Managed Threat Hunting

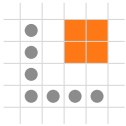
Cyberint

THE GROWING SCALE AND SOPHISTICATION OF THREATS DEMANDS A SHIFT TO PROACTIVE CYBER DEFENSE.

Hunt for Threats – before they become a breach. Getting proactive about cyber defense means that you can no longer rely on your traditional detection mechanisms. Rather, you must assume that you have already been compromised, and hunt proactively to identify and respond to cyber threats, minimizing dwell time and adverse impact.

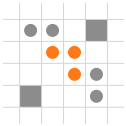
Cyber expertise coupled with accurate Threat Intelligence – is a must. To be able to effectively identify the threat, you need to focus the hunt, based on the tools, tactics and procedures (TTPs) attackers will use. This hypothesis-based hunting requires deep understanding of both the TTPs and your specific threat landscape, essentially identifying who will attack you and how.

CYBERINT'S APPROACH TO THREAT HUNTING



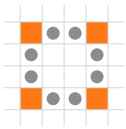
INTELLIGENCE DRIVEN

Leveraging Cyberint proprietary threat intelligence technology to identify your unique threat profile and map adversaries' TTPs to drive the threat hunting.



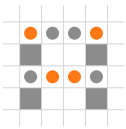
SOAR ENHANCED

Using automated playbooks and orchestration to streamline and support large scale operations and ensure repetitive and effective investigation and response actions.



CONTINUOUS & MANAGED

Ad-hoc hunts can only provide a point-in-time snapshot of your cybersecurity stance. Ongoing hunts, delivered by top ex-military cyber experts, provide you with continuous assurance and resilience.



COLLABORATIVE & TRANSPARENT

Providing visibility across threats in your environment using a single pane. Direct communication with the Information security teams and SOC analysts with full transparency to act hand in hand with the customer in triage, investigation, and response to incidents.

WHAT IS CYBERINT'S MANAGED THREAT HUNTING?

Managed intelligence-driven threat hunting solution that provides ongoing and continuous protection, hunting for threats and responding to security issues in real-time to reduce their impact.

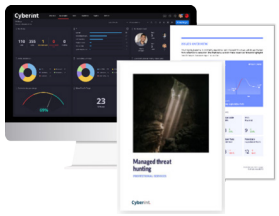
We detect malicious activity in real-time, proactively hunting for threats across your environment. Leveraging Cyberint's proven threat intelligence expertise, proprietary and third-party technologies, and the MITRE ATT&CK™ framework, we provide automated threat hunts, with custom detections, investigations, and response playbooks.

BUSINESS IMPACT

Managed Threat Hunting offering reduces total cost of ownership of in-house effort and costs of cybersecurity technology, operations, and manpower. It provides cost and effort reduction across multiple areas by ensuring:

- Integration with existing EDR systems
- Ongoing subscription (for various threat intelligence feeds, malware sandboxes, or SOAR)
- Skills & manpower on a continuous basis

HOW IT WORKS

Data Collection	Detection	Enrichment, Analysis and Triage	Automation & Orchestration	Containment & Remediation
1	2	3	4	5
Hosted EDR Environment Multi-tenant ENDGAME. An Elastic company CROWDSTRIKE vmware Carbon Black.	**Applied Research Lab** Fully Simulated Organization Adversary Simulation Custom Detection Hunting Hypothesis	**Automated Malware Detonation and Intelligence** **Customized Analysis & Reverse Engineering** **API and Opensource** MITRE ATT&CK™ VirusTotal DOMAINTOOLS	Case Management Automated Playbooks Collaboration Dashboards Siemplify	

HOW CYBERINT EXPERTS DRIVE THE HUNT?

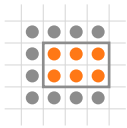
- Threat Intelligence
- EDR technology
- Automate and orchestrate the detection, investigation, and response with SOAR from Siemplify
- Leverage MITRE ATT&CK framework to uncover TTPs and drive the most effective response actions

MITRE ATT&CK™

KEY BENEFITS

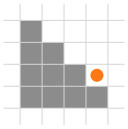
BE ONE STEP AHEAD

Intelligence-driven speeds up hunts enriching detection with the most recent and relevant adversarial TTP's, augmenting the detection and response capabilities beyond EDR and aligning to MITRE ATT&CK™



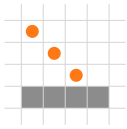
EFFECTIVE MITIGATION AND REMEDIATION

Cyber experts to provide the most effective hunts and reduce cybersecurity TCO by leveraging Cyberint's domain expertise, technology and fast containment



REDUCE IMPACT ON YOUR ORGANIZATION

Leveraging automation with advanced SOAR capabilities helps triage, investigation and remediation, contextualize events, alerts, incidents and provide full transparency to the entire process



GAIN VISIBILITY TO YOUR ENVIRONMENT

Robust case management capabilities and real-time collaboration with SOC analysts augmenting their effectiveness, and the full visibility of where things stand

> *Tracking the bad guys and knowing how they think and what they are doing - this is Cyberint's space and they know what they are doing. Until you use Cyberint, you really don't have the right understanding of who is trying to attack your organization.*
>
> Global eCommerce company

> *It is the managed service that provides real value in turning findings into relevant information and alerts tailored to our business.*
>
> Global US-based retailer

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA
214 W 29th St.
New York, NY 10001
Tel:+1-646-568-7813

ISRAEL
17 Ha-Mefalsim St.
4951447 Petah Tikva
Tel:+972-3-7286-777

UNITED KINGDOM
WeWork Fox Court
14 Grays Inn Rd., Holborn
WC1X 8HN, London
Tel: +44-203-514-1515

SINGAPORE
135 Cecil St.
#10-01 MYP PLAZA 069536
Tel:+65-3163-5760

LATAM
Panama City
Tel:+507-395-1553