WHITE PAPER

Filigran

A Practical Guide to Threat-Informed Defense

Executive summary

As modern organizations evolve and grow more complex, their digital ecosystems become increasingly vulnerable. The expansion of attack surfaces and the sophistication of cyber threats are accelerating, rendering traditional security approaches inadequate and outdated.

This paper explores how **Threat-Informed Defense (TID)**, a methodology promoted by MITRE, offers a proactive, intelligence-driven approach to cybersecurity. By aligning security operations with real-world adversary behaviors, TID enables organizations to prioritize defenses, validate controls, and continuously adapt to emerging threats.

The paper introduces a practical, six-stage **Threat-Informed Defense pipeline** developed by Filigran, designed specifically for the operational realities of modern organizations. It demonstrates how tools like **OpenCTI** and **OpenAEV** can be used to operationalize threat intelligence, simulate adversary behavior, and drive strategic security investments.

Through use cases such as cloud infrastructure protection and ransomware defense, the paper illustrates how Threat-Informed Defense transforms threat data into actionable insights!

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.

OpenAEV

OpenAEV is an open-source platform for organizations to plan and conduct crisis management exercises by simulating real-life attack scenarios and optimizing cyber defense.

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 2025 All rights reserved.