CyberProof®

SERVICE CATALOG

OVERVIEW

CyberProof is a Security Services company that helps enterprises transform their security operations so they can anticipate, adapt and respond to cyber threats with confidence. Our services are powered through our SaaS-based SOC services delivery platform to drive operational efficiency with complete transparency.

SeeMo, our virtual analyst, accelerates threat detection and response activities by learning from and adapting to endless sources of data to provide context and help remediate incidents. In the face of an increasingly hostile threat environment, CyberProof integrates all the key elements you need to detect threats early and respond rapidly and decisively – while offering flexible engagement models that make sense for your business.

CyberProof's team works as an extension of your security team by delivering our services in a "hybrid" or co-delivery model and functioning as an integral part of your threat reduction strategy.

PARTNERS

CLAROTY

cybereason

CROWDSTRIKE

cybersixgill

IBM Security

MICRO FOCUS ArcSight

INTSIGHTS Threat Intelligence Realized.

Microsoft

NOZOMI NETWORKS

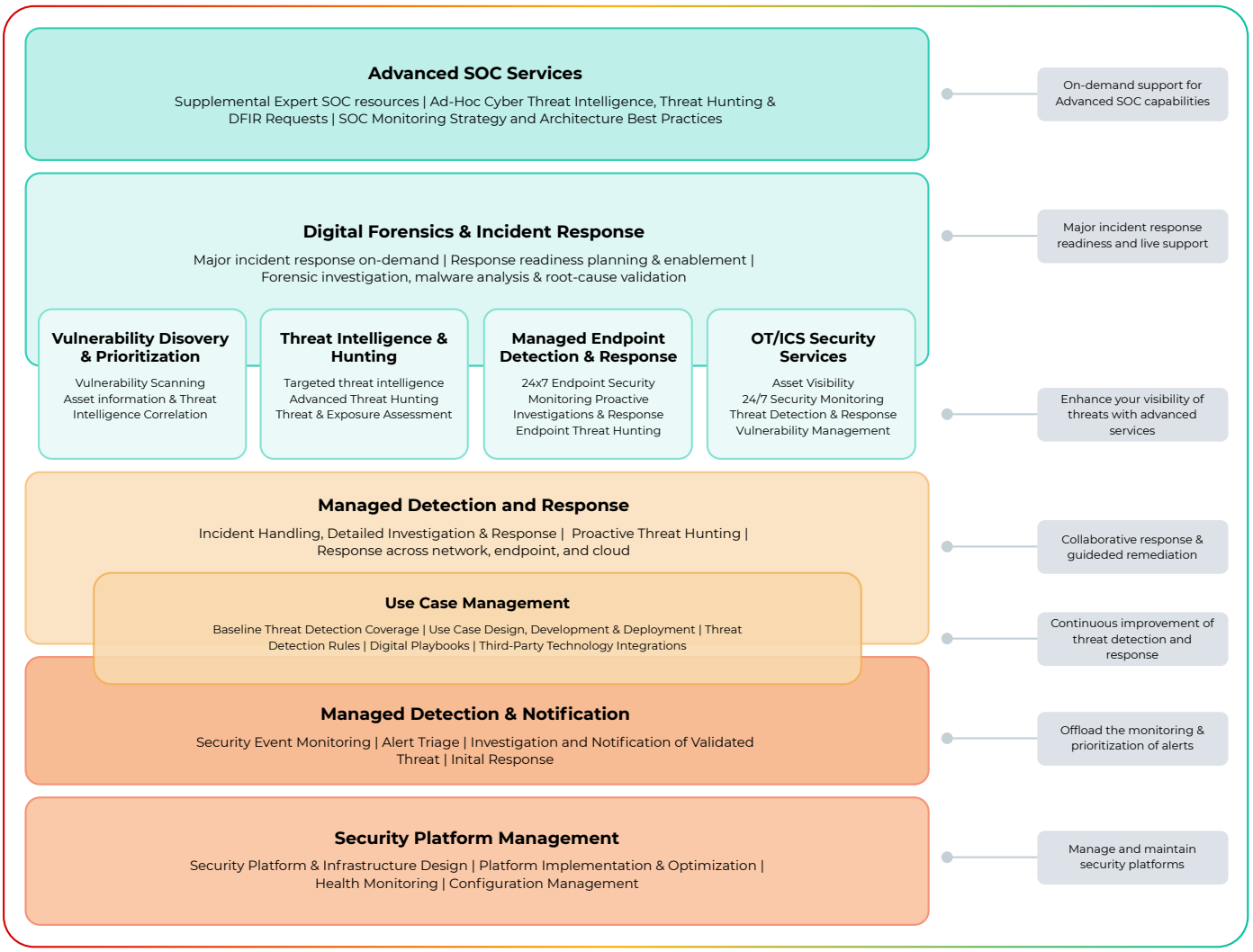
Qualys.

Radiflow

splunk>

OUR PORTFOLIO OF SECURITY SERVICES

Our services are designed to enable flexibility, adapting to customer needs as their requirements change throughout their security transformation journey, and facilitating high-touch engagement. Regardless of the service, you are assigned a service delivery team to ensure efficient and agile delivery of services and that technical requirements are met throughout the client's lifecycle.



CYBERPROOF DEFENSE CENTER (CDC) PLATFORM

The CyberProof Defense Center (CDC) platform acts as a single pane of glass for the customer's security operations and enables us to deliver cloud-native services at speed, with complete transparency and real-time ChatOps collaboration.

24x7 Operations:

Obtain real-time, continuous monitoring, detection, and response via a cloud-based service delivery platform

Customized Playbooks:

Centralize and standardize responses using clearly defined and automated digital playbooks.

Transparency:

See what our analysts see and have visibility into all activities.

Orchestration & Integration:

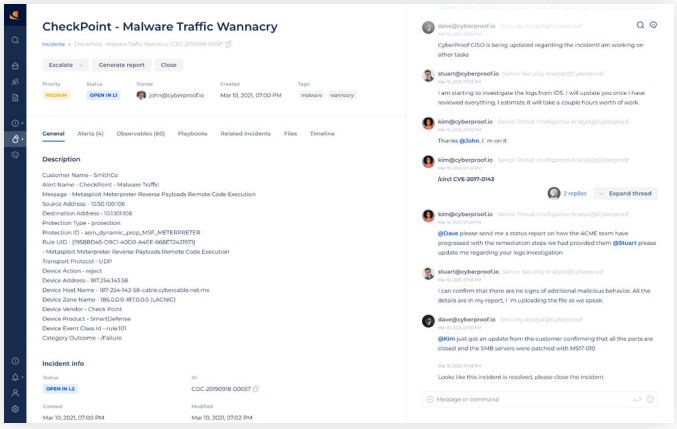
Seamless integration with SIEM, EDR, threat intelligence, vulnerability management, and incident management platforms provides a single pane of glass view.

ChatOps Collaboration:

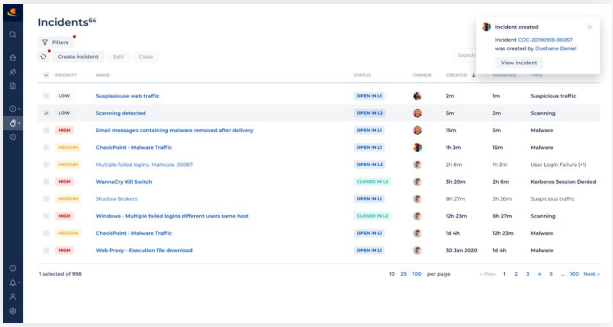
Collaborate with your stakeholders and our nation-state experts in real time to remediate threats quickly and with full transparency.

Automation via SeeMo - Your Virtual Analyst:

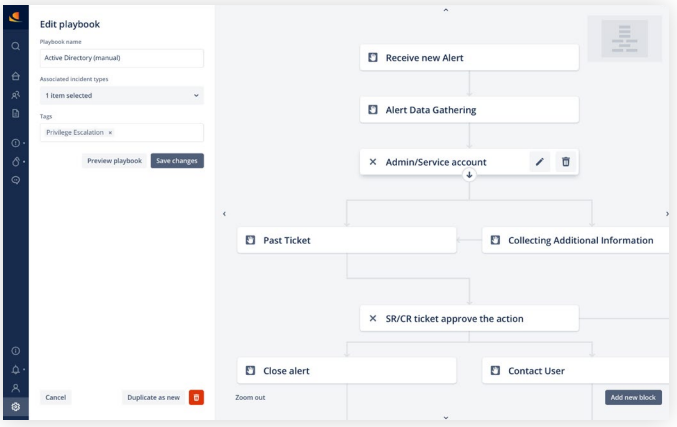
Our smart bot, SeeMo, learns from endless sources of data to automatically enrich alerts, carry out investigations, and execute digital playbooks.



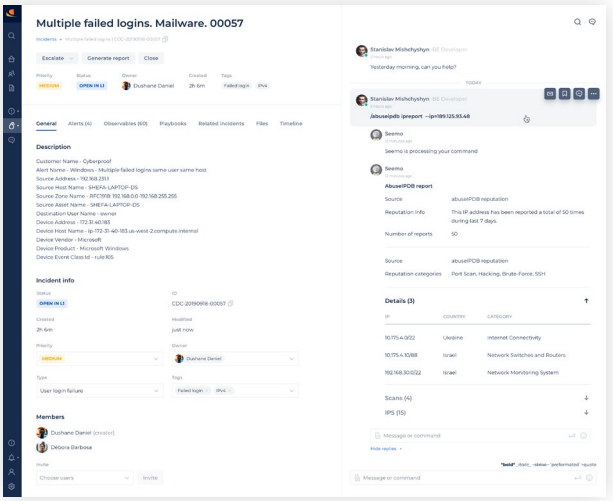
Incident Collaboration and Transparency



Single Pane of Glass of Enriched Alerts



Digital Response Playbooks



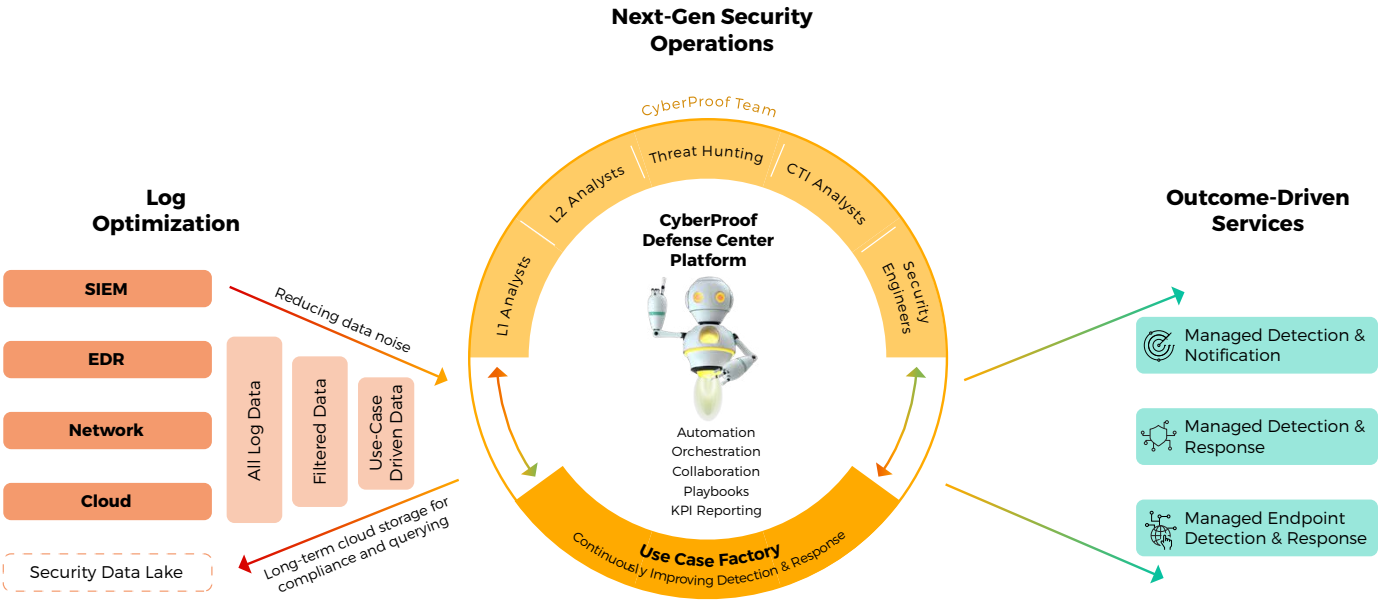
Automated Insights from SeeMo, our Virtual Analyst

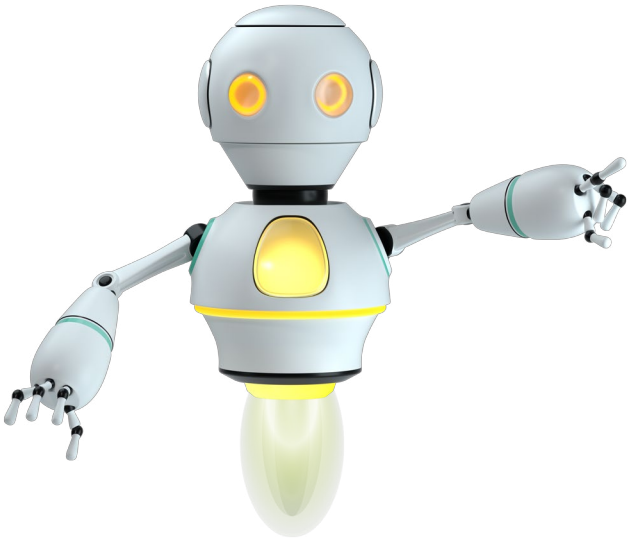
MANAGED DETECTION AND RESPONSE

Our Managed Detection and Response services offer continuous visibility of your environment and offer proactive threat detection and response capabilities across on-prem, cloud, SaaS and endpoint environments.

These services provide 24x7 security alert monitoring, automated enrichment, triage, detailed investigation and response activities to contain threats and minimize impact. Our nation-state level security analysts continuously enhance their investigations with up-to-date information from our threat intelligence and hunting teams to enhance threat detection activities and perform focused investigations to identify previously unknown threats.

Our CyberProof Defense Center (CDC) platform integrates with our clients' existing platform investments (such as SIEM Platform, Vulnerability Management, EDR tools etc.) to provide a single interface for monitoring your security operations, automating time-consuming tasks and collaborating with our team members.





Our MDR services are available in three selectable tiers:

- **Managed Detection and Notification (MDN) –** Monitoring, investigation and notification of validated threats from any environment leveraging the SIEM
- **Managed Detection and Response (MDR) –** Monitoring, hunting, investigating and responding to threats from any environment (endpoint, cloud, network) leveraging the SIEM
- **Managed Endpoint Detection and Response (MEDR) –** As an enhancement to our MDR service, MEDR includes a hunt and respond service directly at the endpoint to reduce dwell time and manage the EDR platform and its contents on an ongoing basis.

Features:

- Continuous collection and aggregation of Security Event logs from security sensors within your on-premises or cloud IT infrastructure
- 24x7 operations monitoring, alert triage, investigation, and initial response
- Managed threat containment and remediation assistance
- Use of CDC platform to act as single pane of glass for alerts collected from security technologies, incident handling workflows, automated responses, and collaboration with team members
- Event-driven, targeted threat hunting and reconnaissance
- Deployment, maintenance and continuous optimization of threat detection and response use case content via our Use Case Factory
- Threat intelligence, through alert enrichment and reporting

Benefits:

- **Extension of your team –** Freeing up your security team's capacity by complementing your staff, so they can shift their focus to higher priority tasks
- **Guided remediation and investigation –** Real-time analyst support via the CDC platform's ChatOps module, as per clearly defined playbooks
- **Transparency into SOC activities –** Full visibility into activities carried out by both our analysts and client teams through our CDC platform
- **Understanding the root cause –** Correlation of multiple alerts into a single incident within our CDC platform, so that you understand the root cause
- **Collaboration with our experts –** Real-time collaboration between multiple teams enabling efficient responses to complex incidents

OUR SERVICES

SECURITY PLATFORM MANAGEMENT

CyberProof's Platform Management team helps you design, deploy, configure and operate on-premises, cloud-native and hybrid security platforms. We help alleviate the complexities of managing solutions such as the Security Information and Event Management (SIEM), Vulnerability Management, Endpoint Detection and Response (EDR) and Threat Intelligence platforms.

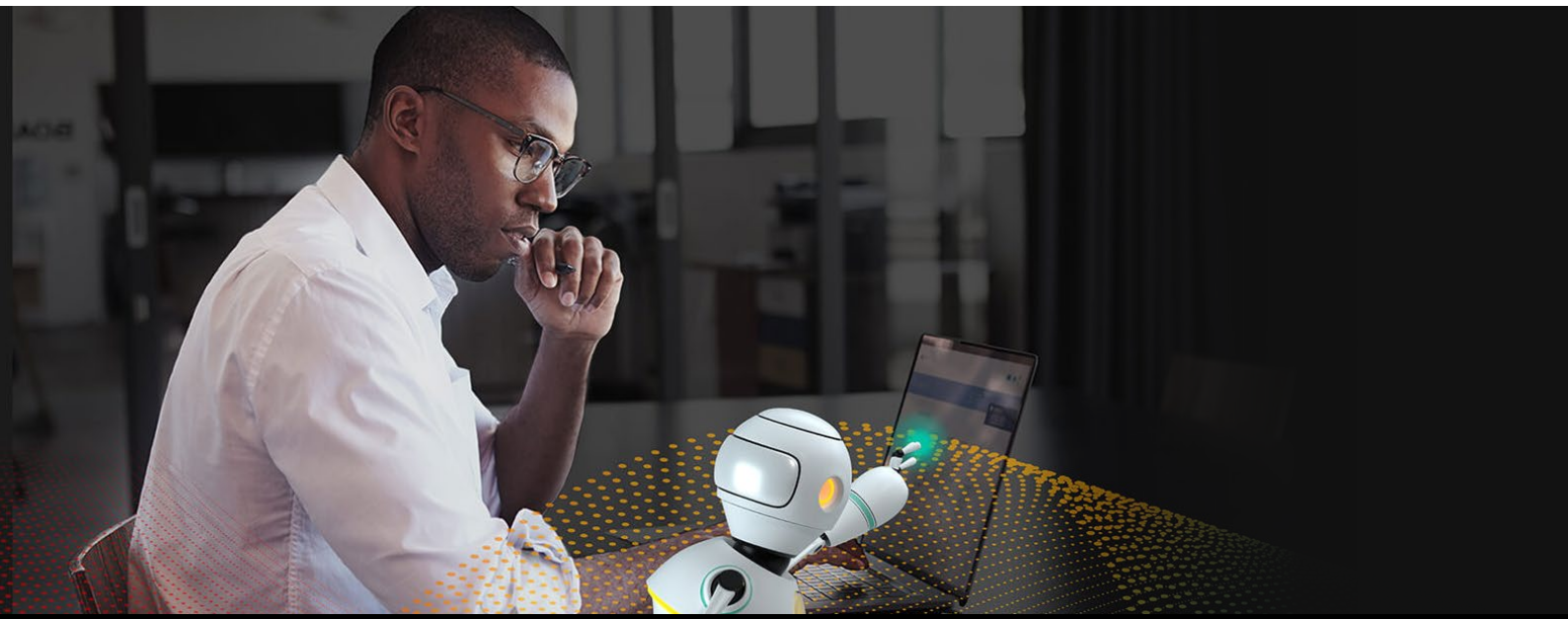
The service monitors for platform availability and performance, maintains security configurations and ensures that software and patches are updated to the recommended standards.

Features:

- Security platform infrastructure design
- Platform implementation and optimization
- Performance and health monitoring and configuration management
- Software updates and patch management

Benefits:

- **Reduced cost of log ingestion and retention –** We help optimize log collection, filtering, parsing, tagging and storage of your data to reduce costs and optimize real-time analysis
- **Assurance you are receiving value –** Our engineers focus on maintaining and optimizing the platform's configuration so it's monitoring the right threats and being updated to the correct patch levels, ensuring you're getting the most out of your solution
- **Rapid deployment –** Rapid platform deployment, enabling fast time-to-value
- **Focus on higher impact activities –** Offload the management and optimization of your platform to our expert staff, allowing your team to invest time in other strategic areas

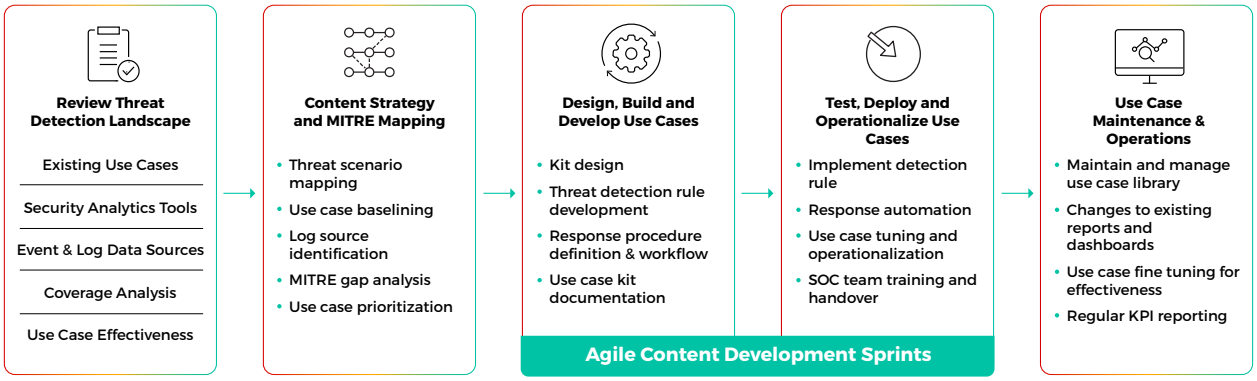


OUR SERVICES

USE CASE MANAGEMENT

Our Use Case Management service continuously identifies and fills threat detection & response gaps. Through the ongoing development and deployment of detection rules, digital playbooks, reporting, and third-party technology integrations, CyberProof improves the efficiency of your cyber defense workflows on an ongoing basis.

The service uses our Use Case Factory (UCF) methodology, uniquely leveraging an Agile development methodology to continuously develop, test and deploy content, packaged into kits. This enables the continuous improvement of each stage of the SOC workflow from detection, investigation, hunting, response and remediation.



Features:

- Baseline threat detection and response capabilities
- Establish use case management and operational governance
- Develop, test and optimize new content packages containing threat detection rules, digital response playbooks and third-party API integrations following Agile development practices
- View of use case life cycle, and coverage aligned to MITRE Framework
- Quarterly use case governance forum to review content strategy, use case roadmap to drive continuous improvement
- Regular KPI reporting to provide coverage analysis, pipeline view and use case effectiveness

Benefits:

- **Use Case Maturity –** Establishes governance to baseline existing threat detection abilities and provide coverage analysis, driving threat detection & response maturity
- **Reduce false positives –** Improves quality of alerts generated by your security analytics platforms - as only use case-related alerts are generated
- **Continuous Improvement –** Continuously detect & respond to the most recent threats targeting your organization
- **Identify and fill threat detection gaps –** Stay on top of coverage gaps and improve the accuracy of security monitoring and threat detection tools
- **Improve each stage of the SOC workflow –** Improve the efficiency and effectiveness of each stage of the SOC workflow from initial response, alert triage and investigation to threat hunting, incident response and remediation

OUR SERVICES

VULNERABILITY DISCOVERY AND PRIORITIZATION

CyberProof provides support through asset discovery, vulnerability identification, and issue prioritization – helping you remediate vulnerabilities that are most likely to have significant impact on your business. We use a unique, threat-centric approach to help you proactively detect vulnerabilities, prioritize issues and effectively minimize exposures. Our approach includes:

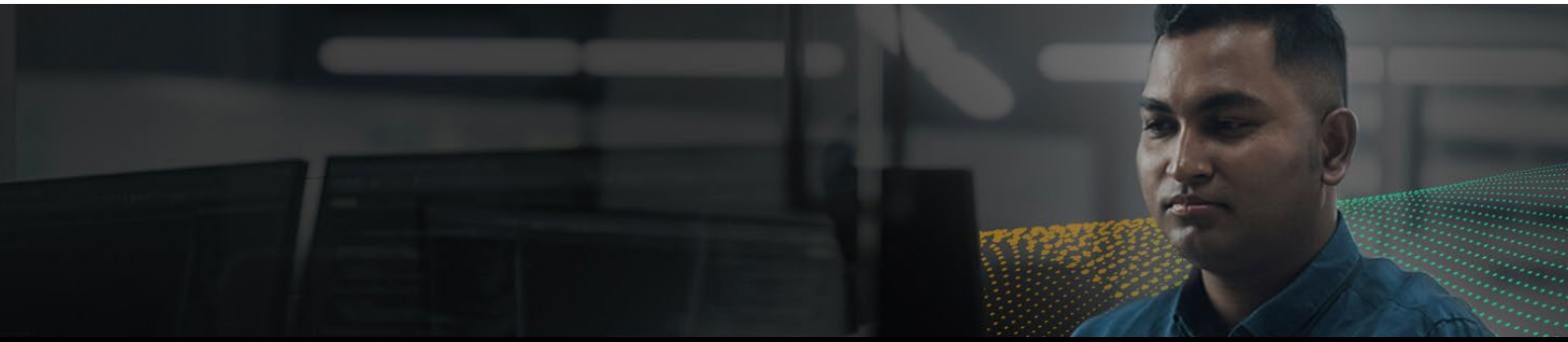
- **Vulnerability Discovery –** Implementing, managing, and operating vulnerability scanning solutions to discover and collect infrastructure and asset vulnerability information
- **Vulnerability Prioritization –** Prioritizing vulnerabilities based on your actual attack surface by correlating internal infrastructure vulnerabilities and asset information with external threat intelligence

Features:

- Planning, design, implementation, configuration, optimization and management of a Vulnerability Management platform
- Asset classification and risk categorization
- Automated scanning of assets for on-premises and cloud environments
- Correlation against live threat intelligence feeds to prioritize high risk vulnerabilities
- Correlation of vulnerabilities and patches (where relevant) for specific hosts, based on CVEs and patch availability
- Regular reporting regarding high-risk vulnerabilities, remediation recommendations and patch availability

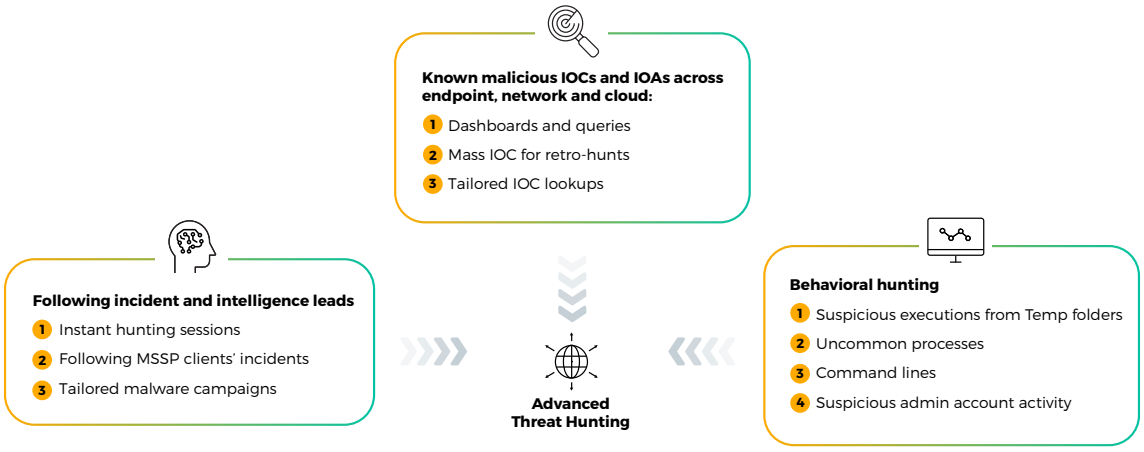
Benefits:

- **Focus on vulnerabilities that matter –** Prioritization of vulnerabilities based on internal and external monitoring
- **Offload the operational workload to our team –** Offload day-to-day vulnerability monitoring, correlation and prioritization to our team, so you can focus on remediation
- **Faster alert triage and enrichment –** Enable more efficient threat detection, with alerts enriched with threat-centric vulnerability data
- **Wide visibility across your IT estate –** Gain visibility into weaknesses across your on-premises and cloud assets that could be exploited in the wild



ADVANCED THREAT HUNTING

CyberProof's dedicated Threat Hunters use a proven methodology to proactively search for malware or attackers hiding in your network. With expertise in defensive & offensive nation-state cyber security, they leverage advanced hunting techniques to build a customized Threat Hunting program that focuses on identifying undiscovered threats. Our Threat Hunters include former 8200 Unit members of the Israel Defense Forces, providing the highest level of experience in carrying out nation-state level investigations.



Features:

- Hunting for known malicious threats
- Incident and Intelligence-Based Hunting, leveraging incidents across our client base and alerts from our Cyber Threat Intelligence team's research
- Behavioral analysis using network, endpoint, user and cloud data
- Hunting based on the Tactics, Techniques and Procedures of the MITRE ATT&CK matrix to identify evidence of infection
- Pre-defined threat hunting packages detailing structured hunting procedures to detect specific types of threats
- Regular reporting of remediation and response recommendations (such as YARA rules), supporting continuous improvement

Benefits:

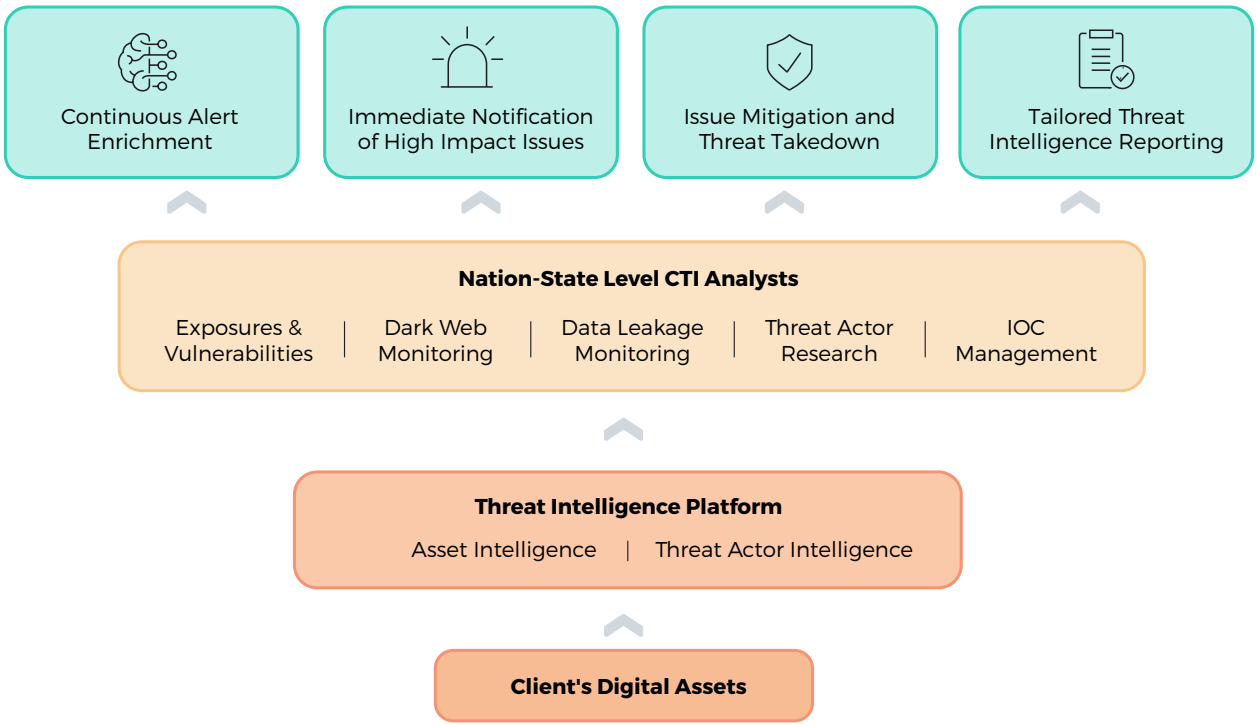
- **Dedicated Threat Hunters –** A team focused full-time on proactive Threat Hunting activities to support forensic investigation, so that you do not need to develop similar skills in-house
- **Identify threats that bypass your defenses –** Proactively hunt for indicators of threats that were previously missed by security tools or security analysts
- **Enhance threat detection capabilities –** Earlier detection of advanced threats by nation state level threat hunters leveraging behavioral analysis techniques to find anomalies
- **Improve incident response –** Our Threat Hunters work as an extension to security analysts and incident responders to enrich alerts and incidents with historical and real-time IOCs and provide feedback to improve detection rules and response steps

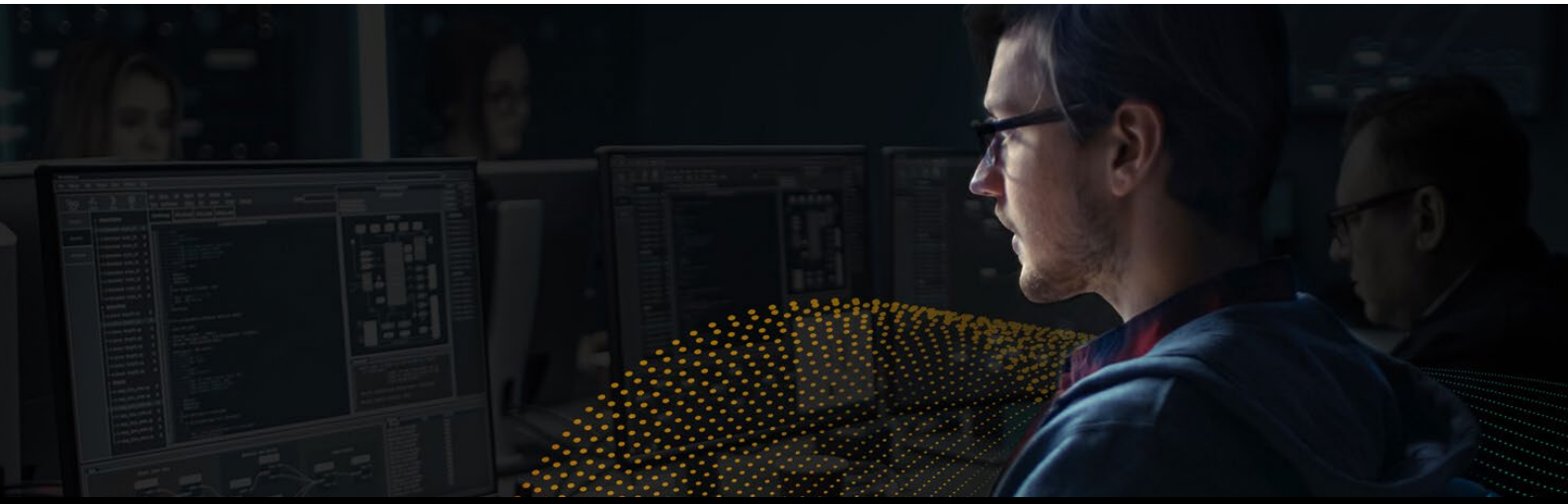
OUR SERVICES

TAILORED CYBER THREAT INTELLIGENCE (CTI)

Our Cyber Threat Intelligence (CTI) team enables the rapid detection of threat and exposures in a way that is accurate, relevant, and actionable. Our experts utilize a combination of threat actor and asset-based intelligence from organic, commercial and open sources and automated procedures to proactively identify, integrate, and correlate threats and exposures in near real-time, assess impact, and prevent critical incidents.

The CDC platform enables the provision of live, verified, and actionable threat intelligence alerts that are tailored to your threat landscape and have gone through the process of validation by our CTI analysts. The CDC platform can also be used to collaborate with our analysts, view pre-defined or customized CTI reports, and provide context for other alerts or incidents being investigated by the SOC.





Features:

- Pre-emptive alerts delivered via our CDC platform for imminent threats with actionable mitigation advice
- Research of targeted intelligence using both asset-based and threat actor-based information across the clear, deep and dark web
- Identification of sensitive data leakage, brand impersonations, malicious mobile applications, fraudulent activities, and exploitable vulnerabilities that may represent an immediate threat
- Proactive threat takedown and remediation
- Threat landscape reporting

Benefits:

- **Timely notification of emerging threats –** Experienced, nation-state trained Cyber Threat Intelligence analysts focused on proactive collection, analysis, validation and dissemination of threat research, saving time & resources on building similar skills in-house
- **Actionable information –** Tactical recommendations to help reduce your attack exposure and technical information such as IOCs, YARA rules etc.
- **Receive tailored intelligence –** Highly relevant threat alert information specific to your threat landscape such as the threat actor, their tools, MITRE mapping, threat type and impact to your business
- **Pre-empt an attack before it impacts your business –** Proactively hunting the clear, deep and dark web for early signs of an attack

OUR SERVICES

OT/ICS SECURITY MONITORING SERVICES

CyberProof provides managed security services for Operational Technology (OT) and Industrial Control Systems (ICS) environments, our CDC platform is pre-integrated with leading OT security technologies to deliver security monitoring, threat detection and response services via a single platform with full transparency. These integrations also enable us to discover previously unmapped assets in OT environments, maintain a centralized dynamic inventory, and obtain a holistic view of your attack surface to prioritize remediations. Our services include:

Supporting the security operations needs of:

- Distributed Control Systems (DCS)
- Industrial Control Systems (ICS)
- SCADA Networks

- **Asset Visibility and Intelligence –** Leveraging the broadest protocol coverage visibility into all three variables of risk in an industrial network: OT, IoT, and Industrial IoT (IIoT) assets, connections, and processes
- **Cyber Threat Monitoring –** Automatically profiling all assets, communications, and processes in industrial networks, generating a behavioral baseline that characterizes legitimate traffic to weed out false positives, and alerting users in real-time to anomalies and known, unknown, and emerging threats
- **Threat Intelligence –** Highly curated, multi-source, and tailored feeds that enriches Root Cause Analytics with proprietary research and analysis of OT zero-day vulnerabilities and ICS-specific indicators of compromise (IoC) linked to adversary tactics, techniques, and procedures (TTP)
- **Vulnerability Detection –** Proactively identifying vulnerabilities and network hygiene issues within the OT environment that can leave OT networks and sites vulnerable to attacks; leveraging proprietary intelligence to continuously monitor the network for new known vulnerabilities

Features:

- Team of security analysts carrying out continuous monitoring of threats and anomalies across different layers in your OT/ICS environments
- Identification of adversary techniques that correspond with the tactics covered in the MITRE ATT&CK for ICS framework
- Implementation and management of leading OT threat detection technology to monitor for early indicators of attack, known threat activity and behavioral anomalies

Benefits:

- **Visibility into critical OT assets –** Enables the discovery of previously unmapped assets in IT and OT environments and maintenance of a centralized dynamic inventory with our CDC platform, which is pre-integrated with leading OT threat detection technologies
- **Detect threats across both IT and OT networks –** A team of SOC analysts, CTI analysts and Threat Hunters that proactively monitors, investigates, and provides timely notification of threats across your OT and IT environments with full transparency into all activities via the CDC platform
- **Proactively identify and fix high-risk vulnerabilities –** Supplements the OT security vulnerability databases and scanning tools with our proven threat-centric vulnerability management framework to discover and prioritize high risk vulnerabilities and exposures

OUR SERVICES

DIGITAL FORENSICS AND INCIDENT RESPONSE

CyberProof offers both remote and on-site support to prepare, manage, and respond to security incidents, reducing potential data loss and helping your team effectively recover from an attack. Our DFIR personnel isolates any unwanted activity, contains it, and works to identify the source of the security breach and helps assess its scope.

Our experts also prepare a thorough incident report detailing the impact of the investigation and sharing any relevant findings. Where necessary, CyberProof's team also has experience in serving in the capacity of litigation support.

Support for a wide range of related DFIR activities including:

- IR readiness assessments
- Compromise assessments
- Business email compromise
- Cyber risk assessment
- Phishing simulations
- Table-top exercises
- Ransomware simulation tests
- Red, blue and purple teaming exercises

Features:

- 24x7 incident response hotline in the event of a security incident or if Incident Response (IR) expertise is needed
- Analysis and prioritization of security incidents and investigation of root cause, establishing a detailed timeline and reconstructing attacks
- Assistance in data collection and providing chain-of-custody
- Forensic investigations and analysis for endpoints, network, mobile and cloud artifacts
- Working closely with the enforcement authorities in transitioning case evidence (where relevant)

Benefits:

- **Rapid response to reduce dwell time –** Pre-defined agreement for incident response support, to avoid costly delays and reputation damage
- **Access to on-call incident responders –** Access to experts who have spent time getting to know your technical environment and business objectives
- **Support for a wide range of proactive IR services –** Repurpose any remaining retainer hours towards other services to improving your incident readiness
- **Understanding of the root cause of an incident –** Tracing how an attack happened using electronic data recovery and malware analysis

OUR SERVICES

ADVANCED SOC SERVICES

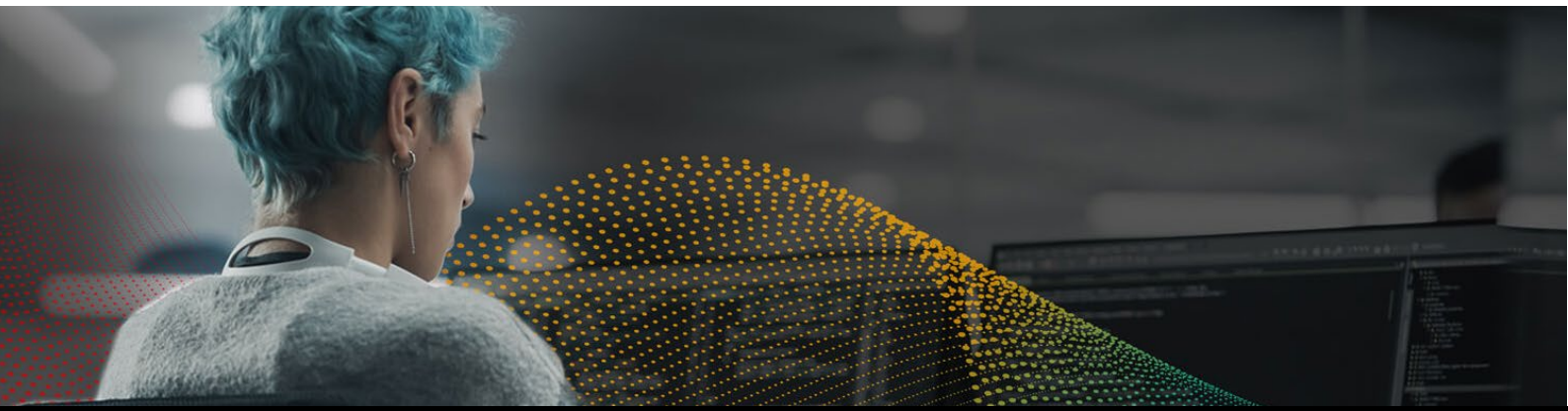
CyberProof's Advanced SOC Services combines expert resources and specialized tools to provide additional threat detection and response capabilities. These services typically apply to scenarios after a threat is contained and risk is minimized by the SOC team – such as detailed investigations, root cause analysis, complex threat hunting, and eradication of threats. Advanced SOC Services provide additional expertise to help enhance SOC operations to proactively detect threats and respond.

Features:

- Detailed investigation and analysis of endpoint malware
- Root cause analysis of Security Incidents and detection of control failures
- Remote forensic investigations covering files or disk image investigations
- Ad-hoc Cyber Threat Intelligence requests, covering:
  - Deep dives on targeted threat campaigns that are of interest
  - Threat actor tactics, techniques, and tools
  - Investigation into third-party breaches
  - Research on specific vulnerabilities and malware variants
- Threat Hunting requests
- Vulnerability assessments and penetration testing
- Advice on SOC monitoring strategy and architecture best practices

Benefits:

- **Improve and validate investigations with L3 expertise –** Supplementing SOC activities with L3 experts for further investigation and validation
- **Access to on-call DFIR specialists –** Rapid access to experts that help you understand the root cause and reduce impact to the business
- **Proactively take action on suspected threats –** Advanced SOC specialists who research targeted attack campaigns that are relevant to your business



ABOUT CYBERPROOF

CyberProof is a security services company dedicated to helping companies use information technology to solve business problems without the fear of cyber-attacks. To achieve this, we combine our expert talent and SeeMo, our virtual analyst with the power of strategic partnerships, visionary clients and academia. Our enterprise-scale approach allows us to effectively anticipate, adapt, and respond to cyber threats in an increasingly connected world while reducing complexity, and provide our customers with unmatched adaptability, transparency, and control.

Our services are powered through our SaaS-based SOC services delivery platform to drive operational efficiency with complete transparency to dramatically reduce the cost and time needed to respond to security threats and minimize business impact.

SeeMo, our virtual analyst, together with our experts and your team automates and accelerates cyber operations by learning and adapting from endless sources of data and responds to requests by providing context and actionable information. This allows our nation-state cyber experts to prioritize the most urgent incidents and proactively identify and respond to potential threats.

CyberProof is part of the UST family. Some of the world's largest enterprises trust us to create and maintain secure digital ecosystems using our comprehensive cyber security platform and mitigation services. For more information, see: www.cyberproof.com

Barcelona | California | London | Paris | Singapore | Tel Aviv | Trivandrum