RAPID7 + CYBERARK

INTEGRATION BRIEF

Protect, Detect, and Mitigate Threats Targeting Users

With CyberArk Core Privileged Access Security Solution and Rapid7 InsightIDR

Whether it be spearfishing or credential theft, preventing every cyber attack is simply impossible. Detecting an attack can feel challenging, but early detection is essential to any organization's security.

"The time from the attacker's first action in an event chain to the initial compromise is typically measured in minutes. Conversely, the time to discovery is more likely to be months." - 2019 Verizon Data Breach Investigations Report.

Rapid7's cloud SIEM, InsightIDR, along with the CyberArk Core Privileged Access Security Solution, provides visibility, protection, and automated workflows to help any organization detect and take action against attacks on its users and administrators. The combination makes life easier for your security operations center: Critical alerts and behavior are prioritized by risk and leverage data across your modern network—on-premise, remote workers, SaaS, and IaaS.

How It Works

Rapid7 InsightIDR is deployed as SaaS and centralizes data from your network, endpoints, cloud hosting, and cloud applications. Security analytics and case management helps your team detect and respond to common and targeted threats.

The CyberArk Core Privileged Access Security Solution provides continuous insight into privileged activities occurring across the network. Any generated alerts and logs can feed into InsightIDR for search, reporting, and other custom use-cases that are specific to your business needs. If an admin or employee user account is determined to be compromised, the user account can be disabled or reset from within InsightIDR investigations. Additionally, if a privileged activity generates a risk score above a certain threshold, CyberArk can mitigate risk by automatically onboarding unmanaged accounts, rotating credentials, or terminating or suspending potentially malicious sessions.

Integration Benefits

1. Bring together all of your data—including privileged access actions—for easy compliance and audit.
2. Investigate risky behavior with the combined context of the CyberArk Core Privileged Access Security Solution and Rapid7 User Behavior Analytics.
3. Create custom alerts and dashboard highlighting privileged access in Enterprise Password Vault.

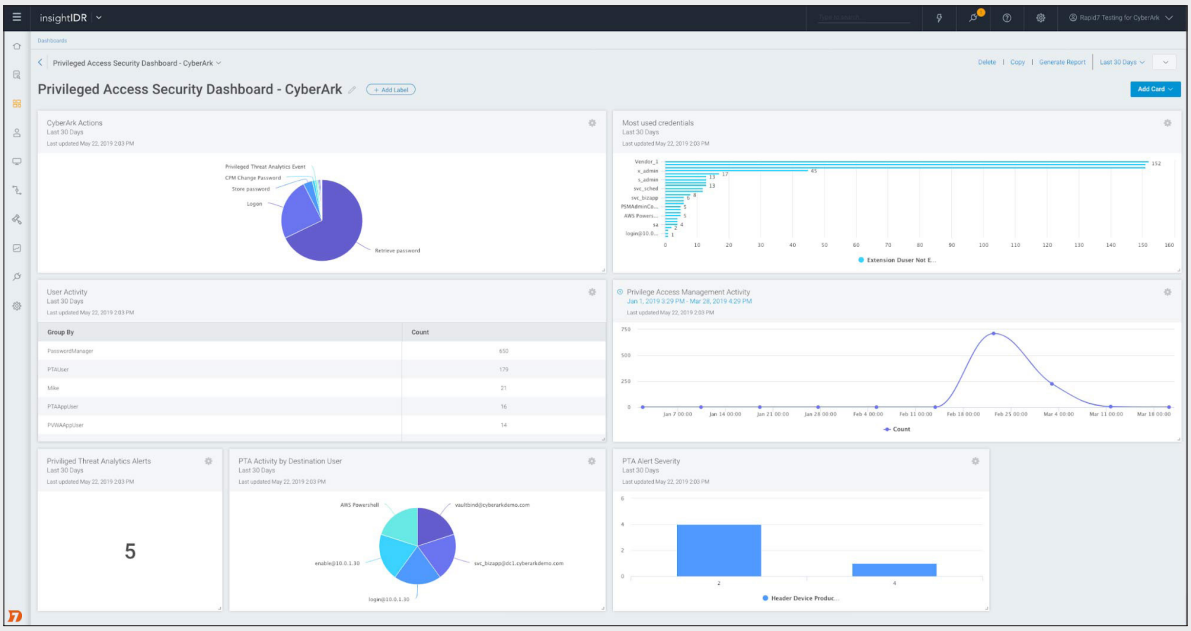

Figure 1: CyberArk data on privileged access presented as visual dashboard cards in InsightIDR.

Overview of the Integration Process

- **Step 1**: Configure CyberArk Vault and threat analytics engine to send events and alerts to Rapid7 InsightIDR.
- **Step 2:** From InsightIDR, setup a new custom event source for the incoming CyberArk data.
- **Step 3:** Verify that CyberArk data is flowing into InsightIDR in Data Collection and Log Search.
- **Step 4:** Use InsightIDR to search, visualize, and report on privileged account activities.

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

How It Works

CyberArk audit logs and alerts can be forwarded to InsightIDR for a centralized detection and investigation experience. InsightIDR automatically structures this data and makes it easy to search, visualize, and build custom alerts for your organization's privileged access activity.

What You Need

Rapid7 InsightIDR	CyberArk Enterprise Password Vault (EPV) 9.95+	CyberArk Privileged Threat Analytics (PTA) 3.6+

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.

About Rapid7

Rapid7 is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and develoment to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks.

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

Support

call +1.866.380.8113

Customer Portal