CUSTOMER STORY

Filigran

Cutting Threat-Hunting Time by 85%: A Game-Changer for ClearDATA

ClearDATA leverages OpenCTI to automate its Cyber Threat Intelligence, accelerating investigations and delivering actionable insights to its healthcare clients.

-90% investigation time

with indicator investigations dropping from 10 min to < 1 min.

4 to 7× faster threat hunts

completion time reduced from 1 week to under 24 hours.

90% faster threat reporting

publication time reduced from 48 hours to 5 hours.

OVERVIEW

CLEARDATA

INDUSTRY

HealthTech

HEADQUARTERS

United States

PRODUCT USED

OpenCTI

USE CASE

- IoC Management & Detection
- Threat Landscape Monitoring
- Threat Intelligence Library
- Vulnerability Monitoring
- Incident & Case Management

About ClearData

Founded in 2009, ClearDATA set out with a clear mission: "Make healthcare better, every single day." Their goal was straightforward: unlock the full potential of cloud technology for healthcare, without ever compromising on security or compliance.

To achieve this, they built the first cloud platform designed exclusively for healthcare, empowering providers, payers, life sciences, and health tech organizations to focus on what they do best: caring for patients.

Today, ClearDATA is the trusted cloud security and compliance partner behind some of the biggest healthcare providers and payers in the industry. With their proprietary CSPM, the CyberHealth™ Platform, and a team of over 150 security and compliance experts, they deliver managed cloud security services and compliance automation, ensuring patient data and sensitive information are always protected. Their specialized teams span across threat intelligence, detection engineering, cyber defense operations, and security architecture, and work together to provide a secure and compliant cloud experience.

Context

Operating at the intersection of cloud technology and healthcare, ClearDATA has faced a rapidly changing cyber landscape. Ransomware, data-extortion operators, and cloud-focused intrusion techniques grew more sophisticated as healthcare organizations accelerated cloud adoption, introducing new layers of exposure around sensitive patient data.

To support its growing security services, ClearDATA initially adopted a dedicated threat intelligence platform, which failed to align with its evolving service model. The company then sought a more sustainable foundation by reassessing how threat intelligence could better support both operational security and customer outcomes, as part of its managed security and threat intelligence offering. As Cody Pickren, Senior Manager of the Cyber Threat Intelligence team, explains, *"Cyber threat intelligence collection is the tip of the spear for our company's knowledge and ability to understand the threat landscape in a way that translates to improving our customers' security posture."*

"Literally everything in our program builds from intelligence, and everything with intelligence begins with collection and OpenCTI."

Cody Pickren
Senior Manager of the Cyber Threat Intelligence team, ClearDATA

Challenges

FRAGMENTED THREAT INTELLIGENCE & MANUAL OPERATIONS

ClearDATA's cyber threat investigations used to rely heavily on manually collecting and correlating indicators from multiple sources, ranging from public threat reports to internal SIEM data, RSS feeds, and vendor alerts aggregated via Slack channels. As Cody Pickren points out, *"We're a small team, and we've got a lot of ground to cover. Anything we can automate or set up to just run in the background is a huge benefit for us."*

EXCESSIVE TIME SPENT ON PLATFORM MAINTENANCE

As ClearDATA's cyber threat intelligence capabilities matured, the team explored open-source tools to support its growing intelligence needs. This approach required the security team to operate and maintain its own threat intelligence infrastructure, consuming valuable time and engineering cycles that could have been dedicated to analysis and security service development. *"We simply didn't have enough engineering cycles to build and support ongoing growth with infrastructure and automation,"* says Cody.

A RIGID CTI PLATFORM HINDERING CUSTOMIZATION & EVOLUTION

After experiencing open-source platforms that proved highly resource-intensive, Cody's team adopted a commercial cyber threat intelligence solution. But it imposed too rigid workflows that were difficult to adapt to healthcare-specific threats and security procedures. Manual processes, like indicator enrichment and reporting, caused inefficiencies. Customization was limited, and many capabilities required additional paid modules, as Cody Pickren recalls. *"We were locked into a closed ecosystem, and everything else was an add-on package that we couldn't justify."*

DATA OVERLOAD MADE IT HARD TO PRIORITIZE AND ACT

ClearDATA needed to move beyond raw threat data to help customers and executives clearly understand which risks required immediate action. *"Being able to quantify threats or exposure with actionable data and show relevant, up-to-the-minute activity with context is what helps leadership understand the necessary urgency."* In highly regulated healthcare environments, alerts, vulnerability disclosures, or compliance requirements alone were often not enough to trigger timely decisions to drive effective mitigation responses. Leadership wants to know what the top priorities are and how to turn them into actionable steps.

Why OpenCTI?

UNIFIED THREAT INTELLIGENCE AND AUTOMATED ENRICHMENT

OpenCTI provided ClearDATA with a centralized view of threat intelligence, bringing together indicators, reports, and analyst-generated insights that had previously been scattered across tools. By unifying this intelligence on a single platform, analysts could work directly on the data without relying on custom scripts or constant engineering support. *"Being able to give our analysts the ability to craft automation for enrichment, correlation, and processing indicators was a huge efficiency boost for us,"* says Cody Pickren.

A MANAGED, ENTERPRISE-GRADE CTI PLATFORM

Adopting the enterprise edition of OpenCTI removed the operational burden of hosting and maintaining threat intelligence infrastructure, allowing ClearDATA's teams to focus on security operations rather than platform upkeep. *"I ran the community version for about a year and a half, and it was a significant time sink,"* Cody recalls.

A MODULAR ARCHITECTURE ADAPTABLE TO CLEARDATA'S SECURITY USE CASES

OpenCTI's advanced customization capabilities enabled ClearDATA to tailor the platform precisely to its unique security needs. By leveraging its modular architecture, ClearDATA could seamlessly integrate threat intelligence directly into its existing security stack and adapt data sources as its services and customer needs evolved. *"The modularity and configurability of data streams was the first and biggest differentiator for us."*

CONTEXT-RICH THREAT INTELLIGENCE THAT SUPPORTS DECISION-MAKING AND URGENCY

By correlating threat intelligence with operational and customer context, OpenCTI helped ClearDATA present risks to customers in a clear, prioritized way. Scoring threats based on factors such as active exposure and relevance to the customer environment made it easier for decision-makers to see what truly required immediate action. *"OpenCTI lets us turn context into a story. That's what makes customers act,"* Cody believes.

"With OpenCTI, we can draw a direct line from intelligence to operational impact."

Cody Pickren
Senior Manager of the Cyber Threat Intelligence team, ClearDATA

Adoption

ClearDATA adopted OpenCTI through a phased approach, initially validating its relevance within an intelligence-driven security model before transitioning to the Enterprise Edition as operational needs grew. The rollout focused on embedding the platform into analysts' daily workflows and supporting detection and response use cases with automation. With Filigran's dedicated support, OpenCTI rapidly became a central pillar of ClearDATA's cyberthreat intelligence and managed detection and response services. As Cody Pickren recalls, *"I still remember just marveling at the difference in stress levels and time commitments between running our own OpenCTI container and having you available, being able to just reach out to support."*

Cody Pickren
Senior Manager of the Cyber Threat Intelligence team, ClearDATA

"Every interaction with Filigran has been about understanding what we're trying to achieve and figuring out how to help us get there. It's a very different mindset from just ticking boxes."

How Filigran helps ClearData

ACCELERATING INVESTIGATIONS WITHOUT INCREASING TEAM SIZE

By automating indicator enrichment and correlation into a structured CTI platform, ClearDATA cut investigation time from **~10 minutes per indicator to under 1 minute**, so analysts can keep pace with alert volumes while focusing on analysis. As Cody says, *"We can just throw an indicator in, and everything is there: history, relationships, correlations. It's a great way to improve investigation efficiency."* ClearDATA now has a unified view of the threat landscape.

RECLAIMING TIME FOR HIGHER-VALUE SECURITY WORK

Without the burden of operating an internal CTI platform, ClearDATA regained engineering and analysis cycles, reducing threat search procedures from **approximately one week to less than 24 hours**. *"Now I've got analysts who can work directly in the data they're fluent in and have an impact, while freeing up my engineers to focus more on the back end."*

FASTER THREAT RESPONSE, SEAMLESS INTEGRATION

OpenCTI enabled ClearDATA to adapt its **threat intelligence workflows** as security operations evolved by creating a clear path from intelligence analysis to operational response. Threat reports and analyst-generated intelligence are enriched and structured in OpenCTI before being used to augment detections across SIEM and EDR environments. This flow of contextualized intelligence significantly shortened the time required to move from analysis to detection and response, giving security teams better visibility during alert triage. As Cody explains, *"It really gave us the ability to customize and integrate better with our platform and existing reports."*

ACTIONABLE INTELLIGENCE DRIVING DECISIONS AND CUSTOMER ACTION

ClearDATA can now deliver contextualized intelligence fast enough to influence mitigation decisions. As Cody Pickren explains, *"When we first started, it was a 24-to-48-hour process to identify, synthesize, and publish a report.* ***Now our average time to publish is around five hours.****"* The security team can clearly explain why a specific risk is important to their customers at this time and what its potential impact on the business would be, which significantly speeds up remediation and increases their customer trust.

The Road Ahead

Moving forward, ClearDATA plans to extend its intelligence-driven security lifecycle by validating detections and defensive controls through attack simulation. Building on OpenCTI as the foundation of its threat intelligence operations, the team sees Filigran's OpenAEV as the next step to test and confirm the effectiveness of security measures against real-world attack scenarios. The long-term goal is to close the entire security lifecycle, from threat identification to response and validation, while supporting the healthcare industry's growing cybersecurity and regulatory requirements.

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