Best Practices for the Hybrid SOC

Why the modern SOC requires a shared-responsibility model.

Today's SOC teams face a vicious spiral of more. According to the Vectra AI State of Threat Detection report:

- More attack surface to cover – 63% of SOC analysts say their attack surface has significantly increased in the past three years.
- More alerts to manage – SOC analysts receive an average of 4,484 alerts a day and are unable to deal with over two thirds (67%) of them, while 83% of the alerts they look at are false positives.
- More burnout and turnover – 3.4 million open cybersecurity jobs remain and 67% of SOC analysts are considering leaving or actively leaving their jobs.

To break this vicious spiral of more, security teams are embracing a hybrid SOC model to augment in-house talent and resources, with talent and resources from third-party Managed Detection and Response (MDR) services. When selecting an MDR service for your hybrid SOC model, start with the challenges you need to solve and the value outcomes you want. From there, you can begin to set your requirements.

Key challenges to consider

What challenges do you need to solve?

The challenges SOC teams face can differ from one organization to another. It is important to focus on the three to five core problems you are trying to solve. Common challenges SOC teams face include:

- Lack of real-time threat detection
- Lack of context understanding to aid in investigation & threat hunting
- Prolonged response time to threats
- Lack of coverage and intelligence controls across hybrid cloud
- Security resource shortage
- Security skills shortage
- Increasing SOC workloads, decreasing productivity
- SOC Analyst burnout, turnover
- Keeping pace with advanced hybrid cloud attacks
- Increasing tool complexity
- Increasing mean-time-to metrics
- Keeping systems up to date and healthy

What value outcomes do you want?

- Improve security posture and maturity
- Prove cyber resilience to modern, emerging attacks
- Deliver global 24x7x365 security operations
- Develop SOC analyst skills and expertise
- Retain and grow SOC talent
- Improve mean-time to detect and respond to attacks
- Gain insights to keep pace with emerging attacker methods
- Define and deliver on service level agreements (SLAs)
- Decrease analyst workload by offloading activities to a third party
- Implement threat hunting practices and/or mature your program

Key Criteria

What requirements should you set?

Focusing on the specific challenges you need to solve and defining the value outcomes you want enables you to set your hybrid SOC requirements. Create your hybrid SOC requirements checklist to begin assessing and evaluating third-party services. Your checklist may include:

- Does the MDR service provide global coverage?
- Does the MDR service provide experienced talent 24x7x365?
- What attack surfaces does the MDR service monitor?
- Does the MDR service have domain expertise in those attack surfaces?
- How many years of experience do the MDR service analysts have?
- How does the MDR service keep up to date on the latest threat landscape?
- How does the MDR service share insights with your in-house analysts?
- Does the MDR service provide dedicated or shared analysts?
- How many dedicated SOC analysts does the MDR service provide?
- How does the MDR service communicate with in-house analysts?
- Does the MDR service have clearly defined SLAs?
- Does the MDR service offer flexible service models?
- Does the MDR service manage system health and uptime?

Keys to success

How Vectra MDR fits into your hybrid SOC

Vectra MDR is 24x7x365 managed detection, investigation and response for hybrid and multi-cloud enterprises. Built on top of the Vectra AI Platform, Vectra MDR provides you with the extended skills and expertise, shared responsibility and technology savvy insights needed to address your challenges and deliver on your value outcomes.

Extend Skills and Expertise

- In-house team of hybrid attack detection and response experts with 10+ years of experience.
- Collaborate and communicate with Vectra MDR analysts to build your analysts' hybrid attack skills and expertise.
- Gain insights and best practices crowdsourced by Vectra MDR analysts to bolster your hybrid attack defense.

Shared-Responsibility Model

- Shared hybrid and multi-cloud attack expertise.
- Shared roles and responsibilities for attack detection, investigation, hunting and response.
- Shared analytics on attacker behavior and emerging attacker TTPs.
- Shared insights into emerging attacker behavior and threat campaigns.
- Transparency, communication and collaboration with shared SLAs, metrics and reporting.

Vectra AI Platform Expertise

- Global 24x7x365 threat monitoring and detection.
- Continuous detection tuning, triage and system health checks.
- Incident response playbook definition and process optimization.
- Technology integration and workflow automation.
- Live in-app analyst collaboration and communication.
- Fast operationalization improves time to value.

Vectra AI Managed Detection and Response (MDR) delivers the cybersecurity skills you need to detect, investigate and respond to advanced hybrid and multi-cloud attacks 24/7/365. Vectra MDR analysts and your in-house SOC team work side by side in the Vectra AI Platform to collaborate and communicate in real-time detecting, prioritizing, investigating and stopping attacks from becoming breaches.

Learn more about the Vectra AI Platform

Explore the Vectra AI Analyst Platform

Schedule a Demo

About Vectra AI

Vectra AI is the pioneer of AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single Open XDR platform. The Vectra AI Platform with patented Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks in 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