CUSTOMER STORY

Filigran

# OpenCTI becomes Controlware's Engine for Scalable Threat Hunting

Controlware built an intelligence-driven detection framework with OpenCTI to scale threat hunting across multiple XDR platforms.

**6 months**
of investigation workload saved each year through proactive threat hunting

**+230%**
increase in detection rule production without adding analysts.

**90%**
faster detection deployment time.

## OVERVIEW

controlware

**INDUSTRY**

Managed IT Services & Cybersecurity

**PRODUCT USED**

OpenCTI

**USE CASE**

- Threat Monitoring and Hunting
- Threat Intelligence Library
- IoC Management & Detection
- Case Management

## About Controlware

Controlware GmbH is one of Germany's leading IT Solution Providers and Managed Service Providers. The company is part of the Controlware Group, which employs more than 1,000 people and generates close to €500 million in annual revenue, including its subsidiary Controlware Austria.
As a digitalization partner for mid-sized and large companies as well as public sector organizations, Controlware develops, implements, and operates resilient IT solutions across Network Solutions, Information Security, Data Center & Cloud, Collaboration, IT Management and Managed Services. Its ISO 27001-certified Customer Service Center delivers both operational support and fully managed services, including comprehensive cyber defense capabilities. With a nationwide presence in the DACH region and strong international partnerships, Controlware supports global projects, while maintaining long-term relationships with leading technology vendors.

> "Threat intelligence is no longer a separate activity. It's now woven directly into detection and hunting."

**Dominik Degroot**
Senior Cyber Security Analyst at Controlware GmbH

# Context

As cyber threats including phishing, infostealers, and ransomware intensified for over 40 clients, Controlware's SOC adapted quickly to reinforce its security posture and protect its growing customer base. Customers were no longer looking only for alert handling but for a partner able to anticipate new threat vectors and react before attackers could execute their objectives. This evolution required a more aligned, intelligence-driven approach to ensure that every customer, regardless of their environment, benefited from the same level of insight and protection.

## Challenges

**PRODUCTIVITY BOTTLENECKS CAUSED BY MANUAL DETECTION WORK**

As an MSSP, Controlware was providing managed services for **customers who were using different XDR platforms with their own query language.** As Dominik Degroot, Senior Cyber Security Analyst at Controlware GmbH, explains, *"Our Sigma rules had to be rewritten manually for each XDR, which turned one rule into three versions. Deployment required logging into every customer environment and testing it separately. It limited how many rules we could produce and how fast we could respond."*

**LIMITED DETECTION EFFECTIVENESS**

Controlware's detection rules existed as isolated artefacts, with no links to threat actors, malware families, or ATT&CK techniques. ***"Without structured intelligence, a rule was just a rule. We couldn't see which actor used that technique or why an alert mattered, and analysts had to invest significant time to gather essential context,"*** Dominik Degroot notes.

**LIMITED CAPACITY TO SCALE DETECTION ENGINEERING**

Managing security for customers means **dealing with millions of events and thousands of incidents every month.** Manual detection workflows imposed a hard ceiling on how fast Controlware could expand its detection coverage. As Dominik Degroot recalls, *"The effort required to deploy and validate each rule across environments significantly slowed down our ability to expand coverage."*

**SOC STUCK IN A TIME-CONSUMING PROCESS**

Without an operational backbone for large-scale hunting, security operations were time-consuming. *"The core problem was to manage detection logic once and deploy it everywhere,"* Dominik remembers.


# Scaling threat hunting with OpenCTI

## A STRUCTURED AND CENTRALIZED STIX THREAT INTELLIGENCE REPOSITORY

OpenCTI provided **a unified, STIX-based knowledge base**, and the **flexibility** to create custom entities for Sigma rules independently of XDR-specific query languages. This turned detection rules into fully modelled, versioned, and searchable objects, all accessible through a single API. As Dominik notes: *"Treating rules as first-class objects was essential. OpenCTI gave us the structure to do that."*

## A KNOWLEDGE GRAPH THAT CONNECTS RULES TO REAL THREATS

With OpenCTI's knowledge graph, detection rules are embedded in a dynamic model, **where each rule is anchored in a living, actionable threat context.** *"OpenCTI isn't just an indicator aggregator.* ***It allowed us to handle threats, malware families, campaigns, TTPs and Sigma rules, all in one structured knowledge base****,"* says Dominik.

## API-FIRST ARCHITECTURE BUILT FOR AUTOMATION AND SCALE

OpenCTI's **API-first architecture** exposed every intelligence and detection object through a consistent, well-documented interface, enabling Controlware **to industrialize detection logic across customer environments.** "*The API was a decisive factor. Without a backend designed for automation, scaling simply wouldn't have been possible,*" Dominik remembers.

## OPEN PLATFORM ENABLING PROACTIVE THREAT HUNTING

Another crucial element for Controlware was having an enterprise-grade intelligence platform that could support proactive threat hunting. By providing a structured backbone for intelligence, workflows, and automation, OpenCTI enabled the team to systematically search for early-stage malicious activity. *"Once we had the right intelligence backbone, we could finally think beyond alerts and start hunting threats proactively."*

# Adoption

Within a few weeks, Controlware deployed OpenCTI, modeled its Sigma workflows, and integrated the platform into daily SOC operations. Controlware used it as the basis for HuntingGrid, the automated multi-XDR search system that Controlware was developing. HuntingGrid retrieves Sigma rules, converts them into the correct query language, runs hunts throughout all customer environments, and aggregates results for analysts.

Thanks to Filigran's clear documentation and guidance, OpenCTI became fully operational very quickly. "*By the end, we had custom workflows, a complete knowledge base, and a team that was trained and ready to work with the new system*," says Dominik.

# How Filigran helps

### FREEING ANALYST TIME FOR HIGH-VALUE DETECTION WORK

By centralizing and automating detection logic, OpenCTI eliminated repetitive manual tasks, allowing analysts to focus on detection engineering and threat hunting rather than operational tasks. "*The most important benefit is the ability to create and manage* ***five times more Sigma rules without increasing management overhead,***" says Dominik. Deployment that used to take weeks now happens within hours across all customers, dramatically strengthening detection coverage.

### ENABLING FASTER AND EARLIER THREAT DETECTION

OpenCTI reduces investigation time and helps the team detect malicious activity much earlier in the attack lifecycle. As Dominik explains: "***With OpenCTI and SOAR enrichment, what used to take significant time of manual analysis per investigation is now basically gone.***"

### ALLOWING DETECTION COVERAGE TO SCALE WITH CUSTOMER GROWTH

By automating rule deployment, **OpenCTI removed the capacity ceiling that previously limited how fast detection coverage could expand** as the customer base grew. "*Before, we could deploy fewer detection rules. Today, deployment happens within hours instead of weeks*," Dominik says.

**"One major success came from the PDF backdoor campaign. Using OpenCTI integrated with our automated threat hunting infrastructure, we identified infections in 12 customers, none of which were detected by their XDR solutions. We detected the backdoor before it downloaded malware, preventing what could have been a widespread compromise.**
**This is our biggest win to date."**

**Dominik Degroot**
Senior Cyber Security Analyst at Controlware GmbH

### TURNING ALERTS INTO ACTION: REDUCING NOISE, FOCUSING ON REAL THREATS

OpenCTI's consistent API enabled Controlware to build HuntingGrid. This results in much more reliable and usable results. *"While XDR tools generate high volumes of generic alerts that require manual triage, HuntingGrid executes targeted, intelligence-driven queries based on structured threat intelligence from OpenCTI. This produces low-volume, high-confidence findings with immediate threat context, fundamentally shifting analyst work from noise management to actionable threat detection."*

## FINANCIAL IMPACT & ROI

With broader, earlier, and more reliable detection, Controlware now prevents incidents that would previously have reached the execution stage. For an MSSP with manufacturing clients, **avoiding even a single cyber-attack could potentially represent hundreds of thousands to millions of euros saved**, from incident response to business interruption, GDPR penalties, or ransom payments.

# The Road Ahead

The next major step for Controlware is integrating OpenAEV to complete the detection-validation loop: OpenCTI will manage Sigma rules, HuntingGrid will execute them across all customer environments, and OpenAEV will validate their effectiveness through simulated attack techniques.

AI is another area of experimentation. Dominik envisions a future where structured intelligence can be queried naturally and where AI helps analysts extract key behaviors from reports or propose detection logic automatically to reduce repetitive work and accelerate response. With XTM One, Filigran is swiftly progressing this vision towards autonomous threat management.

## 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