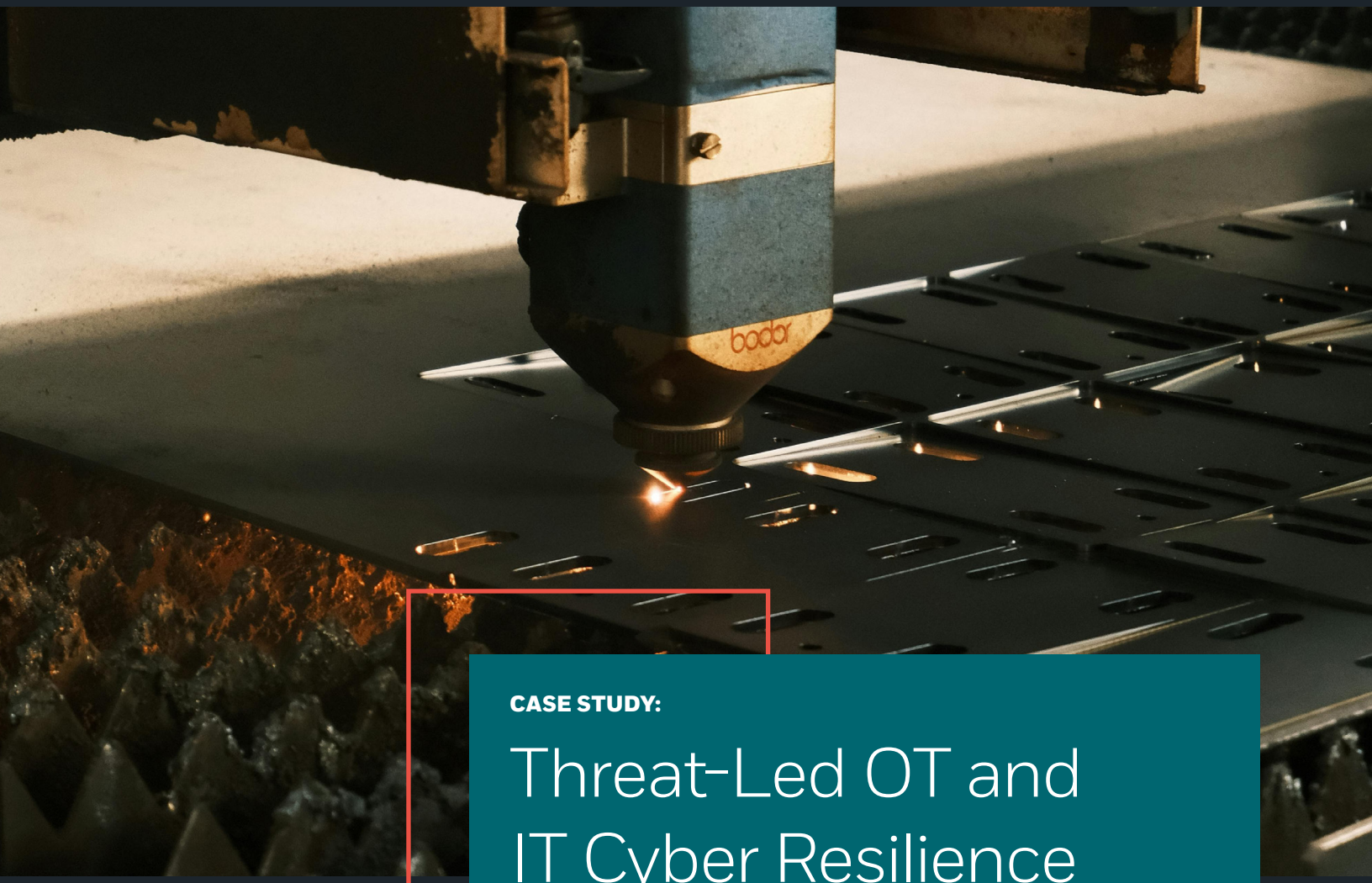
CyberProof®
A UST Company

Better Security,
Together.



CASE STUDY:

Threat-Led OT and IT Cyber Resilience for a Leading U.S. Manufacturing Conglomerate

INDUSTRY: MANUFACTURING

About the Client

The client is a Fortune 500 U.S. manufacturing conglomerate with more than $12B in annual revenue and 5,000+ employees. Operating across 60 facilities, the company integrates IoT-driven smart machinery and OT systems to optimize production, but this also expands its attack surface.

The client's challenge

The manufacturer approached CyberProof to strengthen security across 60 global facilities and more than 5,000 endpoints. The client required a partner capable of delivering 24×7 monitoring, continuous exposure management, and threat-led detection tailored to industrial environments.

Key challenges included:

- Rising OT/IoT threats: Increasing ransomware and supply chain attacks targeting smart factory infrastructure.
- Limited visibility: Siloed monitoring across IT and OT systems created blind spots and delayed detection of lateral movement.
- Expanding attack surface: Legacy assets, third-party vendors, and decentralized networks introduced new exposures.
- Detection and response: Difficulties aligning detection and response strategies with critical operational use cases.

Key Benefits

Unified IT/OT visibility: The Armis-CyberProof platform integration closed visibility gaps and increased security visibility by unifying IT, OT, and IoT monitoring.

Faster detection and response: The manufacturer reduced mean time to detect by 23% and mean time to respond by 29%, accelerating containment of threats before business disruption could occur.

CTEM implementation: A Continuous Threat Exposure Management program prioritized risks, validated defenses, and aligned detections to adversary techniques targeting manufacturing systems.

Regulatory alignment and reporting: This was improved using CyberProof dashboards tailored for manufacturing compliance standards like IEC 62443 and NIST CSF.

Our solution

CyberProof partnered with the client to build an integrated, future-proof cyber defense strategy across IT and OT domains. The deployment featured:

1 24x7 Managed Detection & Response (MDR

Using the CyberProof CDC Reveal360 platform, CyberProof delivered round-the-clock monitoring, threat detection, and rapid incident response across IT, cloud, and OT environments. This reduced mean time to detect (MTTD) by 23% and mean time to respond (MTTR) by 29%, shrinking adversary dwell time and minimizing exposure windows. Services were provided from CyberProof's Ohio SOC during business hours and from the Trivandrum, India SOC outside of business hours.

CyberProof's virtual analyst automated alert triage and incident enrichment, cutting response times significantly.

2 OT/IoT Visibility & Threat Detection via Armis

CyberProof's solutions are integrated with Armis to gain passive, agentless visibility across the client's OT and IoT networks. This integration allowed the platform to ingest Armis telemetry and correlate it with threat intelligence, alerting, and incident management pipelines.

This closed critical OT/IoT blind spots and reduced the risk of ransomware lateral movement from IT into OT systems.

3 Threat Exposure Management via Interpres Integration

CyberProof's CTEM platform assessed and prioritized risk across critical OT assets, correlating Armis visibility data with Google Threat Intelligence and MITRE ATT&CK coverage. This enabled continuous validation of detection coverage and readiness across both legacy systems and modern infrastructure.

CTEM outputs were maintained as a prioritized exposure backlog with clear owners and remediation SLAs aligned to operational criticality.

4 Use Case Management & Operationalization

CyberProof's Use Case Management team developed tailored use cases, which were mapped to operational workflows.

For example:

- Visibility Use Case: Monitoring unauthorized device behavior in OT networks.
- Operational Use Case: Alerting on changes in PLC configuration patterns.
- Playbook: Automated isolation of the affected OT segment and notification to plant operations.

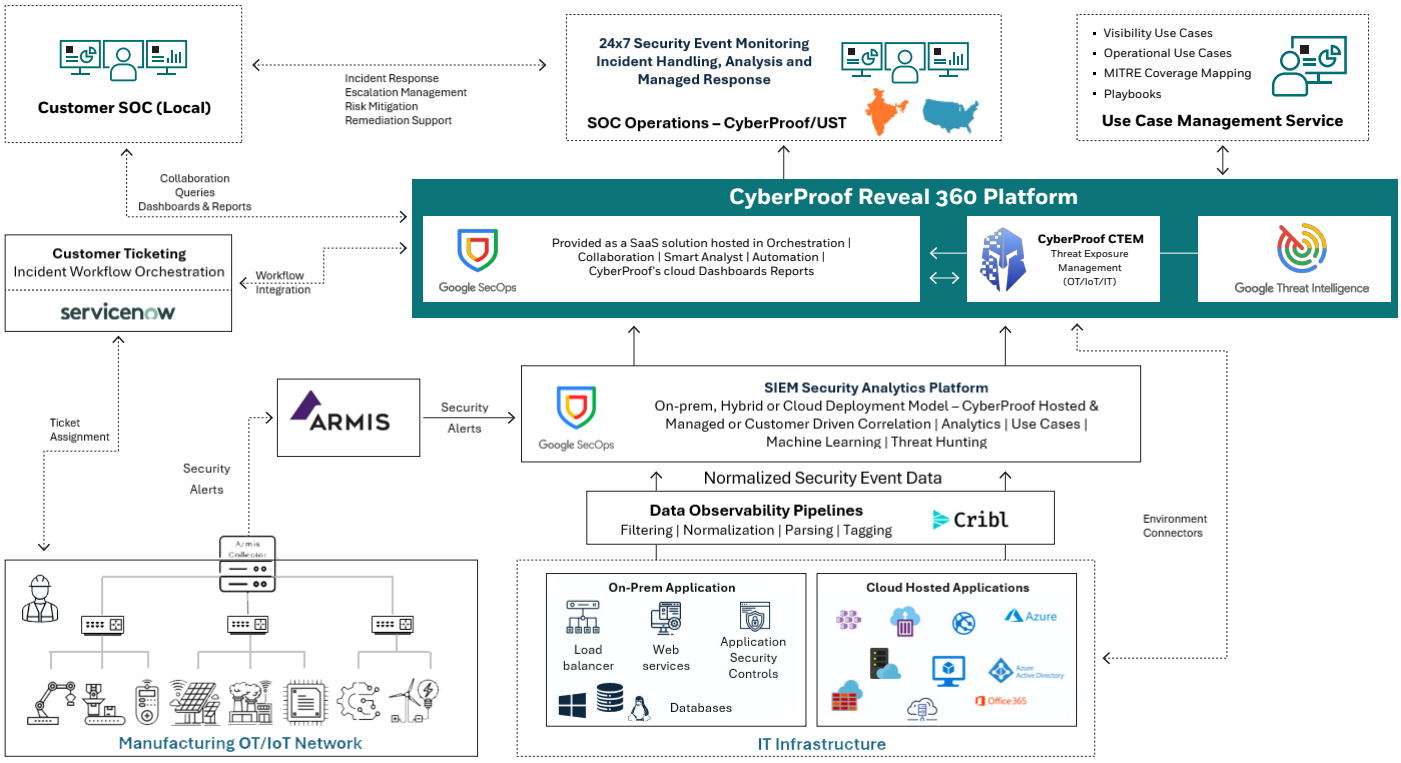
All use cases were mapped to MITRE ATT&CK to ensure coverage of high-risk techniques and to measure detection effectiveness over time.

5 Google Threat Intelligence

Google Threat Intelligence (Mandiant) was leveraged to enrich threat data and identify emerging threats relevant to manufacturing environments, including tactics used by groups targeting industrial controls. These were mapped to CyberProof CTEM for continuous improvement and contextual threat hunting.

This shifted posture from reactive monitoring to intelligence-led defense, enabling anticipatory hardening of OT segments against emerging TTPs.

Cyber Resilience for a Leading U.S. Manufacturing Conglomerate



CyberProof's CDC Reveal360 platform was instrumental in delivering a unified and real-time view of security operations across the client's complex IT and OT environments. Integrating with Armis for IoT/OT visibility, using CyberProof CTEM for threat exposure management, and Google Threat Intelligence for intelligence enrichment, CyberProof provided deep insights and proactive threat coverage.

With the deployment of advanced MDR services, use case engineering, and automated playbooks, the client dramatically improved detection accuracy, accelerated response times, and closed critical visibility gaps. Today, the client operates a highly adaptive and resilient cyber defense ecosystem—supported by continuous exposure management and a unified, risk-aligned approach to operational security.

CyberProof®
A UST Company

Better Security,
Together.

About CyberProof

CyberProof, a UST company, delivers better security operations and drives superior experiences for enterprise customers. Our cloud-first, AI-powered approach to security delivers industry-leading services to drive real business results. We believe that working closely with our customers and partners through a 'better security, together' services model jointly empowers us to defend against the greatest of threats. See: www.cyberproof.com.

Barcelona | California | London | Singapore | Tel Aviv | Trivandrum

© 2025 CyberProof Inc. All Rights Reserved.