

Operational Technology (OT)



Table of contents

03

04

05

06

07

08

The challenge of securing OT

Operational Technology (OT) plays a vital role in keeping essential services running. When these services are disrupted, the impact extends far beyond data loss - it affects safety, production, and even entire communities. When it comes to securing OT systems, companies face significant challenges that leave them vulnerable to potential threats.



Poor visibility

Lack of visibility in an environment can adversely affect security and production. Identifying vulnerabilities before cybercriminals infiltrate systems is vital in OT networks, as it helps prevent unplanned downtime and mitigate operational disruptions.



OT/IT integration

The integration of IT and OT increases risk, as threats from the IT side can easily infiltrate unpatched OT systems. With an increased attack surface, cyber security teams are compelled to prioritize the security of OT environments.



Legacy infrastructure

Organizations managing OT infrastructure often heavily rely on legacy, unsupported operating systems. While gradually updating old infrastructure helps, limiting access to the most "remote" parts is key, as well as disabling non-standard ports and regularly scanning networks for potential threats.



Cloud attack surface

Combining cloud services with integrated IT/OT creates a more vulnerable attack surface. Cybercriminals are exploiting insecure OT devices to gain unauthorized access to cloud infrastructure.

Holm Security meets the threat head-on

At Holm Security, we extend our vulnerability management capabilities beyond traditional IT systems to include Operational Technology, providing complete visibility across both digital and industrial networks.

Fast and precise asset discovery

Our active scanner goes beyond passive monitoring. It actively engages with OT devices to uncover what others miss. It identifies hidden or silent assets, collects software and firmware details, and highlights vulnerabilities and misconfigurations. You'll gain clear visibility into open ports, installed applications, security settings, and even indicators of known threats - helping you build a stronger, more resilient OT environment.



Unauthenticated & authenticated scanning

Unauthenticated scans use an outside-in approach, assessing endpoints, servers, and infrastructure without requiring a login. Authenticated scans go deeper, using credentials to access devices and examine them from the inside out. When combined, these methods provide a comprehensive view of your OT environment, helping you identify hidden risks.



Agent-based asset discovery

In OT environments, many devices are hard to detect through network scanning alone. Our lightweight endpoint agent ensures accurate asset discovery, continuous monitoring, and faster identification of vulnerabilities - without disrupting critical operations.

Supervisory Control and Data Acquisition (SCADA)

A tailored SCADA scan configuration

We've developed a dedicated SCADA scan configuration designed to minimize operational impact while still uncovering critical weaknesses. Our scanner supports systems from over 75 different OT and SCADA vendors, with coverage consisting of more than 1,600 vulnerability tests and over 3,700 unique vulnerabilities across industrial infrastructures. This extensive coverage includes key components, such as SCADA servers, engineering stations, and control-level devices, including PLCs and HMIs.

Covering 75+ vendors



Industrial protocol awareness

Our platform also understands the industrial protocols that power these environments, including Modbus/TCP, Profinet, EtherNet/IP addresses, Siemens S7, OPC, IEC 60870-5-104, and DNP3. This deep protocol awareness allows us to safely assess systems that traditional IT-focused scanners cannot, offering a comprehensive and reliable view of vulnerabilities across the entire OT ecosystem.

One platform with unified products

Our platform includes powerful products integrated with one workflow and risk model.



System & Network Security

Identifying over 200,000 vulnerabilities across business-critical systems/servers, computers, network devices, office equipment and IoT, OT (Operational Technology), and cloud platforms.



Web Application Security

Advanced assessment technologies to identify thousands of vulnerabilities, including OWASP Top 10, in modern web applications.



Cloud Security (CSPM)

Secure your cloud-native platforms by identifying thousands of vulnerabilities across Microsoft Azure, AWS, Google Cloud, and Oracle Cloud — providing proactive protection for your entire cloud ecosystem.



API Security

Assess your APIs for hundreds of vulnerabilities, including those in the OWASP API Top 10, to ensure robust security and safeguard critical data.



Phishing Simulation & Awareness Training

Conduct simulated phishing attacks paired with customized awareness training to build continuous vigilance and strengthen your human firewall.

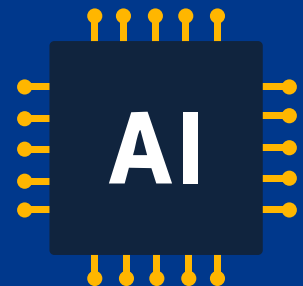
How secure is your organization compared to your industry colleagues?

Based on data from our large customer base across industries, we help you understand your organization's risk exposure compared to others in the same industry.



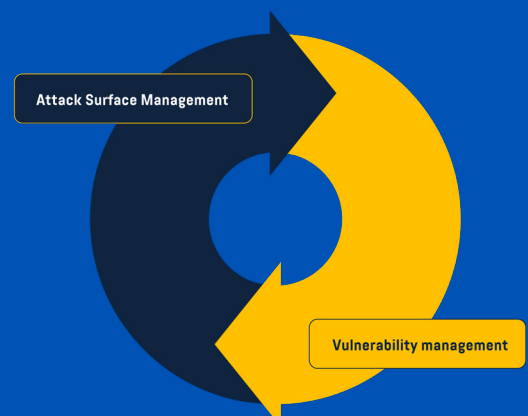
AI-driven threat intelligence – faster, broader & more secure

Our AI-powered Security Research team keeps you updated with the latest vulnerabilities – around the clock, all year round.



Integrated Attack Surface Management (ASM)

Integrated Attack Surface Management fully automates the entire process, from asset discovery and continuous monitoring to identifying vulnerability findings.



Meet today's & future compliance

The future is characterized by a growing number of compliance demands focusing on a systematic and risk-based cyber defense. Organizations can expect more local, regional, and industry-based regulations in the future.



NIS & NIS2

The NIS and NIS2 Directives (entering into effect through 2024 and 2025) require a systematic and risk-based cyber security approach. Holm Security has helped hundreds of organizations comply with the NIS Directive.

GDPR

Our platform helps organizations meet General Data Protection Regulation (GDPR) requirements for regular security assessments and vulnerability testing to identify and address potential vulnerabilities and protect against data leakage.

ISO 27001

To comply with ISO 27001, an organization must establish and maintain an Information Security Management System (ISMS) that meets the standard's requirements. This includes continuous risk assessments to find vulnerabilities.

TISAX

We help organizations in the automotive industry comply with the Trusted Information Security Assessment Exchange (TISAX), ensuring that they have documented processes for finding, assessing, and remediating vulnerabilities to protect against cyber threats.

Why Holm Security?

1 Understand your attack surface

One of the key functions in Next-Gen Vulnerability Management is to help understand your attack surface using automated techniques to continuously identify new assets that could potentially expose your organization to risk.

3 Powerful threat intelligence

Our platform lets you focus on high-risk vulnerabilities and users likely to be exploited. Understand the full context of each exposure to maximize your efforts. Our platform also provides superior built-in threat intelligence to help understand and prioritize risk more efficiently.

2 Unified view to ease prioritization

Reduce business-critical risks with the least amount of effort. This is accomplished by providing a truly unified platform where all your risks are prioritized and listed in one single view.

4 Let the platform do the work

Our platform is fully automated. Once it's been implemented, it runs continuously in the background. No need for software or hardware.

How can we help?

Want to get in touch? We'd love to hear from you. Here's how you can reach us.

+46 8-550 05 582
sales@holmsecurity.com
www.holmsecurity.com

