Managed Extended Detection & Response

CyberProof® A UST Company | Gold Microsoft Partner

Powered by Microsoft Sentinel and Microsoft Defender

As organizations continue to drive digital transformation and enable remote workforce, the security teams face a growing alert volume, diverse attack surfaces, and increasingly sophisticated cyber-attacks. To shore up defenses, companies continue to add security tools, which usually have high false positive rates, making security management even more inefficient.

Increasing number and sophistication of attacks

49%

Respondents said keeping up with security requirements has gotten harder[1]

Security teams are flooded with false positives

44%

Alerts are never investigated[2]

Growing shortage of cyber security talent

>3.2 million

shortage of cyber security professionals[3]

Get a standing watch by your side for managed extended detection and response

Lean on our global Security Operations Services, delivered using our CyberProof Defense Center (CDC) platform, to monitor, triage, investigate and respond to threat activity across cloud, endpoints, identities and application domains, while continuously adding use cases aligned to your threat landscape.

Microsoft 365 Defender
Industry-leading XDR portfolio for automated threat detection and response across domains.

Microsoft Sentinel
AI-powered, cloud-native SIEM for intelligent security analytics at limitless scale and speed.

CyberProof Defense Center (CDC)
Single pane of glass for all threat and automation/ orchestration activity.

Key benefits

Reduce **operational costs** with intelligent log collection and storage using CyberProof Log Collector (CLC)

Accelerate **Mean Time to Detect (MTTD)** and **Mean Time to Respond (MTTR)** using CDC's automation and orchestration capabilities.

Reduce **false positives** with well-tuned and continuously refined detection rules and use cases.

Get **faster time-to-value** using our Infrastructure as Code (IaC) deployment model.

Get in touch with us:

Ameen Hamanulla
ameen.hamanulla@cyberproof.com

Sources :

1. The State of Security, Splunk, 2021
2. ESG: Security Analytics and Operations: Industry Trends in the Era of Cloud Computing 2019
3. ISC2 survey, 2020

Our process for transitioning you to smarter security operations

Plan

- Understand your business goals, key security objectives, and the maturity of your current security operations.
- Design a plan to modernize security operations using Microsoft Sentinel and Microsoft Defender solutions.

Transition

- Set-up cloud-native monitoring infrastructure and connect it, along with your legacy infrastructure, to CyberProof Defense Center for centralized visibility.

Transform

- Migrate the existing use case content from your legacy solution to Microsoft Sentinel and configure personalized use cases (detection rules, playbooks, hunting queries, etc.).

Operate

- 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 KPI reports and dashboards.

Our recent customer stories

Multi-national Insurance enterprise, with over 250k employees, headquartered in France

Challenge

Limited visibility of the hybrid IT environment from their existing solution – ArcSight.

Solution

CyberProof helped them transition from ArcSight to Microsoft Sentinel and Defender and is now supporting with transparent Managed Detection and Response (MDR) services.

500+ Customized use cases

24/7 MDR service

Waterworks company, headquartered in North America

Challenge

Limited visibility of cloud assets after transitioning from on-premises to cloud infrastructure.

Solution

CyberProof set-up Microsoft Sentinel with customized use case content and reporting and integrated with the CDC platform to provide transparent MDR services.

24/7 MDR service

Integration with client's Endpoint Detection and Response Solution and VM platforms

Born digital, CyberProof, a UST company, is a global Microsoft partner, helping enterprises to effectively anticipate, adapt, and respond to cyber threats while reducing complexity.

Gold Microsoft Partner

1,000+ Microsoft Certified Professionals

140+ Clients in Global 1,000

Microsoft Member of Microsoft Intelligent Security Association

Microsoft **Advanced Specialization** Threat Protection

Get in touch with us:

Ameen Hamanulla

ameen.hamanulla@cyberproof.com