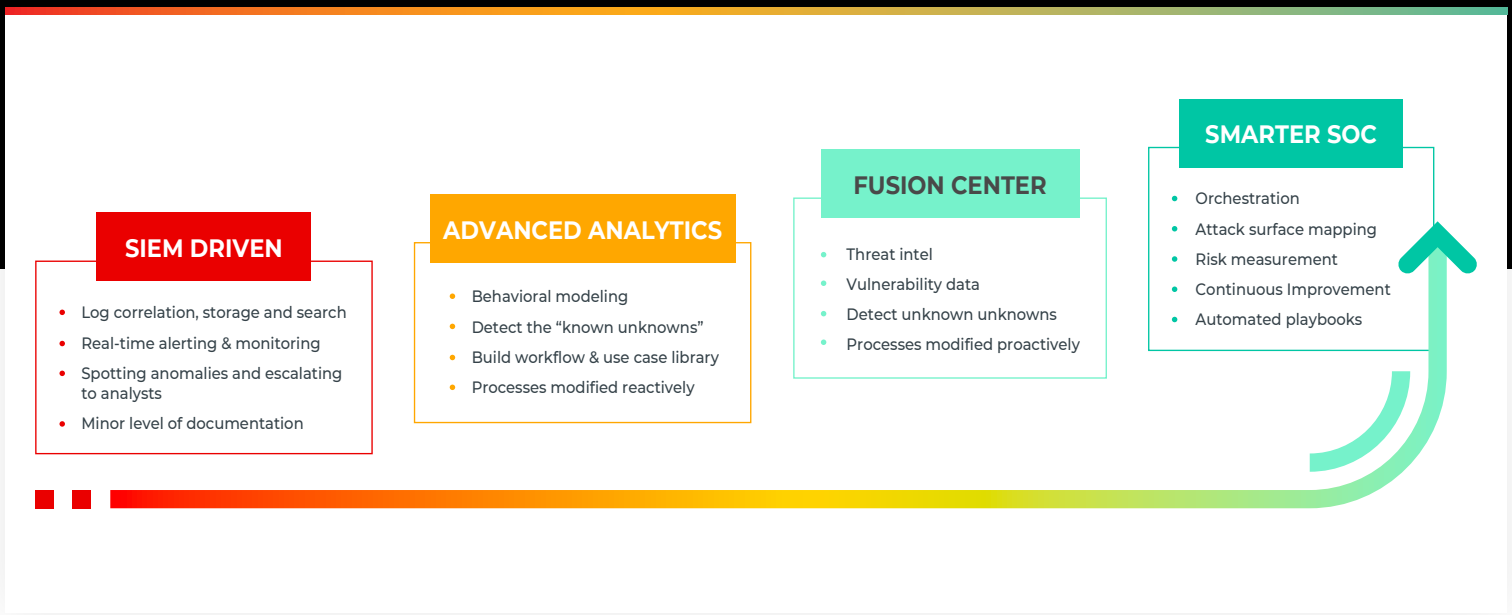
CyberProof®

CYBERPROOF COMPANY OVERVIEW

DRIVING THE ERA OF THE SMARTER SOC

SECURITY OPERATIONS HAVE EVOLVED

Security operations keep changing. In the last decade, we have seen four different stages in the evolution of security operations technology:



SIEM-driven – Security Operation Centers (SOCs) used first-generation technology, documenting logs and manually analyzing for indications of threat. Security operations teams incorporated Security Information Event Management (SIEM) tools to speed up this process and correlate disparate sources of data to generate security alerts.

Advanced Analytics – Fast forward a few years, and "Advanced Analytics" came into play using machine learning and behavioral modeling to minimize false positives and reduce the number of alerts being picked up by analysts.

Fusion Center – By this point, the booming development of cyber security technology in the security industry created multiple platforms – from Network Monitoring to Threat Intelligence and Incident Management, all which could be fused together to get a 360-degree view of cyber risk. With the introduction of Managed Detection and Response (MDR), this model addressed the "visibility across all environments" gap.

But many organizations soon realized the proliferation of cyber technologies coupled with a lack of transparency when outsourcing to traditional Managed Security Service Providers (MSSPs) was not seeing a clear return on investment. This has since made way for a fresh approach to security operations that addresses these very issues – the Smarter SOC.

THIS IS THE ERA OF THE ‘SMARTER SOC’

A Smarter SOC combines people and processes with a technology-agnostic security operations management platform that continuously optimizes and improves cyber defense. By relentlessly focusing on improving the efficiency of operations, a Smarter SOC continuously demonstrates value to stakeholders.

Here are the key challenges that a Smarter SOC aims to solve:

VISIBILITY INTO WHAT MATTERS

What’s Going Wrong?

Organizations’ cyber threat exposure is being distributed across multiple environments – from internal servers, databases and hosts to cloud-hosted/serverless, remote working, OT/IoT and hybrid environments – making it harder to monitor activity. The sheer volume of data and blind spots this produces makes it increasingly difficult to monitor for threats and vulnerabilities that will impact your business the most.

How Does a Smarter SOC Solve This?

Using an Open API architecture and cloud-native monitoring infrastructure brings together disparate data and tools into a single pane of glass. Taking advantage of orchestration and automation continuously enriches alerts and enables remediation teams to respond to validated incidents quickly.

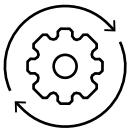
COLLABORATION WITH EXPERTS – AT THE RIGHT TIME

What’s Going Wrong?

The security skills shortage isn’t going away. Yet, simply outsourcing parts of your security operations without transparency or knowledge retention won’t allow you to upskill your team or adapt to future trends.

How Does a Smarter SOC Solve This?

A Smarter SOC adopts a hybrid engagement model with security service providers, that gives you access to the skills and capabilities of an MSSP that are hard to come by without losing control or visibility of day-to-day security operations.



CONTINUOUS IMPROVEMENT

What's Going Wrong?

Security teams are under pressure to reduce the time to detect and respond to cyber security threats while measuring the return on security investment. But staying ahead of the changing threat landscape requires an agile approach that is difficult to sustain, especially if resources are limited.

How Does a Smarter SOC Solve This?

A Smarter SOC uses a continuous improvement approach – future-proofing defenses, focusing time and effort only on the threats that matter to the business, and measurably reducing risk. Detection and response times are continuously reduced by proactively and continuously mapping the attack surface, orchestrating alert enrichment, and automating incident playbooks.

CYBERPROOF IS DRIVING THE ERA OF THE SMARTER SOC

Unlike legacy MSSPs, we leverage the Automation, Orchestration and Collaboration capabilities of our service delivery platform combined with our nation-state level expertise and hybrid engagement model to continuously improve your security operations.

The delivery of our services is led by former Elite Intelligence Unit security experts and supported by SOC teams in India, Israel, Singapore, Spain, and the USA – providing 24/7/365 coverage and monitoring. We bring a wealth of talent from national defense organizations: individuals with deep security operations expertise, software and networking professionals, and information security consultants with extensive business experience.

WHY CUSTOMERS CHOOSE US

Dramatic Reduction of Human Effort With SeeMo - Our virtual analyst BOT, SeeMo, extracts key observables from a security alert, enriches it with additional intelligence and vulnerability data, and takes proactive actions to minimize the risk and accelerate security operations.

Continuously Improve Your Defenses With Our Use Case Factory - We map our extensive library of use cases and digital playbooks to industry frameworks such as MITRE ATT&CK and our own threat intelligence to continuously reduce detection gaps and automate responses in line with your threat profile.

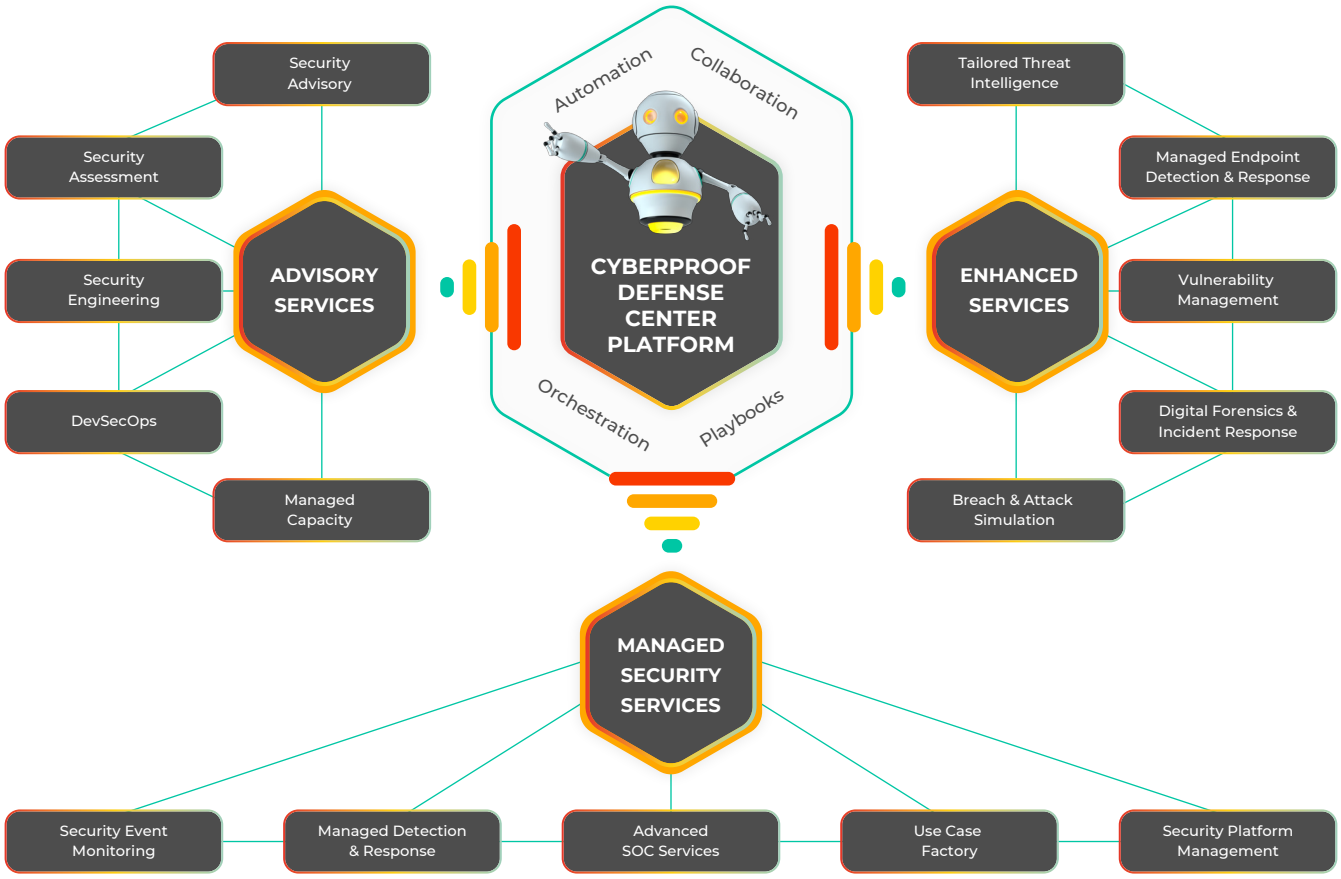
A Flexible, Hybrid Engagement Model For a True Partnership - Our engagement model is designed to operate as an extension of your security team by sharing responsibility for security operations and other security requirements.

Our Platform Facilitates Collaboration and Provides Transparency - The CyberProof Defense Center (CDC) Platform provides a single pane of glass view of security operations and ChatOps functionality to collaborate with stakeholders in real-time.

Modernized, Cloud-Based Security - We are pre-integrated with cloud-native SIEMs, such as Microsoft Azure Sentinel, so customers can use a scalable MDR solution while lowering costs.

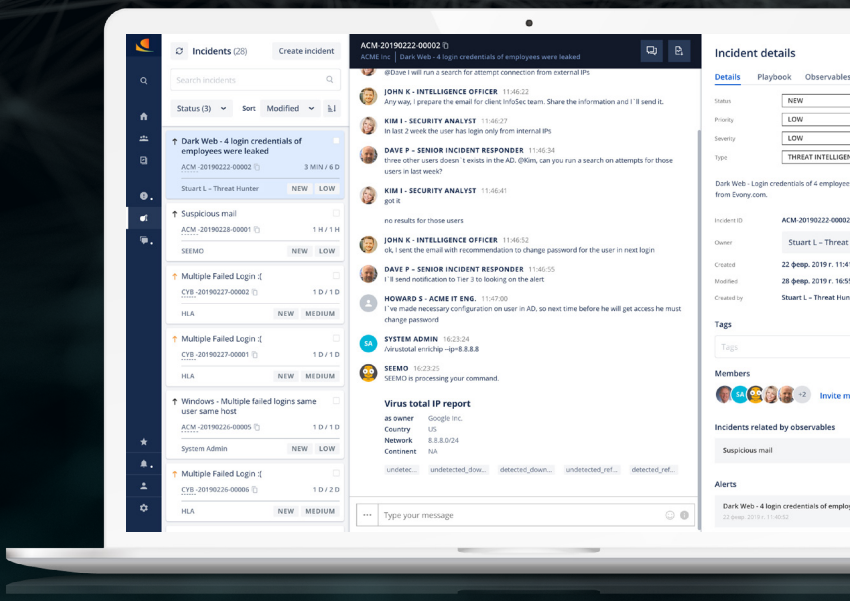
Independently Recognized Leader - In 2020, we were recognized as a Leader in the Midsize Managed Security Services market by Forrester - one of the world's leading independent technology research companies. This is the second time in a row we've been rated a Leader, having achieved the same position in their 2018 evaluation of Emerging Managed Security Services Providers.

OUR SERVICES



CYBERPROOF DEFENSE CENTER (CDC) PLATFORM

The CDC is our SaaS-based service delivery platform that leverages Orchestration, Automation and Collaboration capabilities to simplify and accelerate security operations. The CDC integrates seamlessly with your existing security investments such as your SIEM, EDR, vulnerability management tools, threat intelligence platforms, incident workflow management tools and more. This enables analysts to be more productive, reduces the cost and time needed to respond to threats and facilitates a more coordinated response.



24x7 Operations:

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.

Comprehensive Risk Measurement:

Obtain a holistic view of cyber risk using accurate risk-scoring mechanisms and measurable KPIs.

Orchestration & Integration:

Seamless integration with SIEM, EDR, threat intelligence, vulnerability management and incident management platforms to provide 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.

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.

WE'RE A RECOGNIZED LEADER

Recognized by Forrester as a Leader in Midsize Managed Security Services

Most Innovative Managed Detection and Response Provider 2019

Next-Gen Managed Detection and Response (MDR) at RSA Conference 2020

Cybersecurity Breakthrough Award 2019 for Overall Security Orchestration, Response and Automation Service Provider of the Year

2020 Cyber Security Excellence Award in Managed Detection and Response category

Cyber Defense Winner for Managed Detection and Response 2019

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