US SEC Cyber Security Initiative Risk Alert

Preparing for and complying with the US Security and Exchange Commission Cyber Security Inspections

Background

On April 15th 2014 the United States Securities and Exchange Commission's (SEC) Office of Compliance and Inspections Examinations (OCIE) issued a Risk Alert providing guidance to cybersecurity. The SEC states it will conduct audits and examinations of over 50 registered financial services organizations (broker-dealer and investment advisory firms) to ensure adequate cybersecurity. With the Risk Alert, the SEC is providing a "roadmap" that outlines how the OCIE intends to ensure the firms can improve their security posture, and prepare themselves for a cybersecurity audit. The Alert includes an appendix with a list of potential questions that the firms should be prepared to answer and document.

Deciphering OCIE Questions

Tenable's security and compliance experts have broken down the list of potential questions in the Risk Alert into groups of information that cover various cybersecurity practices. In addition Tenable's SecurityCenter Continuous View (CV) solution provides the necessary reports, dashboards and components necessary to address the technology components of the information requests.

The OCIE Risk Alert information requests can be simplified into the following seven "goal" areas. Adhering to these goal areas will reduce the organization's effort when addressing the SEC OCIE audit.

1. **Maintain accurate inventories**
   Inventory the firm's physical devices, software, platforms, applications and IT assets and document processes to manage addition, change and removal of these assets.

2. **Maintain knowledge of normal operations**
   Document network traffic flows, connections and baselines; critical/sensitive data stores, access privileges from external sources; utilization of encryption; documentation of policy and procedures; event logging practices including retention policies and securing log data.

3. **Discover vulnerabilities and track remediation progress based on risk assessment**
   Discover and prioritize vulnerabilities in all hardware, software and data store assets based on criticality of the asset..The firm must also perform periodic risk assessments and penetration tests to identify cybersecurity risks.

4. **Prevent unauthorized activity**
   Monitor for and prevent unauthorized activity such as unauthorized devices, connections, escalation of user privileges, access, changes, etc. The firm must pay special attention to restricting access to authorized users, monitoring third party access and privilege escalation.

5. **Monitor for malicious activity**
   Involves monitoring for (and, where possible, preventing) malicious activity, such as malware and botnet activity, denial of service, etc. The firm must also rely on data that is aggregated and correlated from multiple sources to detect complex and persistent attacks.

6. **Monitor for data loss**
   Involves monitoring for (and, where possible, preventing) data leakage and data loss. The firm must monitor for unauthorized removal of data over the network, as well through physical means (drives, removal of devices, USB etc.)

7. **Measure compliance**
   Involves conducting audits to determine compliance with policy and accepted standards, including NIST, ISO, COBIT or others. If the firm requires its service providers and partners to perform audits it must document the processes to ensure the audit was done satisfactorily.

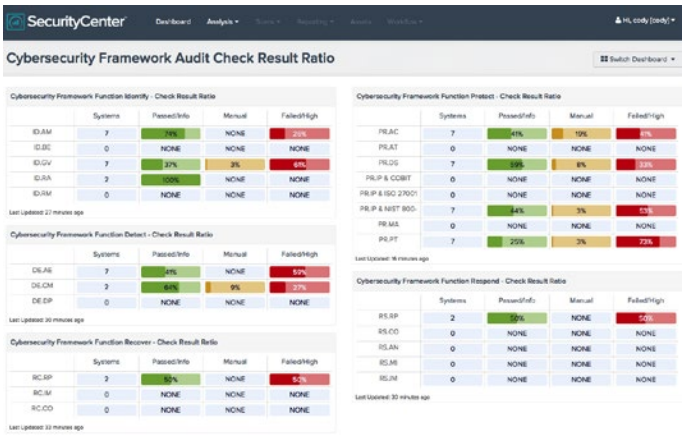
The US SEC's Office Of Compliance Inspections And Examinations issued a Risk Alert that includes questions and tools they can use to assess their firm's cyber-security preparedness. Over 50 financial broker-dealers and investment advisors are subject to the associated inspections.

Solution Components

- Tenable SecurityCenter CV
- Tenable Nessus Vulnerability Scanners
- Tenable Passive Vulnerability Scanners

Key Benefits

- Detect 100% of all assets in the network, and identify their vulnerabilities and security misconfigurations
- Audit the efficacy of deployed system patches and Anti-Virus products
- Demonstrate compliance with industry standards, government regulations and cybersecurity frameworks



Tenable's SecurityCenter Continuous View provides the necessary elements that can be used to address the SEC OCIE questionnaire.

Addressing CyberSecurity And OCIE

Tenable's SecurityCenter Continuous View (CV) is equipped with the tools that help gather data for OCIE's information requests, and is able to provide the documents required to satisfy cybersecurity requirements as laid out by the OCIE.

1. **Compliance and Configuration Assessment**
   Tenable SecurityCenter CV leverages the practices implemented for GLBA, CSC Top 20, PCI DSS and NIST 800-53. This gives it the ability to quickly gather the information needed to directly address the OCIE inspection requirements.
2. **Discovery and Detection**
   By continuously monitoring for host activity as well as their suspicious process, user behavior, registry and software profiles Tenable SecurityCenter CV performs discovery across your environment and also detects any indicators of compromise.
3. **Behavior and Activity Monitoring**
   SecurityCenter CV is capable of the deepest behavior monitoring across the enterprise, including NetFlow analysis, monitoring for data leakage, web and cloud services as well as close monitoring of user accounts for anomalous behavior.
4. **Security Industry Trends and Compliance Frameworks**
   Tenable keeps up to date with security and vulnerability trends and events, and control frameworks to help organizations stay ready to detect and respond instantaneously.
5. **Threat Detection and Vulnerability Assessments**
   Tenable's deep expertise in threat and vulnerability management helps firms assess risk and prioritize the necessary actions to remediate threats and incidents and provide information for OCIE requests.

For an in-depth guide of Tenable SecurityCenter CV's capabilities as they relate to SEC OCIE please reference the publication "Security and Exchange Commission Risk Alert Reference Guide" by Tenable Network Security.

Beyond SEC OCIE – Continuous Monitoring

Tenable SecurityCenter CV is a critical component of security programs as it is the only solution that provides comprehensive Continuous Monitoring across traditional, virtual, mobile and cloud IT environments. By uniquely bringing together vulnerability scanning, network sniffing and event log correlation under a single integrated solution, SecurityCenter CV covers 100% of your IT assets 100% of the time through its library of over 1,000 security intelligence apps to turn data into actionable security information.

Tenable SecurityCenter CV is able to:

- **Perform Automated Discovery**
  Utilizing its network monitoring capability in conjunction with scanning and log collection, SecurityCenter CV discovers all physical, virtual and mobile devices across your environment as soon as they join the network.
- **Comprehensive Vulnerability Assessment**
  SecurityCenter CV enables superior visibility into risks across the enterprise by using a combination of active and passive assessments. With over 60,000 assessments SecurityCenter CV has more than three-times more checks than its nearest competitor, ensuring every risk in the firm is visible.
- **Reporting and Analytics**
  Security analysts using SecurityCenter CV for security operations are able to get analytics relevant to their area of responsibility through SecurityCenter CV's user-based modeling and reporting, allowing them to zero-in on risks in their specific domains.
- **Taking Instantaneous Remediation Action**
  With SecurityCenter CV mitigating threats and reducing their impact becomes easy as all the relevant information is at the right security analyst's fingertips. Incident responders are also able to collaborate with each other to solve security problems with SecurityCenter CV's asset grouping function.

About Tenable

Tenable Network Security is relied upon by more than 22,000 organizations in over 100 countries, 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 award-winning Nessus and SecurityCenter solutions have received the highest-possible rating in Gartner's MarketScope for Vulnerability Assessment and continue to set the standard for identifying vulnerabilities, preventing attacks, and complying with a multitude of regulatory requirements. For more information about Tenable, please visit www.tenable.com.

For More Information

Questions, purchasing, or evaluation:
sales@tenable.com or 410-872-0555
Twitter: @TenableSecurity
YouTube: youtube.com/tenablesecurity
Tenable Blog: blog.tenable.com
Tenable Discussions: discussions.nessus.org
www.tenable.com

tenable® network security