Protect Your Manufacturing Operation’s Network and Data
Your job is to keep your manufacturing facility safe from cyberattacks.

Manufacturing companies have become prime targets for disruptive ransomware attacks. The number of reported ransomware attacks on manufacturing companies more than tripled in 2020 over 2019, with manufacturing organizations accounting for 29% of all ransomware attacks in 2020. These attacks often disrupt manufacturing industrial control systems (ICS) and stop manufacturing-related processes.

These types of cyberattacks can cause ripple effects across the entire supply chain and even cause companies to shut down their operations, as evidenced with the attacks on Honda and Palfinger, which affected their global operations, and the ransomware attack on Steelcase 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 little resources.

So how do you elevate securing your operational technology (OT) to the next level? You need to 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) quick time to value and measurable return on investment.

Here’s how LogRhythm can help.
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, 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 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. The LogRhythm platform scales to massive data volumes while delivering high performance and streamlined administration—reducing your overall operating costs.
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 ICS for financial gain.

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

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.

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.

Network Detection and Response Ensures Vulnerable Assets are Protected
MistNet NDR by LogRhythm provides a machine learning (ML)-driven network threat detection and response solution that eliminates blind spots and monitors your organization’s network and ICS systems in real time, helping to maintain control and protect vulnerable assets, even as Industrial Internet of Things (IIoT) connectivity continues to accelerate.

User Entity Behavior Analytics
UserXDR, LogRhythm’s user entity behavioral analytics (UEBA) solution, 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.

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 and LogRhythm UserXDR.

Deploy On-Prem or in the Cloud

Our flexible deployment options ensure that you get the best fit for your organization—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.

LogRhythm XDR Stack

With the LogRhythm XDR Stack, your team has an integrated set of capabilities 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 enterprise’s vast data stores 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 prioritized 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 and works with more than 80 partner solutions.

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

MistNet NDR by LogRhythm

To defend against cyberthreats in the evolving OT landscape, your organizations must capture, correlate, visualize, and analyze forensic data to drive actionable insight—in real time. MistNet NDR by LogRhythm combines machine learning, rules-based detection and threat intelligence to discover and identify threats across desktops, data centers, and the cloud.

Powered by patent-pending TensorMist-AITM technology, MistNet NDR uses distributed computing that easily scales data collection and analytics and lowers operating costs.
Behind the UI of our NextGen SIEM

Input
- Real-Time Data Collection (on-prem and cloud-sourced)
  - Security Events
  - Other Machine Data
  - Flow Data
  - Audit Logs
  - Application Logs
- Real-Time Data Generation
  - Network Monitoring
    - Gmail, Bizarre, Dropper, Lynx
    - 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 Normalization
  - Metadata Extraction
  - Uniform Data Classification
  - Threat & Risk Contemporization

MACHINE DATA INTELLIGENCE (MDI) FABRIC
- Analytics Output
  - Analytics
    - Machine Analytics
      - Behavioral Profiling
      - AI & Machine Learning
      - Black/Whitelisting
      - Advanced Correlation
      - Statistical Analysis
      - Deep Packet Analytics
    - Search Analytics
      - Unstructured Search
      - Log Analysis
      - Contextual Search
      - Pivot & Drill-Down
      - Visualizations
      - Contextual Lookups

Output
- Actionable Intelligence
  - Incident Tracking & Metrics
  - Risk Prioritized Alarms
  - Reports
  - Real-Time Dashboards

Workflow
- Security Orchestration, Automation and Response
  - Case Collaboration
  - Evidence Locker
  - Automated Response
  - Playbooks

Persistence
- Data Storage and TTL
  - Hot/Warm Tiered Storage
  - Configurable TTL
  - Cold Data Archiving and Retrieval
An Award-Winning Platform

We’re proud of our accolades. We’ve earned every one of them.

From being a Leader in the Gartner Magic Quadrant for the better part of a decade to receiving the Gartner PeerInsights™ Customers’ Choice designation four years in a row, 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. The LogRhythm NextGen SIEM Platform 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. Together, we can be security first.
LogRhythm’s award-winning NextGen SIEM Platform makes the world safer by protecting organizations, employees, and customers from the latest cyberthreats. It does this by providing a comprehensive platform with the latest security functionality, including security analytics; network detection and response (NDR); user and entity behavior analytics (UEBA); and security orchestration, automation, and response (SOAR).

Learn how LogRhythm empowers companies to be security first at logrhythm.com.

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