Maximize Your Enterprise Managed Detection and Response (MDR) Services

How to tightly integrate MDR services into your security organization

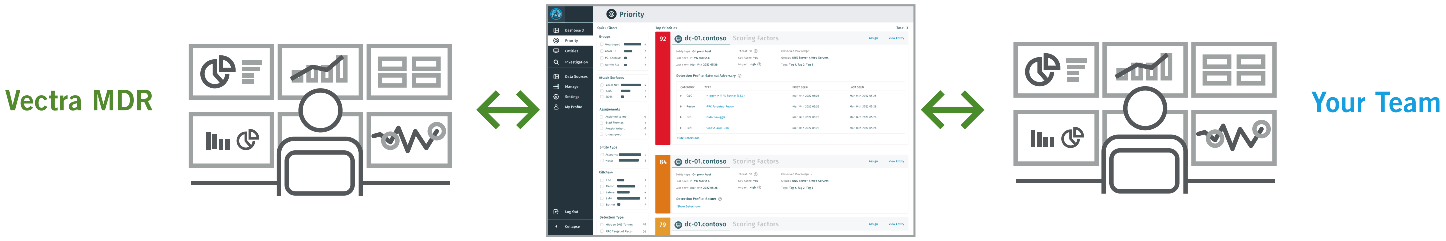
This best practices document highlights effective ways to maximize your investment in enterprise MDR services. Regardless of the structure of your security team, it can be used by leaders, architects, analysts or other team members to help answer the question: "are we maximizing the value of our MDR services?"

Key Challenges

- **24/7/365 threat detection and response** is necessary to detect, investigate and respond to today's attacker tactics, techniques and procedures (TTPs).
- **Coverage for ever-expanding environments** requires a 24/7/365 eyes-on-the-glass service to proactively investigate and stop attacks across public cloud, SaaS, identity and networks.
- **The spiral of more** tools, noise, rules and tuning generates a heavier workload and eventually burnout among security teams.

To stay ahead of attackers across today's hybrid cloud landscape, it's increasingly important to make sure security controls are being optimized 24/7/365. Vectra MDR empowers your organization to keep the control in a **shared responsibility model** with 24/7/365 expertise around the Vectra platform to best utilize Security AI-driven **Attack Signal Intelligence™** and reduce manual tasks, alert noise and analyst burnout. Whether you leverage Vectra MDR to augment your current team or to outsource security operations completely, you gain human analysis and judgement along with your Vectra platform.

How to optimize your MDR services



Shared responsibility

Whether your team is outsourcing security operations or utilizes MDR services for additional resources, it's important to have a complete view of ownership along with transparency around the roles and work that is being done. Vectra MDR logs all actions that are made by both the MDR team and customer teams for full transparency as incidents get investigated and resolved. You know exactly what steps have been taken on your behalf.

Collaborative onboarding

When onboarding a new MDR services team, it's important to have and discuss documented run books. This will enable the MDR team with the ability to mitigate and remediate incidents with a greater capacity during incident response and be more empowered to stop malicious threats with urgency. It's also good practice to reevaluate runbooks often after onboarding — adding or modifying continually so your MDR team is clear on the process and has the best chance for success.

Seamless integration

You rely on multiple tools to accomplish several critical tasks. Your MDR services should integrate into your existing solutions and cloud infrastructures while reducing complexity with valuable expertise. Vectra accomplishes this by providing investigation expertise, configuration optimization and global threat and attack insight. Vectra also natively covers threats across four of your five attack surfaces — cloud, SaaS, identity, and networks while integrating with top EDR (Endpoint Detection and Response) solutions for **complete attack coverage, signal clarity and intelligent control**.

Erase noise and unknown threats

Overwhelming alert noise can result in attackers being overlooked. Your MDR provider should be an expert capable of continuously tuning your threat detection and response solution to ensure that noise levels and alerts remain at a minimum, so you only focus on what matters. The Vectra platform automates alert triage that reduces alert noise by over 80%, while our MDR analysts remain in communication with your team, so when new events or information enter the system — it can be tuned as efficiently as possible.

Extension of your security team

Your MDR provider should be an extension of your security team where experienced security analysts are proactively enabling your security operations. Vectra MDR does this by providing:

- 24/7/365 monitoring and proactive investigations.
- Deep expertise about investigations in the Vectra platform.
- Insight into global threats and emerging attacks.
- Proactive Vectra deployment customization and health checks.
- Shared responsibility empowerment — you maintain control.
- 24/7/365 available communication.
- Recurring meetings with security experts covering customer and global trends, security posture and network events.

Keys to success:

1. Work with an MDR provider that fills your security gaps, allowing you to have as much or as little control as desired.
2. Your MDR provider should be an extension of your team.
3. Your MDR provider should erase the unknown threats that put your organization at risk.

Be empowered to detect, investigate and respond to threats 24/7/365

The combination of today's ever-expanding hybrid cloud landscape and cyber attackers' advanced tactics, creates a multitude of unknown threats for security teams to address. To successfully defend against these threats — 24/7/365 threat detection and response is recommended. MDR services deliver the cybersecurity skills you need to detect, investigate and respond to threats with 24/7/365 human intelligence. MDR analysts and your security team work together across your platform for complete visibility, collaboration and faster resolution times — operating with expertise as an extension of your team. Vectra MDR services enables your organization to keep the control in a **shared responsibility model**, whether you leverage the service to augment your current team alongside the Vectra platform or to outsource security operations completely — you gain complete visibility and transparency of the roles and work that's being completed.

Learn more about Vectra's Managed Detection and Response

About Vectra

Vectra® is the leader in cyber threat detection and response for hybrid cloud. 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 enable 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 cyberattacks.

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