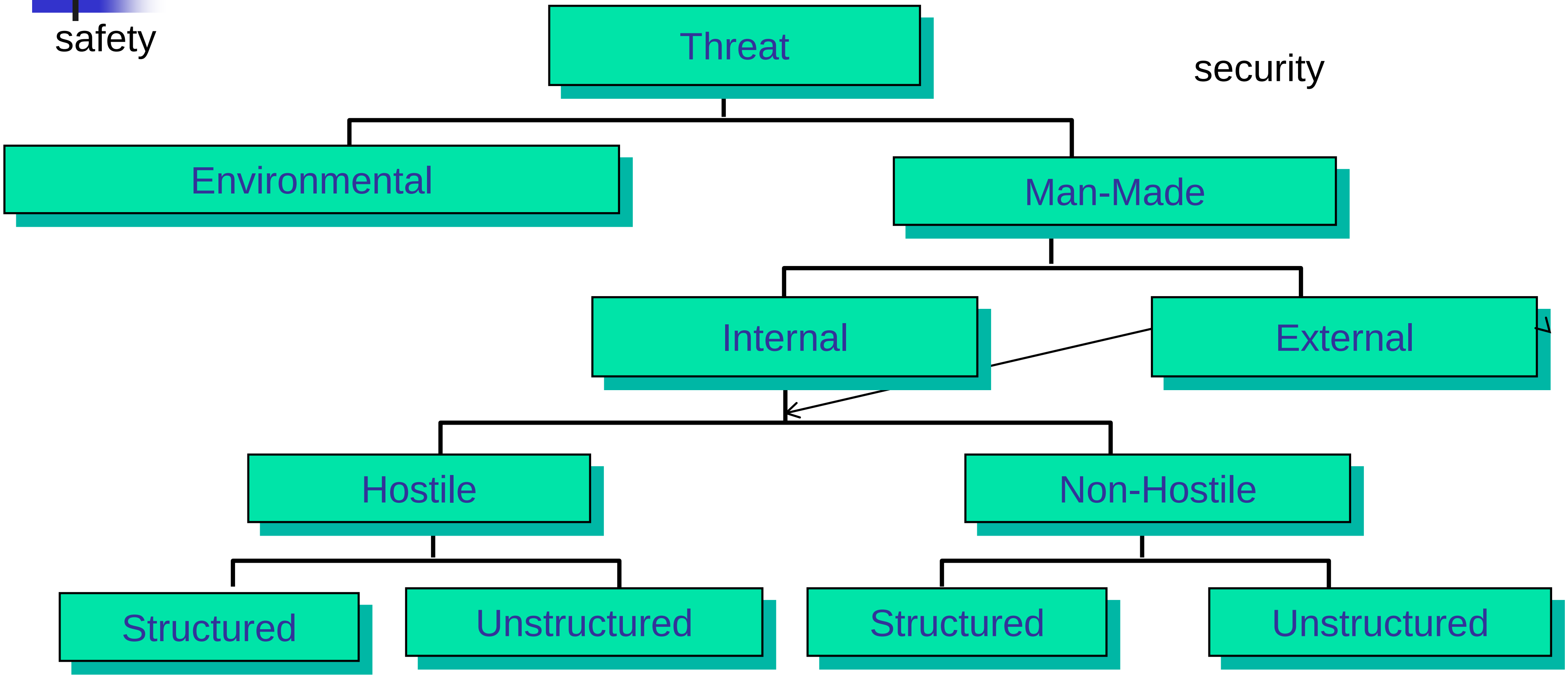
Threat Analysis

Threat analysis

- It has to determines the enemies of a system
  - Who is interested in attacking the system
  - Who can access the resources to attack a system
  - What are the events that may involve the system
- It determines the threats (classes) and the agents in each class
- If there is not a threat that can exploit a given vulnerability, then the assessment may neglect such a vulnerability
- It is strongly related (it may be interleaved with) the attack analysis (is there anyone that can implement this attack?)

A threat taxonomy



safety

security

Threat catalogue

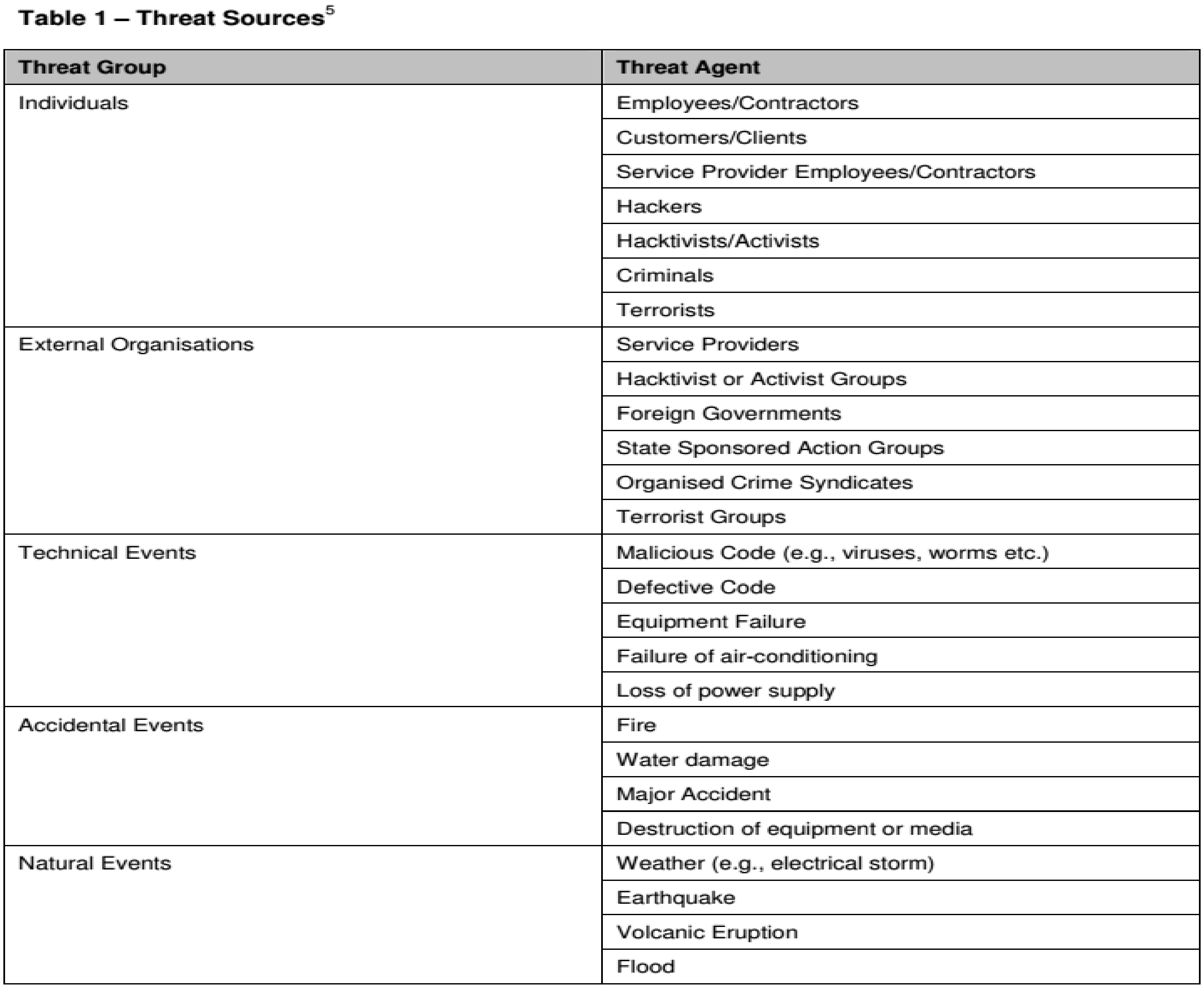


Table 1 – Threat Sources[5]

Threat Group	Threat Agent
Individuals	Employees/Contractors
	Customers/Clients
	Service Provider Employees/Contractors
	Hackers
	Hacktivists/Activists
	Criminals
	Terrorists
External Organisations	Service Providers
	Hacktivist or Activist Groups
	Foreign Governments
	State Sponsored Action Groups
	Organised Crime Syndicates
	Terrorist Groups
Technical Events	Malicious Code (e.g., viruses, worms etc.)
	Defective Code
	Equipment Failure
	Failure of air-conditioning
	Loss of power supply
Accidental Events	Fire
	Water damage
	Major Accident
	Destruction of equipment or media
Natural Events	Weather (e.g., electrical storm)
	Earthquake
	Volcanic Eruption
	Flood

Threat catalogue - Motivation

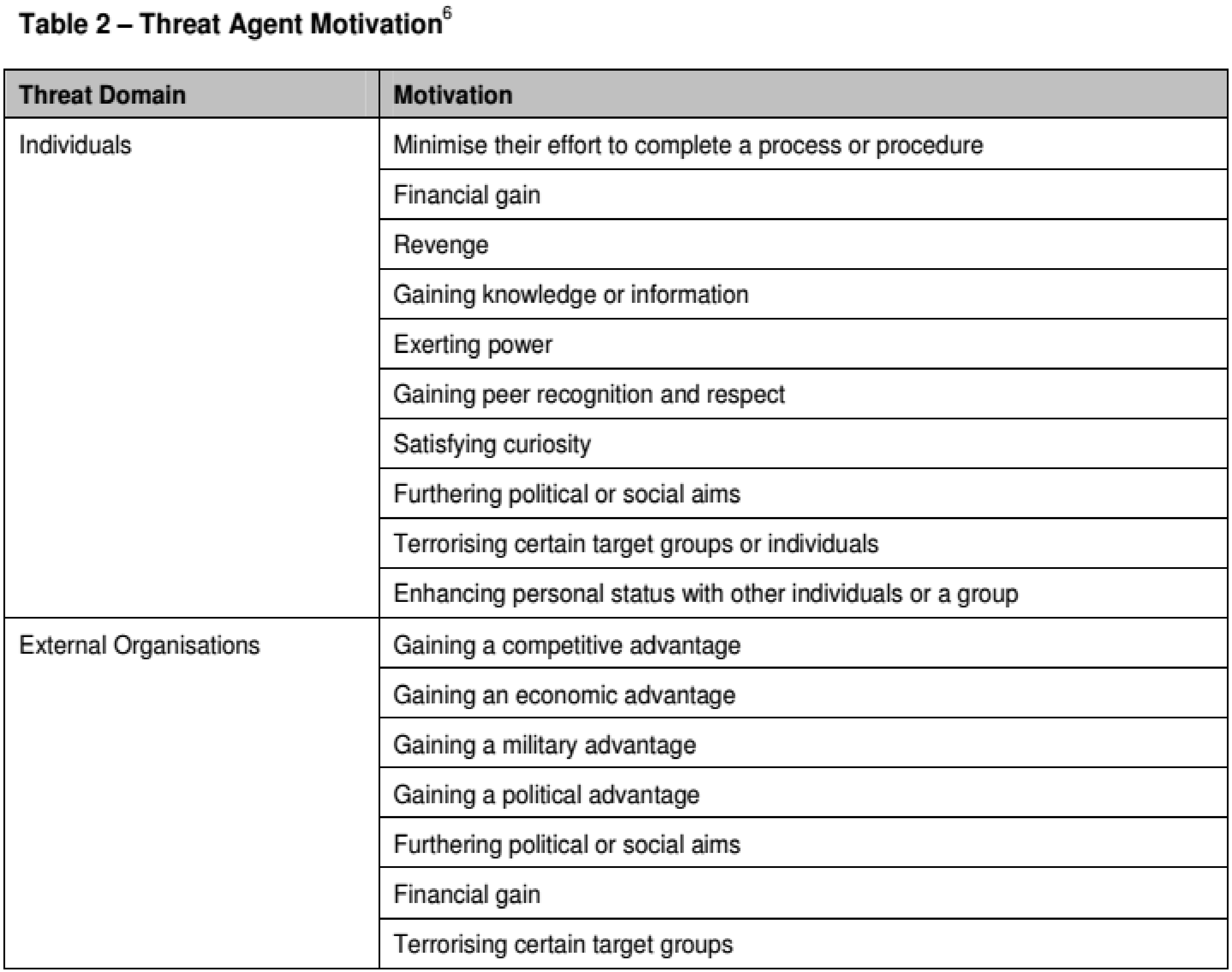


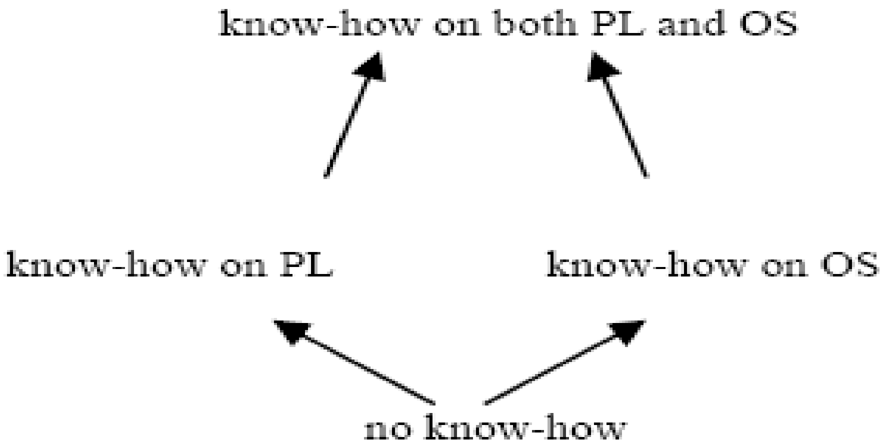
Table 2 – Threat Agent Motivation[6]

Threat Domain	Motivation
Individuals	Minimise their effort to complete a process or procedure
	Financial gain
	Revenge
	Gaining knowledge or information
	Exerting power
	Gaining peer recognition and respect
	Satisfying curiosity
	Furthering political or social aims
	Terrorising certain target groups or individuals
	Enhancing personal status with other individuals or a group
External Organisations	Gaining a competitive advantage
	Gaining an economic advantage
	Gaining a military advantage
	Gaining a political advantage
	Furthering political or social aims
	Financial gain
	Terrorising certain target groups

Threat analysis

- For each agent, the analysis determines
  - The goals= rights on components
  - The resources it has available
    - Tecnological
    - Information (security through obscurity)
    - Know how and abilities
  - The risk attitude
  - The legal access rights
- Agents can be partially ordered according to
  - the resources they can access
  - the risk they are willing to take
- The higher the position, the larger the potential impact
- Attacks can be ordered in the same way

A lattice based description of agents



know-how on both PL and OS

know-how on PL

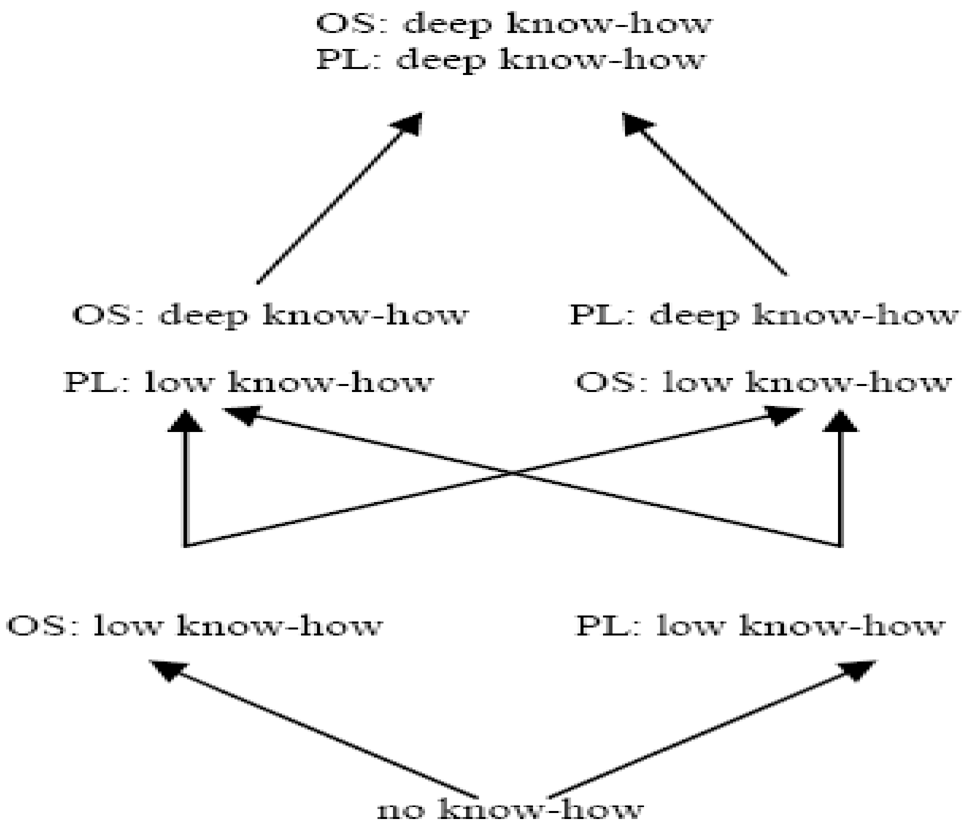
know-how on OS

no know-how

a) A poset modelling the know-how of a threat

A finite model to describe threat agents

A lattice based description of agents



OS: deep know-how
PL: deep know-how

OS: deep know-how
PL: low know-how

PL: deep know-how
OS: low know-how

OS: low know-how

PL: low know-how

no know-how

A more refined model to describe threat agents

Describing agents and attacks

- Each attack is described by a tuple of attributes and a noise
- Each agent is described by a tuple of attributes (same for attack) and an accepted noise
- We have one distinct partial order for each attribute
- This define a partial order for both agents and attacks

Feasible attacks

Given

- a tuple T_A that describes the attack A and where each element evaluates an attribute of A
- a tuple T_M that describes a threat agent M and where each element evaluates the resources that M can access

M can execute A provided that

- Each element of tuple T_M is larger than or equal to the corresponding elemen of T_A
- The noise paired with A is smaller than or equal to the one that is accepted by M

Threat model

- Anytime a security problem is analysed there is the problem of formally determining the actions that any threat agent
  - can execute (owns the resources to execute)
  - cannot execute (lack of resources)
  - is not willing to execute
- should be considered
- It this problem is not solved, the analysis is partial
- Not important when national security is involved

Threat model and partial orders

- The partial orders among threats and attacks are an important way to preserve the coherence of the analysis
- Implement a basic checks because a more powerful threat cannot implement a smaller set of attacks
- But do not support the discovery of threat, of attacks, or if a threat will attack us

What is new for ICT?

- Automated attacks
- Mass attack = automated + autonomous = untargeted attacks
- A threat agent does not attack a system but it programs an agent that can reproduce itself and propagate from one system to another one

Threat Intelligence

- An extension of threat analysis that considers not only who is interested in attacking a system but also how the attack occurs
- A service that several companies offer
- Which vulnerabilities will be exploited and the exploits that will be used
- DoD uses the term of predictive security = understanding how a system will be attacked before the attack occurs

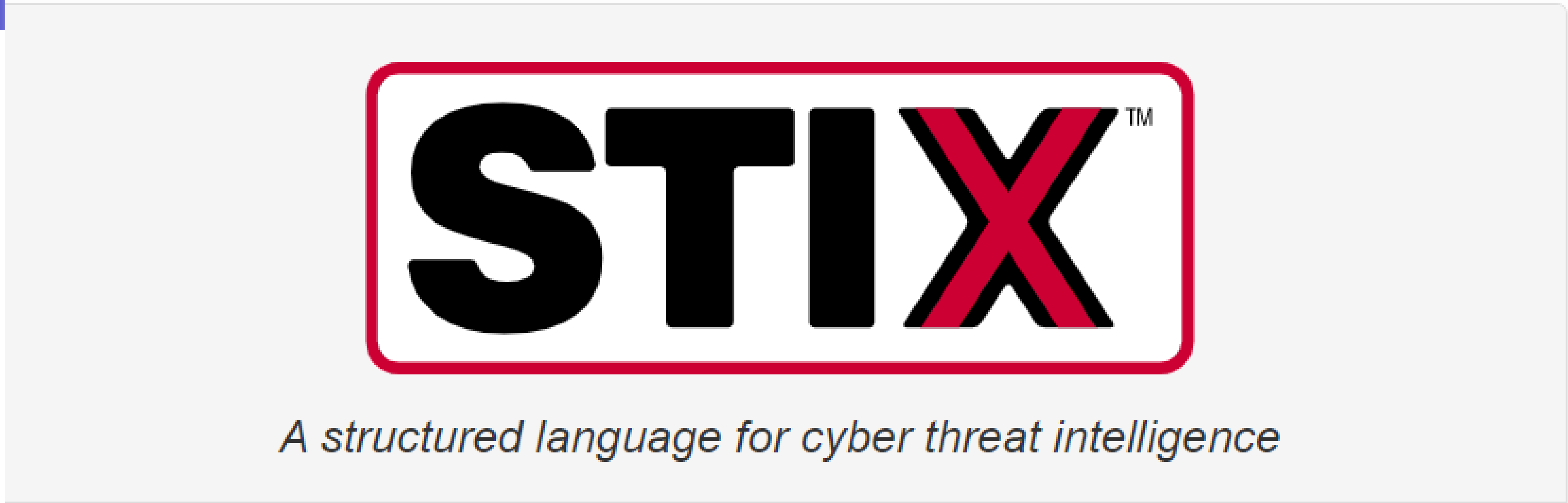
Threat Intelligence Platforms

- Use global security data to help proactively identify, mitigate and remediate security threats.
- New and continually evolving threats are surfacing every day.
- The problem that arises is how to efficiently collect high volumes of data and consequently derive actionable insights to proactively thwart future attacks.

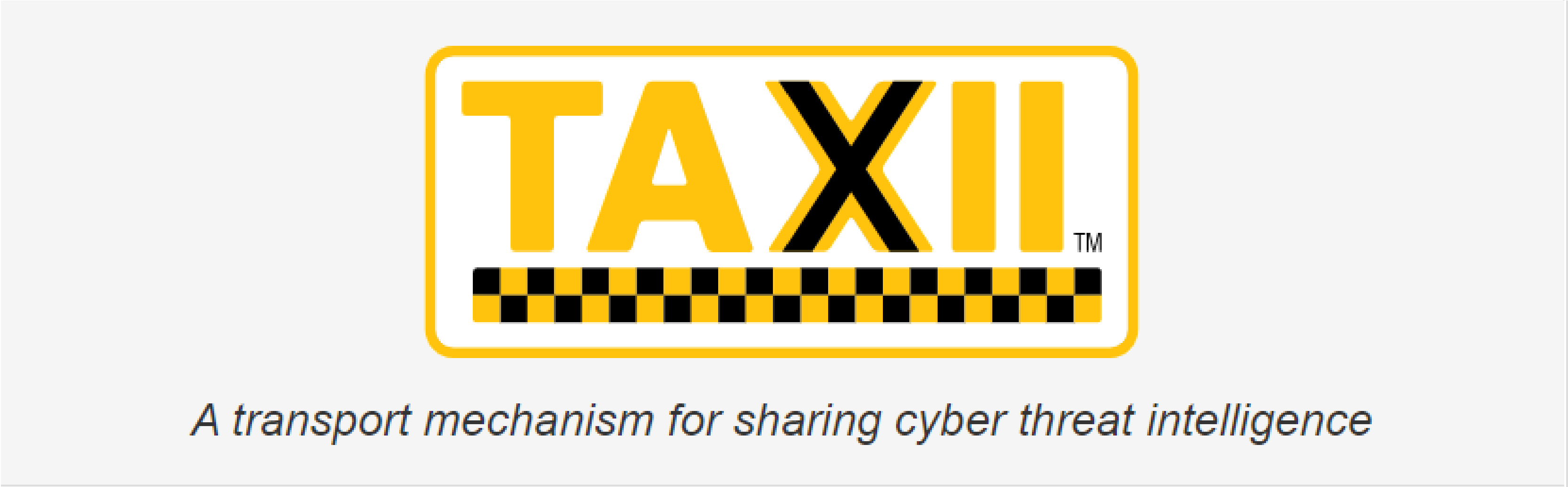
Threat Intelligence Platforms

- TIPs aggregate security intelligence from vendors, analysts and other reputable sources about threats and suspicious activity detected all around the world through threat intelligence feeds.
- This data can come in the form of malicious IP addresses, domains, file hashes and more.
- TIPs then convert these advanced analytics into information for preventing the success of attacks an detecting malicious activity inside a network.

STIX and TAXII



A structured language for cyber threat intelligence

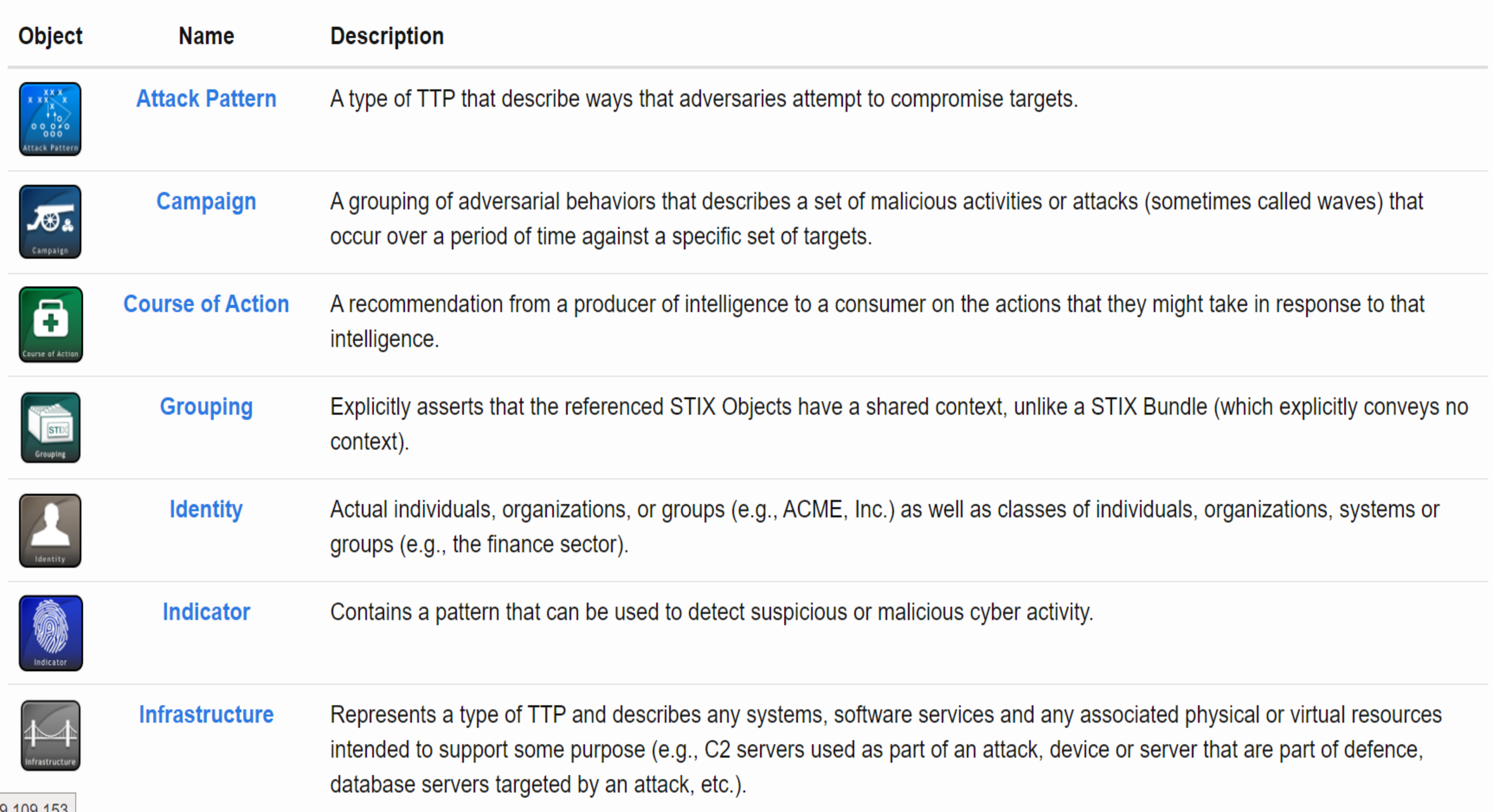


A transport mechanism for sharing cyber threat intelligence

STIX

- Structured Threat Information Expression is a language and serialization format used to exchange cyber threat intelligence (CTI).
- It enables organizations to share CTI with one another in a consistent and machine readable manner, allowing communities to better understand what computer-based attacks they are most likely to see
- It is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

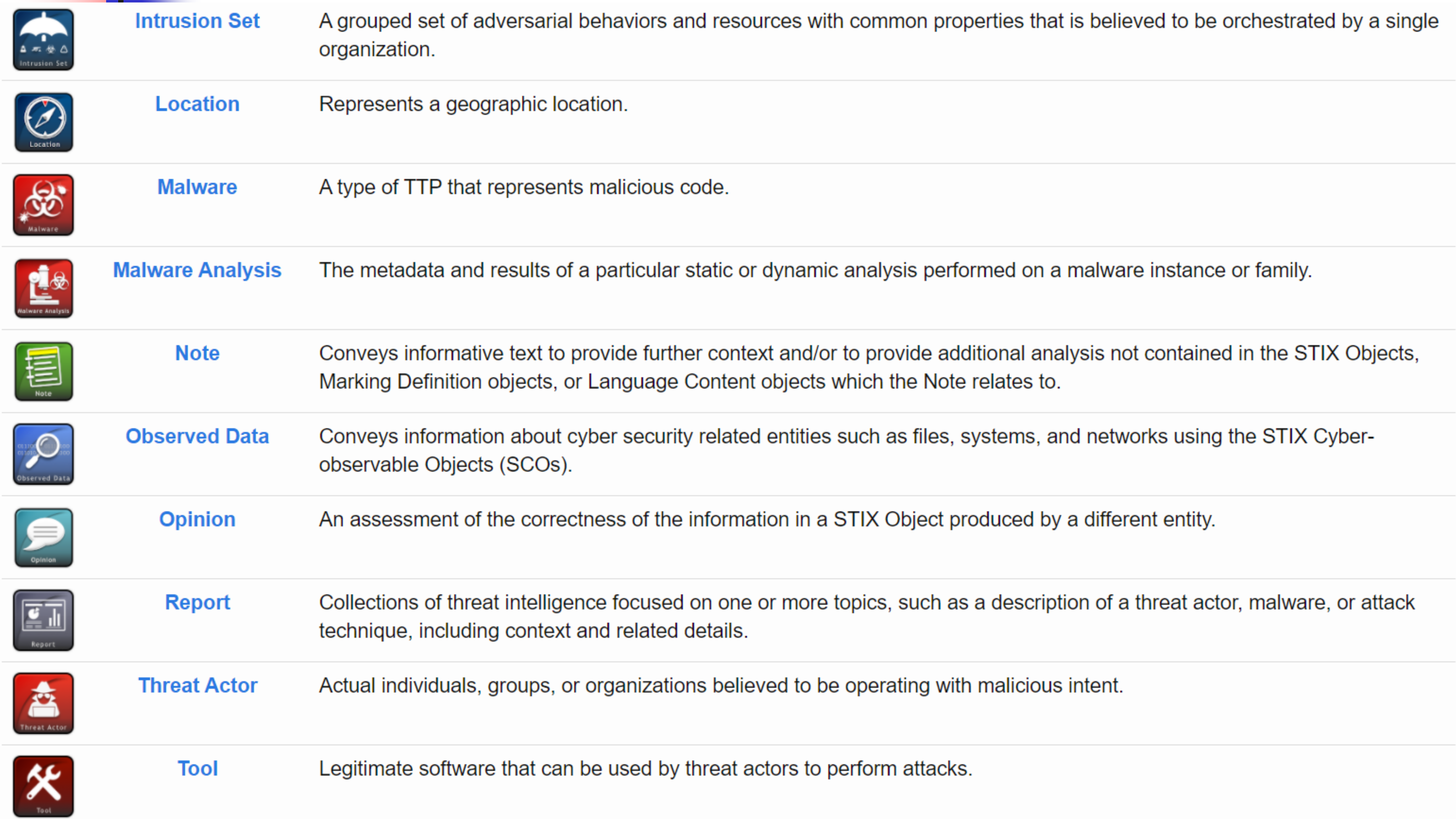
STIX Domain Objects



Object	Name	Description
Attack Pattern	Attack Pattern	A type of TTP that describe ways that adversaries attempt to compromise targets.
Campaign	Campaign	A grouping of adversarial behaviors that describes a set of malicious activities or attacks (sometimes called waves) that occur over a period of time against a specific set of targets.
Course of Action	Course of Action	A recommendation from a producer of intelligence to a consumer on the actions that they might take in response to that intelligence.
Grouping	Grouping	Explicitly asserts that the referenced STIX Objects have a shared context, unlike a STIX Bundle (which explicitly conveys no context).
Identity	Identity	Actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector).
Indicator	Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
Infrastructure	Infrastructure	Represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defence, database servers targeted by an attack, etc.).

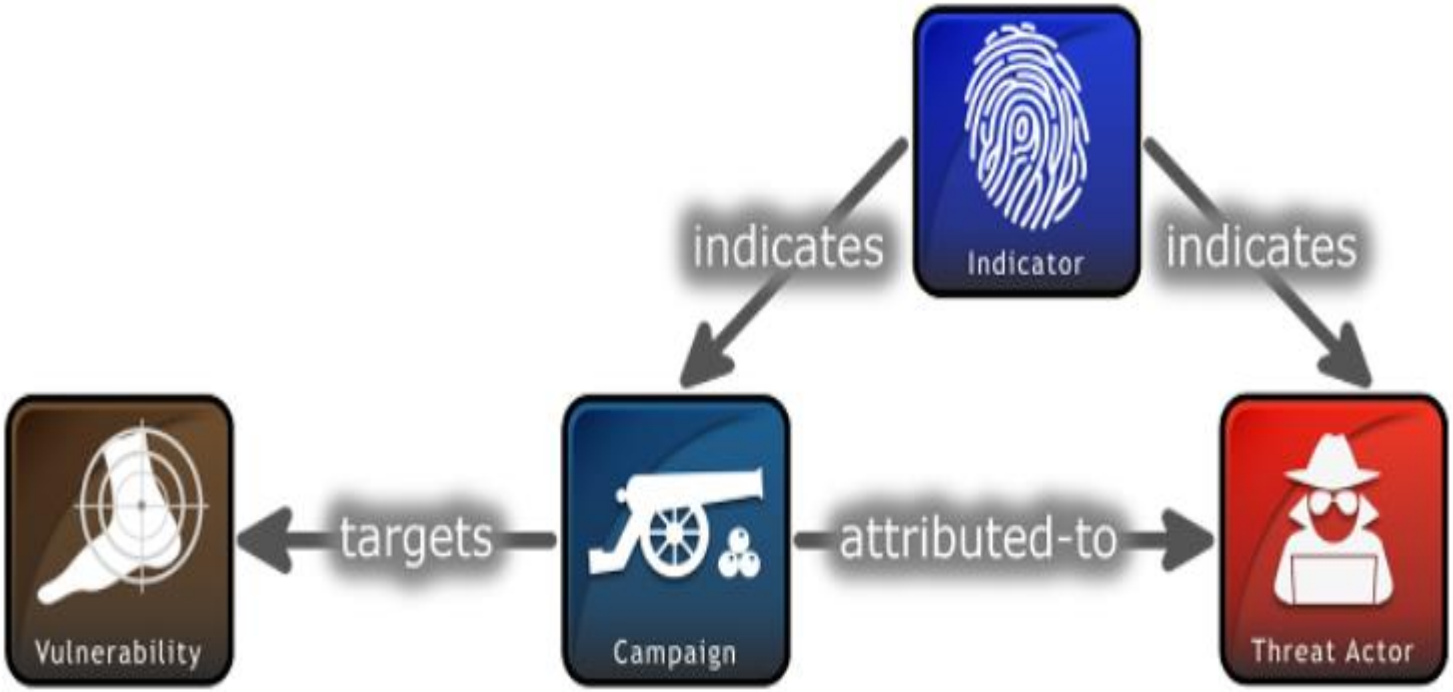
9.109.153

STIX Domain Objects



Intrusion Set	**Intrusion Set**	A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.
Location	**Location**	Represents a geographic location.
Malware	**Malware**	A type of TTP that represents malicious code.
Malware Analysis	**Malware Analysis**	The metadata and results of a particular static or dynamic analysis performed on a malware instance or family.
Note	**Note**	Conveys informative text to provide further context and/or to provide additional analysis not contained in the STIX Objects, Marking Definition objects, or Language Content objects which the Note relates to.
Observed Data	**Observed Data**	Conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).
Opinion	**Opinion**	An assessment of the correctness of the information in a STIX Object produced by a different entity.
Report	**Report**	Collections of threat intelligence focused on one or more topics, such as a description of a threat actor, malware, or attack technique, including context and related details.
Threat Actor	**Threat Actor**	Actual individuals, groups, or organizations believed to be operating with malicious intent.
Tool	**Tool**	Legitimate software that can be used by threat actors to perform attacks.

STIX Relationship



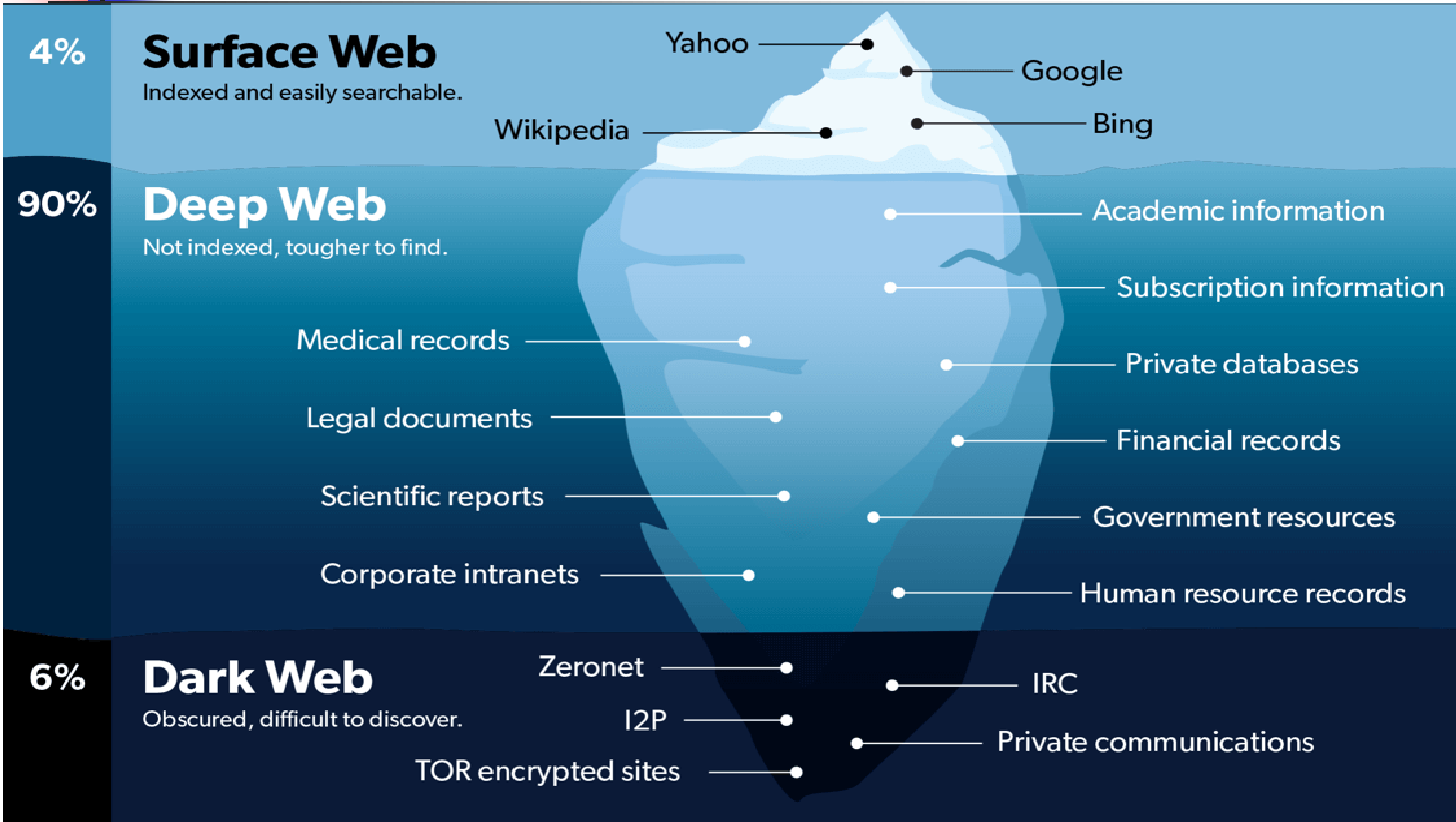
Trusted Automated Exchange of Intelligence Information (TAXII™)

- An application protocol for exchanging CTI over HTTPS.
- TAXII defines a RESTful API (a set of services and message exchanges) and a set of requirements for TAXII Clients and Servers. TAXII defines two primary services to support a variety of common sharing models:
  - Collection
  - Channel

Trusted Automated Exchange of Intelligence Information (TAXII™)

- **Collection** - An interface to a logical repository of CTI objects provided by a TAXII Server that allows a producer to host a set of CTI data that can be requested by consumers: TAXII Clients and Servers exchange information in a request-response model.
- **Channel** - Maintained by a TAXII Server, it allows producers to push data to many consumers and consumers to receive data from many producers: TAXII Clients exchange information with other TAXII Clients in a publish-subscribe model.

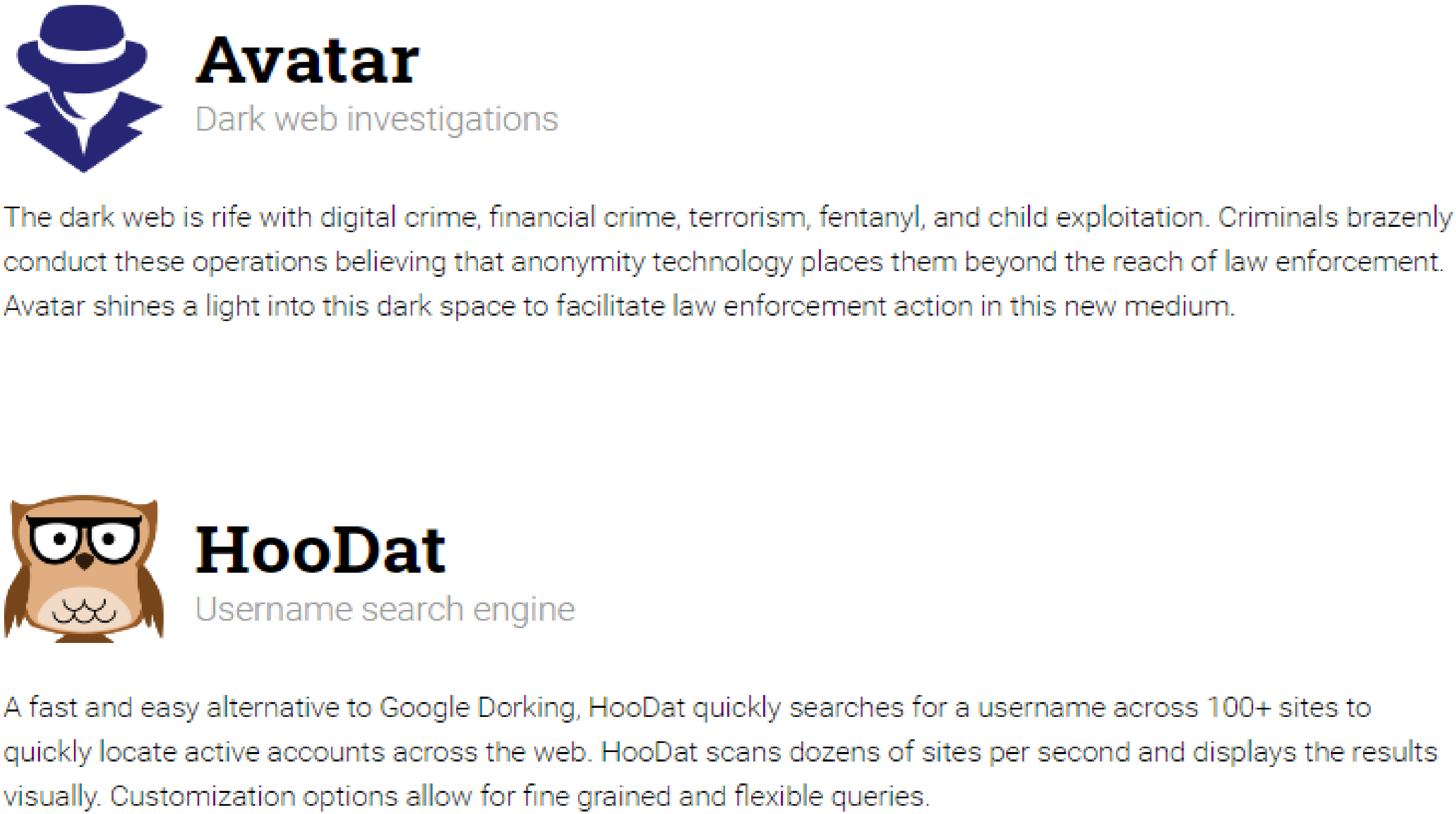
Surface, deep and dark web



Threat intelligence - dark web

- Search engines can easily access the surface content
- The other content is the *Deep Web*, content that has not been indexed by traditional search engines
- The furthest corners of the Deep Web is the *Dark Web*, contain content that has been *intentionally* concealed
- The Dark Web may be used for legitimate purposes as well as to conceal criminal or malicious activities. The exploitation of the Dark Web for illegal practices has garnered the interest of officials and policymakers
- Individuals can access the Dark Web by using special software such as Tor (short for The Onion Router)

Threat intelligence + dark web: some examples of services



Avatar

Dark web investigations

The dark web is rife with digital crime, financial crime, terrorism, fentanyl, and child exploitation. Criminals brazenly conduct these operations believing that anonymity technology places them beyond the reach of law enforcement. Avatar shines a light into this dark space to facilitate law enforcement action in this new medium.

HooDat

Username search engine

A fast and easy alternative to Google Dorking, HooDat quickly searches for a username across 100+ sites to quickly locate active accounts across the web. HooDat scans dozens of sites per second and displays the results visually. Customization options allow for fine grained and flexible queries.

Google Dorking

- A Google dork query is a search string using advanced search operators to find information that is not readily available on a website.
- Google dorking, or Google hacking, can return information difficult to locate through simple queries, i.e. information not intended for public viewing but not adequately protected.
- A passive attack method, Google dorking can return usernames and passwords, email lists, sensitive documents, personally identifiable information and website vulnerabilities. Information is used in illegal activities i.e.espionage, identity theft and cyberstalking

Basic Formula of Dork

"inurl:."domain"/"dorks" “

Where

“inurl” = *input URL (some use operator)*
“domain” = *your desired domain ex. .gov*
“dorks” = *your dork of your choice*

1. **Explore LOG Files For Login Credentials**

   allintext:password filetype:log after:2019

2. **Explore Live Cameras**

   inurl:top.htm inurl:currenttime

   inurl:”lvappl.htm”

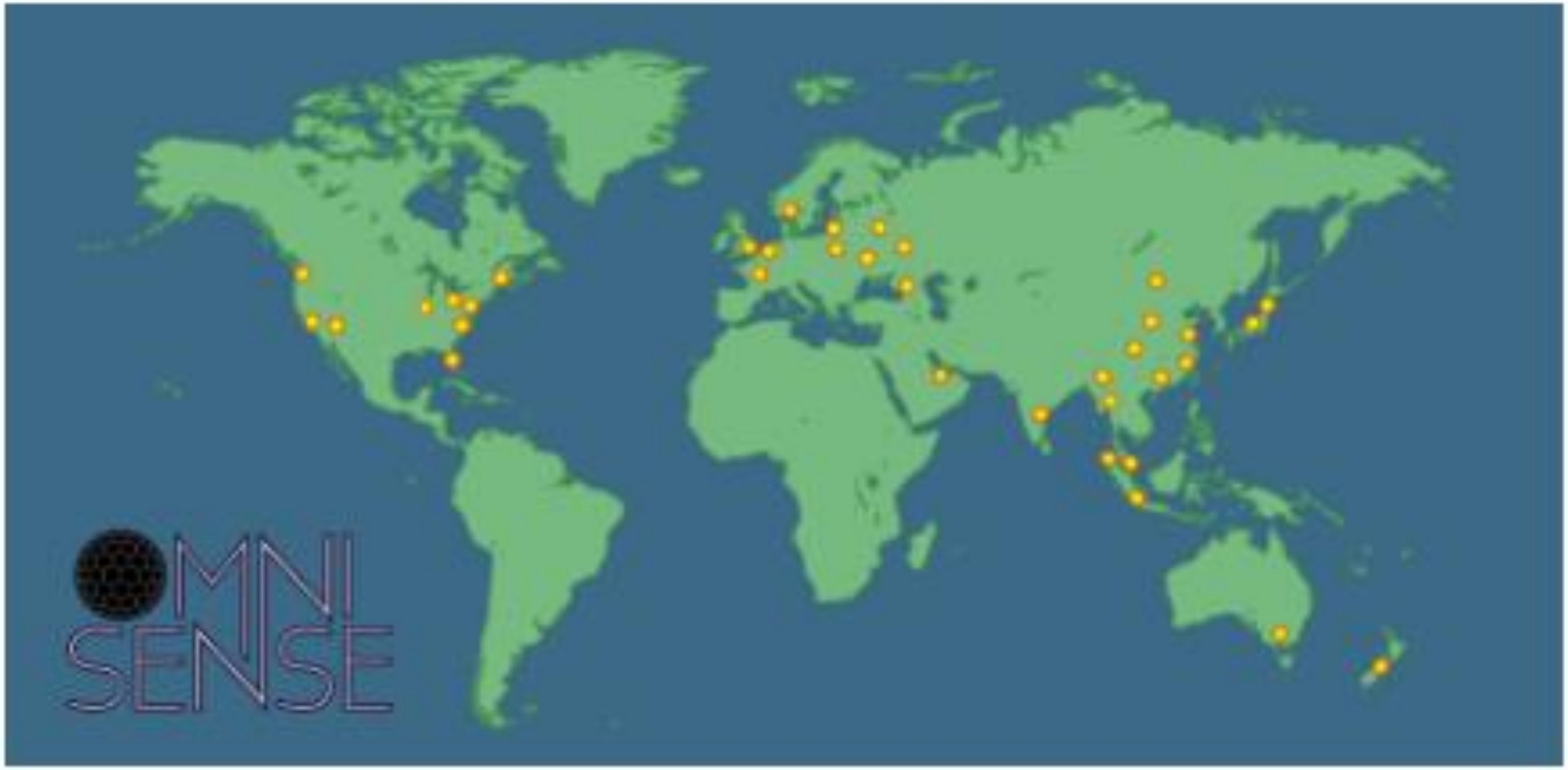
3. **To Explore Open FTP Servers**

   intitle:"index of" inurl:ftp

Omnisense

- Omnisense watches over the internet all the time. Its “listening servers” are dotted across the planet,
- They look at traffic passing around the internet and try to attach IP addresses to each server carrying out certain actions, such as scanning for vulnerabilities or trying to guess passwords on computers en masse
- Once Omnisense has found a server of interest, it carries out a “deep scan” (aka fingerprinting) looking for all the software being run on the host and any domain names associated with the IP address, before giving it a security threat score.
- This information is used to build a black list of dangerous servers

Omnisense



Omnisense listening servers are spread across the globe, permanently monitoring the internet. HYPERION GRAY

Threat Intelligence

- The use of threat intelligence points out som differences between robustness and resilience
- We can evaluate risk with respect to a set of attackers and minimize the overall risk
- Hence, the system is robust with respect to the considered set of attackers
- The robustness may sharply decrease if a distinct attacker appears

Threat Intelligence

- To achieve resilience, we must consider a larger set of attackers than those described by threat intelligence to achieve robustness even with respect to this set
- This results in resilience, the ability of resisting even to unknown attackers
- The larger the set, the more expensive the solution, the lower the return on the investment