WHITE PAPER

Federated Security Operations: Integrating Cybersecurity Across Organizations

Executive Summary

Integrating cybersecurity across organizations and jurisdictions is of growing interest in both the public and private sectors. Ransomware has demonstrated that criminal cyber activity can paralyze the operations of critical infrastructure in even well-resourced industries. And, organizations around the world may find themselves in the crosshairs—or at least caught in the crossfire—of destructive state-sponsored cyber action. While the need is urgent because both the threat landscape and the organization's attack surfaces are expanding, the effort should be approached mindfully. This will help ensure the project is realistic based on the available resources, especially people.

Feeling a sense of heightened urgency, many are looking at approaches that include creating information sharing and analysis centers, federating security operations centers (SOCs), setting up centers focused on critical infrastructure or government agency missions, or creating a single "super SOC." Each of these options can be problematic to execute due to complexity, effectiveness, cost, or all three factors.

"Threat actors continued to pound away at organizations (approximately 150,000 individual detections per week) with a variety of new and previously seen ransomware strains, often leaving a trail of destruction in their wake."[1]

Integrated Cybersecurity Is Difficult to Accomplish

The security operations landscape is challenging even within a single enterprise. The difficulties organizations face include:

- **A fragmented network perimeter:** Because of work-from-anywhere, cloud, supply chain, and other initiatives, the attack surface that needs to be secured has grown dramatically.
- **Evasive attacks:** Sophisticated multistage campaigns by malicious actors can evade traditional prevention security and mimic legitimate activity.
- **Data volume:** The volume of security events creates too much "noise" to rapidly and reliably be able to identify, prioritize, and investigate security incidents.
- **Siloed security:** Point security products provide stove-piped and incomplete pictures, prevent automation, and respond too slowly.
- **Overwhelmed teams:** The scarcity of skilled security professionals makes it difficult to hire and retain adequate cybersecurity staff.

The threat landscape is also evolving with an increase in destructive ransomware, state-sponsored attacks, targeted attacks on operational technology (OT) environments, and advanced persistent cybercrime. Due in part to the steady revenues generated by ransomware, cybercrime groups are becoming increasingly cohesive and well-organized, generating more sophisticated threats and increased reconnaissance capabilities. Compared to a year ago, some attacks are also moving with much greater speed thanks to offensive automation through artificial intelligence (AI).

Building Blocks for Success

Orchestrating security across a consortium or network of organizations is more challenging than integrating security within a single organization—even one that has a global footprint and contains diverse operating components. In a multi-organization operating environment, the members often differ widely in capability and resources, and seldom is someone empowered to make decisions and set standards that are binding across organizations. While integrating security operations across multiple (and often disparate) organizations has some different attributes than integrating cybersecurity for a single organization, the fundamental tools and trends that enable success still apply.

AI and machine learning (ML) are critical ingredients. AI has fundamentally transformed the effectiveness of the cybersecurity industry over the past decade. It is now responsible for virtually all malware analysis and for finding anomalies and threats on an automated basis in near real time. A second technology trend is the rise of cybersecurity mesh architectures. These are platforms of products and services from different vendors that can share data and operations to reduce complexity and improve visibility and response.

The intersection between increasingly mature and powerful AI/ML and the consolidation of security solutions into interoperable platforms is a potential game-changer. This AI-powered platform approach turns the size and complexity of the attack surface from a liability into a potential advantage. By making it a composite collection platform that can see adversaries in motion, the AI/ML can make sense of this data, and the controls respond both at the point of attack and globally.

According to Gartner, by 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a cooperative ecosystem will reduce the financial impact of individual security incidents by an average of 90%.[2]

The Goal of Integrated Cybersecurity

Integrating cybersecurity in a multi-organization environment consists of both establishing situational awareness (creating a common operating picture [COP]) and driving response. These functions are related but can be prioritized and developed separately.

Establishing shared situational awareness is a human problem. Machines don't need a threat dashboard or heat map of activity. They can share data ("tip" and "cue" actions) depending on rules and automation. But even when using automated data feeds, producing situational awareness for analysts, cyber defenders, and decision makers is time- and labor-intensive. Problems of information overload and operator fatigue can impede performance and are most likely to occur during a cyber incident or crisis.

There are two distinct approaches to federating awareness:

- Generating a single shared view, which can produce a user-friendly world view, but likely requires a bespoke solution built from scratch.
- Sharing separate perspectives, for example, each SOC has a "repeater" of the views from other SOCs. This is easier to implement, but requires ongoing manual integration by the human analyst, and integration becomes harder as the number of perspectives to be included grows.

If most of the time and effort in the SOC is spent making sense of what is going on, the time devoted to action needs to be highly efficient. There are at least three options to enable joint response:

- **Data-driven:** working from cyberthreat intelligence in common formats (for example, STIX, TAXII)
- **Function-driven:** leveraging key capabilities and commercial products like security information and event management (SIEM) and security orchestration, automation and response (SOAR)
- **Architecture-driven:** working from architecture-level interoperability

The first option focuses on data interoperability and leveraging existing and widely adopted models and standards. The second leverages cybersecurity components such as SIEM and SOAR tools that typically are designed to work in multivendor environments. This approach to integration offloads much of the work to industry partners. The third offloads even more of the burden of integration to the platform and architecture manufacturers. Importantly, these options are not mutually exclusive, especially in a federated and complex ecosystem of networks and capabilities.

The Role of Cyberthreat Intelligence

Cyberthreat intelligence is a key element of both situational awareness and response. It is produced at multiple levels and used for multiple purposes. These include:

- **Tactical intelligence** (turning data into dots): includes information such as digital signatures that can be used by security devices. It is the predominant category of cyberthreat intelligence by volume and its production and use are largely automated (machine to machine).
- **Operational intelligence** (connecting the dots): is information on threat attributes such as tactics, techniques, and procedures (TTPs) that are used to create threat-actor playbooks of patterns of threat-actor activity. These can be used for orchestrating network defender response. Operational intelligence is typically produced or curated by analysts. Quality and focus are often uneven, which can make it difficult to integrate this data across organizations.
- **Strategic intelligence** (making patterns or pictures out of the dots): is information on threat plans and intentions that is significant and compelling enough to drive change in an organization's operational posture or behavior. This information is typically human generated and interpreted. It is relatively rare but can have a significant impact.

"As environments grow noisier with context-free security alerts and a constant flood of log data, it becomes easier for attackers to intentionally create distractions that make it possible for them to conceal their activities inside the network."[3]

Operational, strategic-level intelligence is key for federated SOC situational awareness. In other words, situational awareness comes from integrating information that is relatively low volume and labor-intensive to produce. By contrast, federating response predominantly relies on tactical intelligence, supported by operational-level playbooks on threat actors and activity.

Framing Questions

A roadmap of key steps helps define the needed outcome, to set requirements for data and response time, and to frame an inventory of current capabilities and assets. Here are some key questions to consider:

- ☐ What is the relative priority of shared situational awareness vs. response?
- ☐ What are the requirements in terms of input data (types and quantity) and speed or timeliness of output?
- ☐ Does every participating organization have a SOC? If so, does it have a common operating picture of its own enterprise?
- ☐ How many views need to be integrated?
- ☐ How do member capabilities map to commercial architectures or functional and product solutions?
- ☐ What are the available or projected resources?
- ☐ What are timelines and deadlines for implementation?
- ☐ And perhaps most importantly, does anyone have directive authority to tell the participating centers what to do?

How to Get Started

Most organizations want their integrated, federated security posture to include COP shared across member organizations. Because the bulk of the defenders' time will be spent on generating situational awareness, it will place a premium on automation of response, often within parameters or playbooks set in advance.

Alternatively, organizations may place a lower priority on establishing shared situational awareness, settling for something coarser that indicates the presence or absence of ongoing threats. Instead, they will emphasize providing shared services and integrated response. In other words, this approach chooses to focus on maximizing the impact of defensive action at the expense of a more complete understanding of a threat.

There is no right answer, but the first step is to decide which goal and what capabilities to develop. This should be made through a conscious choice that reflects the needs and priorities of the organizations being integrated and of key mission stakeholders.

How Fortinet Can Help

Fortinet has had a cybersecurity mesh architecture for years, the Fortinet Security Fabric, that spans the breadth of the digital attack surface and features an open ecosystem integrating with data and security services from over 500 Fabric Partner solutions.

FortiGuard Labs is a world-class producer of cyberthreat intelligence, receiving and processing security telemetry from nearly 7 million devices. FortiGuard Labs can be an important external source of the operational information needed to generate situational awareness, as well as a provider of the tactical intelligence needed to drive integrated and automated response.

Fortinet has powerful and proven products such as FortiSIEM and FortiSOAR that can help a single organization or a coalition that wants to pursue functional or product-focused integrated activity.

Summary

Given the extreme sophistication and volume of today's threats, it's critical to integrate security controls for visibility and response. There are many approaches and components to consider and organizations need to explore their options to determine the best solution for their needs. Regardless of approach, it is key to ensure communication, visibility, and fast response across the infrastructure. This can be achieved with an established mesh architecture and effective threat intelligence.

[1] Joe Robertson and Ricardo Ferreira, "CISO Q&A: Ransomware: A Top-of-Mind Threat Still Today," Fortinet, May 12, 2022.

[2] Gartner®, "Top Strategic Technology Trends for 2022: Cybersecurity Mesh," Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi, 18 October 2021.

[3] Martin Roesch, "How Security Complexity Is Being Weaponized," Dark Reading, March 30, 2022.

July 18, 2022 11:32 AM

1648336-0-0-EN