CASE STUDY

VISMA COMBATS THREATS, AUTOMATES SECURITY, AND EMPOWERS TEAMS WITH SECURITY INTELLIGENCE

OVERVIEW

Visma is an IT and business cloud services managed service provider (MSP) that empowers organizations with innovative technology to simplify and digitize core business processes. Headquartered in Oslo, Norway, Visma serves more than a million customers across Scandinavia and parts of Europe.

Challenge

As one of Europe's leading software companies, Visma has a decades-long history of innovation with acquisitions at the core of its strategy. Today, Visma is a federation of more than 145 individual companies, 350 product teams, 5,000 developers, and 11,000 employees. While each of these independent companies share infrastructure and services, they are self-managed and responsible for the entire lifecycle of their service — including security.

A centralized product security team oversees this diverse mix of global product teams to maintain the highest security standards and defend against targeted attacks across all Visma products. Led by director Espen Johansen, the team focuses heavily on empowering developers with analytics and automation tools that bridge the gap between innovation and security governance, and promote confident decision-making and self-reliance. For Espen — a former ethical hacker, armed forces veteran, data science junky, and guest lecturer on software security at several universities — intelligence is the name of the game. He's drawn to innovations that push boundaries with predictive analytics, AI, and machine learning to drive agility and make intelligence actionable — and even fun. This approach has informed his journey to build a world-class cyber threat intelligence center at Visma.

Solution

"We were contemplating building a cyber threat intelligence platform in house, but after learning about Recorded Future from a trusted colleague, I was intrigued by their methodology and launched a small POC," recounts Johansen. "We were impressed by some of the findings, along with the depth of their open source intelligence and beautifully executed data collection and analysis. It was clear we couldn't build a better service for our delivery teams without extensive effort and time." So, Visma brought Recorded Future on board.

> We've flipped traditional security on its head.
>
> -Espen Johansen

Initially, the team used Recorded Future to surface security risks like typosquat domains and address them quickly with internal take-down capabilities. Security engineers soon came to rely on the platform to help systematically prioritize security incidents, better understand the current threat landscape, and gain deeper insights on the movements of threat actors.

Around that time, in late summer 2018, Visma experienced a highly targeted cyber attack. "It started about seven days before they hit us," Johansen recalls. First, a command and control domain was spawned. A surge in phishing attacks targeting employees followed. Then, a credential stuffing attack opened the door to an old Citrix server. With stolen user credentials, the intruders escalated their privileges, moved laterally, then exfiltrated Active Directory Hive.

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. 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. And 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."

Recorded Future's Insikt Group analyzed the intrusion, and determined the cyberespionage campaign was conducted by a Chinese state-sponsored threat actor, APT10 (also known as Stone Panda, menuPass, CVNX), in an effort to gain access to networks and steal valuable intellectual property or gain commercial advantage.

But Visma wasn't done. A firm believer in industry collaboration, Johansen teamed up with Recorded Future to publish an in-depth analysis of the attack. "We're not the ones who should own the shame. It is the attacker who owns the shame," he says. "The Recorded Future report contains indicators of compromise and methodologies that other people can read. 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."

Visma's transparency and intelligence maturity is lauded by industry pundits and has positioned the organization as a regional authority on cybersecurity best practices.

Results

Today, any development team within Visma can access the Recorded Future platform, known internally as the Visma Cyber Threat Intelligence Service. Hundreds of teams rely on the platform to continuously monitor for and prioritize relevant threats. By easily customizing watch lists and alerts based on their specific needs, they can track things like Visma accounts or secrets distributed on underground markets, hostile brand name mentions, typosquat domains, chatter about pending attacks on company infrastructure, vulnerabilities, and exploits impacting the company's tech stack, and much more. This actionable intelligence helps automate manual security processes, maximize efficiencies, and drive faster, more confident decisions. Meanwhile, custom threat research — such as Recorded Future's ongoing analysis of the COVID-19 pandemic — provides timely, analytical insights to help mitigate organizational risk.

As Visma continues to expand its portfolio through acquisitions, security intelligence from Recorded Future also helps streamline M&A due diligence by providing relevant insights on potential partners, industries, and territories — while accelerating the onboarding process.

Leading with security intelligence is all about empowerment. "We've flipped traditional security on its head," explains Johansen. "By taking a bottom-up approach that delivers integrated, actionable intelligence into team workflows, the attention to security becomes embedded in team culture."

> We discovered the attack at the moment of exfiltration and immediately launched blue team efforts to prepare for, and stop, the second wave.
>
> -Espen Johansen