The ultimate 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 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]

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.

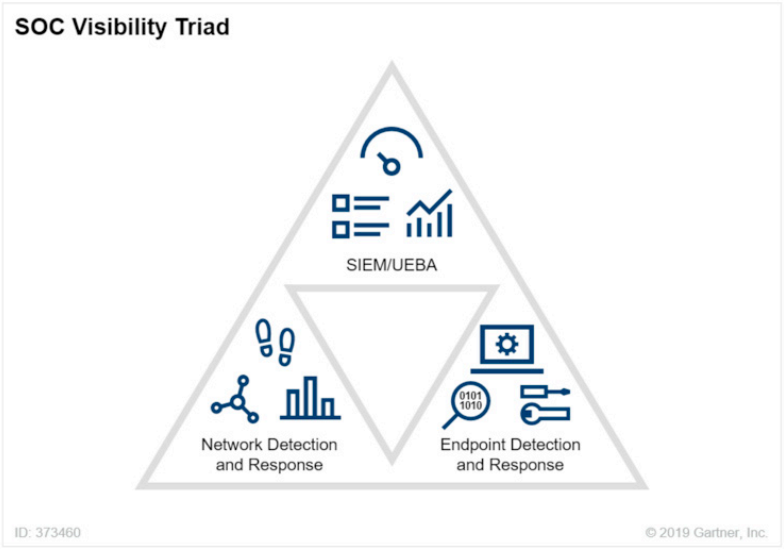

Figure 1. SOC Visibility Triad
Source: Gartner, Applying Network-Centric Approaches for Threat Detection and Response, Augusto Barros et al., March 18, 2019, ID G0037346

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

CrowdStrike endpoint detection and response

Endpoint compromises are all too common, whether from malware, unpatched vulnerabilities or inattentive users. Mobile devices can be easily compromised on public networks, and then reconnected to the corporate network, where the infection spreads. Internet-of-things (IoT) devices are notoriously unsecure.

An EDR solution offers more sophisticated capabilities than traditional antivirus by recording all system activities and events and providing real-time visibility of the processes running on a host or device and interactions among them.

EDR captures execution and memory activities as well as system changes, activities and modifications. Data can be mapped against other security intelligence feeds to detect threats that can be seen only from inside the host. The enhanced visilbity provided by EDR helps security analysts spot patterns, behaviors and indicators of attack before a compromise can occur.

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.

An NDR solution collects and stores key network metadata and augments it with machine learning and advanced analytics to detect suspicious activities on enterprise networks. NDR builds models that reflect normal behavior, and enriches the models with both real-time and historical metadata.

NDR provides an aerial view of the interactions between all devices on the network. In-progress attacks are detected, prioritized and correlated to compromised host devices.

NDR provides a 360-degree, enterprise-wide view—from public cloud and private data center workloads to user and internet-of-things devices.

Splunk Enterprise SIEM

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

Integrating threat detections from both EDR and NDR can make a SIEM an even more powerful tool, enabling security analysts to stop attacks faster. Additionally, threat intelligence feeds can enable SIEMs to more effectively expose attacks. Using these event and threat data sources, the SIEM can help analysts quickly identify the affected host devices and routes of attack. They can more easily investigate to determine the nature of an attack and if it succeeded.

Further, leveraging a security orchestration, automation and response (SOAR) solution like Splunk> Phantom, security teams can automate response decision making, and execute standardized response templates via security tool orchestration.

Based on alerts generated by a SIEM, a SOAR tool can orchestrate rich responses that include directing network security controls, such as firewalls or NAC enforcement points, to block malicious activity. Affected endpoints can be quarantined and tickets created for full remediation.

CrowdStrike, Vectra and Splunk – A powerful triad to find and stop cyberattacks

Security teams that deploy the triad of NDR, EDR and SIEM are empowered to answer a broader range of questions when responding to an incident or hunting for threats. For example, they can answer:

- 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?

Together, they lead to fast and well coordinated responses across all resources, enhance the efficiency of security operations and reduce the dwell times that ultimately drive risk for the business.

Economic loss due to cybercrime is predicted to reach $3 trillion by 2020, according to the World Economic Forum. Nation-states and criminals are taking advantage of a borderless digital world, but by adopting a nuclear triad of visibility, a SOC can protect its organization's sensitive data and vital operations.