

Protect Your Manufacturing Operation's Network and Data



Your job is to keep your manufacturing facility safe from cyberattacks.

Manufacturing companies have increasingly become vulnerable to disruptive ransomware attacks, evidenced by the 1,817 incidents recorded in manufacturing breaches in 2023. Ransomware's upward trajectory persists, with a steady increase for the third consecutive year, now accounting for 42% of these incidents.¹

These attacks often disrupt manufacturing industrial control systems (ICS) and stop manufacturing-related processes. Such cyberattacks can cause ripple effects across the entire supply chain² and even cause companies to shut down their operations, as evidenced with the attacks on Honda³ and Palfinger⁴, which affected their global operations, and the ransomware attack on Steelcase⁵ that caused the company to shut down.

But parsing through increasing amounts of log data across disparate systems and cloud applications can leave major gaps in visibility throughout the environment. Prioritizing threats may become an overwhelming task when strapped with few resources.

So how do you elevate securing your operational technology (OT) to the next level? You should inspire and encourage a security-first mindset across the enterprise. To do so, your team must implement a resilient and adaptable security strategy that builds confidence and board-level support to scale your threat detection and response.

No pressure, right? Luckily, there is a holistic solution that can provide your security operations center (SOC) with a quick time to value and a measurable return on investment.

Here's how LogRhythm can help.



¹ [2023 Data Breach Investigations Report](#), Verizon, June 21, 2023

² [Supply Chain Pivots Need to Start with Cybersecurity](#) Manufacturing Business Technology, Jul. 13, 2020

³ [Cyber Attack Puts Brakes on Production Activities](#) Industry Week, June 10, 2020

⁴ [Global Crane Manufacturer Palfinger Suffers Cyberattack](#) Industry Week, Jan. 25, 2021

⁵ [Steelcase Cyber Attack Should Be a Wakeup Call](#) Industry Week, Nov. 13, 2020



Mature Your Manufacturing Security Operations

[LogRhythm SIEM](#) empowers your team to advance your manufacturing organization's overall security posture and operations maturity. LogRhythm strengthens your SOC and ensures you are ready to face whatever threats may come your way.

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 your manufacturing company has 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. With greater flexibility, your team can customize and tailor it to meet the unique needs of your OT environment.

Gain deep visibility across your manufacturing operation's network.

Through its security operations and analytics capabilities, LogRhythm SIEM improves visibility 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 manufacturing enterprise safe from cyberattacks.

Prove reduced risk to your agency.

Your board needs to feel confident in your team's ability to identify and stop threats and keep the manufacturing firm'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 your manufacturing company faces 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. LogRhythm SIEM scales to massive data volumes while delivering high performance and streamlined administration—reducing your overall operating costs.





Cybersecurity Use Cases for Manufacturing

Manufacturers are a high target for cybercriminals. Hackers seek to infiltrate intellectual property, customer financial information, and propriety information, as well as attack control systems that disrupt production processes.

Ransomware

Manufacturers have an extremely low tolerance for downtime with the production process. Attackers use malware to hack operational technology, such as industrial control systems for financial gain.

Data Exfiltration

Disgruntled employees have direct access to various systems and can act maliciously by carrying out unauthorized data transfers.

Third-Party Tactics

Adversaries leverage third parties to conduct espionage, steal proprietary information, or initiate a potentially disruptive OT attack.

Phishing Attacks

Cybercriminals often reach out to other factory employees or executives from a victim's corporate email address to solicit personal information, gain access to accounts, or for financial schemes. Insider threats hackers can gain a foothold when employees are connecting to business networks from several devices, including mobile, instead of company-issued and vetted machines.

Solutions



Manage Your Firm's Digital Transformation with Security Information and Entity Management (SIEM)

LogRhythm SIEM centralizes data across disparate Smart Manufacturing and Industry 4.0 systems, correlating that data to provide a holistic overview of an organization's environment helping analysts to stop threatening behavior before damage is done.



User Entity Behavior Analytics

LogRhythm UEBA automatically identifies and prioritizes anomalous user behavior, bringing enhanced efficiency to the detection of malicious threats.



Ensure Compliance

Manufacturers face increasingly intense regulatory and compliance oversight. LogRhythm's solutions support auditing requirements through Compliance Automation Suites with embedded content, which provide for long-term and secure data storage as well as wizard-based data recovery.



Build Your Manufacturing Company's SOC on a Solid Foundation

To protect your manufacturing company 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.

LogRhythm SIEM

LogRhythm SIEM 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. LogRhythm SIEM features the following:



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.



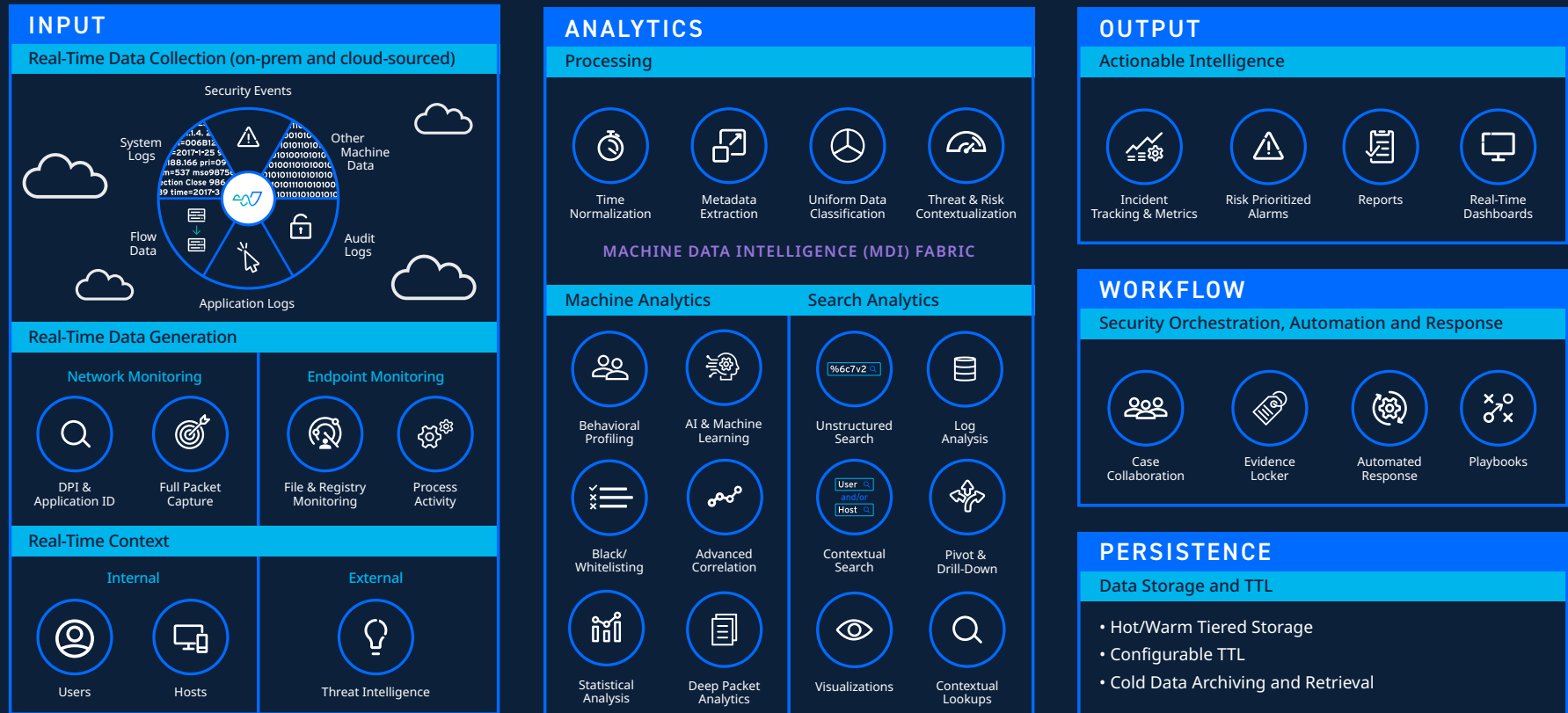
User Analytics - Protect against insider threats with LogRhythm's embedded deterministic user and entity behavior analytics (UEBA) monitoring. To detect anomalies using machine learning, leverage [LogRhythm UEBA](#), our advanced analytics UEBA solution.



Orchestration and Automation - Work smarter, not harder. Collaborate, streamline, and evolve your team's security maturity 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.



Behind the UI of LogRhythm SIEM





An Award-Winning Platform

We're proud of our accolades. We've earned every one of them. The recognition we've received points to our innovation and dedication to delivering security solutions that help you protect your manufacturing organization, your brand, and your reputation.

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. LogRhythm SIEM is designed to improve your overall security posture and defeat any threat that attempts to breach your manufacturing ecosystem.

From R&D to our customer success team, we see ourselves as your partner in the fight against cyberthreats. Customer success is one of our core company values. Let our customers tell you about their experiences firsthand.

Visit www.logrhythm.com to read and watch in-depth reviews from real customers.





Our Commitment to Your Success

LogRhythm Labs

It's crucial to have resources that keep your manufacturing enterprise well informed of the latest incidents and breaches that could pose a threat. [LogRhythm Labs](#) can help with a dedicated team that delivers use case content encompassing the latest information on emerging threats, changing compliance mandates, and security best practices for manufacturing companies.

We Can Help

Dealing with the change that comes with running a SOC takes guts, grit, and the ability to establish confidence when faced with uncertainty and doubt. To be resilient, you need to ensure that security is a top priority in your organization and that you can show the value of your program. For this to happen, you must be a change agent and establish a security-first mindset in your company.

Our [Professional Services](#) can help you keep pace with a changing security landscape, boosting the performance and effectiveness of your security team and platform. Customers use our service offerings to accelerate time to value, ensure seamless deployment, and tune their platform. Customers also rely on our subscription services to augment their security team with our experts. LogRhythm lives and breathes the security-first mindset that creates resilience—from being one of the frontrunners to implement the Zero Trust framework for our own organization to our dedication to innovation and education.



About LogRhythm

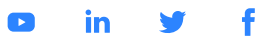
LogRhythm helps security teams stop breaches by turning disconnected data and signals into trustworthy insights. From connecting the dots across diverse log and threat intelligence sources to using sophisticated machine learning that spots suspicious anomalies in network traffic and user behavior, LogRhythm accurately pinpoints cyberthreats and empowers professionals to respond with speed and efficiency.

With cloud-native and self-hosted deployment flexibility, out-of-the-box integrations, and advisory services, LogRhythm makes it easy to realize value quickly and adapt to an ever-evolving threat landscape. Together, LogRhythm and our customers confidently monitor, detect, investigate, and respond to cyberattacks.

Learn more at logrhythm.com.



1.866.384.0713 // info@logrhythm.com // 385 Interlocken Crescent, Broomfield, CO 80021
© LogRhythm Inc. // BR237124-02



www.logrhythm.com