VECTRA

Customer Story | Government

How This Government Authority Slashes Alert Fatigue with Vectra AI

Organization
Government Authority in the Middle East

Industry
Government

The Challenge
This government authority's sprawling network, consisting of over 2000 IPs and a Microsoft 365 environment, produced a constant stream of security alerts — overwhelming analysts and making it difficult to identify critical threats.

The Solution
Vectra AI was the solution of choice due to its ability to cut through noise, prioritize critical alerts, and empower analysts with actionable insights.

The Results
With a streamlined workflow and improved visibility, the security team gained confidence in their ability to detect and respond to threats effectively. Key improvements include reduced alert fatigue, improved threat detection, and significant MTTR improvements.

The Challenge

A sprawling network

Security teams often face a deluge of alerts, many of which are false positives or low-priority issues. This was the case for a government authority in the Middle East responsible for managing critical national infrastructure. Their sprawling network, consisting of over 2000 IPs and a Microsoft 365 environment, produced a constant stream of security alerts — overwhelming analysts and making it difficult to identify critical threats.

"When we were introduced to Vectra in 2021, we knew it was something special. It offers an incredibly streamlined, personalized, and efficient experience."

The Solution

Finding an ally in Vectra AI

To address these challenges, the government authority turned to Vectra AI — a network detection and response solution that acts like a smart filter, cutting through the noise to spotlight genuine threats. In doing so, their analysts now save valuable time while significantly reducing the risk of overlooking potentially devastating attacks.

"When we were introduced to Vectra in 2021, we knew it was something special. It offers an incredibly streamlined, personalized, and efficient experience," said the Cybersecurity Operations Manager.

The platform's intuitive interface and ease of use have also played a crucial role in its widespread adoption. The Cybersecurity Operation Manager elaborates, "Even our junior analysts can easily navigate the platform, investigate triggered alerts, and map activities occurring within the platform and network."

Expanding the arsenal: a multi-pronged defense

To further enhance their security posture, the government authority expanded their use of Vectra AI by adopting additional tools. Vectra Stream integrates with their existing Zeek infrastructure (an open-source network security monitor), enriching Zeek's logs with AI-driven insights. This integration provides them with comprehensive visibility into network activity, including active attacks, behavioral anomalies, and previously unknown threats. Armed with enriched data, this security team can now proactively identify and mitigate threats before they cause harm.

"Before, we lacked visibility into active directory attacks and net flow. Stream helps us fill that gap. It's an amazing solution," said the Cybersecurity Operations Manager.

Expanding their security toolkit, the team has begun incorporating Vectra Match, a signature-based detection tool, into their existing defenses. By identifying known threats based on their unique signatures, Vectra Match enhances their ability to respond swiftly and effectively to diverse attacks.

The Results

Enhanced threat detection and response capabilities

The security team saw immediate impact from their Vectra AI implementation, with analysts experiencing improvements in several key areas, including:

- **Reduced alert fatigue:** By filtering out the noise and prioritizing the most critical threats, Vectra AI significantly reduces the number of alerts that analysts need to review.
- **Improved threat detection:** Vectra AI's advanced capabilities enable the team to spot elusive threats, including compromised accounts, unusual activity patterns, and potential vulnerabilities.
- **Accelerated incident response:** By providing clear, actionable insights, Vectra AI helps the team react to threats with increased speed and precision.

Specific improvements in Mean Time to Respond (MTTR) and Mean Time to Detect (MTTD) for various threats are summarized in the table below:

Threat	Before deploying Vectra AI	After deploying Vectra AI
Abnormal admin traffic	2 to 4 days (MTTR)	1 hour (MTTR)
Unauthorized traffic within the same VLAN	Not possible to detect (MTTD)	30 mins (MTTR)
C2 traffic hidden in encrypted channel	5 days (MTTR)	2 hours (MTTR)
Pass the hash attack	3 days (MTTR)	1 hour (MTTR)
Privileged account theft	10 days (MTTR)	2 hours (MTTR)

"Vectra has been a game-changer for us," said the Cybersecurity Operations Manager, "It helps us see threats that we might otherwise miss, and it gives us the confidence to know that we're focusing on the right things."

By providing enhanced threat detection and response capabilities, Vectra AI has empowered this government authority to shift from a reactive to a proactive security stance. This approach, coupled with the platform's adaptability to evolving threats, ensures that they are well-equipped to navigate the complexities of an ever-changing threat landscape.

"Vectra has been a game-changer for us. It helps us see threats that we might otherwise miss, and it gives us the confidence to know that we're focusing on the right things."

Cybersecurity Operations Manager
Government Authority

"Before, we lacked visibility into active directory attacks and net flow. Stream helps us fill that gap. It's an amazing solution."

Cybersecurity Operations Manager
Government Authority

Read more customer stories

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

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