# Unified Security Monitoring (USM)

## *Real-Time Situational Awareness of Network Vulnerabilities, Events and Configurations*

**January 27, 2009**
**(Revision 2)**

**Renaud Deraison**
Chief Research Officer

**Ron Gula**
Chief Technology Officer

**Marcus Ranum**
Chief Security Officer

# Table of Contents

## Introduction

Modern enterprise networks face a plethora of technical, political and business hurdles that make accurate security and compliance monitoring difficult and costly. Tenable has pioneered a unique "Unified Security Monitoring" approach that is revolutionizing the way our customers are monitoring (i.e. gathering, evaluating, communicating and reporting) security and compliance information. This paper will define "Unified Security Monitoring" and walk the reader through what is unique and how Tenable's "unified" approach overcomes challenges facing enterprise IT and security groups around the globe.

## Unified Security Monitoring Defined

Tenable defines Unified Security Monitoring (USM) as a "unification of real-time vulnerability monitoring (24x7 discovery through remediation), critical log/event monitoring and custom compliance monitoring capabilities in a single, role-based, interface for IT and Security users to evaluate, communicate and report the results for effective decision making".

## How is USM different from what is on the market today?

USM is different and unique from what is on the market today because it combines three distinct point solutions/markets (Vulnerability Management, Security Information Management and Configuration Auditing) into one fully integrated solution.

1. *Real-time vulnerability and patch assessments and vulnerability lifetime management* using a combination of host-based, network and 24x7 passive vulnerability assessment technologies.
2. *Critical security event monitoring* using log and event aggregation and normalization and security event alerting using statistical network anomaly based alerting and signature-based correlation alerts.
3. *Custom compliance monitoring* using a combination of agent-less configuration audit files designed for specific government regulations, best practices or company specific configurations and signature-based alerting when "defined alert criteria for non-compliance" have been met.

## Unified Security Monitoring Solution Description

From a network security feature set, Tenable offers a variety of ways to detect vulnerabilities and security events. Our core technology is extremely powerful for conducting network compliance audits and communicating the results to many different consumers.

Tenable Unified Security Monitoring components:

- **Tenable Security Center** – Tenable's Security Center is a web based management console that unifies the process of asset discovery, vulnerability detection, event management and compliance reporting. The Security Center enables efficient communication of security events to IT, management and audit teams.

- **Tenable Nessus Vulnerability Scanner (Nessus)** – Nessus is an active scanner that provides a snapshot of network assets, their vulnerability exposure, their configuration and if they contain sensitive data.
- **Tenable Passive Vulnerability Scanner (PVS)** – PVS behaves like a security motion detector on the network. PVS maps new hosts and services as they appear on the network and monitors for vulnerabilities 24/7. Part of this process also includes looking for sensitive data in motion as well as real-time change detection.
- **Tenable Log Correlation Engine (LCE)** – LCE correlates and analyzes event log data from raw network traffic, system logs and user activity. LCE is designed to work in conjunction with Security Center to provide a central portal for security management.

## Unified Security Monitoring Solution Benefits

### Asset Centric Analysis

The combination of network scanning, passive network monitoring and integration with existing asset and network management data allows the Security Center to organize network assets into categories. This enables an auditor to review all components of a particular application.

Typically, an auditor reviews a long list of IP addresses that may have vulnerabilities of various severities associated with them. What is usually missing is the correlation of interdependencies of the application's components. The Security Center is a powerful tool in compliance monitoring by providing a complete asset list for applications and ensuring that the weakest link in the chain is accounted for.

For example, consider a typical PeopleSoft deployment for a human resources group. The actual PeopleSoft application may run on one or more Windows servers. Those applications will interact with several databases, be connected over some network switches and possibly have front-end web servers for load-balancing. The entire group of servers comprise the "PeopleSoft" asset. A security problem with a switch or database may be just as critical to one found in the actual PeopleSoft program. To an auditor, being able to work with all of the security issues for one asset type at a time is very efficient.

### Sensitive Data Monitoring

Both Nessus and PVS can identify sensitive data. The Nessus scanner can be easily configured to look for common data formats such as credit card numbers and social security numbers. It can also be easily modified to search for documents with unique corporate identifiers such as employee names, project topics, sensitive keywords and so on. Nessus can perform these searches without an agent and only requires credentials to scan a remote computer. PVS can monitor network traffic to identify sensitive traffic in motion over email, web and chat activity. It can also simply identify servers that host office documents on web servers. The Security Center combines the information about sensitive data gained from Nessus and the PVS in several ways:

- By considering which assets have sensitive data on them, it can be easy to identify if data is being hosted on unauthorized systems.
- Classifying assets based on the sensitivity of the data they are hosting can simplify configuration and vulnerability auditing by only considering those hosts and not the entire network.

- While responding to security incidents or access control violations, having knowledge of the information on the target system can help identify if a system compromise also involves potential theft or modification of data.

Both Nessus and PVS also act as a deterrent. If organizations realize they will be audited for their use of certain types of data, they will be less likely to give it to others or perhaps leave it on unauthorized systems.

## Configuration Audits

Security policies, guidelines, standards and procedures provide a mandate for maintaining network security. A policy is defined as what will and will not be permitted, such as "users are required to have passwords and keep them secure". Guidelines are suggested methods of how to adhere to the policy, such as "users should change passwords on a regular basis". Standards are specific technical rules for a particular platform, such as Microsoft IIS or database servers. A standard might state "passwords must be set to expire every 90 days and must force the user to use a combination of alpha-numeric characters". Finally, procedures provide users and systems administrators with methods for maintaining security, such as "how to install a Microsoft IIS Server Securely". It is important to understand the distinction between these to ensure appropriate compliance.

A configuration audit is one where the auditors verify that servers and devices are configured according to an established standard and maintained with an appropriate procedure. The Security Center can perform configuration audits on key assets through the use of Nessus' local checks that can log directly onto a Unix or Windows server without an agent.

The Security Center ships with several audit standards. Some of these come from best practice centers like the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). Some of these are based on Tenable's interpretation of audit requirements to comply with specific industry standards such as PCI, or legislation affecting financial institutions. In addition to the base audits, it is very easy to create customized audits for the particular requirements of any organization. These customized audits can be loaded into the Security Center and made available to anyone performing configuration audits within an organization.

Once the audit policies have been configured in the Security Center, they can be repeatedly used with little effort. Also, with the knowledge of assets, the Security Center can perform audits intended for specific assets. Through the use of audit policies and assets, an auditor can quickly determine the compliance posture for any specified asset.

## Security Event Audits

The Security Center and LCE can perform the following forms of security event management:

- Secure log aggregation and storage
- Normalization of logs to facilitate analysis
- Correlation of intrusion detection events with known vulnerabilities for identification of high-priority attacks
- Sophisticated anomaly and event correlation to look for successful attacks, reconnaissance activity and theft of information.

For real-time compliance monitoring, Tenable ships LCE with logic that can map any number of normalized events to a "compliance" event. For example, a login failure may be benign, but when it occurs on a financial asset, it must be logged at a higher priority. The Security Center and LCE allow any organization to implement their compliance monitoring policy in real-time. These events are also available for reporting and historical records. LCE also allows for many forms of best practice and human resources (HR) monitoring. For example, unauthorized changes can be detected many different ways through network monitoring. Another useful application of LCE is to determine if users recently separated from the organization are still accessing the system.

# In Depth: Tenable's Real-Time Vulnerability Philosophy

### Blended Assessments

Tenable's vulnerability assessment philosophy, simply put, is a "blended" form of security assessment that utilizes a combination of Tenable's active, passive (unique to Tenable) and host-based techniques. Tenable believes that no one method is better than another. Each has several advantages and disadvantages that can be used to offset a variety of technical and political limitations imposed by large enterprise networks.

### Active Assessments

As previously stated, Tenable manages the Nessus Vulnerability Scanner, which is available for Unix, Windows and Mac OS X operating systems. Nessus can be managed by the Security Center for scheduled scanning, distributed scanning, reporting and remediation management.

When deployed in a distributed architecture, full scans of large Class B networks can be completed within just a few hours.

### Passive Assessments 24x7

Tenable's Passive Vulnerability Scanner (PVS) is a unique offering and is essentially a "vulnerability sniffer" that will produce a list of hosts, their clients, their services and any vulnerability associated with the discovered information. Tenable first offered PVS in October of 2003 and has been continuously improving it. When Tenable's Research group releases Nessus vulnerability checks, similar plugins are written for PVS.

The Windows and Unix versions of PVS can be deployed stand-alone and can produce Nessus compatible information. Multiple PVS sensors can be deployed with a Security Center for distributed management and centralized vulnerability analysis.

When deployed with Tenable's Security Center, passive assessments are completed instantly. Passive vulnerability data from each sensor is continuously fed into the Security Center. A user viewing the Security Center can see all vulnerability data for each host passively detected in near real-time.

### Host-Based Assessments

One of the major challenges faced when maintaining the configuration of large enterprise software deployments is to place an agent on every server. Because of this, Tenable's solution to conduct host-based assessments is agent-less. Tenable's active vulnerability

scanner, Nessus, simply requires credentials to log on to any Unix or Windows host to conduct host-based checks.

Nessus supports the ability to log on to Unix systems via the Secure Shell protocol. It also supports logging on to Windows 2000, XP, 2003 and Vista systems via the SMB network API. Both techniques allow the vulnerability scanner to have direct access to the Windows registry and the various patch management systems under Red Hat, FreeBSD, Solaris and other supported Unix operating systems.

Having access to the underlying configuration of a scanned server increases the speed and accuracy of vulnerability assessment. The absolute patch level can be checked without having to exercise the actual daemons. The speed of checking these systems is also much faster as network latency is not present. Also, knowing the actual patch level of a system can affect how administrator actions are interpreted. For example, if a system administrator has claimed to have patched Apache 1.3, they may have in fact simply disabled it for a given period of time. This allows the Nessus vulnerability scanner to determine the difference between a quick fix and a fully mitigated security issue.

For a large enterprise with many different networks, network administrators and security personnel, the Security Center is ideal for managing security. It can detect security issues through "blended" vulnerability assessments by utilizing host-based, network scans and passive scans. It can communicate this information to senior management in business terms they understand and it can also communicate relevant information to network and system administrators in their language.

With the Security Center, management of host-based, network-based and passive vulnerability assessments is very easy. Any user with the proper credentials can perform analysis of the vulnerabilities discovered by any form of blended assessment. The Security Center has many ready-to-run policies that will invoke only active or host-based forms of assessment. Vulnerabilities detected can be filtered with the click of a button by asset type, by vulnerable port or by network address. This makes it very easy for users to run their own form of assessment or analyze the results of someone else's assessment of their network.

For a more in-depth description of our vulnerability monitoring capabilities, please see these whitepapers:

- Tenable Tools for Security Compliance - The Antivirus Challenge
- Blended Security Assessments
- Dedicated and Distributed Vulnerability Management
- Reliability and Uniqueness of Tenable Nessus Technology
- Web Application Security Testing with the Security Center and Nessus
- Using Nessus to Detect Wireless Access Points

## In Depth: Tenable's Event Management Philosophy

### Critical Event Detection

Tenable's philosophy for security event management is to focus on the generation of easily understood "actionable" events and back that up with extremely scalable tools to navigate the flood of security logs. These actionable events can be sent to network operations centers and can also be used as indicators of where to begin forensic analysis in the vast amount of stored logs.

## Vulnerability and IDS Event Correlation

Tenable has greatly simplified the intrusion detection "false positive" problem by performing real-time vulnerability to IDS event correlation with its Security Center. Modern network IDS devices generate enormous amount of alerts, most of which are real, but ineffective attacks. The Security Center has knowledge of the state of each server's vulnerabilities and automatically correlates known attacks against known vulnerabilities. This can reduce the amount of alerts from millions per day to dozens.

When a correlation occurs, a simple message that says a particular server has been attacked with a technique that is likely to succeed can be sent to system owners, operations people and other places. This unique message can be used to build policies and procedures around events, regardless of the specific event type. It may not be obvious to an administrator what the nomenclature of a particular IDS event name is, but it is not hard to grasp that a critical attack may have occurred.

Security Center's technology is much more accurate than other forms of similar vulnerability correlation techniques because it can also make use of passively detected and host-based detected security information. Traditionally, most vulnerability correlation tools only make use of network scans that grow out of date quickly and are often limited in scope. Security Center can import vulnerability data from PVS. This is a sniffer that monitors network traffic 24x7 and detects new vulnerabilities and applications in real-time.

Security Center can also manage the credentials required to "log" into Unix and Windows servers to conduct host-based vulnerability checks. Information from network scans, passive analysis and host-based checks is then utilized to perform accurate vulnerability correlation with IDS events.

## Statistical and Behavioral Anomaly Detection

Tenable has also simplified the process for automatically detecting trends and deviations from "normal" network activity. LCE can be used to normalize and collect events from many different types of sources including sniffers, firewalls, servers, honeypots and authentication devices.

As LCE receives these events, for each host on the network, it computes the normal event load and the amount of time the host is acting as a client or server. If there are swings in these "normal" loads, alerts can be generated. More interestingly, events that are only slightly statistically significant can be used as pointers to understand "normal" network behavior. This is a very important concept because network usage, load and communication flows often change on a daily basis.

## Custom Business Rules Alerting

In addition to alerting statistical anomalies, LCE can be programmed with any type of event alerting logic desired. Tenable has produced the Tenable Application Scripting Language (TASL), which is similar to JAVA and the Nessus Attack Scripting Language (NASL). TASL gives LCE the ability to perform complex correlation between multiple events with any type of computational dependency. For example, each of these scenarios can be programmed in a simple TASL script:

- Alerting if there have been more than 100 SSH login failures within 5 minutes.

- Alerting if there have been more than 10 authentication failures, a successful login and a password change, which is a common phishing technique.
- Alerting if two different types of NIDS (such as IntruShield and Snort) both see similar normalized attacks.
- Alerting if a specific network generates any outbound events.
- Detecting when "worm" IDS events have infected a host on the monitored network.
- Alerting on IDS events that have occurred.
- Alerting on large numbers of web "404" failures from a single host.
- Alerting on large numbers of TCP sessions (firewall or sniffed) from specific external networks that may indicate known hostile probing or scanning.

When TASL scripts generate new events, they can be fed back into LCE for analysis by other TASL scripts, sent as an IDS event to the Security Center for alerting, sent as an email to a specific user list or simply invoke a custom program.

Tenable has made available several TASL scripts that can be used as-is or as a template when writing new scripts, at http://cgi.tenablesecurity.com/tasl.html.

## Target Based Intrusion Detection

Previously mentioned, PVS sniffs network traffic to discover vulnerabilities in real-time. As it discovers new hosts, new applications and vulnerabilities it is also searching for evidence of likely compromised systems.

Tenable has programmed PVS such that when it detects common applications, it searches outbound traffic for indications of compromise. For example, if PVS observes an Apache web server on a particular host and port, it will look for the results of several common Apache exploits such as displaying the `/etc/passwd` file and invocation of Unix or Windows commands. These patterns are searched for, regardless of the exploit and regardless of any attack masking techniques used.

The alerts generated by PVS are often only in the hundreds per day for even the busiest enterprise networks. This low "false positive" rate makes the data collected by the scanner useable not only by Tenable's Security Center and LCE, but by network management and operations consoles.

## Intelligent Log Normalization and Storage

LCE allows very easy configuration of which logs must be saved and which must be normalized. Simply put, LCE can be configured to process events from close to 200 different log sources such as firewalls and operating systems.

When configuring LCE, it is very easy to select what types of log sources exist and what sort of events must be normalized. LCE also has a mode where any log sent to it can be saved on the local disk, a second disk or on network storage.

This is a very important concept because not all logs may be relevant to understanding your overall security posture, yet there may likely be regulatory requirements to store all logs. LCE can be configured to solve both of these problems. For example, LCE can be used to save all logs for 90 days, yet only normalize intrusion detection, firewall and Windows security events. This allows for efficient analysis of the security events, while still retaining all logs, including those not relevant to security for 90 days.

### High Speed Queries

Having a large amount of events is of little use if it takes 30 minutes to produce a "trending" report. Tenable's approach is that all user interfaces for the Security Center and the LCE handle close to 500 million normalized events and have any query complete in less than a few seconds. This means that a user could sort events, find something of interest and drill directly down into the actual log message in just a few clicks. It also means that a user can jump directly from an interesting intrusion event, to all log events (firewall, operating system, honeypot, etc.) concerning the attacker's IP with one click.

### Role Based Log Analysis

LCE's analysis performance also allows unique accounts to be configured that have limited access to the available data. For example, an account for all DNS administrators could be configured such that when they logged in, they would only be presented with logs that "touched" their servers.

This has several benefits. Foremost, during an incident, all of the relevant logs are available for immediate analysis. This includes historical events as well as those that occurred within the past 5 minutes. Although forensic log analysis is typically the job of the security expert, system administrators will often recognize aberrations in the logs that may otherwise go unnoticed. An additional benefit is that these logs are available for performance, diagnostics and troubleshooting. For example, having access to the firewall logs may help an email administrator troubleshoot the configuration of a high-availability server.

For a more in-depth description of our security event monitoring capabilities, please see these whitepapers:

- Security Event Management
- Correlating IDS Alerts with Vulnerability Information
- Advanced Event Correlation Scripting

## In Depth: Tenable's Compliance Monitoring Philosophy

Tenable's solutions can be applied to achieving a state of compliance by ensuring the proper configuration and monitoring of key assets for security compliance. It is crucial to monitor for compliance in a manner as close to real-time as possible to ensure the organization does not drift out of compliance over time. The greater the gap between monitoring cycles, the more likely it is for compliance violations to occur undetected.

Audit criteria vary among different industries and geographic locations. New legislation is continually being developed that changes the standards for audits in these industries. It is important to be familiar with multiple compliance standards, even if they do not seem to be required at the moment. Changing legislation or shifts in an organization's business offerings require that managers keep abreast of audit criteria in other industries.

For a more in depth review on how Tenable can assist you on specific compliance issues, please request Tenable's Real-Time Compliance Monitoring Whitepaper by emailing Sales at sales@tenablesecurity.com. The Real-time Compliance Monitoring Whitepaper illustrates specifically how Tenable's solutions enable managers to assure compliance with all the following regulations, standards and best practice guidelines:

- BASEL II
- Control Objectives for Information and related Technology (COBIT)
- Defense Information Systems Agency Security Technical Implementation Guides
- (STIG)
- Federal Information Security Management (FISMA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO 17799 Security Standards
- Information Technology Information Library (ITIL)
- Motion Picture Association of America (MPAA) inquiries
- National Institute of Standards (NIST)
- National Security Agency (NSA)
- North American Electric Reliability Council (NERC)
- Payment Card Industry (PCI)
- Recording Industry Association of America (RIAA) inquiries
- Sarbanes-Oxley (SOX)
- Site Data Protection (SDP)
- Various State Laws (California's Database Breach Notification Act - SB 1386)

For a more in-depth description of our compliance monitoring capabilities, please see these whitepapers:

- Application Note: HIPAA
- Application Note: Payment Card Industry (PCI)
- Tenable Product Evaluation Application: HIPAA
- Real-Time PCI Compliance Monitoring
- Network Security Implications of "Visible Ops"
- Protecting Critical Infrastructure - SCADA Network Security Monitoring

## Conclusion

Tenable's Unified Security Monitoring solution has been designed to meet many different challenges faced by IT and security for vulnerability, event and compliance monitoring. Tenable's USM solutions focus on managing secure configuration and management that can be applied to many different compliance guidelines.

## 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/.*

**TENABLE Network Security, Inc.**
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
TEL: 410-872-0555
http://www.tenablesecurity.com/