# ←√7 LogRhythm<sup>•</sup>

#### 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.

# **Open Collection Architecture**

LogRhythm supports a multitude of collection mechanisms. LogRhythm's Open Collection Architecture features a JSON parsing engine embedded within LogRhythm's <u>System Monitor</u> (<u>SysMon</u>), the SIEM's collection mechanism. The engine 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.

In addition, LogRhythm SIEM opened the System Monitor Agent's JSON listener to receive JSON logs from any source using the Lumberjack protocol. This enables security teams to gather crucial security logs from sources not natively supported by LogRhythm and tailor out-of-the-box and custom normalization rules.

### 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 <u>Machine Data Intelligence (MDI) Fabric</u>. Our proprietary MDI Fabric makes data actionable for AI-driven organizations, 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-ofthe-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<sup>™</sup> 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.

					🙆 Live Data 🛛 🛈	0 5 5 =	Security-Analyst-Dashb					
						● + =				Inspector		
Top User (Origin	1) Last 251d 3h 🛛 🕇	Top User (impacte	<b>d)</b> Lest 251d 3h	Top Host (Origin) Las		Top Host (Impacted)		Top Audit AI Eng	ine Al	Field: User (Origin)		
ice Irl wilson	marcus.burnett	admin5	stevenjacobs	192.168.1.30* 162.209.179 215.173 192.1_	EchoTestHost*	webserver2.acme.com 161.200.1.10	mailserver.acme.com 161.200.1.3	AIE: AWS S3 CL	A	ctions Al Engine Ru		
rLwitson ck.samuel ia.orga		larry.smith roger.jones chuck				161.200.1.10			Value	Field		
mark.sk. steven		rodrigo_							admin5			
									admins	i User (Origin)		
h.nick		luke.sky		402.51.74		161.20161.20161.20161.20161.20161.200161.20016				Contextualize Smart Response		
e.skywal nin5		han.solo mark.albright	- phil.gibb	73.39.26	192.168.1.13_				Smart F			
Top Entity (Origin) Last 251d 3h Top Entity (Impacted) Last 251d 3h			ed) Last 251d 3h	Identified Hashes Last 251d 3h		Top Application Last 251d 3h				Plugin AD Account ManagementV3 -		
nary Site oTestEnt		EchoTestEntity		95775c451ed9604d9753465d8 1510070ccdaa2397692999aaa 9407fad6ffc4dae88453d34c48	a921feaeedcf0 32 3021015607a1e 16	DNS - Domain Name System IMAP - Internet Message Access PPTP - Point-to-Point Tunneling	g Pr		Script:	Disable AD Account		
mary Site hoTestEnt ving 12 of 31959 Eve	ents 7 <sup>2</sup> Clear All Filters	EchoTestEntity		1510070ccdaa2397692999aaa 9407fad6ffc4dae88453d34c48 2-d35 t347555 fodo-o-t-c45-3	a921feaeedcf0 32 3021015607a1e 16	IMAP - Internet Message Access PPTP - Point-to-Point Tunneling	g Pr	n Log Network	Script: -file I			
ing 12 of 31959 Eve	ents Y <sup>2</sup> Clear All Filters Log Date <b>*</b>	EchoTestEntity	Priority *	1510070ccdaa2397692999aaa 9407fad6ffc4dae88453d34c48 a-d3L+3-278LL50-d0-d-2-d-L-3 <b>*</b> Favorite	a921feaeedcf0 32 3021015607a1e 16	IMAP - Internet Message Access PPTP - Point-to-Point Tunneling URE Uninterconstitute Researching Packets Classification H	g Pr	Log Network User (Origin)	Script: -File I Target admit	DisableADAccount.ps1 : Account Name*: InS		
ng 12 of 31959 Eve			Priority *	1510070ccdaa2397692999aaa 9407fad6ffc4dae88453d34c48 943543578556545634574555 * Favorite	a921feaeedd0	IMAP - Internet Message Access PPTP - Point-to-Point Tunneling URE Uninterconstitute Researching Packets Classification H	ppr dost Identity Location Direction ★ ∓		Script: -File I Target admit	DisableADAccount.ps1 :Account Name*: InS :Domain*:		
oTestEnt	Log Date \star 🖡 🗸	Log Count *	Type Here	1510070ccdaa2397692999aaa 9407fad6ffc4dae88433d34c48 24 db 127784684943d34c48 <b>★ Favorite:</b> Log Source Type <b>★</b>	#921feaeedd032 1021015607a1e16 #5 Application KBytes/# Classification ★ # ↓ Type Here	IMAP - Internet Message Access PPTP - Point to Point Tunneling INC - Internet Message Access Packets Classification H Common Event ★ # \$	itost Identity Location	User (Origin) 🕇	Script: -File I Target d Target	DisableADAccount.ps1 : Account Name*: InS		
ing 12 of 31959 Eve ons eck All	Log Date \star 🖡	Log Count * T Type Here 1 *	Type Here	1510070ccdaa2397692999aaa 9407faddffcdae84351314c48 ★ Eavoritee Log Source Type ★ ∓ ↓ Type Here	#921feaeedd032 1021015607a1e16 #5 Application KBytes/# Classification ★ # ↓ Type Here	IMAP - Internet Message Access PPTP - Point to Point Tunneling URC - Italitaterwithtis Ammedia eackets Classification H Common Event * Account Added To Circ. Account Added To Circ.	itost Identity Location	User (Origin)	Script -file Target admi Target Target Target Target Goup Myda	DisableADAccount.ps1 :Account Name*: InS :Domain*:		
ing 12 of 31959 Eve ins eck All	Log Date *	Log Count * T Type Here 1 *	Type Here	1510070ccda2237692299aaa 9407faddfredae843334c48 >407faddfredae843334c48 > <b>★ Favorite:</b> Log Source Type ★ ∓ ↓ Type Here ★ MS Windows Event L ◆	#921/fexeedd032 1921015607a1e16 stansurferr Classification KBytes// Type Here Access Granted ✿	IMAP - Internet Message Access PPTP - Point to Point Tunneling TIPS - Holeswitch Point Cunneling TIPS - Holeswitch Point Con- access Classification H Common Event * * Account Added To Gr. * Account Added To Group	pr	User (Origin) 🕈 admin5 admin5	Script - file I Target C SNO C SN	DisableADAccount.ps1 Account Name*: n5 Domain*: Domain com and to Execute:		
ng 12 of 31959 Eve ns eck All	Log Date # # Select Timeframe 06/26/2023 9:56:20.7 & 06/26/2023 9:49:36.140	Log Count ★ 🖡 Type Here 1 t	Type Here 10 10 10 10 10	1510070ccda2397692999aaa 94077addfcdae8833334c4	#221/GaeeddO32 922/01/SeCTate16 ** Application KBytes// Classification ★ # Type Here Access Granted Access Granted	IMAP - Internet Message Access PPTP - Point to Point Tunneling Inc Internet Message Access access Classification H Common Event # 4 Account Added To Croc Account Added To Croup Account Added To Croup	pr	User (Origin) admin5 admin5 admin5	Script: -file I admit C C C mmwde C C C mmwde C C C mmwde S C C C mmw	DisableADAccount.ps1 Account Name*: InS Domain*: oomain.com		
ng 12 of 31959 Eve ns eck All	Log Date # Select Timeframe 06/26/2023 9:56:20.7 06/26/2023 9:49:36.140 06/26/2023 9:48:50.227	Log Count * *	Type Here 10 10 10 10	Storrectube39709299eas 940774d6ffc4dae8845534c48 ★ Eavoritee Log Source Type ★ ∰ Type Here ★ MS Windows Event Log MS Windows Event Log	a921/faseedd032 B0210/S07a1e16 IS Application KBytes// Classification ★ Type Here Access Granted Access Granted	MAP- Index of Market Seage Access PPTP- Point to Point Turneling Common Event * * Account Added To Group Account Added To Group Account Added To Group	pr	User (Origin) admin5 admin5 admin5 admin5 admin5	Script: - file I - file	DisableADAccount.ps1 Account.Name*: n5 Domain*: omain com and to Execute: - file DisableADAccount.ps1 -		
ng 12 of 31959 Eve ns eck All	Log Date # Select Timeframe 06/26/2023 9:45:620.7 06/26/2023 9:49:36.140 06/26/2023 9:49:30.227 06/26/2023 9:47:28.950	Log Count * T Type Here 1 * 1 1 1	Type Here 10 10 10 10 10	1510070xcdax2397692999aas 9x07rdoff cdaxedis351vcda	Application KBytes/file Application KBytes/file Application KBytes/file Access Granted Access Granted Access Granted Access Granted	MAP-Internet Message Access PPTP- Pont 5-Part 5-Part 1- Common Event * 4 Account Added To Crow Account Added To Crow Account Added To Crow Account Added To Crow Account Added To Crow	pr tost Identity Location Direction ★ ∓ Type Here Unknown Unknown Unknown	User (Origin) admin5 admin5 admin5 admin5 admin5 admin5	Script - file I admi admi Target C C C C C C C C C C C C C	DisableADAccount.ps1 Account.Namet: n5 Domaint: omain.com and to Execute: - file DisableADAccount.ps1 - - file DisableADAccount.ps1 - etAccount.admin5 -TargetDomai		
ng 12 of 31959 Eve ns eck All	Log Date Select Timeframe 06/26/2023 9:45:62.07 & 06/26/2023 9:49:36.140 06/26/2023 9:47:28 9:50.27 06/26/2023 9:47:28 9:50.28 04/10/2023 2:55:49.960	Log Count * # Type Here 1 * 1 1 1 1 1	Type Here 10 <b>%</b> 10 10 10 10 10 10	tStollovch&z37/0259044 storfieldsKebsStated ★ Pavorite Log Source Type ★ ▲ Type Here MS Windows Event Log MS Windows Event Log MS Windows Event Log	with reserved on 32 biologona 16 classification * & Type Here Access Granted Access Granted Access Granted Access Granted	MAP: Holment Message Access PPTP- Pacito Basic Luncing Information Control Account Added To Croup Account Added To Croup	pr tot: Identity: Location Direction ★ ∓ Type Here Unknown Unknown Unknown Unknown	User (Origin) admin5 admin5 admin5 admin5 admin5 admin5 admin5	Script- Anter Target admi SNOLD V STIPLIO Comm Pyski Target Comm Dyski Target Comm SNOLD V STIPLIO Comm Dyski Target Comm Dyski Target Comm Dyski Target Comm Dyski Target Comm Dyski Target SNOLD V STIPLIO Target SNOLD V STIPLIO Target Comm Dyski Target SNOLD V STIPLIO SNOLD V STIPLIO	DisableADAccount.ps1 Account.Namet: n5 Domaint: omain.com and to Execute: - file DisableADAccount.ps1 - - file DisableADAccount.ps1 - etAccount.admin5 -TargetDomai		
ng 12 of 31959 Even ns eck All	Log Date Select Timeframe 06/26/2023 9-56:20.7 06/26/2023 9-49:36:140 06/26/2023 9-47:80:50 06/26/2023 9:47:80:50 04/10/2023 1:36:22.077	Log Count * # * * Type Here 1 * 1 1 1 1 1 1	Type Here 10 * 10 10 10 10 10 10 10 10	15100rccdb27/0229904 \$407667/64064555144 \$407667/64064555144 \$407667/64064555144 \$4076777 \$4076777 \$4076777 \$4076777 \$4076777 \$4076777 \$4076777 \$40767777 \$40767777 \$40767777 \$407677777 \$4076777777 \$40767777777 \$407677777777777777777777777777777777777	w2716aeedda 22 W201567742 16 Classification * Type Here Access Granted Access Granted Access Granted Access Granted	MAP. Holmes Messep Access PPTP: Point to Point an Annual Common Event * Common Event * Common Event * Common Event * Comp Account Added To Group Account: Added To Group	pp tost Identity Location Direction ★ Type Here Unknown Unknown Unknown Unknown Unknown Unknown	User (Origin) admins admins admins admins admins admins admins	Script - file I admi admi Target C C C C C C C C C C C C C	DisableADAccount.ps1 Account Namet: n5 Domain*: omain.com and to Execute: -file DisableADAccount.ps1 - -telecount.admin5 -TargetDomain incomains		

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.

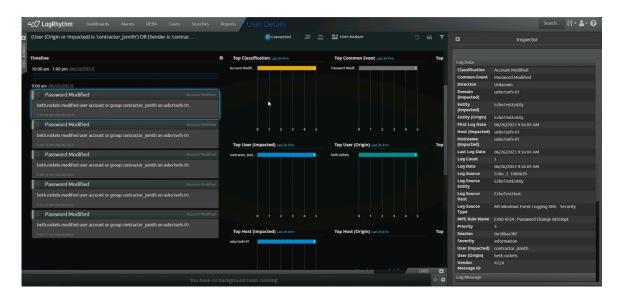


Figure 2: LogRhythm's prebuilt content and incident management workflow.

# 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 <u>LogRhythm Labs</u> 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 <u>Security Operations Maturity Model (SOMM)</u>, 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 <u>targeted services</u> 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.





info@logrhythm.com // 1.866.384.0713 // +44 (0)1628 918 300 // +65 6222 8110 // +61 2 8019 7185 // +97155 642 2224 © LogRhythm Inc. | DS245524-06 www.logrhythm.com