Solution Brief

Tenable and Splunk

Leveraging Vulnerability Data to Enhance Splunk Operational Intelligence

The Challenge

Security teams are overwhelmed by the amount of event data they receive. How do you sort through all the noise and arrive at only the critical security events? SIEM and security big data solutions do a good job of supporting threat detection and incident response through real-time collection and analysis of security events. But what if you could leverage this data for early detection of targeted attacks, compromises and breaches, as well as meet regulatory compliance?

Adding vulnerability data to your SIEM and big data solutions can deliver the insight and context you need to provide a complete picture of your security posture, help you identify blind spots and ultimately avoid risk and loss for your organization.

With the addition of vulnerability management data to your SIEM environment, your organization can tackle the following challenges:

- Assess remote hosts not present during active scans
- Identify and scan new hosts on remote network segments
- Detect cyberthreats that bypass perimeter defenses
- Uncover Splunk-specific vulnerabilities and misconfigurations

The Solution

Combining Tenable™ with Splunk results in comprehensive operational intelligence, significantly improving your organization's security posture. Through collaboration, Tenable and Splunk have developed joint integrations, providing reciprocal support of each other's products and technologies.

Tenable provides Splunk users with continuous monitoring capabilities for complete visibility into all hosts and their potential vulnerabilities, misconfigurations and unpatched components. Tenable collects Splunk logs and event data, which provides added context for enhanced security insight in Tenable SecurityCenter®. Additionally, by passively monitoring network traffic, Tenable detects transient devices, such as unmanaged smart phones, remote network segments with a variety of new hosts or virtual machines, and cloud-based services. This continuous monitoring capability delivers a complete and real-time picture of internal and external uses of applications, systems and devices, which uncovers potential blind spots. The Tenable-built Nessus® Network Monitor (formerly known as Passive Vulnerability Scanner® or PVS) integration for Splunk is available for no charge on Splunkbase.

Tenable also provides Splunk-specific checks to both identify Splunk hosts and assess them for vulnerabilities. As a result, you can protect your systems from potential Splunk-specific exploits.

Splunk's integration with Tenable SecurityCenter and Nessus enables critical vulnerability management and continuous monitoring data to be available in the Splunk Operational Intelligence platform. As a result, Splunk users can discover, assess and prioritize their security posture for all assets, systems and devices, on any platform -- physical, virtual, cloud and mobile. By leveraging Tenable vulnerability and configuration data to conduct deep security analysis, Splunk Operational Intelligence users can obtain the insight, context and intelligence they need to make effective security decisions.

The Splunk-built integration for Tenable SecurityCenter and Nessus is available for no charge on Splunkbase.

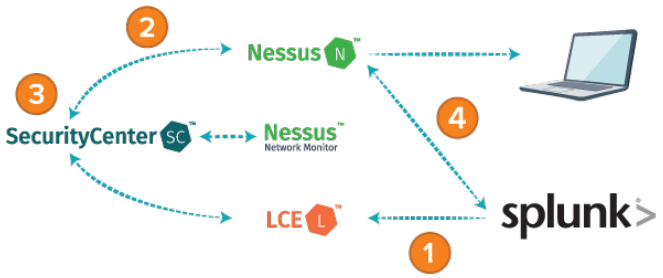
Components:

- Splunk Cloud or Splunk Enterprise
- Tenable SecurityCenter Continuous View
- Tenable Nessus vulnerability scanners

Benefits:

- **Enables** 100% asset discovery by detecting new hosts connected to remote network segments
- **Discovers** mobile devices and virtual machines not present during periodic vulnerability scans
- **Detects** Splunk-specific system vulnerabilities and security misconfigurations
- **Uncovers** cyberthreats missed by traditional perimeter defenses

How It Works

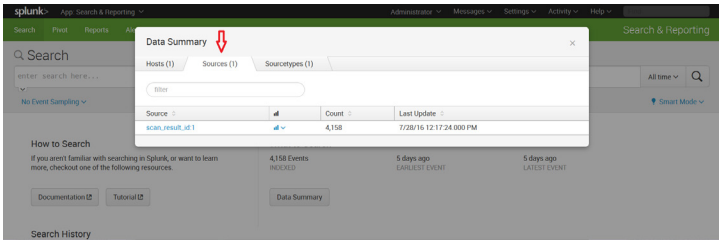


1. Tenable SecurityCenter Continuous View interfaces with Splunk's REST API to import and transfer Splunk log data in real time.

2. As new hosts are identified, SecurityCenter Continuous View creates dynamic asset lists triggering full Nessus vulnerability scans of new hosts.

3. SecurityCenter Continuous View correlates Splunk-exported log data against Tenable-provided vulnerability and threat intelligence to uncover botnets and other cyberthreats.

4. Additionally, Tenable Nessus can scan Splunk hosts for Splunk-specific vulnerabilities to feed into Tenable SecurityCenter.



The Tenable SecurityCenter Continuous View Splunk dashboard shows security vulnerabilities and misconfigurations, enhancing an organization's security posture.

About Splunk

Splunk Inc. is the market-leading platform that powers Operational Intelligence. We pioneer innovative, disruptive solutions that make machine data accessible, usable and valuable to everyone. More than 11,000 customers in over 110 countries use Splunk software and cloud services to make business, government and education more efficient, secure and profitable. Visit splunk.com to learn more.

About Tenable

Tenable™ transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats and reduces exposure and loss. With more than one million users and more than 21,000 customers worldwide, organizations trust Tenable for proven security innovation. Tenable customers range from Fortune Global 500 companies, to the global public sector, to mid-sized enterprises in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus® and leaders in continuous monitoring, by visiting tenable.com.

tenable™

For More Information: Please visit tenable.com
Contact Us: Please email us at sales@tenable.com or visit tenable.com/contact