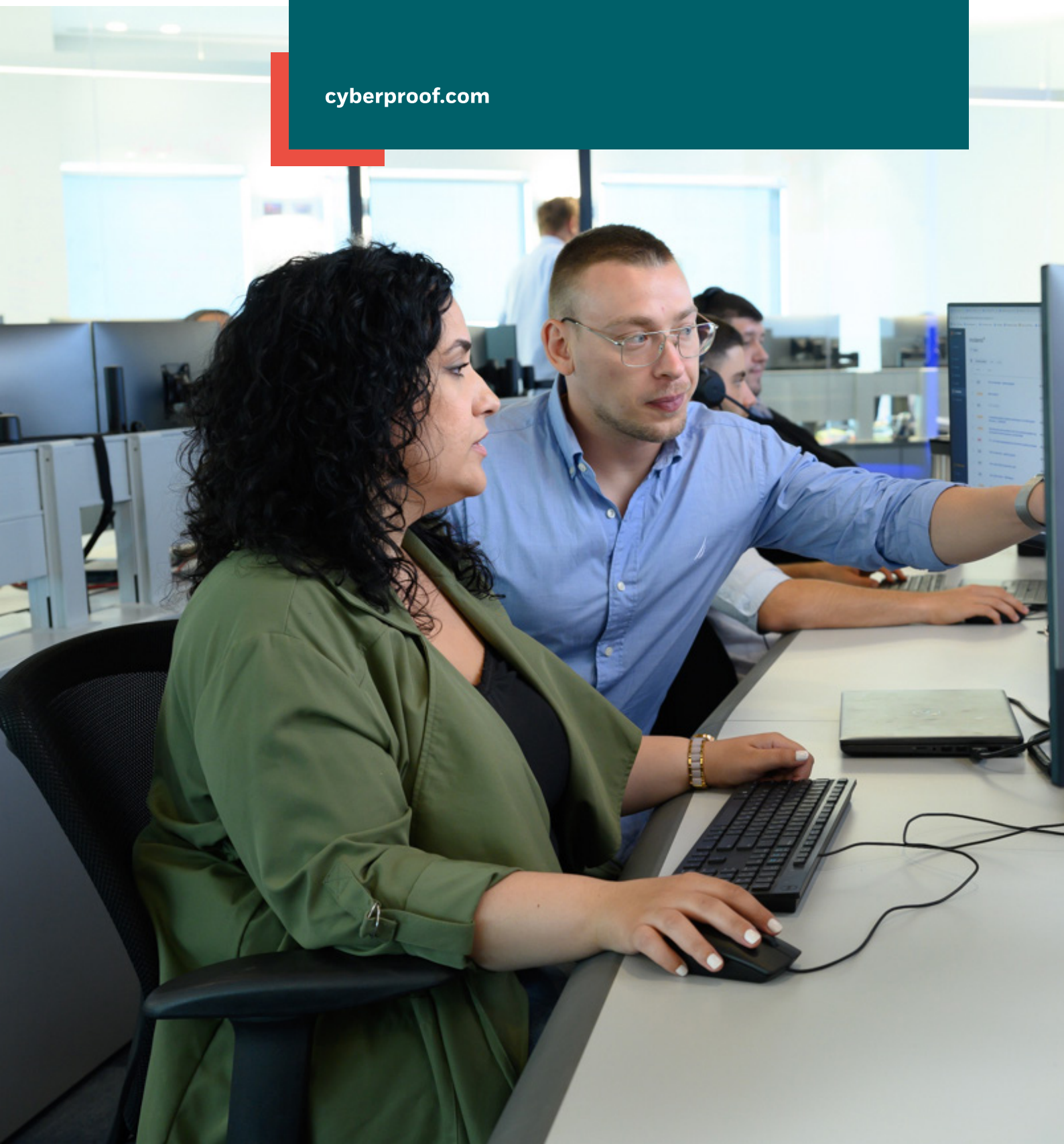
CyberProof®
A UST Company

Managed XDR for Microsoft

cyberproof.com



As you transition your assets from physical data centers to public cloud or multi-cloud infrastructure, security operations must also make the move to the cloud to detect and respond to threats efficiently and cost-effectively. CyberProof, a UST company, has extensive experience helping some of the largest and most complex enterprises transition to and manage cloud-native security operations.

How CyberProof can help

Complete threat visibility of your Microsoft investments and rapid response

Our teams located in Security Operations Centers across the globe act as an extension of your team, carrying out day-to-day security operations from alert triage and validation to threat intelligence enrichment, hunting and incident response. Our CDC platform acts as a transparent, collaborative environment to access our skills and standardize threat management processes.

Dramatically reduce the complexity and costs of log collection

The potentially steep cost of data collection using Microsoft Sentinel can pose a challenge for many large organizations that need to monitor custom log sources that may not be supported and store data for threat hunting and compliance requirements.

This requires a cost-effective log collection solution as part of your security monitoring infrastructure. The CyberProof Log Collector (CLC) filters, parses and tags data from any source, sending only use case driven logs to Microsoft Sentinel while routing long-term and compliance data into a cloud data lake.

Migrate from legacy to cloud-native cyber defense

CyberProof provides the consulting, engineering and operational expertise to transform your cyber defense with the Microsoft Security stack. Our DevOps deployment model provides quick time to value by establishing customized Microsoft Sentinel infrastructures and Use Case content in just a few days. Our CyberProof Defense Center (CDC) platform acts as a single pane of glass for security operations, integrating with both legacy SIEMs and Microsoft Sentinel, so you can take a phased approach while maintaining visibility of both onpremises and cloud security alerts and incidents.

KEY FEATURES

- A team of experts from our CyberProof Defense Centers around the globe conducting alert triage, threat intelligence enrichment, hunting across your environment and incident response
- Our CyberProof Defense Center (CDC) platform, an advanced threat management platform, which natively integrates with Microsoft Sentinel and E5 Security Stack to provide a single interface for accelerated threat detection and response activities
- Set up and configuration of Microsoft Defender Suite to protect endpoints, applications, identities, Office 365 and cloud assets
- Advanced data engineering, to support non-standard data sources, complex log management, regulatory compliance, cost optimization, advanced analytics

Why CyberProof?

Advanced Data Engineering – Our data engineers set up a centralized, cost-effective data lake solution as part of your cloud-native monitoring infrastructure to enable the archiving, fast querying and compliance of Big Data

Quick time to value with DevOps deployment – CyberProof DevOps uses an Infrastructure-as-Code deployment model to automatically establish Microsoft Sentinel infrastructures and pre-configured use case content in just a few days.

Integrate logs from any source – Our CLC can connect all data types from any source that is not supported by default. This improves the flow and handling of data, augmenting Azure Sentinel's predefined rules and capabilities to provide customers with automated and dynamic threat detection.

Continuous Improvement – The Use Case Factory, an agile development methodology led by Use Case engineers and developers, continuously identifies and fills detection and response gaps with customized use case content in our Use Case Catalog consisting of detection rules, digital playbooks and third-party API integrations for response automation.

Transitioning you to cloud-native cyber defense

We provide a combination of consulting, engineering and managed security expertise to transform you to cloud-native security operations leveraging Microsoft Sentinel and Defender Suite.

Plan

- Understand your business goals, security objectives and the maturity of your current SOC process
- Design a plan to migrate to Microsoft Sentinel infrastructure and Defender solutions

Transition

- Takeover of current SOC processes
- Plan phased rollout of legacy security analytics solution
- Pilot new SOC infrastructure

Transform

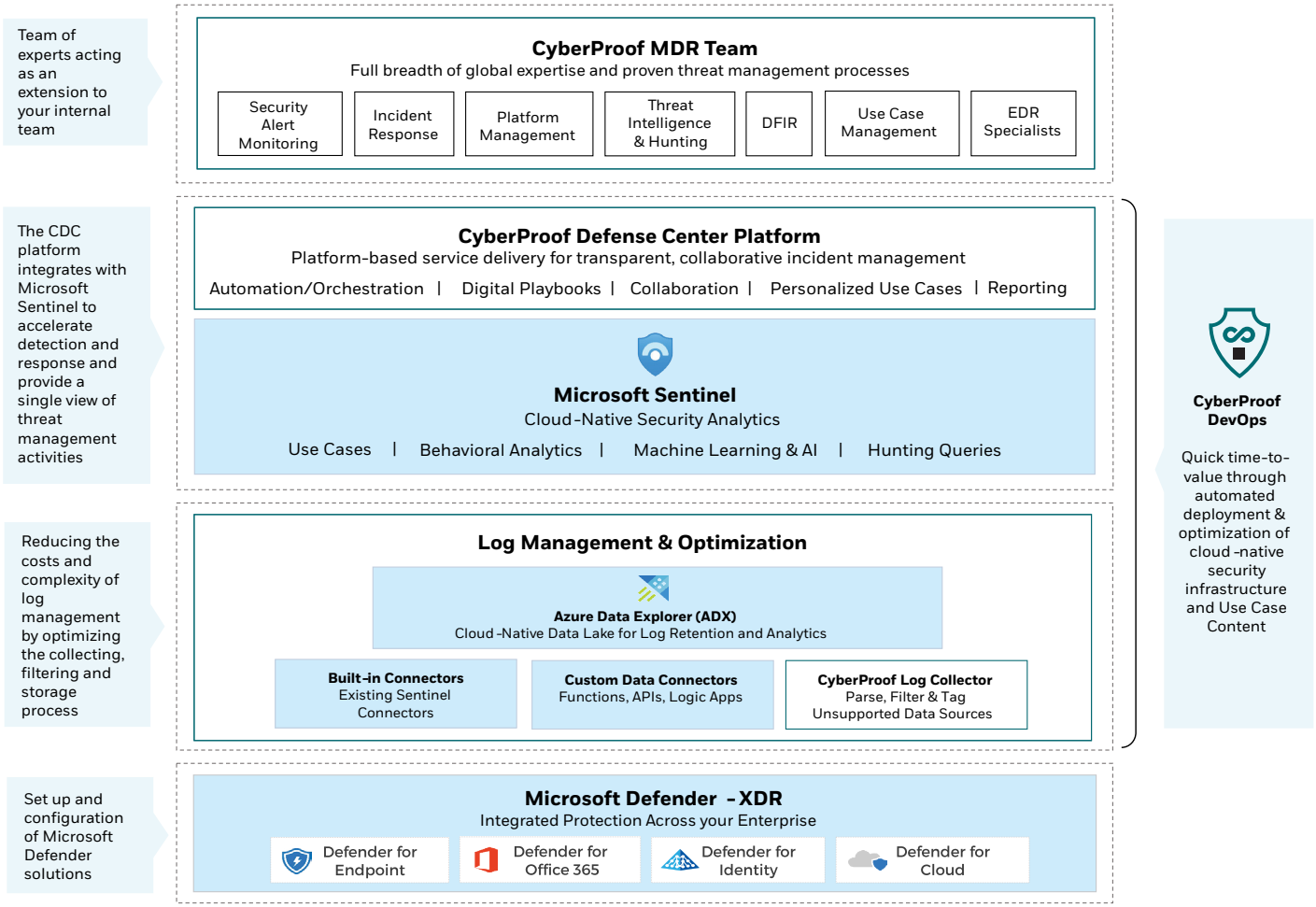
- Establish Cloud-Native Monitoring Infrastructure and required Defender solutions
- Connect to CDC platform for centralized, transparent security operations
- Configure custom use cases, detection rules, hunting queries and digital playbooks

Operate

- Provide continuous Security Event Monitoring, Threat Detection & Response services
- Create customized dashboards and reporting as well as actionable threat intelligence on targeted threats

Next-gen, cloud-native MDR service architecture

Our MDR service architecture leverages the full breadth of expertise provided by our global team, our proven threat management processes, real-time collaboration and escalation procedures, and platform-led technology delivery – allowing us to integrate Microsoft's XDR technology into our end-to-end MDR service.



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 | Paris | Singapore | Tel Aviv | Trivandrum