Noiseless Security:

How ESET MDR Combines AI and Human Expertise to Protect Manufacturing

Cybersecurity
Progress. Protected.

Security Overload: Manufacturing Faces Rising Cyber Risks

With internal security operations teams receiving an average of 11,000 security alerts every day, it's no wonder they are struggling to keep up. The results of a survey published by IDC found that investigating each alert or false positive takes 25–30 minutes, leading to around 25% of alerts and false positives either being ignored or not investigated.

Companies with more resources aren't necessarily any better off, as both numbers hold true whether a company has 500 employees or more than 5,000.

The same IDC survey found that cybersecurity is a concern at the highest levels of corporate leadership. More than half of companies say that their boards are concerned about the costs of productivity losses or regulatory fines from cyberincidents as well as cyberinsurance costs. Again, both hold true regardless of the size of the company.

Internal security operations teams receive

11,000

security alerts every day.

If you're in a business role that makes you responsible for security in a manufacturing organization, the above must be especially troubling. The manufacturing sector is a high-priority target for threat actors because they know that a shutdown leads to revenue loss you can't get back.

Attacks that Made Headlines: Threat Actors Take Aim at Manufacturers

DUVEL MOORTGAT (2024)

At Belgian Brewer Duvel Moortgat, a ransomware attack triggered security alarms that alerted IT staff. They turned off the servers, shutting the production lines down, but the attackers still succeeded in encrypting and stealing a claimed 88GB of data. One of the five plants that was impacted was successfully brought back online from backups, but restoring operations at the other four plants took days.

The attackers imposed a two-week deadline for payment of an undisclosed ransom. The company refused to pay, and the data that included employee passport photos and internal company documents began appearing online.

MKS INSTRUMENTS (2023)

Semiconductor equipment maker MKS Instruments was hit by a ransomware attack that knocked out its ability to process orders or ship products. The company told federal regulators that controls around backup and restoration came up short, making it difficult for MKS to recover quickly, and that the attack cost the company $200 million in lost revenue.

In addition to encrypting business and manufacturing systems, MKS also said the hackers might have exfiltrated workers' Social Security numbers, bank account information, payment card information, and information about disabilities, health, and medical conditions. The data exposure triggered a class-action lawsuit filed by an ex-employee.

NORSK HYDRO (2019)

Norwegian renewable energy company and aluminum manufacturer Norsk Hydro was hit with ransomware, delivered by intercepting a legitimate email conversation and injecting a weaponized attachment. Attackers encrypted files on thousands of servers and PCs and locked out user accounts to prevent IT teams from accessing the affected systems.

Automated production lines were shut down. The company refused to pay the ransom, shifted to manual operations, and painstakingly restored the affected systems from backups. The total estimated cost was $70 million according to the company's earnings report.

BRIDGESTONE AMERICAS (2022)

Tire manufacturer Bridgestone Americas was hit by ransomware and out of an abundance of caution, disconnected many of its manufacturing facilities in Latin America and North America from the affected network.

The company was able to resume normal operations ten days later and at first, believed only business records had been stolen.

However, investigators later found that files containing consumer information had been exposed as well, including social security numbers and bank account information, forcing the company to send out data breach letters to the impacted individuals.

SCHNEIDER ELECTRIC (2023)

The Business Sustainability division of French multinational Schneider Electric suffered a data breach that compromised more than 40GB of data via access to the company's Atlassian Jira system.

The ransomware gang known as Hellcat, announced the breach on social media with this statement: "To secure the deletion of this data and prevent its public release, we require a payment of $125,000 in baguettes." The demand for payment in baguettes was interpreted to be a publicity stunt.

ESET Managed Detection and Response

Given the cyberthreats you face and the business pressures to prevent them from happening, how can you cut through the noise generated by multiple security tools that all generate their own alerts?

The answer is ESET MDR — a 24/7 cybersecurity service that continuously monitors your environment for threats, blocks and contains them before they can execute malicious behavior, and removes and remediates them.

Built on ESET's 30 years of cyber intelligence, ESET MDR harnesses that deep human experience and expertise and applies it at scale through cutting-edge artificial intelligence to cost-effectively protect your business.

How ESET MDR Reduces Alert Noise

ESET's ability to cut through the alert noise comes from a combination of automation, human intelligence, and artificial intelligence, all working together to eradicate the simplest threats and allow security analysts to focus on what really matters.

While it takes internal SOC teams 25–30 minutes to simply investigate a single alert, the ESET MDR service is able to detect, block, prevent further execution, and remediate an attempted attack in an average time of six minutes.

ESET Endpoint Protection detects malware and prevents it from executing on endpoints including laptops, desktops, smartphones, and servers running Windows, Linux, and MacOS. With 17 layers of protection, it achieves a 99.6% detection rate with zero false positives, as validated by the rigorous testing process of AV-Comparatives.

ESET Threat Intelligence, gathered by a worldwide team of security analysts at 11 R&D centers around the globe, monitors the activities of threat actor groups and tracks their tactics and techniques. Much of this intelligence is gathered by ESET LiveGrid, which collects telemetry from ESET-protected endpoints worldwide. This threat intelligence feeds the consoles of ESET Extended Detection and Response, manned by the ESET security analysts who deliver the MDR service.

ESET Extended Detection and Response ingests logs gathered from the ESET endpoints on the network and applies artificial intelligence to filter the noise and triage the most critical alerts. It then uses the knowledge of threat actor attacks furnished by ESET Threat Intelligence to apply yet another instance of artificial intelligence to identify patterns of alerts that indicate an attack is in progress, and packages it as an incident for priority investigation by human analysts.

Human analysts have control over ESET endpoints, allowing them to prevent attacks by killing processes or blocking them, while working with local IT as necessary for involved devices that cannot be directly accessed by ESET analysts.

MDR Ideal for Manufacturing Environments

Here are some of the reasons why ESET MDR is a great fit for manufacturers.

Multi-layered yet lightweight endpoint protection. Get the protection of 17 layers of security in a package that's designed to be light on system resource use and won't bog down key systems.

Protection for legacy systems. Many manufacturers have built-for-purpose systems running on older hardware and software (such as Windows 7, XP or others) that are past end-of-life and no longer have security patches and upgrades available. ESET continues to track the CVEs for legacy systems and develops detection capabilities for threats that target those vulnerabilities.

Protection that works 24/7 for zero-downtime operations. Your production lines need to keep running, and our worldwide operation supports that critical business need.

Protection for air-gapped systems. If you have especially sensitive systems or networks with proprietary data that require the high security of air-gapping, or you have an air-gapped OT network, ESET has several solutions that work as extensions of our MDR service.

Protection that scales with your environment. Bundled endpoint security packages, flexible per-seat licensing and tiered MDR solutions combine to give you highly scalable security that grows with you so you don't have to reinvest as your need for security evolves.

Protection that's fully transparent. The stakes are high in manufacturing security, and high-level executives and boards of directors need to know how you're protected. With ESET MDR, we furnish regular reports on incidents discovered and remediated to prove our performance.

Protection that works as an extension of your own IT. If your IT or dedicated security team is small, ESET MDR lets you delegate attack monitoring, incident response, and threat hunting to trusted, highly experienced specialists while your team has the same visibility we do through our intuitive dashboards.

Protection that's proactive. Proactive threat hunting included with our MDR service puts analysts on the lookout for threats, informed and powered by global intelligence from over 100 million endpoints.

Protection that's affordable. While ESET MDR service requires ESET Endpoint Protection, it works alongside other security tools and solutions to keep "ripping and replacing" to a minimum, and our service model delivers high-value protection at less than the cost of expensive consulting solutions.

ESET Services and Solutions for the OT Network

For operational technology networks that run the shop floor, ESET's MDR service protecting the IT network blocks the 75% of OT attacks that gain a foothold on the IT network and then move laterally to the OT network.[1] ESET security teams track the CVEs and monitor and analyze the threat reports and indicator-of-compromise lists related to OT environments.

ESET also tracks the threat actors targeting industrial control devices, both the larger APT groups as well as smaller crime groups that aren't classified as APTs but are known to target manufacturing.

Some of ESET's manufacturing customers take advantage of ESET knowledge of OT threats and opt to have the ESET MDR service protect the Windows-based computing devices on the OT network. This gives the ESET analysts visibility to the network traffic passing through those devices. Through this mechanism, ESET MDR is able to protect against threats that attack Windows devices and attempt to control or cripple PLCs, such as the PipeDream/InControlller toolkit.

1 Telstra, Secure Manufacturing: The Challenges of IT/OT Convergence

Still other manufacturers who have fully air-gapped or mostly air-gapped systems use the on-premises version of ESET XDR and monitor the security themselves. They have full use of the ESET threat intelligence that our own security analysts use, including updates on the latest tactics and techniques used by the attacker groups that target manufacturing.

Two Tiers of MDR Service

Choose the one that's right for your organization.

MDR

The base tier of MDR is designed to be affordable for smaller manufacturers with as few as 25 seats. ESET experts immediately contain the threat, take action by blocking files and processes, and then notify you of the actions taken and any additional steps you need to take.

- Notification of incidents and actions taken
- Optimization of the ESET Inspect MDR console at the backend level
- Continuous threat hunting
- Feedback to incidents
- Weekly & monthly reports

MDR Ultimate

Larger manufacturers at the enterprise level tend to have dedicated IT security admins who want to work with our analysts through an incident. ESET MDR Ultimate works as a seamless extension of your IT function. We contain the threat and then interact with your internal security personnel on complete remediation.

- Joint response to incidents with remediation guidance
- Optimized ESET Inspect console for your environment
- Continuous and on-demand threat hunting
- 24/7 availability to analysts
- Periodical reports with human interpretation

Parting Thoughts

If your IT team is struggling with multiple security point tools and the onslaught of alerts they generate, ESET MDR service cuts through the noise for you. Instead of security teams investigating each alert in isolation, artificial intelligence applies filtering and recognizes the attack patterns used by the threat actors, followed by either automated response or the intervention of human analysts to block, contain, and remediate the threat.

Take advantage of our deep knowledge of the threat landscape that manufacturers face to protect your business and operations.

LEARN MORE

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection, thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

eset
Cybersecurity
Progress. Protected.

© 1992–2025 ESET, spol. s r.o. – All rights reserved. Trademarks used herein are trademarks or registered trademarks of ESET, spol. s r.o. or ESET North America. All other names and brands are registered trademarks of their respective companies.