DATA SHEET

Vectra Sidekick MDR Service

Vectra Sidekick MDR is a 24/7/365 eyes-on-glass service that proactively investigates malicious activity surfaced by Vectra Detect. It acts as your "sidekick" by applying human intelligence and judgment to help stop ransomware attacks, insider threats and nation-state adversaries before damage is done.

The Sidekick analysts bring the expert opinion to help you get the most out of Vectra while simultaneously building knowledge and skill within your team.

Human intelligence that doesn't sleep

AI is critical for early detection of attacks. We all know, however, that adding human intelligence to the mix delivers the best outcomes – whether to ring alarm bells or to de-escalate an automated response action.

The Sidekick team is watching around the clock, bringing human analysis and judgment when your team is sleeping or otherwise unavailable. A comforting thought in a world where ransomware gangs regularly strike in the dead of night.

Expert opinion on everything Vectra

Given the number of security tools in use, it can be challenging for everyone in your team to understand how to get the most out of any one tool – including Vectra.

The Sidekick team is comprised of security and Vectra subject matter experts. They understand the nuances of the models and bring broad experience in investigating and resolving incidents quickly and efficiently. The Sidekick analysts bring the expert opinion to help you get the most out of Vectra while simultaneously building knowledge and skill within your team.

The AI Advantage

The Sidekick cloud always runs the latest AI focused on enhanced prioritization, campaign analysis, and early identification of disruptive attacks including modern RansomOps. This gives the Sidekick team the advantage in seeing and responding to emerging threat campaigns even faster than an individual user can.

Your Sidekick is a force multiplier for your security team

SideKick MDR acts as a security team multiplier by deploying experienced security analysts to help you fully utilize Vectra's AI to see threats early and stop breaches. With Sidekick MDR layered on top of the Vectra platform, you get:

A boost to your security team with access to experienced security analysts who help expel sophisticated adversaries and ransomware actors.

Expertise, context, and clarity regarding the early telltale signs of an attack, threat or ransomware surfaced by Vectra Detect with analysts to proactively assist in rapid response.

24/7/365 proactive monitoring so you know when a priority 1 threat or ransomware detection requires immediate action and response.

Customization of your Vectra deployment tailored to your unique environment, business objectives and industry risks. This includes customizing controls, providing expert recommendations, environment trends and metrics and accelerating investigations.

Early Threat Identification with rich context

Sidekick analysts provide answers to threat detections, threat background, crowdsourced intelligence and industry trends. Sidekick analysts improve security posture with each analysis, arming teams with expertise, process and procedure enhancements as well as improved incident management. Expert security analysts with the Sidekick MDR team will be available to present and discuss findings from regularly scheduled threat investigations and answer questions about the Vectra solution.

Why Vectra Sidekick MDR

Sidekick MDR goes beyond typical 24x7 monitoring, acting as a trusted security partner to help with strategic activities including threat intelligence, playbook design, and tuning.

> "It was like getting a new pair of binoculars. You don't realize what you're missing until you can see with absolute clarity.
>
> The insights we get all day, every day, are critical. It makes me a better analyst and a better engineer."

Charles Davidson
IT Security Analyst
Private Research Institution

Triage and platform tuning

Security analysts with the Sidekick services team have amassed extraordinary knowledge from observing countless threat behaviors in hundreds of Vectra deployments. The vast insights from the Vectra platform help teams distinguish between malicious versus benign behaviors. With Vectra Sidekick MDR, security teams get support to create custom filters to approve authorized behaviors and even receive individualized suggestions to make the triage process more effective.

Trusted security partner

Vectra is all-in to make sure your organization achieves its security goals by building a more capable and resilient environment. This means transparency and collaboration are present throughout the process. Sidekick analysts work alongside security teams, to provide insights that augment and complement your existing security operations processes.

Sidekick MDR offerings

Sidekick MDR service investigates and responds to threats by combining the expertise of Vectra security analysts with the AI-driven Threat Detection and Response Platform that automatically detects and prioritizes threats.

You have distinctive needs, and Vectra offers two options of the Sidekick MDR service.

Deliverable/Capabilities	Standard	Premium	Description
Security Expertise	✓	✓	Service delivered by experts with extensive backgrounds in threat investigation, incident response, red teaming, malware analysis, ransomware detections, and threat attribution
24/7 Eyes on Glass	✓	✓	Sidekick analysts will have eyes on glass 24x7x365; conducting investigations in the customer environment with the help of Vectra's unique prioritization algorithms
Global Insights	✓	✓	Sidekick analysts conduct investigations for companies across industries and geolocations; giving them a unique view of the ever-changing threat landscape
Added Context	✓	✓	Sidekick analysts will provide findings and recommendations in the system for easy access
Email Alerts	✓	✓	An analyst will email when further investigation is warranted
Closed Loop Communication		✓	Follow-up communication to a designated point of contact after initial email alert
Proactive Health Checks		✓	Sidekick analysts will further analyze traffic, hostID, VSA
Quarterly Briefings and Security Recommendations		✓	Quarter meetings where metrics from Sidekick, lessons learned & best practices are reviewed
Sidekick Reports		✓	Sidekick analysts will send a report providing information about system and service statistics
Proactive Configuration and Onboarding		✓	Sidekick analysts will help with activities such as creation of groups and identify key in-product integrations
Triage Expertise		✓	Sidekick analysts will provide triage support and recommendations
Access to Sidekick Analysts		✓	Chat directly with Sidekick analysts

For more information please contact us at info@vectra.ai.

Email info@vectra.ai vectra.ai

Version: **101921**