Introduction

LECTURE 1 – SITUATIONAL AWARENESS

Agenda

Introduction

- Module Overview
- Assessment Overview

Lecture 1 Material

- Situational Awareness

Lectures

Lectures will available online later, these should be recorded automatically and uploaded on DLE but it will take time.

We will occasionally use mentimeter during live lectures

Got to Menti.com and use code displayed on screen

Further reading: books, articles on the slides and/or DLE

Labs/Assessment

Let's do a tour of the DLE pages….

- Lab: using Ubuntu virtual machine on DLE
- Module will be assessed by group coursework (50%) and individual exam (50%)
- All students are required to choose and enrol in one group. The group enrolment is mandatory and on DLE.
- Material from both lectures and practical sessions will be assessed

Contact Information

Module Team:

Dr Hai-Van Dang (Module Leader – Cyber security)

Communication:

Contact hours: during lectures

Q&A on DLE

Microsoft Teams message

Email hai-van.dang@plymouth.ac.uk – for individual queries – 2 working days

Surgery hour (office hour) and the link to join: see DLE

Questions?

(BEFORE CONTINUING TO LECTURE MATERIAL)

Module Overview

LEARNING OUTCOMES – SCHEDULE - RESOURCES

Learning Outcomes

Illustrate the structure, roles and responsibilities of a security operations centre.

Design and develop technical infrastructures for the management and monitoring of cyber security.

Undertake analysis of data and select appropriate intrusion analysis methodologies to analyse intrusion alarms.

Situational Awareness

Learning outcomes checklist

1. Understand and give examples of situation awareness in general
2. Understand and give examples of situation awareness in cyber
3. Understand how OODA is applied for cyber situation awareness
4. Understand and give examples of threat intelligence in cyber
5. Recognize the loss of SA in threat reports

Reading tasks (at home)

1. Situation awareness and cyber situation awareness: “SoK: Contemporary Issues and Challenges to Enable Cyber Situational Awareness for Network Security”, read section 1, 2 (page 1-4)
2. OODA loop for cyber situation awareness: Lenders, V., Tanner, A. and Blarer, A., 2015. Gaining an edge in cyberspace with advanced situational awareness. IEEE Security & Privacy, 13(2), pp.65-74.
3. SA perspectives: Lundberg, Jonas. "Situation awareness systems, states and processes: a holistic framework." *Theoretical Issues in Ergonomics Science* 16.5 (2015): 447-473.
4. Threat intelligence: Jean Nestor M. Dahj, “Mastering cyber intelligence : gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense” (**download from Primo system of University’s library**), chapter 1, page 3-21)
5. Mitre ATT&CK: Jean Nestor M. Dahj, “Mastering cyber intelligence : gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense” (download from Primo system of University’s library), page 67-75 (subsection “Mitre;s ATT&CK knowledge-based framework)

Other book (for the upcoming lectures): Stephen Northcutt, Judy Novak. Network Intrusion Detection, Third Edition. Sams Publishing 2002,

What is not right in this scenario?

On 27th August 2006, Comair flight 5191 took off from the wrong runway. It was early morning and still dark outside as the captain (highly experienced and trained) was taxiing the aeroplane to the runway. Instead of taking the right runway, he took a wrong turn, which led the plane onto a runway that was too short for take-off. During take-off the cockpit is a designated quiet area to allow for concentration. On this occasion, the captain and co-pilot were chatting

Source: https://www.hse.gov.uk/construction/lwit/assets/downloads/situational-awareness.pdf

And consequences

The chatting was affecting everyone's performance. Allowing this talk meant that **the situational awareness** of the captain and co-pilot was reduced and they failed to spot that they were on the wrong runway. Their perception of reality was different to the actual reality. Despite the co-pilot pointing out that there were no lights on the runway it was another 15 seconds before the captain realised what was happening, by which time it was too late. They failed to stop work despite recoginising a hazard (there were no lights even though it was dark). If they had stopped work and brought their situational awareness in line with actual reality, 49 people would still be alive today!

What is situation awareness and examples?

Verbal answer

What is situation awareness?

Three-level model definition by M.Endsley:

"Situation awareness is the **perception** of the elements of the environment within a volume of time and space, the **comprehension** of their meaning, and the **projection** of their status in the near future."

Source: M. Endsley. Toward a theory of situation awareness in dynamic systems. In *Human Factors Journal*, volume 37(1), pages 32–64, March 1995.

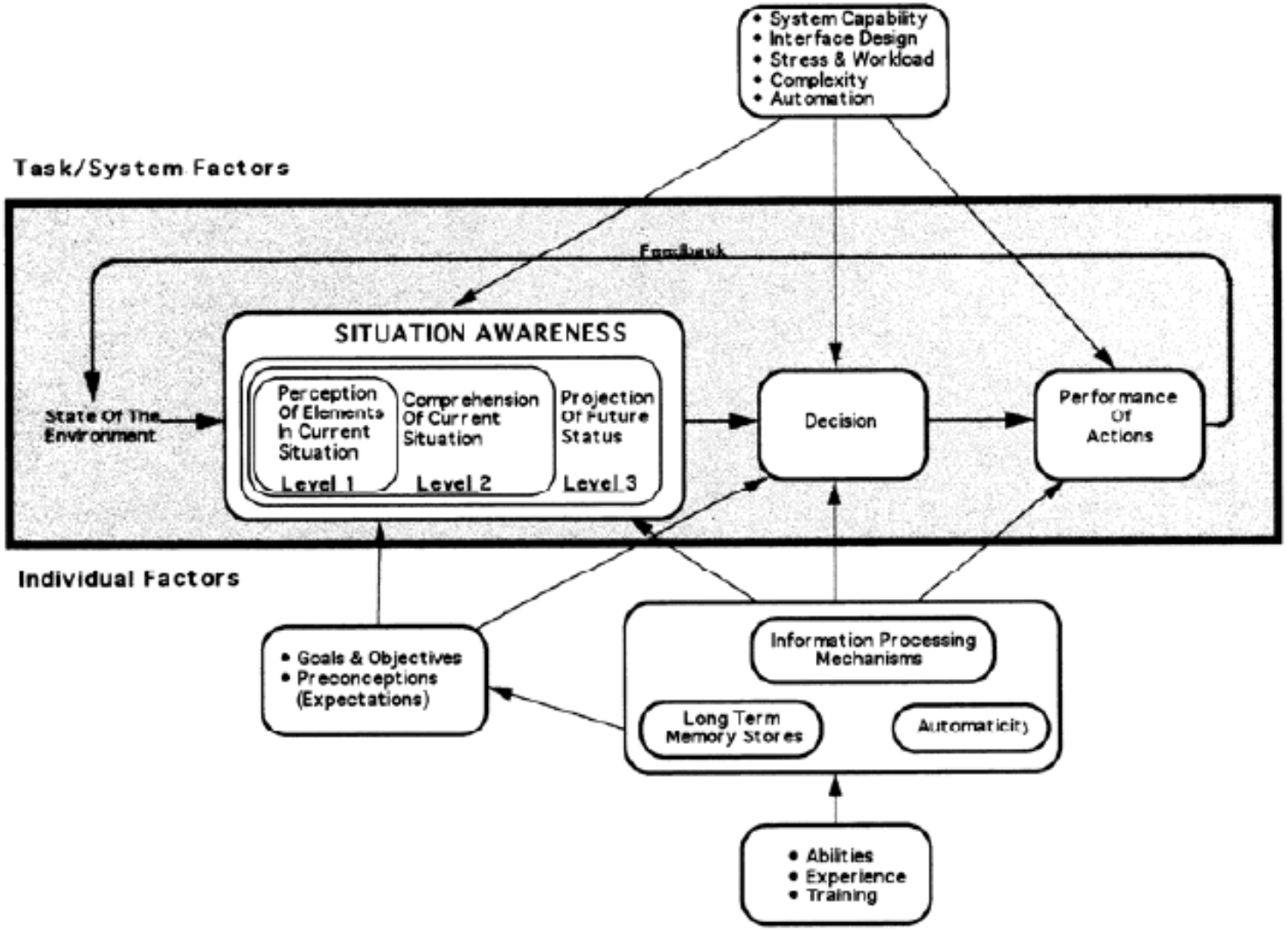


Figure three: The three-level model of situational awareness (from Endsley & Smolensky, 1998).

Source: Husák, Martin, Tomáš Jirsík, and Shanchieh Jay Yang. "SoK: contemporary issues and challenges to enable cyber situational awareness for network security." *Proceedings of the 15th International Conference on Availability, Reliability and Security*, 2020

Activity 1

Menti

Analyse the given example about the Comair flight 5191 accident and identify the “perception, comprehension and expected projection”.

Loss of situation awareness

Levels/Personnel	Flight Crew	Air Traffic Controllers
Level 1 SA	77.4%	72.4%
Level 2 SA	21.1%	17.2%
Level 3 SA	1.5%	10.4%

Table two. Percentage of situational awareness errors made at each level by flight crew and air traffic controller in the analysis of 262 errors committed in 143 incidents (data from Jones & Endsley, 1996).

LEVELS	Descriptions of error types	Percentages
Level 1 SA	Data not available	13.0 %
	Data hard to detect or discriminate	11.1%
	Failure to observe or monitor data	35.1%
	Misperception of data	8.7%
	Forget data	8.4%
Level 2 SA	Lack of, or incomplete, mental model	6.9%
	Use of incorrect mental model	6.5%
	Over-reliance on default values	4.6%
	Other	2.3%
Level 3 SA	Lack of, or incomplete, mental model	0.4%
	Over-projection of current trends	1.1%
	Other	1.9%

Table three. Taxonomy of 262 errors based on the analysis of 143 aviation incidents (data from Jones & Endsley, 1996).

Source: Stanton, Neville A., Peter RG Chambers, and John Piggott. "Situational awareness and safety." *Safety science* 39.3 (2001): 189-204.

Cyber situation awareness

An application of generic situational awareness (SA) into the cyber domain

- perceiving the cyber environment,
- understanding the current security situation,
- being able to project how the situation will evolve

Activity 2: What are new challenges of situation awareness in cyber space compared to physical world? menti

Example

Perception: The system seems slower than normal

Comprehension: after analysing the unusually slow network traffic, identify it is a DDoS attack

Projection: predict that the system will be disrupted within a few hours

Tools for Cyber situation awareness

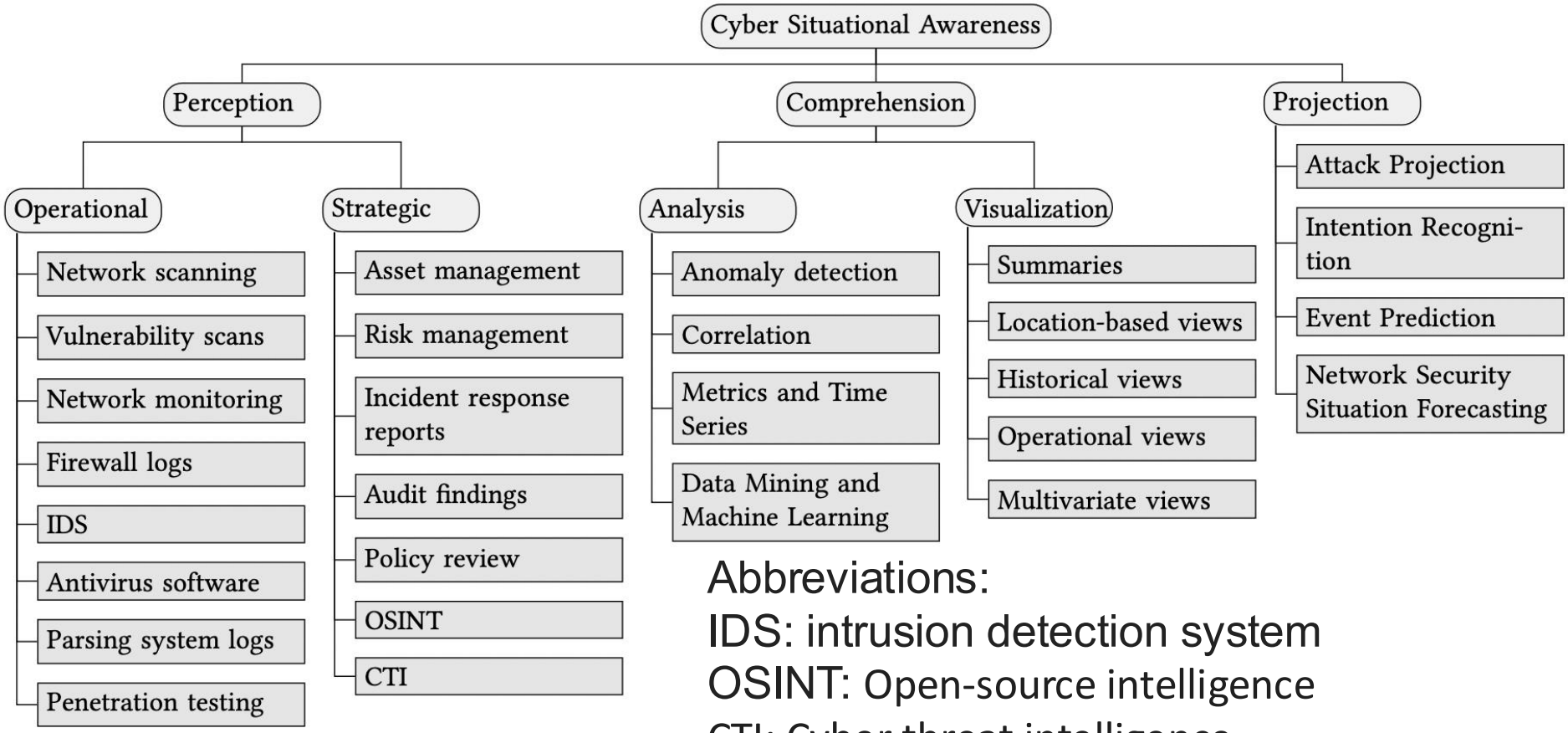


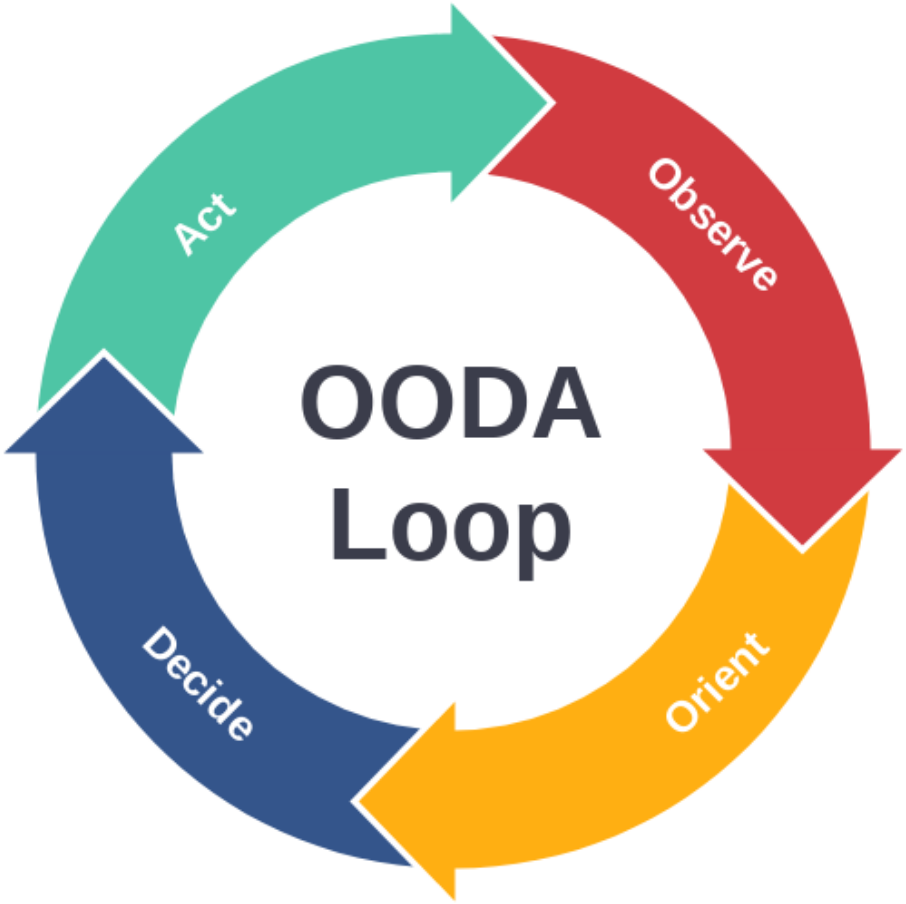
Figure 3: Taxonomy of Cyber Situational Awareness tools and components.

Source: Husák, M., Jirsík, T. and Yang, S.J., 2020, August. SoK: Contemporary issues and challenges to enable cyber situational awareness for network security. In *Proceedings of the 15th International Conference on Availability, Reliability and Security* (pp. 1-10).

OODA loop for cyber situation awareness

- Developed by military strategist and United State air force colonel John Boyd
- OODA for cyber situation awareness: used as a conceptual framework for achieving human cyber situational awareness
- OODA for SOC (Security Operating Center): enables efficient monitoring, analysis, decision-making, and action, ensuring the security of digital assets.

OODA loop for cyber situation awareness



Observe

What is the current situation? What is the reason you want to change? how bad do you want to change?

Orient

Where are you currently at relative to where you want to go? How far is it to your destination?

Decide

What is the exact path you are going to take? How are you going to handle challenges and set backs?

Act

What's the approach and method you will take to implement the decisions? What is your action plan?

OODA loop for cyber situation awareness – Activity 3 (menti)

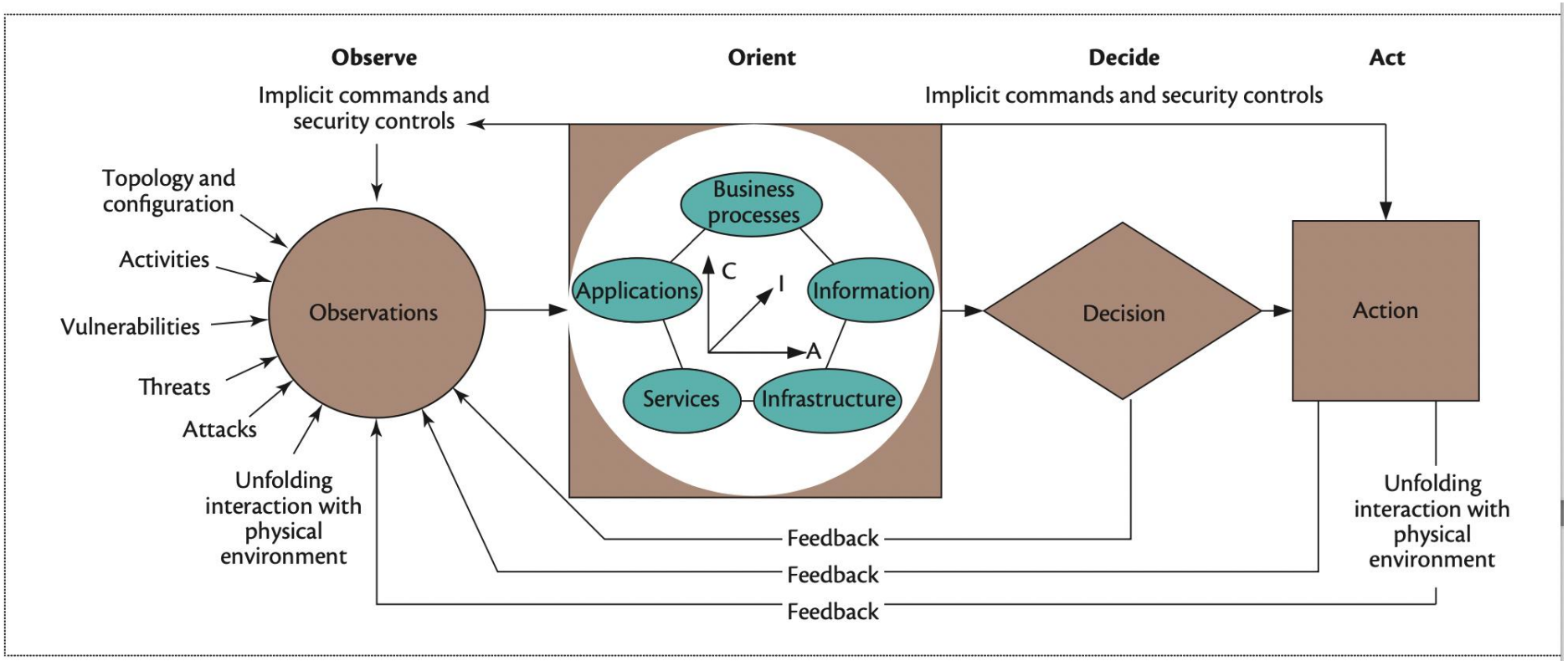


Figure 3. OODA (observe, orient, decide, act) loop for advanced situational awareness in cyberspace (inspired by Christian Sorensen's "Cyber OODA: Towards a Conceptual Cyberspace Framework"[4]). The goal is to process this cycle quickly by observing and reacting to unfolding events more rapidly than an opponent and therefore gain the advantage.

C: confidentiality, I: integrity, A: availability

Source: Lenders, Vincent, Axel Tanner, and Albert Blarer. "Gaining an edge in cyberspace with advanced situational awareness." IEEE Security & Privacy 13.2 (2015): 65-74.

Example

Assume you observe anomalous network traffic patterns indicating a malware infection on a central network node, what will you do (Orient, Decide, Act)?

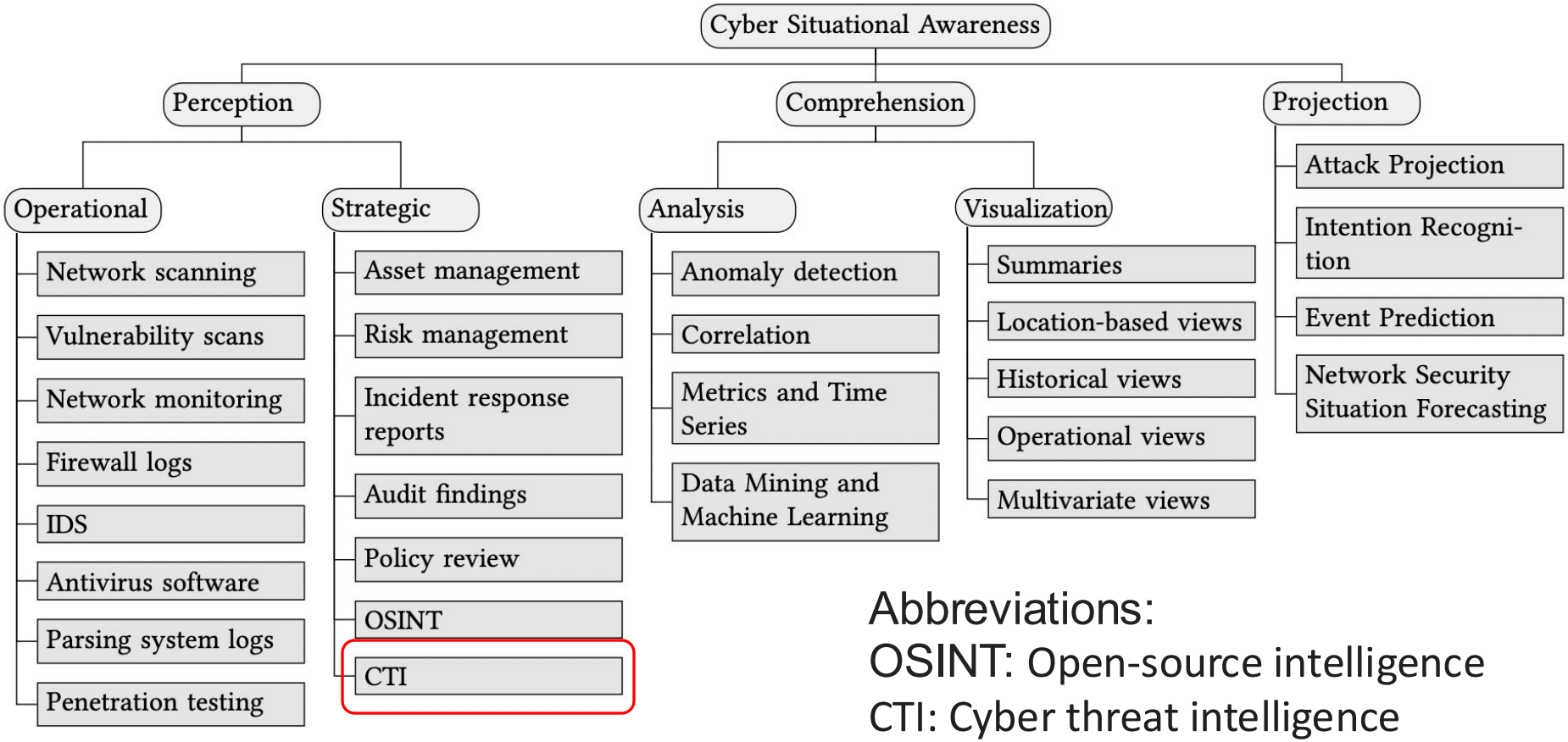
(verbal answer)

Situational Awareness perspectives

Situation awareness (SA) has some focus areas which are interdependent:

- SA states (awareness): Research on SA states concerns how to describe the contents of SA and what contents to describe
- SA systems (distribution/exchange of SA): Research on SA systems concerns the location, distribution, and properties of SA in systems
- SA processes (updating SA states and guides when SA change): Research on SA process concerns how to describe processes of achieving and maintaining SA, and relations to processes of using SA (e.g. decision-making, coordination).

Cyber Threat Intelligence (CTI)



Abbreviations:
OSINT: Open-source intelligence
CTI: Cyber threat intelligence

Figure 3: Taxonomy of Cyber Situational Awareness tools and components.

Threat intelligence and Cyber threat intelligence

Method for situation awareness: threat intelligence

“TI is the process of acquiring, via multiple sources, knowledge about threats to an Environment” [Source: Bromiley, Matt. "Threat intelligence: What it is, and how to use it effectively." *SANS Institute InfoSec Reading Room* 15 (2016): 172.]

“Cyber threat intelligence (CTI) is the process of taking disparate pieces of information about a cyber attack and identifying the context in which it happened and what that means.” [Source: book “Cyber Threat Intelligence_ The No-Nonsense Guide for CISOs and Security Managers 2021”, page 17]

What CTI does

- analyzes data and uncovers the essential patterns of threats
- define context regarding **indicators of compromise** (**IoCs**) and the **Tactics, Techniques and Procedures** (TTP) of adversaries.
- Intelligence analysts and security professionals rely on IoCs to detect threat actors' activities.
- CTI is an **evidence-based** product and process.

Example of IoCs: domain information, IP addresses, SSL/TLS certificate information, file hashes, network scanning information, vulnerability assessment information, malware analysis results, packet inspection information, social media news (in raw format), email addresses, email senders, email links, and attachments.

The structure and position of the intelligence team in the organization security unit

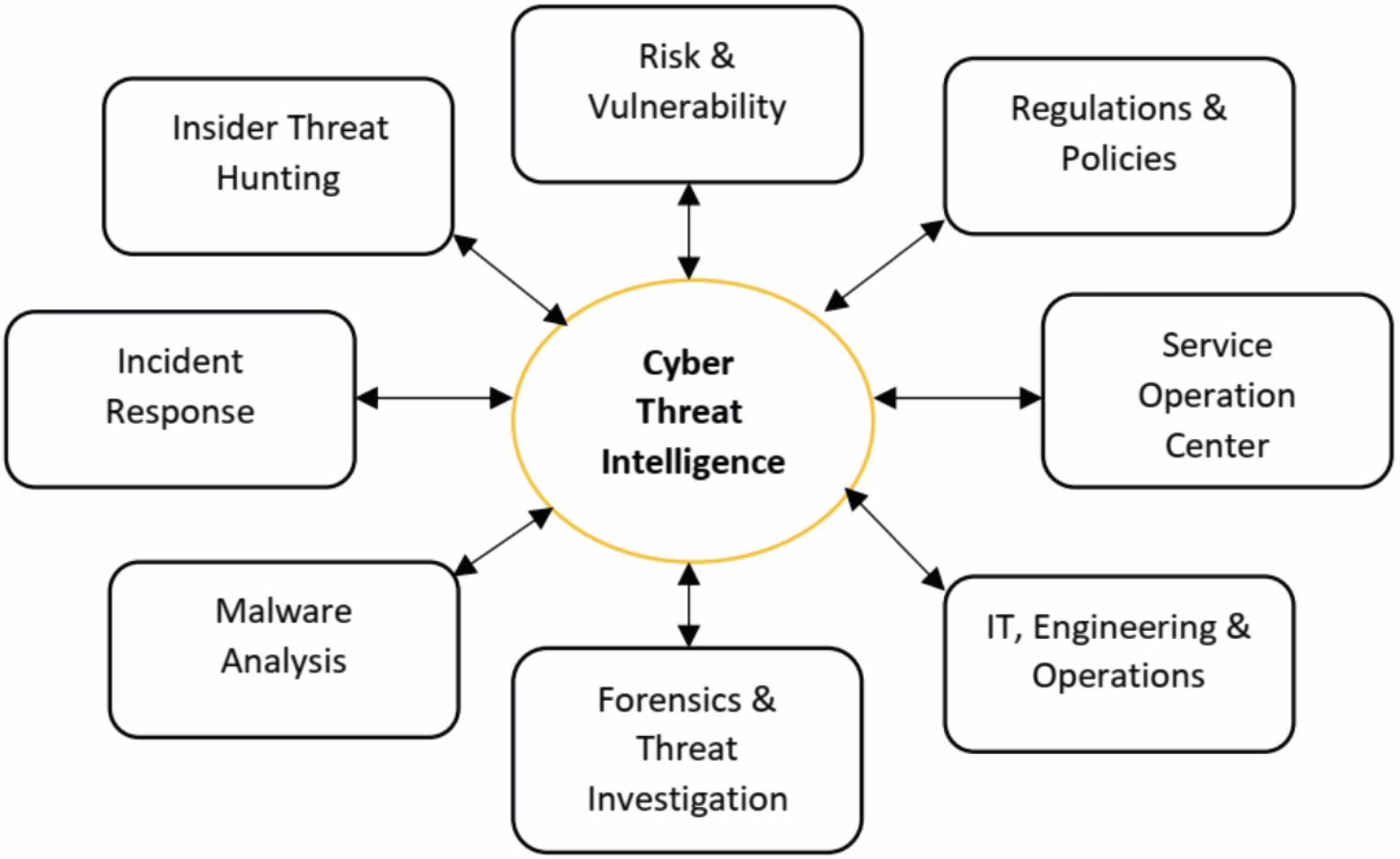


Figure 2.7 – Recommended threat intelligence position in the security landscape

Threat intelligence life cycle

Activity 4, menti

Read page 11-21, "Mastering cyber intelligence : gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense (download from DLE/primo or use the link below)

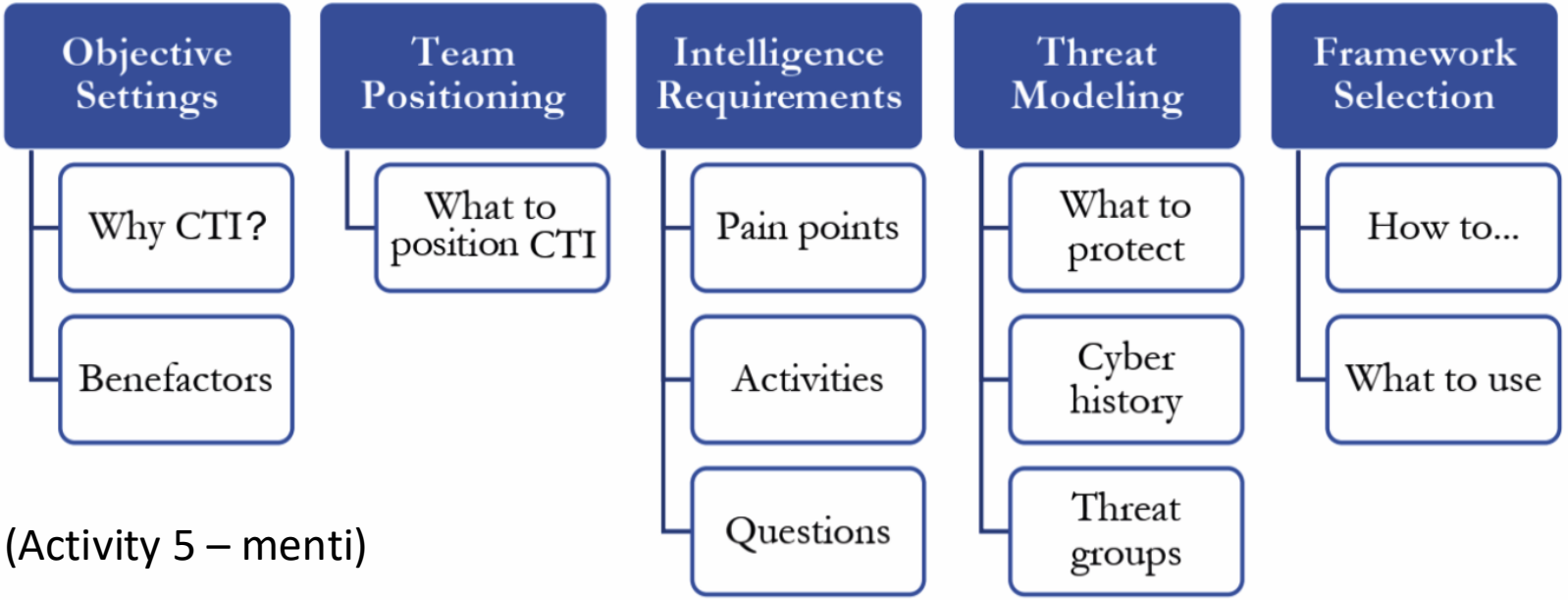
Figure 1.1 – Threat intelligence life cycle

Download link: https://portal-igpublish-com.plymouth.idm.oclc.org/iglibrary/obj/PACKT0006204

Source: Figure 1.1, page 5, Jean Nestor M. Dahj, "Mastering cyber intelligence : gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense"

1. Planning, objectives and direction

Read page 11-16, “Mastering cyber intelligence : gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense” , subsection “Planning, objectives and direction” and “Intelligence data processing”



(Activity 5 – menti)

Figure 1.4 – Threat intelligence planning and direction summary

Source: Figure 1.4, Jean Nestor M. Dahj, “Mastering cyber intelligence : gain comprehensive knowledge and skills to conduct threat intelligence for effective system defense”

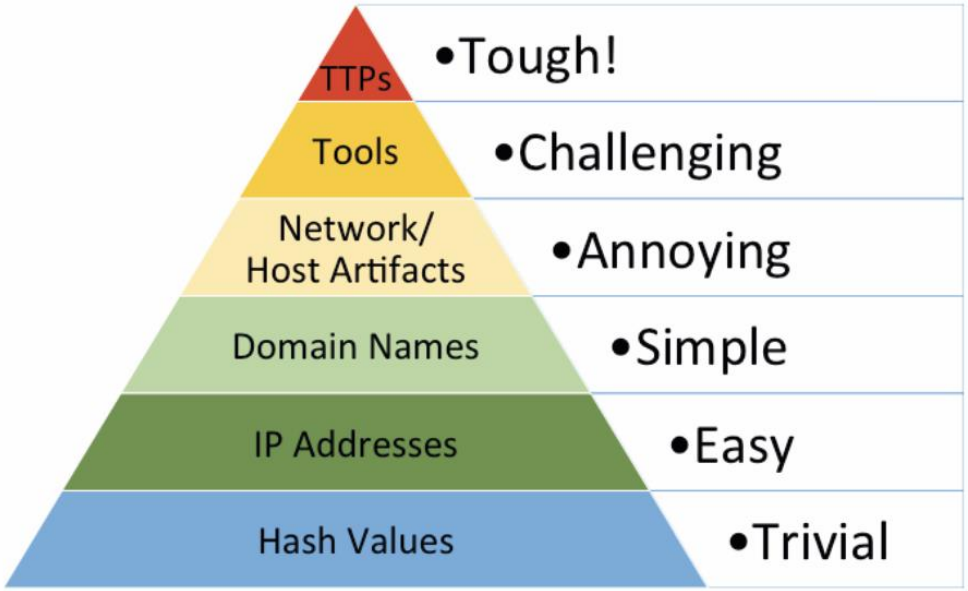
CTI requirements example - questions

CTI requirements (in the form of a question)	Prospective answer	Collection requirements (example for future steps)
Have attempted attacks happened in the organization?	Yes or no.	Check past security, networks, intrusion detection logs, and so on.
How did the organization detect or prevent the attack?	Firewall policies, deep packet inspection, intrusion detection and prevention, and so on.	Collect the relevant logs to understand the policies, rules, and so on.
What useful information was extracted from the attack?	Adversary details: origin (region), IP addresses, domains, attack model, and so on.	Collect the relevant logs.
Which vulnerabilities are being exploited globally?	Password brute forcing, phishing (social engineering), ransomware, and so on.	Collaborate with other organizations or other CTI analysts. Refer to online platforms to get information on those vulnerabilities, and so on.
How the organization been hacked before? How did it happen?	Yes or no. Through phishing. An HR executive opened an attachment from a malicious email who pretended to be an employee.	Refer to malware analysis, opensource feeds of malicious web links, emails, and so on.
What prospective vulnerabilities and threats are under research?	Crypto security, identity theft, high-level espionage, and so on.	Refer to online forums, the dark web, and so on.

Table 2.1 – CTI requirements – main questions

CTI requirements example – pain points
Pyramid of pain - IoCs and pain levels

Pyramid of pain provides correlations between indicator types and pain levels, illustrating the amount of pain it will cause adversaries should you block those IOCs



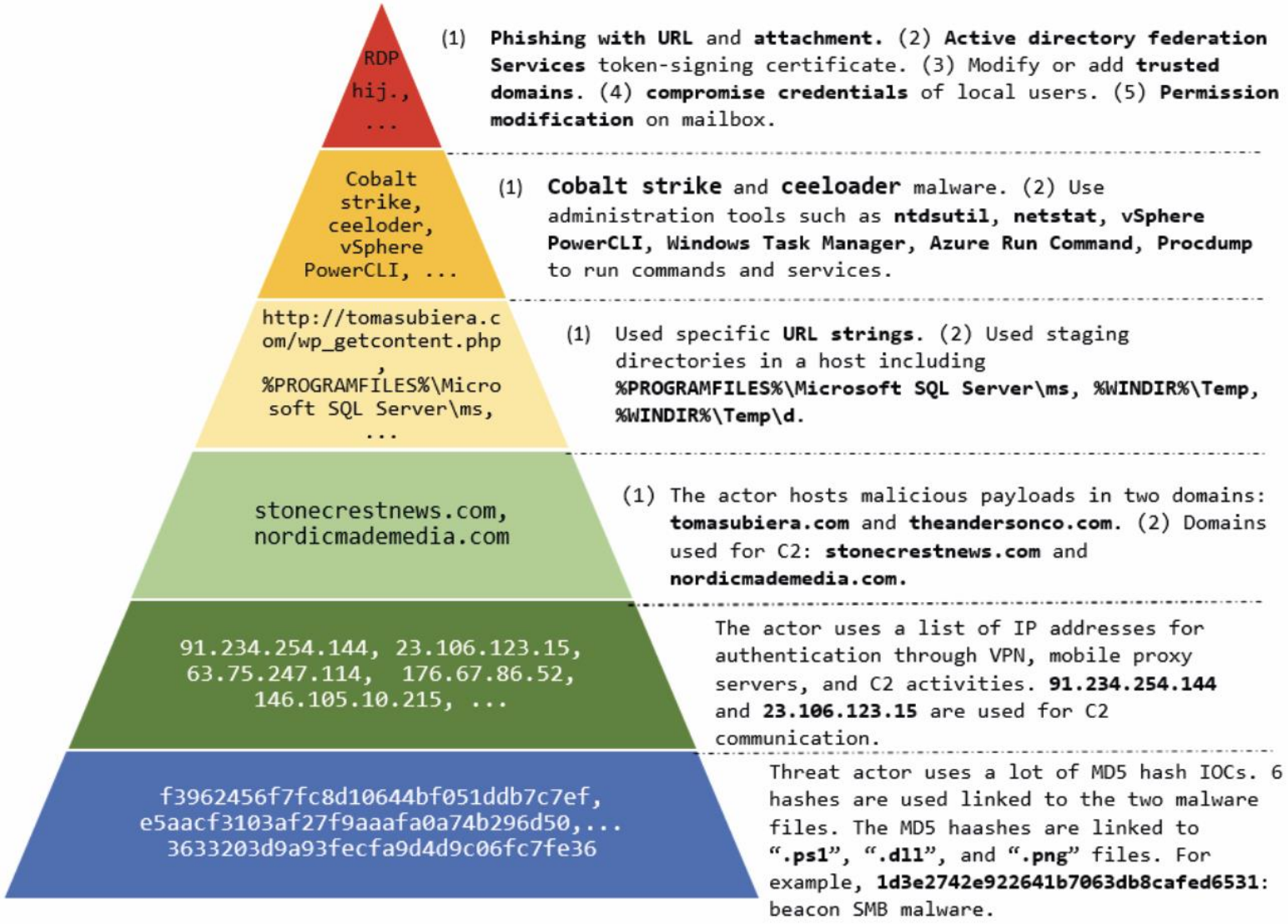


Figure 13.5 – The PoP illustration for a Nobelium activity targeting government and business entities around the globe

2. Collection

- Internal sources: intrusion analysis data by using the Lockheed Martin Kill Chain, such as internal malware analysis data (one of the most valuable data sources of threat intelligence), domain information, and TLS/SSL certificates, network element logs and records of past incident responses
- External sources: external malware analysis and online sandbox tools, technical blogs and magazines, the dark web, and other resourceful sources such as open source and counterintelligence data, Malware zoos

Example

Suppose an attacker sends an email to a person in the organization who downloads and opens an attachment. A trojan is installed on the system and creates a communication link with an adversary. The relevant data needs to be available to detect and react to such an incident.

For example, the threat intelligence analyst can use the network, domain, and certain protocol information to detect and prevent the trojan from infecting the system.

3. Data processing

- aims to process and format the big, collected data into a readable or easy-to-understand arrangement.
- needs to be automated by using intelligence platforms.
- Security information and event management (SIEM) tools are mostly used to facilitate intelligence data processing and exploration.
- Frameworks such as MITRE ATT&CK, Diamond model, and Kill Chain can all be used to process intelligence data smartly.

4. Analysis and production

- the interpretation step where the processed data is converted into indicators of compromise, alerts, and alarms, with the capability to notify all the relevant parties of any potential threats.
- requires human expertise.
- this is where human errors/ bias cause disruptions.
- Structured analytic techniques (SAT), created by the United States Government, can be used to avoid bias.

5. Dissemination

- distribute the intelligence product to the consumers.
- The dissemination step must be tracked to ensure continuity between intelligence cycles in a project
- Let's assume that an intelligence request has been logged in the system. A ticket should be created, reviewed, updated, answered, and shared with the relevant parties.
- write valuable reports that convey an honest message with the appropriate metrics and indicators to support the output

6. Feedback

- The benefactors, consumers, or target audience of the intelligence product evaluate and assess the project and mark it as successful or not.
- This feedback is then used as the initial objectives for the next CTI cycle's planning and direction phase

Intelligent frameworks

1. Lockheed Martin's Cyber Kill Chain framework
2. MITRE's ATTA&CK knowledge-based framework
3. Diamond model of intrusion analysis framework

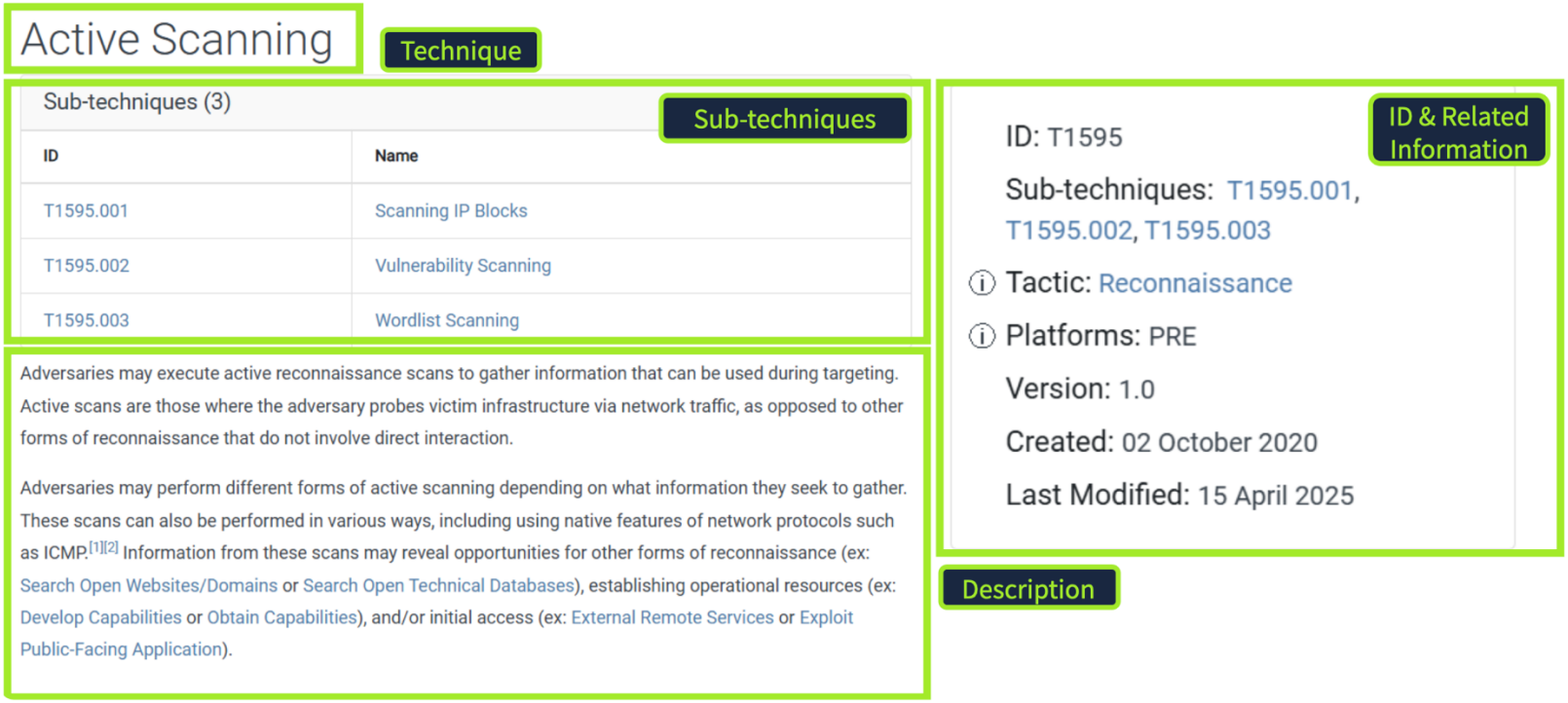
Cyber threat intelligence – Framework – Mitre's ATT&CK

- ATT&CK stands for Attack, Tactics, Techniques and Common Knowledge.
- Created in 2013 by MITRE to reflect the adversary's attack life cycle, from preparation to consequences
- Three domains: ATT&CK for Enterprise (incudes the adversary's behavior in most computer operating systems e.g. Linux, Windows, macOS, and cloud systems), ATT&CK for Mobile(adversaries' behavior in mobile systems e.g. Android and iOS, ATT&CK for ICS (adversaries' behavior in industrial control systems)
- ATT&CK structure:
  - Tactics: adversaries' objectives (the "Why" of the attack)
  - Techniques: adversaries' methods (the "How")
  - Matrix: includes tactics and techniques

(Activity 6 – menti)

https://attack.mitre.org

Example


Active Scanning
Technique
Sub-techniques (3)
Sub-techniques
ID
Name
T1595.001
Scanning IP Blocks
T1595.002
Vulnerability Scanning
T1595.003
Wordlist Scanning
ID & Related Information
ID: T1595
Sub-techniques: T1595.001, T1595.002, T1595.003
Tactic: Reconnaissance
Platforms: PRE
Version: 1.0
Created: 02 October 2020
Last Modified: 15 April 2025
Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction.
Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.[1][2] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: External Remote Services or Exploit Public-Facing Application).
Description

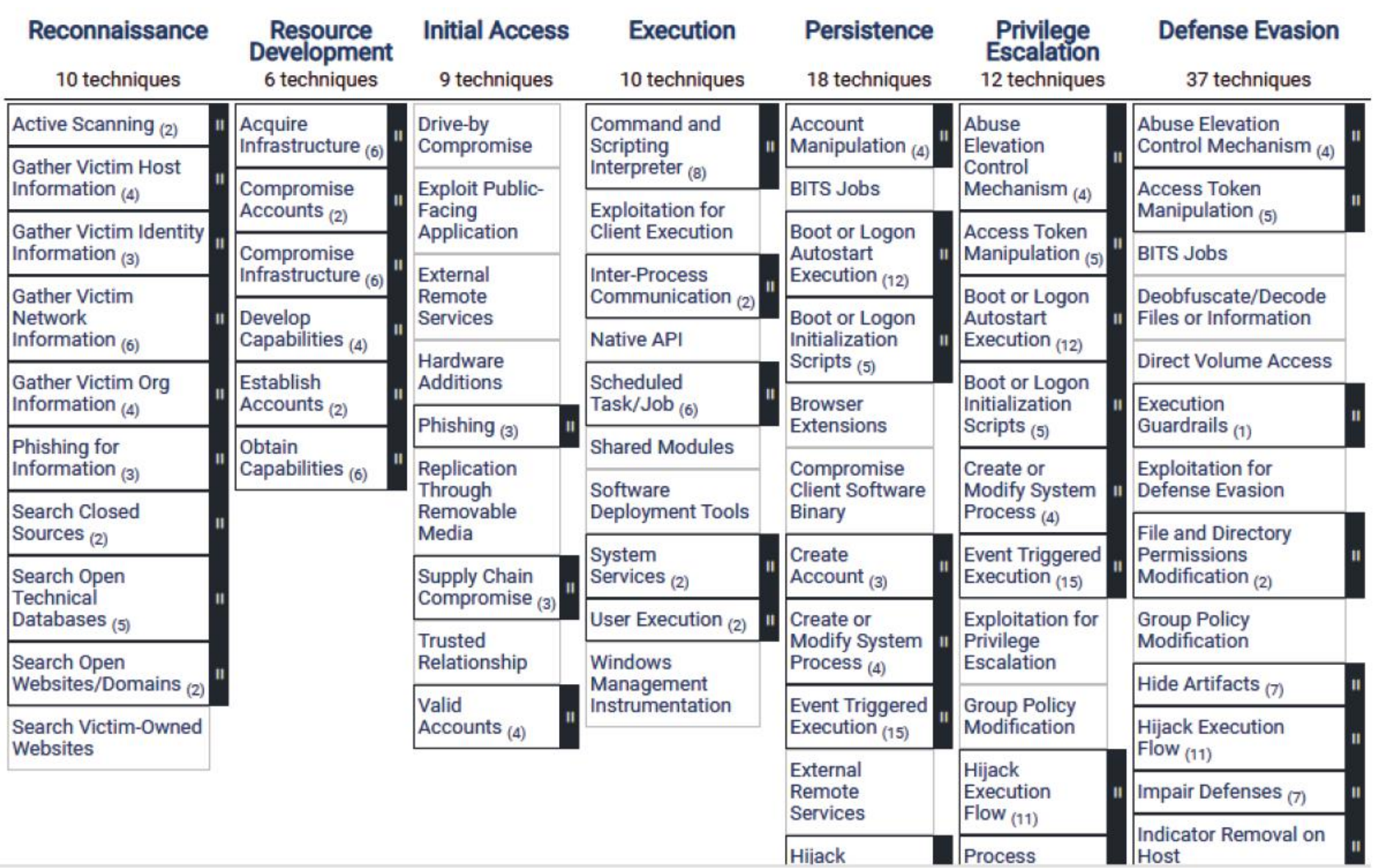


Figure 3.5 – Illustration of the ATT&CK matrix for Enterprise (full table can be seen at `https://attack.mitre.org/`)

Activity 7 - Identify the tactic, technique and subtechnique (method) in an attack using Mitre's ATT&CK (menti)

An adversary came across joe@abc.co.za on LinkedIn. Joe is a fan of soccer. They initiate an attack against Joe's organization. They choose to access the system using spearphishing (social engineering) by using another staff's email (Alice's email). They prepare and weaponize (embed malicious code) an excellent sports journal in PDF format. The journal is sent to Joe with a spoofed sender email address. Joe receives an email from someone pretending to be Alice with a legit ABC company email domain (alice@abc.co.za). The email contains a PDF that states, "Possible transfer of Kylian Mbappe to Liverpool FC. Hey Joe, did you see the latest rumor about the arrival of Mbappe to Anfield? Check the attached article." Joe, excited, opens the attachment and reads the article. The system is compromised.

Example-Where CTI helps?

- Security Operations Center (SOC) is a team of IT security professionals tasked with monitoring, preventing , detecting , investigating, and responding to threats within a company's network and systems.

CTI helps in triage (the process of evaluating, classifying, prioritizing, and responding to security alerts to identify and address real threats while filtering out false positives)

What is SOC? https://www.paloaltonetworks.com/cyberpedia/what-is-a-soc

Situation Awareness in Information Environment

The information environment is the aggregate of individuals, organizations and systems (resources) that collect, process, disseminate, or act on information.

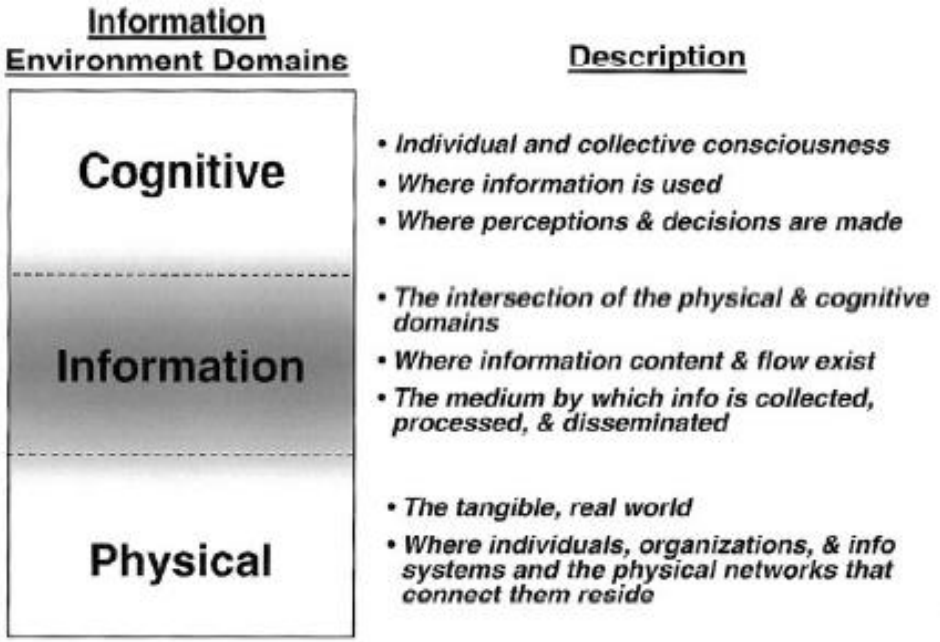
The information environment can be broken into three distant domains, but these are not separate and information can pass across different domains (social-technical, cyber-physical, etc.)

1) Physical

2) Information

3) Cognitive

Information Environment



Information Environment Construct

Source: Cordray III, Robert, and Marc J. Romanych. "Mapping the information environment." *IO Sphere* (2005): 7-10.

Physical Domain

The physical domain can be used to take in contextual information:

* location

* environmental hazards

* traffic of physical objects

This can provide situational information, but also operational technology (e.g., robot arms) have cross cyber and physical domains.

Information domain

The bulk of cyber-security information, used for situational awareness, is gathered in this domain. For IT security, all can be collected here. Here most information necessary for situational awareness is:

* generated
* collected
* processed
* stored
* disseminated
* displayed
* protected

The Cognitive domain

The human cognition is a nice term for how computer-human interactions

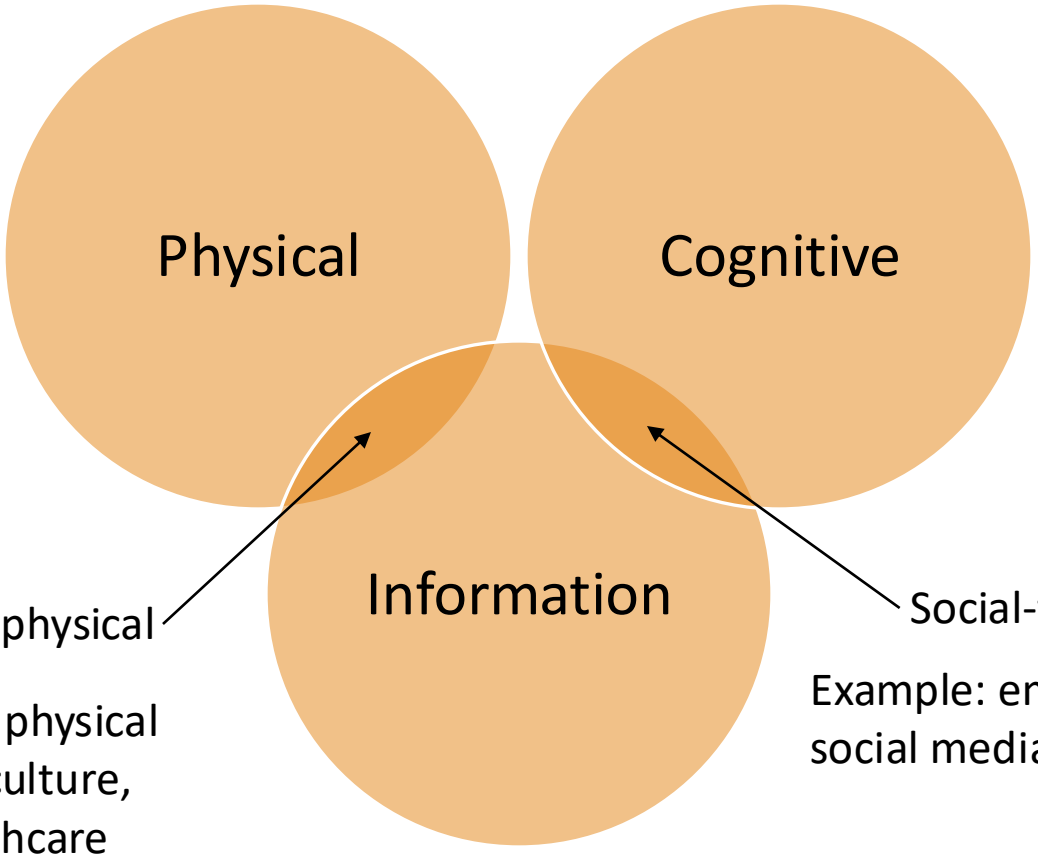
* Most systems designed to be user driven
* Accurate data can be misinterpreted
* Processing information
* Constructing understanding
* Applying knowledge
* Solving issues

Activity 8

Menti

Cyber physical and social technical

The three domains are not separate



Example: cyber physical systems in agriculture, transport, healthcare

Example: emails, blogs, social media sites

Benefits of Situational Awareness, threat intelligence

What is going on in your environment?

How can this information be used to aid decisions?

* organisation risk assessment

* organisation cyber-security prevention/detection

* security hardening of single devices or network/network segments

* response to attack/compromise

* [also good for getting hired]

Benefits of Situational Awareness, threat intelligence in Policies and Governance

Organisational assets exist to enable day-to-day operations. Prioritizing protecting these assets should be clear based on possible outcomes.

* Nothing is “100% secure”, prioritizing important.
* Asset protection policy prevent security incidences/breaches
* Intrusion detection detects when incident/breach occurs
* Policy determine how to respond to issues

The better the understanding about how individual/networked assets are used, by who, and when, determine likelihood of issue and the threat intelligence help prioritise security solutions.

SA terms for this module

We will think of situational awareness in terms of four components:

1. Know what the system is, and how it should work
2. Track the digital information in the system
3. Understand behaviours (e.g. abnormal vs normal)
4. React to abnormal or malicious behaviours

There are many terms for general SA, but these work best with a lot of the networking aspects we will be focusing on

1. Know the system

Before jumping into network cybersecurity, need an understanding of the network setup (topology) users, and uses

* legitimate users of internal/public-facing systems and networks

* authorized devices on network and use

* approved processes and application (where allowed, how used)

The more precise the information to security personally and detection solutions, the easier to detect issues and address them. Well-defined policies, trained employees, updated systems, detailed network diagrams, and well designed security systems help.

2. Track the information

Knowing what *should be* and knowing *what is* are different. Cybersecurity teams cannot directly monitor all in information domain (let alone all domains) monitoring tools are needed.

* observed devices, processes/applications, and users

* watch known vulnerabilities in devices, processes, and applications

* how usage of various systems and devices is changing

* what usage patterns and cycles exist for systems, devices, and users

Different terms, but need information points and a way to integrate that information that is useful to analysts.

3. Understand behaviours

A security issue occurs when something that shouldn't happen, does happen. Some of these are very difficult to detect. Some high-level methods to understand behaviours are:

* direct policy violation

* deviations from historical data

* unusual outliers showing up in outlier-detection analyses

* “newness” identification

* tactic, technique, and procedure matching

We will discuss more technical methods later in this module

4. React

Going through steps 1-3 is not very useful if in the end you or an organisation does not plan to act on the threat intelligence/SA.

* report to the appropriate people
* ethically analyse the incident further
* clean up system, removing threat
* hardening system to prevent repeat

Threat Reports – or live

Kaspersky

McAfee

FireEye

Government

NVSC

Cisco

Gartner

SANS

(2020 https://www.varonis.com/blog/cybersecurity-statistics/)

(2021, https://umbrella.cisco.com/info/cybersecurity-threat-trends-report)

Activity 9– Match (menti)

1. Movie streaming service
2. Online game store
3. Food delivery
4. Mobile company
5. Company finance (payslip)

a. Vulnerability in GPS tracking
b. Online payment vulnerability
c. Website vulnerabilities
d. 3G/4G vulnerabilities
e. Server vulnerabilities

Activity 10

1. Choose your group (5-6 students)
2. Pick a company (or a conceptual company with a service). Example: Movie streaming service, Online game store, food delivery, university
3. Look for some threat reports by using the relevant keywords. Example: if you choose a university in question 2, you can use keyword threat report + education sector to search for the information

2020 https://www.varonis.com/blog/cybersecurity-statistics/

2021 https://umbrella.cisco.com/info/cybersecurity-threat-trends-report

2024 https://www.cisco.com/c/dam/m/en_in/events/security-conclave-2024/radware-threat-report-summary-2024.pdf

4. Find 3 statistics you think that company should be aware about for their threat analysis and why.
5. Prepare 2 slides: slide 1 – describe the company (question 2), slide 2 – name of the report and 3 important statistics of the potential threat, and present in 2 minutes