynamic	Not Set	911 bytes
Apache 2_2 Web Server	Dynamic	Not Set	830 bytes
Customer Ranges	Static	Not Set	41 bytes
Demo Network	Static	Not Set	15 bytes
Demo Unix Servers	Static	Not Set	70 bytes
Demo Windows Servers	Static	Not Set	68 bytes
Exchange - W2003	Dynamic	Not Set	13 bytes
Exchange - W2K	Dynamic	Domain	166 bytes
IIS 5_0 Web Server	Dynamic	Not Set	633 bytes
IIS 5_1 Web Server	Dynamic	Not Set	533 bytes
Nessus Servers	Dynamic	Not Set	14 bytes
Office Chicago	Static	Not Set	11 bytes
Office Miami	Static	Not Set	11 bytes
Office New York	Static	Not Set	11 bytes
Passive Windows XP	Dynamic	Not Set	54 bytes
Sendmail 8_11	Dynamic	Not Set	176 bytes
Sendmail 8_12	Dynamic	Not Set	239 bytes
Sendmail 8_13	Dynamic	Not Set	153 bytes
Sendmail 8_9	Dynamic	Not Set	24 bytes
Web Servers	Dynamic	Not Set	1892 bytes

*Security Center Dynamic and Static Asset Lists*

## Evaluation

In short, this standard is an overall review that an organization must perform to verify it remains within HIPAA compliance. One part of the evaluation will be assessing new risks.

EVALUATION TIP: Security Center has a nightly process that downloads all current vulnerability checks as developed and maintained by a dedicated Tenable research team. Review the last 25 updates to your vulnerability checks using the Security Center console and administrator account. Also, periodically check the Tenable BLOG available at <http://blog.tenablesecurity.com/> for news and articles on advancements in Tenable products to address new technical risks. Nessus host-based compliance checks were announced on Tenable's BLOG.


### Using Tenable Products to find unpatched/infected MS06-040 devices

Tenable has had many of our customers call in to discuss ways they can look throughout their enterprise to find the latest round of security issues from the last "Microsoft Tuesday". Here is a quick list of things you can look for with our products:

- Nessus can be used to perform a network scan for any Windows host effected by the MS06-040 patch. The scan [does not need credentials](#), but the scanner does need to be able to communicate with the target on ports 445 or 139.
- If you do have domain credentials, plugin [22182](#) performs a patch audit looking for the applicability of the missing patch. Doing an audit with credentials will also allow for testing of the other "local" security issues besides MS06-040.
- If you've completed an active Nessus scan for MS06-040, the [Security Center](#) will correlate NIDS events (from Tipping Point, Snort, Dragon, etc.) that target vulnerable MS06-040 devices.
- For devices infected by Mocolbot/Wargbot, Nessus plugin [11329](#) can detect this. This plugin requires credentials.
- For devices infected with the [BOLQ](#) worm/trojan that exploits MS06-040 (and delivers the Mocolbot trojan), if you have a [Passive Vulnerability Scanner](#) deployed on your perimeter, you can query your Security Center to list any devices which browse on port 445 and 18067. Any devices which browse on port 445 across your perimeter should be considered suspect for a wide variety of issues regardless.
- Lastly, if you have deployed the [Log Correlation Engine](#), you can query it for activity on ports 445 and 18067 as well. Tenable has also released a [TASL script](#) which looks for [Mocolbot](#) activity in any log source. The LCE also has many generic log correlation techniques such as looking for crowd surges and suspicious proxy connections in any log sources. We've [blogged](#) about the [crowd\\_surge.tasl](#) script previously and it has been updated to alert when there is a surge of visitors to sites tracked by the [Internet Storm Center](#).

Posted by Ron Gula on August 16, 2006 | [Permalink](#)

*Tenable BLOG Article Advising Tenable Customers about a newly reported technical risk vulnerability*

LAST 25 PLUGIN UPDATES FROM NESSUS.ORG (last update: Sun Aug 27 04:21:42 EDT 2006 )		
ID	NAME	FAMILY
22242	[GLSA-200608-20] Ruby on Rails: Several vulnerabilities	Gentoo Local Security Checks
22237	SSA-2006-230-02 php	Slackware Local Security Checks
22236	SSA-2006-230-01 libtiff	Slackware Local Security Checks
22235	Docebo GLOBALS Variable Overwrite Vulnerability	CGI abuses
22234	Zen Cart autoLoadConfig Remote File Include Vulnerability	CGI abuses
22233	Zen Cart custom SQL Injection Vulnerability	CGI abuses
22232	Owl Intranet Engine <= 0.91 Multiple Vulnerabilities	CGI abuses
22231	CubeCart < 3.0.12 Multiple Vulnerabilities	CGI abuses
22230	SquirrelMail session_expired_post Arbitrary Variables Overwriting Vulnerability	CGI abuses
22229	Informix Dynamic Server Multiple Vulnerabilities	Gain root remotely
22228	Informix Detection	Service detection
22227	RMI Registry Detection	Service detection
22226	Symantec Backup Exec Multiple Heap Overflow Vulnerabilities	Windows
22225	HP OpenView Storage Data Protector Backup Agent Remote Arbitrary Command Execution Vulnerability	Gain root remotely
22224	RHSA-2006-0619: httpd	Red Hat Local Security Checks
22223	RHSA-2006-0605: perl	Red Hat Local Security Checks
22222	RHSA-2006-0582: kdbase	Red Hat Local Security Checks
22221	RHSA-2006-0575: kernel	Red Hat Local Security Checks
22220	RHSA-2006-0393: ntp	Red Hat Local Security Checks
22219	RHSA-2006-0354: elfutils	Red Hat Local Security Checks
22218	[GLSA-200608-19] WordPress: Privilege escalation	Gentoo Local Security Checks
22217	[GLSA-200608-18] Net::Server: Format string vulnerability	Gentoo Local Security Checks
22216	[GLSA-200608-17] libwmf: Buffer overflow vulnerability	Gentoo Local Security Checks
22215	[GLSA-200608-16] Warzone 2100 Resurrection: Multiple buffer overflows	Gentoo Local Security Checks
22214	[GLSA-200608-15] MIT Kerberos 5: Multiple local privilege escalation vulnerabilities	Gentoo Local Security Checks
22213	FreeBSD : mysql -- format string vulnerability (825)	FreeBSD Local Security Checks
View More: <input type="text" value="100"/> 		

Security Center Last 25 Updates

## HIPAA Security Rule: Physical Safeguards

The Security Rule summarizes physical safeguards as “physical measures, policies and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.”

### Workstation Use

In CMS’s paper entitled “Security Standards: Physical Safeguards” there is a list of questions for a covered entity to consider in including “Do the policies and procedures identify workstations that access EPHI and those that do not?” As recommended in previous standards and implementation specifications consider dynamic and/or static asset list management within Security Center as a tool to use to help in this ongoing task in a large organization.

Configuration management is a technology that can play a part in complying with the workstation use standard. Another question posed to covered entities by CMS for the workstation use standard is “Do the policies and procedures specify the use of additional security measures to protect workstations with EPHI, such as using privacy screens, enabling password protected screensavers or logging off the workstation?”



If your organization has implemented a centralized configuration management technology does it cover all workstations? Do all your workstations run on the same platform? Can you audit your workstations and demonstrate the successful implementation of standard policies like password length and complexity whether you have used a centralized configuration technology or not?

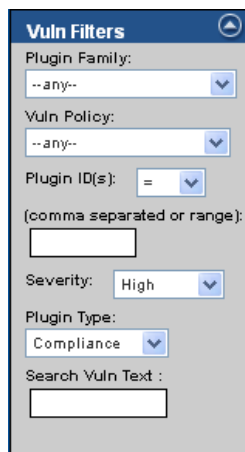
Tenable has implemented an agent-less technology for use with Nessus and Security Center for checking the configuration of hosts, servers or workstations running on Linux, Unix and Windows platforms.

EVALUATION TIP: The agent-less technology and ability to check individual host configurations warrants a Tenable paper of its own. They are highly customizable to meet many compliance standards and needs. However, Tenable has produced some out of the box checks for use in evaluations based on typical Healthcare industry requirements. Use the out of the box checks to perform a configuration management audit on workstations and servers within your lab. Please note that these types of host-based audits can be controlled via asset lists in Security Center. If you wanted to just verify workstations and servers that handle EPHI you could build static and/or dynamic assets and then use Security Center to run the audit checks only for your asset lists. Please note to run these types of checks you must use Nessus 3 and not an open source Nessus scanner.

Available Configuration Audit Policies		
Standard	File	Description
<a href="#">CERT</a>	<a href="#">CERT UNIX Checklist</a>	Contains many of the checks listed in CERT's UNIX Security Checklist v2.0 guide.
<a href="#">GLBA</a>	<a href="#">Windows User Audit</a>	This audit policy tests for user auditing settings, such as their password complexity and logging access failures and logons that are common in financial networks. (Last updated December 18, 2007.)
<a href="#">GLBA</a>	<a href="#">Windows System Audit</a>	This audit policy tests for password policies, system permissions, required auditing and system settings that are common in financial networks. (Last updated December 18, 2007.)
<a href="#">GLBA</a>	<a href="#">Solaris System Audit #1</a>	This audit policy tests for password policies, system permissions, required auditing and system settings that are common in financial networks.
<a href="#">GLBA</a>	<a href="#">Solaris System Audit #2</a>	This audit policy checks for basic password policy settings, has an example of using an MD5 checksum to see if a proper banner has been configured, checks that SSH is running and if an FTP service is found, it also checks if <i>ftpusers</i> has been set.
<a href="#">HIPAA</a>	<a href="#">Windows User Audit</a>	This audit policy tests for user auditing settings, such as their password complexity and logging access failures and logons that are required on systems holding patient health information (PHI). (Last updated December 18, 2007.)
<a href="#">HIPAA</a>	<a href="#">Windows System Audit</a>	This audit policy tests for password policies, system permissions, required auditing and system settings that are common in financial networks. (Last updated December 18, 2007.)
<a href="#">MS Vista</a>	<a href="#">Windows Vista Default Security</a>	This Security Configuration Template provides settings to support the Windows Vista Security Guide. (Last updated February 7, 2008.)
<a href="#">MS Vista</a>	<a href="#">Windows Vista EC Desktop</a>	This Security Configuration Template provides settings to support the Windows Vista EC (Enterprise) Desktop settings for the Windows Vista Security Guide. (Last updated December 18, 2007.)
<a href="#">MS Vista</a>	<a href="#">Windows Vista EC Domain</a>	This Security Configuration Template provides settings to support the Windows Vista EC (Enterprise) Domain settings for the Windows Vista Security Guide. (Last updated February 7, 2008.)
<a href="#">MS Vista</a>	<a href="#">Windows Vista EC Laptop</a>	This Security Configuration Template provides settings to support the Windows Vista EC (Enterprise) Laptop settings for the Windows Vista Security Guide. (Last updated December 18, 2007.)

Some of the "out of the box" host, workstation and server configuration checks provided by Tenable

EVALUATION TIP: The host configuration checks are grouped with passive and active vulnerabilities within Security Center. Conceptually, having a host that is not configured correctly can be considered as a risk or technical vulnerability. For reporting and GUI queries become familiar with using the Plugin Type filter and setting it to "compliance" for your host configuration checks.



Security Center Cumulative View Plugin Type Filter

Detailed Vulnerabilities		
Severity	Plugin ID (Port/Protocol) Name	Family
IP		
1. High Type/Status	88002 (0/tcp) Account lockout threshold host: 000.00.000.000	Compliance Checks
<b>Vulnerability Details</b> The vuln was first discovered on 2006-08-30 It was most recently observed on 2006-08-30  Vulnerability Report Description: "Account lockout threshold" : [FAILED] Remote value: 0 Policy value: [3..5]		
2. High Type/Status	88149 (0/tcp) Audit account logon events host: 000.00.000.000	Compliance Checks
<b>Vulnerability Details</b> The vuln was first discovered on 2006-08-30 It was most recently observed on 2006-08-30  Vulnerability Report Description: "Audit account logon events" : [FAILED] Remote value: "no auditing" Policy value: success, failure		

Some Host Configuration Checks displayed in Security Center

## HIPAA Security Rule: Technical Safeguards

The Security Rule summarizes technical safeguards as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”

### Access Control: Automatic Logoff

This implementation specification is summarized as “Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.” In CMS’s paper entitled “Security Standards: Technical Safeguards” it poses two sample questions for covered entities to consider:

1. Do current information systems have an automatic logoff capability?
2. Is the automatic logoff feature activated on all workstations with access to EPHI?

Well known mechanisms are already built into operating systems and desktop software to perform automatic logoff but you may want to audit for consistent settings and behavior across your enterprise.

Linux/Unix hosts have different ways of configuring automatic logoff of inactive sessions depending on Linux distribution and software being used. For example, the SSH daemon configuration file, profile file, or .bashrc configuration file are all possibilities for setting inactivity timeout values. The following informative article published on Oracle’s website highlights many settings to consider for securing Linux hosts:

[http://www.oracle.com/technology/pub/notes/technote\\_naqvi.html](http://www.oracle.com/technology/pub/notes/technote_naqvi.html)

Using Security Center, Nessus and the host-based compliance checks we can regularly self audit our enterprise to ensure the settings we adopt as a security/operational policy remain intact. If we follow the advice of the article and implement an inactivity timeout in /etc/profile we can regularly check that the setting remains unchanged using Security Center and Nessus, as we can for many of the settings recommended in the article. We can focus our audit scans to Linux only hosts using dynamic and/or static asset lists to keep scan time to a minimum. However, it should be noted that the Nessus host-based compliance checks do distinguish checks by operating system platform and it is possible to build one audit file of checks addressing multiple platforms.

EVALUATION TIP: Use the following host-based compliance check to audit your Linux hosts present in your lab for the interactive timeout out being set as recommended in the Oracle article. The check expects the inactivity timeout to be set to 15 minutes.

```

<check_type:"Unix">
<if>
  <condition>
    <custom_item>
      type: FILE_CHECK
      description: "Profile file exists"
      file: "/etc/profile"
    </custom_item>
  </condition>
  <then>
    <custom_item>
      #System          : "Linux"
      type             : FILE_CONTENT_CHECK
      description      : "Profile inactivity set to 15 mins"
      file             : "profile"
      search_locations : "/etc"
      regex            : "^[#]*[ \t]*TMOUT=.*"
      expect           : ".*TMOUT=900"
    </custom_item>
  </then>
</if>
</check_type>

```

Severity	Plugin ID (Port/Protocol) Name	Family
	IP	
1. High	60131 (0/tcp) Profile inactivity set to 15 mins	Compliance Checks
Type/Status	host: [REDACTED]	
	<b>Vulnerability Details</b> The vuln was first discovered on 2006-10-18 It was most recently observed on 2006-10-18  Vulnerability Report Description: "Profile inactivity set to 15 mins" : [FAILED] - error message: The file "profile" does not contain ^[#]*[ \t]*TMOUT=.*	

Security Center highlighting compliance check failure for above check

The password protected screensaver is very popular on Windows hosts but the settings are actually very difficult to audit accurately at a workstation level. This is because they can be set at two different levels: group policy or individual user. Both of which can be controlled by an Active Directory deployment or set individually on each host where group policy settings override user level settings. To further complicate matters, a combination of local policy files and registry settings control a user's screensaver settings, the registry settings being created on the fly when the user logons. These on the fly registry keys create an interesting dilemma for audit technology when ultimately it would need to sign every user onto every host and then check registry keys to ensure a 100% accurate audit over all possible implementations of the Windows screensaver policy. Producing false positives, which are indications of risk where no risk exists, can have a negative effect in remediation efforts as resources are assigned to track down non-issues.

As you are probably starting to understand with the entire Tenable product suite there are different ways to accomplish a task. This HIPAA security rule talks about security awareness and training as do other popular compliance standards. A simple Windows key combination, "[Windows Key] + L", can password lock a Windows workstation leaving the screensaver inactivity timeout as a catchall in case somebody forgets to lock their workstation before leaving it unattended. Windows security event log monitoring with LCE can be used to audit individual hosts and look for the presence of the Windows logon event and distinguish those logon events caused by unlocking a password locked workstation. Unless a Windows workstation simply was not used it would be unusual to see a week of audit activity without unlocked workstation logon events occurring. Windows provides in its Security event logs the ability to differentiate logon events and LCE can use this when building normalized events to represent the various logon types:

<http://www.windowsecurity.com/articles/Logon-Types.html>

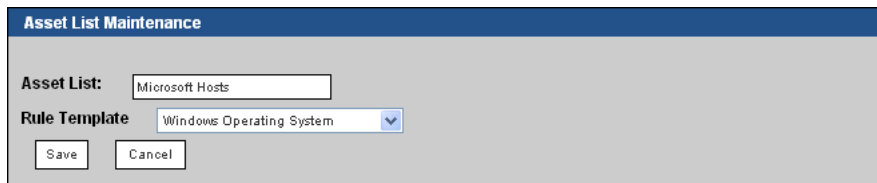
EVALUATION TIP: The following laboratory setup will perhaps be one of the most intricate in this paper and will demonstrate the usefulness of having different types of security data stored for correlation under the same GUI console, Security Center. We will combine both dynamic asset discovery and normalized operating system event logs to build a list of hosts that can be demonstrated to be out of compliance with an automatic logoff policy. In a large enterprise we may even discover hosts that we failed to inventory accurately and missed configuring to forward their operating system logs to LCE.

From scanning the laboratory with PVS and/or Nessus we should have detected Windows Hosts dynamically. Before continuing with this evaluation tip ensure Windows Hosts have been identified by using the “List OS” Analysis Tool in the Security Center Browse Cumulative Vulnerabilities View.



*Browse Cumulative Vulnerabilities List OS Tool*

Build a dynamic asset list named “Microsoft Hosts” which will automatically continue to synchronize itself with the cumulative database and the hosts detected as running Windows operating systems.



*Creating a dynamic asset list of Microsoft hosts*

For your laboratory Windows hosts install the LCE client and configure both the clients and LCE so that the Windows Security Event logs are forwarded over TCP/IP encrypted for normalization. Alternatively, you may use third party or custom software to send the Security Event logs using the popular syslog protocol to LCE over UPD/IP. Please ensure that Windows event auditing is configured to record successful logon attempts on your Windows hosts otherwise the Security Event logs will be missing the logon events we want to capture and normalize. Choose one of your Windows hosts and trigger logon events that are in response to a screensaver being engaged or by password locking the host by using “[Windows Key] + L”. You should be able to see “windows-Successful\_Unlock\_Logon” normalized events recorded in LCE and viewable via the Security Center GUI. If you are having difficulties please contact your designated Tenable Sales Engineer as there are several integration points that if not configured correctly will result in failure.

Count	Event
2612	windows-Successful_Logoff
2515	windows-Successful_Network_Logon
92	windows-Successful_Unlock_Logon
80	windows-Successful_Service_Logon
20	windows-Successful_Interactive_Logon
6	windows-Successful_RemoteInteractive_Logon
4	windows-Successful_CacheInteractive_Logon

*Normalized Windows Logon/Logoff Activity*

Install the Create Asset List (CAL) tool on your Security Center host. Configure it so that all hosts that are in the Microsoft Hosts dynamic asset list are used to check LCE for the absence of the “windows-Successful\_Unlock\_Logon” event.

```
# The windows-Successful_Unlock_Logon event indicates locking of the
# Windows host via screen save policy or manually using [Windows Key] + L.
# Microsoft Hosts.ip contains all dynamically detected windows hosts using
# active and/or passive scanning and is set up as such in Security Center 3.
# MicrosoftNoLock will contain all those Windows hosts in Microsoft Hosts.ip
# that we couldn't find a "windows-Successful_Unlock_Logon" event for by using
# the inverted switch. MicrosoftNoLock will appear in SC 3 as a static asset
# list we can report on and query via the SC 3 GUI.
#
AssetListName:MicrosoftNoLock
TargetIPs:
TargetEvents:windows-Successful_Unlock_Logon
TargetPorts:
FilterIPs:
FilterPorts:
TargetAssets:Microsoft Hosts.ip
INVERTED:yes

NEXT
```

*CAL Configuration Example*

You can schedule the CAL tool, but just for evaluation simply run the tool with the “-i” switch and build a new asset list, MicrosoftNoLock, which will contain those hosts that for the last 24 hours have never had the host locked and require their screensaver policy to be examined. Use the Security Center GUI to look at the new dynamic asset list to see those Microsoft hosts that require examination for being out of policy and the cumulative database to gain further insight into the purpose of the hosts. For example, a web server as the IIS HTTP service has been detected or a Mail Exchange server because mail protocol services like SMTP and POP3 have been detected. Microsoft servers are likely to be left running without interactive users, however your organization’s employee workstations are not, so we expect to see host lock activity.

"MicrosoftNoLock" active IP addresses	[ASSET LISTS]
██.██.██.17	
██.██.██.50	
██.██.██.60	
██.██.██.70	
██.██.██.80	
██.██.██.95	
██.██.██.120	
██.██.██.160	
██.██.██.165	
██.██.██.200	
██.██.██.203	
██.██.██.250	
██.██.██.252	
██.██.██.5	
██.██.██.59	

*Reviewing CAL created Asset List in Security Center*

## Audit Controls

The audit controls implementation specification can be summarized as “Implementing hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.”

In CMS’s paper entitled “Security Standards: Technical Safeguards” there are three questions posed to a covered entity to consider for the Audit control standard which follow in bold text and have comments.

**What audit control mechanisms are reasonable and appropriate to implement so as to record and examine activity in information systems that contain or use EPHI?**

Collecting operating system logs like those produced by Linux, Unix and Windows is very common. They supply lots of information like log-in attempts and execution failures. LCE has many clients including host agents which can forward operating system logs for normalization and correlation in LCE. Many network appliances like firewalls and switches can be configured to use the popular syslog protocol to forward event logs over a network to LCE. The following is a quote from Wikipedia: “Syslog is typically used for computer system management and security auditing.”

**What are the audit control capabilities of information systems with EPHI?**

Host operating system logs are common for determining information system activity. Application logs can also be another level of auditing information system activity logs however and they tend to be very unique and custom to an organization. LCE uses parsing rules encapsulated in “.prm” files for normalization and customers are encouraged and invited to build their own “.prm” files for their highly unique application logs to improve visibility into information system activity.

**Do the audit controls implemented allow the organization to adhere to policy and procedures developed to comply with the required implementation specification at § 164.308(a)(1)(ii)(D) for Information System Activity Review?**

The Information System Activity Review implementation specification is already mentioned earlier in this paper.

EVALUATION TIP: Tenable has plenty of sample TASL scripts for running over normalized events in LCE for determining and highlighting information system activity. Configure the LCE Windows client on a Windows host and/or the Linux client on a Linux host and install the invalid\_user\_logon.tasl. Purposely trigger log-in failures and configure LCE to forward the correlated events raised by the TASL script to be forwarded as alerts to Security Center.

Change Detection <span style="float: right;"><a href="#">[BACK TO TOP]</a></span>	
File	Description
<a href="#">Detect Change</a>	This script alerts on changes to the local network, to systems, to users and to applications. For example, it will alert when software is updates, users are added and new hosts are found.
<a href="#">New MAC</a>	This script alerts when new Ethernet addresses have been detected in DHCP, passive network logs and other sources. It will issue a New_Mac or New_Wireless_MAC alert when a new Ethernet address is detected.
<a href="#">New System User</a>	This script automatically learns valid system user names by extracting unique account names from SSH, Windows, VNC and other types of applications. When a new account name is found, it will generate a New_System_User event.
<a href="#">User to MAC</a>	This script tracks DHCP leases as well as active directory authentication events to dynamically learn each user's MAC address and then alert when this changes.

Compromise Detection <span style="float: right;"><a href="#">[BACK TO TOP]</a></span>	
File	Description
<a href="#">Attack and Connect to Blacklist</a>	This script detects when a host is attacked and then the host makes a connection to a known blacklisted IP address. This can indicate participation in a botnet.
<a href="#">Botnet with Scan</a>	Detects when there has been BOTNET activity followed by scanning. This indicates that a remote attacker is utilizing a BOTNET node to scan for vulnerabilities.
<a href="#">IDS event Followed by Change</a>	This script subscribes to a variety of change detection events, statistical hits and host based events such as Tripwire file changes and SE Linux denied process events. It then correlates these with high quality or high threat IDS alerts. The idea is to see if there have been network attacks that caused a detectable change on your network.
<a href="#">NIDS Compromise Correlate</a>	This script correlates when two different types of intrusion sensor technologies (such as Snort and TippingPoint) agree that a command shell or serious attack has occurred.
<a href="#">NIDS Compromise Detection</a>	This script generically considers NIDS events to discover hosts that were recently attacked and are now attacking others, scanning others or invoking "backdoor" or "Trojan" connection attempts.
<a href="#">NIDS Compromise Event Spike</a>	This script subscribes to critical NIDS events and alerts if one host is the source of more than 100 events in a 1 minute period.
<a href="#">NIDS Compromised Server</a>	This script automatically learns which local IP addresses are servers and then checks to see if these systems are attacking other systems. Requires IDS events as well as realtime Passive Vulnerability Scanner alerts.
<a href="#">Successful Login After Multiple Failures</a>	This script looks for valid SSH or Windows logins occurring after there have been several login failures. This sort of activity can indicate SSH or Windows brute force attacks. It requires the brute_force_password_guessing.tasl script to generate Password_Guessing events.
<a href="#">Suspicious Outbound Connections</a>	This script correlates critical NIDS attacks with outbound network connections to port 21, 69 and 80 in an attempt to find post-compromise file grabs by worms and automated exploit tools.

*A small sample of Tenable TASL scripts used by customers*

EVALUATION TIP: Review the TASL script detect\_change.tasl and consider its use as part of your efforts to comply with the HIPAA Security Rule. The script looks for change that would be common within many organizations and could be determined by many log sources. Consider it enhancement to maximize its performance within your own organization. If you are going to forward custom logs produced by custom applications, perhaps review your ability to normalize them for change events and then incorporate those change events into the TASL script.

## HIPAA Security Rule: Additional Considerations

Within Technical Safeguards the Transmission Security standard includes the Encryption implementation specification which can be summarized as "Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate." Also within Technical Safeguards the Access Control Standard includes the Encryption and Decryption implementation specification which can be summarized as "Implement a mechanism to encrypt and decrypt electronic protected health information." Tenable does not currently sell commercial products for encryption. However, if your organization makes it a compliance policy to encrypt all EPHI before transmission internally and/or externally it should be noted that PVS has a real-time alerting facility which can be integrated into Security Center and LCE and can be used to probe unencrypted transmissions for sensitive type information which may indicate an accidental or malicious disclosure of EPHI. Tenable has explored this functionality with customers for the detection of credit cards and social security numbers within unencrypted file transmissions, for example, FTP and HTTP. EPHI in the form of HIPAA X12 EDI transactions has very unique fingerprints that would help in the detection of unencrypted X12 file transmissions. For example, consider this snippet from a HIPAA X12 transaction file:

CLM\*111446666\*90.40\*

CLM01 is the Patient Account number which could be their SSN and in the example is “111446666”. And CLM02 is a total claim charge. It does not matter that the line would continue with more elements or that there are more lines since we already have something reasonably unique to distinguish an X12 EDI transaction file, in this case a Health Care Claim 837 X12 transaction. 837's contain lots of EPHI data. You could customize the PVS to have your own devised real-time alerts for detection of potential breaches in security for disclosing unencrypted EPHI. Talk to your sales manager about Tenable partnered Professional Service organizations if you would wish to outsource this kind of customization work or any customization work in general.

The Tenable 3D Tool, as its name suggests, renders technical vulnerability data in 3 dimensions on a Windows Desktop. It summarizes visually the level of risk within your infrastructure very effectively. It takes its data from the cumulative database held in Security Center. The HIPAA Security Rule when browsing through its implementation standards seems very focused on those hosts and devices that hold EPHI, however, can you use the 3D Tool's topology view to get a feel of how all your hosts and devices are interconnected in your infrastructure? Can the 3D Tool for example help you identify external entry points into your infrastructure that would allow unwanted guests and can it help you evaluate whether those entry points have appropriate security measures? Would it help in complying with an ongoing review of change within your infrastructure handling EPHI?

## About Tenable Network Security

Tenable, headquartered in Columbia, Md., USA, is the world leader in Unified Security Monitoring. Tenable provides agent-less solutions for continuous monitoring of vulnerabilities, configurations, data leakage, log analysis and compromise detection. For more information, please visit us at <http://www.tenablesecurity.com/>.

---

### GLOBAL HEADQUARTERS

**Tenable Network Security**  
7021 Columbia Gateway Drive,  
Suite 500  
Columbia, MD 21046  
410.872.0555  
[www.tenable.com](http://www.tenable.com)

---

