Filigran

REPORT

Cyberthreats in the Financial Sector:

Exploring the 2025 evolving threat landscape and how to stay resilient in 2026

Table of Content

Introduction

In 2025, the **financial sector** faced accelerated **digital transformation**, growing geopolitical tension, and increased regulatory scrutiny. Institutions were required to maintain availability, data security, and **operational resilience** while adopting new technologies like artificial intelligence, open banking, and cloud-native systems – however, this same transformation attracted both old and new cyber threat activities, which continue to rise in volume and sophistication

Whether in retail banking, asset management, or insurance, for executive leaders in the financial sector, **cybersecurity is now a major business risk**, affecting financial stability, compliance, customer trust, and enterprise value.

This report explores why the sector remains a frequent target, key **cyber threat trends** in identified in 2025, evolving regulations, and how **intelligence-driven threat management platforms** have become vital in maintaining security resilience.

Executive Summary

- In 2025, the financial sector remained one of the most targeted industries globally, with **90% of breaches driven by financial gain**. Data breaches accounted for **64% of incidents**, while ransomware represented **36%**, costing institutions an average of **USD 5.56 million per breach**, making finance the **second most expensive industry** for cyber incidents.
- Artificial intelligence has reshaped the **financial threat landscape**, accelerating exploitation timelines and enabling sophisticated **fraud and social engineering**. Unmanaged "**shadow AI**" introduces compliance and data leakage risks, with **20% of AI-related incidents linked to shadow AI** and **97% of affected organizations lacking proper access controls**.
- **Supply chain compromise** is now systemic, with third-party involvement in **30% of breaches**, highlighting the cascading impact of vulnerabilities across interconnected ecosystems. **Ransomware** remains highly disruptive, affecting **12.8% of B2B financial organizations**, often using **double extortion** tactics that trigger regulatory reporting and prolonged recovery.
- Regulatory frameworks such as **DORA** have shifted resilience from aspiration to obligation. Financial institutions must now demonstrate **intelligence-led risk management**, threat-led penetration testing, and robust **third-party oversight**. Failure to comply exposes organizations to escalating **regulatory, financial, and reputational risks**.
- In 2025, leading bank executives, central banks, and international financial authorities increasingly characterized **cybersecurity as a primary threat to financial stability**, emphasizing systemic exposure, **third party concentration**, and the need for **resilience driven approaches** rather than isolated technical controls
- Financial institutions seeking to demonstrate **regulatory compliance** must not only develop a deep understanding of their **threat landscape**, but also establish the means to **continuously test and validate their defenses.**

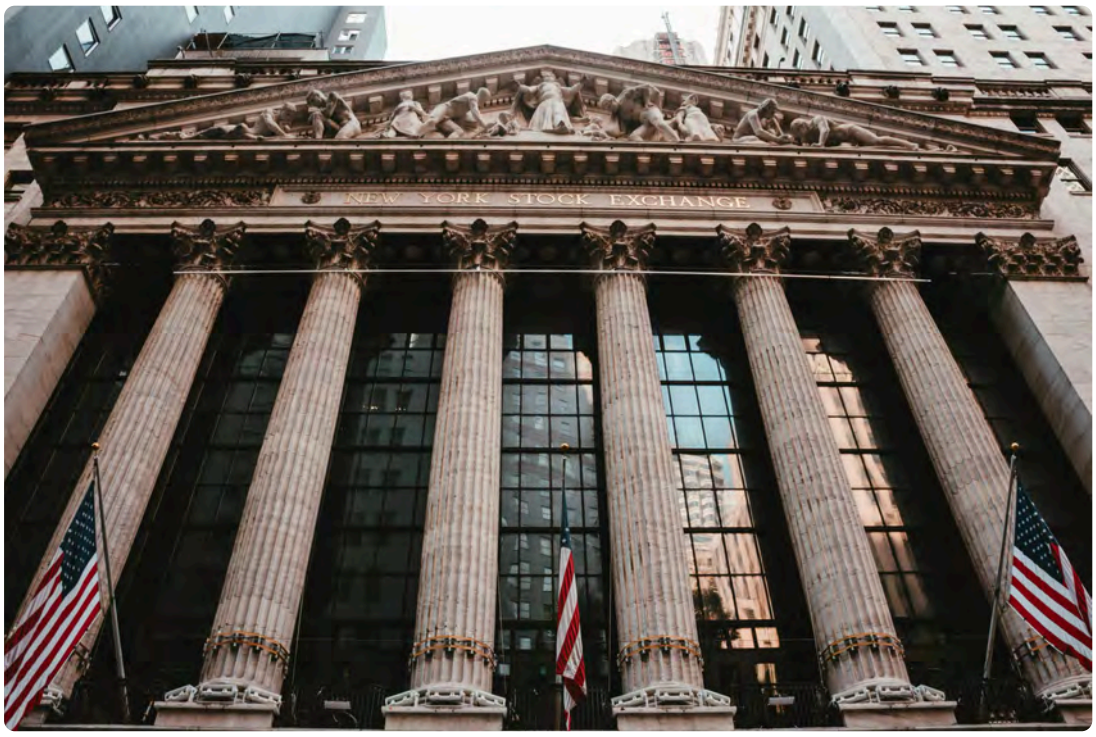


Photo by Aditya Vyas from Unsplash

Why the Financial Sector Remained a Prime Target in 2025

Financial institutions remain among the most attractive targets for cyber threat actors due to the concentration of high-value assets, sensitive data, and systemic importance they represent. Banks, insurers, payment service providers, and investment firms process and store vast quantities of personally identifiable information, financial account data, authentication credentials, and proprietary business intelligence. In 2025, data-driven attacks dominated the threat landscape, with **data breaches accounting for approximately 64% of incidents** impacting the financial sector, while ransomware activity represented roughly 36% of reported cases [1].

The primary motivation behind these attacks remains **financial gain**. Approximately 90% of breaches affecting financial institutions in 2025 were financially motivated, with espionage-related activity representing a smaller but increasing proportion [4].

The primary motivation behind these attacks remains financial gain. Approximately 90% of breaches affecting financial institutions in 2025 were financially motivated

Attackers frequently seek to monetize access through fraudulent transactions, credential resale, identity theft, or extortion schemes. The types of data most compromised included **personal data (54%)**, internal organizational data (35%), and credentials (22%), reflecting a clear emphasis on enabling downstream fraud and persistent access [4].

The methods used to achieve initial compromise further underline the sector's exposure. **Hacking techniques** accounted for 45% of breaches, **malware** for 37%, and **social engineering** for 25%, demonstrating that threat actors continue to exploit both technical vulnerabilities and human factors at scale [4]. These attack vectors are particularly effective in complex financial environments where legacy infrastructure, third-party dependencies, and high transaction volumes coexist.

"The biggest risk to me is cyber."

— Jamie Dimon, CEO of JPMorgan Chase, interview on the Acquired podcast, July 2025

Beyond direct financial losses, the systemic nature of the financial sector amplifies the consequences of cyber incidents. Disruptions to payment systems, trading platforms, or core banking services can propagate rapidly across markets, affecting counterparties and customers far beyond the initially impacted institution. This systemic risk is reflected in breach cost metrics, with the financial sector remaining the **second most expensive industry for data breaches in 2025**, with an average cost of USD 5.56 million per incident [8]. Regulatory penalties, remediation costs, operational downtime, and reputational damage all contribute to this elevated impact profile.

5.56M

USD millon per incident

Average cost of data breaches in 2025 in the financial sector.

AI Generated Image

Top Cyber Threat Trends That have affected the Financial Sector in 2025

Artificial intelligence reshaping the threat landscape

Artificial intelligence has emerged as one of the most transformative forces in the 2025 cyber threat landscape. Its impact is not limited to a single attack vector but spans multiple fronts, fundamentally altering how threat actors identify targets, execute campaigns, and evade detection. In the financial sector, AI has accelerated attack speed, increased operational scale, and introduced new classes of risk tied to both malicious use and unmanaged adoption. Three developments in particular have defined AI's influence in 2025: the rise of **AI-enhanced cyberattacks**, the weaponization of generative AI for fraud and social engineering, and the growing prevalence of **shadow AI** within organizations. [2,3,8]

INCREASED ATTACK SOPHISTICATION FROM AI-ENHANCED CYBERATTACKS

Threat actors in 2025 increasingly integrated AI into core stages of the attack lifecycle, including reconnaissance, vulnerability discovery, exploitation, and post-compromise activity. Automated vulnerability scanning powered by **machine learning significantly reduced the time between vulnerability disclosure and active exploitation**. This compression of attacker timelines has proven especially challenging for financial institutions operating large and heterogeneous IT environments.

Advanced malware observed in 2025 demonstrated greater adaptability, with some strains capable of dynamically altering behavior during execution in response to detected security controls. This emerging class of **adaptive or agentic malware** complicates signature-based detection and places additional pressure on behavioral and intelligence-driven defenses. AI-assisted automation also enabled attackers to scale campaigns horizontally, reaching larger numbers of financial targets with minimal incremental cost. [3,5,6,8]

The implications for the sector are significant. Faster exploitation cycles reduce the effectiveness of traditional patch management processes, while adaptive malware increases **dwell time** and lateral movement opportunities. Over time, this trend is likely to widen the gap between attackers capable of leveraging AI and organizations that lack mature **detection and response capabilities**.

> "A thing that terrifies me is apparently there are still some financial institutions that will accept the voiceprint as authentication. That is a crazy thing to still be doing. AI has fully defeated that."
>
> — Sam Altman, CEO of OpenAI, speaking at a U.S. Federal Reserve conference (July 2025)

GENERATIVE AI ENABLING FRAUD AND SOCIAL ENGINEERING

Generative AI has had a particularly pronounced impact on fraud and social engineering campaigns targeting financial institutions and their customers. In 2025, phishing, business email compromise, and invoice fraud campaigns increasingly leveraged AI-generated content that was contextually accurate, linguistically fluent, and tailored to specific individuals or organizations, effectively eliminating many of the **telltale indicators** that traditional security awareness training and email filtering solutions relied upon [3,5].

During the same period, **deepfake technologies** matured significantly, enabling realistic voice and video impersonation of executives, relationship managers, or trusted third parties. In several documented cases, attackers used synthetic voice or video to pressure employees into authorizing urgent transactions or disclosing sensitive information, exploiting trust, authority, and time pressure to bypass well-established controls such as call-back procedures and approval hierarchies [5,11].

The growing availability of generative AI tools on underground markets further exacerbated this trend, with **fraud-as-a-service** offerings lowering the barrier to entry for less technically skilled actors while sustaining high success rates. As a result, generative AI is increasingly undermining **traditional identity-based verification models**, substantially increasing fraud risk and complicating the ability of financial institutions to distinguish legitimate communications from malicious ones, particularly in high-trust operational contexts.

AI Generated Image

SHADOW AI AND UNMANAGED AI EXPOSURE

Alongside malicious AI use, the rapid and often uncontrolled adoption of AI tools within organizations has introduced a new category of risk. Shadow AI refers to AI models, applications, or integrations deployed without formal security assessment, governance, or monitoring. In 2025 shadow AI-related incidents accounted for approximately **20% of AI-related breaches** [8]. Notably, **97% of organizations** that experienced AI-related security incidents lacked adequate AI access controls.

20%

Percentage of AI related breaches due to Shadow AI incidents 2025

In the financial sector, where employees increasingly rely on AI-powered tools for data analysis, customer interaction, and decision support, shadow AI can result in inadvertent **data leakage**, unauthorized data processing, or exposure of sensitive information to third-party systems.

Attackers can exploit vulnerabilities in these tools or manipulate model inputs and outputs to facilitate fraud, reconnaissance, or indirect system compromise. As regulatory scrutiny of data handling intensifies, unmanaged AI usage also presents significant compliance and **governance challenges**.[8]

Supply chain and third-party risk as a systemic threat

Supply chain compromise remained one of the most consequential threat vectors for the financial sector in 2025. Financial institutions depend on extensive ecosystems of software vendors, cloud service providers, managed service providers, and fintech partners. This interdependence creates a risk environment in which a single **compromised supplier** can expose dozens or even hundreds of downstream organizations [2, 4, 5, 7, 15]

Third-party involvement was identified in approximately **30% of breaches** affecting financial institutions in 2025, a marked increase compared to previous years [4]. File transfer solutions, managed service platforms, and API-based services remained particularly attractive targets due to their privileged access to sensitive data. The **MOVEit breach**, which continued to have repercussions into 2025, remains a reference case for how zero-day exploitation of widely deployed third-party software can result in mass data theft across the financial sector[7].

The long-term implication of this trend is a shift from isolated incidents toward **systemic cyber events**. Even organizations with mature internal security controls remain vulnerable to weaknesses in their supplier ecosystem, challenging traditional risk ownership models and complicating regulatory accountability.

Several Tier-1 U.S. banks, including JPMorgan Chase, Citigroup, and Morgan Stanley, assessed customer-data exposure following a breach at a shared third-party service provider in 2025, demonstrating how reliance on **common vendors** can create systemic exposure across the sector. The episode highlighted that even mature security programs remain vulnerable to failures outside the organizational perimeter, triggering regulatory response and customer impact analysis despite the absence of a direct intrusion [7,9].

As another example, the cryptocurrency exchange Bybit suffered a **USD 1.5 billion theft** after attackers exploited weaknesses in third-party wallet infrastructure involved in transaction signing. Although affecting a crypto platform, the breach underscored wider financial-sector risks associated with third-party dependencies in critical transaction flows, which can lead directly to extreme financial loss. [11,12].

> "Cyber-criminal activity and cyber risks associated with third-party providers represent persistent and evolving threats to financial system resilience."
>
> — Board of Governors of the Federal Reserve System, Cybersecurity and Financial System Resilience Report, July 2025

Organized cybercrime and Hacktivism

Organized cybercrime groups continue to account for a large share of financially motivated intrusions in 2025 [2,3]. A relatively small number of highly active groups were responsible for a disproportionate share of incidents, combining intrusion capabilities with fraud, insider recruitment, and money laundering infrastructure. Groups such as S**cattered Spider, LockBit affiliates, and BlackBasta** were active across financial targets, leveraging **initial access brokers** to streamline operations [3,6].

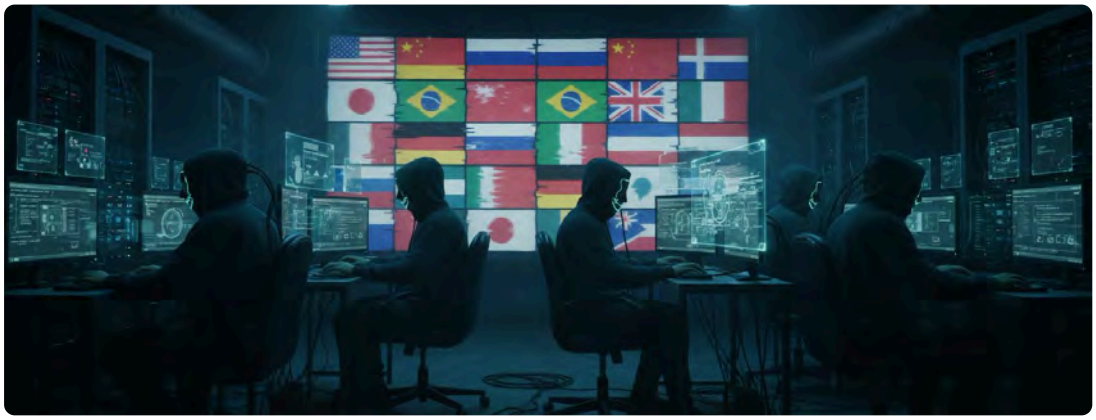
Hacktivist activity also remained elevated, particularly against banks, which accounted for approximately **69% of hacktivist attacks** targeting the financial sector during the year [1]. Groups such as NoName057(16), Keymous+, and DarkStorm Team were especially active in the EU, combining DDoS attacks with influence campaigns, with attack peaks correlating closely with elections and periods of heightened political tension. Although primarily focused on service disruption rather than data theft, they imposed significant operational burdens on security teams and contributed to **reputational risk**.

Banking institutions were particularly affected by **large-scale DDoS attacks** in 2025, which are repeatedly linked to hacktivist campaigns that disrupt customer access to online banking and payment platforms rather than stealing data [1,14].

Advanced persistent threats and geopolitical pressure

State-aligned and advanced persistent threat (APT) actors continued to target financial institutions for intelligence collection, economic insight, and strategic positioning. These campaigns often leveraged **zero-day vulnerabilities** and long-term access strategies, with objectives extending beyond immediate financial gain, with state-linked APT groups undergoing surveillance, currency manipulation intelligence, and preparation for **disruptive contingencies** [6].

Geopolitical instability in 2025 sustained elevated levels of disruptive activity against financial entities, including distributed DDoS campaigns and cyber-enabled **influence operations**. Although the direct financial impact of these attacks was often limited, their cumulative effect strained **operational resilience** and increased the complexity of incident response in already high-pressure environments.



AI Generated Image

Ransomware and double extortion tactics

Ransomware remained one of the most disruptive threats to the financial sector in 2025. Attackers increasingly combined encryption with **data exfiltration**, threatening public disclosure to exert additional pressure on victims. Ransomware variants such as **Akira, Datacarry, and BlackLock** were among the most frequently observed targeting financial institutions in Europe during the year [1].

Approximately **12.8% of B2B financial organizations** experienced ransomware attacks in 2025, reflecting a sustained upward trend [5]. Beyond ransom payments, these incidents triggered regulatory reporting obligations, customer notification requirements, and prolonged recovery efforts, significantly increasing **total incident cost** and operational disruption.

Throughout 2025, ransomware activity against U.S. financial institutions increasingly focused on data exfiltration rather than system encryption. Even when banking services remained operational, stolen data triggered mandatory disclosure, regulator engagement, and extended investigations. This shift reinforced that ransomware now presents a **governance and trust** challenge as much as a technical one, significantly raising the total impact of incidents [9,13].

AI Generated Image

2025: The Start of a Stricter and More Complex Cyber Regulatory Landscape for the Financial Sector

The year 2025 marked a decisive shift in how regulators approach cybersecurity in finance, placing unprecedented emphasis on **digital operational resilience**, cyber risk governance, and third-party oversight. 2025 marks the year when Cyber resilience became no longer aspirational, but rather a **legal and supervisory requirement**.

Regional Overview

EUROPEAN UNION

The **Digital Operational Resilience Act (DORA**) became fully applicable in January 2025, transforming resilience requirements into enforceable, day-to-day obligations. Financial entities must demonstrate effective ICT risk management, comprehensive incident reporting, operational resilience testing, and robust oversight of **critical third-party providers.**

The ECB's **TIBER-EU SSM Implementation Guide** clarified expectations for threat-led penetration testing (TLPT), removing ambiguity around timelines and reinforcing **intelligence-led testing** aligned with real-world threat scenarios.

NORTH AMERICA

Regulatory focus continued to emphasize **breach disclosure timelines**, executive accountability, and third-party risk management. U.S. regulators, including the SEC and OCC, strengthened requirements for timely incident reporting and **governance transparency**, while frameworks like the **FFIEC Cybersecurity Assessment Tool** remained central to resilience evaluations.

ASIA-PACIFIC

Regulatory maturity varied across APAC, but there was increasing convergence toward **resilience-based frameworks** and cross-border information sharing. Initiatives such as **MAS TRM Guidelines** (Singapore), **HKMA's Cybersecurity Fortification Initiative** (Hong Kong), and **Australia's CORIE framework** reflect a growing emphasis on intelligence-led testing and operational resilience.

MIDDLE EAST & AFRICA

The region saw accelerated adoption of cybersecurity frameworks in 2025, driven by systemic risk concerns and digital transformation. In the Middle East, The **UAE Central Bank enforced Information Security Regulations**, while **Saudi Arabia's SAMA Cybersecurity Framework** mandated governance, risk management, and resilience testing for financial institutions. While for Africa, regulatory maturity remains uneven, but key markets such as South Africa advanced operational resilience requirements through the **Prudential Authority's ICT Risk Guidelines**, aligning with global standards on incident reporting and third-party oversight.Across both regions, regulators are increasingly prioritizing **critical infrastructure protection**, cloud security, and cross-border collaboration to mitigate systemic cyber risks.

AI Generated Image

Key Regulatory Changes in 2025

THREAT-LED PENETRATION TESTING (TLPT) BECOMING MANDATORY

Under Articles 26 and 27 of DORA, significant institutions must conduct **intelligence-led penetration tests** at least every three years. These tests are not theoretical exercises, they are performed on live production systems by qualified external teams, using real-world threat scenarios. The goal is to validate resilience against advanced attacks and demonstrate measurable improvement over time. Supervisors expect TLPT to be a learning process, not a one-off compliance check, stressing the importance of adopting C**ontinuous Threat Exposure Management (CTEM)** methodologies.

THIRD-PARTY RISK OVERSIGHT ELEVATED

Supply chain compromise has emerged as a systemic risk, with third-party involvement in roughly **30% of breaches**. DORA explicitly prioritizes continuous monitoring and resilience testing of critical ICT service providers, including cloud and managed service partners. Institutions must maintain **dynamic visibility** into dependencies and ensure contractual and operational safeguards are in place.

INCIDENT REPORTING AND GOVERNANCE TIGHTENED

Material cyber incidents, such as ransomware or large-scale data breaches, trigger mandatory reporting obligations under **strict timelines**. Regulators expect clear classification, rapid escalation, and transparent communication. Failure to comply can result in supervisory action and reputational damage.

ICT ASSET AND AI GOVERNANCE UNDER SCRUTINY

The rise of **shadow AI** and unmanaged AI deployments introduces new compliance challenges. DORA requires institutions to maintain accurate ICT asset inventories, enforce access controls, and manage third-party risks. AI platforms, whether internal or external, now fall under the scope of **critical ICT assets**, demanding governance frameworks that address data security and operational integrity.

Regulation trends for FS to watch out for going forward

Looking ahead, regulatory focus will intensify in three areas:

AI RISK MANAGEMENT:

Expect new guidance on securing **generative AI** and adaptive malware risks. Supervisors will likely demand evidence of AI governance and monitoring.

CONTINUOUS RESILIENCE PRACTICES:

TLPT will evolve from a triennial "exam" to an **ongoing exposure management cycle**. Institutions that embed resilience testing into daily operations will gain a compliance and security advantage.

GLOBAL REGULATORY CONVERGENCE:

Beyond Europe, similar frameworks are emerging worldwide. Multinational institutions should prepare for **harmonized standards** and cross-border supervisory coordination.

"Concerted efforts are needed to strengthen cybersecurity across financial sectors, including supervisory capacity, sector-wide incident response, and continuous understanding of the threat landscape."

— International Monetary Fund, Strengthening Cybersecurity: Lessons from the Cybersecurity Survey, March 2025

Preparing for 2026 and Beyond: Turning Threat Awareness into Resilience

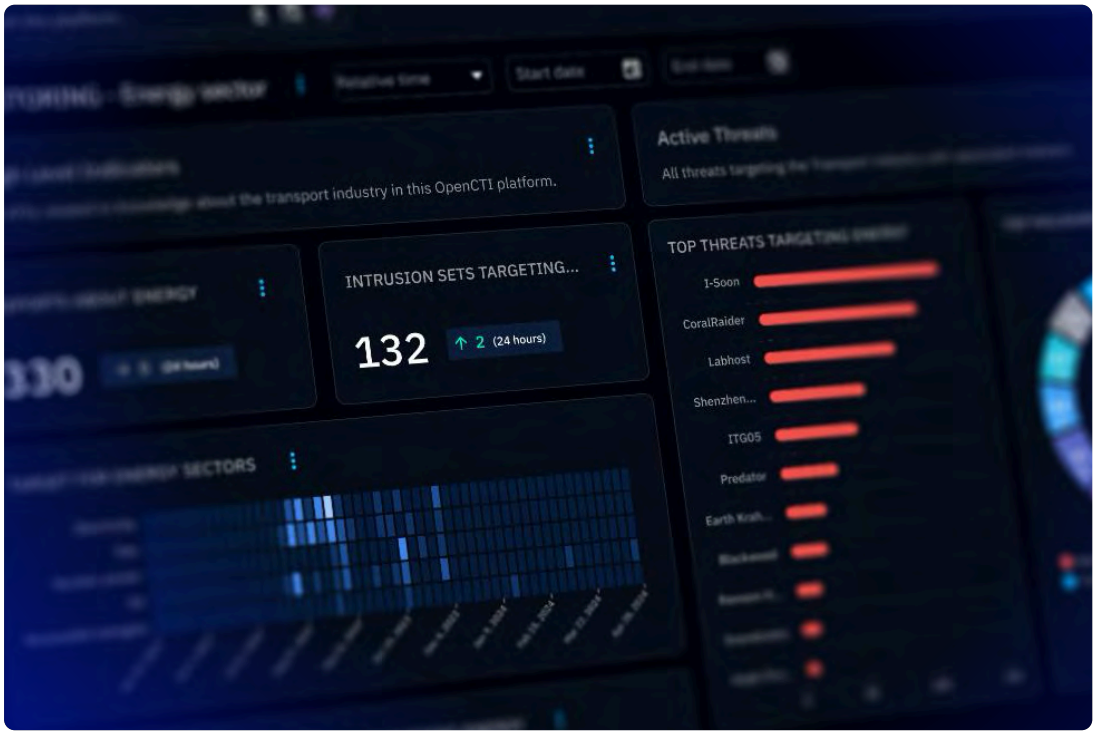
The cyber threat trends observed in 2025—AI accelerated attacks, systemic third party exposure, ransomware with regulatory impact, and geopolitical pressure—highlight a common reality for financial institutions: risk is no longer static, isolated, or purely technical. Threats evolve faster, propagate across **interconnected ecosystems**, and increasingly exploit gaps between assets, suppliers, people, and processes.

Building resilience for 2026 and beyond therefore requires more than traditional prevention and response controls. Financial institutions must develop a **continuous understanding of their threat exposure**, grounded in real world adversary behavior. This means moving beyond lists of indicators to intelligence that provides context—connecting threat actors, techniques, vulnerabilities, and impacted critical functions—so organizations can prioritize what truly matters and adapt as the landscape changes.

At the same time, accelerated exploitation and supply chain risk make **assumed security posture** insufficient. Institutions must be able to validate their defenses against intelligence led scenarios, safely and continuously, to identify weaknesses before attackers do. This shift toward continuous, **threat informed exposure management** reflects how leading organizations are responding to increasingly sophisticated and fast moving adversaries.

Regulation reinforces this evolution. Frameworks such as DORA formalize expectations around intelligence led testing, third party oversight, and **measurable improvement in resilience**. Compliance now depends on the ability to demonstrate how threats are understood, how defenses are tested, and how risk is actively reduced over time.

Together, these pressures point toward a **unified approach**—one that connects threat intelligence, exposure validation, and regulatory evidence into a single operational discipline. The following section explores how this approach can be operationalized to strengthen resilience in the financial sector.



Leveraging Filigran's eXtended Threat Management (XTM) Platform for Financial Institutions

Facing these new industry challenges, as well as the increase in global regulations, traditional security approaches in the financial sector are not enough — institutions need solutions that combine **deep threat intelligence** with proactive exposure validation to confidently prove their resilience. This is where Filigran's **eXtended Threat Management (XTM)** platform comes in.

Filigran's open source XTM platform, leveraging both **OpenCTI** and **OpenAEV**, enables organizations to move beyond compliance checklists toward a sustainable, **intelligence-driven security posture**. Together, these two products enable financial institutions to not only understand the threats they face, but also validate their defenses against real-world attack scenarios, continuously improve their resilience, and provide the much-needed regulatory proof that they are, in fact, safe.

OpenCTI

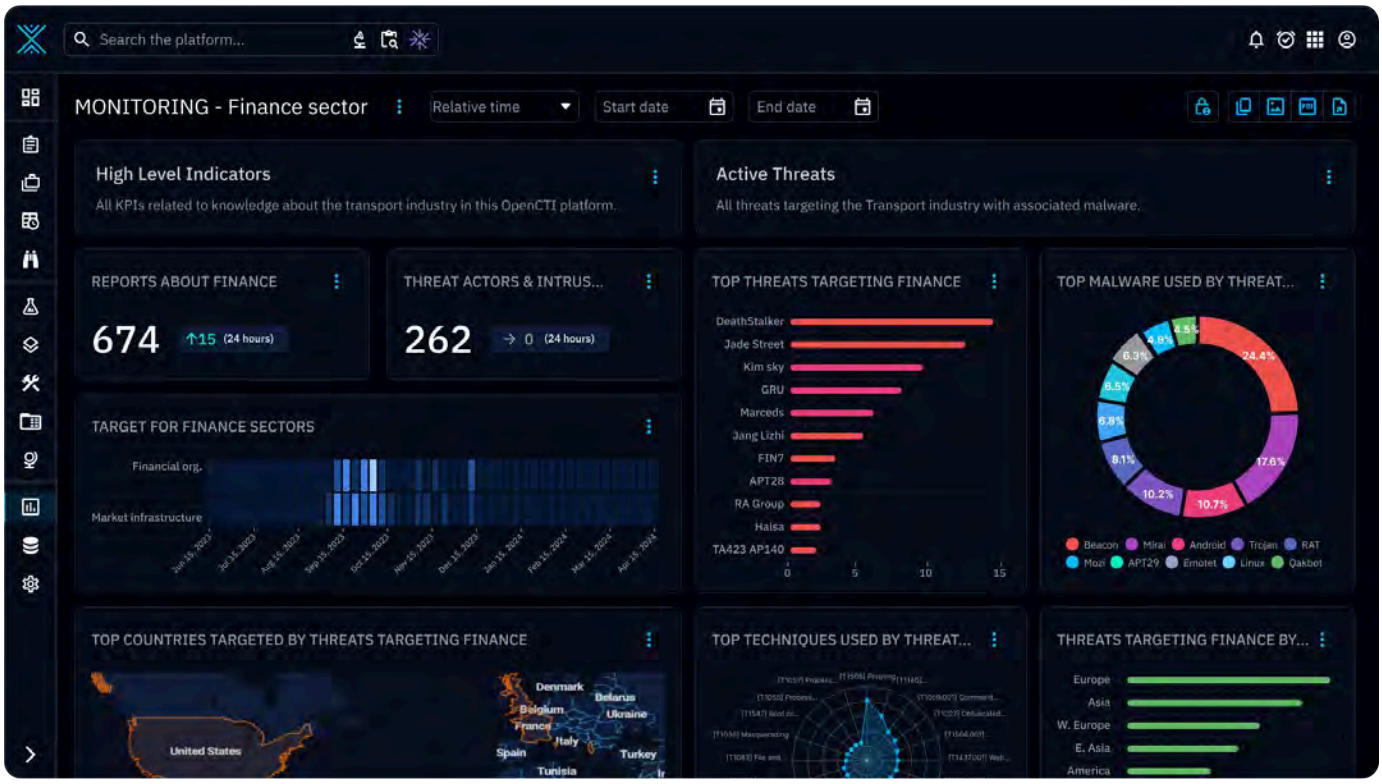
OpenCTI: Turning Intelligence into Action

CENTRALIZED THREAT KNOWLEDGE BASE

OpenCTI provides a single source of truth for threat intelligence by aggregating and modeling data from multiple sources—covering threat actors, campaigns, tactics, techniques, and vulnerabilities. Using **STIX 2.1** and **MITRE ATT&CK** mappings, it enables financial institutions to pivot from isolated indicators to complete **attack chains**. This structured approach ensures intelligence is contextual and actionable, supporting both operational defense and strategic planning.

DYNAMIC DASHBOARDS & KNOWLEDGE GRAPHS

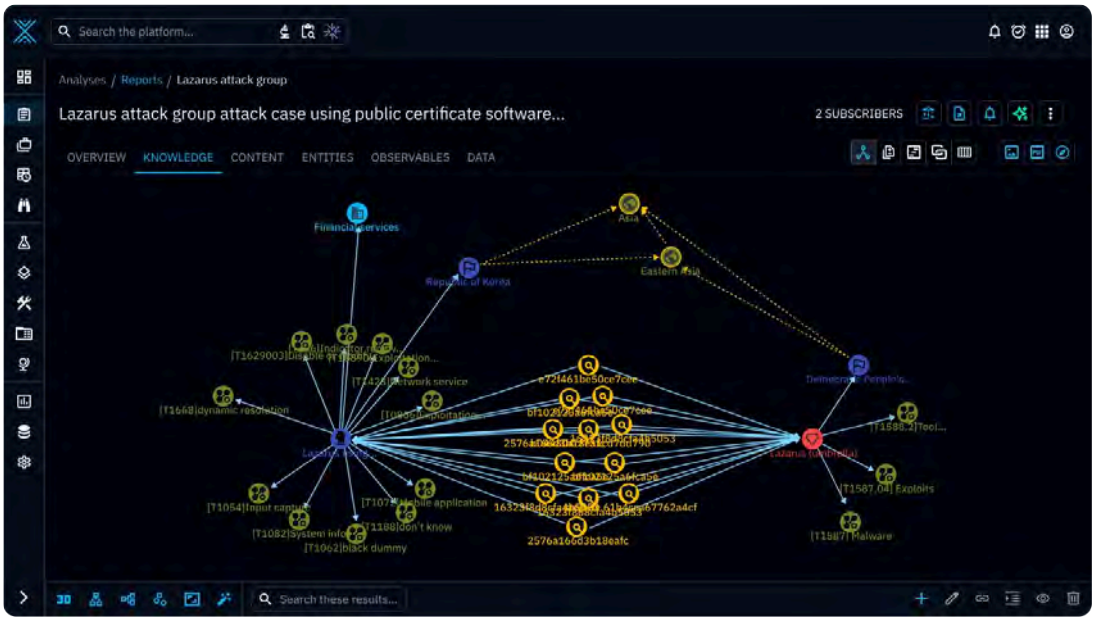
Security leaders and analysts can visualize sector-specific threats through customizable dashboards and **interactive knowledge graphs**. These tools allow CISOs to monitor campaigns, track exposure across critical functions like payments or core banking, and generate insights for executive decision-making. By consolidating complex data into intuitive visual formats, OpenCTI enhances **situational awareness** and accelerates response.



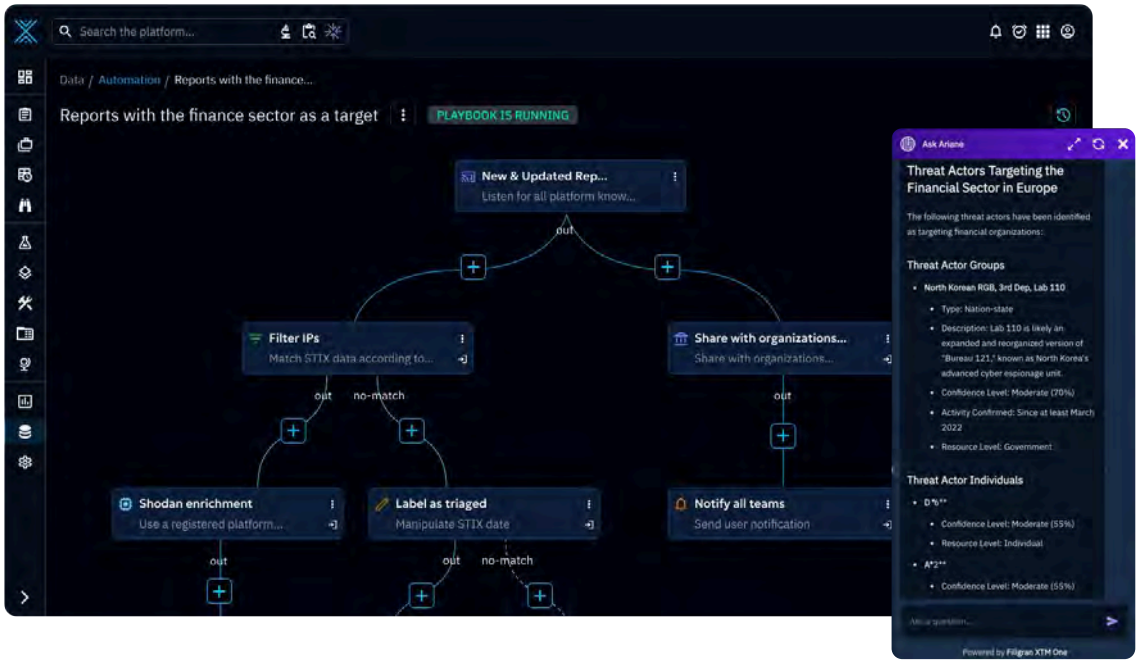
OpenCTI Dashboard

AUTOMATION & AI INSIGHTS

OpenCTI includes automation through **playbooks** and AI-assisted reporting. Playbooks streamline repetitive tasks such as IOC enrichment and threat tagging, while **Ask AI** generates tailored intelligence reports in minutes. These capabilities reduce manual effort, improve consistency, and help institutions meet DORA's stringent **documentation requirements** without sacrificing speed or accuracy.



OpenCTI
Knowledge Graph



OpenCTI
Automation Playboook
& Ariane Chatbox

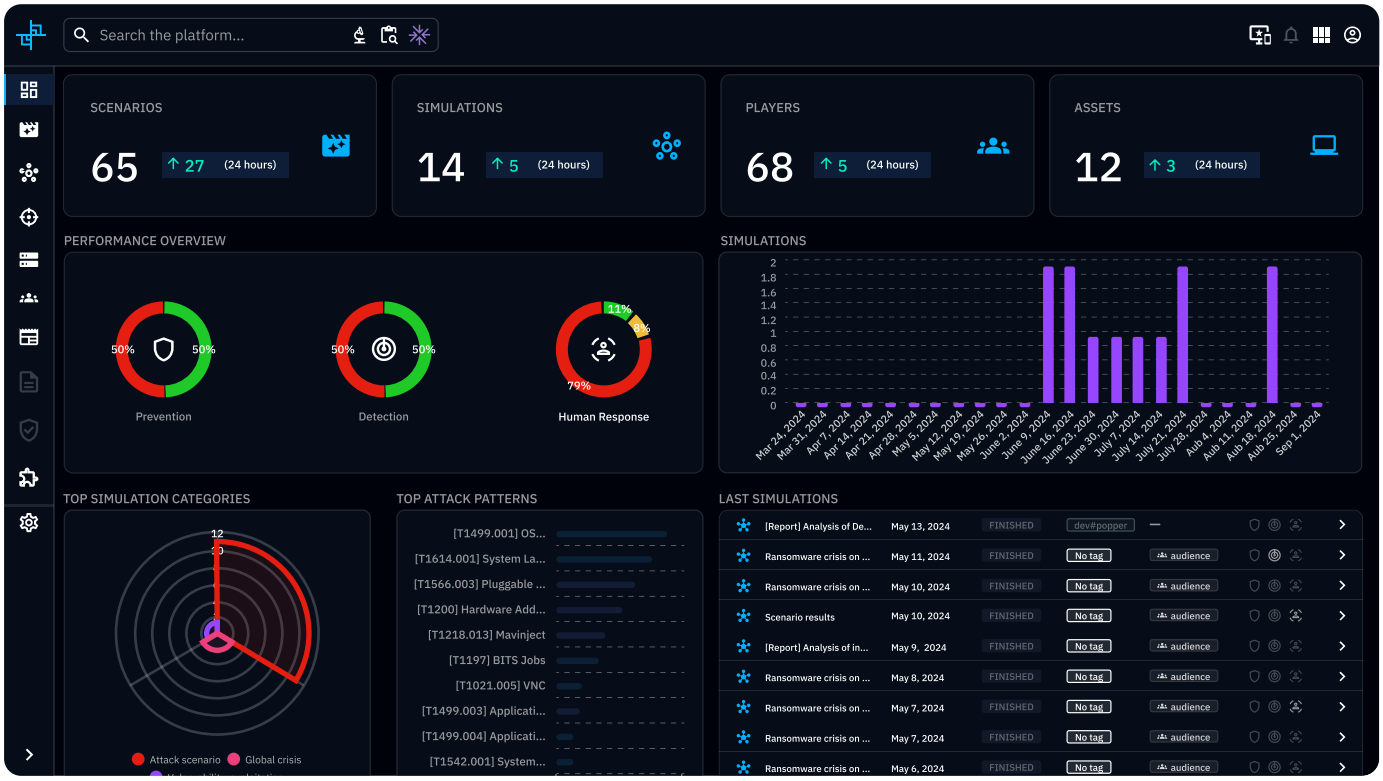
CONTINUOUS TLPT READINESS

OpenCTI supports **Threat-Led Penetration Testing (TLPT)** by mapping **Critical or Important Functions (CIFs)** to ICT assets and linking them to real-world threats. This creates a **living scope model** that evolves with the organization, ensuring TLPT scenarios remain relevant and traceable over time. Institutions can demonstrate progress across test cycles, satisfying regulatory expectations for **measurable improvement**.

OpenAEV

OpenAEV: From Simulation to Continuous Exposure Management

OpenAEV redefines breach and attack simulation by embracing **Adversarial Exposure Validation (AEV)** – a proactive approach to assessing and reducing cyber risk. It transforms TLPT from a one-off compliance exercise into a **continuous resilience program**.



OpenAEV Dashboard

THREAT-INFORMED ATTACK SCENARIOS

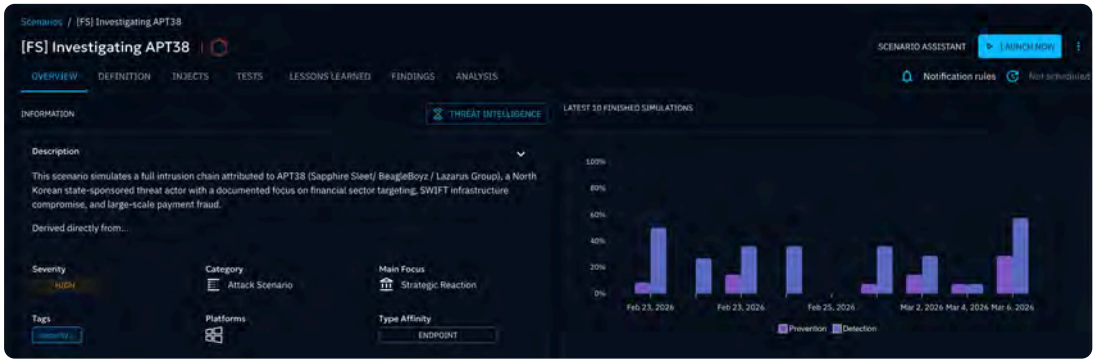
OpenAEV converts prioritized threats from OpenCTI into **executable scenarios** aligned with MITRE ATT&CK. These scenarios allow external red teams and internal security teams to validate defenses against realistic adversary behaviors, ensuring that tests reflect genuine risks rather than generic templates.

SAFE TESTING ON LIVE SYSTEMS

DORA requires TLPT to be performed on **live production system**s without jeopardizing operational integrity. OpenAEV achieves this balance through controlled simulations that exercise defenses while maintaining strict safeguards. This approach delivers meaningful insights without disrupting critical services.

CONTINUOUS VALIDATION & METRICS

Unlike traditional penetration tests, OpenAEV enables **continuous exposure management**. It measures detection speed, prevention efficacy, and residual risk for each scenario, providing **quantifiable evidence** for regulators and boards. These metrics demonstrate not just that a test occurred, but how resilience improved as a result.



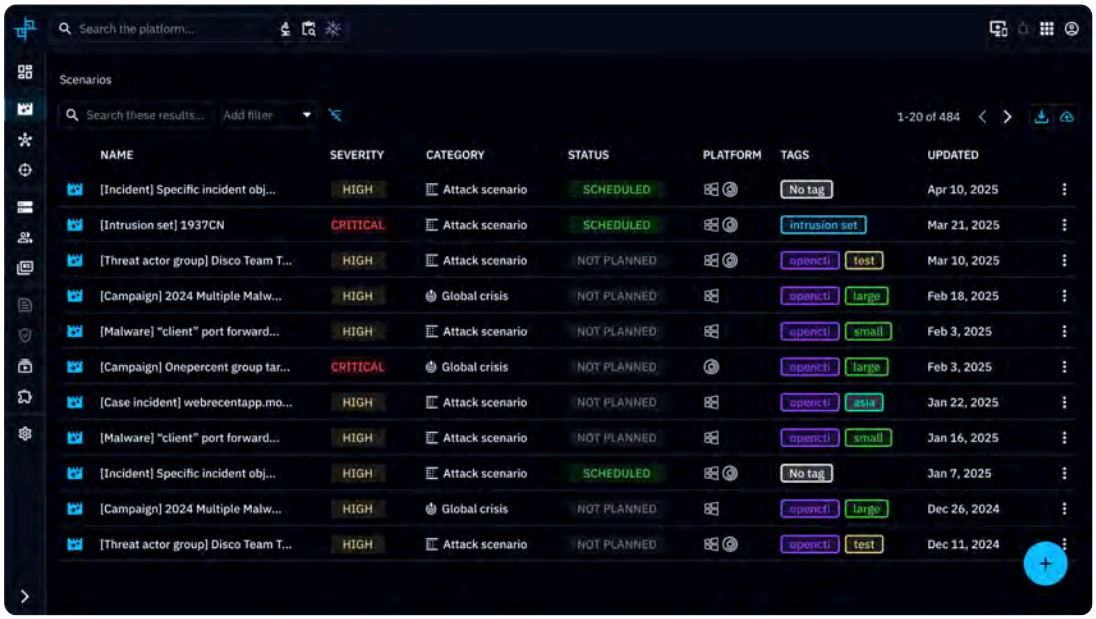
OpenAEV
Investigating APT38

AI-POWERED AUTOMATION

Enterprise Edition introduces **AI-driven scenario generation** and risk-based remediation guidance. This reduces time-to-test, improves prioritization, and ensures that validation efforts remain aligned with evolving threat landscapes. OpenAEV also leverages AI-driven scenario generation and risk-based remediation guidance

HUMAN READINESS ASSESSMENT

Cyber resilience is not only technical—it's organizational. OpenAEV incorporates **tabletop exercises** to evaluate incident response maturity, ensuring that people and processes are as robust as technology. This holistic approach strengthens overall **operational resilience**.



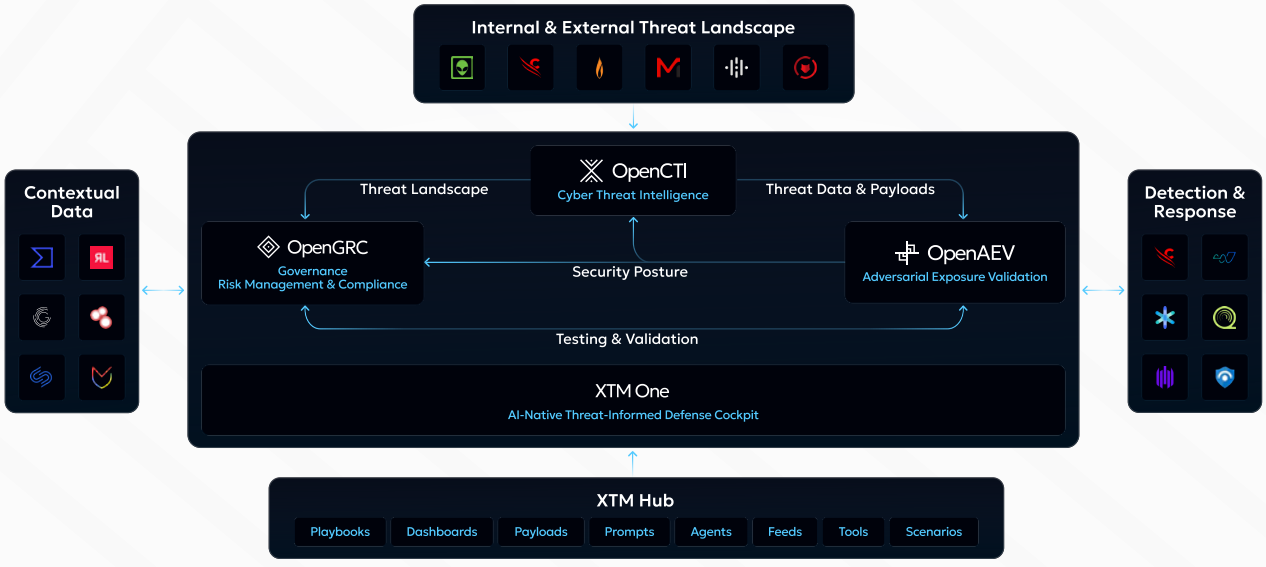
OpenAEV Scenarios

Extended Threat Management: From Compliance to Competitive Advantage

Filigran's XTM platform does more than help financial institutions comply with **Articles 26, 27, and 46 of DORA** or similar regulatory requirements. It enables a fundamental shift from reactive defense to **proactive resilience**. By integrating OpenCTI and OpenAEV, institutions gain a unified framework for **threat-informed defense**, continuous validation, and transparent reporting. The result is a security posture that is not only stronger but **demonstrably so**, offering a critical advantage in a sector where trust and operational continuity are everything.

Filigran eXtended Threat Management (XTM) Platform

The open-source threat intelligence, advanced adversary simulation, and strategic cyber risk management solution



Sources

[1] ENISA Threat Landscape Report 2025

[2] FS-ISAC Cybersecurity Risk Report 2025

[3] CrowdStrike Global Threat Report 2025

[4] Verizon Data Breach Investigations Report 2025

[5] Kaspersky Financia Sector Threat Landscape in 2025

[6] IBM X-Force Threat Intelligence Index 2025

[7] SecurityScorecard – Cybersecurity of Europe's Top 100 Financial Institutions 2025

[8] IBM Cost of a Data Breach Report 2025

[9] CSO Online – JPMorgan, Citi, Morgan Stanley assess fallout from third-party data breach (2025)

[10] Check Point Research – Top Attacks and Breaches: January 2025

[11] CRN – 10 Major Cyberattacks and Data Breaches in 2025

[12] Infosecurity Magazine – Top Cyber-Attacks of 2025

[13] ABA Banking Journal – Key decisions bankers face in response to ransomware attacks (2025)

[14] Cloudflare – DDoS Threat Report, Q2 2025 (Cloudflare Radar)

[15] Board of Governors of the Federal Reserve Rystem, Cybersecurity and Financial System Resilience Report, 2025

ABOUT FILIGRAN

Filigran stands out for its expertise in open-source solutions for end-to-end threat management. It offers the Filigran **eXtended Threat Management (XTM) suite**, designed to help organizations understand their threat environments, anticipate and detect incidents, and strengthen their overall security posture. The suite currently includes two solutions:

- **OpenCTI**: structures and operationalizes cyber threat intelligence at technical, operational, and strategic levels.
- **OpenAEV**: helps identify critical security gaps through advanced attack simulations, resilience testing, and crisis management exercises.

Today, more than 6,000 organizations worldwide rely on Filigran's solutions. With a team of over 200 employees across the globe, Filigran supports leading companies such as Marriott, Thales, Hermès, Airbus, Novartis, and Bouygues Telecom, as well as for public entities including the European Commission, ENISA, ANSSI, the French Ministry of the Interior, the New York State Cyber Command, and several U.S. and Australian federal agencies. Filigran has also built a strong ecosystem of partners, including Deloitte, Orange Cyberdefense, Deepwatch, Arctic Wolf, Google Cloud Security, Atos, Wavestone, and Intrinsec.