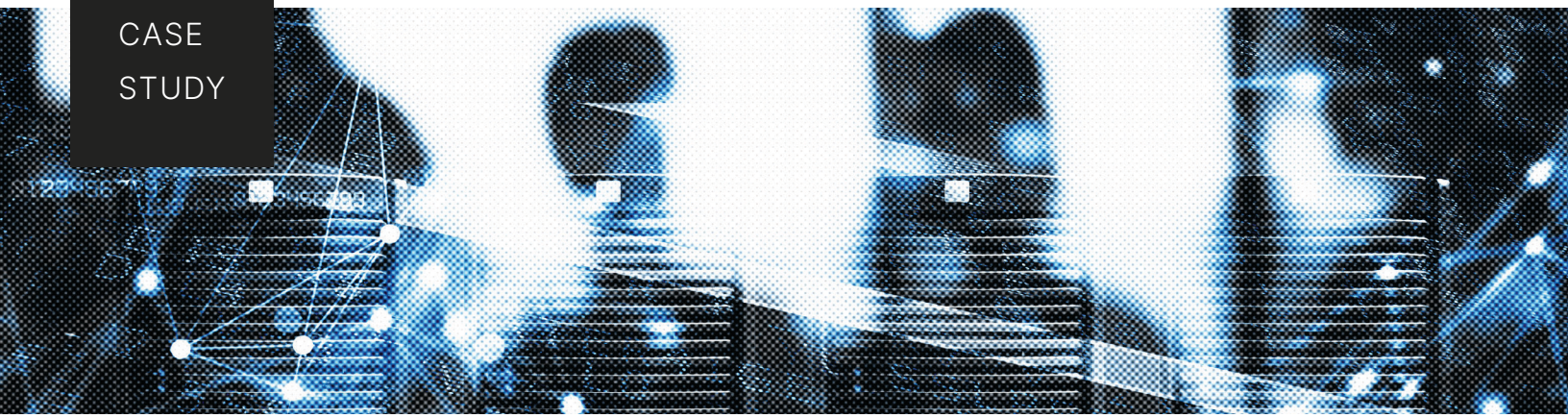
Recorded Future®

CASE STUDY



Visma Evolves Worldwide Security Program with Recorded Future®

Centralized analysts use the Recorded Future Intelligence Cloud to equip 170 autonomous teams with actionable insights into threats and vulnerabilities

VISMA

Use Cases:

Threat hunting; dark web monitoring; brand impersonation detection (domain abuse, including typosquats); leaked data monitoring; vulnerability disclosure monitoring; location & event risk monitoring

Challenge:

Curating security intelligence to drive incident response, threat hunting, and vulnerability management across multiple teams and regions

Solution:

The Recorded Future Intelligence Cloud, including:

- Threat Intelligence
- Vulnerability Intelligence
- Brand Intelligence
- Geopolitical Intelligence
- Identity Intelligence

Outcomes:

- Internal teams and senior leaders alerted to risk across diverse threat landscape
- Risk assessment and security decision-making streamlined for M&A execution
- Enabled automation and actionable intelligence across Visma Security Program
- Intelligence-led approach to security helps Visma stay ahead of evolving threats

Headquartered in Norway, Visma is a federation of 170 individual companies that benefit from shared infrastructure, services, and business development support. The company's 14K employees provide secure, innovative software solutions to more than 1.5 million customers in Europe and Latin America.

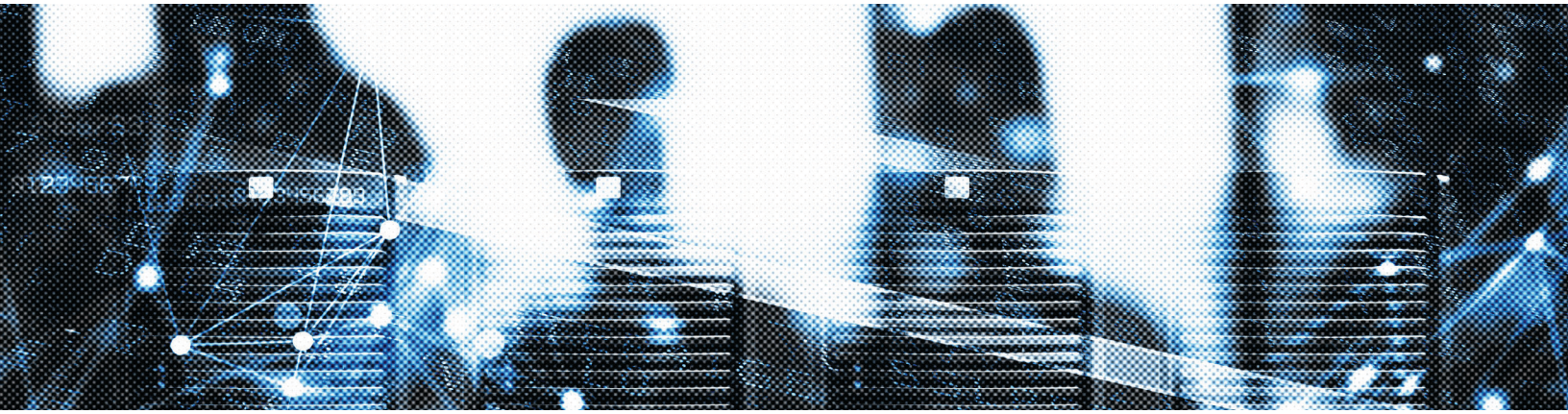
CSO Espen Johansen first brought Recorded Future aboard to gain actionable insights, analytics, and automation capabilities through intelligence to drive scale and agility. Johansen recalls changing his team's strategy after witnessing the power of the Intelligence Cloud firsthand.

"We were contemplating building a cyber threat intelligence platform in house," he says, "but after learning about Recorded Future and the depth of their open source intelligence, data collection and analysis, it was clear we couldn't build a better service for our delivery teams without extensive effort and time."

Security Operations Manager Catalin Curelaru, who leads Visma's Infrastructure Security Program and Cyber Threat Intelligence (CTI) service based on Recorded Future's Intelligence Cloud, says the team extends actionable intelligence from Recorded Future to its many member companies.

"Basically, our team serves our portfolio companies through the Visma Security Program through our CTI service that delivers monitoring capabilities, and by delivering tactical and operations expertise with a few security analysts," he explains. "We offer security services across many teams — it's not a very top-down approach — so we tend to work very laterally serving areas like applications, infrastructure, solutions and people."

Along with helping to prevent attacks, the insights, analytics, and automation Visma gets from Recorded Future play a pivotal role in evolving the security program itself. Curelaru adds, "We launched CTI a couple of years ago focused on product security, now we're building services to support other areas like infrastructure security and vulnerability intelligence."



> "As luck would have it, I could call Recorded Future, who I trusted, to dig deeper into the incident, gather additional intelligence, and ensure proper attribution."
>
> *Espen Johansen,*
> *Chief Security Officer at Visma*

Using actionable intelligence and threat research in the face of a targeted attack

Shortly after bringing Recorded Future on board, Visma experienced a highly targeted cyber attack. "It started about seven days before they hit us," Johansen recollects the campaign that began with a command and control domain followed by phishing attacks targeting employees, credential stuffing, and the compromise of an old Citrix server. With stolen user credentials, the intruders escalated their privileges, moved laterally, then exfiltrated Active Directory Hive.

With the help of Recorded Future, they didn't go unnoticed. "We discovered the attack at the moment of exfiltration and immediately launched blue team efforts to prepare for, and stop, the second wave — the real purpose of the attack," Johansen says. "Through existing security programs, coordinated response of our security teams, and good advice from our partners, we were able to prevent client data from being compromised."

Recorded Future's Insikt Group analyzed the intrusion, and determined the cyberespionage campaign was conducted by the Chinese state-sponsored threat actor, APT10. "As luck would have it, I could call Recorded Future, who I trusted, to dig deeper into the incident, gather additional intelligence, and ensure proper attribution," Johansen recalls, adding that the team partnered with Recorded Future to publish an in-depth analysis of the attack so other teams could deflect the threat.

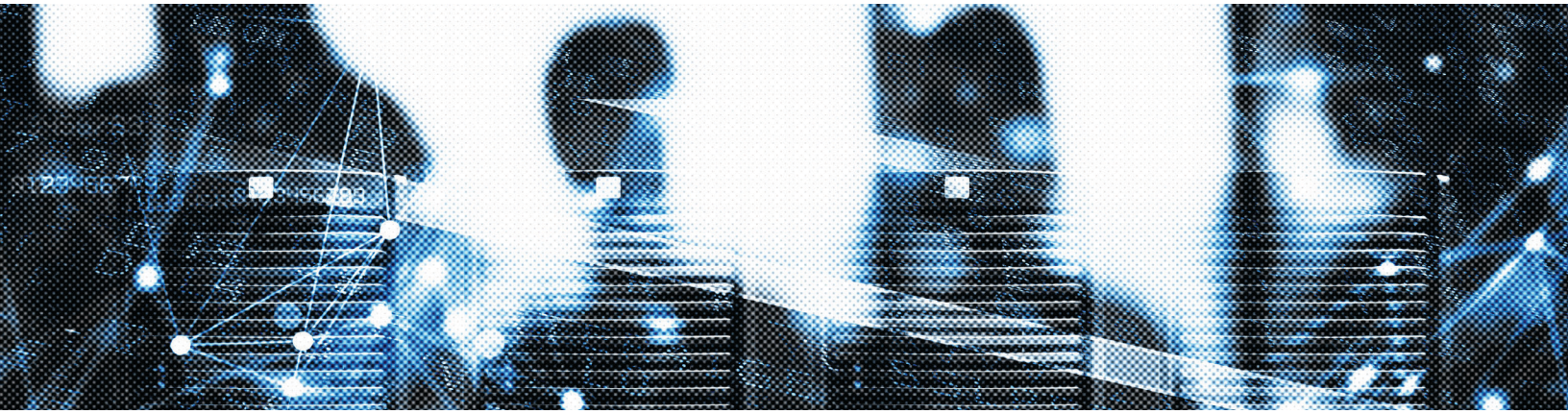
"The Recorded Future report contains indicators of compromise and methodologies that other people can read," the CSO explains. "They can learn how this actor works, in detail, then prepare their own defenses. If you don't share these stories, you're depriving the public of the ability to defend itself."

Automated threat monitoring speeds resolution

Security analysts within the Visma ecosystem routinely rely on the Intelligence Cloud to surface risk from their dynamic threat landscape. By easily customizing watch lists and alerts, the Visma team can track dark web activity, hostile brand mentions, typosquats, chatter about pending attacks, and vulnerabilities impacting Visma's entire technology stack.

"We build in lots of alerts on certain keywords in order to help prevent potential events or incidents," Curelaru says. "Alerting through Recorded Future has been very helpful, especially when we're looking for very specific operational intelligence like mentions on different code repositories or forums."

The team leader recollects one occasion when Recorded Future alerted the team to publicly exposed code on a GitHub repository and resolution took place quickly. Actionable intelligence also accelerated mitigation of a significant vulnerability in Microsoft Outlook by delivering context around which Visma companies used the popular email application.



"We are also able to detect infostealers, the first entry points for the bad guys and cyber criminals," Curelaru says. "Overall, Recorded Future makes some very good catches we wouldn't otherwise have visibility into."

Threat & Geopolitical Intelligence help support M&A decisions and onboarding

As Visma continues its decades-long strategy of growth through mergers and acquisitions, Recorded Future adds value at every stage. Curelaru says the Threat and Geopolitical Intelligence Modules inform strategic decisions about prospective partners, industries, and territories — while accelerating the security onboarding process.

"We use Recorded Future to do due diligence as we assess companies during the M&A phase so that we know what to expect," he explains. "We create reports that show whether companies have had cybersecurity incidents in the past, and if they've tried to make that information unavailable for some reason."

Upon engaging acquired companies, Visma provides support but allows existing teams to remain autonomous. "We serve our companies that utilize the central Visma Security Program, and also offer support for those that have their own security experts" Curelaru explains. "If a company has its own security department or a different vision for cybersecurity, they can still have their own view. We're not trying to drive the controls, but we do at least want to have some baselines and know their levels of maturity."

Visma's unique growth strategy constantly brings new security teams into the fold and gives analysts access to powerful tools and services like CTI. At the same time, the Intelligence Cloud lets the central security team stay ahead of risk from Visma's fast-growing digital presence.

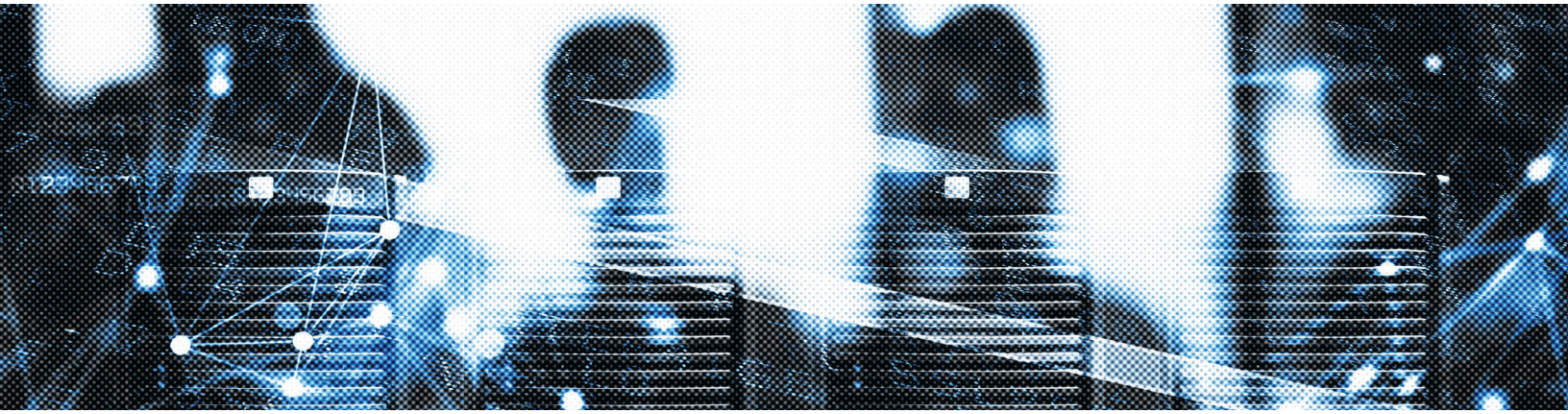
"Recorded Future is a key source of intelligence that we use for IOCs when we're doing threat hunting," explains Curelaru. "If an alert gets triggered by the Recorded Future malware logs sourcing, it could be an employee of Visma and we're responsible for those devices. The alert means we need to do some hunting internally to see what device could be compromised, when the compromise happened, and why we didn't catch it with the other EDR tools we have in place."

Intelligence helps business leaders stay informed in the face of the Russia-Ukraine Crisis

Along with helping to prioritize incident response and threat hunting efforts, targeted threat intelligence equips the team to forewarn business leaders about possible risk from world events. Having weathered the global pandemic, the focus shifted to tracking conflict in the Ukraine.

"We operate in Finland, Poland and Romania so we monitor the region for cyber risk that could be relevant to us very carefully," Curelaru says. "In the beginning it was things like, 'What were the triggers? What were the cyber operations a month before the war started?' With Recorded Future's Ukraine Resource Center and other sources, we were able to see different types of wipers and attacks happening in the region."

When the conflict began, the Visma team relied on research from the Recorded Future's Insikt Group® and the Geopolitical Intelligence Module to help them get context on the threats arising from the war. "The reports were very informative," Curelaru says. "Recorded Future helps the security team curate intelligence so we can give brief keynotes to top management on what they should care about most. The Geopolitical Intelligence Module gives our team a good understanding of what physical security threats our leadership needs to care about as we assess intelligence from different sources."



> We've flipped traditional security on its head. By delivering integrated, actionable intelligence into team workflows, the attention to security becomes embedded in team culture."
>
> *Espen Johansen*

Encouraging security maturity across the company

The Visma Security Program takes a modern approach to incenting autonomous companies' to augment their cyber defenses. By gamifying their program, the team encourages the autonomous companies to move up the maturity ladder by allowing them to earn and redeem points based on their security practices. Using Recorded Future is one of the hallmarks of a more mature company.

"Through the Visma Security Program we offer a gamified approach to security maturity level for our companies and applications. Based on certain onboarding criteria companies can be covered by our endpoint protection service and/or the CTI service," Curelaru explains "By bringing all the pieces together in this gamified tool, we get a better picture of which companies and applications are more mature and what controls they use. A company that uses a security scanning service or CTI service built on Recorded Future, along with other security services, might be at the platinum level."

Automation promotes efficiency

As the program evolves, Visma looks to integrate threat intelligence into more security operations. Curelaru says the group plans to leverage Recorded Future's automation capabilities to maximize efficiencies and promote closer collaboration.

Every time I see a new feature, I ask, 'Do we have API on this in order to be able to automate it?'" Curelaru says. "Automation delivers the value for the Infrastructure Security Program and we're also planning to incorporate Recorded Future intelligence into a redesign of our Infrastructure Vulnerability Management Service. When we see a vulnerability with a higher risk score, we use the tool to collaborate with multiple teams to assess the impact on the different companies that we have."

Intelligence-led approach keeps Visma at the forefront

Visma's transparency and intelligence maturity positions the organization as an authority on cybersecurity best practices. At the end of the day, the CSO says leading with intelligence translates into empowerment.

"We've flipped traditional security on its head," Johansen states. "By delivering integrated, actionable intelligence into team workflows, the attention to security becomes embedded in team culture."