CyberProof®
A UST Company

CLOUD-SCALABLE THREAT DETECTION & RESPONSE SERVICES

PRE-INTEGRATED WITH MICROSOFT AZURE SENTINEL AND DEFENDER FOR ENDPOINT

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. Migrating to the cloud also brings an additional perimeter which requires constant vigilance for early signs of a cyber attack.

To help solve these challenges, CyberProof have 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.

AZURE SENTINEL – HARNESS THE POWER OF A CLOUD-NATIVE SIEM WITHOUT THE MANAGEMENT OVERHEADS

Azure Sentinel is pre-integrated with the CDC Platform, so customers 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.

MICROSOFT DEFENDER FOR ENDPOINT (MDE) - DETECTION, HUNTING AND RESPONSE OF THREATS AT THE ENDPOINT

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

KEY BENEFITS

- 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 retro-hunting, 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

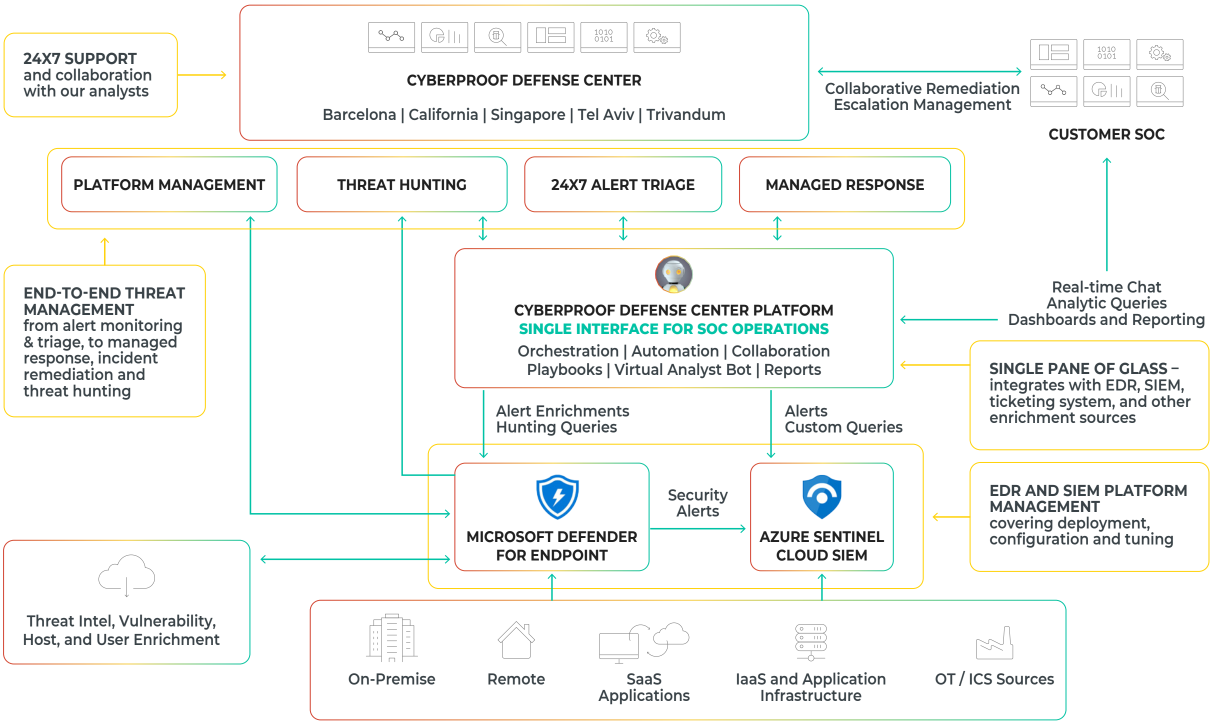
KEY OUTCOMES

Single View of Security Operations: The CyberProof Defense Center (CDC) is pre-integrated with Microsoft Azure 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: Create tailored risk scoring and operational dashboards & reporting – providing insights for internal and multi-layer customer stakeholders and for compliance purposes

SERVICES ARCHITECTURE



24X7 SUPPORT and collaboration with our analysts

CYBERPROOF DEFENSE CENTER

Barcelona | California | Singapore | Tel Aviv | Trivandum

Collaborative Remediation Escalation Management

CUSTOMER 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 Bot | 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

MICROSOFT DEFENDER FOR ENDPOINT

Security Alerts

AZURE 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

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 operational capabilities

Onboard & Enable

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

Migrate & Transition

- Connect Azure Sentinel and Defender for Endpoint to 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, triage issues, investigate incidents and support with remediation and recovery activities
- Create customized dashboards and reporting as well as actionable threat intelligence on targeted threat

WHY CYBERPROOF?

Recognized as 'Leader' by Forrester in the Midsize Managed Security Services Market

Flexible, **Hybrid Engagement Model** for a True Partnership

Our Virtual Analyst Bot Significantly Reduces Human Effort

Our Platform Facilitates **Collaboration** And Provides **Transparency**

Use Case Factory Continuously Improves Your Defenses

Have delivered the **largest and most complex** deployment of Azure Sentinel in the world

CyberProof
A UST Company