CyberProof®
A UST Company

ADVANCED THREAT HUNTING SERVICES

CyberProof's dedicated Threat Hunters proactively search for malware and 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.

IDENTIFY THREATS THAT BYPASS YOUR DEFENSES

Challenge - On average, 44% of emerging threats are missed by security tools. But SOC teams are often only able to allocate their existing analysts, who aren't trained Threat Hunters, to spend a limited amount of time sifting through different systems for hidden threats.

Our Solution - We have a dedicated Threat Hunting team whose primary role is to proactively hunt for indicators of threats that have been previously missed by security tools or security analysts. Our Threat Hunters carry out investigations drawing from relevant incidents, dark web activity, as well as MITRE ATT&CK techniques.

UNCOVER THREATS HIDING IN YOUR NETWORK

Challenge - Research shows that attackers can be inside a network for days, weeks, and even months before being discovered – preparing and executing attacks, while evading security defences.

Our Solution - We enable earlier detection of advanced threats by using behavioral analysis techniques to hunt for anomalies in the network, endpoint, cloud and insider activity. Our Threat Hunters also use a process of continuous feedback to improve analytics, detection rules and response actions.

IMPROVE INCIDENT RESPONSE EFFORTS

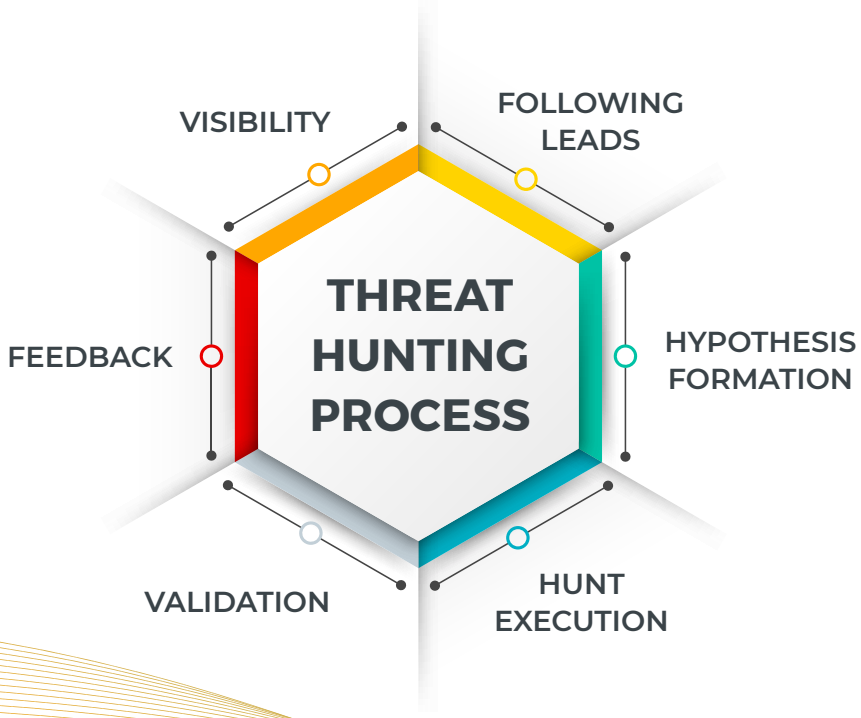
Challenge - Obtaining context regarding compromised systems can be time consuming if you don't have supporting data. This becomes even more critical when presenting evidential information to regulators after a breach.

Our Solution - Our Threat Hunters work as an extension to your security analysts and incident responders to enrich alerts and incidents with historical and real-time IOCs, support forensic investigations and uncover where threats have compromised other systems in the network.

WHAT'S INCLUDED?

- **Hunting for Known Malicious Threats -** Leveraging IOA and IOC feeds to perform hunting for known malicious threats that might be lurking within the perimeter.
- **Incident and Intelligence-Based Hunting -** Leveraging incidents across our client base, and alerts from our Cyber Threat Intelligence team's research into the clear, deep and dark web.
- **Behavioral Analysis -** Using network, endpoint, user and cloud data to understand your attack surface and detect deviations.
- **Tactics, Techniques and Procedures-Based Hunting -** Identifying your detection gaps against the MITRE ATT&CK matrix and hunting for evidence of infection.
- **Hunting Packages and Reports -** Pre-defined service packages detailing specific scenarios and the associated hunting activities. Scheduled reporting including remediation and response recommendations such as YARA rules providing continuous improvement of detection capabilities.

CYBERPROOF'S THREAT HUNTING PROCESS



Visibility - Retrieve and aggregate data from endpoint agents, network sensors, cloud instances, email gateway and more.

Following Leads - Acquire leads from incident reports, intelligence, or environment baseline knowledge regarding potential threats to the environment that were identified.

Hypothesis Formation – Develop actionable hypotheses targeting the activities threat actors might perform in the environment and how they might operate during each phase of an attack.

Hunt Execution – Retrieve and analyze results iteratively using live and historic relevant data to detect malicious activity.

Validation – Validate the identified events to determine and separate false positive detections from the data that matches the hypothesis but is not actually malicious. Information about validated events which may represent potential breaches is shared with clients via agreed channels.

Feedback – Enhance the efficiency of future hunts by reviewing results and fine tuning our hunting procedures to better suit your environment using feedback from client resources, and CyberProof analysts and experts.

WHY CYBERPROOF?

Dedicated Threat Hunting team - Expert Threat Hunters focused full time on proactive Threat Hunting activities to support forensic investigation, saving you time and money on building similar skills in-house.

We go beyond basic Threat Hunting methods - Threat Hunting efforts are often only focused on retro-hunting on known indicators and signatures using simple hunting queries in the SIEM or EDR. We use advanced procedures such as incident and intelligence-based hunting, TTPs, and anomaly hunting to widen the scope of sources for faster detection.

Hunting based on intelligence from our MDR clients - We use incident and threat information from our SOC clients and coverage of dark web forums to build accurate hypotheses and more efficiently hunt for relevant adversary activity.

Customized Threat Hunting programs - We adopt a multi-layered approach to Threat Hunting by starting with an onboarding process to understand the customer's environment and objectives, then building a roadmap to progressively adopt Threat Hunting capabilities and enhance these over time.

ABOUT CYBERPROOF

CyberProof is a security services company that helps organizations to intelligently manage 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. 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