VECTRA®

Cognito® Sidekick Service

Service overview

The Cognito Sidekick Service from Vectra® is a subscription program that gives you access to our dedicated team of security analysts, who will customize a set of prioritized recommendations to enhance your overall security posture.

Sidekick extends the value of your organization's investment in the Cognito platform with Vectra security experts who will meticulously analyze the results from your Cognito deployment to identify potential security events in your organization. Vectra 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 descriptions

Vectra security analysts will work closely with you to deliver the service package you choose.

Sidekick Essentials. Designed for smaller deployments with requirements for visibility into the health and security posture of the monitored infrastructure.

Sidekick Standard. Designed for security operations that desire dedicated analysts and experts to enhance a program's operational efficiency.

Sidekick Global. Designed for global security operations with multiple locations around the world.

	Sidekick Essentials	Sidekick Standard	Sidekick Global
Regular threat investigations	✓	✓	✓
Weekly report	✓	✓	✓
Recurring technical review meeting	Monthly	Biweekly	Biweekly
Dedicated analyst	–	✓	✓
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	80

Service highlights

Regularly scheduled threat investigations

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

These events will be annotated with tags and notes within Cognito Detect™ to inform your team about the resulting analysis. In cases where events of interest are found only within Cognito Recall™, a tag and note will be placed on relevant hosts in Cognito Detect with a reference to the details within Cognito Recall for review. Tags and notes are added according to a documented and agreed-upon standard.

Weekly report

Your Vectra security team will deliver weekly reports that highlight hosts and detections of interest that have been uncovered during Sidekick 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.

Technical review sessions

An expert security analyst from Vectra 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

Vectra will proactively notify your security team in advance of weekly reports or scheduled review meetings if during a threat investigation a critical detection, host or potential security event is identified that requires immediate attention and response.

Playbook creation and design

You will have access to our advisory services to assist in creating standard operating procedures for your security team, improving your security processes and ability 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.

Ad-hoc incident expert assistance

You can request ad-hoc expert assistance to further review specific events within your Cognito environment. This service is instrumental in the event of a confirmed breach or high-priority malware outbreak that requires incident-response expertise.

Your 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 via the Vectra support portal, we will promptly assign a security analyst experienced in incident response to work remotely with your team.

Vectra staffing

The Vectra security-analyst team is comprised of Cognito platform experts, security operations center analysts, and experienced incident responders. The team is a worldwide organization that provides extensive global coverage. Vectra will provide the appropriate staff to deliver your specific services.

Requirements

In order for Vectra to deliver the Cognito Sidekick Service, you will need to enable the Cognito support VPN and provide access to Cognito Recall. In addition, the Cognito brain appliance requires external SMTP routing to allow hosts and detections to be assigned to the Sidekick analyst team.

Service schedule

The Cognito Sidekick Service is delivered remotely during business hours, which is 9 a.m. to 5:30 p.m. local time from Monday through Friday, excluding Vectra and local holidays. With Sidekick Global, service hours for proactive notification of Priority 1 events are extended to 24 x 7 x 365.

For more information about the Cognito Sidekick Service, please contact a service representative at +1 408 326 2034 or email us at sales-inquiries@vectra.ai.

VECTRA®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai