# MISP and threat intelligence

MISP Project - https://www.**misp-project.org**

Koen Van Impe - https://www.cudeso.be
koen.vanimpe@cudeso.be
@cudeso

June 2021

TLP:White

# What is threat intelligence?

## Threat Intelligence (TI)

Gartner

- evidence-based **knowledge**, including context, mechanisms, indicators, implications and actionable advice.
- about an existing or emerging **menace** or hazard to IT or information assets.
- It can be used to **inform decisions** regarding the subject's **response** to that menace or hazard.

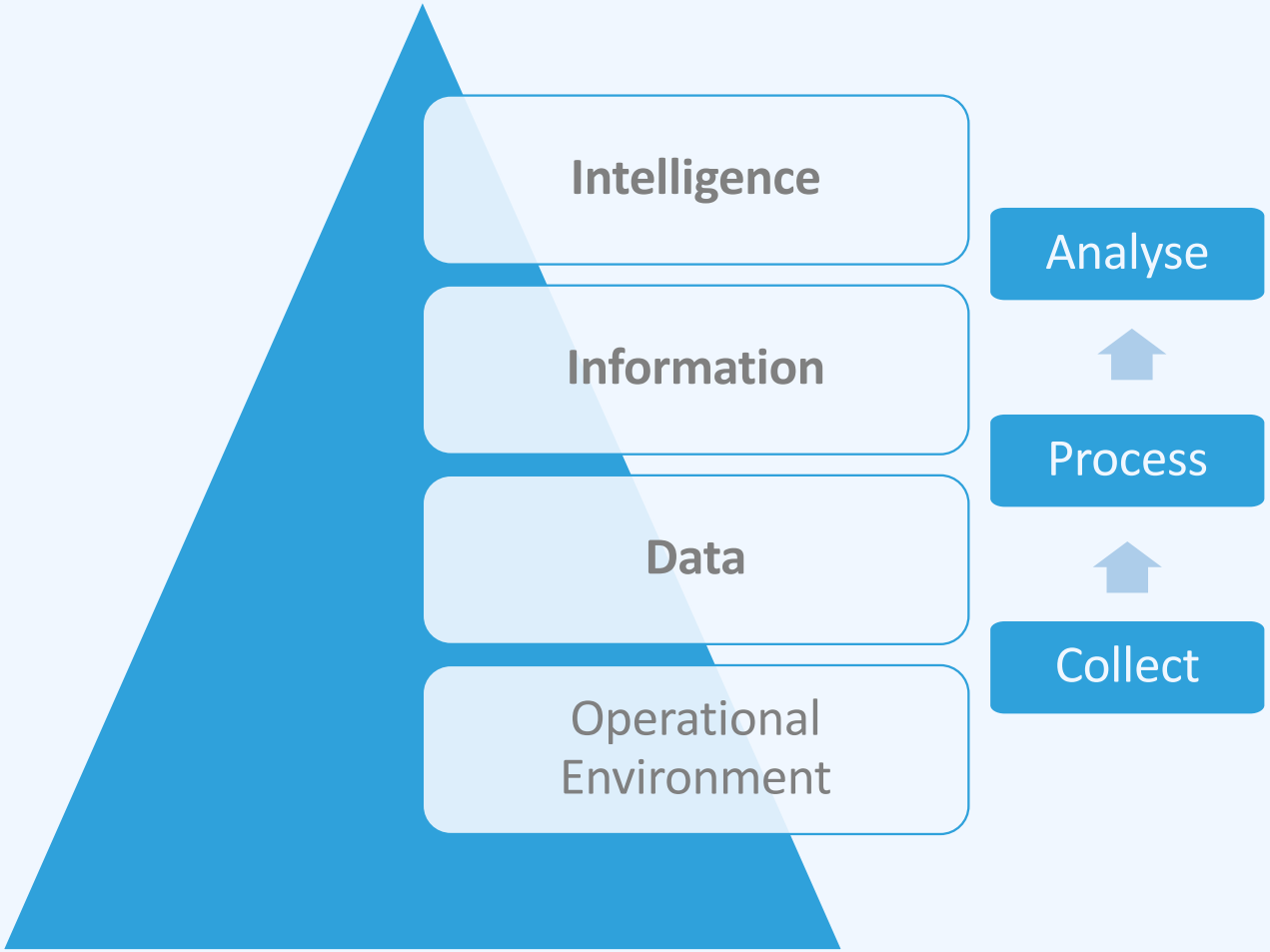
# What is threat intelligence?

## Threat Intelligence (TI)

Gartner

- evidence-based **knowledge**, including context, mechanisms, indicators, implications and actionable advice.
- about an existing or emerging **menace** or hazard to IT or information assets.
- It can be used to **inform decisions** regarding the subject's **response** to that menace or hazard.
- Understand **threats targeting an organisation**.
  - Attackers motives and behaviours.
  - Faster and better informed decisions.
  - To prepare, protect, detect and respond to these threats.

# Intelligence is more than Information. Or data.



# Threat intelligence use cases

*"What", "Where" and "When"*

Atomic indicators
**Security controls**
Defend organisation

Threat data feeds

**Tactical**

*"How"*

TTPs, capabiliities and infrastructure
**Prioritize operations**
Address blind spots in detection

Threat feeds with context
Operational threat reports

**Operational**

*"Why" and "Who"*

High level risks and trends
**Business decision making**

Threat landscapes

**Strategic**

# Threat intelligence use cases

*"What", "Where" and "When"*

Atomic indicators
**Security controls**
Defend organisation

Threat data feeds

## Tactical

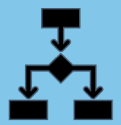
SOC analyst
Firewall
Proxy
SIEM

*"How"*

TTPs, capabiliities and infrastructure
**Prioritize operations**
Address blind spots in detection

Threat feeds with context
Operational threat reports

## Operational



SOC analyst
Incident response
Vulnerability mgmnt
Threat monitoring

*"Why" and "Who"*

High level risks and trends
**Business decision making**

Threat landscapes

## Strategic

CISO
CTO
Board

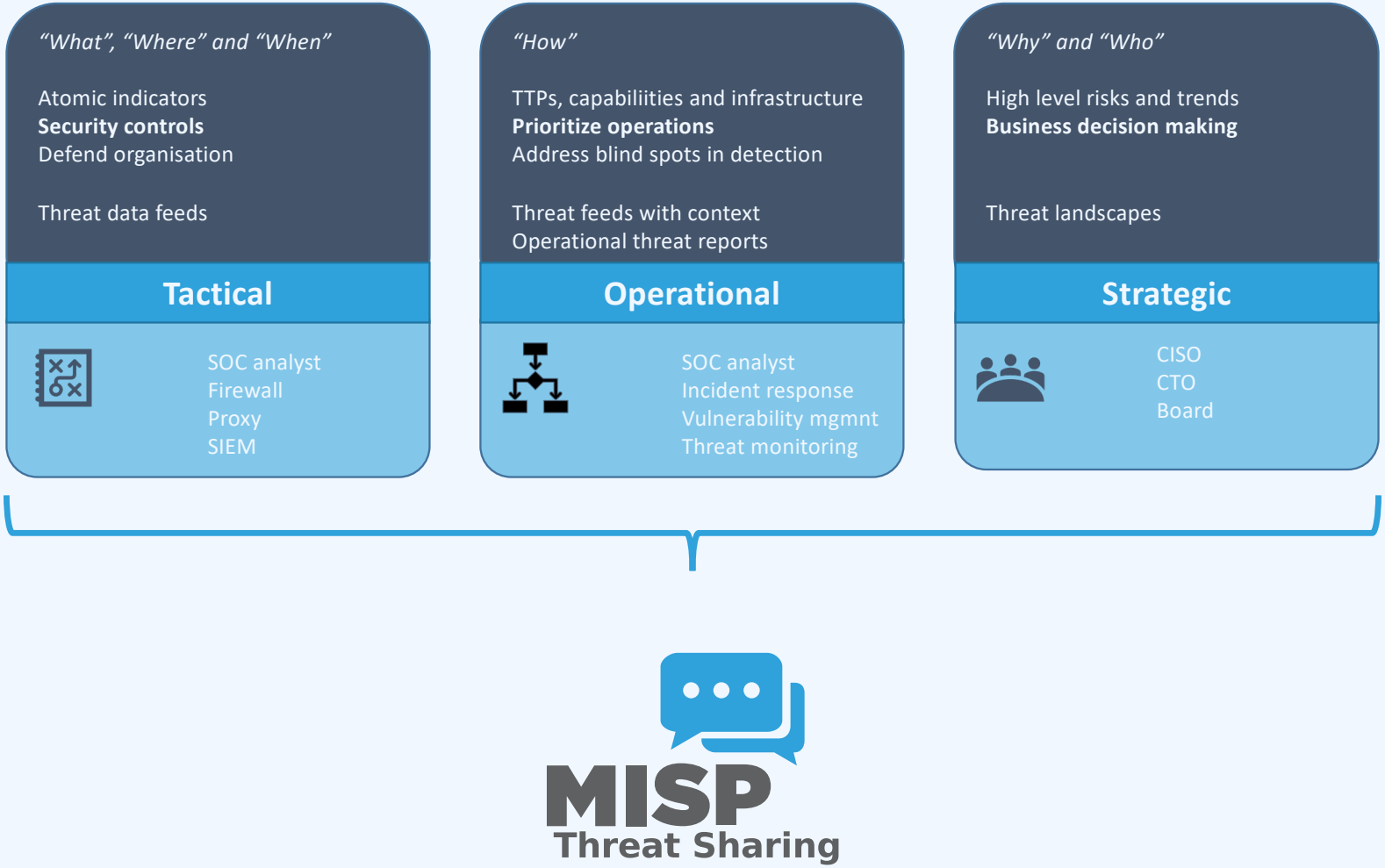
Capability

# Threat intelligence use cases

| *"What", "Where" and "When"* | *"How"* | *"Why" and "Who"* |
|---|---|---|
| Atomic indicators<br>**Security controls**<br>Defend organisation<br><br>Threat data feeds | TTPs, capabiliities and infrastructure<br>**Prioritize operations**<br>Address blind spots in detection<br><br>Threat feeds with context<br>Operational threat reports | High level risks and trends<br>**Business decision making**<br><br>Threat landscapes |
| **Tactical** | **Operational** | **Strategic** |
| IP-address: **1.2.3.4**<br>File hash: **abcd1234**<br>File name: **malware.exe** | **malware.exe** has file hash **abcd1234** and exfiltrates data to **1.2.3.4** beween **1-Jan-21** and **2-Jan-21** | Threat group **ZXY** attacks **energy facilities** in **Europe** with objective to steal company secrets |

Capability

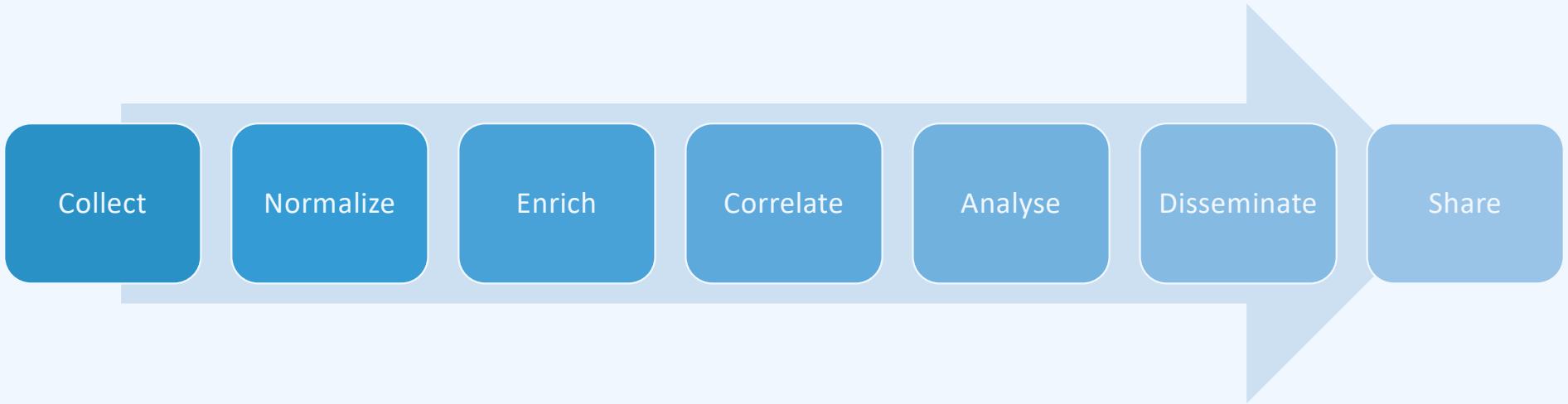
# Threat intelligence use cases




MISP
Threat Sharing

# What is MISP?

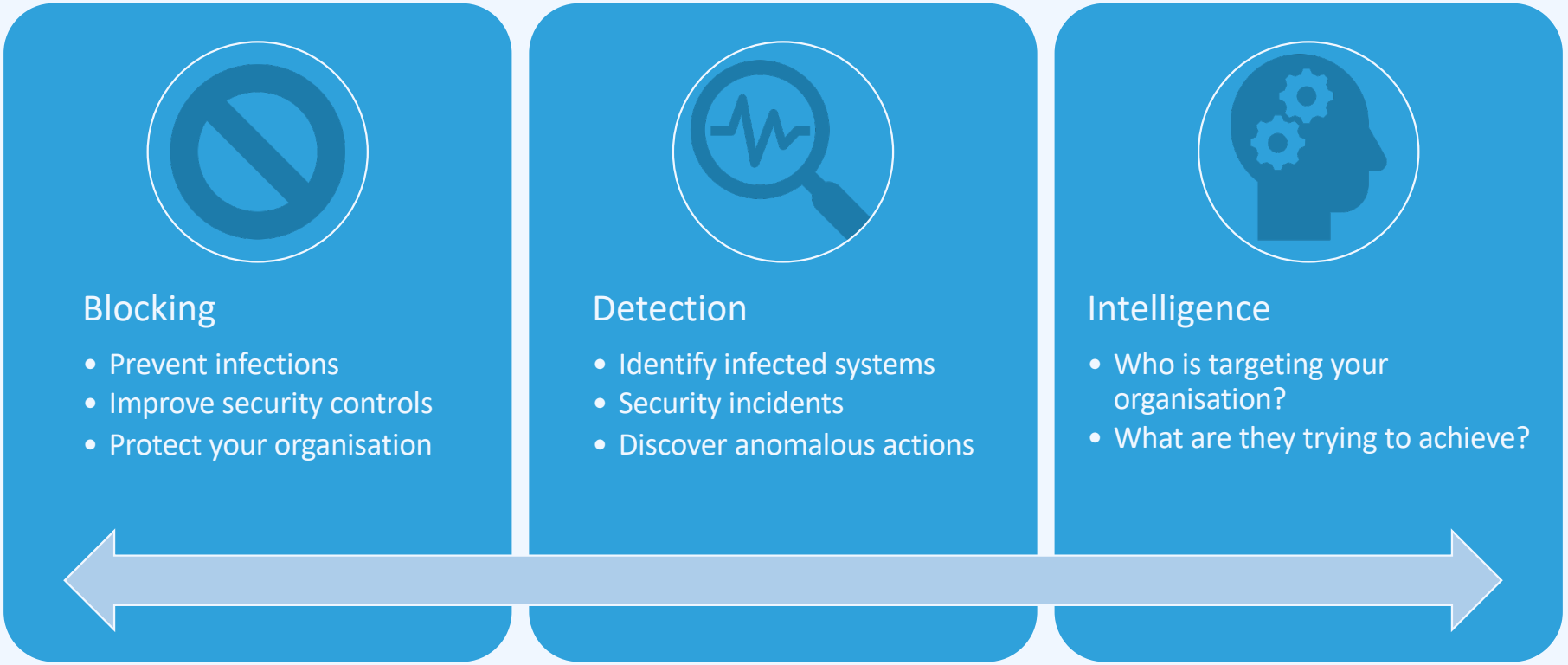
## MISP is a **Threat Information Sharing Platform**




- Free and Open Source and exists >10 years
- CIRCL leads development
- Used by >6000 organisations worldwide
- Security teams, national and government CSIRTs, commercial providers

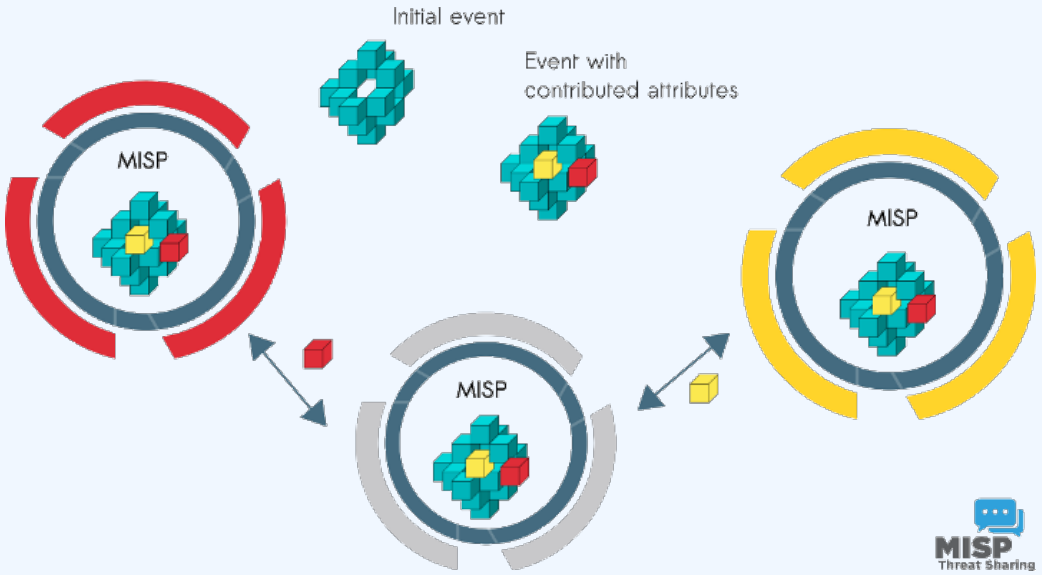
Co-financed by the European Union
Connecting Europe Facility

# Diferent users. Different objectives.



# Everyone can receive data. Everyone can contribute to data.

- Core functionality is sharing
- Everyone can be a **consumer** and/ or a contributor/**producer**
- Quick benefit without the obligation to contribute
- Low barrier to get acquainted to the system



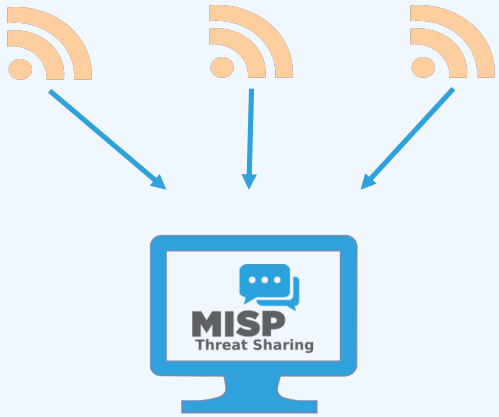
# How does it work?

# How does it work?

- Setup MISP server
  - Your environment

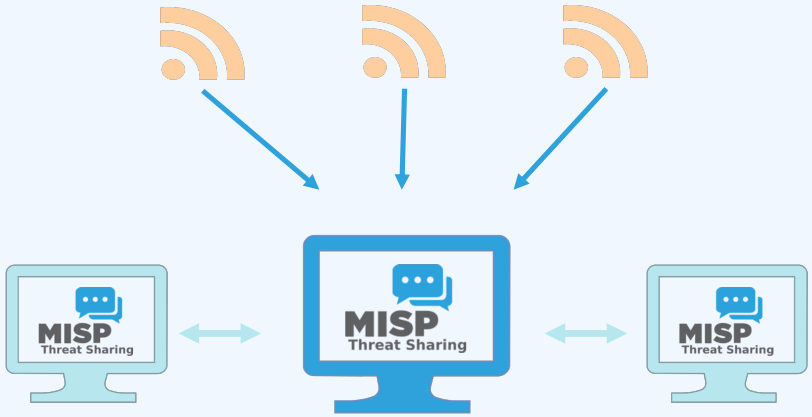
## How does it work?

- Setup MISP server
  - Your environment
- Connect to threat data feeds
  - Free and commercial feeds
  - IP addresses, file hashes, domains, TTPs



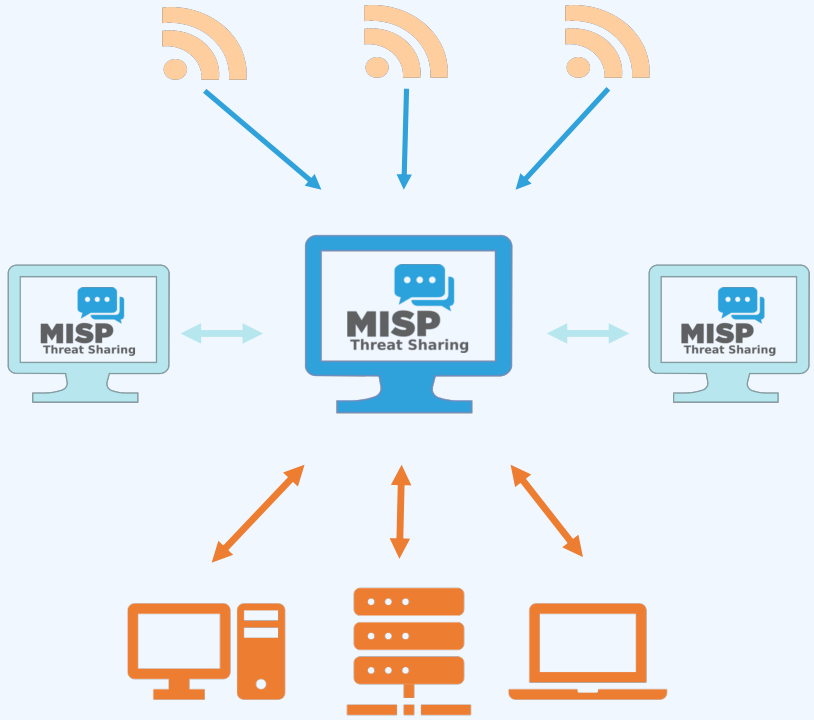
# How does it work?

- Setup MISP server
  - Your environment
- Connect to threat data feeds
  - Free and commercial feeds
  - IP addresses, file hashes, domains, TTPs
- Connect to trusted providers
  - Government and sector/industry MISP



# How does it work?

- Setup MISP server
  - Your environment
- Connect to threat data feeds
  - Free and commercial feeds
  - IP addresses, file hashes, domains, TTPs
- Connect to trusted providers
  - Government and sector/industry MISP
- Query and update security controls
  - Proxy server, firewall, logs, endpoints
  - SIEM, IDS



# Typical process



**Analysis**

- Trusted provider
- Identifies threat for a sector / organisation

**Threat event**

- Detection package
- Indicators of compromise
- Activities and behaviour

**Victim**

- Receives MISP event
- Verification and approval

**Infrastructure**

- Query for activity
- Block activity

Share back and report back

## Use cases for received threat events

Block IP address on firewall

Block malicious URL on proxy

Query logs for activity

Scan endpoints with custom rules

IDS signatures

SIEM alerts

# What do you need?

# What do you need?

- **Hardware** and software
  - One server with Linux (preferably Ubuntu Linux)
  - Average storage and memory (250GB/64GB)
  - MISP uses a web server (Apache) and database server (MariaDB)


- **Installation**
  - MISP is usually installed from source via Github

- **Infrastructure integration**
  - Customizations for integration with security controls
  - Base capabilities are included
  - Needs to be tuned to your environment

# MISP details

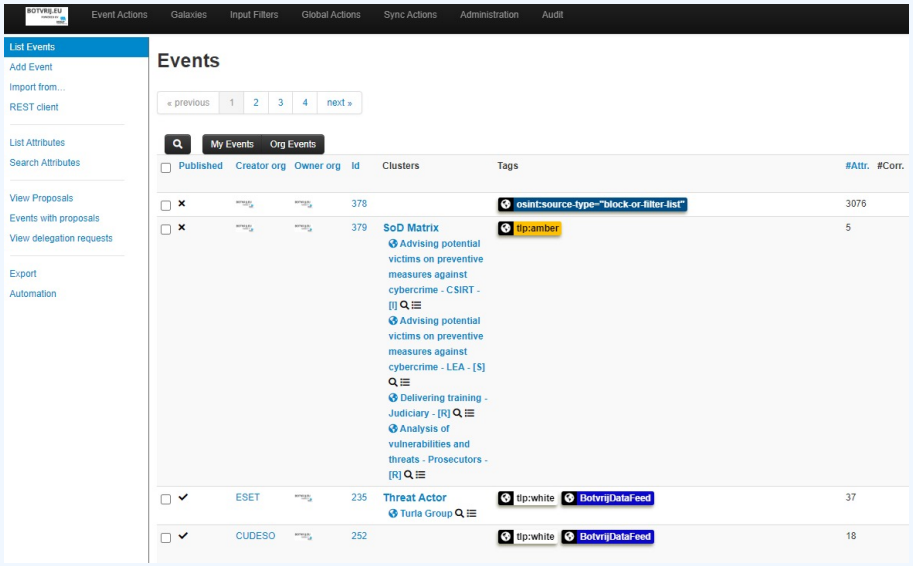
# Access to MISP

- **Web** interface
  - Multiple users and groups
  - Role based access

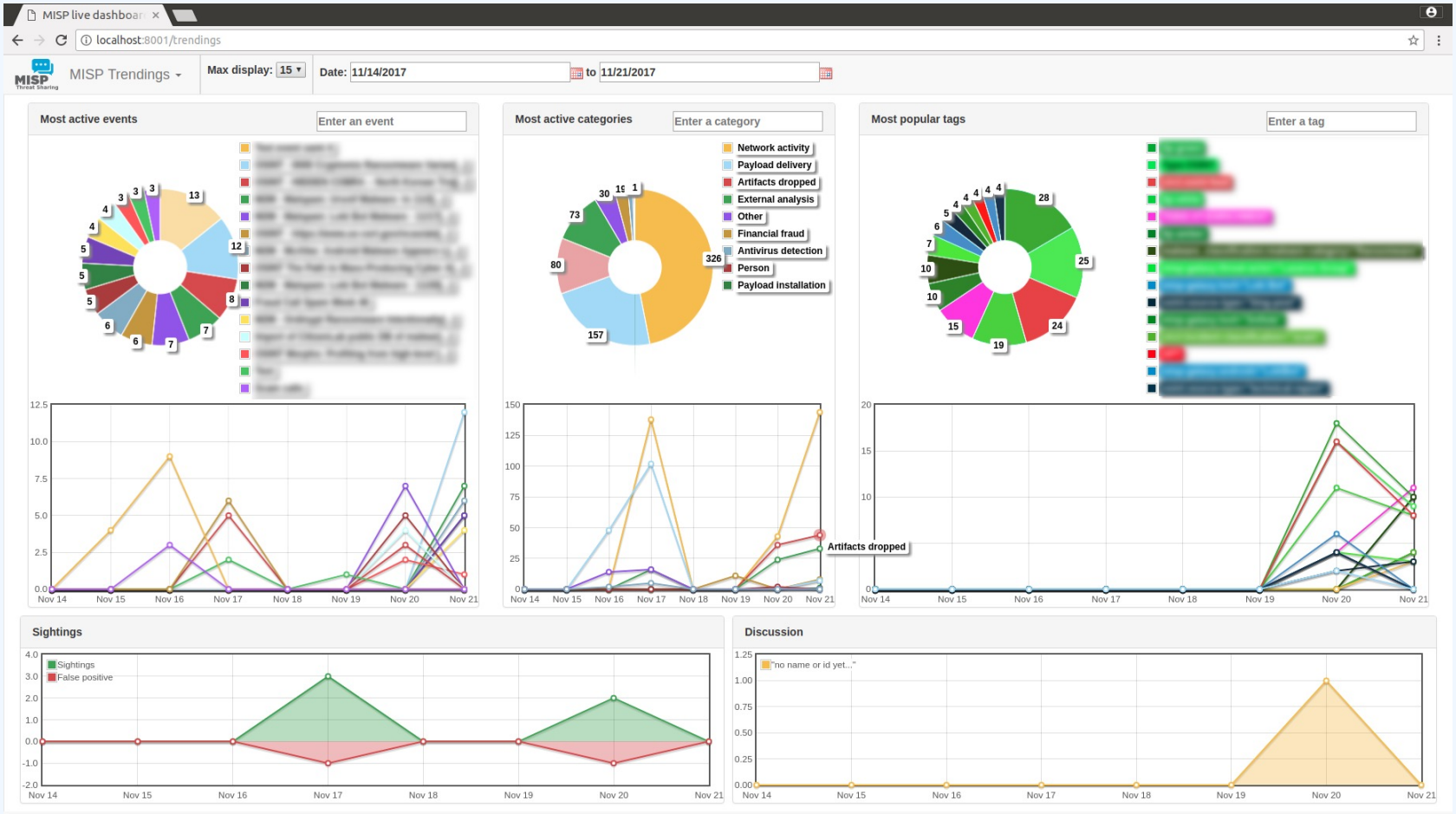

- **API** access for automation
  - Integration with other tools
  - Synchronization with security controls
  - Python library

# MISP user interface

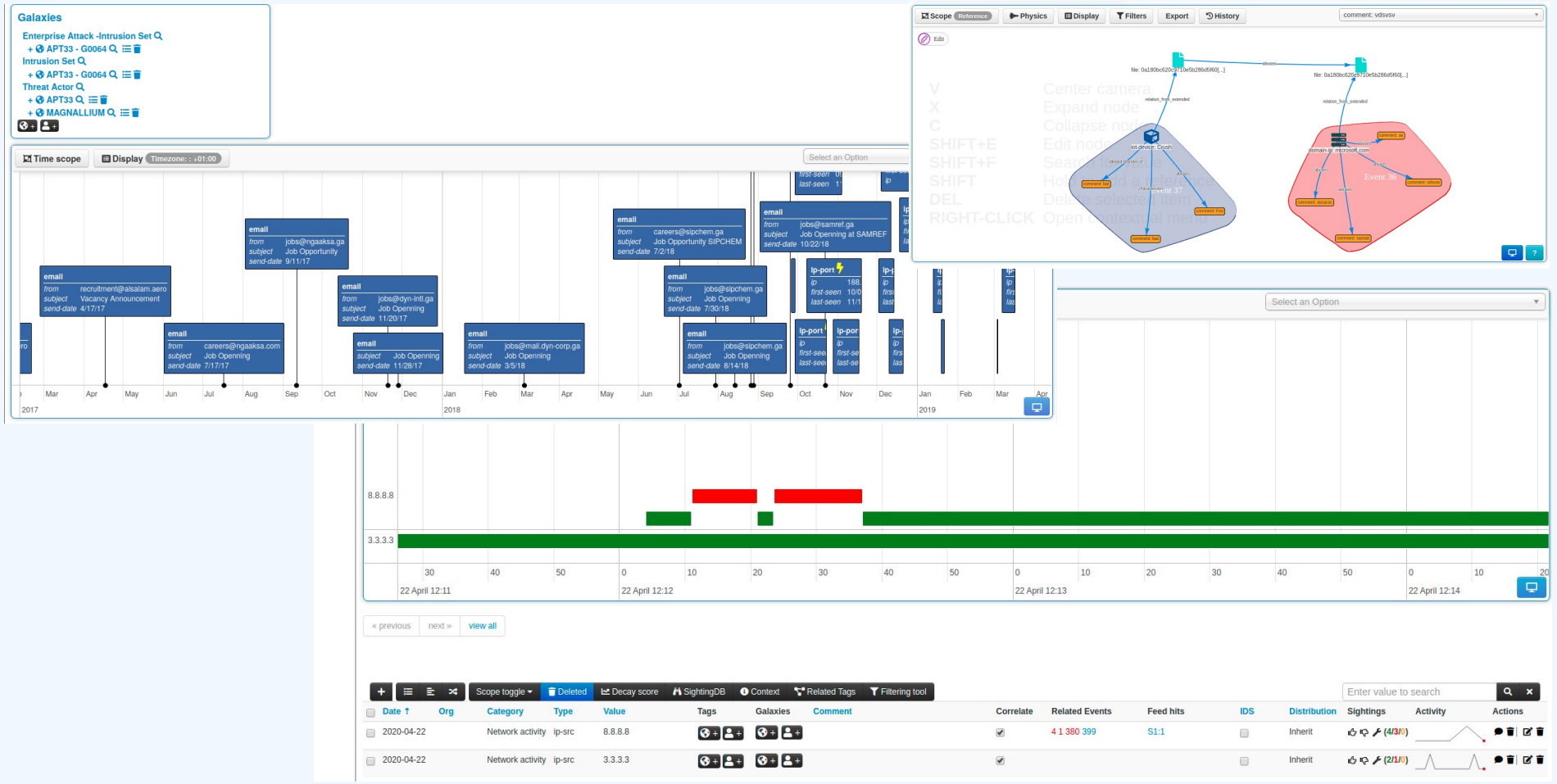
- Events are containers of **contextually** linked information
  - From an incident, a security report or a threat actor analysis
- Contains attributes with **indicators**
- Tools, techniques and procedures
- Your desired (or expected) actions
  - Block, detect



# MISP dashboard with trends and statistics

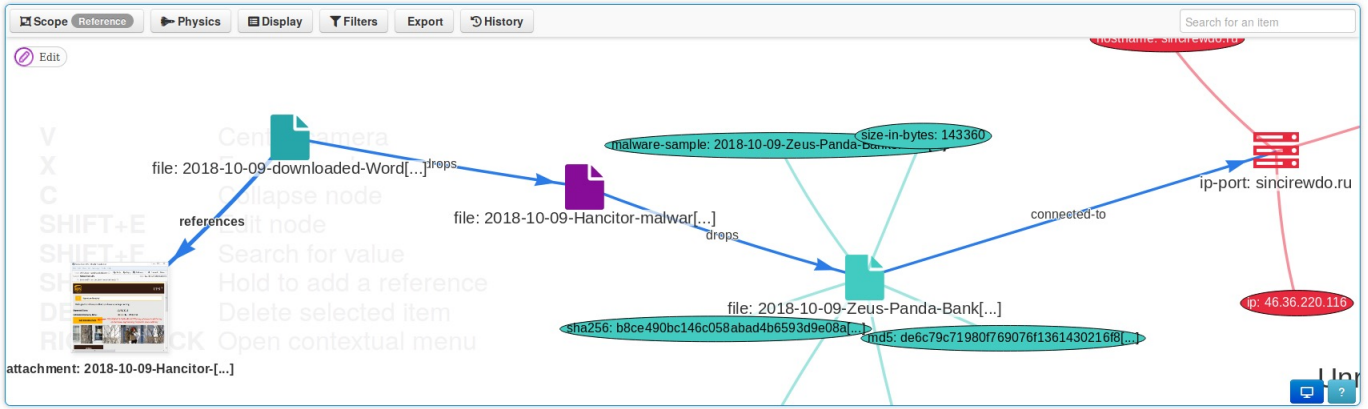


# Timeline and clusters of activities

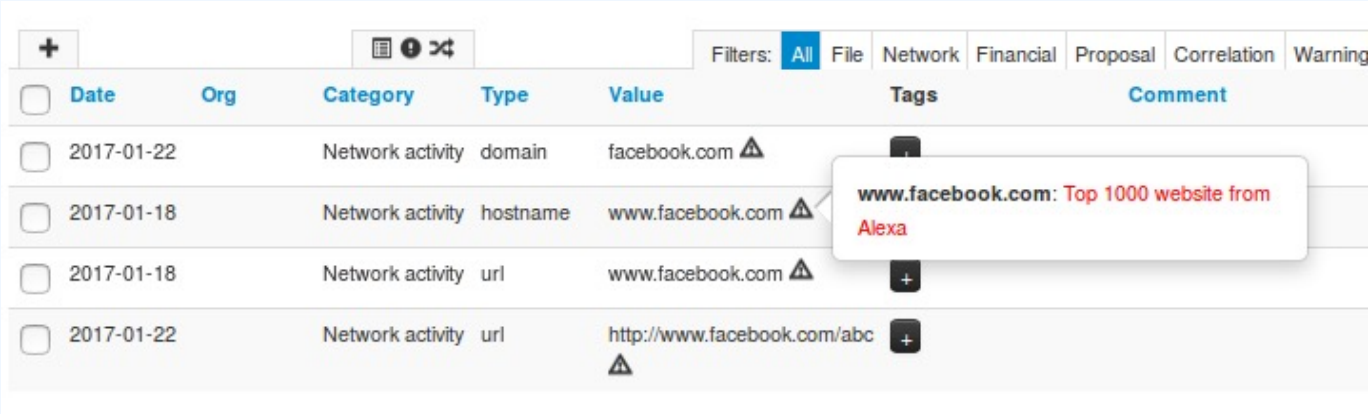


# Information quality management

- Contextualization

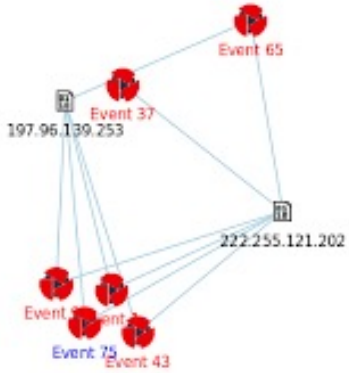


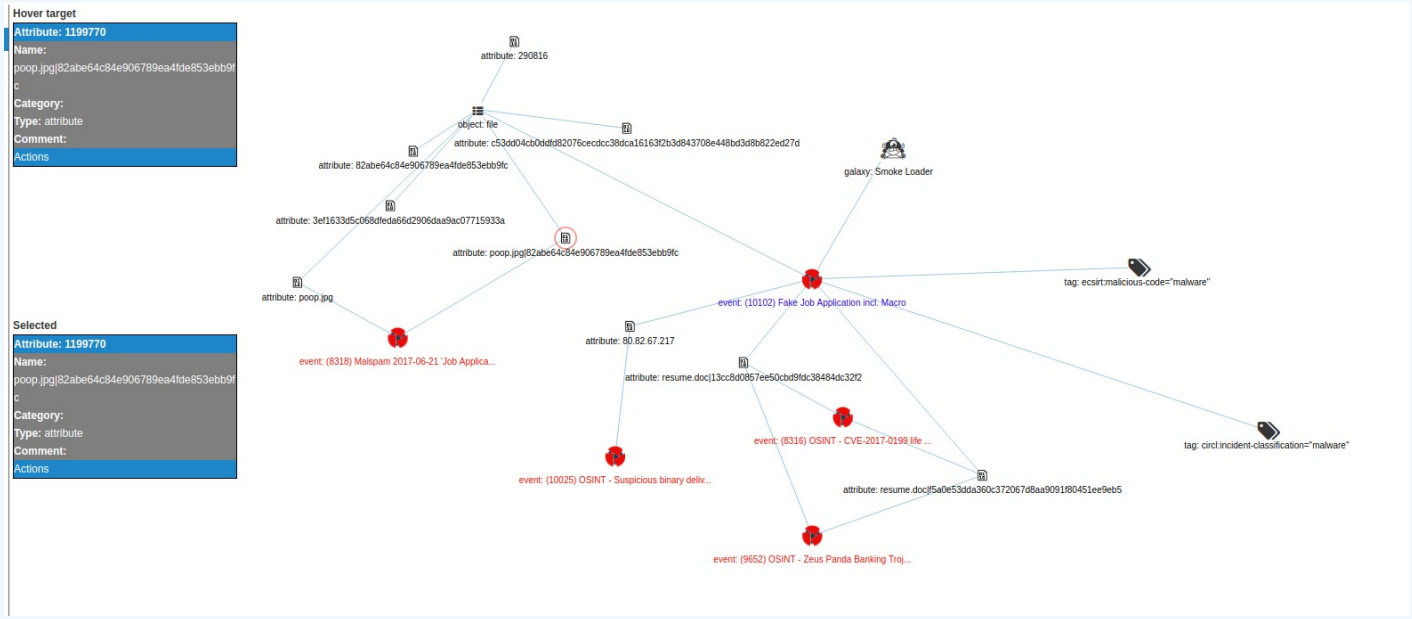

- False positive management




# Correlating data

- Correlate on indicators and context



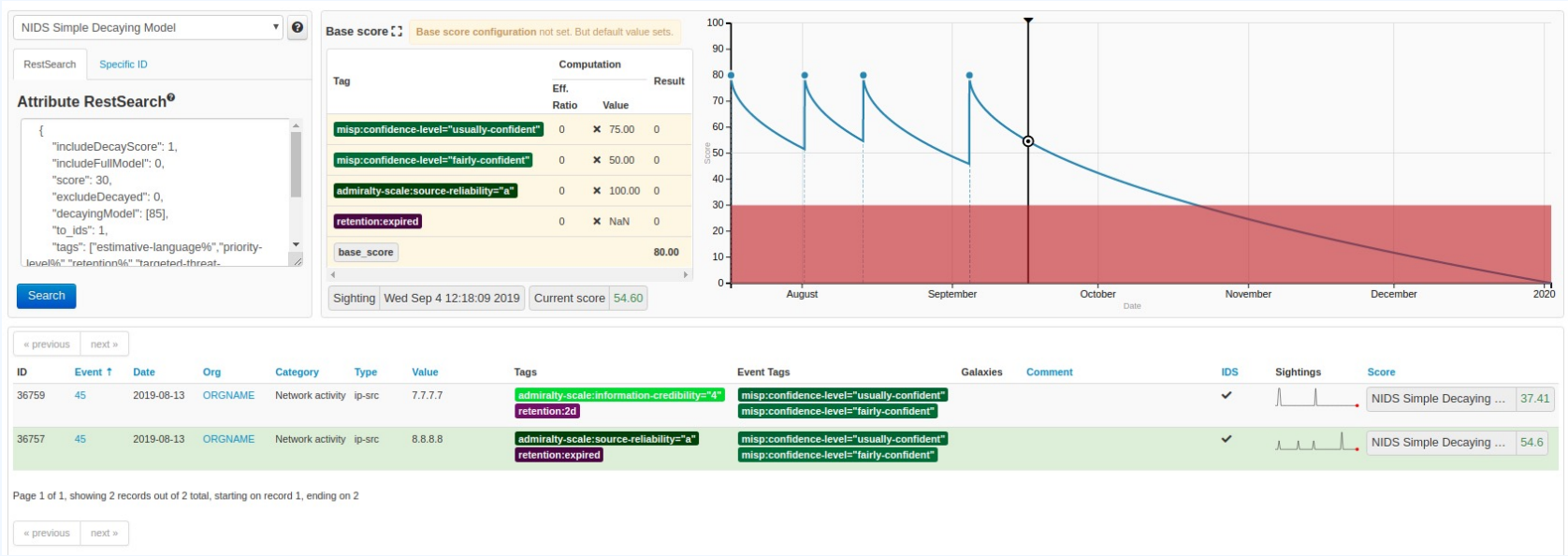



# Continuous feedback loop

- Feedback on observed indicators
- Confirm presence of activity


# Relevant indicators

- Remove older (less- / non relevant) indicators



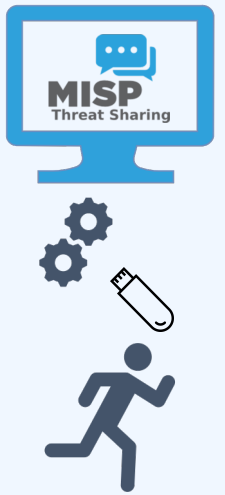
# MISP in industrial environment

# MISP in industrial / ICS environment

- “Normal” MISP
- Export threat events

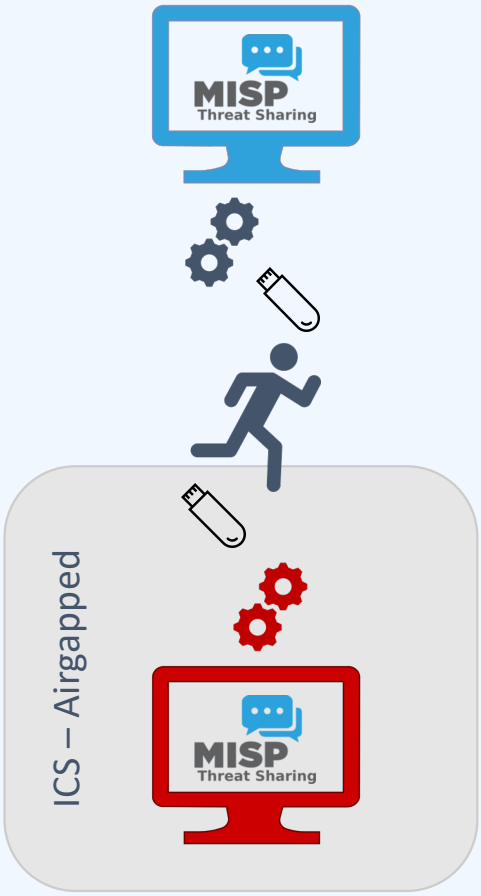
# MISP in industrial / ICS environment

- “Normal” MISP
- Export threat events
- Transfer via USB
  - Scan via kiosk



# MISP in industrial / ICS environment

- “Normal” MISP
- Export threat events
- Transfer via USB
  - Scan via kiosk
- Import threat events



# Questions?