LogRhythm

Solution Brief

Services for Customer Success

There is a lot riding on the shoulders of your security operations team — protecting the organization's reputation, safeguarding sensitive client information, and ensuring the organization's ability to deliver products and services. Our Services team can help you safeguard your mission-critical systems with expert support, guidance, and expedited onboarding to realize a faster time to value and to supplement any talent gaps in your team.

LogRhythm Services empower your team to:

- Obtain rapid results with services that will get you operating efficiently; from onboarding log sources to security analytics to incident management, we'll help you ensure your environment is secure by enabling seamless threat detection, investigation, and response
- Discover best practices while taking advantage of the knowledge base of expert consultants
- Design use cases specific to your business needs or lean on our expert recommendations to get the most value out of your deployment

We're your trusted partner to help you achieve your goals, and that starts with a strong, expedited deployment followed by consistent enablement and iterative content development. Our consultants will use their experience to rapidly bring your systems onboard and enable your team to seamlessly take on daily operations. If you require additional support in building your platform outside of the initial launch and self-guided resources, our Services team is here to help you accelerate deployment and content development based on your requirements and use cases.

Benefits

- **Quick Deployment and Onboarding:** Expert support and guidance will enable you to rapidly ensure your SIEM platform is fully optimized
- **Execute Seamlessly:** Deploy the platform, easily implement use cases that are specific to your company, and train your employees quickly
- **Flexible Options:** Self-guided training along with hourly and recurring services help you gain a faster time to value; choose what works best for your business

Service Tiers

Specialized service options to meet evolving business requirements

Standard Success

Our LogRhythm experts will guide you through setting up your log sources, help customize your dashboards, searches, and reports, and create use cases specific to your organization. We'll keep you security-focused through threat hunting consultation, building analytics rules, and streamlining incident response through case management to further strengthen your security operations program. In addition, explore self-guided resources such as online training, videos, and community advice.

LogRhythm Axon: Included with your license, you will receive two onboarding sessions and three months of enablement with weekly meetings to help you get started with confidence.

LogRhythm SIEM: For simple architectures*, you will receive our standard configuration and deployment of your system, followed by enablement sessions every other week to continue building your skills and developing use case content. We will also upgrade your system with each quarterly release.

Enhanced Success

Enhanced Success expands on the value of Standard Success with increased access to your consultant. Tap into our team's expertise to refine your goals and create a 360-degree view of your environment. As your team encounters challenges or new feature releases, our consultants will be there to support you and present best practices to keep your team focused on outcomes.

LogRhythm Axon: Extends your weekly enablement sessions beyond the three-month trial period.

LogRhythm SIEM: Includes configuration, deployment, and quarterly upgrades for distributed architectures* and increases the frequency of your enablement sessions to weekly.

Signature Success

Signature Success is a comprehensive service that takes Enhanced Success to the next level by providing clients with a more expansive and well-rounded approach to security. Our team of experts work tirelessly to ensure that we deliver the highest quality services, including maturity assessments, collection architecture guidance, audit readiness preparation and LogRhythm SIEM/Cloud to LogRhythm Axon migrations. These added services aid you in maintaining a secure environment while also building a mature security operation. Our Signature Success consultants are available to meet with you several times per week, providing a flexible schedule that accommodates your needs.

LogRhythm Axon: Extends your weekly enablement sessions beyond the three-month trial period and increases the frequency and flexibility of your sessions.

LogRhythm SIEM: Includes configuration, deployment, and quarterly upgrades for enterprise architectures* and increases the frequency of your enablement sessions to weekly.

Deployment Sizing	Simple*	Distributed*	Enterprise*
Core Systems (XM, PM, DP, DX, WC)	Up to 8	Up to 8	Up to 25
Sensors (SMA, OC, NetMon)	Up to 20	Up to 20	Up to 20
Redundancy	—	HA or DR	HA and/or DR
Dark Site Environments	—	Supported	Supported
FIPS Environments	—	—	Supported

Success Service Packaging

		Product Restrictions	Standard Success	Enhanced Success	Signature Success	Professional Services
			Consistent Programs Throughout the Term			Accelerate Specific Scope
Foundation	Customer Success Manager		✓	✓	✓	✓
	LogRhythm Community & Documentation		✓	✓	✓	✓
	Product Coaching		✓	✓	✓	✓
	Deployment & Onboarding	Axon	✓	✓	✓	✓
		SIEM	Simple	Distributed	Enterprise	✓
	Upgrades & Health Checks	SIEM	Simple	Distributed	Enterprise	✓
	Ad Hoc Consulting	SIEM		2 Days Per Year	5 Days Per Year	
Discover	Agent Deployment		✓	✓	✓	✓
	Log Source Onboarding		✓	✓	✓	✓
	Custom Processing Policies		✓	✓	✓	✓
	Saved Search		✓	✓	✓	✓
	Dashboards		✓	✓	✓	✓
	Reports		✓	✓	✓	✓
Defend	Log Source Gap Analysis		✓	✓	✓	✓
	Security Use Case Development		✓	✓	✓	✓
	Response Playbooks	SIEM	✓	✓	✓	✓
	Compliance		✓	✓	✓	✓
	Threat Hunting Enablement & Coaching		✓	✓	✓	✓
	Custom Rule Validation with Echo		✓	✓	✓	✓
Grow	Security Operations Maturity Assessments				✓	✓
	Growth Roadmap Development				✓	✓
	Architecture Design				✓	✓
	Audit Readiness Assessment & Prep				✓	✓
	Support Monitoring & Escalation				✓	
Enable	Self-paced On Demand Courses		$	$	✓	$
	Instructor-Led Courses, Virtual and In-Person				✓	
	Learning Lab Access				✓	
	Role-based Learning Paths & Certifications				✓	
	LogWars Access				✓	
Logistics	Schedule	Axon	Weekly	Weekly	Weekly + Ad Hoc	Defined by SOW and PMO
		SIEM	Every Other Week			
	Duration	Axon	3 Months	6-36 Months	6-36 Months	Defined by SOW and PMO
		SIEM	6-36 Months			

✓ Included with Subscription $ Available Add-on ✓ Scope for Accelerated Delivery

Accelerate Specific Scope

Professional Services

Access specialized resources to help jumpstart a specific need for your company. LogRhythm will configure agents, onboard log sources, enable security analytics, and implement reports, lists, dashboards, custom content, and LogRhythm SIEM/Cloud to LogRhythm Axon migrations. Based on a statement-of-work (SOW), you can accelerate specific scope for greater vantage points into the platform for analysis.

Features

Our experts can help you with:

Agent Deployment: Set up agents and collectors to easily ingest on-premises and cloud sources.

Log Source Onboarding and Parsing: Ensure proper parsing policies and help create new policies for unidentified log sources.

Saved Search: Build out business specific searches to execute on-demand or run as a scheduled report.

Dashboards: Customize widgets and dashboards based off your business needs for security visibility and analysis.

Reports: Create and save reports that identify and track pertinent security information which can run ad-hoc or on a scheduled basis.

Security Analytics: Surface the most pertinent threats to your business by building out-of-the box and custom analytics rules.

Use Case Development: Achieve your business and security objectives by developing use cases that are specific to your organization's goals.

Threat Hunting: Learn how to combat the most pertinent and latest cybersecurity threats specific to your environment. We'll help guide you through best practices to continuously monitor and respond to threats.

Case Management: Automate incident response by prioritizing your security operations center (SOC) team's processes through investigation workflows, automatic creation of cases from analytics rules, and case email notifications.

Response Playbooks: Ensure the right response activity related to surfaced threats.

Compliance: Reduce the burden of assuring and demonstrating regulatory compliance by easily deploying prebuilt reports.

Maturity Assessments: Assess your current security posture and identify opportunities for planned improvement.

Growth Planning: Identify goals and create milestones that will help you build a mature security operation.

Architecture Design: Design effective log collection strategies based off your requirements to help you be cost effective and efficient.

Audit Readiness: Get expert guidance and support to ensure you are fully prepared for your next regulatory audit, allowing you to navigate the process with confidence and ease.

LogRhythm Services Use Cases

Our Services team provides specialized resources to help jumpstart compliance reporting, workflow development, and more. Here are a few sample use cases to show how we can maximize your LogRhythm ROI and ensure your platform's success and health.

Compliance Focus

LogRhythm will setup, configure agents and log sources, and refine reports, lists, alarms, and investigations.

CIS	Center for Internet Security
NIST	800-53 and cybersecurity framework
HIPAA	Healthcare Compliance Automation Modules
CCF	LogRhythm's Consolidated Compliance Framework

Log Focus

LogRhythm will onboard log sources with built-in AI Engine rules for greater vantage points into the SIEM for analysis.

Phishing	Requires 0365 or email with IMAP protocol
Malware	Requires AV or IDS/IPS logs
Remote Desktop	Requires FW logs
Exfiltration	Requires FW, or IDS/IPS, or AV, or LogRhythm NDR, or LogRhythm UEBA

LogRhythm SmartResponse™

LogRhythm streamlines workflows supporting log sources with prebuilt SmartResponse actions.

Active Directory	Windows update and services
LogRhythm Case	Case report and management
Ticketing System	ServiceNow
Endpoint Detection/ Response (EDR)	CrowdStrike, Sophos, SentinelOne, Cybereason, Cisco AMP, and Cisco Secure Endpoint

Long-term Focus

LogRhythm will regularly feed and maintain your MITRE ATT&CK, compliance, log source, and custom Analytic Co-Pilot ransomware needs.

MITRE ATT&CK	Requires PowerShell, SysMon, and 0365
LogRhythm NDR	NDR offering
Ransomware	Astaroth, Colbalt Strike, Pass the Hash, Robinhood, TripleThreat
Ransomware IOC	BcdEdit.exe, PowerShell.exe, Vssadmin.exe, Wbadmin.exe, Wmic.exe

Contact your sales rep for more information or visit LogRhythm Services for Customer Success for additional offerings.

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