



Managed Threat Hunting

Cyberint

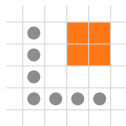
THE GROWING SCALE OF THREATS AND SOPHISTICATION OF EVADING DETECTION DEMANDS DOING THINGS DIFFERENTLY.

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 they 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.

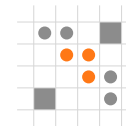
Even though the latest average dwell time of attacks before they're contained is **56 days**, there're still lots of cases when threat actors remain undetected underscoring the need for managed threat hunting in addressing that. *(M-Trends 2020 Report. FireEye Mandiant)*

CYBERINT'S APPROACH TO THREAT HUNTING



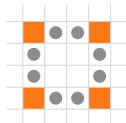
INTELLIGENCE DRIVEN

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



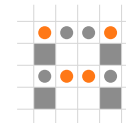
SOAR ENHANCED

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 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.



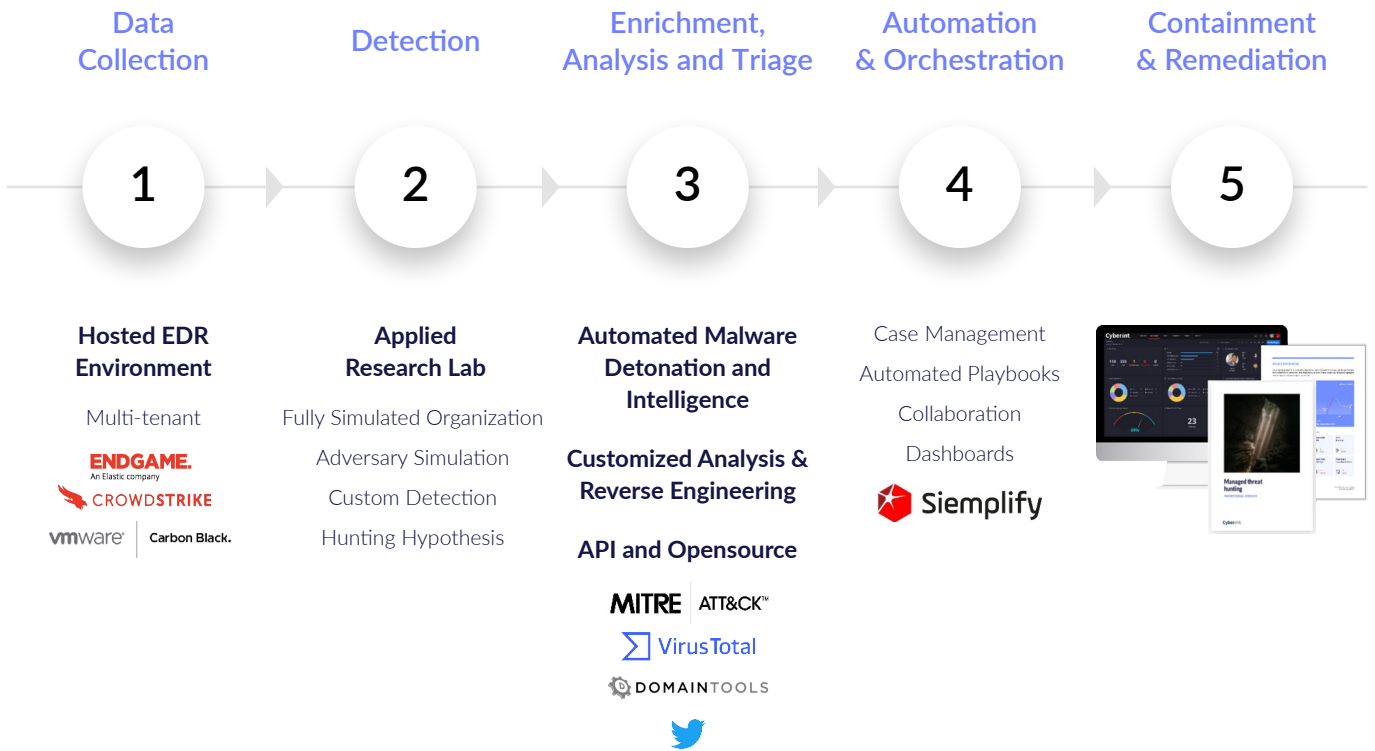
We detect malicious activity in real-time, provide visibility to help reduce potential attack surface, and perform forensic investigation going back in time to detect malicious activity. Leveraging Cyberint's proven threat intelligence expertise, third-party technologies, and the MITRE ATT&CK™ framework,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



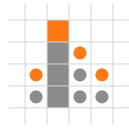
HOW CYBERINT EXPERTS DRIVE THE HUNT?

- 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™

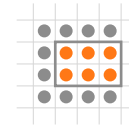
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	ateral Movement	Collection	Exfiltration	Command and Control
Drives-by-Compromise	AppleScript	bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account 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 Shimming	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	Authentication Package	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	BITS Jobs	Exploitation for Privilege Escalation	Code Signing	Exploitation for Credential Access	Remote Desktop Protocol	Remote File Copy	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	Bootkit	Extra Window Memory Injection	Compiled HTML File	Forced Authentication	Remote Desktop Protocol	Remote File Copy	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	File System Permissions Weakness	Component Firmware	Hooking	Network Sniffing	Remote Services	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Capture	Password Policy Discovery	Replication Through Removable Media	Data from Removable Media	Exfiltration Over Physical Medium	Multi-Stage Channels
	Installs/Uninstalls	Component Firmware	Hooking	Control Panel Items	Kerberoasting	Peripheral Device Discovery	Shared Webroot	Input Capture	Exfiltration Over Physical Medium	Multi-hop Proxy
	LSASS Driver	Component Object Model Hijacking	Image File Execution Options Injection	DCShadow	LLNMI/NBLS-MS Poisoning	Permission Groups Discovery	Screen Capture	Man in the Browser	Scheduled Transfer	Multiband Communication
	Launchpad	Create Account	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	Process Discovery	Screen Capture	Man in the Browser	Scheduled Transfer	Multilayer Encryption
	Local Job Scheduling	DLL Search Order Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	Query Registry	Video Capture	Man in the Browser	Scheduled Transfer	Port Knocking
	Malware	Path Hijacking	Path Interception	Disabling Security Tools	Private Keys	Remote System	Video Capture	Man in the Browser	Scheduled Transfer	Remote Access Tools
	PowerShell	Path Hijacking	Path Interception	Disabling Security Tools	Private Keys	Remote System	Video Capture	Man in the Browser	Scheduled Transfer	Remote Access Tools

KEY BENEFITS



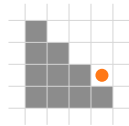
BE ONE STEP AHEAD CONTINUOUSLY

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™



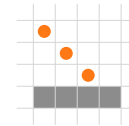
EFFECTIVE MITIGATION AND REMEDIATION

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