LogRhythm

The Security Intelligence Company

Security Intelligence and Analytics Platform

Attacks can originate from both inside and outside your environment. To stop them from resulting in a data breach or other cyber incident, you need a unified view into all threats facing your organisation. Use LogRhythm to detect emerging threats and neutralise them quickly.

Next-Gen SIEM

Log Management

Network Monitoring & Forensics

Endpoint Monitoring & Forensics

Unified Security Intelligence & Analytics

User and Entity Behaviour Analytics

Network Behaviour Analytics

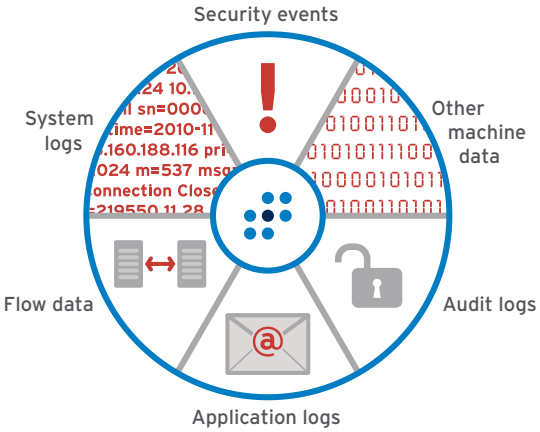
Endpoint Behaviour Analytics

Security Orchestration and Automation

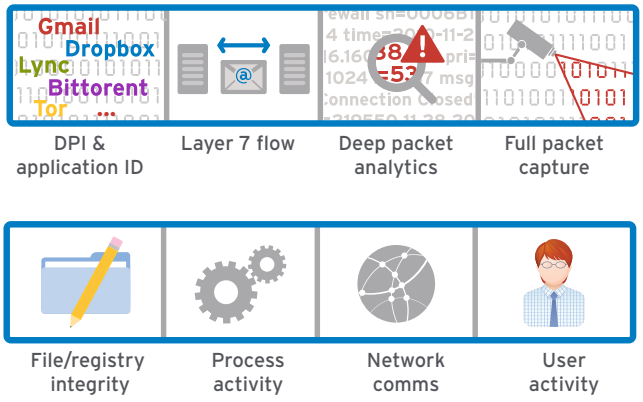
LOGRHYTHM SECURITY INTELLIGENCE AND ANALYTICS PLATFORM

INPUT

REAL-TIME DATA COLLECTION

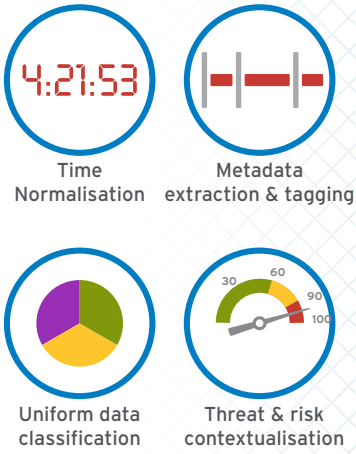


REAL-TIME DATA GENERATION

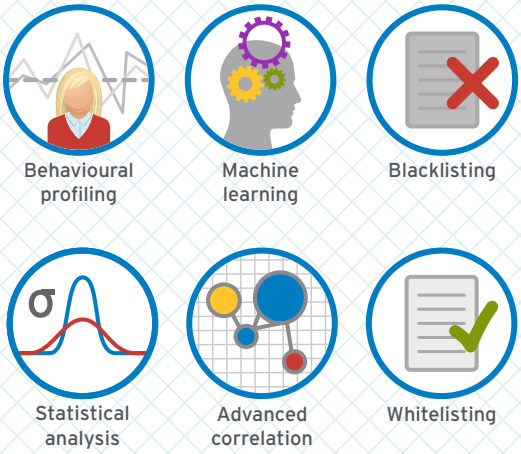


ANALYTICS

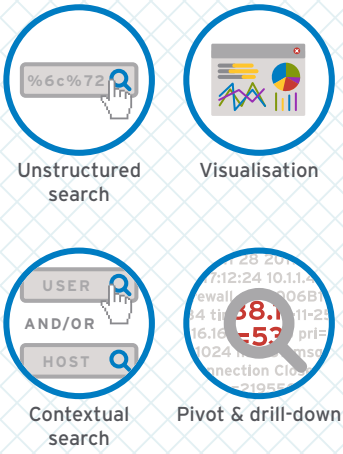
PROCESSING



MACHINE ANALYTICS



SEARCH ANALYTICS



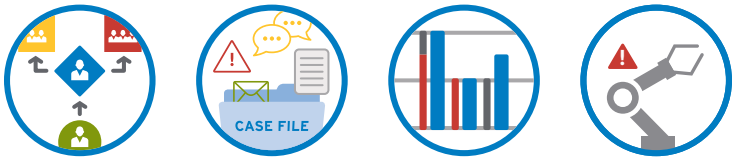
MACHINE DATA INTELLIGENCE (MDI) FABRIC

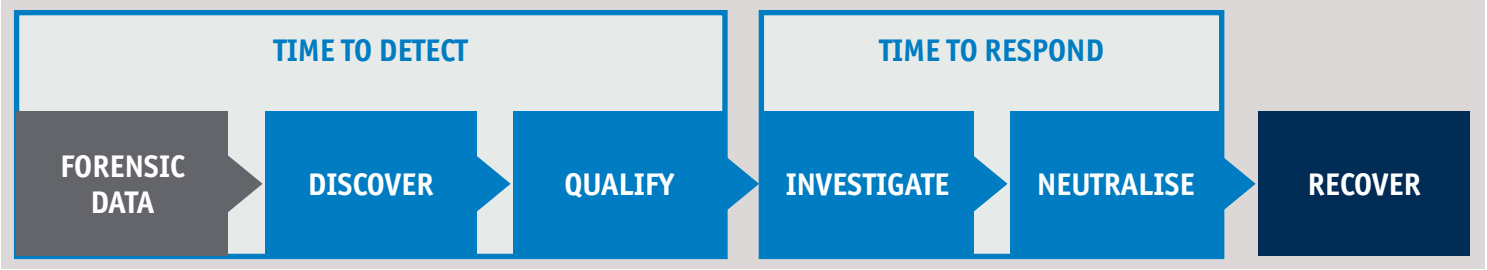
LogRhythm Labs Research & Intelligence

OUTPUT

ACTIONABLE INTELLIGENCE

SECURITY ORCHESTRATION AND AUTOMATION





Unify your security intelligence

Accomplish your mission

Security is your mission. It's ours, too. Empower your valuable personnel with a platform built for security intelligence and analytics. Implement security and compliance use cases quickly and effectively. Focus your team on protecting your organisation, rather than customising a tool.

Centralise your visibility

Gather all of the forensic evidence generated by your IT environment – with or without agents. Eliminate data silos and get centralised visibility with LogRhythm.

Monitor networks and endpoints

Fill in your forensic data gaps with endpoint and network monitoring. Our network and endpoint sensors ensure that you have all of the forensic detail you need to detect and neutralise advanced threats.

Understand your data

Get the intelligence you need, without the noise. Our Machine Data Intelligence (MDI) Fabric automatically contextualises over 785 different data sources. By extracting metadata and classifying security events, LogRhythm helps you use log and machine data to detect, respond to and neutralise advanced threats.

Know the true time of occurrence

Don't miss critical attack sequences. Our patented TrueTime™ function records the actual time of occurrence, automatically correcting offsets tied to different time zones, device clocks and collection latencies.

Seamlessly incorporate threat intelligence

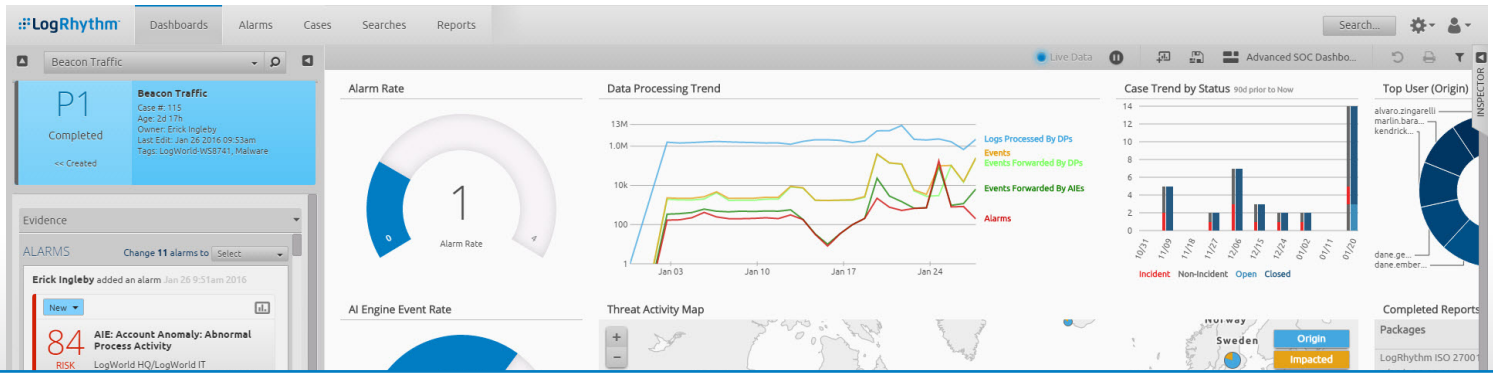
Threats are dynamic, and attack vectors are constantly changing. Stay ahead by using the rich context enabled by threat intelligence from STIX/TAXII-compliant providers, commercial and open-source feeds, and internal honeypots. Use this data to reduce false-positives, detect hidden threats, and prioritise your most concerning alarms.

LogRhythm Labs supports your team

LogRhythm Labs is a research and development team focused on security and compliance. The Labs team develops data processing rules for over 785 devices and applications, security analytics modules to protect your full attack surface, and compliance automation modules for 15 frameworks. The Labs team is comprised of recognised experts in intrusion detection, incident response, malware analysis, compliance, and other critical domains.

> **"LogRhythm's security analytics completely changed our visibility and monitoring capabilities to laser focus our time on the alarms that matter the most."**
>
> Source: Security Officer, Large Enterprise Retail Company

LOGRHYTHM SECURITY INTELLIGENCE AND ANALYTICS PLATFORM



Modernise your threat detection and response

Uncover the most critical threats

With machine learning and other automated data analysis techniques, LogRhythm's real-time security analytics help you detect advanced threats. Event corroboration and data-driven threat contextualisation calculate a granular risk score for each alarm so your team can focus on the most concerning issues.

Stop insider threats and account takeover

You can only shut down compromised accounts if you can see them. Our User and Entity Behaviour Analytics (UEBA) illuminate insider threats and stolen credentials so you can catch imposters, identify privilege abuse and stop user-based threats. LogRhythm Labs regularly develops new UEBA content, including behavioural profiling, peer group analytics, statistical analytics and advanced correlation to help you stay ahead of new threats.

Detect network and endpoint anomalies

See what's happening on your endpoints and network to detect compromises like spear phishing and zero-day exploits. LogRhythm's Endpoint and Network Threat Detection Modules are continually updated to ensure you stay one step ahead of cyber adversaries.

Search with power and precision

Get the answers you need, fast. Whether you're hunting for threats or investigating an incident, our search technology's Elasticsearch backend helps you work efficiently. Only LogRhythm empowers you to search with both unstructured and contextualised criteria, streamlining search creation and result analysis.

Orchestrate and automate security operations

Neutralise threats quickly using the collaborative workflows enabled by our embedded case management function, and automate incident investigation and remediation with pre-staged SmartResponse™ automation actions. Track detection and response times so you can optimise processes over time.

Streamline compliance

LogRhythm provides pre-configured compliance automation modules for several regulatory frameworks, including FISMA, GPG 13, HIPAA, ISO 27001, NERC CIP, PCI DSS, SOX, DoDi 8500.2, NEI 08-09, NIST Cybersecurity Framework, NIST 800-53 and NRC RG 5.71.

See LogRhythm in action

We can help you to detect, respond to and neutralise cyber threats before they can damage your business. To see how, watch our online demo at www.logrhythm.com/demo.

SC MAGAZINE

Gartner
A 2016 LEADER
SIEM Magic Quadrant

VENDOR LANDSCAPE AWARD
CHAMPION
INFO-TECH

FROST & SULLIVAN
2015 Global SIEM
Enabling Technology Leadership Award