

Security Exchange Commission Risk Alert Reference Guide

June 11, 2014

(Revision 1)

Table of Contents

Introduction	4
This Guide	5
The Seven Cybersecurity Goals	5
Goal 1: Maintain accurate inventories	5
Goal 2: Maintain knowledge of normal operations	6
Goal 3: Discover vulnerabilities and track remediation progress	6
Goal 4: Prevent unauthorized activity	7
Goal 5: Monitor for malicious activity	8
Goal 6: Monitor for data loss	9
Goal 7: Measure compliance	9
SecurityCenter Components	10
Compliance & Configuration Assessment	10
Compliance Summary - Check Result Ratio	10
GLBA Dashboard	11
NIST 800-53 Trending Dashboard	12
Cybersecurity Framework Audit Check Result Ratio Dashboard	13
Discovery & Detection	14
Daily Host Alerts Trend (Last 5 Days)	14
Malicious Process Detection Dashboard	15
Hosts Per Class C	15
New Hosts (Last 5 Days)	16
Monitoring	16
NetFlow by Port (Last 72 Hours)	16
Data Leakage Monitoring Dashboard	17
Event Trending By Type - Data Leak	17
File and Directory - Software Installed Events (Past 7 Days)	18
Malicious Process Monitoring	18
Netflow Top Talkers By IP Address (Last 24 Hours)	19
PVS Network Trending - Cloud Data	19
Web Activity	20
Security Industry Trends	21
CoCS 20 Critical Security Controls - Control 1 New Devices Detected	21
CoCS 20 Critical Security Controls - Control 15 Controlled Access/Data Leakage	22
CoCS 20 Critical Security Controls - Control 17 - Data Protection	22
Malware Detection - Viewing the Invisible	23
SANS 6 - Category 2 - System and Data Changes	24
SANS 6 - Category 3 - Network Activity	25
Sensitive Data - Potential Sensitive Information Active Scanning	26
Threat Detection & Vulnerability Assessments	27
Vulnerability Top Ten - Top 10 Remediations	27
Vulnerability Top Ten - Top 10 Exploitable Vulnerabilities	27
Vulnerability Top Ten - Top 10 Most Vulnerable Hosts	28
Vulnerabilities Discovered (Last 30 Days)	28
Top 100 Users Generating Events (Last 72 Hours)	29
Malware Detections	29
Network Changes	30

Potential Suspicious Activity	30
Potential Data Loss.....	31
CVE Analysis / CVE Trending by Year Dashboards.....	32
Event Vulnerabilities - Exploitable and Malware.....	33
Event Vulnerability Indicators Dashboard.....	33
Malicious URL.....	34
Malware Detection Dashboard.....	34
PVS Trust Dashboard.....	35
The Next Steps	36
Features to Enhance Security Posture	36
Pivoting and Contextual Filtering.....	36
Combination Asset Modeling	37
User Based Modeling and Reporting	37
Create Assets	37
Create Reports from Dashboards/Collections	37
Logging.....	39
Audit Files for Compliance Checking	39
The Difference Between Vulnerability and Audit Scanning.....	40
Scanning Methodology	40
Summary.....	41
About Tenable Network Security.....	42

Introduction

On April 15, 2014, the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) issued a Risk Alert describing its Cybersecurity Initiative. This Risk Alert states:

"OCIE's cybersecurity initiative is designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats. As part of this initiative, OCIE will conduct examinations of more than 50 registered broker-dealers and registered investment advisers focused on the following: the entity's cybersecurity governance, identification and assessment of cybersecurity risks, protection of networks and information, risks associated with remote customer access and funds transfer requests, risks associated with vendors and other third parties, detection of unauthorized activity, and experiences with certain cybersecurity threats."¹

The Risk Alert contains an Appendix that is "a sample request for information and documents used in this initiative."² The information requests in the Appendix advocate various cybersecurity practices. In general, cybersecurity practices can be grouped into the seven "goal" areas listed below.

1. Maintain accurate inventories
 - For physical devices, software platforms, and applications
2. Maintain knowledge of normal operations
 - For example, expected connections and data flows, utilization of encryption, backup services, documentation of policy and procedures, etc.
3. Discover vulnerabilities and track remediation progress
 - Includes prioritizing remediations based on risk assessment
4. Prevent unauthorized activity
 - Involves monitoring for and preventing unauthorized activity such as use of unauthorized devices, unauthorized connections, unauthorized escalation of user privileges, unauthorized access, and unauthorized changes
5. Monitor for malicious activity
 - Involves monitoring for (and, where possible, preventing) malicious activity, such as malware and botnet activity, and denial of service
6. Monitor for data loss
 - Involves monitoring for (and, where possible, preventing) data leakage and data loss
7. Measure compliance
 - Involves conducting audits to determine compliance with policies and accepted standards

The Tenable suite of products can assist a firm in achieving these goals. Tenable's SecurityCenter allows a single console to administer continuous active scanning, passive detection, log analysis, vulnerability management, and compliance checking across an organization. Because SecurityCenter is completely scalable and customizable, dashboards and reports can be fine-tuned to deliver the most advanced analysis of cybersecurity risks. SecurityCenter Continuous View (SCCV) allows organizations to improve cybersecurity threat mitigation by integrating vulnerability and threat management into one package.

¹ OCIE Cybersecurity Initiative, SEC National Exam Program Risk Alert, Vol. IV, Issue 2 (Apr. 15, 2014).

² Ibid.

This Guide

The objective of this technical guide is to provide Tenable customers and prospective customers with details on many SecurityCenter components and dashboards that can assist a firm in achieving the seven cybersecurity goals listed above. For each component, a screenshot, description, and other details are given, as well as a section describing how the component applies to the SEC OCIE Risk Alert. Each component is mapped both to the seven cybersecurity goals and to the applicable requests in the Appendix of the OCIE Risk Alert.

All of the listed components are available in the SecurityCenter app feed, an app store of dashboards, reports, and assets. For each component, its category and tags are given, so it can be easily found in the feed.

Each component's requirements are noted. These might include:

- Active vulnerability data – Vulnerability data collected actively by the Nessus vulnerability scanner
- Passive vulnerability data – Vulnerability data collected by the Passive Vulnerability Scanner (PVS), which can identify vulnerabilities on the network by passively sniffing packets
- Event vulnerability data – Vulnerability data collected by the Log Correlation Engine (LCE), which can identify vulnerabilities by reviewing the logs from applications and devices on the network
- Compliance data – Compliance data collected by performing configuration audits using Nessus and audit files; hundreds of audit files, covering everything from applications to devices to industry standards, are available
- Log data – Syslog data collected and normalized by LCE from network devices

This guide is comprised of three primary chapters. This first chapter provides an overview and information about the seven cybersecurity goals. The second chapter contains some example components and dashboards. The last chapter provides helpful suggestions on next steps, and how to use SecurityCenter to achieve the maximum value from the firm's investment.

The Seven Cybersecurity Goals

Goal 1: Maintain accurate inventories

This goal involves maintaining accurate inventories for devices, software platforms, and applications.

Associated requests in the SEC OCIE Risk Alert Appendix:

- Physical devices and systems within the Firm are inventoried (Request 1, sub-bullet)
- Software platforms and applications within the Firm are inventoried (Request 1, sub-bullet)
- The Firm has a process to manage IT assets through removal, transfers, and disposition (Request 10, sub-bullet)

Associated SecurityCenter components:

Component	Page
CoCS 20 Critical Security Controls - Control 1 New Devices Detected	21
Daily Host Alerts Trend (Last 5 Days)	14
File and Directory - Software Installed Events (Past 7 Days)	18
Hosts Per Class C	15
Malicious Process Detection Dashboard	15
Network Changes	30
New Hosts (Last 5 Days)	16

Goal 2: Maintain knowledge of normal operations

This goal involves maintaining knowledge of normal network operations, such as expected connections and data flows, utilization of encryption, and backup services.

Associated requests in the SEC OCIE Risk Alert Appendix:

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated (Request 1, sub-bullet)
- Connections to the Firm's network from external sources are catalogued (Request 1, sub-bullet)
- Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance (Request 1, sub-bullet)
- The Firm periodically tests the functionality of its backup system (Request 10, sub-bullet)
- Please indicate whether the Firm makes use of encryption (Request 11)
- Maintaining baseline information about expected events on the Firm's network (Request 21, sub-bullet)

Also associated with this goal are the many requests in the Appendix for policy and procedure documentation, as these documents describe normal operations.

Associated SecurityCenter components:

Component	Page
CoCS 20 Critical Security Controls - Control 17 - Data Protection	22
Malware Detection Dashboard	34
NetFlow by Port (Last 72 Hours)	16
Netflow Top Talkers By IP Address (Last 24 Hours)	19
Network Changes	30
Potential Suspicious Activity	30
PVS Network Trending - Cloud Data	19
PVS Trust Dashboard	35
SANS 6 - Category 3 - Network Activity	25
Top 100 Users Generating Events (Last 72 Hours)	29
Web Activity	20

Goal 3: Discover vulnerabilities and track remediation progress

This goal involves discovering vulnerabilities, prioritizing remediations based on risk assessment, and tracking the progress of those remediations.

Associated requests in the SEC OCIE Risk Alert Appendix:

- Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value (Request 1, sub-bullet)
- Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences (Request 3)
- Please indicate whether the Firm conducts periodic risk assessments to identify physical security threats and vulnerabilities that may bear on cybersecurity (Request 4)
- The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities (Request 10, sub-bullet)
- Conducting penetration tests and vulnerability scans (Request 21, sub-bullet)

Associated SecurityCenter components:

Component	Page
CVE Analysis / CVE Trending by Year Dashboards	32
Event Vulnerabilities - Exploitable and Malware	33
Malware Detection Dashboard	34
Malware Detection - Viewing the Invisible	23
Sensitive Data - Potential Sensitive Information Active Scanning	26
Vulnerabilities Discovered (Last 30 Days)	28
Vulnerability Top Ten - Top 10 Exploitable Vulnerabilities	27
Vulnerability Top Ten - Top 10 Most Vulnerable Hosts	28
Vulnerability Top Ten - Top 10 Remediations	27

Goal 4: Prevent unauthorized activity

This goal involves monitoring for and preventing unauthorized activity, such as unauthorized devices, unauthorized connections, unauthorized escalation of user privileges, unauthorized access, and unauthorized changes.

Associated requests in the SEC OCIE Risk Alert Appendix:

- The Firm maintains controls to prevent unauthorized escalation of user privileges and lateral movement among network resources (Request 10, sub-bullet)
- The Firm restricts users to those network resources necessary for their business functions (Request 10, sub-bullet)
- The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications (Request 10, sub-bullet)
- Aggregating and correlating event data from multiple sources (Request 21, sub-bullet)
- Monitoring the activity of third party service providers with access to the Firm's networks (Request 21, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm's networks (Request 21, sub-bullet)
- Evaluating remotely-initiated requests for transfers of customer assets to identify anomalous and potentially fraudulent requests (Request 21, sub-bullet)
- Testing the reliability of event detection processes (Request 21, sub-bullet)
- The Firm's network was breached by an unauthorized user (Request 24, sub-bullet)
- The compromise of a customer's or vendor's computer used to remotely access the Firm's network resulted in fraudulent activity, such as efforts to fraudulently transfer funds from a customer account or the submission of fraudulent payment requests purportedly on behalf of a vendor (Request 24, sub-bullet)
- The Firm received fraudulent emails, purportedly from customers, seeking to direct transfers of customer funds or securities (Request 24, sub-bullet)

Associated SecurityCenter components:

Component	Page
CoCS 20 Critical Security Controls - Control 1 New Devices Detected	21
CoCS 20 Critical Security Controls - Control 15 Controlled Access/Data Leakage	22
CoCS 20 Critical Security Controls - Control 17 - Data Protection	22

Daily Host Alerts Trend (Last 5 Days)	14
Event Vulnerability Indicators Dashboard	33
File and Directory - Software Installed Events (Past 7 Days)	18
Malicious Process Detection Dashboard	15
NetFlow by Port (Last 72 Hours)	16
Network Changes	30
Potential Suspicious Activity	30
SANS 6 - Category 2 - System and Data Changes	24
Top 100 Users Generating Events (Last 72 Hours)	29
Web Activity	20

Goal 5: Monitor for malicious activity

This goal involves monitoring for (and, where possible, preventing) malicious activity, such as malware and botnet activity, denial of service, etc. (Note that data leakage is not covered here, but in the next goal.)

Associated requests in the SEC OCIE Risk Alert Appendix:

- The Firm maintains controls to secure removable and portable media against malware and data leakage (Request 10, sub-bullet)
- The Firm maintains protection against Distributed Denial of Service (DDoS) attacks for critical internet-facing IP addresses (Request 10, sub-bullet)
- Aggregating and correlating event data from multiple sources (Request 21, sub-bullet)
- Establishing written incident alert thresholds (Request 21, sub-bullet)
- Monitoring the Firm’s network environment to detect potential cybersecurity events (Request 21, sub-bullet)
- Monitoring the Firm’s physical environment to detect potential cybersecurity events (Request 21, sub-bullet)
- Using software to detect malicious code on Firm networks and mobile devices (Request 21, sub-bullet)
- Monitoring the activity of third party service providers with access to the Firm’s networks (Request 21, sub-bullet)
- Testing the reliability of event detection processes (Request 21, sub-bullet)
- Malware was detected on one or more Firm devices (Request 24, sub-bullet)
- Access to a Firm web site or network resource was blocked or impaired by a denial of service attack (Request 24, sub-bullet)

Associated SecurityCenter components:

Component	Page
CoCS 20 Critical Security Controls - Control 15 Controlled Access/Data Leakage	22
CoCS 20 Critical Security Controls - Control 17 - Data Protection	22
Event Vulnerability Indicators Dashboard	33
Malicious Process Detection Dashboard	15
Malicious Process Monitoring	18
Malicious URL	34
Malware Detection Dashboard	34
Malware Detections	29

Malware Detection - Viewing the Invisible	23
Potential Suspicious Activity	30
PVS Trust Dashboard	35

Goal 6: Monitor for data loss

This goal involves monitoring for (and, where possible, preventing) data leakage and data loss.

Associated requests in the SEC OCIE Risk Alert Appendix:

- The Firm has a process to manage IT assets through removal, transfers, and disposition (Request 10, sub-bullet)
- The Firm maintains controls to secure removable and portable media against malware and data leakage (Request 10, sub-bullet)
- The Firm maintains a written data destruction policy (Request 10, sub-bullet)
- Aggregating and correlating event data from multiple sources (Request 21, sub-bullet)
- Using data loss prevention software (Request 21, sub-bullet)
- Testing the reliability of event detection processes (Request 21, sub-bullet)
- An employee or other authorized user of the Firm's network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive customer or Firm information, or damage to the Firm's network or data (Request 24, sub-bullet)
- Since January 1, 2013, if not otherwise reported above, did the Firm, either directly or as a result of an incident involving a vendor, experience the theft, loss, unauthorized exposure, or unauthorized use of or access to customer information? (Request 25)

Associated SecurityCenter components:

Component	Page
CoCS 20 Critical Security Controls - Control 15 Controlled Access/Data Leakage	22
CoCS 20 Critical Security Controls - Control 17 - Data Protection	22
Data Leakage Monitoring Dashboard	16
Event Trending By Type - Data Leak	17
Potential Data Loss	31
Sensitive Data - Potential Sensitive Information Active Scanning	26

Goal 7: Measure compliance

This goal involves conducting audits to determine if organizations and associated networks comply with policies and accepted standards.

Associated requests in the SEC OCIE Risk Alert Appendix:

- Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes (Request 9)
- Please indicate whether the Firm conducts periodic audits of compliance with its information security policies (Request 12)
- If the Firm conducts or requires cybersecurity risk assessments of vendors and business partners with access to the Firm's networks, customer data, or other sensitive information, or due to the cybersecurity risk of the outsourced function, please describe who conducts this assessment, when it is required, and how it is conducted. If a questionnaire is used, please provide a copy. If assessments by independent entities are required, please describe any standards established for such assessments. (Request 16)

Associated SecurityCenter components:

Component	Page
Compliance Summary - Check Result Ratio	10
Cybersecurity Framework Audit Check Result Ratio Dashboard	13
GLBA Dashboard	11
NIST 800-53 Trending Dashboard	12

SecurityCenter Components

Listed in this section are dashboards and components sorted by the SecurityCenter category under which they can be found.

Compliance & Configuration Assessment

The Compliance & Configuration Assessment category contains dashboards and reports that aid with configuration, change, and compliance management. Many of these require the use of Tenable audit files to return useable data. The dashboards in this section usually contain a Pass/Fail matrix showing a ratio on the pass/fail status of an audit check. Passed checks are displayed with a green background, failed checks are displayed with a red background, and advisories and checks that must be verified manually are displayed with an orange background. Failed checks and checks requiring manual verification should be further investigated.

Compliance Summary - Check Result Ratio

Goal 7: Measure compliance

This component provides a ratio view of systems that have been checked for a variety of compliance standards. The ratio bar provides a visual of the number of compliance checks that have either passed, failed, or that require some manual verification.

The cells in this component use the audit files released after July 1, 2013, which incorporate a reference tag that maps many audit checks to a respective standard. In the case of this component, the audit files must contain "800-53|AC-1" on the reference line of the applicable

audit check. For example, "reference: CCE|CCE-8912-8,800-53|IA-5,PCI|8.5.12,800-53|CM-6". In this screenshot, you can see the reference added. Please note that when creating filters and reports, the "800-53: AC-2" shown in the example is actually "800-53|AC-2" in the data query.

Systems	Passed	Manual Check	Failed
8500.2	0	NONE	NONE
800-53	4	45%	55%
BSI-100-2	2	54%	14%
CAT	9	81%	14%
CCE	2	26%	3%
CCI	8	28%	15%
CIS Level	6	28%	24%
HIPAA	3	59%	NONE
PCI	12	49%	8%
PCI-2.0	2	60%	5%
PCI-3.0	2	46%	NONE
SANS-CSC	2	59%	7%
STIG-ID	9	81%	14%

Category: Compliance & Configuration Assessment
 Tags: BSI, CCE, CCI, CIS, Compliance, DoD, HIPAA, NIST, PCI, SANS, STIG, Pass/Fail

Requirements: Compliance data, local checks, current audit files

Related Resources

Compliance Summary Dashboard
 Compliance Summary Report
 NIST 800-53 Report



- **8500.2** - The DoDI 8500.2 directive provides an overview of all information assurance configurations and implementation standards for the DoD.
- **800-53** - NIST Special Publication 800-53 R4 Security and Privacy Controls for Federal Information Systems and Organizations provides a catalog of security and privacy controls for federal information systems and organizations.
- **BSI-100-2** - The IT-Grundschutz Standards and Catalogues are a set of recommendations designed to assist an organization in achieving an appropriate security level for information throughout an organization.

- **CAT** - Findings from a DISA STIG are grouped into three Categories (CAT) based on the severity of the weakness.
- **CCE** - Common Configuration Enumeration (CCE) provides a framework for mapping security related system configuration issues across multiple information sources and tools.
- **CCI** - Control Correlation Identifier (CCI) provides a standardized identifier and description for each of the singular, actionable statements that comprise an Information Assurance control or best practice.
- **CIS Level** - The Center for Internet Security (CIS) maintains a series of configuration benchmarks that have two configuration levels, Level-I and Level-II.
- **HIPAA** - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule regulates the information systems used to process and store PHI.
- **PCI DSS** - The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive set of security standards required by major credit card companies to protect cardholder data. Every business that accepts, stores, and transmits credit card data must comply with the PCI DSS.
- **PCI-2.0** - Checks specific to PCI DSS version 2.
- **PCI-3.0** - Checks specific to PCI DSS version 3. This is the latest version of the PCI DSS standard.
- **SANS-CSC** - The Council on CyberSecurity Critical Security Controls (CSCs) were created by a consortium of international agencies and experts from private industry and around the globe to simplify the most critical controls needed around all industries.
- **STIG-ID** - The Security Technical Implementation Guides (STIGs) and the NSA Guides are the configuration standards for DOD IA and IA-enabled devices/systems.

How This Applies to the SEC OCIE Risk Alert

Compliance standards are extremely helpful in assisting with the proper configuration of systems. Tenable's audit files provide references to standards using the reference line mentioned in the component description. This component will help the firm identify all the current audit standards being checked against. The Risk Alert advocates monitoring systems' regulatory compliance. See the Appendix to the Risk Alert:

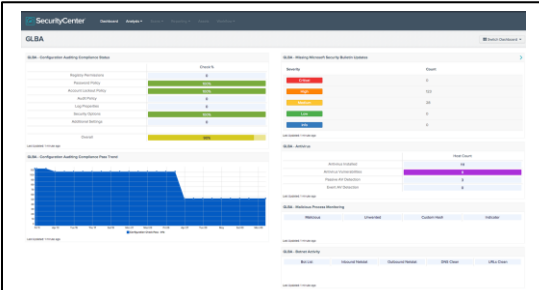
- Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO); the Firm has used to model its information security architecture and processes. (Request 9)
- The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications. (Request 10, sub-bullet)
- Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, in what month and year was the most recent such audit completed, and by whom was it conducted? (Request 12)

GLBA Dashboard

Goal 7: Measure compliance

This dashboard summarizes audit results as they relate to the controls described by the Federal Financial Institutions Examination Council's (FFIEC) guidance on host level malicious code prevention for Section 501 (b) compliance of the Gramm-Leach-Bliley Act (GLBA). The FFIEC guidance provided in their "Information Security Booklet" for host level malicious code prevention includes controls for patch application, security-minded configurations, antivirus, and the periodic auditing of host configurations. The booklet is a member of the FFIEC IT Examination Handbook series and provides coordinated guidance for GLBA Section 501(b) compliance. The booklet can be searched online or downloaded as a PDF.

The Configuration Auditing Compliance Status and Pass Trend dashboard components measure compliance using configuration check results as they relate to best practice configuration settings typically used within financial institutions for Microsoft platforms. The checks are executed by using Tenable Network Security's GLBA Windows System Audit with Tenable Network Security's Nessus vulnerability scanner in conjunction with its agentless compliance



Category: Compliance & Configuration Assessment

Tags: Audit, Compliance, GLBA, MS Bulletin, Microsoft, Trending, Malicious, Indicator, and Botnet

Requirements: Active, Passive, Compliance and Event Data.

Related Resources

NIST 800-53 Trending Dashboards
 Cybersecurity Framework Audit Summary Dashboards
 800-53 Configuration Auditing Dashboards

checks feature. The trend data for passing checks that is used for the area graph is produced by repetitive auditing and is automatically stored within SecurityCenter's central management console. Compliance results are grouped in the Status component by policy families normally found within Windows Group Policy. These can be removed if the audience of the dashboard prefers just an overall compliance status.

The Missing Microsoft Security Bulletin Updates dashboard component provides overall totals for missing security patches by severity. There are five severity ratings: Informational, Low Risk, Medium Risk, High Risk, and Critical Risk. The ratings are derived from risk score ranges found within version 2 of the Common Vulnerability Scoring System (CVSS). The results are produced by Nessus' agentless credentialed scanning and/or through Nessus patch management integration.

The Antivirus dashboard component leverages Nessus' antivirus auditing plugins. For more information regarding the plugins, please see the Tenable blog post "[Auditing Anti-Virus Products with Nessus](#)". It's very relevant to note that when host-based antivirus isn't working, it can be an indicator of malicious code infection.

The Malicious Process Monitoring and Botnet Activity dashboard components don't roll under the FFIEC's host level controls for malicious code prevention; however, one malicious code infection and its activity may lead to further infections so it is appropriate to include the components on the compliance dashboard especially when it's taken into consideration that a single agentless audit policy can be used to produce all the data needed by the dashboard. To learn more about the Malicious Process Monitoring and Botnet Activity dashboard component indicators please see the comprehensive Indicators dashboard, which displays close to 100 different indicators of compromise and suspicious activity using SecurityCenter Continuous View.

If you intend to run more Tenable configuration audits beyond the GLBA Windows System Audit for network appliances, applications, and operating systems found within your organization, please use the SecurityCenter repository feature for segmenting results. The components used by the dashboard can be easily modified to filter by repository.

How This Applies to the SEC OCIE Risk Alert

Many, if not all, of the firms that are subject to the SEC Cybersecurity Risk Alert are required to comply with GLBA. The Risk Alert advocates monitoring systems' regulatory compliance. See the Appendix to the Risk Alert:

- Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes. (Request 9)
- The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications. (Request 10, sub-bullet)
- Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, in what month and year was the most recent such audit completed, and by whom was it conducted? (Request 12)

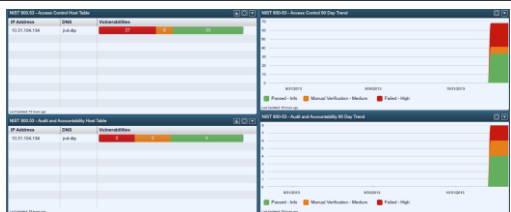
NIST 800-53 Trending Dashboard

Goal 7: Measure compliance

This dashboard provides a series of host tables and trending charts of an organization's compliance with NIST 800-53 standards, based on the FIPS 200 Publication families. The components in this dashboard use the audit files released after July 1, 2013, which incorporate a new reference tag that maps many audit checks to a respective standard. In the case of this dashboard, the audit files must contain "800-53|AC-1" on the reference line of the applicable audit check. For example "reference: CCE|CCE-8912-8,800-53|IA-5,PCI|8.5.12,800-53|CM-6". Please note that when creating filters and reports, the "800-53: AC-2" shown in the example is actually "800-53|AC-2" in the data query.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert specifically lists NIST standards among those that can be used as an information security model. Organizations should review the NIST standards if they are not already doing so. This



Category: Compliance & Configuration Assessment

Tags: Accounts, Asset, Audit, Authentication, Compliance, Disaster Recovery, FIPS, Management, NIST, Physical

Requirements: Compliance Data, Local Checks, and current audit files.

Related Resources

- 800-53 Configuration Auditing Dashboards
- NIST 800-53 Reports
- Chapter and Control IP Summary CCI to NIST 800 53 Reports

dashboard provides the overall compliance status for the firm as it relates to NIST standards. The Risk Alert advocates monitoring systems' regulatory compliance. See the Appendix to the Risk Alert:

- Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes. (Request 9)
- The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications. (Request 10, sub-bullet)
- Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, in what month and year was the most recent such audit completed, and by whom was it conducted? (Request 12)

Cybersecurity Framework Audit Check Result Ratio Dashboard

Goal 7: Measure compliance

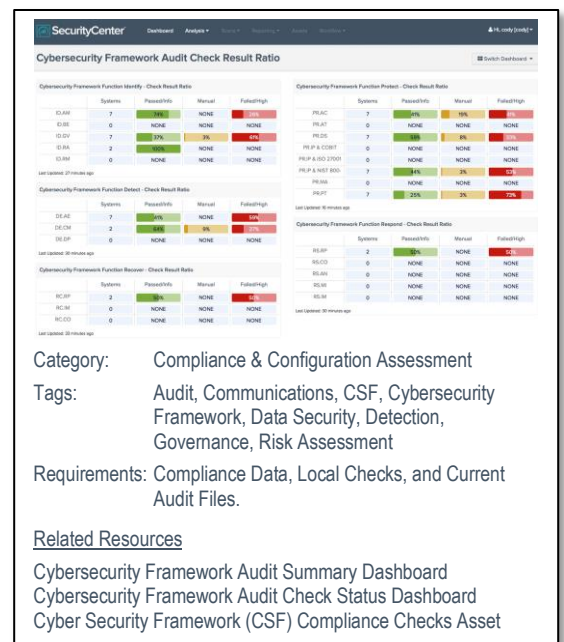
SecurityCenter and Nessus have the ability to check compliance status using audit files. SecurityCenter is able to report on the compliance status of the Cybersecurity Framework using compliance data previously collected. This dashboard provides series of ratio-based indicators for compliance checks performed.

Using the flexible features native to Tenable products, the audit files used when conducting compliance scans can be utilized for more than one type of compliance verification. A clear case in point is the new Cybersecurity Framework (CSF) developed by NIST. The details for CSF can be found at <http://www.nist.gov/cyberframework>.

As part of the Framework, NIST provides references to other standards such as NIST 800-53, COBIT 5, and ISO/IEC 27001. Using data already collected with audit files created or modified after July 2013, security professionals and auditors can begin to validate compliance with CSF, thus giving SecurityCenter customers an edge over others in beginning the analysis of compliance.

This dashboard provides coverage for the following CSF functions:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.
- **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.
- **Detect** – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events, Security Continuous Monitoring, and Detection Processes.
- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning, Communications, Analysis, Mitigation, and Improvements.
- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning, Improvements, and Communications.



How This Applies to the SEC OCIE Risk Alert

The OCIE Cybersecurity Initiative is derived from the NIST “Framework for Improving Critical Infrastructure Cybersecurity”, later called the Cybersecurity Framework (CSF). Using the Nessus audit files containing reference checks for the CSF, the firm can easily determine its compliance. This dashboard specifically reports on CSF compliance. The Risk Alert advocates monitoring systems’ regulatory compliance. See the Appendix to the Risk Alert:

- Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes. (Request 9)
- The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications. (Request 10, sub-bullet)
- Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, in what month and year was the most recent such audit completed, and by whom was it conducted? (Request 12)

Discovery & Detection

The Discovery & Detection category aids in trust identification, rogue detection, and new device discovery. Many of the dashboards and components in this section monitor logs or traffic patterns such as NetFlow. The data displayed often helps to identify subnets in use and if there are indicators of compromise within the subnets.

Daily Host Alerts Trend (Last 5 Days)

Goal 1: Maintain accurate inventories

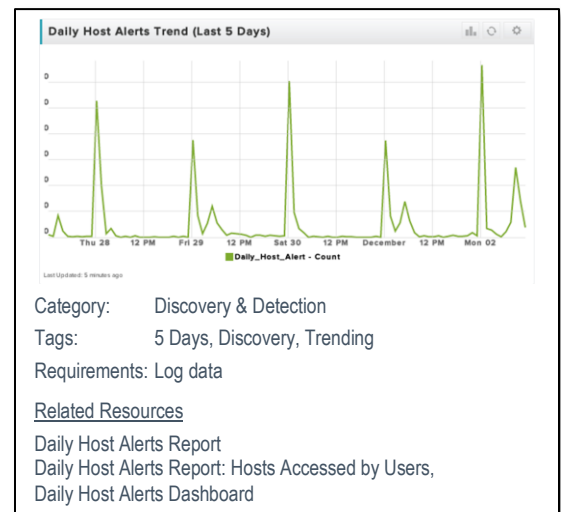
Goal 4: Prevent unauthorized activity

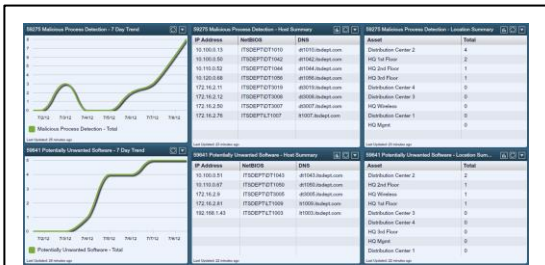
This component presents a line graph of Daily_Host_Alert events by time for the last 5 days. The LCE event Daily_Host_Alert generates, once per day, an alert the first time an event from a local host (such as a DNS lookup or LCE Client connect) is seen. For systems like servers that are always on, there will be a spike around midnight for these events. Other computers may start out their day at various times. This trend graph can assist in looking for anomalies such as systems coming online at unexpected times, unknown systems popping up, or unexpected activity blackouts from known systems.

How This Applies to the SEC OCIE Risk Alert

If the count of events per day in this trend graph is substantially different from the number of inventoried hosts, this may indicate that the device inventory needs to be updated, or that unauthorized systems are present on the network. If the count shows unexplained variances from day to day, this may also indicate that unauthorized systems are present on the network. The Risk Alert advocates maintaining an inventory of physical devices and monitoring for the presence of unauthorized devices on the network. See the Appendix to the Risk Alert:

- Physical devices and systems within the Firm are inventoried. (Request 1, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm’s networks. (Request 21, sub-bullet)





Category: Discovery & Detection
 Tags: 7 Days, Asset, Backup, Botnet, Getting Started, Malicious, Services, Software, & Trending

Requirements: Active Data

Related Resources

- Malicious Process Detection Report
- OpenSSL HeartBleed Report
- Malware Indicators Report

Malicious Process Detection Dashboard

- Goal 1: Maintain accurate inventories
- Goal 4: Prevent unauthorized activity
- Goal 5: Monitor for malicious activity

This dashboard was designed to be used with the Malicious Process Detection in Nessus, including both the malware and potentially unwanted software plugins. When reporting locations, the dashboard uses SecurityCenter’s asset lists. If both static asset lists (to label network subnets as locations) and dynamic asset lists (to group hosts by attributes like operating system) are being used, then SecurityCenter’s GUI-driven report builder will allow refining of the subset of assets. The historical trend graphs use daily snapshots automatically taken by SecurityCenter. The 7-day timeframe can be easily modified to a shorter or longer period.

This dashboard contains two series of three components, with one series focusing on plugin 59275 “Malicious Process Detection”, and the other on plugin 59641 “Malicious Process Detection: Potentially Unwanted

Software”. Both of these plugins use MD5 hashes to determine if one or more running processes on the remote Windows host matches known malware or software known to violate some corporate policies. The components show a 7-day trend, host table, and asset summary. These components provide an overview of known malicious activity on the network.

How This Applies to the SEC OCIE Risk Alert

The identification of malicious process and unauthorized services is critical in assessing risk to any environment. Malicious process can be used to exfiltrate data through backdoor tunnels, or “dial home” to a malicious attacker, allowing the attacker to conduct data theft and other activities. The Risk Alert advocates monitoring systems for malicious activity and suspicious services. See the Appendix to the Risk Alert:

- Using software to detect malicious code on Firm networks and mobile devices (Request 21, sub-bullet)
- Testing the reliability of event detection processes. If so, please identify the month and year of the most recent test (Request 21, sub-bullet)
- Malware was detected on one or more Firm devices. Please identify or describe the malware. (Request 24, sub-bullet)

Hosts Per Class C

Goal 1: Maintain accurate inventories

This component displays live hosts across /24 network blocks. The component can be modified to report across /16 or /8 network blocks. If more sophisticated Variable Length Subnet Mask (VLSM) network division is required, it is recommended to leverage the Hosts Per Asset List table and upload the network ranges required with appropriate labels.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates maintaining an inventory of physical devices and monitoring for the presence of unauthorized devices on the network. See the Appendix to the Risk Alert:

- Physical devices and systems within the Firm are inventoried. (Request 1, sub bullet)

IP Address	Total
192.168.1.0/24	75
10.100.0.0/24	114
10.0.25.0/24	37
10.0.20.0/24	37
10.0.0.0/24	96

Last Updated: 4 minutes ago

Category: Discovery and Detection
 Tags: Asset, Discovery, Hosts, Identify, Network, Subnet

Requirements: Active, Passive and Event Data

Related Resources

- Tracking Systems Not in DNS - Networks Report
- Inconsistent Hostnames and IP Addresses
- PCI Indicator Report

New Hosts (Last 5 Days)

IP Address

Last Updated: 58 minutes ago

Category: Discovery and Detection

Tags: 5 Days, Discovery, Hosts, Identify, Mac Address, New

Requirements: Passive Vulnerability and Event Data

Related Resources

Discovery Scan Report
Daily Host Alerts Report
Internet Explorer Zero Day Report

New Hosts (Last 5 Days)

Goal 1: Maintain accurate inventories

This component presents a table of new hosts discovered in the last 5 days. These hosts were discovered not with the Daily_Host_Alert event, but instead with the PVS New_Host_Alert and LCE New_MAC events. The New_MAC event records the first time a new MAC address is ever seen on the network; the New_Host_Alert event records the first time a new IP address is ever passively detected. These events are generated for any new host seen on the network, whereas the Daily_Host_Alert event is only generated for hosts in the “include-network” range. This table can be used to correlate discovered hosts with the Daily_Host_Alert events.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates maintaining an inventory of physical devices and monitoring for the presence of unauthorized devices on the network. See the Appendix to the Risk Alert:

- Physical devices and systems within the Firm are inventoried. (Request 1, sub-bullet)

Monitoring

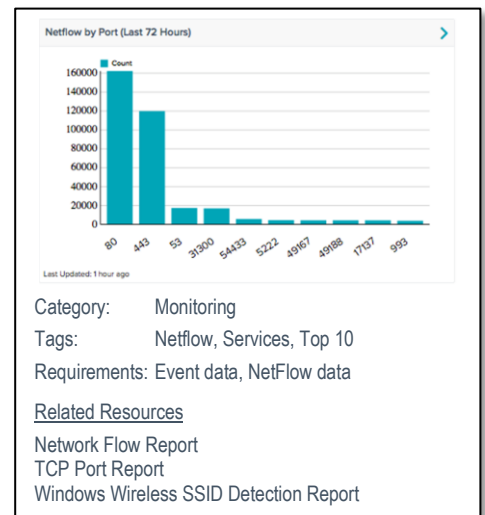
The Monitoring category provides intrusion monitoring, alerting, and analysis. This section is different from the “Discovery & Detection” section because it contains dashboards and components that are meant for deep log and trend analysis. Many of these components require additional software such as LCE Clients, or networking equipment such as IDS sensors.

NetFlow by Port (Last 72 Hours)

Goal 2: Maintain knowledge of normal operations

Goal 4: Prevent unauthorized activity

This chart displays the top 10 TCP ports with the highest session counts. This information can assist in understanding and monitoring the dataflows and services active on the network. Note that this component requires the Tenable NetFlow Monitor (TFM) LCE Client.



How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates maintaining knowledge of normal operations, as well as preventing unauthorized activity. The information displayed by this component can assist in identifying the top ports/services in use on the network and whether or not they are authorized. See the Appendix to the Risk Alert:

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated. (Request 1, sub-bullet)
- The Firm restricts users to those network resources necessary for their business functions. (Request 10, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm’s networks. (Request 21, sub-bullet)



Category: Monitoring
 Tags: 25 Days, Analysis, DLP, FISMA, Getting Started, Indicator, Network, PCI, PII, SANS, Top 10
 Requirements: Passive Vulnerability Data

Related Resources

DLP Indicator Component
 Top 10 Vulnerabilities Component
 Top Ten Systems Component

Data Leakage Monitoring Dashboard

Goal 6: Monitor for data loss

The Passive Vulnerability Scanner analyzes data in motion and can identify sensitive data such as credit card information, as well as general types of documentation sharing. This dashboard creates multiple tables to show observed shared data. The PVS identifies a wide variety of file sharing and data in motion activity, which can be used to highlight communications inbound to and outbound from a network. This dashboard was created entirely with the “Data Leakage (PVS)” plugin family filter. The PVS also generates real-time logs from data in motion that are collected by the Log Correlation Engine.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates preventing data leakage and loss. See the Appendix to the Risk Alert:

- The Firm maintains controls to secure removable and portable media against malware and data leakage. (Request 10, sub-bullet)
- Using data loss prevention software. The indicators in this component highlight data loss vulnerabilities and events, as well as highlighting other activities that have the potential for data leakage, in order to enable rapid detection of potential data loss so that it can be addressed. (Request 10, sub-bullet)

Event Trending By Type - Data Leak

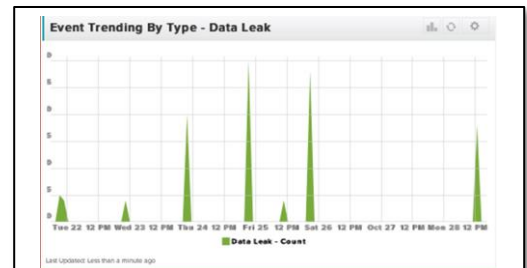
Goal 6: Monitor for data loss

This component displays a 7-day trend analysis of data leakage events. The LCE flags logs from the Passive Vulnerability Scanner or other Data Leak Prevention (DLP) products that indicate the presence of sensitive data, such as a credit card or Social Security numbers, as “data-leak” events. PVS must be specifically configured with DLP rules available from the Tenable Support Portal. Some of the included normalized events are described below.

- **PVS-Social_Security_Number_Client_Data_Leakage_Detected** – The Passive Vulnerability Scanner detected a Social Security number being leaked.
- **PVS-Credit_Card_Server_Data_Leakage_Detected** – The Passive Vulnerability Scanner detected a credit card number being leaked.
- **IntruShield-Sensitive_Content** – The Intrushield IPS has detected sensitive content.
- **Snort-Sensitive_Data** – A Snort sensor detected an event classified as Sensitive Data.
- **Snort-SDF_Combo_Alert** – A Snort sensor detected an event classified as SDF_COMBO_ALERT.
- **Sophos-Sensitive_Data** – A Sophos sensor detected an event classified as Sensitive Data.
- **Sophos-SDF_Combo_Alert** – A Sophos sensor detected an event classified as SDF_COMBO_ALERT.
- **McAfee DLP (iGuard)** – Several Alert Types

How This Applies to the SEC OCIE Risk Alert

The data-leakage event helps the firm identify leaked sensitive information through passive scanning and log analysis. The trending data also illustrates logging practices across the network. The Risk Alert advocates monitoring for data leakage. See the Appendix to the Risk Alert:



Category: Monitoring
 Tags: 7 Days, Analysis, Backdoor, DLP, Events, Enforcement, and Trending
 Requirements: Log Data and Passive Vulnerability Data

Related Resources

Event Trending By Type Dashboard
 PVS Detections Report - Traffic
 Elevated Privilege Failures Report

- Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance. (Request 1, sub-bullet)
- The Firm maintains controls to secure removable and portable media against malware and data leakage. If so, please briefly describe these controls. (Request 10, sub-bullet)
- Using data loss prevention software. (Request 21, sub-bullet)



File and Directory - Software Installed Events (Past 7 Days)

Goal 1: Maintain accurate inventories
Goal 4: Prevent unauthorized activity

This component graphs the last seven days of file and directory change events. The LCE “detected-change” event type automatically recognizes many types of system events that indicate change and creates secondary higher-level events. The Software_Installed normalized event reports when LCE encounters logs that indicate software has been installed. The raw logs indicate the system events Linux-DPKG_Software_Installed, OSX-Software_Installed, or Windows-Software_Installed that occurred along with time and host IP address. To see the detailed log events, the user must review the raw logs of the applicable type.

How This Applies to the SEC OCIE Risk Alert

The firm can monitor all software installation events regardless of the host operating system. As long as logs are sent to LCE, the normalization routines will create the Software_Installed event, thus

tracking the event, IP address, and date/time stamp. The Risk Alert advocates monitoring systems to maintain a software inventory. See the Appendix to the Risk Alert:

- Software platforms and applications within the firm are inventoried. (Request 1, sub-bullet)
- The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities. (Request 10, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm’s networks. (Request 21, sub-bullet)

Malicious Process Monitoring

Goal 5: Monitor for malicious activity

This component takes many of the various detection technologies for botnets, malicious file hashes, anomalous network traffic, spikes in system logs, and continuous scanning activity, and places them into one spot. Some of the plugins and normalized events used in the matrix are described below.

- **Malicious Process Detection (59275):** The MD5 hash of one or more running processes on the remote Windows host matches known malware.
- **Malicious Process Detection Potentially Unwanted Software (59641):** The MD5 hash of one or more running process on the remote Windows host matches software known to violate some corporate policies. Verify that the remote processes are authorized in your environment.
- **Linux Malicious Process Detection (71261):** The MD5 hash of one or more running processes on the remote Linux host matches known malware.
- **Mac OS X Malicious Process Detection (71263):** The MD5 hash of one or more running processes on the remote Mac OS X host matches known malware.
- **Multiple_System_Crashes:** The Log Correlation Engine has detected multiple system crash and restart events on the network. Large numbers of unexpected reboots and crashes could indicate a worm, hardware problems, or other important issues.



- **Statistics-Process_Large_Anomaly:** The LCE stats daemon has found a process execution type event spike. For all events of this type being sent to the LCE, the stats daemon has compared this hour's event rate for each unique targeted IP address to the same hour in each previous day for the entire body of collected data. Large changes in event rates can indicate new applications, new types of network usage, and in some cases, abuse.
- **Statistics-Virus_Large_Anomaly:** The LCE stats daemon has found a virus type event spike. For all events of this type being sent to the LCE, the stats daemon has compared this hour's event rate for each unique targeted IP address to the same hour in each previous day for the entire body of collected data. Large changes in event rates can indicate new applications, new types of network usage, and in some cases, abuse.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates monitoring the network for malicious activity. See the Appendix to the Risk Alert:

- Monitoring the Firm's network environment to detect potential cybersecurity events. (Request 21, sub bullet)
- Using software to detect malicious code on Firm networks and mobile devices. (Request 21, sub bullet)

Top Talkers By IP Address (Last 24 Hours)

IP Address	LCE	Count
192.168.1.104	192.168.1.104	38392
192.168.1.104	192.168.1.104	15611
192.168.1.104	192.168.1.104	13290
192.168.1.104	192.168.1.104	10257
192.168.1.104	192.168.1.104	9950

Last Updated: 8 hours ago

Category: Monitoring
 Tags: netFlow
 Requirements: Event Data

Related Resources
[NetFlow Dashboard](#)
[TCP Report](#)
[Passive Network Forensics Dashboard](#)

Netflow Top Talkers By IP Address (Last 24 Hours)

Goal 2: Maintain knowledge of normal operations

This component presents the analyst with a table of the Top 5 IP addresses talking on the network, along with a packet count for each over the last 24-hour reporting period.

How This Applies to the SEC OCIE Risk Alert

NetFlow is a feature found in many routers and firewalls that collects IP network traffic statistics as it enters or exits an interface. LCE provides the ability to analyze this data to monitor data flows and trending traffic patterns. The NetFlow data collection can provide details about port usage and NetFlow operations. The Risk Alert advocates monitoring systems to maintain a baseline for data flows and other communication trending. See the Appendix to the Risk Alert:

- Connections to the Firm's network from external sources are catalogued. (Request 1, sub bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm's networks. (Request 21, sub bullet)

PVS Network Trending - Cloud Data

Goal 2: Maintain knowledge of normal operations

LCE provides a trending view of the SSL traffic from clients to services that have been associated with a cloud file storage service. Traffic is identified in the following three methods:

- **Inbound** – Traffic from IP addresses considered external to your network, going to addresses that are internal to your network
- **Outbound** – Traffic from IP addresses considered internal to your network, going to addresses that are external to your network
- **Internal** – Traffic between IP addresses that are considered internal

PVS Network Trending - Cloud Data

Last Updated: 1 month ago

Category: Monitoring
 Tags: 5 Days, Analysis, Cloud, Network, Traffic, Trending, Inbound, Internal, Outbound
 Requirements: Log Data and Passive Data

Related Resources
[PVS Network Trending Dashboard](#)
[Threatlist Trending Dashboard](#)
[TCP Port Report](#)

How This Applies to the SEC OCIE Risk Alert

This component provides a historic view of the firm's use of Secure Sockets Layer (SSL) to access cloud file storage. The component also helps to track the direction of the data flow. Should a significant change in directional flow occur, this could mean a data exfiltration attack is underway. The Risk Alert advocates monitoring system data flows. See the Appendix to the Risk Alert:

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated. (Request 1, sub-bullet)
- Please indicate whether the Firm makes use of encryption. If so, what categories of data, communications, and devices are encrypted and under what circumstances? (Request 11)

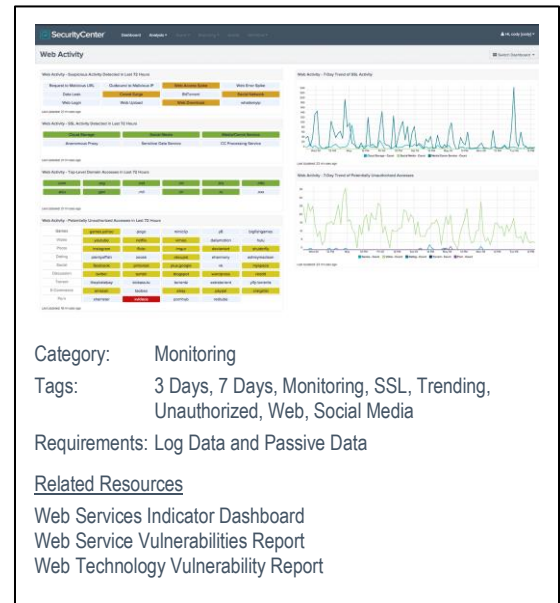
Web Activity

Goal 2: Maintain knowledge of normal operations

Goal 4: Prevent unauthorized activity

This dashboard presents web activity detected in the last 72 hours, with some 7-day trending. This dashboard can be used to monitor web accesses and look for suspicious or potentially unauthorized activity. Note that this dashboard relies on PVS detections being forwarded to the LCE. Make sure that the PVS is configured to send syslog messages to the LCE: in Configuration > PVS Settings > Syslog, include the LCE host (with port 514) in the Realtime Syslog Server List. The LCE listens for syslog messages by default. The dashboard collection contains the following components:

- **Web Activity - Suspicious Activity Detected in Last 72 Hours:** This matrix presents detections of potentially suspicious web activity that have occurred in the last 72 hours.
- **Web Activity - SSL Activity Detected in Last 72 Hours:** This matrix presents informational indicators of SSL events that have occurred in the last 72 hours, including access to cloud file storage, access to social media (such as Facebook or Twitter), access to media/communication services (such as Netflix or Skype), access to anonymous proxy services (which allow anonymous access to the Internet), access to services commonly used for sensitive data, and access to services used for processing credit card transactions.
- **Web Activity - Top-Level Domain Accesses in Last 72 Hours:** This matrix presents informational indicators of top-level domains of interest accessed in the last 72 hours. These indicators use the Domain_Summary, Domain_Failure_Summary, and SSL_Cert_Summary events, which all provide lists of domains accessed; searches are performed within these events to find specific domains of interest. Each summary event for a given IP address provides the domains accessed by that IP since the last such event for that IP (which may be as often as hourly). This component can be altered to add or remove domains of interest as needed. If failed attempts to access domains do not need to be tracked, remove the Domain_Failure_Summary event from the filter for these indicators. Note that the PVS-DNS_Top_Level_Domain_Queries event is not used here, as its output will not necessarily be limited to the last 72 hours.
- **Web Activity - Potentially Unauthorized Accesses in Last 72 Hours:** This matrix presents warning indicators of popular but potentially unauthorized domains of interest accessed in the last 72 hours. These indicators use the Domain_Summary, Domain_Failure_Summary, and SSL_Cert_Summary events, which all provide lists of domains accessed; searches are performed within these events to find specific domains of interest. Each summary event for a given IP address provides the domains accessed by that IP since the last such event for that IP (which may be as often as hourly). This component can be altered to add or remove domains of interest as needed. If failed attempts to access domains do not need to be tracked, remove the Domain_Failure_Summary event from the filter for these indicators.
- **Web Activity - 7-Day Trend of SSL Activity:** This chart presents a 7-day trend graph of various SSL events, including access to cloud file storage, access to social media (such as Facebook or Twitter), and access to media/communication services (such as Netflix or Skype).



- **Web Activity - 7-Day Trend of Potentially Unauthorized Accesses:** This chart presents a 7-day trend graph of accesses to popular but potentially unauthorized domains, including several games, video, dating, torrent, and porn sites. This chart uses the Domain_Summary, Domain_Failure_Summary, and SSL_Cert_Summary events, which all provide lists of domains accessed; searches are performed within these events to find specific domains of interest. Each summary event for a given IP address provides the domains accessed by that IP since the last such event for that IP (which may be as often as hourly). This component can be altered to add or remove domains of interest as needed. If failed attempts to access domains do not need to be tracked, remove the Domain_Failure_Summary event from the filter in each series.

How This Applies to the SEC OCIE Risk Alert

Web activity should be monitored closely. Suspicious activity may indicate policy violations, compromised systems, or the presence of a network attacker. This dashboard is designed specifically to assist in the monitoring of web activity, by tracking DNS requests and other web-related events, using both passive detection and log correlation. The Risk Alert advocates monitoring system data flows. See the Appendix to the Risk Alert:

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated. (Request 1, Sub-bullet)
- Aggregating and correlating event data from multiple sources. (Request 21, Sub-bullet)
- Monitoring the Firm’s network environment to detect potential cybersecurity events. (Request 21, Sub-bullet)

Security Industry Trends

The Security Industry Trends category contains components and dashboards that are influenced by trends, reports, and analysis from information security industry leaders. These dashboards and components may address current zero-day vulnerabilities, or highlight recommendations from industry leaders such as SANS.

CoCS 20 Critical Security Controls - Control 1 New Devices Detected

IP Address	NetBIOS	DNS
10.31.254.253		
10.31.104.146		
10.31.100.110		

Last Updated: 2 minutes ago

Category: Security Industry Trends

Tags: Asset, Compliance, Discovery, Hosts, New, SANS, Identify, and CSC

Requirements: Active Data, Passive, and Event Vulnerability Data

Related Resources

Council on CyberSecurity - Critical Security Controls Report
System Configuration Report
Systems Last Scanned (Date Ranges) Assets

CoCS 20 Critical Security Controls - Control 1 New Devices Detected

Goal 1: Maintain accurate inventories
Goal 4: Prevent unauthorized activity

This component identifies new hosts detected within the last 48 hours by LCE, PVS, or Nessus. One of the three detection methods is required for this component to function, and it provides additional functionality if all three are present.

To track when a host is first discovered, the component monitors all detection methods. These detection methods are plugins 19506 (Nessus Scan Information), 12 (PVS Host TTL Discovered), and 800000 (LCE Host Discovered). Within the plugin output, the Vulnerability Discovered field specifies when a vulnerability was first discovered; filtering on this field can be used to identify vulnerabilities discovered within a certain time frame. In this case, using the specified plugins and the Vulnerability Discovered field enables detection of new devices that have connected to the network within the last 48 hours.

How This Applies to the SEC OCIE Risk Alert

When identifying risk, an organization must first start with identifying the applicable assets. This component helps to list new assets discovered on the network by monitoring the active, passive, and event detection methods for identifying new assets. The Risk Alert advocates maintaining an inventory of physical devices and monitoring for the presence of unauthorized devices on the network. See the Appendix to the Risk Alert:

- Physical devices and systems within the Firm are inventoried (Request 1, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm’s networks (Request 21, sub-bullet)

CoCS 20 Critical Security Controls - Control 15 Controlled Access/Data Leakage

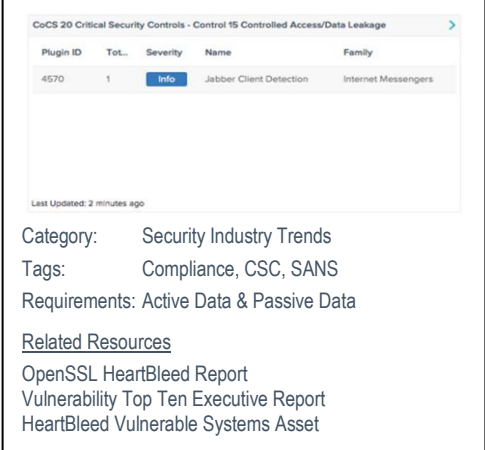
Goal 4: Prevent unauthorized activity

Goal 5: Monitor for malicious activity

Goal 6: Monitor for data loss

This component utilizes plugins from the PVS Data Leakage family as well as P2P file sharing, IRC, IM, FTP, and others to monitor for sensitive information on the wire. The description of the plugin families are:

- FTP – Checks that look for vulnerabilities in FTP servers. These include common issues and misconfigurations regardless of vendor, as well as vendor specific issues that have been publicly disclosed.
- Peer-To-Peer File Sharing – Checks that look for the presence of peer-to-peer file sharing software and associated vulnerabilities.
- Internet Messengers – Plugins that monitor for Instant Messenger software such as AIM, Yahoo Messenger, and Skype.
- IRC Clients – A set of plugins to detect traffic and vulnerabilities in IRC client software.
- Peer-To-Peer File Sharing – Checks that look for peer-to-peer traffic indicating file sharing activity.
- Data Leakage – Plugins that look for signs of confidential information traversing the network (e.g., Social Security numbers).
- IRC Servers – A set of plugins to detect traffic and vulnerabilities in IRC servers.



CoCS 20 Critical Security Controls - Control 15 Controlled Access/Data Leakage

Plugin ID	Tot..	Severity	Name	Family
4570	1	Info	Jabber Client Detection	Internet Messengers

Last Updated: 2 minutes ago

Category: Security Industry Trends

Tags: Compliance, CSC, SANS

Requirements: Active Data & Passive Data

Related Resources

- OpenSSL HeartBleed Report
- Vulnerability Top Ten Executive Report
- HeartBleed Vulnerable Systems Asset

How This Applies to the SEC OCIE Risk Alert

This component monitors several plugin families, all of which can be used to identify sources of unauthorized data flows such as FTP and IRC. These unauthorized sources can be used to compromise sensitive data and may impact business value. These methods are often used in the data leakage attacks and can help assess the accuracy of data leakage software. The Risk Alert advocates monitoring for data leakage. See the Appendix to the Risk Alert:

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated. (Request 1, sub-bullet)
- Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value. (Request 1, sub-bullet)
- The Firm maintains controls to secure removable and portable media against malware and data leakage. (Request 10, sub-bullet)
- Please indicate whether the Firm makes use of encryption. (Request 11)
- Using data loss prevention software. (Request 21, sub-bullet)

CoCS 20 Critical Security Controls - Control 17 - Data Protection

Goal 2: Maintain knowledge of normal operations

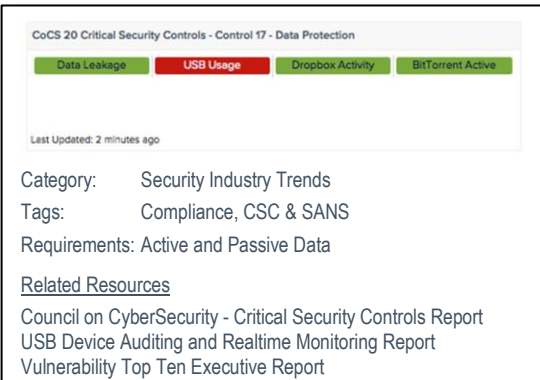
Goal 4: Prevent unauthorized activity

Goal 5: Monitor for malicious activity

Goal 6: Monitor for data loss

This component uses the passive plugins for data leakage, Dropbox detection, and BitTorrent protocol detection, as well as a plugin to enumerate USB usage on Windows systems for the last 7 days. The plugins used in this component are described below.

- **Plugin Family Data Leakage** – Plugins that look for signs of confidential information traversing the network (e.g., Social Security numbers).
- **Plugin 2576 (BitTorrent P2P Protocol Detection)** – The remote host is running the BitTorrent P2P protocol.



CoCS 20 Critical Security Controls - Control 17 - Data Protection

Data Leakage	USB Usage	Dropbox Activity	BitTorrent Active
Active	Active	Active	Active

Last Updated: 2 minutes ago

Category: Security Industry Trends

Tags: Compliance, CSC & SANS

Requirements: Active and Passive Data

Related Resources

- Council on CyberSecurity - Critical Security Controls Report
- USB Device Auditing and Realtime Monitoring Report
- Vulnerability Top Ten Executive Report

- **Plugin 4936 (Dropbox Software Detection (DNS))** – Dropbox is installed on the remote host. Dropbox is an application for storing and synchronizing files between computers, possibly outside the organization.
- **Plugin 35730 (Microsoft Windows USB Device Usage Report)** – By connecting to the remote host with the supplied credentials, this plugin enumerates USB devices that have been connected to the remote host in the past.

How This Applies to the SEC OCIE Risk Alert

This component provides indicators of data access using several potential unauthorized methods. BitTorrent and Dropbox can be easily misconfigured, allowing for data to be copied to several remote locations, resulting in data loss. When a firm deploys DLP software, this component will help monitor the USB drive activity. The Risk Alert advocates monitoring systems for malicious activity and suspicious services. See the Appendix to the Risk Alert:

- The Firm maintains controls to secure removable and portable media against malware and data leakage. If so, please briefly describe these controls. (Request 10, sub-bullet)
- The Firm’s information security policy and training address removable and mobile media. (Request 10, sub-bullet)
- The Firm maintains a written data destruction policy. (Request 10, sub-bullet)
- Using data loss prevention software. (Request 21, sub-bullet)
- An employee or other authorized user of the Firm’s network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive customer or Firm information, or damage to the Firm’s network or data. (Request 24, sub-bullet)

Malware Detection - Viewing the Invisible

Goal 3: Discover vulnerabilities and track remediation progress

Goal 5: Monitor for malicious activity

This component provides a series of indicators that provide security analysts with a notification of possible compromise, as discussed in the “Viewing the Invisible” posting on the Tenable Discussion Forums (<https://discussions.nessus.org/thread/7100>). Listed below is a detailed explanation of the indicators:

- **Vuln For IP** – This indicator looks for any vulnerability data related to IP addresses mentioned in the posting.
 - 46.4.69.25, 46.166.162.147, 69.60.98.203, 109.200.22.160-109.200.22.163, 176.74.178.45, 176.74.178.119-176.74.178.120, 176.74.178.202-176.74.178.203, 216.118.232.245
 - Please note you will need to edit the component to add the IP address filter.
 - Both the filter and the Condition text must be modified.
- **Event For IP** – This indicator looks for any event data related to IP addresses mentioned in the posting.
- **Self Signed** – The X.509 certificate chain is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL, as attackers could establish a man-in-the-middle attack against the remote host.
- **Revoked Certificate** – The remote server is using a certificate that has been revoked.
- **Expired Certificate** – The remote server has a certificate that has expired.
- **commonName Mismatch** – This service presents an SSL certificate for which the “commonName” (CN) does not match the hostname on which the service is listening.
- **Wrong Hostname** – The commonName (CN) of the SSL certificate presented on this service is for a different machine.
- **Cert Untrusted** – The server’s X.509 certificate does not have a signature from a known public certificate authority. This situation can occur in three different ways, each of which results in a break in the trust chain, below which certificates cannot be trusted.
 - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when

Malware Detection - Viewing the Invisible

Vuln For IP	Event For IP	Self Signed
Revoked Certificate	expired certificate	commonName Mismatch
Wrong Hostname	Cert Untrusted	Blacklisted
Malicious Process	Unmanarc RCS	Backdoors

Last Updated: 1 minute ago

Category: Security Industry Trends

Tags: Analysis, Botnet, Certificate, Detection, Events, Exploit, Indicator, Malicious, Threat, Virus, Vulnerabilities, Watchlist

Requirements: Active, Passive, and Event Data

Related Resources

Behind the Mask Dashboard
Insider Threats v2 Report
Unsupported Windows Software Startup Detection Report

intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.

- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's "notBefore" dates, or after one of the certificate's "notAfter" dates.
 - Third, the certificate chain may contain a signature that either didn't match the certificate's information, or could not be verified. Bad signatures can be fixed by having the certificate with the bad signature re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.
 - If the remote host is a public host in production, any break in the chain nullifies the use of SSL as attackers could establish a man-in-the-middle attack against the remote host.
- **Blacklisted** - The remote server uses an SSL certificate that is either fraudulent or was issued from a certificate authority that is considered to be untrustworthy.
 - **Malicious Process** - The MD5 hash of one or more running processes on the remote Windows, Linux, or Mac OS X host matches known malware. Verify that the remote processes are authorized in your environment.
 - **Unmanarc RCS** - This host appears to be running Unmanarc Remote Control Server (URCS). While it does have some legitimate uses, URCS may also have been installed silently as a backdoor, which may allow an intruder to gain remote access to files on the remote system. If this program was not installed for remote management, then it is likely that the remote host has been compromised. An attacker may use it to steal files, passwords, or redirect ports on the remote system to launch other attacks.
 - **Backdoors** - Plugins that detect high-profile backdoors, trojan horse programs, worm infections, and systems with signs of compromise.

How This Applies to the SEC OCIE Risk Alert

This component really focuses the attention towards possible certificate usage by malware. Some malware will use encryption to hide the data that is collected, but malware often uses invalid certificates. This matrix assists in monitoring these events and misconfigurations. The Risk Alert advocates monitoring systems for malicious activity and misconfigured encryption components. See the Appendix to the Risk Alert:

- Please indicate whether the Firm makes use of encryption. If so, what categories of data, communications, and devices are encrypted and under what circumstances? (Request 11)
- Using software to detect malicious code on Firm networks and mobile devices. (Request 21, sub-bullet)
- Using the analysis of events to improve the Firm's defensive measures and policies. (Request 21, sub-bullet)
- Malware was detected on one or more Firm devices. Please identify or describe the malware. (Request 24, sub-bullet)

SANS 6 - Category 2 - System and Data Changes

Goal 4: Prevent unauthorized activity

The focus of the SANS Top 6 Categories of Critical Log Information (<http://www.sans.edu/research/security-laboratory/article/sixtoplogcategories>) is on identifying the most critical log reports for a wide cross-section of the information security community. These are the top reports that should be reviewed on a regular basis, and that have the highest likelihood of identifying suspect activity.

This indicator matrix focuses on the Systems and Data Change Reports category (Category 2), and alerts on various system and critical security changes to devices and networked assets. Listed below are descriptions of some of the normalized events and plugin families used in the matrix:

- **User_Added**: The Log Correlation Engine has encountered a log that indicates that a user account has been added.

Users Added	Users Changed	Users Removed
New Users	New Services	File Change
Software Installed		

Last Updated: 4 minutes ago

Category: Security Industry Trends
Tags: Detection, SANS
Requirements: Passive Vulnerability Data and Event Logs

Related Resources
Group Management Events Report
File Integrity Events Over Time Component
Account Weakness - Suspicious Login Activity Component

- **User_Change:** The Log Correlation Engine has encountered a log that indicates a user account attribute has changed.
- **User_Removed:** The Log Correlation Engine has encountered a log that indicates that a user account has been removed or disabled.
- **New_User:** The Log Correlation Engine detected a new active user account on a monitored system.
- **LCE-Monitored_File_Modified:** The LCE Client has reported on a file that has had its checksum, owner, group, or permissions changed.
- **LCE-Monitored_File_Removed:** The LCE Client has reported on a file that has been removed.
- **LCE-Monitored_File_Re-added:** The LCE Client has reported on a file that had been removed, has now been re-added with no change to the file itself.
- **LCE-Monitored_File_Re-added_Changed:** The LCE Client has reported on a file that had been removed, has now been re-added with changes.
- **Port Scanners:** This plugin family contains the port scanning functionality of Nessus. By monitoring this family, the firm can detect services running on local clients.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates maintaining inventories of both physical devices and software, maintaining knowledge of normal operations, and preventing unauthorized activity. The indicators in this component highlight the presence of new hosts, new users, new software installed, and when a large spike in network changes is detected. See the Appendix to the Risk Alert:

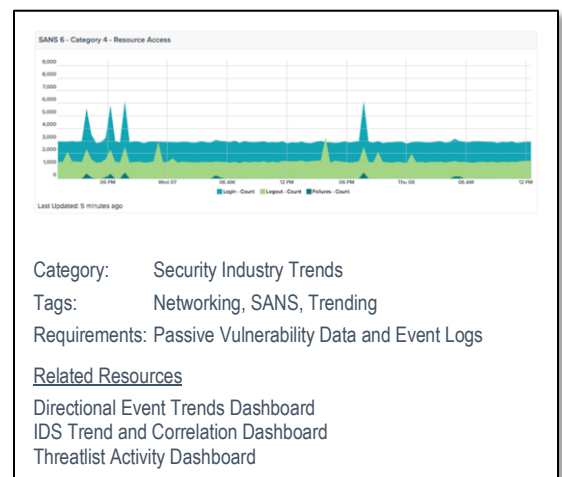
- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated. (Request 1, sub-bullet)
- The Firm maintains controls to prevent unauthorized escalation of user privileges and lateral movement among network resources. (Request 10, sub-bullet)
- The Firm restricts users to those network resources necessary for their business functions. (Request 10, sub-bullet)
- The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications. (Request 10, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm’s networks. (Request 21, sub-bullet)

SANS 6 - Category 3 - Network Activity

Goal 2: Maintain knowledge of normal operations

The focus of the SANS Top 6 Categories of Critical Log Information (<http://www.sans.edu/research/security-laboratory/article/sixtoplogcategories>) is on identifying the most critical log reports for a wide cross-section of the information security community. These are the top reports that should be reviewed on a regular basis, and that have the highest likelihood of identifying suspect activity.

This component focuses on the Network Activity Reports category (Category 3), and displays a 7-day trend analysis of network events. Observed application logs from the Passive Vulnerability Scanner as well as logs from the Tenable NetFlow Monitor (TFM) and the Tenable Network Monitor (TNM) are logged to this LCE event type. Event names are used to designate the collection type (PVS, TNM, or TFM) as well as session length and amount of bandwidth transferred. Real-time logs from the Passive Vulnerability Scanner, Sourcefire’s RNA, ArpWatch, and some other sources that indicate network changes are also logged. The PVS will log application sessions based on protocols such as SSH, SSL, VNC, RDP, and other applications.



How This Applies to the SEC OCIE Risk Alert

The trend graph shows the traffic inbound, outbound and internal. Inbound traffic is from IP addresses considered external to your network, going to addresses that are internal to your network. Outbound traffic flows from IP addresses considered internal to your network to addresses that are external to your network. Internal traffic is between IP addresses that are considered internal. The Risk Alert advocates maintaining an understanding of the data flow baseline and related traffic patterns. See the Appendix to the Risk Alert:

- Connections to the Firm's network from external sources are catalogued. (Request 1, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm's networks. (Request 21, sub-bullet)

Sensitive Data - Potential Sensitive Information Active Scanning

Goal 3: Discover vulnerabilities and track remediation progress

Goal 6: Monitor for data loss

This indicator-based component triggers when certain elements are found by an active Nessus scan. The indicators within the matrix identify several methods of copyrighted materials stored on computers or services that can be used to transfer sensitive information. The indicators in this component are described below.

- **Copyright (FTP)** – An FTP server is hosting potentially copyrighted media (MP3, WAV, AVI, or ASF files). Remove these files if this is not authorized usage.
- **Copyright (SMB)** – Potentially copyrighted media files (MP3, OGG, MPG, AVI, etc.) have been found on the remote SMB shares. Remove these files if this is not authorized usage.
- **Copyright (HTTP)** – A web server is hosting potentially copyrighted media (MP3, WAV, AVI, or ASF files). Remove these files if this is not authorized usage.
- **Office Files (SMB)** – Office-related files (DOC, PPT, XLS, PDF, etc.) were discovered on remote SMB shares. Ensure that these files have proper access controls set on them.
- **Office Files (HTTP)** – A web server is hosting office-related files (DOC, PPT, XLS, PDF, etc.). Ensure that these files do not contain sensitive information and that they have proper access controls set on them.
- **SMB Shares** – Network shares were discovered.
- **USB Drives** – USB drives have been connected to network hosts. Ensure that this is acceptable.
- **NFS Exports** – Network File System (NFS) shares are exported. Ensure that this is intended.
- **P2P Sharing** – Peer-to-peer file sharing software and associated vulnerabilities were discovered.
- **Databases** – Vulnerabilities were discovered in database software (IBM DB2, Microsoft SQL Server, MySQL, Oracle, PostgreSQL, etc.).

Sensitive Data - Potential Sensitive Information Active Scanning

Copyright (FTP)	Copyright (SMB)	Copyright (HTTP)	Office Files (SMB)
Office Files (HTTP)	SMB Shares	USB Drives	NFS Exports
P2P Sharing	Databases		

Last updated 1 minute ago

Category: Threat Detection & Vulnerability Assessments

Tags: File, PCI

Requirements: Active Scan Data

[Related Resources](#)

- Web Server Database Plugin Family Dashboards
- Council on CyberSecurity - Critical Security Controls Report
- SANS Top 20 Critical Controls Report

How This Applies to the SEC OCIE Risk Alert

This component can help to address many items a firm should consider as a part of its information security and risk management programs. These indicators provide an indication of the compromise or misuse of data at rest, and can help identify the location of sensitive assets, such as shared drives, unencrypted file services, and databases, and focus initial hardening efforts. The Risk Alert advocates monitoring systems for data storage integrity and confidentiality. See the Appendix to the Risk Alert:

- Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value. (Request 1, sub-bullet)
- The Firm's information security policy and training address removable and mobile media. (Request 10, sub-bullet)
- The Firm maintains controls to secure removable and portable media against malware and data leakage. If so, please briefly describe these controls. (Request 10, sub-bullet)
- The Firm maintains a written data destruction policy. (Request 10, sub-bullet)
- The Firm periodically tests the functionality of its backup system. If so, please provide the month and year in which the backup system was most recently tested. (Request 10, sub-bullet)

- Please indicate whether the Firm makes use of encryption. If so, what categories of data, communications, and devices are encrypted and under what circumstances? (Request 11, sub-bullet)
- Any software or other practice employed for detecting anomalous transaction requests that may be the result of compromised customer account access. (Request 13d)
- Identifying and assigning specific responsibilities, by job function, for detecting and reporting suspected unauthorized activity. (Request 21, sub-bullet)
- Monitoring the Firm's network environment to detect potential cybersecurity events. (Request 21, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm's networks. (Request 21, sub-bullet)

Threat Detection & Vulnerability Assessments

The Threat Detection & Vulnerability Assessments category contains components and dashboards that aid with identifying vulnerabilities and potential threats. The content in this category is based on the identification of vulnerabilities and the associated risk. Many filters used are focused on the plugin names, groups, and/or severity to illustrate the risk posed by vulnerabilities.

Vulnerability Top Ten - Top 10 Remediations

Goal 3: Discover vulnerabilities and track remediation progress

This table displays the top 10 remediations for the network. For each remediation, the risk reduction for the network if the remediation is implemented is shown, along with the number of hosts affected. The list is sorted so that the highest risk reduction is at the top of the list. Implementing the remediations will decrease the vulnerability of the network.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates regular system maintenance and timely installation of patches, as well as periodic risk assessments. The information displayed by this component can assist in prioritizing remediations and addressing cybersecurity vulnerabilities. See the Appendix to the Risk Alert:

Solution	Risk Red...	Hosts...
Update to JDK / JRE 7 Update 45, 6 Update 65, or 6 Update 55 or later and, if necess...	1.88%	17
Update to JDK / JRE 7 Update 45, 6 Update 65, or 6 Update 55 or later and, if necess...	1.48%	15
Microsoft has released a set of patches for Visual Studio .NET 2003, 2005, and 2008. ...	0.83%	55
Upgrade to PuTTY version 0.63 or later.	0.53%	112
Microsoft has released a set of patches for XP, 2003, Vista, 2008, 7, 2008 R2, 8, 2012...	0.46%	13
Update the affected packages : RHEL 6 : kernel (RHSA-2013-1801)	0.42%	3
Upgrade to Firefox ESR 24.2 or later.	0.34%	11
Microsoft has released a set of patches for Microsoft Office 2003, 2007, and 2010. Off...	0.34%	23
Update the affected openssl packages.	0.32%	73
Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, 2008 R...	0.30%	22

Last Updated: 15 hours ago

Category: Threat Detection & Vulnerability Assessments
 Tags: Remediation, Top 10, Vulnerabilities
 Requirements: Active and Passive Vulnerability Data

Related Resources
 Windows Vulnerability Summary Report
 Exploitable Vulnerabilities Summary Report
 Critical and Exploitable Vulnerabilities Report

- Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value. (Request 1, sub-bullet)
- Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. (Request 3)
- The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities. (Request 10, sub-bullet)

Plugin ID	Name	Severity	Host Total
48831	IPMI Cntrlr Suite Zero Authentication Bypass	Critical	17
70472	Oracle Java SE Multiple Vulnerabilities (October 2013 CPU)	Critical	15
66932	Oracle Java SE Multiple Vulnerabilities (June 2013 CPU)	Critical	7
45544	Oracle Java JDK / JRE 6 < Update 20 Multiple Vulnerabilities	Critical	1
52002	Oracle Java SE Multiple Vulnerabilities (February 2011 CPU)	Critical	1
56566	Oracle Java SE Multiple Vulnerabilities (Oct 2011 CPU)	Critical	1
57959	Oracle Java SE Multiple Vulnerabilities (Feb 2012 CPU)	Critical	1
59462	Oracle Java SE Multiple Vulnerabilities (June 2012 CPU)	Critical	1
62593	Oracle Java SE Multiple Vulnerabilities (October 2012 CPU)	Critical	1
64454	Oracle Java SE Multiple Vulnerabilities (February 2013 CPU)	Critical	1

Last Updated: 15 hours ago

Category: Threat Detection & Vulnerability Assessments
 Tags: Exploit, Getting Started, Top 10, Vulnerabilities
 Requirements: Active and Passive Vulnerability Data

Related Resources
 Remediation Instructions Report by Vulnerability Report
 Vulnerabilities Over 30 Days Report
 HTTP Server Vulnerabilities Report

Vulnerability Top Ten - Top 10 Exploitable Vulnerabilities

Goal 3: Discover vulnerabilities and track remediation progress

This table displays the top 10 exploitable vulnerabilities on the network. The list is sorted so that the most critical vulnerability is at the top of the list. For each vulnerability, the severity and the number of hosts affected is shown.

How This Applies to the SEC OCIE Risk Alert

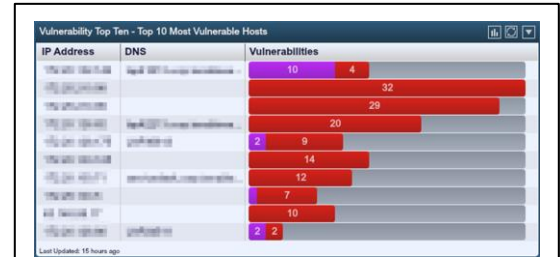
The Risk Alert advocates regular system maintenance and timely installation of patches, as well as periodic risk assessments. The information displayed by this component can assist in prioritizing remediations and addressing cybersecurity vulnerabilities. See the Appendix to the Risk Alert:

- Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value. (Request 1, sub-bullet)
- Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. (Request 3)
- The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities. (Request 10, sub-bullet)

Vulnerability Top Ten - Top 10 Most Vulnerable Hosts

Goal 3: Discover vulnerabilities and track remediation progress

This table displays the 10 hosts on the network that have the greatest number of exploitable critical and high severity vulnerabilities. The list is sorted so that the most vulnerable host is at the top of the list. For each host, a bar graph of its critical and high severity vulnerabilities is shown.



Category: Threat Detection & Vulnerability Assessments

Tags: Exploit, Top 10, and Vulnerabilities

Requirements: Active and Passive Vulnerability Data

Related Resources

Chrome, Firefox, Opera and Safari (PVS) Report

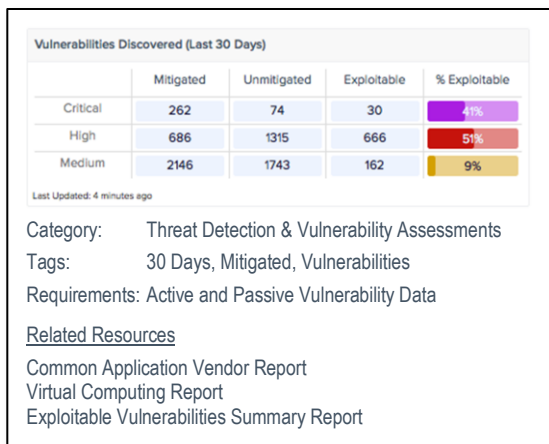
Media Player Vulnerability Report

Exploits by Platform Report

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates regular system maintenance and timely installation of patches, as well as periodic risk assessments. The information displayed by this component can assist in prioritizing remediations and addressing cybersecurity vulnerabilities. See the Appendix to the Risk Alert:

- Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value. (Request 1, sub-bullet)
- Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. (Request 3)
- The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities. (Request 10, sub-bullet)



Category: Threat Detection & Vulnerability Assessments

Tags: 30 Days, Mitigated, Vulnerabilities

Requirements: Active and Passive Vulnerability Data

Related Resources

Common Application Vendor Report

Virtual Computing Report

Exploitable Vulnerabilities Summary Report

Vulnerabilities Discovered (Last 30 Days)

Goal 3: Discover vulnerabilities and track remediation progress

This component displays vulnerability tracking information for the last 30 days. Information on Critical, High, and Medium severity vulnerabilities discovered in the past 30 days is presented, including the number of vulnerabilities that have been mitigated, number of vulnerabilities still unmitigated, number of unmitigated vulnerabilities that are exploitable, and the percentage of unmitigated vulnerabilities that are exploitable.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates regular system maintenance and timely installation of patches. The information displayed by this component can assist in assessing how well cybersecurity vulnerabilities are being addressed. The numbers in the exploitable vulnerabilities column especially should be kept very low. See the Appendix to the Risk Alert:

- The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities. (Request 10, sub-bullet)

Top 100 Users Generating Events (Last 72 Hours)

Goal 2: Maintain knowledge of normal operations

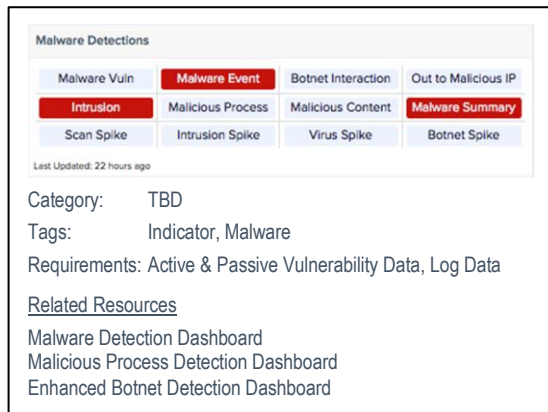
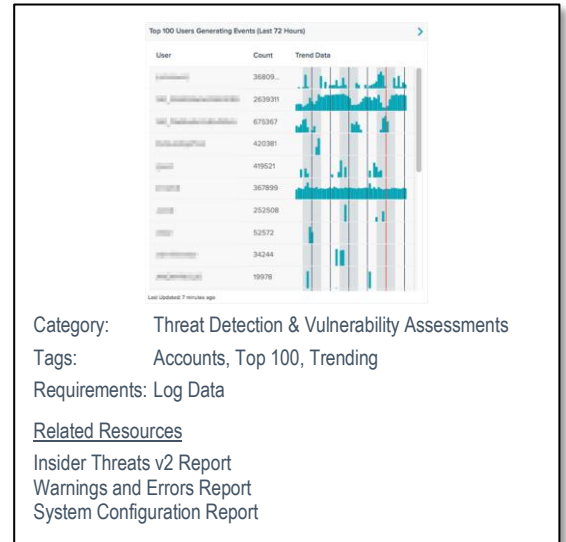
Goal 4: Prevent unauthorized activity

This table displays the top 100 users generating events on the network, with trending. This information can assist in monitoring the users accessing the network.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates maintaining knowledge of normal operations, as well as preventing unauthorized activity. The information displayed by this component can assist in identifying who the top users on the network are and whether or not they are authorized. See the Appendix to the Risk Alert:

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated (Request 1, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm's networks (Request 21, sub-bullet)
- The Firm's network was breached by an unauthorized user (Request 24, sub-bullet)



Malware Detections

Goal 5: Monitor for malicious activity

This matrix displays various indications of malware and malicious cybersecurity events on the network. Red indicators signify that activity of high severity has occurred. The indicators in this component are described below.

- **Malware Vuln** – Indications of system compromise have been actively and passively detected, and backdoors for persistent intruder access may have been established.
- **Malware Event** – In the last 72 hours, log events indicating the presence of a virus were detected.
- **Botnet Interaction** – A network host has been determined either to be part of a botnet, or to be communicating with a botnet.
- **Out to Malicious IP** – In the last 72 hours, a network host sent outbound traffic to an IP address known to be malicious.
- **Intrusion** – In the last 72 hours, log events indicating a potential intrusion were detected.
- **Malicious Process** – The MD5 hash of one or more processes running on a network host matches known malware.
- **Malicious Content** – A web server hosting malicious content was detected.
- **Malware Summary** – Malware events observed on hosts have been summarized. If this indicator is highlighted, then malware events have occurred.
- **Scan Spike** – A spike in events related to network scanning activity has occurred.
- **Intrusion Spike** – A spike in events related to network intrusion activity has occurred.
- **Virus Spike** – A spike in virus events has occurred.
- **Botnet Spike** – A spike in events related to botnet activity has occurred.

How This Applies to the SEC OCIE Risk Alert

The indicators in this component highlight various malware vulnerabilities (including botnet interaction, malicious processes, and web hosting of malicious content) and malware events (including virus and intrusion events, and large spikes in the number of such events) in order to enable rapid detection of malicious activity so that it can be addressed. The Risk Alert advocates monitoring for cybersecurity events and malware. See the Appendix to the Risk Alert:

- Monitoring the Firm's network environment to detect potential cybersecurity events. (Request 21, sub-bullet)
- Using software to detect malicious code on Firm networks and mobile devices. (Request 21, sub-bullet)

Network Changes

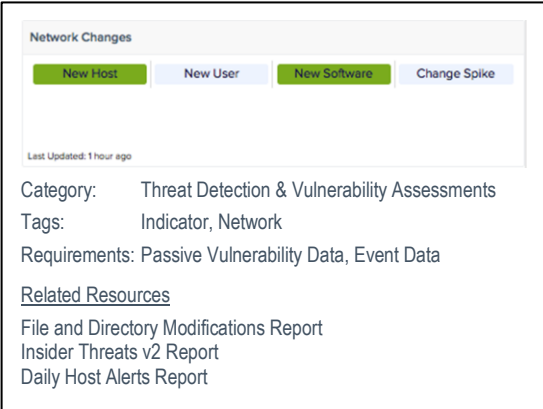
Goal 1: Maintain accurate inventories

Goal 2: Maintain knowledge of normal operations

Goal 4: Prevent unauthorized activity

This matrix displays various indications of network changes over the last 72 hours. Green indicators signify that a change has occurred, and further investigation may be warranted to determine if the change was authorized. The normalized events used in this component are described below.

- **PVS-New_Host_Alert:** The Passive Vulnerability Scanner detected a new host.
- **New_MAC:** The Log Correlation Engine detected an Ethernet address it has not seen before.
- **New_User:** The Log Correlation Engine detected a new active user account on a monitored system.
- **Software_Installed:** The Log Correlation Engine has encountered a log that indicates that software has been installed.
- **Statistics-Detected_Change_Large_Anomaly:** The LCE stats daemon has found a “detected-change” type event spike. For all events of this type being sent to the LCE, the stats daemon has compared this hour’s event rate for each unique targeted IP address to the same hour in each previous day for the entire body of collected data. Large changes in event rates can indicate new applications, new types of network usage, and in some cases, abuse.



Network Changes

New Host New User New Software Change Spike

Last Updated: 1 hour ago

Category: Threat Detection & Vulnerability Assessments

Tags: Indicator, Network

Requirements: Passive Vulnerability Data, Event Data

Related Resources

File and Directory Modifications Report

Insider Threats v2 Report

Daily Host Alerts Report

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates maintaining inventories of both physical devices and software, maintaining knowledge of normal operations, and preventing unauthorized activity. The indicators in this component highlight the presence of new hosts, new users, new software installed, and when a large spike in network changes is detected. See the Appendix to the Risk Alert:

- Physical devices and systems within the Firm are inventoried (Request 1, sub-bullet)
- Software platforms and applications within the Firm are inventoried (Request 1, sub-bullet)
- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated (Request 1, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm’s networks (Request 21, sub-bullet)

Potential Suspicious Activity


Goal 2: Maintain knowledge of normal operations

Goal 4: Prevent unauthorized activity

Goal 5: Monitor for malicious activity

This matrix displays various indications of network activity over the last 72 hours that departs from the baseline or may otherwise be suspicious. Spikes in event rates can indicate new applications, new types of network usage, and in some cases, abuse. Green indicators signify that the activity has occurred, and further investigation may be warranted to determine if the activity is authorized. Some of the normalized events used in this component are described below.

- **Statistics-Connection_Large_Anomaly:** The LCE stats daemon has found a “connection” type event spike. For all events of this type being sent to the LCE, the stats daemon has compared this hour’s event rate for each unique targeted IP address to the same hour in each previous day for the entire body of collected data. Large changes in event rates can indicate new applications, new types of network usage, and in some cases, abuse.
- **Statistics-Connection_Reception_Large_Anomaly:** The LCE has detected an anomaly in the amount of connections that a host on the network has received. This anomaly was large and indicates a very significant change in the behavior of how the system is being accessed by other computers.



Potential Suspicious Activity

Connect Spike Access Spike Network Spike Process Spike

Long-Term Crowd Surge Long TCP Large Xfr TCP

Last Updated: 20 hours ago

Category: Threat Detection & Vulnerability Assessments

Tags: Anomalies, Indicator, Network

Requirements: Event Data

Related Resources

Council on CyberSecurity - Critical Security Controls Report

Snort Events - Past 7 Days Report

Suspicious Proxies, Relays and SPAM Component

- **Statistics-Web_Access_Large_Anomaly:** The LCE stats daemon has found a “web-access” type event spike. For all events of this type being sent to the LCE, the stats daemon has compared this hour’s event rate for each unique targeted IP address to the same hour in each previous day for the entire body of collected data. Large changes in event rates can indicate new applications, new types of network usage, and in some cases, abuse.
- **Statistics-File_Access_Large_Anomaly:** The LCE stats daemon has found a “file-access” type event spike. For all events of this type being sent to the LCE, the stats daemon has compared this hour’s event rate for each unique targeted IP address to the same hour in each previous day for the entire body of collected data. Large changes in event rates can indicate new applications, new types of network usage, and in some cases, abuse.
- **Crowd_Surge:** The Log Correlation Engine detected a large number of unique local hosts visiting the same remote server.
- **Statistics-Process_Large_Anomaly:** The LCE stats daemon has found a “process” type event spike. For all events of this type being sent to the LCE the stats daemon has compared this hour’s event rate for each unique targeted IP address to the same hour in each previous day for the entire body of collected data. Large changes in event rates can indicate new applications, new types of network usage, and in some cases, abuse.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates maintaining knowledge of normal operations, preventing unauthorized activity, and monitoring for cybersecurity events and malware. The indicators in this component highlight various suspicious activities that might indicate unauthorized or malicious activity, including large spikes in activity, long-term activity, crowd surges, long (more than 47 hours) TCP sessions, and large (more than 1GB) TCP transfers. See the Appendix to the Risk Alert:

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated (Request 1, sub-bullet)
- Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm’s networks (Request 21, sub-bullet)
- Maintaining baseline information about expected events on the Firm’s network (Request 21, sub-bullet)

Potential Data Loss

Goal 6: Monitor for data loss

This matrix displays various indications of potential for data leakage and loss. Red indicators signify that activity of high severity has occurred. Green indicators signify that activity that has the potential for data loss has occurred and further investigation may be warranted. Some of the plugins and normalized events used in the matrix are described below.

- **WMI USB Drives Enumeration (24274):** By connecting to the remote host with the supplied credentials, it is possible to extract the list of USB drives of the remote host and the drive name attached to each.
- **Microsoft Windows USB Device Usage Report (35730):** By connecting to the remote host with the supplied credentials, this plugin enumerates USB devices that have been connected to the remote host in the past.
- **USB Statistics (800032):** USB Event Statistics
- **PVS-SSL_Session_Cloud_Data:** The PVS has logged an SSL session initiated from a client to a service and has identified the name of the SSL certificate in use. This particular type of SSL certificate is associated with a cloud file storage service.
- **PVS-Email_Attachment_Detection:** The Passive Vulnerability Scanner has detected an email attachment.
- **FTP:** This plugin family contains checks that look for vulnerabilities in FTP servers. These include common issues and misconfigurations regardless of vendor, as well as vendor specific issues that have been publicly disclosed.
- **Peer-To-Peer File Sharing:** This plugin family contains checks that look for peer-to-peer traffic indicating file-sharing activity.
- **Data Leakage:** This plugin family contains plugins that look for signs of confidential information traversing the network (e.g., Social Security numbers).
- **Internet Messengers:** This plugin family contains plugins that monitor for Instant Messenger software such as AIM, Yahoo Messenger, and Skype.

The screenshot shows a dashboard titled "Potential Data Loss". At the top, there are three buttons: "Data Loss Vuln" (red), "Data Loss Event" (light blue), and "USB Usage" (green). Below these are three more buttons: "Internet Messaging" (green), "Cloud Storage" (green), and "E-mail Attachment" (green). Underneath the buttons, it says "Last Updated: 45 minutes ago". Below that, there are fields for "Category: TBD", "Tags: DLP, Indicator", and "Requirements: Active & Passive Vulnerability Data, Event Data". At the bottom, there is a section for "Related Resources" with links to "USB Device Auditing and Realtime Monitoring Report", "OpenSSL HeartBleed Report", and "Vulnerability Top Ten Executive Report".

- **IRC Clients:** This plugin family contains a set of plugins to detect traffic and vulnerabilities in IRC client software.
- **IRC Servers:** This plugin family contains a set of plugins to detect traffic and vulnerabilities in IRC servers.

How This Applies to the SEC OCIE Risk Alert

The indicators in this component highlight data loss vulnerabilities and events, as well as highlighting other activities that have the potential for data leakage, in order to enable rapid detection of potential data loss so that it can be addressed. The Risk Alert advocates preventing data leakage and loss. See the Appendix to the Risk Alert:

- The Firm maintains controls to secure removable and portable media against malware and data leakage (Request 10, sub-bullet)
- Using data loss prevention software (Request 21, sub-bullet)

CVE Analysis / CVE Trending by Year Dashboards

Goal 3: Discover vulnerabilities and track remediation progress

These dashboards trend outstanding CVEs and recently mitigated issues in a variety of tables and trend lines. Common Vulnerabilities and Exposures (CVE®) is a dictionary of publicly known information security vulnerabilities and exposures. The CVE common identifiers provide a baseline for evaluating coverage of tool and services, while facilitating the exchange of data between security products. CVE common names provide a common approach to identifying a vulnerability or exposure, using a standard name for each. Using a standardized approach to describing a vulnerability or exposure allows for consistent approach to measure the firm risk exposure. Another key benefit to CVE is using a common method for evaluation of tools and databases. The dashboard collections contain the following components:



- **CVE Mitigated Within Last 30 Days** – This component displays a bar chart of recently mitigated CVE vulnerabilities, by severity, for the CVE ID years 2010 to 2014.
- **CVE Trending by Severity** – This component shows a 90 day analysis of vulnerabilities discovered by severity. Each trend line is assigned to a severity, and tracks the total CVE IDs for the last 5 years.
- **CVE Trending by Year** – This component shows a 90 day analysis of vulnerabilities discovered. Each trend line is assigned to a year (2010-2014) and tracks the total CVE IDs for the respective year.
- **Outstanding CVE Breakdown** – This component displays a breakdown of present CVE vulnerabilities by severity for the CVE ID years 2010 to 2014.
- **Outstanding CVE Totals By Year** – This component shows the total CVE ID count for each severity level for the years displayed. Also presented is a column that displays if any exploitable vulnerabilities exist for any CVE ID for the years displayed.
- **Top 10 CVE Issues for Year** – The top ten CVE issues for the specified year. The summary table is sorted by CVE ID and displays the CVE, total matches, and severity.

How This Applies to the SEC OCIE Risk Alert

When performing risk and vulnerability assessments, a firm must have a sustainable method of identifying vulnerabilities and flaws found in information systems. CVE has become the standard method of identification for software and application vulnerabilities. These dashboards aid the firm in identifying vulnerabilities and their severity. These dashboards also allow for the firm to track software patches and show evidence of vulnerability scanning over time. The Risk Alert advocates monitoring systems for vulnerabilities and exposures. See the Appendix to the Risk Alert:

- Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. (Request 3)
- Please describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated. (Request 3.b)
- The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities. (Request 10, sub-bullet)
- Conducting penetration tests and vulnerability scans. (Request 21, sub-bullet)

Event Vulnerabilities - Exploitable and Malware

	Total	Total %	Exploitable	Malware
Vulnerabilities	89	0%	27	0
Check	0	0%	0	0
Overflow	37	0%	0	0
DoS	46	0%	0	0
Statistics	1922	98%	0	0
Injection	3	0%	0	0
Detection	347	17%	0	0
Disclosure	22	0%	0	0
Execution	30	0%	0	0
Physics	2	0%	0	0

Category: Threat Detection & Vulnerability Assessments

Tags: Events, Exploit, Indicator, Malware, and Vulnerabilities

Requirements: Event Data

Related Resources

Apache Vulnerability Report
WSUS Monitoring Report
Exploits by Platform Report

Event Vulnerabilities - Exploitable and Malware

Goal 3: Discover vulnerabilities and track remediation progress

This component displays a matrix of various event vulnerability indicators and the risk posed by those events. Each row in the matrix is focused on the top 10 most common event vulnerability keywords. The matrix contains columns for the total number of vulnerabilities, the percentage of vulnerabilities, which have the keyword, and the number of vulnerabilities that are exploitable or exploitable by malware. The color schemes used to communicate potential risk to users are: black text on green is informational and indicates items that may be normal but should be reviewed; black text on orange indicates an item that must be reviewed, but could be a false positive; white text on red indicates a high severity item that should be addressed as soon as possible; and white text on purple indicates a critical severity item that must be addressed immediately.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates monitoring for cybersecurity events and malware. See the Appendix to the Risk Alert:

- The Firm maintains controls to secure removable and portable media against malware and data leakage. (Request 10, sub-bullet)
- Using software to detect malicious code on Firm networks and mobile devices. (Request 21, sub-bullet)
- Evaluating remotely-initiated requests for transfers of customer assets to identify anomalous and potentially fraudulent requests. (Request 21, sub-bullet)

Event Vulnerability Indicators Dashboard

Goal 4: Prevent unauthorized activity

Goal 5: Monitor for malicious activity

This dashboard contains a series of components that provide an easy way to view vulnerabilities identified by the Log Correlation Engine (LCE). By using different color schemes, the user is able to identify quickly which vulnerabilities pose more risk than others. The Log Correlation Engine (LCE) examines log event data to find vulnerabilities. The Tenable Event Vulnerabilities plugins that report this information are in the ID range of 800000 - 899999. This collection of components provides a very inclusive set of the indicator style components that provide a detailed view into the vulnerabilities identified by LCE.

How This Applies to the SEC OCIE Risk Alert

The Risk Alert advocates monitoring for cybersecurity events and malware. See the Appendix to the Risk Alert:

- The Firm maintains controls to secure removable and portable media against malware and data leakage. (Request 10, sub-bullet)
- Using software to detect malicious code on Firm networks and mobile devices. (Request 21, sub-bullet)
- Evaluating remotely-initiated requests for transfers of customer assets to identify anomalous and potentially fraudulent requests. (Request 21, sub-bullet)

Category: Threat Detection and Vulnerability Assessments

Tags: Browser, Database, Detection, Events, Exploit, Indicator, Malicious, OS, Statistics, Threat, Vulnerabilities, Web

Requirements: Event Data

Related Resources

Social Network Activity Executive Report
Malware Indicators Report
Council on CyberSecurity - Critical Security Controls Report

Malicious URL

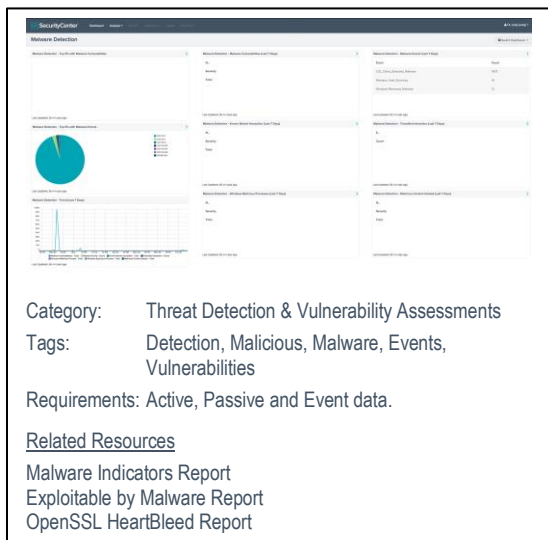
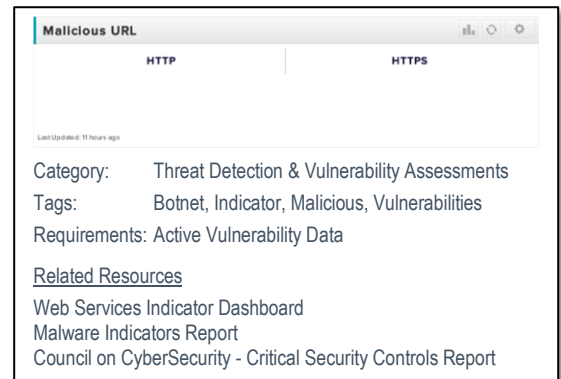
Goal 5: Monitor for malicious activity

This component has two indicators: one for HTTP and one for HTTPS. The indicators use plugin 52670, Web Site Links to Malicious Content. If the web site contains links that are listed in public malware databases as being malicious, the indicator will turn red. This might happen when either a user of the web site creates a link (e.g., comments added to a blog post) or the site has been compromised.

How This Applies to the SEC OCIE Risk Alert

This component provides an indication of a comprised web site in a user forum or a malicious URL injected into the website code. The Risk Alert advocates monitoring for malicious activity. See the Appendix to the Risk Alert:

- Using software to detect malicious code on Firm networks and mobile devices. (Request 21, sub-bullet)
- Access to a Firm web site or network resource was blocked or impaired by a denial of service attack. Please identify the service affected, and the nature and length of the impairment. (Request 24, sub-bullet)
- The availability of a critical Firm web or network resource was impaired by a software or hardware malfunction. Please identify the service affected, the nature and length of the impairment, and the cause. (Request 24, sub-bullet)
- The Firm was the subject of an extortion attempt by an individual or group threatening to impair access to or damage the Firm's data, devices, network, or web services. (Request 24, sub-bullet)



Malware Detection Dashboard

Goal 2: Maintain knowledge of normal operations

Goal 3: Discover vulnerabilities and track remediation progress

Goal 5: Monitor for malicious activity

This dashboard displays information that can be useful for detecting malware on the network. It makes use of vulnerability data from Nessus scans, PVS detections, and event data from the LCE. For related CSV reports, see the Malware Detection CSV Reports (<https://discussions.nessus.org/docs/DOC-1049>) and More Malware Detection CSV Reports (<https://discussions.nessus.org/docs/DOC-1056>) postings on the Tenable Discussions Forum.

The dashboard collection contains multiple components to identify malware and suspicious activity in the last 7 days. The top IP addresses with malware vulnerabilities detected by Nessus and the PVS are presented, as well as the top IP addresses with malware events reported by various applications and collected by the LCE.

How This Applies to the SEC OCIE Risk Alert

This dashboard provides logging for several events related to malware detection, and reports on the data collected via active scanning for systems within the firm. The most common indicators of compromise should be reviewed on daily basis. Firms with good scanning practices will benefit most from a dashboard such as this one.

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated. (Request 1, sub-bullet)
- Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance. (Request 1, sub-bullet)
- Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. (Request 3)
- Malware was detected on one or more Firm devices. Please identify or describe the malware. (Request 24, sub-bullet)

PVS Trust Dashboard

Goal 2: Maintain knowledge of normal operations

Goal 5: Monitor for malicious activity

This dashboard presents trust relationships between clients and servers that have been passively gathered via PVS plugins 3 and 15. These plugins collect data on internal client trusted connections and internal server trusted connections. Results are sorted by TCP port and displayed in a series of matrix indicators within the individual components. Viewing the plugin output provides insight into devices that are establishing trusted connections to each other. The dashboard is comprised of four components, that use plugin 3 (Internal client trusted connection) and 15 (Internal server trusted connection) to evaluate trust relationships. The dashboard collection contains the following components:

- **Clients Connecting To Servers Over Command/Control Ports:** This client matrix component collects data on internal trusted client connections. Results are sorted by TCP port and displayed in a series of matrix indicators within the individual component. The most common command and control ports are displayed.
- **Established Client/Server Relationships Over Last 90 days:** This trend component graphs data on internal client trusted client and server connections over a 90-day period.
- **Servers Connecting To Clients Over Command/Control Ports: Server:** This matrix component collects data on internal trusted server connections. Results are sorted by TCP port and displayed in a series of matrix indicators within the individual component. The most common command and control ports are displayed.
- **Traffic Over Possible Bad Ports:** This malware matrix component collects data on internal client trusted client connections. Results are sorted by TCP port and displayed in a series of matrix indicators within the individual component based on the TCP ports of common malware that are known to establish command and control sessions between hosts.

Category: Threat Detection & Vulnerability Assessments
Tags: Passive, Trust, Client, Server
Requirements: Passive Data

Related Resources
Trust Relationships 1-50 Client(s) or Server(s) Asset
Trust Relationships 50-100 Client(s) or Server(s) Asset
Trust Relationships 100-500 Client(s) or Server(s) Asset

How This Applies to the SEC OCIE Risk Alert

The ability of PVS to track trust relationships allows the firm to monitor details of data flows and track the relationship of each flow. The firm can also identify systems that are heavily used and designate them as critical systems. Trust relationships can also be monitored for tracking client transactions, as the clients would need to establish a trusted connection to the firm's systems to conduct business. The trust analysis also facilitates the event detection process and can improve the firm's defense posture. The Risk Alert advocates monitoring systems for data flow and network traffic analysis. See the Appendix to the Risk Alert:

- Maps of network resources, connections, and data flows (including locations where customer data is housed) are created or updated. (Request 1, sub-bullet)
- The Firm restricts users to those network resources necessary for their business functions. If so, please describe those controls, unless fully described within policies and procedures. (Request 10, sub-bullet)
- Evaluating remotely initiated requests for transfers of customer assets to identify anomalous and potentially fraudulent requests. (Request 21, sub-bullet)
- Monitoring the activity of third party service providers with access to the Firm's networks. (Request 21, sub-bullet)
- Aggregating and correlating event data from multiple sources. (Request 21, sub-bullet)
- Testing the reliability of event detection processes. If so, please identify the month and year of the most recent test. (Request 21, sub-bullet)
- Using the analysis of events to improve the Firm's defensive measures and policies. (Request 21, sub-bullet)

The Next Steps

The needs and requirements of every organization are different. The guide has illustrated how to find much of the content needed to provide a base on which to build a customized cybersecurity program tailored to the firm’s cybersecurity requirements. The next step is to implement methodologies to succeed with a successful cybersecurity program.

A successful cybersecurity program will protect the firm, prevent improper conduct, and promote adherence to the firm’s regulatory obligations. The program should consist of continuous active scanning, passive detection, log analysis, vulnerability management, and compliance checking. Tenable’s SecurityCenter allows a single console to administer these activities across the organization. As the firm will quickly find, SecurityCenter is completely scalable and customizable. This allows the firm to fine-tune a solution by customizing components, reports, and assets to satisfy their risk management cybersecurity needs, and deliver an advanced and comprehensive cybersecurity risk management program.

Tenable products represent the “best in class” for managing cybersecurity with SecurityCenter Continuous View (SCCV). SCCV detects emerging threats through real-time discovery of resources, new systems, unexpected or unusual connections, and relationships between devices. With active and passive scanning, SCCV can identify vulnerabilities before they become compromised. The methods used by incident response teams and cybersecurity threat detection are native to SCCV by integrating Nessus and PVS. Additionally, LCE brings in an unmatched methodology to log normalization and vulnerability identification using log data. No other cybersecurity platform has this level of vulnerability and threat management in one package.

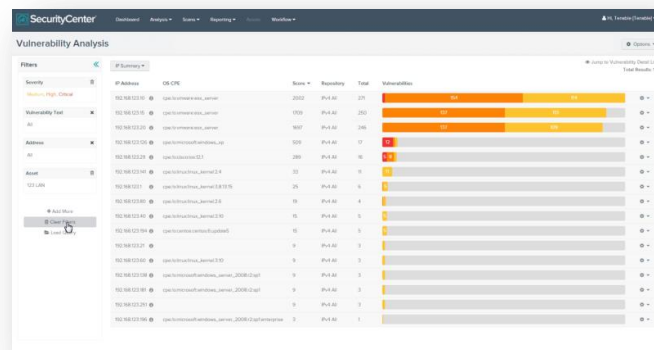
Active scanning is, for the most part, a snapshot-in-time view of vulnerabilities that exist in an organization’s environment. In a typical organization, scans occur on a quarterly or even monthly basis. However, the scans only tell you what happened in that moment, not what happened in the intervening days between scans. For example, if a new system was added to a network the day after a quarterly scan, it could be another 90 days before anyone is aware of any missing patches, vulnerabilities, or installed backdoors on the system. By scanning more frequently (and introducing real-time, passive scanning), organizations will have more accurate metrics that show how long a detected vulnerability was present and when it was mitigated.

Features to Enhance Security Posture

Tenable SCCV delivers several features to enhance the security posture of the firm. The core functionality of SecurityCenter provides an easy-to-use and scalable reporting platform through dashboard collections and reports. With the addition of the SecurityCenter app feed, SCCV gives its users more information at their fingertips with little or no customization required. Combined with LCE and the many available LCE Clients, data that is important to cybersecurity can be collected. The LCE can collect normal syslogs, Windows Event logs, NetFlow, and several other data sources.

Pivoting and Contextual Filtering

Tenable SCCV 4.8 introduces the concept of pivoting from one data set during forensic analysis to another while keeping the relevant context and scope of the analysis. For example, a security analyst can go from analyzing the exploits on a compromised device to examining the network communications of that device with a single click. This provides extremely intuitive analysis by giving the security analyst an educated guess on what to inspect next.





While in the HTML5 UI, pivoting can be done between vulnerability data and threat data, without losing context, enabling a more intuitive analysis. This is accomplished while in any Analysis drop-down, by selecting the filters icon to expand the area to the top left of the screen.

Combination Asset Modeling

Tenable SCCV 4.8 also introduces combination assets, or assets of assets, that make it easy to handle very large networks as well as organize assets based on business function, geography, or any system property. This allows organizations to organize, analyze, and manage groups of assets based on technical or functional groupings.

Assets of assets are dynamically updated so that any changes to the network and device topology are immediately reflected in the management framework. Being able to organize assets dramatically improves security analysis; for example, attack path scenarios can be quickly built and analyzed.

User Based Modeling and Reporting

Security analysts using Tenable SCCV can now manage their areas of responsibility through SCCV user-based modeling. Administrators can define who owns and manages specific assets, and summarize security status by areas of ownership. SCCV also packages by owner reports and dashboards that show the security posture, allowing security analysts to focus on their incidents and analyses, helping them to work more efficiently and greatly improving the time to respond to incidents.

Create Assets

Assets can be created using pre-defined templates that are sorted into categories. Assets can be used to expedite the creation of policies, dashboards, and reports. Custom assets can also be created to suit specific organizational needs. Tenable automatically delivers many pre-built assets within the security "app store" via a searchable catalog.

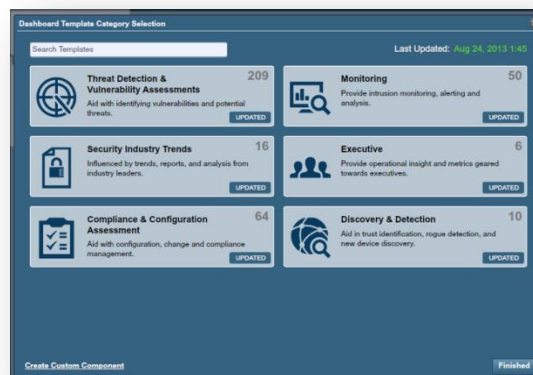


There are many different types of assets that can be created, such as static, dynamic, combination, LDAP query, and watchlist. The most powerful assets are dynamic, which take advantage of flexible grouping of condition statements to create assets lists. For example, Nessus or PVS results can be parsed to build a dynamic list of IP addresses that have port 80 open. Rules are very sophisticated and can take into account addressing, open ports, and specific or discovered vulnerabilities.

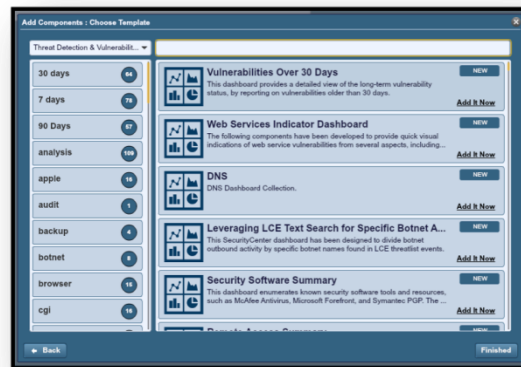
Create Reports from Dashboards/Collections

SecurityCenter provides flexible reporting options, in a wide variety of standard formats. Pre-defined report templates are available, and dashboards/collections can be easily exported to reports and shared with key personnel.

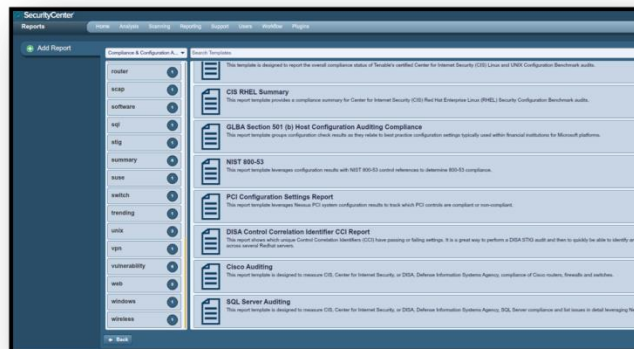
Tenable automatically delivers updated dashboards, dashboard components, and templates via the security "app store" via a searchable catalog, providing easy access to components without the need to manually download them. New analytics are automatically delivered as they are developed by Tenable researchers.



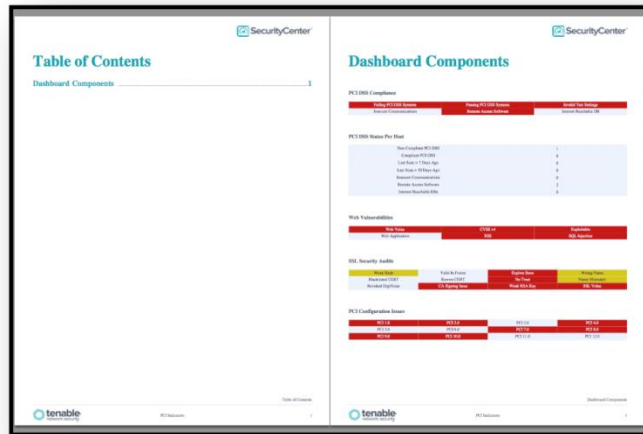
The simplified dashboard creation with a wizard and a simplified workflow allows selecting the right dashboards or creating custom views for reviewing analytics of importance.



Similar to dashboards, a report creation process is available. The security “app store”, in addition to dashboards and components, provides direct access to a library of pre-built reports and pluggable components as developed by Tenable researchers.



Reports can even be created from dashboards. View and choose the right dashboard details and components, and then convert the final dashboard to a report.



For more detailed information on creating and managing users and groups, and creating fully customized assets and components, see the Tenable SecurityCenter User Guide available on the [Tenable Support Portal](#).



Iterators are an important feature similar to a for/next loop. Iteration can be by vulnerability, IP, or port. Combined with the LCE, iteration can be by event type or event user. The iterator function is perfect to create reports that, for example, present host-by-host vulnerability details, such as all the high vulnerabilities listed by host, or what hosts are impacted by a specific vulnerability.

To keep associated elements on the same page in a report, use the Group element and put all the associated elements into the group. This will not affect the content of the report, but will attempt to keep all the elements together with a minimum of whitespace between them. If the group should have a title, use a Section instead.

Logging

The inclusion of log analysis is essential. Incorporating events logs allows the firm to maintain a more comprehensive record of event data for analysis. Intelligence from logs, events, and network data are also available for advanced vulnerability management. Tenable's LCE can accept up to 8,192 simultaneously connected LCE Clients. Those clients can be any mixture of Mac OS X, Windows, or RHEL/CentOS 5/6.

LCE analyzes log data to passively detect and identify a variety of vulnerabilities. LCE detects running applications and services to provide additional data for software inventory and identification.



Integrating the Log Correlation Engine with SecurityCenter, Nessus, and Passive Vulnerability Scanner will implement a continuous security and compliance monitoring architecture for real-time analytics and reporting.

Audit Files for Compliance Checking

Tenable provides more than 500 audit policies and over 50,000 individual checks against all major regulatory standards, including PCI DSS, HIPAA, SOX, FISMA/CyberScope, and others. A wide range of certified policies based on the Center for Internet Security (CIS) benchmarks are available, including for operating systems, databases, applications, network and virtual infrastructure, sensitive content, and anti-virus. Utilizing the policies that fit the firm's needs will assist in auditing against common standards, security settings, and configurations.

The advantage of using Nessus to perform vulnerability scans and compliance audits is that relevant data can be obtained at one time. For example, knowing how a server is configured, how it is patched, and what vulnerabilities are present can help determine measures to mitigate risk.

The Difference Between Vulnerability and Audit Scanning

When an audit is performed, Nessus attempts to determine if the host is compliant, non-compliant, or if the results are inconclusive and need to be verified manually. Compliance results in Nessus are logged as “Pass”, “Fail”, and “Warning”. The Nessus user interface and Tenable’s SecurityCenter log results as “Info” for passed, “High” for failed, and “Medium” for inconclusive (e.g., a permissions check for a file that is not found on the system).

Unlike a vulnerability check that only reports if the vulnerability is actually present, a compliance check always reports something. This way, the data can be used as the basis of an audit report to show that a host passed or failed a specific test, or if it could not be properly tested.

Scanning Methodology

To focus on a large amount of systems in a relatively small amount of time involves greatly cutting back on the time spent per system. For example, a firm might only scan for interesting ports instead of all ports. This can dramatically decrease scanning time.

There are two general ways to utilize Nessus. First, a single scan policy could be created that performs all of the required functions including discovery, scanning a handful of ports, and using specific plugins. Such a policy would be convenient and easy to manipulate if a repeat scan is required. However, putting everything into one policy is not efficient. If any adjustments need to be made to the policy, scanning of the network would have to start over from the beginning, or only the remaining hosts will be scanned with the new scan policy. If time is not a factor and the scan options are not subject to change often, a single policy is a viable option.

The second option is to create one policy for each phase. This involves separate policies for host discovery, port scanning, and vulnerability checks. Using one policy at a time to refine the target list allows for efficient scans and the ability to make adjustments to the next policy based on previous results.

For example, the first policy would focus on simple host discovery using “ping” and no additional port scanners. This policy would not utilize any plugins or port scanners. The second policy would then only be applied to hosts found during the discovery phase. This policy would focus on port scanning to look for services that are important, or that are frequently found with vulnerabilities. By selecting a small list of ports, tens of thousands of hosts can be quickly scanned in a relatively short amount of time. The third policy would then look for vulnerabilities in the services previously found. The exact list of vulnerabilities will vary depending on the selected services, the nature of the services, and the time involved. For example, enabling all web server checks (i.e., server, CGI, CGI XSS) for web servers found on ports 80 and 443 by the previous policy would significantly increase the time required to perform the scan. Carefully selecting plugins to look for specific information, high-risk vulnerabilities, and “low hanging fruit” (vulnerabilities that are trivial to exploit) allows the firm to conduct a meaningful and helpful assessment despite a large number of systems and typically small time frames. The final challenge is to put the results of all the scans into meaningful reports to assist the organization. Exporting the results and sharing with administrators allows them to import the data into their own Nessus scanner and use report filtering to work with the data.

Scanning large networks will always be a balance between how much can be scanned versus the allocated time window. Using extra scanners allows performing a significant amount of additional assessment work. Refining scans to suit the target environment will produce more accurate data. For example, if the target network is purely a Windows environment, removing services that are generally not found on that operating system (e.g., SSH) can save time and allow looking for additional Windows-specific services.

Using SecurityCenter to manage the scans and data can provide the firm not only with a single place to house the data, but also advanced reporting ability as well as historical trending data. If large scans must be run periodically to determine not only the vulnerabilities present, but to also verify that patches are being applied, SecurityCenter can manage multiple Nessus scanners and correlate all the data into a comprehensive report.

Summary

The Cybersecurity Initiative of the U.S. Securities and Exchange Commission's Office of Compliance Inspections and Examinations (OCIE) is designed to assess cybersecurity preparedness in the securities industry. The April 15, 2014 Risk Alert issued by OCIE includes an Appendix of requests for information that are "intended to empower compliance professionals in the industry with questions and tools they can use to assess their firm's level of preparedness, regardless of whether they are included in OCIE's examinations."³

This guide has provided many SecurityCenter examples that can assist a firm in maintaining accurate inventories, maintaining knowledge of normal operations, managing vulnerabilities, detecting unauthorized activity, malware, and data loss, and measuring compliance. Regardless of a firm's current level of preparedness for OCIE examinations, these components, either used as provided or custom-tailored, can assist a firm in achieving many of the outlined cybersecurity goals.

³ OCIE Cybersecurity Initiative, SEC National Exam Program Risk Alert, Vol. IV, Issue 2 (Apr. 15, 2014).

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations, including the entire U.S. Department of Defense and many of the world's largest companies and governments, to stay ahead of emerging vulnerabilities, threats and compliance-related risks. Its Nessus and SecurityCenter solutions continue to set the standard to identify vulnerabilities, prevent attacks and comply with a multitude of regulatory requirements. For more information, please visit www.tenable.com.

GLOBAL HEADQUARTERS

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com

