VECTRA

Customer Story | Information Technology & Services

Advens Achieves 100x Investigation Workload Reduction and Exposes Compliance Risks with Vectra AI

Advens is a leading managed security services provider (MSSP) based in France, specializing in managed detection and response. Its Security Operations Center (SOC) supports nearly 200 clients, delivering continuous threat monitoring and swift incident response across complex and rapidly evolving environments.

Organization
Advens

Industry
Information Technology & Services

The Challenge
Advens struggled with fragmented visibility and noisy, inconsistent alert data, making effective threat hunting and investigation difficult.

The Solution
By deploying Vectra AI, Advens gained unified visibility across network, cloud, and identity, enabling faster detection and more efficient, accurate investigations.

Security Transformation

Platform value at a glance

Through its deployment of Vectra AI, Advens has empowered its SOC to deliver more comprehensive threat detection, investigation and response capabilities, while dramatically improving analyst efficiency and effectiveness across their client portfolio.

Vectra AI's Impact	Outcome
Coverage	• Unified visibility across network, identity, and cloud environments • Detection of sophisticated attacks where EDR can't be deployed • Reduced client exposure by containing attack paths before they could be exploited
Clarity	• Provided human-readable alerts with rich context, streamlining investigation effort • Used AI-driven triage and stitching to link related detections across client environments
Control	• Accelerated investigations by up to 100x, scaling services without increasing headcount • Improved client compliance posture with rapid discovery of high-risk behaviors across internal assets • Delivered client-ready reporting to highlight risks such as expired certificates and misconfigurations

The Challenge

Fragmented visibility, slow investigations, and missed compliance gaps

Advens operates as an extension of its clients' security teams. In many cases, limited documentation and architectural context make it difficult to establish visibility across the modern network spanning cloud, identity, and on-prem environments. As a result, the SOC team must adapt to a wide range of setups and maturity levels.

"Often, our clients don't have a complete picture of the environment," said Sebastien Wojcicki, Head of Operations & Security Excellence at Advens. "There's no global architecture schema, so it's hard to know who is using what, where administrators are connecting from, or what exactly needs to be covered."

The team had to stitch together fragmented logs from disparate tools — firewalls, EDR, and domain controllers — each with different formats and no unified view. This lack of standardization and continuity made thorough threat hunting and investigation difficult for many clients.

"Security wants to block threats. IT wants everything to be up and running. We're in the middle," Wojcicki shared.

The Solution

Achieving unified visibility across network, identity, and cloud

Advens deployed the Vectra AI Platform to close visibility gaps and enhance threat detection, investigation, and response across its diverse client environments. With broader visibility into network, identity, and cloud activity, the team gained a clearer view of attacker movement and could respond more effectively.

"The first thing that surprised me was the visibility Vectra AI brings," Wojcicki said. "Once deployed, you can see what's happening across the network — communications, behaviors. This is something we don't usually get, even on sensitive DMZs."

"NDR gives us critical visibility into file server activity that we can't get elsewhere. We can't deploy EDR or enable logging. It's too resource-intensive. But with metadata visibility, we've tracked data leaks and even caught someone copying a CEO's personal information onto their laptop to pay for their home internet."

Rather than relying on siloed log sources and manual pivoting, the team now uses enriched metadata and behavioral detections to spot unusual activity faster.

"Firewall logs show us which systems are communicating, but they don't tell us what was actually exchanged. Figuring that out takes time. And because each log source uses a different format, we're constantly switching between tools to piece everything together," Wojcicki explained.

Vectra AI centralizes that process. With contextual alerts that correlate activity across domains, analysts can quickly investigate suspicious behaviors without needing to stitch together information from multiple systems.

Metadata also extends the investigation window, often 14 to 30 days, giving Advens the ability to uncover subtle patterns without the cost and complexity of storing raw logs.

"The longer the retention, the better the outcome," says Wojcicki. "It gives us the time we need to investigate subtle, low-priority behaviors that could easily escalate."

Compliance value: surfacing hidden risk

Vectra AI's metadata search and investigation capabilities aren't just used for threat detection — they're a core part of Advens' compliance offering.

"We get absolutely a lot of value from hunting for compliance-based violations in the platform. Even during early test deployments, the first thing we do is crawl Vectra AI's metadata to uncover bad behaviors, things like ID documents stored in open file shares or users accessing sensitive HR files. It gives CISOs immediate visibility to say, 'This behavior needs to stop.' That not only prevents these issues from staying hidden, but also helps customers avoid audit findings, costly fines, and the reputational damage that comes with compliance failures," Wojcicki explained.

Clients gain immediate visibility into violations they never knew existed. Even common violations, such as expired certificates, lateral movement from unmanaged assets, or unauthorized BYOD behavior, are surfaced within hours or days.

This capability is especially powerful for clients in regulated industries or public sector environments, where compliance audits are frequent and unforgiving.

"The first thing that surprised me was the visibility Vectra AI brings. Once deployed, you can see what's happening across the network — communications, behaviors. This is something we don't usually get, even on sensitive DMZs."

SEBASTIEN WOJCICKI
Head of Operations & Security Excellence at Advens

"Investigating Vectra AI alerts takes 100 to 1,000 times less effort than dealing with raw firewall logs. The platform gives us context we used to spend hours trying to build ourselves."

SEBASTIEN WOJCICKI
Head of Operations & Security Excellence at Advens

Accelerating investigations and stopping multi-domain attacks

Beyond visibility, Vectra AI also improved how the team operates day to day. The intuitive query system, powered by enriched metadata and DSL-like syntax, enabled rapid access to relevant entities (devices, users, behaviors).

Even purple team exercises have benefited. Vectra AI regularly detects simulated attacks that go unnoticed by other tools, especially when attackers use unmanaged devices or operate outside traditional coverage zones.

These improvements have made investigations faster and more intuitive, especially when working across hybrid environments.

"Having a joint view of M365 and on-prem environments is really helpful. That ability to pivot is essential. It lets us investigate faster and with more accuracy." Wojcicki added. "Many clients still don't believe multi-domain attacks are real until we show them. We run simulations, like golden HTML attacks, and Vectra AI consistently detects them, while Microsoft tools miss the cross-domain movement."

"NDR gives us critical visibility into file server activity that we can't get elsewhere. We can't deploy EDR or enable logging—it's too resource-intensive. But with metadata visibility, we've tracked data leaks and even caught someone copying the CEO's personal information onto their laptop to pay for their home internet."

SEBASTIEN WOJCICKI
Head of Operations & Security Excellence at Advens

The Results

Stronger detection. Streamlined investigations. Scalable impact.

Advens has cut investigation effort dramatically by shifting away from log-heavy workflows.

"Investigating Vectra AI alerts takes 100 to 1,000 times less effort than dealing with raw firewall logs," Wojcicki shared. "The platform gives us context we used to spend hours trying to build ourselves."

Vectra AI's behavioral detections have also revealed subtle threats, including an exfiltration attempt from a smartphone connected through a docking station — activity that would have been buried in raw logs.

"We saw suspicious exchanges and unusual queries that helped us pinpoint the activity," Wojcicki said. "Vectra AI gave us the detail we needed to understand what was happening."

These gains don't just benefit Advens analysts; they scale across the MSSP's client base. With less noise and more actionable context, Advens can contain threats earlier, reduce client exposure, and deliver timely reporting on risks that could compromise compliance posture — reinforcing trust in their security operations.

LEARN MORE

Vectra Investigate Datasheet | Threat Hunting Blog | Vectra Investigate Demo

For more information please contact us: Email: info@vectra.ai | vectra.ai