Cyber Threat Intelligence and Threat Hunting in the Energy Domain

CSP006_S_E

PRESENTATION BY:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

Acknowledgement

- *Co-Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

Cyber Threat Intelligence and Threat Hunting in the Energy Domain

Overview

- Topic-1: Introduction to Threat Intelligence and Threat Hunting
- Topic-2: Data Sources and Collection
- Topic-3: Threat Actors and Tactics
- Topic-4: Practical Threat Modelling and Security Investigation

Agenda

01. Threat Intelligence

02. Sources of Intelligence

03. Threat Hunting

OBJECTIVES

At the end of this session, you should be able to …

1. Identify the different types of adversaries that pose a threat to our computer systems
2. Identify the different types of intelligence we can use to characterise threats
3. Explore different open-source tools that allow us to share intelligence and automate responses
4. Recognise the wide range of publicly available sources of Cyber Threat Intelligence

Threat Intelligence

What is cyber threat intelligence (CTI)

The use of skills, knowledge, and experience to collect and evaluate the reliability of information related to threat actors/an adversary, including their intentions, capabilities and potential opportunities, in order to mitigate possible cyber-attacks and the harm they may cause.

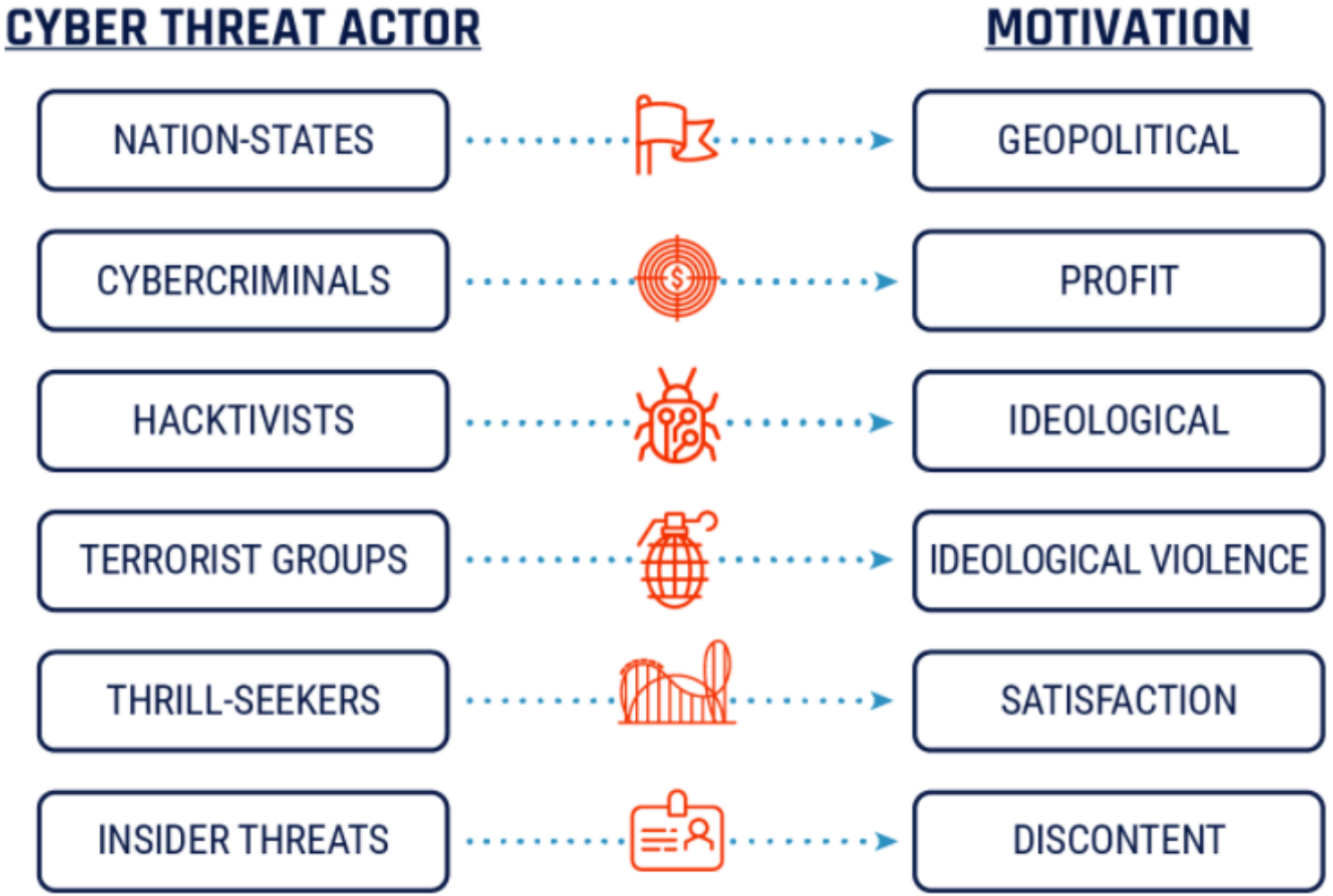
Adversaries want to attack computer systems, it is important to understand their intent:

- Political motivations?
- Hacktivism?
- Economical gain?

Their capabilities are just as important. Are the adversaries a state-sponsored hacking group, technically skilled criminals, or script kiddies who are playing around with new tools? There is a wide range of capabilities in these groups. Some may not be relevant.


Intent
Insubstantial Threat
Impending Threat
THREAT
Capability
Potential Threat
Opportunity

Types of threat actors in the Wild



Source: Top 7 Popular Cyber Threat Models - SecurityMadeSimple.org

Key Concepts

Adversary / Threat Actor

The person or team of people behind the keyboard, carrying out the cyber-attack. This can be loosely defined, e.g. *Military Unit 26165*, or a specific individual, e.g. *Kevin Mitnick*.

Campaign

Sustained malicious operations of an adversary that carry a single focus or end goal, e.g. impair a company's online service, or sabotage an oil & gas refinery.

Tactics, Techniques, and Procedure (TTP)

A way of describing a method or set of methods used by adversaries to compromise a machine or system.

Indicators of Compromise (IoC)

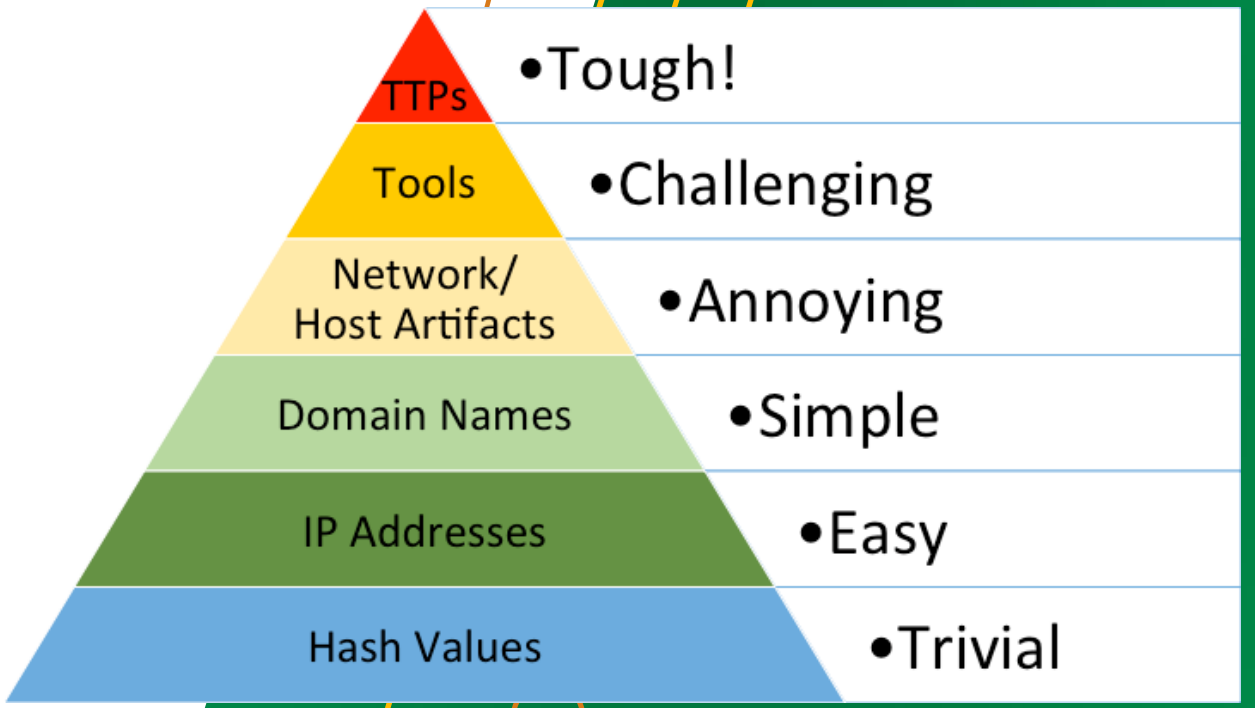
Pieces of forensic data, found in system logs, files, network packet captures, etc., that identify malicious activity on a computer system or network.

SANS Institute Pyramid of Pain

The *pain* refers to the pain you can cause an adversary, if you were able to detect and identify the elements in that level of the pyramid.

The higher up the pyramid, the more *painful* it is for attackers.

The wider the section of the pyramid is, the more accurate and actionable the information is.



SANS is an acronym for SysAdmin, Audit, Network, and Security.

Hash Values

Hashing algorithms produce a **message digest** from a given input, and are used to verify the integrity of a piece of software to ensure no malicious changes have been made.

Common hashing algorithms include **SHA1**, **MD5**, and **SHA256**.

Hashing algorithms are one-way functions*.

A change in even one bit of the input produces a different hash.

Input	Input
Hello	Hallo
Output	**Output**
8b1a9953c4611296a827abf8c47804d7	1de11cf8b803fb31cacb13ce23c0b361

▸ Audacity 3.1.2 64 bit installer

SHA256 Checksum:

```
6a3f5f7c1801d30de40e02477be87b429336e3ed42d65cf6f12cdb9a101d1906
```

▸ Audacity 3.1.2 64 bit zip file

SHA256 Checksum:

```
3d1d4e097c48b7d685c8061920b84ac4ac0257d40ae17567de223d75f41bbb40
```

IP, domain, network artefacts

- Domains allow us to use human-readable names for websites and online services.
- IP addresses are a very definite, but domains can be used to fool humans.
- Many malware families are using Domain Generation Algorithms (DGAs) to procedurally create and register domains.
- This gives the planted malware flexibility in finding a connection back to the attackers.

```
Standard query 0x6c4f  A pivuogusodtoku.ddns.net
Standard query 0xb48b  A onogibuluremg.ddns.net
Standard query 0x66fc  A geevheuqsemaif.ddns.net
Standard query 0x7b8c  A egisrihuwuwoom.ddns.net
Standard query 0x6660  A enaxontugahoun.ddns.net
Standard query 0xb015  A vauqomadassaeb.ddns.net
Standard query 0x56da  A opdeikixaxec.ddns.net
Standard query 0xa24e  A oticrivievhuow.ddns.net
Standard query 0x6644  A uqodupegbo.ddns.net
Standard query 0x63d0  A xisenuun.ddns.net
Standard query 0x0243  A omexithamisi.ddns.net
Standard query 0xbeca  A uxtoleite.ddns.net
Standard query 0x12b6  A uglaweedipwaho.ddns.net
Standard query 0x57dc  A ahtilenearo.ddns.net
Standard query 0x3e8c  A niesivaxumo.ddns.net
Standard query 0xd3f6  A iricilec.ddns.net
Standard query 0x734a  A uqadvoduurgeuhi.ddns.net
Standard query 0x94b1  A ehwepikeisi.ddns.net
Standard query 0xc9e9  A ehukguaggox.ddns.net
Standard query 0x292f  A onwaukfitamia.ddns.net
Standard query 0x2975  A idxoebsad.ddns.net
Standard query 0xac37  A ihneuwvaixq.ddns.net
Standard query 0x8b92  A subaukewoktalev.ddns.net
```

Tactics, Techniques, and Procedures (TTP)

TTPs are a hierarchical classifications of adversary behaviour. Using TTPs in combinations with the MITRE ATT&CK Framework makes it easier to "fingerprint" a threat group.

A **tactic** is the highest-level method to achieve a goal via cyber-attack.

E.g. *Infection with Malware via Spear Phish* (Initial Access).

A **technique** is how the tactic is employed.

E.g. Crafting malicious exploit inside PDF file (T1566.001).

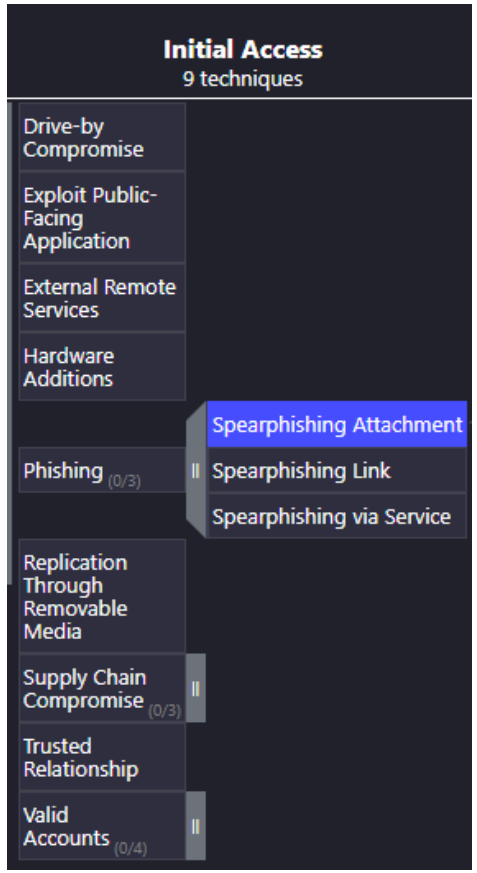
A **procedure** is how the technique is delivered.

E.g. the commands that are used to create the PDF and send the email.

The term TTP is sometimes used to generally describe how an adversary operates.

MITRE ATT&CK Framework

MITRE's ATT&CK Framework allows for easy identification and sharing of TTPs



Procedure Examples

ID	Name	Description
G0018	admin@338	admin@338 has sent emails with malicious Microsoft Office documents attached.[1]
S0331	Agent Tesla	The primary delivered mechaism for Agent Tesla is through email phishing messages.[2]
G0130	Ajax Security Team	Ajax Security Team has used personalized spearphishing attachments.[3]

Detection

ID	Data Source	Data Component
DS0015	Application Log	Application Log Content
DS0022	File	File Creation
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

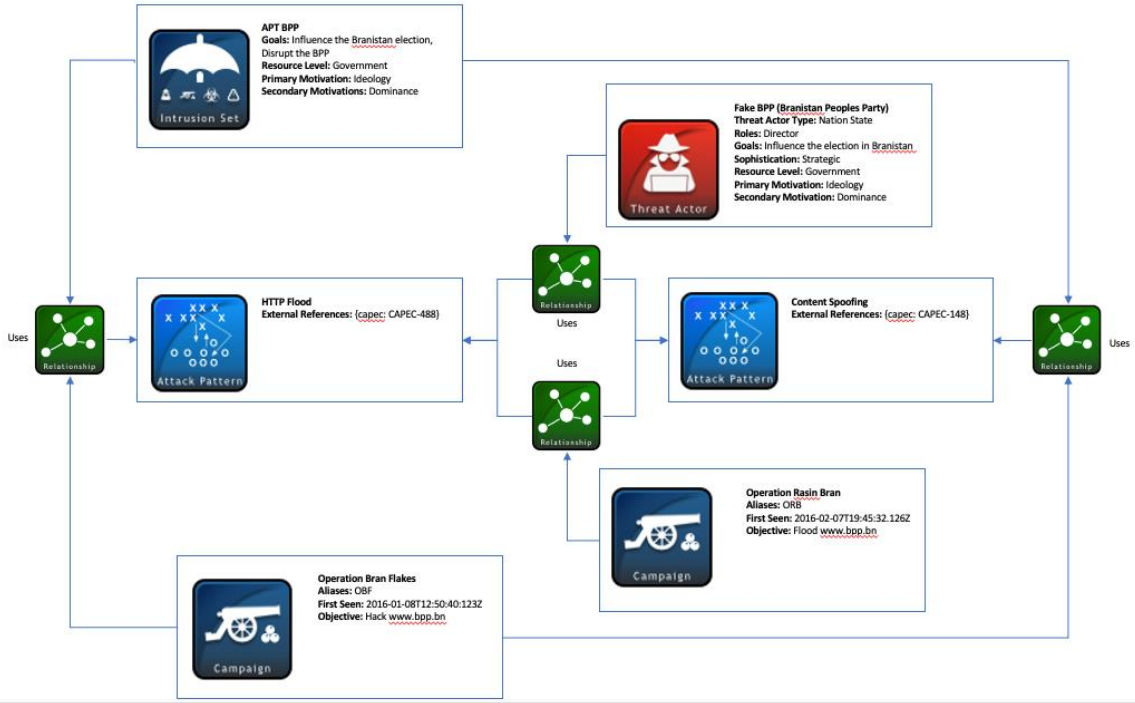
Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
M1031	Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.

Structured Threat Information eXpression (STIX)

Language and serialization format for exchanging CTI

Can be visually represented for an analyst or stored as JSON




```
{
    "type": "bundle",
    "id": "bundle--56be2a3b-1534-4bef-8fe9-602926274089",
    "objects": [
        {
            "type": "indicator",
            "spec_version": "2.1",
            "id": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4f",
            "created": "2014-06-29T13:49:37.079Z",
            "modified": "2014-06-29T13:49:37.079Z",
            "name": "Malicious site hosting downloader",
            "description": "This organized threat actor group operates
            "indicator_types": [
                "malicious-activity"
            ],
            "pattern": "[url:value = 'http://x4z9arb.cn/4712/']",
            "pattern_type": "stix",
            "valid_from": "2014-06-29T13:49:37.079Z"
        },
```

Malware Information Sharing Platform (MISP)

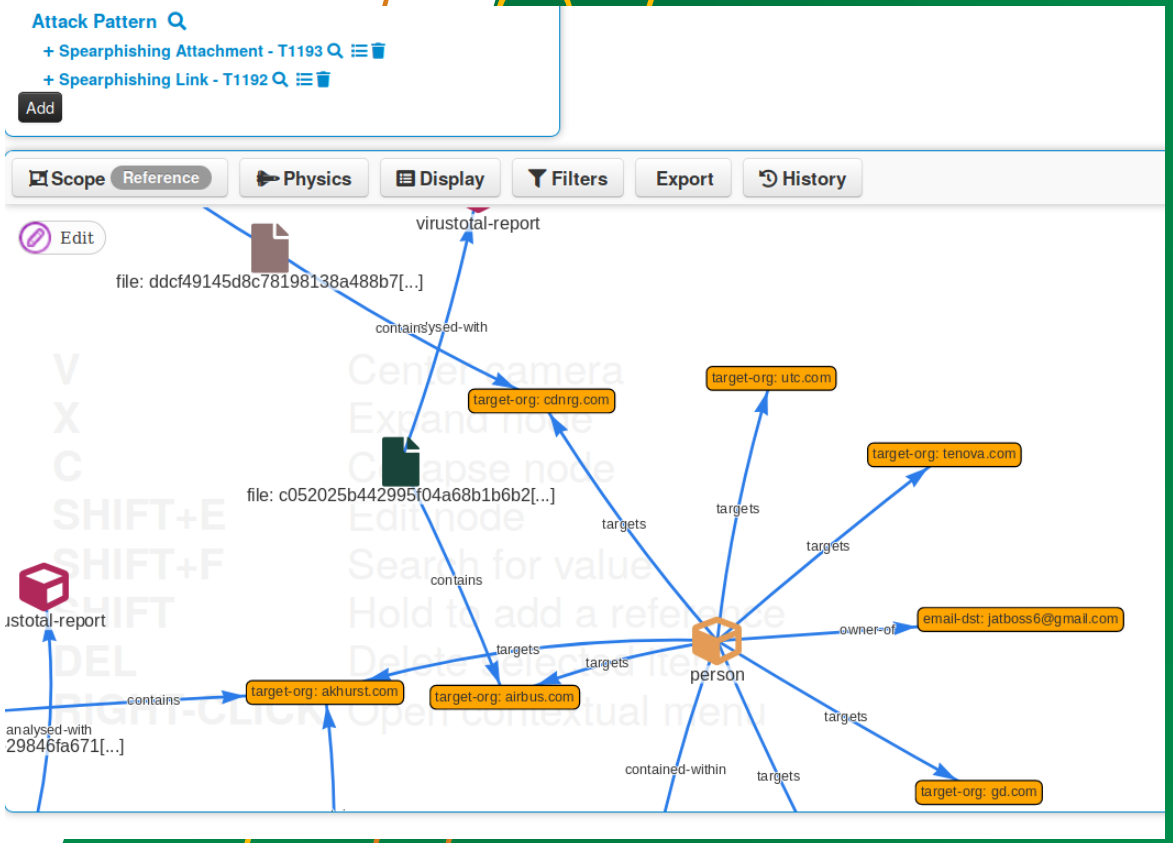
Open-Source threat intelligence platform.

Can automatically Snort, Suricata, Bro, Zeek IDS rules.

Can export to STIX, OpenIOC, text or csv.

Python, Ruby, Go, and HTTP libraries available.

Can integrate with ElasticSearch/Logstash/Kibana (ELK).



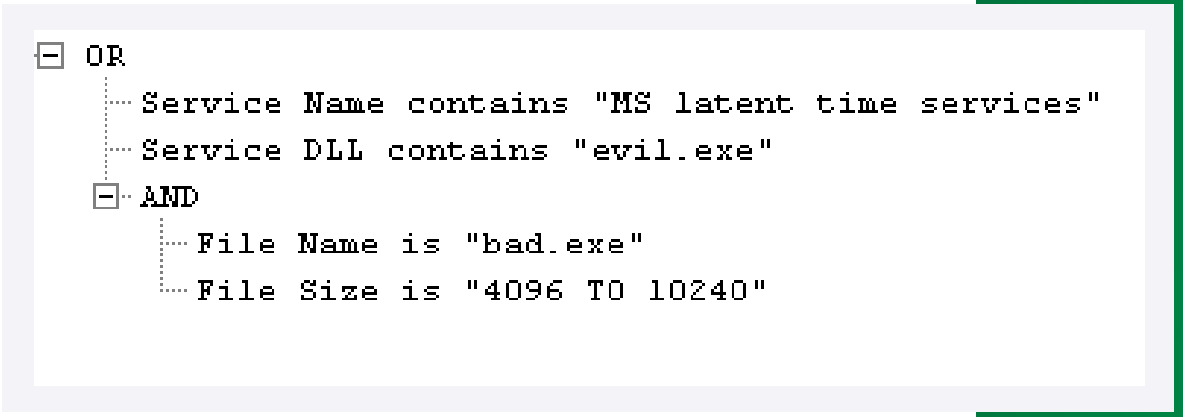
OPENIOC

Another open standard for sharing information on malicious activities.

The name of a service is "MS latent time services“

OR

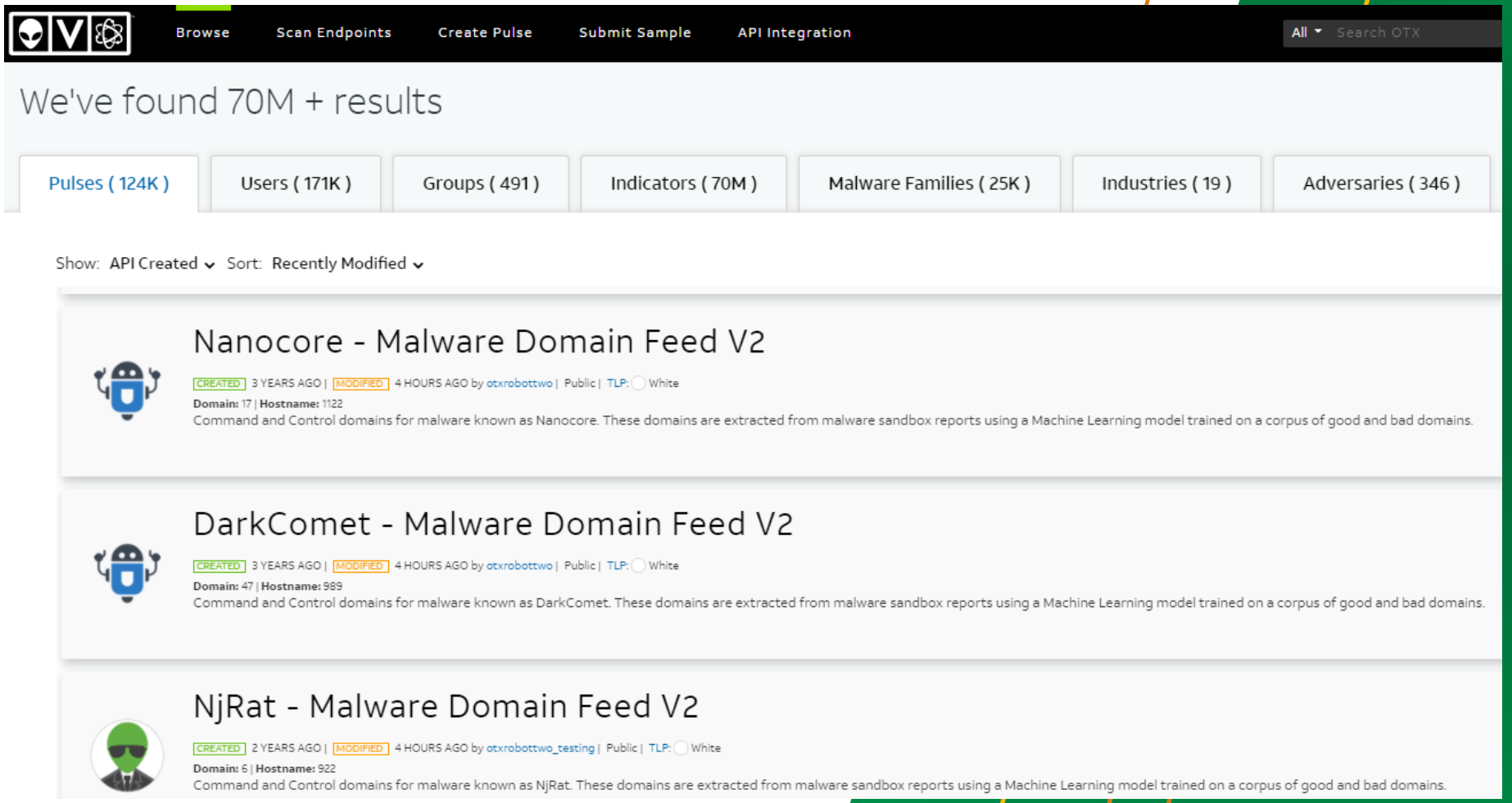
The ServiceDLL name contains "evil.exe“



OR

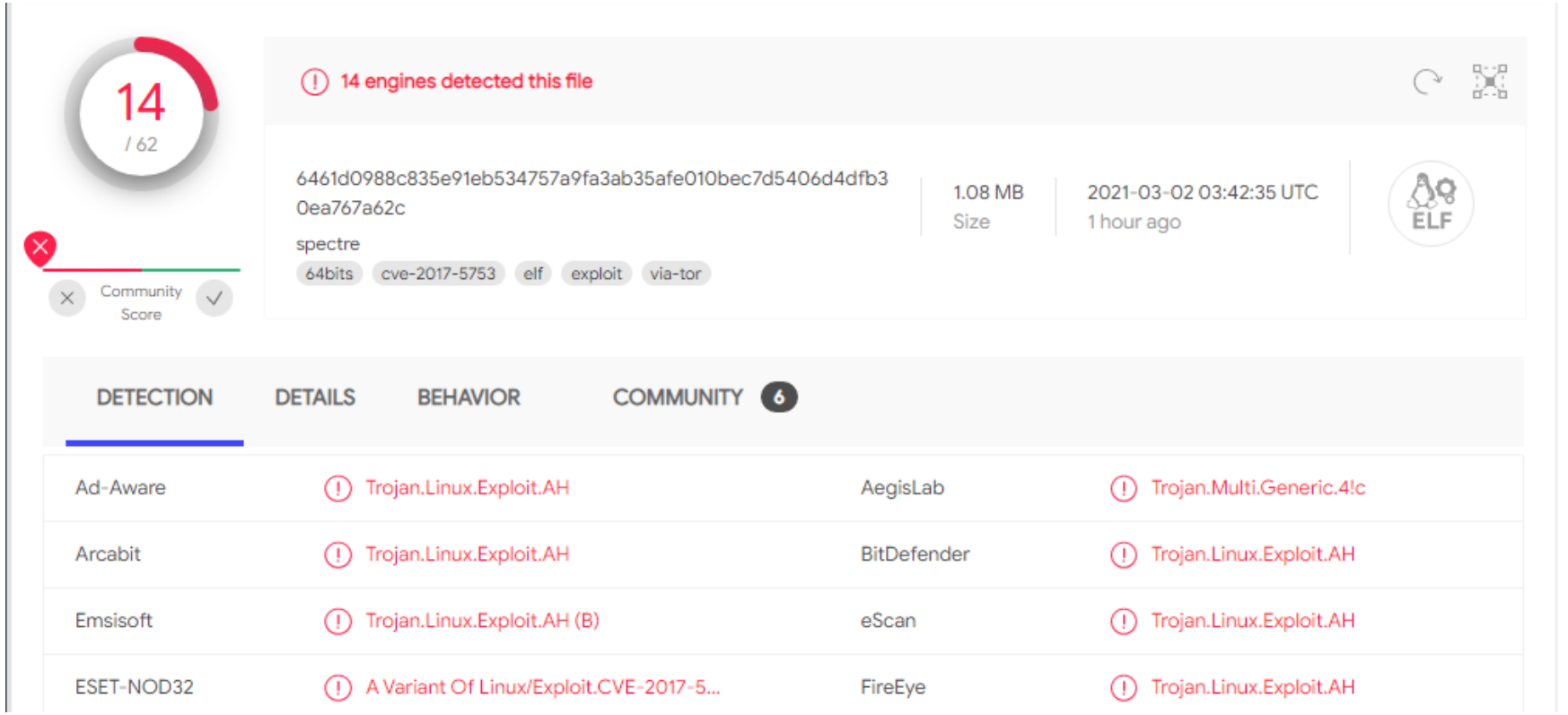
The filename is "bad.exe" **AND** the file size attribute of that file is within the range 4096 to 10240 bytes.

AlienVault Open Threat Exchange (OTX)

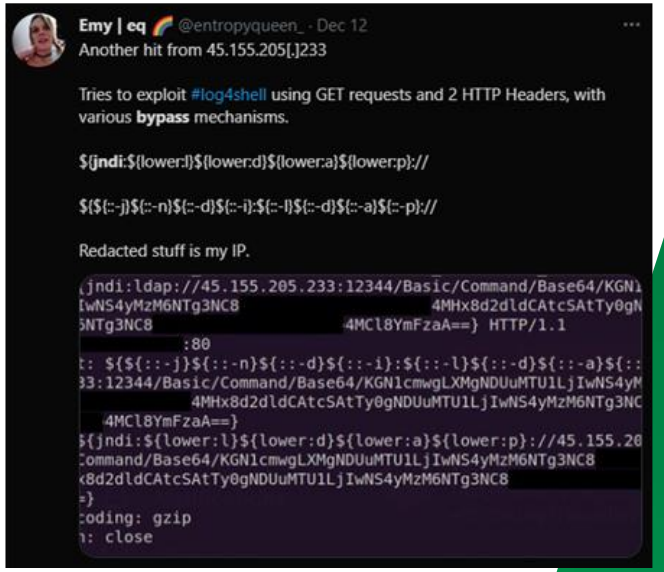


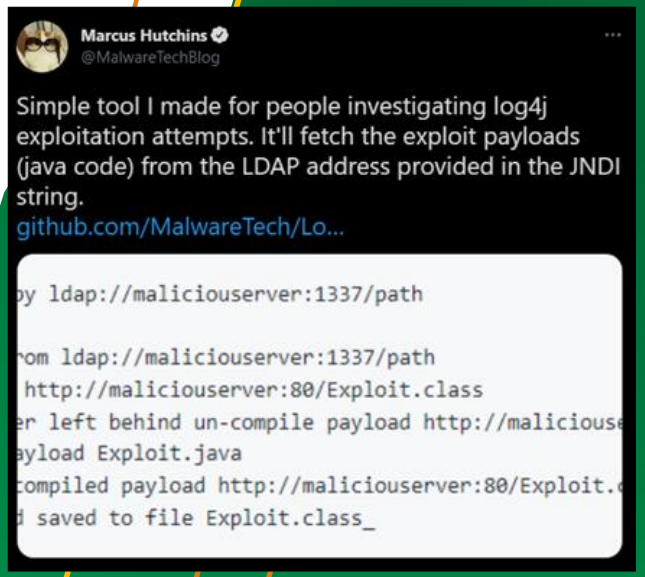
Virustotal

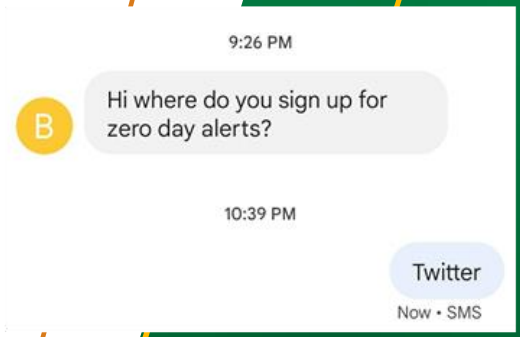
Upload any file and VirusTotal will run it against a range of the worlds best anti-virus tools



Social media







Sources of Intelligence

Sources of Intelligence

Threat Hunting

What is Threat Hunting?

Define, what you consider as threat hunting

Do you have any experience?

Are you interfacing with threat hunters, e.g. by providing information to them?

How are new threats detected in your environments? Active or passive?

Threat Hunting

The art of searching through networks and systems in order to detect and isolate threats.

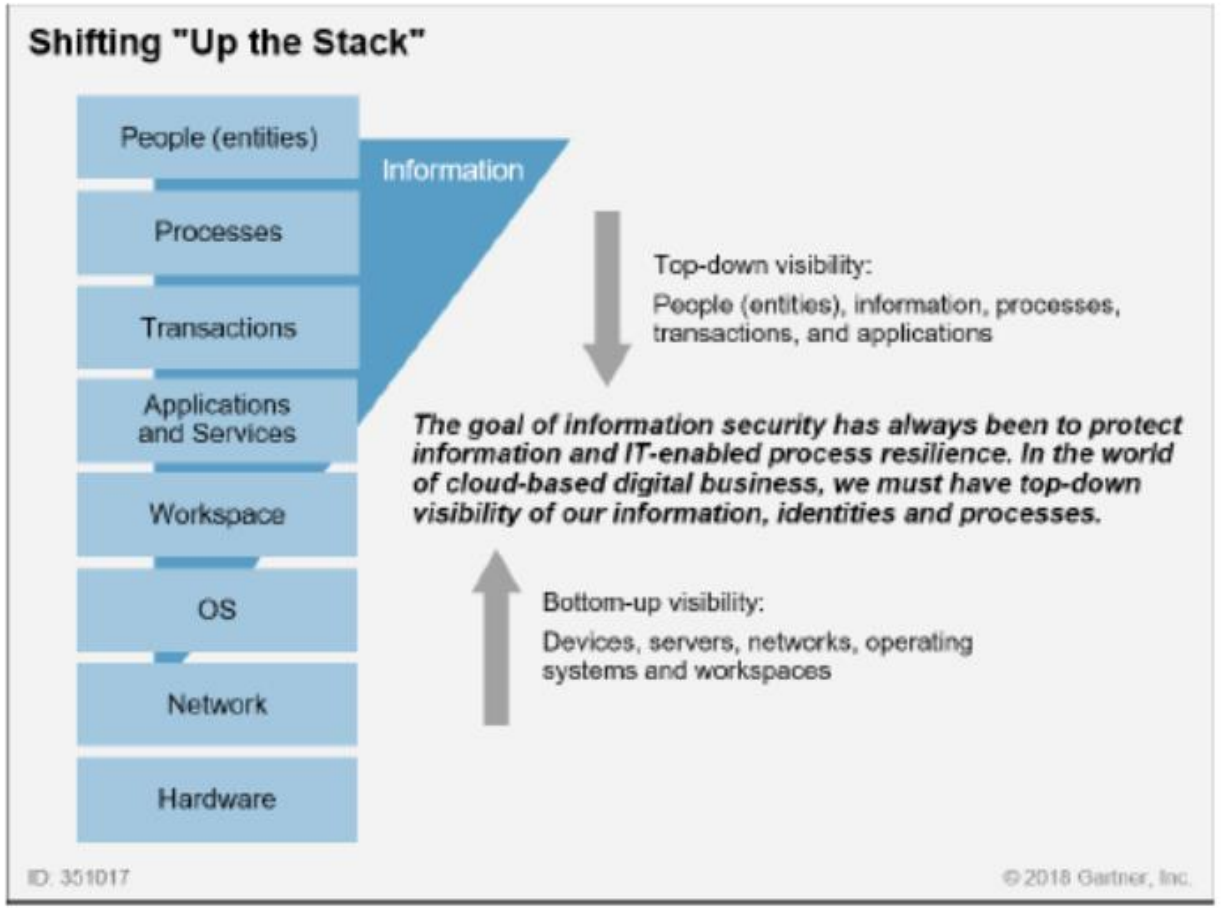
- It is a proactive measure
- It targets advanced threats
- It assumes breach of security solutions in place

Threat Hunting is typically done without explicit call for an investigation

- Done without an actual cause
- Hunts are repeated

Threat Hunting often builds on Security Monitoring, but is not the same

Why Threat Hunting?



Some Vocabulary

Dwell Time – Number of days an attacker is present in a victim system before being detected

Hypothesis – A research question that can be asked right at the start of the hunt - Subsequently data and indicators are evaluated whether they support the hypothesis or not.

TTPs – Tactics, Techniques and Procedures

Benefits

Due to the basic principle – we are looking for attackers that had success, so we can find them

- Complete oversight of a typical organization is not possible at this point

Improves detection capabilities

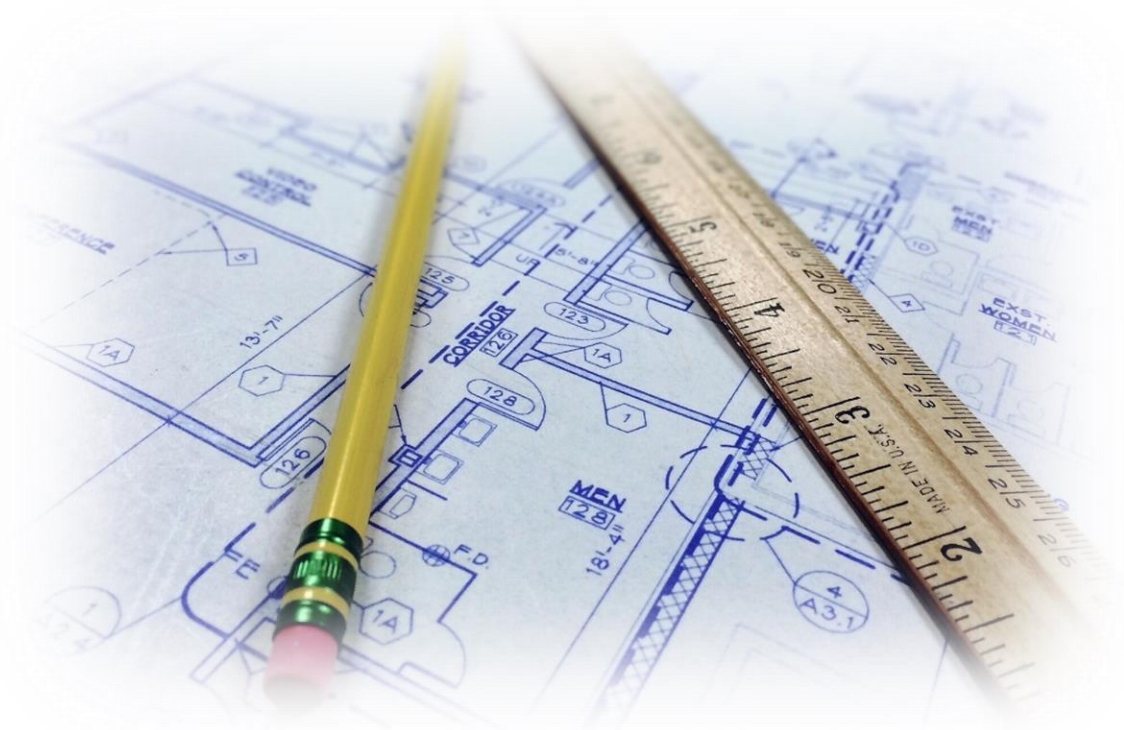
- Permanently hones skills
- Supports early detection of potential attack vectors
- Increases awareness towards your attack surface

Improves your data collection

Cyber Incident Response Plans

Structured approach to preparation

- What measures should be in place, what information gathered?
- What to do in case of an incident?
- Contact Information
- Based on risk analysis and BIA.
- Different forms of attack



Require

- Thorough analysis
- Regular maintenance
- Awareness & Training

Cyber Incident Response Readiness

Assessing your Cyber Incident Response Readiness

- Structured approaches exist

One good example:

- Checklists developed by the Australian Government
- Simple and usable

https://www.cyber.gov.au/sites/default/files/2022-07/ACSC%20Cyber%20Incident%20Readiness%20Checklist_A4.pdf

Cyber Incident Response Readiness

☐	Up-to-date hard copy versions of the Cyber Incident Response Plan and playbooks are stored in a secure location (in case of electronic or hardware failure) and are accessible to authorised staff members.
☐	Specific playbooks to supplement the Cyber Incident Response Plan have been developed, that define step-by-step guidance for response actions to common incidents, and roles and responsibilities.
☐	A Cyber Incident Response Team (CIRT) and a Senior Executive Management Team (SEMT) – or equivalents - have been formed to manage the response, with approved authorities.
☐	All relevant IT and OT Standard Operating Procedures (SOPs) are documented and have been reviewed or tested in an exercise to ensure they remain current and responsible personnel are aware of their roles, responsibilities and processes.
☐	Arrangements for service providers, including cloud and software as a service, to provide and retain logs have been established and tested to ensure these include useful data and can be provided in a timely manner.
☐	Log retention for critical systems have been configured adequately and tested to confirm that they capture useful data. Refer to the ACSC publications including Windows Event Logging and Forwarding for specific guidance.

The Threat Hunting Maturity Model

Describes

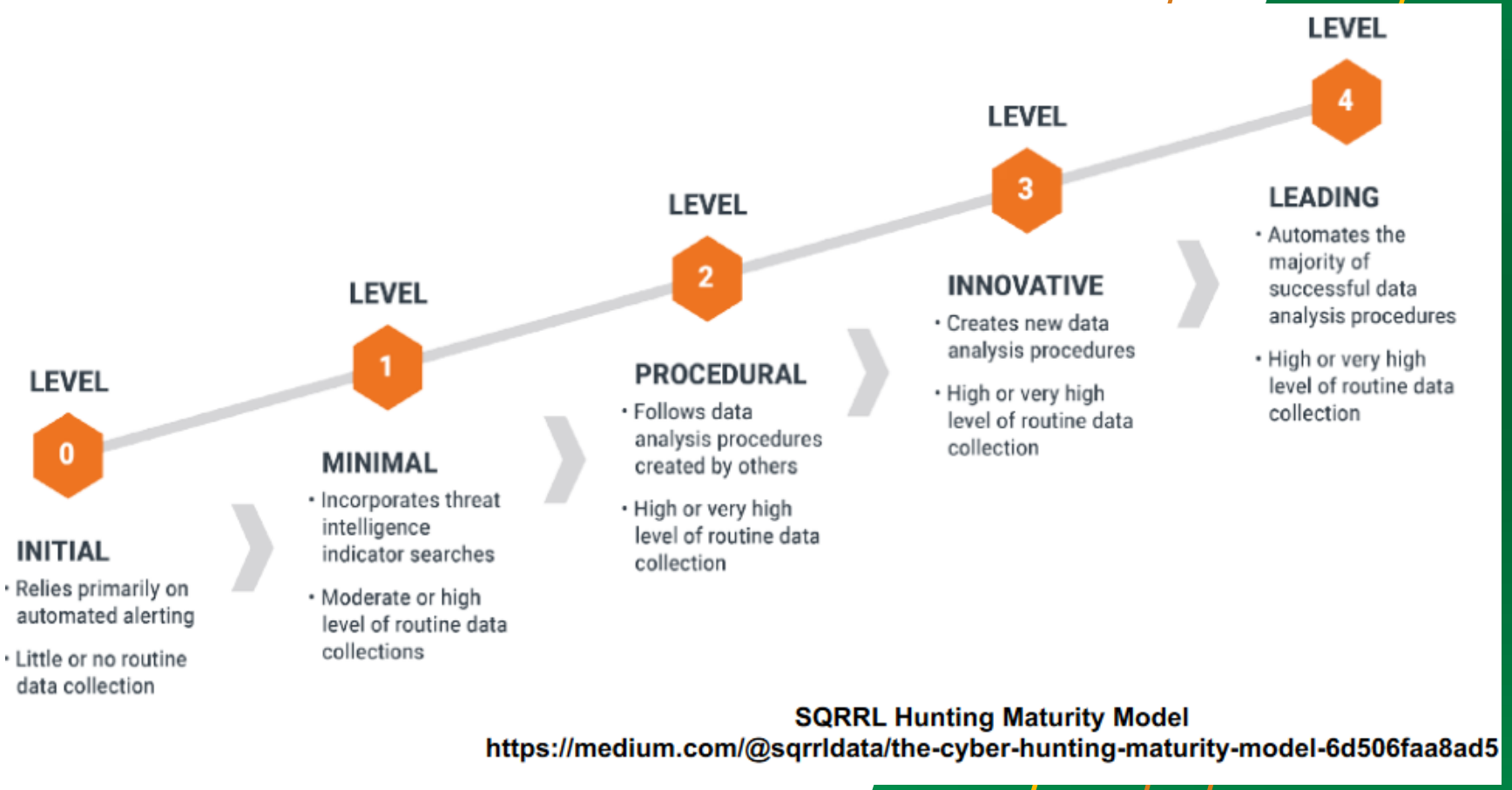
- Development levels
- Associated possibilities

Divided into three levels from 0 to 4

Based on three key factors

- Quantity and quality of data
- The ways in which different data sources are visualized and analyzed
- Automation of data enrichment with sources, e.g. from Threat Intelligence or DNS

The Threat Hunting Maturity Model



SQRRL Hunting Maturity Model
https://medium.com/@sqrrldata/the-cyber-hunting-maturity-model-6d506faa8ad5

The Threat Hunting Maturity Model

Higher levels cannot be achieved by using tools alone

- Requires teams to find new threat actors
- Is based on human creativity and thinking out of the box
- Combined with automating non-creative tasks and basic information acquisition and enrichments
- Working in teams

The maturity model can be used as a roadmap for enhancing Threat Hunting Teams

Threat Hunting KPIs

Key Performance Indicators (KPIs) help to analyze and visualize the success of a threat hunting system

Metrics can support decision makers

- as a warning mechanism that things go south
- in making the right decision by making actual results comparable to theoretical ones

Metrics like these should never be used

- As sole mechanic for remuneration
- To compare different analysts

Threat Hunting KPIs

Effort based KPIs
- What did we do to enhance our hunts?

Success based KPIs
- How did we succeed in our hunts?

Management based KPIs
- How is Threat Hunting integrated into the organization?

Some examples on the following slides

Effort based KPIs

Number of Threat Hunts completed

Number of data sources connected

Number of analysts involved after a completed threat hunt

Average time dedicated to a Threat Hunt

Number of incomplete threat hunts

Number of hypotheses that were (not) found by the threat hunting model used

Number of non-malicious findings by category (security risk, logging vulnerability, incorrect user permissions, tool misconfiguration, etc.)

Success based KPIs

Number of false positives reduced

Number and type of findings (malicious, non-malicious)

Number of non-malicious findings by category (security risk, logging vulnerability, incorrect user permissions, tool misconfiguration, etc.)

Reduce record size by filtering detected non-malicious activity

Number of newly detected attack techniques

Number of new detections generated

Dwell time of findings (elapsed time until detection)

Number of proactively detected incidents compared to reactively detected incidents- Severity of incidents

The number of compromised, unsecured or misconfigured systems detected

Number of resolved findings by severity

Management based KPIs

Threat hunting management budget

Data model and data quality assurance process established

All threat hunts are driven by threat intelligence relevant to the organization.

Threat Hunting team works closely with other teams.

New detection mechanisms are implemented on an ongoing basis.

All threat hunts performed are properly documented.

All generated detections are properly automated.

Improvements made to the threat hunting process

Summary

- A threat is a combination of capability, opportunity, and malicious intent
- Adversaries have many motivations, and can come from anywhere; from within the victim organisation, or from a foreign power
- There are many ways to catalogue and share threat intelligence using open-source tools: STIX, MISP, OpenIOC
  - Some of these tools provide programming interfaces for automating Firewall and IDS/IPS configurations
- There is publicly available intel from both public and private sector organisations
  - Cyber security firms, organisations dealing with big data, government bodies, etc.

Connect with CyberSecPro:
How to register and other practical information

1. Website:
   www.cybersecpro-project.eu
2. X (Twitter):
   https://twitter.com/CyberSecPro_eu
3. LinkedIn:
   https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Thank you

Please send all questions to:
Stefan Schauer
Stefan.Schauer@ait.ac.at
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at