CyberArk Privileged Threat Analytics™ Integrated with RSA Security Analytics

Highlights:

- Conduct targeted threat analytics on the most critical privileged attack vectors to quickly detect and rapidly respond to cyber attacks
- Avoid a lengthy deployment process by leveraging existing infrastructure and data within the enterprise
- Enable the Security Operation Center (SOC) to prioritize alerts that involve privileged accounts and quickly respond to the most damaging threats
- Reconstruct suspicious privileged account activity to identify potential content exfiltrated

CyberArk has integrated with RSA Security Analytics to deliver targeted threat analytics on privileged account activity. By combining CyberArk Privileged Threat Analytics with RSA Security Analytics, organizations are able to analyze a rich set of data in order to detect, alert, and rapidly respond to cyber attacks.

Cyber attackers target privileged accounts in order to reach the heart of the enterprise and gain access to sensitive, valuable data. CyberArk, the trusted experts in privileged account security, has integrated their solution with RSA Security Analytics in order to help organizations detect and quickly respond to anomalous privileged account activities. CyberArk Privileged Threat Analytics conducts targeted analytics on the most critical data, enabling organizations to detect indicators of an attack in real-time, correlate network, logs, endpoint and privileged identity data, prioritize alerts that require immediate attention, and quickly respond in order to stop an in-progress attack.

A bi-directional integration with RSA Security Analytics and CyberArk Privileged Threat Analytics delivers a rich data set for threat analytics on privileged activity, enabling the joint solution to correlate and enrich with more data and provide critical threat intelligence with each detected incident. The integration also enables organizations to receive real-time threat alerts in the RSA Security Analytics dashboard and investigation for single-pane-of-view analysis of all unusual/abnormal network and identity activity across the organization. Combined, these two solutions deliver industry-leading user and entity behavior threat analytics on the most critical attack vectors – those involving privileged accounts.

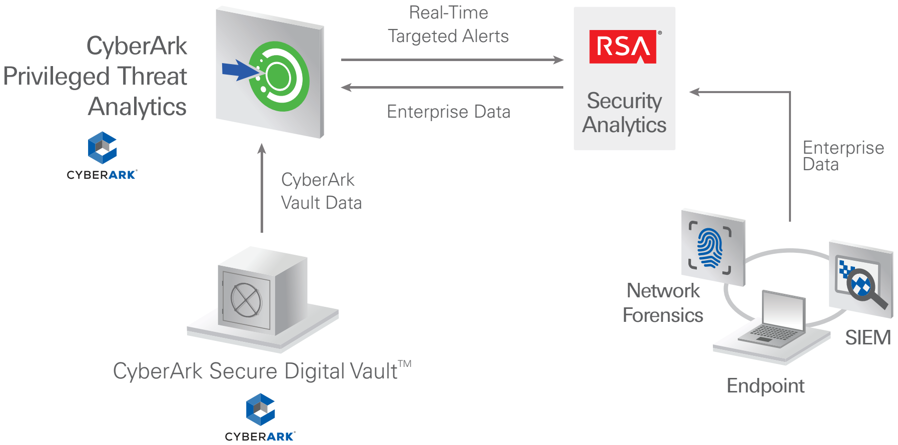

Figure 1. CyberArk Privileged Threat Analytics and RSA Security Analytics joint solution delivers enterprise-wide, targeted threat intelligence

RSA Security Analytics provides a monitoring and investigation platform to detect advanced threats, while focusing on the most important incidents so security teams can rapidly investigate. It provides real-time collecting, filtering, enrichment and analysis of network packets, NetFlow, endpoint and log data via a highly configurable infrastructure.

Interoperability of CyberArk Privileged Threat Analytics and RSA Security Analytics

Privileged Threat Analytics collects data from across the enterprise and conducts User Behavior Analysis (UBA) with custom, built-in algorithms. The analytic engine gathers data from multiple sources including:

- CyberArk Digital Vault – Privileged Threat Analytics seamlessly integrates with the CyberArk Digital Vault to pull real-time privileged account data. This data feed provides fine-grained detail of privileged account activities on individual users, even when using shared accounts. Note: The CyberArk Vault also integrates directly with RSA Security Analytics [1]
- Enterprise-wide system data – By leveraging data collection capabilities from across the enterprise, RSA Security Analytics log and network packet appliances sends enterprise-wide data, such as privileged account login activity on Windows and UNIX endpoints, to CyberArk Privileged Threat Analytics. This data feed provides a rich set of data for analytics and new insights when correlated with digital vault data and network forensics.

When Privileged Threat Analytics detects anomalous privileged account activities, for example, a privileged user accessing a server during irregular hours, the solution will generate an alert in real-time. Threat alerts are sent to RSA as syslog messages in RSA Common Event Format (CEF). Alerts include detailed, critical intelligence which helps incident response (IR) and SOC analyst teams provide enriched context to detected incidents and enables to instantly pinpoint suspicious behavior root cause and quick prioritization of critical alerts. By sending alerts to the RSA Security Analytics dashboard, security teams can receive, triage, and respond to alerts from a single-pane-of-view..

Conclusion

Threat analytics is a critical component of a comprehensive security strategy. Since attackers are targeting privileged accounts, organizations need to detect, alert, and quickly respond to anomalous privileged account activity. This joint solution enables organizations to leverage existing data and infrastructure in order to quickly and seamlessly add threat analytics to their overall security solution.

Joint CyberArk-RSA Security Analytics Solution:

- Conduct industry-leading, targeted, threat analytics on the most critical attack vectors to detect indicators of a cyber attack
- Leverage RSA Security Analytics to conduct threat analytics on enterprise-wide data without requiring a lengthy deployment process
- Enable security teams to prioritize incidents that involve privileged accounts and quickly respond before irreparable damage is done

Partner Products:

- RSA Security Analytics

CyberArk Products:

- 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 FireEye

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 Account Security Solution Integrated with RSA Security Analytics solution brief