



Bassem Hemida

## Welcome to SANS Night Talk

In an era where cyber threats are increasingly sophisticated and pervasive, a robust defence strategy is more crucial than ever.

This talk delves into the cutting-edge approach of threat-informed defence, emphasizing the integration of threat intelligence across all levels of an organization.





# **THREAT-INFORMED DEFENCE**

---

## **INTEGRATING THREAT INTELLIGENCE AT ALL LEVELS**

You will get insights into

Threat Informed Defence

Understanding the Threat

Threat Profiling and landscape

Fusion Model for Threat Management

Threat Management Lifecycle

Integration at all levels

Q&A



# Nice meeting you!

## About me

A cybersecurity Senior Manager/CISO/Threat Management Lead with over a decade of technical professional services experience working with corporates and multinational organizations throughout Europe and Middle East in the financial, public and energy sectors.

## Professional Experience

Threat Management  
Security Architecture  
Incident Response and Threat Hunting Operations  
Digital Forensics and Intrusion Detection  
Red Teaming, Covert Operations and Cybersecurity Crisis Simulation  
IT/OT Cyber Strategy



GSE #301



<https://bhemida.com>



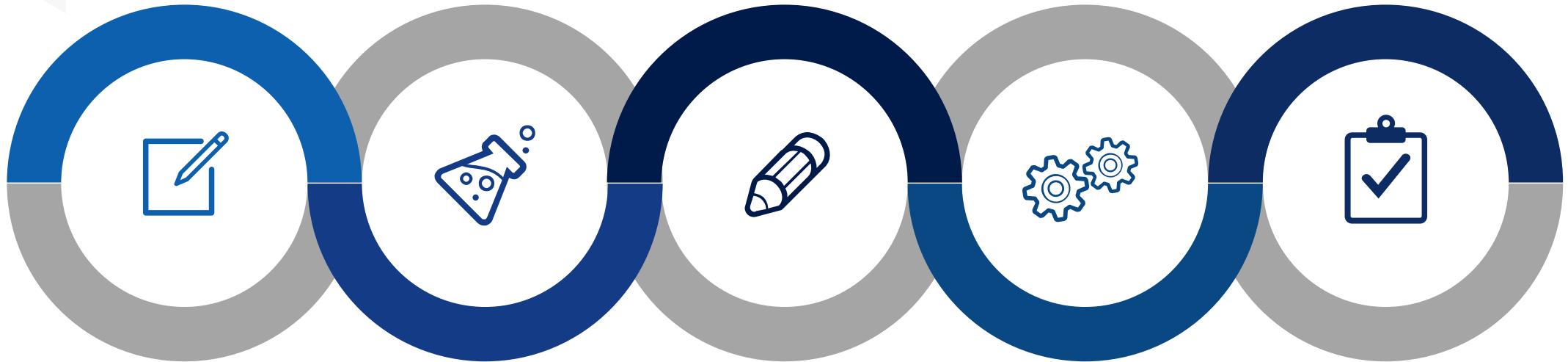
## Threat Informed Defence

Threat informed defence is a proactive **approach** to cyber risk management that involves **integrating** cyber capabilities/functions to **identify** and prioritise **threats** that are most likely to be successful and can **impact the business**.

**Support** in selecting and implementing secure, vigilant and resilient controls to **mitigate** those threats and **reduce the risk**.



# Threat Informed Defence Approach



## Identify Threats

Identify the potential threats that an organization or system may face

## Analyse Threats

Analyse in order to determine their likelihood and potential impact

## Prioritise threats

Prioritise in order to focus defence efforts on the most significant threats

## Implement Defences

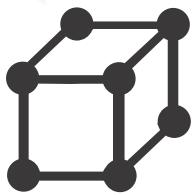
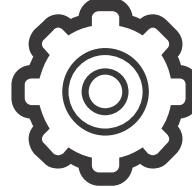
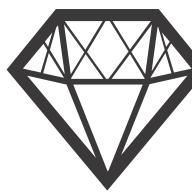
Defences and response plans can be implemented to mitigate the risks associated with those threats

## Monitor and update

Ongoing monitoring and analysis of potential threats, in order to keep pace with the constantly evolving threat landscape



# Why Threat Informed Defence

Business	Full Chain	Operations	Risk Management	Scale up
 <p>Limited financial resources and personnel resources. Therefore, there is a must to prioritize security investments.</p>	 <p>Cyberattacks are not singular events but part of an overall scenario, chain of events, or operation, so considering security controls in this way benefits defenders. Instead of trying to develop requirements against “virtual private network (VPN) compromises,” we can think through a full compromise scenario.</p>	 <p>Prioritize efforts to mitigate actual threats and implement defensive controls with the best return.</p>	 <p>Implement controls and countermeasures to reduce the risks. Eliminate the risk by discontinuing the activity or process that introduces the risk.</p>	 <p>Acknowledge and accept the potential consequences without implementing additional controls.</p>



# Understanding the Threat

## Cyber Threat

Cyber Threat is when combination of **intent, capability and opportunity exist which can lead to a potential impact on business**. These three distinctive areas are important when assessing the threat landscape and who the Threat Actors are.

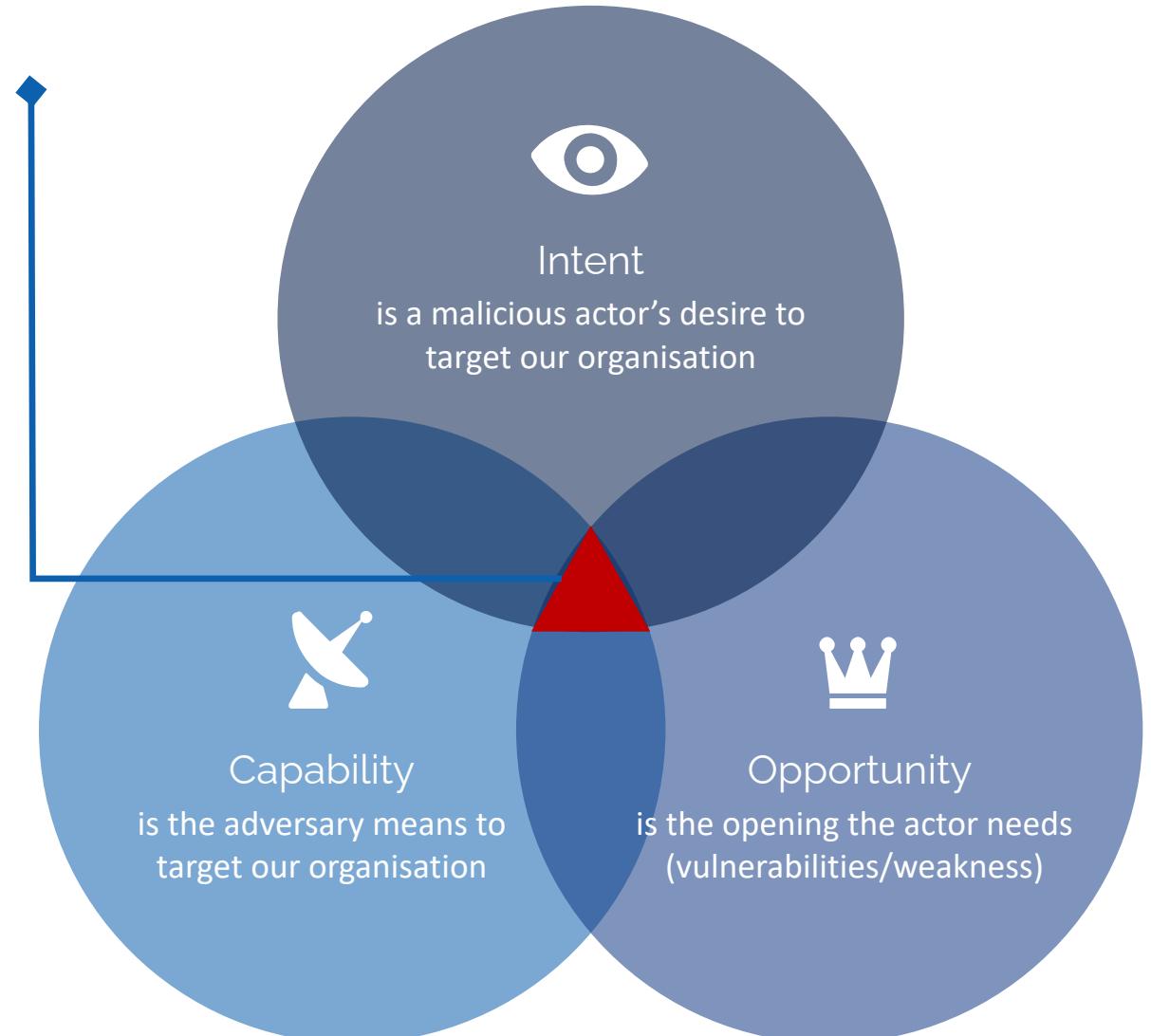
## C2M2 Objective

Cybersecurity Capability Maturity Model, The Threat and Vulnerability Management (THREAT) domain comprises three objectives:

1. Reduce Cybersecurity Vulnerabilities.
2. Respond to Threats and Share Threat Information.
3. Support Management Activities.

## DORA Reporting Requirements

**Digital Operational Resilience Act (DORA)**, when it comes to the data fields on the **reporting of significant cyber threats**, the ESAs have considered the **voluntary nature of reporting** in accordance with Article 19 of DORA. Threat reporting should cover the DORA mandatory required nine fields.



# Threat Landscape

## Who: Threat Actors

Who might have the intent and capabilities and wait for the opportunity?

- Cyber criminals.
- Skilled individual hackers.
- Nation states.
- Insiders/partners.
- Competitors.
- Hacktivists.

## Why: Intent

What are they after? Mission Critical Services and information?

- Financial Fraud.
- Sabotage and Disruption.
- Competitive Advantage.
- Stealing Trade Secrets.
- Ransom.
- Hacktivism.
- Espionage.

## How: Capability

Tools, tactics, techniques and procedures

- Ransomware
- (Infostealer) Malware
- Malvertising
- DDoS
- Remote monitoring and management
- Generative AI

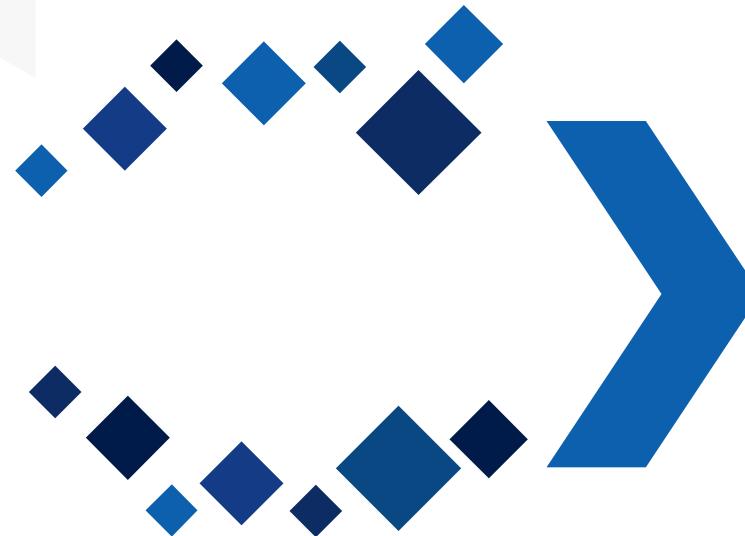
## How: Opportunity

The opening window the actor needs:

- Vulnerabilities
- Cloud
- Compromised credentials
- Supply chain
- Third part
- Geopolitics events



# Fusion Model for Threat Management



## Brainstorming

Understanding frameworks like the Cyber Kill Chain, Diamond Model, and Pyramid of Pain is key to effective cybersecurity. Each offers unique insights into identifying and responding to threats, providing a comprehensive view of the threat landscape.



## Conceptualisation

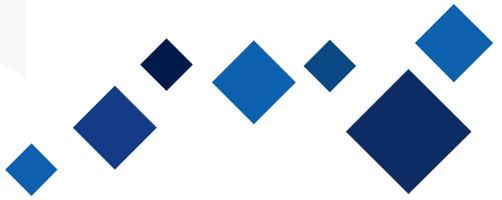
Using the 7D Course of Action—Discover, Detect, Deny, Disrupt, Degrade, Deceive, and Destroy—helps organizations respond strategically at each attack stage. This alignment makes defences more targeted and effective.



## Threat (PIR)

With these concepts integrated, organizations can set Priority Intelligence Requirements (PIRs) that focus on the most critical threats. This ensures that resources and attention are directed toward the highest risks, enhancing the effectiveness of threat detection and response.

# Fusion Model for Threat Management



## Brainstorming

Understanding frameworks like the Cyber Kill Chain, Diamond Model, and Pyramid of Pain is key to effective cybersecurity. Each offers unique insights into identifying and responding to threats, providing a comprehensive view of the threat landscape.

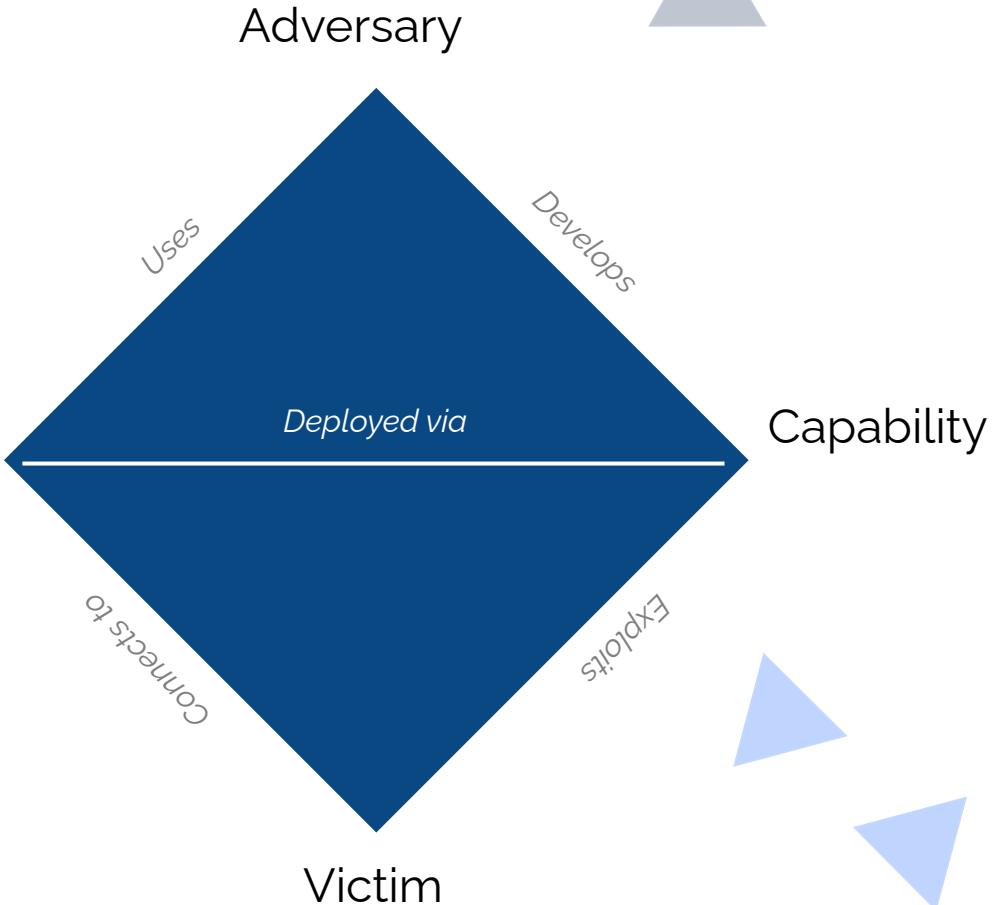




Brainstorming

Brainstorming

Infrastructure



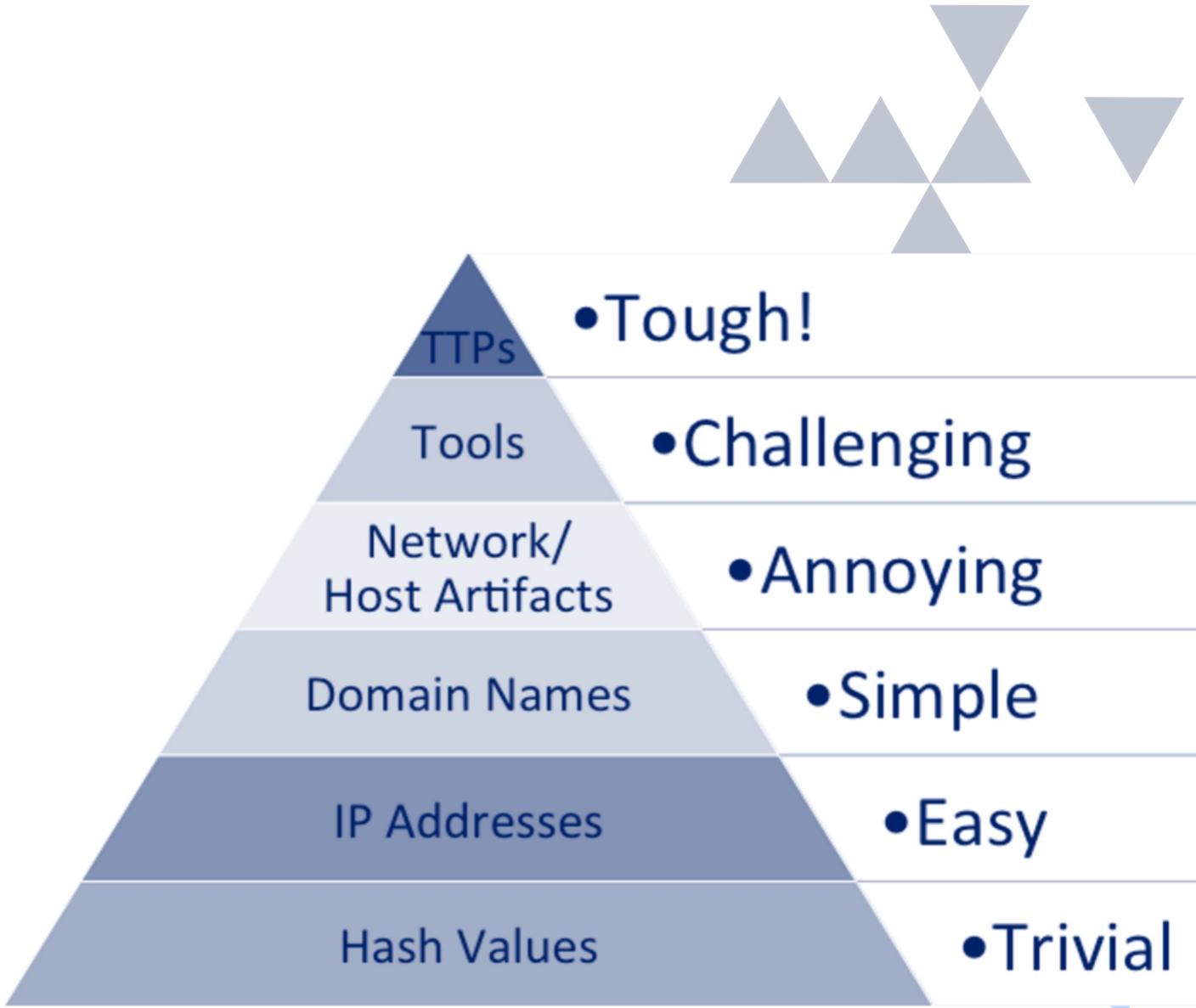
## DIAMOND MODEL

- The Diamond Model of Intrusion Analysis is a model used to categorize information about an intrusion into its four primary components, which facilitates better mental sorting of data using working memory, and better pattern recognition



The Diamond Model of Intrusion Analysis. Source URL <https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf>

<https://bhemida.com>



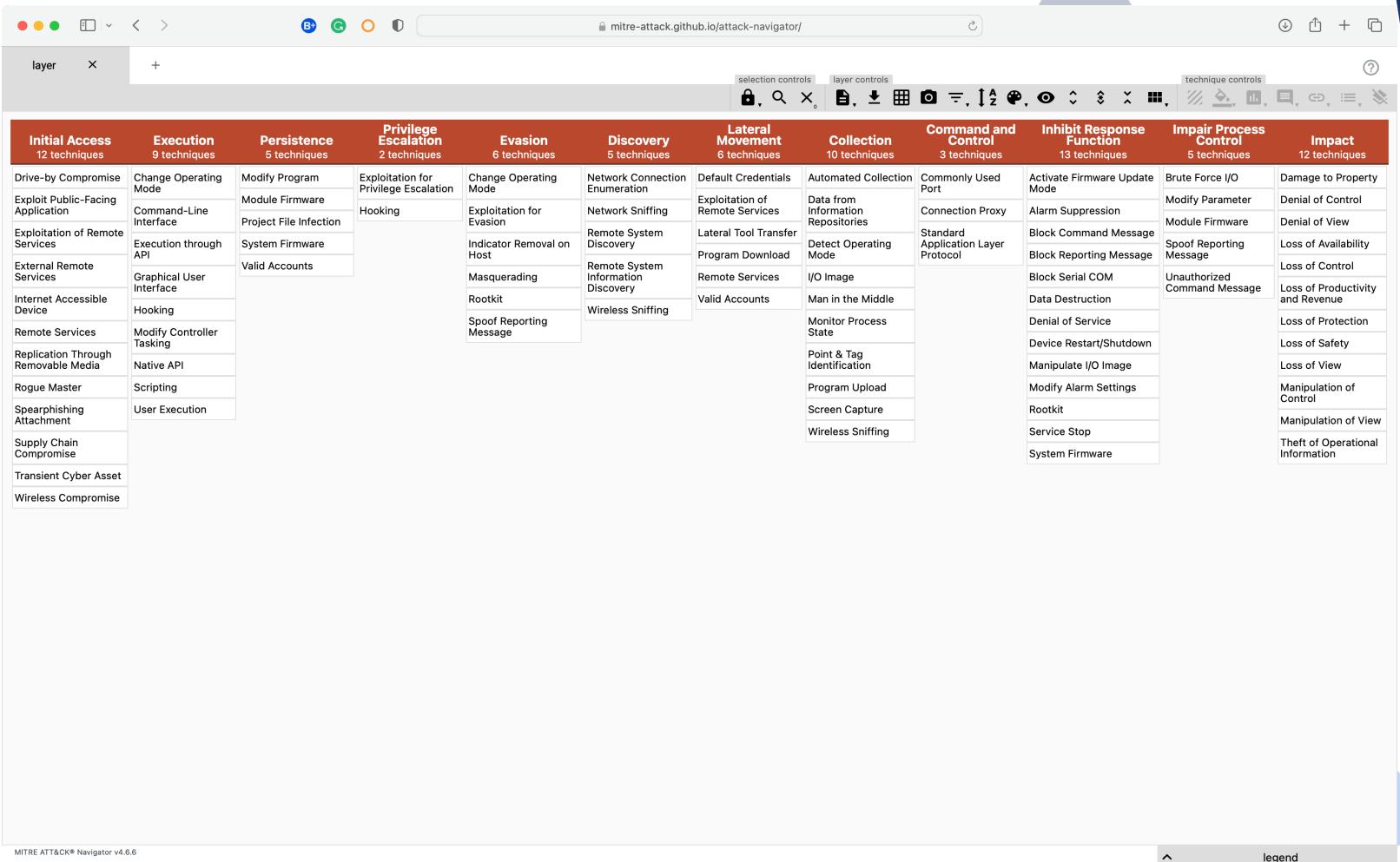
## PYRAMID OF PAIN

- A model that is used to show how much pain it causes the adversary when indicators at different levels are identified and alerted upon.
- At the top of the pyramid are tactics, techniques, and **procedures**, which if identified, require that an attacker change nearly every aspect of how they operate



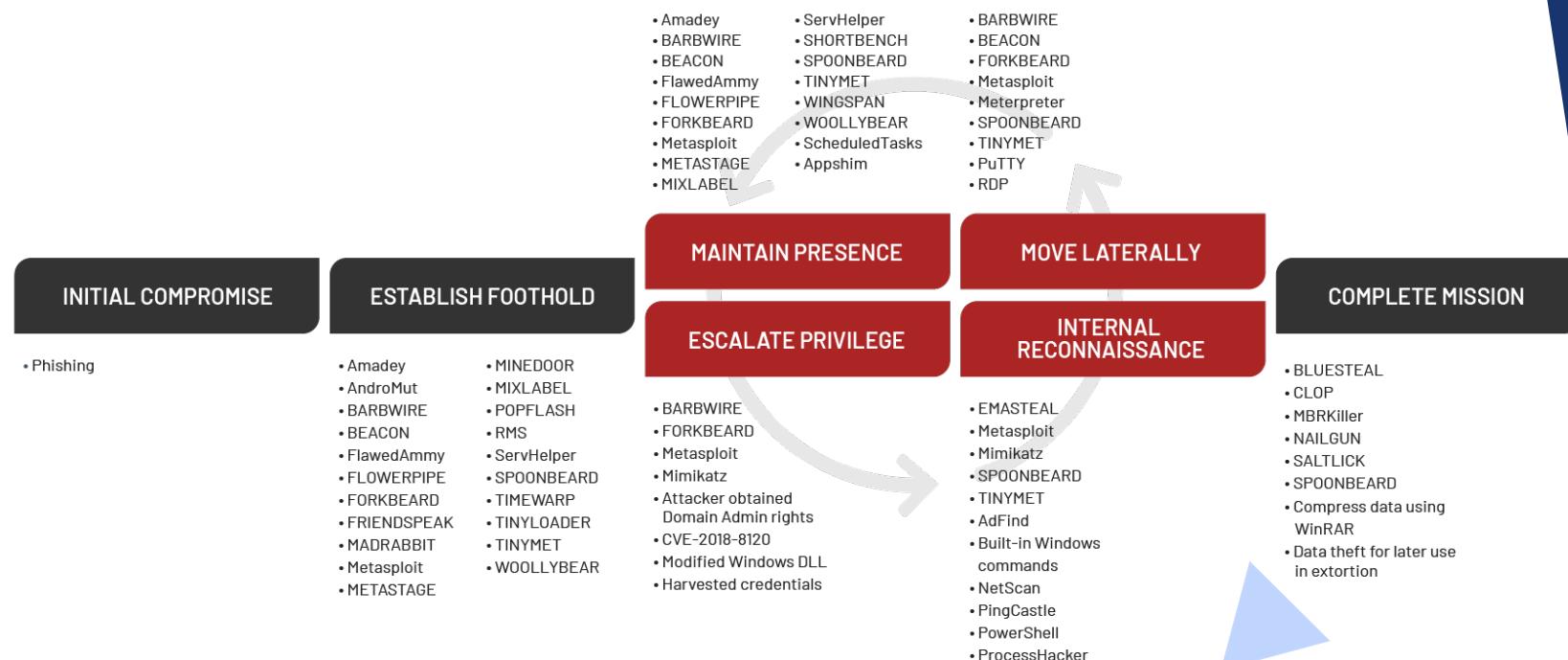
# MITRE ATT&CK TTPS

- Tactics: The adversary's technical goal
- Techniques: How the adversary achieves that goal.
- Sub-techniques: More granular techniques
- Procedures: The specific implementation of the technique or sub-technique



# CYBER KILL CHAIN

- The Cyber Kill Chain is a conceptual framework developed by Lockheed Martin to describe the stages of a cyberattack and to help organizations understand and counteract cyber threats.
- By understanding these stages, security teams can implement measures to detect, interrupt, or mitigate attacks at each stage of the chain





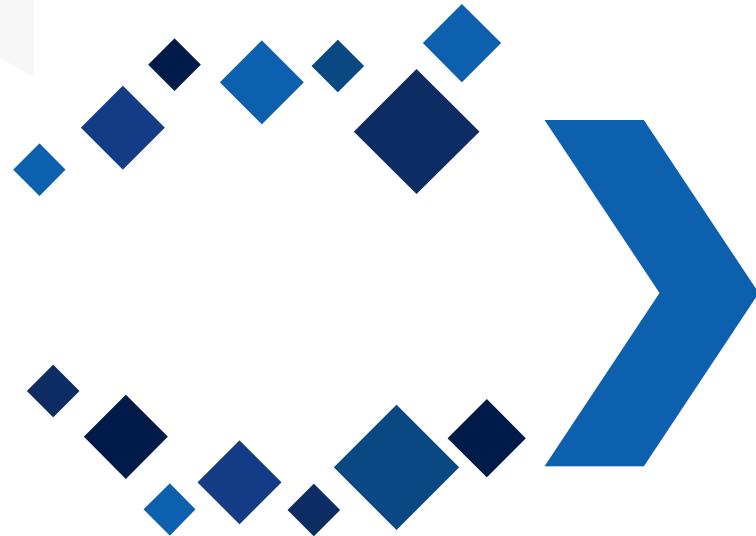
# COUNTERINTELLIGENCE

---

- The practice of identifying, understanding, and countering the efforts of adversaries who seek to infiltrate, disrupt, or manipulate an organization's digital assets and information systems.

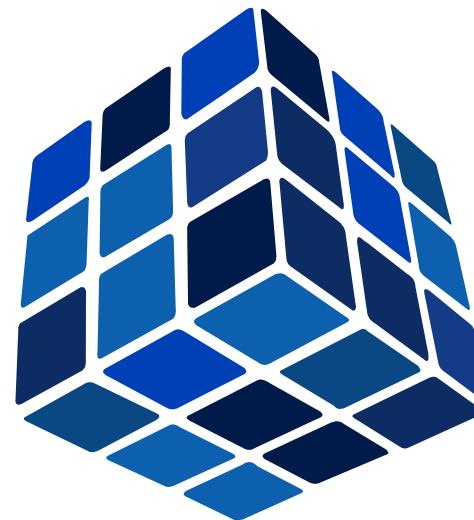


# Fusion Model for Threat Management



## Brainstorming

Understanding frameworks like the Cyber Kill Chain, Diamond Model, and Pyramid of Pain is key to effective cybersecurity. Each offers unique insights into identifying and responding to threats, providing a comprehensive view of the threat landscape.



## Conceptualisation

Using the 7D Course of Action—Discover, Detect, Deny, Disrupt, Degrade, Deceive, and Destroy—helps organizations respond strategically at each attack stage. This alignment makes defences more targeted and effective.

# 7D COURSE OF ACTIONS

- a framework that outlines a set of defensive actions organizations can take in response to cyber threats. Each "D" represents a specific type of action: Detect, Deny, Disrupt, Degrade, Deceive, Divert, and Destroy.
- When mapped onto the Cyber Kill Chain, the 7D COA can be applied at various stages to counteract or mitigate the progression of an attack.

	<b>Discover</b>	<b>Detect</b>	<b>Deny</b>	<b>Disrupt</b>	<b>Degrade</b>	<b>Deceive</b>	<b>Destroy</b>
<b>Reconnaissance</b>	Identify and understand potential threats and targets	Monitoring tools to detect scanning and queries	Restrict access to sensitive information			Deploy honeypots to deceive attackers	
<b>Weaponization</b>	<b>Recognize patterns of weaponization techniques</b>	Identify malicious payloads via analysis		Use IPS to disrupt attack vectors		Feed false data to confuse attackers	
<b>Delivery</b>	<b>Identify delivery methods such as phishing emails</b>	Email and web filters to detect threats	Block phishing and malicious websites				
<b>Exploitation</b>	Recognize signs of exploitation attempts	Monitor for unusual system behavior	Apply patches and updates		Use DEP and ASLR to reduce effectiveness		
<b>Installation</b>	Detect the presence of installation activities	Use antivirus and EDR tools	<b>Application whitelisting and privilege management</b>			Remove or quarantine malware	
<b>Command and Control (C2)</b>	<b>Identify C2 communication attempts</b>	Monitor outbound traffic for C2 communication		Use firewalls to disrupt C2 channels	Degrade communication quality/bandwidth		
<b>Actions on Objectives</b>	Discover indicators of the attacker's end goals	Monitor for malicious activity (e.g., data exfiltration)	Use encryption and DLP tools	Disable key functions, isolate networks		Deploy decoys or fake data	Eradicate malware, restore systems from backups

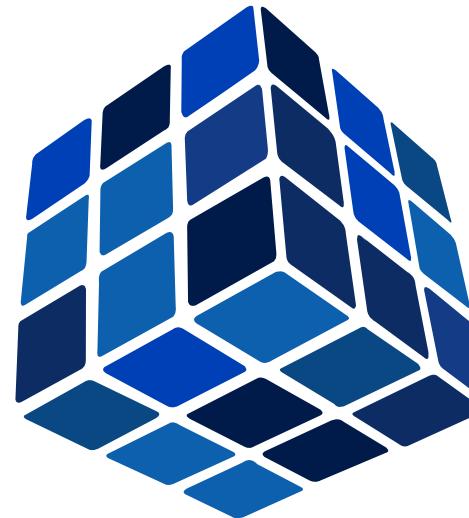


# Fusion Model for Threat Management



## Brainstorming

Understanding frameworks like the Cyber Kill Chain, Diamond Model, and Pyramid of Pain is key to effective cybersecurity. Each offers unique insights into identifying and responding to threats, providing a comprehensive view of the threat landscape.



## Conceptualisation

Using the 7D Course of Action—Discover, Detect, Deny, Disrupt, Degrade, Deceive, and Destroy—helps organizations respond strategically at each attack stage. This alignment makes defences more targeted and effective.



## Threat (PIR)

With these concepts integrated, organizations can set Priority Intelligence Requirements (PIRs) that focus on the most critical threats. This ensures that resources and attention are directed toward the highest risks, enhancing the effectiveness of threat detection and response.

## Feedly PIR Blueprint: Example

### General Threat Landscape

What are the most critical vulnerabilities trending on the Web and Social Media?

What are the new malware families mentioned on the Web in the last 30 days?

What are the most popular cyber attacks reported on the Web?

### Vulnerabilities and Exploits

What are the most critical vulnerabilities affecting our tech stack?

Priority

What proof of exploit, proof of concept, and zero-days could impact our strategic vendors?

MED

What are the most recent TTPs used to exploit the Windows OS or other OS?

MED

Which malware families associated with Lazarus Group are being leveraged against iOS or Android?

HIGH

### Malware

What new and emerging malware families could impact our sector?

HIGH

Which TTPs are being used during ransomware attacks?

MED

What are the latest IoCs associated with common ransomware?

MED

What are the latest IoCs published by trusted sources?

MED

What malware is being used to attack the finance sector?

MED

What are all the threat intelligence reports covering LockBit?

### Adversary Tactics and Activities

What cyberattacks or data breaches could impact our organization?

HIGH

Which threat actors are targeting software supply chains and how?

HIGH

Can we collect YARA and Sigma rules on TTPs used to gain initial access?

What techniques are threat actors using to conceal malicious packages in repositories?

How is Keylogging being leveraged in recent attacks?

### Emerging Threats

Which organizations have been impacted by data breaches in the Biopharma Industry?

MED

What are the latest TTPs and lures being used in spear-phishing attacks in the healthcare industry?

### Geopolitical Risks

What are the current and ongoing geopolitical issues with impact on the UK market?

MED

What role Turkey playing in the Russian invasion of Ukraine?



<https://bhemida.com>



# THREAT (PIR)

- Priority Intelligence Requirements (PIRs) are those intelligence requirements that are key to the mission of the organization and the team.
- PIRs take the guesswork out of the Planning and Direction step of the intelligence cycle as you go straight to the stakeholders to find out precisely what they need.



## Feedly PIR Blueprint: Example

### Requirements

### Priority

#### General Threat Landscape

What are the most critical vulnerabilities trending on the Web and Social Media?

MED

What are the new malware families mentioned on the Web in the last 30 days?

MED

What are the most popular cyber attacks reported on the Web?

MED

#### Vulnerabilities and Exploits

What are the most critical vulnerabilities affecting our tech stack?

HIGH

What proof of exploit, proof of concept, and zero-days could impact our strategic vendors?

HIGH

What are the most recent TTPs used to exploit the Windows OS or other OS?

Which malware families associated with Lazarus Group are being leveraged against iOS or Android?

#### Malware

What new and emerging malware families could impact our sector?

HIGH

Which TTPs are being used during ransomware attacks?

MED

What are the latest IoCs associated with common ransomware?

MED

What are the latest IoCs published by trusted sources?

MED

What malware is being used to attack the finance sector?

What are all the threat intelligence reports covering LockBit?

#### Adversary Tactics and Activities

What cyberattacks or data breaches could impact our organization?

HIGH

Which threat actors are targeting software supply chains and how?

HIGH

Can we collect YARA and Sigma rules on TTPs used to gain initial access?

What techniques are threat actors using to conceal malicious packages in repositories?

How is Keylogging being leveraged in recent attacks?

#### Emerging Threats

Which organizations have been impacted by data breaches in the Biopharma Industry?

MED

What are the latest TTPs and lures being used in spear-phishing attacks in the healthcare industry?

What is the potential for deepfake technology to be used during cyberattacks?

What are the recent trends with botnet attacks that leverage IoT devices?

#### Geopolitical Risks

What are the current and ongoing geopolitical issues with impact on the UK market?

MED

What role Turkey playing in the Russian invasion of Ukraine?

### Sharing actionable insights

	Newsletter	MSFT Teams or Slack	TIP	MISP	SIEM	XSOAR	Power BI	Ticketing System	Other API Access
--	------------	---------------------	-----	------	------	-------	----------	------------------	------------------



### Feedly AI

Examples of the AI Models you can use in Feedly to collect on the example PIRs

Threat Intelligence Dashboard & CVE Insight Cards

Threat Intelligence Dashboard

Threat Intelligence Dashboard

High Vulnerability AND Custom List with your tech stack  
(Proof of Exploit OR Proof of concept OR Zero-day) AND Custom List with your strategic vendors

Tactics and Techniques AND (Microsoft Windows OR Operating Systems)

Malware Families Associated with Lazarus Group AND iOS OR Android

New Malware AND (Your Industry OR Your Industry Companies)  
(Ransomware OR Ransomware as a service) AND Tactics and Techniques  
Wiperware AND Indicators of Compromise

Malware AND (Finance Industry OR Finance Companies)  
LockBit AND Threat Intelligence Reports

(Cyber Attacks OR Data Breach) AND (Your Organization OR Your Organization's Subsidiaries)  
Threat Actors AND (Software supply chain OR Malicious Packages OR Compromise Software Supply Chain (Enterprise T1195.002))

Initial Access (Enterprise TA0001) AND (YARA rules OR Sigma rules)

Malicious Packages AND Tactics and Techniques

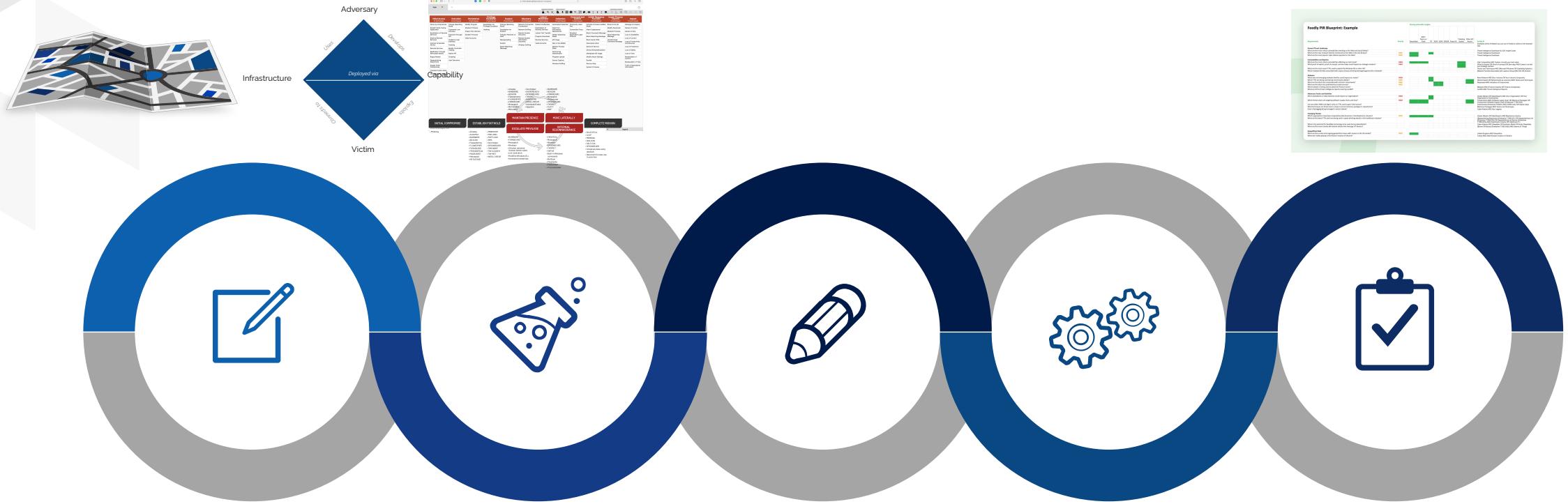
Cyber Attacks AND Key Logging

(Cyber Attacks OR Data Breach) AND Biopharma Industry  
(Spearphishing Attachment (Enterprise T1566.001) OR Spearphishing Link (Enterprise T1566.002) OR Spearphishing via Service (Enterprise T1566.003)) AND (Healthcare Industry OR Healthcare IT)  
Cyber Attacks AND (Deepfake OR Synthetic Media OR Audio Deepfake)  
(Botnet OR Botnet (Enterprise T1583.005)) AND Internet of Things

United Kingdom AND Geopolitics

Turkey AND 2022 Russian invasion of Ukraine

# Threat Informed Defence Approach



## Identify Threats

Identify the potential threats that an organization or system may face

## Analyse Threats

Analyse in order to determine their likelihood and potential impact

## Prioritise threats

Prioritise in order to focus defence efforts on the most significant threats

## Implement Defences

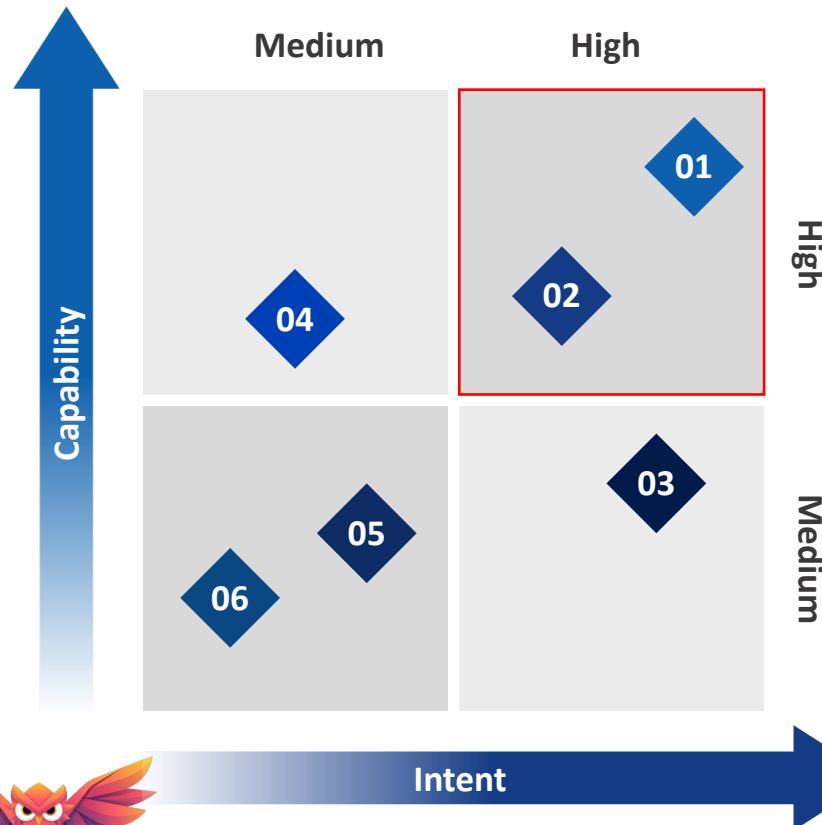
Defences and response plans can be implemented to mitigate the risks associated with those threats

## Monitor and update

Ongoing monitoring and analysis of potential threats, in order to keep pace with the constantly evolving threat landscape



# Prioritise threats

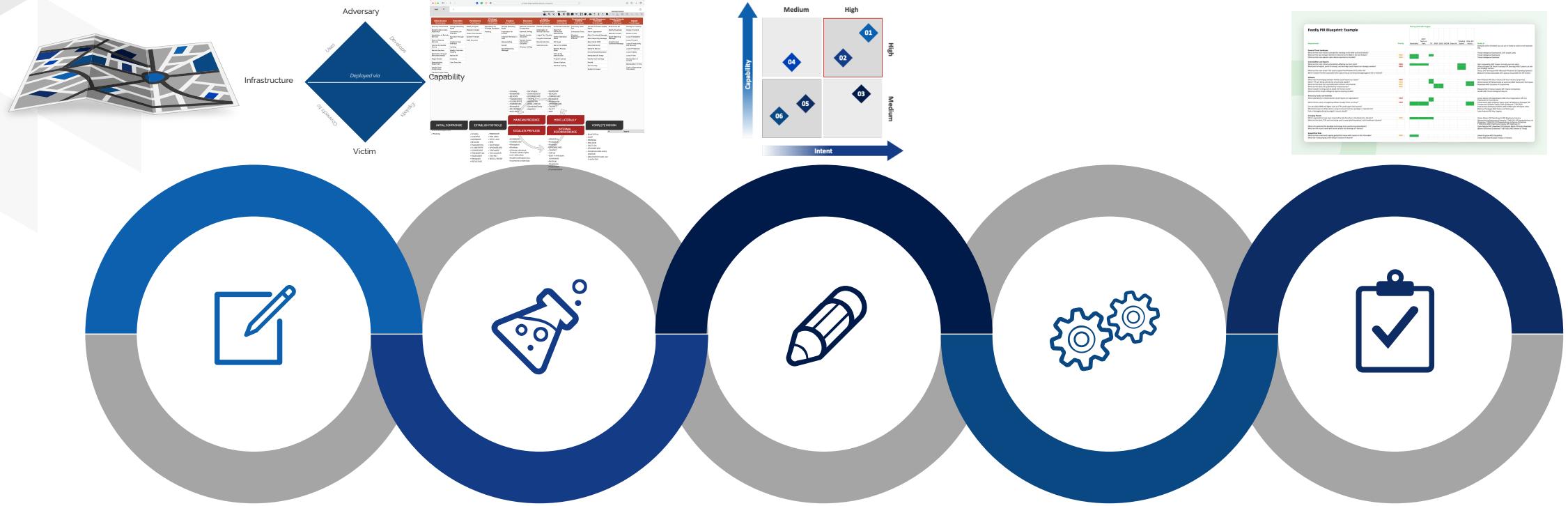


Capability	Intent					
	None	Little	Expressed	Determined	Dedicated	
Extensive	3	4	5	5	5	5
Advanced	3	4	4	5	5	5
Developed	2	3	4	4	5	5
Moderate	1	2	3	3	3	4
Low	1	1	2	3	3	3



Legend	Rating
Very Low	1
Low	2
Moderate	3
High	4
Significant	5

# Threat Informed Defence Approach



## Identify Threats

Identify the potential threats that an organization or system may face

## Analyse Threats

Analyse in order to determine their likelihood and potential impact

## Prioritise threats

Prioritise in order to focus defence efforts on the most significant threats

## Implement Defences

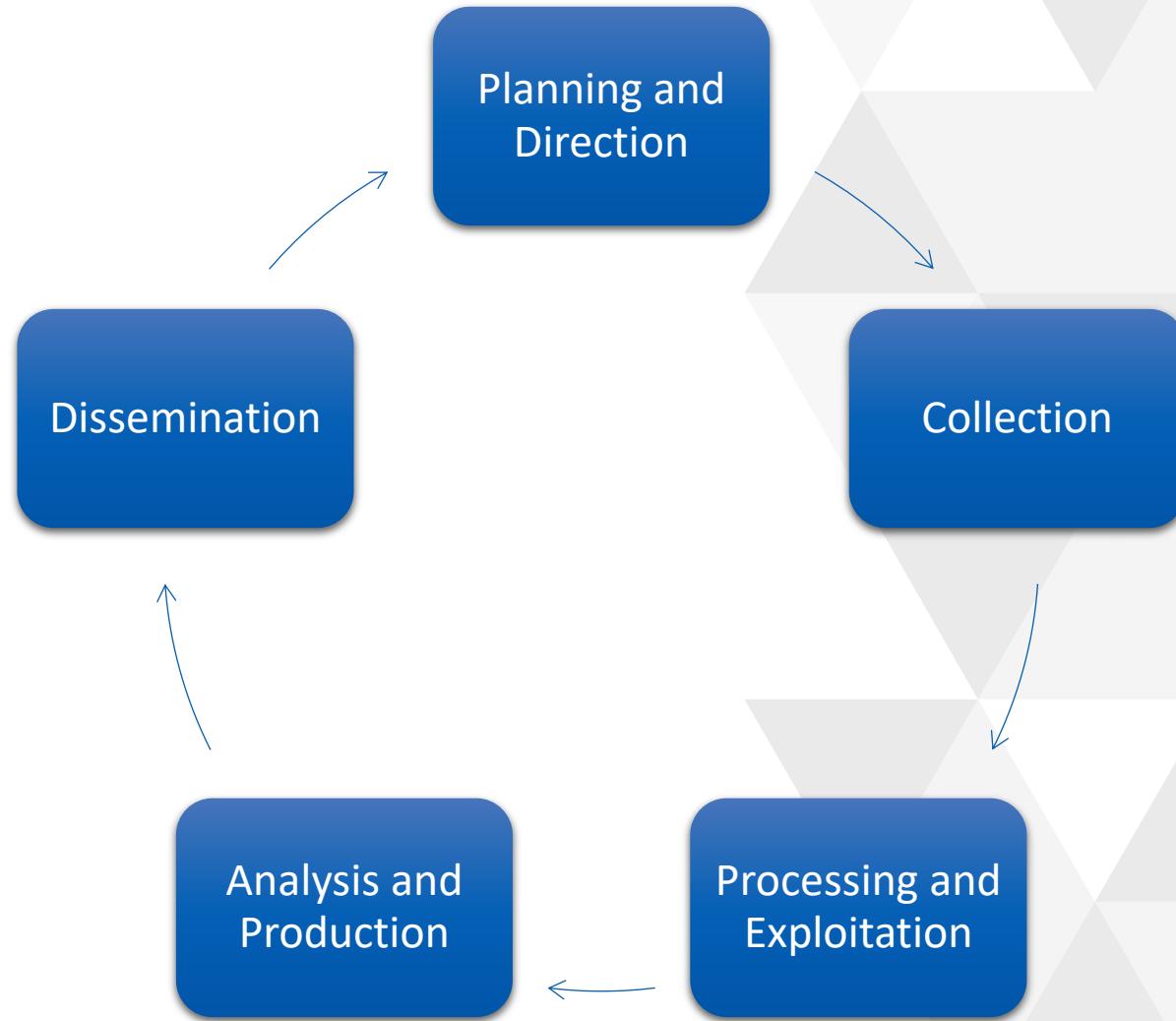
Defences and response plans can be implemented to mitigate the risks associated with those threats

## Monitor and update

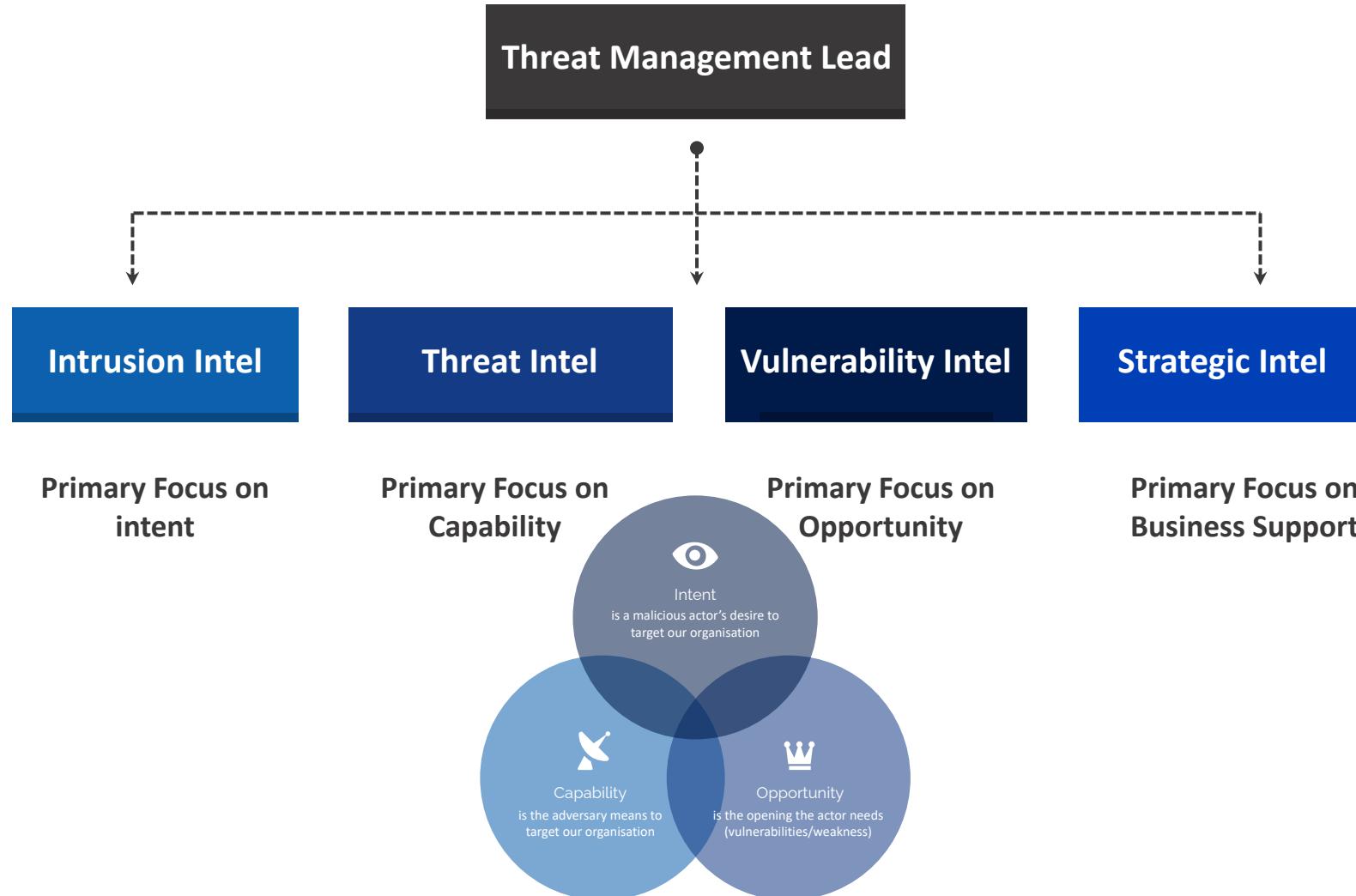
Ongoing monitoring and analysis of potential threats, in order to keep pace with the constantly evolving threat landscape



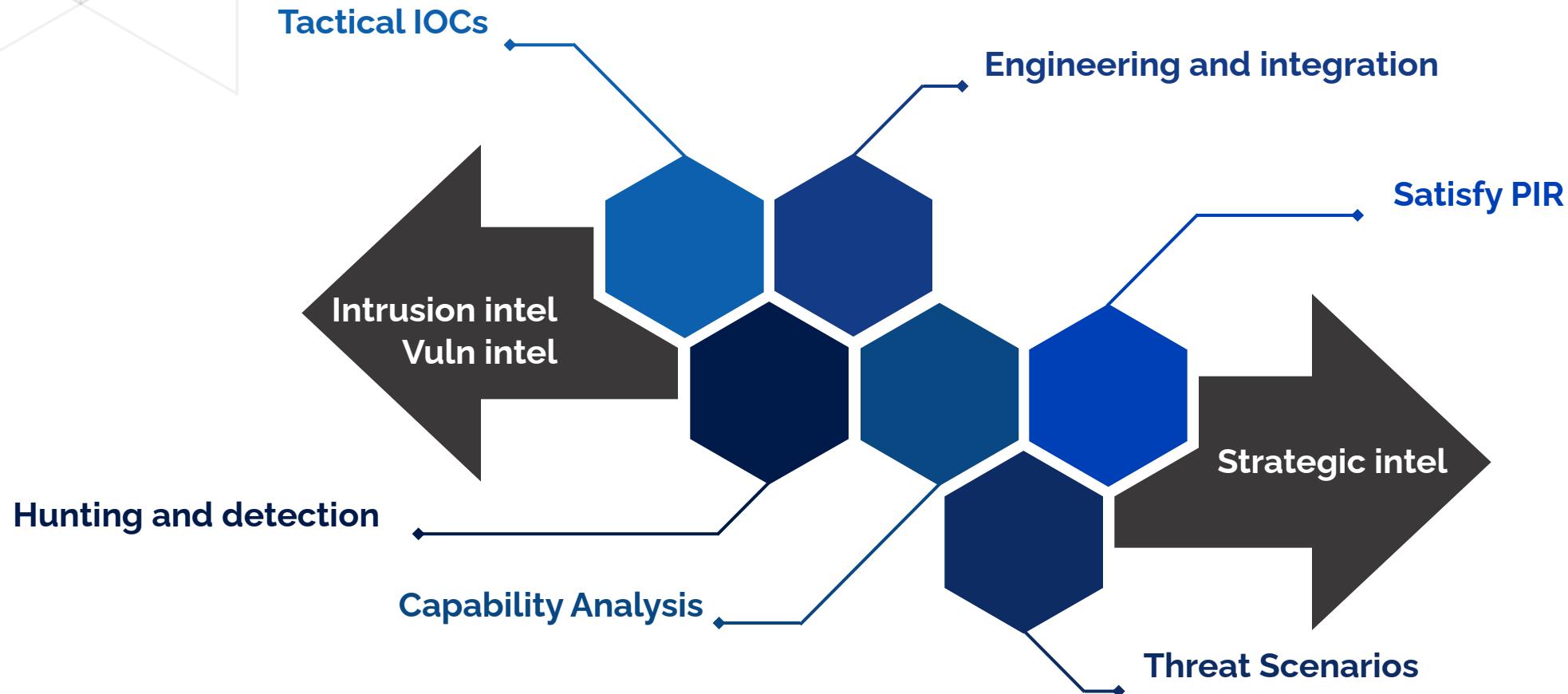
# Threat Management Lifecycle



# Threat Management Operating Model



# Threat Intelligence

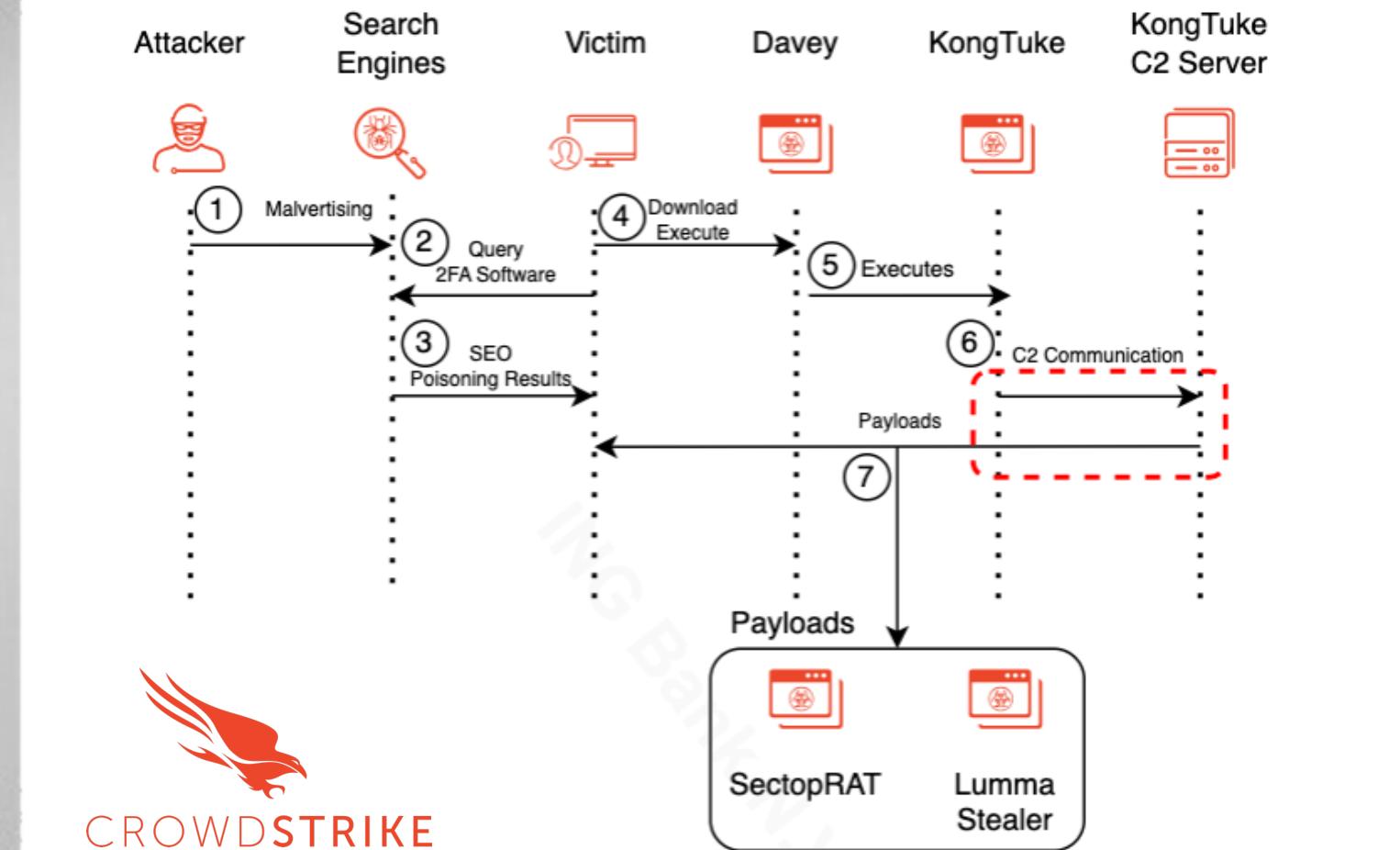


# Capabilities Analysis

## BRIEF

To deliver information stealers, the malware operators have leveraged various distribution methods, including malspam, SEO poisoning, and commodity downloaders.

Malvertising Leads to Davey Crypter Executing KongTuke Backdoor; Operators Deploy DarkGate, SectopRAT, and Lumma Stealer



# Capabilities Analysis

## BRIEF

To deliver information stealers, the malware operators have leveraged various distribution methods, including malspam, SEO poisoning, and commodity downloaders.

Malvertising Leads to Davey Crypter Executing KongTuke Backdoor; Operators Deploy DarkGate, SectopRAT, and Lumma Stealer



Tactic	Technique	Observable
Resource Development	T1587.002 - Develop Capabilities: Code Signing Certificates	The Davey crypter binary was signed using a code-signing certificate, which has not yet been revoked
Execution	T1059.003 - Command and Scripting Interpreter: Windows Command Shell	The KongTuke operators executed several reconnaissance commands via <b>cmd.exe</b>
	T1204.002 - User Execution: Malicious File	The attackers relied on victims executing the Davey payload
Persistence	T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	DarkGate created a registry subkey for persistence in <b>\REGISTRY\USER\[user]\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce</b> under the name <b>fdkehf</b> .
Defence Evasion	T1027 - Obfuscated Files or Information	Davey decrypts KongTuke XOR key
	T1036 - Masquerading	Davey was embedded into a legitimate copy of Sophos File Scanner Service (version 1.11.3)
Command and Control	T1573.001 - Encrypted Channel: Symmetric Cryptography	KongTuke communicates with its C2 server over HTTP and encrypts network traffic using RC4

# Capabilities Analysis

## BRIEF

Top 10 MITRE ATT&CK TTPs  
eCrime and Hacktivist Actors Have  
Used in the Last 24 Months

MITRE ATT&CK ID	Technique Name
T1059	Command and Scripting Interpreter
T1021	Remote Services
T1003	OS Credential Dumping
T1562	Impair Defences
T1566	Phishing
T1027	Obfuscated Files or Information
T1070	Indicator Removal on Host
T1204	User Execution
T1588	Obtain Capabilities
T1071	Application Layer Protocol



CROWDSTRIKE



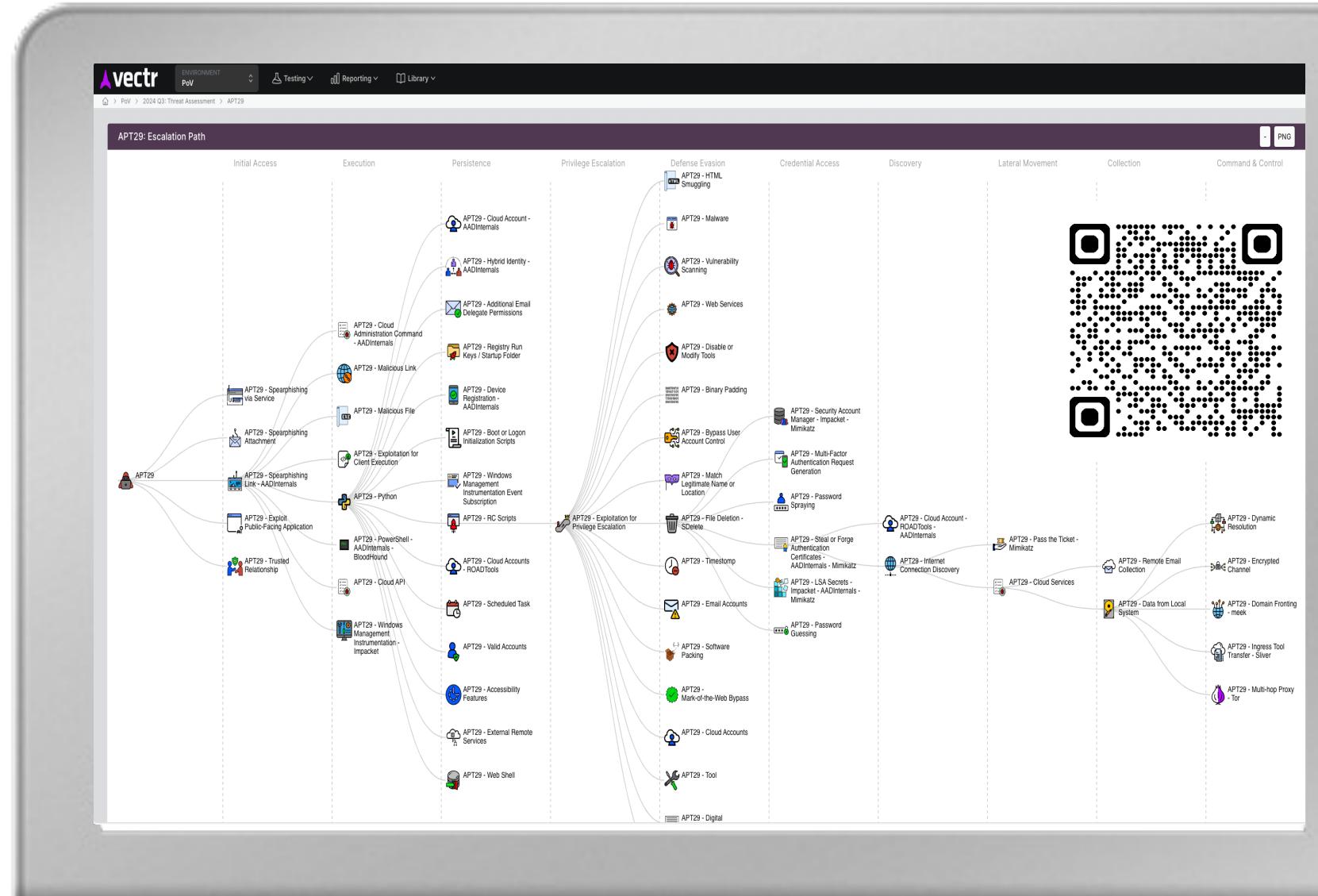
# Threat Scenarios

## BRIEF

VECTR™ helps facilitate the process to test controls, record outcomes and report on your resilience and improvement over time



<https://bhemida.com>



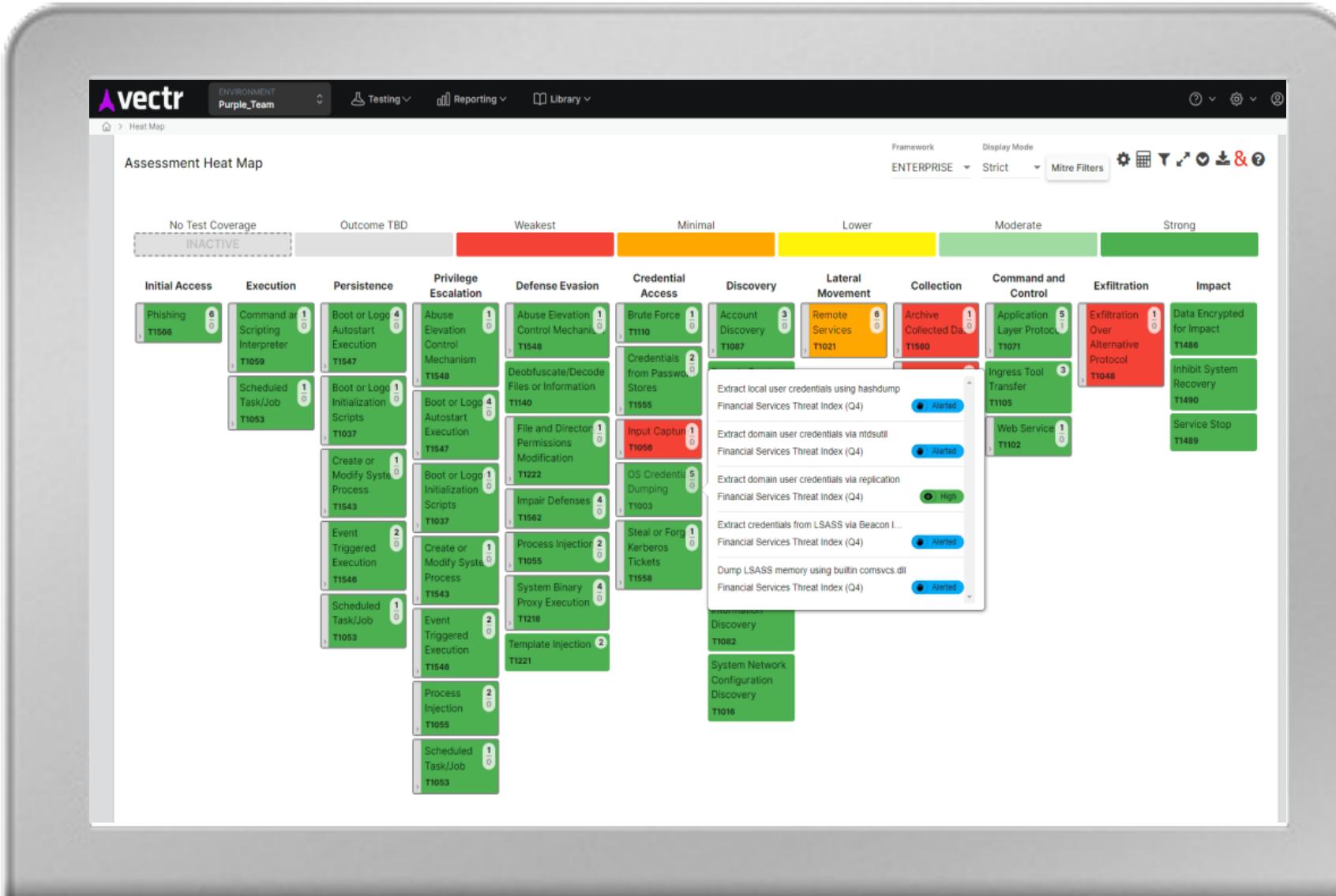
# Threat Scenarios

## BRIEF

VECTR™ helps facilitate the process to test controls, record outcomes and report on your resilience and improvement over time



<https://bhemida.com>



## Intrusion Intelligence

Compromised Credentials

Brand Intelligence

Attack Surface Management

Threat Intel

Vuln Intel

Incident Enrichment

Phishing Analysis

Responsible Disclosure



# Compromised Credentials

## BRIEF

Information stealers enable cyber criminal actors to harvest information and money stored in cryptocurrency wallets.



<https://bhemida.com>

Name	Stealer Malware Logs 2024-07-27	
Identity	[REDACTED]	
Domain	[REDACTED]	
Authorization URL	[REDACTED] index.html	
Description	This credential data was derived from stealer malware logs. These logs are legally obtained through proprietary methods from multiple underground sources. Most data is available within 48 hours after the infection. Refer to exfiltration date for each specific exposure.	
Detection Date	Aug 4, 2024, 16:53	
Exfiltration Date	Jul 27, 2024, 16:46	
Type	Clear	
Hashes	Algorithm: SHA1	Hash: ac317e730954074265384adcede5e27570d5e06c
	Algorithm: SHA256	Hash: 2b5f4c3719392d518dc385829d5e74c566887f322185b89c3f35361a0230ec82
	Algorithm: NTLM	Hash: 6668bd536f7b807d3a0cf45e8caa6e13
	Algorithm: MD5	Hash: 53a36c189602b5fabf6fb837de9301b
Properties	Letter, Number, Symbol, UpperCase, LowerCase, AtLeast12Characters	
Password	[REDACTED]	
Compromised Host	Operating System: Windows 11 Pro (10.0.22631) x64 OS User Name: [REDACTED] Exposed Credentials: 44 <a href="#">Show Incident Report</a> File Path Location: C:\Windows\winhlp32.exe Time Zone: UTC+02:00 Name of the Machine: DESKTOP-[REDACTED] User Account Control Setting: N/A Antivirus: Windows Defender	
Malware Family	LummaC2 <span style="background-color: yellow;">MALWARE</span>	
Technology	Category: VPN <span style="background-color: red;">TECHNOLOGY</span> Tag: Citrix NetScaler Access Gateway	
IP Address	[REDACTED]	

•|• Recorded Future®

# Vulnerability Intelligence

**Vulnerability Assessment**

**Threat Validation**

**Intrusion Intel**

**Threat Intel**

**Vulnerability Intelligence**

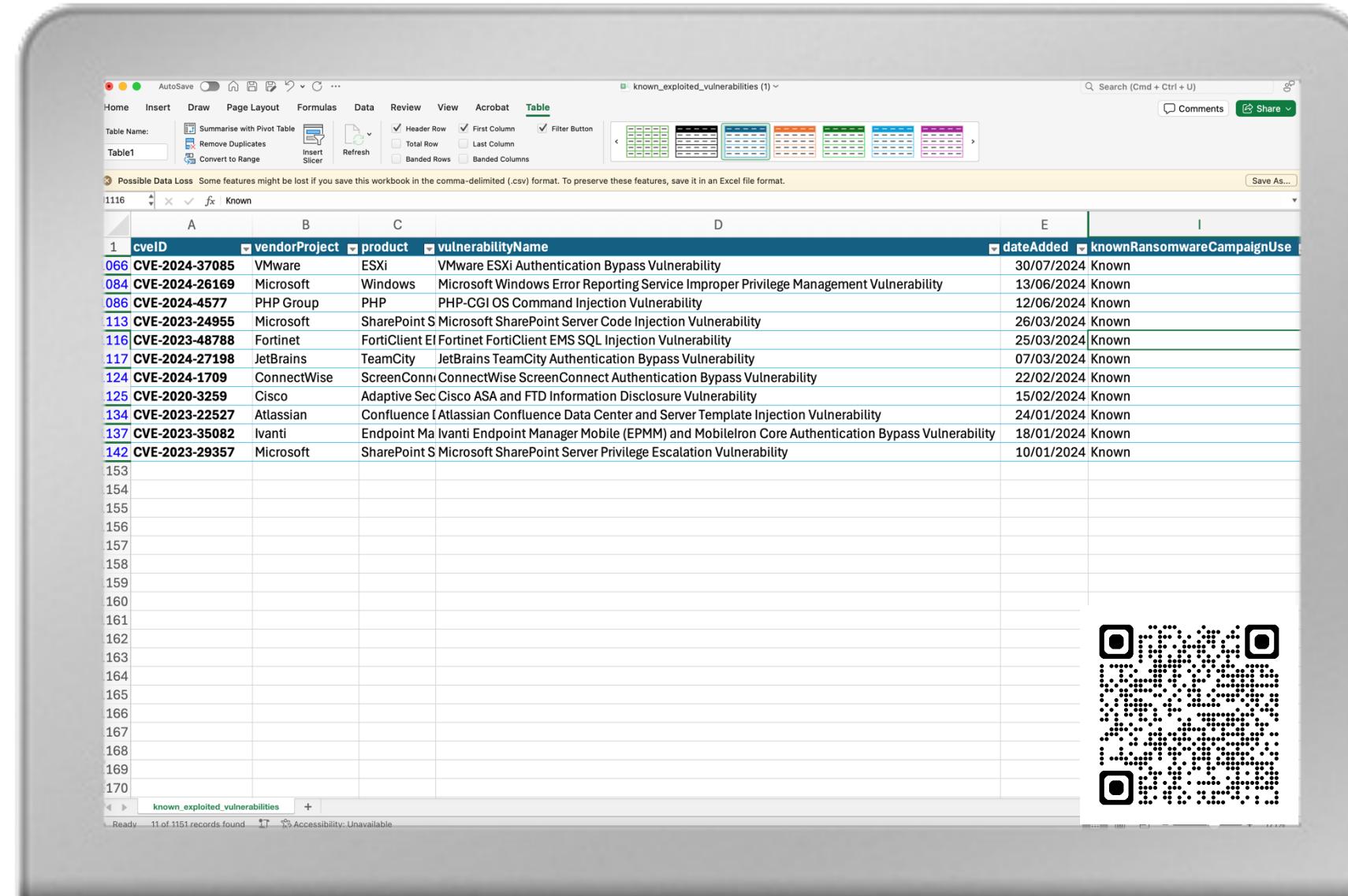


# Vulnerability Intel

## BRIEF

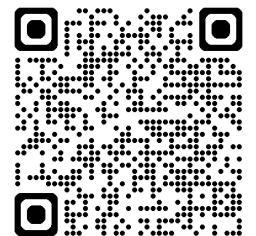
**Known Exploited Vulnerabilities Catalog**, CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild.

Organizations should use the KEV catalog as an input to their vulnerability management prioritization framework.



The screenshot shows a Microsoft Excel spreadsheet titled "known\_exploited\_vulnerabilities". The table has the following columns:

	cveID	vendorProject	product	vulnerabilityName	dateAdded	knownRansomwareCampaignUse
1	<a href="#">CVE-2024-37085</a>	VMware	ESXi	VMware ESXi Authentication Bypass Vulnerability	30/07/2024	Known
2	<a href="#">CVE-2024-26169</a>	Microsoft	Windows	Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability	13/06/2024	Known
3	<a href="#">CVE-2024-4577</a>	PHP Group	PHP	PHP-CGI OS Command Injection Vulnerability	12/06/2024	Known
4	<a href="#">CVE-2023-24955</a>	Microsoft	SharePoint S	Microsoft SharePoint Server Code Injection Vulnerability	26/03/2024	Known
5	<a href="#">CVE-2023-48788</a>	Fortinet	FortiClient EMS	FortiClient EMS SQL Injection Vulnerability	25/03/2024	Known
6	<a href="#">CVE-2024-27198</a>	JetBrains	TeamCity	JetBrains TeamCity Authentication Bypass Vulnerability	07/03/2024	Known
7	<a href="#">CVE-2024-1709</a>	ConnectWise	ScreenConnect	ConnectWise ScreenConnect Authentication Bypass Vulnerability	22/02/2024	Known
8	<a href="#">CVE-2020-3259</a>	Cisco	Adaptive Sec	Cisco ASA and FTD Information Disclosure Vulnerability	15/02/2024	Known
9	<a href="#">CVE-2023-22527</a>	Atlassian	Confluence	Atlassian Confluence Data Center and Server Template Injection Vulnerability	24/01/2024	Known
10	<a href="#">CVE-2023-35082</a>	Ivanti	Endpoint Manager	Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass Vulnerability	18/01/2024	Known
11	<a href="#">CVE-2023-29357</a>	Microsoft	SharePoint S	Microsoft SharePoint Server Privilege Escalation Vulnerability	10/01/2024	Known
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						

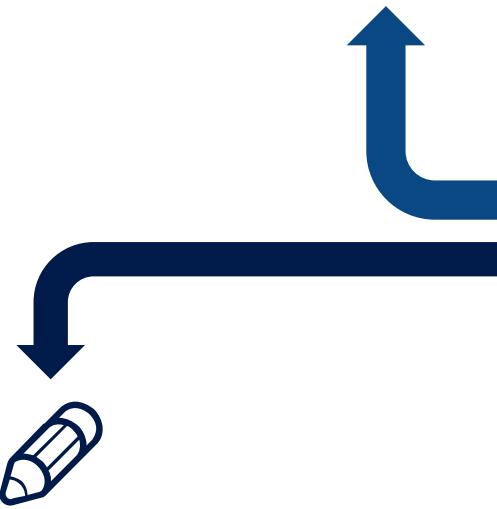


# Integration at All Levels



## IT and Infrastructure

Prioritise fixing and patching vulnerabilities and fix policies and configurations that introduce a risk



Prioritise onboarding capabilities to provide required prevention against applicable threats



## Threat Management



## Risk Management

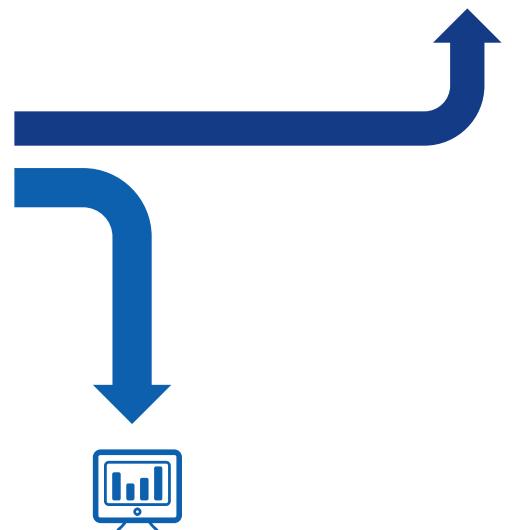
Keep them informed with applicable threats and Influence prioritising implementing security control to mitigate risks.



## Offensive Operations

Influence offensive operations with applicable and most relevant TTPs.

DORA TLPT



## Detection and Response

Feed with relevant IOCs and threats applicable to organization

## Q&A

