VECTRA
SECURITY THAT THINKS.®

DATA SHEET

Microsoft and Vectra complete the vision of the SOC visibility triad

As evidenced by unprecedented cybercrime, traditional security defenses have lost their effectiveness. Threats are stealthy, acting over long periods of time, secreted within encrypted traffic or hidden in tunnels. With these increasingly sophisticated threats, security teams need quick threat visibility across their environments.

In the Gartner research report "*Applying Network-Centric Approaches for Threat Detection and Response*" published March 18, 2019 (ID: G00373460), Augusto Barros, Anton Chuvakin, and Anna Belak introduced the concept of the SOC Visibility Triad.

In this note, Gartner advises:

"The escalating sophistication of threats requires organizations to use multiple sources of data for threat detection and response. Network-based technologies enable technical professionals to obtain quick threat visibility across an entire environment without using agents."[1]

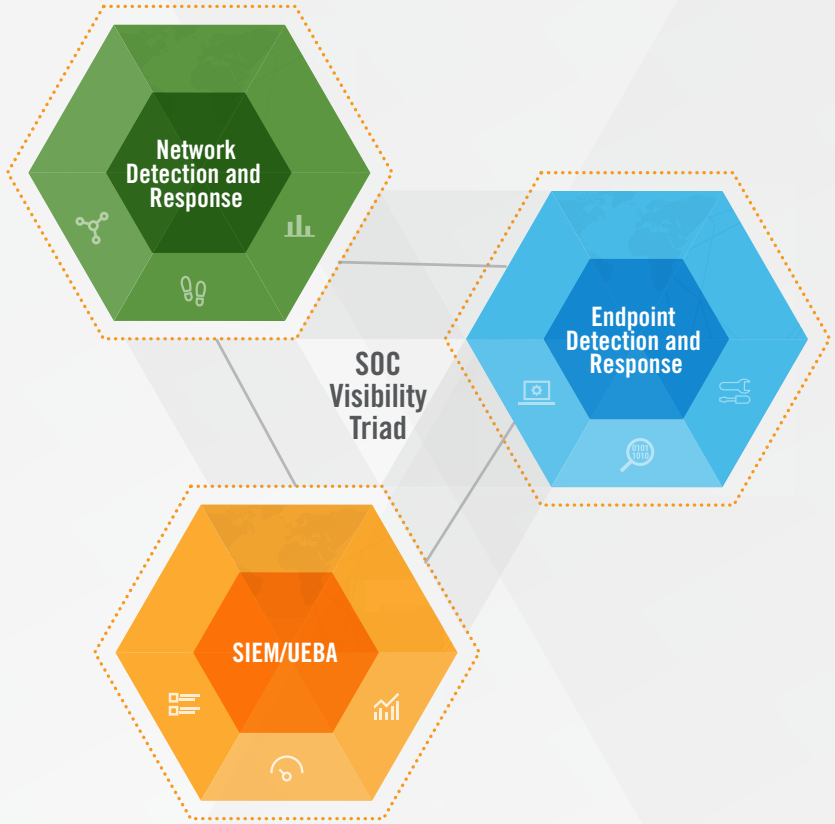

Figure 1. SOC Visibility Triad

Source: Gartner, Applying Network-Centric Approaches for Threat Detection and Response, Augusto Barros et al., March 18, 2019, ID G0037346

According to the research, "modern security operations tools can also be represented with an analogy to the 'nuclear triad,' a key concept of the Cold War. The triad consisted of strategic bombers, intercontinental ballistic missiles (ICBMs) and missile submarines. As shown in Figure 1, a modern SOC has its own nuclear triad of visibility, specifically:

1. **SIEM/UEBA** provides the ability to collect and analyze logs generated by the IT infrastructure, applications and other security tools. (See "SIEM Technology Assessment" for details.)

2. **Endpoint detection and response** provides the ability to capture execution, local connections, system changes, memory activities and other operations from endpoints. (See "Endpoint Detection and Response Architecture and Operations Practices" for details.)

3. **Network-centric detection and response (NTA, NFT and IDPS)** is provided by the tools focused on capturing and/or analyzing network traffic, as covered in this research. "[2]

This three-prong approach gives SOCs increased threat visibility, detection, response, investigation, and remediation powers.

Microsoft Defender Advanced Threat Protection

Endpoint compromises are all too common, whether from malware, unpatched vulnerabilities, misconfigurations, or inattentive users. Mobile devices can be easily compromised on public networks, and then reconnected to the corporate network, where the infection spreads.

Microsoft Defender Advanced Threat Protection (ATP) is a unified endpoint security platform for preventative protection, post-breach detection, automated investigation, and response.

Microsoft Defender ATP behavioral-based and cloud- powered threat and malware protection prevents sophisticated and never-before-seen threats from impacting devices. It provides deep optics into the operating system, including memory and kernel, help to detect 0-days,advanced attacks, and data breaches.

This visilbity helps security analysts spot patterns,behaviors, indicators of compromise or other hidden clues. That data can be mapped against other security intelligence feeds to detect threats that can only be seen from inside the host.

Vectra network detection and response

Network metadata is the most authoritative source for finding threats. Only traffic on the wire reveals hidden threats with complete fidelity and independence. Low-resolution sources, such as analyzing logs, only show you what you've seen, not the fundamental threat behaviors that attackers simply can't avoid as they spy, spread and steal.

The Vectra platform provides an aerial view of the interactions between all devices on the network. By applying security research and data science, Vectras AI behavioral models detect in-progress attacks, prioritized and correlated to compromised host devices. It collects and stores key network metadata and augments it with machine learning and advanced analytics to detect suspicious activities on enterprise networks.

With a native integration to Microsoft Defender ATP, a security team can pair the aerial view from Vectra with the ground level view from Microsoft Defender ATP. Analysts can view context from Microsoft in the Vectra platform and automatically disable accounts or execute Microsoft Defender ATP host isolation directly from the Vectra console. Security teams can also accelerate investigations with an immediate pivot into Microsoft Defender ATP with local context from Vectra used as the parameters for Microsoft Defender ATP scope and scale.

Microsoft Azure Sentinel

For decades, security teams have relied on SIEMs as a dashboard to security activities across their IT environment. SIEMs collect event log information from other systems, provide data analysis, event correlation, aggregation and reporting.

Azure Sentinel is able to ingest syslogs from Vectra Cognito and Microsoft Defender ATP. When an incident occurs, analysts can use pre-built applications and Vectra dashboard widgets to quickly identify the affected host devices and accounts. They can more easily investigate to determine the nature of an attack and if it succeeded.

A SIEM also can communicate with other network security controls, such as firewalls or NAC enforcement points, to direct them to block malicious activity. Threat intelligence feeds can enable SIEMs to proactively prevent attacks as well.

Microsoft and Vectra – fulfilling the vision of the SOC Visibility Triad

Security teams fulfill the vision of the SOC Visibility Triad with native integrations between the Vectra Cognito platform, Microsoft Defender ATP and Azure Sentinel. They are empowered to answer a broader range of questions that cannot otherwise be answered in isolation. For example;

- Did another asset begin to behave strangely after communicating with the potentially compromised asset?
- What service and protocol were used?
- What other assets or accounts may be implicated?
- Has any other asset contacted the same external command-and-control IP address?
- Has the user account been used in unexpected ways on other devices?

With native integrations that bring together context from each data source, integrated enforcement like account disable and host isolation and pre-built SOC Visibility dashboards, these solutions combine to deliver well coordinated responses, enhance the efficiency of security operations and reduce the dwell times that ultimately drive risk for the business.

For more information please contact a service representative at sales-inquiries@vectra.ai.

[1] Gartner, *Applying Network-Centric Approaches for Threat Detection and Response*, Augusto Barros et al., March 18, 2019, ID G00373460
[2] Ibid.

Email info@vectra.ai vectra.ai