Why Your Manufacturing Business Needs MDR

Modern manufacturing operations are built on a foundation of cloud-based tools, IoT-enabled machinery, and complex supply chains—all of which expand the attack surface. The 2025 DBIR confirms that 73% of breaches in manufacturing involved external actors, with system intrusion being the most common vector.

Notably, 15% of breaches involved third-party suppliers, reflecting a 68% year-over-year increase in supply chain risk. Threat actors are also becoming more organized and professionalized. As noted in the SOCRadar Threat Landscape Report, attackers are leveraging Ransomware-as-a-Service (RaaS), AI tools, and stolen credentials to breach manufacturing networks faster and more efficiently.

To counter these risks, manufacturers need MDR - an agile, scalable cybersecurity approach. MDR's integration of telemetry, analytics, and human expertise has been shown to improve vulnerability and threat management effectiveness by up to 60% over traditional security methods (SOCRadar Report).

The frequency of ransomware attacks on governments, businesses, consumers, and devices is expected to rise to

every 2

seconds by 2031

Source: *Cybercrime Magazine: Top 10 Cybersecurity Predictions and Statistics For 2024*.

FROM PREVENTION TO MDR

In-house security teams often struggle to keep pace with the volume, variety, and sophistication of cyber threats. Ransomware remains a significant concern, with 33% of breaches involving ransomware or extortion techniques. A notable trend is the exploitation of zero-day vulnerabilities, which has seen a 180% increase compared to the previous year. Additionally, the use of stolen credentials remains a prevalent method for attackers, appearing in almost one-third of all breaches.

> **“AI services lower barriers to entry, increasing the number of cyber criminals, and will boost their capability by improving the scale, speed, and effectiveness of existing attack methods.“**
>
> James Babbage, Director General for Threats at the National Crime Agency.

Threat actors are using such tools to shorten the time it takes from initial access to data theft or ransomware deployment. This is a challenge not just in the context of ransomware but the full range of threats facing organizations—from crypto mining malware and botnets to banking trojans and spyware.

The cumulative impact of these trends should focus manufacturing IT security leaders on an inescapable truth. Bad actors’ motivation to succeed is often greater than companies’ preparedness via preventive measures. They go to great lengths to get into the corporate environment unseen.

That’s why organizations should balance prevention with detection and response. This is what ESET’s prevention-first approach focuses on, by blending multiple layers of security technology. It aims to protect by blocking malicious code or actors from entering or damaging a user’s system.

However, if these measures are bypassed by sophisticated actors, there is fast and reliable detection and response to mitigate advanced threats that manage to compromise a system. Think of it as locking and bolting all your doors and windows but then installing motion detection alarms to catch suspicious activity if anyone does make it inside the house.

XDR is a key asset here. It enables security operations (SecOps) teams to gain unparalleled visibility into their IT environment from a single pane of glass, and spot anomalies indicating threats via high-fidelity alerts. XDR is an evolution of EDR, which optimizes threat detection, investigation, response and hunting in real time.

XDR ENABLES YOU TO ANSWER SEVERAL KEY QUESTIONS ABOUT A CYBERATTACK:

How did it start?
Where did it start?
When did it start?
Which endpoints are infected?
Is it contained?
How do we prevent it in the future?

XDR unifies security-relevant endpoint detections with telemetry from security and business tools such as network analysis and visibility (NAV), email security, identity and access management, cloud security, and more. It is a cloud-native platform built on big data infrastructure to provide security teams with flexibility, scalability, and opportunities for automation.

Most importantly, it can help you take rapid remedial action to resolve incidents before they severely impact the organization.

However, even with the help of XDR, SecOps teams face major challenges from an organizational perspective - especially skills gaps, tool complexity, budget and resource constraints, and integration of tooling; not to mention a rapidly evolving threat landscape. That's why many manufacturing companies are turning to MDR; the most effective way to detect and contain ever-changing, sophisticated threats.

HOW MDR ADDRESSES CONTEMPORARY THREATS

Although MDR varies from provider to provider, it should include at least some variation of the following:

- **24/7 Threat Monitoring and Detection:**
  Continuous monitoring of an organization's network, endpoints, and cloud environments.
- **Proactive Threat Hunting:**
  Unlike traditional security measures that react to alerts, MDR involves proactive threat hunting which helps in identifying APTs and zero-day vulnerabilities.

51%

is the number

of organizations that have formally established threat hunting methodologies in 2024, compared to 35% in 2023.
Source: *SANS: The Evolution of Enterprise Threat Hunting: Detailed Insights from the SANS 2024 Survey*.

Organizations using telemetry can achieve up to a

60% improvement

in their ability to manage vulnerabilities and threats compared to those relying solely on traditional security measures..
Source: Forrester: The Four Steps for More Proactive Security, 2024.

- **Expert Analysis and Response:**
The expertise of security professionals allows for nuanced analysis and rapid decision-making, which is crucial for addressing complex security incidents.

- **Global threat intelligence:**
Accurate, current and relevant telemetry collected from across the globe provides actionable intelligence for rapid incident response and optimized threat hunting.

- **Continuous Improvement:**
By analyzing past incidents, using advanced threat intelligence, focusing on real threats, and providing regular security health checks and reports, MDR services help prevent the recurrence of similar attacks by enabling teams to improve cyber-resilience.

KEY FUNCTIONS OF MDR

MDR can bring tremendous benefits for organizations that want to mitigate cyber risk, but don't have the in-house resources effectively helping them to close skills gaps, save costs and enhance detection and response. A high-performance solution should enable organizations to:

Monitor

Experienced threat hunters keep track of the entire customer IT environment, and actively monitor malware and APT groups to provide the highest level of situational awareness.

Detect

Threat actors have countless ways to sneak through perimeter defenses, but by leveraging behavioral analytics, they can be spotted for rapid remediation.

Triage

An initial assessment and categorization of alerts filters out false positives and gathers necessary information.

Prioritize

Intelligent analytics rank these alerts by severity to ensure the most critical threats are addressed first. This is a critical phase of the MDR workflow, given how many IT teams struggle with alert overload.

Investigate

Automated tools and human expertise combine to dig deeper into alerts, performing data and log analysis in order to understand their nature and scope. They will need to calculate whether an alert is a true positive or not, and what steps must be taken to resolve it.

Respond

An effective MDR service will either provide basic response actions to block and contain the threat, or containment and full remediation of any compromized systems. The latter could entail a password reset, patching specific endpoints, or even reimaging computers.

The benefits of outsourcing detection and response are simple but compelling:

- The MDR provider takes care of all management of the back-end technology, freeing up staff to focus on high-value, strategic tasks rather than drowning in security alerts.

- The MDR provider may also optimize the backend technology to align with each customer's risk profile and infrastructure.

- With detection and response managed by a third party, there will be no need to pay hefty salaries to attract and retain the best cybersecurity talent.

- Customers can benefit from their provider's economies of scale, ability to attract the best talent, and insight into other customer organizations and threat environments.

Strengthen Your Cybersecurity with ESET MDR

Cybersecurity is an essential part of manufacturers' IT operations. Yet in most cases, it isn't their primary focus, nor should it be. They need to be able to concentrate on their core business, and leave the battle against a diverse, determined, and growing cohort of threat actors to the experts. This is where trusted security partners come in, bringing extensive resources and decades of industry expertise.

ESET MDR, designed for compatibility with diverse manufacturing infrastructure, helps protect your supply chains and operational technology. It ensures seamless integration with your existing ICS and OT security systems, providing a unified security posture for manufacturing environments, reduces the risk of unauthorized access, secures your cloud infrastructure, and facilitates compliance with security governance and regulatory policies.

Tailored services are available to meet the diverse needs of manufacturing businesses of all sizes. It's time to snuff out cyber risk with expert assistance.

LEARN MORE

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

ESET®
Digital Security
Progress. Protected.