CyberProof®
A UST Company

MANAGED DETECTION & RESPONSE (MDR)

RAPIDLY DETECT AND RESPOND TO VALIDATED INCIDENTS ACROSS YOUR IT ESTATE

Security teams are struggling to reduce the time to detect and respond due to complexity and volume of alerts being generated from multiple security technologies. CyberProof's MDR service enables you to detect and respond to validated threats faster without adding more the complexity to your security infrastructure.

FASTER DETECTION & RESPONSE

The CyberProof Defense Center (CDC) platform includes SeeMo, our virtual analyst, who can automate up to 85% of L1+L2 activities including alert monitoring, enrichment, triage, investigation and issue containment. Our human analysts, along with SeeMo, work with you in a hybrid engagement model to support IR activities - or, depending on the defined workflow, automated response playbooks can be deployed.

SINGE VIEW OF SECURITY OPERATIONS

Our lightweight, open API architecture enables us to integrate the CDC platform with your existing security investments without additional infrastructure. It correlates limitless volumes of data regardless of where it resides to provide a single pane of glass view of enriched alerts and incident handling activities.

PROACTIVE INCIDENT HANDLING

Our global response team proactively carry out detailed investigations to search across the enterprise for signs of suspicious activity and remediate threats using tailored responses.
We use our curated library of threat detection and response content to continuously configure and tune customized detection rules and response procedures, accessible by the customer as Use Case Kits.

WHAT'S INCLUDED?

- **24x7 Security Monitoring –** round-the-clock security alert monitoring, enrichment and triage
- **Incident Handling –** incident investigation, issue prioritization and response process aligned to leading industry standards and incident handling methodologies
- **Tailored Threat Intelligence –** active monitoring of multiple threat sources across the clear, dark and deep web, and real-time visibility of targeted threats to organizations' specific assets, data and people
- **Remote & On-Site Incident Response –** DFIR experts who work in close collaboration with your technical and executive teams to prepare for, respond to and recover from a cyber breach
- **Multi-Layered Threat Hunting –** usage of a unique combination of sources to search for threats lurking in your envionrment including known IOCs, incident information, proprietary threat intelligence, MITRE blind spots and behavior anomolies
- **Continuously Optimized Use Cases & Digital Playbooks –** efficiently manage incident workflows
- **Real-Time Collaboration –** transparent activities providing you with support for issue containment, remediation, risk mitigation, and personalized reporting

HOW IT WORKS

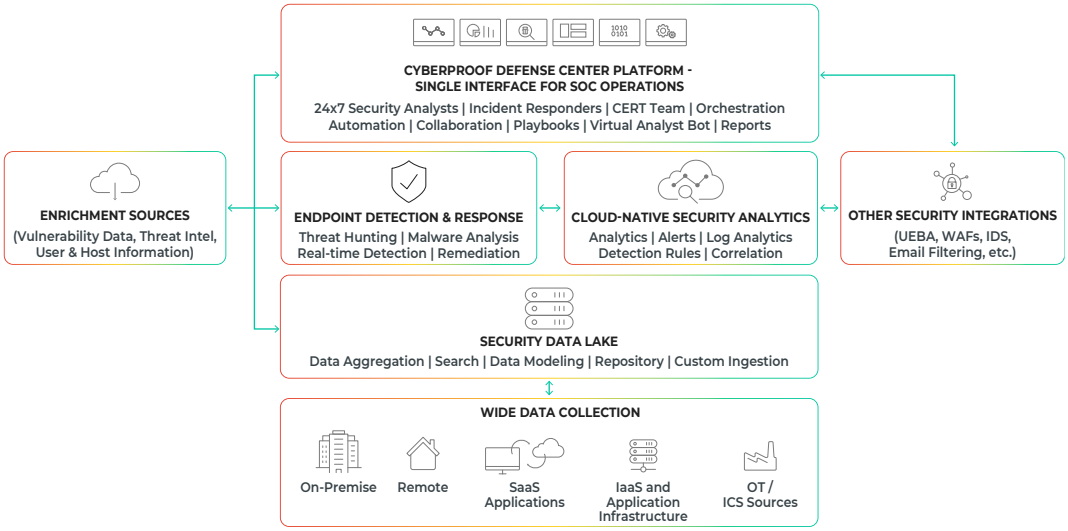
SINGLE INTERFACE view of security operations with real-time support from our analysts

END-TO-END SECURITY alert monitoring & enrichment, threat detection & response, incident remediation and threat hunting

EDR/SIEM PLATFORM MANAGEMENT covering deployment, configuration & tuning

LIMITLESS DATA COLLECTION, correlation and tagging from multiple sources

TELEMETRY INTEGRATION AND ANALYSIS across endpoints, the network, applications, the cloud and OT



CYBERPROOF DEFENSE CENTER (CDC) PLATFORM

WHY CYBERPROOF?

Independently Recognized Leader - CyberProof is a MDR award winner and recognized as a "Leader" by Forrester in the midsize managed security services market

SeeMo, Your Virtual Analyst Bot - SeeMo acts as a virtual member of your team to automate L1+L2 SOC activities and significantly reduce human effort

Continuous Improvement - Our Use Case Factory continuously optimizes tailored use cases consisting of prevention controls, detection rules and automated response playbooks

Transparency and Collaboration - Our platform facilitates real-time collaboration and provides transparency into security operations

Hybrid Engagement Model - Flexible, hybrid model so you only use what you need from us with complete transparency

Modernized, Cloud-based Security - Our platform allows you to scale up and down services as needed without upfront infrastructure investment

Leverage Existing Infrastructure - We can integrate with your existing technology investments or augment your SOC with the latest capabilities from our ecosystem of innovative vendor partnerships

ABOUT CYBERPROOF

CyberProof is a security services company that intelligently manages your incident detection and response. Our advanced cyber defense platform enables operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact. SeeMo, our virtual analyst, together with our experts and your team automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts to prioritize the most urgent incidents and proactively identify and respond to potential threats.

We collaborate with our global clients, academia and the tech ecosystem to continuously advance the art of cyber defense.

For more information, see: www.cyberproof.com

LOCATIONS

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