Washington University of Science and Technology

SOC LAB

QRADAR SIEM

QRadar SIEM monitors and correlates threat intel, network, and user behavior anomalies to prioritize high-fidelity alerts. Easy-to-use dashboards provide details to investigate and remediate threats in near real time. It is an IBM product. To learn more about IBM Security QRadar SIEM, visit: https://www.ibm.com/products/qradar-siem.

> IBM Security® QRadar® SIEM is more than a tool; it is a teammate for SOC analysts—with advanced AI, powerful threat intelligence and access to the latest detection content.

Importing Vulnerability Assessment information to identify active hosts, open ports, and potential vulnerabilities.

10 Step Procedure

1. Click the **Admin** tab.
2. In the navigation menu, click **Data Sources** > **Vulnerability**.
3. Click the **VA Scanners** icon.
4. On the toolbar, click **Add**.
5. Enter values for the parameters (depends on scanner type you want to add).
For example, if you want to conduct a scan against the 192.168.0.0/16 network and specify 192.168.1.0/24 as the CIDR range, only results from the 192.168.1.0/24 range are integrated.)
6. Click **Save**.
7. On the Admin tab menu, click **Deploy Changes**.
8. Click the **Schedule VA Scanners** icon, and then click **Add**.
9. Specify the criteria for how often you want the scan to occur.
Depending on the scan type, the criteria includes how frequently QRadar imports scan results or starts a new scan. You also must specify the ports to be included in the scan results.
10. Click **Save**.

Payload Indexing: 7 Steps

1. Click the **Admin** tab.
2. In the System Configuration section, click **Index Management**.
3. In the Search field, type **quick filter**.
4. Right-click the **Quick Filter** property that you want to index.
5. Click **Enable Index**.
6. Click **Save**, and then click **OK**.
7. To disable a payload index, choose one of the following options:

• Click **Disable Index**.
• Right-click a property and select **Disable Index** from the menu.

Deploy QRadar First:

- Install QRadar appliance.
- Configure your installation.
- Collect event, flow, and vulnerability assessment data.
- Tune your installation.

QRadar Network Hierarchy to

- Understand network traffic and view network activity.
- Monitor specific logical groups or services in your network, such as marketing, DMZ, or VoIP.
- Monitor traffic and profile the behavior of each group and host within the group.
- Determine and identify local and remote hosts.

- To explore further find the full IBM QRadar Guide from the Lab Resources and practice.