VECTRA
SECURITY THAT THINKS.®

DATA SHEET

Vectra Sidekick Services

Overview

The Vectra® Sidekick Services subscription portfolio gives you access to a team of security analysts who will customize a set of prioritized recommendations to enhance your overall security posture.

Vectra Sidekick Services extend the value of your organization's investment in the Cognito® Network Detection and Response (NDR) platform by enabling you to work with Vectra security experts who meticulously analyze the results from your Cognito deployment to identify potential security events in your organization.

The Sidekick services team will deliver a weekly report as well as meet with you regularly to present findings from threat investigations, discuss detections that have been identified, and address challenges and questions about your Cognito platform.

Service highlights

Regularly scheduled threat investigations

An expert security analyst with the Sidekick services team will spend time remotely analyzing events in your Cognito platform with the goal of identifying events of potential security interest to your organization.

These events are annotated with tags and notes about the details within Cognito for review and are added according to a documented and agreed-upon standard.

Weekly reporting

Sidekick services include the delivery of weekly reports that highlight hosts and detections of interest found during threat investigations. The report details critical, high and other events with recommendations for response processes. Reports also track low-level issues and provide supporting data and security artifacts with appropriate recommendations.

Vectra Sidekick Services

Security analysts will work closely with you to deliver the Vectra Sidekick Services package you choose.

	Regular reporting	Active monitoring business hours	Active monitoring 24 x 7
Regularly scheduled threat investigation	✓	✓	✓
Weekly report	✓	✓	✓
Recurring review meeting	Monthly	Bi-weekly	Bi-weekly
Dedicated analyst	—	✓	✓
Triage and platform tuning services	—	✓	✓
Operational playbook creation	—	✓	✓
Proactive notification of Priority 1 events	—	Local business hours	24 x 7 x 365
Annual on-call hours for ad-hoc expert assistance	20	40	40

Technical review sessions

An expert security analyst with the Sidekick services team will be available to present and discuss findings from regularly scheduled threat investigations and answer questions about the Cognito platform.

Proactive notification of Priority 1 events

A Sidekick services security analyst will notify your security team in advance of weekly reports or scheduled review meetings if a critical detection, host or security event is identified that requires immediate attention and response.

Playbook creation and design

With Sidekick services, you will have access to our advisory services to assist in creating standard operating procedures for your security team, improving your security processes and helping you to successfully resolve future cyberthreats.

Your security team will directly benefit from our extensive experience responding to the world's most advanced threats, building modern security operations centers and securing business-critical data environments.

Triage and platform tuning

Security analysts with the Sidekick services team have decades of in-depth experience that no other company can match. Our team has amassed extraordinary knowledge from observing countless threat behaviors in hundreds of Cognito platform deployments. The vast insights from the Cognito platform help you distinguish between malicious versus benign behaviors. With Vectra Sidekick Services, security teams can create custom filters to approve authorized behaviors and even receive individualized suggestions to make your triage process more effective.

Ad-hoc incident expert assistance

You can request ad-hoc expert assistance to further review specific events in your Cognito platform environment. This service is instrumental if serious data exfiltration behaviors occur or if a high-priority malware outbreak requires incident-response expertise.

Your Sidekick services incident-response expert will assist you by providing Cognito platform insights that augment and complement your existing security operations processes. Once you request expert assistance, Vectra will promptly assign a security analyst experienced in incident response to work remotely with your team.

Requirements

In order for Vectra to deliver Vectra Sidekick Services, you will need to enable the Cognito support VPN, provide access to Cognito Recall™, and accept the default Sidekick services access terms as outlined in Schedule K of the Vectra terms of service. In addition, acceptance of the enhanced Sidekick services access terms as outlined in Schedule K of the Vectra terms of service is required for Sidekick Active Monitoring.

For more information about Vectra Sidekick Services, please contact a service representative at sales-inquiries@vectra.ai.

Email info@vectra.ai vectra.ai

Version: **072120**