

TENABLE PLUGIN FOR IBM SECURITY QRADAR

ENHANCE OPERATIONAL INTELLIGENCE WITH VULNERABILITY INSIGHTS

BUSINESS CHALLENGE

Organizations depend on the ability to harness operational data and correlate threats for proper response actions. Without having full security context and vulnerability insights from Tenable within QRadar, security leaders are missing an essential piece to make informed decisions on protecting business critical assets.

SOLUTION

The Tenable[®] App for QRadar, coupled with the Tenable integration with QRadar Vulnerability Manager (QVM) combines Tenable's Cyber Exposure insights that lead the market in coverage, accuracy and zero day research with the strength of QRadar's log and flow consolidation capabilities. This gives security teams confidence to correlate events, take action on flaws and meet compliance standards. Using Tenable and QRadar together provides familiar workflows for data enrichment and additional context on QRadar offenses, allowing users to associate and correlate Tenable findings to offenses to further enhance threat detection and vulnerability prioritization.

VALUE

The Tenable solution for QRadar provides the ability to:

- Discover additional hosts that were previously unknown to QRadar
- Gather up to date vulnerability data during investigations
- Enrich existing events with Tenable's vulnerability insights
- Improve remediation decision making with a comprehensive dashboard



TECHNOLOGY COMPONENTS

- Tenable.io, Tenable.5.13 or higher, Tenable.ot, Tenable.ad
- Tenable App for QRadar (IBM Security App Exchange)
- QRadar Security Intelligence Platform
- QRadar Vulnerability Management

KEY BENEFITS

- **Automatically sync** Tenable data into QVM
- **Ensure** all systems are known
- **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 IBM SECURITY

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. Learn more at ibm.com/security

FEATURES

With this integration, you can:

- Sync vulnerability information from Tenable platforms
- Scan a host during an investigation
- Configure rule-based scanning
- Initiate a scan with a right click
- Prioritize remediation based on the likelihood of a vulnerability being exploited
- Get the latest vulnerability summary for a host during an investigation
- Parse Tenable.ot events with embedded Device Support Module (DSM)

HOW IT WORKS

QRadar VM:

1.a Get vulnerabilities from Tenable and import them into QVM

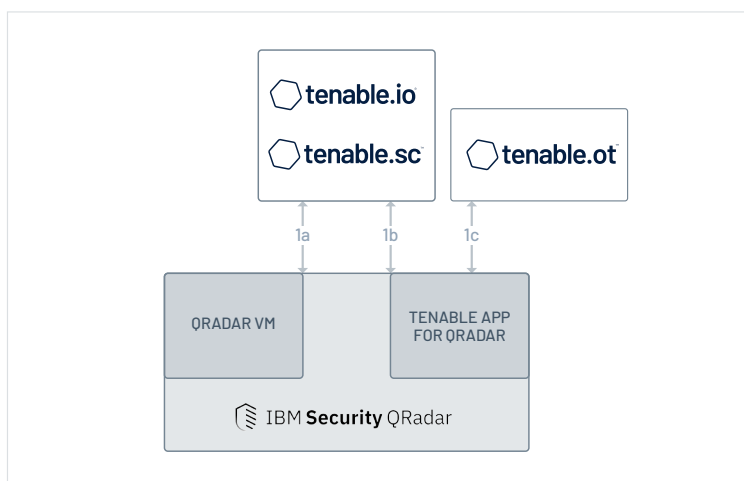
Tenable App for QRadar:

1.b For a given machine on an Offense:

- Get a summary of Vulnerabilities
- Initiate a scan with a right-click
- Scan a host during an investigation

1.c Parse Syslog events from

Tenable.ot using embedded DSM



MORE INFORMATION

Tenable App for QRadar: Exchange.xforce.ibmcloud.com

For support please contact:

ibm.com/mysupport for QRadar Support

support@tenable.com for the Tenable App for QRadar

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

