LogRhythm

Joint Solution Brief

LogRhythm and CyberArk

Combines privileged access management with threat management for enhanced threat detection

Benefits

- Identify privileged access related anomalies and malicious activities in real time
- Gain deep visibility into privileged account activities
- Improve auditing processes with informative data on user patterns and activities

Solution Overview

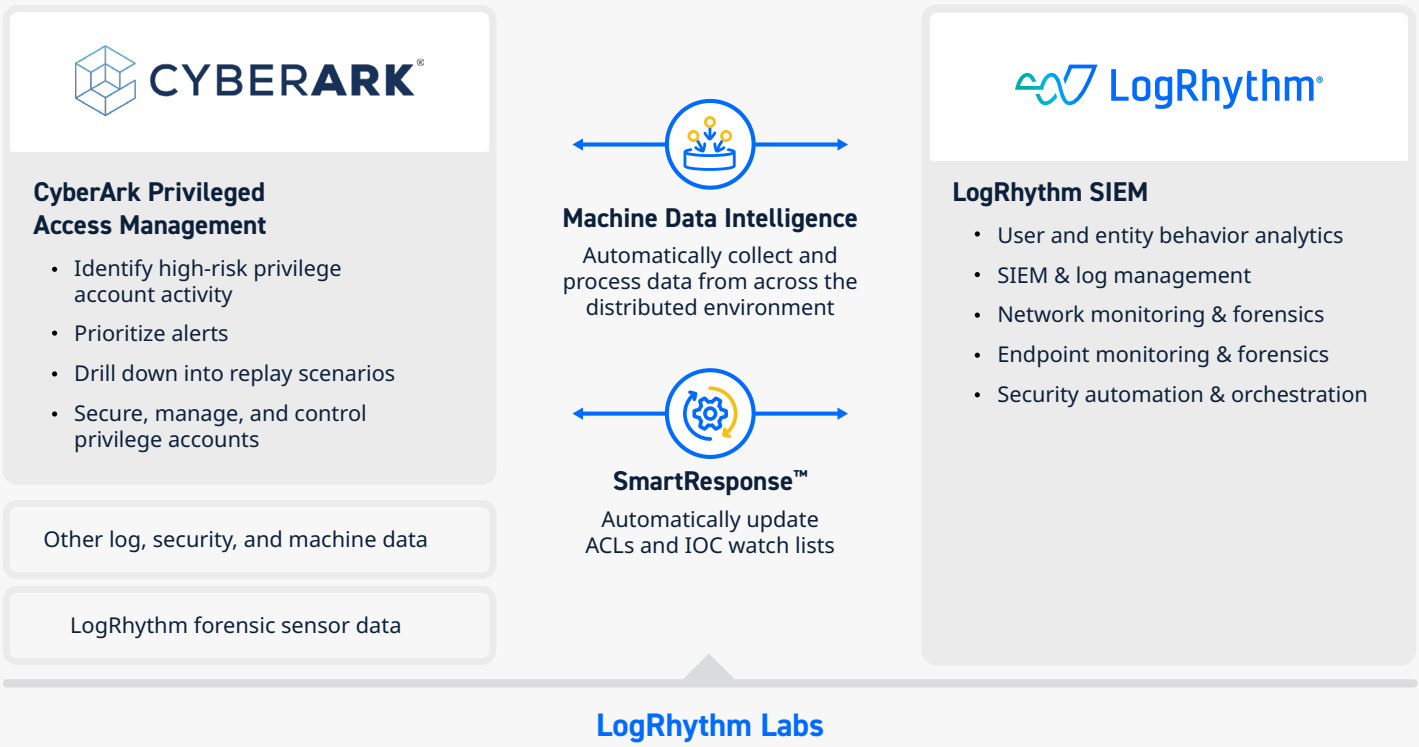
Modern organizations are digitally transforming their businesses with the use of cloud technologies and the addition of a remote workforce, increasing privileged accounts, and widening the attack surface. To protect these accounts and the critical resources to which they provide access, organizations require comprehensive controls to effectively monitor, detect, and respond to all privileged account activity in real time. LogRhythm SIEM integrates with CyberArk to address this need. LogRhythm leverages CyberArk privileged account data to deliver more valuable insights about advanced threats targeting privileged accounts. Security teams benefit from detailed forensic evidence, including tracking and reporting on all privileged activity, meeting audit and compliance requirements.

As logs are ingested from CyberArk Private Access Management (PAM) into the LogRhythm SIEM platform, the LogRhythm SmartResponse™ for CyberArk can automatically disable a user when their activity is suspicious and needs further investigation. The security administrator can also lower a user account security policy during an investigation to reduce privileged access.

CYBERARK

About LogRhythm and CyberArk

LogRhythm and CyberArk work together to help organizations increase visibility and protect against modern cyberattacks. The combined solution empowers security teams to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence. LogRhythm and CyberArk empower security teams to navigate a changing threat landscape with confidence.



Log Collection

Securing any security operations center (SOC) begins with high-fidelity and trustworthy log data. While other vendors outsource their log collection methodology to the SOC analyst, LogRhythm provides log sources reviewed by dedicated security experts with dozens of years of security experience. LogRhythm Machine Data Intelligence (MDI) Fabric optimizes and stabilizes the ideal route of collection for over 950 log sources. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts that allow for precision rule creation and comprehensive remediation efforts in the event of an attack. Privileged activity alerts from CyberArk Privileged Threat Analytics (PTA) are sent to LogRhythm. The alerts are then correlated with other real-time data collected from the organization.

The LogRhythm and CyberArk integration includes Common Event Format (CEF) Syslog to detect common attack patterns.

How It Works

CyberArk PAM secures, isolates, controls, and monitors privileged user access and activities to critical Unix, Linux, and Windows-based systems, databases, virtual machines, network devices, mainframes, websites, SaaS applications, cloud consoles, and more. LogRhythm ingests the privileged data and application security logs. The data is incorporated by LogRhythm into automated advanced correlation rules to deliver highly focused alerts that identify when an organization is experiencing privileged access threats and/or suspicious activity is occurring within their environment. Normalized data is used for analysis storage and reporting, via a consolidated dashboard.

How Automated Workflows Work

To streamline security response workflows, organizations can use SmartResponse automation. LogRhythm SmartResponse accelerates response to cyberthreats to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the LogRhythm SmartResponse for CyberArk.

The LogRhythm SmartResponse for CyberArk contains multiple actions, which are configured to execute automatically in response to an alarm, or manually through analyst workflow. For example, if a user account is suspected of being compromised, it can be automatically disabled to reduce the risk of further compromise and to allow for investigation. LogRhythm SmartResponse centralizes functionalities of manual and automated actions between LogRhythm SIEM and CyberArk.

SmartResponse™ Automated Actions for CyberArk

Action	Description	Use Case
Account History	Displays CyberArk credential access details for a target account during a specific period	Display contextual information about a specified user account, such as user, action performed, and reason given
Disable User	Disables CyberArk user	Disable user account for further investigation
Enable User	Enables CyberArk user	Re-enables a user after investigation
Force Credential Change	Changes password immediately	Forces password rotation of a CyberArk account
Lower Account Security Policy	Drops an account down to the next lowest security policy listed in the policySecuritySets parameter	Lower the account's security policy, preventing more privileged user access
Raise Account Security Policy	Raises an account up to the next highest security policy listed in the policySecuritySets parameter	Temporarily moves an individual account to the more restrictive security platform so it can perform specific tasks

For more information, request a LogRhythm demo.

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 300 // +65 6222 8110 // +61 2 8019 7185 // +97155 642 2224

www.logrhythm.com