VECTRA
SECURITY THAT THINKS®

DATA SHEET

# Vectra Advisory Services

## Overview

Vectra® Advisory Services give you access to strategic advice from expert security practitioners to shape your security operations capabilities, improve your security posture and enhance your incident response capabilities.

Chief information security officers (CISOs), security architecture leaders and heads of security operations can draw upon the decades of professional experience of Vectra security consultants.

**Vectra Advisory Services are tailored to your organization's specific needs to build and scale your security operations. Our core expertise includes SOC transformation, benchmarking and metrics, and incident response planning.**

Vectra works with you to develop recommendations, requirements and processes that will create agile and effective security incident responses to help you get more from your security technology investments, people and processes to reduce the risk of breach.

AI – with its intelligence-driven operations – is replacing manual human tasks, enabling security teams to focus on more vital operational responsibilities. This has prompted the widespread adoption of machine learning, automation, and behavior-based threat detection-and-response methodologies for the security operations centers (SOCs).

Vectra Advisory Services are tailored to your organization's specific needs to build and scale your security operations. Our core expertise includes SOC transformation, benchmarking and metrics, and incident response planning.

**"62% of detected incidents resulted in a breach of information, devices, or system reported."– The SANS Institute[1]**

## HIGHLIGHTS

**SOC TRANSFORMATION:** Vectra consultants perform analysis and workshops mapped to industry standards and compliance regulations to deliver a SOC maturity assessment report with a plan of processes and methodologies to improve your security team's performance and analyst agility.

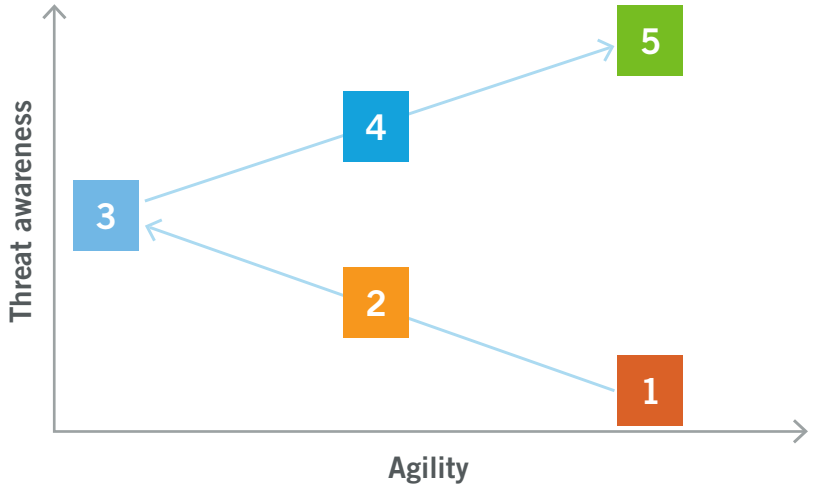
**BENCHMARKING AND METRICS:** Vectra presents data by specific industries and highlights relevant differences between them. This data is scored and compared to your own data over a specified time range. Vectra then collects metrics that show how your detection and response performance compares to industry peers who also use the Cognito platform.

**INCIDENT RESPONSE PLANNING:** Vectra guides you through breach scenarios and events that occur in the real world and explains how to detect and respond in a timely manner to avoid these catastrophic incidents.

[1] SANS Institute SANS 2019 Incident Response (IR) Survey, 2020

## SOC transformation

Slowing down attackers is only part of the security challenge; we must speed up defenders, too. Organizations must quickly detect, understand, respond, and recover from the attackers that successfully penetrate their systems. A mature SOC benefits from faster response time to security events as well as increased threat awareness and agility to implement corrective actions.




Measuring security operations maturity

| Maturity | Typical Detection | Typical Response | Risk Awareness |
|---|---|---|---|
| Predictive Defense | Internal (Hunting, Deception) + External | Highly Proactive | Very High |
| Intelligence Driven | Internal (Hunting) + External | Threat/Adversary Driven | High |
| Process Driven | Internal (Hunting) + External | Service Driven (SLAs) | Medium |
| Tool Driven / Signature Based | External | Tool Driven | Low |
| Reactive / Adhoc | External, User Report | Reformat, Reinstall, Restore | Very Low |

Vectra consultants perform analysis and workshops mapped to industry standards and compliance regulations to deliver a SOC maturity assessment report with a plan of processes and methodologies to improve your security team's performance and analyst agility. Vectra Advisory Services ensure a smooth transition to a behavior-based threat detection-and-response approach to bring your SOC to full maturity.

## Benchmarking and metrics

It is important for security and the business to speak the same language to ensure that security operations are delivering value. This requires metrics that demonstrate business value that span people, processes and technology.

Measurements – such as visibility across the attack lifecycle, efficacy of security tools, and overall team performance for incident response – provide context that helps business leaders better understand the state of their security program and how to improve it.

In addition to internal SOC metrics, understanding trends and operational performance from similar organizations in the same industry enables CISOs to better understand and plan around the threat landscape. This also paves the way for prioritizing risks that require mitigation and identifying opportunities to improve security agility.

Vectra presents data by specific industries and highlights relevant differences between them. This data is scored and compared to your own data over a specified time range. Vectra then collects metrics that show how your detection and response performance compares to industry peers who also use the Cognito platform.

Vectra presents this information in an easy-to-comprehend, visually appealing manner that makes a compelling and convincing case for presentations to board members and senior stakeholders.

## Incident response planning

Time is a precious commodity when dealing with a serious security incident and can make the difference between a contained issue or a damaging breach.

Vectra guides you through breach scenarios and events that occur in the real world and explains how to detect and respond in a timely manner to avoid these catastrophic incidents.

During workshops, Vectra reviews the strategic and operational aspects of publicly disclosed breaches to help CISOs and senior security leaders map, conceptualize and apply new knowledge and insights in the context of your own SOC.

After having a tailored incident response plan in place, with appropriate resources Vectra will help you test and validate your new threat detection and response capabilities through formal red-team attack testing.

This testing approach is designed to harden your security operations team's ability to operate under the pressures and ambiguity of a cyberattack and develop valuable learning and development opportunities for self-improvement.

## Summary

Vectra Advisory Services enable CISOs and other security leaders to align their SOC capabilities with business objectives to minimize risk. Vectra identifies opportunities to reduce the risk of a breach, improve security operations efficiency, ensure compliance, and strengthen security in the cloud.

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

Email info@vectra.ai vectra.ai


Version: **071920**