TLP:WHITE

EU ATT&CK Conference
1st of June 2021

StrangeBee

TTPs with MITRE ATT&CK in TheHive

Who am I

- **Jérôme Leonard**
- **20 years in** Cybersecurity
- **Former DFIR** and **CTI** analyst
- Co-creator of **TheHive Project**
- Cofounder & CPO **StrangeBee**

StrangeBee

The Agenda

- Quick introduction of TheHive
- Prepare TheHive with ATT&CK patterns
- Enrich Cases with Tactics, Techniques and Procedures
- What’s for next versions of TheHive ?

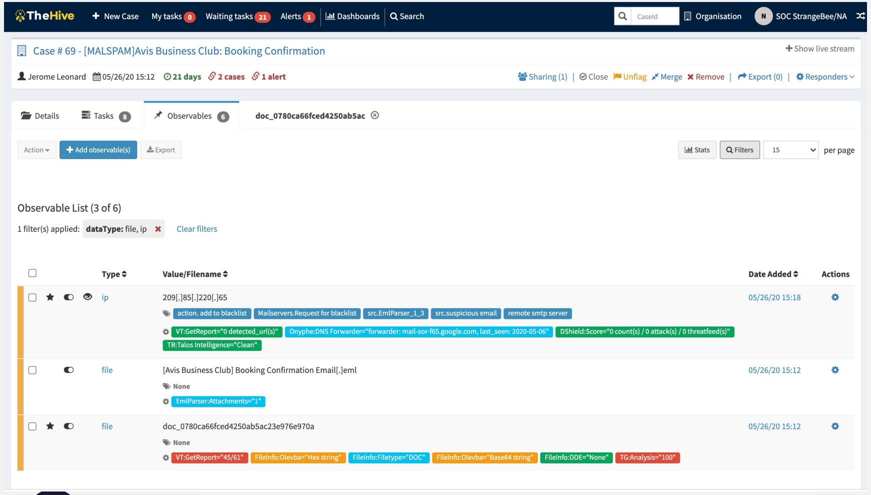
TheHive 4

Getting ready to welcome new major features

TheHive overview

TheHive

Security Incident Response Platform



Case # 69 - [MALSPAM]Avis Business Club: Booking Confirmation

Jerome Leonard 05/26/20 15:12 21 days 2 cases 1 alert

Observable List (3 of 6)

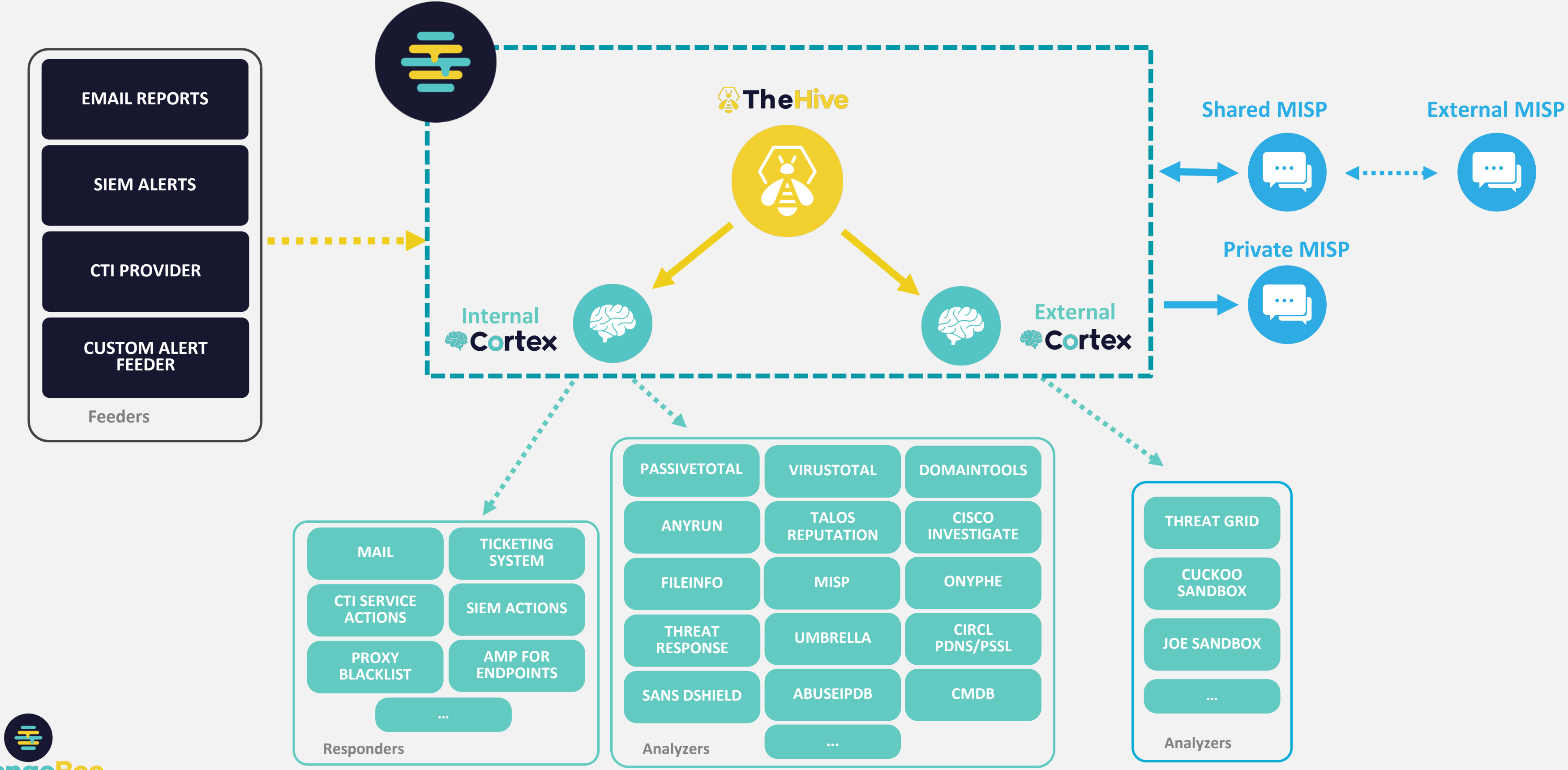
1 filter(s) applied: **dataType:** file, ip

☐	Type	Value/Filename	Date Added	Actions
☐ ★	ip	209[.]85[.]220[.]65 action. add to blacklist, Mailservers.Request for blacklist, src.EmlParser_1_3, src.suspicious email, remote smtp server VT:GetReport="0 detected_url(s)" Onyphe:DNS Forwarder="forwarder: mail-sor-f65.google.com, last_seen: 2020-05-06" DShield:Score="0 count(s) / 0 attack(s) / 0 threatfeed(s)" TR:Talos Intelligence="Clean"	05/26/20 15:18	⚙
☐	file	[Avis Business Club] Booking Confirmation Email[.]eml None EmlParser:Attachments="1"	05/26/20 15:12	⚙
☐ ★	file	doc_0780ca66fced4250ab5ac23e976e970a None VT:GetReport="45/61" FileInfo:Olevba="Hex string" FileInfo:Filetype="DOC" FileInfo:Olevba="Base64 string" FileInfo:DDE="None" TG:Analysis="100"	05/26/20 15:12	⚙

- **Organize**, structure and archive incidents including technical artifacts
- **Aggregate**, collect and triage Alert
- **Manage** Cases and Tasks
- **Enrich** IOCs and Observables
- **Implement** IR workflows and playbooks
- **Take care** of information classification levels (TLP & PAP)
- Collaborative & multi tenant platform
- Built-in integration with Cortex for Analysis and Active Responses

StrangeBee

Typical Integration



EMAIL REPORTS

SIEM ALERTS

CTI PROVIDER

CUSTOM ALERT FEEDER

Feeders

TheHive

Internal Cortex

External Cortex

Shared MISP

External MISP

Private MISP

MAIL

TICKETING SYSTEM

CTI SERVICE ACTIONS

SIEM ACTIONS

PROXY BLACKLIST

AMP FOR ENDPOINTS

…

Responders

PASSIVETOTAL

VIRUSTOTAL

DOMAINTOOLS

ANYRUN

TALOS REPUTATION

CISCO INVESTIGATE

FILEINFO

MISP

ONYPHE

THREAT RESPONSE

UMBRELLA

CIRCL PDNS/PSSL

SANS DSHIELD

ABUSEIPDB

CMDB

…

Analyzers

THREAT GRID

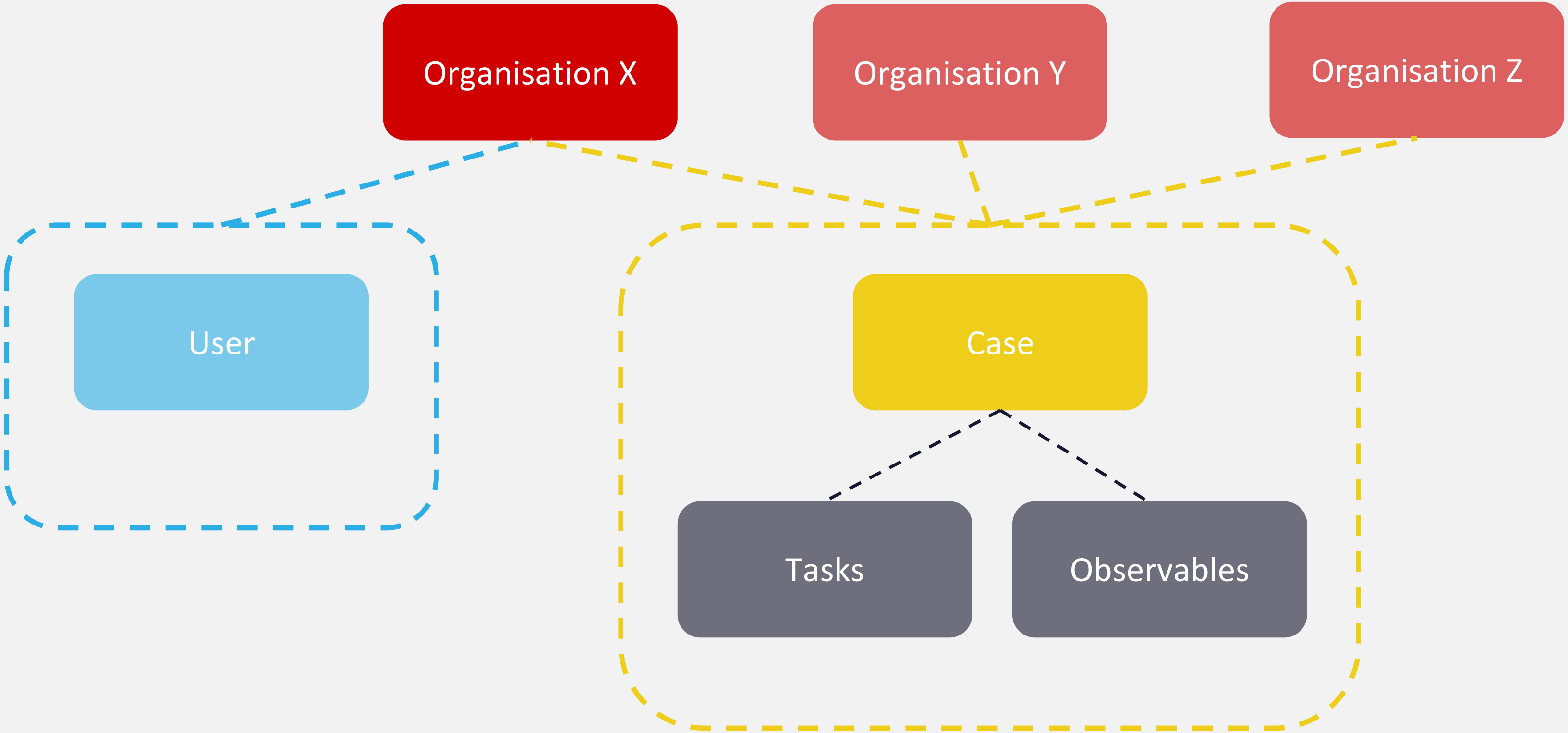
CUCKOO SANDBOX

JOE SANDBOX

…

Analyzers

Data schema



StrangeBee

TheHive 4.1

Welcome MITRE ATT&CK

TheHive 4.1 – introducing MITRE ATT&CK

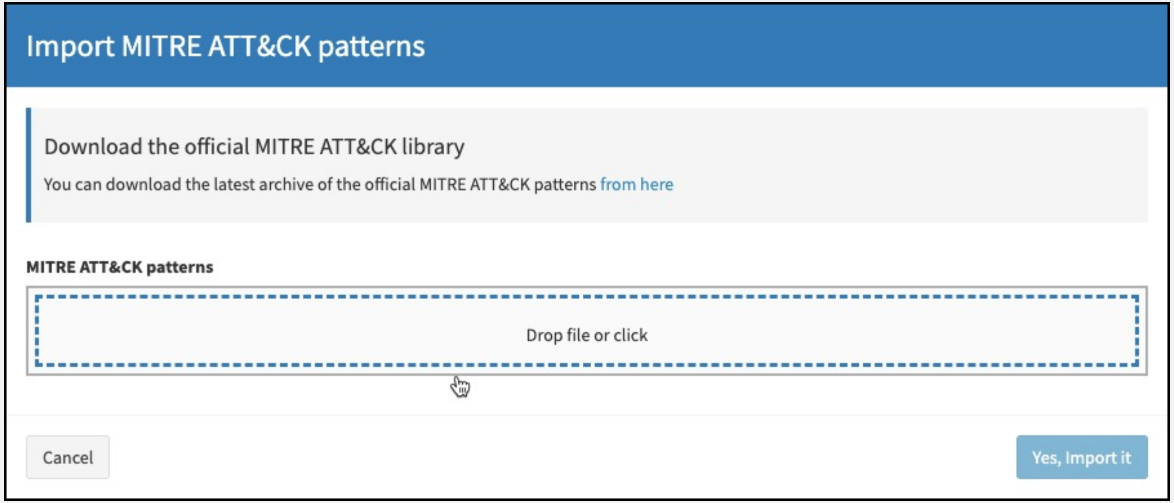
- Released in March’21
- First step in the roadmap
- Enable and setup ATT&CK patterns in TheHive
- Enrich Cases with TTPs

Using TTPs in TheHive

Setup

Setting up ATT&CK patterns

- Not installed by default
- Import latest version
- Can be updated



Import MITRE ATT&CK patterns

Download the official MITRE ATT&CK library

You can download the latest archive of the official MITRE ATT&CK patterns from here

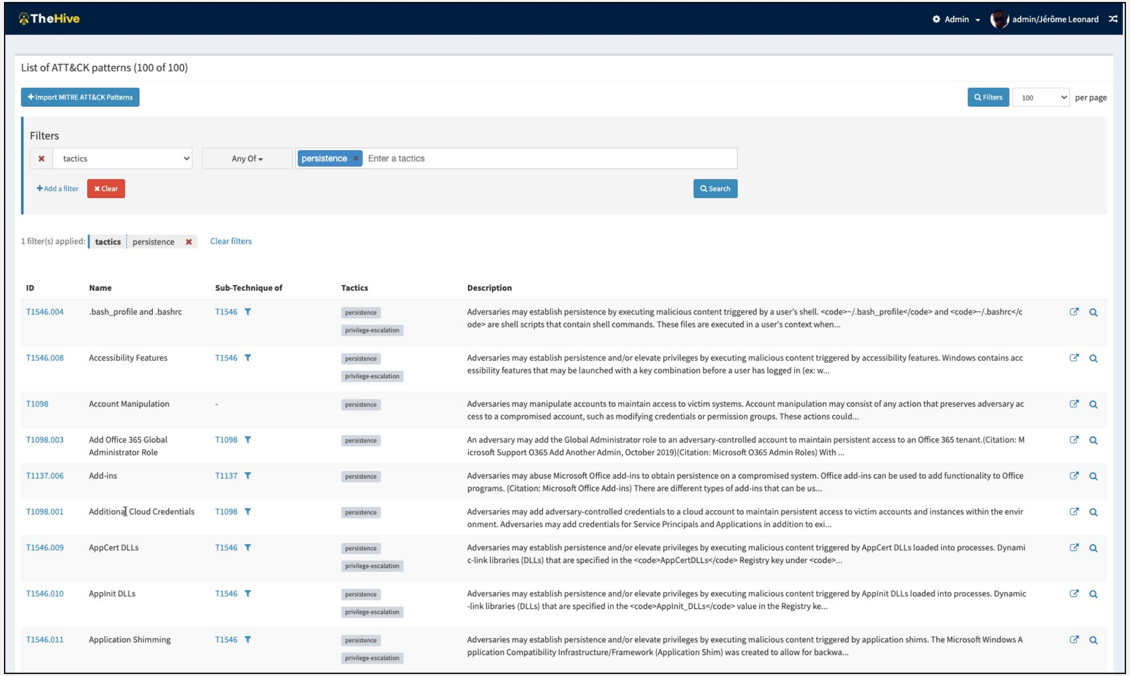
MITRE ATT&CK patterns

Setting up ATT&CK patterns

- Library added in the database (https://github.com/mitre/cti)
- Support STIX 2.0 JSON file format
- Designed for Enterprise tactics for the moment

Setup ATT&CK patterns

- List of Techniques
- Use filters like all other lists in the application



List of ATT&CK patterns (100 of 100)

100 per page

Filters

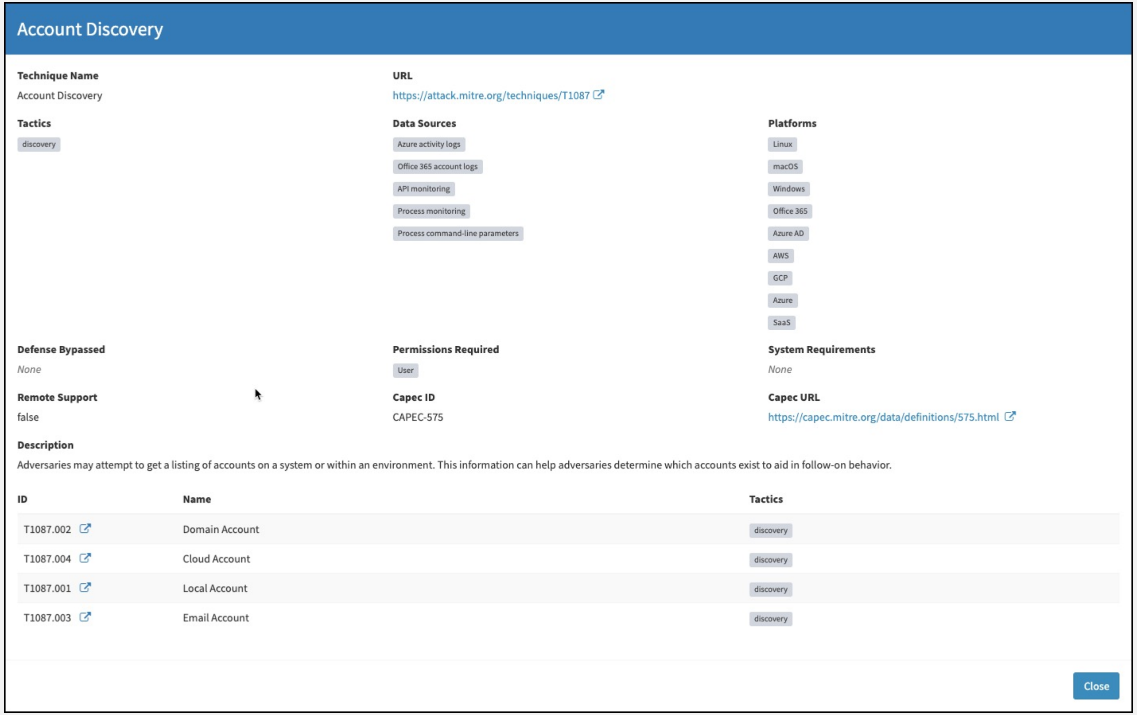
tactics — Any Of — persistence — Enter a tactics

1 filter(s) applied: tactics persistence

ID	Name	Sub-Technique of	Tactics	Description
T1546.004	.bash_profile and .bashrc	T1546	persistence privilege-escalation	Adversaries may establish persistence by executing malicious content triggered by a user's shell. <code>~/.bash_profile</code> and <code>~/.bashrc</code> are shell scripts that contain shell commands. These files are executed in a user's context when...
T1546.008	Accessibility Features	T1546	persistence privilege-escalation	Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by accessibility features. Windows contains accessibility features that may be launched with a key combination before a user has logged in (ex: w...
T1098	Account Manipulation	-	persistence	Adversaries may manipulate accounts to maintain access to victim systems. Account manipulation may consist of any action that preserves adversary access to a compromised account, such as modifying credentials or permission groups. These actions could...
T1098.003	Add Office 365 Global Administrator Role	T1098	persistence	An adversary may add the Global Administrator role to an adversary-controlled account to maintain persistent access to an Office 365 tenant.(Citation: Microsoft Support O365 Add Another Admin, October 2019)(Citation: Microsoft O365 Admin Roles) With ...
T1137.006	Add-ins	T1137	persistence	Adversaries may abuse Microsoft Office add-ins to obtain persistence on a compromised system. Office add-ins can be used to add functionality to Office programs. (Citation: Microsoft Office Add-ins) There are different types of add-ins that can be us...
T1098.001	Additional Cloud Credentials	T1098	persistence	Adversaries may add adversary-controlled credentials to a cloud account to maintain persistent access to victim accounts and instances within the environment. Adversaries may add credentials for Service Principals and Applications in addition to exi...
T1546.009	AppCert DLLs	T1546	persistence privilege-escalation	Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppCert DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the <code>AppCertDLLs</code> Registry key under <code>...
T1546.010	AppInit DLLs	T1546	persistence privilege-escalation	Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by AppInit DLLs loaded into processes. Dynamic-link libraries (DLLs) that are specified in the <code>AppInit_DLLs</code> value in the Registry ke...
T1546.011	Application Shimming	T1546	persistence privilege-escalation	Adversaries may establish persistence and/or elevate privileges by executing malicious content triggered by application shims. The Microsoft Windows Application Compatibility Infrastructure/Framework (Application Shim) was created to allow for backwa...

Setup ATT&CK patterns

- Access Techniques details
- Open related Techniques description pages on MITRE website



Account Discovery

Technique Name
Account Discovery

URL
https://attack.mitre.org/techniques/T1087

Tactics
discovery

Data Sources
Azure activity logs
Office 365 account logs
API monitoring
Process monitoring
Process command-line parameters

Platforms
Linux
macOS
Windows
Office 365
Azure AD
AWS
GCP
Azure
SaaS

Defense Bypassed
None

Permissions Required
User

System Requirements
None

Remote Support
false

Capec ID
CAPEC-575

Capec URL
https://capec.mitre.org/data/definitions/575.html

Description
Adversaries may attempt to get a listing of accounts on a system or within an environment. This information can help adversaries determine which accounts exist to aid in follow-on behavior.

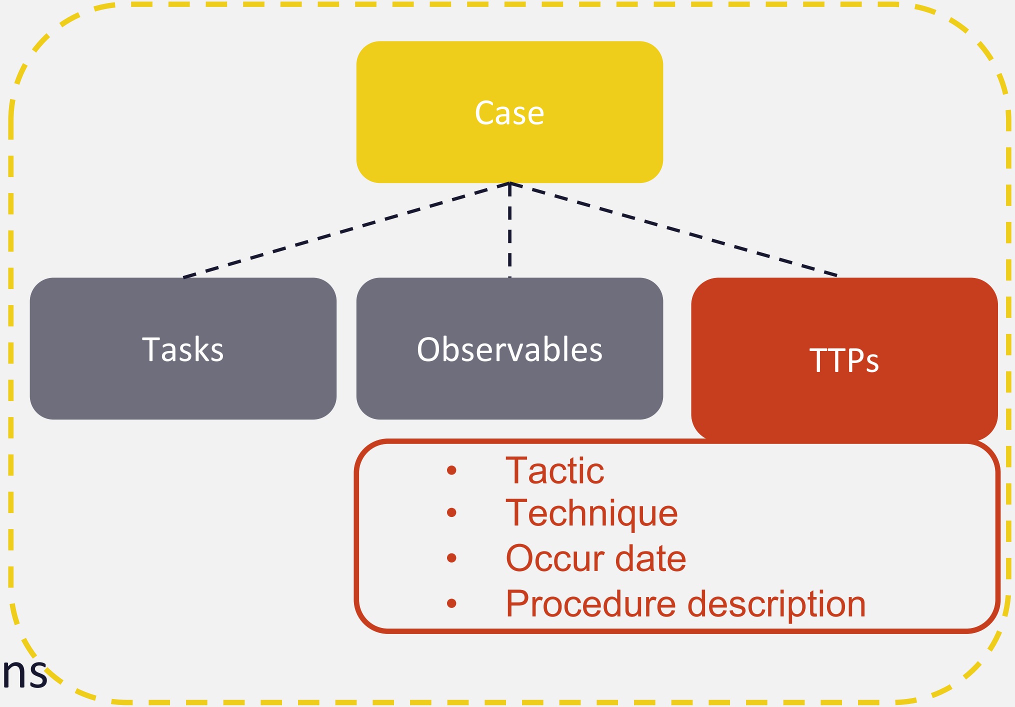
ID	Name	Tactics
T1087.002	Domain Account	discovery
T1087.004	Cloud Account	discovery
T1087.001	Local Account	discovery
T1087.003	Email Account	discovery

Using TTPs in TheHive

Enrich your Cases

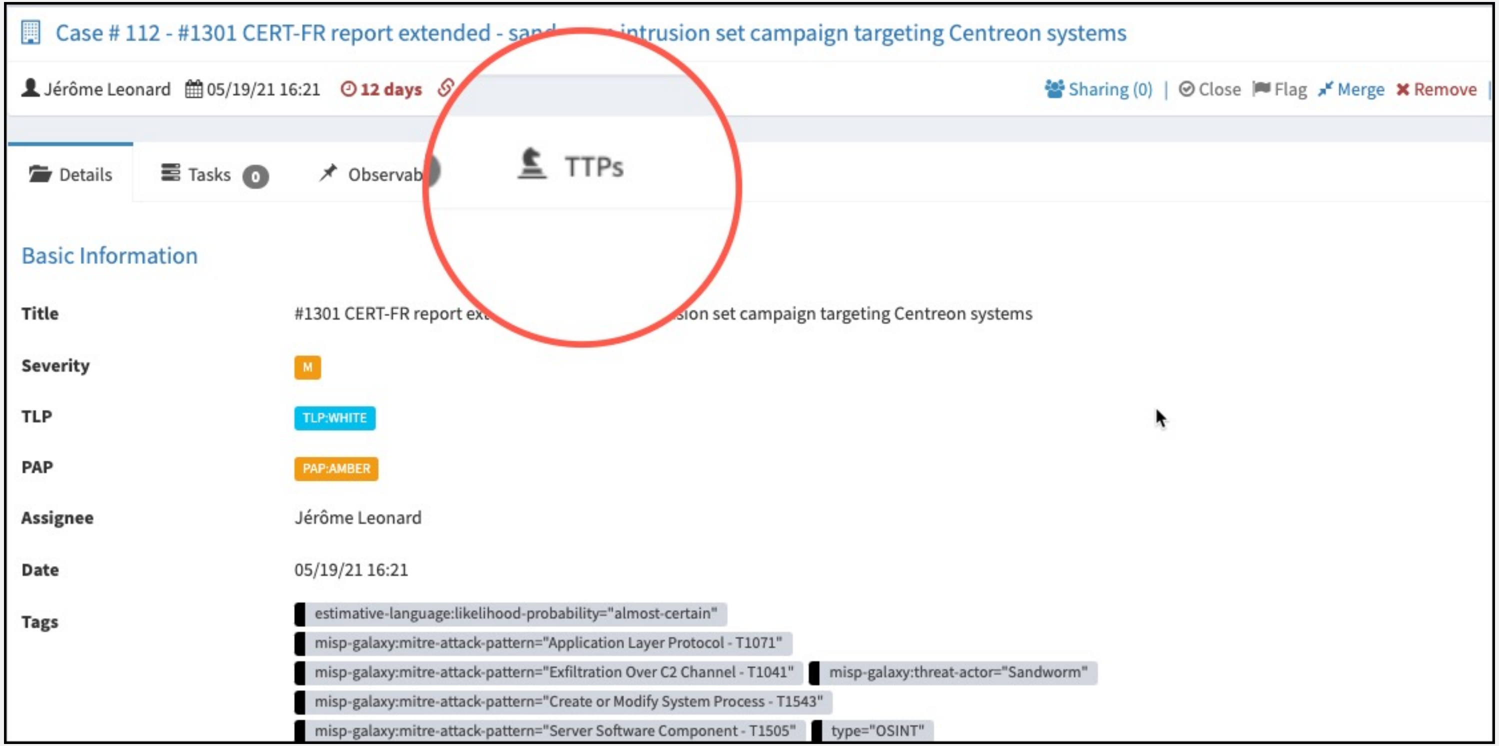
TTP in the data model

- Add TTPs in a Case
- Defined by:
  - ○ Technique
  - ○ Tactic
  - ○ Date of occurrence
  - ○ Procedure description (optional)
- Can be shared across Organisations



StrangeBee

New TTP tab



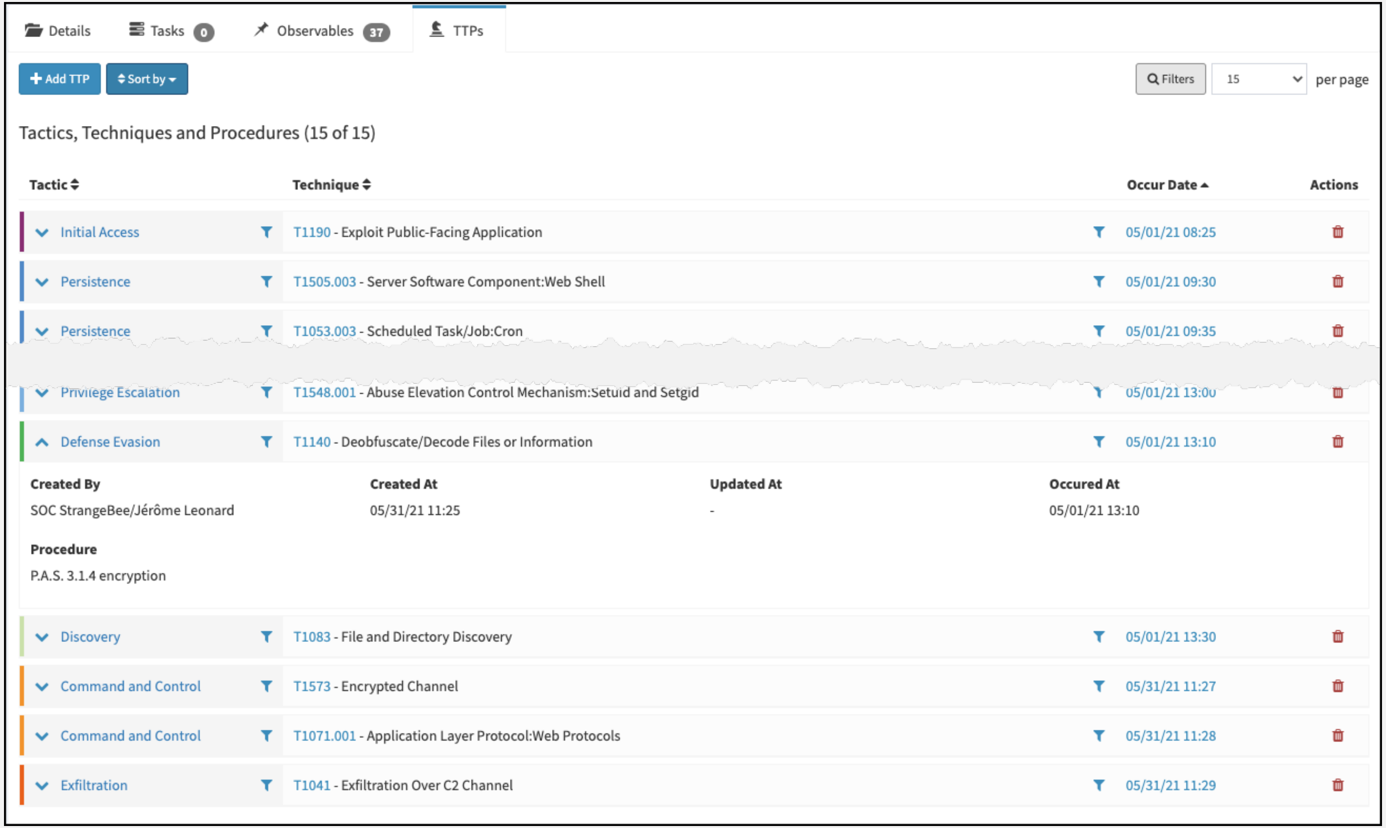
Case # 112 - #1301 CERT-FR report extended - san intrusion set campaign targeting Centreon systems

Jérôme Leonard 05/19/21 16:21 12 days

Basic Information

Title	#1301 CERT-FR report ex sion set campaign targeting Centreon systems
Severity	M
TLP	TLP:WHITE
PAP	PAP:AMBER
Assignee	Jérôme Leonard
Date	05/19/21 16:21
Tags	estimative-language:likelihood-probability="almost-certain" misp-galaxy:mitre-attack-pattern="Application Layer Protocol - T1071" misp-galaxy:mitre-attack-pattern="Exfiltration Over C2 Channel - T1041" misp-galaxy:threat-actor="Sandworm" misp-galaxy:mitre-attack-pattern="Create or Modify System Process - T1543" misp-galaxy:mitre-attack-pattern="Server Software Component - T1505" type="OSINT"

List of TTPs related to a Case



Tactics, Techniques and Procedures (15 of 15)

Tactic	Technique	Occur Date	Actions
Initial Access	T1190 - Exploit Public-Facing Application	05/01/21 08:25	🗑
Persistence	T1505.003 - Server Software Component:Web Shell	05/01/21 09:30	🗑
Persistence	T1053.003 - Scheduled Task/Job:Cron	05/01/21 09:35	🗑
Privilege Escalation	T1548.001 - Abuse Elevation Control Mechanism:Setuid and Setgid	05/01/21 13:00	🗑
Defense Evasion	T1140 - Deobfuscate/Decode Files or Information	05/01/21 13:10	🗑

Created By	Created At	Updated At	Occured At
SOC StrangeBee/Jérôme Leonard	05/31/21 11:25	-	05/01/21 13:10

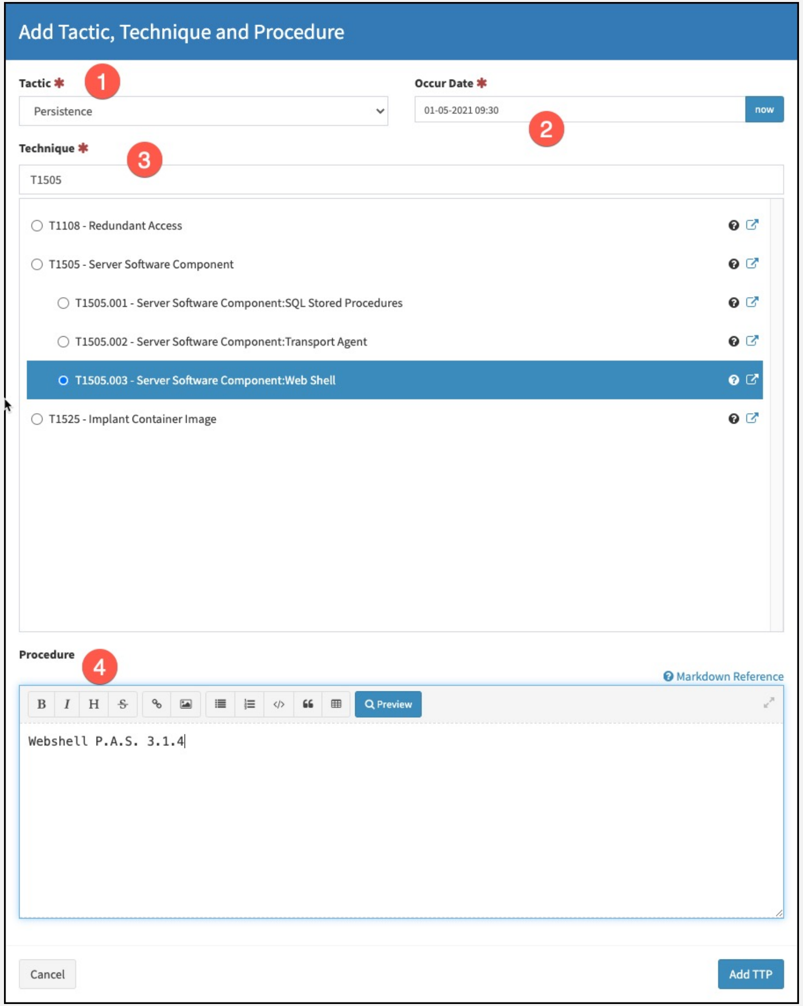
Procedure

P.A.S. 3.1.4 encryption

Tactic	Technique	Occur Date	Actions
Discovery	T1083 - File and Directory Discovery	05/01/21 13:30	🗑
Command and Control	T1573 - Encrypted Channel	05/31/21 11:27	🗑
Command and Control	T1071.001 - Application Layer Protocol:Web Protocols	05/31/21 11:28	🗑
Exfiltration	T1041 - Exfiltration Over C2 Channel	05/31/21 11:29	🗑

Enrich a Case with a TTP

1. Define the *Tactic*
2. Specify the occur date
3. Look for & select the right *Technique or Sub-technique*
4. Add a *Procedure* description (optional)



Add Tactic, Technique and Procedure

Tactic * 1
Persistence

Occur Date *
01-05-2021 09:30 now
2

Technique * 3
T1505

○ T1108 - Redundant Access
○ T1505 - Server Software Component
○ T1505.001 - Server Software Component:SQL Stored Procedures
○ T1505.002 - Server Software Component:Transport Agent
○ T1505.003 - Server Software Component:Web Shell
○ T1525 - Implant Container Image

Procedure 4
Markdown Reference

```
Webshell P.A.S. 3.1.4
```

StrangeBee

Coming features

Coming features

- Enrich MISP support with TTPs (import & share)
- Support TTPs in Alerts
- Cases and Alerts similarities upon patterns
- Links to Observables
- Distinguish collections of patterns: support Mobile tactics, ICS

StrangeBee

Thank You

✉ jerome@strangebee.com

@TheHive_Project | @StrangeBeeInc

StrangeBee