

Cloud-Scalable Security Monitoring, Detection & Response Services

CyberProof Managed Security Services Pre-Integrated With Microsoft Azure Security Stack

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, 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, and
- 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

Microsoft's Azure Sentinel is a cloud-native Security Information & Event Management (SIEM) platform that uses AI and automation to deliver intelligent security analytics and threat intelligence across the enterprise without any investment in infrastructure setup or maintenance. 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.



Native integration with Office 365 and Azure assets

Extend your security monitoring to SaaS applications and cloud workloads and identify genuine threats that require quick response

Key Benefits

- 24x7 security monitoring **frees up your team** to focus on more critical incidents
- 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 detecting and responding to validated incidents
- Provide security **metrics and reporting that matter** to the business
- **Integrate next-generation SOC capabilities** at speed without the investment

Our services

- **Security Event Monitoring**
- **Managed Detection and Response**
- **Managed Endpoint Detection and Response**
- **Advanced SOC Services**
- **Use Case Factory**
- **Security Platform Management**
- **Tailored Threat Intelligence**
- **Vulnerability Management**
- **Breach and Attack Simulations**

Key Outcomes

Single View of Security Operations

The CyberProof Defense Center (CDC) is pre-integrated with Microsoft Azure Sentinel to provide a single pane of glass – facilitating Sentinel's many services

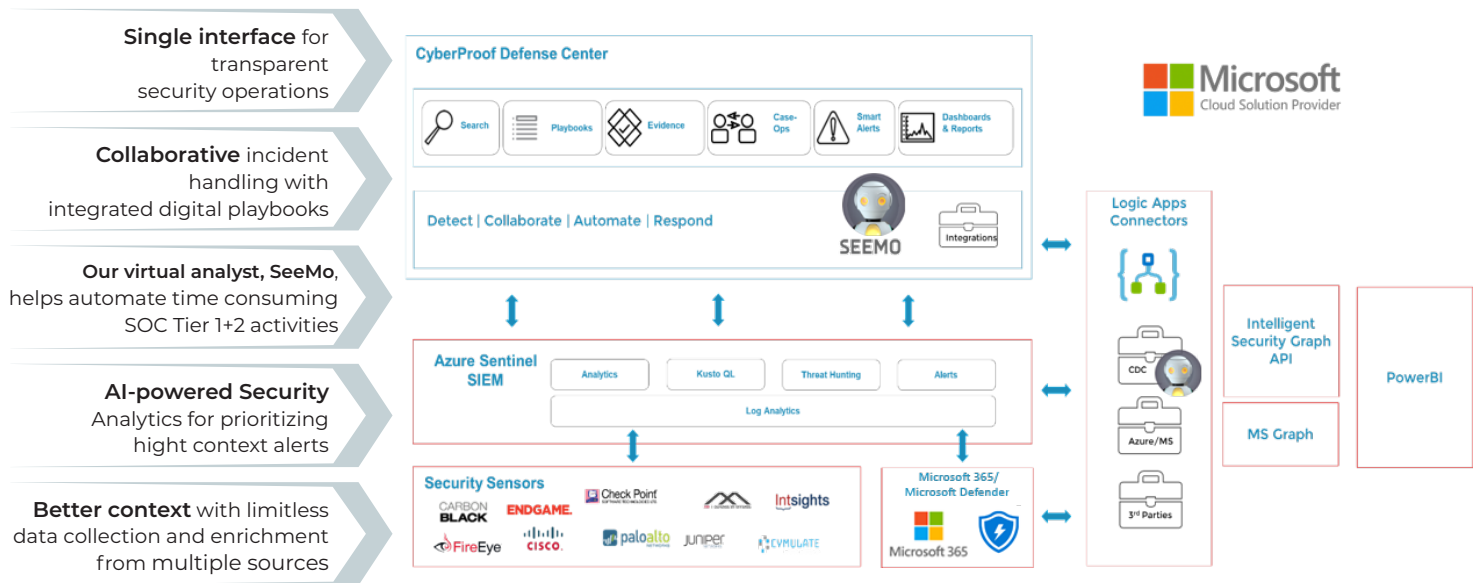
Shorter Detection & Response Time

Next-generation SOC capabilities drive operational efficiency and dramatically reduce the cost and time required to respond to security threats

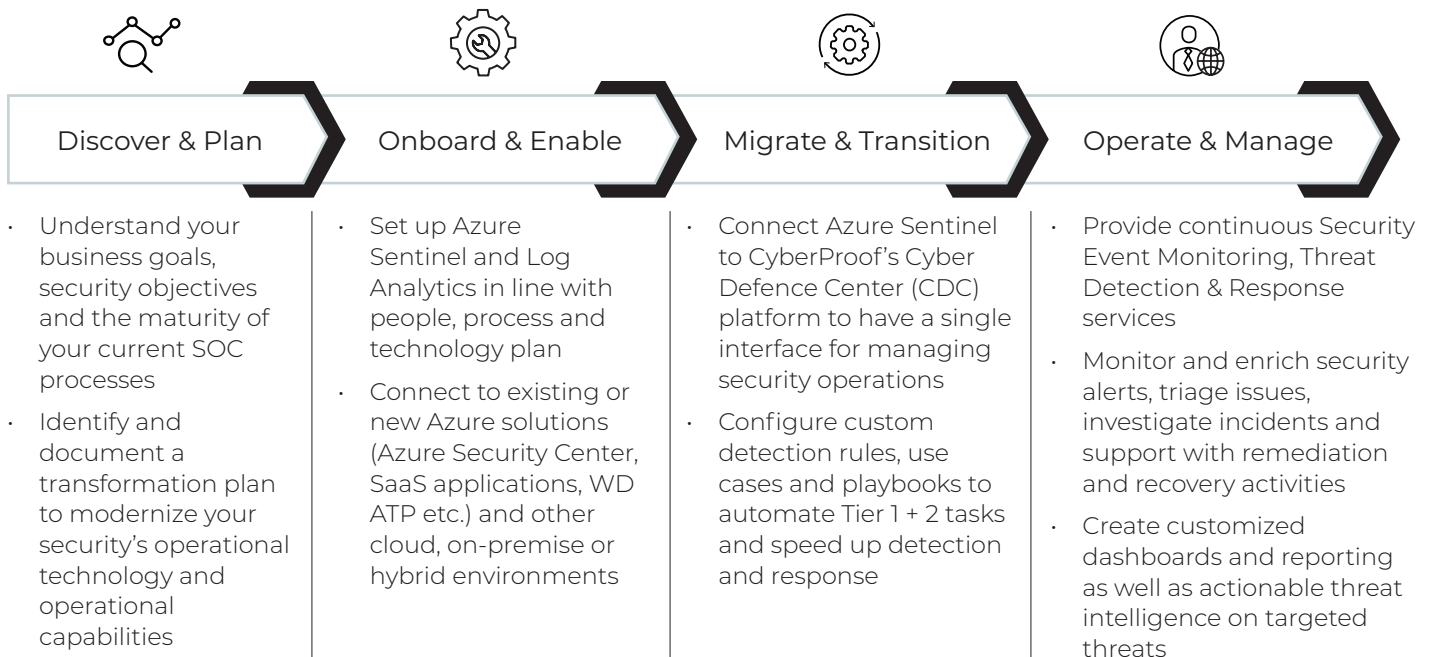
Dashboards & Reporting To Measure Risk

Create tailored risk scoring and operational dashboards & reporting – providing insights for internal and multi-layer customer stakeholders and for compliance purposes

End to End Integration with Microsoft Azure Security Stack



How we transition you to a Smarter SOC



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



Modernized, **Cloud-based Security**