CyberProof®
A UST Company

Cloud-scalable Threat Detection and Response services

Pre-integrated with Microsoft Sentinel and Defender for Endpoint

cyberproof.com

Security teams are struggling to reduce the time to detect and respond to threats due to the complexity and volume of alerts being generated from multiple security technologies. Migrating to the cloud also brings forward an additional layer of complexity which requires constant vigilance for early signs of a cyber attack.

To help solve these challenges, CyberProof has partnered with Microsoft to provide cloud-scalable security monitoring, threat detection, and response services across your IT estate.

Reducing alert fatigue and speeding up detection and response

Our proprietary service delivery platform, the CyberProof Defense Center (CDC) Platform, uses Automation, Orchestration, and Collaboration features to:

- Provide a single view of security operations
- Speed up detection and response capabilities
- Facilitate real-time communication with our nation-state level analysts to help remediate incidents

Harnessing Microsoft Sentinel's cloud-native SIEM – without overhead

Microsoft Sentinel is pre-integrated with the CDC Platform, so clients can see value straight away by dramatically reducing the number of alerts while automating SOC tier 1 and 2 activities such as alert enrichment, escalation, investigation, containment, and remediation.

Hunting and response with Microsoft Defender for Endpoint (MDE)

Our EDR engineers can set up, configure, and manage MDE platforms on behalf of our clients. Our CDC platform integrates with MDE to act as a single interface for providing 24x7 advanced threat detection, hunting, and response services.

KEY FEATURES

- 24x7 monitoring, alert triaging, and investigation, freeing up your team to focus on high priority activities
- Machine Learning and Behavioral Analysis can reduce alert fatigue by up to 90%
- Large-scale collection and correlation of data from endpoint, cloud, network, and identities for high-context alerts
- Increase your SOC team's efficiency by leveraging our CDC platform's automation and orchestration capabilities
- Agile development and optimization of Use Cases to continuously adapt to the latest threats
- Proactive threat hunting using IOC retrohunting, intelligence from our CTI team, and behavioral analysis techniques

OUR SERVICES

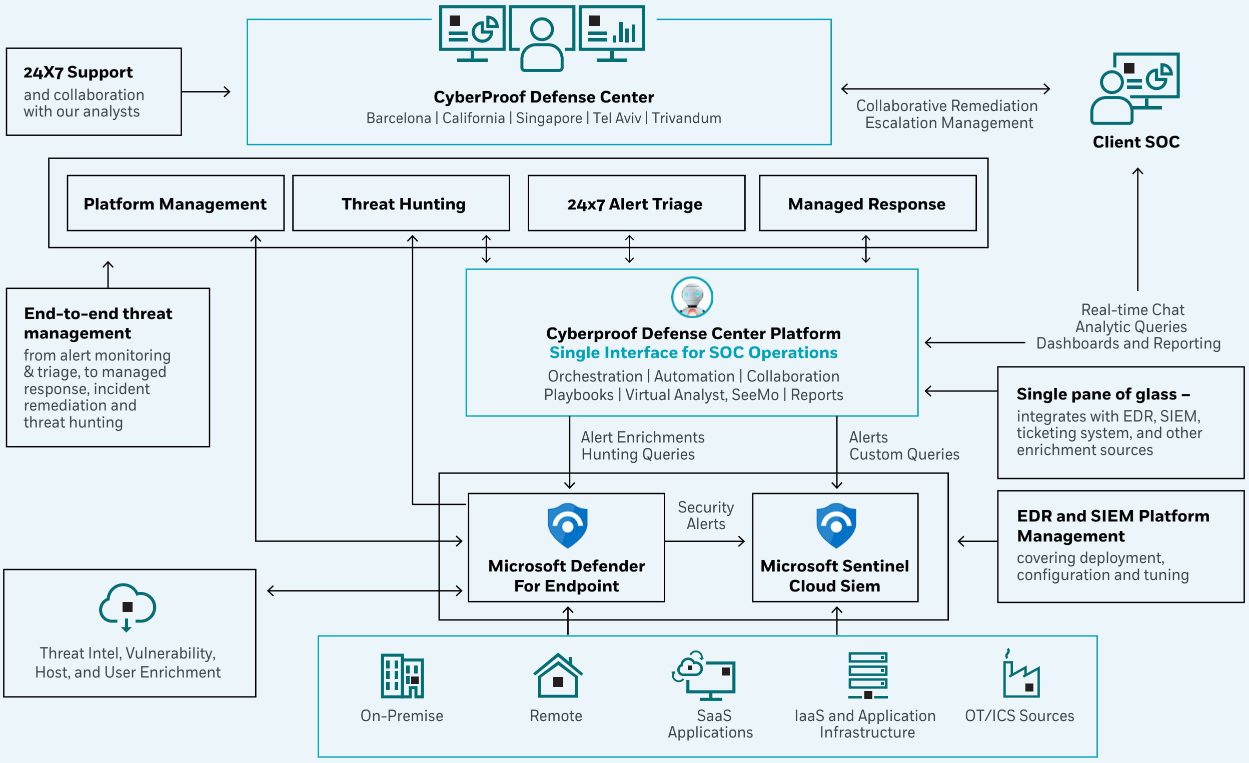
- Security Event Monitoring
- Managed Detection and Response
- Managed Endpoint Detection and Response
- Advanced SOC Services
- Agile Use Case Management
- Security Platform Management

KEY OUTCOMES

Single View of Security Operations: The CDC is preintegrated with Microsoft Sentinel and Defender for Endpoint to provide a single pane of glass.

Shorter Detection & Response Time: Next-generation SOC capabilities drive operational efficiency and dramatically reduce the cost and time required to respond to security threats.

Dashboards & Reporting to Measure Risk: The CDC supports tailored risk scoring and operational dashboards & reporting – providing insights for internal and multi-layer client stakeholders and for compliance purposes.


24X7 Support
and collaboration with our analysts
CyberProof Defense Center
Barcelona | California | Singapore | Tel Aviv | Trivandum
Collaborative Remediation
Escalation Management
Client SOC
Platform Management
Threat Hunting
24x7 Alert Triage
Managed Response
End-to-end threat management
from alert monitoring & triage, to managed response, incident remediation and threat hunting
Cyberproof Defense Center Platform
Single Interface for SOC Operations
Orchestration | Automation | Collaboration
Playbooks | Virtual Analyst, SeeMo | Reports
Real-time Chat
Analytic Queries
Dashboards and Reporting
Single pane of glass –
integrates with EDR, SIEM, ticketing system, and other enrichment sources
Alert Enrichments
Hunting Queries
Alerts
Custom Queries
Security Alerts
Microsoft Defender For Endpoint
Microsoft Sentinel Cloud Siem
EDR and SIEM Platform Management
covering deployment, configuration and tuning
Threat Intel, Vulnerability, Host, and User Enrichment
On-Premise
Remote
SaaS Applications
IaaS and Application Infrastructure
OT/ICS Sources

SERVICES ARCHITECTURE

How we transition you to a smarter SOC

Discover & Plan

- Understand your business goals, security objectives, and the maturity of your current SOC processes
- Identify and document a transformation plan to modernize your security's operational technology and capabilities

Onboard & Enable

- Set up Microsoft Sentinel and Defender for Endpoint in line with a plan for people, process, and technology
- Connect to existing or new Microsoft solutions (Microsoft Defender for Cloud, SaaS applications, etc.) and other cloud, on-prem. or hybrid environments

Migrate & Transition

- Connect Microsoft Sentinel and Defender for Endpoint to the CDC platform to have a single interface for managing security operations
- Configure custom detection rules, use cases, and playbooks to automate Tier 1 + 2 tasks and speed up detection and response

Operate & Manage

- Provide continuous Security Event Monitoring, Threat Detection & Response services
- Monitor and enrich security alerts and triage issues - investigating incidents and supporting with remediation and recovery activities
- Create customized dashboards and reporting as well as actionable threat intelligence on targeted threats

Why CyberProof

Recognized as "leader" by Forrester in the midsize managed security services market

Our virtual analyst bot significantly reduces human effort

Use Case Factory continuously improves your defenses

Flexible, **hybrid engagement model** for a true partnership

Our platform facilitates **collaboration** and provides **transparency**

Delivered the **largest and most complex** deployment of Microsoft Sentinel in the world

CyberProof®
A UST Company

About CyberProof

CyberProof, a UST company, helps our clients transform their security to a cost-effective, cloud-native technology architecture. Our next-generation Managed Detection & Response (MDR) service is built to support large, complex enterprises by combining expert human and virtual analysts. Our services are enabled by our purpose-built platform, the CyberProof Defense Center – enabling us to be more agile, collaborate better, and deliver powerful analytics. Our integrated security services include Threat Intelligence, Threat Hunting, and Vulnerability Management. Our experts innovate to meet our clients' needs with custom use cases, integrations, and automations.

For more information, visit www.cyberproof.com

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