APTs & CVEs & TTPs, OH MY!

LOST IN THE CTI WILDERNESS

Micah VanFossen

AGENDA

INTELLIGENCE LIFECYCLE

CYBER THREAT INTELLIGENCE (CTI) 101

TYPES OF CTI

THREAT MODELING

CTI RESOURCES

BETTER CTI COLLECTION/PROCESSING

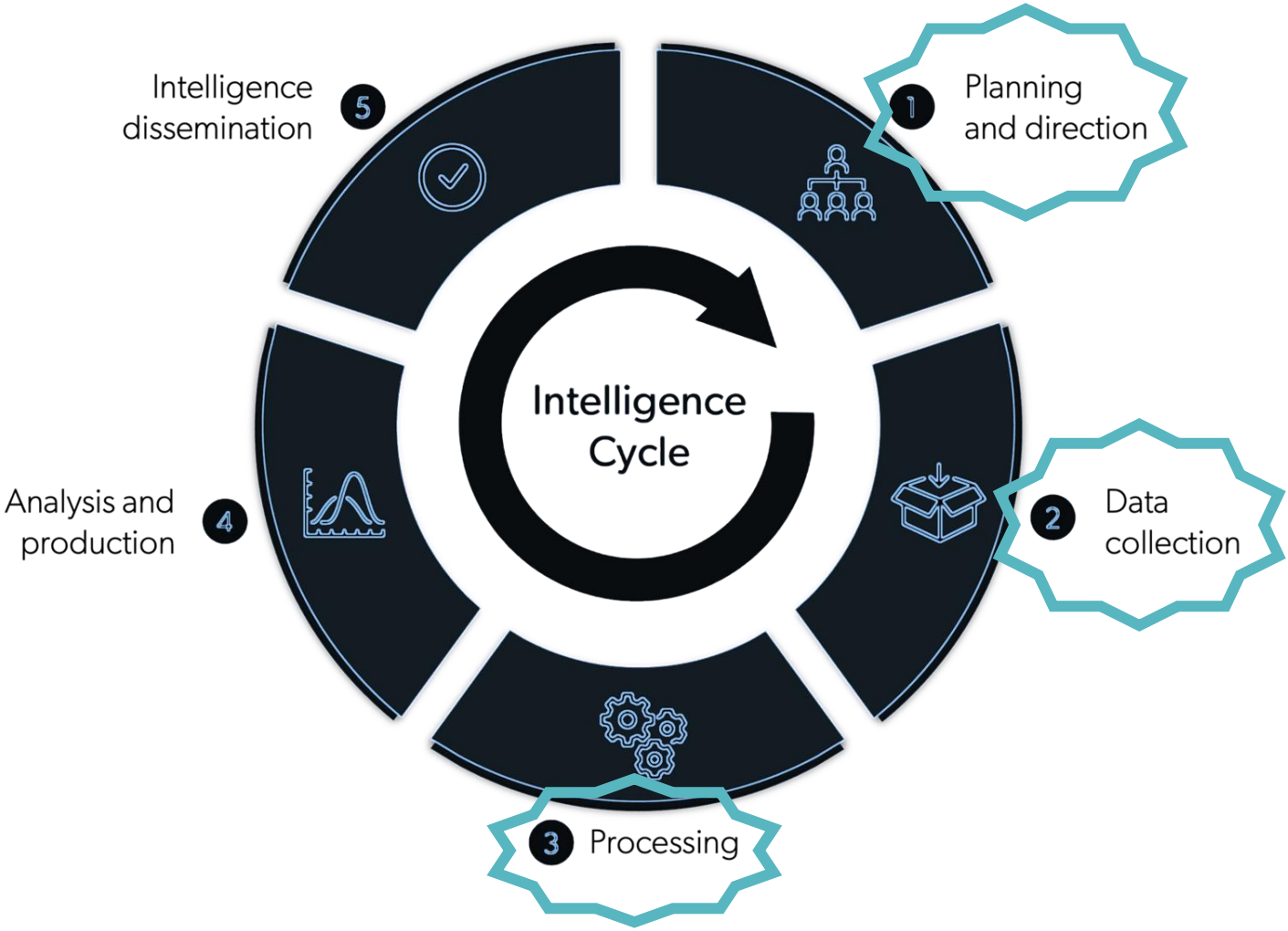
WAYS TO OPERATIONALIZE CTI

INTEL ON MYSELF

- 5 years in cybersecurity
- *Security & Data Analytics Engineer* - Focused on data normalization, transformation, and visibility, CTI, detections, threat hunting
- Too many certs (24), ok amount of degrees (2)
- SIII Cyber Games program
- Blog focused on SecOps - https://purplevan.substack.com/
- TID Ecosystem - https://start.me/p/X25q7l/threat-informed-defense-ecosystem

INTELLIGENCE LIFECYCLE

DATA -> IMPACT

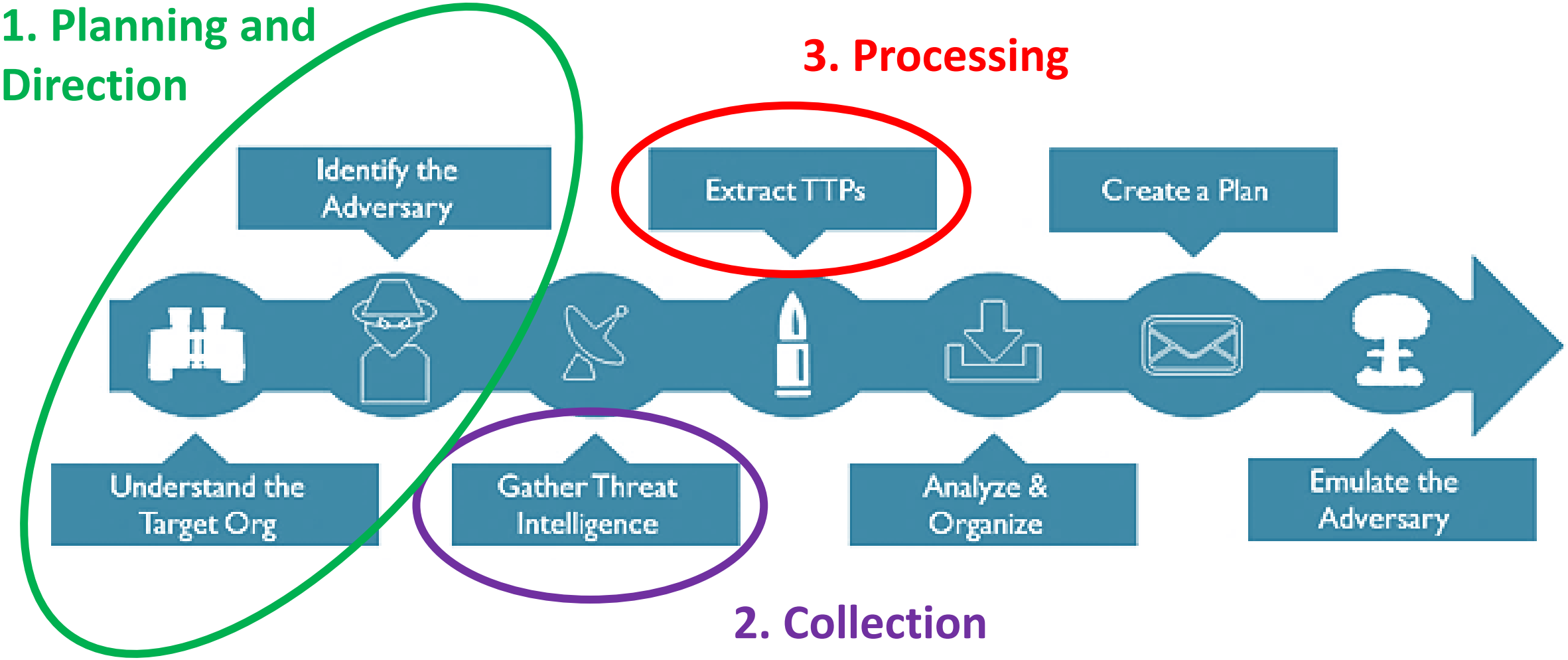


CYBER THREAT INTELLIGENCE 101 – SO WHAT?

- Purpose: Drive decisions and reduce risk/uncertainty
- Method: Utilize evidence-based knowledge, context, indicators, capabilities, and behaviors of a threat to assess how that may impact the organization and tie it to defensive actions

1. Clear BLUF, concise reports
2. Indicators/Observables – STIX, YARA, SIGMA, IOCs - what you add to security stack
3. Recommendations that are actionable (block, hunt, patch, mitigate)
4. Collect data -> Conduct analysis -> Influence security decisions with data (now it's "intel")

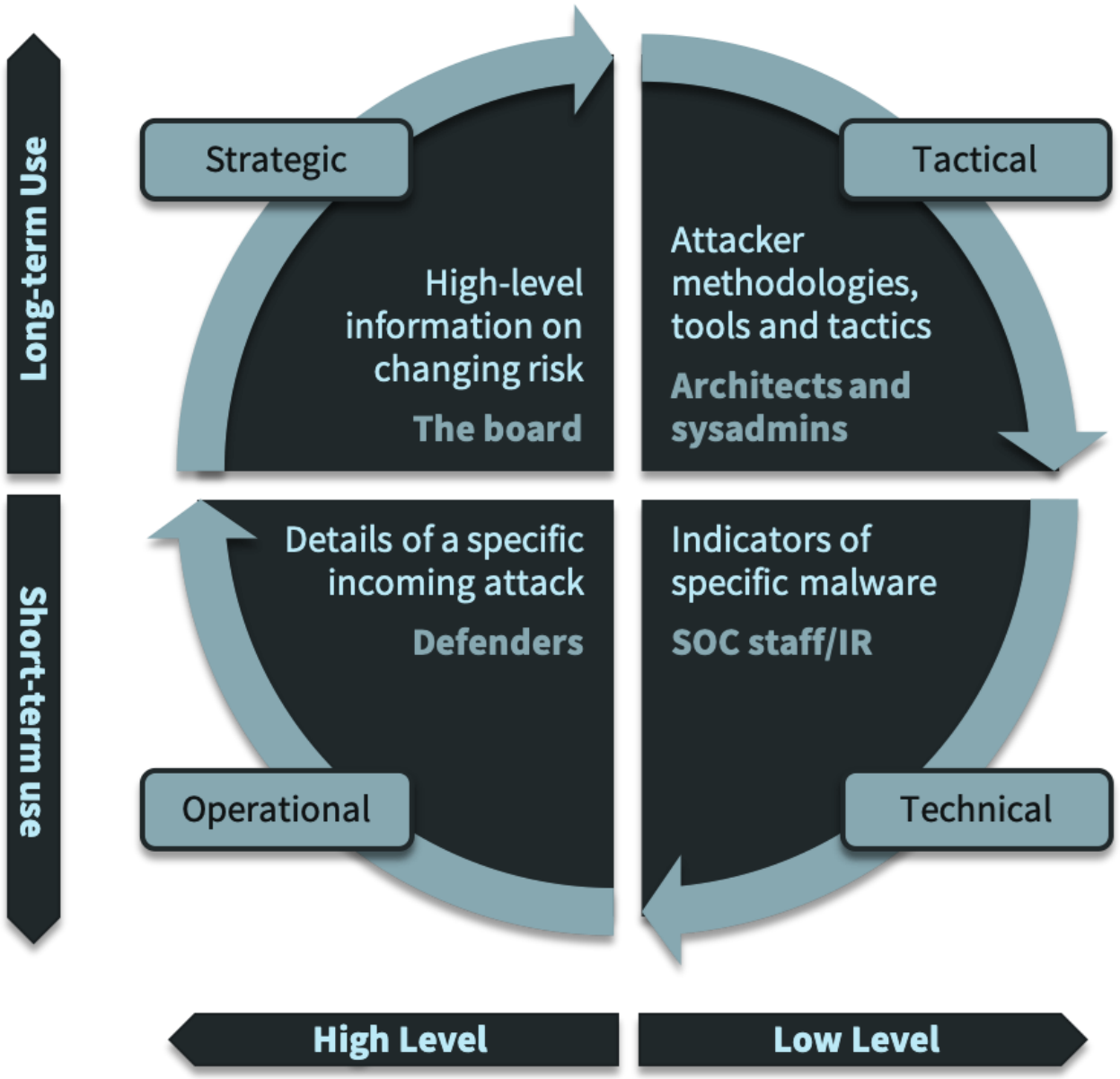
WORKFLOW



Katie Nickels and Cody Thomas presentation: "ATT&CKing the Status Quo: Threat-Based Adversary Emulation with MITRE ATT&CK"

TYPES OF CTI

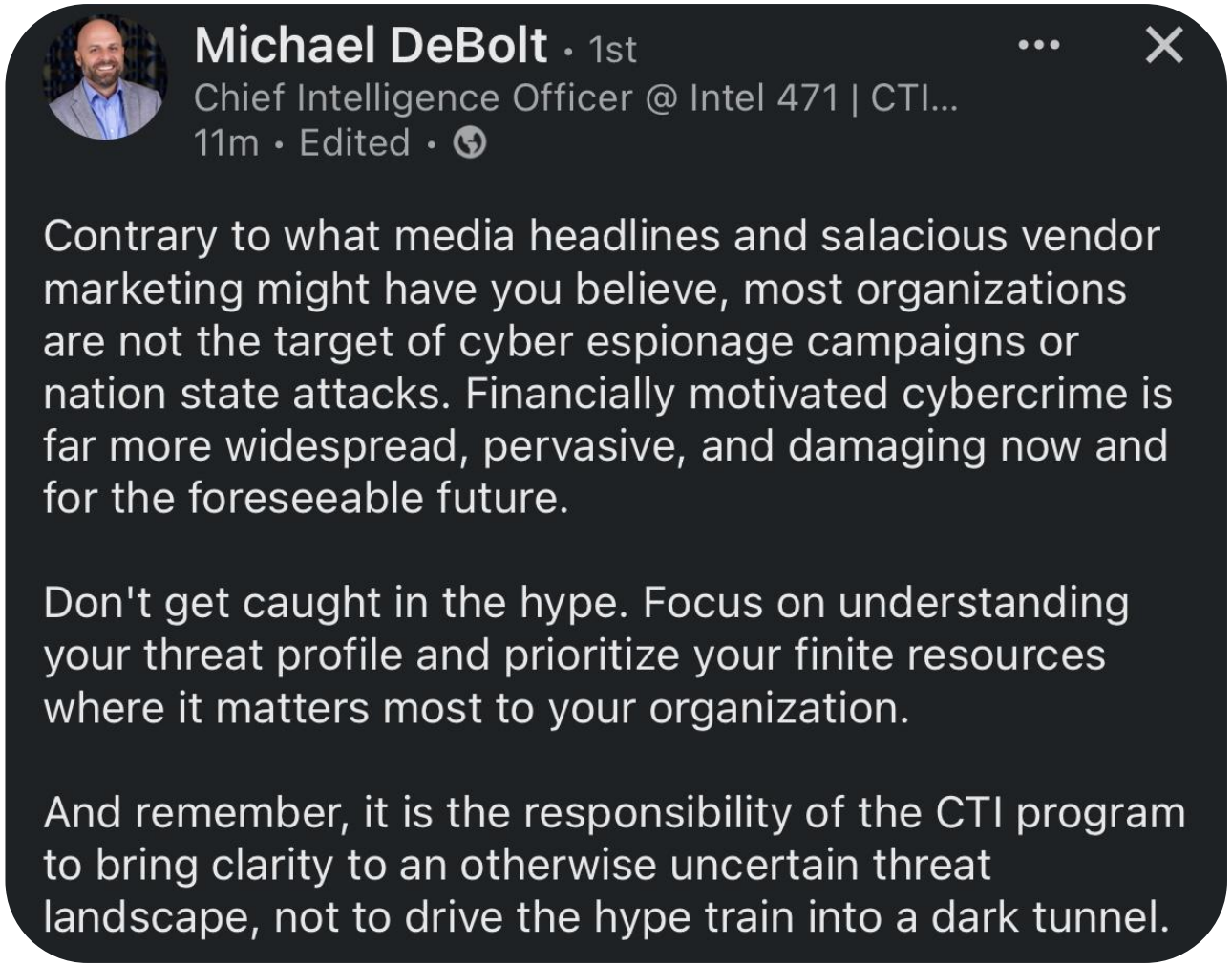
WHO DID WHAT TO WHOM?



https://www.securnite.com/index.php/onepress_service/cyber-threat-intelligence/

PLANNING & DIRECTION

Aims to identify or discover consumer intelligence requirements



CTI "BRINGERS OF CLARITY"

- Avoid hype
- Identify useful/relevant information
- NOT an IOC feed
- Pre and post compromise
- Learn biases

USING A THREAT MODEL

Prioritize threats	Map Prioritized Threats to Techniques	Identify Detection Gaps	Fill Detection Gaps
• Who cares about what you do, what you have, where you do it?	• What do they use, act, work (Pyramid of Pain)	• What coverage exists, what risks exist?	• Reduce risk and blind spots

WHAT MATTERS TO YOU

Security teams:

1. Overwhelmed by amount of information about threat actors, malware, tools, and vulnerabilities
2. Inability to effectively prioritize threats
3. No clear prioritization = every potential threat is equally urgent
4. Teams cannot focusing on the most critical risks
5. Attempt to defend against every possible threat -> vulnerable to the ones that are truly most likely to impact them

- Threat Intelligence “help teams become more strategic, understand which threats are targeting them, and figure out how to defend against them”
- Most organizations struggle to use Threat Intelligence to deliver on this promise

https://www.snapattack.com/threat-profiles-figuring-out-which-threats-matter/

PRIORITIZE THREATS

- **Industry** – "Which threat actors are targeting other organizations in our industry? How have they done it?"
- **Region** – "Which threat actors have targeted organizations in our region?"
- **Technology** – "Are there certain technologies used by our organization that make us more of a target for certain threats?"
- **Motivations** – "Is the actor financially motivated and looking to deploy ransomware? Or are we worried about a targeted attack, theft of IP, etc.?"
- **Recency** – "Is this threat new and actively used? When was it last observed?"
- **Relevance** – "How likely is this to impact our organization?"
- **Prevalence** – "How commonly are those tactics used?"
- **Impact** – "If it were to impact us, how bad would the damage be?"

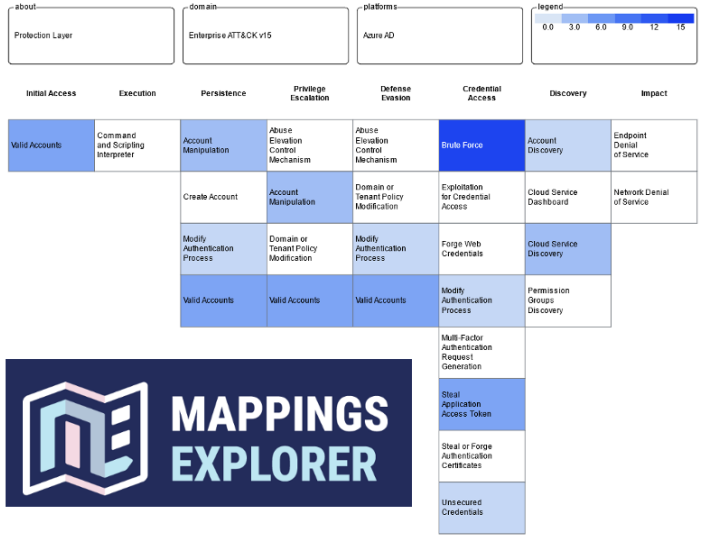
https://www.snapattack.com/threat-profiles-figuring-out-which-threats-matter/

- What threat actors commonly target my industry or size? (Intent)
- What tactics, techniques, & procedures are used by these groups? (Capability)
- What are our business-critical functions, information, and systems that we must protect? (Crown Jewels)

ATT&CK MAPPING

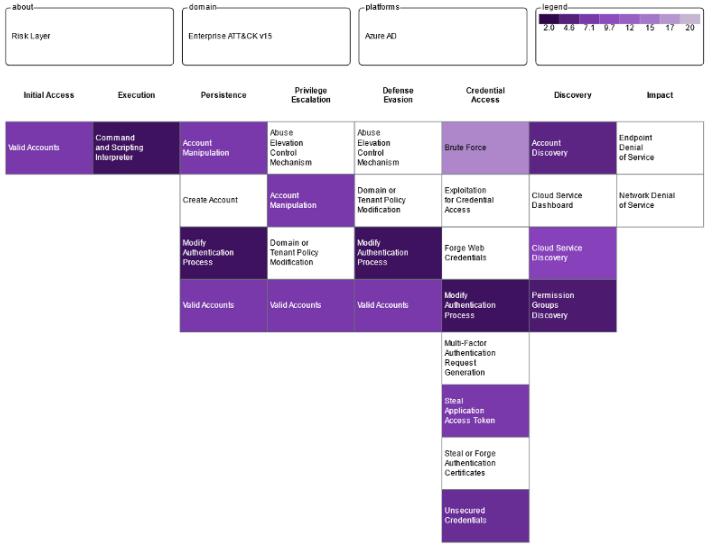
Threat

Defense



MAPPINGS EXPLORER

Risk



Mission Decomposition	System Decomposition	Vulnerability Identification	Cyber Threat Intelligence	Defense & Risk Analysis	Mitigation & Remediation	Monitoring Analysis & Evaluation

THREAT MODELING WITH ATT&CK

https://medium.com/mitre-engenuity/turn-your-threat-model-to-supermodel-with-att-ck-a6dfaa6787c2

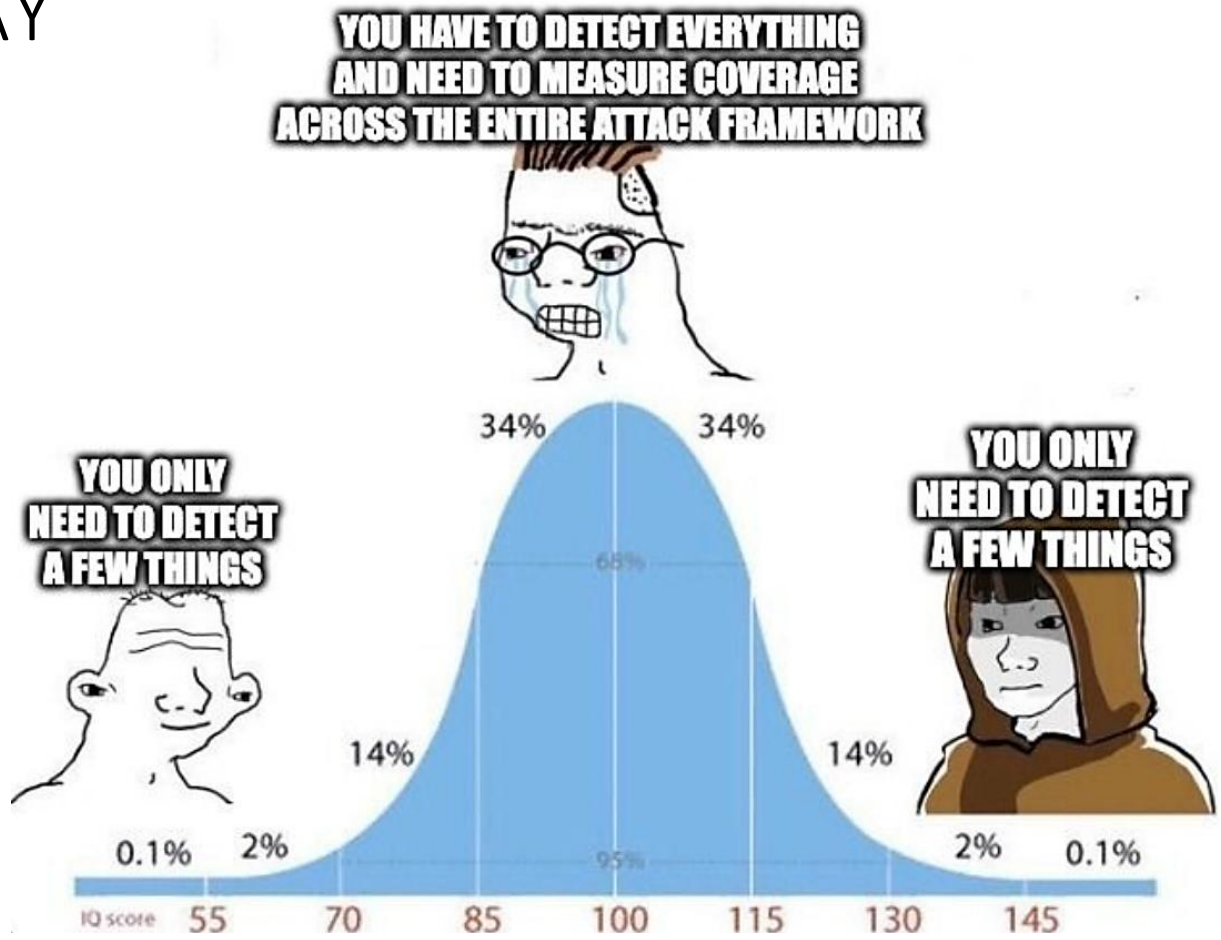
ATT&CK MAP THE RIGHT WAY

Detect important things

Don't play bingo with ATT&CK

- You'll never fully cover T1071.001 App Layer Protocol - Web Protocols

Map to find holes and close clear visibility gaps, not to get all 'green' boxes



COLLECTION

Information and data is gathered from various sources to meet identified intelligence requirements

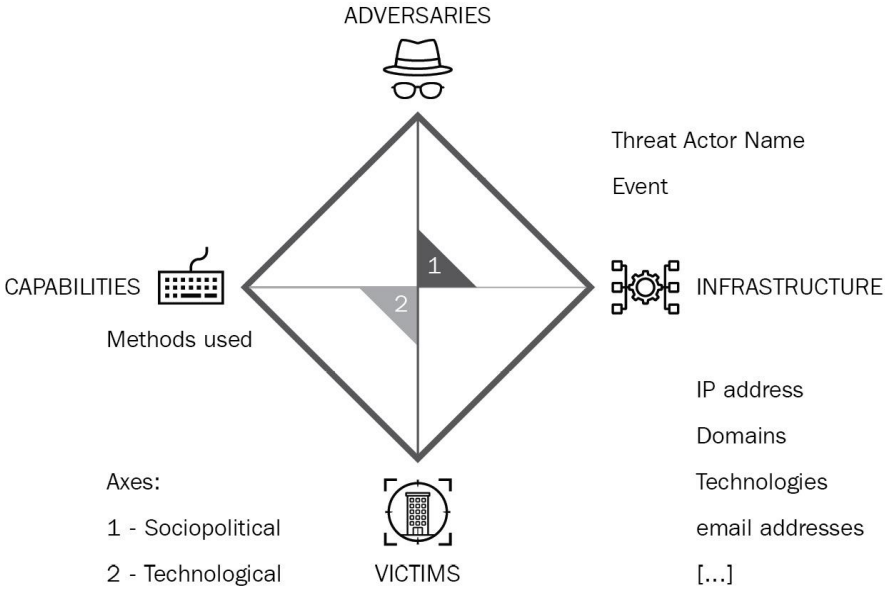
HOW/WHAT?

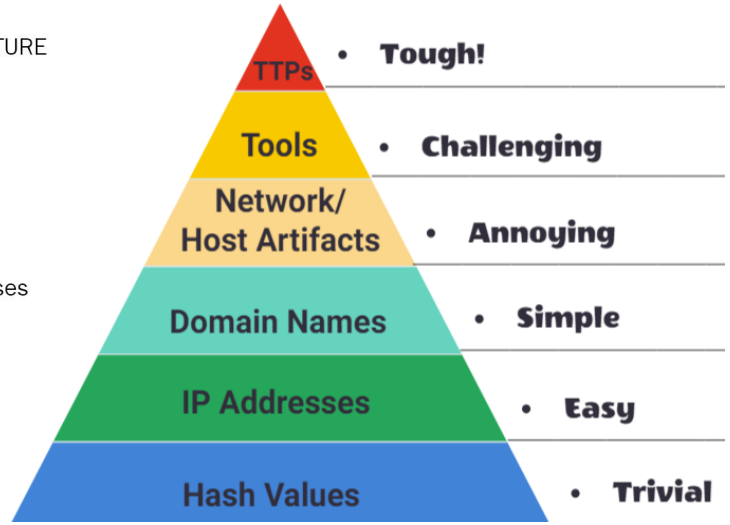
VULNERABILITY INTELLIGENCE
(CVES)

ADVERSARY INTELLIGENCE
(TTPS, APTS)

GOOD CTI SOURCES

What?





Where?

Threat Actor Reports

DFIR / Campaign Reports

Annual Trends

Feedly, Start.me - RSS feeds

From FREE

CISA / FBI - Joint Alerts/Advisories

MITRE ATT&CK

DFIR Report

Palo Alto Unit 42

TrustedSec

Google T.A.G

CrowdStrike

Sophos

Huntress

Red Canary

Recorded Future

Intel 471

Zero Fox

Wiz

INITIAL ACCESS

Top initial access vectors:

- Public Facing Vulnerability Exploitation
- VPN Abuse / Brute Forcing
- Phishing
- Web – malvertising, fake browser updates, SEO poisoning
- Valid Account/Credential Abuse
- Misconfigurations

Sources:

Red Canary - Threat Detection Report 2025

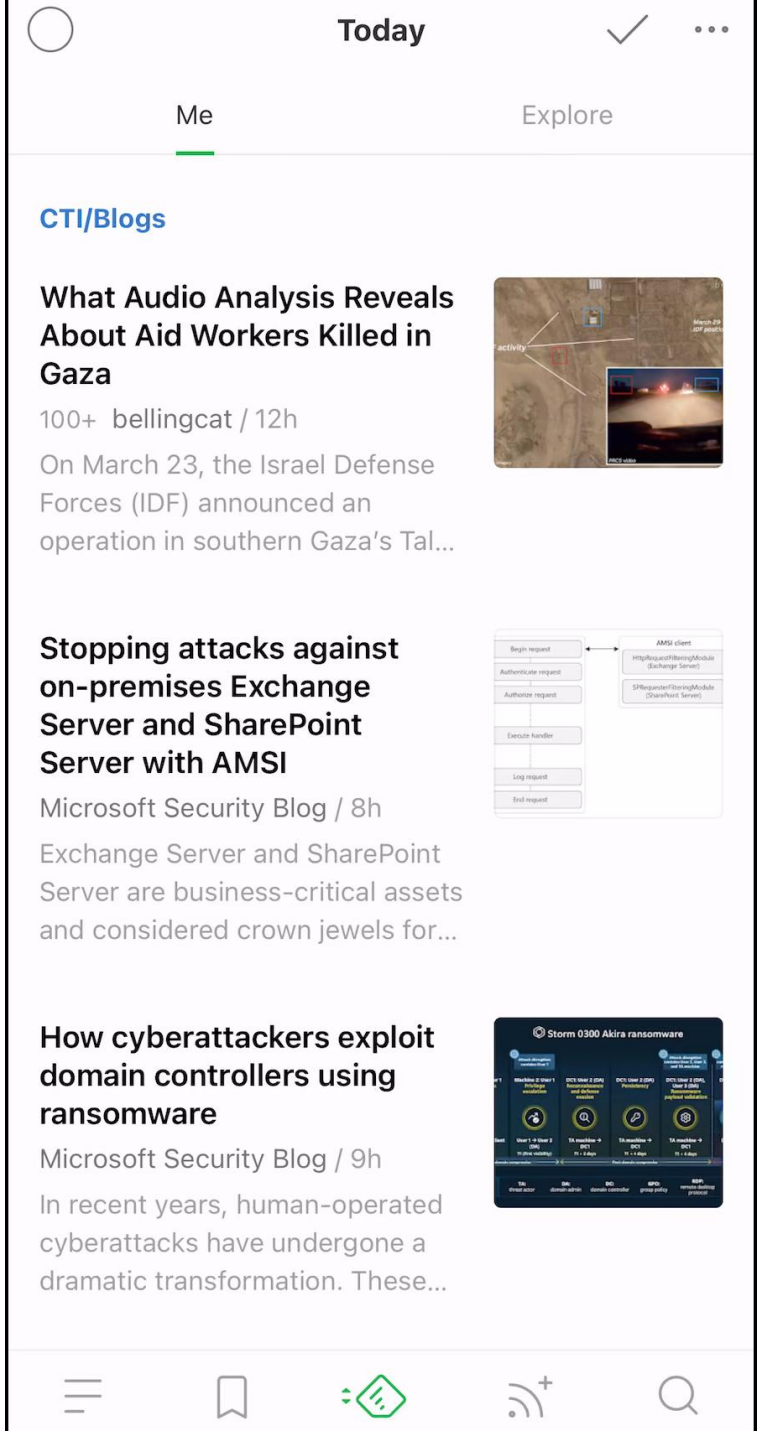
IBM X-Force - Threat Intelligence Index 2024

CISA - Advisory 2022

WNE Security - Most Common attack vectors for initial access 2025

Sophos – Active Adversary Report 2025


feedly


Today
Me
Explore
CTI/Blogs
What Audio Analysis Reveals About Aid Workers Killed in Gaza
100+ bellingcat / 12h
On March 23, the Israel Defense Forces (IDF) announced an operation in southern Gaza's Tal...
Stopping attacks against on-premises Exchange Server and SharePoint Server with AMSI
Microsoft Security Blog / 8h
Exchange Server and SharePoint Server are business-critical assets and considered crown jewels for...
How cyberattackers exploit domain controllers using ransomware
Microsoft Security Blog / 9h
In recent years, human-operated cyberattacks have undergone a dramatic transformation. These...
Storm 0300 Akira ransomware

RSS / TLDR

Risky.Biz (every 2 days)
https://news.risky.biz/

Metacurity (daily)
https://www.metacurity.com/

TLDR Infosec (daily)
https://tldr.tech/infosec

Example

Breaches, hacks, and security incidents

Moroccan government leaks: Algerian hacker group JabaRoot DZ has leaked data from two Moroccan government agencies—the Ministry of Economic Inclusion and the National Social Security Fund (CNSS). [*Additional coverage in Yabiladi*]

Dutch government breach: The Dutch government is investigating a data breach of three ministries. The incident is impacting the Ministry of the Interior, the Ministry of Economic Affairs, and the Ministry of Climate and Green Growth. The government has not disclosed the nature of the incident. [*Additional coverage in BNR*]

NetJets breach: Hackers have breached and stolen customer information from private business jet company NetJets. The hack took place last month after the attacker phished an employee. The company says only a "*very small number of owners*" were impacted. NetJets is owned by Warren Buffett's Berkshire Hathaway company. [*Additional coverage in Bloomberg*]

DGO hack: German intelligence is probing a suspected Russian hack of the German Association for East European Studies (DGO). [*Additional coverage in DW*]

Sensata ransomware attack: Industrial sensor maker Sensata has disclosed a major ransomware attack that has impacted operations, such as "*shipping, receiving, manufacturing production, and various other support functions.*"

GenNomis leak: A South Korean AI nudify and face-swapping service has left a database exposed on the internet without a password. The database contained over 93,000 images generated through the service. According to the researcher who found it, the database allegedly belonged to a company named GenNomis by AI-NOMIS and contained

START.ME SITES

infosecn1nja | Cyber Threat Intelligence | startme | infosecn1nja

Radware Threat Map

radware
Live Threat Map
Powered by Radware's Threat Intelligence
RE...
Filter Attacks
UNDER ATTACK
CONTACT SALES
Timeline
Data
Contact Us
Cookie Preferences

Google Cloud (Mandiant)

- Windows Remote Desktop P...
- Suspected China-Nexus Thre...
- DPRK IT Workers Expanding ...
- BitM Up! Session Stealing in ...
- Ghost in the Router: China-...

1/10

The DFIR Report

- Fake Zoom Ends in BlackSuit...
- Confluence Exploit Leads to ...
- Cobalt Strike and a Pair of S...
- The Curious Case of an Egg-...
- Inside the Open Directory of...

1/7

Top 10 Ransomware Victim...

Top 10 Ranwomware Grou...

Kaspersky

- GOFFEE continues to attack ...
- Attackers distributing a mine...
- How ToddyCat tried to hide ...
- A journey into forgotten Nul...
- TookPS: DeepSeek isn't the ...

1/10

Crowdstrike

- CrowdStrike Wins Google Cl...
- April 2025 Patch Tuesday: O...
- CrowdStrike Secures AI Deve...
- How to Navigate the 2025 I...
- Kubernetes IngressNightmar...

1/10

Latest News

- Ransomware Attack Preventi...
- Justice Department Impleme...
- Microsoft rolling Windows R...
- Patient data leaked from cyb...
- US Defense Department can...

1/20

Recent Ransomware Victims

- Lynx has just published a...
- Termite has just publishe...
- Play has just published a...
- Akira has just published ...
- Lynx has just published a...

1/10

Cyber Threat Report

- Lanskap Keamanan Siber Ind...
- ACSC Annual Cyber Threat R...
- CrowdStrike Global Threat R...
- M-Trends

MSRC & MSTIC

- Stopping attacks against on-...
- Exploitation of CLFS zero-da...
- Threat actors leverage tax se...

Unit 42

- How Prompt Attacks Exploit ...
- OH-MY-DC: OIDC Misconfig...
- Evolution of Sophisticated P...

Red Team Blogs

- dAWShund – framework to ...
- iOS 18.4 - dlsym considered ...

Latest Ransomware Group

← Vulnerability Database

Explore Vulnerabilities

Search by CVE ID or technology

Severity | Vendor advisory | Affected technologies | Published at | Has fix | Has public exploit | Has CISA Kev exploit | Is high profile threat

Showing 158 results

CVE ID	Severity	Score	Technologies	Component name	CISA KEV exploit	Has fix	Published date
CVE-2025-1974	CRITICAL	9.8	Ingress NGINX ...	k8s.io/ingress-ngi... +1	No	Yes	Mar 24, 2025
CVE-2023-25610	CRITICAL	9.3	FortiOS +2	cpe:2.3:o:fortinet:f...	No	Yes	Mar 24, 2025
CVE-2025-30154	HIGH	8.6	GitHub	N/A	Yes	No	Mar 19, 2025

CVE-2023-25610: FortiOS vulnerability analysis and mitigation

High-profile threat • High-profile threat • High-profile threat • High-profile threat • High-profile threat

Overview | CVSS Information

9.3
Score

Published March 24, 2025

Severity CRITICAL

CNA Score 9.8

High-profile Vulnerability Yes

Affected Technologies

FortiOS

Fortinet FortiProxy

+1 See all ›

Has Public Exploit No

Has CISA KEV Exploit No

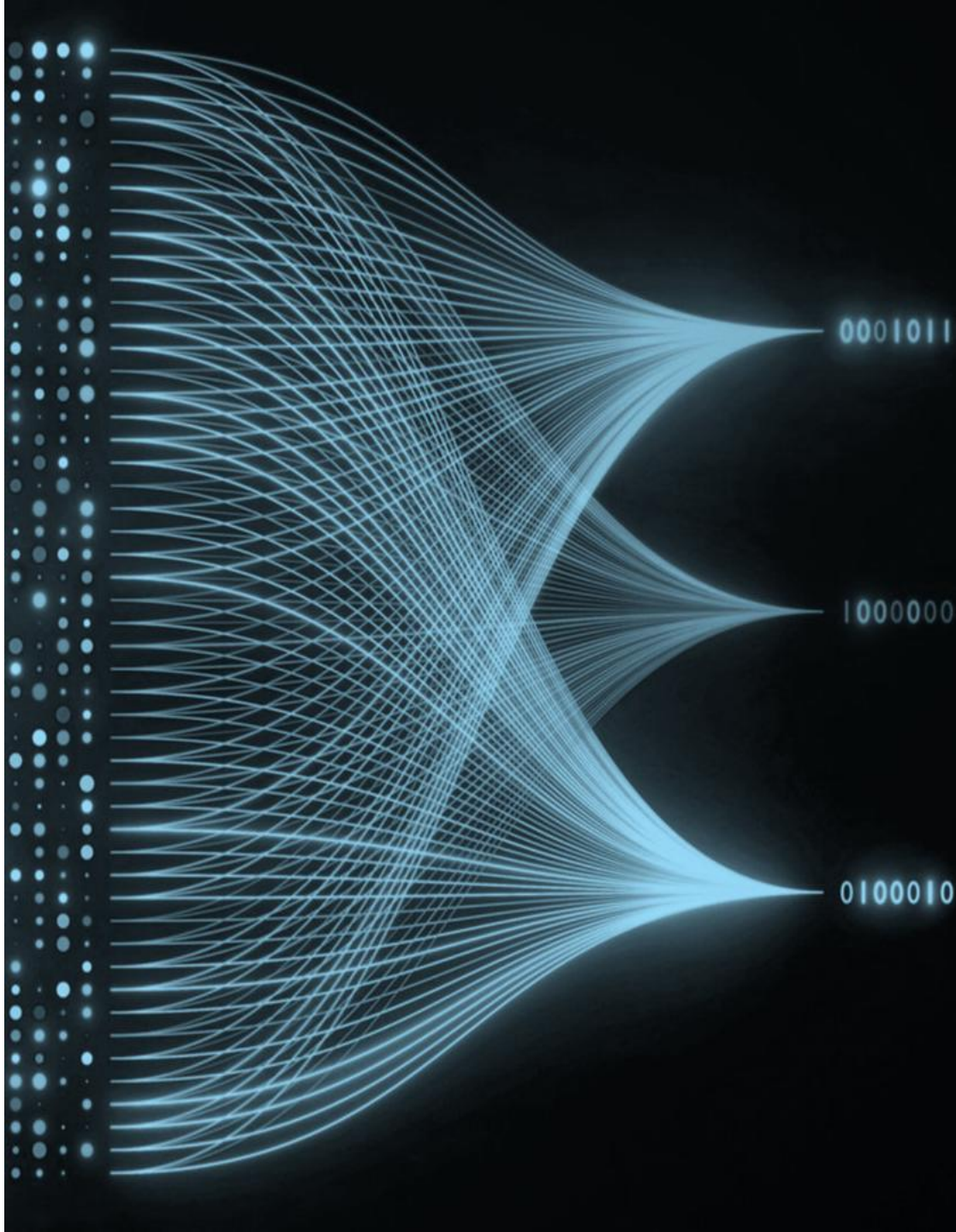
Overview

A critical buffer underwrite vulnerability (CVE-2023-25610) was discovered in the administrative interface of multiple Fortinet products, including FortiOS, FortiManager, FortiAnalyzer, FortiWeb, FortiProxy, and FortiSwitchManager. The vulnerability was internally discovered by Fortinet and disclosed on March 7, 2023. This security flaw affects multiple versions of these products and could allow remote unauthenticated attackers to execute arbitrary code or perform denial-of-service attacks via specially crafted requests (Fortinet PSIRT).

Technical details

PROCESSING

- Data is cleaned (remove duplicates, inconsistencies, irrelevant info)
- Data is transformed into formats suitable for analysis (STIX 2.1)
- Data is enriched with additional context and metadata



TOOLS

RAG

Automation

CTID TRAM – TTP mapping

CVE Notifier – alert of new cve

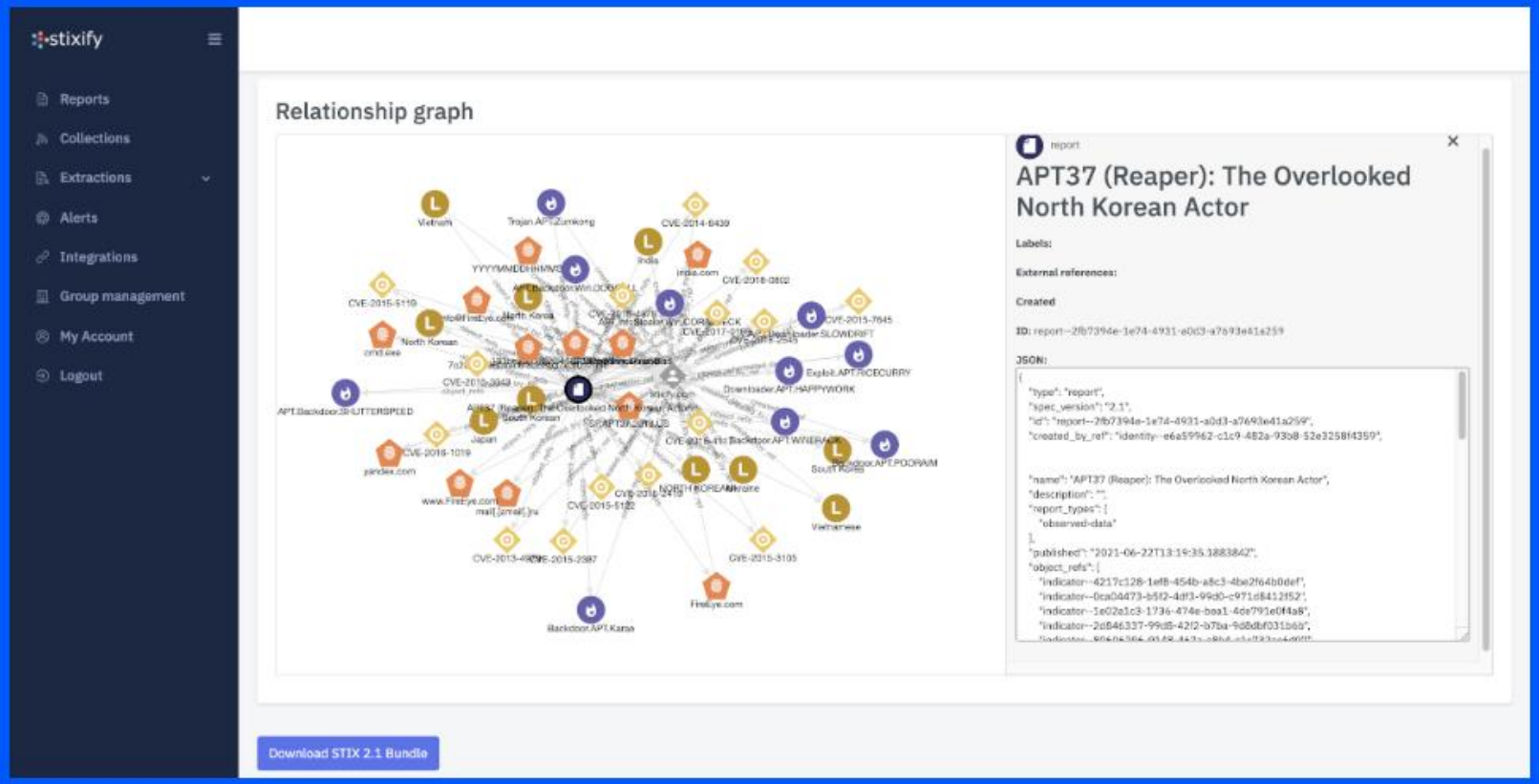
DOGESEC - multiple

OPENCTI – collect, knowledge base, and graph analysis

Feedly – TTP/IOC extract/export, AI

DOGESEC
much intelligence. wow.

ABOUT BLOG SUPPORT COMMUNITY



We build software for cyber threat intelligence analysts.

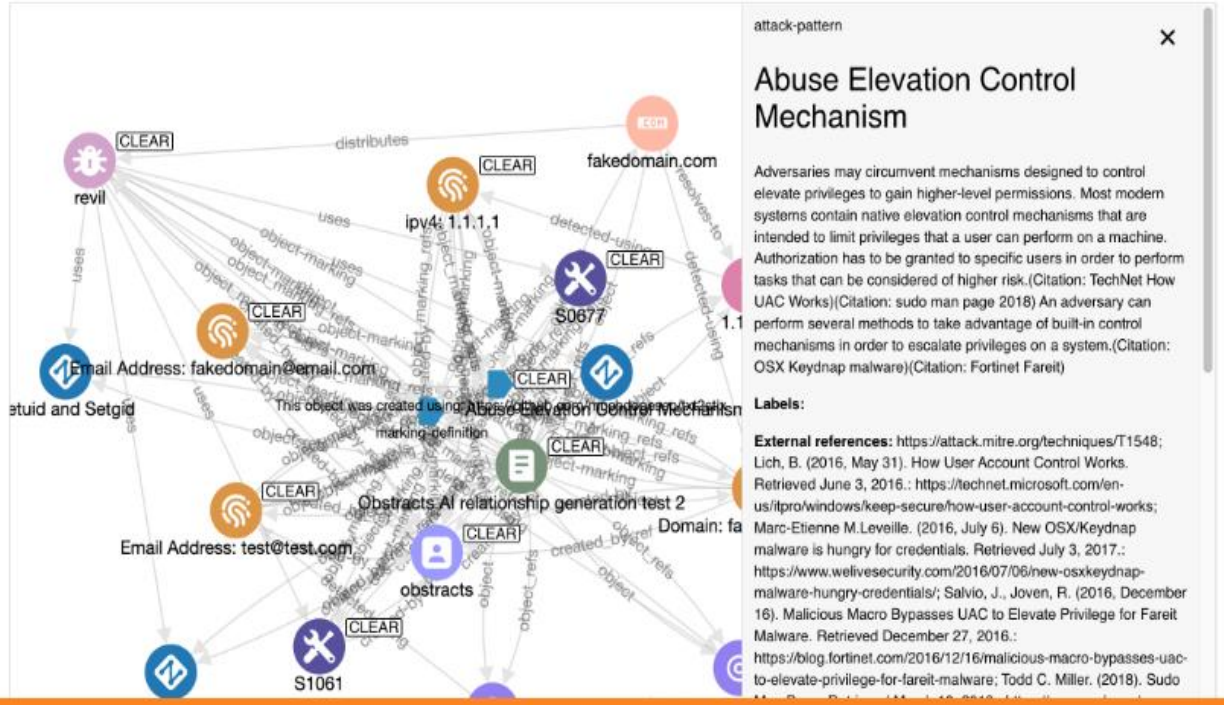
obstracts

SIGN UP SIGN IN

obstracts

- Latest Posts
- Feeds
- Intel Search
- API Docs
- TAXII API Docs
- Team Management
- Support

Extraction Graph



Turn any blog into structured threat intelligence

Search IoCs and TTPs across the blogs you subscribe to.

vulmatch

SIGN UP SIGN IN

vulmatch

- Vulnerabilities
- Products
- KEV
- EPSS
- API Docs
- TAXII API Docs
- Team Management
- Support

CVE List

Use this page to search and filter vulnerabilities. Click on a CVE ID to find out more about it.

CVE ID | CPE ID(Accepts partial) | CWE ID

ATT&CK ID | Base score min | Capec ID

☐ Only show CVEs vulnerable to products in my SBOM

FILTER

Matching Vulnerabilities

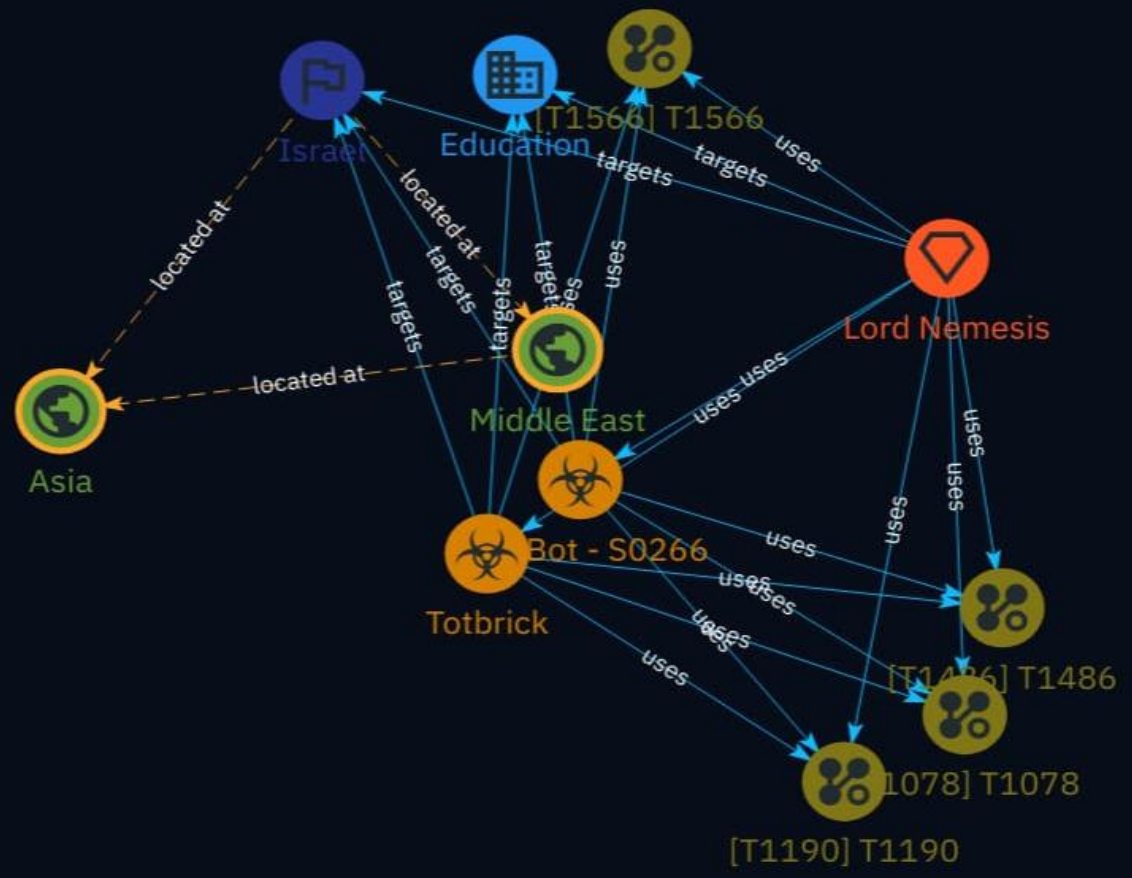
CVE ID	CVE Description	Date Published	Base Score
CVE-2024-56803	Ghostty is a cross-platform terminal emulator. Ghostty, as allowed by default in 1.0.0, allows attackers to modify the window title via a certain character escape sequence and then insert it back to the command line in the user's terminal, e.g. when the user views a file containing the malicious sequence, which could allow the attacker to execute arbitrary commands. This attack requires an attacker to send malicious escape sequences followed by convincing the user to physically press the "enter" key. Fixed in Ghostty v1.0.1.	2024-12-31	5.1
CVE-2024-56063	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDeveloper Essential Addons for Elementor allows Stored XSS.This issue affects Essential Addons for Elementor: from n/a through 6.0.7.	2024-12-31	6.5
CVE-2024-56062	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Royal Royal Elementor Addons allows Stored XSS.This issue affects Royal Elementor Addons: from n/a through 1.3.987.	2024-12-31	6.5
CVE-2024-13085	A vulnerability, which was classified as critical, has been found in PHPGurukul Land Record System 1.0. Affected by this issue is some unknown functionality of the file /admin/login.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2024-12-31	7.5
CVE-2024-	A vulnerability classified as critical was found in PHPGurukul Land Record System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/search-property.php. The manipulation of the argument searchdata leads to sql injection. The attack	2024-12-31	6.5

Straightforward vulnerability management

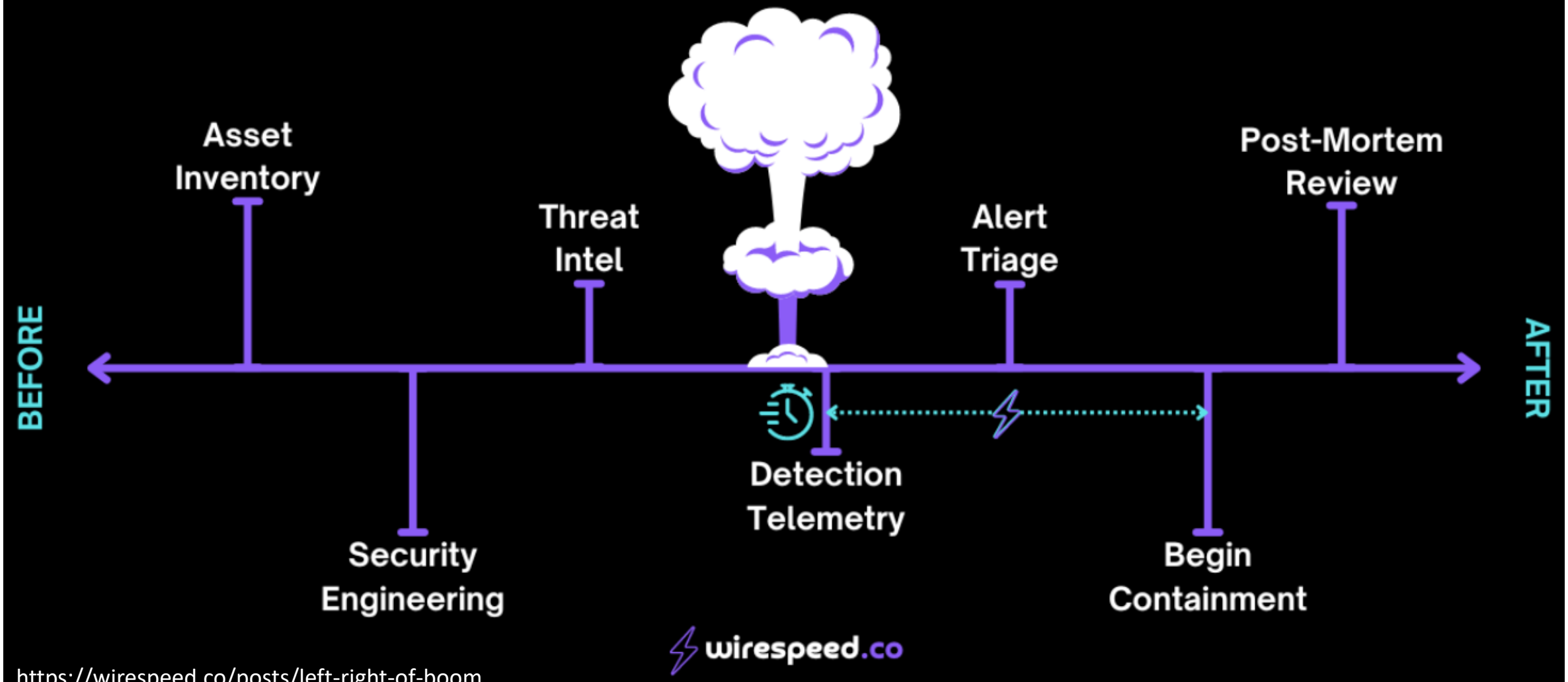
Know when software you use is vulnerable, how it is being exploited, and how to detect an attack.

Lord Nemesis Strikes: Supply Chain Attack on the Israeli Academic Sector

OVERVIEW | KNOWLEDGE | CONTENT | ENTITIES | OBSERVABLES | DATA

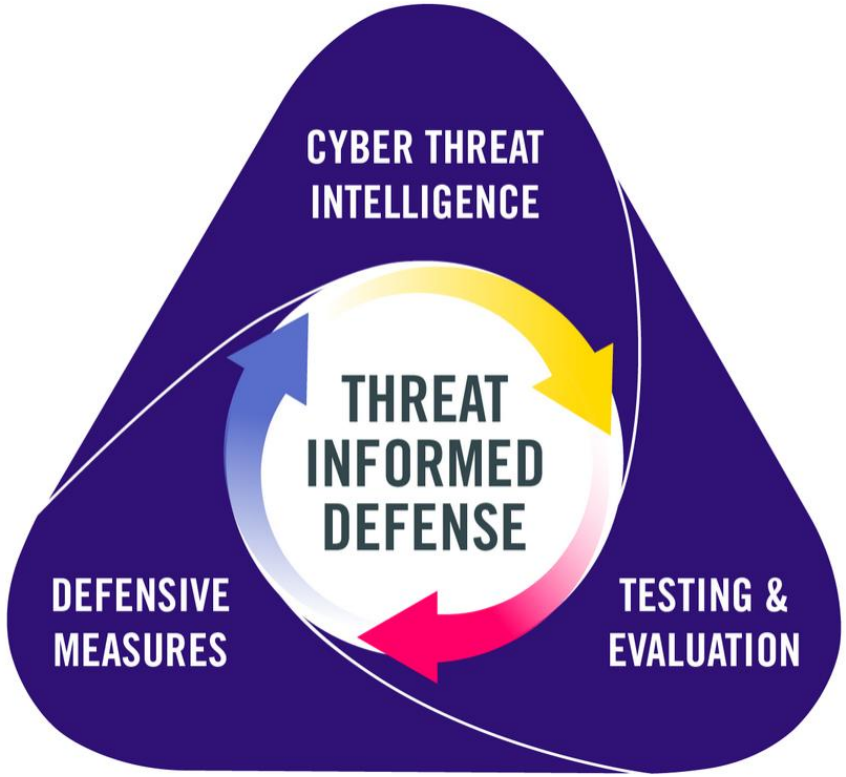


LEFT & RIGHT OF BOOM



https://wirespeed.co/posts/left-right-of-boom

ONWARD AND UPWARD



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

Threat Informed Defense - align defensive measures to real-world observations of adversary tradecraft

Cyber Threat Intel – Know the Adversary & Self

- Know the adversary, their objectives, behaviors, and their tactics/techniques/procedures (TTPs)
- Identify and prioritize most likely threats

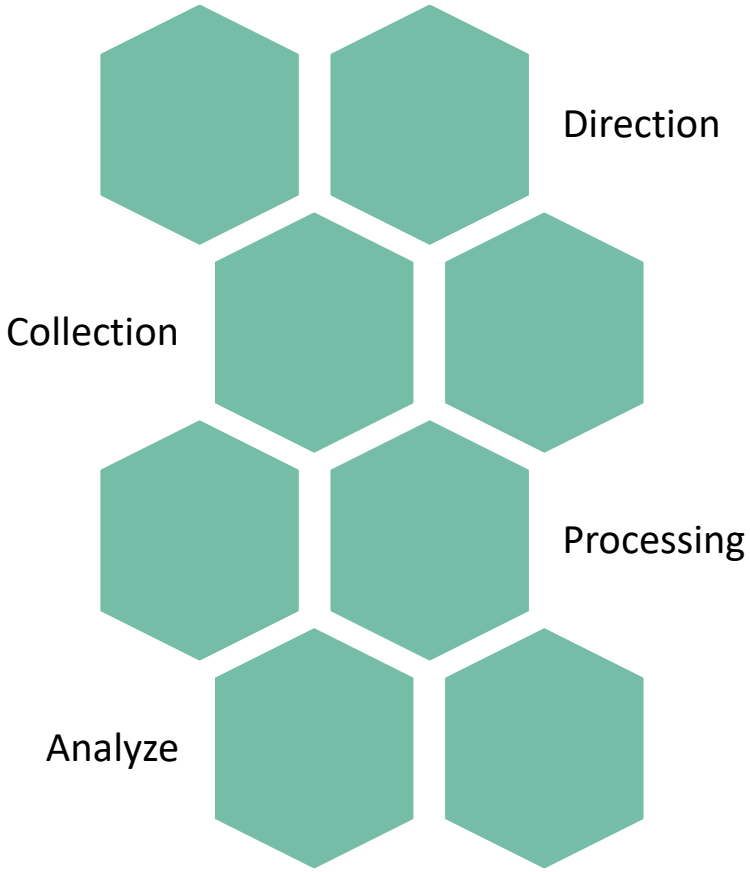
Testing and Evaluation – Learn and Improve

- Assess defenses by emulating real adversary TTPs
- Continuous validation of security controls with threat-led attack simulations of prioritized threats

Defense Measures – Proactively Defend

- Implement prevention, detection, and mitigation tailored to known threats based on data-driven analysis
- Evolve defenses as environment and threats change

FINAL TIPS & TAKEAWAYS



1. Gather PIRs and seek feedback
2. Identify what is best to track
3. Collect efficiently
4. Process properly and use automation
5. Bring clarity
6. Iterate

THANK YOU