VECTRA
SECURITY THAT THINKS.®

CASE STUDY

The EDAG Group Flips the Script on Ransomware

The word no company wants to hear became an unfortunate reality for one of the world's largest independent development partners to the automotive and aviation industries — *ransomware*. On the night of March 13, 2021, The EDAG Group, based in Wiesbaden, Germany, knew something wasn't right when a large number of business-critical systems suddenly became unusable. Sure enough, after consulting with it external IT security experts, it was determined that EDAG had in fact fell victim to a ransomware attack that left their IT systems handcuffed.

A Different Outcome for Ransomware

In a scenario that had potential for a headline making breach, The EDAG Group knew the stakes were high as they were up against a ransomware attack. Fortunately, their security team is locked in on today's attack surface, and by quickly stepping in they were able to control the attack so EDAG was get their systems back up and running.

> "Our IT security experts can now work much more efficiently."
>
> **Maria Fladung**
> *IT Security Officer*
> *EDAG*

EDAG

Organization

EDAG Group

Industry

Automobile & Automotive

Challenge

Victim of encryption Trojan that shut down their business-critical systems and IT systems

Selection criteria

An AI-driven platform that ensures accurate visibility into security threats and attacks that make it inside EDAG

Results

- Meaningful collection and enrichment of data anywhere EDAG has workloads — cloud, data center, IoT and all across the enterprise
- Immediate visibility across the environment and elimination of any potential relapses by the threat actor
- A comprehensive view of potential threats without any invasive technology

In the midst of working to restore systems, EDAG knew, that they needed an approach that would make sure that there where no suspicious activity left int he network and any attacks heading towards EDAG in the future, don't stand a chance. That plan included a proof of concept (POC) with Vectra to deliver AI-driven threat detection and response. This would ensure accurate visibility into security threats and attacks that make it inside EDAG. Within just a few days, EDAG was provided with POC hardware and help from the security experts at Orange Cyberdefense.

"It was clear to us that we would only be able to start again properly and safely after the attack if we were able to recognize dangerous behavior in the network quickly and precisely. Vectra's automated platform enables us to do just that – 24/7," explains Maria Fladung, IT Security Officer at EDAG.

The AI-driven approach to detection and response from Vectra captures a meaningful collection of data and enriches it with security insights and context to give EDAG an advantage over adversaries by anticipating their every move. In addition, Vectra is able to apply this approach anywhere EDAG has workloads — cloud, data center, IoT and all across the enterprise — so visibility never becomes an issue again regardless of where deployments exist.

POC to New BFF

A successful POC led to a rapid deployment of Vectra. With quick action from Orange Cyberdefense, Vectra was easily integrated into The EDAG Group's incident response strategy. Vectra was able to immediately improve visibility across the environment and eliminate any potential relapses by the threat actor.

"With Vectra and the Cognito platform, we have gained an anchor of trust in our IT network and have increased visibility considerably," says Fladung.

> "With Vectra and the Cognito platform, we have gained an anchor of trust in our IT network and have increased visibility considerably."
>
> **Maria Fladung**
> *IT Security Officer*
> *EDAG*

A complete team effort all around, Orange Cyberdefense provided valuable knowledge about the best practices for handling a security incident of this magnitude and ultimately positioned EDAG with the best possible outcome considering the circumstances. The EDAG Group is now equipped with a comprehensive view of potential threats without any invasive technology, and two defenders who are up to the task in Orange Cyberdefense and Vectra.

"Our IT security experts can now work much more efficiently." concludes Fladung.

> "Our IT security experts can now work much more efficiently."
>
> **Maria Fladung**
> *IT Security Officer*
> *EDAG*

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai