LogRhythm

Data Sheet

LogRhythm SIEM

Gain unmatched visibility, protection, and threat detection across all surface areas, systems, and assets

For organizations that require a self-hosted solution (either on-premises or in the cloud that is managed by a customer or partner) due to regulatory requirements or IT preference, LogRhythm SIEM is the industry's most complete platform, providing the latest security functionality and analytics. LogRhythm SIEM offers embedded modules, dashboards, and rules that help you quickly deliver on the mission of your security operations center (SOC): threat monitoring, threat hunting, threat investigation, and incident response at a low total cost of ownership.

LogRhythm SIEM streamlines incident investigation and response through a visual analyst experience. Analysts see an entire security story about a user or host helping your team quickly investigate and respond to threats. LogRhythm SIEM provides the details you need to investigate and shut down attacks before serious damage occurs.

LogRhythm supports a multitude of collection mechanisms. LogRhythm features a JSON parsing engine embedded within LogRhythm's System Monitor (SysMon), the SIEM's collection mechanism. The engine, which is compatible with LogRhythm version 7.13 and later, ingests cloud-native log sources significantly faster and can collect thousands of messages per second. LogRhythm offers unlimited System Monitors, making scaling easy and at no additional cost.

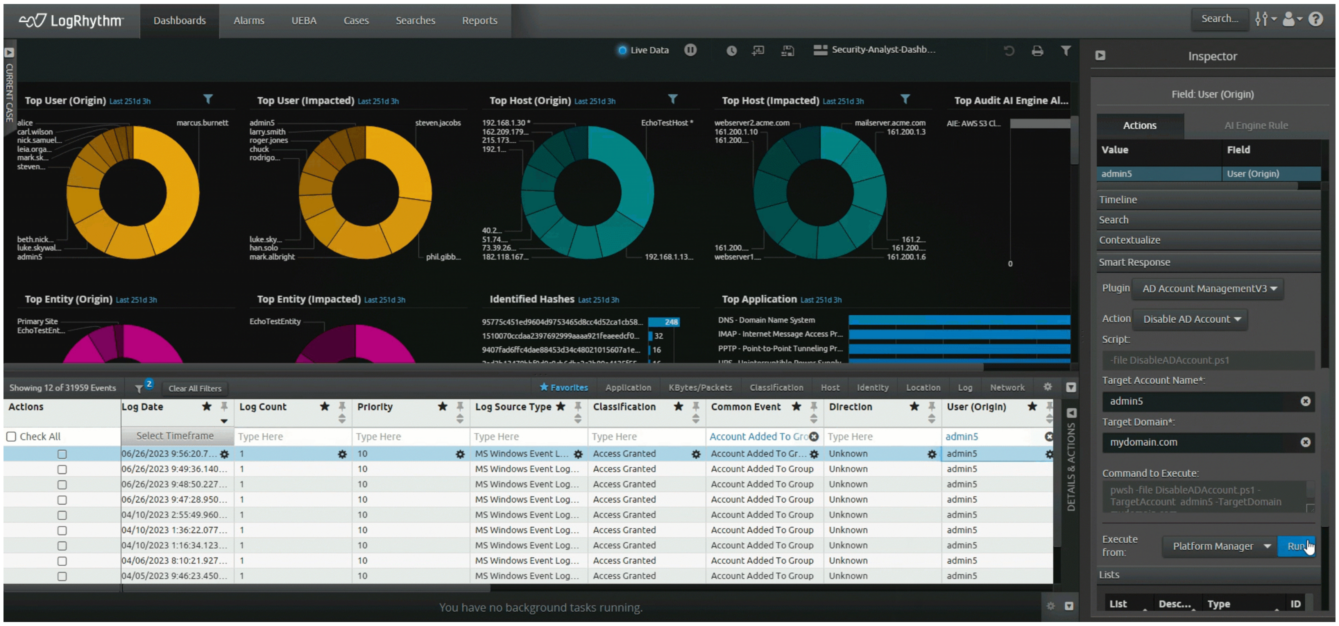
Benefits

- **Gain Greater Visibility:** Search across important log data to understand what's happening across your environment
- **Automate Detections of Attacks:** Use LogRhythm's embedded SOAR and SmartResponse™ automated responses and playbooks to shut down attacks and limit damage and disruption
- **Reduce Detection and Response Time:** Combine machine learning, machine data intelligence, and search analytics to reduce the time it takes to discover threats
- **Demonstrate Regulatory Compliance:** Leverage LogRhythm's out-of-the-box content to map your compliance and regulatory needs

Out-of-the-box Capabilities

LogRhythm SIEM simplifies work and decreases mean time to detect (MTTD) and mean time to respond (MTTR) by enabling security operations across the threat lifecycle.

- **Collect**: Gather, normalize, and interpret data from more than 1,000 third-party products and cloud sources.
- **Normalize:** Translate and contextualize complex data into simple language upon ingestion with LogRhythm's Machine Data Intelligence (MDI) Fabric, enabling analysts to focus on security, not configuration of the SIEM.
- **Qualify**: Use prebuilt threat analytics, Threat Intelligence Service feeds, and risk-based prioritization to focus your efforts.
- **Investigate**: Leverage LogRhythm's powerful Web Console to investigate alarms and threat hunt with built-in collaboration (case) tools.
- **Detect**: Choose from over 1,100 preconfigured, out-of-the-box correlation rule sets and use a wizard-based drag-and-drop GUI to create and customize rules for your environment.
- **Neutralize**: Leverage community and custom LogRhythm SmartResponse™ automated actions to perform common tasks such as block an IP on a firewall or disable a user account and automated playbooks to shut down an attack.
- **Recover**: Leverage threat intel to detect if the threat returns or left a back door; apply lessons learned to bolster defenses.
- **Comply**: Streamline the compliance process with our Consolidated Compliance Framework that provides reporting for dozens of regulations.
- **Maintain**: Obtain bi-weekly Knowledge Base updates and receive regular improvements and additions to log sources, detections rules, and other important content.


LogRhythm
Dashboards
Alarms
UEBA
Cases
Searches
Reports
Search...
Live Data
Security-Analyst-Dashb...
CURRENT CASE
Top User (Origin) Last 251d 3h
Top User (Impacted) Last 251d 3h
Top Host (Origin) Last 251d 3h
Top Host (Impacted) Last 251d 3h
Top Audit AI Engine Al...
Top Entity (Origin) Last 251d 3h
Top Entity (Impacted) Last 251d 3h
Identified Hashes Last 251d 3h
Top Application Last 251d 3h
DNS - Domain Name System
IMAP - Internet Message Access Pr...
PPTP - Point-to-Point Tunneling Pr...
Favorites
Application
KBytes/Packets
Classification
Host
Identity
Location
Log
Network
DETAILS & ACTIONS

Showing 12 of 31959 Events

Clear All Filters

Actions	Log Date	Log Count	Priority	Log Source Type	Classification	Common Event	Direction	User (Origin)
☐ Check All	Select Timeframe	Type Here	Type Here	Type Here	Type Here	Account Added To Gro	Type Here	admin5
☐	06/26/2023 9:56:20.7...	1	10	MS Windows Event L...	Access Granted	Account Added To Gr...	Unknown	admin5
☐	06/26/2023 9:49:36.140...	1	10	MS Windows Event Log...	Access Granted	Account Added To Group	Unknown	admin5
☐	06/26/2023 9:48:50.227...	1	10	MS Windows Event Log...	Access Granted	Account Added To Group	Unknown	admin5
☐	06/26/2023 9:47:28.950...	1	10	MS Windows Event Log...	Access Granted	Account Added To Group	Unknown	admin5
☐	04/10/2023 2:55:49.960...	1	10	MS Windows Event Log...	Access Granted	Account Added To Group	Unknown	admin5
☐	04/10/2023 1:36:22.077...	1	10	MS Windows Event Log...	Access Granted	Account Added To Group	Unknown	admin5
☐	04/10/2023 1:16:34.123...	1	10	MS Windows Event Log...	Access Granted	Account Added To Group	Unknown	admin5
☐	04/06/2023 8:10:21.927...	1	10	MS Windows Event Log...	Access Granted	Account Added To Group	Unknown	admin5
☐	04/05/2023 9:46:23.450...	1	10	MS Windows Event Log...	Access Granted	Account Added To Group	Unknown	admin5

You have no background tasks running.

Inspector

Field: User (Origin)

Actions | AI Engine Rule

Value	Field
admin5	User (Origin)

Timeline
Search
Contextualize
Smart Response

Plugin: AD Account ManagementV3
Action: Disable AD Account
Script: -file DisableADAccount.ps1
Target Account Name*: admin5
Target Domain*: mydomain.com
Command to Execute: pwsh -file DisableADAccount.ps1 -TargetAccount admin5 -TargetDomain
Execute from: Platform Manager
Run

Lists

List	Desc...	Type	ID

Figure 1: Automate repetitive tasks with LogRhythm's embedded SOAR solution.

Problems We Solve

Log Collection and Management

Swiftly search across your organization’s vast data to easily find answers, identify IT and security incidents, and quickly troubleshoot issues. LogRhythm offers a universal collection service that enables your team to collect data and store it in a single location.

Endpoint Monitoring

Fulfill security and compliance use cases by supplementing traditional log collection with rich host activity data from data collection and endpoint monitoring. LogRhythm can enhance log collection further using additional features such as file integrity monitoring (FIM), which prevents corruption of key files by identifying when and by whom files and associated permissions are created, viewed, modified, and deleted. LogRhythm also uses Registry Integrity Monitoring (RIM), which helps detect when registry keys are added, changed, or deleted assisting in the detection of persistent threats after entering the environment.

Security Analytics

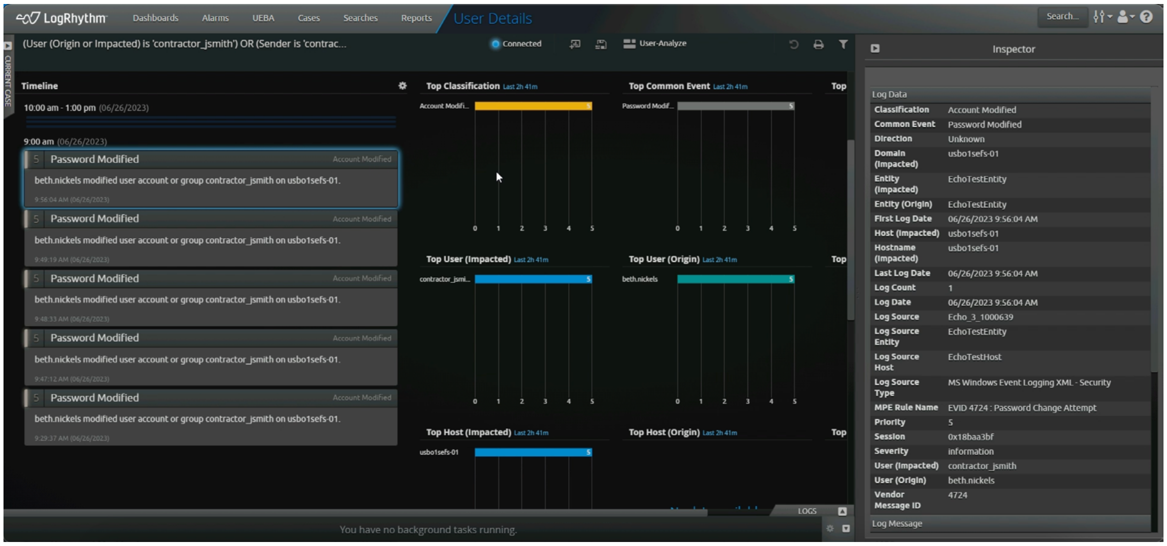
Don’t get bogged down in meaningless alarms and alarm fatigue. With advanced machine analytics, your team will accurately detect malicious activity through security and compliance use case content and risk-based prioritized alarms that immediately surface critical threats.

User Analytics

Protect against insider threats with LogRhythm’s embedded deterministic user and entity behavior analytics (UEBA) monitoring. To detect anomalies using machine learning, leverage LogRhythm UEBA, our advanced analytics UEBA solution.

Orchestration and Automation

Work smarter, not harder. Collaborate, streamline, and evolve your team’s security maturity and accelerate your team’s efficiency and productivity with security orchestration, automation, and response (SOAR) that is embedded in LogRhythm SIEM and integrates with more than 80 partner solutions. LogRhythm’s case management capabilities centralize investigations, enabling your team to easily create or escalate a case, assign a priority to individual cases, and track remediation efforts. LogRhythm SmartResponse automates a wide range of analyst tasks, increasing productivity and accelerating incident response. Through our ecosystem of trusted partners, SmartResponse automated actions deliver broader capabilities designed to satisfy your organizational needs. Choose from fully automated playbook actions or semi-automated, approval-based response actions.



(User (Origin or Impacted) is 'contractor_jsmith') OR (Sender is 'contrac...

Timeline

10:00 am - 1:00 pm (06/26/2023)

9:00 am (06/26/2023)

5 Password Modified — Account Modified
beth.nickels modified user account or group contractor_jsmith on usbo1sefs-01.
9:56:04 AM (06/26/2023)

5 Password Modified — Account Modified
beth.nickels modified user account or group contractor_jsmith on usbo1sefs-01.
9:49:19 AM (06/26/2023)

5 Password Modified — Account Modified
beth.nickels modified user account or group contractor_jsmith on usbo1sefs-01.
9:48:33 AM (06/26/2023)

5 Password Modified — Account Modified
beth.nickels modified user account or group contractor_jsmith on usbo1sefs-01.
9:47:12 AM (06/26/2023)

5 Password Modified — Account Modified
beth.nickels modified user account or group contractor_jsmith on usbo1sefs-01.
9:29:37 AM (06/26/2023)

You have no background tasks running.

Log Data

Classification	Account Modified
Common Event	Password Modified
Direction	Unknown
Domain (Impacted)	usbo1sefs-01
Entity (Impacted)	EchoTestEntity
Entity (Origin)	EchoTestEntity
First Log Date	06/26/2023 9:56:04 AM
Host (Impacted)	usbo1sefs-01
Hostname (Impacted)	usbo1sefs-01
Last Log Date	06/26/2023 9:56:04 AM
Log Count	1
Log Date	06/26/2023 9:56:04 AM
Log Source	Echo_3_1000639
Log Source Entity	EchoTestEntity
Log Source Host	EchoTestHost
Log Source Type	MS Windows Event Logging XML - Security
MPE Rule Name	EVID 4724 : Password Change Attempt
Priority	5
Session	0x18baa3bf
Severity	information
User (Impacted)	contractor_jsmith
User (Origin)	beth.nickels
Vendor Message ID	4724

Log Message

Figure 2: LogRhythm’s prebuilt content and built-in incident management tools help you find answers quickly so you can focus on what matters.

How We Help

LogRhythm has assembled the world's most capable and respected ecosystem of people and partners to help your team build a resilient defense at the cutting edge of cyber technology.

LogRhythm Labs

Nobody understands adversaries better than we do. Our LogRhythm Labs team proactively analyzes emerging threats from all corners of the web and builds rules, dashboards, reports, and compliance modules to give your organization the upper hand.

Security Maturity

With two decades of experience in cybersecurity, LogRhythm brings together the most complete technology to help you improve your security posture. With our Security Operations Maturity Model (SOMM), we help you set a baseline and then we create a plan to achieve your security goals together.

Preferred by Security Pros

Most cybersecurity tools are complicated, clunky, and frustrating to use. LogRhythm SIEM is easy to set up and use, enabling analysts to quickly see the entire threat landscape and a timeline of events. We help busy and lean security teams meet security operational goals and save time.

Services to Support Your Team

When you work with LogRhythm, our team of experts are available to help you with your security goals. We offer targeted services to help you achieve expert-level status and improve your organization's security maturity.

The LogRhythm-powered SOC includes our SIEM solution and security use case content from LogRhythm Labs, all supported by the real-world expertise of our Customer Success team.

Request a demo today: logrhythm.com/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