

# Blue Team Tools: MISP

---



**Phil Chapman**

SENIOR INSTRUCTOR

@cyberphil4 [www.cyberphil.co.uk](http://www.cyberphil.co.uk)







Creator: Christophe Vandeplas

---

A threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information across many threat actors.





**MISP is used by multiple organizations to store, share and collaborate on cyber security IoCs and malware analysis.**

**Downloads from:**

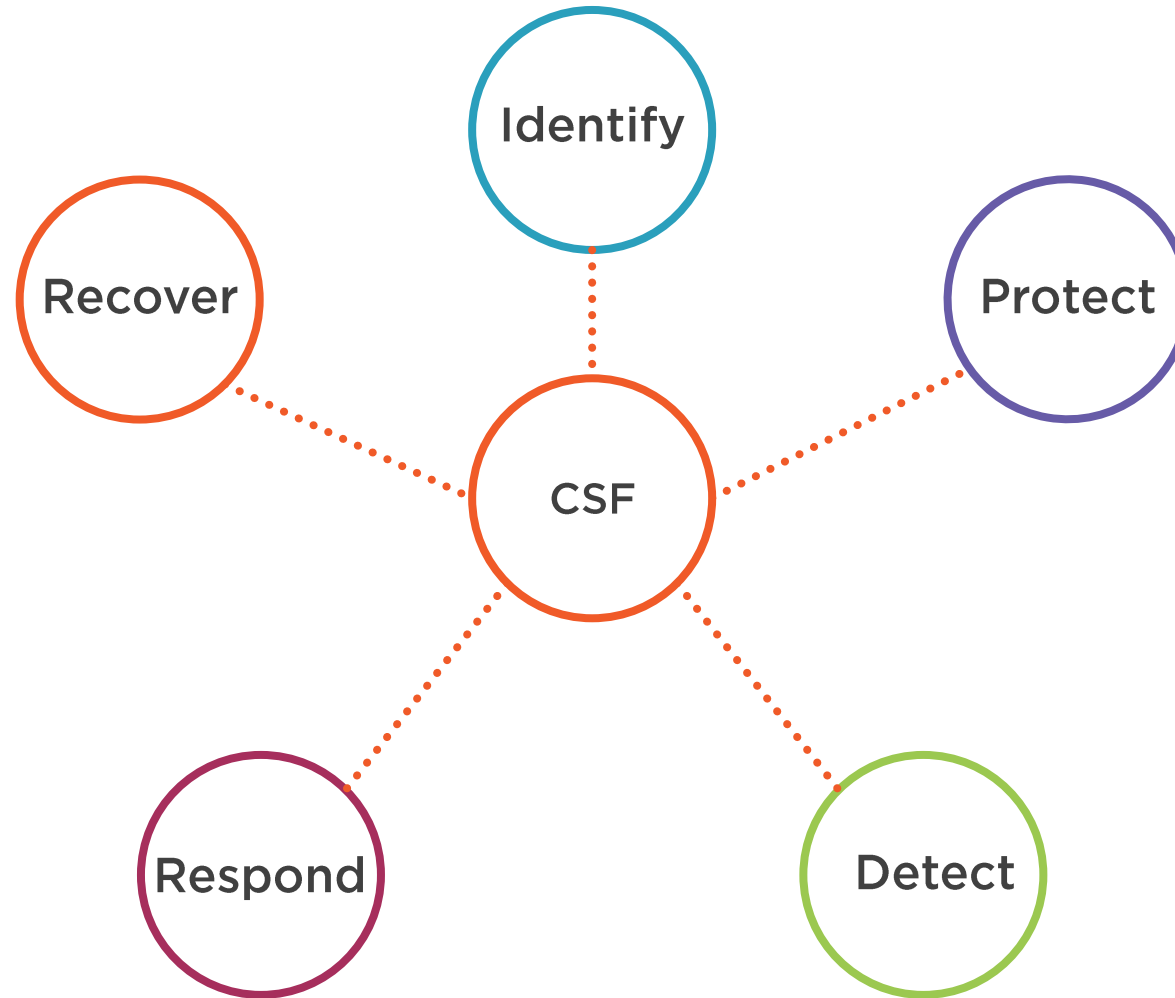
- [www.misp-project.org/download](http://www.misp-project.org/download)

**MISP is packed with multiple features**

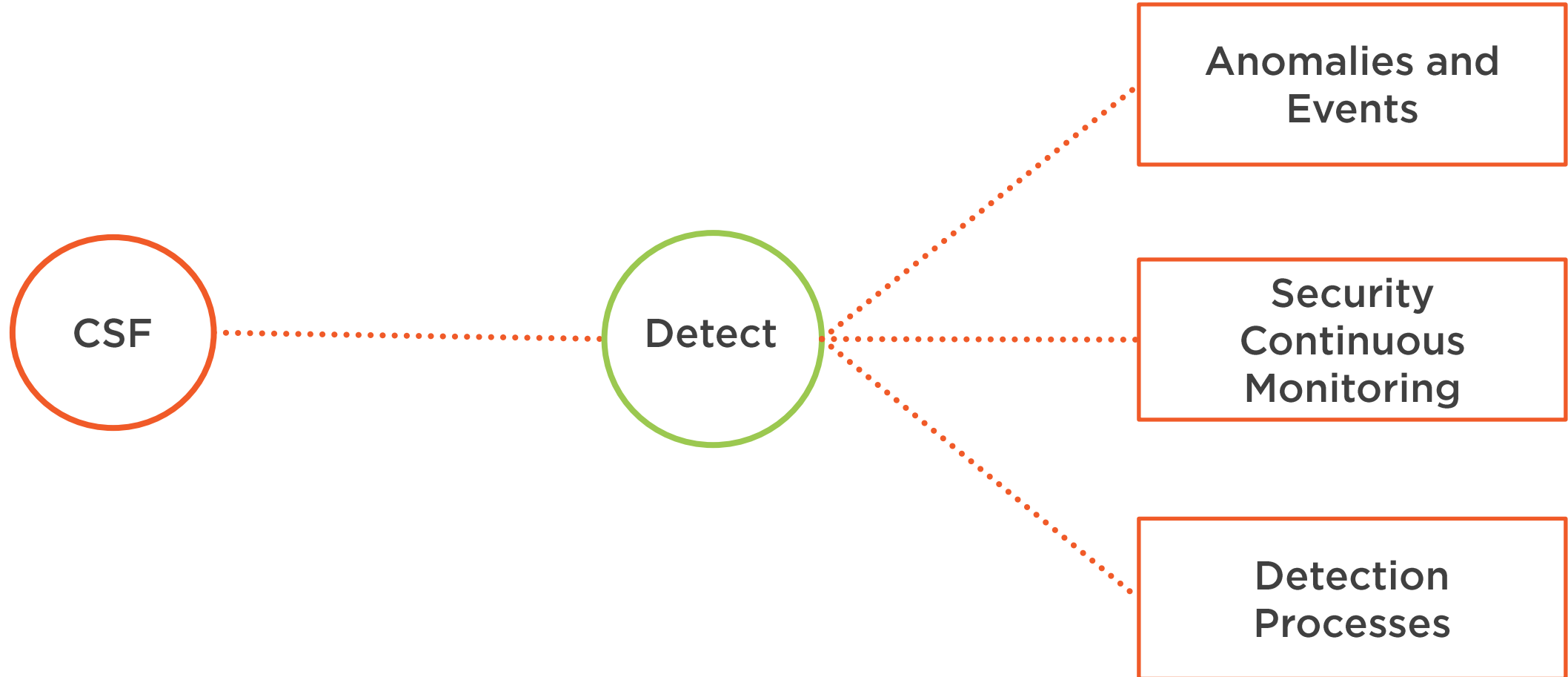
- Sharing with humans
- Sharing with machines



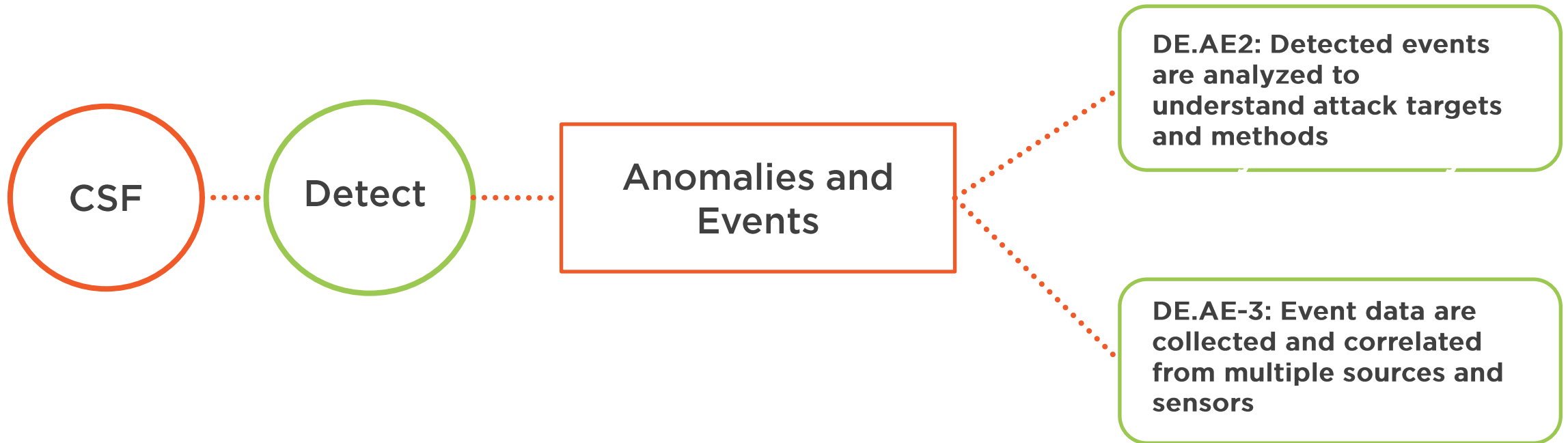
# NIST Cybersecurity Framework



# NIST Cybersecurity Framework



# NIST Cybersecurity Framework



# MITRE ATT&CK

## Data Analysis Type

Network Analysis

OS Analysis

Application Analysis

File Analysis

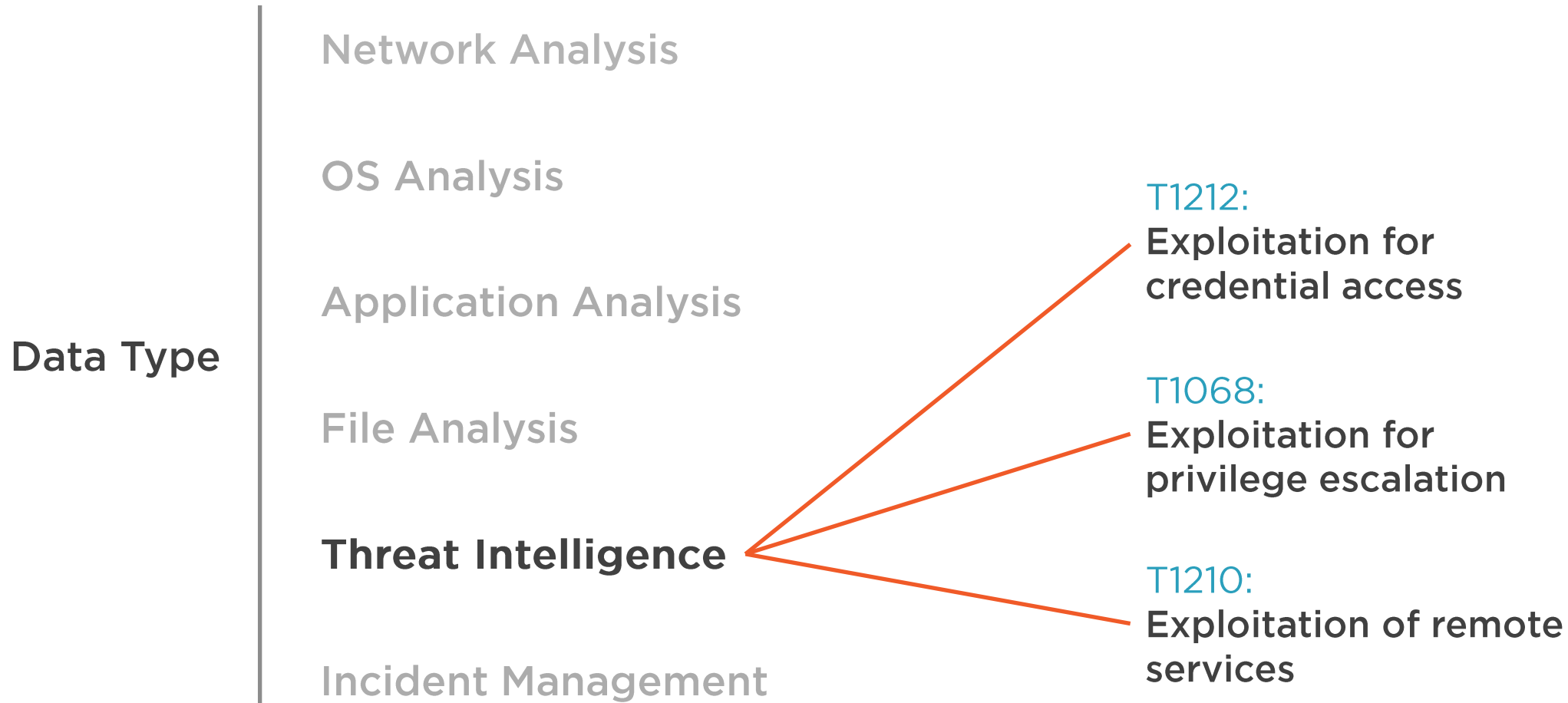
Threat Intelligence

Incident Management





# MITRE ATT&CK



# Demo



## MISP

- Overview
- Installation
- Initial Configuration



# More Information

## Capabilities

### Features

MISP features and functionalities

<https://www.misp-project.org/features/>

MISP Project Book

<https://github.com/MISP/misp-book>

## Related Information

### MISP Threat Sharing

[www.misp-project.org](http://www.misp-project.org)

### Other related tools

- CISA Automated Indicator Sharing
  - ([www.cisa.gov](http://www.cisa.gov))
- Virus Total
  - ([www.virustotal.com](http://www.virustotal.com))
- MITRE ATT&CK
  - ([attack.mitre.org](http://attack.mitre.org))

