

CASE STUDY

Large Industrial Company Validates Threats and Aligns Security Program to Business Goals

Expanding Beyond Threat Hunting

Proactive security is vital to this large industrial company, but its primary service provider only focused on threat-hunting. The security team wanted a more comprehensive approach that could also help fulfill its compliance requirements.

The team looked for a solution that could provide:

- A complete picture of its security posture.**
 The team wanted to know which security tools and processes were working and where there were gaps so it could focus its resources where they were needed most.
- Insights into its security restrictions.**
 Endpoint security is vital for a manufacturing organization, but it can also have adverse side effects and cause specific applications to fail, slowing down the business. The security team wanted to ensure a good balance between its endpoint security and its business goals.
- Data on security performance against emergent threats.**
 The company wanted to continuously assess its defenses against immediate threats so it could confidently report to management how it would perform against such an attack.

The Cymulate Solution

The team evaluated a few security validation platforms, but during a 30-day trial with Cymulate, it quickly saw that Cymulate checked all its requirements.



We immediately saw the value Cymulate could provide our organization.”

— CISO

Overview

Industry	Manufacturing
HQ	Middle East
Company Size	5-10K employees



Cymulate gives me peace of mind and confidence in our cybersecurity.”

— CISO

Use Case

- Threat Validation

Results

- Continuous and automated third-party validation
- Daily validation of latest threats
- Comprehensive view of security posture

The CISO explained that the security team uses Cymulate to balance security and business priorities, demonstrate compliance, rationalize security investments, extend validation across IT and OT environments and rapidly test defenses against emerging threats.

Balance security goals with business goals

“By running attack simulations with Cymulate, we can determine the minimal security restrictions required to keep our organization safe and running efficiently. We no longer add to our security stack just because it seems it would help — we test and see if the new tools, configurations or segmentation ensure more protection or add restrictions for no reason.”

Proof of compliance

“Because we continuously track our security performance with Cymulate, I always show the platform’s analytics during our compliance audits. They appreciate that I consistently have a third party evaluate my security, which gives them an unbiased perspective. Additionally, I can show them that even if an attack penetrates my defenses, I still have compensating controls to protect the organization.”

Rationalize investments

“With Cymulate, we are more confident in our communication with leadership. We know with certainty where we are strong and weak, and we can rationalize our investments.”

Extend the scope to OT

“After seeing the benefits in the corporate network, we extended the Cymulate endpoint assessment to our OT endpoint devices. It enabled us to see the differences in protection between IT and OT devices.”

Test against emergent threats

“Whenever a new Cymulate threat is released, we automatically run an assessment to evaluate our protective strengths and also identify any vulnerabilities. This is very useful for providing rapid assurance to our management.”

Benefits

- **Baseline and improve performance.** Cymulate enables the team to gradually strengthen its cybersecurity by providing a benchmark and monitoring performance.
- **Security insights.** The team has a comprehensive view of its cybersecurity and can make data-based decisions to promote the organization’s business goals without compromising its cybersecurity posture.
- **Great customer support.** The Cymulate team assisted the organization with initial product implementation and continues to be a supportive partner in its cybersecurity journey.

About Cymulate

Cymulate is the leader in proactive, AI-powered security that continuously proves, prioritizes and adapts against real attacker behavior – before incidents occur. More than 1,000 enterprise security teams rely on Cymulate for autonomous threat validation and cyber defense engineering. Founded and led by experienced red teamers who know that testing alone does not deliver better security, Cymulate goes beyond threat validation to build threat- and exposure-informed cyber defenses. For more information, visit www.cymulate.com.