



Introducing CoreTIDE

Powering the OpenTIDE ecosystem, the first open source DetectionOps platform, developed at the European Commission



We are (mostly) the EC DIGIT S.2 CATCH Squad



Amine BESSON
(Behemoth Cyberdefence, NL)



Claus HOUMANN
(EC DIGIT S1, LU)



Remi SEGUY
(EC DIGIT S2, LU)

European Commission
Directorate-General for Digital Services
Directorate S Cybersecurity
Cybersecurity Operations Centre
**Cyber Analytics, Trending,
Correlations & Hunting (CATCH)**



Threat Detection Engineering and Hunting
Capability of the EC CSOC

We maintain detection readiness across
systems and infrastructures

**CoreTIDE was developed and adopted
as our key platform to support our
Detection Engineering Operations**

Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission



Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

The CoreTIDE Framework



Project Timeline



- Predecessor: Trying to feed cloud detection intel to a SOC without cloud knowledge. This had some challenges. Hired Amine and told him 'solve these challenges'
- Amine built a R&D project to try to improve detection ideas handover to SOC
- Evolved as a central system for Detection Engineering
- Currently powers CATCH (Cyber Analytics, Trending, Correlations and Hunting), a DE and TH capability in the wider EC CSOC community
- Supports the team transition scaling to high maturity targets by adopting DevOps delivery principles

[March 2022] R&D Starts

[22Q3] Expansion to Managed Detection Rules

Full content Migration from other systems

[23Q1] Adoption of new wiki, complex MDRv3 patterns

[23Q3] Lookup support, TVM Chaining, Relationship graph, new references

[24Q1] Code Refactors, Open Sourcing



[22Q2] First working group to create models

Official adoption at CATCH

[22Q4] Implementation of trunk based deployment solutions

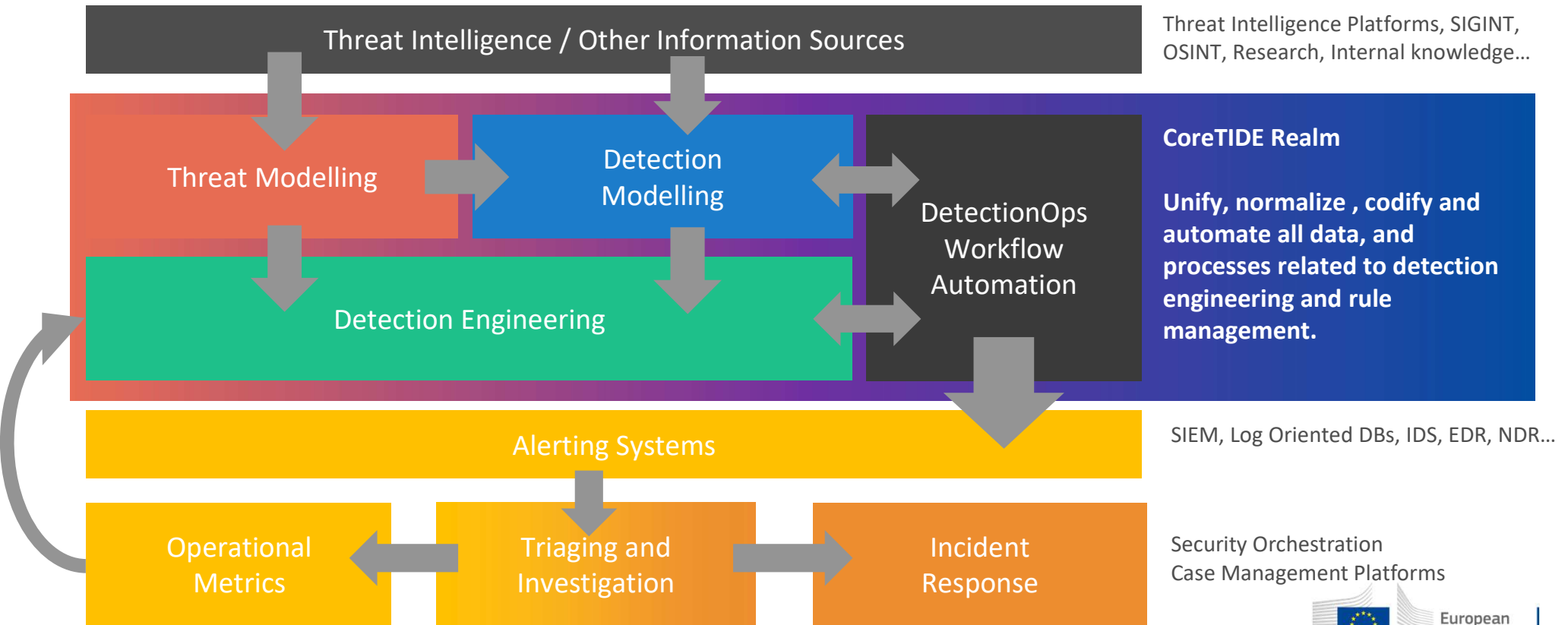
[23Q2] Foundational data model solutions : scoped vocabularies, meta definitions, code modularization...

[23Q4] MDR expansion



Disclaimer: *The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission*

Detection Engineering Tech Landscape



ATT&CK is useful, but limited

Scheduled Task/Job

Sub-techniques (5)	
ID	Name
T1053.002	At
T1053.003	Cron
T1053.005	Scheduled Task
T1053.006	Systemd Timers
T1053.007	Container Orchestration Job

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.^[1]

ID: T1053
 Sub-techniques: T1053.002, T1053.003, T1053.005, T1053.006, T1053.007
 Tactics: Execution, Persistence, Privilege Escalation
 Platforms: Containers, Linux, Windows, macOS
 Permissions Required: Administrator, SYSTEM, User
 Effective Permissions: Administrator, SYSTEM, User
 Supports Remote: Yes
 CAPEC ID:

What ATT&CK Describes

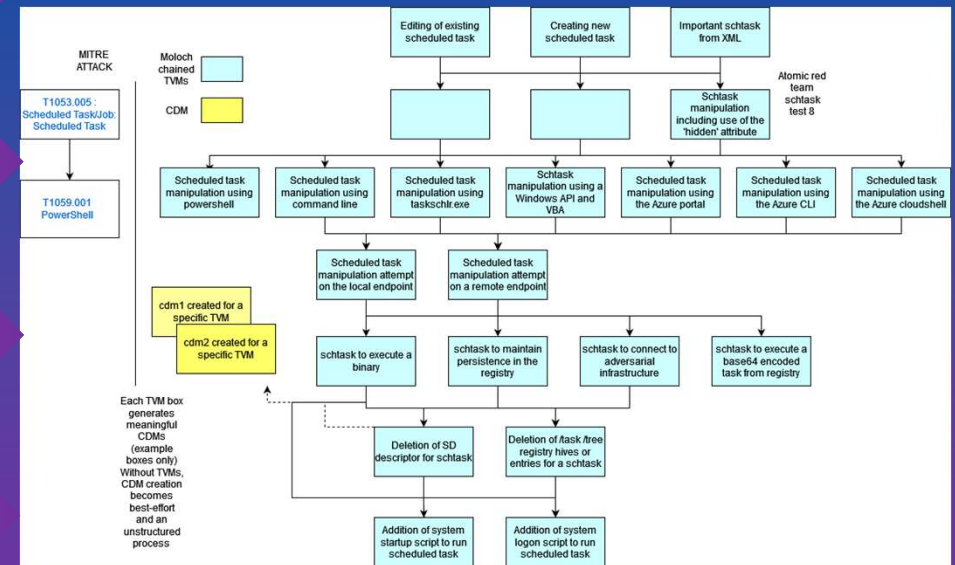
Threat Decomposition

Detection Coverage Analysis

Enrich with real-world Examples

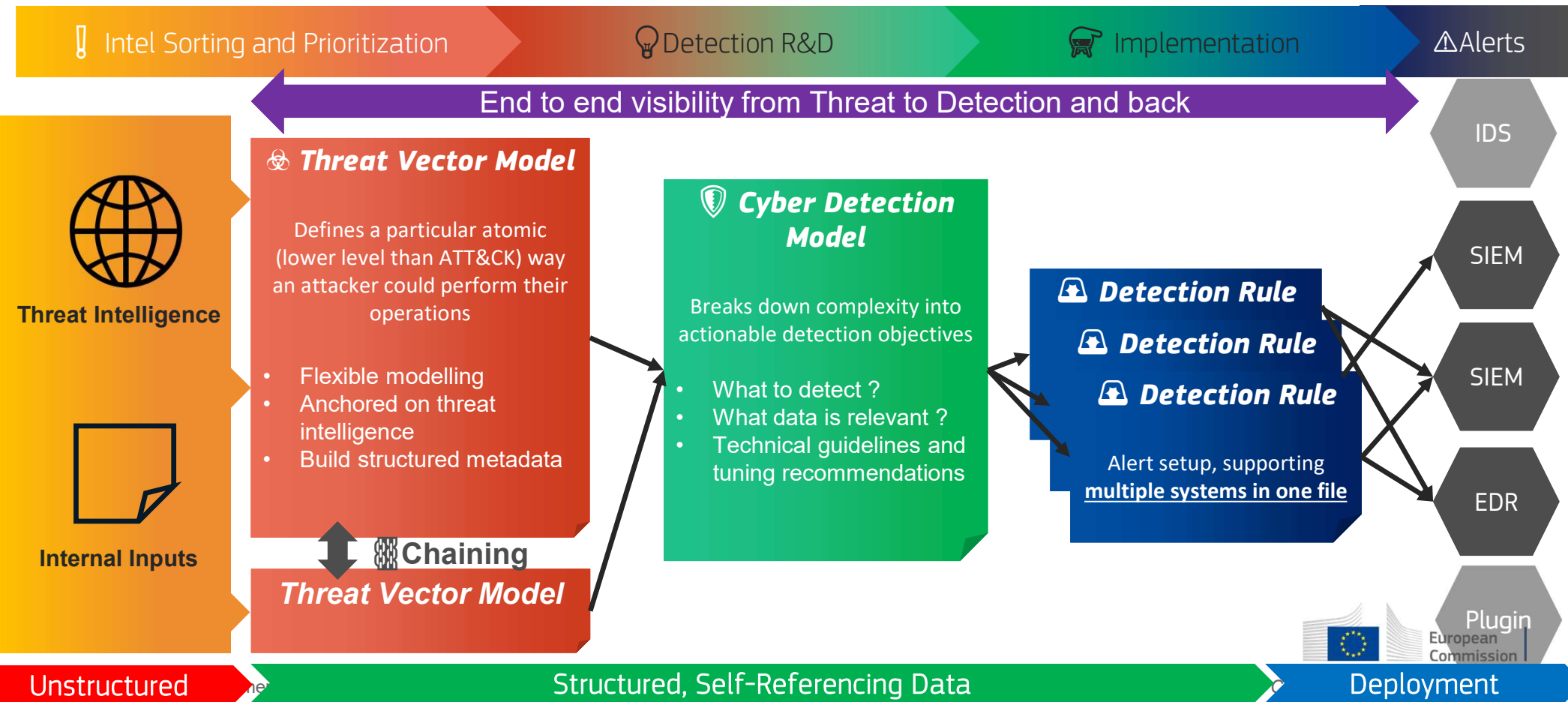
Further research co-related TTPs

Research Detection Methods



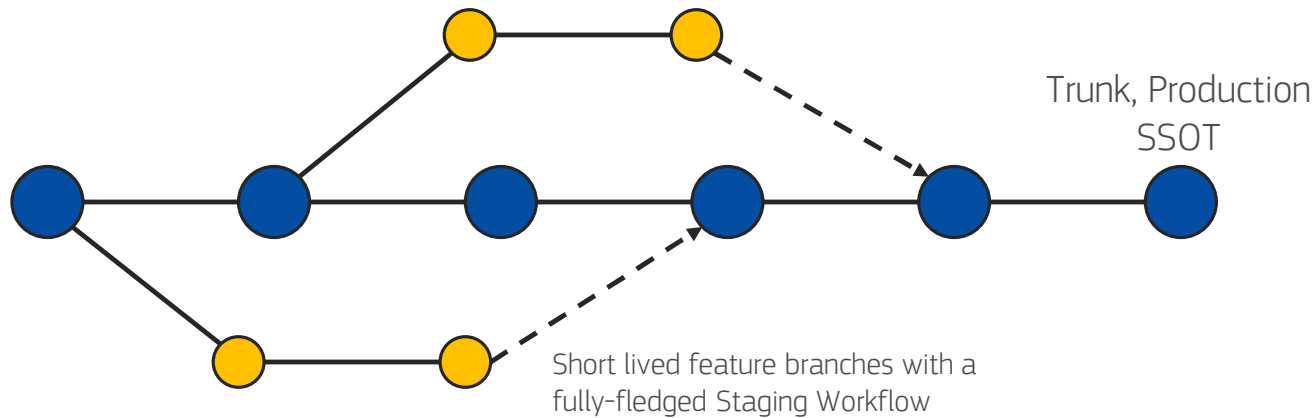
Detection Engineers break down threats into smaller actionable elements

CoreTIDE Threat-Driven Workflow





CoreTIDE is a DetectionOps Platform

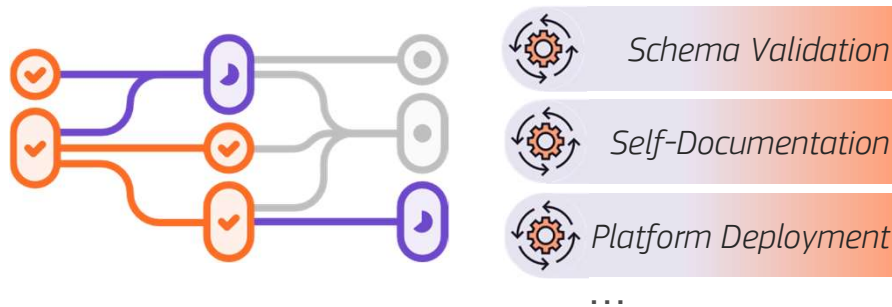


Using a Trunk Based Development Strategy to leverage **as-code** objects in a **Git** repository, CoreTIDE codifies key workflows in a repeatable, tailored, and automated modern **DevOps** flow.

Threat-driven workflows can be adopted natively to create a continuous lifecycle, adopting DevOps maturity deep into DE : **DetectionOps**



Primary support for Gitlab, but codebase is portable to other tools



Push-Based CI Service triggers multiple automation engines to perform workflow tasks on every commit



What do you need ?



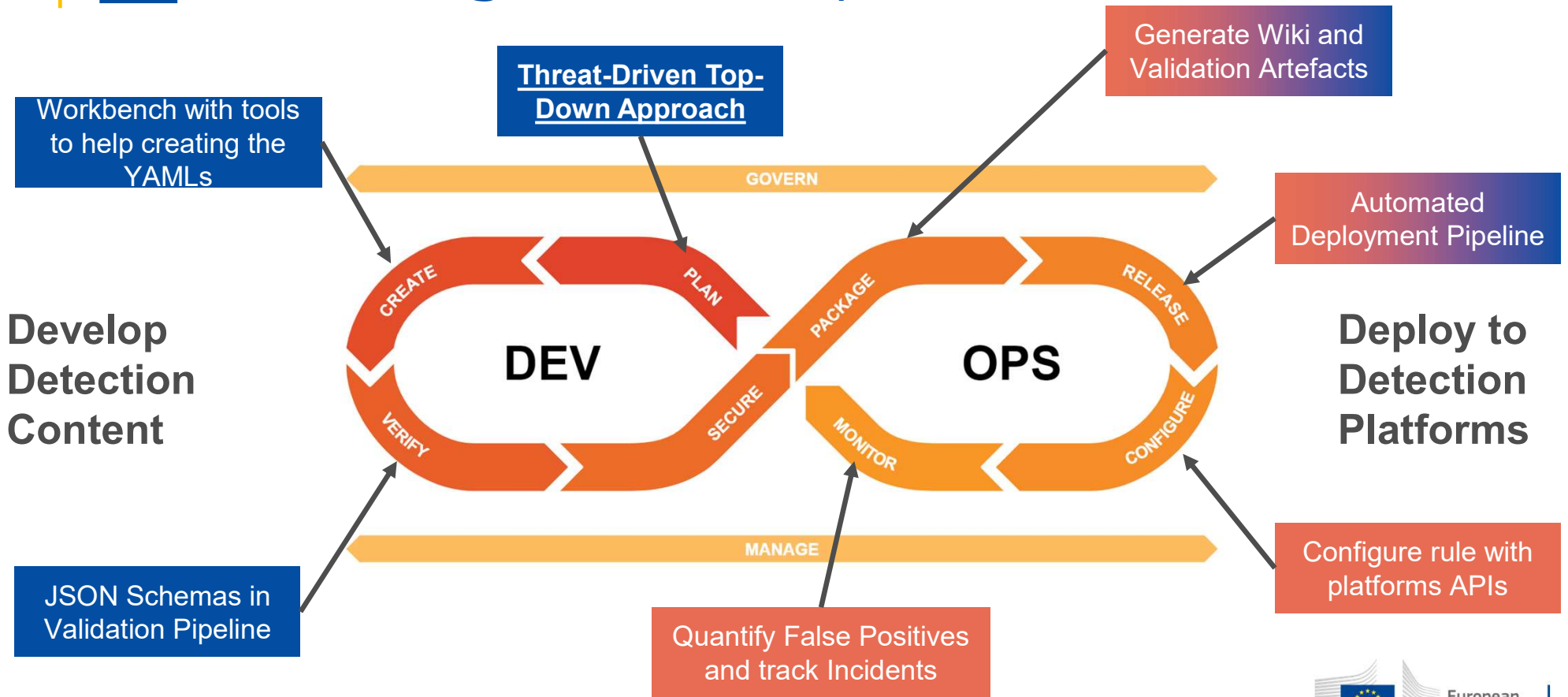
- Adopt basic DevOps tooling
 - Gitlab (out-of-the-box) or another Version Control System + CI Service (need to write your own pipelines from CoreTIDE scripts).
 - VSCode to get the full tooling and developer experience
- Clone our StartTIDE repo on (<https://code.europa.eu/ec-digit-s2/opentide/starttide>) and push to your Gitlab/VCS
- If you want a local copy, clone CoreTIDE (<https://code.europa.eu/ec-digit-s2/opentide/coretide>) as well, by default the pipelines will fetch our latest public repository and inject it in your pipelines.
- Tweak some configurations, especially deployment engines for detection as-code
- Add CI variables (check scripts and configuration to see what's expected)
- Branch, Create, Merge, Document, Deploy, **Profit**



Disclaimer: *The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission*

✓ Pioneering DetectionOps

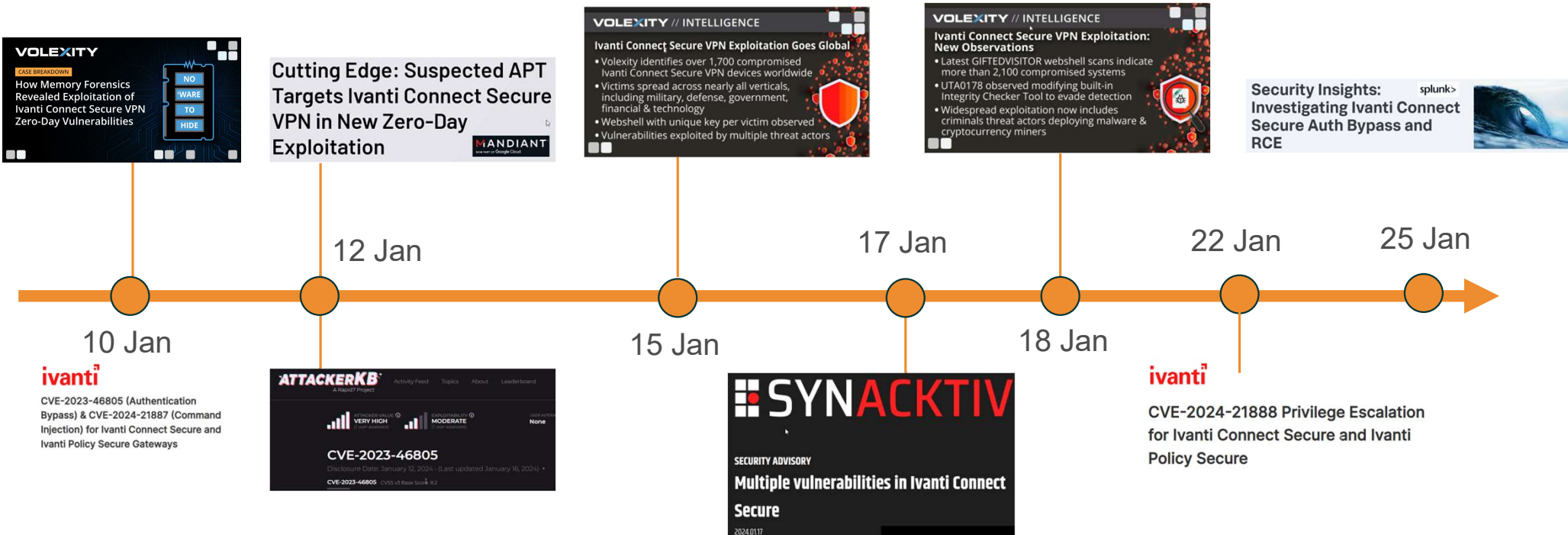
Re-do this slide to clarify what we mean with DetectionOps





CoreTIDE in Practice

Decomposing the recent Ivanti threats into actionable outcomes

Threat Inputs



Initial Breaking Down into Models

- First break-down into 2 Threat Vector models that synergise each other.
-  [TVM0000] - Authentication bypass on Ivanti Connect Secure appliances
 - CVE-2023-46805
-  [TVM0000] Command injection on web components of Ivanti Connect Secure appliances
 - CVE-2024-21887

Resolve "🦠 TVM CREATE web server authentication bypass on ICS"

Overview 0 Commits 3 Pipelines 3 Changes 2

Add a to do

on Manager.yaml deleted 100644 → 0

Search (e.g. *.vue) (Ctrl+I)

Models Library/Threat Vector Models/TVM0032 - authentication bypass on Ivanti Connect Secure appliances.yaml 0 → 100644

+61 -0 Viewed

```
22 + threat:
23 +   #actors:
24 +     #- TAM0010
25 +   killchain: Exploitation
26 +   att&ck:
27 +     - T1190 #Exploit Public-Faci
28 +   domains:
29 +     - Embedded
30 +     - Enterprise
31 +     - Networking
32 +   terrain: |
33 +     Ivanti Connect Secure applia
34 +   targets:
35 +     - Remote access
36 +     - VPN Client
37 +   platforms:
38 +     - Placeholder
39 +   severity: Highly significant i
40 +   leverage:
41 +     - Infrastructure Compromise
42 +     - Elevation of privilege
43 +     - Log tampering
44 +     - Modify configuration
45 +     - Tampering
46 +     - New Accounts
```



```
1 + id: TVM0032
2 + name: authentication bypass on Ivanti Connect Secure appliances
3 + criticality: Severe
4 + references:
5 +   public:
6 +     1: https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
7 +     2: https://nvd.nist.gov/vuln/detail/CVE-2023-46085
```

```
47 +   impact:
48 +     - Business disruption
49 +     - Operating costs
50 +     - Reputational Damages
51 +     - Data Breach
52 +   viability: Almost certain
53 +   description: |
54 +     Attackers may identify a vulnerability on Ivanti Connect Secure appliances
55 +     (that provide remote VPN access to corporate infrastructures) to bypass
```

Complete Overview from Threat to Detection (CI/CD pipeline for documentation)



[TVM0032] authentication bypass on Ivanti Connect Secure appliances

 **Criticality:Severe**  : A Severe priority incident is likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.

 **TLP:CLEAR**  : Recipients can spread this to the world, there is no limit on disclosure.

 **ATT&CK Techniques** T1011 : Exfiltration Over Other Network Medium, T1041 : Exfiltration Over C2 Channel, T1070 : Indicator Removal, T1190 : Exploit Public-Facing Application

 Version : 1,  Creation Date : 2024-01-15,  Last Modification : 2024-01-29,  Model author :

Description

chained exploitation of CVE-2023-46805 or CVE-2024-21893 together with CVE-2024-21887.

Attackers may chain exploits on vulnerabilities CVE-2023-46805 and CVE-2024-21893 on Ivanti Connect Secure (ICS) appliances (that provide remote VPN access to corporate infrastructures) to fully compromise the vulnerable appliance.

The code on the appliance checks whether access to the requested uri_path requires authentication or not. For endpoint `/api/v1/totp/user-backup-code` the check is done only on the start of the string.

So an attacker can append additional characters that are passed to the webserver without additional checks. Using path traversal technique, it is then possible to access API endpoints that would require authentication when accessed directly. For example, successful request to `/api/v1/totp/user-backup-code/../../../../system/system-information` will return the system information.

CVE-2023-46805 allows then to access any other uri_path without authentication and enables exploitation of CVE-2024-21887.

Later it was reported that initial mitigations for CVE-2023-46805 could be bypassed by exploiting CVE-2024-21893 to bypass authentication and enabling CVE-2024-21887 without using vulnerable uri paths or to drop custom webshells ([BUSHWALK LIGHTWIRE CHAINLINE](#) and others have been observed).

Exploitation of the SSRF generates up to 2 log events:

- AUT31556 on `/dana-ws/saml.ws`
- ERR31093: Program saml-server recently failed.

Likewise, exploitation of CVE-2024-21893 or CVE-2024-22024 enables exploitation of CVE-2024-21887.

Other TTPs

- *Configuration and data theft* Exfiltration of configuration or cache data either in the response to the request (so on apparently legit activity) or by replacing or creating a new file under unauthenticated uri path.
- CAV Web Server Log Exfiltration
- Internal Check tool tampering
- System log clearing: In some instances, logs have been cleared using the legitimate system utility therefore generating event ID ADM20599.

Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission



Complete Overview from Threat to Detection Continued



Model Data

Cyber Kill Chain

Cyber attacks are typically phased progressions towards strategic objectives. The Unified Kill Chains help develop (or realign) defensive strategies to raise cyber resilience.

Exploitation : Techniques to exploit vulnerabilities in systems that may, amongst others, result in c

Domains

Infrastructure technologies domain of interest to attackers.

- Embedded** : Firmware, middleware and low level software running on devices which are typically
- Enterprise** : Generic databases, applications, machines and systems that are usually on premis
- Networking** : Communications backbone connecting users, applications and machines.

Targets

Granular delimited technical entities holding a value to the organization, that are targeted by adversarie Veris.

- Remote access** : Server - Remote access
- VPN Client** : Placeholder

Platforms concerned

Actual technologies used by the organization that will be exploited by adversaries during a successful i

Placeholder : Placeholder

Severity

The severity summarizes the overall danger of incident the vector will provoke, and is to be de

Highly significant incident : A cyber attack which has a serious impact on central gov economy.

Leverage acquisition

Technical aftermath of the attack from the target perspective, differentiated from impact as it d adversary.

- Infrastructure Compromise** : The compromised target is likely to be used to further e
- Elevation of privilege** : Capacity to augment leverage over the target system by up
- Log tampering** : Log tampering or modification
- Modify configuration** : Modify configuration or services
- Tampering** : Threat action intending to maliciously change or modify persistent data, su as the Internet.
- New Accounts** : Ability to create new arbitrary user accounts.

Impact

Analysis of the threat vector from the organizational perspective, in non technical term. This ai

- Business disruption** : Business disruption
- Operating costs** : Increased operating costs
- Reputational Damages** : Damages to the organization public view may be achieved by
- Data Breach** : Non-public information has been accessed from the outside, and succes

Vector Viability

Described with estimative language (likelihood probability), describes how likely the analyst b credibility of underlying sources, data, and methodologies based Intelligence Community Dire

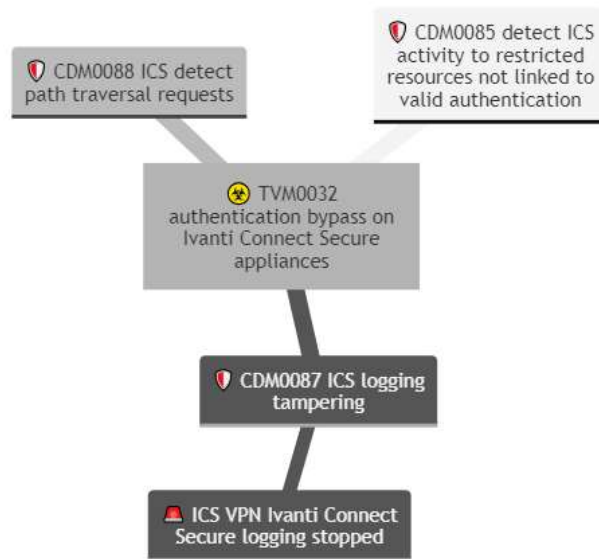
Almost certain : Nearly certain - 95-99%

Disclaimer: *The views expressed are solely those of the writers and may not be regarded a*

Complete Overview from Threat to Detection Continued



Relations



Descendants

Detection Models (3)	Detection Rules
[CDM0085] detect ICS activity to restricted resources not linked to valid authentication	✗ No Detection Rules
[CDM0087] ICS logging tampering	ICS VPN Ivanti Connect Secure logging stopped
[CDM0088] ICS detect path traversal requests	✗ No Detection Rules



Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

Advanced Modelling and Detection-as-Code capabilities

DetectionOps Workflows

...DemoTide

Resolve "MDR ICS Ivanti Connect Secure logging stream stop or reduced"

```

Merged Remi SEGUY requested to merge 1815-edr-ics-ivanti-connect- into main 1 month ago
Overview 7 Commits 12 Pipelines 12 Changes 1
Compare main and latest version
Search (e.g. *.vue) (Ctrl+P)
Models Library/Managed Detection Rules/ICS VPN Ivanti Connect Secure logging stream stopped.yml
ICS VPN I...opped.yml +100 -0
1 name: ICS VPN Ivanti Connect Secure logging stopped
2 uid: e069ee5c-8d43-4bff-8bc6-99b1e3445e4
3 #references:
4 #public:
5 #1:
6 #internal:
7 #2:
8 #restricted:
9 #3:
10 #reports:
11 #-
12 #
13 metadata:
14 tlp: clear
15 version: 1
16 created: 2024-01-30
17 modified: 2024-02-02
18 author: frederic.gillet@ext.ec.europa.eu
19 #
20 description: |
21 Attacker could leverage a vulnerable ICS appliance to gain access. As a side
22 effect of a successful compromise, logs are no longer generated and/or send
23 to log collection.
24 #
25 If a ICS VPN appliance stops sending logs and is marked active in the Lookup
26 investigate with CS splunk team (DIGIT ISMS SPLUNK <DIGIT-ISMS-SPLUNK@ec.europa.eu>) and
27 DIGIT SNET GRC Governance Compliance team DIGIT-SNET-GRC@ec.europa.eu.
  
```

Select a snippet

- Threat Vectors Template
- MDR Systems Deployment : Microsoft Sentinel Template
- MDR Systems Deployment : Splunk Enterprise Template
- Business Requests Template
- Threat Actors Template
- Lookup Metadata Template
- MDR Systems Deployment : Carbon Black Cloud Enterprise EDR Template
- Detection Rules Template

```

30 response:
31 alert_severity:
32 #playbook:
33 responders:
34 configurations:
35 splunk:
  
```

Critical

Identifier: SEV0005

Criticality: No Criticality Assigned

```

metadata:
  tip: clear
  version: 1
  created: 2024-0
  modified: 2024-
  author: frederi
description: |
  Attacker could
  effect of a suc
  to log collecti
  If a ICS VPN ap
  investigate wit
  DIGIT SNET GRC
detection_model: CDM0087
  
```

Detection Models

Detection Models

CDM0087 :

ICS logging tampering

Identifier: CDM0087

Criticality: Severe | TLP: CLEAR

See in CoreTIDE Wiki

- Search for stop or gaps in log collection from Ivanti Pulse Connect (ICS).
- search for any signature ID (code) related to logging such as log cleared or deleted, etc.

DataTide, IndexTide, DeployTide

```
Engines > modules > code.py > ...
1 import sys
2 import git
3
4 sys.path.append(str(git.Repo(".", search_parent_directories=True).working_dir))
5
6 from Engines.modules.tide import DataTide
7 from Engines.modules
8 (class) Models
9 AVAILABLE_MDR_DEPLOY TIDE Models Data Interface.
10 SPLUNK_SECRETS = Dat Exposes all the Models Data indexed in the OpenTIDE Instance
11 VOCABULARIES = DataT
12 TVM_DATA = DataTide.Models.tvm
```

```
AVAILABLE_MDR_DEPLOYERS = DeployTide.mdr
SPLUNK_SECRETS = DataTide.Configurations.mdr
VOCABULARIES = DataTide.Vocabularies.Index
TVM_DATA = DataTide.Models.tvm
```

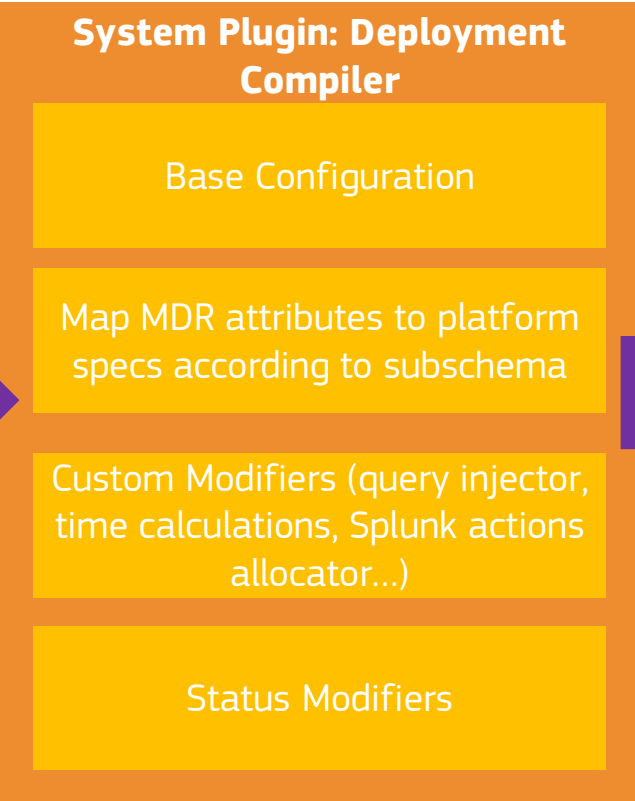
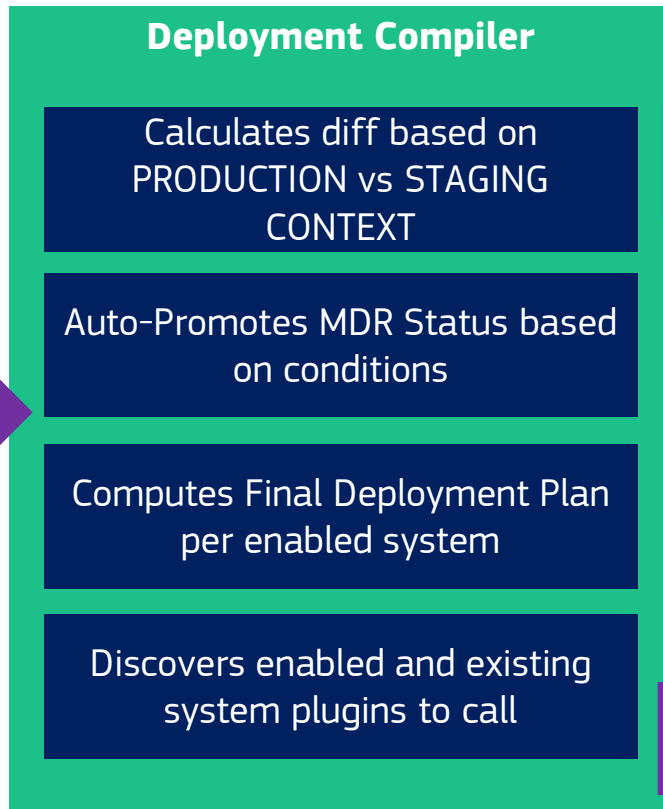
mdr: dict[str, DeployMDR]

```
10 AVAILABLE_MDR_DEPLOYERS = DeployTide.mdr
11 SPLUNK_DEPLOYER = DeployTide.mdr["splunk"].deploy()
12 SPLUNK_SECRETS = DataTide.Configurations.Systems.deploy
13 VOCABULARIES = DataTide.Vocabularies.Index
14 TVM_DATA = DataTide.Models.tvm
```

def deploy(deployment: list[str]) -> No ×
Deploy MDR Objects onto target systems

- DataTide is a single unified interface to access all data from the OpenTIDE Instance.
- Upon import, IndexTIDE caches all data from the OpenTIDE instance CoreTIDE was injected into, and expose dataclasses for an easier, well typed access to any data from configurations to model data.
- The index is cached in the DataTide object for high performances in-memory (especially recursions).Support hot reloading
- DeployTIDE exposes an interfaceto deployment engines using hot-pluggable modules, meaning we can easily write new deployment engines (or custom ones if you want an internal CoreTIDE repo)

Deployment Pipeline



Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

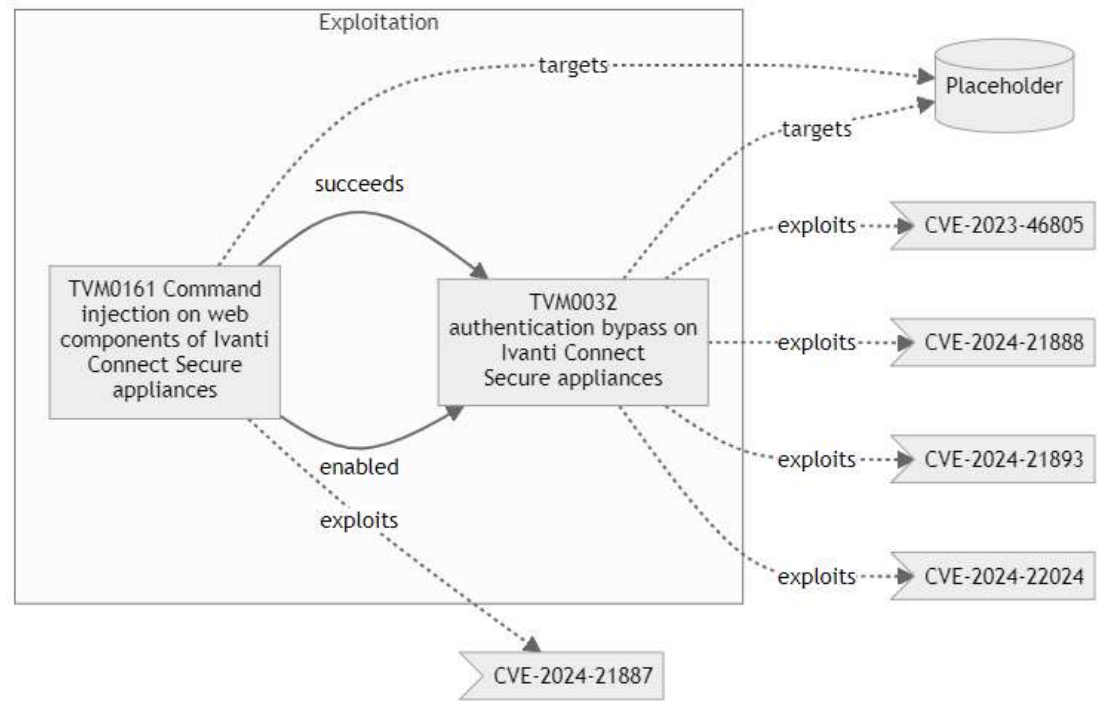
Using Threat Chaining to describe complex relationships

```
chaining:
- relation:
  - vector: TV
  - description:
  - bypass
  - cve:
  - domains:
  - terrain:
  - targets:
```

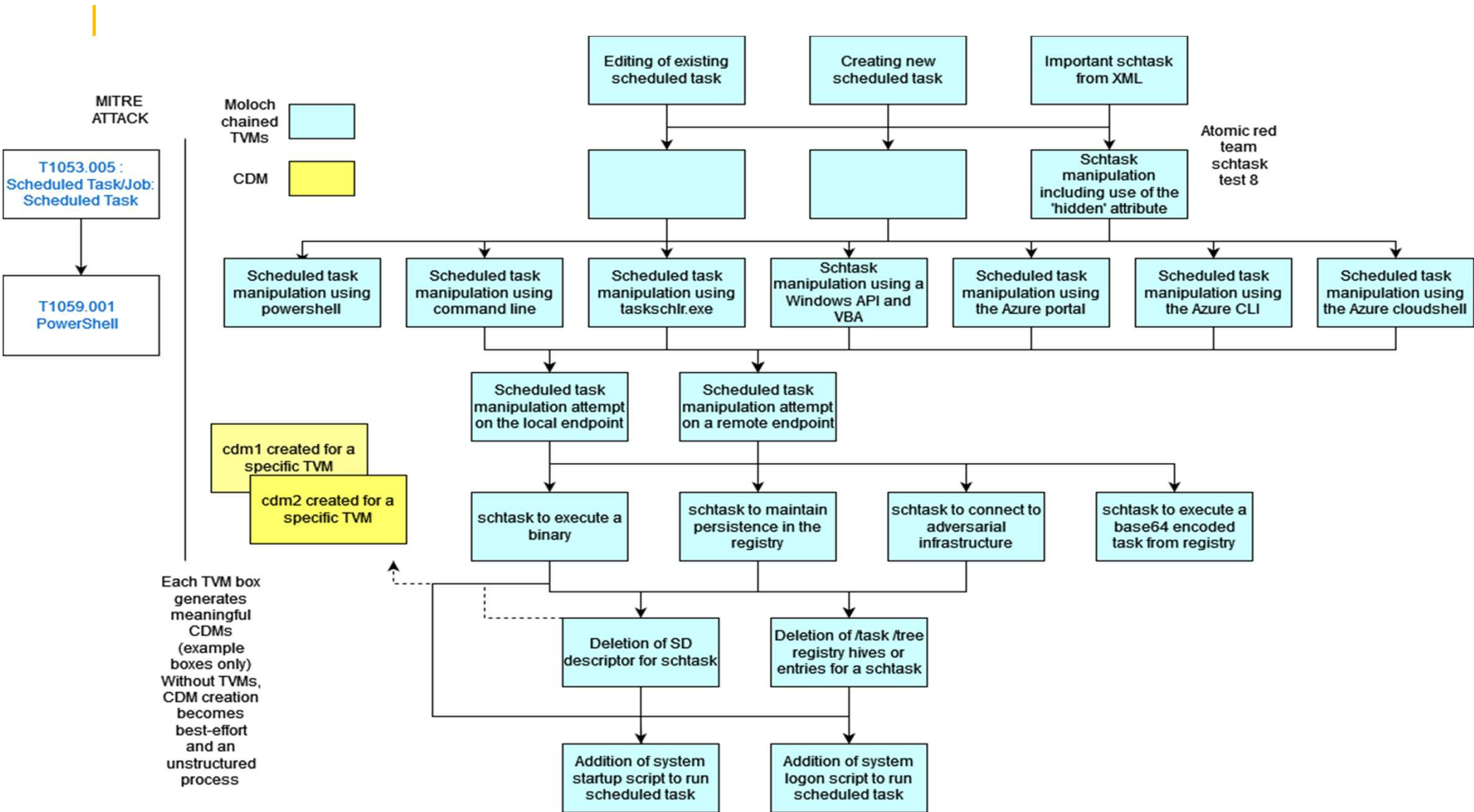
synergize
Identifier: CHN0022
Criticality: No Criticality Assigned
Supportive: TVMs which successful execution allows other TVMs to be more easily performed, or produce larger impact.
See in CoreTIDE Wiki
Both TVM supports each other in performing adversary operations

- TVM chaining is a way of connecting related threat vectors together horizontally to represent complex real-world interactions between procedures and techniques
- Each TVM has separately defineable detection objectives, but is now put into the context of a wider ecosystem of interrelated threats
- Allows to model campaign, offensive tools, reported killchains effectively

Threat Chaining



Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission



Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission

The OpenTIDE Initiative



An Open Detection Engineering ecosystem



Open Threat Informed Detection Engineering is the overarching project developing tooling, practices and content to support the community of Detection Engineers

<https://code.europa.eu/ec-digit-s2/opentide>



Engine Powering OpenTIDE
Instances



Starter project to immediately
create an instance



(Upcoming) A public instance
containing freely accessible models

**Current
projects
directly in
scope**



Disclaimer: *The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission*

Data Sharing – Upcoming



- **ShareTIDE** : Publicly accessible *TLP:CLEAR* models – open source threat and detection intel, modeled and coupled to chaining and detection objectives/rules (needs community contributions – like all the detection ideas presented throughout the day today.....)
- Closed loop knowledge sharing communities - sharing models that are not TLP:CLEAR
- Sharing architecture options/examples:
 - Automated sharing via MISP to existing communities based on your model TLPs and/or sharing metadata
 - Share data over a translation later to relevant STIX Objects
 - OpenTIDE sharing infrastructure where a CI workflow plugin automates the sharing



Disclaimer: *The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission*

Roadmap

- The OpenTIDE/CoreTIDE white paper
- Plugging farther into the community and creating review strategies to weigh the relevance of models based on community members in the same vertical, organization, size as the one you configured locally (community review module, optionally included in your OpenTIDE instance?)
- Reweighting the severity of threats based on local modifiers (for example, if you don't use AWS, then any shared TVM related should be scored down on your OpenTIDE Instance).
- Scaling the framework with New Objects, like Offensive Software Model or Log Collection Models and model them deeper in the framework
- New Deployment Engines
- Rules testing
- Engaging with the community, getting feedback and encouraging contributions !



Disclaimer: *The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission*

If there's time – summarizing notes

- John Lambert: **Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.**
 - TIDE builds a knowledge graph
- Collaborative security:
 - TIDE lets knowledge sharing communities work together at detecting better, faster
- MITRE ATT&CK/D3FEND:
 - TIDE does not compete with these great projects, but is a companion
- Need to detect at a lower level than the procedural, RE: the SpectreOps blog series: 'on-detection-from-tactical-to-functional' or at a higher level in the Detection pyramid of pain (David Bianco) – TIDE lets you do this



Disclaimer: *The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission*

Thank you!

Visit <https://code.europa.eu/ec-digit-s2/opentide>
for updates and additional materials