Filigran

WHITE PAPER

Operationalizing Threat Intelligence for National Security

How threat intelligence helps government agencies stay ahead of evolving cyber threats and protect critical infrastructure

Summary

Executive summary

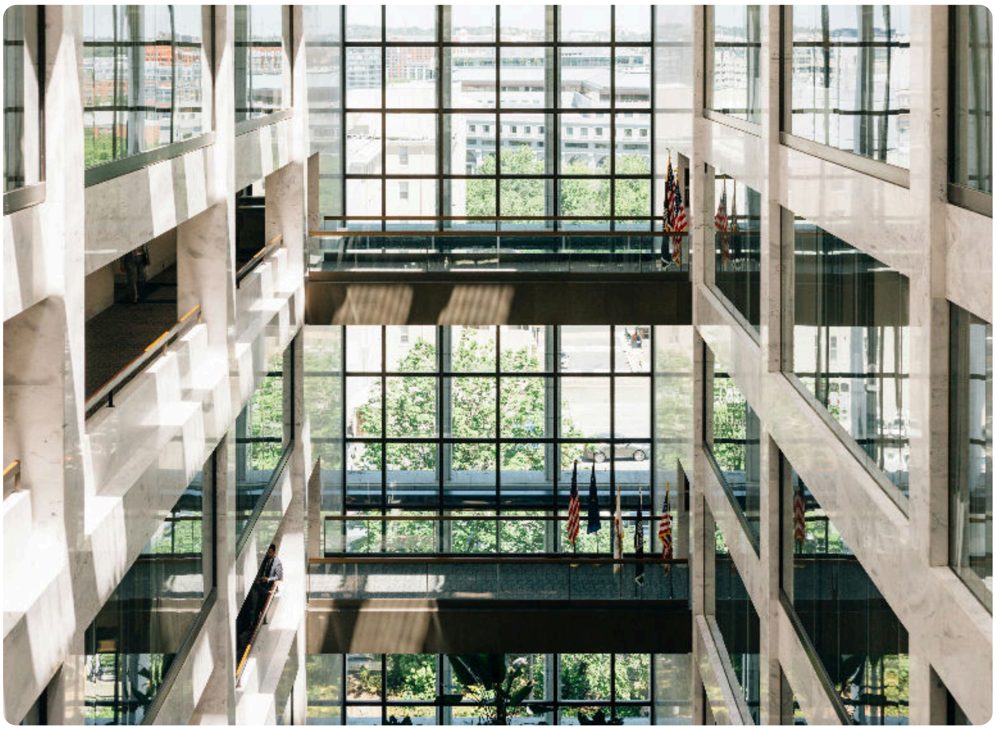


Photo by Erol Ahmed on Unsplash

Government agencies face relentless cyber threats, from state-sponsored attacks to cyber espionage targeting critical infrastructure and defense networks. As geopolitical tensions escalate, adversaries exploit vulnerabilities with increasingly advanced tactics, agencies must adopt a proactive, intelligence-driven cybersecurity strategy.

OpenCTI Enterprise Edition (EE) empowers government organizations to proactively identify, analyze, and mitigate cyber threats before they escalate into major security incidents. By integrating OpenCTI EE into their cybersecurity operations, agencies can:

HARDEN THEIR DEFENSES WITH REAL-TIME, ACTIONABLE INTELLIGENCE

Government agencies and defense organizations are prime targets for **state-sponsored cyberattacks, espionage, and critical infrastructure sabotage**. Attackers use advanced tactics to evade detection, making it essential for agencies to **anticipate** threats rather than react to them.

OpenCTI EE **aggregates, enriches, and correlates threat intelligence** from multiple sources, delivering **actionable insights** in real time. This allows security teams to **anticipate and block attacks** before they cause damage, rather than responding after the fact.

REDUCE MEAN TIME TO DETECT AND MEAN TIME TO RESPOND TO CYBER THREATS

Cyber intrusions against government and defense entities often remain undetected for **weeks or even months**, allowing adversaries to **exfiltrate classified data, disrupt military operations, or compromise national security infrastructure.** Rapid detection and response are crucial to **prevent long-term damage**.

OpenCTI EE automates threat intelligence processing, enabling **faster detection of indicators of compromise (IoCs)** and improved correlation with ongoing attacks. By **correlating intelligence with past attack campaigns**, agencies can **swiftly neutralize threats** before they escalate into full-scale breaches.

PREVENT FINANCIAL LOSSES AND OPERATIONAL DISRUPTIONS

Cyberattacks on government institutions can **cripple essential public services, disrupt military readiness, and expose classified intelligence**. Ransomware, supply chain breaches, and insider threats can lead to **billions in financial losses and erode public trust**.

By proactively **detecting and mitigating cyber threats targeting government networks**, OpenCTI EE helps **protect public sector operations** from costly shutdowns, data breaches, and cyber extortion. Its automation capabilities **reduce dependency on manual threat analysis**, allowing agencies to **focus resources on mission-critical defense operations**.

AUTOMATE INTELLIGENCE CORRELATION TO UNCOVER STATE-SPONSORED ATTACK PATTERNS

Nation-state actors often conduct **long-term, stealthy cyber campaigns** targeting government agencies, military units, and critical infrastructure. Without an advanced threat intelligence platform, security teams may only see **isolated incidents**, missing the bigger picture of coordinated attacks.

OpenCTI EE **automates the correlation of cyber threats across classified and open-source intelligence**, linking IOCs to known **adversary tactics, techniques, and procedures (TTPs)**. This allows agencies to attribute threats to specific state actors, predict their next moves, and strengthen preemptive cyber defenses.

EFFECTIVELY SHARE THREAT INTELLIGENCE AT SCALE AND AT SPEED

In today's hyper-connected digital environment where organisations are increasingly exposed through highly distributed networks and supply chains, it is essential that government agencies and industry partners share information and collaborate on how to swiftly and effectively identify and mitigate emerging threats potentially affecting their environment or national critical infrastructure.

Government agencies including National Cyber Security Agencies and CERTs can leverage OpenCTI EE scalability and native threat-sharing and data segregation capabilities to establish an effective Cyber Threat Sharing & Collaboration framework. It enables real-time, bi-directional sharing of vital information with domestic partners and stakeholders, partners in other jurisdictions, national critical infrastructure, and the community.

Such critical capability should include the means to communicate with a broad community through various channels and the information shared can range from strategic threat reports to machine-readable data. which serve to equip Security operations personnel will benefit from the time sensitive information and defensive controls will be significantly enhanced. Lastly it should provide the opportunity for members to share their intelligence and sightings back for broad visibility.

Several government agencies have already adopted OpenCTI EE, leveraging its advanced threat intelligence capabilities to **stay ahead of evolving cyber threats and protect critical infrastructure**. By operationalizing intelligence within a centralized platform, they have improved situational awareness, enhanced threat response efficiency, and strengthened national security resilience.

The Growing Cyber Threat To Government And Defense

As cyber threats escalate at an unprecedented rate, how prepared are you to safeguard your daily operations in the government and defense sectors?

The year 2024 marked a record high for such incidents, posing substantial challenges to national security. Notably, state-sponsored actors like Advanced Persistent Threats (APTs) have been implicated in compromising critical infrastructure networks, further escalating risks to governmental operations. [1]

A particularly alarming development is the rise in ransomware attacks targeting public sector organizations, causing disruptions and financial losses. In 2024, the UK's NCSC reported a 16% increase in hostile cyber incidents [2]. Notably, the ransomware attack in North Miami, Florida, in August 2024 shut down city operations for nearly a week [3]. These attacks underscore the pressing need for robust cybersecurity measures within government agencies.

Compounding these challenges is a significant cybersecurity workforce shortage. In the US, nearly 500,000 positions are currently unfilled [4]. This talent gap weakens cyber defenses, making policy-driven initiatives even more critical.

In response to these escalating threats, governments have introduced key legislative measures aimed at bolstering cyber defenses:

- **UK: Cyber Security and Resilience Bill** – Enhancing national cyber resilience and critical infrastructure protection. [5]
- **US: Cybersecurity Information Sharing Act (CISA)** – Facilitating real-time intelligence-sharing between government and private sectors. [6]
- **Australia: 2023-2030 Cyber Security Strategy** – Strengthening national cybersecurity posture with long-term initiatives. [7]

While these legislative measures are a step in the right direction, addressing cyber threats requires a **comprehensive approach**, where laws work in tandem with **proactive, real-time threat intelligence**.

By operationalizing intelligence, **national CERTs, law enforcement agencies, and defense organizations** can **identify, assess, and neutralize threats before they escalate**. Programs like the **U.S. CISA's operational collaboration model** and **ENISA's Cyber Threat Intelligence (CTI) framework** in Europe show how intelligence-sharing translates policy into action, improving national security in real time.

To outpace evolving cyber threats, **a proactive, intelligence-driven approach is no longer optional—it's essential** to safeguarding national interests.

[1] CISA, PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
[2] Reuters, UK facing increased hostile activity in cyberspace, security official warns. https://www.reuters.com/technology/cybersecurity/uk-facing-increased-hostile-activity-cyberspace-security-official-warns-2024-12-03/
[3] WSJ Pro, Hack on North Miami Tests Ransom Payment Bans. https://www.wsj.com/articles/hack-on-north-miami-tests-ransom-payment-bans-077be398
[4] FOX News, Outgoing WH official calls for US to bolster cybersecurity workforce by hiring non-degree holders. https://www.foxnews.com/politics/outgoing-official-us-cybersecurity-workforce-non-degree-holders
[5] Gov.uk, Cyber Security and Resilience Bill. https://www.gov.uk/government/collections/cyber-security-and-resilience-bill
[6] CISA, Cybersecurity Information Sharing Act of 2015. https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Information%2520Sharing%2520Act%2520of%25202015.pdf
[7] Australian Government Department of Home Affairs, 2023-2030 Australian Cyber Security Strategy. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/2023-2030-australian-cyber-security-strategy

What Does It Mean To Operationalize Threat Intelligence?

Transforming cybersecurity data into actionable insights

Organizations are flooded with cybersecurity data from countless sources, making it difficult to separate noise from meaningful intelligence. **Threat Intelligence Platforms (TIPs)** help cut through the clutter, converting raw data into actionable insights.

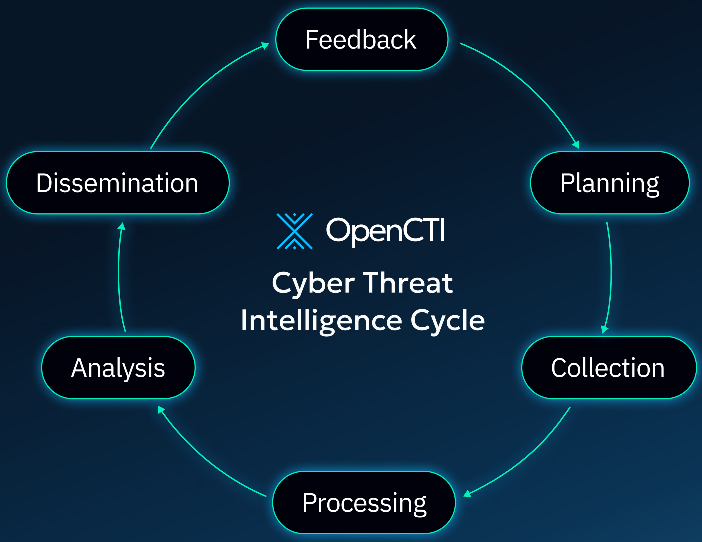
By automating data collection, aggregation, and analysis, TIPs enable security teams to detect, prioritize, and respond to potential threats more promptly. This not only enhances situational awareness but also strengthens proactive defense measures, reducing the risk of cyberattacks. Integrating diverse data streams, TIPs provide context that empowers organizations to stay ahead of evolving threats.

OpenCTI is at the forefront of this transformation. Its open-source Community Edition has gained widespread adoption for its ability to structure, automate, and disseminate threat intelligence. For organizations requiring advanced capabilities, **OpenCTI Enterprise Edition** delivers enhanced automation, governance, scalable access control, and dedicated support—helping security teams build a more adaptive and resilient defense strategy.

The Threat Intelligence Lifecycle

Use OpenCTI Enterprise Edition to successfully implement a Cyber Threat Intelligence capability and lifecycle in your organization. The cyber threat intelligence lifecycle is **a continuous and iterative process** organizations use to gather, analyze, and utilize threat intelligence to enhance their cybersecurity posture.

Below is an explanation of each stage:



1.DIRECTION AND PLANNING

Purpose: This initial stage involves setting the goals and objectives for the threat intelligence program. It includes defining the necessary information, identifying the stakeholders, and determining the scope and priorities.

Activities: Establishing requirements, deciding on intelligence priorities, and creating a collection plan.

Outcome: A clear set of objectives and a strategic plan for collecting and analyzing threat intelligence.

2. COLLECTION AND COMPILATION

Purpose: This stage focuses on gathering raw data and information from various sources. The data collected should align with the intelligence requirements established during the planning stage.

Sources: Open sources (OSINT), internal data, threat feeds, dark web, social media, and partnerships.

Outcome: A repository of raw threat data that will be processed and analyzed.

3. PROCESSING

Purpose: In this stage, the raw data collected is processed and transformed into a usable format. This includes filtering out irrelevant information and normalizing data for consistency.

Activities: Data cleaning, structuring, deduplication, and enrichment.

Outcome: Structured and organized data ready for in-depth analysis.

4. ANALYSIS AND REVIEW

Purpose: This is the core stage where the processed data is analyzed to produce actionable intelligence. Analysts interpret the data to identify patterns, trends, and potential threats.

Activities: Correlating data points, identifying indicators of compromise (IOCs), developing and testing threat hypotheses using structured analytic techniques, and incorporating broader activities—such as threat actor profiling, assessing geopolitical impacts, and mapping threats to frameworks like MITRE ATT&CK—to understand emerging threats.

Outcome: Actionable threat intelligence reports that provide insights into potential and emerging threats.

5. DISSEMINATION AND SHARING

Purpose: The analyzed intelligence is shared with the relevant stakeholders and disseminated to technical cybersecurity systems within the organization. This ensures that decision-makers and security teams are informed and can take appropriate actions but also allows detection / prevention systems to be more efficient.

Activities: Reporting findings, creating alerts, and distributing intelligence through appropriate channels.

Outcome: Informed stakeholders on how to implement security measures based on shared intelligence and supercharged cybersecurity detection / prevention systems with fresh, high fidelity, and accurate technical cyber threat intelligence.

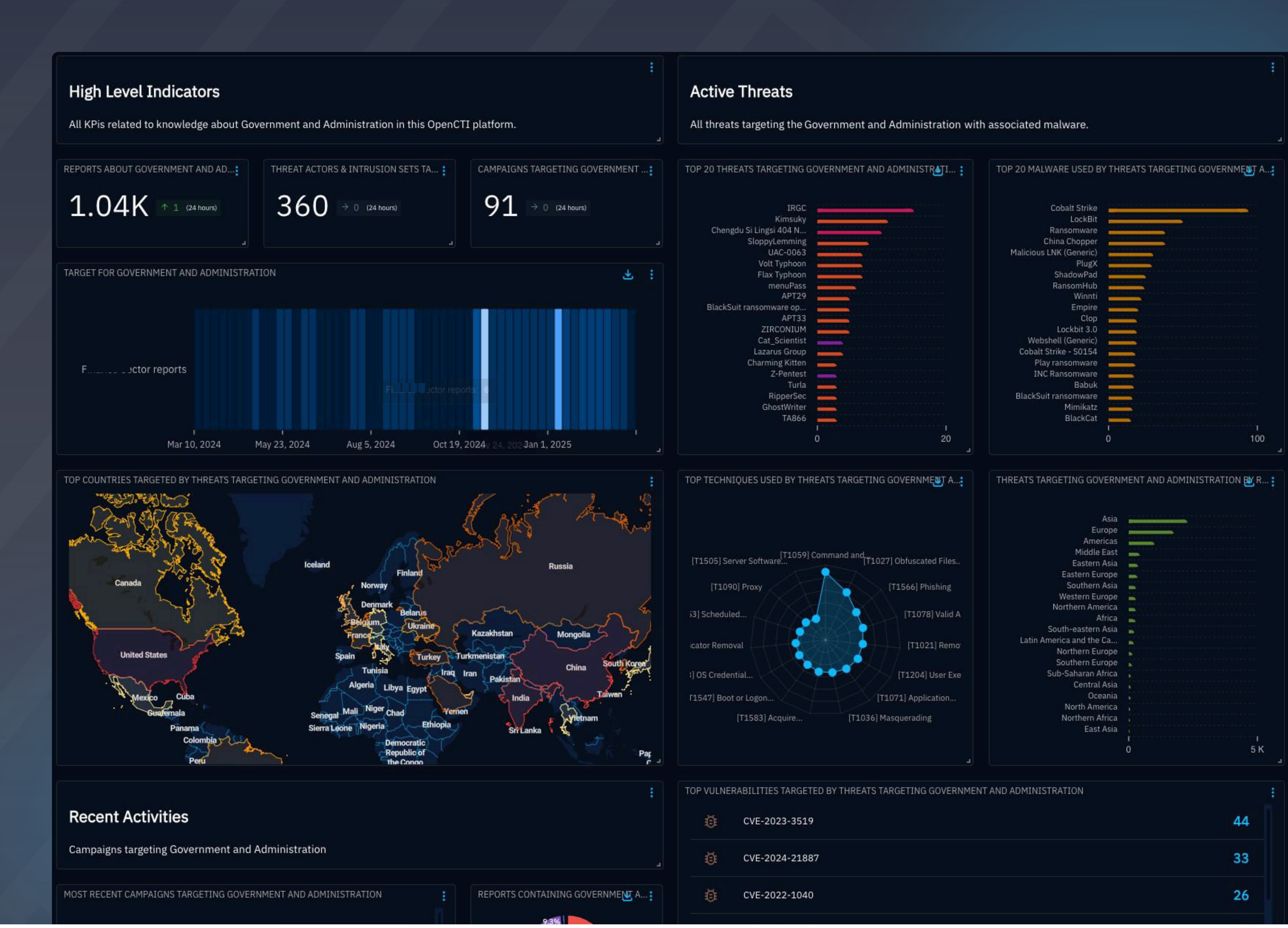
6. FEEDBACK & CONTINUOUS IMPROVEMENT

Purpose: This final stage focuses on evaluating the effectiveness of the threat intelligence process and making continuous improvements. Stakeholder feedback is collected to refine and enhance the intelligence lifecycle.

Activities: Collecting feedback, assessing the impact of intelligence, and updating processes and strategies.

Outcome: An improved and evolving threat intelligence program that adapts to new threats and changing requirements.

The threat intelligence lifecycle is an ongoing process that helps organizations stay ahead of cyber threats by continuously collecting, processing, analyzing, and sharing threat information. By iterating through these six stages, organizations can enhance their threat detection capabilities, improve their response strategies, and strengthen their overall cybersecurity posture.



High Level Indicators

All KPIs related to knowledge about Government and Administration in this OpenCTI platform.

Active Threats

All threats targeting the Government and Administration with associated malware.

REPORTS ABOUT GOVERNMENT AND AD...	THREAT ACTORS & INTRUSION SETS TA...	CAMPAIGNS TARGETING GOVERNMENT ...
1.04K ↑ 1 (24 hours)	360 → 0 (24 hours)	91 → 0 (24 hours)

Recent Activities

Campaigns targeting Government and Administration

TOP VULNERABILITIES TARGETED BY THREATS TARGETING GOVERNMENT AND ADMINISTRATION

CVE-2023-3519	44
CVE-2024-21887	33
CVE-2022-1040	26

Why OpenCTI EE Is Uniquely Positioned For Government

Introducing OpenCTI

At Filigran, it is our mission to **operationalize cyber threat intelligence across the organization** by bringing together external and internal information through deep technical integrations and turn this information into meaningful, actionable insights.

OpenCTI is the flagship platform under Filigran's **(XTM) Extended Threat Management Suite**. It is a highly scalable, flexible, and innovative open-source platform, and its primary role is consolidating and organizing intelligence about known and emerging threats and observables into one accessible location. This consolidation offers invaluable insights at the strategic level and enables the operational integration of intelligence across various cybersecurity platforms, enhancing organizational readiness and response capabilities.

OpenCTI is a critical capability for organizations seeking to adopt a more proactive intelligence-led approach to cybersecurity that leverages enhanced contextual awareness, automation and data-driven decision making.

The automation component emphasizes reducing manual intervention by using data-driven insights to propose decision-ready scenarios, highlight priorities, and assess the impact of various threats. OpenCTI is critical here, providing the necessary data for effectively evaluating cybersecurity postures and planning.

As a fully independent and contained platform, OpenCTI can be deployed on-premises, as SaaS or in air-gapped environments, or using a hybrid model, and is highly customizable to align with organizations' processes and workflows across different teams such as CTI, Threat Hunting, SOC, DFIR, Vulnerability Management and Purple Teams.

OPENCTI ENTERPRISE EDITION UNIQUE FEATURES

As an **all-in-one platform**, OpenCTI EE includes all the following in one software package: Threat Intelligence Management, Threat Hunting, Incident Response, Investigations, Case Management, Automation & Playbooks, and Threat Sharing. It supports a high degree of customization. And the fully self-contained platform that can operate entirely on-premises, in isolation. It does not require central processing or enrichment or require 3rd party resources (e.g. central vendor infrastructure) to operate.

Some of our key features include:

- **Unlimited use subscription**: OpenCTI EE supports unlimited users, organizations, integration of feeds and enrichment sources, unlimited playbooks.
- **Standardization**: full alignment with and implementation of STIX 2.1, ensuring data integrity and no loss of objects or context during threat sharing.
- **Threat sharing**: a wide variety of collaboration capabilities to disseminate intelligence (human and machine readable) within highly distributed environments or with partner agencies, industry or the public; as well as powerful mechanisms for communication and collaboration between entities.
- **Native built-in air-gap**: our scalable and flexible architecture allows cyber threat intelligence deployments across security domains.
- **Integrated solution**: OpenCTI EE is able to ingest various formats of structured and unstructured data, lending itself for multiple use cases e.g. internal CTI, all-source-intelligence platforms to support operators during deployment and Foreign Information Manipulation and Interference (FIMI)

MINI USE CASE

AUTOMATED THREAT SHARING FOR NATIONAL CERTS

CERTs use platforms like OpenCTI to automatically share cyber threat indicators (e.g., malicious IPs, phishing domains) with other national and international cybersecurity teams.

For example, when a phishing campaign targets government employees, the national CERT can immediately shares details with banks, telecom providers, and other essential services to block the threat.

OPENCTI EE ALLOWS ORGANIZATIONS TO SOLVE THE FOLLOWING PROBLEMS

- Limited understanding of the evolving threat landscape
- Meaningless, un-prioritized alerts in their SIEM
- SOC analysts are highly reactive and not proactive due to limited situational awareness, context and visibility.
- No mechanism in place to aggregate, process and analyze data at scale and at speed.
- A cyber threat intelligence capability that is not operationalized
- Limited or no means to share and collaborate threat intelligence with their internal and external stakeholders, and peers in the industry.

OPENCTI EE ASSISTS ORGANIZATIONS TO ACHIEVE THE FOLLOWING OUTCOMES

- Better understand its adversaries, their tactics and techniques and the threats that are targeting their organization, industry, geography and supply chain or ecosystem.
- Improve efficiency of security operations – increased awareness and respond more effectively when an indicator of compromise is detected
- Leverage insights to inform cyber security strategy, cyber resilience planning and testing.
- Collaborate with peers and exchange valuable insights with internal and external stakeholders.
- Increase the level of preparedness and overall resilience

OpenCTI EE fosters a collective defense approach, enabling organizations to stay ahead of evolving threats. Thanks to its open source nature, the code of OpenCTI is available for end-to-end code review and inspection. The OpenCTI EE key capabilities make it the definitive choice for government and defense sector seeking a cutting-edge, intelligence-driven cybersecurity strategy.

Why OpenCTI EE is uniquely positioned and the de facto global standard for Governments and Defense sectors

MULTIPLE CLASSIFICATION SCHEMES IN PARALLEL

We worked on a design for a recent project that was to accommodate intelligence sharing between a large number of coalition partners, part of which entailed supporting multiple simultaneous classification marking systems, including US CUI, AGSCS, and TLP for commercial feeds.

OpenCTI supports multiple hierarchical schemes to be defined and used simultaneously, so we were able to retain the marking of each document and manage ABAC per group and user on that basis. Notes and sightings were also classified in this way, and since this is part of the STIX standard, the markings would travel with the data through standard import/export.

We have a third-party application that would manage dissemination based on markings for documented synchronized over low-bandwidth, high-latency links, and also performed any marking mappings required. However, OpenCTI EE could use the built-in playbooks to filter and add/replace markings if using specific contents or criteria to process these.

MINI USE CASE

LEVERAGE INTEL TO FIGHT AGAINST CYBER CRIMES

Law enforcement agencies use cyber threat intelligence to prevent, investigate, and respond to cyber crimes. They work with cybersecurity experts, private companies, and international partners to track down cybercriminals and protect the public.

If a police cyber unit receives intelligence about a phishing campaign targeting local businesses, they can work with banks and internet providers to shut down fraudulent websites, warn potential victims, and trace the criminals behind the attack.

DELEGATING USER MANAGEMENT TO SUB-ORGANIZATIONS ON THE PLATFORM

For our larger users, we were asked to allow delegation of user administration to administrators of specific sub-organizations on the platform. This allows a platform to have multiple sub-organization administrators on the same platform who can undertake user administration directly, without being granted full platform administration that might include platform configuration or administration of users outside their own organization.

MODEL CHANNELS AND ENTITIES RELATING TO FIMI

During 2022 - 2023, OpenCTI was modified to include supporting Channels for FIMI tracking and reporting. This feature was added specifically to address FIMI intelligence, which was adopted by the EU-CERT and US Government, including the Channel Entity type, and later DISARM as an Attack Pattern Framework modelled similarly to ATT&CK and LMKC.

For the Threat Intelligence community, defending against disinformation and Foreign Information Manipulation & Interference (FIMI) requires efficient knowledge sharing. The OpenCTI platform is one of the most advanced and performant solutions to support this critical effort.

CUSTOMIZABLE RETENTION POLICY

In 2024 the ability to customize retention policy on an instance using any property of the indicator was added. This allowed specific types of entity - such as atomic indicators from internal, high-confidence-high-trust sources - to be retained for a longer period than for lower-confidence noisier sources. These conditions include the creator, author, itype, marking, and most other properties, and layer on top of the existing decay curve for indicators, which are also based on itype and filter conditions.

MINI USE CASE

MANAGE CLASSIFIED INFORMATION

Defense agencies handle sensitive intelligence that must be carefully managed. They use **air-gapped networks**, completely isolated from the internet to analyze possible threats, protect classified data while creating and sharing intelligence at different security levels. This approach enables cyber units to prevent leaks.

MINI USE CASE

SHARE KNOWLEDGE WITH SELECTED PARTNERS

Intel agencies monitor and track cyber operations by foreign adversaries, helping to prevent cyber espionage and cyber warfare.

When a national intelligence agency identifies a foreign hacking campaign targeting critical infrastructure, that intelligence agency can use OpenCTI to analyze the attack methods, create a classified report for top government officials, and provide a declassified version to key private-sector partners to help them strengthen defenses.

Extend the ecosystem

OpenCTI is designed to empower the entire cybersecurity ecosystem—not just advanced users—by making threat intelligence more **inclusive, accessible, and actionable**. Government agencies can extend their threat-sharing capabilities to reach a broader network, ensuring that organizations of all sizes and maturity levels can contribute to and benefit from a collective defense approach.

With OpenCTI, participation in cyber threat intelligence in the government and defense sector is possible at any stage of maturity:

Foundational stage	Organizations can start by accessing shared reports hosted in the main OpenCTI EE environment, gaining critical insights without requiring complex infrastructure.
Developing stage	Organizations who are more comfortable in using threat intelligence can establish their own machine-based exchanges using OpenCTI Community Edition and seamlessly link with the main EE instance.
Advanced stage	For highly mature entities, OpenCTI EE offers a fully integrated platform to leverage advanced threat intelligence capabilities while remaining connected to the broader intelligence-sharing ecosystem.

By bridging organizations at different maturity levels, OpenCTI creates **a unified and collaborative defense fabric** where all stakeholders—critical infrastructure, government agencies, and private organizations—can actively contribute to a more resilient cybersecurity landscape.

Filigran's Strategic Partnerships

With Governments, Intelligence Agencies, Law Enforcement, and Defense

FEDERAL BUREAU OF INVESTIGATIONS

The FBI and Filigran collaborate and co-design on OpenCTI to combat cybercrime and provide timely information to the public on emerging threats, leveraging Cyber Threat Intelligence (CTI) used by thousands of its field agents.

Read more

EUROPEAN UNION (EEAS)

The EU has adopted a common standard for analyzing and exchanging structured threat information on Foreign Information Manipulation and Interference (FIMI), through a more interoperable and machine-readable approach. Information is shared more efficiently, and with a greater level of detail when it comes to understanding the manipulative tactics, techniques and procedures of FIMI disinformation campaigns. The standard used to analyze and share information is built on the DISARM framework, the STIX standard and the OpenCTI platform.

Read more

With Industry & Standards Organizations

OASIS OPEN – CYBER THREAT INTELLIGENCE

At Filigran we focus heavily on the application and operationalization of Cyber Threat Intelligence, and we have a long history of supporting the development and adoption of the STIX standard. The OpenCTI platform fully aligns with the STIX 2.1 standard, and as a member of the OASIS CTI Technical Community we actively contribute to the advancement and enrichment of the STIX standard, as well as TAXII and other emerging standards.

Read more

OASIS OPEN – DAD-CDM

Since 2022 Filigran has taken a leadership role with partners OASIS, DISARM Foundation and others to develop a data model to identify and share data related to disinformation and interference. Filigran is a founding member of the Defending Against Disinformation Common Data Model project. The DAD-CDM serves as a valuable resource, particularly in the identification and alerting of vast disinformation and interference activity and AI-empowered attacks. Jean-Philippe Salles, VP Product at Filigran, is the co-chair of the DAD-CDM Project Governing Board (PGB).

Read more

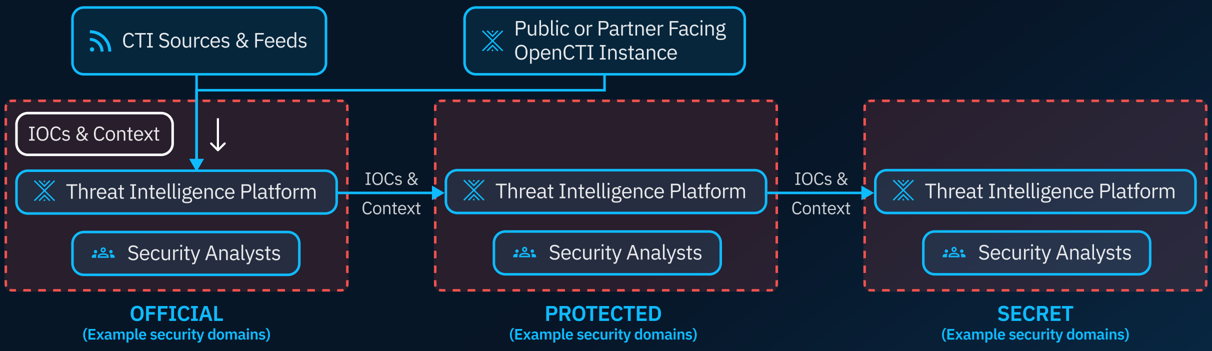
Deployment Options

OpenCTI EE is commonly used by Government, Law Enforcement and Defense organizations for its **scalability** and **highly flexible architecture** to deliver a variety of use cases, including **airgap environments** and **threat sharing and collaboration frameworks**.

OpenCTI EE can be deployed **on-premises** as a self-hosted, self-managed solution, or on **Filigran SaaS** in a dedicated, private tenants, or via Cloud Provider Marketplace where it deployed in the customer's account but delivered as SaaS. All options are the same OpenCTI EE version, Filigran does not favor or prioritize one deployment option over the other.

OPENCTI EE NATIVELY SUPPORTS AIRGAP ENVIRONMENTS

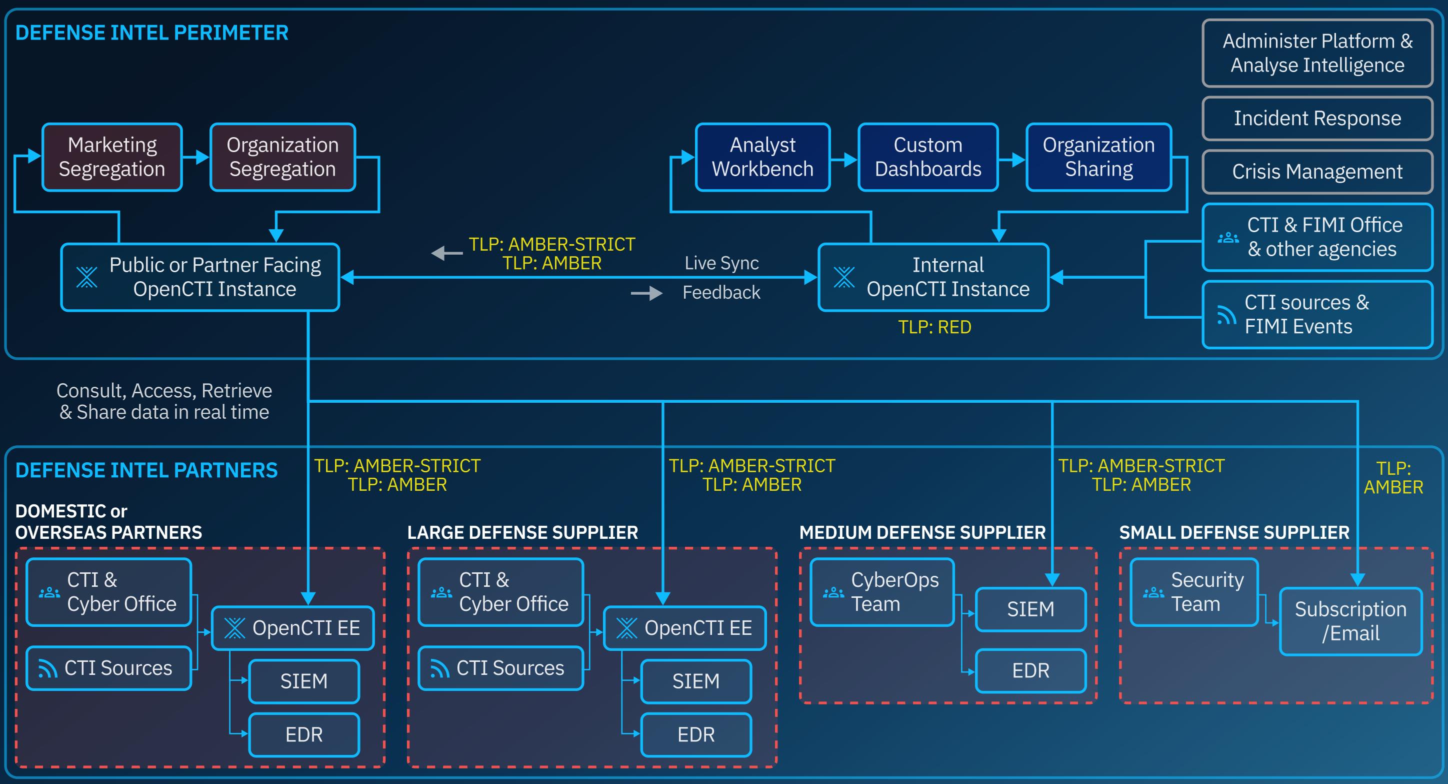
The CTI Ecosystem supports the ingestion, processing, analysis, and transmission of data across multiple security domains and zones. OpenCTI natively supports transmission through data diodes in airgap environments. The multiple platforms are typically deployed on-premises.



CTI Sources & Feeds
Public or Partner Facing OpenCTI Instance
IOCs & Context
Threat Intelligence Platform
Security Analysts
IOCs & Context
Threat Intelligence Platform
Security Analysts
IOCs & Context
Threat Intelligence Platform
Security Analysts
OFFICIAL
(Example security domains)
PROTECTED
(Example security domains)
SECRET
(Example security domains)

OPENCTI EE NATIVELY SUPPORTS THREAT SHARING AND COLLABORATION WITH PARTNERS OR THE PUBLIC

A broad variety for sharing using public dashboards, custom dashboards per organization or user group, FRI & feedback, sharing of machine-readable data via multiple methods. Partner instance can be on-premises or SaaS.



Strengthening Cyber Resilience with OpenCTI EE

Operationalizing threat intelligence is no longer optional for governments and defense agencies around the world. With OpenCTI Enterprise Edition, these entities can streamline intelligence gathering, automate workflows, and enhance collaboration, ensuring faster and more effective responses to cyber threats.

As cyber risks grow in scale and sophistication, now is the time to strengthen threat intelligence capabilities. Proactive defense requires robust, scalable, and actionable intelligence to stay ahead of adversaries.

Take the next step today. Contact Filigran for a consultation, **request a demo** of OpenCTI EE, or explore additional resources below to see how intelligence-driven cybersecurity can transform your defense strategy.

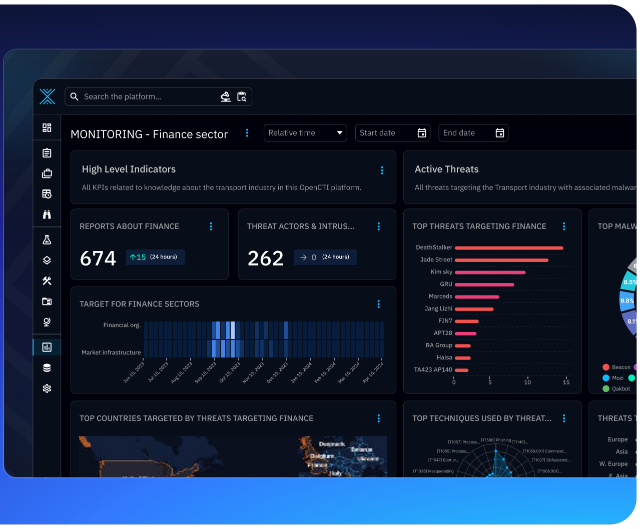
ADDITIONAL RESOURCES

- ✓ More about OpenCTI Enterprise Edition
- ✓ Explore further: Intelligence Driven SOC
- ✓ Explore further: Threat Monitoring and Hunting
- ✓ Explore further: Intelligence-driven defense against disinformation
- ✓ Explore further: Intelligence-led Breach and Attack Simulation

Future-proof your cybersecurity

Investing in OpenCTI Enterprise Edition is not just an upgrade in technology—it's a strategic move to future-proof your organization and simplify the complexities of modern cybersecurity.

Get started today



MONITORING - Finance sector

High Level Indicators

All KPIs related to knowledge about the transport industry in this OpenCTI platform.

Active Threats

All threats targeting the Transport industry with associated malwar

REPORTS ABOUT FINANCE: 674 ↑15 (24 hours)

THREAT ACTORS & INTRUS...: 262 → 0 (24 hours)

ABOUT FILIGRAN

Filigran stands out for its expertise in open-source cybersecurity solutions and offers the **Filigran eXtended Threat Management (XTM)** suite to help organizations anticipate cyberattacks and manage threats end-to-end. The suite currently includes two solutions: **OpenCTI**, threat intelligence platform to operationalize holistic threat intelligence; and **OpenBAS**, breach and attack simulation platform to identify critical security gaps and strengthen organizational security posture. Filigran solutions are now trusted by over 6,000 public and private organizations worldwide.

Filigran employs over 80 team members globally, dedicated to supporting leading companies such as Marriott, Thales, Hermès, Airbus, Novartis, and Bouygues Telecom, as well as public sector entities like the European Commission, ENISA, ANSSI, the New York State Cyber Command, and various American and Australian federal agencies. Filigran has also established a strong partner ecosystem with companies like Deloitte, Orange Cyberdefense, Deepwatch, Arctic Wolf, Google Cloud Security, Atos, Wavestone, and Intrinsec.

Filigran

contact@filigran.io |