tenable®

Tenable and Cortex XSOAR
Automated Vulnerability Management and Response

Business Challenge

Organizations struggle with focus and upkeep on security tools within their security environment. These gaps put them at greater risk resulting in the growth of their threat landscape. Without integrating Tenable's vulnerability data into Cortex XSOAR, organizations are left without a way to utilize automated workflows and maximize resources for accelerated incident response.

Solution

The Cortex XSOAR integration with Tenable combines Tenable's Cyber Exposure insights with the Cortex SOAR engine for complete visibility into an organization's security infrastructure and attack surface. Security and IT teams are provided with management insights, pre-configured workflows and real-time dashboards to automate time-intensive, manual processes for streamlined incident response. Organizations can utilize the integration to represent and correlate vulnerabilities, assets and scan data from Tenable combined with Cortex's XSOAR engine for improved incident response.

Value

The Cortex integration for Tenable provides the ability to:

- Provide pre-defined parameters for running Vulnerability Management scans without requiring knowledge about Vulnerability Management configuration & internal network infrastructure

- Define approval processes for running adhoc infrastructure vulnerability scans

- Allow for the creation of automated workflows across security tools

- Centralize your vulnerability insights by viewing a single dashboard

CORTEX™ XSOAR
BY PALO ALTO NETWORKS

Technology Components

- Tenable.io or Tenable.sc 5.13+

- Cortex XSOAR

Key Benefits

- **Improve incident response time**

- **Enrich incident response** with vulnerability context

- **Improve processes** with configured workflows

- **Automate** your teams' manual tasks

- **Connect** Tenable to disparate security tools

- **Enforce SLA** on response actions

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

- Get the latest vulnerability summary for a host during an investigation

- View a single dashboard with configured vulnerability feeds
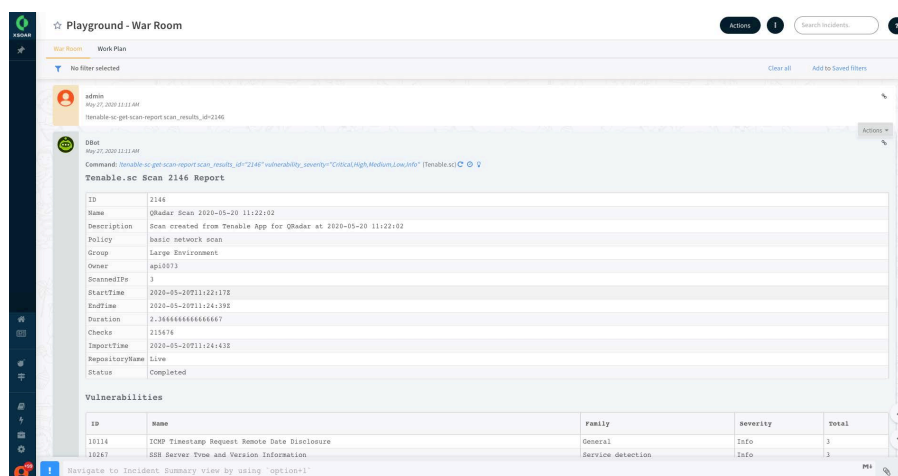
This image features a report showing Tenable vulnerability data within Cortex XSOAR that can be run by security teams to better understand and respond to threats to the organization.

More Information

Try our Products:
https://www.paloaltonetworks.com/cortex/xsoar
https://www.tenable.com/products/tenable-sc/evaluate

Documentation:
https://docs.paloaltonetworks.com/cortex/cortex-xsoar

For support please contact:
https://support.paloaltonetworks.com/support