The Cyber Threat Landscape. Introduction to vulnerabilities.

TLP:CLEAR

INTRO

1. Actors
2. Threats
    1. Social Engineering
    2. Insider Threat
    3. Malware
    4. Unathorised Access
    5. System Design Failre
3. Attack Vectors
4. Attack Surface
5. Threat Intelligence
6. Threat Reports
7. Threat Landscape
8. How does it look in real life?

WHO ARE THE ACTORS?

EXPLORER

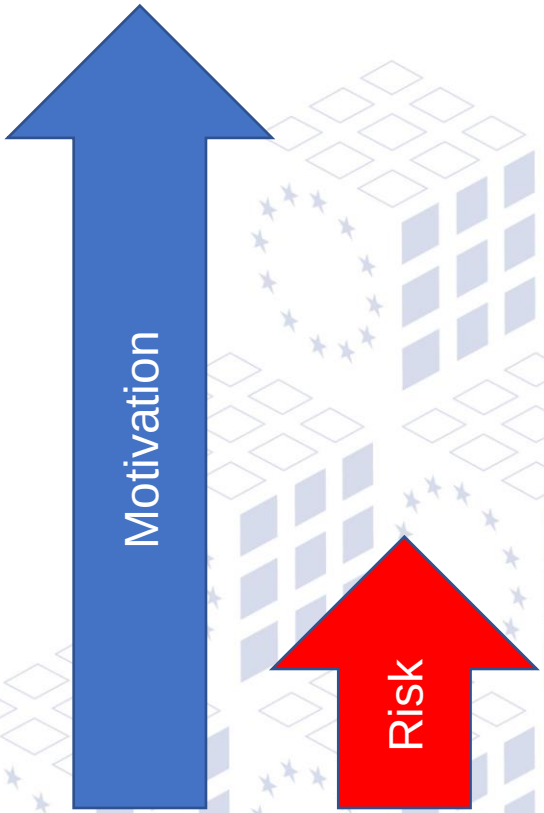
A.K.A. Script-kiddies

Drivers:

1. Curiosity
2. Show-off
3. Test skills

TTP:

1. Free or commercial hacking tools
2. Phishing
3. Opportunistic targeting
4. Reconnaissance

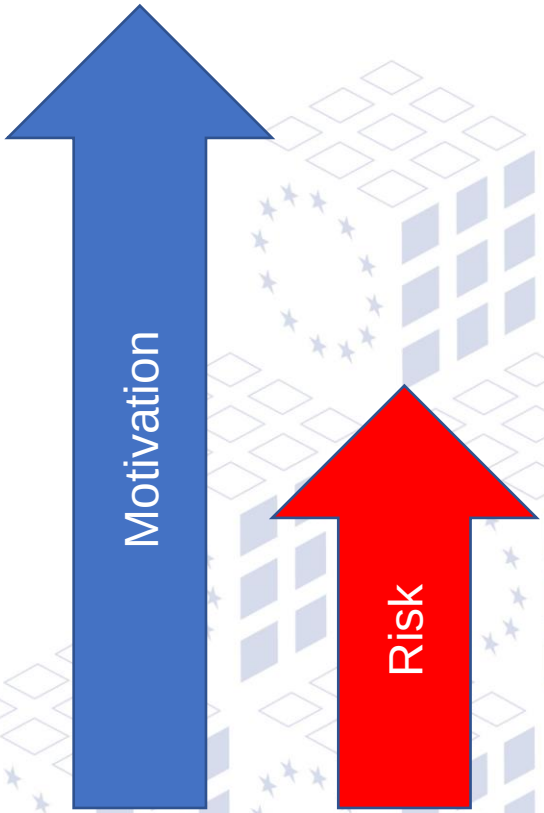


Explorers do not intend to inflict serious damage, but they might change a page on a website to embarrass someone or do something to advertise to the world how clever they are.

HACKTIVIST

Drivers:
1. Beliefs
2. Publicity
3. Ideology
4. Emotions

TTP:
1. DDoS, Deface, Doxxing
2. Ransomware (RaaS)
3. Public announcements
4. Propaganda
5. Short-term focus

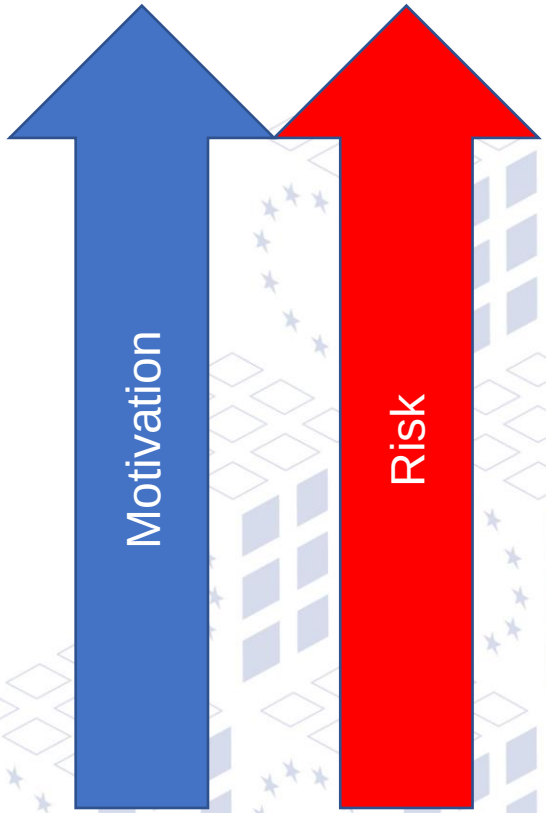


Hacktivists are motivated by ideology or are animated by an emotive force. The hacktivists' idealism drives them to act collectively in common cause against an enemy.

CYBERTERRORIST

Drivers:
1. Ideology
2. Fear
3. To intimidate
4. To Destabilise

TTP:
1. Custom tools
2. 1 day Exploits
3. APT
4. Leaks, sabotage
5. Targeted attacks

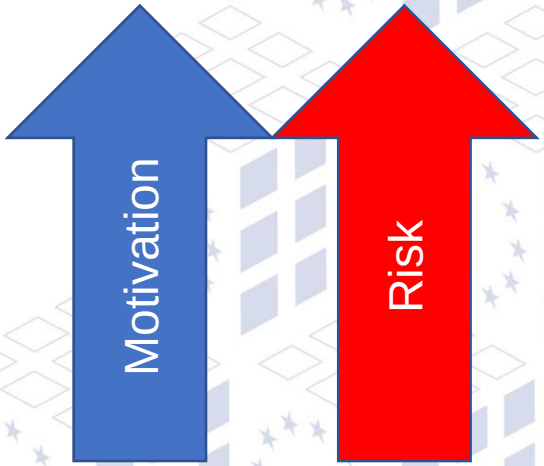


Cyber Terrorists strive to intimidate and destabilize a society by destroying or disrupting computer or communication networks. They like to target online infrastructure, such as nuclear power plants, natural gas pipelines, and electrical power grids.

CYBERCRIMINAL

Drivers:
1. Money

TTP:
1. Social Engineering
2. Identity theft
3. Ransomware
4. Opportunistic



Cybercriminals want money plain and simple. To achive this they steal, extort, mislead their victims.

CYBERWARRIOR

A.K.A. Nation-State hacker

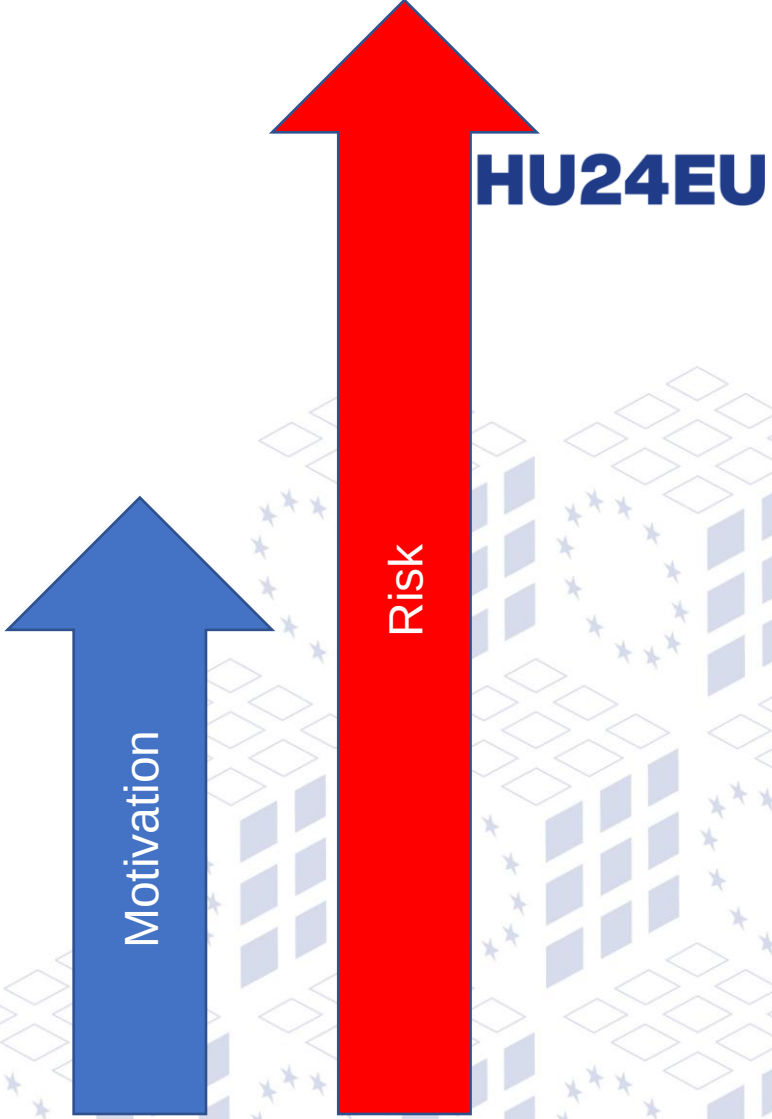
HU24EU

Drivers:

1. National Interest
2. Beliefs or money
3. Destroy, Distrupt or damage

TTP:

1. Tailor-made tools
2. Cyber Weapons
3. Espionage, extortion
4. 0 day Exploits



Cyberwarriors are the least self-interested, but are nonetheless the most dangerous because they have the resources of a nation-state at their disposal. Cyberwarriors are motivated by the national interests of their home country

TLP:CLEAR

THREATS

A **threat** is any potential event, action, or entity that can cause harm, damage, or compromise the **CIA** of a system, person, or organization. In cybersecurity, a threat refers to anything that could exploit a vulnerability to breach security, cause data loss, disrupt services, or cause harm to systems and networks. Threats can be intentional (like hackers or malware) or unintentional (such as system failures or user errors).

THREATS: SOCIAL ENGINEERING

Social Engineering is the act of manipulating people to gain advantage, often at the expense of those targeted.

All social engineering attacks are designed to benefit the attacker.

Most well-known Social Engineer: Kevin Mitnick

Techniques:

- Language
- Sense of urgency
- Quid pro quo
- Emotions (curiosity, excitement, anger, sadness, guilt)

Remember:
People want to help!

TLP:CLEAR

PHISHING

- Phishing is a Social Engineering attack **exploits** email as the **attack vector** and that it **targets anyone** with an email address.
- Phishing is simply **malicious spam** that is sent to as many people as possible with the hope that at least one will be taken in.
- Phishing has categorial meaning — it can be used to refer to all electronic social engineering attacks, such as **spear phishing**, **whaling**, **smishing**, and **vishing**

SPEARPHISHING

- Both spear phishing and whaling can be described as a social engineering attack that uses email to **target a specific individual** or group with the intent of stealing confidential information or profiting in some way.
- In a spear phishing attack, the bad actor targets an individual or category of individuals with lower profiles, such as the employees at that security company.

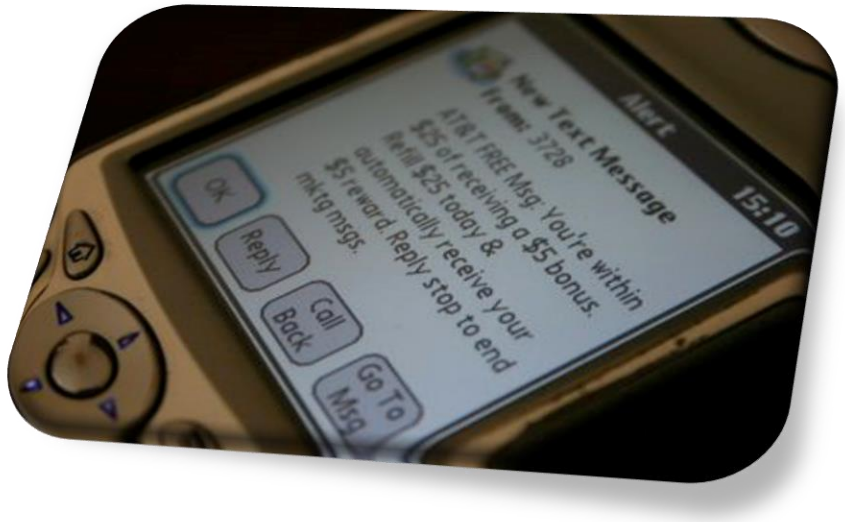
TLP:CLEAR

WHALING

- Both spear phishing and whaling can be described as a social engineering attack that uses email to **target a specific individual** or group with the intent of stealing confidential information or profiting in some way.
- In a whaling attack, the bad actor targets high-ranking individuals within an organization. When creating a whaling email, the attacker often does research on their target so that they can personalize the email in order to gain their target's trust.

SMISHING, VISHING

- SMS phishing (smsishing) & Voice phihing (vishing)
- With SMSishing and vishing are identical to phishing, spear phishing or whaling, except that the attack vectors are different.



TLP:CLEAR

PRETEXTING

- Pretexting is a type of social engineering attack that involves a situation, or pretext, created by an attacker in order to lure a victim into a vulnerable situation and to trick them

WATERING HOLE

- Watering hole is a computer attack strategy in which an attacker guesses or observes which websites an organization often uses and infects one or more of them with malware. Eventually, some member of the targeted group will become infected.

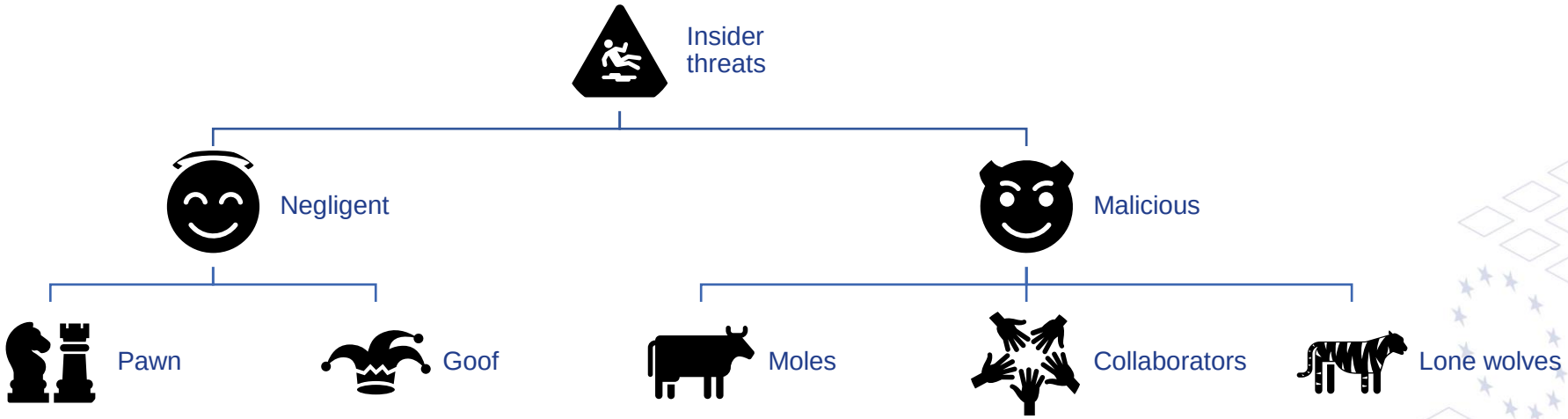
TLP:CLEAR

TAILGATING

- Tailgating involves a bad actor following someone with security clearance into a secure building or an access-controlled room

TLP:CLEAR

THREATS: INSIDER THREAT



- **Negligent**
  - No goals, careless action
- **Goals of Malicious:**
  - espionage
  - fraud
  - intellectual property theft
  - sabotage

TLP:CLEAR

THREATS: NEGLIGENT

A pawn is an authorized user who has been manipulated into unintentionally helping the bad actor, often through social engineering techniques, like tailgating or spear phishing.

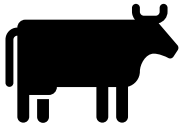
A goof is an insider who deliberately takes potentially harmful actions but harbors no malicious intent.

The goof is

- Arrogant
- Ignorant
- Incompetent
- Refuses following policies

TLP:CLEAR

THREATS: MALICIOUS



Mole is an outsider who gain access to the organization by posing as a vendor, partner, contractor, or employee.

Collaborators are authorized users who work with a third party.

Lone wolves work independently and without outside influence.

Attack vectors could be

- Tailgating
- Shoulder surfing
- Dumpster diving
- Eavesdropping

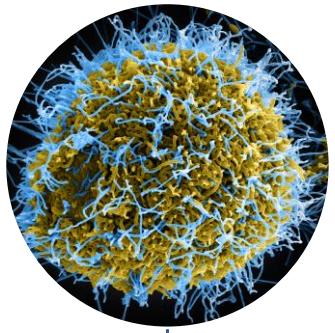
TLP:CLEAR

THREATS: MALWARE

TLP:CLEAR

VIRUS

A computer virus is a type of malicious code or program written to alter the way a computer operates and that is designed to spread from one computer to another. A virus operates by inserting or attaching itself to a legitimate program or document that supports macros in order to execute its code. In the process a virus has the potential to cause unexpected or damaging effects, such as harming the system software by corrupting or destroying data.



Virus

Resident virus

Non-resident virus

Viruses

- Boot sector virus
- Network viruses
- File infector
- Direct action virus
- Browser hijacker
- Overwrite viruses
- Web scripting virus

WORM

Worm malware does not need a host system and can spread between systems and networks without user action, whereas a virus requires a user to execute its code.

TLP:CLEAR

ROOTKIT

A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or an area of its software that is not otherwise allowed. A rootkit often masks its existence or the existence of other software. It operates near or within the kernel of the operating system, but it cannot self-replicate or spread across systems.

KEYLOGGER

A keylogger is a computer program that records every keystroke made by a computer user, with the purpose of gaining fraudulent access to passwords and other confidential information. Keyloggers are a type of spyware, which is malware designed to spy on victims. Because they can capture everything you type, keyloggers are one of the most invasive forms of malware.

POTENTIALLY UNWANTED PROGRAM

A potentially unwanted program (PUP) is a program that may be unwanted, despite the possibility that a user consented to download it. PUPs include spyware, adware, and dialers, and are often downloaded in conjunction with a program that the user wants.

SPYWARE

Spyware is malware that obtains covert information about a user’s computer activities by transmitting data secretly from the hard drive. Spyware is a type of malware that collects personal information and gathers data about a user without consent

TLP:CLEAR

ADWARE

Adware is a form of malware that hides on a device and displays ads. Some adware also monitors a user’s online behaviour so it can target them with specific ads.

TLP:CLEAR

DIALER

A dialer is a malicious program that is installed on a computer and tries to use the dialing features, often running up expensive phone bills for the victim. A dialer is unlike other types of spyware, though it is sometimes included with free software downloads.

TLP:CLEAR

ADVERSIAL ARTIFICAL INTELLIGENCE

Adversarial machine learning is a technique used in machine learning to fool or misguide a neural network with malicious input. Adversarial artificial intelligence uses specialized inputs created for the purpose of confusing a neural network, resulting in the misclassification of an input. These notorious inputs can be indistinguishable to the human eye but cause the network to fail to correctly identify an image.

RANSOMWARE

Ransomware is a type of virus that encrypts or prevents access to the information on a computer and restores access only after the user pays a ransom.

TLP:CLEAR

TROJAN HORSE

A Trojan horse virus is a virus disguised to look like something it is not. For example, viruses can be hidden within unofficial games, applications, file-sharing sites, and bootlegged movies. A remote access Trojan (RAT) virus is Trojan malware that can remotely control an infected computer.

TLP:CLEAR

DROPPER

A dropper is a type of Trojan horse that is designed to install malware on a computer. Once the dropper is installed, two things can happen: The dropper installs the embedded malware, or the dropper downloads the malware to the targeted computer.

TLP:CLEAR

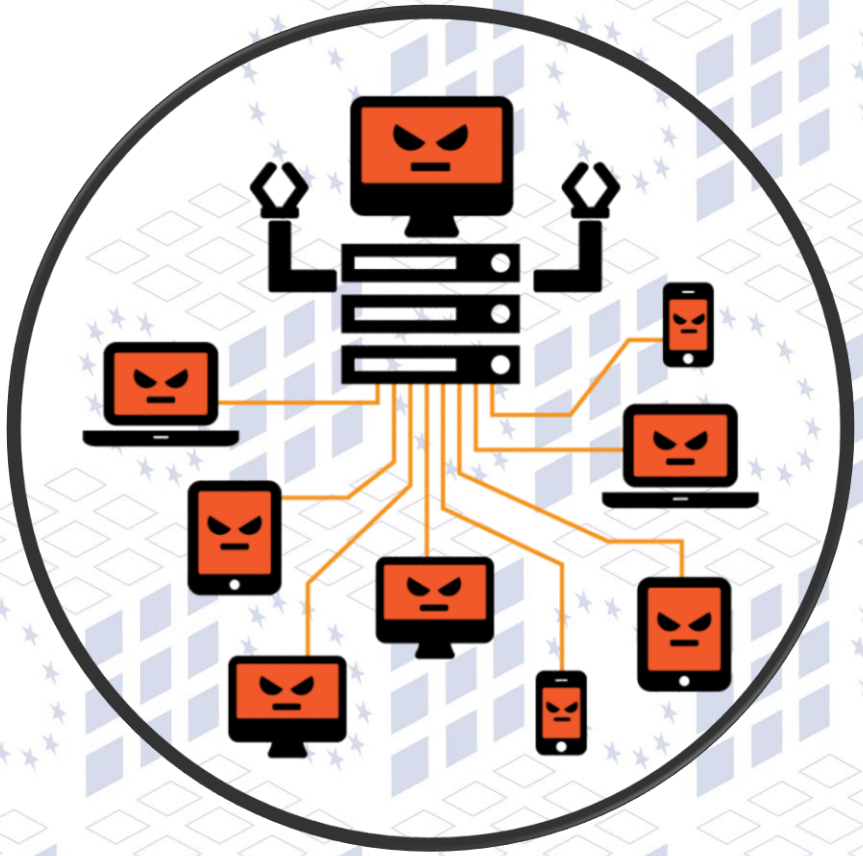
ROGUEWARE / SCAREWARE

Rogue security software, also known as rogueware or scareware, misleads a user into believing that there is malware on their computer and then prompts them to pay for antimalware, which is either fake or malware.

TLP:CLEAR

BOTNET MALWARE

Botnet malware controls its infected host through a command and control (C&C) server. An infected computer is named a bot, or robot, and a collection of infected computers is known as a botnet.



TLP:CLEAR

CRYPTOJACKER

Cryptojacking is the illegal use of computing resources to mine cryptocurrency. Attackers use malware or scripting to hijack a computer. For example, Coinhive was a cryptocurrency mining service that allowed website owners to embed JavaScript code on their websites, which hijacked the resources of connected computers for cryptomining purposes. This type of exploit is called in-browser mining.

THREATS: UNAUTHORISED ACCESS

…to physical places

…to computer systems

TLP:CLEAR

THREATS: SYSTEM DESIGN FAILURE

System design failure is a security flaw in a computer system or application that the bad actor exploits to gain access to a computer system.

- Stored clear passwords
- Reused unsafe code
- Lack of input validation
- Use of inadequate variables

VULNERABILITIES

Figure 14: Percentage of CVEs by Severity (Percentage of the total)

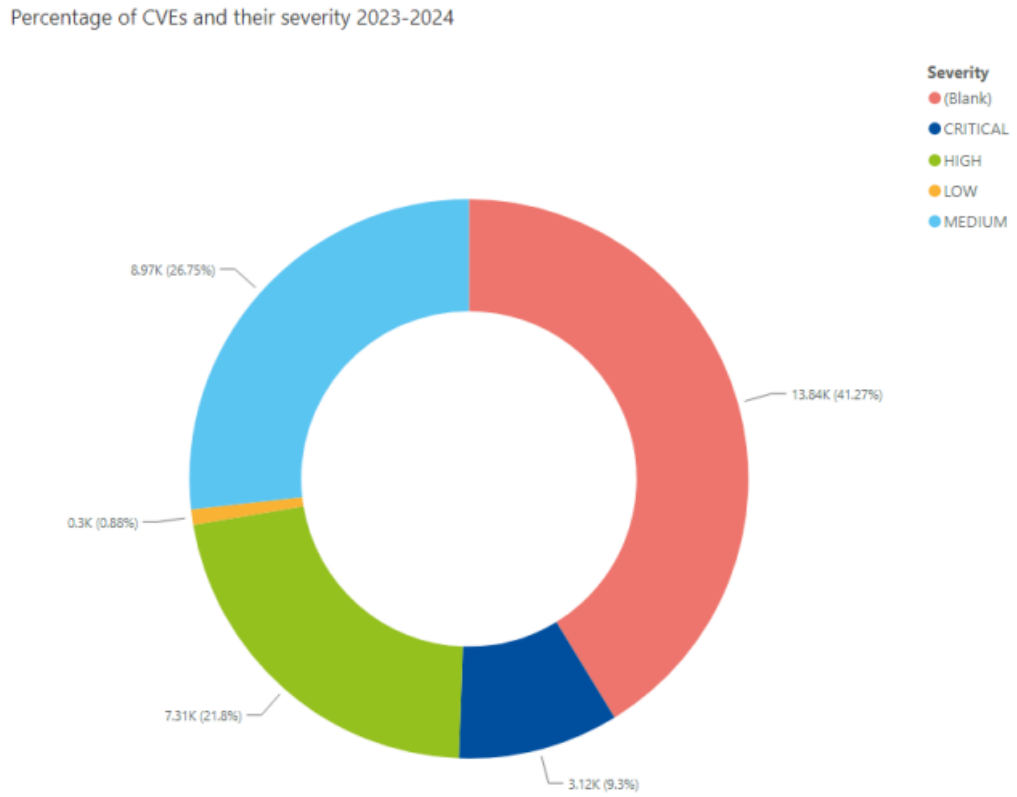
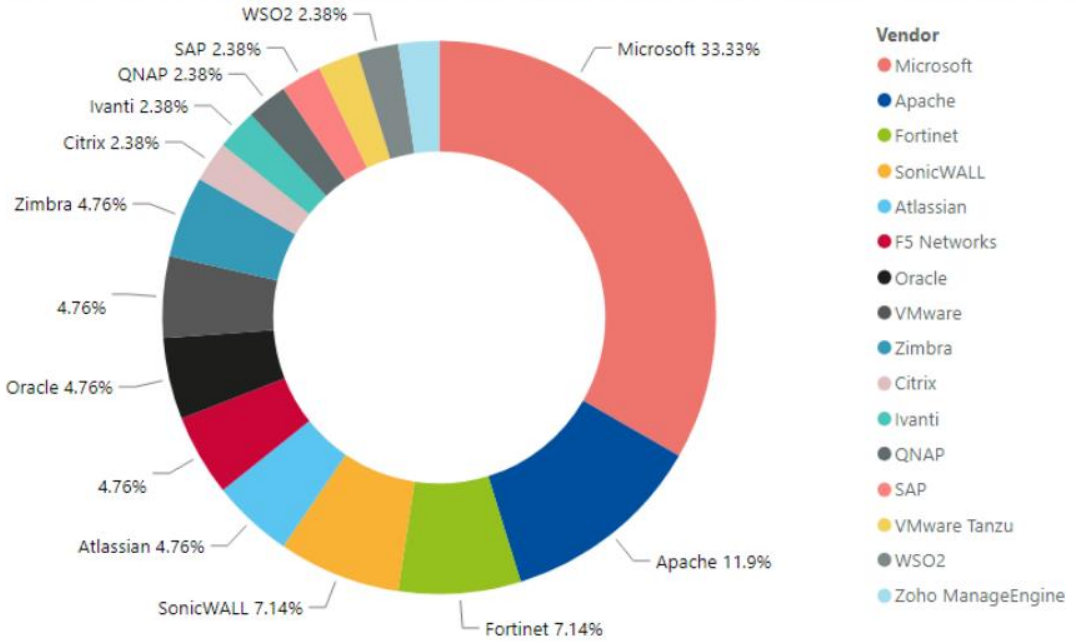
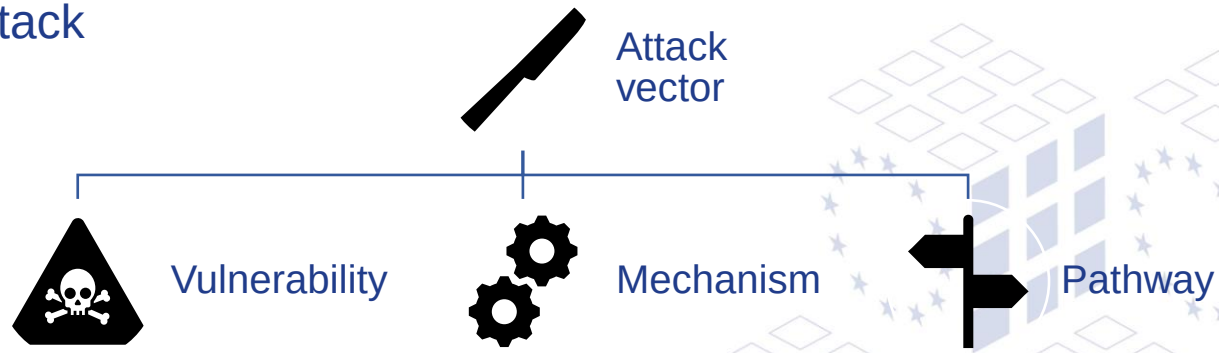


Figure 18: 2022 Top routinely exploited vulnerabilities by Vendors (2023 version hasn't been published)



ATTACK VECTOR

An attack vector is the method used to attack a target. It can be either a specific Method or Category of attack



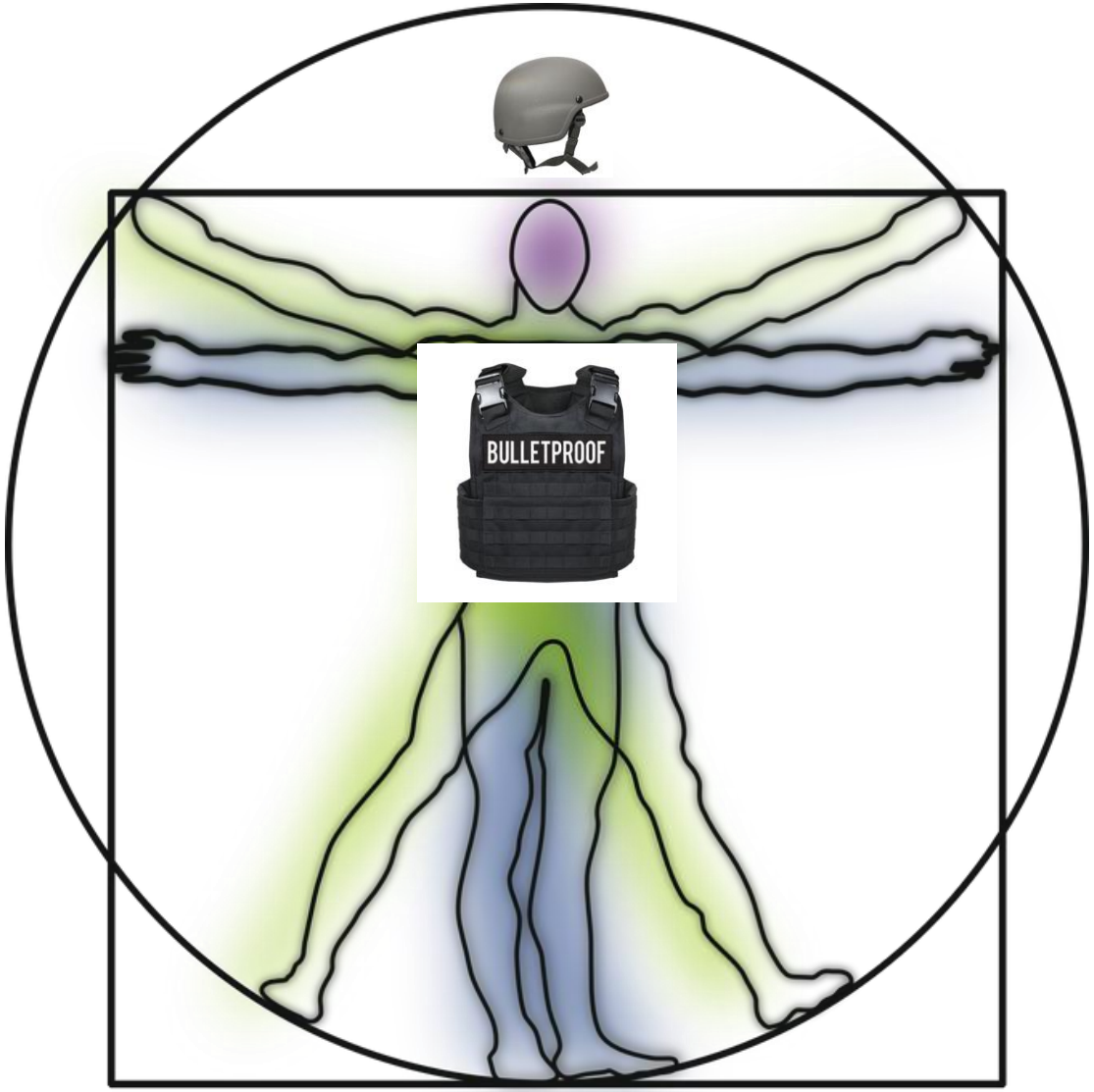
Attack Method	SQLi
	DDoS
	XSS
Attack category	Social Engineering
	Malware attacks
	Supply chain attacks

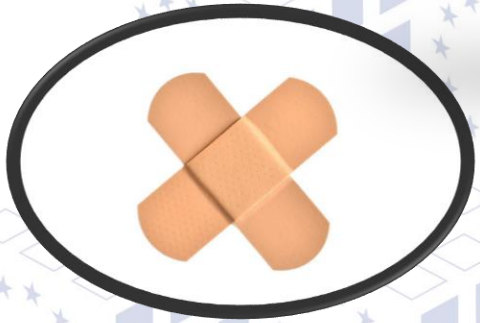
Vulnerability	Mechanism	Pathway
Server	Botnet	Internet
Buffer overflow	Backdoor	Watering hole
Open database	Logic bomb	Human

TLP:CLEAR

HU24EU

ATTACK SURFACE





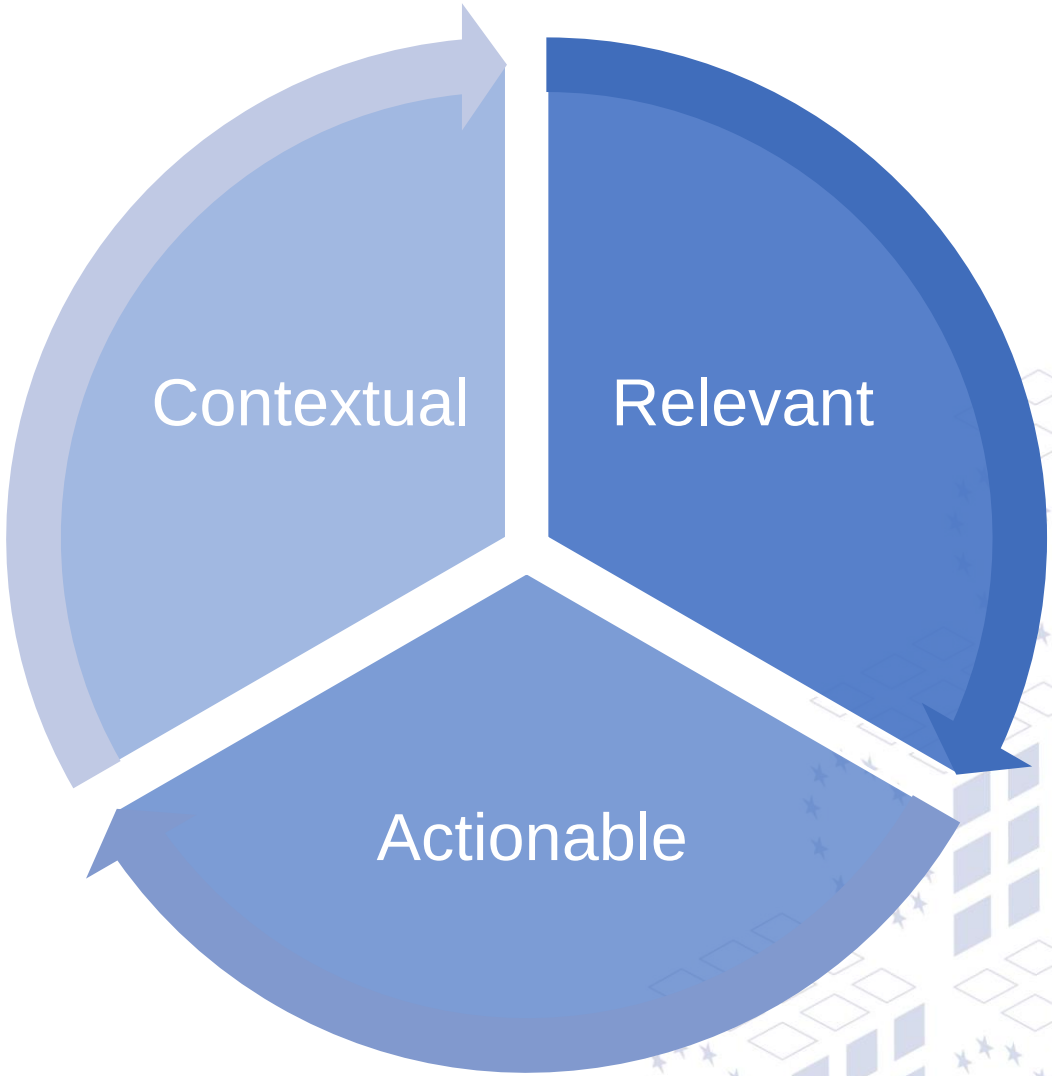
WHAT IS THREAT INTELLIGENCE?

„Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard.”

Gartner, 16 May 2013

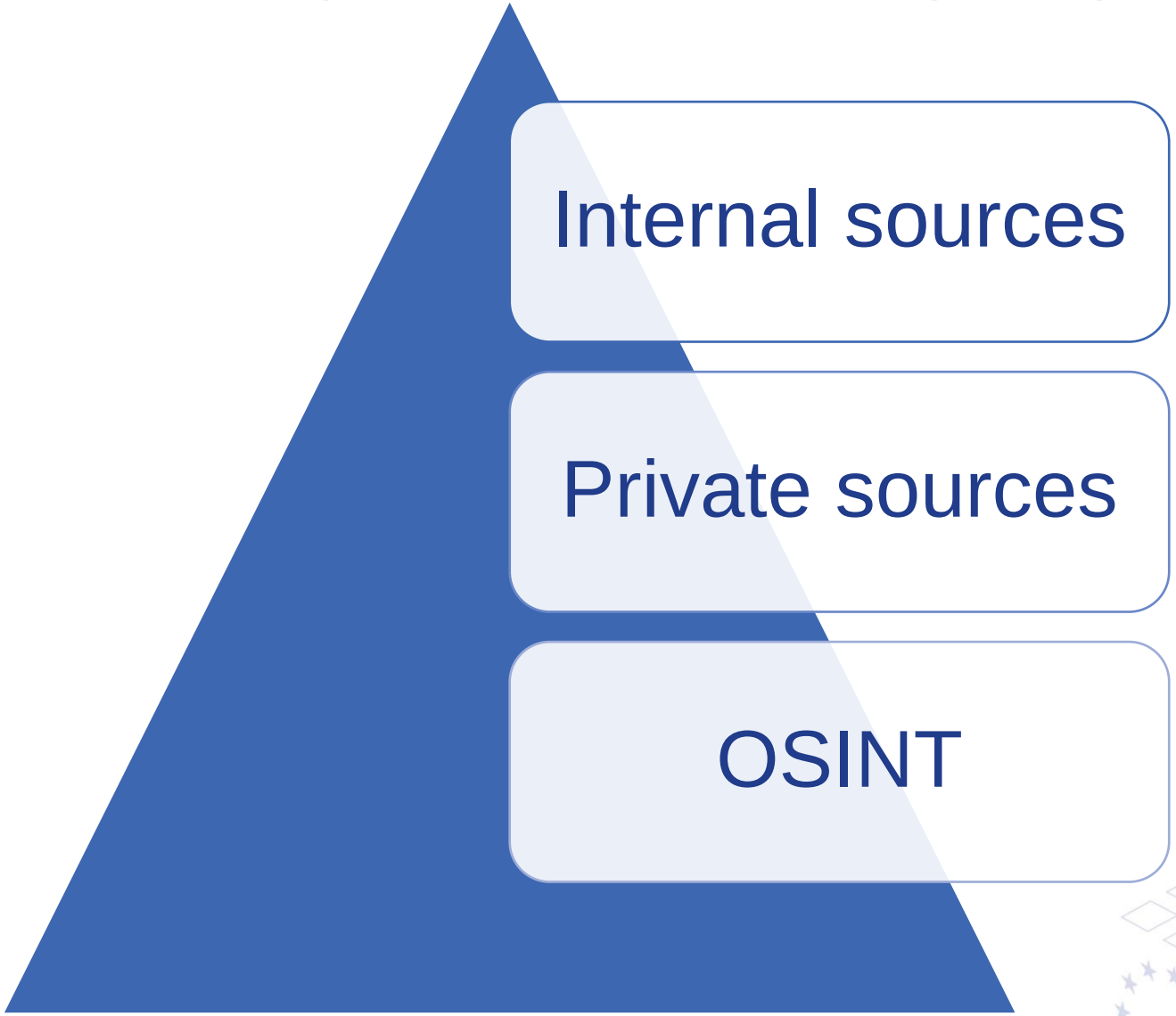
TLP:CLEAR

WHAT IS THREAT INTELLIGENCE?



TLP:CLEAR

WHERE DO I FIND INTELLIGENCE?



Reliability

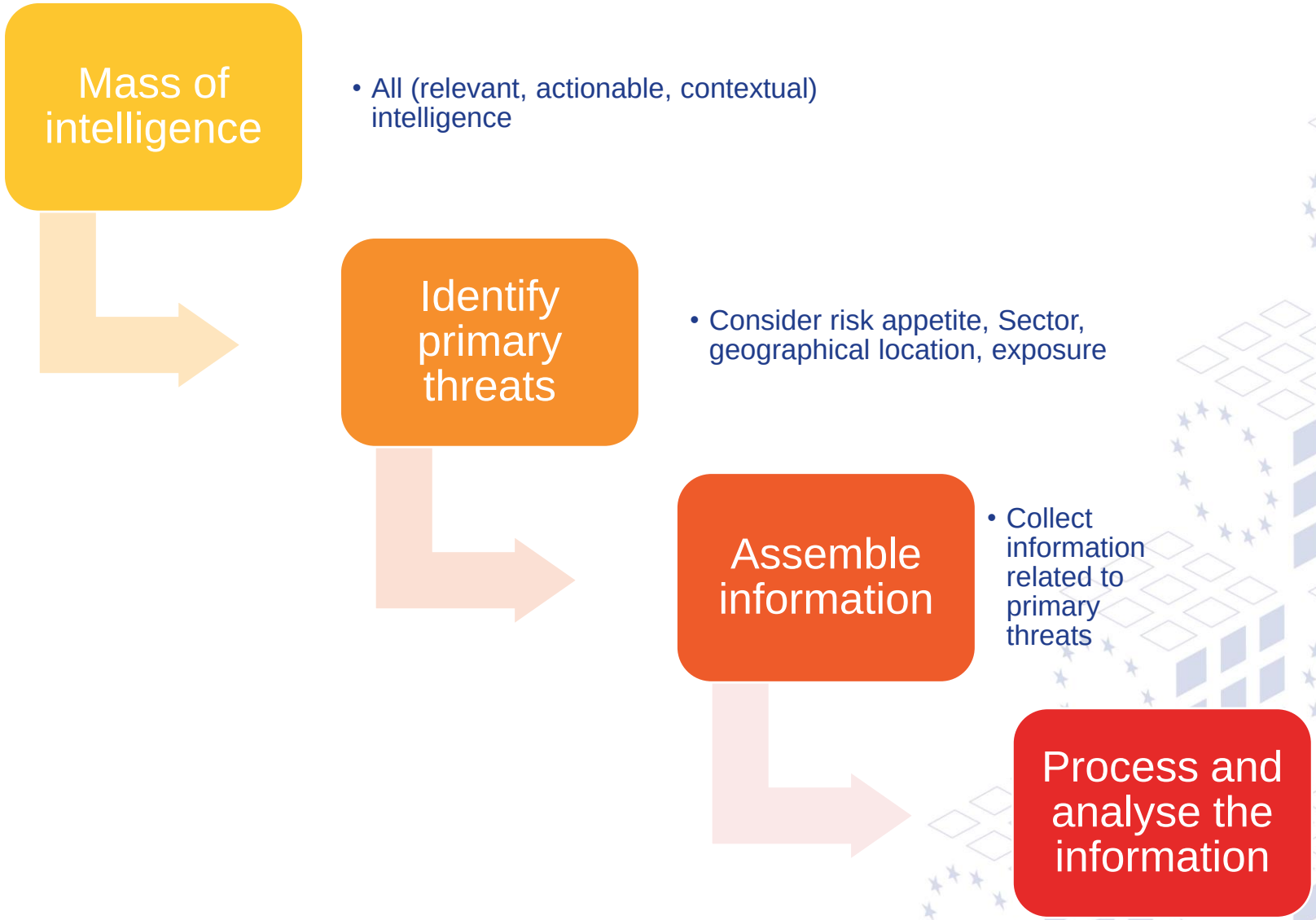
server logs, network device logs, past incident reports, captured network traffic

TI providers, Communities (FIRST, CNW)

GreyNoise, ENISA, CISA, NIST, CVSS

TLP:CLEAR

I HAVE INTELLIGENCE, WHAT'S NEXT?



TLP:CLEAR

TLP:GREEN

THREAT REPORTS

Quick overview:

	Critical	Urgent	Important
Industrial Sector	0	1	2
Vulnerabilities	0	2	1
Malware	0	0	6
Breaches/Hacks/Leaks	0	0	1
General News	0	0	8

Industrial Sector

Optigo Networks ONS-S8 Spectra Aggregation Switch

"Successful exploitation of these vulnerabilities could allow an attacker to achieve remote code e
Priority: 2 - Urgent
Relevance: General

<https://www.cisa.gov/news-events/ics-advisories/icsa-24-275-01>

Mitsubishi Electric MELSEC iQ-F FX5-OPC

"Successful exploitation of this vulnerability could allow a remote attacker to cause a Denial-of-
crafted PKCS#12 format certificate."
Priority: 3 - Important
Relevance: General

<https://www.cisa.gov/news-events/ics-advisories/icsa-24-275-02>

OSINT Report

EOR-24-38 Week 39
[24 - 30 September 2024]

This week's stories

[BE] - KillSec lists Belgian MediCheck, a provider of medical control management solutions
[BE] - BlackSuit lists Belgian retail chain LolaLiza [Update: Week 37-24]
[FI] - The website of Finland's cyber minister hijacked
[FR] - French grocery producer Albert Ménès allegedly breac
[DE] - German manufacturer Schumag hit by cyber-attack
[HU], [IT], [MD], [PL] - Novel "Octo2" mobile banking malware
European banking app users
[LV] - Latvian TV Balticom hit by cyber-attack to spread Russ
[PT] - Qilin lists Luso Cuanza, a Portugal based provider of I
businesses
[ES] - Abyss lists Spanish mining company Tolsa
[GLOBAL] - MoneyGram indicates cyber incident is causing
[GLOBAL] - Israel-Hamas conflict related hacktivist activity [
[GLOBAL] - Website defacement incident impacted UK railwa
network
[GLOBAL] - Russia-Ukraine related hacktivist activity [Week
[GLOBAL] - Swiss canton hit by cyber-attack
[US] - China-nexus Salt Typhoon group breach US internet s

TLP: CLEAR

[IT-ISAC] Open Source News October 1, 2024

Title: Microsoft Defender Adds Detection of Unsecure Wi-Fi Networks

Date Published: September 30, 2024

https://www.bleepingcomputer.com/news/security/microsoft-defender-now-automatically-detects-unsecure-wi-fi-networks/

Excerpt: "Microsoft Defender now automatically detects and notifies users with a Microsoft 365 Personal or Family subscription w
unsecured Wi-Fi networks. The Defender privacy protection feature (also known as Defender VPN) protects your privacy and secu
Wi-Fi or an untrusted network, where your data and identity could be exposed or stolen. To do that, it encrypts and routes your in
Microsoft's servers and hides your internet address (IP address) using a VPN (Virtual Private Network). Microsoft announced today
upgraded to automatically alert users they're exposed to attacks and can now be configured to enable automatically for better saf
un-safe Wi-Fi (suspicious Wi-Fi). These detections are possible using Defender heuristics that examine multiple characteristics of a
is suspicious," Microsoft said. "As with unsecure Wi-Fi, you get a notification for un-safe Wi- Fi as well and can turn on Defender VI
help defend you against attackers setting up a rogue wireless access point to trick users into connecting to it in Evil Twin attacks. A
can steal sensitive information in Man-in-the-Middle (MiTM) attacks or use phishing techniques to get more information."

Title: JPCERT Shares Windows Event Log Tips to Detect Ransomware Attacks

TLP:GREEN

ENISA THREAT LANDSCAPE

7 prime cybersecurity threats were identified, with threats against availability topping the chart and followed by ransomware and threats against data, and the report provides a relevant deepdive on each one of them by analysing several thousand publicly reported cybersecurity incidents and events:

Ransomware
Malware
Social Engineering
Threats against data
Threats against availability: Denial of Service
Information manipulation and interference
Supply chain attacks

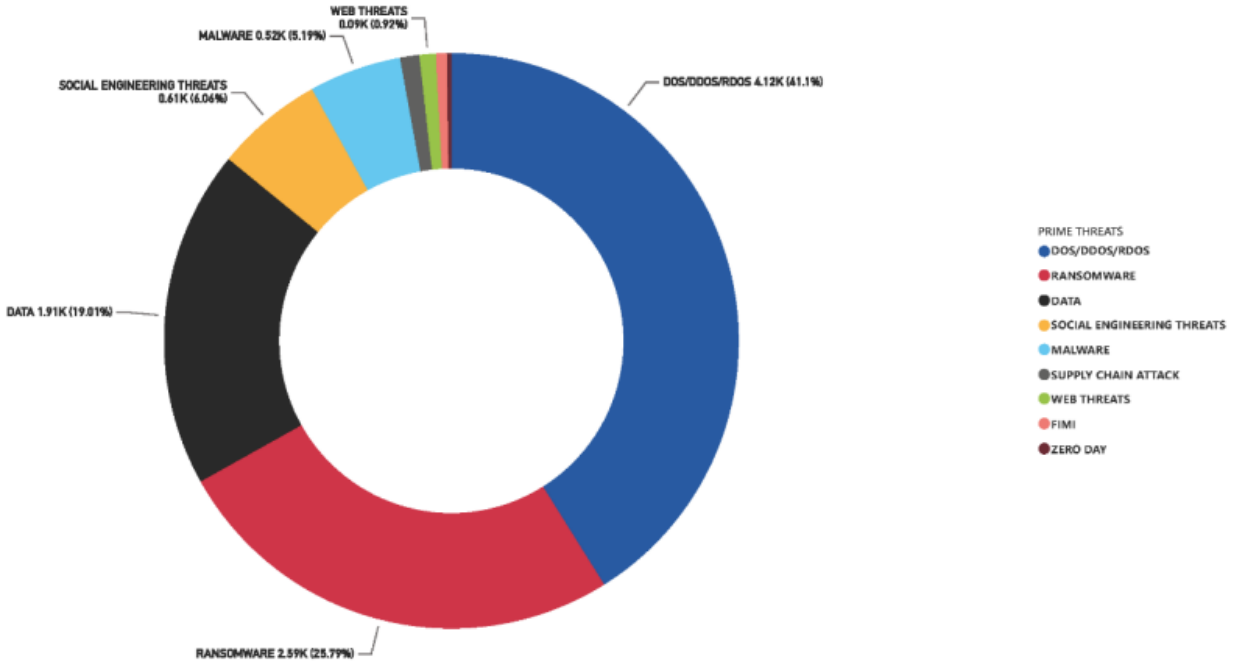
TLP:CLEAR

ETL 2024

„The ongoing regional conflicts still remain a significant factor shaping the cybersecurity landscape. The phenomenon of hacktivism has seen steady expansion, with major events taking place (e.g. European Elections) providing the motivation for increased hacktivist activity”

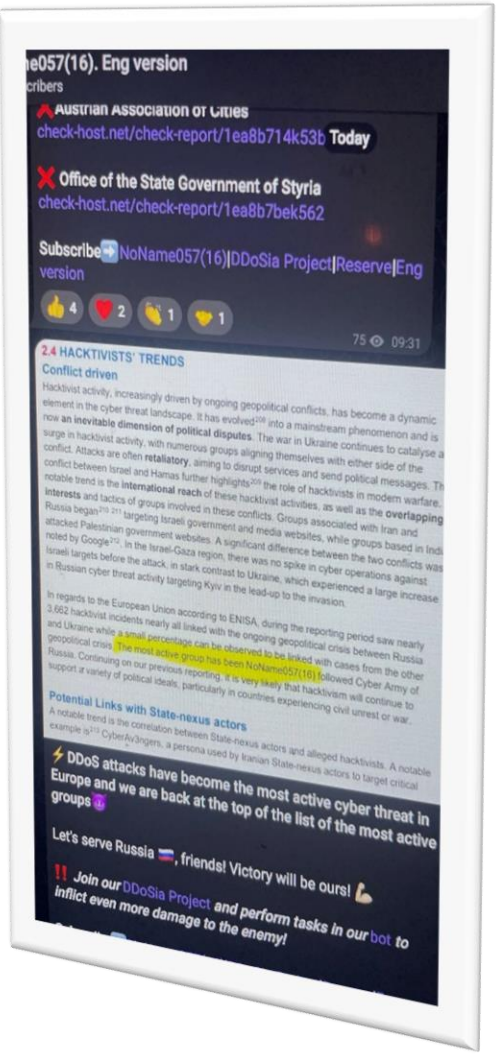
„The threat of AI-enabled information manipulation has been observed…”

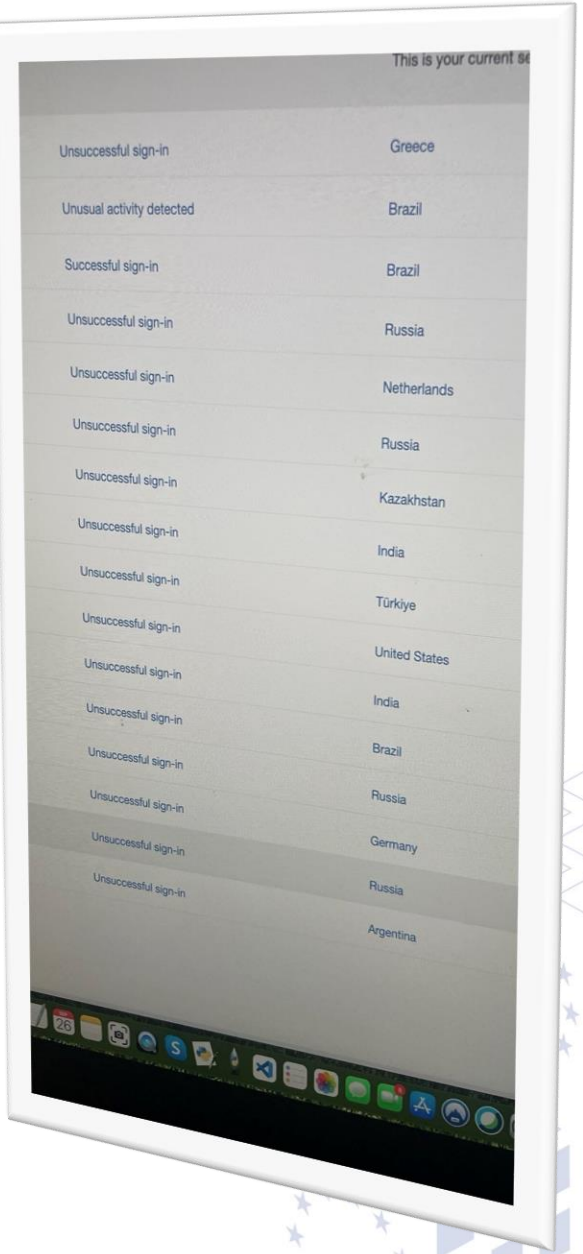
Figure 2: Breakdown of analysed incidents by threat type (July 2023 till June 2024)

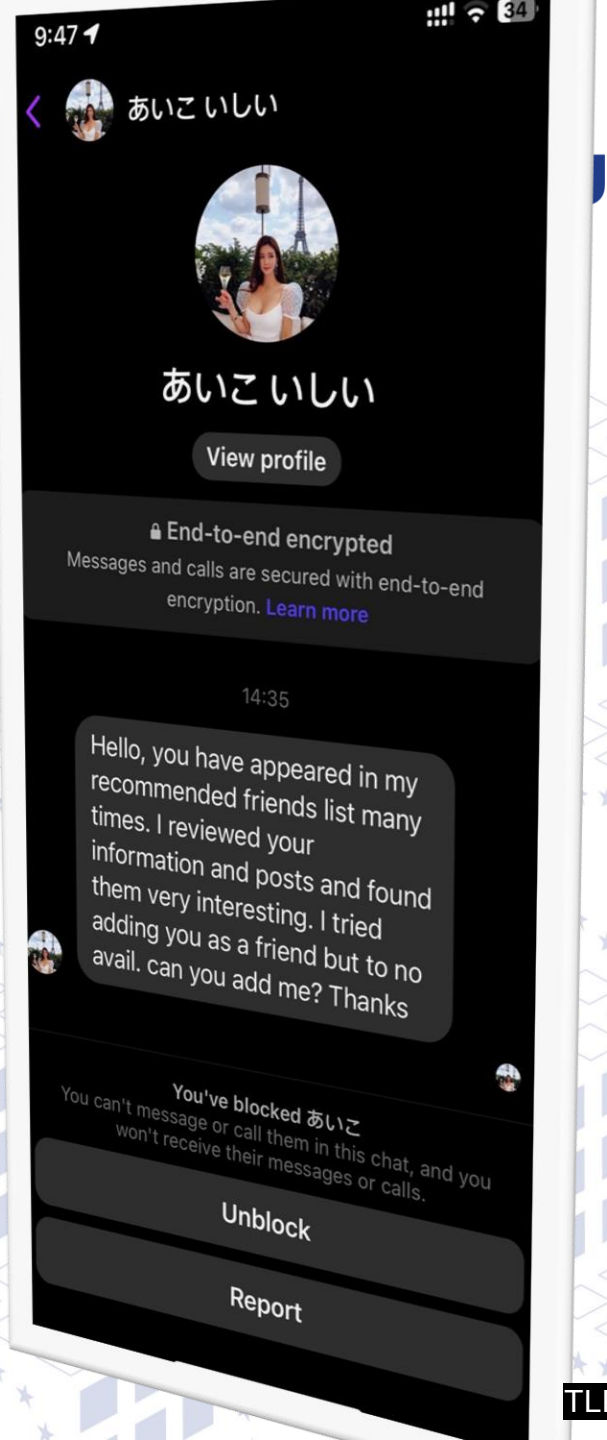


„AI tools for cyber criminals: Threat actors used tools such as FraudGPT and large language models to co-author scam emails and generate malicious PowerShell scripts.„

IS IT REAL?







TLP:CLEAR

HU24EU

Thank you for your time!