CyberArk Privileged Account Security Solution Integrated with RSA Security Analytics

Highlights

- Identify high-risk privileged account activity in real-time
- Prioritize alerts for privileged accounts and quickly investigate and respond to critical threats
- Enhance network, logs, and endpoint data with privileged account activity information
- Drill-down into CyberArk to replay privileged user sessions for forensics analysis
- Secure, manage, and control privileged accounts across the organization

CyberArk has integrated with RSA Security Analytics to deliver a real-time privileged activity monitoring solution. By combining the CyberArk Privileged Account Security Solution with RSA Security Analytics, security analysts and audit teams can now access the information they need to identify and respond to the most critical incidents, those involving privileged accounts, while meeting demanding compliance requirements.

Cyber attackers target privileged accounts in order to reach the heart of the enterprise and gain access to sensitive, valuable data. To protect these accounts and the critical resources they provide access to, organizations require comprehensive controls in place to effectively monitor, detect and respond to all privileged account activity in real time.

CyberArk's Privileged Account Security solution integrated with RSA Security Analytics enables security teams to monitor and protect privileged activity and gain unified, real-time visibility to identify critical security threats. The solution generates exceptionally detailed tracking and reporting on privileged activities, meeting audit and compliance requirements.

Centralized Privileged Account Activity Collection and Incident Management

The CyberArk Privileged Account Security Solution is an enterprise-class, unified solution that manages and secures all privileged accounts. It secures credentials, including passwords and SSH keys, controls access to these accounts, isolates and records privileged sessions for auditing and forensics analysis. Built on a single platform, the solution centralizes all privileged activity and provides a single data source into RSA Security Analytics.

CyberArk enhances RSA's security management visibility into privileged account threats by sending all privileged activity as syslog messages in RSA Common Event Format (CEF). Integrating the CyberArk Solution enables RSA Security Analytics to fully monitor and archive all privileged user and account activities. This includes individual user activity when using shared accounts as well as application logins. These alerts are then correlated with other real-time information collected from the organization, and the most critical security threats are identified.

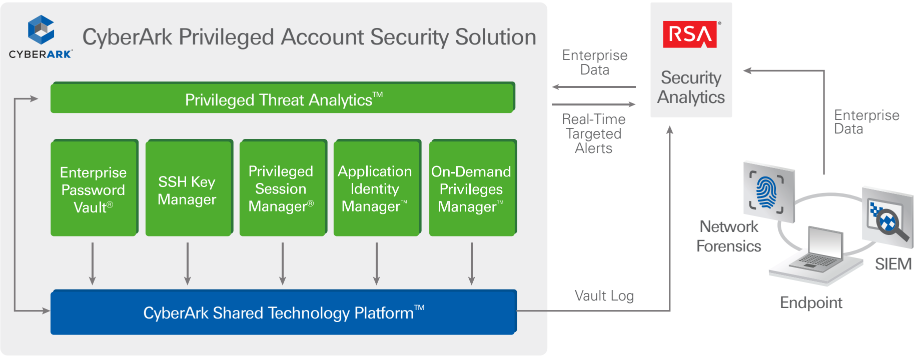
CYBERARK
CyberArk Privileged Account Security Solution
Privileged Threat Analytics™
Enterprise Password Vault®
SSH Key Manager
Privileged Session Manager®
Application Identity Manager™
On-Demand Privileges Manager™
CyberArk Shared Technology Platform™
Enterprise Data
Real-Time Targeted Alerts
Vault Log
RSA
Security Analytics
Enterprise Data
Network Forensics
SIEM
Endpoint

Figure 1. CyberArk and RSA Security Analytics joint solution for enterprise-wide privileged activity monitoring and compliance

Real-time Privileged Activity Monitoring and Compliance

By integrating and correlating the log data of privileged account activity into RSA Security Analytics, security and forensic analysts now have the widest range and depth of actionable information available via a unified dashboard. This rich data enables analysts to gain a real-time view of enterprise-wide threats that originate from privileged account activity, as well as deeper forensics analysis and evidence collection by drilling-down into privileged user sessions.

Capabilities include:

- Link events that are triggered through the use of privileged accounts with the individuals who initiated them; reveal who had access to which systems and data, when and for what purpose
- Quickly investigate alerts by replaying exactly what transpired with video playback revealing the user's actions
- Review command-level logs that are sent to RSA when anomalous activity is detected (e.g. credit card information is being copied); remotely locate and monitor the session in real-time via CyberArk Privileged Session Manager and terminate the session if required in order to disrupt the potential attack
- Monitor changes within the CyberArk Vault by sending activity logs to RSA every time a privileged user accesses the vault to make changes (e.g. creating a new administrator account, etc.)
- Generate compliance reports to show which privileged user accessed an organization's most sensitive assets, modified configuration settings and ran programs on the network

Advanced Behavioral Analysis, Monitoring and Detection Capabilities

The joint CyberArk Privileged Account Security and RSA Security Analytics solution is bi-directional, whereby RSA sends enterprise-wide data of privileged account logins directly to CyberArk Privileged Threat Analytics[1]. This enables CyberArk Privileged Threat Analytics to conduct User Behavior Analysis (UBA) based on a rich set of data, facilitating a joint solution to correlate additional data, reducing false positives and enhancing the overall value of the alerts. When CyberArk Privileged Threat Analytics detects anomalous privileged account activities, the system generates real-time alerts to the RSA Security Analytics dashboard enabling security teams to quickly monitor and respond to alerts from a single-pane-of-view.

Conclusion

The integration of the CyberArk Privileged Account Security Solution and RSA Security Analytics enables organizations to focus their efforts and resources on the highest priority targets and identify the most significant risks. The joint solution supports a more comprehensive approach to unified visibility with centralized policy-based privileged activity management. Once deployed, the solution effectively arms organizations with the information they need to identify and respond to the most critical incidents and meet demanding compliance requirements.

Joint CyberArk-RSA Security Analytics Solution:

- Provides enterprise-wide, real-time visibility to identify and investigate critical security threats associated with privileged activity
- Enables enhanced forensics analysis and evidence collection by drilling-down into privileged user sessions to understand the true nature and scope of the event
- Meets a diverse set of compliance requirements with individual accountability combined with detailed tracking and reporting on all privileged activity
- Improves security with end-to-end privileged activity lifecycle management
- Enables fast and effective incident response using automated controls

Partner Products:

- RSA Security Analytics

CyberArk Products:

CyberArk Privileged Account Security Solution:

- CyberArk Shared Technology Platform™
- CyberArk Privileged Threat Analytics™

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.

About RSA

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. Through visibility, analysis, and action, RSA solutions give customers the ability to detect, investigate and respond to advanced threats; confirm and manage identities; and ultimately, help prevent IP theft, fraud and cybercrime. For more information on RSA, please visit www.rsa.com.

[1] This is a companion piece to our CyberArk Privileged Threat Analytics™ Integrated with RSA Security Analytics solution brief