



# Managed Threat Hunting

Cyberint

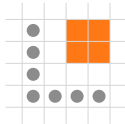
---

## 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.

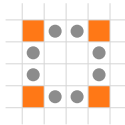
**Cyber expertise coupled with accurate Threat Intelligence – is a must.** To be able to effectively identify the threat, you need to focus the hunt, based on the tools, tactics and procedures (TTPs) attackers will use. This hypothesis-based hunting requires deep understanding of both the TTPs and your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

## CYBERINT'S APPROACH TO THREAT HUNTING



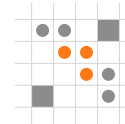
### INTELLIGENCE DRIVEN

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



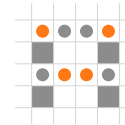
### CONTINUOUS & MANAGED

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.



### SOAR ENHANCED

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



### 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.



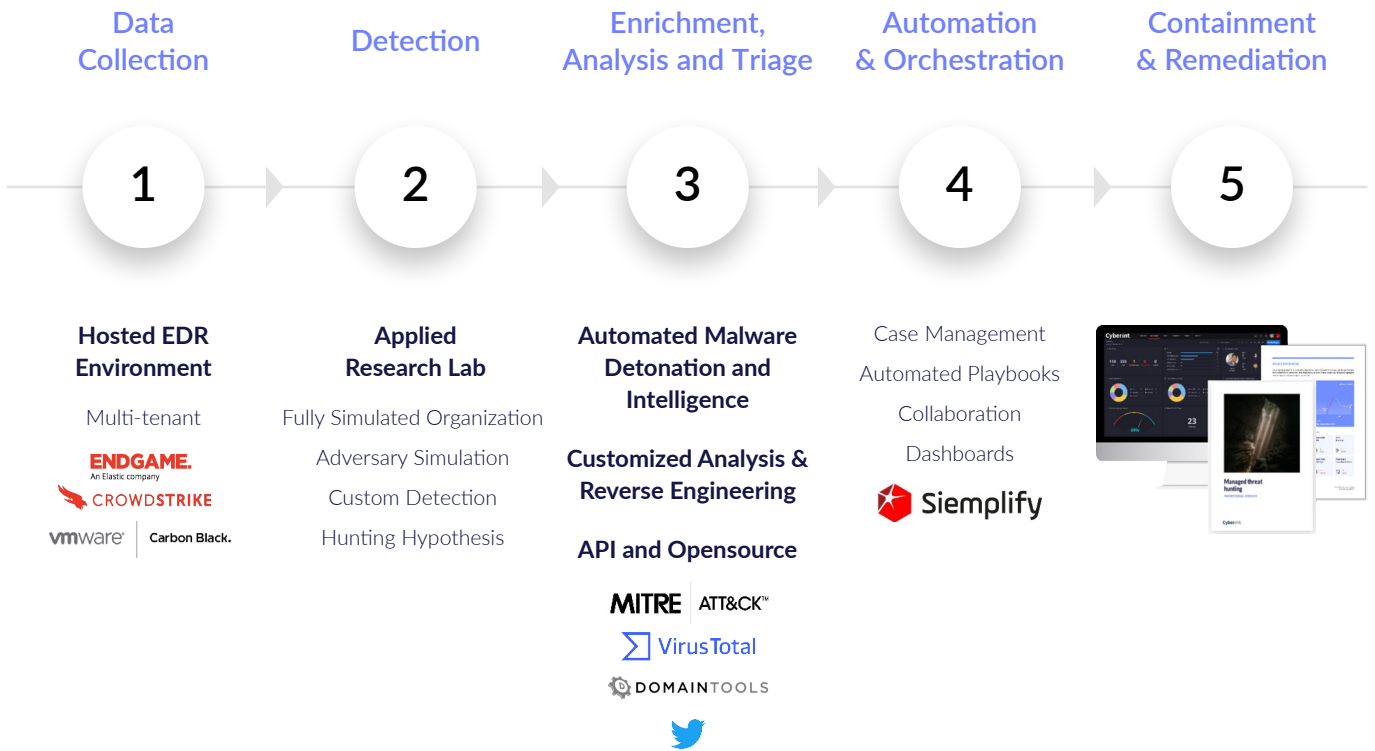
We detect malicious activity in real-time, proactively hunting for threats across your environment. Leveraging Cyberint's proven threat intelligence expertise, proprietary and third-party technologies, and the MITRE ATT&CK™ framework, we provide automated threat hunts, with custom detections, investigations,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



# HOW CYBERINT EXPERTS DRIVE THE HUNT?

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



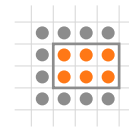
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	ateral Movement	Collection	Exfiltration	Command and Control
Drives-by Compromise	AppleScript	bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Automated Exfiltration	Commonly Used Port
Explicit Public-Facing Application	QMSTP	Accessibility Features	Accessibility Features	Binary Packing	Bash History	Application Window Discovery	Distributed Component Object Model	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInet DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Logon Scripts	Data Staged	Data Transfer-Size Limits	Custom Command and Control Protocol
Spearfishing Attachment	Control Panel Items	AppInet DLLs	Application Shimminig	Clear Command History	Credentials In Files	Network Service Scanning	Pass the Hash	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearfishing Link	Dynamic Data Exchange	Application Shimminig	Bypass User Account Control	QMSTP	Credentials In Registry	Network Share Discovery	Pass the Ticket	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearfishing via Service	Execution through API	Authentication Package	CLI Search Order Hijacking	Code Signing	Exploitation for Credential Access	Remote Desktop Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Exploitation for Privilege Escalation	Code Signing	Forced Authentication	Network Sniffing	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Extra Window Memory Injection	Compiled HTML File	Hooking	Password Policy Discovery	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	File System Permissions Weakness	Component Firmware	Input Capture	Peripheral Device Discovery	Replication Through Removable Media	Data from Removable Media	Screen Capture	Multi-Stage Channels
	Installs/Uninstalls	Change Default File Association	Hooking	Control Panel Items	Kerberoasting	Permission Groups Discovery	Shared Webroot	Input Capture	Video Capture	Multi-hop Proxy
	LSASS Driver	Component Firmware	Image File Execution Options Injection	DCShadow	LLNMI/NBES-MS Poisoning	Query Registry	SSH Hijacking	Man in the Browser	Man in the Browser	Multiband Communication
	Launchpad	Component Object Model Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Process Discovery	Taint Shared Content	Screen Capture	Port Knocking	Multilayer Encryption
	Local Job Scheduling	Create Account	Path Interception	Disabling Security Tools	Password Filter DLL	Query Registry		Video Capture	Remote Access Tools	
	Malware	DLL Search Order Hijacking								
	PowerShell	Path Hijacking								

## KEY BENEFITS



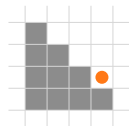
### BE ONE STEP AHEAD

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™



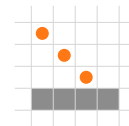
### EFFECTIVE MITIGATION AND REMEDIATION

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](http://www.cyberint.com) | [sales@cyberint.com](mailto:sales@cyberint.com) | [blog.cyberint.com](http://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