← 7 LogRhythm<sup>®</sup>

p infinigate

# LogRhythm Axon

A Cloud-Native SIEM Platform



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. When security teams are stretched to the limit, LogRhythm Axon helps lighten the load to make your life easier.

LogRhythm Axon is a cloud-native SIEM platform built for security teams that are overwhelmed by immense amounts of data and an ever-evolving threat landscape. Optimized for the analyst experience, LogRhythm Axon's powerful security analytics, intuitive workflow, and simplified incident response give analysts contextual insight into cybersecurity threats so they can reduce noise and quickly secure the environment. LogRhythm Axon reduces the burden of managing threats and the operating infrastructure, helping security teams prioritize and focus on the work that matters.

#### Benefits

- **Save Time:** An open cloud-native SIEM platform that alleviates time spent managing and maintaining infrastructure while easily integrating with other applications.
- Gain Comprehensive Visibility: Automatically collect data from SaaS, self-hosted cloud, and on-prem sources from LogRhythm's hosted collectors and on-prem agents. Metadata extraction combined with easy-to-use tools to build custom parsers ensures visibility across your environment in a centralized console.
- Find Threats Faster: Search driven widgets and an intuitive dashboard make it easier to monitor, detect, investigate, and respond to threats. Ensure threat detection engineering with the ability to test your analytics rules.
- Execute Seamlessly: Surface critical threats and secure your environment with powerful security analytics and simplified incident response. Leverage out-of-the-box content or author your own custom content.

# **Cloud-Native SIEM Made Easy**



Scalable and Open Cloud-Native SaaS Platform



Powerful Security Analytics U

Simplified Incident Response



Automatic Log Collection and Enrichment



Optimized for the Analyst Experience



## **Key Features**

#### **Open Cloud-Native SaaS Architecture**

Ease the burden of managing and maintaining infrastructure to focus on the work that matters and scale smoothly as your security operations center (SOC) grows. Designed to easily integrate with other cloud services and on-premises applications, LogRhythm Axon automatically onboards new data sources. With a cloudnative architecture, automated updates enable continuous and quick delivery of enhancements.

#### Automatic and Flexible Collection of Logs

Flexible collection of logs from SaaS, self-hosted cloud, and on-prem at the point of ingestion gives you visibility as soon as possible. Integrations from LogRhythm Axon cloud collector, LogRhythm Axon agent, and customizable API and Webhook integration ensures you have visibility into your environment.

### Unique Machine Data Intelligence (MDI) Fabric

Log data is normalized and enriched into LogRhythm Axon to uniquely improve searchability and analytics across disparate log sources. With deep intelligence into unique data source types and pre-built processing rules, MDI Fabric ensures that metadata is automatically and accurately extracted at the point of ingestion.

### Analytics Rule Builder

Leverage quality out-of-the box content mapped to the MITRE ATT&CK<sup>®</sup> framework and build your own custom threat detections based on criteria that matters to your organization. Quickly investigate suspicious activity by automatically surfacing critical threats for investigation in the LogRhythm Axon dashboard.



Figure 1: Surface the most critical threats for investigation using the analytics rule builder.

### **Analytics Rules Testing**

Enable threat detection engineering with the ability to test analytics rules to confirm rules are fine-tuned and optimized for your environment. Easily conduct red team exercises and penetration tests to check for exploitable vulnerabilities.

#### **Case Management and Alerts**

Increase SOC efficiency by automating incident response and investigation workflows through automatically creating cases from analytics rules for faster response times. Prioritize workflows by assigning threat severity levels to surface which events require immediate attention and always stay on top of case activity via the case management dashboard and email notifications.

407	LogRhythm	B Last 21 hours Search logs			# a 🦂 🌢 @ +		
	Case List			+ New Case			
ô	43 Items 💿 🛙	tm(s) Applied Clear Al					
				Lasz Updated	Searchy Duration: 15d 2th 46m		
					Constant: 01(/0223,652:58 PM Loss Upstanted: 01(/12/2023,933:11 AM		
		Tuesday Malware invation 23417 The usual tuesday reader of malware	😝 jaha anishelogitythen.com				
			😫 john an ith flog ty then com		Ourse		
		Suspicious traffic from 221.2.155.199 22475: Traffic was detected from the Enclose and threat lat.	🖨 jahn.amitheliogitythen.com		Columnary John and Milling Replacements		
		OS Credential Dumping 09/05/2023 05:10:00 PM Z 22474: clustered streeweeter	😝 john.anith@logitythen.com		john anathdiogstythen care 💿		
		OS Credential Dumping 05/05/2023 05:10:00 PM Z 2013 Credential dumping tragers a release of these passes	🖨 john.amithékogrhythen.com		Traffic was detected from the Firebol sev3 threat list. Most connections are blocked on multiple locations. Traffic is getting		
		Scheduled Task 09/05/2023 05:10:00 PM 2 22472: A scheduled task may facilitate initial or recurring ea	😝 john.smithälioptythen.com		through to the UK Demo Webconsole.		
	14 Mature	System Information Discovery 05/05/2023 05:10:00 2017: An adversely may attempt to get detailed information	😝 john unithékogstythen.com		E scratt		
		OS Credential Dumping 06/05/2023 05:10:00 PM Z 224/D: Credential dumping triggers a release of these passe	😝 john amkhildesyntythen eans				
		Scheduled Task 05/05/2023 05:10:00 FM Z 22021 A scheduled task way fastinate while is recovering on	😝 jahn anätisting tyrken sam				
		Scheduled Task 09/05/2023 05:10:00 PM 2 23402 A scheduled task may facilitate initial or recurring va-	e jaha anithdioptycher.com		Today 533 AM		
			😝 jaha anithélogitychen.com		Collaborator(s) added: john.smith@iogrhythm.com		

Figure 2: Prioritize the work that matters and improve SOC efficiency with case management.

#### **Policy Builder**

LogRhythm's Policy Builder feature only requires a few clicks to create log parsing policies for logs. Easy guided workflows help build new policies to ensure future data can be easily searched and automatically fed into visualizations.

Sample Log Message	Message Interpreter		Identification Rules Normalization Rules Common Event Rules		
"text processors": ( "array predecate": (	1		<li>Event knins+http://schemar</li>		
	1				
"Key": "username", "value": "user1"					
		🗸 🖿 System			
"Key": "host", "value": "workstation1"					
"value": "workstation1" )	1 1 1				
1	1				
"bracketed value": ( "[square]",	1				
"(curly)", "(parenthesis)",	1				
"Cangleo"	1				
Tarin 107 El Palo Allo Networks Contes EREContes IDR J & EL DR BOC Inter	1 2 2		Audit Soccess	Policy Results Proview	
browner access to a particular the				Identification Rules	
"cve": "CVE-2021-44028".	1		1087729	Normalization Rules	
"double mac":				The following are results of applyin	
"00:60.68.45.67.63.00.60.68.45.4(:92.68.0 0",				Internal Database Field	
"dsv": { "csv,guote": "field1,field2,\"field3\"",	1.1		Security	A flar	
<pre>http://www.inteldt.field2;field31; http://www.inteldt.field2;field31; http://www.inteldt.field2;field31;</pre>	Add to Identification Bules		DCE1.legrhythm.com	Result Message	
"feld1;field2;\"field3\""; "semicolon sick"; "field1;field2;field3";	Add to Normalization Rules			Vendor Message ID	
"colon_quose": "field1:field2:\"field3\"", "colon_tick": "field1:field2:field3",	Add to Common Event Rules				
"pipe_quete": "field1[field2]("field3("",	Add Text Processor				
"pipe_sick": "field1 field2 'field3" ). "email address":	Add Sequence		word		

Figure 3: Easily parse unidentified logs with LogRhythm Policy Builder feature.

# Intuitive Dashboard, Assisted Search, and Reporting Capabilities

Search the entire log store at any time and continuously monitor via dashboards to enhance visibility into investigations and security analytics. Facilitate fast decision making with assisted search that prompts context as an analyst types in search keys and values. Search common events to find relevant security events across different vendors' log sources without having prior knowledge of the underlying log structure. Save dashboards and searches and schedule specific reports daily, monthly, and/or quarterly.

#### **Guided and Instinctive Workflows**

Detect, investigate, and respond to threats more easily with workflows that are consistent across the platform which additionally reduces ramp time on the platform.



Figure 4: Leverage widgets to surface common security use cases.

#### Simplified Licensing

Simplify budgeting and make it more predictable with licensing based on the daily ingest rate of data and the length of time it is retained in the platform.

#### Professional and Consulting Services

Gain a faster time to value with flexible options to choose what is right for your business. Learn more about <u>services for LogRhythm Axon</u>.

### **About LogRhythm**

LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights so they can respond with speed and efficiency. With deployment flexibility, out-of-the-box integrations, and advisory services, customers can confidently monitor, detect, investigate, and respond to cyberattacks.

#### Interested in seeing LogRhythm Axon in action? Request a demo today!