SOLUTION OVERVIEW

TENABLE FOR SPLUNK ENTERPRISE

ENHANCE OPERATIONAL INTELLIGENCE WITH IT AND OT VULNERABILITY INSIGHTS

BUSINESS CHALLENGE

Organizations depend on Splunk Enterprise to harness operational IT, OT and Active Directory (AD) data to detect and respond quickly to threats. Without the ability to integrate critical vulnerability intelligence into the platform, security leaders are at risk of weakening incident investigations by not having full security context to take the right actions.

SOLUTION

The Tenable® integrations with Splunk Enterprise combines Tenable's Cyber Exposure insights with Splunk's correlation capabilities for complete visibility into all assets across the modern attack surface and their potential vulnerabilities, misconfigurations and unpatched components in a single analytics platform. Using Tenable and Splunk together enables joint customers to sync IT, OT and AD vulnerability information, prioritize vulnerability remediation based on actual risk, request a remediation scan and view the latest vulnerability summary for a machine during an investigation.

VALUE

The Tenable integration for Splunk provides the ability to:

- Discover additional hosts that were previously unknown to Splunk
- Erich existing events with vulnerability context and state information
- Centralize vulnerability alerting and reporting
- Respond faster to the most critical vulnerabilities with Predictive Prioritization
- Utilize Adaptive Response Actions with Splunk Enterprise Security (optional)

FEATURES

With this integration, you can:

- Sync vulnerability information, including state from Tenable platforms
- Prioritize remediation based on the likelihood of a vulnerability being exploited
- Scan a host during an investigation
- Request a remediation scan during an investigation (Tenable.sc)
- Get the latest vulnerability summary for a host during an investigation
- View a single dashboard with configured vulnerability feeds
- Transform Tenable.ot Syslog events into Splunk

TECHNOLOGY COMPONENTS

- Tenable.io, Tenable.sc 5.13+, Tenable.ot, Tenable.ad
- Tenable Add-on for Splunk
- Splunk Enterprise 8.0+
- Tenable App for Splunk (optional)
- Splunk Enterprise Security (optional)
- CIM 4.X

KEY BENEFITS

- **Automatically sync** Tenable data into QVM
- **Ensure** all systems are known
- **Automate** closed-loop remediation
- **Improve remediation** decision making with vulnerability insights

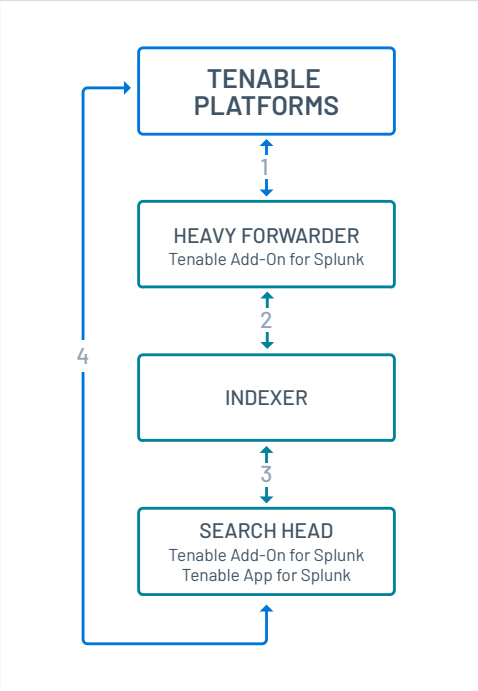
ABOUT TENABLE

Tenable®, Inc. is the Cyber Exposure company. Over 30,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include more than 50 percent of the Fortune 500, more than 30 percent of the Global 2000 and large government agencies. Learn more at www.tenable.com.

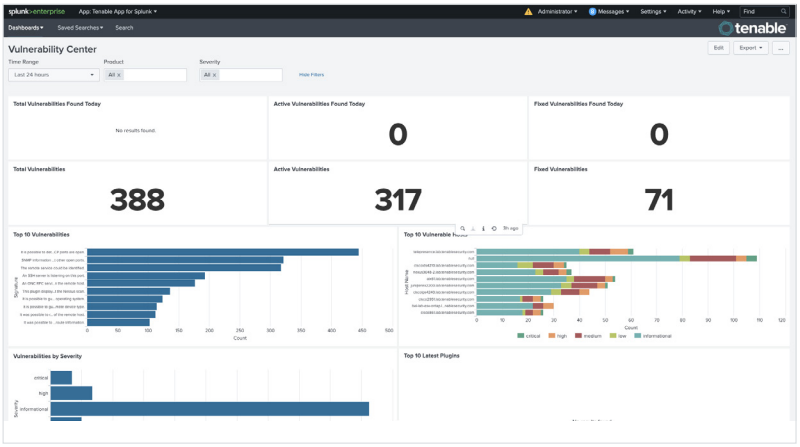
ABOUT SPLUNK

Splunk Inc. (NASDAQ: SPLK) turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to solve their toughest IT, Internet of Things and security challenges. Join millions of passionate users and discover your "a ha" moment with Splunk today. Learn more at splunk.com

HOW IT WORKS



1. All vulnerabilities are gathered from Tenable
2. Tenable data is indexed into Splunk
3. Tenable data is searchable and reportable in default Splunk reports and the Tenable App for Splunk
4. Adaptive Response actions can be invoked to enrich Splunk Enterprise notable events



Tenable App for Splunk Vulnerability Dashboard

MORE INFORMATION

Tenable Add-on and App for Splunk: https://splunkbase.splunk.com

Installation and configuration documentation: docs.tenable.com/integrations.htm

For support please visit: https://community.tenable.com