Cyber Threat Intelligence: It’s not ***just*** about the Feeds

Iain Dickson
@wan0net

What will I be covering?

- What is Cyber Threat Intelligence?
- What data source types support a CTI capability?
- What are the Lockheed Martin Cyber Kill Chain and Diamond Model?
- What data is required to generate actionable CTI?
- How does Cyber Threat Intelligence Support Defensive Cyber Ops?

What is Cyber Threat Intelligence?

Threat **information** that has been aggregated, transformed, analysed, interpreted, or enriched to provide the necessary context for **decision-making** processes.

NIST 800-150 “Guide to Threat Information Sharing”

Threat, Vulnerability, and Risk

Threat

Any circumstance or event with the potential to adversely impact organizational operations, assets, or individuals.

×

Vulnerability

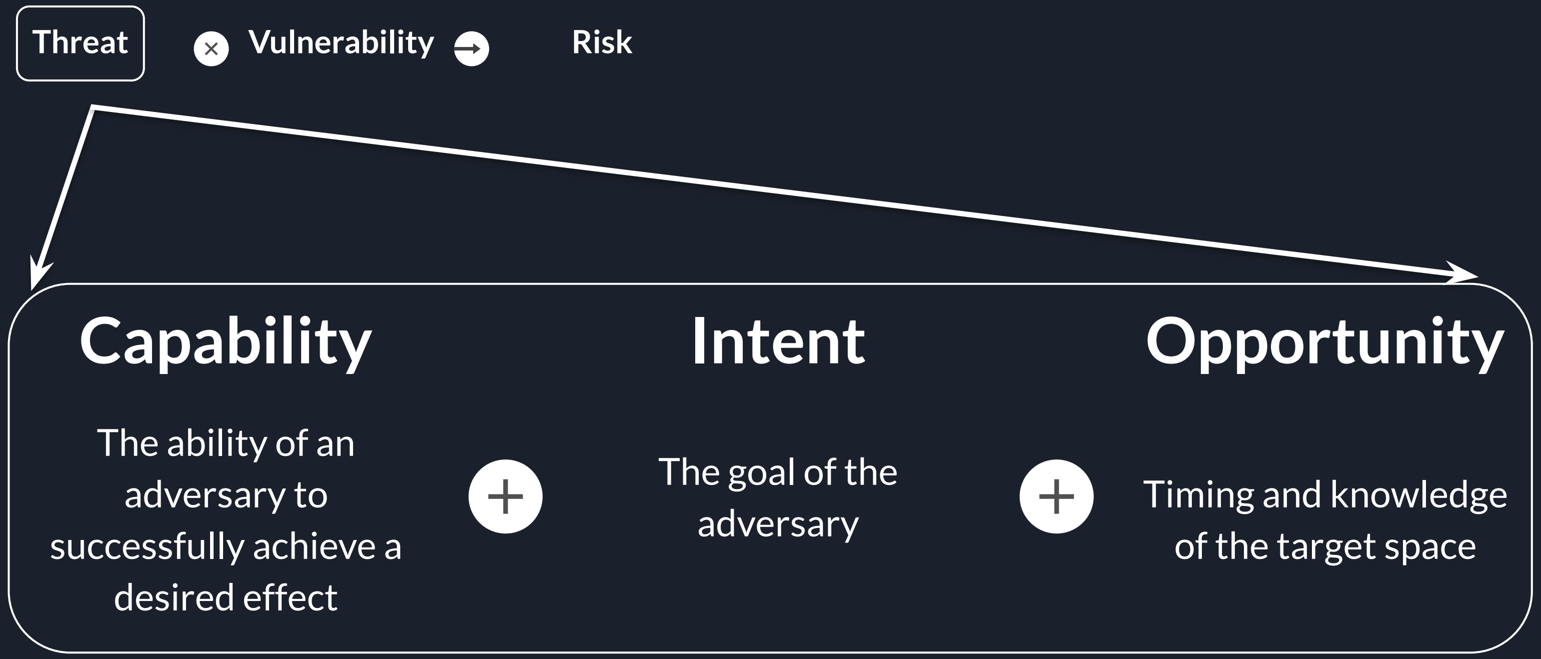
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered.

→

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event.

Capability, Intent, Opportunity



Threat × Vulnerability → Risk

Capability

The ability of an adversary to successfully achieve a desired effect

+

Intent

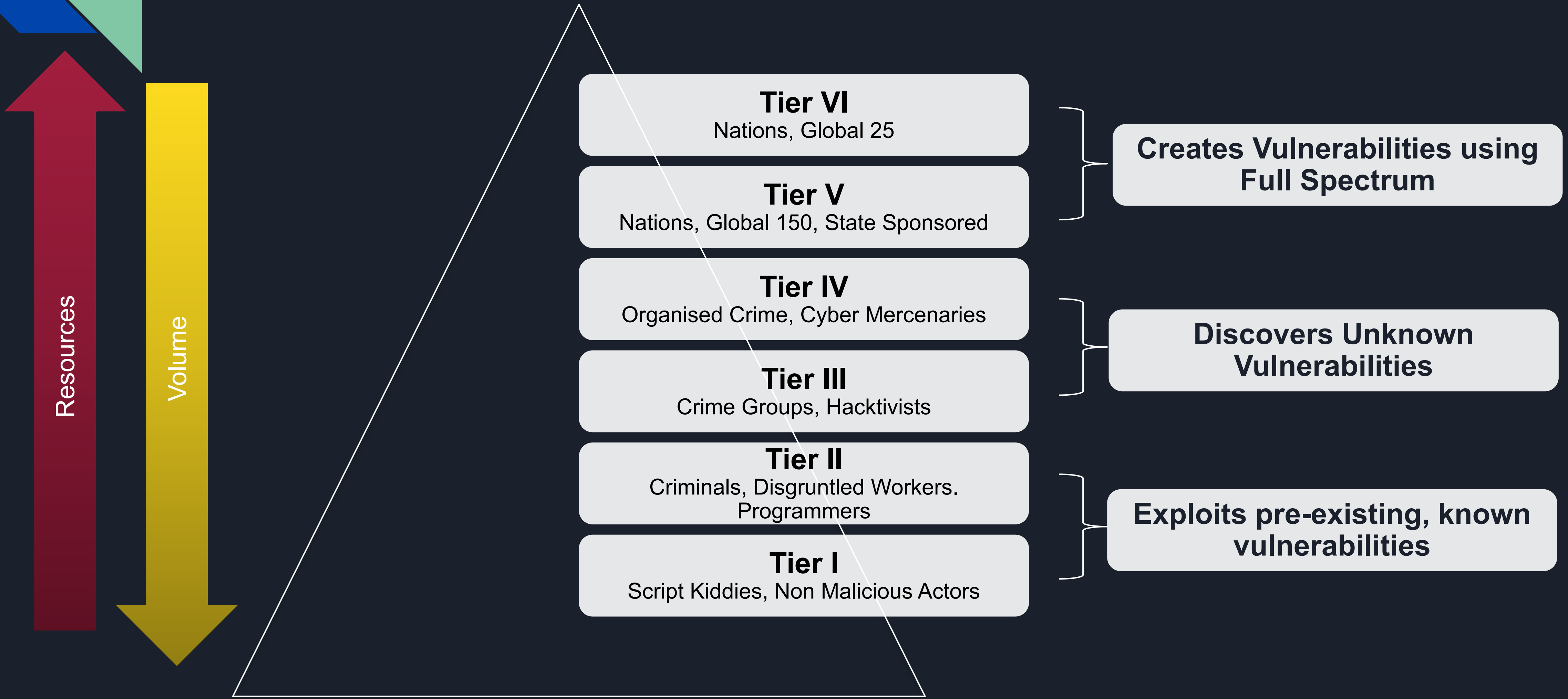
The goal of the adversary

+

Opportunity

Timing and knowledge of the target space

Threat Actor Tiers



Tier VI
Nations, Global 25

Tier V
Nations, Global 150, State Sponsored

Creates Vulnerabilities using Full Spectrum

Tier IV
Organised Crime, Cyber Mercenaries

Tier III
Crime Groups, Hacktivists

Discovers Unknown Vulnerabilities

Tier II
Criminals, Disgruntled Workers. Programmers

Tier I
Script Kiddies, Non Malicious Actors

Exploits pre-existing, known vulnerabilities

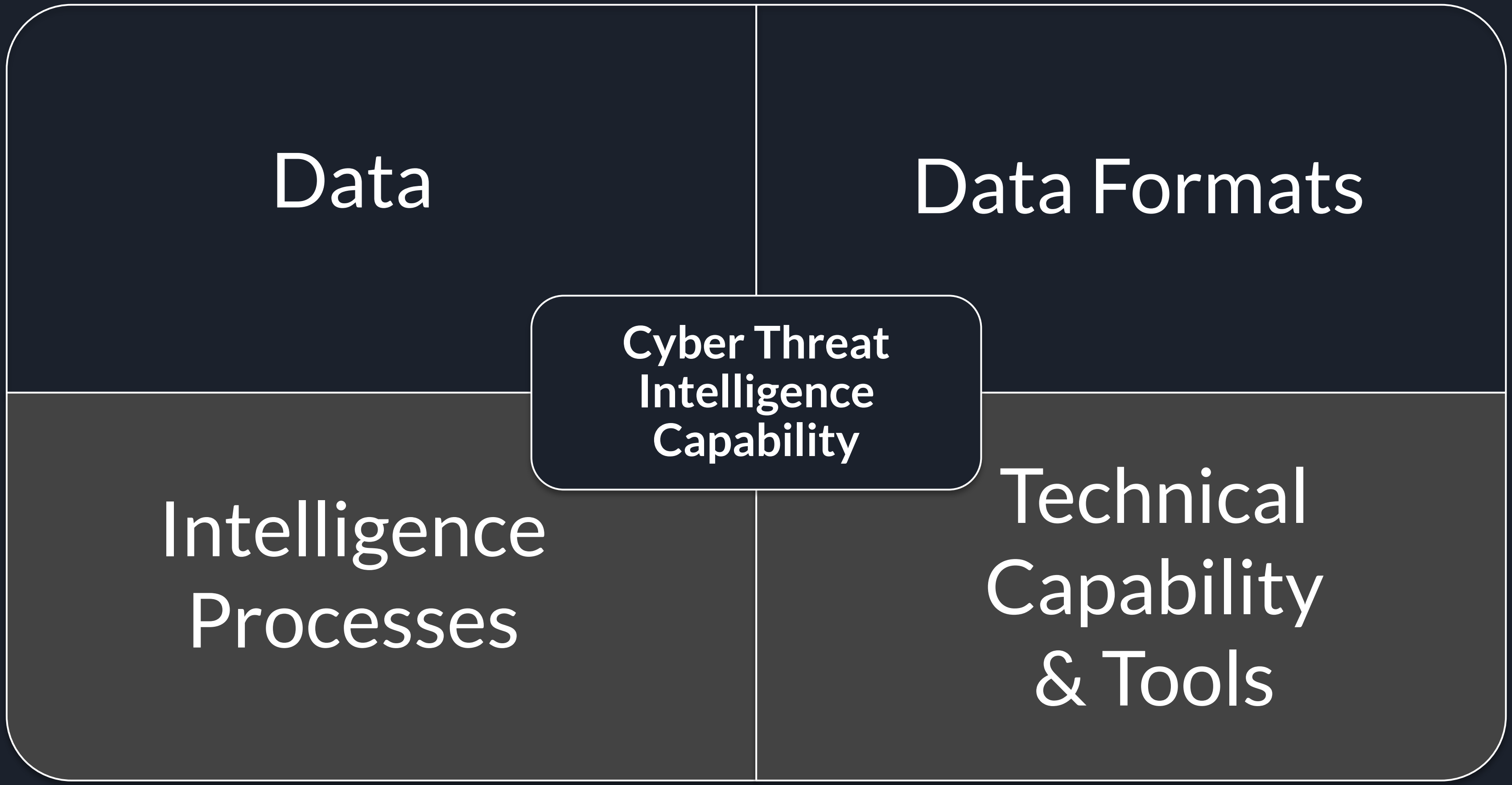
https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

Actionable Threat Intelligence is ...

- **Predictive** allowing future decision making
- **Relevant** to your organisation
- **Accurate**ly reported by your team
- **Timely** delivery to your audience
- **Accessible** to your intended audience

What data sources types support a CTI capability?

Component Parts of CTI Capability



Data

Data Formats

Cyber Threat Intelligence Capability

Intelligence Processes

Technical Capability & Tools

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.

- Sun Tzu

Data

External

- External Threat Intelligence
  - External threat information that allows you to identify potential future threats from “patient zero” or provide context about previous threats
- External Enrichment
  - Information about external networks, business processes, people and data.

Internal

- Internal Incident and Event Data
  - Events occurring on your network, as well as any identified security incidents.
- Internal Enrichment
  - Information about your IT networks, business processes, people and data.

Data Formats

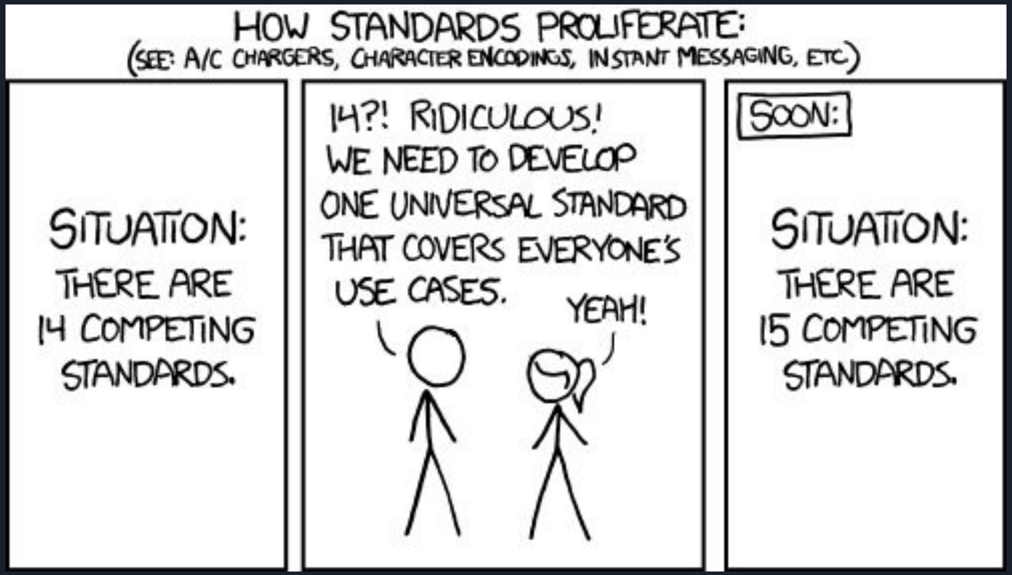
- Data formats allow interchange of threat intelligence with partners. It allows the integration of disparate tools to create a best of breed solution, and also to suit your audience.
- There are a number of standards for different use cases:
  - STIX 1.0 and STIX 2.0 (not interchangeable)
  - IODEF
  - MISP (is a tool but has its own standards)
  - PDF and DOCX
- Different vendors will also offer different formats, or even make their own brand new formats.
- Choose your formats, and make your data fit.

MISP Threat Sharing

STIX™

PDF

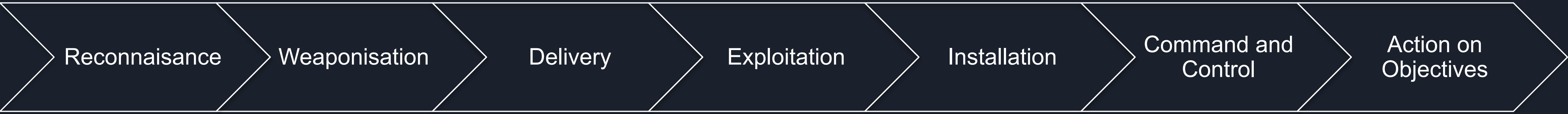
W


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

What are the Lockheed Martin Cyber Kill Chain and Diamond Model?

Lockheed Martin Cyber Kill Chain (CKC)

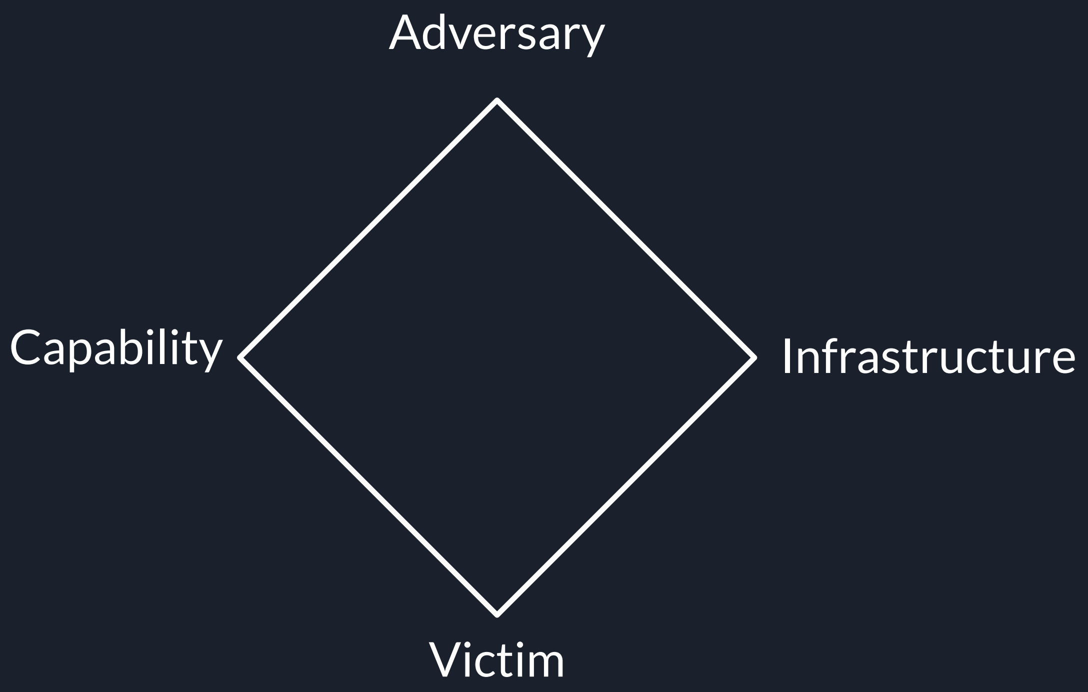
- Used to model a cyber intrusion into a number of discrete phases with dependencies.
- An adversary has to advance through the phases to achieve their final objectives.
    - CKC’s can also be linked (multiple chains to achieve an ultimate objective)
- Allows you to structure the information you have, and identify information gaps:
    - What did they do during _______ phase?
    - How did they move from _______ to ______?
    - What information dependencies would they have to achieve ______ phase?



Reconnaisance → Weaponisation → Delivery → Exploitation → Installation → Command and Control → Action on Objectives

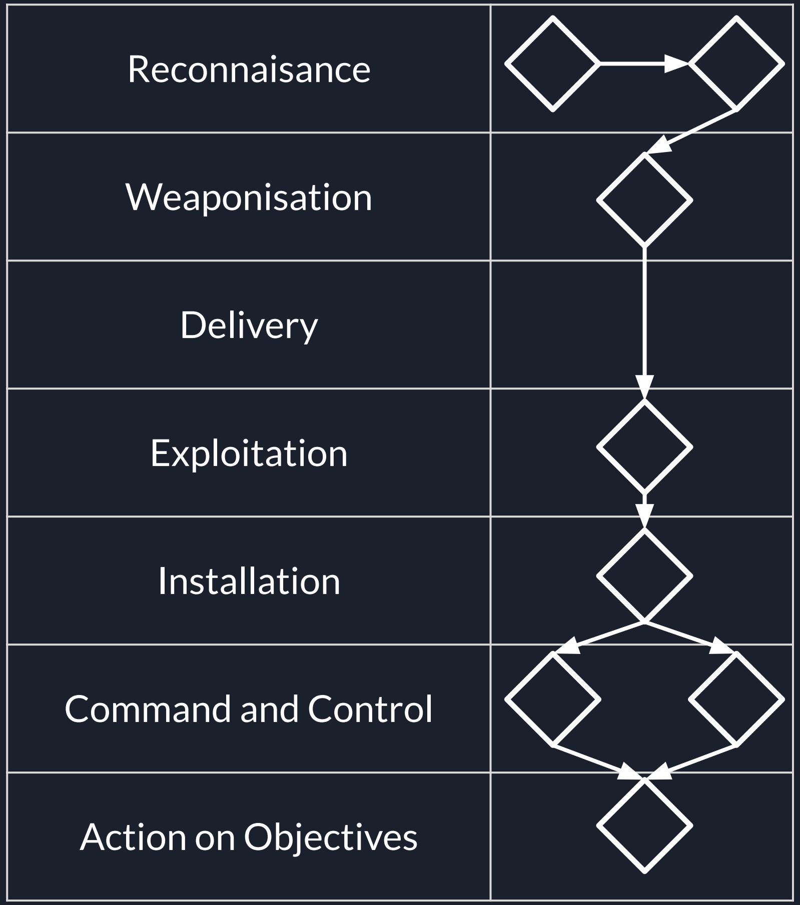
Diamond Model

- Can be used to model a single Cyber event or a complete intrusion.
- Breaks down the information
- You may not have all of these for a given event, but you will have some.
- Allows you to structure the information you have, and identify information gaps:
    - How did they achieve an action?
    - Who is behind the action?
    - Who is targeted by the action?
    - Where is the action coming from?



Bringing the Two Together

- Diamond Model is used to model a single event.
- Kill Chain is used to model the relationships between events.
- The two can be used to generate persistent models for evaluating future activity
  - We’ve seen an adversary using similar attack chains…
- Moves from indicator based to behaviour based detection



Reconnaisance

Weaponisation

Delivery

Exploitation

Installation

Command and Control

Action on Objectives

What data is required to generate actionable CTI?

Scenario

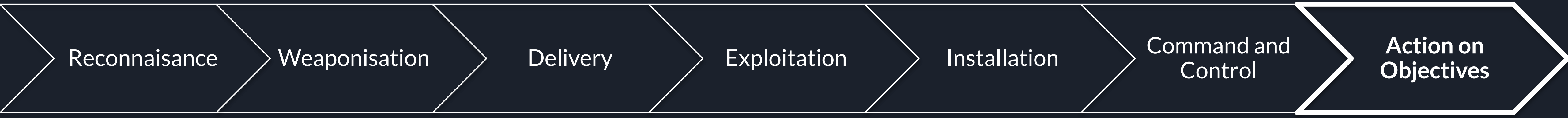
- You’ve received a phone call from the Australian Cyber Security Centre stating that they’ve detected a zipped file on a known UNICORN Command and Control domain that appears to have come from your network.
- The zipped file holds a number of documents containing the header “PROPRIETARY”.

This a fairly simple scenario, but you can *literally* only have this information to begin an investigation.

Action on Objectives

Intruders take actions to achieve their original objectives

- Adversary
    - What are UNICORN known to exfiltrate from compromised networks?
- Infrastructure
    - Is the C2 domain compromised or owned by UNICORN?
    - Has the C2 domain been seen by other targets?
        - Can we give them a heads up?
    - Where did they exfiltrate the data from on our network?
- Victim
    - What is the value of the data that was taken to my company?
        - What is the value of the data that was taken to an adversary?
        - What is the negative value of this being stolen against us?
- Capability
    - How did the adversary transfer the data?
    - Did they use internal software?

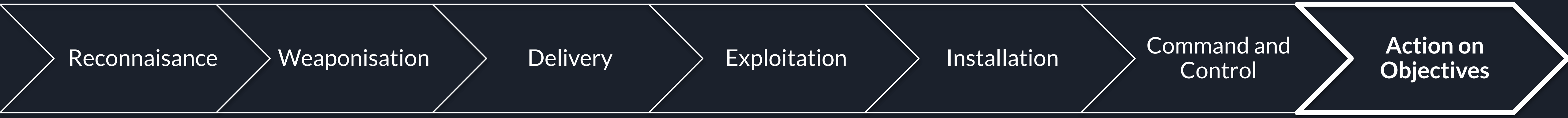


Action on Objectives

Intruders take actions to achieve their original objectives

- External Threat Intelligence
  - Threat Reporting
  - International News
  - Political Profiles
- External Enrichment
  - Passive DNS
  - IP Reputation
  - IP GeoLocation
  - Hacker Forums

- Internal Incident and Event Data
  - Proxy Logs
  - Mail Logs
  - PCAP
  - Internal DNS Logs
  - Security Incident Data
- Internal Enrichment
  - Project Information
  - Knowledge Management Processes
  - Approved Software Lists

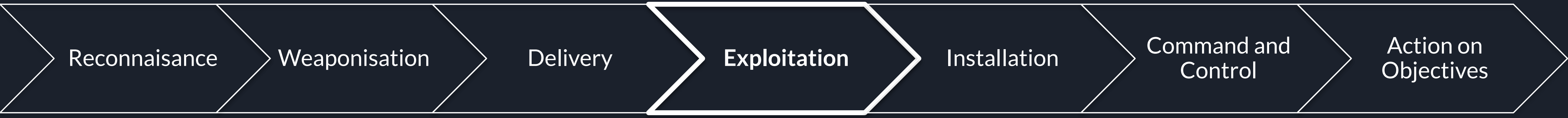


Exploitation

Exploitation targets an application, operating system or user vulnerability.

- Adversary
  - What type of adversary is able to develop / use this exploit?
    - Tier 6-5 – State Based
    - Tier 4-3 - Organised
    - Tier 2-1 – Script Kiddy
- Infrastructure
  - Where was it used?
  - Where else in my organisation does this vulnerability exist?

- Victim
  - Was the exploit tailored to the victim in any way?
- Capability
  - What vulnerability was used?
    - Software?
    - Hardware?
    - Business process?
  - How was the exploit packaged?
  - What did the exploit run when it attained code execution?

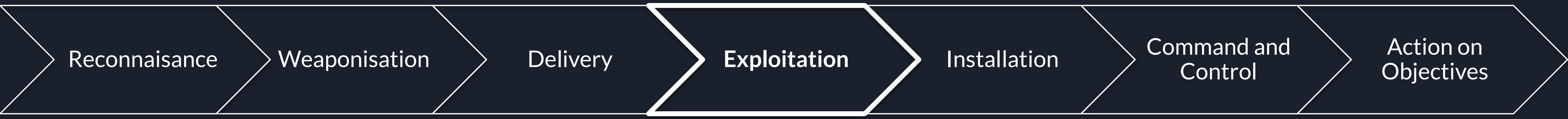


Exploitation

Exploitation targets an application, operating system or user vulnerability.

- External Threat Intelligence
  - Threat Reporting
  - Malware Reporting
  - Behavioural Reporting
- External Enrichment
  - Exploit Databases
  - Anti Virus Databases
  - Vulnerability Databases

- Internal Incident and Event Data
  - Host Based Intrusion Prevention / Endpoint Detection and Response
  - Windows Event Logs
  - Physical Security Reporting
- Internal Enrichment
  - Approved Software Lists
  - Hardware Inventory
  - OS Image Build Documentation
  - Business Processes
  - HR Documentation



Reconnaisance

Weaponisation

Delivery

Exploitation

Installation

Command and Control

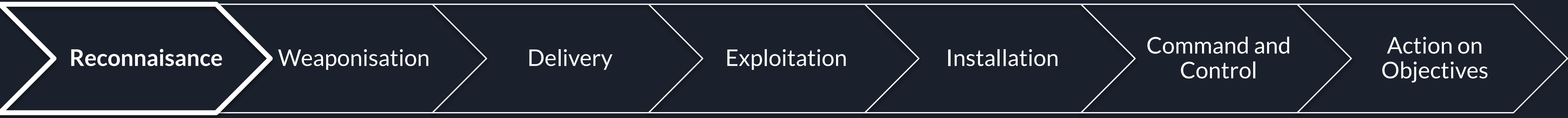
Action on Objectives

Reconnaissance

Research, identification and selection of targets

- Adversary
  - What adversaries would want to target my company in general?
- Infrastructure
  - Was any evidence of active recon seen against your network from indicators previously identified?

- Victim
  - What does my company do?
  - What information about my company and its projects exists on the internet?
  - Are there any specific groups an adversary would want to target?
- Capability
  - What types of recon could an adversary do against your organisation, its members and its IT systems?

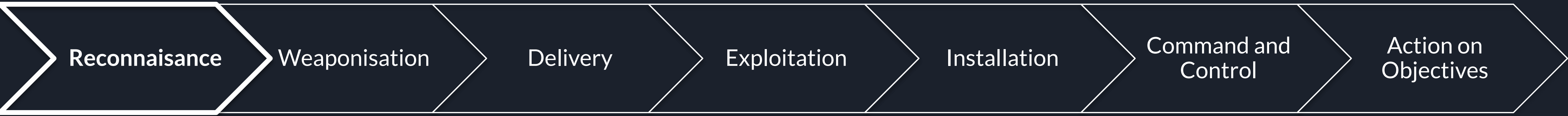


Reconnaissance

Research, identification and selection of targets

- External Threat Intelligence
  - Threat Reporting
- External Enrichment
  - Careers Sites
  - Professional Social Media
  - Personal Social Media
  - Reconnaissance Sites

- Internal Incident and Event Data
  - Incidents involving Phishing, Spear Phishing
  - PCAP
  - Intrusion Detection System Logs
- Internal Enrichment
  - Policies and Processes
  - HR Information on Personnel



Reconnaisance

Weaponisation

Delivery

Exploitation

Installation

Command and Control

Action on Objectives

The list of data goes on...

Anti Virus Definitions
Spam Email Content
Phishing Links
URL Reputation
Domain reputation
Passive DNS
Web Server logs
Mail Server logs
Travel Documentation
Firewall Logs
Company Directories List
Company Project List

Public Suffix List
Proxy Logs
Procurement Documentation
Geolocation Data
VPN Logs
Threat Intelligence Reporting
Political Profiles
Long Term Plans
News Media
National Calendars
Previous Security Incidents
Hacker Forums

Exploit Databases
Vulnerability Databases
Internal DNS Logs
Data Ownership and Provenance
Company Locations List
Google
Facebook
“Dark Web”
Intrusion (Detection | Prevention) System
Approved Software Lists
Tender Documentation
...

How does actionable Cyber Threat Intelligence support Defensive Cyber Ops?

Incident Response

Incident Response investigates, contains, and responds to cyber intrusions on an organisations networks. PICERL is a well known model used for these activities.

Intelligence Led Defensive Posture

- Deciding what infrastructure, what detection rules, based on incoming threat intelligence.
- A combination of your own internal product and external product that is relevant to your companies field, customers.
- Used to focus your defensive measures on those threats that are relevant to you, and to also improve your detection capabilities for those threats.

Penetration Testing

A controlled attack simulation that helps identify susceptibility to application, network, and operating system breaches.

Cyber Threat Emulation - Using an adversary's actual techniques against an victim network.

- Using an adversaries "playbook" to test your own networks capability.
- Prioritisation of people, technology and money towards likely TTP's.
- Can also be used once you've received a penetration teams report to identify priorities for remediation.

In closing

Summary

- Cyber Threat Intelligence enables decision making. It allows you to fully understand risk in your environment appropriately.

- It's supported by a number of different data sources, both internal and external.

- The Lockheed Martin Cyber Kill Chain and Diamond Model can help you structure your investigations, and then identify your information gaps before providing an end product.

- CTI can support defensive cyber operations in both a proactive and reactive manner, enabling decisions to be made about improving a networks defensive posture.

Thanks!

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Diamond Model for Intrusion Analysis

https://apps.dtic.mil/dtic/tr/fulltext/u2/a586960.pdf

Little Bobby Comics

https://www.littlebobbycomic.com

icd@wan0.net
@wan0net