VECTRA

Customer Story | Manufacturing

How this manufacturing company stopped not one, but two attacks, with Vectra MDR

The Challenge

Attackers flock to a hybrid environment

As this company grew more and more global, their environment stretched to both on-premises and on the cloud. This hybrid environment was targeted by many hybrid attackers who used various tactics to launch ransomware and malware attacks.

2023 OT Ransomware Attack in Brazil

Vectra AI detected a potential WannaCry ransomware attack on the company's Brazil server, which was initiated by a bad actor on a USB stick used on a company device.

2023 E-Mail Malware Attack on India

Vectra AI detected Command & Control in a couple of user devices located in India, signifying a possible malware attack. Attackers bypassed prevention controls through a phishing email, then searched for administration privileges to advance albeit without success.

The Solution

24x7x365 coverage gets ahead of hybrid attackers

Both attacks were detected by Vectra MDR analysts who closely monitored the company's systems.

2023 OT Ransomware Attack in Brazil

Vectra MDR quickly escalated the infected host to the company and recommended host isolation with an email and phone call. Within 30 minutes of the notification, the host was isolated. The next day, the company enacted remediation by blocking the USB, patching the environment for the WannaCry virus, and conducted a full scan and device clean-up under the guidance of Vectra MDR.

2023 E-Mail Malware Attack in India

Vectra MDR escalated the strange detections to the company through email and later, in a phone call. Within 30 minutes, the device was isolated. The next day, the device was cleaned up under the guidance of Vectra MDR.

Organization

Global Manufacturing Company

Industry

Manufacturing

The Challenge

14 production facilities in 8 countries
5,000-6,000 employees

The Solution

After growing globally, the customer added Vectra MDR to their Vectra AI solutions to cover hybrid attacks.

The Results

Two attacks, one ransomware and the other malware, were detected and stopped by Vectra MDR, protecting the customer's global systems and preventing costly recoveries.

Customer Benefits

Vectra MDR adds a layer of protection to hybrid environments

Vectra MDR provides:

- 24x7x365 global monitoring on the customer's environment, even beyond the customer's working hours
- Direct consultation and recommendations for response actions
- Access to industry experts with years of experience in security and the Vectra AI Platform
- AI-driven triage and prioritization of real attacks instead of false positives

> **"We started Vectra's MDR service a couple years ago to keep our response times faster with the help of analysts on the Vectra MDR team. They provided 24/7 expertise and offered consultation on understanding detections to our local IT to us. In addition, the MDR team's P1 escalations via phone call allows us to quickly analyze and minimize risk."**
>
> **IT Manager**
> Cybersecurity

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