LogRhythm

Joint Solution Brief

SecureAuth

Combining the LogRhythm SIEM platform and SecureAuth for integrated identity and access management security

Benefits

- **Discover dangerous user-based activity:** Improve overall security posture by detecting misused credential behavior where the majority of breaches occur
- **Embed security orchestration:** Streamline response process with automation
- **Detect known and unknown threats:** Apply full-spectrum analytics to uncover unexpected authentication attempts
- **Attain visibility:** Uncover all aspects of user, network, and endpoint behavior activity throughout the IT environment

Solution Overview

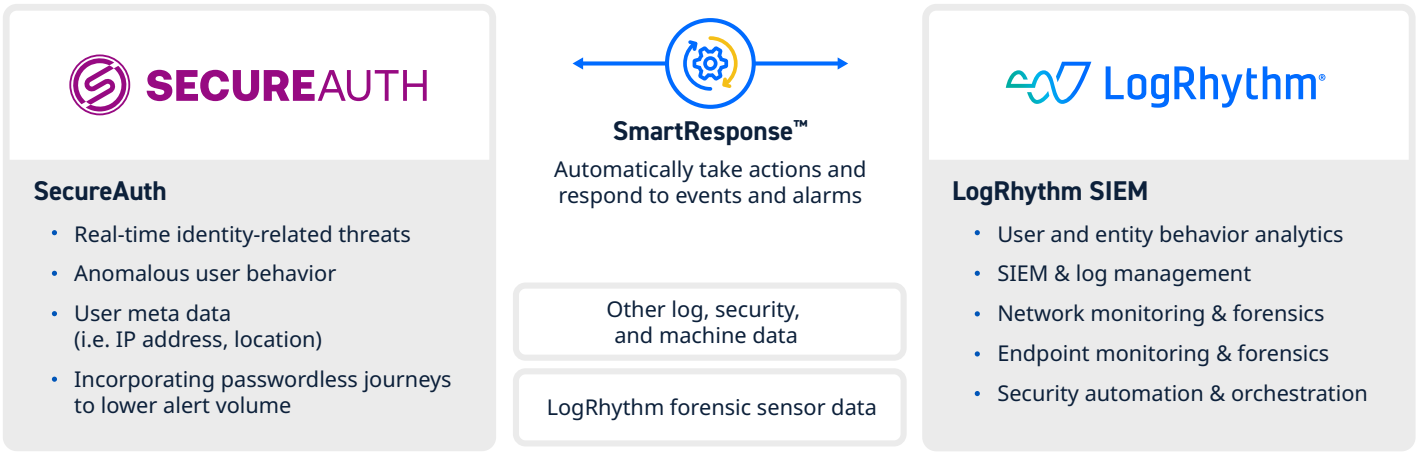
LogRhythm and SecureAuth have developed an integrated solution for comprehensive enterprise security protection, intelligence, and threat management. The LogRhythm SIEM platform, along with LogRhythm's user and entity behavior analytics (UEBA), employs diverse and complementary analytical methods, including scenario- and behavioral-based analytics, to automatically incorporate authentication workflow data imported directly from SecureAuth, delivering real-time cyberthreat protection based on up-to-date situational awareness and comprehensive security analytics. This allows for profiling and advanced anomaly detection across the full spectrum of threats.

Combining the value of best-in-class identity and access management with the threat management capabilities of the LogRhythm SIEM platform allows LogRhythm and SecureAuth to be tightly integrated. The combined offering empowers customers to identify behavioral anomalies, insider threats, external threats, and to prioritize their responses based on accurate enterprise security intelligence.

SECUREAUTH

About LogRhythm and SecureAuth

LogRhythm and SecureAuth work together to help organizations around the globe increase network visibility and protect against modern cyberattacks, as the majority of breaches involve misused credential data. LogRhythm offers extensive support for and integration across SecureAuth's IAM product portfolio. The combined solution empowers security teams to identify behavioral and authentication anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence. LogRhythm and SecureAuth empower security teams to navigate a changing threat landscape with confidence. Together, LogRhythm and SecureAuth help you achieve your Zero Trust initiatives.



Cyber Threat Intelligence Collection

The LogRhythm SIEM platform ingests accurate authentication data collected by SecureAuth, so customers experience advanced enterprise security intelligence and threat management capabilities. The combination delivers the ability to monitor and secure a range of systems and applications throughout customers' IT environments, helping them respond to security threats based on accurate, relevant, and up-to-date information. SecureAuth and LogRhythm work together to provide identity and access management, secure workforces and customer identities in the cloud, hybrid, and on premises.

LogRhythm ingests real-time authentication data shared by SecureAuth to alarm when suspicious or unauthorized authentication meets preset thresholds/conditions. By sharing normalized authentication data for a given environment, SecureAuth allows the LogRhythm SIEM platform to identify anomalies that can be correlated among identity, network, and endpoint threat data. This allows customers to save time and resources by focusing security personnel on alerts that matter.

How It Works

Customers can configure alerts specific to their needs, providing real-time alerting, which is then ingested by LogRhythm SIEM. Based on the customer's configurations and normalized authentication data, LogRhythm can incorporate data from SecureAuth into automated advanced correlation rules to deliver highly focused alerts that identify authentication failures and/or suspicious activity occurring within the environment.

How Automated Workflows Work

Threat intelligence data regarding identity and access management is continually imported from SecureAuth into LogRhythm for immediate recognition of user/entity, network, and endpoint behavior involving malicious sources, emerging threats, and indicators of compromise. This provides deep forensic visibility into activity to and from threatening IPs, URLs, and domains that have been identified by SecureAuth allowing for the delivery of operational threat intelligence to customers' security controls for real-time blocking and monitoring.

To streamline security response workflows, organizations can use LogRhythm SmartResponse™, which is part of LogRhythm's security orchestration, automation, and response (SOAR) solution. LogRhythm SmartResponse accelerates response to suspicious or unauthorized authentication requests to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the LogRhythm SmartResponse for the SecureAuth integration. While LogRhythm has a dedicated engineering team that builds actions, this is by nature, an open framework that enables SecureAuth customers to modify actions or write their own custom integrations.

The LogRhythm SmartResponse for SecureAuth contains multiple actions that are configured to execute automatically in response to an alarm or manually through analyst workflow. Each action can also be configured to require approval before execution.

SmartResponse Automated Actions for SecureAuth

Action	Description	Use Case
Create Configuration File	Execute this action and rerun it before using the plugin's other available actions whenever the fixed-value parameter is changed	Functionality must run first before other LogRhythm SmartResponse functions can be executed
Pull Account History	Pulls account history of specified user	Allows analyst to pull account history of a specified user
Add User to Group	Adds user to a specified group	Allows addition of a user to a group
Change a Directory Property	Changes a specified property of a given directory	Allows a directory property to be changed for use in Risk Score analysis
Reset Password	Resets the password of a specified user account	Allows password to be reset for a specified user account

For more information, request a LogRhythm demo.
logrhythm.com/schedule-online-demo

info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 330 // +65 6222 8110 // +61 2 8019 7185

www.logrhythm.com