Filigran

WHITE PAPER

Threat-Informed Defense for the Technology Sector

A practical guide to help technology organizations align security operations with real-world threats using a **Threat-Informed Defense** strategy.

Summary

Executive summary

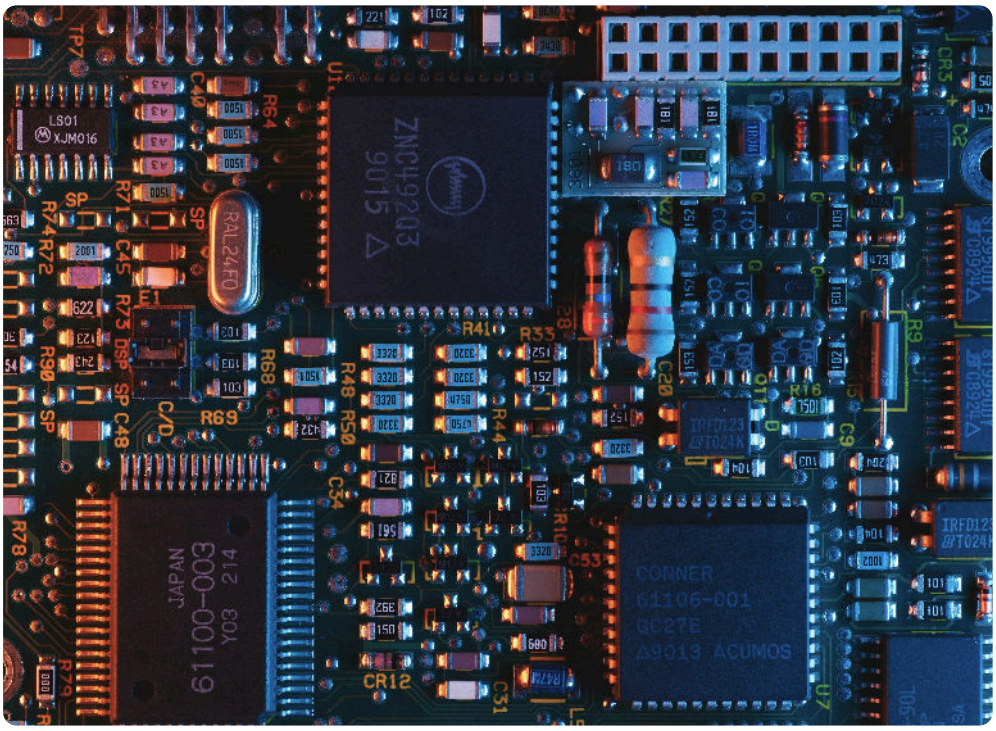

Photo by Umberto on Unsplash

As technology companies accelerate their development and innovation across cloud-native platforms, AI, and SaaS ecosystems, they face an increasingly complex and dynamic threat landscape. Traditional security models struggle to keep pace with the speed and scale of modern tech environments.

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 technology companies. It demonstrates how tools like **OpenCTI** and **OpenBAS** 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!

Why Technology Companies Are Moving Towards Threat-Informed Defense

Technology companies are built to move **fast**. Whether delivering SaaS platforms, scaling AI models, or managing complex cloud-native environments, they operate in a landscape defined by rapid innovation, distributed teams, and constant change. But this same agility that fuels growth also introduces risk, expanding the attack surface, increasing complexity, and creating blind spots that adversaries are quick to exploit.

What we need is a **security strategy** that's underpinned by **dynamic** and **contextual threat intelligence**, that takes adversary behavior and intent into account and allows tech organizations to test their security controls against the evolving threat landscape. This is where **Threat Informed Defense (TID)** comes into picture - as a proactive, intelligence-driven methodology that aligns security operations with the real-world behaviors of adversaries.

Threat-Informed Defense: Methodology

Threat-Informed Defense as an approach was first advocated by MITRE. This approach leverages MITRE ATT&CK to map out known tactics, techniques, and procedures (TTPs) used by the threat actors of most concern, enabling organizations to prioritize defenses based on current threats most likely to impact them, rather than attempting to cover the entire threat landscape. Threat-Informed Defense is grounded in three pillars:

- **Cyber Threat Intelligence:** The integration of threat intelligence is crucial for Threat-Informed Defense. It provides timely, contextual insights into emerging threats, attackers of concern, and evolving attack vectors. Particular emphasis here is on using threat intelligence not just to look at the indicators but to actually understand the adversary behaviors and motives, which are more stable over time and more expensive for adversaries to change. This threat intelligence can then really enhance detection, improve incident response, and reduce the likelihood of successful attacks.
- **Defensive Measures:** These are the security controls that an organization uses to protect its business. Understanding the adversary is only the first step but if an organization fails to act on that knowledge and adjust its defenses to meet those threats, it misses the core value of a TID.
- **Testing & Evaluation:** By regularly testing against the latest threat intelligence and evolving adversary TTPs, organizations can maintain an accurate and dynamic understanding of their security posture. Exercises like red and purple teaming should incorporate adversary emulation - replicating the tactics, techniques, and attack sequences of specific, relevant threat actors - to ensure realism and relevance.

Figure 01: MITRE Threat-Informed Defense

Threat-Informed Defense empowers security teams to shift from being reactive to proactive, having a continuous approach to identify and remediate security gaps. Its not just a framework or a collection of tools, its a mindset shift:

Understand how adversaries operate by mapping their tactics, techniques, and procedures (TTPs) to your specific environment → Simulate realistic attacks to test and validate your defenses before adversaries do → Continuously adapt by integrating threat intelligence into engineering, security, and DevOps workflows → Prioritize investments based on the threats most likely to impact your business

It is the same philosophy that underpins Filigran's open-source based eXtended Threat Management (XTM) suite.

At Filigran, we believe in **continuous threat management** to be able to **stop attacks before they materialize**. Our mission is to **help security teams operationalize threat intelligence and let it flow through their entire security ecosystem** - making it strategic, timely, and actionable. **XTM is a modular suite that transforms threat intelligence into real-world defense.**

And by integrating prioritized intel to validate adversary exposure security teams can elevate their security posture and respond strategically.

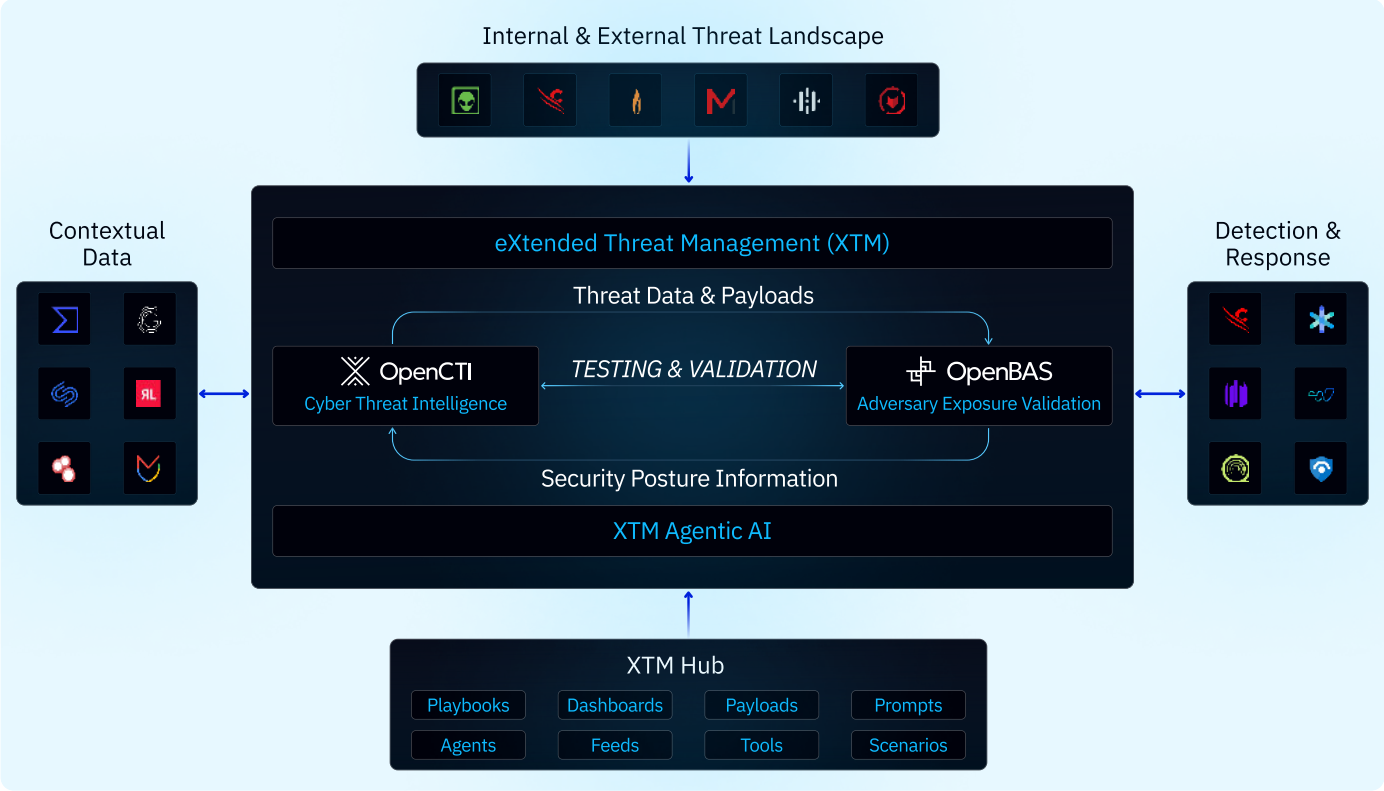

Figure 02: Filigran's XTM Suite

Breaking Down Threat-Informed Defense into Actionable Chunks

Threat-Informed Defense provides us an approach, which can be interpreted and actioned in different ways. At Filigran, we have developed a Threat-Informed Defense Pipeline to focus on actionable chunks that aligns our solution with the operational realities of Technology companies:

Figure 03: Filigran's TID Pipeline

STAGE 1: STRATEGIC THREAT LANDSCAPE ASSESSMENT

The first stage of this framework is developing a thorough understanding adversary behavior and prioritizing threats based on real-world intelligence. Today, security teams have access to a lot of threat intelligence but a majority of it is very generic and un-actionable for an individual organization.

For sectors like technology, threats are highly dynamic and frequently tailored to exploit sector-specific vulnerabilities such as software supply chains and cloud infrastructure. **Tech companies need to evaluate threats for their strategic intent, operational evidence, and attacker capability and motivation.**

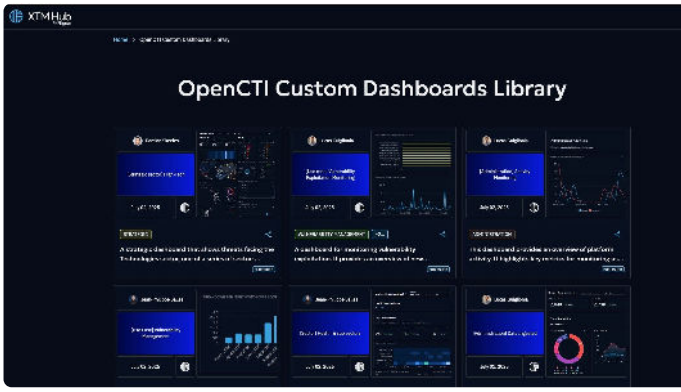

Figure 04: OpenCTI Custom Dashboard Library

Filigran's Threat Intelligence Platform, **OpenCTI**, supports this stage by enabling structured analysis of threats to the Tech sector, including APTs, supply chain risks, and cloud-native exploits. It integrates geopolitical and sector-specific intelligence to help prioritize threats, while allowing analysts to annotate inclusion decisions directly on threat entities.

You can download this Technology dashboard from our dashboard library as part of the XTM Hub, then, further adapt it to your specific context, for example adding geographical and organizational layers.

STAGE 2: ACTOR AND MALWARE TRACKING

Keeping pace with evolving threats requires more than static lists —it demands a dynamic, intelligence-driven approach. This stage focuses on continuously monitoring threat actors and malware families through adaptive watchlists that evolve as new intelligence emerges.

A structured triage process ensures that **incoming reports are reviewed efficiently, allowing teams to assess and act on relevant IOCs and TTPs.** This helps maintain a clear, current view of the threat landscape and ensures that only the most pertinent threats are tracked.

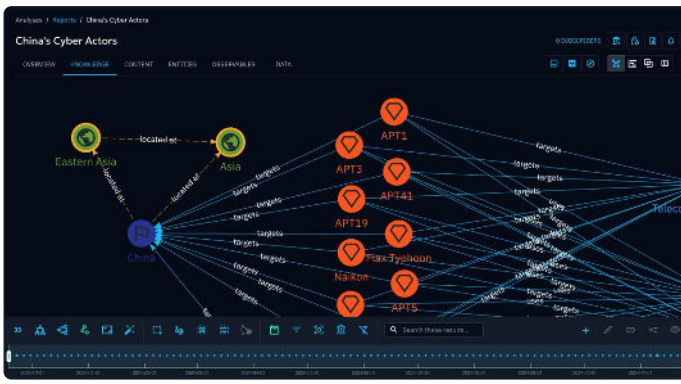

Figure 05: OpenCTI Knowledge Graph

OpenCTI streamlines this process by linking tracked threats to their current operational methods and real-time indicators (aligned with MITRE ATT&CK framework and attack patterns), presenting visualizations using an easy-to-follow graph-based data model.

As new intelligence is ingested, related IOCs are automatically tagged and distributed to detection platforms like SIEM, EDR, and SOAR. Any new TTPs or malware that the tracked threats have employed, or new vulnerabilities that they are exploiting, are flagged for triage by the appropriate teams. Analysts can also **generate automated, stakeholder-ready reports** that highlight the TID function's progress in addressing these emerging threats, reducing manual effort while keeping security leadership informed and aligned. This approach helps maintain the overall direction and success of the threat-informed defense program.

STAGE 3: TTP AND REPORT MAPPING

Identifying how attacker behaviors align - or don't - with your current defenses is critical for closing security gaps. This phase centers on aggregating TTPs (tactics, techniques, and procedures) from tracked threats and comparing them against your organization's defensive controls.

By applying these comparisons, teams can highlight which techniques are most active or concerning and where coverage is weakest—particularly across cloud workloads, containers, and CI/CD environments. This stage also **links the threat intelligence with the rest of the security processes, mainly to test the effectiveness of security controls**.

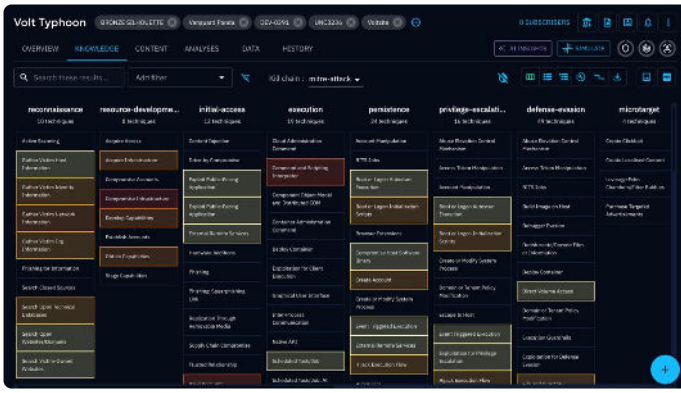

Figure 06: Report Mapping on OpenCTI

To support this, **OpenCTI** offers a structured way to aggregate TTPs, getting them ready to be prioritized for adversarial exposure validation aka breach and attack simulation. You can **aggregate TTPs across all tracked threats of interest**, highlighting those of highest activity or most concern. You can then import similar ATT&CK matrices for your defensive controls, and compare these against the attackers to identify gaps that need to be addressed.

STAGE 4: BREACH ASSESSMENT SIMULATION

After comparing tracked threat attacker TTPs against current security controls at a theoretical level, it is then time to move to the third pillar to test and validate how the security controls actually perform in practice.

One of the most fundamental use of threat intelligence is to **check how your security tools will perform against the most probable threats**. Unfortunately, this process is currently very siloed and adhoc through threat hunting, pentesting or vulnerability management. What we need is a continuous and automated way to run simulations to validate our defenses against adversarial exposure.

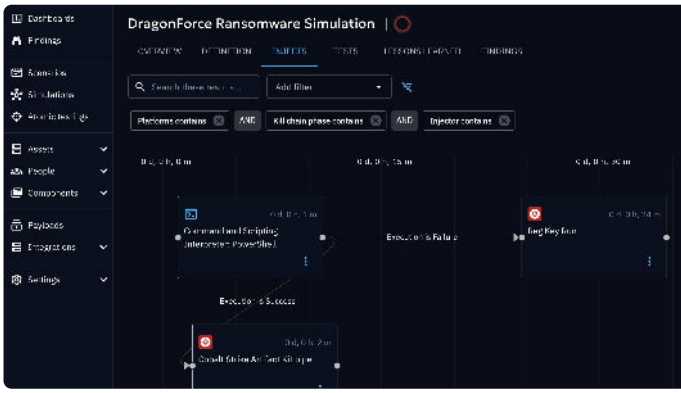

Figure 07: DragonForce Ransomware Simulation on OpenBAS

These simulations can range from **automated tests** across standard operating environments to more complex purple team exercises that blend technical exploits with human-driven tactics. Regular testing also helps **detect control regressions** caused by system changes or misconfigurations.

In this stage, **OpenBAS** drives the execution of these simulations, while **OpenCTI** captures and contextualizes the results. Both platforms are integrated with each other. OpenBAS can run scheduled tests across client and server builds, simulating both general threat behaviors and specific campaigns. The outcomes, whether successful detections or missed signals, are fed back into OpenCTI, where analysts can assess how current controls stack up against known threats. This integration ensures that testing isn't just a checkbox, but a **continuous feedback loop that sharpens detection and response over time.**

STAGE 5: CONTROL VALIDATION AND INVESTMENT

The final phase focuses on translating threat intelligence into strategic action. By reviewing control gaps in the context of specific threat actors, their associated TTPs and the results of simulations; teams can **prioritize remediation efforts** based on both risk relevance and business impact. This approach not only **sharpens day-to-day response** but also **informs long-term planning** by tracking how defensive coverage evolves over time.

To support this, security teams can use both **OpenCTI** and **OpenBAS** to connect the dots between threat data, missing coverage (both technical and human-side) and security investment decisions. OpenCTI's historical snapshots and OpenBAS's time-series based reporting help visualize trends in coverage, making it easier to demonstrate progress and justify future security investments.

OpenBAS provides you remediation guidance to help you prioritize your security efforts and investments. Once you simulate a relevant threat to check the exposure and exploitability of your critical assets against it, OpenBAS will provide comprehensive findings and highlight where you need to make changes, whether re-configuration, upgrade or replacement. It will also give you tailored remediation guidance if available.

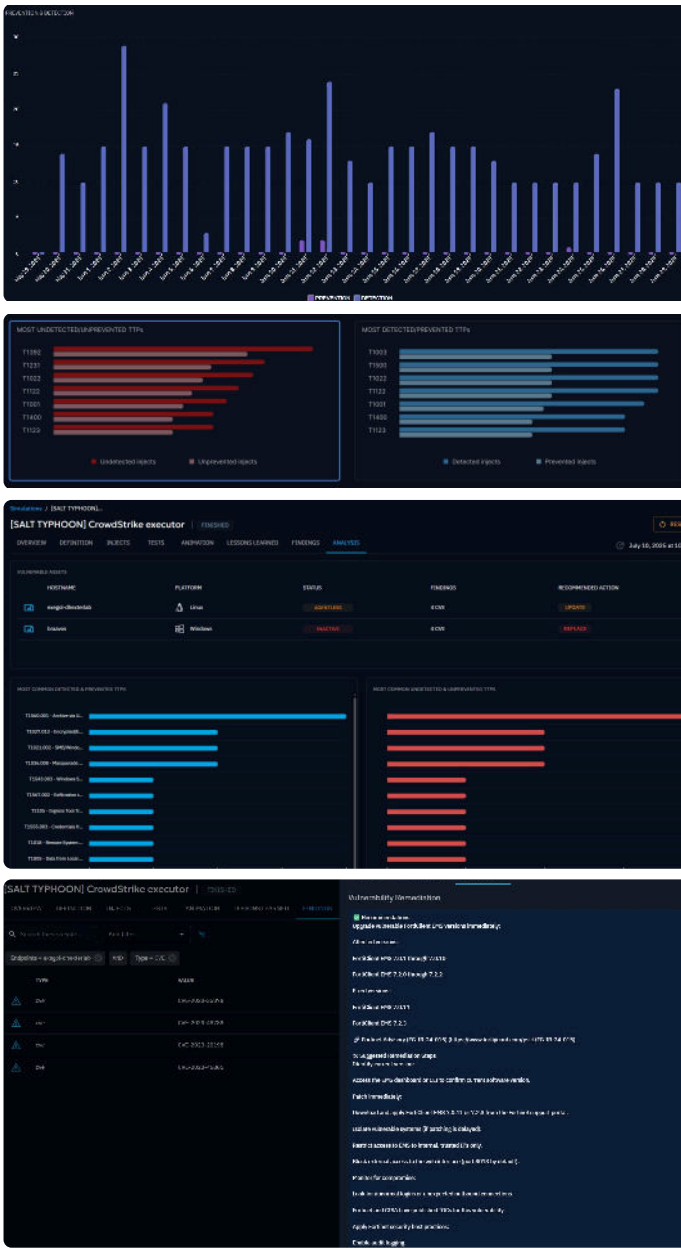

Figure 08: Translate threat intelligence into strategic actions

STAGE 6: QUARTERLY REVIEW

While testing and identifying new threats should be run continuously as part of a true **Continuous Threat Exposure management (CTEM)** program, the strategic threat landscape and primary tracked threats should also be reviewed on at least a quarterly basis. By regularly reviewing historical data and aligning it with business priorities, teams can identify where to invest, what to improve, and how to better align security operations with long-term goals.

OpenCTI and OpenBAS make these reviews both comprehensive and efficient. OpenCTI consolidates intelligence-driven insights, control gap trends, and threat actor mappings into executives-ready reporting, while OpenBAS contributes detailed simulation results that reflect real-world control performance. **Together, they provide a clear picture of how defenses have evolved, where regressions may have occurred, and which areas require renewed focus.** This integrated reporting supports executive visibility, compliance needs, and cross-functional alignment - ensuring that security decisions are grounded in evidence and impact.

Use Cases: Threat-Informed Defense in Practice

Simulate Adversary Behavior Against Cloud-Native Infrastructure

Modern infrastructure environments, especially those built on cloud-native principles, are dynamic, distributed, and increasingly complex. This makes them attractive targets for adversaries who exploit misconfigurations, overlooked dependencies, and gaps in detection coverage.

Use Threat-Informed Defense pipeline to **test and improve your cloud infrastructure security**:

Step 1 Use the MITRE ATT&CK for Cloud matrix to identify tactics and techniques relevant to your cloud provider like AWS, Azure or others.

Step 2 Ingest cloud-specific threat intelligence into OpenCTI and focus on IOCs and TTPs related to cloud misconfigurations, credential abuse, and lateral movement in cloud environments.

Step 3 Feed threat intelligence into your **SIEM**, **EDR**, and **SOAR** platforms to create detection rules for cloud-specific threats.

Step 4 Build simulations in OpenCTI using the aggregated TTPs based on known threat actors.

Step 5 Run simulations in OpenBAS to to test detection and response capabilities in your cloud environment.

Step 6 Use a threat coverage matrix to track which ATT&CK techniques you can detect, prevent, or respond to.

Step 7 Regularly update your controls and detections based on new threat intelligence and lessons learned from simulations or incidents.

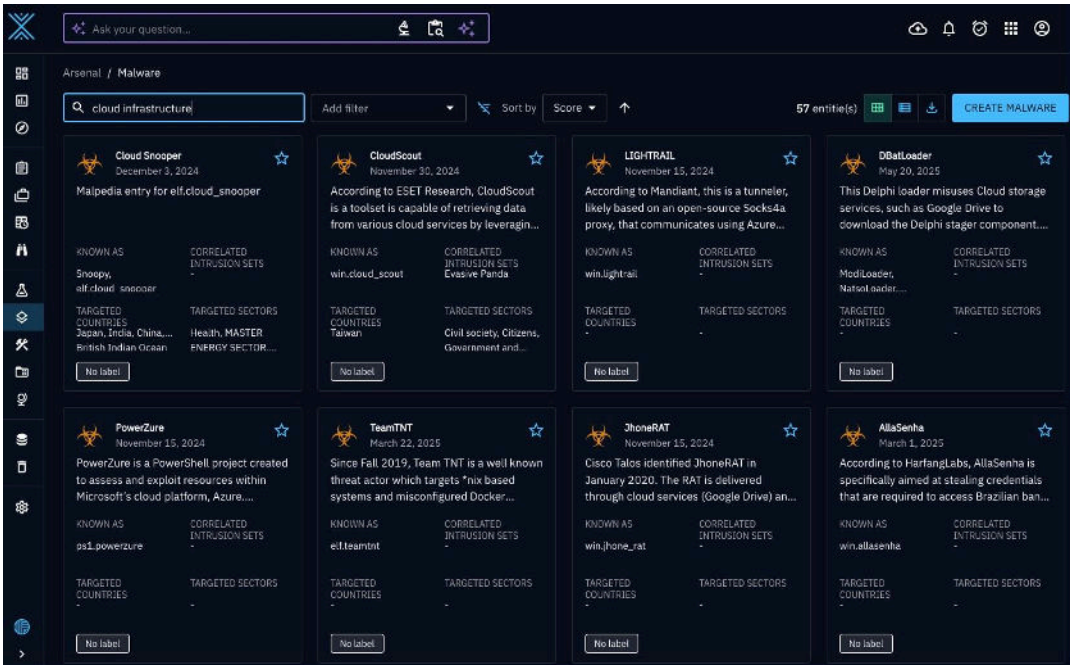

Figure 09: Merge Your TI Feeds for a Focused Analysis on Malware Known to Target Cloud Infrastructure

Arm Your Defenses Against Ransomware Attacks

Ransomware has evolved into one of the most disruptive and costly threats facing the technology sector. As tech companies increasingly rely on cloud-native infrastructure, distributed teams, and continuous delivery pipelines, their attack surfaces have expanded - and so has their exposure to ransomware campaigns.

How Threat-Informed Defense **enables organizations to mitigate ransomware risk**:

Step 1 Use OpenCTI's analysis features including AI Insights and graph analysis to understand Ransomware TTPs used in common campaigns like phishing, RDP brute force, PowerShell or lateral movement.

Step 2 Identify how these techniques could be executed in your cloud environment, for example, are backups accessible from the same network or are IAM roles overly permissive?

Step 3 In OpenBAS, define 'expected response' from your security tools and teams in the event of a ransomware attack.

Step 4 You can use pre-built scenarios to run against known ransomware like 'DragonForce'.

Step 5 Run technical simulations and tabletop exercises to cover both technology and human-side of readiness.

Step 6 Regularly update your controls and detections based on new threat intelligence and lessons learned from simulations or incidents.

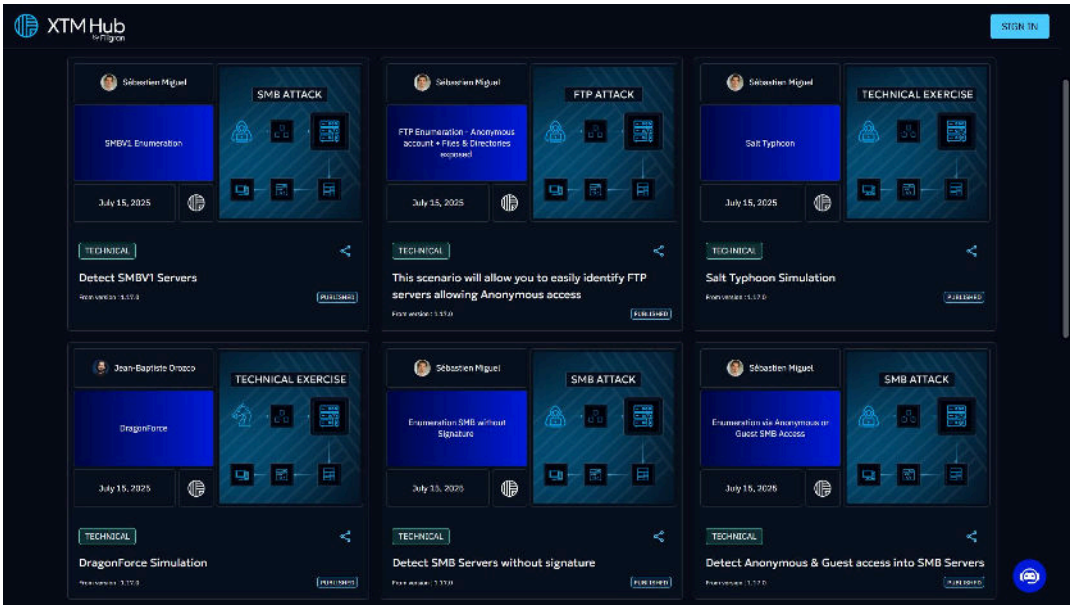

Figure 10: Pre-built Scenario Library in the XTM Hub Includes DragonForce Simulation

Conclusion

To stay ahead of modern cyber threats, technology companies need more than just tools - they need a strategy. **Threat-Informed Defense** gives them that strategy by turning threat intelligence into action. With the right tools and a clear process, teams can test their defenses, close security gaps, and make smarter investments.

Filigran's TID pipeline helps make this possible. It brings together threat data, testing, and reporting into one continuous cycle - so companies can stay secure, agile, and ready for whatever comes next.

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 100 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.