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*
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

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

Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission.
ATT&CK is useful, but limited

Scheduled Task/Job

<table>
<thead>
<tr>
<th>ID</th>
<th>Name</th>
<th>Sub-techniques (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1053.002</td>
<td>AT</td>
<td>ID: T1053 Sub-techniques: T1053.002, T1053.003, T1053.005, T1053.006, T1053.007</td>
</tr>
<tr>
<td>T1053.003</td>
<td>Cron</td>
<td></td>
</tr>
<tr>
<td>T1053.005</td>
<td>Scheduled Task</td>
<td></td>
</tr>
<tr>
<td>T1053.006</td>
<td>Systemd Timers</td>
<td></td>
</tr>
<tr>
<td>T1053.007</td>
<td>Container Orchestration Job</td>
<td></td>
</tr>
</tbody>
</table>

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.\[1\]

What ATT&CK Describes

Detection Engineers break down threats into smaller actionable elements
CoreTIDE Threat-Driven Workflow

**Threat Vector Model**
- Defines a particular atomic (lower level than ATT&CK) way an attacker could perform their operations
  - Flexible modelling
  - Anchored on threat intelligence
  - Build structured metadata

**Cyber Detection Model**
- Breaks down complexity into actionable detection objectives
  - What to detect?
  - What data is relevant?
  - Technical guidelines and tuning recommendations

**Detection Rule**
- Alert setup, supporting multiple systems in one file

**Intel Sorting and Prioritization**

**Detection R&D**

**Implementation**

**Alerts**

**Threat Intelligence**

**Internal Inputs**

**Chaining**

**Structured, Self-Referencing Data**

**Unstructured**

**Deployment**
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

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

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

- Schema Validation
- Self-Documentation
- Platform Deployment
- ...

Confidential - Limited
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](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](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

- Threat-Driven Top-Down Approach
- Generate Wiki and Validation Artefacts
- Automated Deployment Pipeline
- Configure rule with platforms APIs
- Quantify False Positives and track Incidents
- JSON Schemas in Validation Pipeline
- Workbench with tools to help creating the YAMLs

Develop Detection Content

Deploy to Detection Platforms
CoreTIDE in Practice

Decomposing the recent Ivanti threats into actionable outcomes
Threat Inputs

10 Jan
CVE-2023-46805 (Authentication Bypass) & CVE-2024-21888 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways

12 Jan
Cutting Edge: Suspected APT Targets Ivanti Connect Secure VPN in New Zero-Day Exploitation

15 Jan

17 Jan
Volexity // Intelligence
Ivanti Connect Secure VPN Exploitation Goes Global
- Volexity identifies over 1,700 compromised Ivanti Connect Secure VPN devices worldwide
- Victims spread across nearly all verticals, including military, defense, government, financial & technology
- Webshell with unique key per victim observed
- Vulnerabilities exploited by multiple threat actors

22 Jan
Ivanti Connect Secure VPN Exploitation: New Observations
- Latest GFI-LORDOR webshell scans indicate more than 2,500 compromised systems
- LFA6178 observed modifying built-in Integrity Checker Tool to evade detection
- Widespread exploitation now includes criminal threat actors deploying malware & cryptocurrency miners

25 Jan
CVE-2024-21888 Privilege Escalation for Ivanti Connect Secure and Ivanti Policy Secure

Disclaimer: The views expressed are solely those of the writers and may not be regarded as stating an official position of the European Commission
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"
Complete Overview from Threat to Detection
(CI/CD pipeline for documentation)

[TVMO0032] 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:** 1.0
**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/http/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 webservice 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/http/user-backup-code/.../system/system-information` will return the system information.

CVE-2023-46805 allows them 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 (BUSHNAIL LIGHTWIRE CHAINLINE) and others have been observed.

Exploitation of the SSRF generates up to 2 log events:

- AUT31556 on `/data/ws/smt_/as`.
- ERR2092: Program smt-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 (as on apparently legit activity) or by replacing or creating a new file under unauthenticated `uri_path`.
- CAV Web Server Log Exfiltration
- Internal Chedi 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 p 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 definitive technical entities holding a value to the organization, that are targeted by adversarial Vars.

- 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

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 go
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 r
- 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, such 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 Damage: 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
Complete Overview from Threat to Detection
Continued

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

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

**Mutation**
- Continuous Schema Migrations
- MDR Auto-Promotion
- Dynamic ID Assigner

**Validation**
- CVE Checks against NVD
- UUID Formatting
- ID Duplication
- ID/Name File Name Alignment
- Lookup Metadata Checks against Content

**Documentation**
- Self-Documented Schemas
- Vocabularies
- Lookups
- Navigation index on home page
- Generate connected knowledge graph

**Framework Generation**
- Make Templates
- Make VSCode Snippets
- Index Models in Vocabularies
- Indexes and Build Reports
- Generate JSON Schema from TIDE Schemas

**Deployment**
- Calculates Deployment Scope
- Promote MDR
- Auto-plugin detection
- Status modifiers
- MDR, Lookups, and Metadata Lookups Deployment

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

TideMetaSchemas are a superset of JSON Schema aimed at automated schema generation and scale with large, complex dynamic data models. Every Model in the framework is defined as a TideMetaSchema.

- **TideMetaSchema**, defining a model class
- **Vocabulary files**, knowledge DB for allowed values and metadata
- **Common definitions**, referenced by TideMetaSchema
- **Recomposable sub-schemas**, which are injected if enabled at a config level (e.g. systems)

Monolithic, self-encapsulated single JSON Schema (per model) used for IDE autocompletion and Validation.

Template that is injected into vscode snippets

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

• 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 interface to deployment engines using hot-pluggable modules, meaning we can easily write new deployment engines (or custom ones if you want an internal CoreTIDE repo).

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

**Deployment Compiler**
- Calculates diff based on PRODUCTION vs STAGING CONTEXT
- Auto-Promotes MDR Status based on conditions
- Computes Final Deployment Plan per enabled system
- Discovers enabled and existing system plugins to call

**System Plugin: Deployment Compiler**
- Base Configuration
- Map MDR attributes to platform specs according to subschema
- Custom Modifiers (query injector, time calculations, Splunk actions allocator...)
- Status Modifiers

**API Calls to Platform**

**COMMIT: Modified MDR Files**

---

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

- 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.

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

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, modelized 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