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.sc 5.13 or higher
- 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
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
- View a dashboard to track scan status
- Prioritize remediation based on the likelihood of a vulnerability being exploited
- Get the latest vulnerability summary for a host during an investigation

How It Works

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

Tenable App for QRadar:
1.b Get a summary of vulnerabilities for a given machine on an Offense

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