

# First Summer School on Security and Privacy in 6G Networks

## TRUST AND CYBER THREAT INTELLIGENCE IN THE PERSPECTIVE OF 6G



Robson de Oliveira Albuquerque  
University of Brasília

Faculty of Computer Science and Engineering, UCM  
Madrid (Spain), June 24 - 28, 2024

**YOU CAN GET A  
COPY OF THIS  
PRESENTATION....**

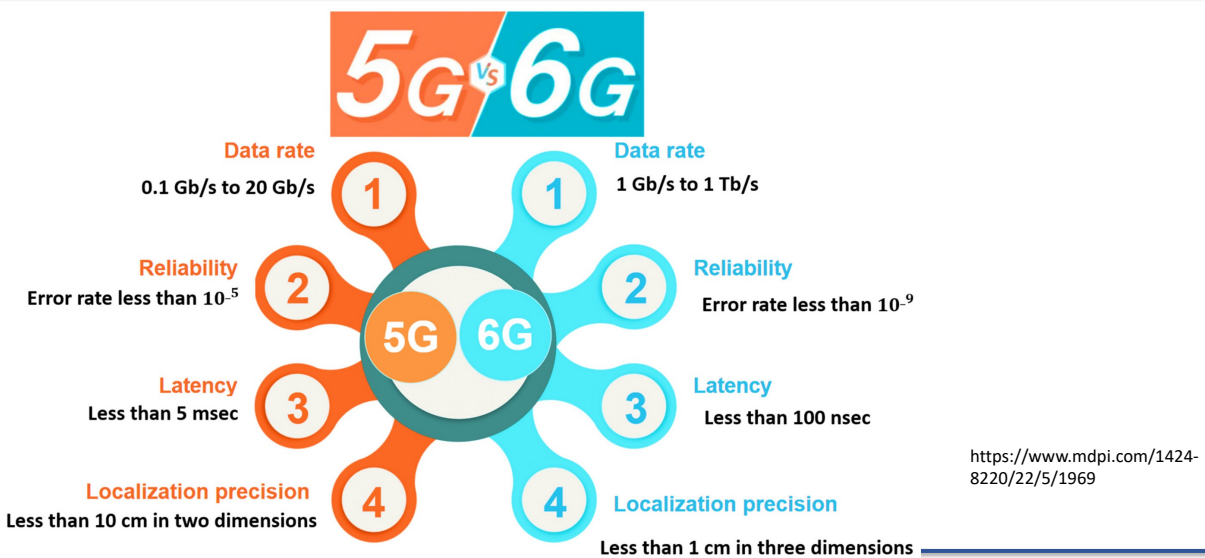
[https://drive.google.com/file/d/1aQq5BpNAGxfcA4e-6P1DtSjR0mNYOYMW/view?usp=drive\\_link](https://drive.google.com/file/d/1aQq5BpNAGxfcA4e-6P1DtSjR0mNYOYMW/view?usp=drive_link)



# AGENDA

- 6G and SECURITY PERSPECTIVES
- TRUST
- CYBER THREAT INTELLIGENCE

# 6G and SECURITY PERSPECTIVES



# 6G and SECURITY PERSPECTIVES

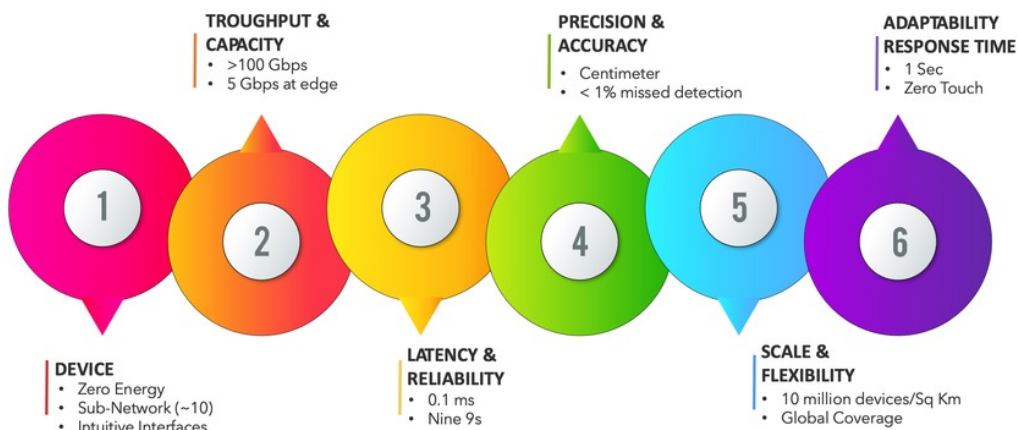


<https://ttconsultants.com/what-is-6g-overview-of-6g-networks-technology/>

5

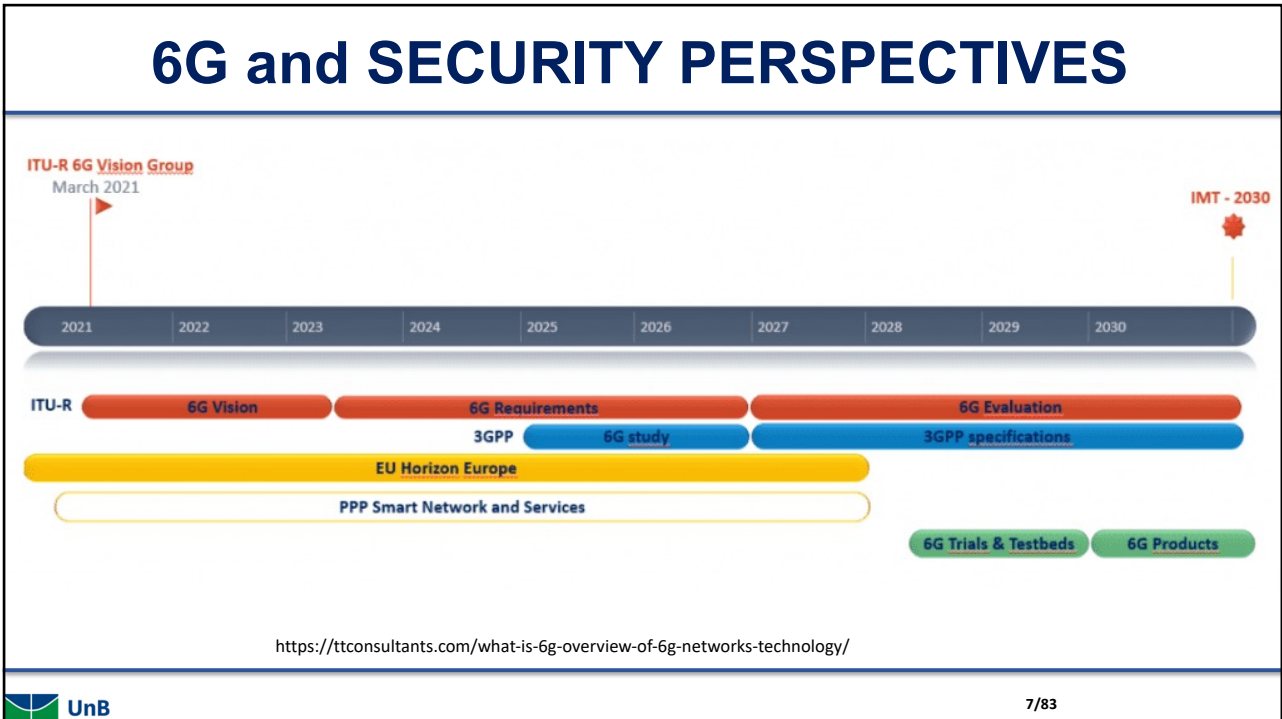
# 6G and SECURITY PERSPECTIVES

## Key requirements and characteristics of 6G

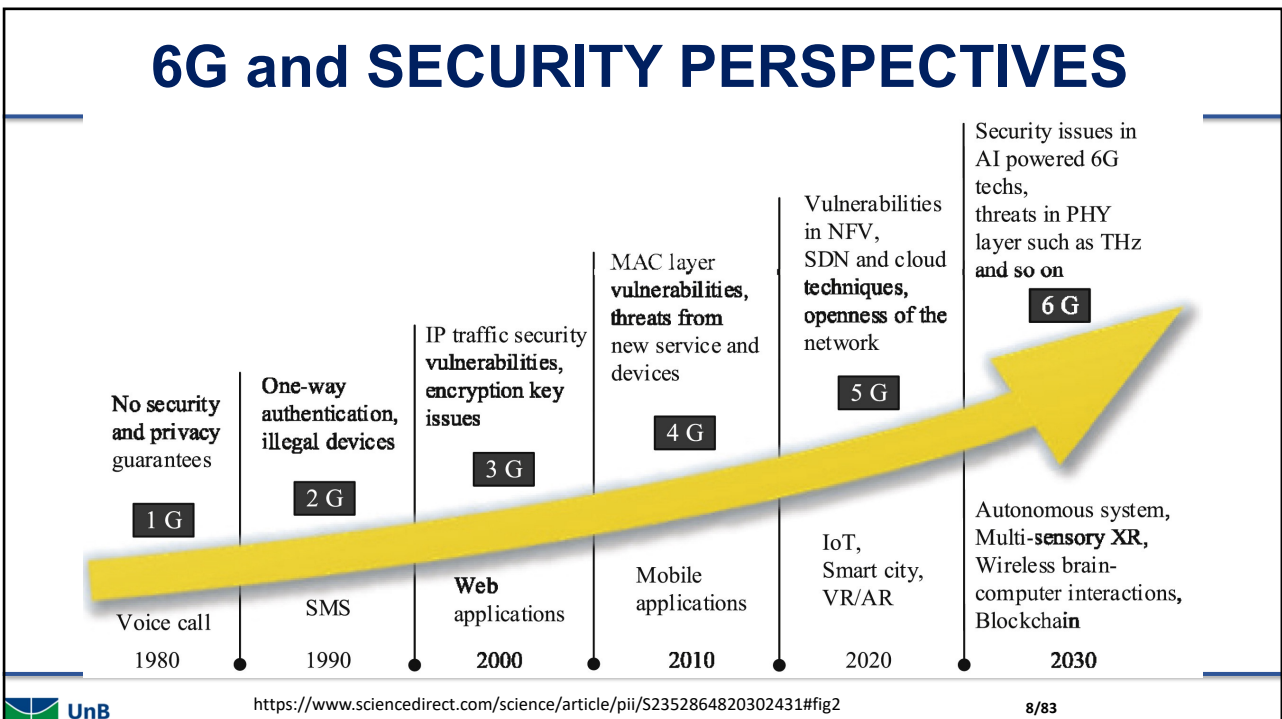


[https://www.researchgate.net/publication/365836709\\_Implementing\\_Intelligence\\_in\\_5G\\_Mobile\\_Networks-A\\_Practical\\_Approach](https://www.researchgate.net/publication/365836709_Implementing_Intelligence_in_5G_Mobile_Networks-A_Practical_Approach)

6

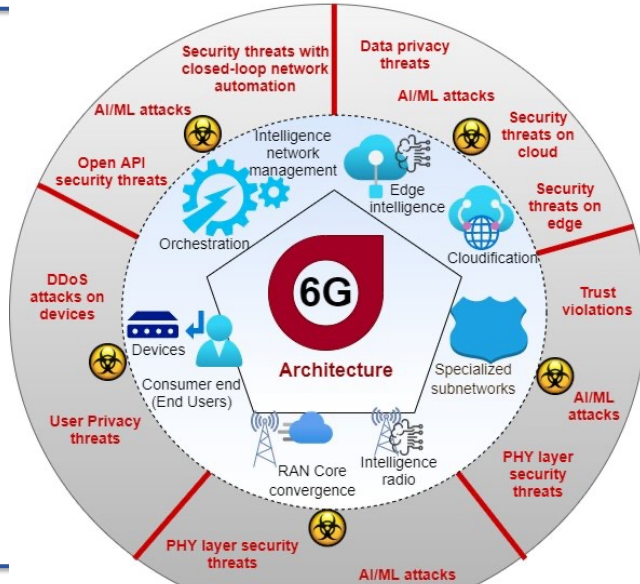


7



8

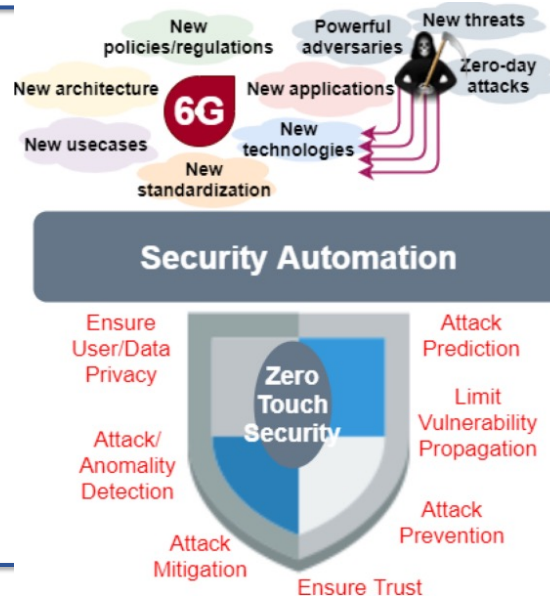
# 6G and SECURITY PERSPECTIVES



## Security and Privacy issues in 6G networks

[https://www.researchgate.net/publication/351275174\\_The\\_Roadmap\\_to\\_6G\\_Security\\_and\\_Privacy/](https://www.researchgate.net/publication/351275174_The_Roadmap_to_6G_Security_and_Privacy/)

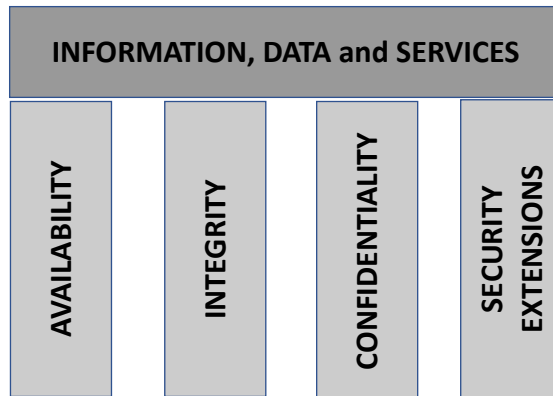
# 6G and SECURITY PERSPECTIVES



<https://www.semanticscholar.org/paper/The-Roadmap-to-6G-Security-and-Privacy-Porombage-G%C3%BCr/f9c6ad24e2a0812dff53902e5941b62e60934345>

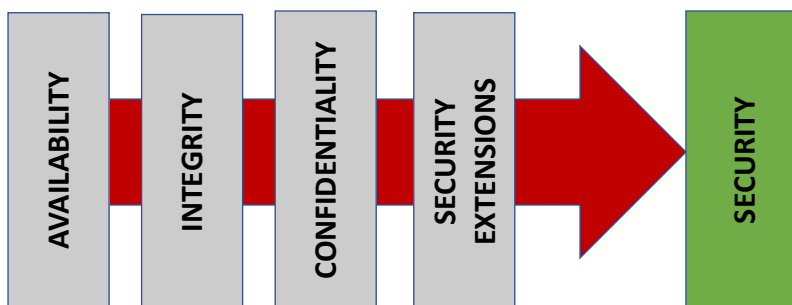
# 6G and SECURITY PERSPECTIVES

## Information security pillars:



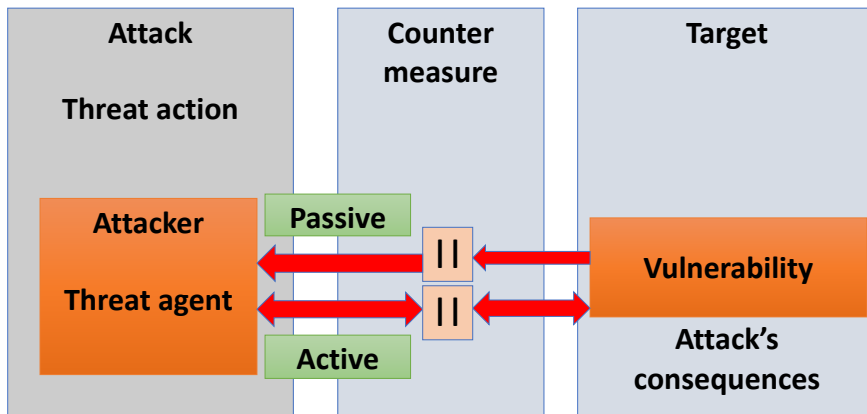
# 6G and SECURITY PERSPECTIVES

## Security objectives:



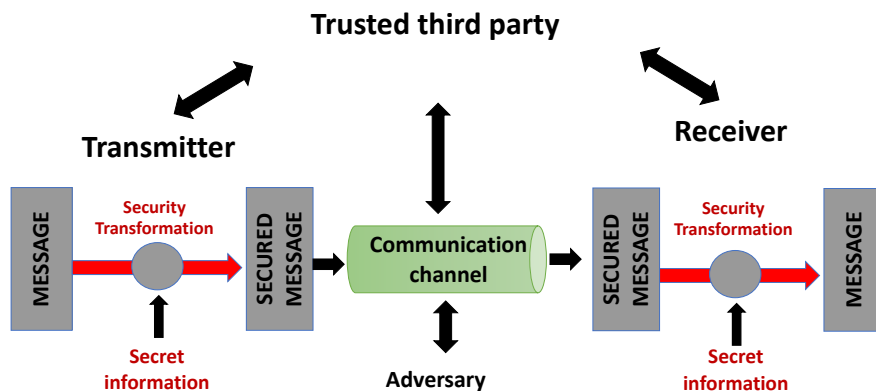
# 6G and SECURITY PERSPECTIVES

## Attacks simplified:



# 6G and SECURITY PERSPECTIVES

## Security model:



# 6G and SECURITY PERSPECTIVES

**What about CyberSecurity?**

Cybok 1.1

UnB

15/83

15

# AGENDA

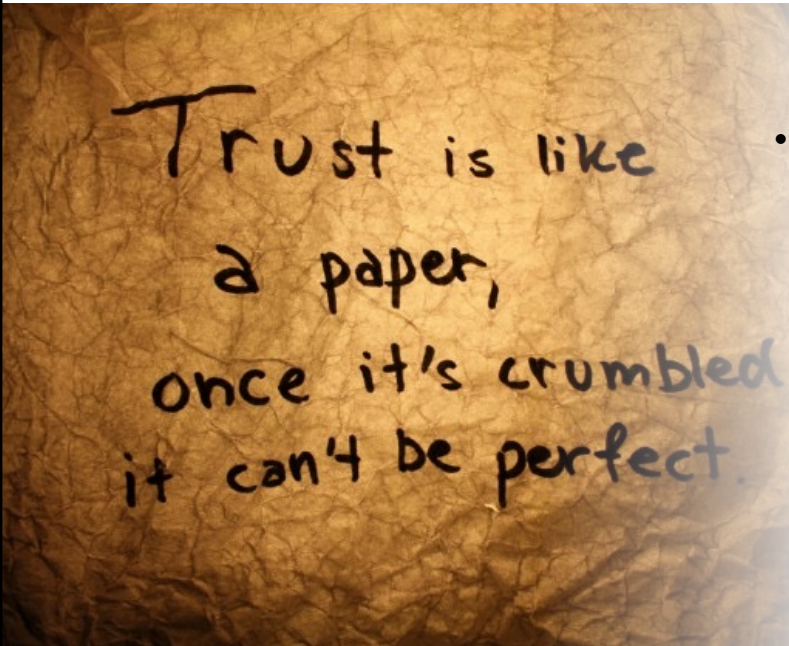
- 6G and SECURITY PERSPECTIVES
- **TRUST**
- CYBER THREAT INTELLIGENCE

UnB

16/83

16





Trust is like  
a paper,  
once it's crumbled  
it can't be perfect.

- Human social aspect:
  - To believe that someone is good and honest and shall not harm you;
  - Something that is safe and trustable;
  - Depends on the context:
    - A trusts B to...;
    - A doesn't trust B to...;

17

## TRUST

### In computing systems:

- Trust is relative to a particular context;  
**A shall trust B to get a ride, but A doesn't trust B to drive his car;**
- Trust has a directional aspect;  
**A can trust B, but it does not mean B trusts A;**
- Trust has evulative and temporal aspect;  
**Trust A has in B can increase over the time;**
- Trust can be influenced by reputation;  
**A trusts B and now starts trusting C by recommendation of B;**
- Trust is not transitive;  
**If A trusts B and B trusts C, it does not mean A trusts C;**

18


# TRUST

- Do not make confusion of **TRUST** with **REPUTATION**;
- **REPUTATION**:
  - Is an opinion someone has about others or something;
  - Has similar attributes to trust, but it is different;

**Trust: I trust A for a reason;**

**Reputation: He has a good reputation for conducting business**




19/83

19


# TRUST

## In 6G

SIX-Trust for 6G:  
Toward a Secure and Trustworthy Future Network

<https://ieeexplore.ieee.org/abstract/document/10268440>

<b>Trustworthy AI</b> Privacy-preserving Explainable Unbiased	<b>Trust Evaluation</b> Static Dynamic	<b>Trust Relationship</b> Federated Decentralized
<b>Trustworthy Architecture</b> Distributed Autonomous	<b>Trustworthy Protocols</b> 6G-AKA EAP-TLS+	<b>Trustworthy Underlay</b> DPKI NFV/NFVI
<b>Trusted Foundation</b> Asymmetric Crypto Post-quantum Crypto	<b>Trusted Platform</b> TEE Blockchain	<b>Trusted Hardware</b> TPM eSIM/iSIM eTPSIM


20/83

20

## TRUST

For instance, would you trust this code?

```
unsigned char *buffer, *bp;  
int r;  
buffer = XXXXXX_malloc(1 + 2 + payload + padding);  
bp = buffer;  
*bp++ = XXX1_HB_RESPONSE;  
s2n(payload, bp);  
memcpy(bp, pl, payload);
```

## TRUST

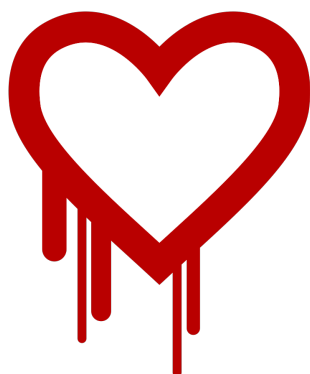
The previous code is...



- It was a serious vulnerability in the popular OpenSSL cryptographic software library.
- It allowed stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.
- It is the core for security and privacy over the Internet for applications

## TRUST

### Consequences...



- Allowed anyone on the Internet to read the memory of the systems protected by the vulnerable version.
- It compromised the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content.
- Allowed the eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

## TRUST

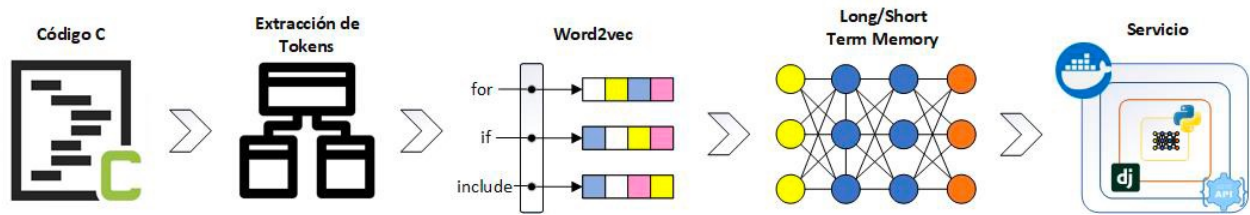
### Using Machine Learning to address buffer overflow in C ?

**Método para identificar buffer overflow en código C mediante Técnicas de Procesamiento de Lenguaje Natural**

**Submitted to XVIII Reunión Española de Criptología y Seguridad de la Información  
León 23 – 25 de octubre de 2024.**

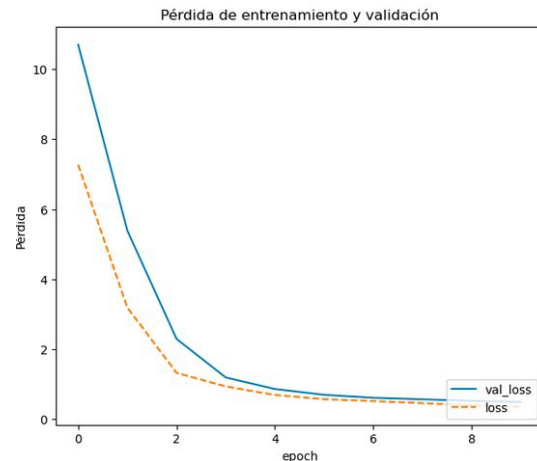
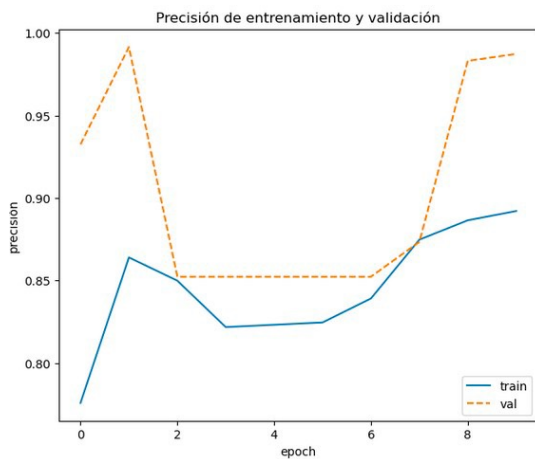
# TRUST

## Using Machine Learning to address buffer overflow in C



# TRUST

## Some results of the research...



# TRUST

## Some results of the research...

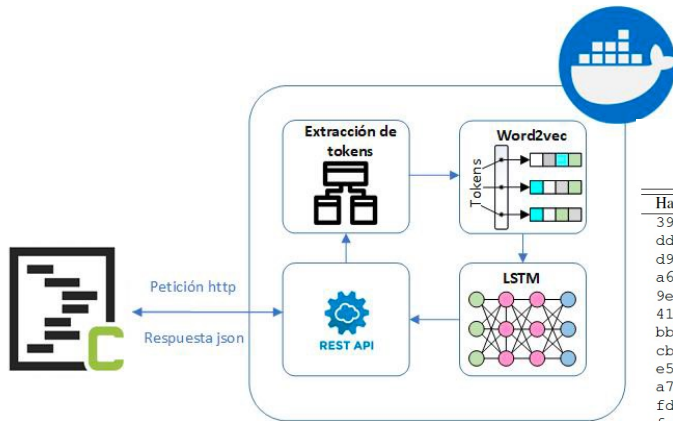
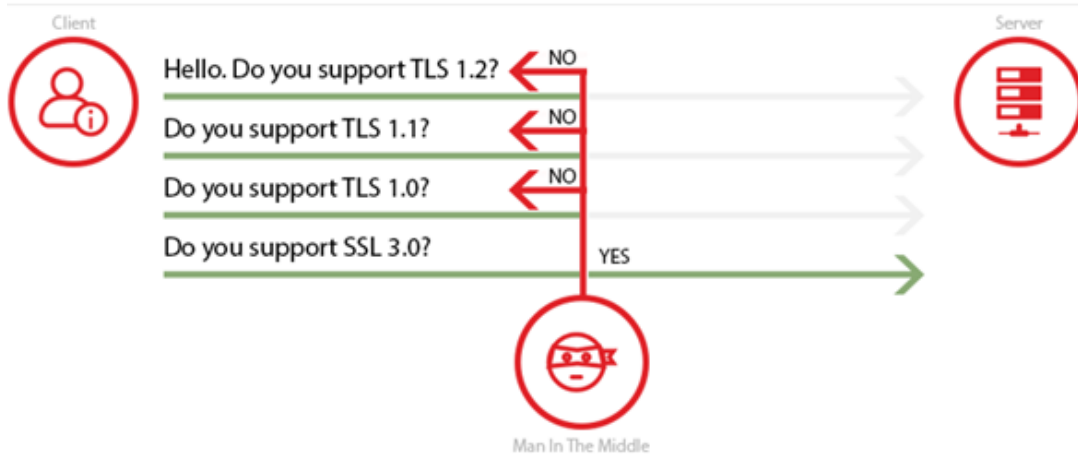


Tabla II  
PRUEBAS REALIZADAS CON CÓDIGO C

Hash	Esperado	Obtenido
3966c51d93f5abd729bd7c4963c86c6c1c	buffer overflow	buffer overflow
ddb5753ac0d84677f97760962a574		
d99fc496667c299831d8f7d47bbe175d0d	buffer overflow	buffer overflow
a6f3912ea84621c218e1563d94130c		
9e76e7f48ba55abe4e513d00e6fa5c2ee8	buffer overflow	not vulnerable
41d015808201248439d3702a45bf53		
bb86dfd403af77e14682403e30fd863fdf	not vulnerable	buffer overflow
cbe03516a2212677b10ac414d2ef30		
e51d9aa9dec0b525afb4660f0abcc3fb6	not vulnerable	not vulnerable
a76c668e56aac4326355383deebf2e		
fdb915b9943b3b2b20451fc58f9c9fcd7	not vulnerable	buffer overflow
fe2703ee3dea3ba05f8c13a4f38d14		

# TRUST

## Other exemple...



# TRUST

## Padding Oracle On Downgraded Legacy Encryption



# TRUST

### What would you say? Would you trust it?



#### Cipher Suites

#### # TLS 1.1 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits)	FS	
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 4096 bits	FS	<b>WEAK</b>
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits)	FS	
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 4096 bits	FS	<b>WEAK</b>
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits)	FS	
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 4096 bits	FS	<b>WEAK</b>
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)			<b>WEAK</b>
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)			<b>WEAK</b>
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)			<b>WEAK</b>

#### # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits)	RSA	FS	
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits)	RSA	FS	
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 4096 bits			FS
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 4096 bits			FS
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH secp256r1 (eq. 3072 bits)	RSA	FS	<b>WEAK</b>
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits)	RSA	FS	<b>WEAK</b>
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b)	DH 4096 bits			FS <b>WEAK</b>
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	DH 4096 bits			FS <b>WEAK</b>
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)	ECDH secp256r1 (eq. 3072 bits)	RSA	FS	<b>WEAK</b>
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits)	RSA	FS	<b>WEAK</b>
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x67)	DH 4096 bits			FS <b>WEAK</b>
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33)	DH 4096 bits			FS <b>WEAK</b>
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (0xc012)	ECDH secp256r1 (eq. 3072 bits)	RSA	FS	<b>WEAK</b>
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	DH 4096 bits			FS <b>WEAK</b>
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d)				<b>WEAK</b>
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c)				<b>WEAK</b>
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)				<b>WEAK</b>
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)				<b>WEAK</b>
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)				<b>WEAK</b>
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)				<b>WEAK</b>
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)				<b>WEAK</b>


# TRUST

## What would you say?

**SSL Report: enisa.eu**  
Assessed on: Tue, 25 Jun 2024 07:59:16 UTC | HIDDEN | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	<a href="#">2a02:5b40:4:224:0:0:0:d</a> urifw1.level27.eu Ready	Tue, 25 Jun 2024 07:54:22 UTC Duration: 146.778 sec	<b>B</b>
2	<a href="#">185.3.216.14</a> urifw1.level27.eu Ready	Tue, 25 Jun 2024 07:56:49 UTC Duration: 147.183 sec	<b>B</b>

 31/83

31

# TRUST

## Let's try?

### 5 min activity...

<https://www.ssllabs.com/ssltest/index.html>



 32/83

32



## AGENDA

- 6G and SECURITY PERSPECTIVES
- TRUST
- CYBER THREAT INTELLIGENCE

## CYBER THREAT INTELLIGENCE

### Threat definition (ISO 27000):

- potential cause of an unwanted incident, which can result in harm to a system or organization;



### Vulnerability definition (ISO 27000):

- weakness of an asset or control that can be exploited by one or more threats



## CYBER THREAT INTELLIGENCE

### Risk definition (ISO 27000):

- effect of uncertainty on objectives
  - An effect is a deviation from the expected — positive or negative.
- Residual risk
  - risk remaining after risk treatment
  - can contain unidentified risk



## CYBER THREAT INTELLIGENCE

### • Risk Analysis (ISO 27000):

- process to comprehend the nature of risk and to determine the level of risk
- provides the basis for risk evaluation and decisions about risk treatment
- includes risk estimation.



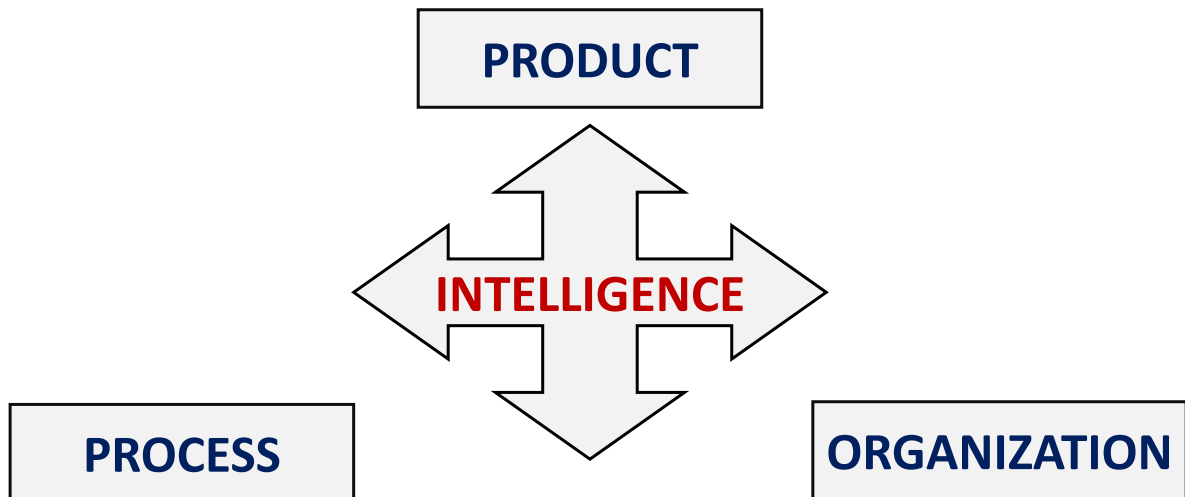
# CYBER THREAT INTELLIGENCE

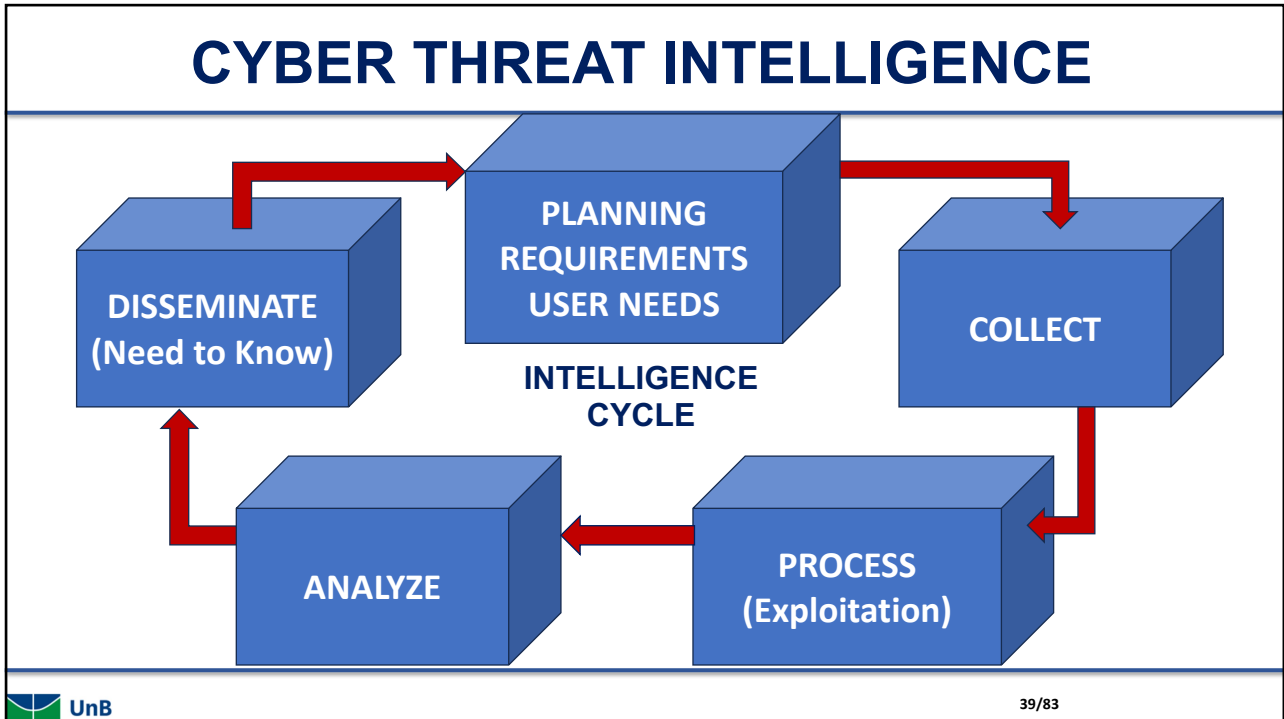
## And Cyber?

- Related to computers;
- Related to Machinery;
- Related to Internet;
- Related to technology;
- Many more...

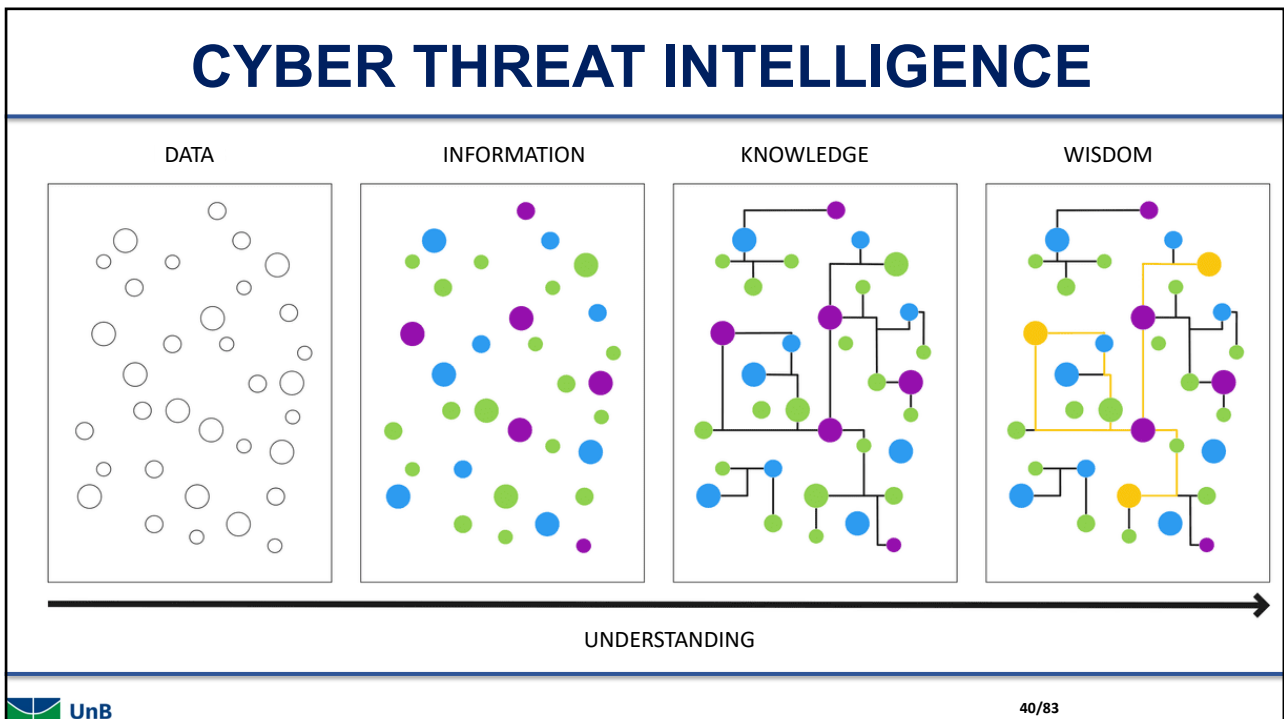


# CYBER THREAT INTELLIGENCE



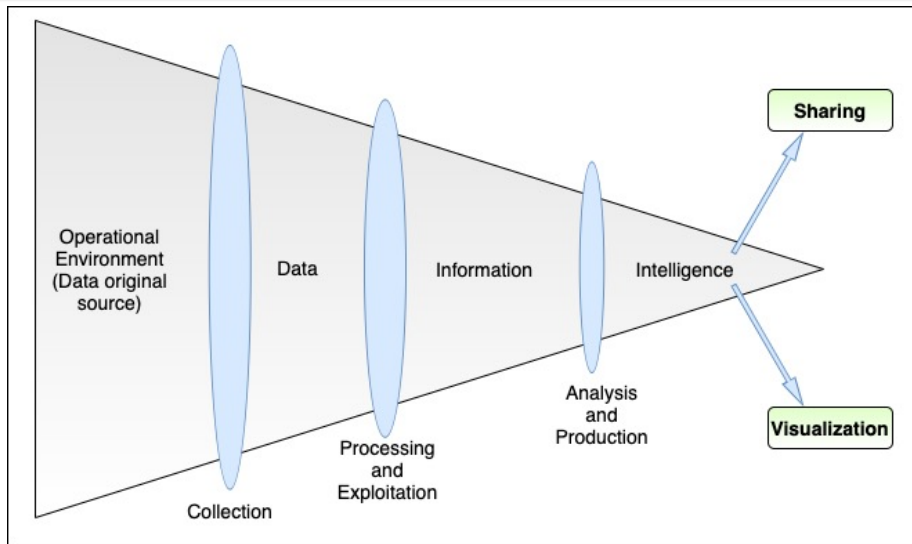


39



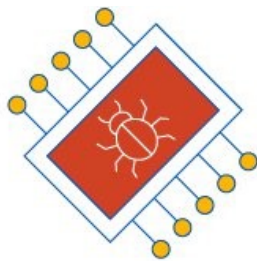
40

# CYBER THREAT INTELLIGENCE

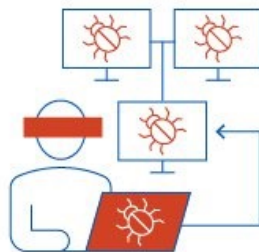


# CYBER THREAT INTELLIGENCE

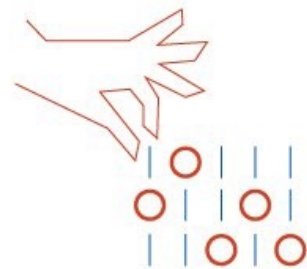
## TTPs



Tactics/Tools



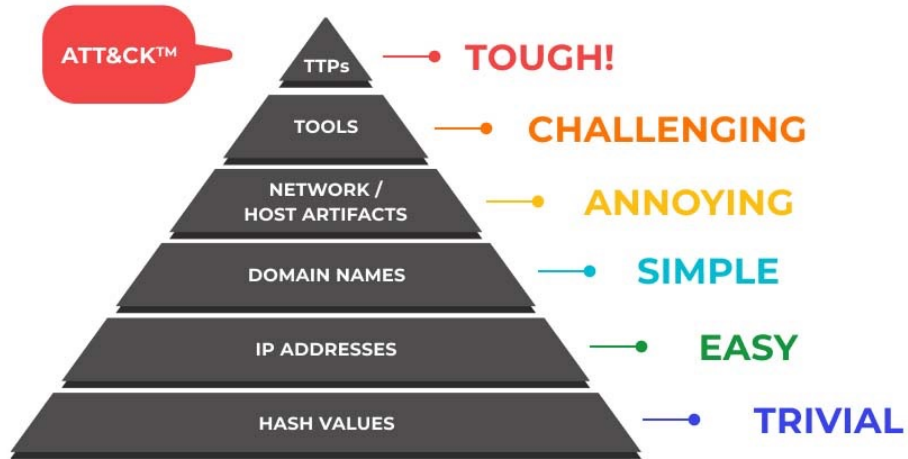
Techniques



Procedures

# CYBER THREAT INTELLIGENCE

## What is MITRE ATT&CK?



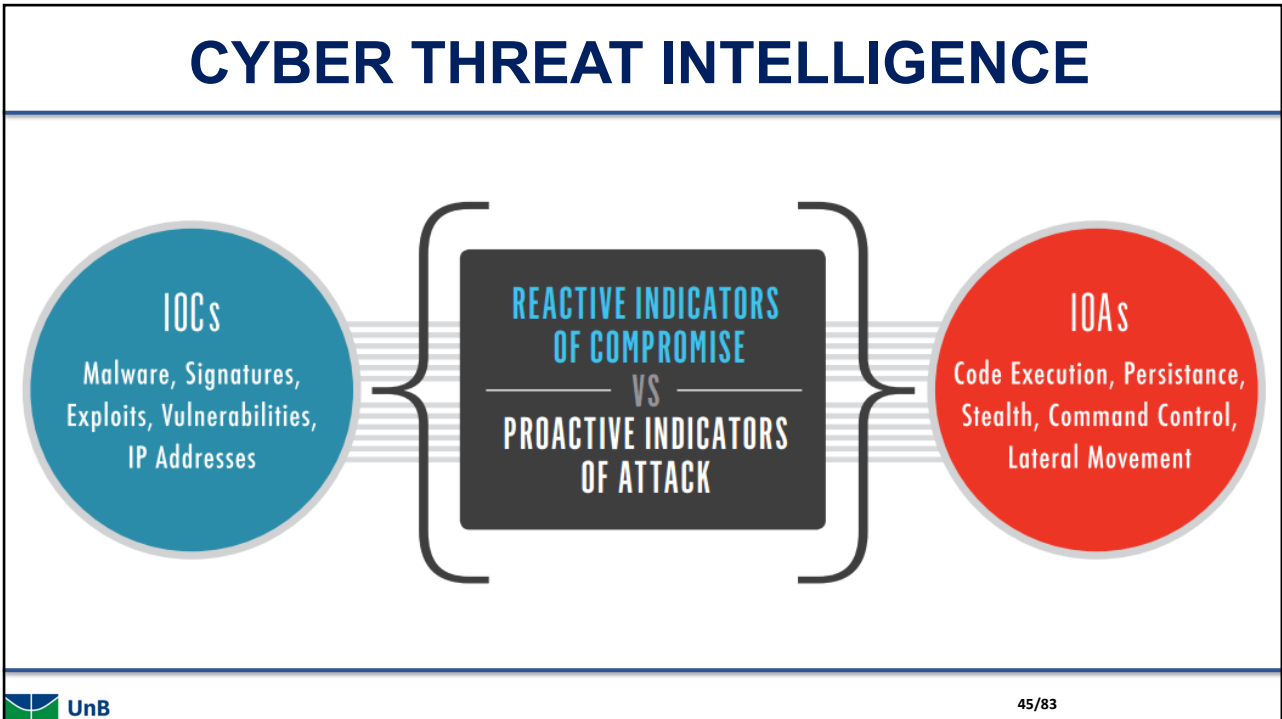
# CYBER THREAT INTELLIGENCE

Let's play a little?

5 min activity...

<https://mitre-attack.github.io/attack-navigator/>





45



46

## CYBER THREAT INTELLIGENCE

### Actionable Intelligence

- To have the necessary information immediately available to deal with the situation at hand (**context is key**);
- temporal aspect is essential because the situation can evolve and escalate quickly;
- it is considered the “golden nugget”;
- It has a purpose;



## CYBER THREAT INTELLIGENCE

### It is a complicated issue...

- Who wants information they can't trust?
- Intelligence from an untrustworthy source is not actionable.
- It is important that the producer and consumer trust each other.
- This trust must be based on transparency and verification.





## CYBER THREAT INTELLIGENCE

### How to define threat intelligence...

- IT Depends on the source you check...
- There is no single definition accepted by all...



## CYBER THREAT INTELLIGENCE

### Some say threat intelligence is...

- product resulting from: collection, processing, integration, analysis, evaluation and interpretation of available information;
- related to the interest of the topic and the interest of those who want to know about a threat;

## CYBER THREAT INTELLIGENCE

### **Some say threat intelligence is...**

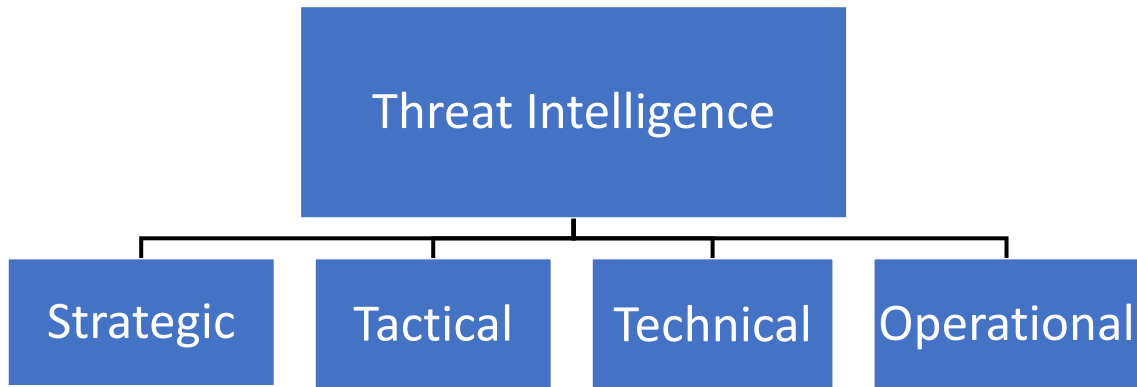
- Information and knowledge about an opponent obtained through:
  - observation
  - investigation
  - analysis or understanding.

## CYBER THREAT INTELLIGENCE

### **Some say threat intelligence is...**

- Knowledge based on:
  - evidence
  - context
  - mechanisms
  - indicators
  - implications and practical advice on an existing or emerging threat or danger to assets

# CYBER THREAT INTELLIGENCE



# CYBER THREAT INTELLIGENCE

## Threat intelligence:

- It must have



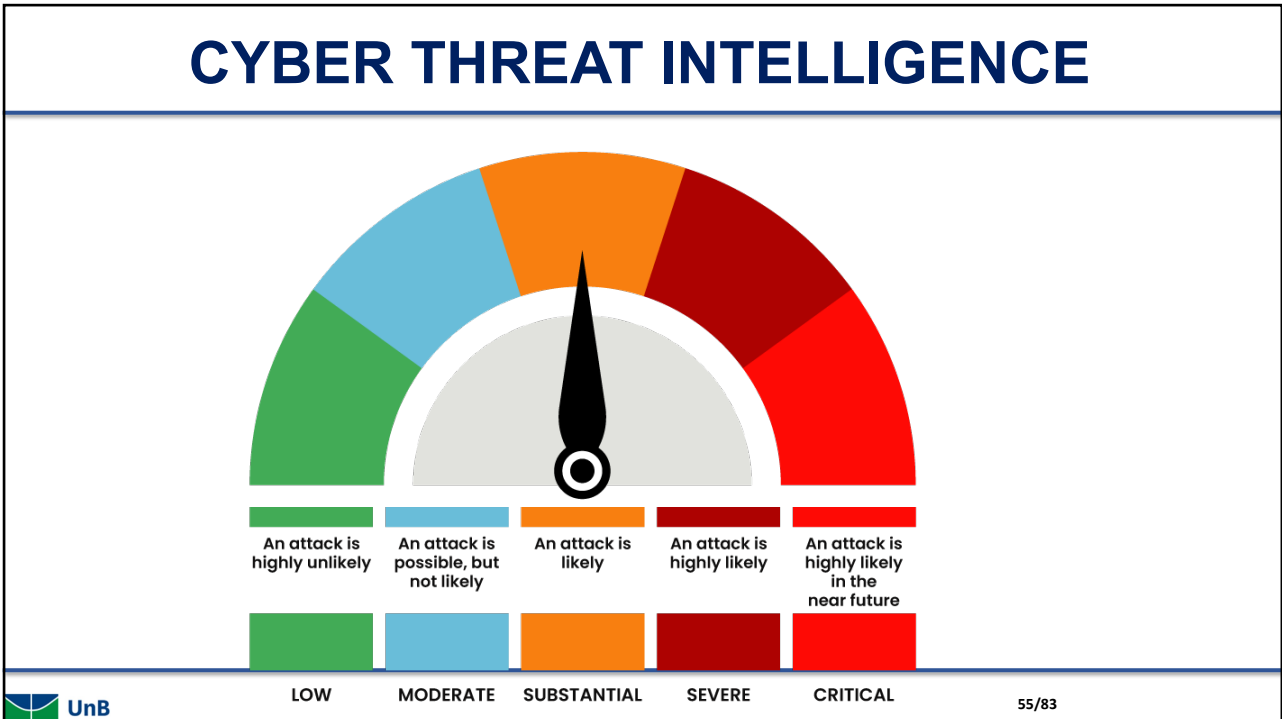
Precision



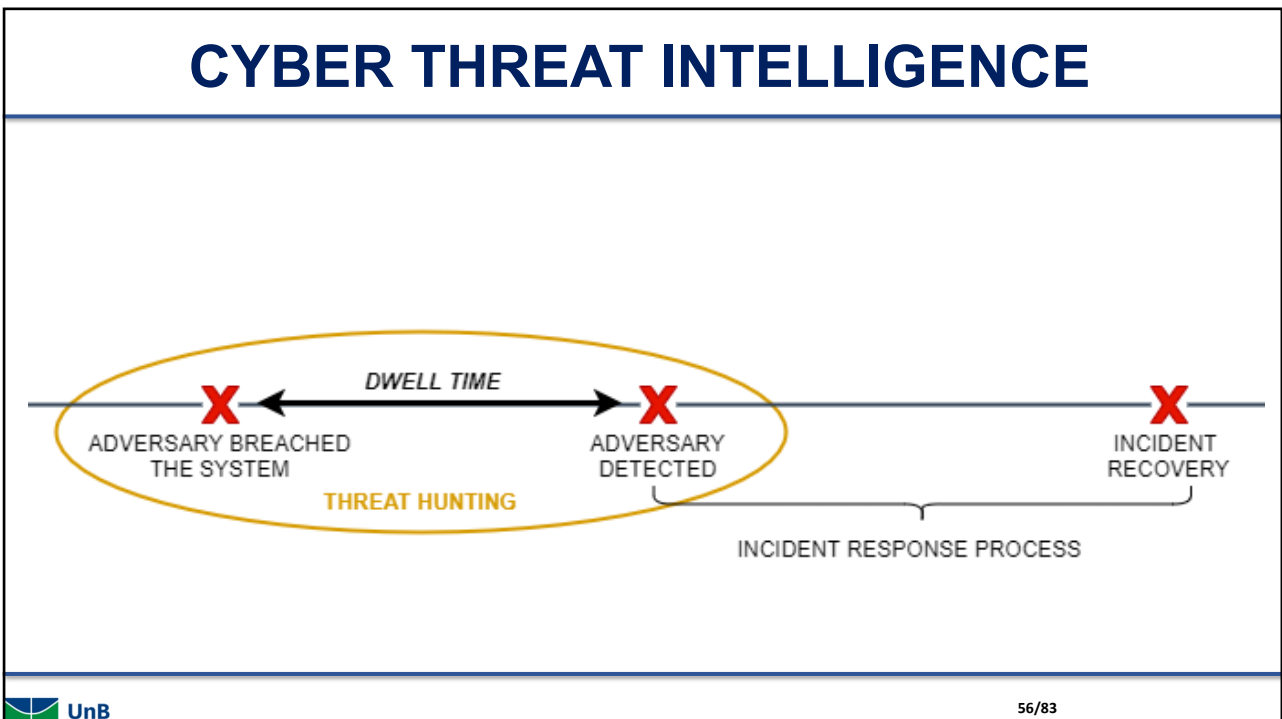
Opportunity



Relevant

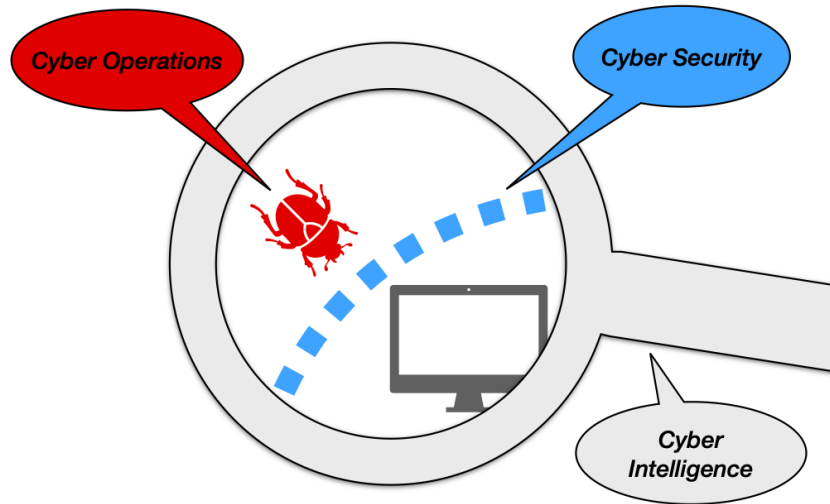


55

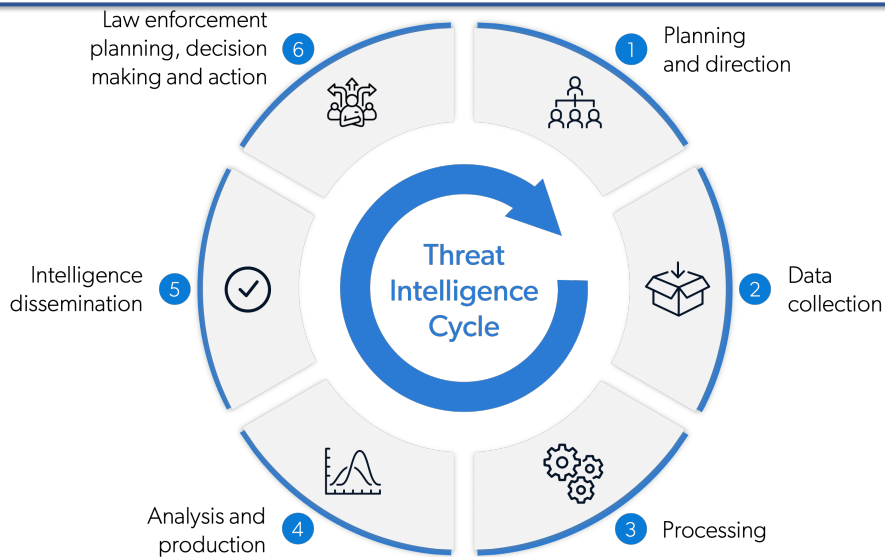


56

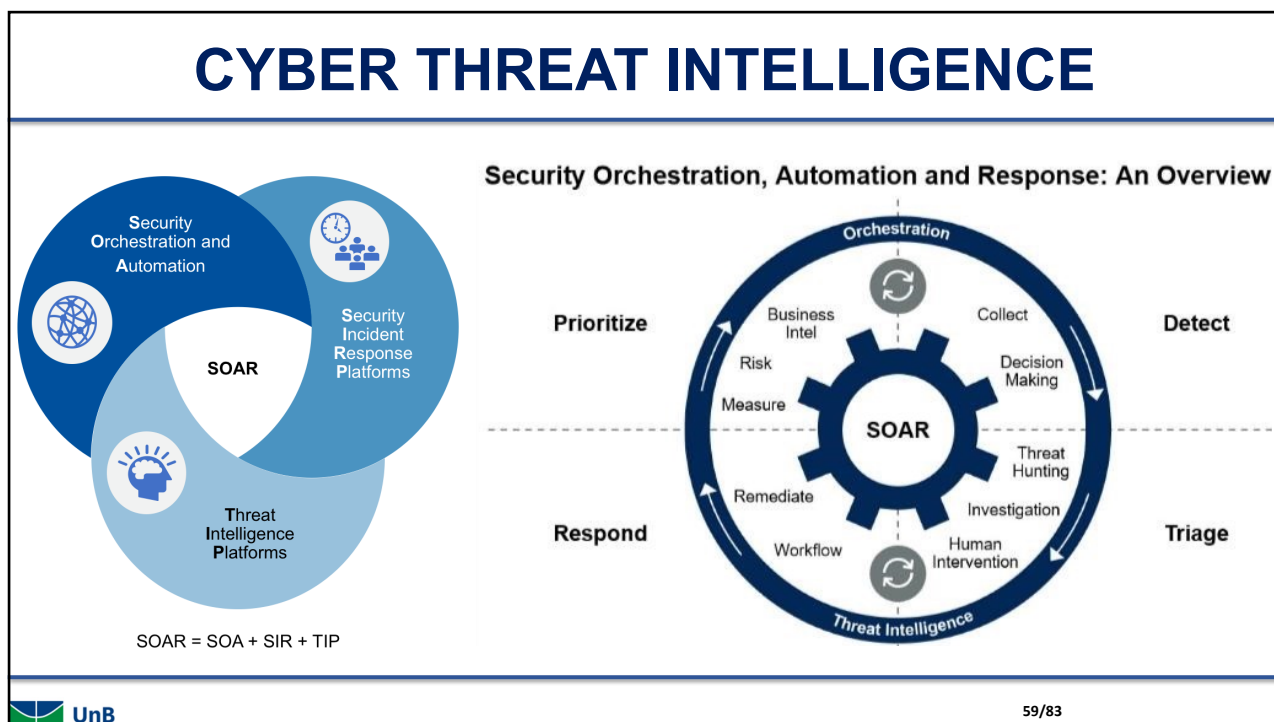
# CYBER THREAT INTELLIGENCE



# CYBER THREAT INTELLIGENCE



## CYBER THREAT INTELLIGENCE



59

## CYBER THREAT INTELLIGENCE

### CTI standards:

- **STIX (Structured Threat Information eXpression)**
- **language to standardize:**
  - **specifications;**
  - **dumps of data;**
  - **event communication;**
  - **Other things as needed...**

UnB

60/83

60

# CYBER THREAT INTELLIGENCE

## STIX domains









	Attack Pattern		Identity		Location
	Campaign		Indicator		Malware
	Course of Action		Infrastructure		Malware Analysis
	Grouping		Intrusion Set		Note


 61/83

61

# CYBER THREAT INTELLIGENCE

## STIX domains

	Observed Data		Tool
	Opinion		Vulnerability
	Report		Relationship
	Threat Actor		Sighting

 62/83

62

## CYBER THREAT INTELLIGENCE

### STIX (structure): json

```
{
  "type": "campaign",
  "id": "campaign--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",
  "spec_version": "2.1",
  "created": "2016-04-06T20:03:00.000Z",
  "modified": "2016-04-06T20:03:23.000Z",
  "name": "Threat actor XZY who attacks the finance sector",
  "description": "campaign of XZY Group against services in the
  financial sector."
}
```

## CYBER THREAT INTELLIGENCE

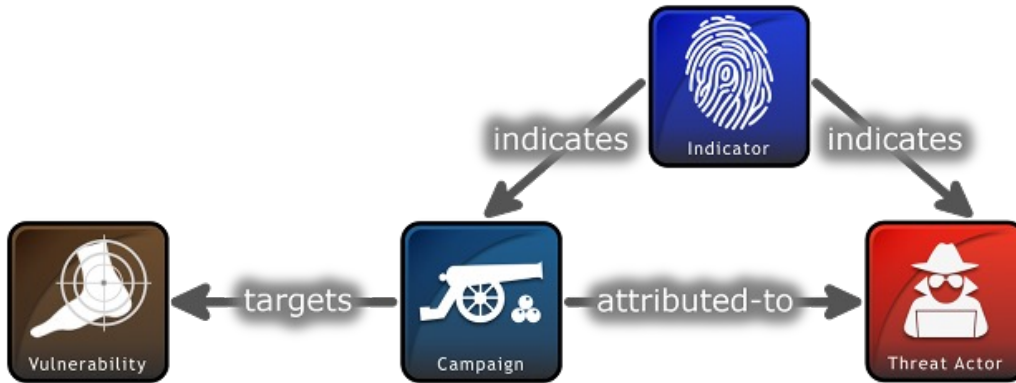
### STIX (relationship): json

```
{
  "type": "relationship",
  "spec_version": "2.1",
  "id": "relationship--1b9f02a9-2239-4d28-a55d-0e36ab7064c3",
  "created": "2021-12-20T12:39:22.417899Z",
  "modified": "2022-07-03T20:00:09.969896Z",
  "relationship_type": "indicates",
  "source_ref": "malware--e9140892-5f2f-439b-928d-4e87345fe07a",
  "target_ref": "indicator--8926a394-5c2b-4fad-9353-b0e7c9f3a5a3",
  "confidence": 55
}
```



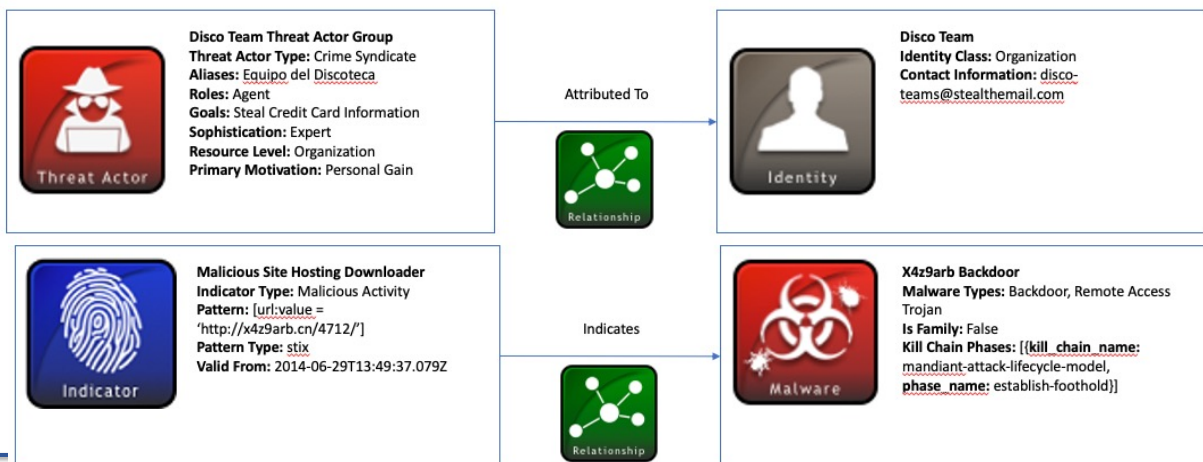
# CYBER THREAT INTELLIGENCE

## STIX (relationship): visualize



# CYBER THREAT INTELLIGENCE

## STIX (relationship): visualize

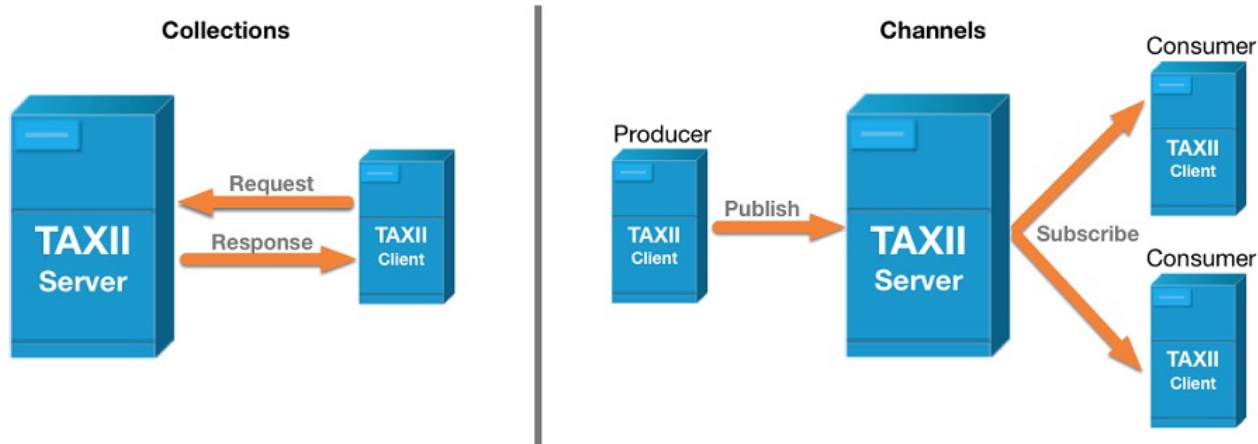


## CYBER THREAT INTELLIGENCE

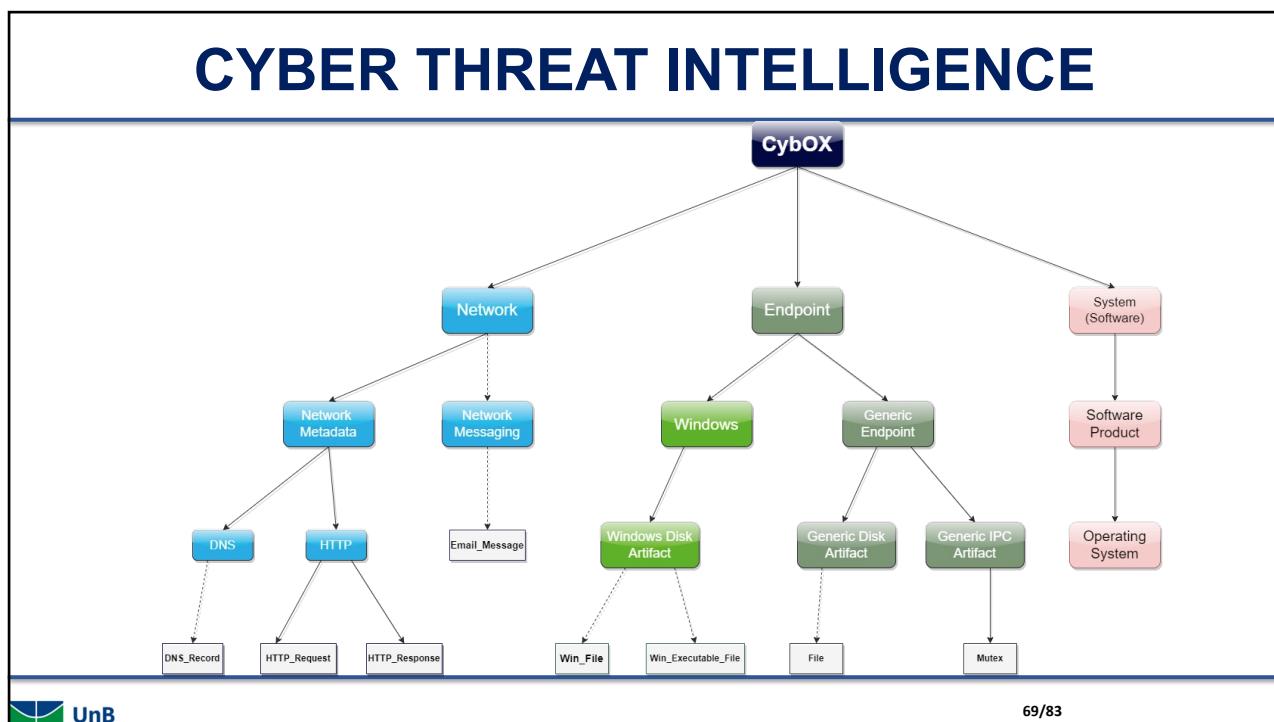
### TAXII

- Trusted Automated Exchange of Intelligence Information
- Application protocol to Exchange CTI using HTTPS;
- defines an API RESTful and a set of requirements for clients in TAXII Servers

## CYBER THREAT INTELLIGENCE



## CYBER THREAT INTELLIGENCE



69

## CYBER THREAT INTELLIGENCE

### CTI tools

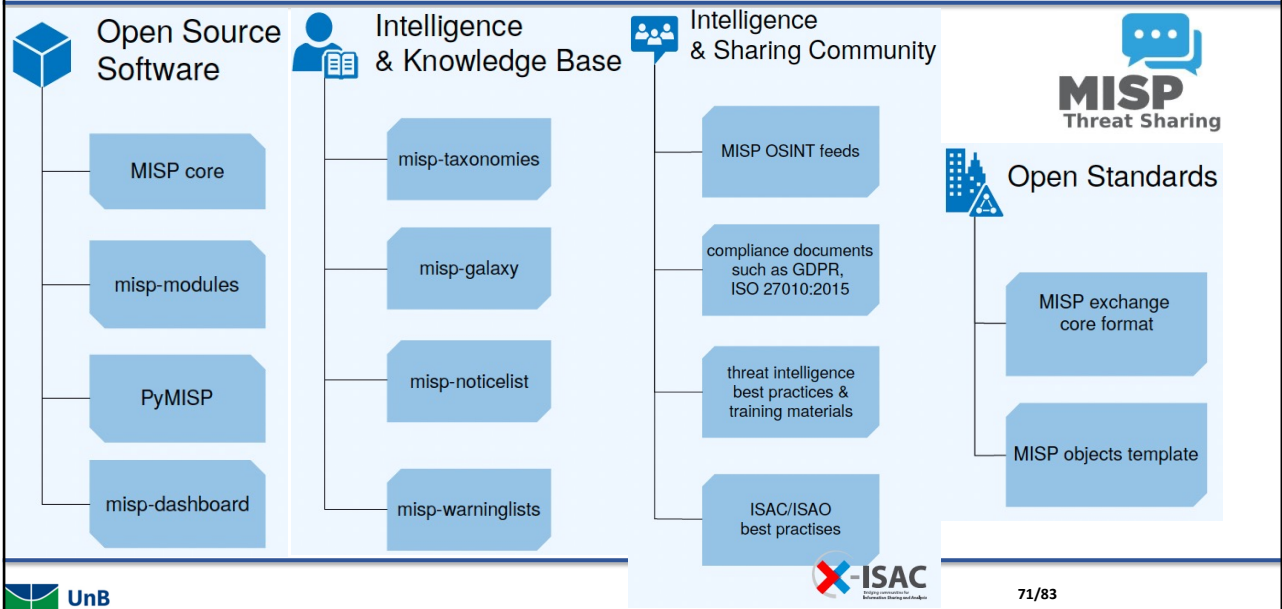
- Basically implements the standards and tries to organize CTI data;
- Tries do provide a way to organize the CTI cycle;
- Used to help in incident response issues;
- Document information;

UnB

70/83

70

# CYBER THREAT INTELLIGENCE



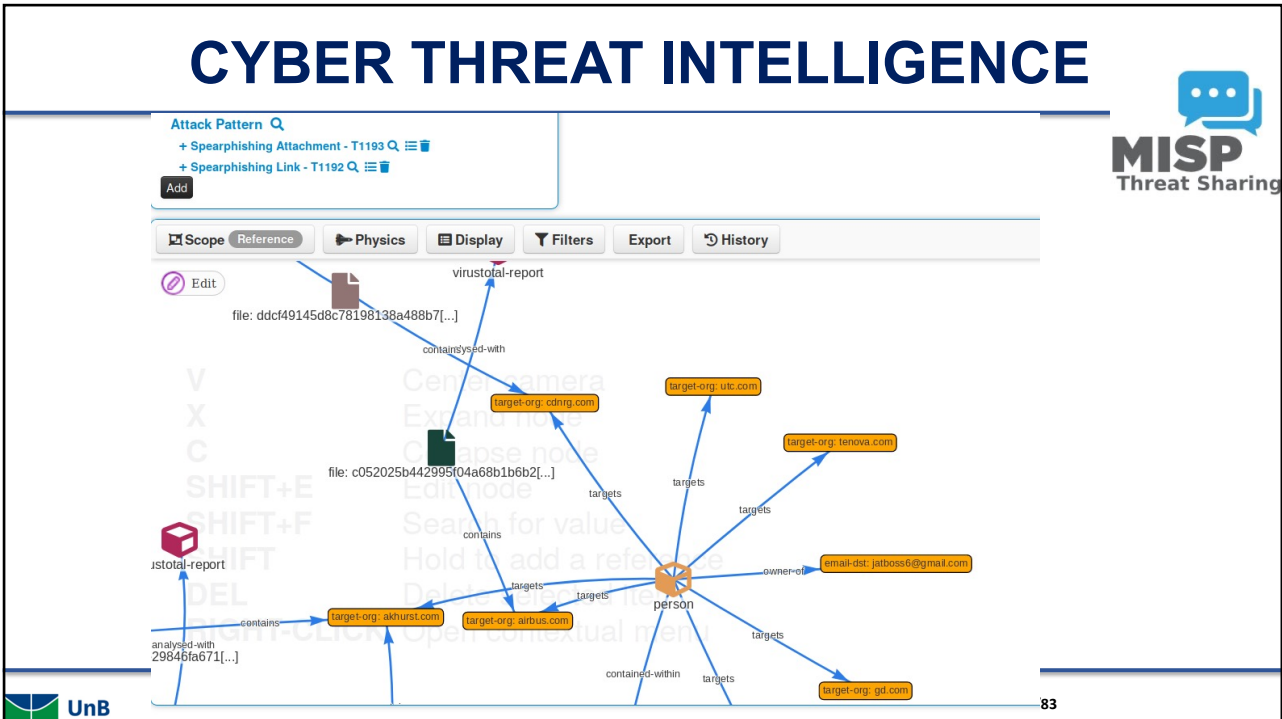
71

# CYBER THREAT INTELLIGENCE

The screenshot displays the MISP web interface for a specific event. On the left, a sidebar shows event details for ID 10728, including metadata like Uuid, Org (CIRCL), Date (2018-05-04), and Threat Level (Low). The main area features a 'Distribution graph (atomic event)' which is a donut chart showing the event's distribution across different sharing groups: 'Your organisation only' (red), 'This community only' (yellow), 'All communities' (green), and 'Sharing group' (blue). Below the graph are filters for 'All', 'Attributes', and 'Object attributes'. The central part of the interface shows a network graph of related events and objects, with a search bar and various interaction options like 'Expand node', 'Collapse node', and 'Edit node'. On the right, a detailed view of a 'Matched event' (ID: 10728) is shown, including its analysis status, threat level, and tags such as 'osint-feed', 'ip-white', and 'malware-classification:malware-category="Ransomware"'. The bottom of the interface shows a snippet of a YARA rule: `estimative-language:confidence-in-analytic-judgment="high"`.

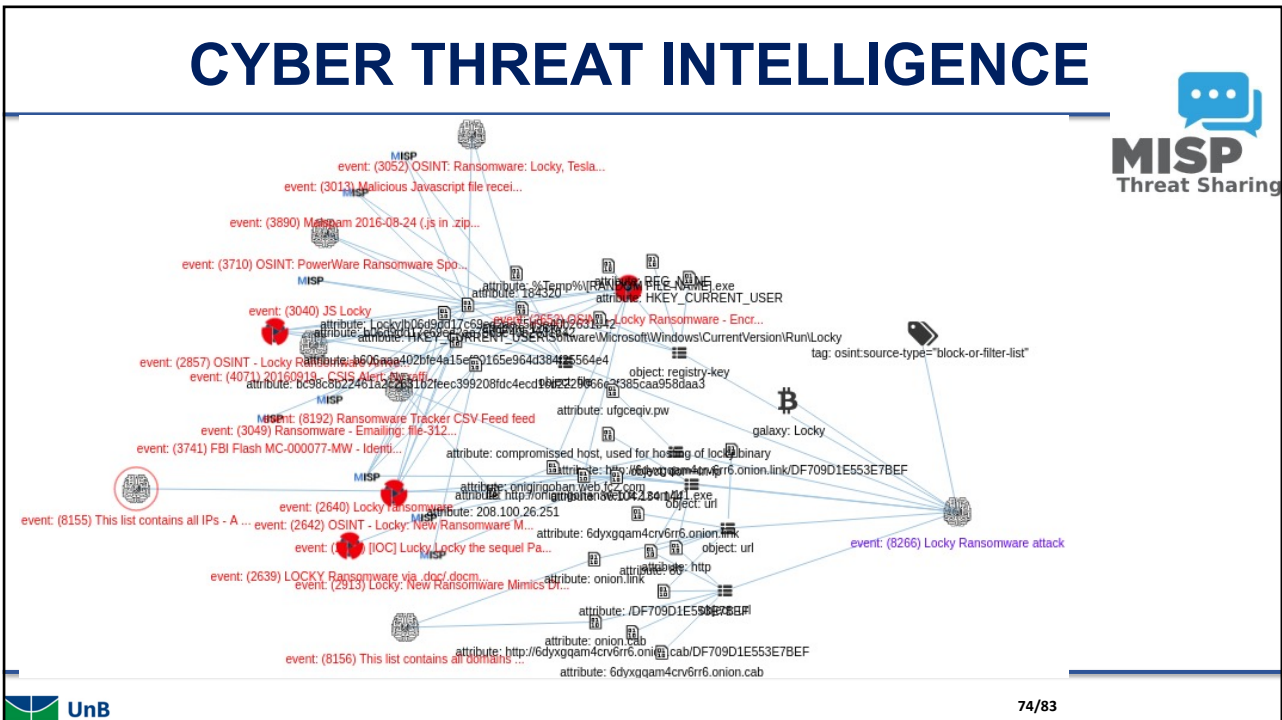
72

# CYBER THREAT INTELLIGENCE




73

# CYBER THREAT INTELLIGENCE




74


# CYBER THREAT INTELLIGENCE



## MISP (**observations**):


- Own standard
  - DATA MODELS
  - MISP CORE FORMAT
  - MISP TAXONOMIES
  - MISP GALAXY
  - MISP OBJECTS
  - DEFAULT FEEDS




75/83

75

# CYBER THREAT INTELLIGENCE



**Inputs**

**Cyber Threat Intelligence**

Aggregate cyber threat intelligence feeds and pieces of information from multiple systems and services.

**Sightings & incidents**

Handle sightings, incidents and cases including investigations directly in the platform.

**Vulnerabilities & exploits**

Ingest vulnerabilities information, available exploits and on-going campaigns targeting them.

**Assets & artifacts**

Import asset management data such as software versions and artifacts from the information system.

Modelization      Reasoning

Generative AI      Automation

**Outputs**

**Cyber Threat Intelligence**

Knowledge base about threat actors, malware, tactics and landscape.

**Detection**

Feed detection capabilities with curated and accurate detection as code.

**Incident Response**

Handle case management, response, investigation, sandboxes and forensics.

**Reports & dashboards**

Be alerted and visualize trends on the relevant threats to an organization.


**Risk Analysis**

Feed risk analysis with accurate information about cyber threats.

**Anticipation**

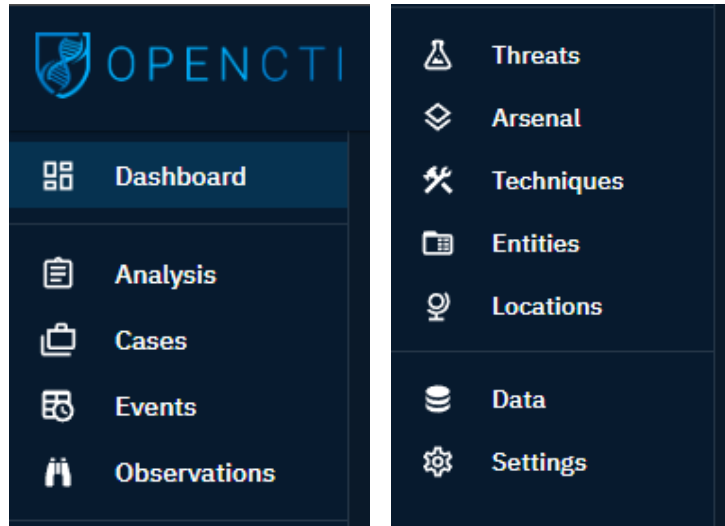
Create stress tests, exercises, purple teaming based on actual threats.

Operational
Strategic


76/83

76

# CYBER THREAT INTELLIGENCE



# CYBER THREAT INTELLIGENCE



## CYBER THREAT INTELLIGENCE

### CTI sharing problems:

- What will I share?
- Who will I share with?
- Why will I share?
- In what format will I share?
- Is there any temporal aspect to consider?
- Is knowledge/information classified?

## CYBER THREAT INTELLIGENCE

Let's try?

5 min activity



<https://demo.opencti.io/dashboard>



## FINAL REMARKS

- So... It was a really long journey of concepts, technologies, problems...
- I will leave you with a research avenue with one question...

**How to apply trust and cyber threat intelligence in the perspective of 6g considering what you have seen in this week?**

## FINAL REMARKS

**Q&A**



# First Summer School on Security and Privacy in 6G Networks

## TRUST AND CYBER THREAT INTELLIGENCE IN THE PERSPECTIVE OF 6G



Robson de Oliveira Albuquerque  
University of Brasília

Faculty of Computer Science and Engineering, UCM  
Madrid (Spain), June 24 - 28, 2024