Managed Threat Hunting

Cyberint

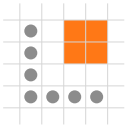
THE GROWING SCALE OF THREATS AND SOPHISTICATION OF EVADING DETECTION DEMANDS DOING THINGS DIFFERENTLY.

Hunt down threats - don't stop at detection. Cyber expertise isn't nice to have, it's a must now. Taking proactive approach is what's essential to detect threats currently evading security control in order to minimize dwell time and impact them eventually make.

With the increasing complexity and sophistication of the attacks by using LOLBins, threat actors are aiming to compromise networks and assets. This means - they are more and more capable in using those methods to scale their malicious activity and evade detection by the existing security solutions.

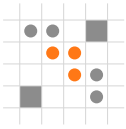
Even though the latest average dwell time of attacks before they're contained is **56 days,** there're still lots of cases when threat actors remain undetected underscoring the need for managed threat hunting in addressing that. *(M-Trends 2020 Report. FireEye Mandiant)*

CYBERINT'S APPROACH TO THREAT HUNTING



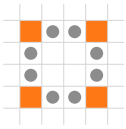
INTELLIGENCE DRIVEN

Leveraging proprietary robust ML-driven threat intelligence technology to drive the threat hunts.



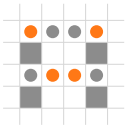
SOAR ENHANCED

Orchestrating technology flow and automating processes, operations in a growing scale of events, data points, and enrichment.



CONTINUOUS & MANAGED

Ad-hoc hunts are not enough in an "assumed breach" mindset. Ongoing hunts to discover of threats and incidents across the endpoint fleet with containment and remediation, delivered by ex-military security experts.



COLLABORATIVE & TRANSPARENT

Providing visibility across the endpoints in your environment using a single pane. Direct communication with your security team with full transparency to act hand in hand with the customer when investigating and verifying security incidents.

WHAT IS CYBERINT'S MANAGED THREAT HUNTING?

Managed intelligence-driven threat hunting solution that provides ongoing and response, hunting and responding to security issues in real-time to reduce their potential impact.

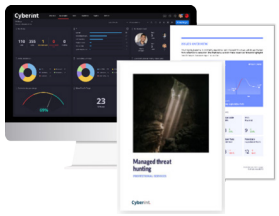
We detect malicious activity in real-time, provide visibility to help reduce potential attack surface, and perform forensic investigation going back in time to detect malicious activity. Leveraging Cyberint's proven threat intelligence expertise, third-party technologies, and the MITRE ATT&CK™ framework, the offering builds and automates 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
- Near-effortless deployment
- 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?

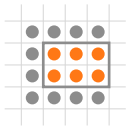
- Threat Intelligence
- EDR technology
- Automate and orchestrate the detection, investigation, and response with SOAR from Siemplify
- Leverage MITRE ATT&CK framework to uncover TTPs and drive the most effective response actions

MITRE ATT&CK™

KEY BENEFITS

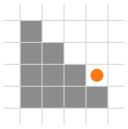
BE ONE STEP AHEAD CONTINUOUSLY

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™



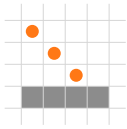
EFFECTIVE MITIGATION AND REMEDIATION

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



KNOW YOUR SITUATION

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

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