LogRhythm®
The Security Intelligence Company

Unleash the power of your SOC

LogRhythm products and solutions overview

2019

Detect and respond to threats faster

Increase the efficiency and effectiveness of your security team

As sophisticated threats attempt to breach your network at an extraordinary rate, keeping your organisation safe may seem like a daunting task. You might find that your team is strapped for resources and expending valuable time sorting through a mass of log data – just to spot a true threat. When your team is racing against the clock, you need to detect and neutralise a threat fast before it wreaks havoc on your organisation.

LogRhythm can help.

At LogRhythm, we understand the complexity of your job. Our laser focus on security translates into targeted innovation to give your team the solutions it needs to overcome the challenges it faces every day. The LogRhythm NextGen SIEM Platform is designed to improve your organisation's overall security posture and defeat any threat that attempts to breach your environment.

Mature your security operations

The LogRhythm NextGen SIEM Platform empowers your team to advance your organisation's overall security posture and operations maturity. LogRhythm helps you strengthen your security operations to ensure you are ready to face the constantly evolving threat landscape.

Detect threats earlier and faster than ever before.

When it comes to stopping threats, seconds matter. We built the LogRhythm UI for speed and efficiency. LogRhythm enables you to surface threats, search through log data, make decisions, collaborate, and respond to security incidents faster than ever before. Through machine learning and scenario-based analytics, LogRhythm surfaces emerging threats as they occur so your team can act fast.

Do more with the resources you have in place today.

Focus on detecting and responding to threats instead of spending your valuable time maintaining, caring for, and feeding your SIEM. LogRhythm includes a library of continuously updated data processing content and threat scenarios, so your team won't have to spend time writing scripts, building rules, and creating reports. And because of the platform's flexibility, your team can tailor it to meet the unique requirements of your organisation.

Gain deep visibility across your network.

Through its security operations and analytics capabilities, the LogRhythm NextGen SIEM Platform eliminates blind spots across the enterprise, giving you complete visibility into your IT and OT environments. LogRhythm collects data from physical, virtual, and cloud sources to ensure that you always know what's happening on your network. You'll spot and catch every anomaly and threat – enabling you to successfully keep your business safe from cyberattacks.

Prove reduced risk to your board.

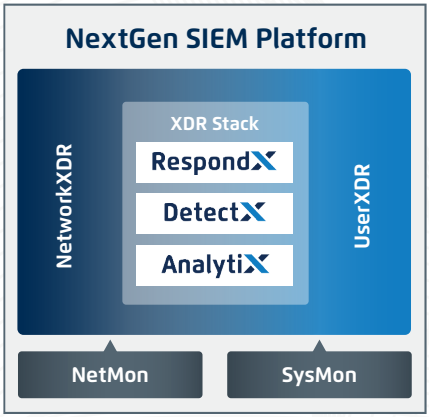
Your board needs to feel confident in your team's ability to identify and stop threats and keep the company's reputation and critical assets secure. And you need the board to continue to invest in your security programs. With reports that illustrate the types of threats you face and your team's detection and response trendlines, you'll be able to readily demonstrate your team's value.

Build for today. Scale for tomorrow.

The amount of data your team is responsible for protecting is large and is growing rapidly. It's important to know that your investment will easily flex to meet your future needs. The LogRhythm platform scales to massive data volumes while delivering high performance and streamlined administration—reducing your overall operating costs.

Build your SOC on a solid foundation

To protect your organisation from risk, your team must be able to detect and respond to a threat—before your network is compromised. How do you do this successfully? Shorten your mean time to detect (MTTD) and mean time to respond (MTTR) to a cyberthreat.



The LogRhythm NextGen SIEM Platform

Our NextGen SIEM solution operates as your team's central nervous system to alert on threats and enact countermeasures—all in real time. With LogRhythm, your team will detect and respond to threats measurably faster. Your security operation will become more effective and efficient through automated workflows and accelerated threat detection and response capabilities.

The LogRhythm NextGen SIEM Platform is comprised of the LogRhythm XDR Stack, LogRhythm UserXDR, and LogRhythm NetworkXDR.

LogRhythm XDR Stack

With the LogRhythm XDR Stack, your team has an integrated set of products that deliver on the fundamental mission of your SOC: threat monitoring, threat hunting, threat investigation, and incident response at the lowest total cost of ownership.

AnalytiX

Swiftly search across your organisation's vast data to easily find answers, identify IT and security incidents, and quickly troubleshoot issues.

DetectX

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

RespondX

Work smarter, not harder. Collaborate, streamline, and evolve your team with security orchestration, automation, and response (SOAR) that is seamlessly integrated into the LogRhythm NextGen SIEM.

UserXDR

Detect anomalous user behaviour before data is corrupted or exfiltrated with user and entity behaviour analytics (UEBA).

NetworkXDR

Go beyond limited traffic analysis to detect rapidly spreading network-borne threats and reduce risk to your organisation.

Deploy on-prem or in the cloud

Our flexible deployment options ensure that you get the best fit for your organisation—no matter what your goals and environmental needs may be. LogRhythm Cloud provides our complete NextGen SIEM experience with the ease and flexibility of a SaaS solution.

Compliance

Your organisation faces unique compliance challenges. The LogRhythm NextGen SIEM Platform provides the capabilities to address these challenges:

GDPR

LogRhythm's GDPR Compliance Module makes it easier to meet the regulation aimed at protecting the personal data of European Union (EU) citizens.

GPG 13

Automate log management and apply real-time analytics to expose areas of non-compliance with a Good Practice Guide (GPG) 13-optimised indexing structure and directly address control obligations mandated in GPG 13.

NIS Directive

The EU's Network and Information Security (NIS) Directive aims to boost the resilience of cybersecurity defences across Europe. The directive is particularly focused on industries and organisations that rely heavily on IT to provide services essential to everyday life and national security. LogRhythm provides the solutions needed to comply.

PCI DSS

The LogRhythm Payment Card Industry Data Security Standard (PCI DSS) Compliance Automation Module lets you easily access specific investigations, alarms and reports that are automatically associated with the correct PCI DSS asset categories.

ISO 27001

LogRhythm will categorise, identify and normalise your data for simplified reporting and analysis to meet International Standards Organisation (ISO) 27001 guidelines.

SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) facilitates financial transactions via its secure messaging system. Any organisation wishing to operate as a trusted partner on SWIFT must adhere to its security principles and controls and document and prove their adherence. LogRhythm supports the ability to do so.

Security Operations Maturity Model (SOMM)

How prepared is your business to detect and respond to modern security threats?

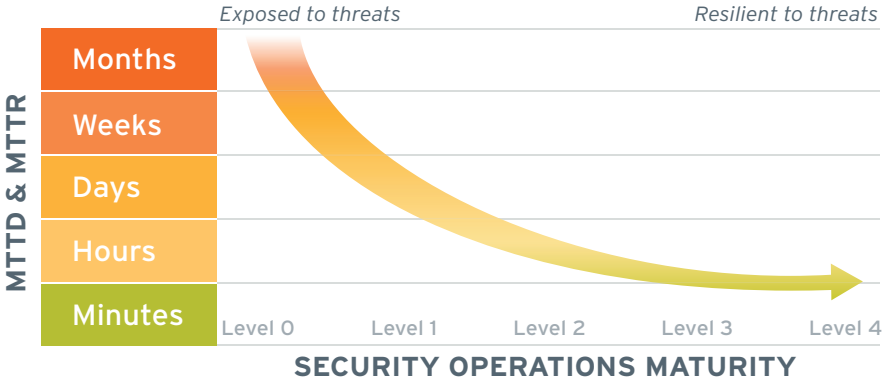
To understand how prepared your organisation is to counter the threats it faces, you must determine the effectiveness and maturity of your security operations.

The LogRhythm Security Operations Maturity Model (SOMM) helps organisations measure and benchmark the effectiveness of their security operations and to mature their security operations capabilities. Mature security operations teams kill threats early through technology-enabled processes that drive down their mean time to detect (MTTD) and mean time to respond (MTTR)—rapidly detecting and neutralising threats before real damage occurs.

LogRhythm's SOMM provides a practical guide for organisations that wish to reduce their MTTD and MTTR—dramatically improving their resilience to cyberthreats.

When evaluating the fundamental maturity of security operations, LogRhythm believes the TLM framework serves as the foundation of the security operations centre (SOC) and should be where organisations place the greatest emphasis.

Organisations that adopt LogRhythm's SOMM will be able to plan for the future and realise continuous improvement of their security operations maturity. It provides a roadmap to successfully reduce risk.



To find out more about our Security Operation Maturity Model, please download our white paper. https://logrhythm.com/uk-security-operations-maturity-model-white-paper

Threat Lifecycle Management (TLM)

Prevent major data breaches by reducing time to detect and respond to threats

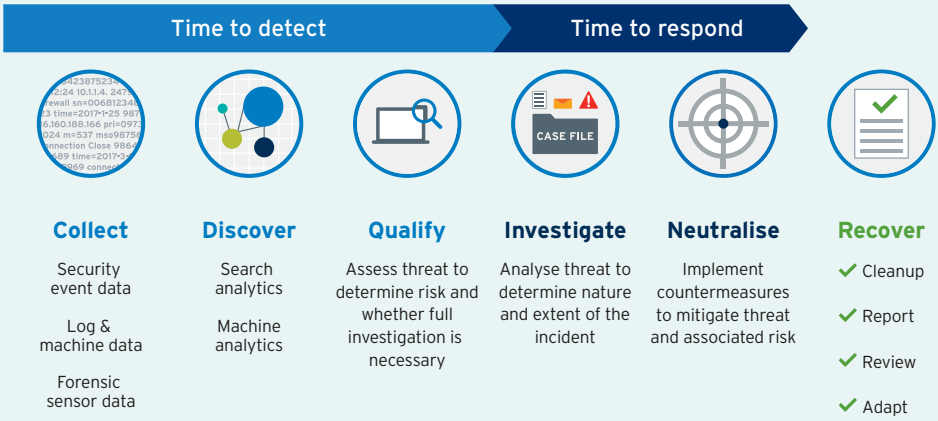
The central concept of the Threat Lifecycle Management (TLM) framework is that the earlier you detect and mitigate a threat, the less the ultimate cost will be to your business.

By implementing an effective end-to-end threat management process that focuses on reducing detection and response times, you will have the ability to prevent high-impact security incidents, such as major data breaches.

TLM can help you improve the efficiency of your security operations through a series of aligned capabilities and processes. It begins with broad and deep visibility across your IT environment and ends with rapid mitigation and recovery from a security incident. The six steps of TLM are shown below:

You can enable effective TLM at a scale appropriate to your business through modern technology, specifically in the areas of:

- Advanced machine analytics are key to discovering potential threats quickly.
- Security automation and orchestration capabilities increase analyst efficiency to support the entire threat investigation, through to full remediation and recovery.

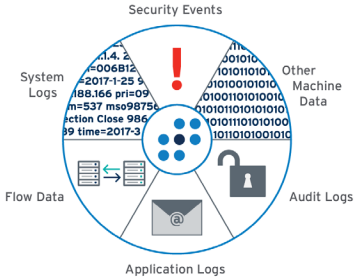


Detect and kill threats intelligently

NextGen SIEM capabilities and Threat Lifecycle Management framework delivered by the LogRhythm platform empowers organisations to rapidly detect and respond to damaging cyberthreats in today's rapidly evolving and increasingly complex threat landscape.

INPUT

Real-Time Data Collection



Real-Time Data Generation

Network Monitoring

- DPI & Application ID
- Full Packet Capture

Endpoint Monitoring

- File & Registry Monitoring
- Process Activity

Real-Time Context

Internal

- Users
- Hosts

External

- Threat Intelligence

ANALYTICS

Processing

- Time Normalisation
- Metadata Extraction

MACHINE DATA INTEL

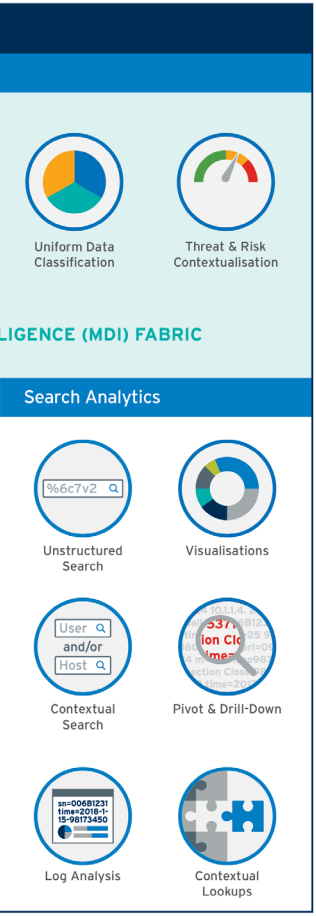
Machine Analytics

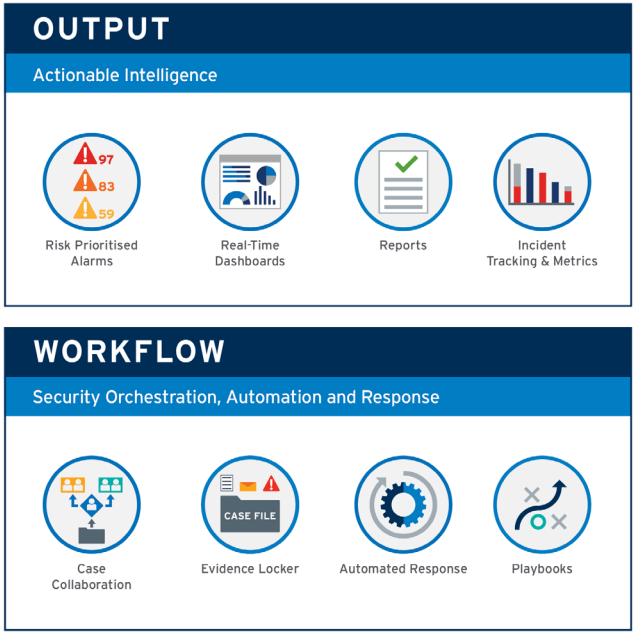
- Behavioural Profiling
- AI & Machine Learning
- Statistical Analysis
- Advanced Correlation
- Black/Whitelisting
- Deep Packet Analytics

Platform Overview

The end-to-end NextGen SIEM Platform integrates:

- Endpoint Monitoring
- Network Monitoring
- Log Management
- Security Analytics
- User and Entity Behaviour Analytics (UEBA)
- Network Detection and Response (NDR)
- Security Orchestration, Automation and Response (SOAR)





Embedded expertise

LogRhythm Labs

You may not be an expert in every area of security – which is why we built a team of dedicated security experts. Our LogRhythm Labs team delivers unparalleled security research, analytics, and threat intelligence services. By delivering actionable intelligence and advanced analytics, your team is empowered to greatly reduce its time to detect and remediate the latest security threats.

NetMon Freemium

Detect threats in real-time with our free network monitoring and forensics tool

Download NetMon Freemium for real-time network-based threat detection and network-based incident response and achieve enterprise-wide visibility for free.

Here are six ideas of how to use our free tool to discover threats on your network:

1. Surface data exfiltration activities: Identify long-running sessions, 'low and slow' sessions hidden in normal traffic, anomalous outbound network sessions, and other activities indicative of data exfiltration.

2. Discover operational anomalies: Verify that you aren't seeing protocols or traffic that you think you've blocked or traffic between systems that should be isolated from each other.

3. Find hidden security threats: Catch security threats hiding in low-level chatty protocol like DNS, SMNP or Kerberos.

4. Detect botnets and beaconing: Identify traffic using anomalous ports. View malformed packet headers. Recognise command and control call-backs.

5. Expose nuisance apps and bandwidth hogs: Discover when apps that violate corporate policy are being used. Find out who, or what, is taking up the most bandwidth.

6. See where your network traffic is going: Identify outbound IP and URL destinations and classify traffic by ingress, egress or lateral motion in your network.

Download NetMon Freemium today: logrhythm.com/freemium-emea/

LogRhythm Services

Whether you're new to LogRhythm or you're a long-time LogRhythm user, our services teams can help you improve your security intelligence maturity.

LogRhythm Labs

Your secret weapon against cyberthreats

With the growing number of cyberthreats, their increasing level of sophistication and your limited IT resources, it can be difficult to uncover new vulnerabilities and attack methods.

LogRhythm Labs is a dedicated team that delivers security research, analytics and threat intelligence services to help protect your organisation from damaging cyberthreats. Our research-based content helps you detect and respond to threats and risks by combining advanced analytics with actionable intelligence.

Global Support Services

Find success with your LogRhythm implementation

To help you be successful with your LogRhythm implementation, you can choose the support level (standard or premium) that meets your needs, providing you access to highly trained, experienced support staff.

If you are a current customer and experiencing a technical issue or have a question about your LogRhythm NextGen SIEM Platform, you can use the LogRhythm Support Portal or call your local LogRhythm Support team.

LogRhythm Training

Enrol in LogRhythm University

LogRhythm University provides in-depth product training for customers' security administrators and analysts. Instructor-led tuition is available in person at any one of the LogRhythm global training facilities, virtually or at your site.

"The visibility LogRhythm has given us has been a game changer. The insight we now have is unparalleled and gives us confidence that we can detect and mitigate a threat as soon as it appears."

-Donald Andango, Information Security Specialist, Salford Royal NHS Foundation Trust

Schedule a customised demo today: www.logrhythm.com/demo

Contact us

UK: +44 (0)1628 918 330
Germany: +49 89 919292 – 200
Dubai: +971 55 6422224

europe@logrhythm.com | www.logrhythm.com

LogRhythm®
The Security Intelligence Company