Leverage Rapid7 Vulnerability Intelligence to add deep security context to IBM’s QRadar SIEM

Solution Overview

For today’s IT and Security Operations teams the need for a centralized logging and correlation tool has become a major cornerstone for most organizations. By leveraging Rapid7’s rich vulnerability and exploit data, an organization can leverage this information in conjunction with other log data sources to provide greater context and insight into the events happening within environment. IBM’s QRadar provides real-time actionable intelligence, meanwhile delivering an efficient and effective incident management workflow. Furthermore, vulnerability and asset data within QRadar streamlines the process of conducting post incident forensic analysis.

How it works

A Nexpose scan is conducted to assess the risk posture of the systems within an organization. The vulnerability data is then taken and used to calculate the RealRisk™ score associated with each system detected. QRadar’s Vulnerability Management plugin is then configured to query the Nexpose server at specified intervals for the latest vulnerability data. Once the data is in QRadar it can be used to add context which support prioritization of remediation and mitigation activities.

Overview of Integration Process

1. Step 1: Nexpose performs security assessment
2. Step 2: XML report generated with vulnerability findings
3. Step 3: Nexpose is added as VA scanner within QRadar
4. Step 4: Scheduled task created to pull data on a periodic basis
5. Step 5: XML report gets generated with the latest vulnerability data
6. Step 6: Data gets imported automatically and normalized within QRadar

Integration Benefits

- Security Context Awareness into the vulnerability state of assets.
- Better Correlation Rules with more security centric data to leverage in rule creation for more accurate alerting.
- Single Pane View into your security events, reporting, forensics, and incident investigation.
- In Depth Investigations with additional security information about each asset (ports, services, applications, etc.)
- Automated Vulnerability data import on a scheduled basis to correspond with latest scans.

Solution Components

What you need:

- Rapid7 Nexpose 5.x
- IBM QRadar 7.x
- QRadar Vulnerability Management Plugin
About IBM

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 and development provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security, and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world’s broadest security research and development organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

About Rapid7

Rapid7’s security solutions deliver visibility and insight that help you make informed decisions, create credible action plans, and monitor progress. They simplify risk management by uniquely combining contextual threat analysis with fast, comprehensive data collection across your users, assets, services and networks, whether on premise, mobile or cloud-based. Rapid7’s simple and innovative solutions are used by more than 2,500 enterprises and government agencies in more than 65 countries, while the Company’s free products are downloaded more than one million times per year and enhanced by more than 200,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a “Top Place to Work” by the Boston Globe. Its products are top rated by Gartner® and SC Magazine. For more information about Rapid7, please visit [http://www.rapid7.com](http://www.rapid7.com).

Contact us today to learn more

1-866-772-7437

1-866-7-RAPID7