

Managed Detection & Response (MDR)

Rapidly detect and respond to the incidents
that threaten your organization

cyberproof.com



Security teams are struggling to reduce the time to detect and respond due to the complexity and volume of alerts being generated from multiple security technologies. CyberProof's MDR service enables you to detect and respond to validated threats faster without adding more complexity to your security infrastructure.



Faster detection & response

The CyberProof Defense Center (CDC) platform includes SeeMo, our virtual analyst, who can automate up to 85% of L1+L2 activities including alert monitoring, enrichment, triage, investigation and issue containment. Our human analysts, along with SeeMo, work with you in a hybrid engagement model to support incident response activities - or, depending on the defined workflow, automated response playbooks can be deployed.



Singe view of security operations

Our lightweight, open API architecture enables us to integrate the CDC platform with your existing security investments without additional infrastructure. It correlates limitless volumes of data regardless of where it resides to provide a single pane of glass view of enriched alerts and incident handling activities.



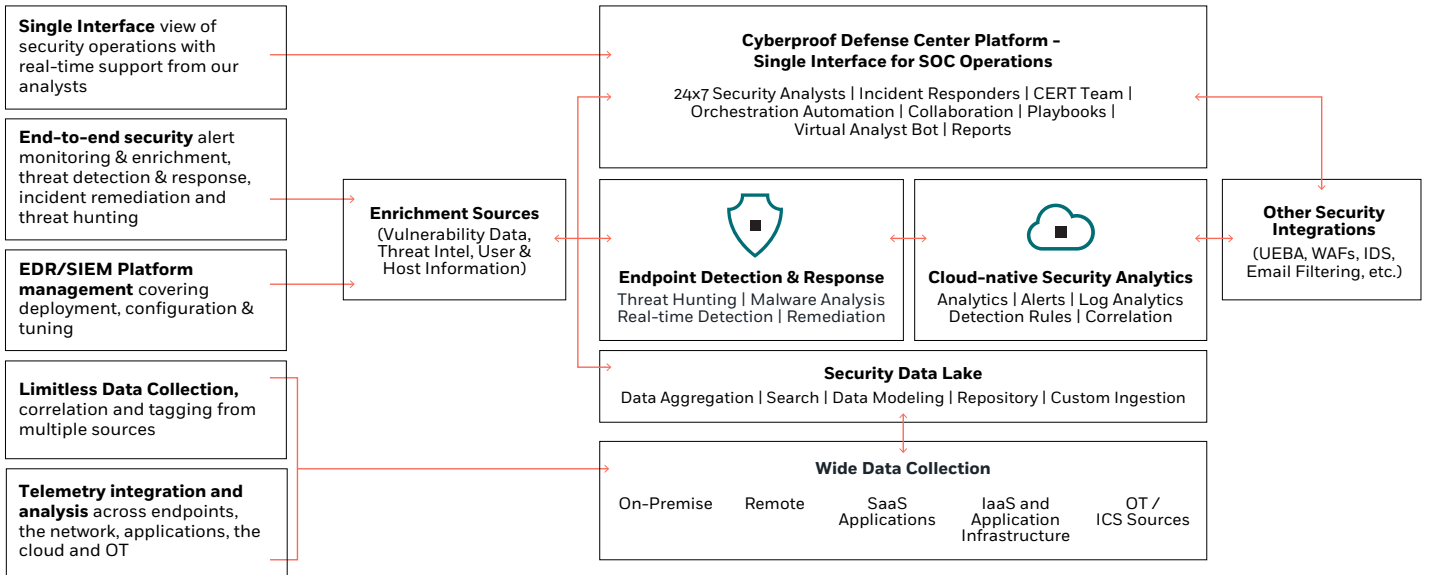
Proactive incident handling

Our global response team proactively carries out detailed investigations to search across the enterprise for signs of suspicious activity and remediate threats using tailored responses. We use our curated library of threat detection and response content to continuously configure and tune customized detection rules and response procedures, accessible by the customer as Use Case Kits.

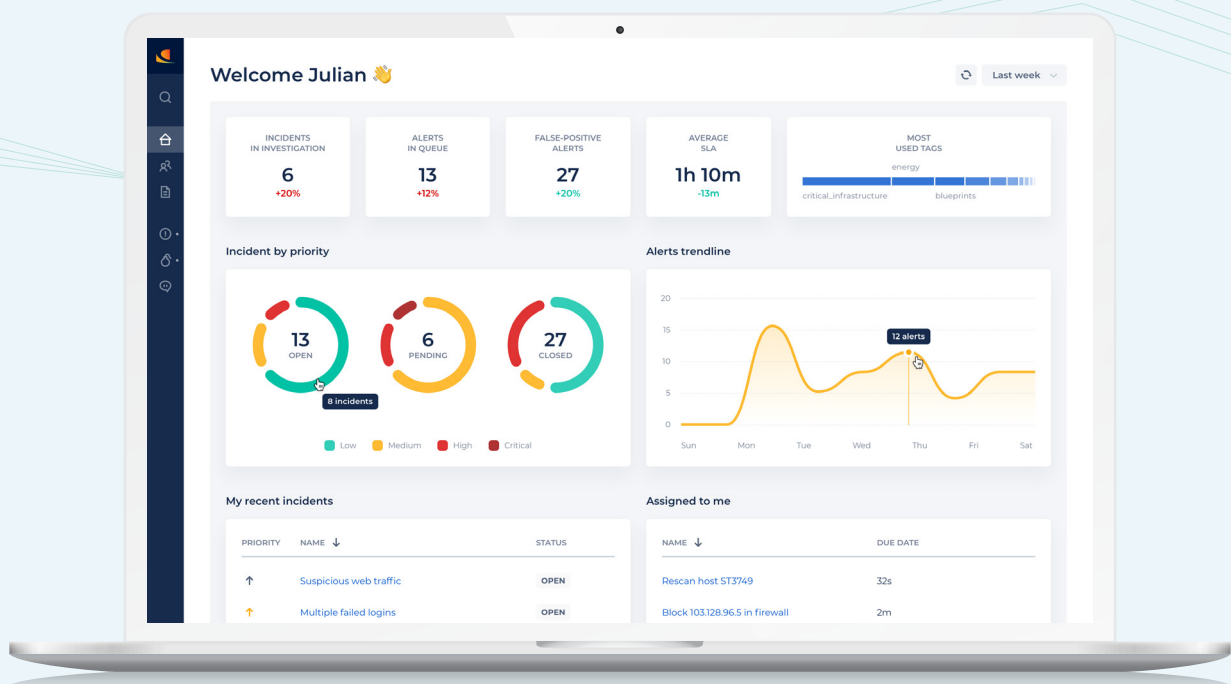
What's included?

- **24x7 Security Monitoring** – round-the-clock security alert monitoring, enrichment and triage
- **Incident Handling** – incident investigation, issue prioritization and response process aligned to leading industry standards and incident handling methodologies
- **Tailored Threat Intelligence** – active monitoring of multiple threat sources across the clear, dark and deep web, and real-time visibility of targeted threats to organizations' specific assets, data and people
- **Remote & On-Site Incident Response** – DFIR experts who work in close collaboration with your technical and executive teams to prepare for, respond to and recover from a cyber breach
- **Multi-Layered Threat Hunting** – usage of a unique combination of sources to search for threats lurking in your environment including known IOCs, incident information, proprietary threat intelligence, MITRE blind spots and behavior anomalies
- **Continuously Optimized Use Cases & Digital Playbooks** – efficiently manage incident workflows
- **Real-Time Collaboration** – transparent activities providing you with support for issue containment, remediation, risk mitigation, and personalized reporting

How it works



CyberProof Defense Center (CDC) Platform



Why CyberProof?



Independently Recognized Leader - CyberProof is a MDR award winner and recognized as a "Leader" by Forrester in the midsize managed security services market



SeeMo, Your Virtual Analyst Bot - SeeMo acts as a virtual member of your team to automate L1+L2 SOC activities and significantly reduce human effort



Continuous Improvement - Our Use Case Factory continuously optimizes tailored use cases consisting of prevention controls, detection rules and automated response playbooks



Transparency and Collaboration - Our platform facilitates real-time collaboration and provides transparency into security operations



Hybrid Engagement Model - Flexible, hybrid model so you only use what you need from us with complete transparency



Modernized, Cloud-based Security - Our platform allows you to scale up and down services as needed without upfront infrastructure investment



Leverage Existing Infrastructure - We can integrate with your existing technology investments or augment your SOC with the latest capabilities from our ecosystem of innovative vendor partnerships



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