Enable In-Depth Scanning

With CyberArk Application Identity Manager™ and Rapid7 InsightVM or Nexpose

Securing and managing privileged credentials (passwords and SSH Keys) used by applications is a challenge facing many organizations today. Furthermore, ensuring that privileged credentials are changed periodically, as well as being auditable, can be overwhelming to manage. When performing vulnerability scans, it is considered best practice to audit your systems using privileged accounts in order to obtain deeper insight into the vulnerabilities present on the host. Rapid7's leading vulnerability management solution, InsightVM, or our top-rated on-premise solution, Nexpose, in conjunction with CyberArk Application Identity Manager™, allows for credential-protected scans based on secured privilege credentials retrieved from CyberArk on a per-scan basis. This frees an administrator from the worry of having to update privileged account credentials in numerous locations, and ensures that all scans run using secured credentials.

HOW IT WORKS

Privileged account credentials are managed using CyberArk and are associated with a specific asset or group of assets. Sites (logical groupings of assets) are created in InsightVM* to perform a vulnerability scan. Prior to running a scan, Rapid7 and CyberArk are linked together within the InsightVM Administration tab. InsightVM will then query the CyberArk Secure Digital Vault™ for the credentials for each asset, both on a 1:1 (single credential for a single asset) and 1:many level (global credential for multiple assets). Once completed, InsightVM will utilize credentials from CyberArk for authenticated scans. (Credentials themselves are not stored in the Security Console, but rather are handled ephemerally and for the purposes of the scan only.)

Note: CyberArk Application Identity Manager automatically rotates the credentials based on an organization's security policy or on demand.

*All mentions of Rapid7 InsightVM associated with the CyberArk Application Identity Manager also apply to Rapid7 Nexpose.

INTEGRATION BENEFITS

- Secure credentials and simplify management by centrally storing and rotating Rapid7 InsightVM or Nexpose privileged account credentials.

- Enable better security visibility using admin credentials to scan, allowing InsightVM (or Nexpose) to dig deeper into a system for security assessment.

- Maintain comprehensive audit trail for compliance initiatives.

Overview of the Integration Process

- Step 1: Create privileged account stores in CyberArk Secure Digital Vault
- Step 2: Create site(s) in Insight VM with assets
- Step 3: Connect InsightVM and CyberArk consoles within the InsightVM UI
- Step 4: Run an InsightVM scan of your site(s) and automatically pull in admin credentials

Note: Rapid7 Professional Services can be engaged to help set up this integration.

Figure 1: Configuring credential management with CyberArk in InsightVM
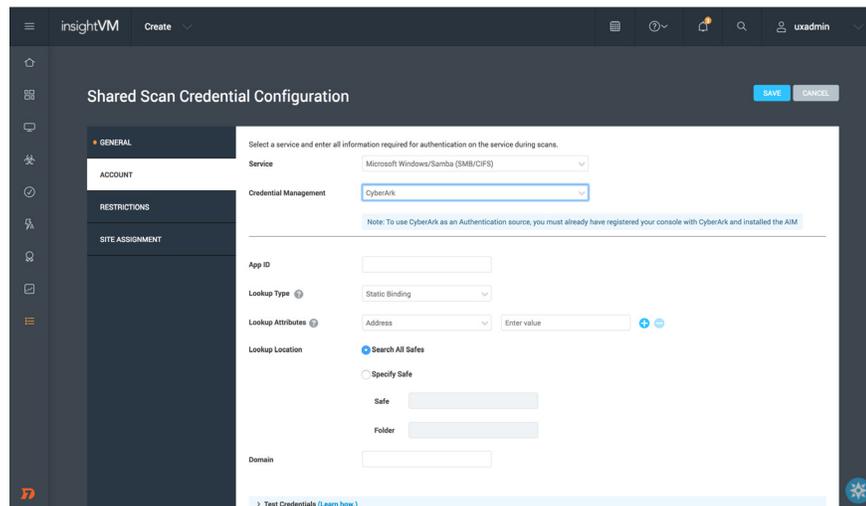
How It Works

InsightVM or Nexpose requests a credential from CyberArk, CyberArk returns the correct key, and InsightVM (or Nexpose) is then able to run an Authenticated Scan.

What You Need

Rapid7 InsightVM or Rapid7 Nexpose 6

CyberArk Password Vault Version 9.3.0

CyberArk Application Identity Manager 7.2.13

SUPPORT

Please contact Rapid7 for support or assistance at +1.866.380.8113 or support@rapid7.com

About CyberArk

CyberArk is the only security company that proactively stops the most advanced cyber threats—those that exploit insider privileges to attack the heart of the enterprise. The company has pioneered a new category of targeted security solutions to protect against cyber threats before attacks can escalate and do irreparable business damage.

To learn more about CyberArk, visit www.cyberark.com

Blog: www.cyberark.com/blog/

Twitter: @CyberArk

Facebook: www.facebook.com/CyberArk

About Rapid7

Rapid7 is a leading provider of security data and analytics solutions that enable organizations to implement an active, analytics-driven approach to cybersecurity. We combine our extensive experience in security data and analytics and deep insight into attacker behaviors and techniques to make sense of the wealth of data available to organizations about their IT environments and users. Our solutions empower organizations to prevent attacks by providing visibility into vulnerabilities and to rapidly detect compromises, respond to breaches, and correct the underlying causes of attacks.

To learn more about Rapid7 or get involved in our threat research, visit www.rapid7.com.