THREATBOARD

ENHANCING THE HUNT
Large, resourceful nations have dominated warfare throughout history because they had the intellectual and economic resources to sustain the advantage. In today's cyber landscape, a small dedicated group of people and a single keystroke are all it takes to inflict significant damage—cascading and wreaking havoc on societies and economies around the world.

These from sophisticated guerrilla warfare style attacks are hard to uncover. To mitigate the risk, organizations must have timely information about threats and a full view of the entire threat landscape—from a single local area network (LAN)/wide area network (WAN) to an organization responsible for monitoring widely dispersed individual networks. Dispersed LANs/WANs can also vary in the type of assets and endpoints monitored. Everything from typical servers and workstations to incident command systems (ICS) and Internet of Things (IoT) devices can be critical for organizations. Another issue facing today's threat intelligence analysts and threat hunters is the amount of time and effort required to search for threat intelligence and to correlate a specific threat, malware, and vulnerability information in a timely fashion.

Gaining visibility of the entire threat landscape is imperative to the success of the analysis and hunt. Recent supply chain attacks demonstrate that malware embedded into supposedly legitimate software can allow unfettered access to all organizational assets. Once this access is acquired, other internal targets and vulnerabilities can be exploited to ensure continued access—even if the original entry point is discovered and remediated.

**UNDERSTANDING THE SECURITY GAPS**

The lack of visibility and understanding of the millions of data streams that move into and around an organization's networks every day is the core of the problem. Current security systems can only process a fraction of these streams in real-time. Other security systems rely on indicators of compromise (IOCs) to trigger an alert—which could require hours of human review to determine.

The majority of IOCs are either signature or behavioral-based. If one indicator of the attack is dropped during the analysis phase, the IOC may be missed altogether. To compound this further, most adversaries are aware of the measures that organizations use to detect threats. Attackers can simply avoid these by varying the attack so it does not trigger the pattern that causes an IOC to cause an alert. A simple technique is to "stage" the attack from multiple sources or multiple destinations, never creating a single session to execute an attack.

Newer detection methods using state of the art artificial intelligence (AI) have already been proven not to be reliable. Attackers simply send unassociated attack data with the actual attack data to "train" the AI to look for a different signature, pattern, or behavior. For example, staging the reconnaissance phase from one internet protocol (IP) location to determine the attack surface, launching probes to determine the feasibility from another IP source, and finally a direct exploit attempt from a third IP in the final stage. By varying IP sources and timing of the attack from worldwide locations, it can be simple enough to avert detection from many security measures and appliances.

In some cases, one part of that sequence may be detected as a possible attack. Still, because the full attack was not part of the detected pattern, it will be disregarded as an unsuccessful attempt or anomaly. To further exploit an organization's asset, once on the inside, attackers can use a compromised system to perform reconnaissance and exploit additional systems internally. This lateral movement will not be associated with the initial external attack in most cases. The exploitation of these unpatched internal systems may manifest itself as a system failure or platform not performing as expected. This activity's first indicator could be a help desk or service ticket from an administrator or end-user reporting platform issues.

A security team's lack of awareness and correlation of the external events and the internal events makes it nearly impossible to identify relevant threat intelligence that can then be used to identify new threats against an organization, address undetected events, and develop effective defenses against the entire threat landscape. No matter how good an organization's cybersecurity detection and protections are, these broad-scale attacks can only be detected when all the relevant data is stored, correlated, and available to analysts and threat hunters. For organizations with access to the vast amount of data, it is almost impossible to parse, correlate, research, and act upon findings at machine speed.

Adversaries know this. They also know modified attack patterns or zero-day attacks will eventually get through. For this reason, hunt teams must continuously try to find and contain undetected adversaries that have bypassed their defenses.

Another concern is attacks that have already occurred and may have been detected either internally or externally. Critical information relating to the event is often overlooked, dropped, or misclassified. Analysts and threat hunters have varying degrees of expertise and experience. Ensuring that the right information is acted on is even more difficult—attempting to find these events after the fact is problematic for even the most advanced analyst, threat hunt, and response teams.

Government agencies and security teams have developed or purchased many different systems to gather information about what is happening in their environments. These systems collect information from endpoints, networks, email servers, etc., and send it to the security information and event management (SIEM) system or data lakes for correlation, alerts, and response. The results of this are large data silos. If these data silos are not consolidated and shared, an organization can easily miss events that could be correlated to identify attacks that are subverting their defenses.

Much of the information currently collected by SIEMS and security, orchestration, automation, and response (SOAR) appliances lacks depth and provides only a cursory snapshot of a select few observables limited by the various collecting technologies. For example, an endpoint agent can only report specific events that affect a single destination and operating
system, usually identifying only objects that may have executed. The information collected is limited to items that exhibit behaviors deemed worthy of collection. Evasive objects, unsupported platforms, or statically embedded content is not captured.

**SOLUTIONING THE SECURITY GAPS**

The traditional organizational approach to security is inflexible, prone to human error, and ineffective. The threats we face today change frequently and are difficult for existing security and risk mitigation techniques to keep up with. We are always one step behind the attackers—learning from previous attacks, creating signatures and baselines but never anticipating the next attack quantitatively.

Organizations tend to convince themselves that they can predict the next attack (the black swan concept) and are always surprised by unexpected events. Not a single U.S. agency was prepared for the Sunburst attack; they would have prevented it if they were. After the attacks, people began to think that the attacks were predictable, so security measures are being tightened to prepare for future similar attacks. The next attack won’t be like Sunburst. System disruption will be a more likely tactic. In the face of global cyber warfare tactics, this demonstrates that we can no longer rely on traditional security to keep our vital systems safe—we must look for new strategies.

If a security team could implement a solution to analyze threat information automatically, classify, aggregate, tag, and store data for each of the events that move in and around their network, it would close the visibility gap. The body of information created would provide a searchable data fabric of information monitored and controlled within an organization. That capability would be invaluable for recognizing relevant external threat intelligence, supporting incident response, and combating vulnerabilities that evade defenses.

The threat hunting team would have comprehensive knowledge of events to compare against global intelligence to help define which data is relevant for their organization. The operations team would have the information and ability to understand the data being collected in the SIEM, SOARS, and other automated information sharing (AIS) systems to tie together attack events and respond more effectively. Hunt teams would have better visibility to identify and correlate previously undetected internal threats. This information could be shared to enable collaboration and accelerate decisions. It could also be used to hunt, identify, and correlate previously under-detected events.

Analysts would be able to search using relevant attributes (e.g., hashes, strings, behavior attributes, similarity, etc.) to identify large-scale attacks that previously went undetected. Because all the relevant data is within a single data fabric, analysts could assess any given cyber threat campaign’s true extent.

Hunt teams would have a highly valuable and relevant single pane of glass to work with. It would also enable security operations teams to connect incidents, analytics, and events to paint a complete picture of an emerging attack.

**COMPONENTS OF A DATA FABRIC INFRASTRUCTURE**

To create a complete data fabric of cyber threat information, the infrastructure should collect from as many data sources as possible—the network, endpoints, email, storage, and cloud. Initial data sources feeding into the infrastructure can be selected based on where the organization perceives the most significant risks or where threats present themselves.

High-volume data feeds can be accomplished via application programming interfaces (API) that allow real-time ingestion and bulk uploads from sources. Those bulk sources can be from historical data in cloud-based containers or cleansed datasets from isolated LANs/WANs. Data inputs are fed into a high-volume automated natural language processor (NLP) analysis engine. NLP analysis has the advantage of automatically analyzing critical information objects in less than a second, providing the performance and scalability required to cover a vast body of data input. These essential objects of information identified by the NLP engine can be customized based on past and future technology threats. Objects identified by the first NLP engine can be Internet Protocol (IP) addresses, machine names, protocols, file hashes, sectors affected (healthcare, critical infrastructure, etc.), and advanced persistent threat (APT) characteristics. The output of this initial analysis is to gather essential information that will be critical to the correlation of events across the data fabric. The objects are then tagged to create a level playing field of critical information for analysts and threat hunters at any skill level.

The identified critical objects automatically move to the attribution layer of the fabric and start the enrichment process using organizational and third-party threat intelligence sources. At this layer an enrichment process that uses the previously identified NLP objects as their parameters begins. The enrichment process using numerous free, open, paid, and customer-provided threat sources, starts the enrichment process. Next, a secondary NLP engine begins processing the combined original event data and enriched data. This secondary NLP process is key to being able to increase the accuracy of the enriched threat data.

As data progresses from the attribution layer into the data services layer, a microservice handler processes the tagged data based on enrichment attributes. Data that will be used for analytics will be stored in our Janus Graph container. This container holds data that is critical to analytics and metrics—both visually and as data that is being correlated with previous and future events. The microservice handler also directs data that is required for fast queries into an elastic search database. Data not required for graphing and or rapid retrievals, such as ancillary data, analyst notes, and work products will be stored in a SQL database container.

By the time an analyst or threat hunter first observes the event, the data fabric has already gathered all available threat research information. It makes this information available to the analyst—reducing labor and time-intensive research and correlation. This process alone saves the organization hours of research time per analyst/threat hunter, allowing for optimized operations.
PERATON’S THREATBOARD

Data is only as good as the ability of an analyst to view, understand, and act on it. Peraton’s ThreatBoard technology—built upon a data fabric platform—uses Fractals as the front end to the data fabric of information.

ThreatBoard is Peraton’s direct ingestion, enrichment, and threat hunting platform and is made possible by our unique approach to using a data fabric architecture. Consuming all relevant event data within an organization is a change from existing security processes, which use multiple tools and platforms for specific results, i.e., AV solution, agent-based, IAM, host-based, and network analysis. ThreatBoard’s capabilities enable Level I analysts to add value in the investigation stage because our NLP and correlation technology automatically identifies threat indicators capturing all information needed to respond to unknown events.

Threat hunters can utilize ThreatBoard for multi-conditional correlation to search through data stores and uncover hidden cyberattacks. Over time, with a data fabric intelligence infrastructure in place, threat hunters can traverse large historical data stores—greatly enhancing detection and reducing the impact from breaches and newly identified targeted attacks.

In building a data fabric threat intelligence infrastructure, an organization would implement Peraton’s solutions to generate and store detailed information on cyber incidents and IoCs, making them accessible for search and analytics tools. The infrastructure would allow for real-time alerting, investigations, and response.

How ThreatBoard Uses Peraton’s Fractals Software

Fractals is a browser-based web application that allows every user, regardless of their level, to quickly customize how they want and need to see data. Fractals contains a rich resource library of pre-configured widgets that were designed with analysts, threat hunters, and incident responders in mind. There are currently 24 widgets ranging from "All incident information" to worldwide graphical displays of real-time attacks. This library of widgets is at the heart of what a data fabric does—it enables everyone to work from the same datastore of complete threat information.

A critical piece of a data fabric threat infrastructure is integration with a communication system. ThreatBoard has key integrations with common messaging platforms such as ServiceNow®, BMC Remedy, and Microsoft Teams. Integration with other systems can be accomplished through our API. This type of communication allows individuals working an incident to collaborate and allows ThreatBoard to continuously update ticketing systems as new data is applied to an incident or work product.

The concept of a data fabric—making the same enriched data available to all consumers of the data—is the first step in breaking through the data silo problems, increasing operational efficiencies, and reducing time to act for security-related events that most organizations struggle with.

For organizations struggling to find value in big data deployments, creating a data fabric focused on collecting all data and objects during the threat lifecycle offers an immediate and high-value use. The data fabric becomes the intelligence repository for all analysis, threat hunting, and retrospective hunting.

As the central repository for gathering events and information from security tools and other AIS systems, the data fabric is an integral part of the threat intelligence infrastructure. In such infrastructures, the data fabrics role remains the same. Consumers working with the data fabric will have event enrichment to use while making risk and response decisions. More importantly, consumers will have the tools and processes they need to match objects to high-risk events and know what to do when an unknown and potentially damaging event is surfaced.

THE FUTURE OF THREAT HUNTING

The adage that “insanity is doing the same thing over and over and expecting a different result” holds true for the traditional organizational approach to security. A modern and evolving approach to security against modern and evolving threats requires new thinking.

The data fabric and Peraton’s ThreatBoard create the next modern and complementary analytics technology. When these solutions are used in concert with Peraton’s incident response, threat hunting, and risk mitigation subject matter experts, they form the foundation for a comprehensive threat intelligence infrastructure that easily extends and integrates with an organization’s current security products.

ThreatBoard is a new holistic approach to defending an organization from today’s threats—and the evolving threats of tomorrow. By breaking through the data silos, leveling the playing field, and enriching data at machine speed, this new approach transforms your organization’s security posture. An organization with Peraton’s ThreatBoard infrastructure now has a "single pane of glass" view of all cyber-related events.

CONTACT

Timothy Singletary

tsingl01@peraton.com, (315) 838-7112