CyberProof®
A UST Company

CYBER SECURITY SERVICES FOR CONVERGED IT/OT SYSTEMS

PROACTIVELY DETECT & RESPOND TO THREATS ACROSS YOUR OT SYSTEMS

As Operational Technology (OT) and IT networks become increasingly interconnected, sensitive data and entry points can be exploited by attackers. CyberProof helps organizations detect and respond to threats across converged IT/ OT ecosystems with an integrated Security Operations Center.

HOW CYBERPROOF CAN HELP

VISIBILITY INTO CRITICAL OT ASSETS

Challenge: You can't defend what you can't see. Attackers are often able to compromise OT networks without being detected because organizations don't have an updated inventory of their OT assets or their related processes and connections.

Solution: The CyberProof Defense Center (CDC) platform is pre-integrated with leading OT threat detection technologies, enabling real-time visibility into networked assets, ports, and protocols and changes. This enables the discovery of previously unmapped assets in IT & OT environments and maintenance of a centralized dynamic inventory.

EFFICIENT DETECTION AND RESPONSE ACROSS BOTH IT & OT NETWORKS

Challenge: Attackers target both IT & OT networks to compromise critical data. The data flowing between these environments is unfamiliar to security analysts when investigating malicious activity on Programmable Logic Controllers (PLCs), Human Machine Interfaces (HMIs), or SCADA servers.

Solution: A team of SOC experts, CTI analysts and Threat Hunters proactively monitors, investigates, and responds to threats across your IT & OT environment, with full transparency via the CDC platform.

PROACTIVELY IDENTIFY AND FIX HIGH-RISK VULNERABILITIES

Challenge: Threat exposure is distributed across various legacy and emerging environments – physical servers, hosts, serverless, remote working environments, IT or OT networks, and hybrid environments. This makes it difficult to prioritize the vulnerabilities that impact your business the most.

Solution: Our team supplements the OT security vulnerability databases and scanning tools with our proven threat-centric vulnerability management framework to discover, prioritize, and validate high-risk vulnerabilities and exposures.

OUR SERVICES

- **Threat Detection and Response -** Automatically profile all assets, communications, and processes in industrial networks. Generate a behavioral baseline that characterizes legitimate traffic to weed out false positives, and alert users in real time to anomalies and known, unknown or emerging threats.

- **Asset Visibility and Intelligence –** Leverage the broadest protocol coverage visibility into all three variables of risk in the industrial network: OT, IoT, and IIoT assets, connections, and processes.

- **Threat Intelligence –** Obtain a highly curated, multi-source, and tailored feed that enriches Root Cause Analytics with proprietary research and analysis of OT zero-day vulnerabilities and ICS-specific indicators of compromise (IoC) linked to adversary tactics, techniques, and procedures (TTP).

- **Vulnerability Management –** Proactively identify and fix configuration and other network hygiene issues that can leave OT networks and sites vulnerable to attacks. Leveraging proprietary intelligence, we continuously monitor the network for new vulnerabilities.

# CYBERPROOF DEFENSE CENTER (CDC) PLATFORM

CyberProof provides access to the CDC platform as part of our service, enabling orchestration, automation and collaboration – and integrating and accelerating IT/OT security operations with full transparency:

- **Single interface** view of SOC activities

- **Customized reporting** to measure tailored KPIs and summarize EDR incident handling

- **Orchestration** to integrate with various sources and technologies

- **SeeMo, our virtual analyst,** who automates previously manual analyst tasks and provides helpful alert insights

- **Chatops collaboration** with stakeholders and our teams in real time

SERVICE ARCHITECTURE

Our service architecture leverages the full breadth of expertise provided by our skilled, global team – and our proven threat management processes (with defined roles), real-time collaboration and escalation procedures, and platform-led technology delivery – allowing us to integrate multiple tools into a single view via our CDC platform.
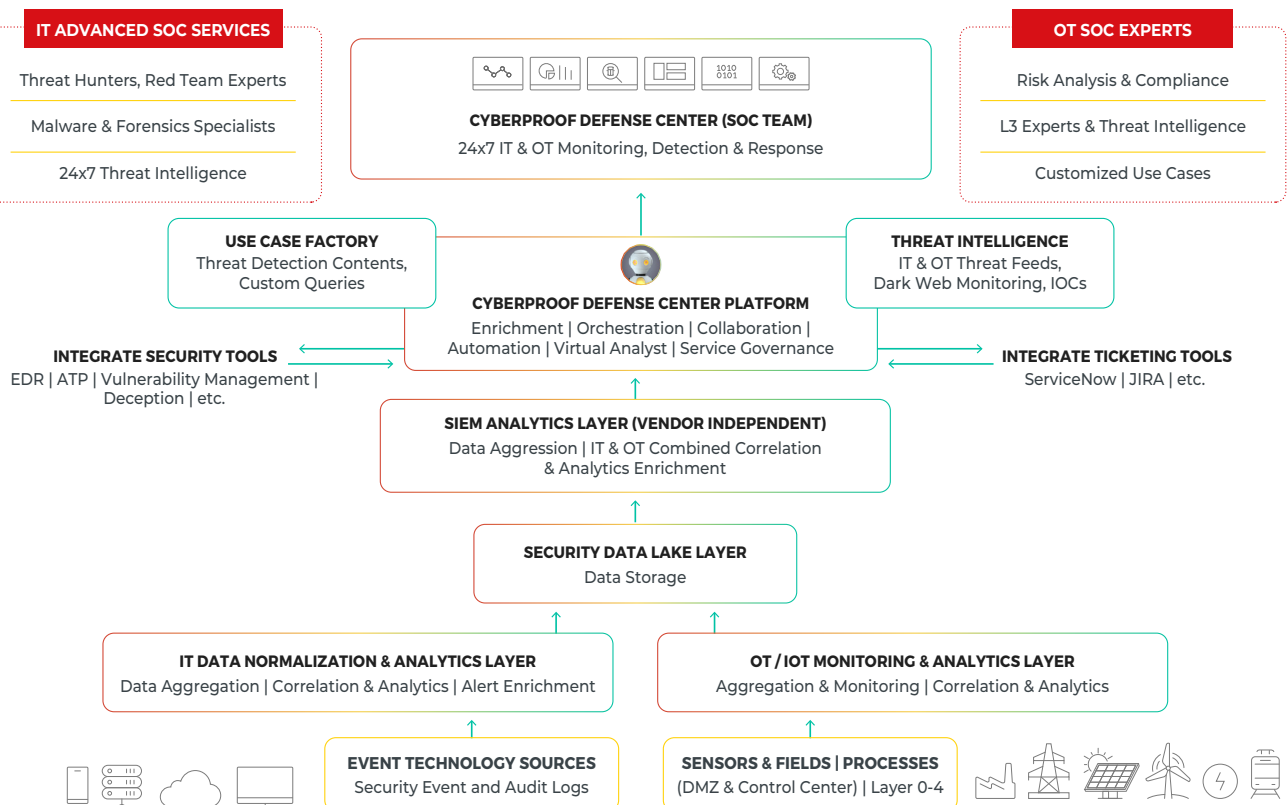
WHY CYBERPROOF?

Independently Recognized Leader – An MDR award winner, we were recognized as "Leader" by Forrester in the Midsize Managed Security Services Market in 2020 – and by ISG in their 2021 Provider Lens Report for Managed Security Service Providers in North America and France.

Trusted Partner for Both IT & OT SOC – CyberProof serves as a single security services partner – one provider helping you with OT threat detection and supporting a broad range of protocols & vendors, while providing advanced MDR capabilities for your IT network.

CDC Platform Provides Transparency and Collaboration – CyberProof's platform provides a collaborative environment with real-time ChatOps to coordinate between internal and external teams and maintains complete transparency into security operations.

Continuous Improvement – We use our curated library of threat detection and response Use Case content to continuously configure and tune customized detection rules, response playbooks, and third-party integrations.

ABOUT CYBERPROOF

CyberProof is a cyber security platform and services innovator that is dedicated to helping companies use information technology to solve business problems without the fear of cyber-attacks. To achieve this, we combine our expert talent and SeeMo, our virtual analyst, with the power of strategic partnerships, visionary clients and academia.

Our enterprise-scale approach allows us to effectively anticipate, adapt, and respond to cyber threats in an increasingly connected world while reducing complexity, and provide our customers with unmatched adaptability, transparency, and control.

CyberProof is part of the UST family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services. For more information, see: www.cyberproof.com

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