LogRhythm®

The Security Intelligence Company

Some assembly required: Cybersecurity and manufacturing

The pieces are there

Over the centuries, manufacturing has built the world around us. But in that time the process of manufacturing has changed fundamentally. Today's plants and factories are complicated systems, connected with supply chains and other facilities around the world. However, those connections can put facilities at risk of cyberattack.

Many manufacturing operations contain disparate legacy systems that were not designed with cybersecurity in mind. When they operated in isolation, physically separated from other systems, this arrangement may not have presented a large risk. However, the transformation to Industry 4.0 has networked operations, leading to a jumble of pieces obscuring what occurs beneath[1].

What's on the line

At the heart of manufacturing opportunities – and threats – is the Internet of Things (IoT). Forbes.com reported that, in 2016, the IoT represented $178bn in investment[2]. The IoT offers real-time insight into what is happening on the line, can detect defects when they happen and allows finer control and adjustment of processes. Unfortunately, this interconnectedness can result in vulnerabilities. Much of the existing infrastructure that IoT controls are being integrated with are legacy systems. Industrial Control Systems (ICS), often managed by Supervisory Control and Data Acquisition (SCADA) systems, are common and at risk. The most famous cyberattack on an industrial system is likely Stuxnet. Discovered in 2010, the malware caused major damage to Iran's nuclear research programme[3].

While the development of Stuxnet is thought to have been state-backed, a more recent attack, in 2015, shows the real danger manufacturers face. According to German officials, an unnamed German steel mill was hacked and the controls for a blast furnace were compromised. The furnace could not be safely shut down and the attack resulted in massive damage[4].

The threat to manufacturers is real and growing. Kaspersky Labs reports that one in three cyberattacks against ICS computers in the first half of 2017 was in the manufacturing sector[5].

It's not just widgets you stand to lose

Modern manufacturers have more than a warehouse full of widgets at risk. Sophisticated cyberattacks can cost you dearly. You can lose:

- **Intellectual property**: You can lose years of R&D and millions in expenditures if someone steals your IP. You might have invented it, but when knock-offs are flooding the market, it won't matter.
- **Proprietary information**: Plans for marketing campaigns, strategic partnerships, budgets and forecasts can give a competitor the edge.
- **Contracts**: If you can't deliver products on time or a cyberattack has affected the quality of production, future contracts are at risk. If they are government or military contracts, they may be at risk even if there is no interruption in production.
- **Production**: If you can't bring your product to market on time, you're wasting huge resources, such as idle trucks or advertising spend, when the product isn't available.
- **Fines**: If your attackers caused privacy or regulatory breaches, this could result in fines.
- **Lives**: Manufacturing facilities can be dangerous places. Cyberattackers can put lives at risk if they gain control of equipment.

[1] What Everyone Must Know About Industry 4.0
https://www.forbes.com/sites/bernardmarr/2016/06/20/what-everyone-must-know-about-industry-4-0/#72ee7bbd795f
[2] Top 5 Digital Transformation Trends In Manufacturing
https://www.forbes.com/sites/danielnewman/2017/08/08/top-5-digital-transformation-trends-in-manufacturing/#d5d02ac249f0
[3] The Real Story of Stuxnet
https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
[4] A Cyberattack has Caused Confirmed Physical Damage for the Second Time Ever
https://www.wired.com/2015/01/german-steel-mill-hack-destruction/
[5] Industrial cybersecurity threat landscape in H1 2017 https://www.kaspersky.co.uk/about/press-releases/2017_industrial-cybersecurity-threat-landscape-in-h1-2017-every-third-ics-computer-under-attack-was-from-manufacturing-sector

But it's not just the physical plant that is under threat. Intellectual property (IP) is at risk, too. That IP can represent millions in R&D investment and may have taken years to accumulate. Furthermore, manufacturers who work with government or military contracts must consider the risk around handling sensitive or classified information which could attract not just industrial espionage but the attention of state-sponsored cybercriminals.

Putting the pieces together

Perhaps the greatest difficulty in planning and implementing protection against cyberattacks is that organisations do not know about the majority of attacks that occur. One cybersecurity company recently estimated that as many as 71 per cent of compromises go undetected[6]. While stopping intruders from gaining access is an important first line of protection, it's not enough.

Mean time to detect (MTTD) an attack is crucial. When a system's perimeter defences are penetrated — and sooner or later they will be — a business needs to know as quickly as possible so that it can respond.

Manufacturers face a major challenge as their disparate systems, including legacy and embedded systems, often mean there is no single overview available. This can slow detection or even allow threats to go undetected. A system that cuts across systems and silos and provides a unified view can greatly reduce MTTD.

Mean time to respond (MTTR) is the next step in the effective defence of systems. This is how long it takes to act on an identified security breach. Detection without response is like a burglar alarm without a police department. Ideally, you want to respond quickly enough to stop damage being done or intellectual property being stolen. There's no point closing the factory door after the IP has left the plant.

The leadership at aviation leader Airbus is so concerned about the vulnerabilities in ICS that such threats are a focus of its cybersecurity division. It runs labs in several countries that develop tools for penetration testing, code verification and validation, threat hunting, incident response and forensics.

A safety checklist

- Take an inventory of everything that connects to a network, especially if it connects the business and manufacturing sections of your organisation.
- Audit legacy components for vulnerabilities and correct them or replace them.
- Ensure remote access to systems is secure and minimise it where possible.
- Keep security systems updated.
- Use an integrated solution that gives you transparency across your organisation to reduce MTTD and MTTR.

[6] Surfacing Critical Cyber Threats Through Security Intelligence
https://logrhythm.com/pdfs/whitepapers/lr-security-intelligence-maturity-model-ciso-whitepaper.pdf

Unfortunately, not many manufacturers have such resources. A report from Deloitte reveals that 75 per cent of surveyed organisations lacked the skills and resources to deal with cyberthreats.

Fortunately, there is a way to get the resources needed without breaking the bank.

The final piece

LogRhythm offers a consolidated perspective, a holistic view of their entire IT/OT environment via a single pane.

LogRhythm's NextGen SIEM Platform monitors your environment to detect malicious activity and enable a rapid response. Its embedded UEBA solution provides deep visibility into user activity, helping detect insider threats, compromised accounts, privileged account abuse, and other user-based threats. Security automation and orchestration (SAO) frees up time so in-house IT teams can focus on other important tasks and improving operational efficiency.

Network and data monitoring lets you detect and respond quickly to threats, such as ransomware attacks, shutting down these processes as soon as they are detected. The platform can recognise data exfiltration, spear phishing, botnet beaconing, inappropriate network usage, lateral movement and suspicious file transfers.

In addition, LogRhythm's centralised solutions for dedicated log management and security information and event management (SIEM) are designed for quick deployment and scalability.

LogRhythm CloudAI collects data from the corporate environment to the production line and forwards it to the cloud, where it is subjected to machine learning across long periods of time to decipher what are normal or unusual patterns of behaviour. This provides indications of compromise and lets you know who has accessed what, as well as when and if any changes have been made.

CloudAI sends alerts with a risk score to suggest whether something warrants investigation.

Why LogRhythm is the smart call

LogRhythm offers a broad range of capabilities that enable a customised fit for manufacturing companies, addressing business needs on time and on budget.

- Endpoint Monitoring
- Network Monitoring
- Log Management
- Security Analytics
- User Entity and Behaviour Analytics (UEBA)
- Network Traffic and Behaviour Analytics (NTBA)
- Security Automation and Orchestration (SAO)

Increasing environmental and safety concerns mean manufacturers can face regulatory and compliance challenges. Successful audits start with good records, and LogRhythm's solutions support auditing requirements via Compliance Automation Suites with embedded content and enable long-term and secure data storage as well as wizard-based data recovery.

Together, LogRhythm's offerings provide manufacturers with industry-leading monitoring, detection, automation, compliance and auditing support, comprehensive reporting and protection against advanced threats. All the pieces are in place to realise Industry 4.0.

About LogRhythm

LogRhythm is a world leader in NextGen SIEM, empowering organisations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralising damaging cyberthreats. The LogRhythm platform combines user and entity behaviour analytics (UEBA), network traffic and behaviour analytics (NTBA) and security automation and orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) workflow serves as the foundation for the AI-enabled security operations centre (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many accolades, including being positioned as a Leader in Gartner's SIEM Magic Quadrant.

"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

LogRhythm®

The Security Intelligence Company

Security. Made Smarter.

Contact us

UK: **+44 (0)1628 918 330**
Germany: **+49 89 919292 - 200**
Middle East & North Africa: **+971 55 6422224**
europe@logrhythm.com | **www.logrhythm.com**

LogRhythm, Clarion House, Norreys Drive, Maidenhead, SL6 4FL, United Kingdom.