WHITE PAPER

Filigran

Operationalizing Threat Intelligence for National Security

Executive summary

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:

OpenCTI

OpenCTI is an open-source platform that helps organizations structure and operationalize their holistic cyber threat intelligence. Designed for cybersecurity teams, it enables the anticipation of future attacks by contextualizing, storing, and using threat information across technical, operational, and strategic levels.

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.

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.

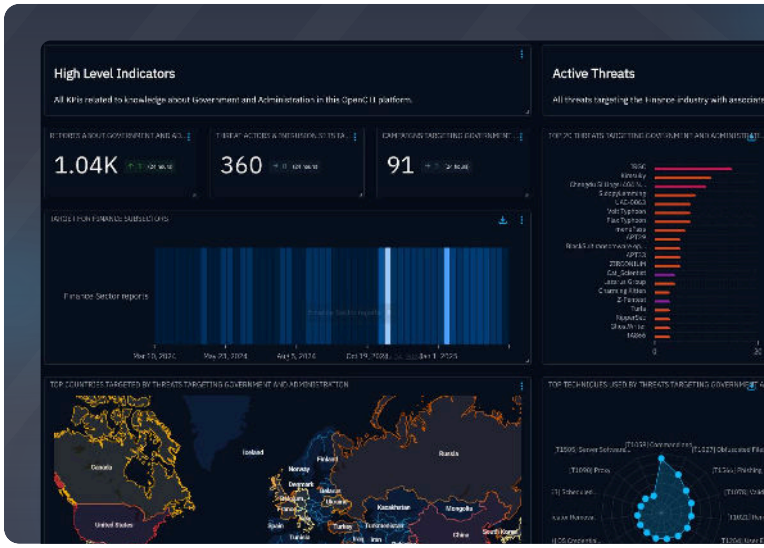
OpenCTI EE **automates the correlation of cyber threats across classified and open-source intelligence**, linking IOCs to known **adversary tactics, techniques, and procedures (TTPs)**. This allows agencies to attribute threats to specific state actors, predict their next moves, and strengthen preemptive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



Conclusion

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.

Explore the comprehensive capabilities of OpenCTI Enterprise Edition

Learn more

Gain deeper insights, demos, and live Q&A with our expert, Damian Skeeles, Jermain Njemanze and Danial Kamran.

Join our Webinar Series

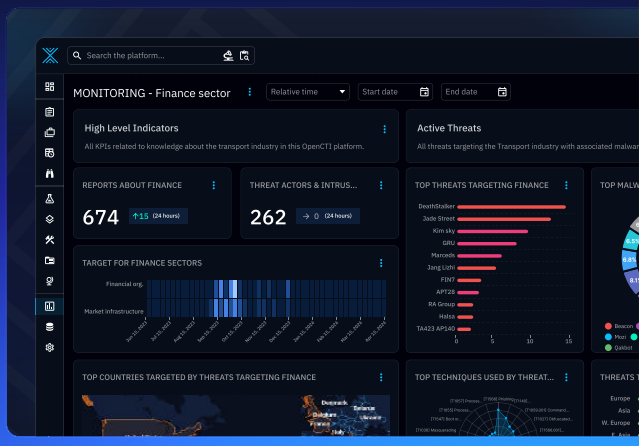
Learn how OpenCTI supports defense against disinformation and Foreign Information Manipulation & Interference (FIMI) with efficient knowledge sharing.

Discover use cases

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



ABOUT FILIGRAN

Filigran, a cybertech company founded in 2022, offers open-source cybersecurity solutions covering end-to-end threat intelligence management, attack simulations, and security posture validation for organizations.

Filigran

contact@filigran.io |