# Protect your OT Environment with Vectra NDR and Vectra Match

**Digital transformation in business operations is driven by numerous technological initiatives, including in OT (operational technology) environments. With these innovations come many changes that present new challenges.**

In an IT and OT world, attackers are bypassing prevention controls, infiltrating, compromising credentials, gaining privileged access, moving laterally and exfiltrating sensitive corporate data through a means of credential phishing, breaching existing IT applications, committing supply chain attacks among other methods.

When it comes to OT attacks, infiltrating your OT environment is the first step. This can be achieved by a threat moving through your network perimeter — bypassing firewalls, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). The challenge for security teams boils down to how rapidly an attack is detected, especially once it penetrates your network perimeter.

### Key challenges addressed:

- Keeping your business operations intact no matter what
- Increasing SOC analyst workflow efficiency
- Growing IT & OT, cloud complexity, vulnerabilities and exploits

## Vectra Match for air-gapped environments

To keep a critical network safe, a common practice has traditionally been to establish an air gap, which equals disconnecting your specific network from *"untrusted"* or less secure networks, the internet or even the outside world in general. This dramatically helps reduce the overall risk of a cyberattack occurring. However, implementing an air-gapped environment is not failproof.

Security teams oftentimes create a two-way protocol (such as those used in legacy SIEM and IDS systems) and implement many common industrial protocols into a one-way connection. Some IDS solutions also have the functionality to use data diodes to enable two-way communications that simply cannot work without the ability to respond on the same session.

Vectra Match with Vectra NDR provides the threat detection and response you need for your entire network:

- **Accelerate threat hunting and investigation workflows:** Identify network-based indicators of compromise (IOCs) such as domains and IPs, as well as malicious attacker behavior to align your SecOps team and narrow down the most critical and urgent threats on your air-gapped environment.
- **Optimize existing investments in your IT and OT** by combining NDR and Suricata capabilities that are deployed on a single sensor.
- **AI-enabled operations optimize SecOps workflows** and investments with consolidated security tooling and signature-based context into your existing SIEM tools, processes and workflows.

## Key capabilities

### Signal clarity

Combining NDR and Suricata provides SecOps teams with the insights needed for better threat hunting and precise separation of threats and noise.

### Better threat detection and response

Gain clarity on known and unknown threats across your OT environment by combining Vectra Match signature context and the power of Vectra NDR with Security AI-driven Attack Signal Intelligence™.

### Optimized workflow

Optimize your current SecOps security solution investments and architecture with Vectra Match by consolidating the number of sensors in your infrastructure.

## What it means for your OT environment

With Vectra NDR and Vectra Match your organization is more resilient to OT attacks:

- Up and running with actionable detections in days if not hours.
- Future-proof your defense as your IT and OT attack surface expands.
- Erase the fear from IT and OT high-risk threats going undetected and executing.

Your security analysts are more effective:

- Reduce analyst burnout with accurate detection of malicious true positives.
- Increase analyst throughput by accelerating investigation and response.
- Builds analyst expertise and skills hunting and defending against both known and unknown threats.

With Vectra NDR and Vectra Match your organization is more resilient to exploits attacking your OT environment. Vectra Match ingests intrusion detection signature context for more efficient and effective threat investigations and hunting. The goal is to gain complete clarity about known and unknown threats across your network by combining Vectra Match signature context and the power of Vectra NDR with Attack Signal Intelligence.

**Resources to Learn More**

## About Vectra

Vectra® is the leader in hybrid cloud threat detection and response. Vectra's patented Attack Signal Intelligence detects and prioritizes threats across public cloud, SaaS, identity, and networks in a single platform. Vectra's Attack Signal Intelligence goes beyond simple anomaly detection to analyze and understand attacker behavior. The resulting high-fidelity signal and deep context enables security operations teams to prioritize, investigate and respond to cyber-attacks in progress sooner and faster. Organizations worldwide rely on the Vectra platform and MDR services to stay ahead of modern cyber-attacks. Visit www.vectra.ai.

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