CyberProof®

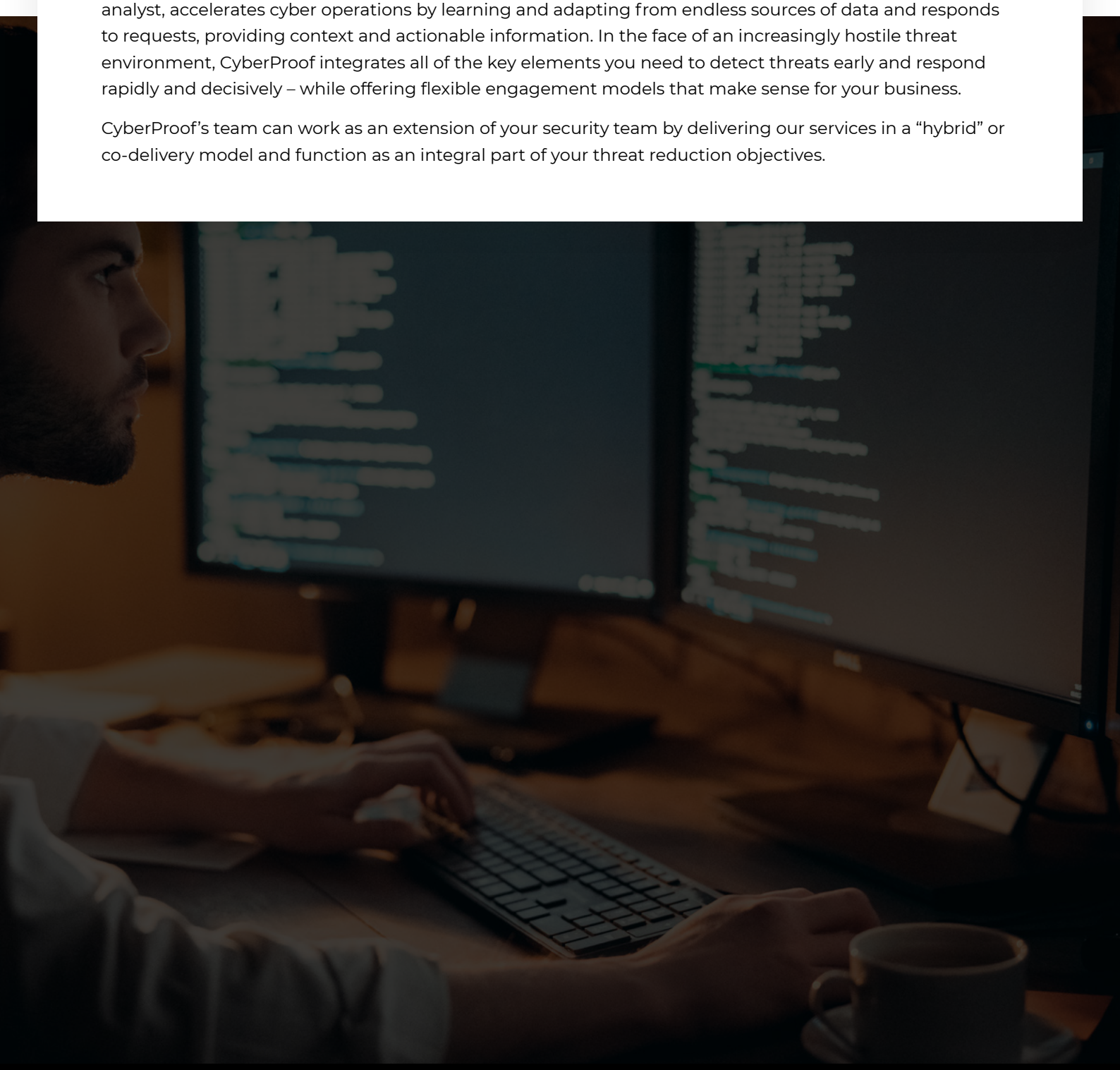
SERVICE CATALOG

OVERVIEW

CyberProof is a next-generation security services provider that provides managed detection and response services. Our services are powered through our world-class security orchestration and automation (SOAR) platform to drive operational efficiency with complete transparency.

Our unique operational experience, nation-state experts, and collaboration platform mean that you can focus on your business, while we monitor and respond to your security incidents and risks. SeeMo, our virtual analyst, accelerates cyber operations by learning and adapting from endless sources of data and responds to requests, providing context and actionable information. In the face of an increasingly hostile threat environment, CyberProof integrates all of 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 can work as an extension of your security team by delivering our services in a "hybrid" or co-delivery model and function as an integral part of your threat reduction objectives.



KEY PLATFORM ADVANTAGES

24x7x365 Operations:

Real-time, continuous monitoring, detection and response via a cloud-based platform

Smart Automation:

Accelerated detection and response through our SOAR platform's alert enrichment and incident prioritization

Actionable Intelligence:

Holistic, contextualized view of security risks with customizable reporting for different stakeholders

Minimized False Positives:

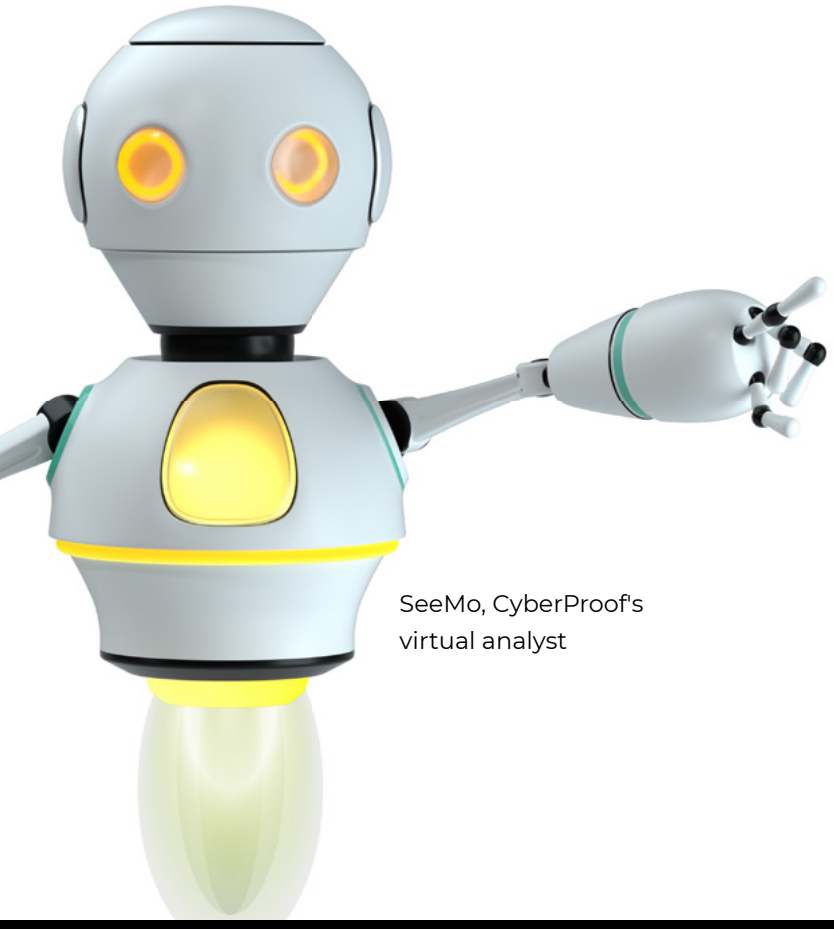
Automated alert enrichment and validation reduces alert fatigue while prioritizing incidents

Continuous Risk Reduction:

Orchestration & automation capabilities that provide faster time to response

Nation-State Expertise:

Access to nation-state level cyber expertise backed by global threat intelligence, to collaboratively solve complex issues



SeeMo, CyberProof's virtual analyst

- **Managed Security Services –** Security Event Monitoring, Managed Response, Use Case Engineering, Advanced SOC Services, and Security Platform Management
- **Enhanced Services –** Tailored Threat Intelligence, Breach & Attack Simulation, Managed Endpoint Detection & Response, Vulnerability Management, and Digital Forensics and Incident Response (DFIR) Retainer
- **Advisory Services –** Security Advisory, Security Assessment, Security Engineering, Staff Augmentation, and DevSecOps

MANAGED SECURITY SERVICES

CyberProof provides continuous security event monitoring and response capabilities by leveraging the CyberProof Defense Center (CDC) platform – a cloud-based SOC Orchestration, Automation, and Response platform. Services are delivered out of our state-of-the-art facilities in India, Israel, Spain, and Singapore.

Each team has experienced SOC Level 1 analysts who perform continuous security event monitoring and triage as well as SOC Level 2 analysts who are responsible for incident handling, security analytics, threat hunting, and managed response capabilities. In parallel, our SOC Content Specialists continuously develop new threat detection content, workbooks, and dashboards and maintains existing content.

SECURITY EVENT MONITORING

Reduce false positives and alert fatigue, discover hard-to-detect events, and enrich alerts with relevant contextual information to surface high risk incidents.

We monitor your security alerts and suspicious events, collected from multiple internal and external customer data sources. Threats are detected as they emerge in your critical cloud and on-premises infrastructure.

SeeMo, our virtual security analyst, proactively analyzes incoming alerts, automatically enriches them with additional data, queries for additional external information, and extracts observables that are useful from alerts – providing an effective triage process. This not only simplifies triage and the initial response process, but also helps eliminate false positives and noise.

Service Components

24x7 monitoring and triage of alerts	Manual or automated event enrichment and observable extraction	Issue validation and false positive isolation	Incident prioritization and playbook-driven response and escalation

MANAGED DETECTION AND RESPONSE

Detailed incident investigation and analysis, containment, and working with our customer stakeholders to mitigate risks and minimize business exposure.

Our global response team proactively handles incidents and collects the response activities for analysis and reinforced learning, leading to a continuous reduction in response time and associated exposure risk.

Utilizing ChatOps collaboration, managed incident response facilitates investigations and containment leveraging the collective expertise of the SOC analysts, threat intelligence experts, security specialists and customer team members. This improves efficiency and ensures full transparency, leading to better decision making.

Service Components

Incident handling and issue prioritization	Threat investigation, isolation and response	Event-driven targeted threat hunting and reconnaissance	IOC extraction and analysis
Continuous threat detection rule review	Playbook optimization and enhancement	Regular targeted threat reconnaissance report	Customized, self-configurable reports and dashboards

USE CASE FACTORY

Continuously develop customized attack scenario use cases, threat detection rules, and digital playbooks, in line with each customer's threat profile and cyber trends.

We baseline your detection rules against the MITRE ATT&CK matrix and identify gaps. In addition, we take input from senior analysts as well as from threat intelligence & hunting experts to continually develop, test, and deploy new use cases, threat detection rules, and digital playbooks to enhance detection of critical threats.

Our Use Case Factory is unique, involving not just threat detection rules but also well-defined alert response procedures that are automated and support dashboards, workbooks, and reports. Moreover, we have a team of specialist cyber experts who focus on creating automations that improve detection & response time.

Service Components

Continuously develop and maintain threat detection contents	Create SIEM rules and define EDR policies	Manage and maintain rules and security policies
Define incident response procedures and processes	Create, manage, and maintain digital playbooks	Facilitate use case automation

ADVANCED SOC SERVICES

Enhance SOC operational activities to improve investigation and tailored threat hunting activities - for effective issue isolation and faster response and remediation.

CyberProof's Advanced SOC Services combines expert resources and specialized tools to assist with detailed investigations, root cause analysis, complex threat hunting, and eradication of threats. The advanced SOC services assist customers with additional activities that need to be performed after the issue is resolved and the risk is mitigated.

Advanced SOC services are offered to customers as a bundle of hours; customers may make ad-hoc requests to the SOC team to leverage our advanced capabilities. A security specialist will work with customer stakeholders to define the scope and agree on the effort – and the utilized hours will be tracked in the weekly security operations report.

Service Components

Complex issue root cause analysis & detection of control failures	Advanced malware analysis and reverse engineering	Static and dynamic malware assessment and IOC extraction	Digital forensics covering file, app, ISO and image investigation
Cyber threat Intelligence investigations and reconnaissance	Vulnerability intelligence, assessments and exploit validation	Advice on security policy enforcements and issue mitigations	Input on SOC monitoring strategy and architecture best practices

SECURITY PLATFORM MANAGEMENT

Expert support services for timely patching and remediation of your IT and security systems.

CyberProof's SOC Engineering team helps customers design, deploy, configure, manage, and maintain robust SIEM platforms. As part of platform management services, our team works with customers to design and build secure data collection, event monitoring, and security analytics infrastructures.

In addition, the team continuously manages the security content covering security rules, policies, and configurations to ensure they are up to date and relevant – and aligned to the organization's targeted threats and associated risks.

Service Components

Security platform architecture, implementation and management	Flexible deployment models	Change management
Performance and health monitoring and configuration management	SIEM platform rule optimization and alert fine tuning	Service reporting

ENHANCED SERVICES

CyberProof's enhanced services complement our security event monitoring & response services – by wrapping around additional services that provide the ability to proactive hunt for threats, detect anomalies, and manage vulnerabilities and configuration weaknesses.

CyberProof's nation-state trained experts provide comprehensive support: Our Threat Intelligence (TI) team provides a continuous view of targeted threats and performs tailored threat investigations, while our Digital Forensics team leads complex incident examinations – performing root cause analysis, malware reverse engineering, and forensic investigations. In parallel, our Vulnerability Management & Red Team provide vulnerability assessments, intelligent prioritization, and continuous breach simulation.

TAILORED THREAT INTELLIGENCE

Deeper insights and earlier attack detection – based on knowledge of adversaries' modus operandi.

CyberProof's Threat Intelligence (TI) team enables the rapid detection of deceptions and threat actors in a way that is accurate, relevant, and actionable. Our experts utilize threat methodologies, dedicated intelligence, and automated procedures to proactively identify, integrate, and correlate vulnerabilities, assess impact, and prevent critical incidents.

The CDC has an early warning system that provides preemptive alerts for imminent threats and translates this intelligence into security actions. By proactively detecting cyber threats in near real time, we analyze, categorize, and prioritize cyber threats using proprietary data mining algorithms and unique deep learning capabilities.

Service Components

Tactics, techniques and procedures (TTP) analysis	IOC sharing & implementation	Periodic and on-demand reports
Targeted phishing identification, investigation, and takedown	Alert investigation and brand monitoring	Domain squatting

BREACH & ATTACK SIMULATION

Continuously test and validate your security defenses against real-life attack scenarios for faster identification and remediation of critical risks.

CyberProof partners with breach & attack simulation platforms to continuously exercise your defenses with the widest range of attack vectors, providing an Advanced Persistent Threat (APT) simulation of your security posture at all times. We analyze your ability to respond to real incidents with post-exploitation solutions and provide you with a clear picture of your organization's vulnerabilities from every point of exposure.

These solutions align to the MITRE ATT&CK matrix and Cyber Kill Chain methodologies – to break down complex and persistent attack methods used by hackers and create robust prevention, faster response, and actionable remediation that minimizes business impact.

Service Components

- Visualize attack surfaces and map attack paths
- Test for threats leveraging vectors such as email, browsing, and WAF
- Black, gray, and white box penetration testing exercises
- Actionable and prioritized remediation advice
- Continuously run attack simulations to identify security control gaps
- Lateral movement simulations to identify internal control gaps
- Clear visibility of security control posture and vulnerabilities

MANAGED ENDPOINT DETECTION & RESPONSE

Better endpoint visibility with endpoint security technologies that provide effective monitoring of suspicious activities.

CyberProof partners with leading endpoint protection, detection, and response technologies. We provide a continuous and fully managed endpoint detection & response service delivered through our cloud-based EDR solution. Our cyber experts design, deploy, and operate the EDR capability to prevent, detect, and proactively respond to threats in the endpoint environment.

CyberProof can leverage your existing EDR platform or you can let us deploy one for you. Either way, we manage your EDR as an integrated part of our managed security services.

Service Components

- Analysis of endpoint security events and alerts
- Deployment of customizable policies
- Manual investigations and threat hunting
- Quick response and remediation at scale
- Continuous 24x7 triage
- Alignment to the MITRE ATT&CK matrix
- Intuitive attack visualization

VULNERABILITY MANAGEMENT

Identify, contextualize, and validate vulnerabilities and assist in prioritization, remediation, and mitigation of exposure.

At CyberProof, we provide a holistic approach to managing vulnerability risks to uncover weaknesses in your organization. Our threat centric approach to vulnerability management helps provide organizations with an accurate view of risk exposure.

We utilize threat methodologies, dedicated intelligence, and automated procedures to proactively identify vulnerabilities, assess impact and prevent critical incidents. As an integral part of the CyberProof service platform, vulnerability intelligence findings are picked up by our security analysts who review simulation reports and recommendations and decide how best to respond.

Service Components

- Continuous vulnerability detection
- Event correlation and prioritization
- Automated Red Team and Blue Team exercises
- Vulnerability data centralization and de-duplication
- Breach & attack and lateral movement simulation
- Simulation of real-life attack exposing your crown jewels

DIGITAL FORENSICS AND INCIDENT RESPONSE (DFIR) RETAINER

Prepare for, manage, and respond to major cyber security incidents while minimizing the overall organizational impact.

CyberProof offers both remote and on-site support in reducing potential data loss and effectively recovering from an attack. Once engaged, our DFIR personnel isolates any unwanted activity and contains it.

The team identifies the source of any security breach (where possible), and determine its full extent. In addition, our cyber security experts prepare a thorough incident report detailing the impact of the investigation and any relevant findings. Where necessary, CyberProof's team also has experience in serving in the capacity of litigation support.

Service Components

- Establishing a detailed timeline and reconstructing attacks
- Containing the source of unwanted activity
- Determining what sensitive information has been compromised
- Providing a management report detailing the findings
- Assisting in data collection and providing chain-of-custody
- Identifying tools and methods employed by attackers
- Working with authorities in transitioning case evidence

ADVISORY SERVICES

Cyber security strategy means taking actions that improve the resiliency of infrastructure and of service offerings. By taking a top-down approach to cyber security, you guide the overall strategy that ultimately protects your organization against unauthorized access to systems and lessens residual risk to the organization.

Working with CyberProof gives you access to a higher level of cyber expertise. We offer cyber resources to support complex cyber incident detection and improvement activities, providing an end-to-end approach to cyber risk. Our team has extensive experience and follows a clearly defined governance model. Assessments are aligned to specific industry standards, and our outcome-based service delivery is tailored to meet your requirements. We partner with leading technology vendors – leveraging technologies as an enabler for improving cyber capabilities.

SECURITY ADVISORY

Develop a resilient, risk-based security strategy aligned to your business and make informed security decisions.

Risk management is the continuous process of identifying, assessing and responding to risk. As an organization, it is your responsibility to make sure these steps are taken to meet the obligations of clients, customers, and other stakeholders. CyberProof can assist in assessing the likelihood and impact of risk events and quantify the impact to the business, thus allowing a path forward on risk avoidance, acceptance, transference or mitigation efforts.

It is understood that unlimited budgets and staffing do not exist, and CyberProof can help ease the burden in this regard. Partnering with a trusted advisory allows risk decisions to be well informed and made in the proper context of business strategy.

Service Components

Cybersecurity strategy	Cyber risk management	Data privacy and compliance	Third-party risk assurance

SECURITY ASSESSMENT

Identify critical vulnerabilities in your estate and security controls while providing actionable insights to relevant stakeholders.

Our team provides an innovative approach to vulnerability assessment and penetration testing. With highly skilled staff and a detailed process, we identify areas of improvement with actionable steps to mitigate identified risks.

Our security maturity assessment is a gap analysis and baseline exercise that documents your “as is” state and compares it against your desired future state. A maturity plan is then established to further mature your security program. Understanding where your security strategy resides helps determine areas of focus and how to properly align efforts.

Service Components

- Red team simulations
- Services that go far beyond typical penetration testing
- Testing implementation to ensure alignment with compliance needs
- Actionable insight into attack methods
- Assessment of technical, operational and security-based controls

SECURITY ENGINEERING

Build robust cyber security infrastructures supporting on-premise, cloud and hybrid models.

CyberProof helps organizations design, build, configure and operationalize cyber security capabilities – working closely with specialist vendor technologies. We focus on providing scalable, cost-effective solutions and ensure the technologies chosen are future proof, and aligned with the organization’s overall cyber strategy.

CyberProof also provides assistance to customers with large-scale digital transformation, cloud deployments, architecture reviews, and assessment services around your cloud portfolio. We help assess your environment against best practices aligned to industry frameworks, and provide recommendations and improvements to enhance cyber resiliency.

Service Components

- Develop robust security architecture and transformation strategy
- Develop solutions architecture and detailed technology designs
- Architecture reviews, control gap analysis and assessments
- Digital transformation and cloud migration
- Build, configure, deploy and operationalize security technologies

STAFF AUGMENTATION

Assistance for your in-house team with a broad range of highly experienced security consultants.

CyberProof's security analysts can assist you with network planning to avoid unauthorized access, develop reports to share, recommend changes to policies or systems, and ensure software & hardware is updated. Our staffing model supports placing individuals within your organization, remote workers, or providing assistance for a defined period.

Our SIEM specialists can engage with your team to provide in-depth, hands-on operational support. Our vCISO services are designed to augment security teams by providing technical knowledge, compliance and governance expertise. In addition, we can provide a vDPO who has the expertise to assist with data mapping, impact assessments and GDPR readiness.

Service Components

- Expert SIEM, vCISO, and vDPO services
- Full alignment with your data retention policies
- Development of the necessary security to mitigate risks
- Collaboration in co-managed or fully managed SIEM deployments
- Direct focus on confidentiality, integrity and availability

DevSecOps

Application security management that detects security vulnerabilities on a continuous delivery throughout the software development lifecycle (SDLC) to produce secure, high- quality products.

According to industry benchmarks, fixing a vulnerability found during the deployment phase could cost 6x more than it would have cost to fix during the coding phase. Furthermore, fixing vulnerabilities identified during the testing phase could cost upwards of 15x more. This challenge prompted the establishment of a developer-led approach – according to which the earlier problems are identified, the quicker and more cheaply they can be fixed.

With CyberProof's robust security program, developers not only understand the threat landscape - CyberProof equips them with the tools and security best practices to detect and remediate vulnerabilities early in the life cycle.

Service Components

- Discovery assessment, identifying areas for improvement
- Vulnerability management across the application development lifecycle
- Staff augmentation to scale resources
- Secure coding methodology, integrating secure coding controls
- Security awareness training that supports best practices

ABOUT CYBERPROOF

CyberProof is a security services company that intelligently manages your incident detection and response. Our advanced cyber defense platform enables 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. We collaborate with our global clients, academia and the tech ecosystem to continuously advance the art of cyber defense.

CyberProof is part of the UST Global 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

LOCATIONS

Aliso Viejo | Barcelona | London | Singapore | Tel Aviv | Trivandrum