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.

https://bhemida.com

THREAT-INFORMED DEFENCE

INTEGRATING THREAT INTELLIGENCE AT ALL LEVELS

You will get insights into

Nice meeting you!

GSE #301

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

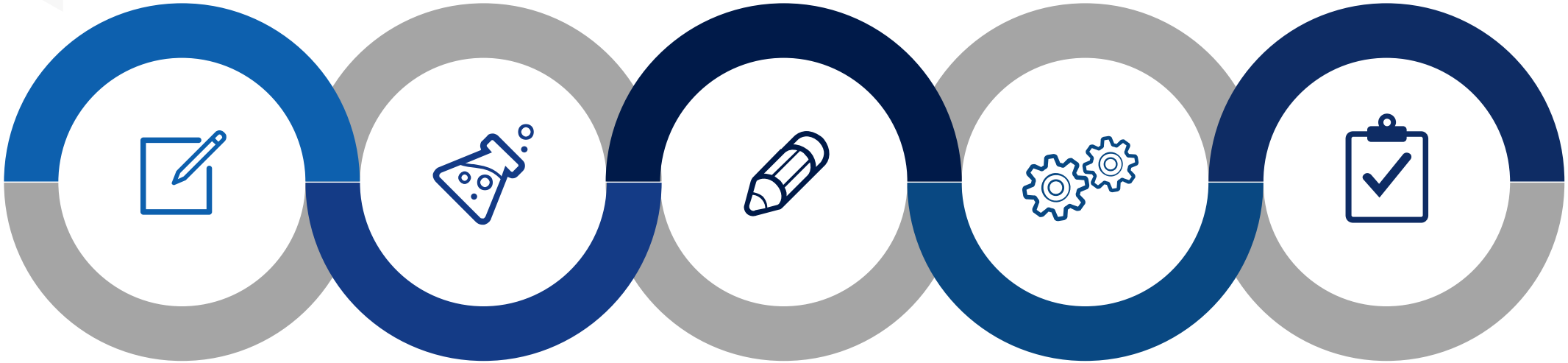
Threat Management
Security Architecture
Incident Response and Threat Hunting Operations
Digital Forensics and Intrusion Detection
Red Teaming, Covert Operations and Cybersecurity Crisis Simulation
IT/OT Cyber Strategy

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

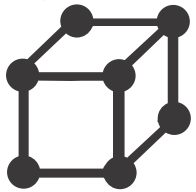
Defences and response plans can be implemented to mitigate the risks associated with those threats

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

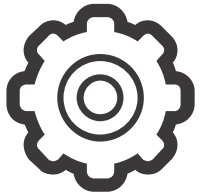


Limited financial resources and personnel resources. Therefore, there is a must to prioritize security investments.

Full Chain

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.

Operations



Prioritize efforts to mitigate actual threats and implement defensive controls with the best return.

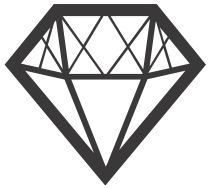
Risk Management

Implement controls and countermeasures to reduce the risks.

Eliminate the risk by discontinuing the activity or process that introduces the risk.

Acknowledge and accept the potential consequences without implementing additional controls.

Scale up



Scale up cyber strategy to the next level to enhance cyber defence and risk management against modern and emerging threats.

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.

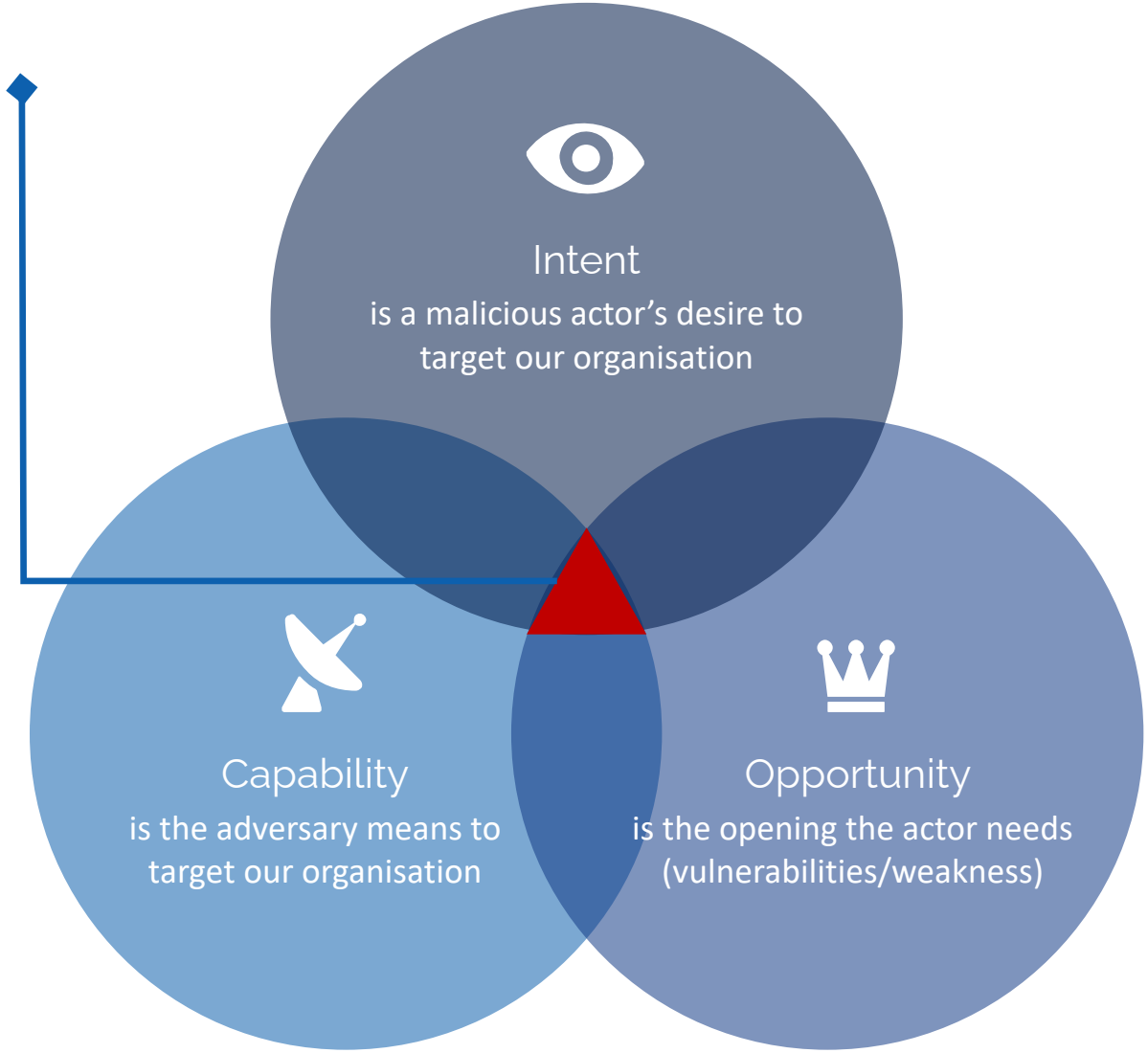
C2M2 Objective

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.

How: Capability

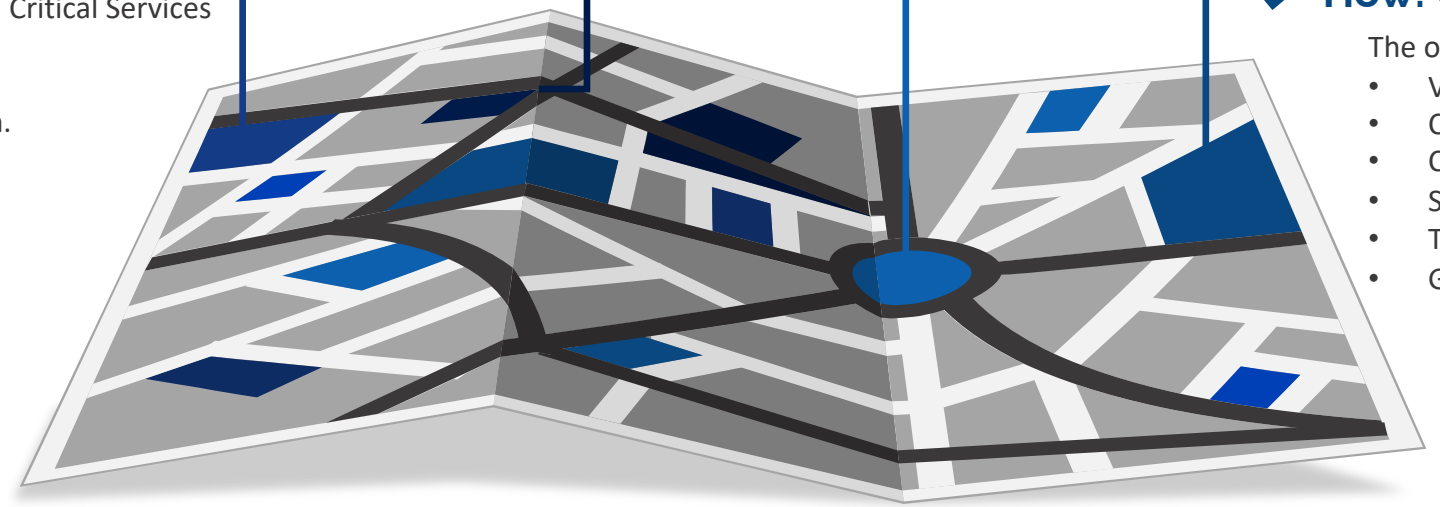
Tools, tactics, techniques and procedures

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

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: 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

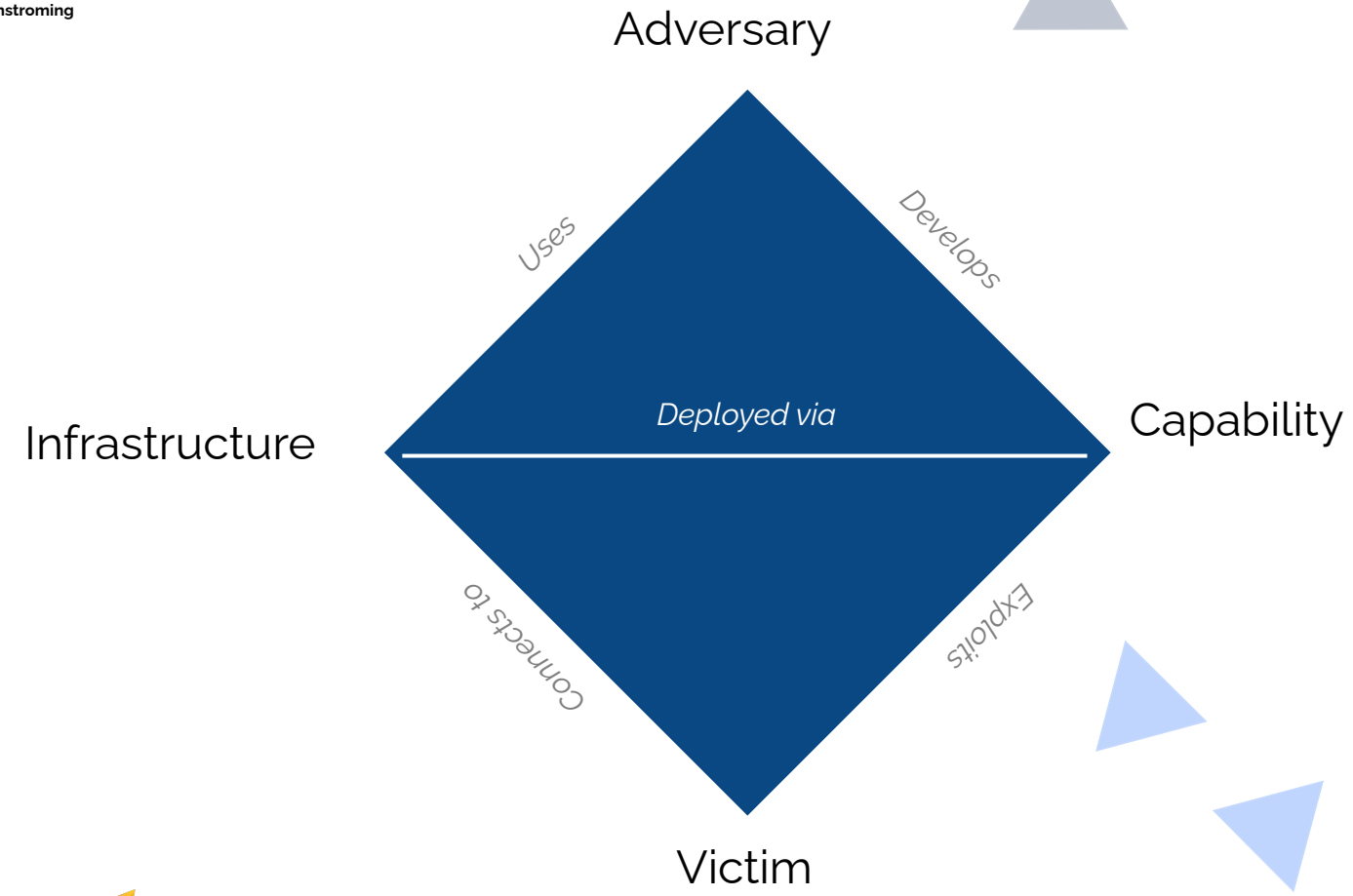
Brainstorming

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.

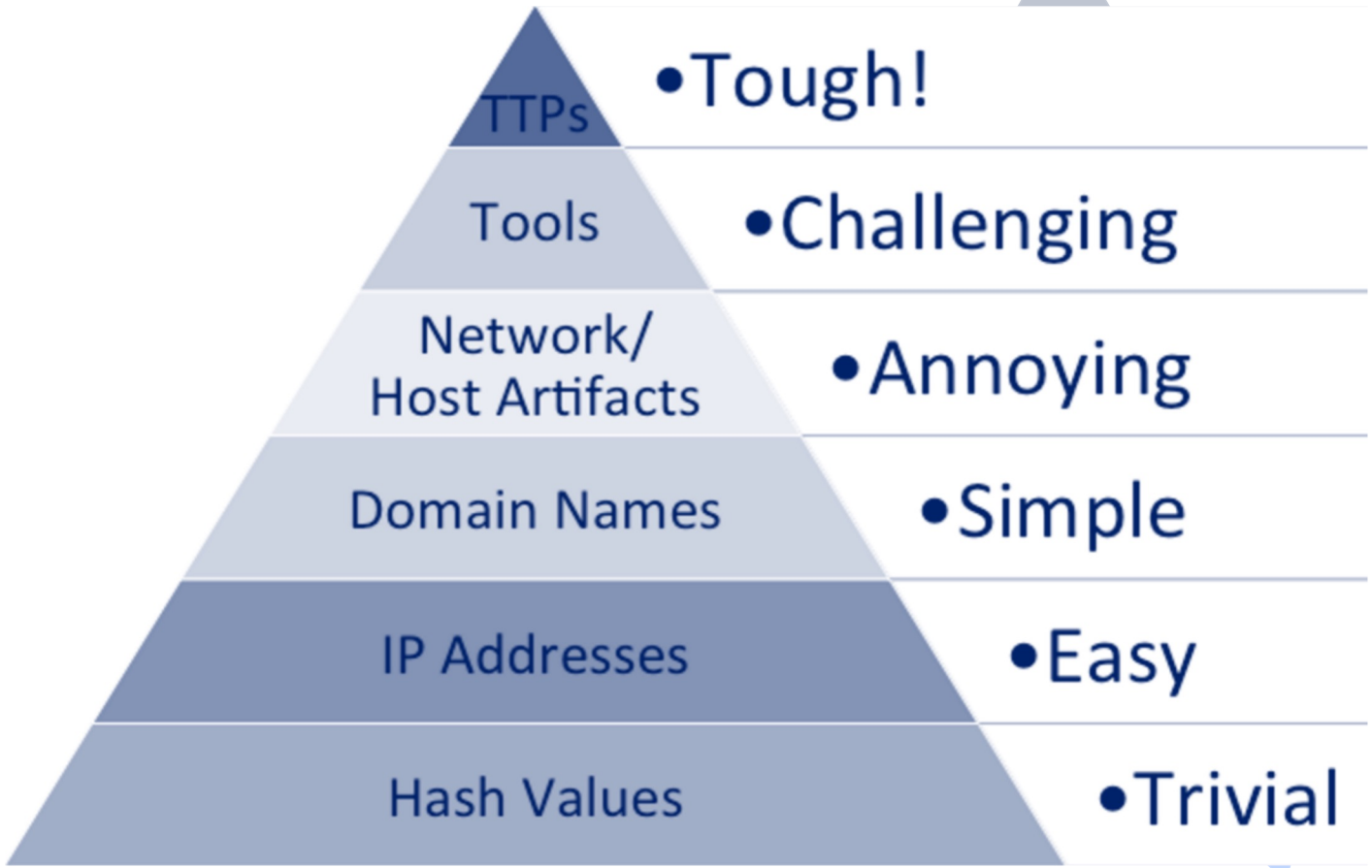
Brainstroming

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

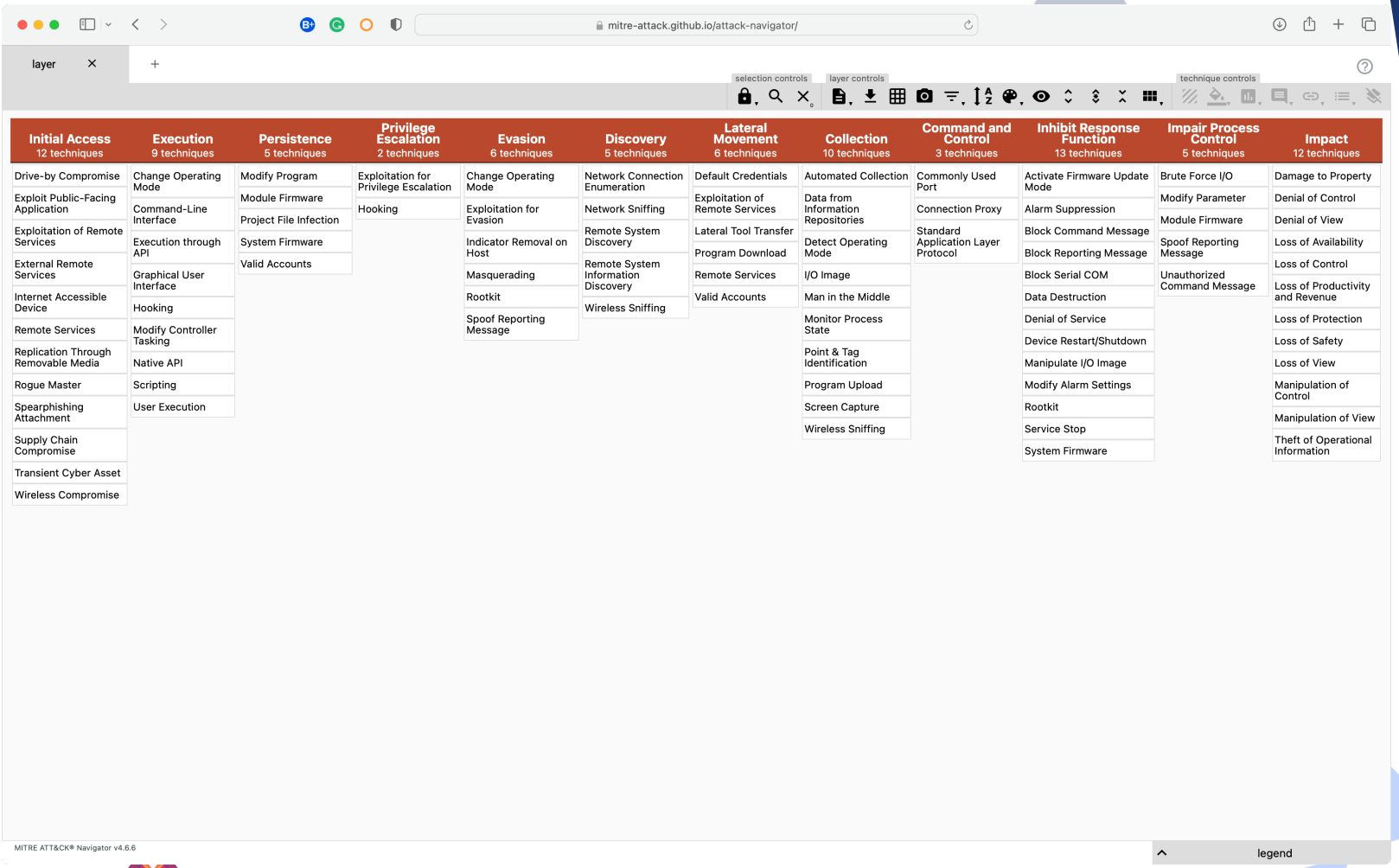


PYRAMID OF PAIN

- 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

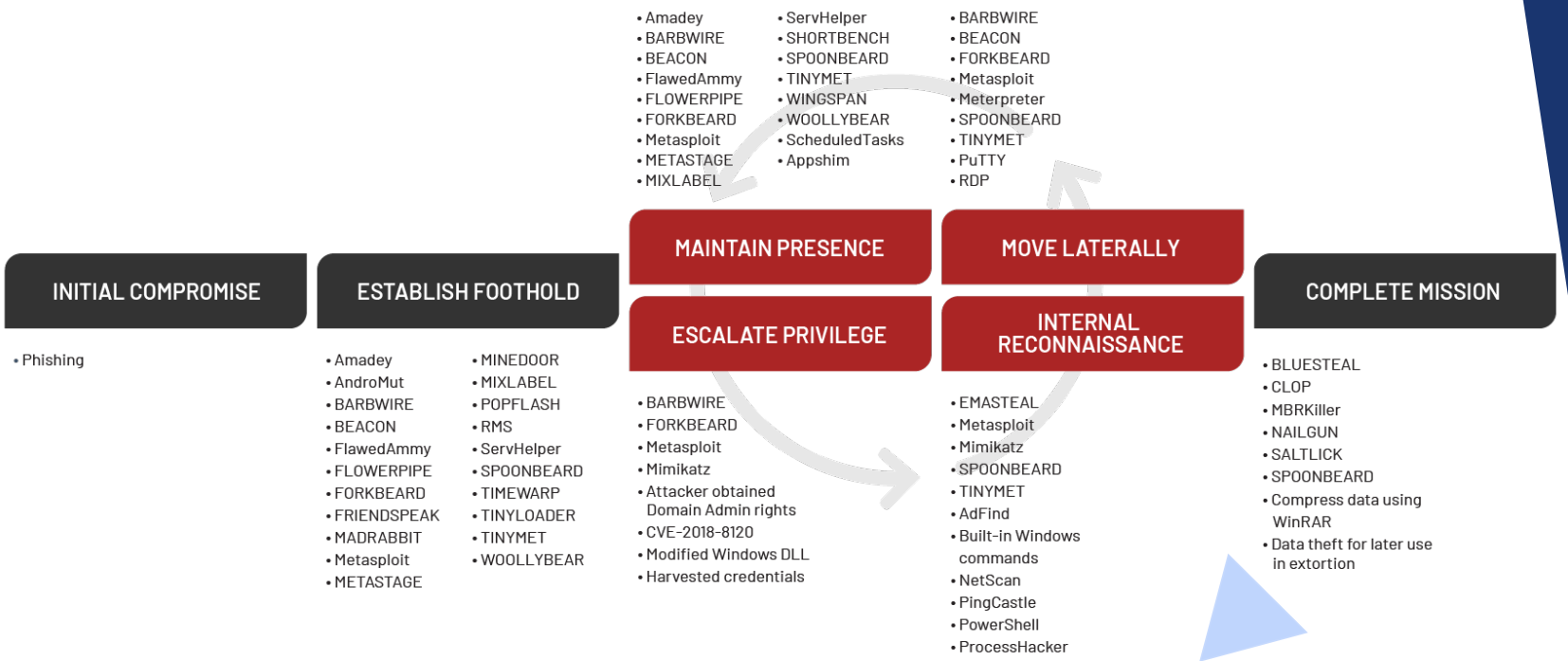
- Tactics: The adversary's technical goal
- Techniques: How the adversary achieves that goal.
- Sub-techniques: More granular techniques
- Procedures: The specific implementation of the technique or sub-technique



https://bhemida.com

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



https://bhemida.com

COUNTERINTELLIGENCE

- The 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.

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Identify and understand potential threats and targets	Monitoring tools to detect scanning and queries	Restrict access to sensitive information			Deploy honeypots to deceive attackers	
Weaponization	**Recognize patterns of weaponization techniques**	Identify malicious payloads via analysis		Use IPS to disrupt attack vectors		Feed false data to confuse attackers	
Delivery	**Identify delivery methods such as phishing emails**	Email and web filters to detect threats	Block phishing and malicious websites				
Exploitation	Recognize signs of exploitation attempts	Monitor for unusual system behavior	Apply patches and updates		Use DEP and ASLR to reduce effectiveness		
Installation	Detect the presence of installation activities	Use antivirus and EDR tools	**Application whitelisting and privilege management**				Remove or quarantine malware
Command and Control (C2)	**Identify C2 communication attempts**	Monitor outbound traffic for C2 communication		Use firewalls to disrupt C2 channels	Degrade communication quality/bandwidth		
Actions on Objectives	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

https://bhemida.com

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	Priority
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?	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?	
Geopolitical Risks	
What are the current and ongoing geopolitical issues with impact on the UK market?	MED
What role Turkey playing is the Russian invasion of Ukraine?	

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.

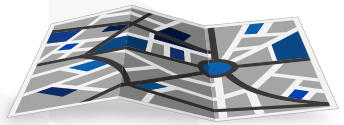
https://bhemida.com

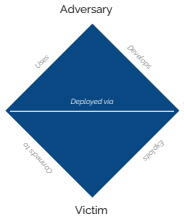
feedly

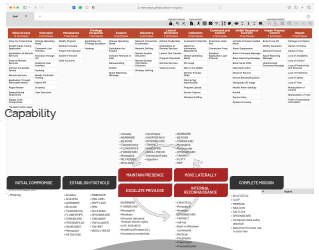
Feedly PIR Blueprint: Example

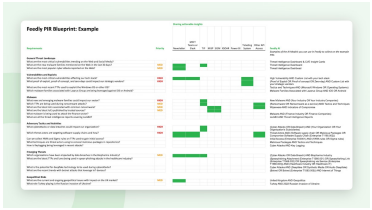
Requirements	Priority	Sharing actionable insights: Newsletter	MSFT Teams or Slack	TIP	MISP	SIEM	XSOAR	Power BI	Ticketing System	Other API Access	Feedly AI *Examples of the AI Models you can use in Feedly to collect on the example PIRs*
General Threat Landscape											
What are the most critical vulnerabilities trending on the Web and Social Media?											Threat Intelligence Dashboard & CVE Insight Cards
What are the new malware families mentioned on the Web in the last 30 days?	MED	■		■							Threat Intelligence Dashboard
What are the most popular cyber attacks reported on the Web?	MED	■									Threat Intelligence Dashboad
Vulnerabilities and Exploits											
What are the most critical vulnerabilities affecting our tech stack?	HIGH	■	■						■		High Vulnerability AND Custom List with your tech stack
What proof of exploit, proof of concept, and zero-days could impact our strategic vendors?	HIGH								■		(Proof of Exploit OR Proof of concept OR Zero-day) AND Custom List with your strategic vendors
What are the most recent TTPs used to exploit the Windows OS or other OS?											Tactics and Techniques AND (Microsoft Windows OR Operating Systems)
Which malware families associated with Lazarus Group are being leveraged against iOS or Android?											Malware Families Associated with Lazarus Group AND iOS OR Android
Malware											
What new and emerging malware families could impact our sector?	HIGH			■							New Malware AND (Your Industry OR Your Industry Companies)
Which TTPs are being used during ransomware attacks?	MED			■						■	(Ransomware OR Ransomware as a service) AND Tactics and Techniques
What are the latest IoCs associated with common ransomware?	MED				■	■				■	Wiperware AND Indicators of Compromise
What are the latest IoCs published by trusted sources?	MED				■	■					
What malware is being used to attack the finance sector?											Malware AND (Finance Industry OR Finance Companies)
What are all the threat intelligence reports covering LockBit?											LockBit AND Threat Intelligence Reports
Adversary Tactics and Activities											
What cyberattacks or data breaches could impact our organization?	HIGH			■							(Cyber Attacks OR Data Breach) AND (Your Organization OR Your Organization's Subsidiaries)
Which threat actors are targeting software supply chains and how?	HIGH	■	■							■	Threat Actors AND (Software supply chain OR Malicious Packages OR Compromise Software Supply Chain (Enterprise T1195.002))
Can we collect YARA and Sigma rules on TTPs used to gain initial access?											Initial Access (Enterprise TA0001) AND (YARA rules OR Sigma rules)
What techniques are threat actors using to conceal malicious packages in repositories?											Malicious Packages AND Tactics and Techniques
How is Keylogging being leveraged in recent attacks?											Cyber Attacks AND Key Logging
Emerging Threats											
Which organizations have been impacted by data breaches in the Biopharma Industry?	MED	■	■	■							(Cyber Attacks OR Data Breach) AND Biopharma Industry
What are the latest TTPs and lures being used in spear-phishing attacks in the healthcare 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)
What is the potential for deepfake technology to be used during cyberattacks?											Cyber Attacks AND (Deepfake OR Synthetic Media OR Audio Deepfake)
What are the recent trends with botnet attacks that leverage IoT devices?											(Botnet OR Botnet (Enterprise T1583.005)) AND Internet of Things
Geopolitical Risks											
What are the current and ongoing geopolitical issues with impact on the UK market?	MED	■									United Kingdom AND Geopolitics
What role Turkey playing is the Russian invasion of Ukraine?											Turkey AND 2022 Russian invasion of Ukraine

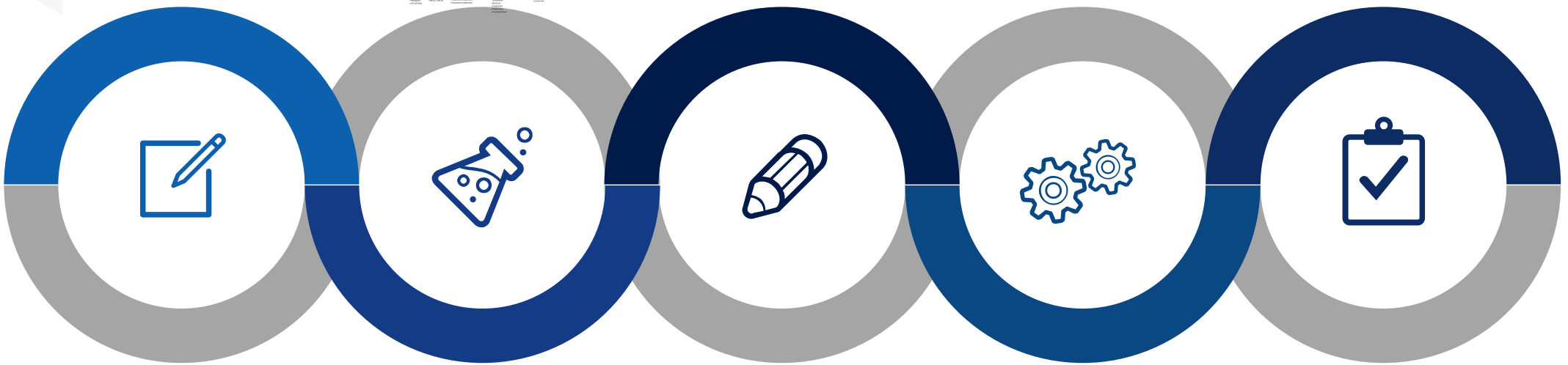
Threat Informed Defence Approach











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

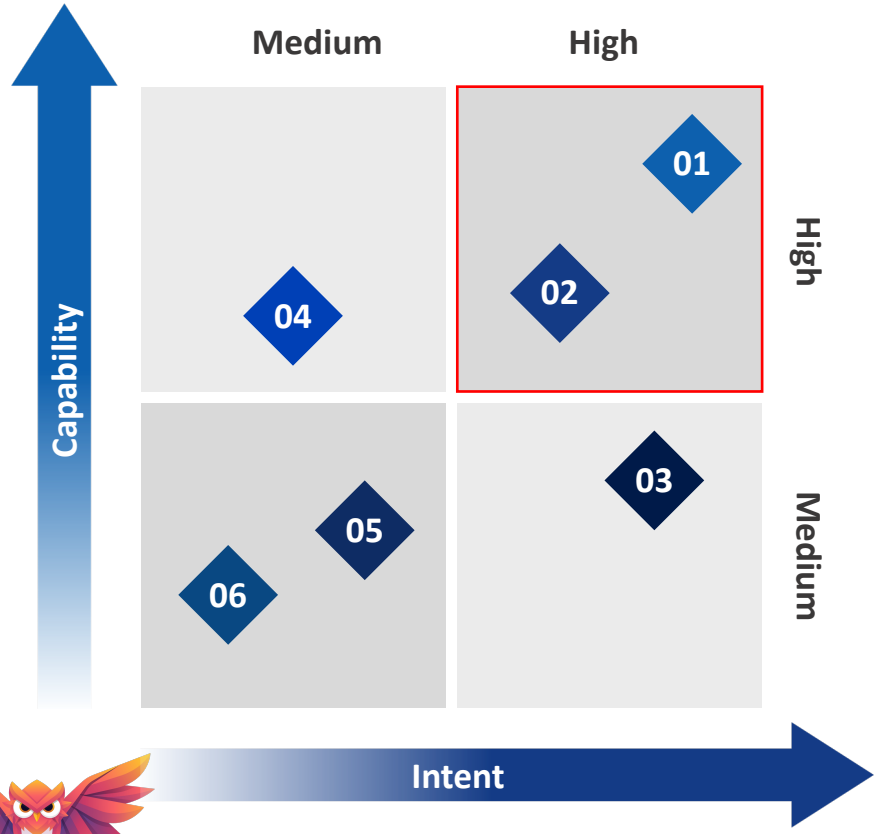
Implement Defences

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

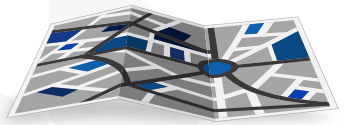
Prioritise threats

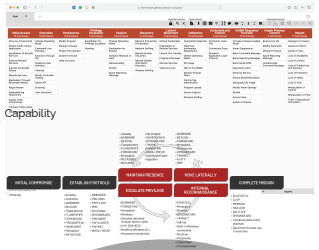


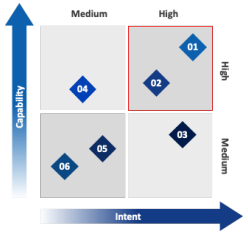
Capability	Intent				
	None	Little	Expresed	Determined	Dedicated
Extensive	3	4	5	5	5
Advanced	3	4	4	5	5
Developed	2	3	4	4	5
Moderate	1	2	3	3	4
Low	1	1	2	3	3

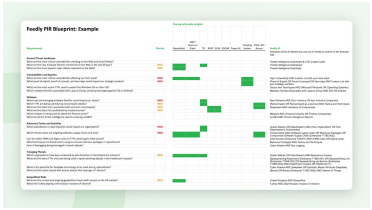
Legend	Rating
Very Low	1
Low	2
Moderate	3
High	4
Significant	5

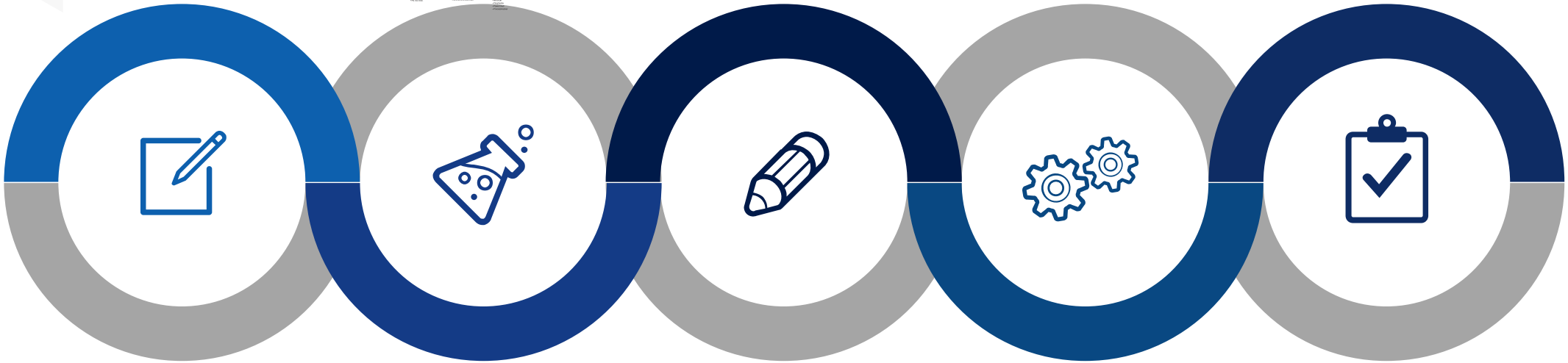
Threat Informed Defence Approach











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

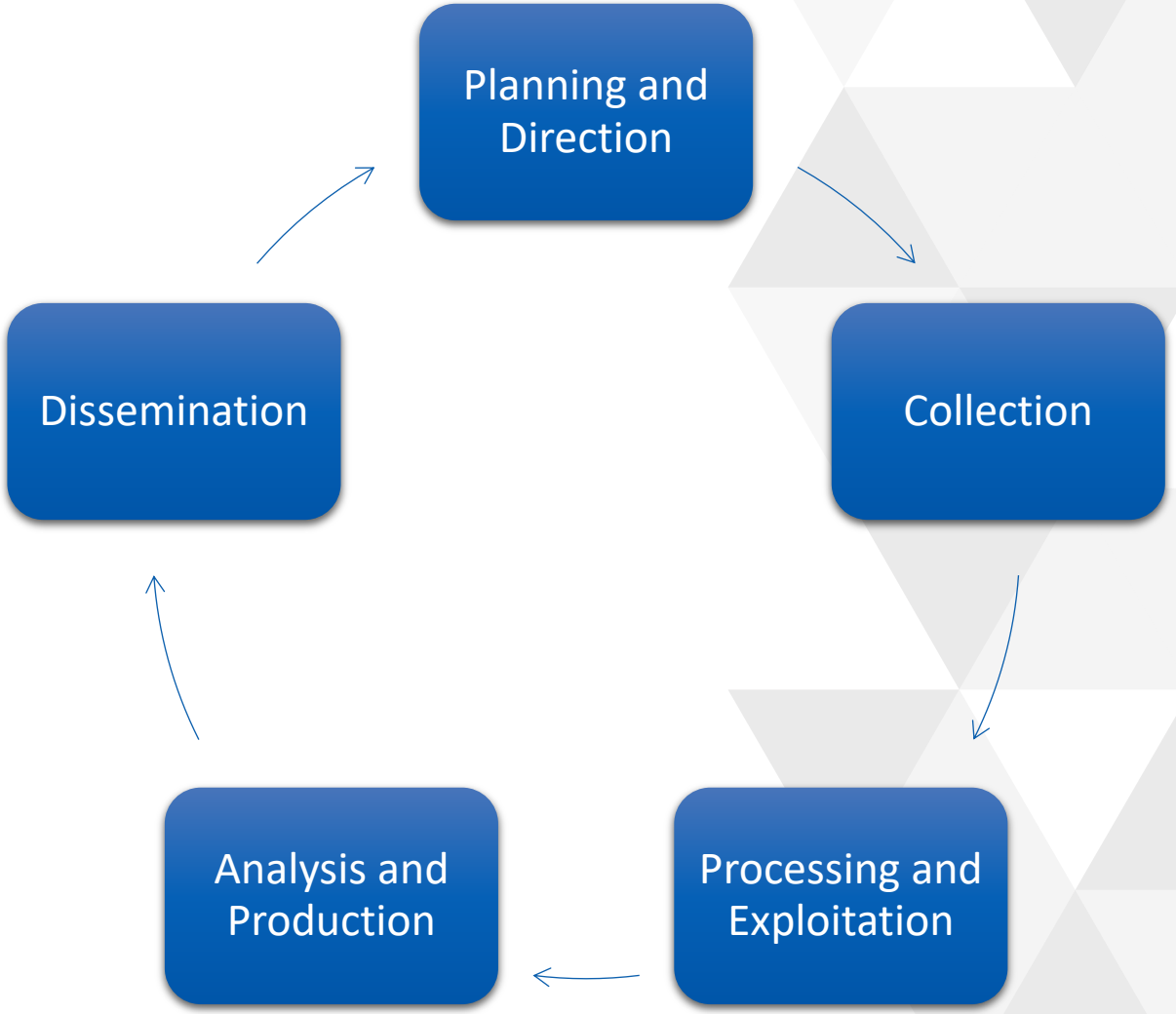
Implement Defences

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

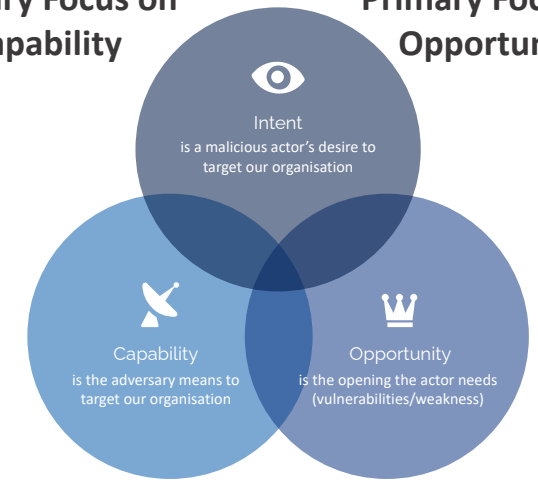
Threat Management Lifecycle



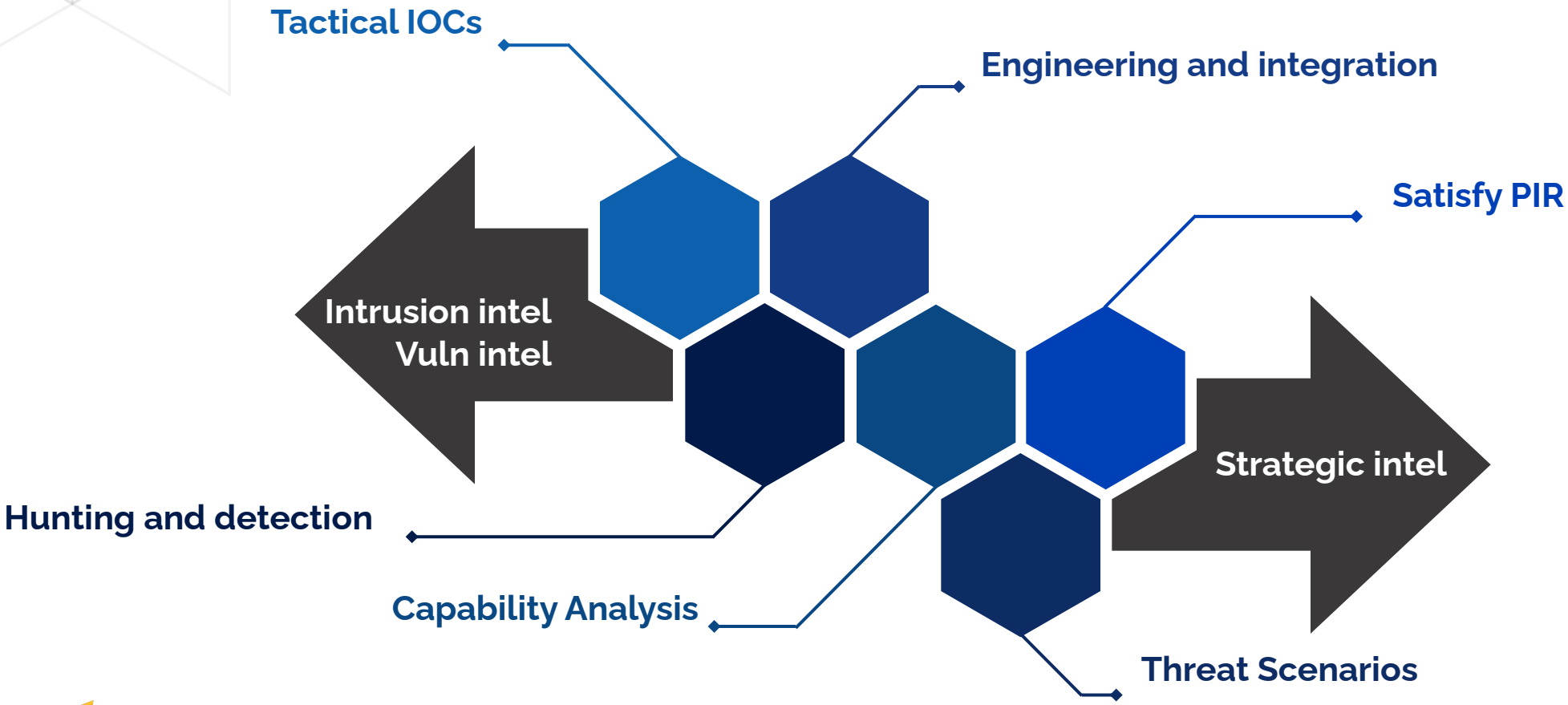
Threat Management Operating Model

Threat Management Lead

Intrusion Intel	Threat Intel	Vulnerability Intel	Strategic Intel
Primary Focus on intent	Primary Focus on Capability	Primary Focus on Opportunity	Primary Focus on Business Support



Threat Intelligence

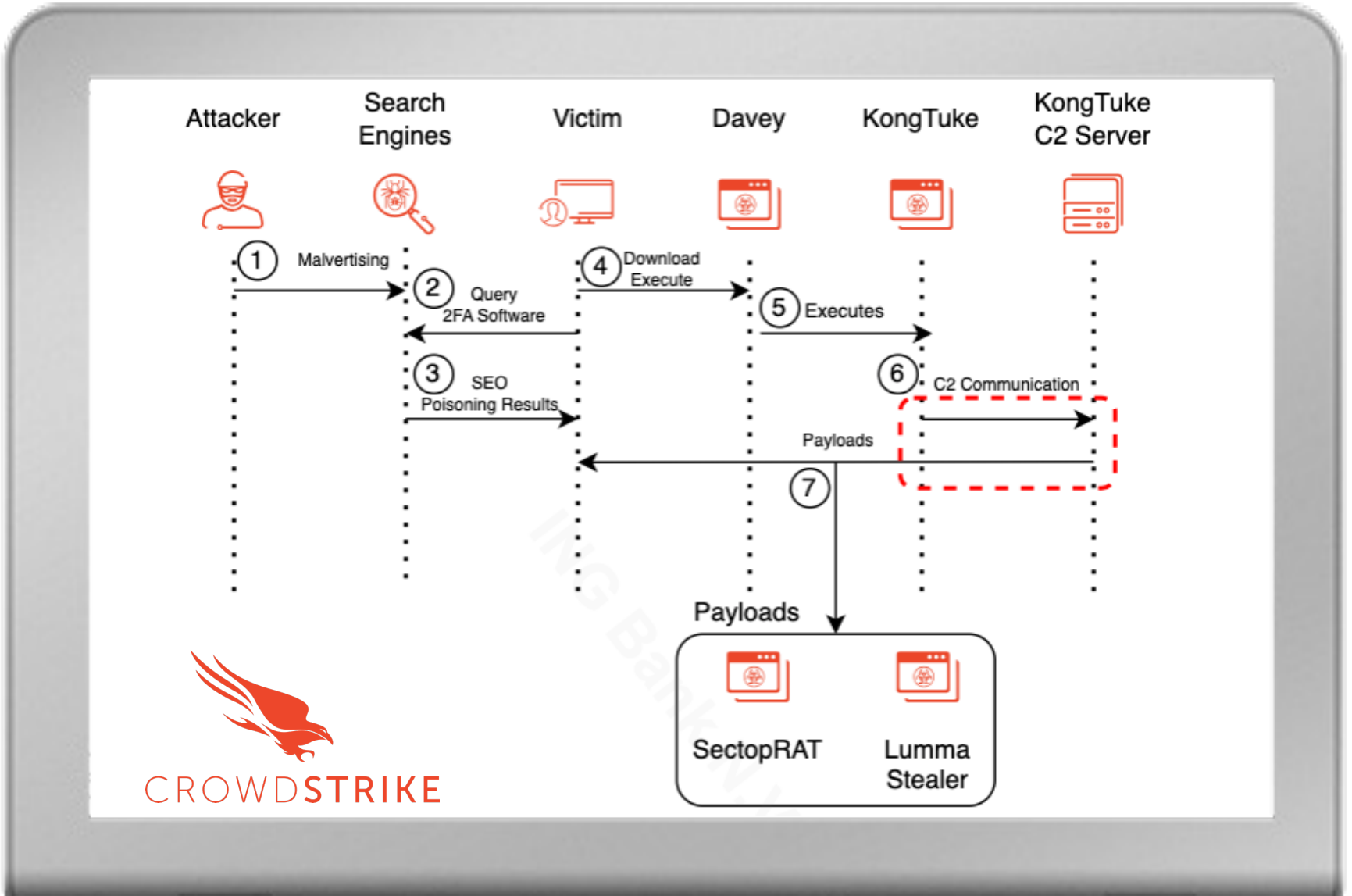


Capabilities Analysis

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 **cmd.exe**
	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 **\REGISTRY\USER\[user]\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce** under the name **fddkehf**.
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

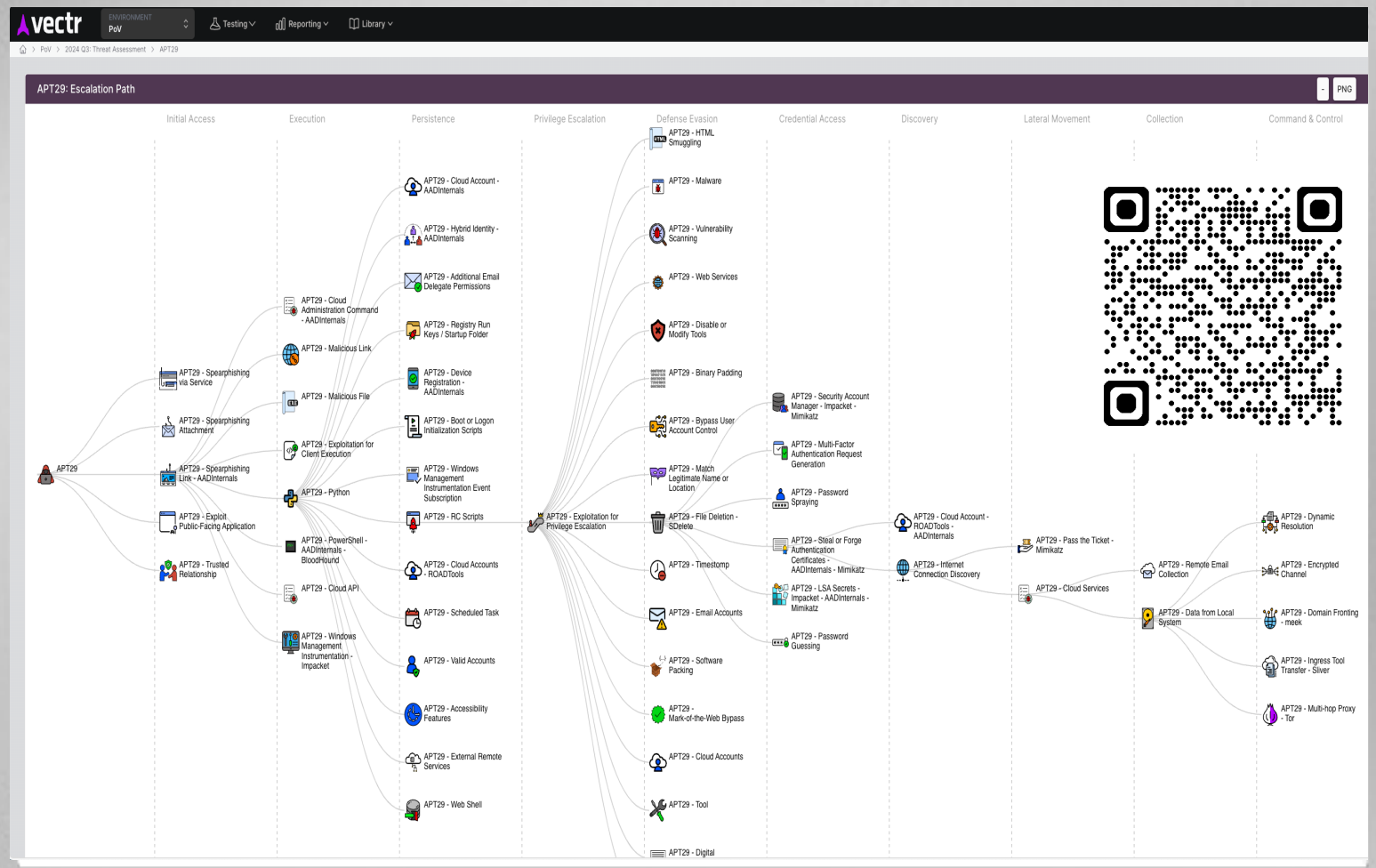
Top 10 MITRE ATT&CK TTPs eCrime and Hacktivist Actors Have Used in the Last 24 Months

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

Threat Scenarios

BRIEF

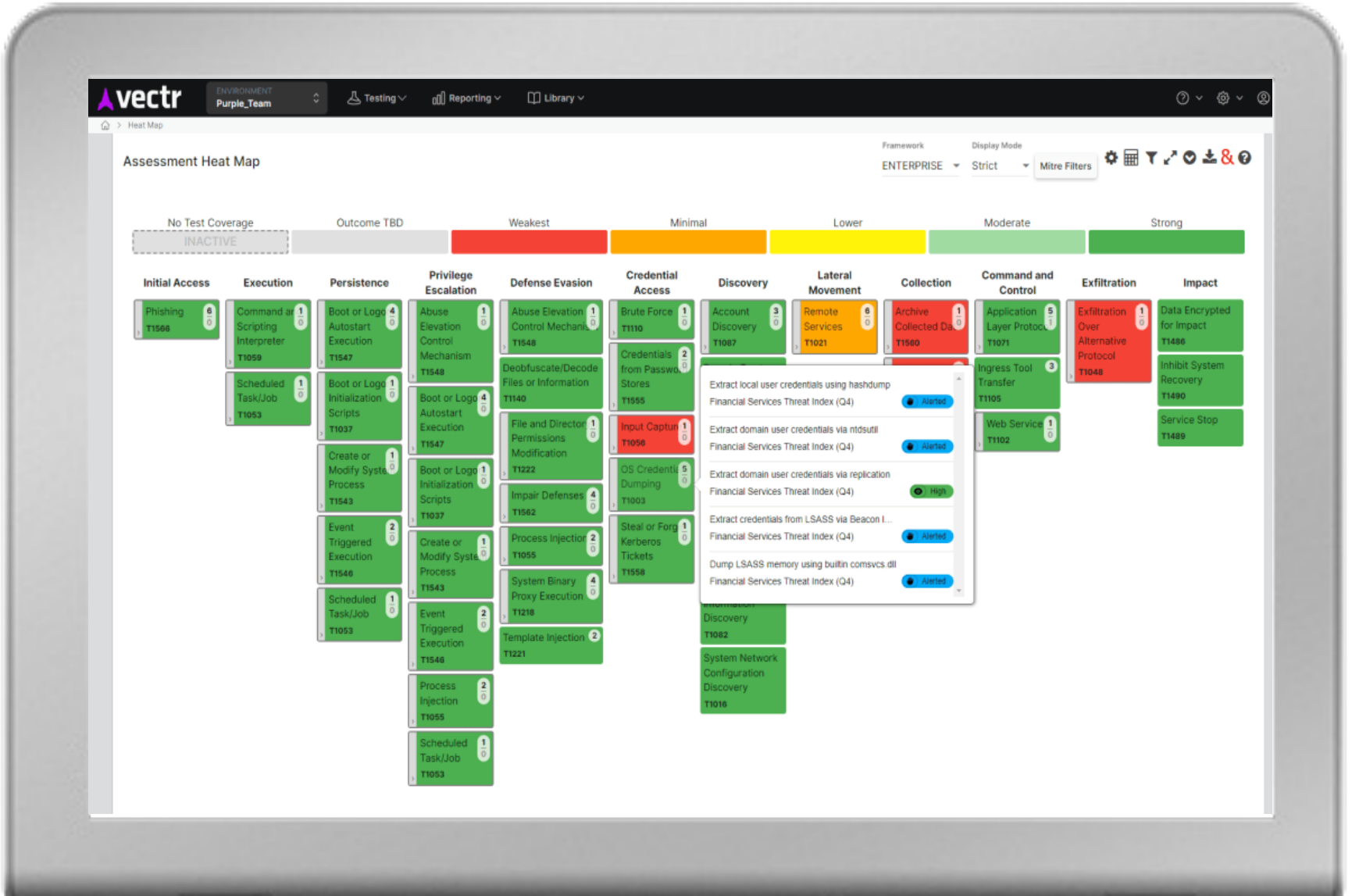
VECTR™ helps facilitate the process to test controls, record outcomes and report on your resilience and improvement over time



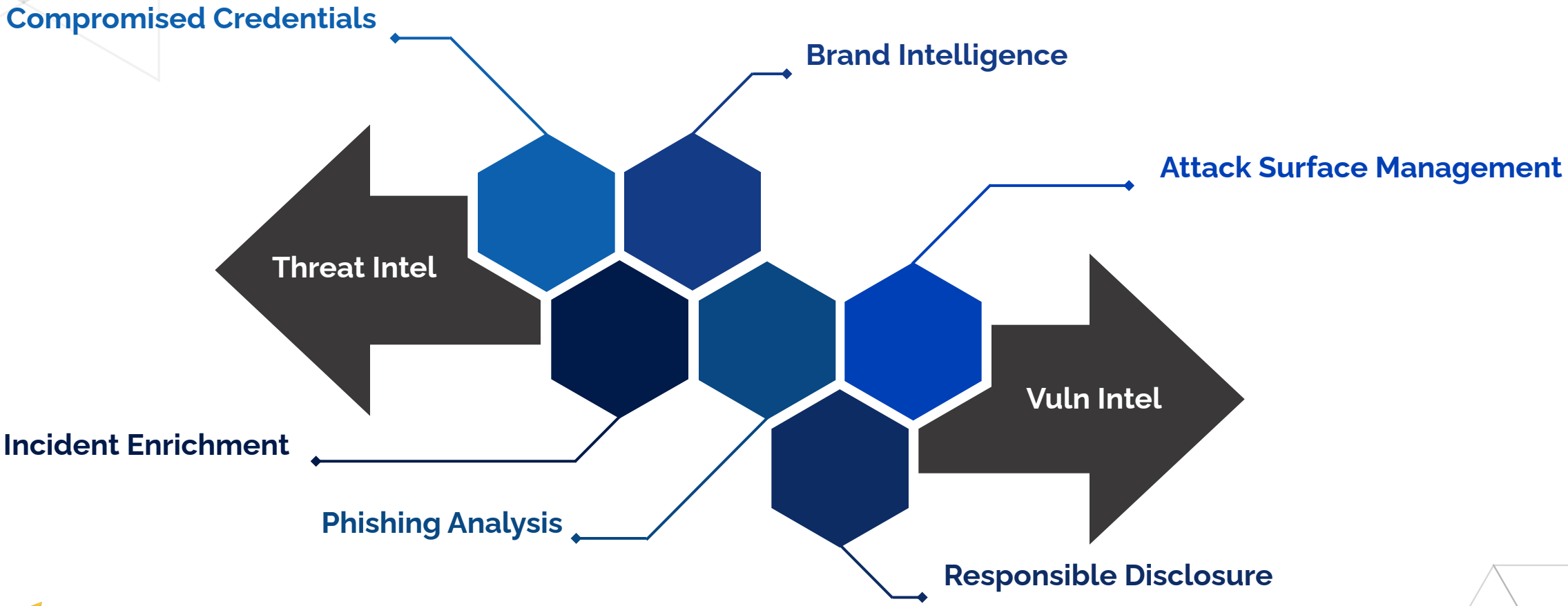
Threat Scenarios

BRIEF

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



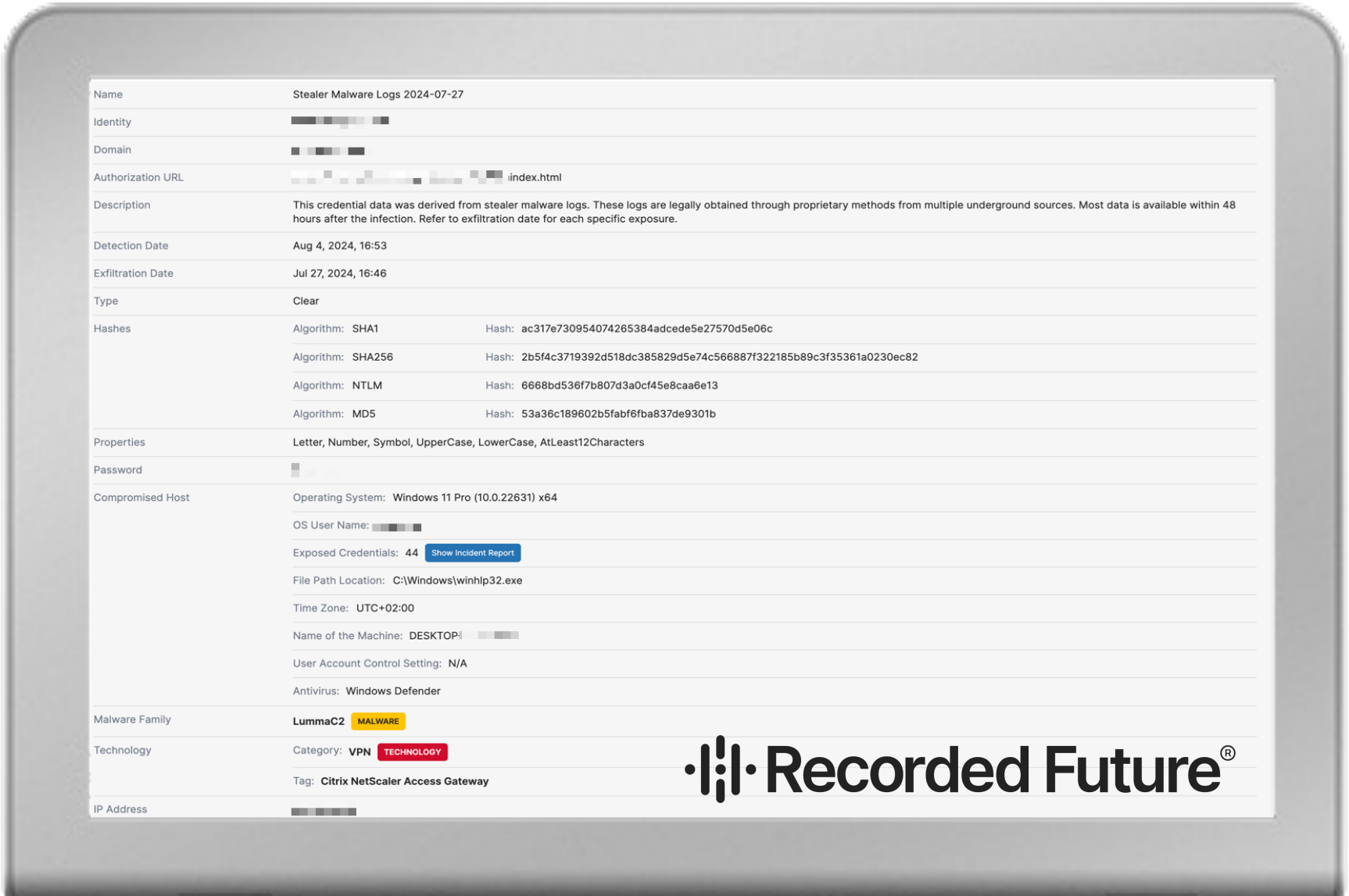
Intrusion Intelligence



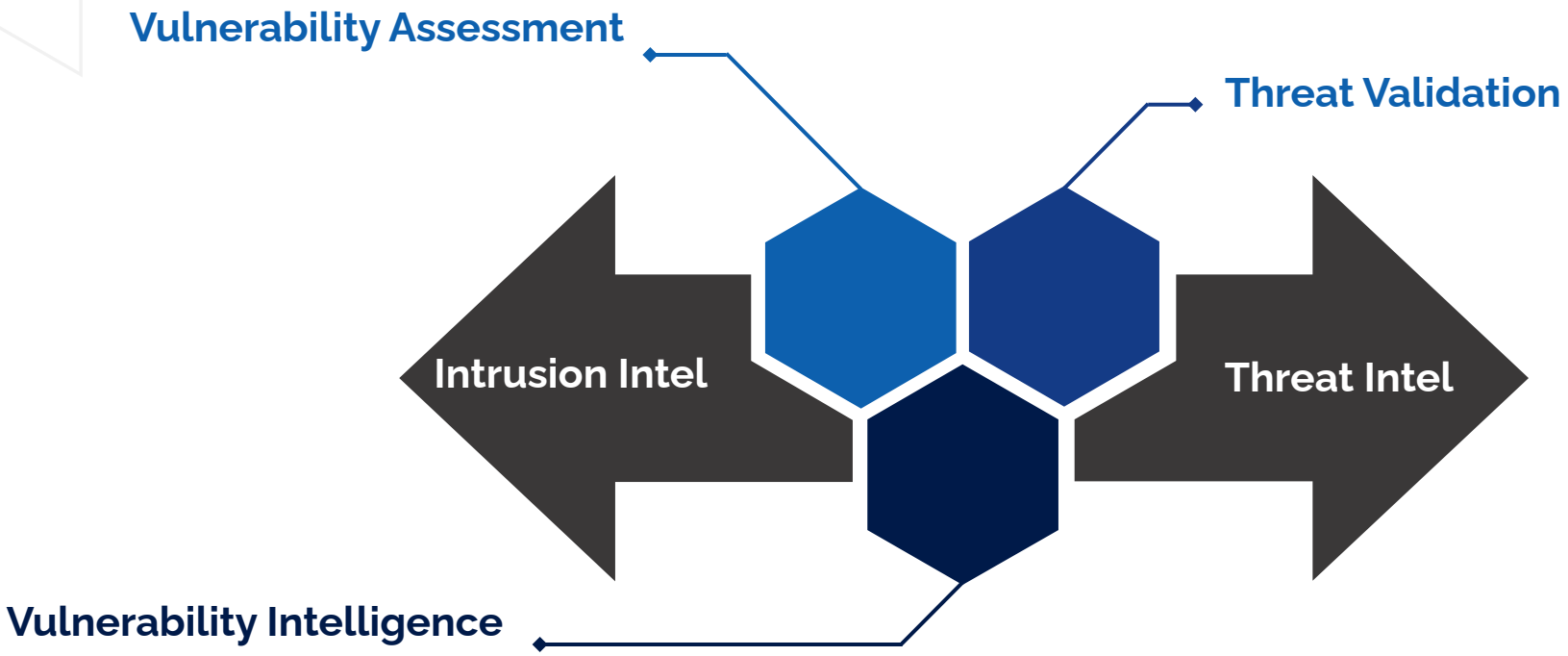
Compromised Credentials

BRIEF

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



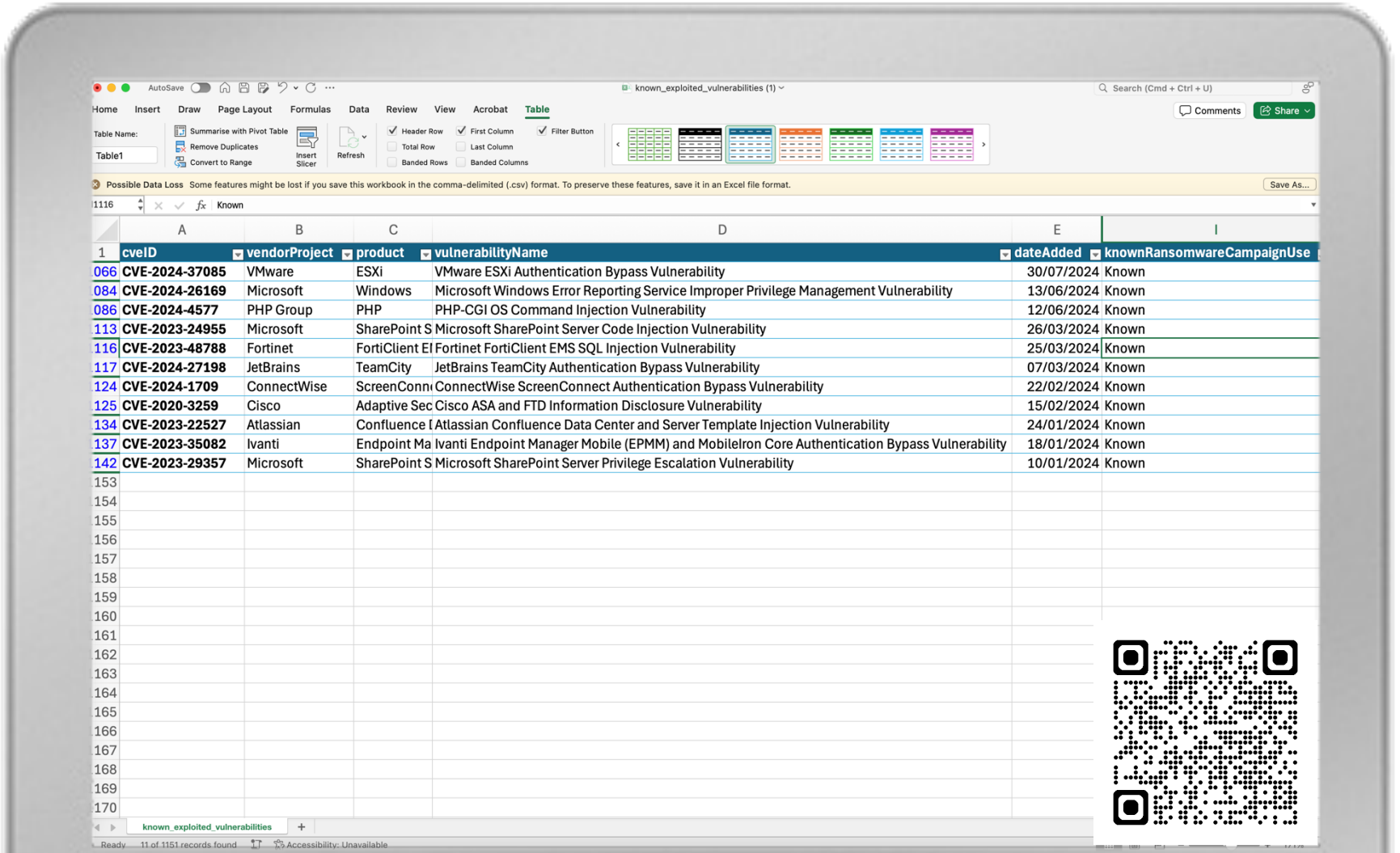
Vulnerability Intelligence



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.



	cveID	vendorProject	product	vulnerabilityName	dateAdded	knownRansomwareCampaignUse
066	CVE-2024-37085	VMware	ESXi	VMware ESXi Authentication Bypass Vulnerability	30/07/2024	Known
084	CVE-2024-26169	Microsoft	Windows	Microsoft Windows Error Reporting Service Improper Privilege Management Vulnerability	13/06/2024	Known
086	CVE-2024-4577	PHP Group	PHP	PHP-CGI OS Command Injection Vulnerability	12/06/2024	Known
113	CVE-2023-24955	Microsoft	SharePoint S	Microsoft SharePoint Server Code Injection Vulnerability	26/03/2024	Known
116	CVE-2023-48788	Fortinet	FortiClient EI	Fortinet FortiClient EMS SQL Injection Vulnerability	25/03/2024	Known
117	CVE-2024-27198	JetBrains	TeamCity	JetBrains TeamCity Authentication Bypass Vulnerability	07/03/2024	Known
124	CVE-2024-1709	ConnectWise	ScreenConn	ConnectWise ScreenConnect Authentication Bypass Vulnerability	22/02/2024	Known
125	CVE-2020-3259	Cisco	Adaptive Sec	Cisco ASA and FTD Information Disclosure Vulnerability	15/02/2024	Known
134	CVE-2023-22527	Atlassian	Confluence I	Atlassian Confluence Data Center and Server Template Injection Vulnerability	24/01/2024	Known
137	CVE-2023-35082	Ivanti	Endpoint Ma	Ivanti Endpoint Manager Mobile (EPMM) and MobileIron Core Authentication Bypass Vulnerability	18/01/2024	Known
142	CVE-2023-29357	Microsoft	SharePoint S	Microsoft SharePoint Server Privilege Escalation Vulnerability	10/01/2024	Known

Integration at All Levels

IT and Infrastructure

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

Threat Management

Architecture

Prioritise onboarding capabilities to provide required prevention against applicable threats

Risk Management

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

Detection and Response

Feed with relevant IOCs and threats applicable to organization

Offensive Operations

Influence offensive operations with applicable and most relevant TTPs. DORA TLPT

Q&A