TRUST aWARE

Enhancing Digital Security, Privacy and TRUST in softWARE

MISP Guide Demo and Security and Privacy (S&P) Taxonomy

ABI Lab / CERTFin

Italy, Milan / 27th March / TRUST aWARE 2nd Technical Meeting

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

Security and Privacy (S&P) Threats

- **MISP Taxonomies of Privacy Focused Threats**

  Defines a shared taxonomy, to be implemented in a structured, automated and governed exchange of indicators compromise related to cyber threats

  In order to provide a taxonomy classifying the privacy threats it is first needed to understand **what a S&P threat is as to define its perimeter**

- **S&P perimeter**:

  →Looking after an actionable definition of S&P Threat

  →Systematic review of literature (Research Papers and Industry Specific) and a range of reputable sources to outline additional S&P Threats under the cybersecurity standpoint including:

  →NIST

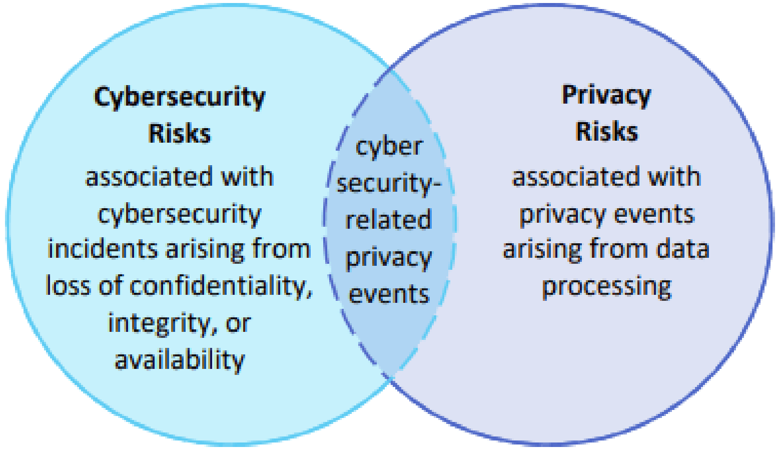
  →OWASP

  →ENISA

  →MITRE

  →ThreatMatch

  →SoTA Taxonomies


Cybersecurity Risks
associated with cybersecurity incidents arising from loss of confidentiality, integrity, or availability
cyber security-related privacy events
Privacy Risks
associated with privacy events arising from data processing

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

How we defined the perimeter of S&P threats: Analysis of Privacy definitions over the years (1890-2023)

“***the right to be let alone***” freedom from intrusion

“***the right to informational self-determination***”, “control, edit, manage, and delete information about themselves and decide when, how and to what extent that information is communicated to others

The right to privacy: “***Individuals, groups, or institutions have the right to control, edit, manage, and delete information about them and decide when, how, and to what extent that information is communicated to others.***”

“to protect the individual against infringement of his/her personality right as the result of the handling of his/her personal data”

“the protection of individuals (single and in groups) against infringement of their private spheres and their personality, in particular as the result of handling of their data.”

privacy threat means any threat or ***series of connected threats to unlawfully use or disclose to the public Personally Identifiable Non-Public Information that was misappropriated from a user for the purpose of demanding money, including virtual, digital, and electronic currency, securities, or other property of value from a user***;

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

How we defined the perimeter of S&P threats: EDPS and GDPR

According to the EU Data Protection Supervisor ***"Privacy is the ability of an individual to be left alone, out of public view, and in control of information about oneself"***.

According to GDPR, ***"data privacy means empowering your users to make their own decisions about who can process their data and for what purpose."***

*One can distinguish **the ability to prevent intrusion** in one's physical space ("physical privacy", for example with regard to the protection of the private home) and the ability **to control the collection and sharing of information about oneself** ("informational privacy").*

↓

*The concept of privacy therefore **overlaps, but does not coincide, with the concept of data protection**."*

Source: https://edps.europa.eu/data-protection/data-protection/glossary/p_en

GDPR data privacy requirements.

- *Article 12 — Transparency and communication*
- *Articles 13 & 14 — When collecting personal data*
- *Article 15 — Right of access*
- *Article 16 — Accuracy*
- *Article 17 — Right to erasure*
- *Article 18 — Right to restrict processing*
- *Article 20 — Data portability*
- *Article 21 — Right to object*

Source: https://gdpr.eu/data-privacy/

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

Definition of S&P Threats

S&P threat definition overlap of both regulatory and cybersecurity mindsets

S&P Threat definition:

A threat which belongs to one or both of the following scenarios:

***Cybersecurity Incident** that leads to a breach of privacy, undermining the Confidentiality, Integrity and Availability in any phase of the data life cycle management (e.g., Data acquisition, Data processing etc.)*

***Act** – whether malicious or not – that result to a **non-compliance of regulatory requirements** (e.g., through unauthorized data processing, unauthorized selling of personal information, etc.), affecting individual's privacy as well as leading to potential adverse consequences to fundamental rights, stigmas, or more tangible harms such as discrimination, economic loss, or physical harm. Moreover, it includes cases in which the perpetrator violates one of the EU data protection principle*

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

D4.7 - MISP Taxonomies

- S&P Taxonomy: by adhering to the definition of S&P Threat, we finalised that the privacy threats can fall under two main groups (i.e., Cybersecurity Incidents and Compliance Issues), which are spread across **5 categories**:

  1. **Information collection:** threats that occur when the way of accessing and collecting individuals' personal data does not follow the principle of informed consent, hence constituting an unlawful action (e.g., legitimacy of interest is not pursued by the data controller or by a third party)
  2. **Information processing:** vulnerabilities originated from the use, storage, and manipulation of the collected personal data whose way of processing does not constitute a legitimate interest and/or does not satisfy transparency requirements
  3. **Information dissemination:** threats that lead to the disclosure of personal data beyond the lawful boundaries defined by the purpose of the data controller or a third party
  4. **Invasions:** threats that directly target individuals (i.e., intrusions and social engineering)
  5. **Compliance:** covers threats that do not comply with regulatory requirements
     - *Not complying with individual rights*
     - *Not providing contact details of a responsible person*
     - *Improper personal data breach response*

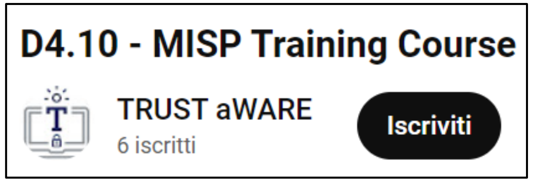
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

MISP Training – Goals and Contents

- **Goal: develop proficiency** in using the MISP platform **from both user and admin sides**, describing the main MISP features and the required front-end/back-end configurations, as well as troubleshooting aspects.

- Duration of the training course ≈ **50 mins**

Available on **YouTube**



D4.10 - MISP Training Course

TRUST aWARE

6 iscritti

- The training course is divided in **11 lessons** and includes:
  - **Theoretical aspects** (e.g., description of user interface, features, configurations, etc.)
  - **Practical scenarios**
  - **Recommendations**

- Follows a logical thread:

MISP Installation procedure → Description of MISP core features → Extras → Troubleshooting

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

MISP Training – Goals and Contents

MISP Training course

MISP core features

[01:42] **How to install MISP**
[07:40] **Create a new user** (**MISP-as-a-Service**)
[09:56] **Create a MISP event**

- a. [15:36] Free-text-import tool
- b. [16:32] Manual input
- c. [17:29] Objects
- d. [18:41] Templates

[19:44] **Publishing a MISP event**
[20:44] **Delegating a MISP event**
[22:43] **Propose a change to a MISP event**
[23:57] **Contact reporter**
[24:44] **Searching MISP events and attributes**
[27:14] **Synchronizing two MISP instances**

MISP extras

Miscellaneous

- a. [31:18] **Configure MISP e-mail alerts via Postfix**
- b. [33:38] **Publish News**
- c. [34:41] **Create a Sharing Group**
- d. [38:49] **Enable and import private taxonomies**
- **e. MISP Settings Customization**
  - i. [42:14] Login-page
  - ii. [44:05] Homepage
  - iii. [45:25] Receive notifications only for specific tags
- **f. Enable default MISP feeds**

[48:03] **Troubleshooting**

- **a. MISP2MISP sync fail**
  - i. Authentication fail
  - ii. Destination not reachable
  - iii. Remote user not a sync user
- **b. Unable to pull MISP events/feeds**
  - i. Kill/Restart dead workers
  - ii. Review Scheduled tasks
  - iii. Fix NTP Server sync
- **c. Unable to send-out e-mails from MISP**

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377

MISP Training – Goals and Contents

Main issue	Sub-case	Solution
Possible reasons why a synchronization between MISP instances fail	**Authentication fail**	The organization with which you are synchronized has changed either the **Authkey or the server certificate file** (.pem). Therefore, it is necessary to request new ones and integrate them into your MISP instance.
	Destination not reachable	There might be a **network problem**, most likely related with the firewall rules / proxies.
	Remote user not a sync user	The **Authkey provided by the counterpart do not belong to a sync user**. Request the counterpart to provide an Authkey belonging to a sync user.
The MISP instance is unable to pull events and/or feeds	**Dead Workers** *Administration > Server Settings & Maintenance > Workers*	**Individually restore dead workers** (highlighted in red) 1. Remove the dead worker by clicking the trash can located on the right side of the webpage; 2. Start a new worker.
	Scheduled Tasks are not running *Administration > Scheduled Tasks*	We need to modify the “**Scheduled Time**” **and force the next run**. To achieve it, make sure to set the time (e.g., *pull_all*) in a way that it is subsequent to the system time reported at the bottom of the webpage (e.g., current time +1 min) and press on “**Update all**”.
	Misalignment between the MISP clock and the system clock	We might be the need to **synchronize a Linux System Clock with NTP Server** by using the following commands: 1. Install Timesync Service *apt-get install systemd-timesyncd* 2. Verify the service is running: *sudo systemctl status systemd-timesyncd* 3. Enable the Clock Synchronization: *sudo timedatectl set-ntp true* 4. Verify the status of the NTP sync: *timedatectl* 5. Synchronize Hardware clock: *sudo timedatectl set-local-rtc 1* If the previous steps do not work, try the following commands. If these also fail, it would be advisable to perform an internet search: 1. List all valid timezones: *timedatectl list-timezones* 2. Jot down the desired timezone 3. Set the desired timezone (e.g., UTC): *sudo timedatectl set-timezone UTC* 4. Verify Changes: *timedatectl*
Unable to send out e-mails from MISP	**Postfix configuration**	Need to configure Postfix. See video «Configure MISP e-mail alerts via Postfix» [31:18].
	MISP server settings *Administration > Server Settings & Maintenance > MISP*	To enable the MISP platform to send e-mails, we need to set the following flag to false. *MISP.disable_emailing = false*
	MISP user settings *Administration > List Users*	1. Select the target user and press on the Edit button; 2. Flag the option «Event published notification»; 3. Confirm with the current password and click on the «Edit user» button.

MISP Troubleshooting

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377

MISP Training Course

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 101021377.

D4.10 - MISP Training Course

Enhancing Digital Security, Privacy and TRUST in softWARE

ABI Lab / CERTFin

Gabriele Gamberi (gabriele.gamberi@certfin.it)

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 101021377