Unified Exploit Intelligence Management:

Automating Emerging Threat Response with VulnCheck and Filigran

The Challenge

Security teams are overwhelmed by the constant flood of new vulnerabilities, many of which are never exploited. Without context, teams struggle to determine which CVEs pose a real risk to their organization. Traditional vulnerability scanning lacks active threat and exploit intelligence, leading to wasted resources, alert fatigue, and delayed remediation. Cyber defenders need both context and clarity to act quickly and precisely.

Why OpenCTI + VulnCheck?

Filigran's OpenCTI platform is an open-source threat intelligence solution that enables organizations to centralize, visualize, and operationalize cyber threat data. Through its native support for STIX 2.1 and graph-based intelligence, OpenCTI provides a unified view of threat actors, malware, campaigns, and vulnerabilities. This allows organizations to prioritize threat intelligence based on a threat landscape that's relevant to them.

VulnCheck feeds enrich the OpenCTI platform with real-time, actionable exploit and vulnerability intelligence. The VulnCheck connector for OpenCTI automatically ingests and structures exploit timelines, KEVs, EPSS scores, threat actor usage, botnet activity, and more, giving defenders immediate context on which CVEs are actively exploited in the wild and by whom.

Key Benefits

Integrated Intelligence
Centralize vulnerability and threat actor data in OpenCTI without manual triage across tools and teams.

Context-Rich Vulnerability Graphs
Understand who's exploiting what, how, and when via STIX objects in OpenCTI's knowledge graph.

Faster, Smarter Response
Gain early warning indicators and timelines for emerging threats and exploit development.

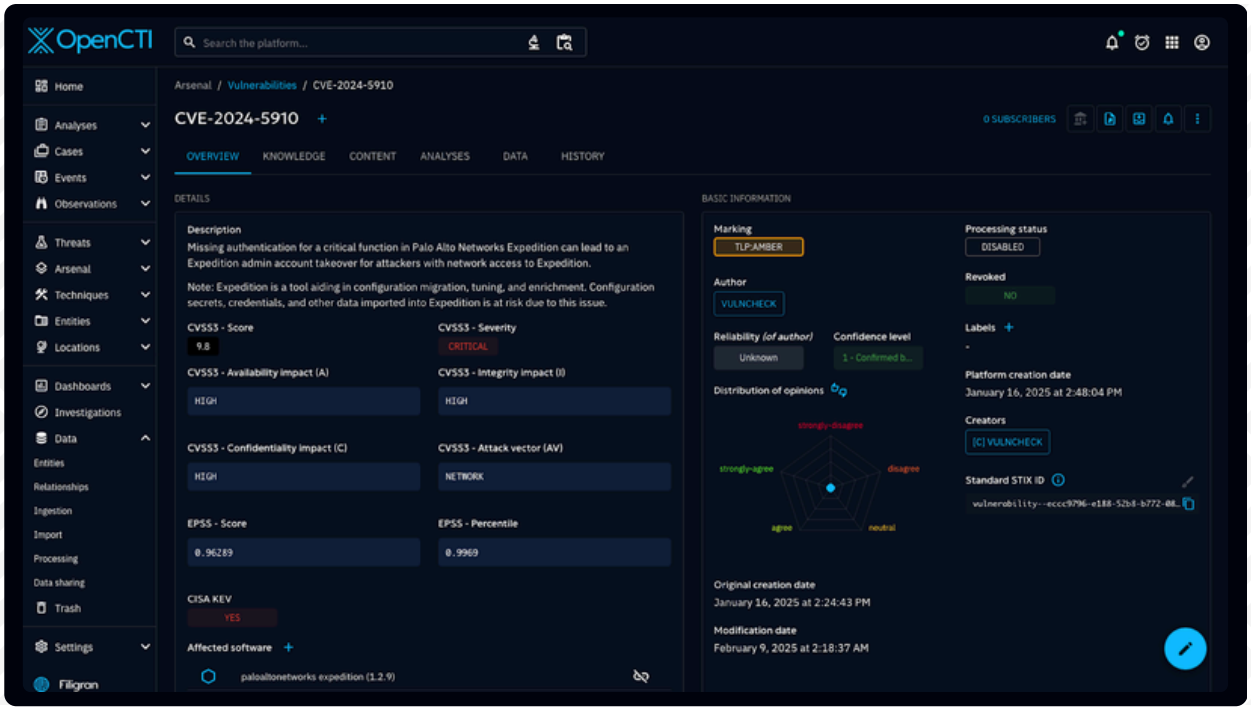
Threat-Driven Prioritization
Focus remediation efforts on CVEs with known exploitation, using KEV and EPSS enrichment from VulnCheck.

Get Results with VulnCheck + OpenCTI

With VulnCheck integrated into OpenCTI, organizations gain a unified, enriched intelligence environment. The VulnCheck connector delivers vulnerability metadata (CVSS, CPE, CISA KEV), exploit activity, initial access methods, IP and botnet context, and threat actor links, structured automatically into STIX 2.1.

Supported use cases include:

- Exploit-Centric Vulnerability Management
- Emerging Threat Monitoring
- Threat Actor Attribution
- Incident Enrichment & Response



How to Get Started

The VulnCheck connector for OpenCTI can be deployed using OpenCTI's standard connector framework. Visit vulncheck.com or filigran.io to learn more and request a demo.

About VulnCheck

VulnCheck delivers next-generation exploit and vulnerability intelligence solutions for enterprise, government and product teams to prevent large-scale remote code execution events with better, faster exploit data, massive-scale real-time monitoring and predictively-built detection artifacts. VulnCheck's 300M+ unique data from 400+ sources points help vulnerability management and response teams outpace adversaries - autonomously.

About Filigran

Filigran, founded in September 2022, stands out in the cybertech ecosystem for its commitment to revolutionizing end-to-end cyber threat management. Its mission is to develop proactive open source solutions, designed to empower cybersecurity teams to anticipate attacks before they materialize and better manage their cyber threat risks. Filigran solutions are used by over 6,000 public and private organizations worldwide.