Threat Informed Defence:

~~Crafting a Developer Centric Threat Detection Framework~~

Play the Metagame

Kade Morton. Co-Founder. Arachne Digital

Thank You to Our Sponsors and Hosts!

AppSec NZ
appsec.org.nz

OWASP
NEW ZEALAND
owasp.org.nz

AUT
UNIVERSITY
TE WĀNANGA ARONUI O TAMAKI MAKAU RAU

BASTION
SECURITY GROUP

DATACOM

aws

84.

PentesterLab

plexure

VERACODE

Without them, this Conference couldn’t happen.

Topics covered

Threat Informed Defence

The Intelligence Cycle

MITRE ATT&CK

Business Context

Technical Context

Risk Context

Mitigation and Detection

Use Cases

Logs

Summary

If you want a copy of these slides:

https://github.com/arachne-threat-intel/community/tree/main/slides/OWASP2024

Presenter

Kade Morton

- Worked in cyber security for 6 years
- Worked in consulting, government, banking, critical infrastructure
- Focus on cyber threat intelligence (CTI) and blue teaming

Kade Morton

LinkedIn Profile

If you don’t trust QR codes

https://www.linkedin.com/in/kade-morton-34179283/

Timely & Actionable

Cyber Threat Intelligence

ARACHNE

https://github.com/arachne-threat-intel

Community

GitHub

Arachne Digital

LinkedIn Page

https://www.linkedin.com/company/arachne-digital

We want to protect a web app

Assumed to be hosted on a Linux web server

OWASP has a threat modelling process
https://owasp.org/www-community/Threat_Modeling_Process

It uses STRIDE to identify threats

STRIDE looks at possible threats

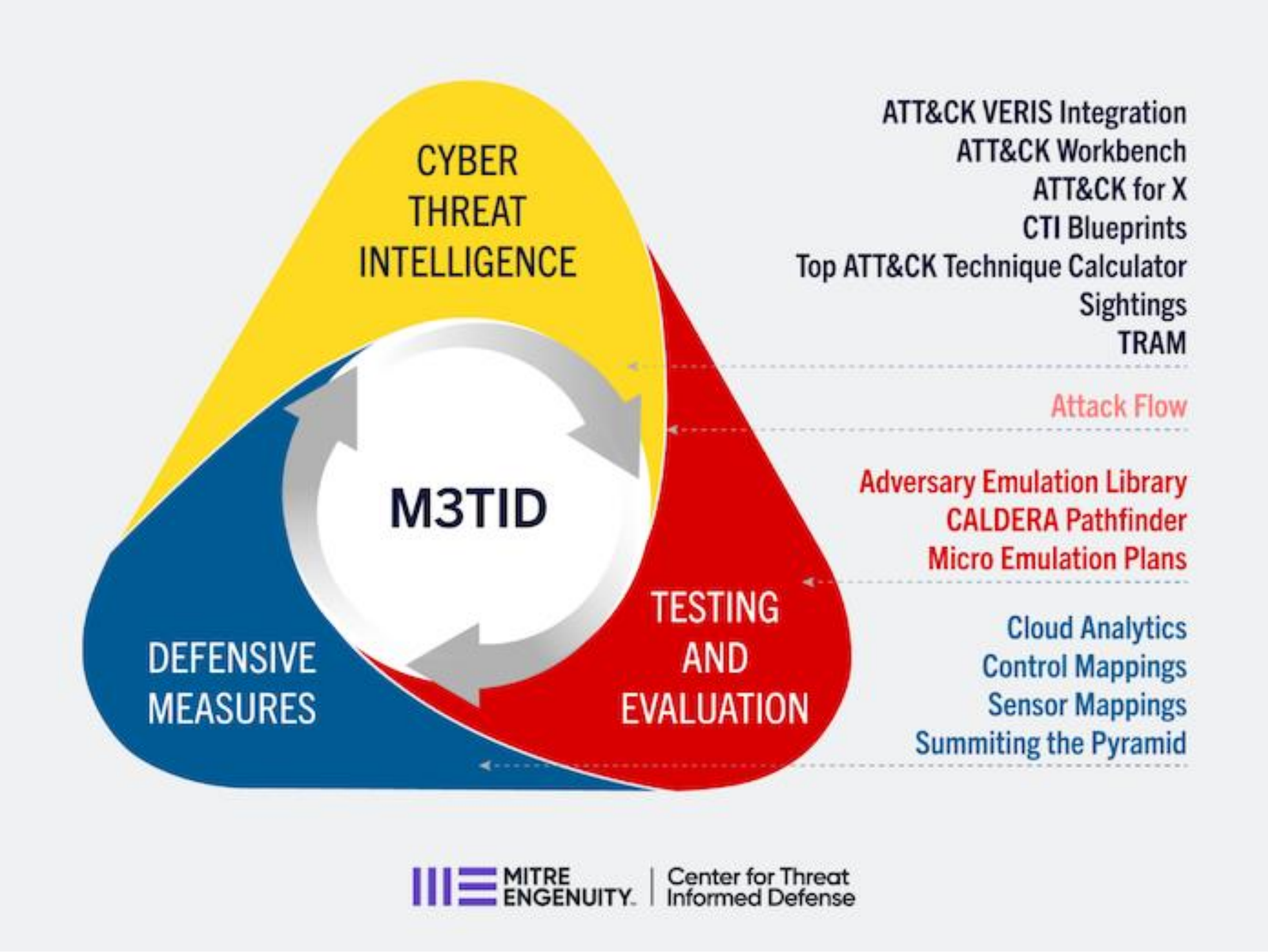
Good to account for all possible threats during development, once out of development we want to know specifically want we have to defend against.

We want to use real world data to define real threats

Threat Informed Defence

Threat-Informed Defense is the systematic application of a deep understanding of adversary tradecraft and technology to improve defenses.

We need an easier way to explain this.



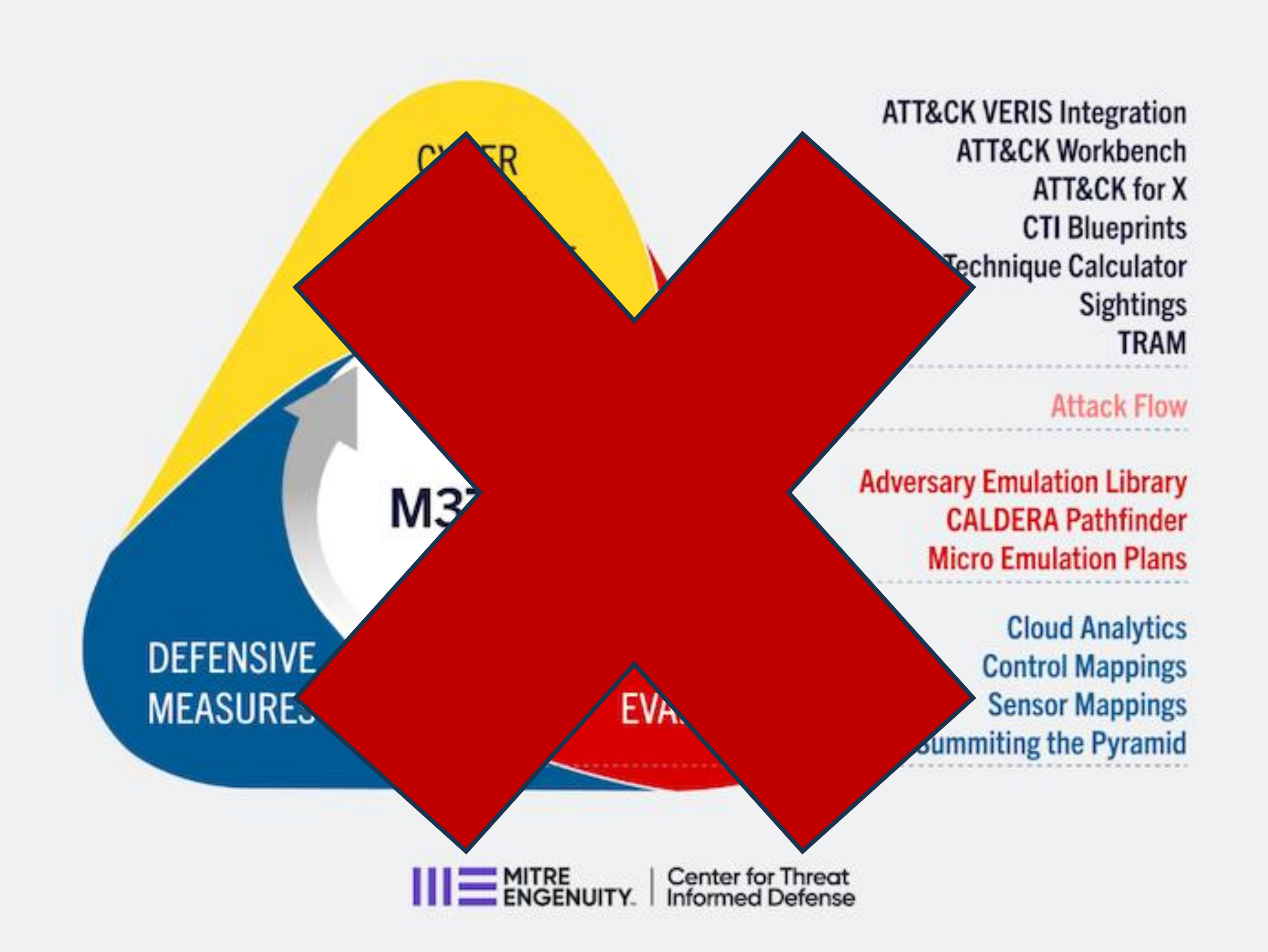
https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/threat-informed-defense/

My slides were done, but then…

I was trying to explain my talk to structural engineer, someone totally outside of computer science.

He said “oh, so the message is basically play the metagame?”

Thank you Lewis Goldby!



https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/threat-informed-defense/

I need two volunteers!

Audience participation.

What could possibly go wrong?

Play the Metagame

Metagaming is playing a game with prior knowledge of what is considered to be more fitting to earn the best or most desired results.

For example, you've been watching your buddy play Street Fighter II in the arcade. You notice they uses the same moves and combos over and over. Therefore, when you play against them, you use a character and moves that you know can beat them.

Instead of going in blind, your foreknowledge of their favorite strategies gives you an advantage.

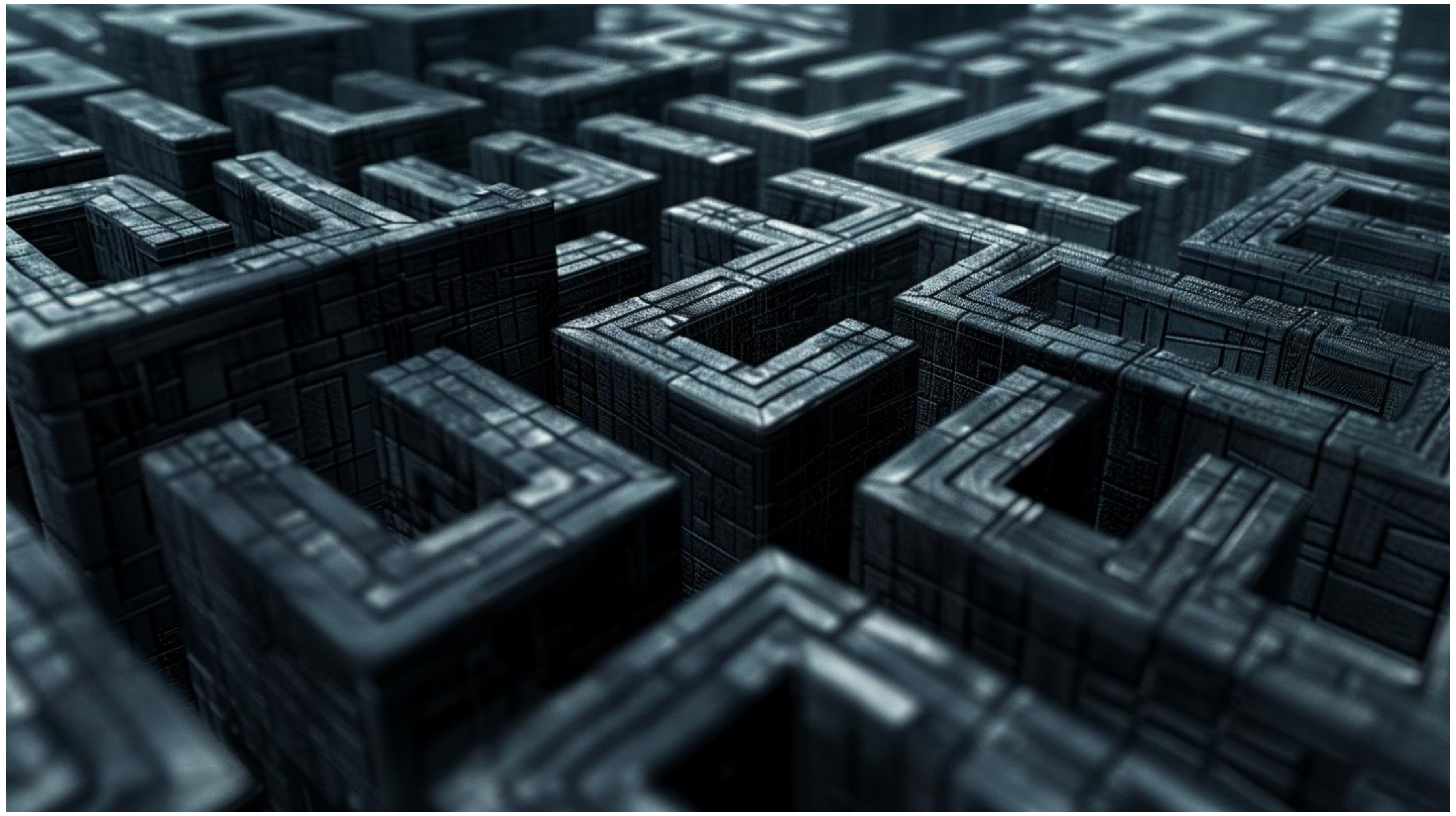
https://tvtropes.org/pmwiki/pmwiki.php/Main/Metagame

Threat Informed Metagame

Threat-Informed Defense is the systematic application of a deep understanding of adversary tradecraft and technology to improve defenses.

OR

Figure out the moves of your adversary and your weaknesses, protect accordingly.



How do we figure out the metagame?

Threat-Informed Defense is the systematic application of a deep understanding of **adversary tradecraft** and technology to improve defenses.

Start with adversary tradecraft.

Mission – protect our web app.

Planning and Direction – the instruction to go get data on adversary tradecraft.

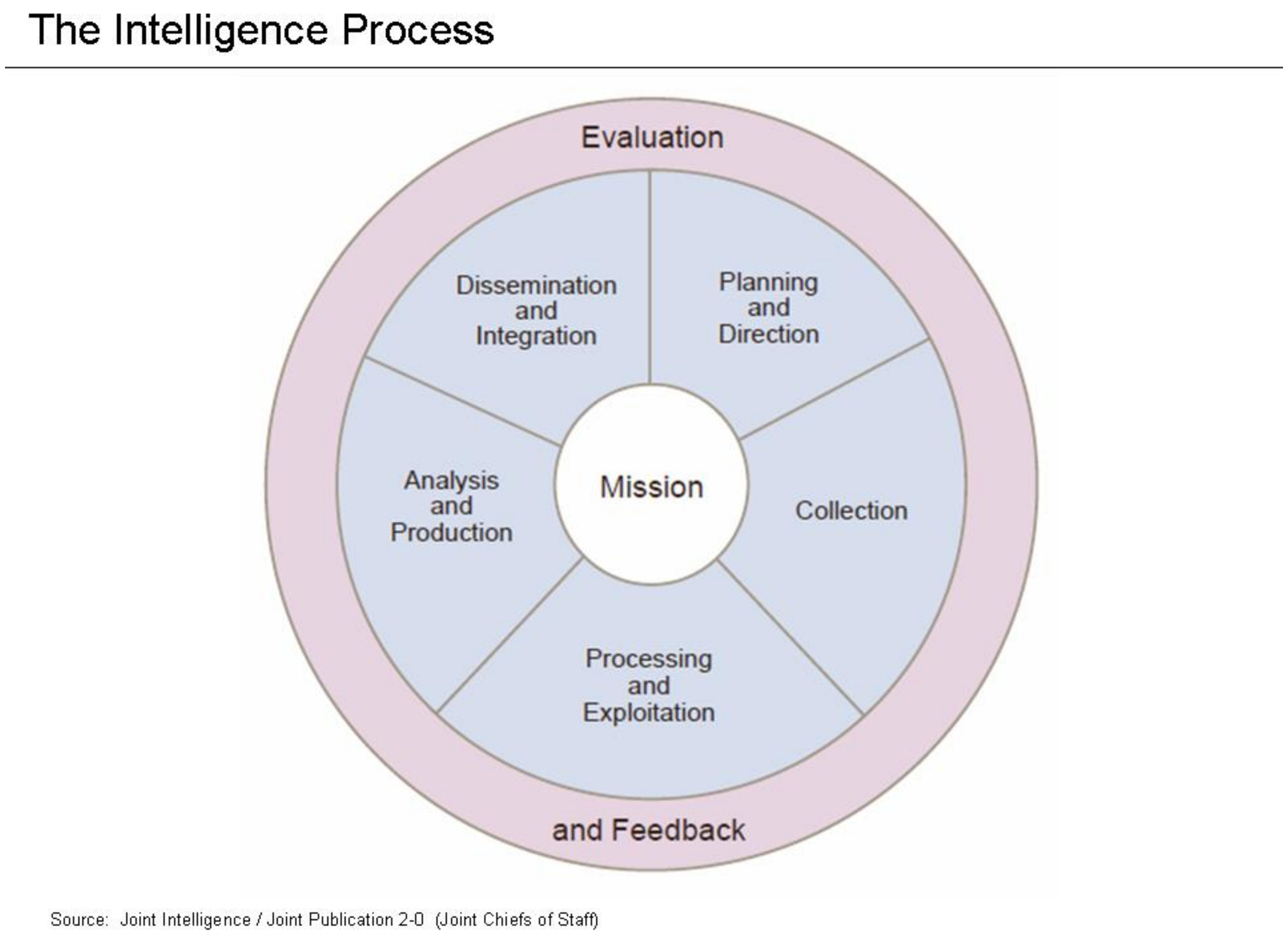
Collection – gather the data on adversary tradecraft.

Processing – turn the data into information.

Analysis – turn the information into intelligence.

Dissemination – give the intelligence to who needs it.

Evaluation and Feedback – what can be done better for next time.



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

By Joint Chiefs of Staff - http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf, Public Domain, https://commons.wikimedia.org/w/index.php?curid=47853466

Data, Information, Intelligence

Operational environment – where the web app is, the internet.

Collection – gathering data from various sources.

Data – raw, unprocessed facts and figures.

Processing – converting data into a usable, organised format.

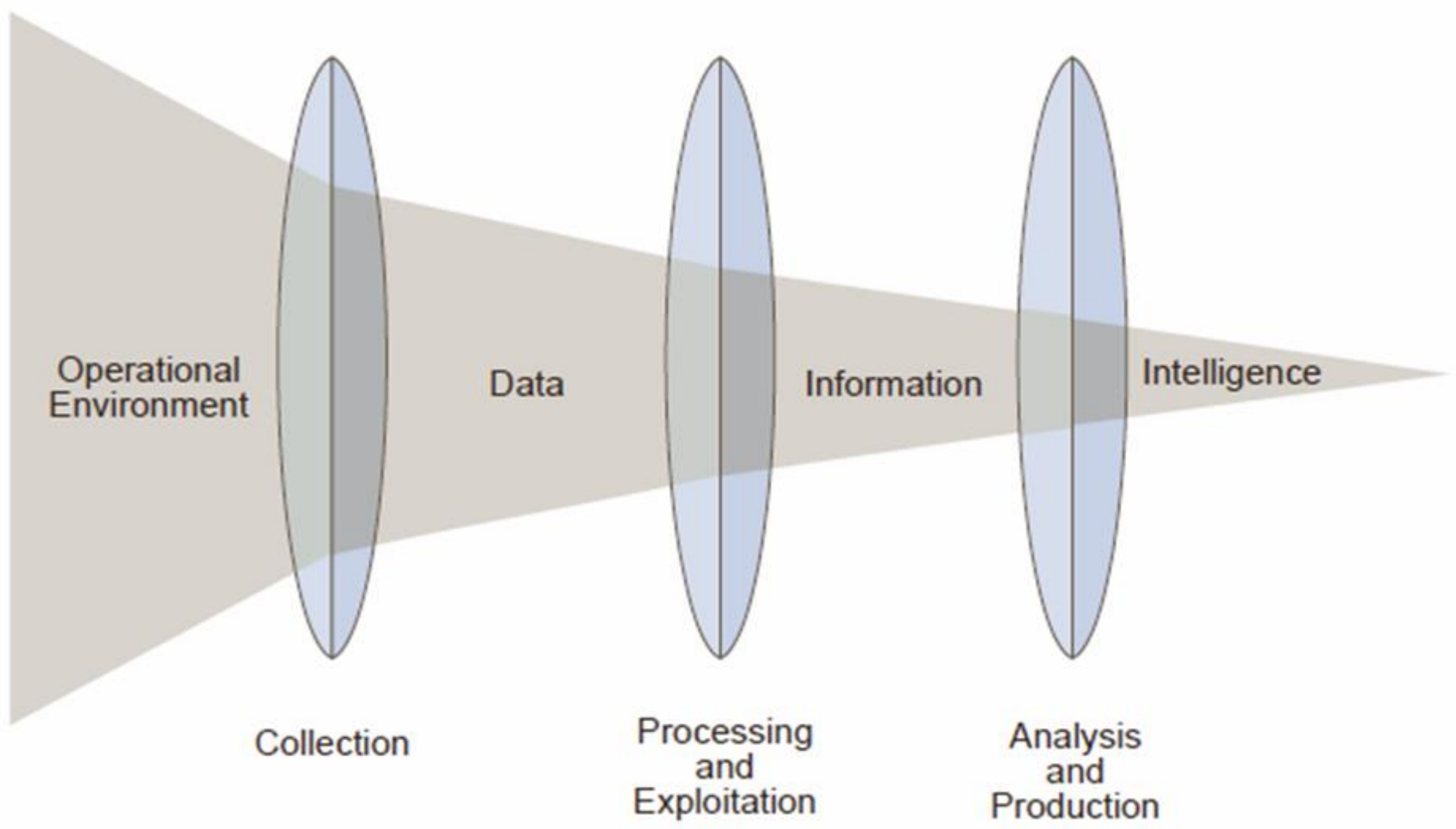
Information – data that has been organised and given context. Information answers the basic "who, what, where, when" questions..

Analysis - Evaluating the information to identify patterns, relationships, and insights.

Intelligence - the result of analyzing information to draw conclusions and make predictions. It is actionable knowledge that answers the "why" and "how" questions, providing insights that support decision-making.

The decision making being how do we protect our web app.

Relationship of Data, Information and Intelligence



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

By U.S. Joint Chiefs of Staff JP2-0 - http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf, Public Domain, https://commons.wikimedia.org/w/index.php?curid=47853614

Collection

Let's go gather data on internet based threats.

Can be as simple as using a search engine, can be as complex as a collection pipeline.

Example collection pipeline – A python program that takes in keywords, feeds them to a metasearch engine, and provides continuous results.

Looking for cyber threat actors (CTAs) that target **your industry** and **your geography**.

Note that hacking can be indiscriminate if driven by vulnerabilities.

For example, hackers targeting education institutions in Oceania.

https://web.archive.org/web/20170916125412/http://www.automatingosint.com/blog/2017/04/building-a-keyword-monitoring-pipeline-with-python-pastebin-and-searx/

Processing and Analysis

We've got a bunch of data.

For example, a number of news articles covering high profile hacks for similar organisations.

Remember our quote: Threat-Informed Defense is the systematic application of a deep understanding of **adversary tradecraft** and technology to improve defenses.

Let's look at adversary tradecraft.

MITRE ATT&CK

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.

https://attack.mitre.org/

It covers Tactics, Techniques and Procedures (TTPs).

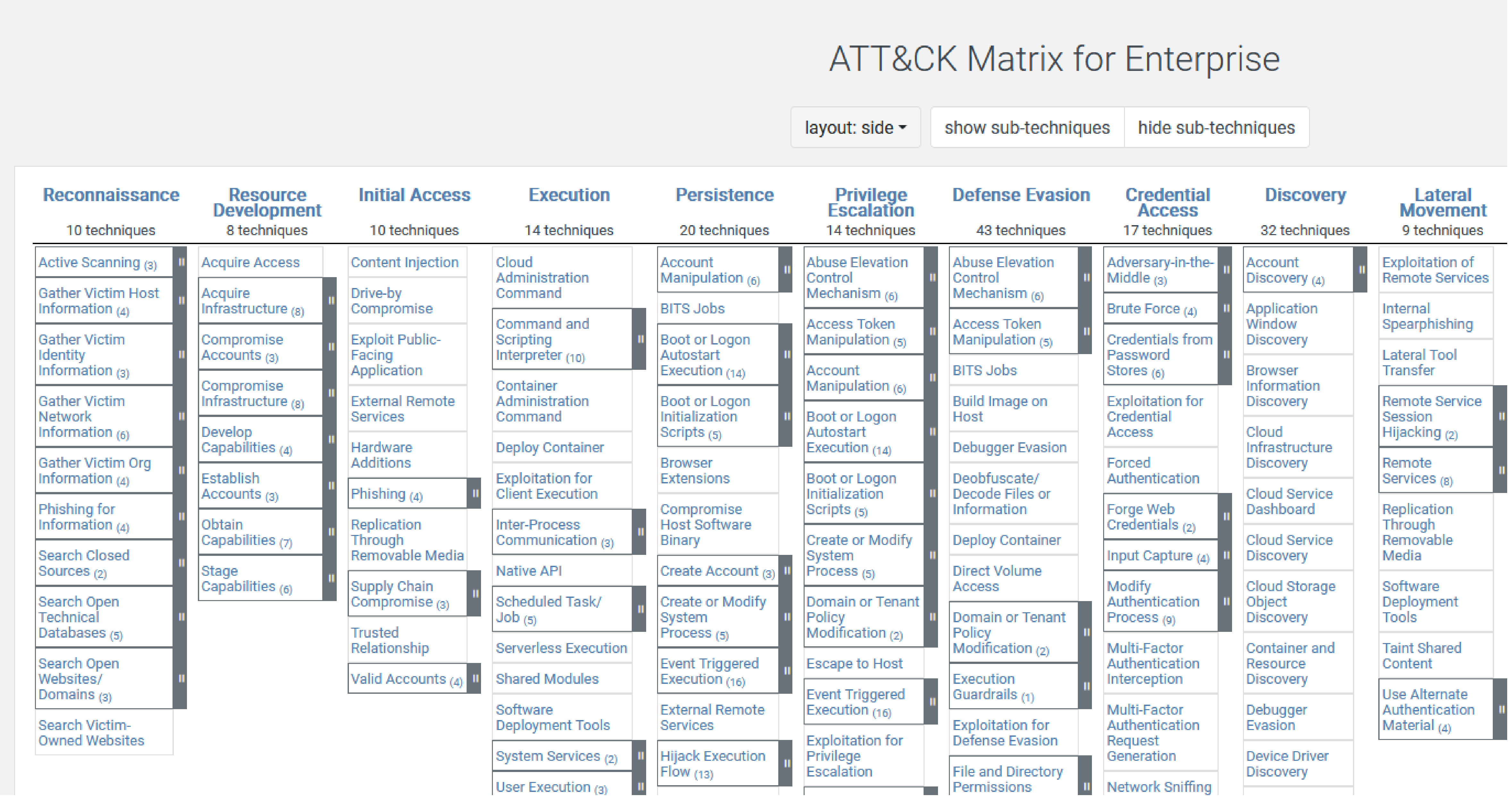
Tactics are the columns, Reconnaissance, Resource Development, etc

Techniques are each entry.

Procedures are how the technique is executed.

Each Technique maps to mitigations and detections.

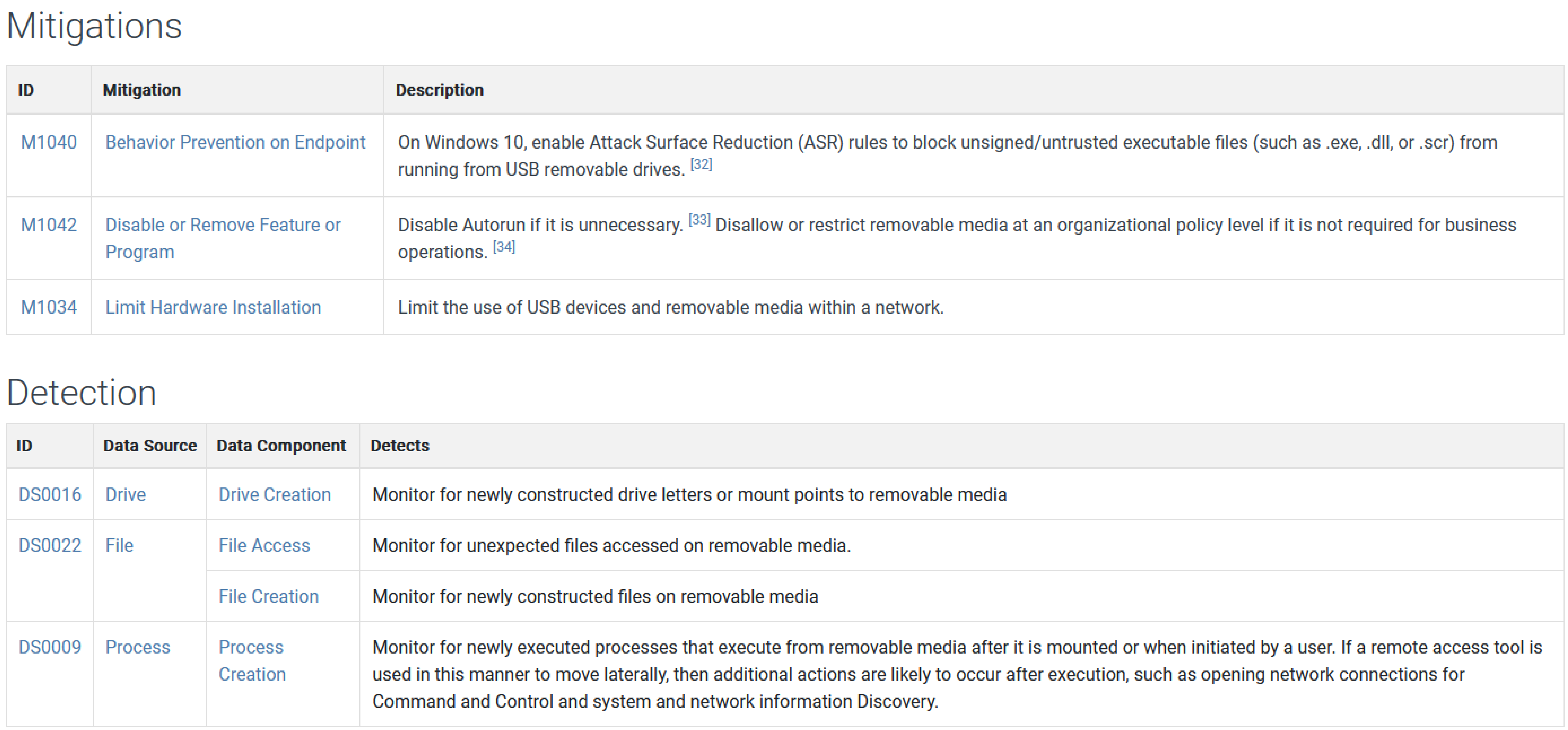
If you know the TTPs you care about, you know how to stop or at least detect them.



ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (6)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Drive-by Compromise	Command and Scripting Interpreter (10)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (6)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer
Gather Victim Network Information (6)	Compromise Infrastructure (8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Inter-Process Communication (3)	Compromise Host Software Binary	Create or Modify System Process (5)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through Removable Media	Native API	Create Account (3)	Domain or Tenant Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools
Search Open Technical Databases (5)	Stage Capabilities (6)	Supply Chain Compromise (3)	Scheduled Task/Job (5)	Create or Modify System Process (5)	Escape to Host	Direct Volume Access	Modify Authentication Process (9)	Container and Resource Discovery	Taint Shared Content
Search Open Websites/Domains (3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain or Tenant Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)
Search Victim-Owned Websites		Valid Accounts (4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery	
			Software Deployment Tools	Hijack Execution Flow (13)		Exploitation for Defense Evasion	Network Sniffing		
			System Services (2)			File and Directory Permissions			
			User Execution (3)						

Mitigations and Detections



Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to block unsigned/untrusted executable files (such as .exe, .dll, or .scr) from running from USB removable drives. [32]
M1042	Disable or Remove Feature or Program	Disable Autorun if it is unnecessary. [33] Disallow or restrict removable media at an organizational policy level if it is not required for business operations. [34]
M1034	Limit Hardware Installation	Limit the use of USB devices and removable media within a network.

Detection

ID	Data Source	Data Component	Detects
DS0016	Drive	Drive Creation	Monitor for newly constructed drive letters or mount points to removable media
DS0022	File	File Access	Monitor for unexpected files accessed on removable media.
		File Creation	Monitor for newly constructed files on removable media
DS0009	Process	Process Creation	Monitor for newly executed processes that execute from removable media after it is mounted or when initiated by a user. If a remote access tool is used in this manner to move laterally, then additional actions are likely to occur after execution, such as opening network connections for Command and Control and system and network information Discovery.

How to map to MITRE ATT&CK

There is no formal training for mapping to MITRE ATT&CK.

MITRE have published best practice: https://www.cisa.gov/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf

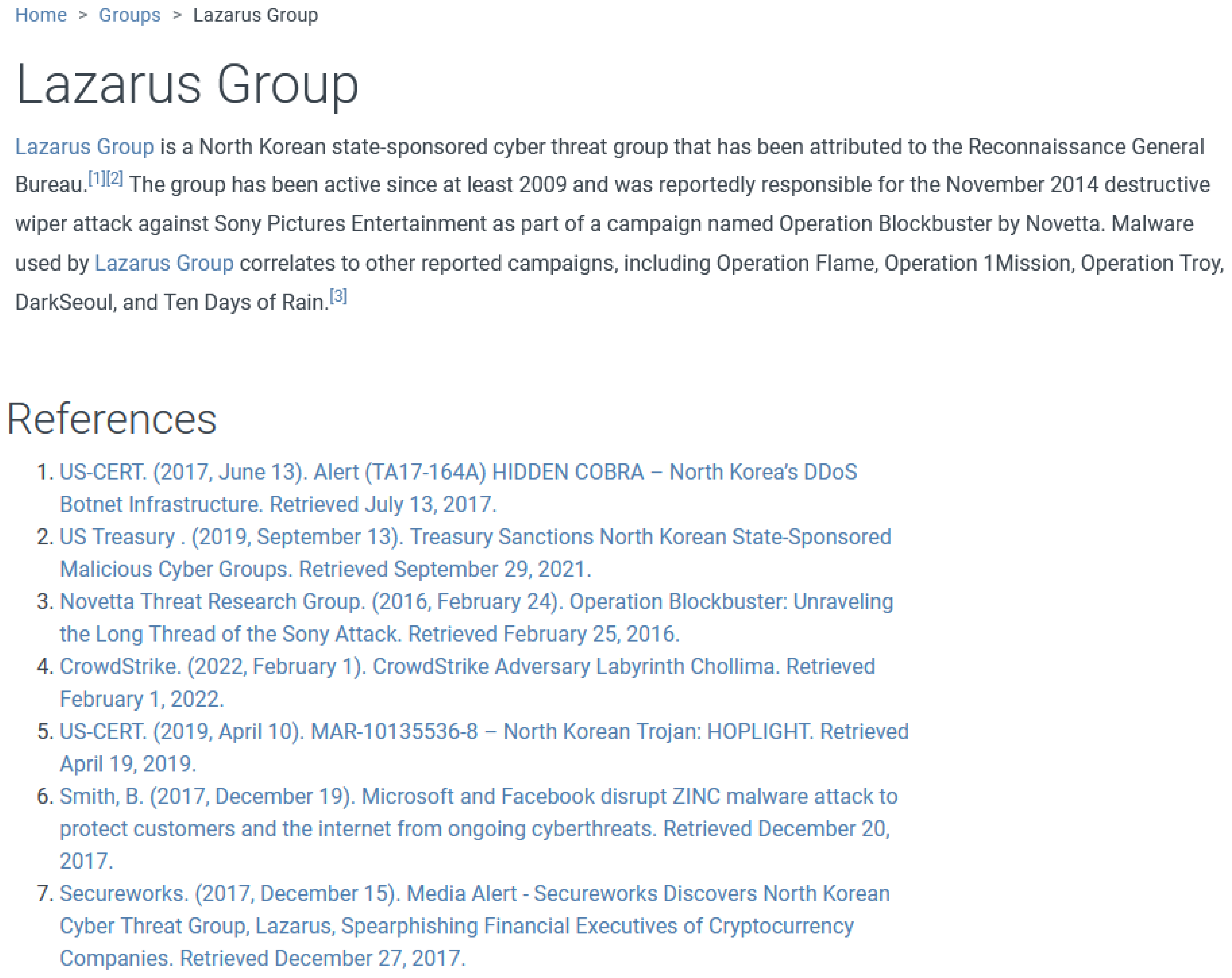
There are tools that use machine learning to match free text to MITRE ATT&CK

TRAM - https://github.com/center-for-threat-informed-defense/tram

Thread - https://arachne.digital/thread and https://github.com/arachne-threat-intel/thread

There are some databases out there that list TTPs against CTAs but the information is often dated.

Best to collect it yourself so you know it's fresh.



Home > Groups > Lazarus Group

Lazarus Group

Lazarus Group is a North Korean state-sponsored cyber threat group that has been attributed to the Reconnaissance General Bureau.[1][2] The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain.[3]

References

1. US-CERT. (2017, June 13). Alert (TA17-164A) HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure. Retrieved July 13, 2017.
2. US Treasury . (2019, September 13). Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups. Retrieved September 29, 2021.
3. Novetta Threat Research Group. (2016, February 24). Operation Blockbuster: Unraveling the Long Thread of the Sony Attack. Retrieved February 25, 2016.
4. CrowdStrike. (2022, February 1). CrowdStrike Adversary Labyrinth Chollima. Retrieved February 1, 2022.
5. US-CERT. (2019, April 10). MAR-10135536-8 – North Korean Trojan: HOPLIGHT. Retrieved April 19, 2019.
6. Smith, B. (2017, December 19). Microsoft and Facebook disrupt ZINC malware attack to protect customers and the internet from ongoing cyberthreats. Retrieved December 20, 2017.
7. Secureworks. (2017, December 15). Media Alert - Secureworks Discovers North Korean Cyber Threat Group, Lazarus, Spearphishing Financial Executives of Cryptocurrency Companies. Retrieved December 27, 2017.

You now know the metagame

You now which CTAs target **your industry** and **your geography** (and the indiscriminate ones).

You know the **current** TTPs. You know how to mitigate them and detect them.

CTAs > TTPs

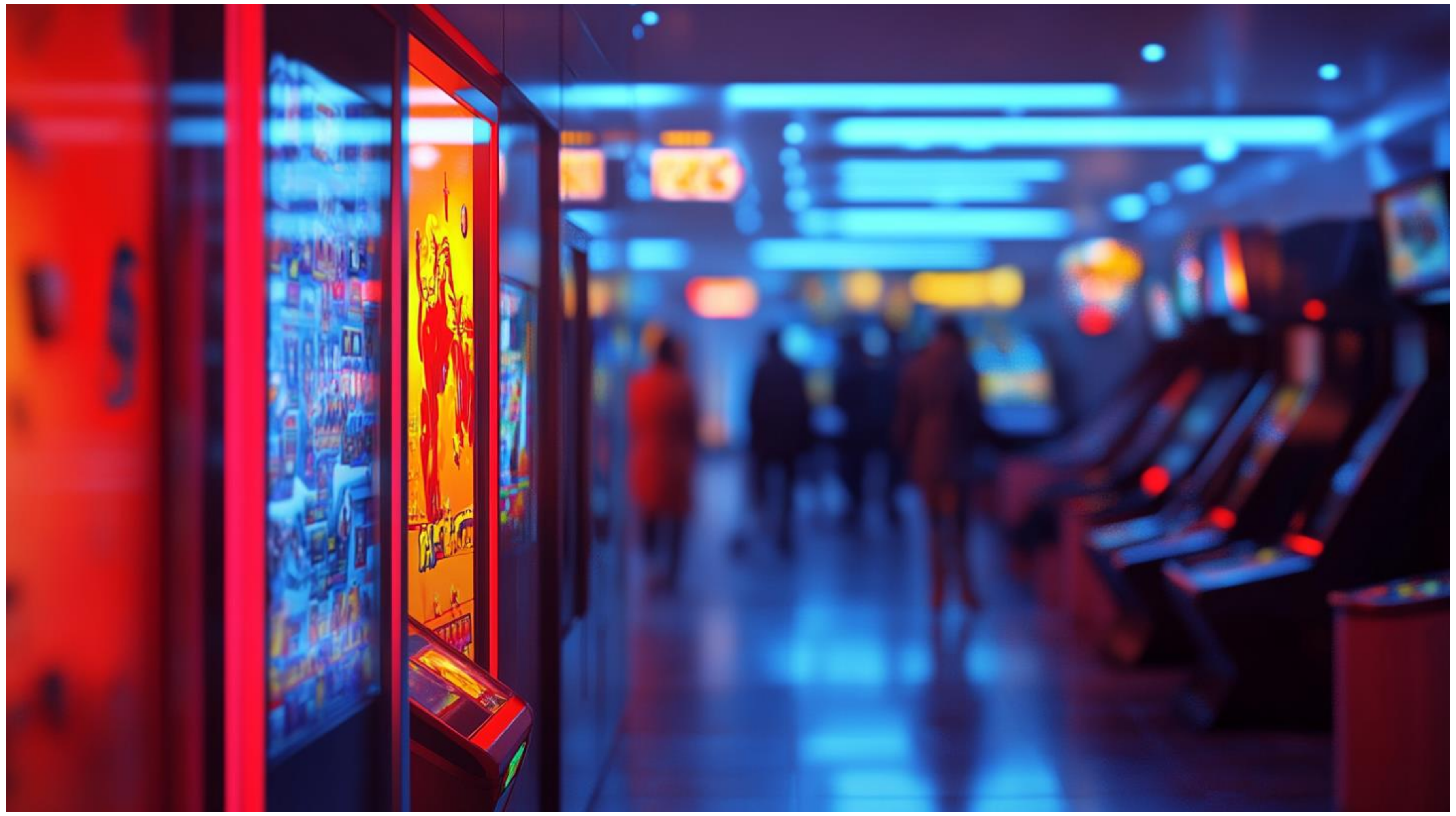
TTPs > Mitigative controls > Issue mitigated

TTPs > Detective controls > Detection use case

But wait, there's more!

But there is another part to Threat Informed Defence.

Threat-Informed Defense is the systematic application of a deep understanding of adversary tradecraft and **technology** to improve defenses.



Business context

Business context is the context around the role of the asset in the organisation, the type of data it handles, and its importance to business operations.

Understanding the business context of an asset helps in identifying criticality and potential impact on the business.

*Business Context Exampl*e: The application handles sensitive financial data, making it more likely to be targeted and the impact of being targeted is higher than other applications the organisation has.

Detection Use Case: Monitor for unauthorised access attempts because we know the application is likely to be targeted.

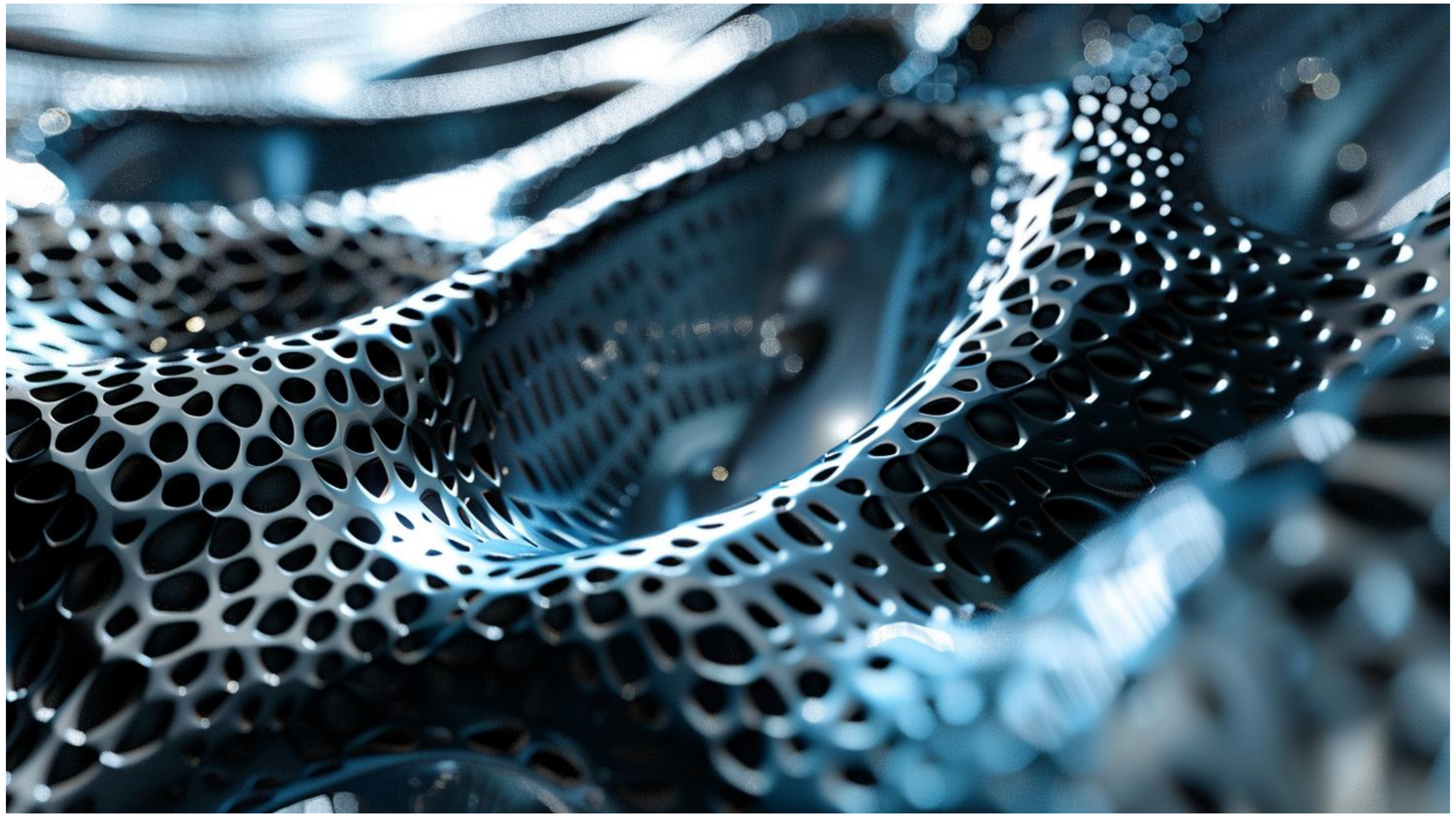
Technical context

Technical context is the context around the technical aspects, such as configurations, user roles, access controls, and how the asset integrates with other systems.

Understanding technical context aids in identifying potential technical vulnerabilities and dependencies.

Technical Context Example: If set server configurations change it disables set security controls.

Detection Use Case: Detect configuration changes.



Risk context

Review existing risk assessments related to the web application (if you have them).

Identify specific risks that have been documented, such as data breaches, unauthorised access, or system vulnerabilities.

Reviewing the risks related to an asset that have already been identified helps in define what could go wrong related to the asset.

Risk Example: There is a risk of known vulnerabilities in the web server being exploited because the server is end of life.

Detection Use Case: Monitor for traffic attempting to exploit known vulnerabilities in server.

You now know yourself

You now understand the business, technical and risk context

Business context > Mitigative controls > Issue mitigated

Business context > Detection use case

Technical context > Mitigative controls > Issue mitigated

Technical context > Detection use case

Risk context > Mitigative controls > Issue mitigated

Risk context > Detection use case

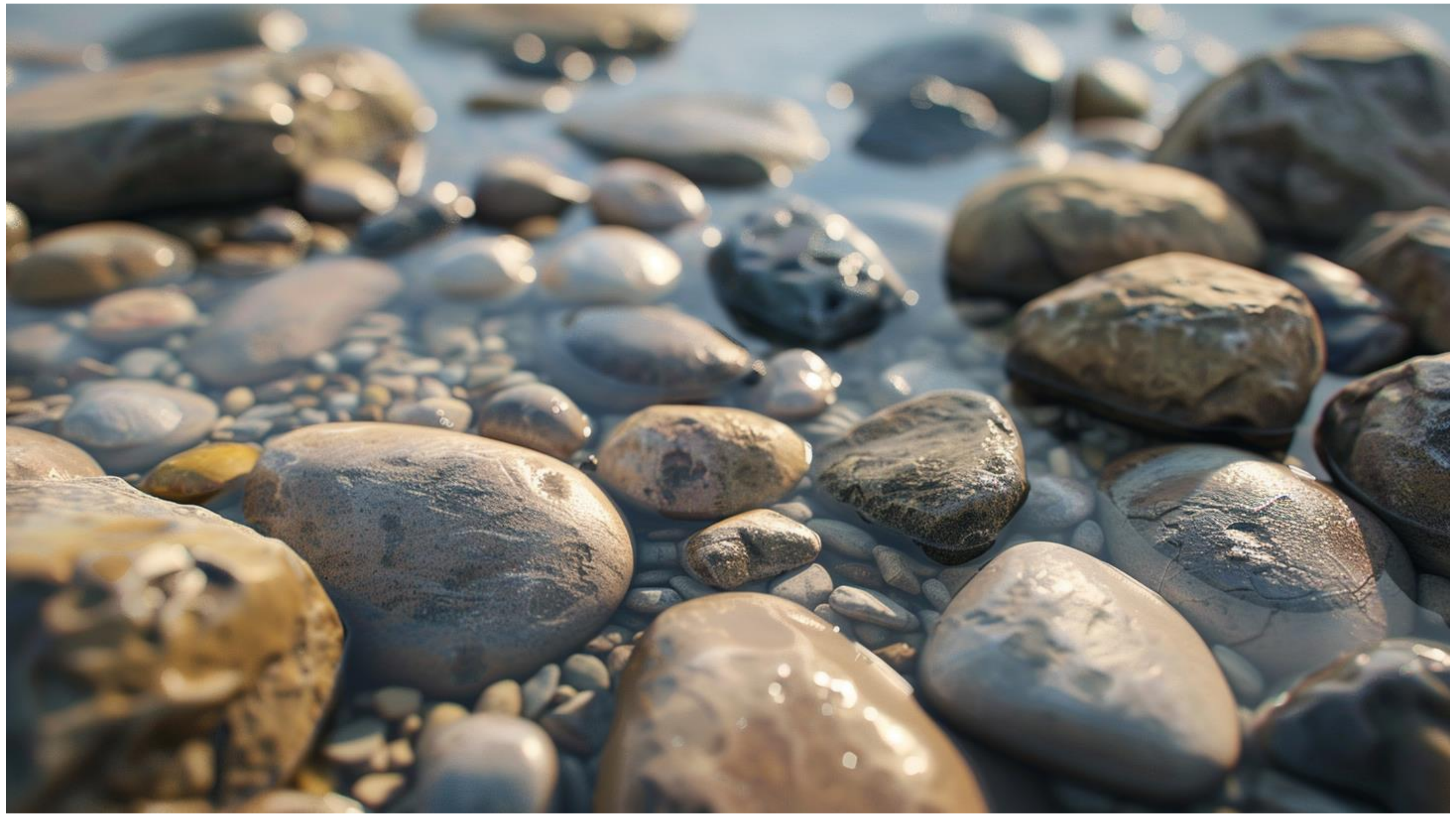
And you understand the whole

Threat-Informed Defense is the systematic application of a deep understanding of **adversary tradecraft** and **technology** to improve defenses.

It wouldn’t be a security presentation without a Sun Tzu quote!

Hence the saying: If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

https://suntzusaid.com/book/3/18



Applying this information

Look to put in place controls for each point, both adversary tradecraft and the information specific to the application, to either mitigate the potential issue, or monitor for it.

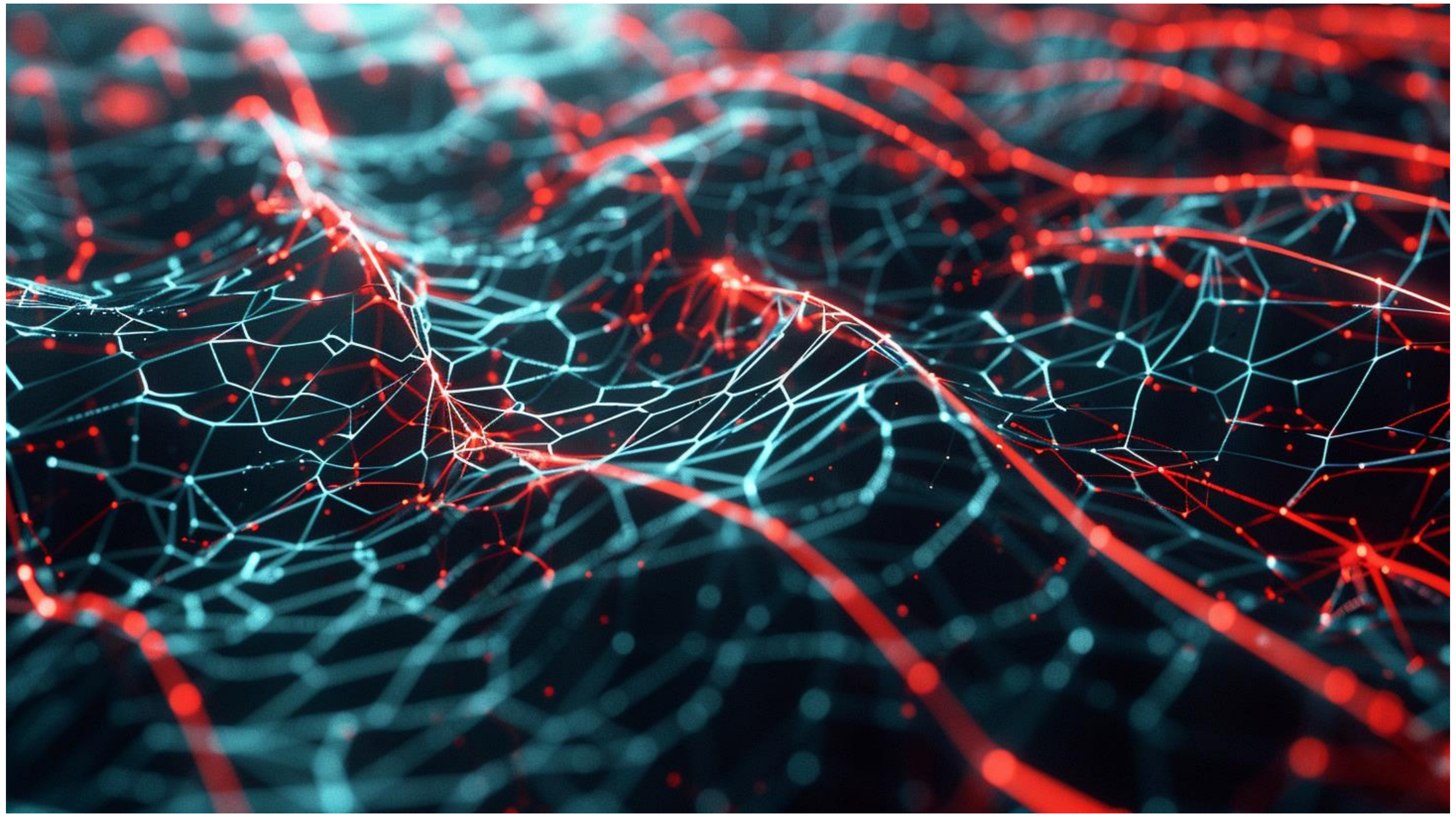
Mitigating controls are relatively self explanatory. For example, if there is an internet facing login portal, we need to configure two factor authentication. The mitigating control mitigates or removes the issue to a certain extent.

Detection is harder.

Detection requires a lot

You need:

- Logs
- The right logs
- Log aggregator
- Log storage
- A tool to analyse logs, SIEM (Security Information Event Management) tool
- The right queries/alerts
- A team to monitor alerts around the clock
- A team to perform incident response if an incident is detection, and this may be out of hours
- An incident response plan
- Buy in from the rest of the business to make the incident response plan work
- The plan needs testing
- Etc
- Etc



Assuming you have all that

Use cases define queries/alerts

Queries/alerts define the logs required

T1053 Scheduled Tasks has been defined as a TTP that an adversary in your threat model uses often.

The use case is to monitor scheduled tasks.

The queries/alerts might look like this:

```
RULE "Detect Suspicious Scheduled Task Activity"

CONDITIONS:
   // Condition 1: Monitor for the execution of task scheduling processes
   IF process_name IN ["cron", "atd", "systemd-timer"] AND
      command_line CONTAINS ["/bin/bash", "/usr/bin/python", "/usr/bin/perl", "/bin/sh"]
   THEN
       SET priority = HIGH
       SET alert_message = "Suspicious task scheduling process execution detected"

// Condition 2: Monitor for unusual process spawning from task scheduling processes
   IF parent_process_name IN ["cron", "atd", "systemd-timer"] AND
      child_process_name IN ["<suspicious_process>"] AND
      command_line CONTAINS ["<suspicious_argument>"]
   THEN
       SET priority = HIGH
       SET alert_message = "Suspicious process spawned from scheduled task“

// Condition 3: Monitor for file creation or modification in critical directories
   IF file_path IN ["/etc/cron.d/", "/etc/cron.daily/", "/etc/systemd/system/", "/var/spool/cron/crontabs/"] AND
      (file_action == "CREATE" OR file_action == "MODIFY")
   THEN
       SET priority = MEDIUM
       SET alert_message = "File creation/modification in scheduled task directory"
```

Logs

We need to capture:

Parent and child process names

Command line arguments

File paths

File actions (creation, modification, or deletion)

Auditd Logs: Configure audit rules to capture the required information

Log File: /var/log/audit/audit.log

Syslog: Configure syslog to capture and forward the required information

Log File: /var/log/syslog or /var/log/messages

Detections are now in place

Logs are now configured to capture the right information for queries/alerts, that cover all of our detection use cases.

We've gone all the way from collecting information from the threat landscape to configuring the exact field in the exact log that we need!

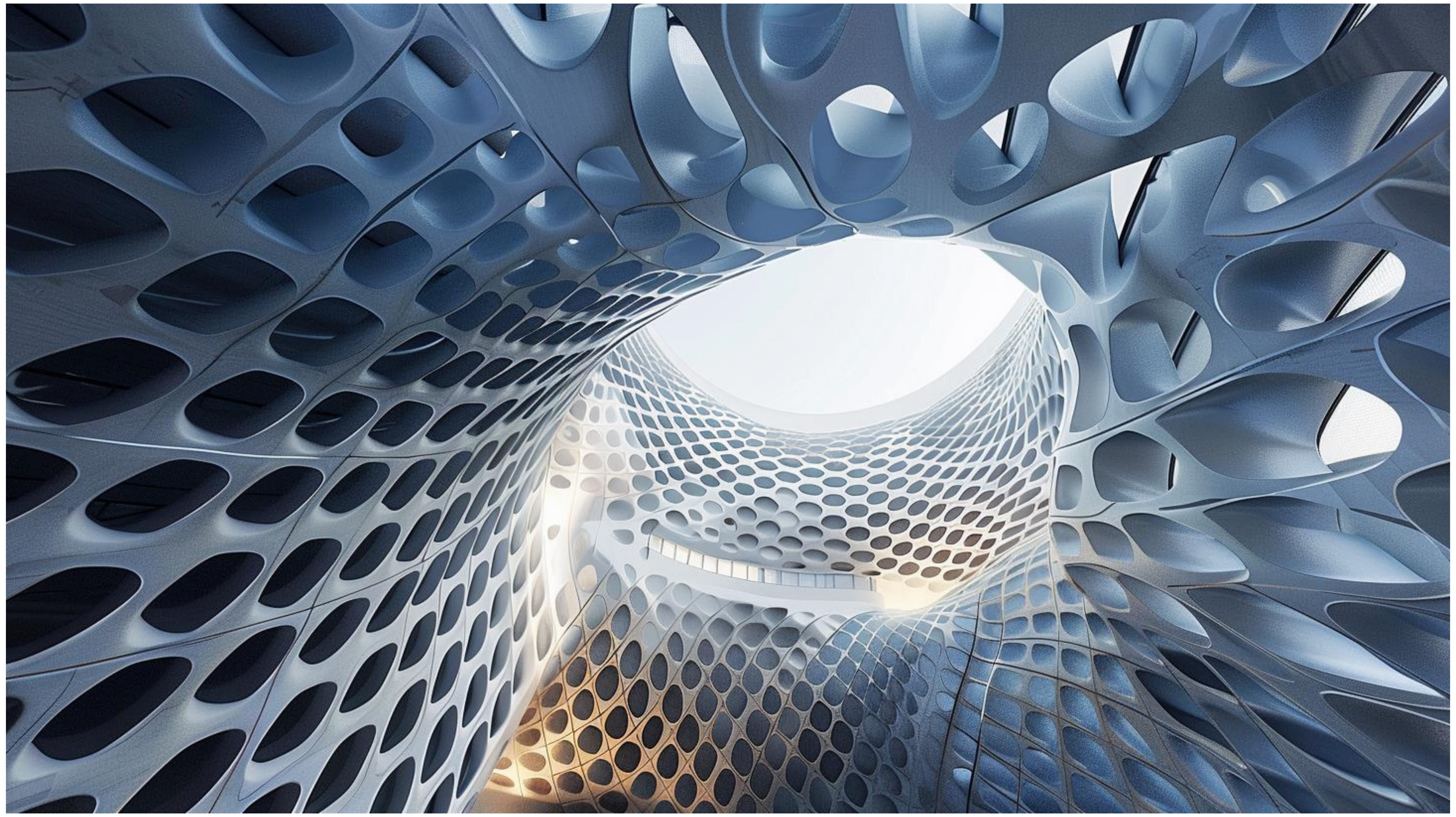


Figure out the metagame and play!

Threat-Informed Defense is the systematic application of a deep understanding of adversary tradecraft and technology to improve defenses.

Threat landscape defines the cyber threat actors to care about.

The cyber threat actors define the tactics, techniques and procedures to care about.

The tactics, techniques and procedures define detection use cases – Adversary tradecraft in threat informed defence

The business, technical and risk context define detection use cases – Technology in threat informed defence

The detection use cases defines the specific fields in the logs you need to onboard to your detection tools.

You have a methodology for protecting your web application!