binalyze!

Proactive and Swift: How ARES Cyber Intelligence Reduces Incident Response Times and Assures Customers

Company overview

Founded in 2019, ARES Cyber Intelligence GmbH is based in Upper Austria. The company initially targeted the underserved cybersecurity needs of small to medium businesses but quickly expanded its reach to include large global enterprises. Unlike traditional IT security providers, ARES focuses solely on cybersecurity solutions.

The firm works alongside its managed and Incident Response (IR) retainer clients to preemptively identify and mitigate cyber threats, aiming to prevent attacks before they can cause harm. ARES also provides crucial support to retainer and non-retainer customers during and after cyber incidents.

Challenges

- Complex and slow toolchain (hundreds of tools and scripts)
- Scalability and efficiency issues
- Capacity and resourcing challenges
- High dependency on technical expertise
- Incomplete visibility

Introduction to Challenges and Problems

ARES Cyber Intelligence initially grappled with a toolchain that was not only cumbersome but also ill-suited for the rapid and scalable response required in today's dynamic cybersecurity environment. This was particularly apparent during ransomware cases, which accounted for about 85% of their reactive incident response cases. "Our tools were working, but they were complex and not fast enough for large-scale incidents," explained the CTO of ARES, Lukas Waldenberger. "Before, we used to select from a mixture of standard tools on our forensic workstation: Linux tools, a few Windows tools, self-written PowerShell, and a Python script - we counted once, it was in the hundreds of tools we could choose from to investigate." Each tool was selected for specific tasks but was not cohesive when combined for large-scale incident management.

This piecemeal approach led to significant operational inefficiencies, notably during complex security breaches that required quick and comprehensive handling.

Moreover, the reliance on multiple tools without a unified view of the incident platform presented significant challenges in training, coordination, and collaboration needed for incident response. Waldenberger highlights that responding to ransomware incidents often involved substantial challenges, particularly as none of the 200 cases they handled were for existing retainer customers. This lack of pre-existing relationships meant the necessary security tools were not already in place, necessitating a start-from-scratch approach for each incident. Specifically, when incidents occurred at remote locations, the response team faced travel times that could exceed six hours, further delaying the critical initial stages of evidence gathering and analysis.

Customer
ARES Cyber Intelligence

Industry
Managed Security Service Provider

Region
DACH Market (Germany, Austria, Switzerland)

Founded
2019

Website
ares-ci.com AND myincident.ai

Success Highlights:

- **Halved Mean Time to Remediation** (MTTR) in ransomware attacks
- **Resolved cases within 1.5 hours** from start to finish
- **Rapid initiation of investigations**—from hours/days to minutes
- **Consolidated 100+ tools** into a single investigative platform
- **Eliminated labor-intensive** tasks like lab setup

The toolchain was initially built to focus on individual systems, which became a significant limitation when analyzing hundreds of machines at once during a security breach. "When all the obvious evidence is wiped by the threat actor, our old system just couldn't keep up," Waldenberger commented. This cumbersome approach underscored the need for more efficient, rapid, and scalable deployment capabilities in their incident response toolkit, highlighting the essential need to pivot towards a system that could effectively handle the demands of modern cybersecurity threats.

Solution: Implementation of Binalyze AIR

The transition to Binalyze AIR at ARES Cyber Intelligence has significantly transformed their incident response workflow. The team, consisting of about four or five individuals, no longer needs solely senior technical professionals, thanks to AIR's ability to distribute tasks across various areas of expertise. "Binalyze AIR allows our team to split up the areas of expertise," the CTO explained, highlighting how the solution supports diverse roles from security analysts to malware engineers, each focusing on their specific strengths.

The shift from a cumbersome toolchain to Binalyze AIR has streamlined operations considerably. Previously, analyzing hundreds of systems in response to incidents was a daunting task due to scalability issues. "With Binalyze, it's easy to analyze hundreds of machines at once, a capability we didn't have before," remarked the CTO. This scalability is complemented by the system's ease of deployment and the unified interface, which offers a single pane of glass that is functional and well-designed. "The ease of deployment with AIR is a game-changer. We can prepare everything quickly at the press of a button, significantly speeding up the mean time to respond (MTTR) and allowing better planning and preparation," he added.

Binalyze AIR's flexibility in tool integration further enhances its appeal. "The platform allows the interchangeable use of YARA, or osquery, and Sigma rules, providing a robust triage capability that adapts to various incident scenarios. I can use all three, depending on which would satisfy my use case or my detection the best," said the CTO, emphasizing the solution's adaptability. "The built-in MITRE ATT&CK analyzer offers quick insights into attacks, facilitating rapid and fact-based investigation progression".

Waldenberger explains that choosing the right solution in cybersecurity can be daunting. "You don't want to be restricted on day one, finding you can't do certain tasks or needing another product for what should be straightforward," he says. Binalyze AIR's built-in MITRE ATT&CK Analyzer simplifies complexity by providing a quick overview of public-knowledge attack vectors. This way, investigations are fact-based. "We don't have to guess but can systematically build on each fact, efficiently enhancing our incident resolution process."

From a business perspective, AIR has enabled ARES to optimize resource allocation and handle multiple incidents simultaneously without compromising service quality. "Now, with AIR, it's easier to assign the right resources and collaborate on incidents, which reduces the burden significantly," the CTO noted. This efficiency has mitigated the need for extensive resources and allowed ARES to offer new types of services, enhancing their business model and customer assurance.

Rapid Incident Response Use Case for Existing SOC Customers

For ARES Cyber Intelligence's managed SOC customers, and using the multi-tenant capabilities, preparations are made in advance by setting up a blank tenant configured for immediate action. This readiness allows for a rapid response when an incident occurs.

In a notable case, a vulnerability in a system permitted remote code execution, which the existing Endpoint Detection and Response (EDR) system managed to partially thwart by blocking additional payloads from the internet. However, the EDR did not provide visibility into whether the threat actor had performed further actions such as reconnaissance or command issuance.

Using Binalyze AIR, they conducted a thorough investigation and resolved the case within one and a half hours—approximately five times faster than traditional methods. AIR's capabilities allowed them to drill down into the incident timeline to analyze the threat actor's actions precisely. This was crucial as the EDR had limitations in detecting encrypted command inputs, which Binalyze AIR could more granularly identify and evaluate, distinguishing between potential threats and routine admin activities.

> **"Binalyze AIR extends our visibility beyond what our EDR can achieve, enabling precise investigations into threat actor activities. This enhanced capability is crucial for building a fact-based, accurate case narrative without relying on guesswork."**
>
> – Lukas, CTO of ARES Cyber Intelligence

Conclusion

Binalyze AIR has provided ARES Cyber Intelligence with a powerful, scalable, and user-friendly platform. The solution supports a more collaborative and flexible investigation approach, dramatically reduces response times, and allows the team to manage their workload more effectively, making it a cornerstone of operational success.