Booz | Allen | Hamilton

ACHIEVING ACTIVE NETWORK DEFENSE THROUGH PREDICTIVE ANALYTICS

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

ACHIEVING ACTIVE NETWORK DEFENSE THROUGH PREDICTIVE ANALYTICS

THE CHALLENGE: TRADITIONAL INTRUSION DETECTION IS OVERMATCHED BY TODAY'S CYBER THREATS

Network monitoring and intrusion detection capabilities are a critical component of the Department of Defense's extensive defense-in-depth cybersecurity architecture. To protect the department's more than 15,000 networks around the globe and the sensitive data coursing through them, DoD cyber protection forces closely monitor those networks, hunting for threats, both external and internal.

But in doing so, DoD network defenders confront ever-growing challenges: The prevailing technologies underlying most intrusion detection systems (IDSs) in use today fail to keep pace with the exploding increase in speed, number, sophistication and malicious effects of today's cybersecurity threats. There are two key reasons for this. First, current network defense tools and methods operate too slowly to be highly effective in today's cybersecurity environment. The volume and speed of network traffic that IDSs and Network Operations Center (NOC) staffs must monitor and parse through simply overwhelm today's capabilities with the result being more successful attacks. In a bid to keep pace, traditional network monitoring tools ingest data into large data science systems that use session analysis and signature detection to identify anomalies. The result is significant latency and events are detected only after data is ingested, processed, and analyzed.

Second, today's IDSs still rely heavily on searching through vast volumes of network traffic for signatures - telltale behaviors, activities, and components of known threat sources and vectors - to detect potential attacks. The problem with such tools is they can only find and block malicious activity and threat sources that are already well known and understood. New breeds and sources of threats - such as the 2014 Heartbleed bug or the advanced persistent threat (APT) attack that hit the Office of Personnel Management in 2014 and 2015 - are undaunted by signature-based detection tactics. The result is that most malware resides on organization networks for many months before being discovered. Experts across the field recognize that the use of mutating hashes, sophisticated obfuscation mechanisms, self-propagating malware, and intelligent malware components are confounding signature and behavioral-based tools.

Another problem with signature-based detection tools is they yield high numbers of false positives, or alerts, for security staffs to investigate and assess for further action. A false positive is normal or expected behavior that is identified as anomalous or malicious. *Government Computer News* reported earlier this year that about 37% of reports are found to be false.[1]

False positives occur, for example, when an alert rule based on a signature is written too broadly into an IDS tool and thus flags down both legitimate and illegitimate traffic. Such tools are binary in nature: If a signature match is found, an alert is triggered; no match, no alert. That means the tool cannot discern between a signature activity that may be innocuous in one circumstance and potentially highly dangerous in another. For Chief Information Security Officers (CISOs) and their teams, the challenge of achieving optimal tuning of alerts is nearly impossible: If they calibrate rules too precisely, they may miss something important; too loosely, and security teams are overwhelmed chasing down false positives.

The problem with having lots of false positives, of course, is they divert valuable time and attention from legitimate alerts, resulting in a weakened state of cyber readiness. They also drain considerable staff resources, injecting high cost and inefficiency into cybersecurity operations. Consequently, alerts based on rules that generate repeated false positives are often ignored or disabled, effectively blinding security staffs to the problem the alerts were originally created to detect.

In the end, network intrusion detection regimes founded primarily on signature-based approaches translate into weaker cyber security postures and, therefore, the

potential for severely degraded national security. Their utility is limited against the most sophisticated threats, such as advanced persistent threats (APTs), which are becoming the tool of choice for today's espionage. Said retired Col. Cedric Leighton, a former deputy director of training for the National Security Agency (NSA): "APTs can do the work of a thousand spies and they can do it far more efficiently than human agents can."[2]

Many military and intelligence planners are aware of the imperative to evolve their network defenses beyond signature-based intrusion detection tools. As Vice Adm. Michael Gilday, Commander of U.S. Fleet Cyber Command, recently told Congress: "We are piloting and deploying new sensor capabilities to improve our ability to detect adversary activity as early as possible. This includes increasing the diversity of sensors on our networks, moving beyond strictly signature-based capabilities to behavioral sensing, and improving our ability to detect new and unknown malware. We also have the need to be able to analyze this sensor data at machine speed, and are working with partners to investigate ways to utilize emerging data sciences technologies to help with the analysis of our networks."[3]

In short, DoD and intelligence agencies must find detection approaches that can repel new types of threats; analyze network traffic in real-time to mitigate attacks before they can do damage; and vastly reduce false positives that divert attention from legitimate threats and waste considerable resources.

A NEW PERSPECTIVE: AN ACTIVE NETWORK DEFENSE THAT WIDENS THE DETECTION APERTURE AND REDUCES FALSE POSITIVES

"I firmly believe the future lies in automation and machine learning for defense. Not only does this change the dynamic of speed and scale, but it allows us to use our people where they are most needed." - Vice Adm. Michael Gilday, Commander of U.S. Fleet Cyber Command, Testimony before the Senate Armed Services Subcommittee on Cybersecurity, May 23, 2017.

Signature-based detection, which identifies attacks by tracking down symptomatic markers produced by specific threats, will remain a critical part of today's network defenses. But it is not sufficient: Signature-based tools, by nature, discover only known varieties of malicious activity and, then so, only after they display symptoms and have infected the network.

"I firmly believe the future lies in automation and machine learning for defense. Not only does this change the dynamic of speed and scale, but it allows us to use our people where they are most needed." - Vice Adm. Michael Gilday, Commander of U.S. Fleet Cyber Command

Effectively addressing today's evolving threat landscape requires advanced, complimentary capabilities and approaches that address the shortfalls of signature-based tools and methods. We propose employing a combination of leading-edge streaming and data analytics technologies that identify in real-time very slight anomalies in baseline traffic patterns that identify known and unknown threats even *before* they exhibit malicious behaviors. Such active network defense capabilities bring unparalleled speed, analytics, and precision to the task of network intrusion detection to address the shortfalls associated with signature-based tools.

To better understand this approach, consider today's medical triage process at a typical hospital emergency room. When a sick patient arrives, she is evaluated based on the symptoms she presents. For example, based on known protocols, a patient with a fever, headache and sore throat may receive an evaluation for strep throat - a serious but not immediately dangerous illness. Upon further screening, she may be returned to a healthy state with antibiotics and rest.

But a patient presenting symptoms having no known protocols requires a unique investigation to determine the source of the problem. Doctors may begin with known protocols and perform multiple tests to understand the similarities and differences with other illnesses. Determining the severity of these symptoms in combination may prioritize this patient's care above a patient with a sore throat. Documenting these anomalies may result in identifying a new illness that can be added to future protocols used to diagnose new patients.

As with diseases, new breeds and varieties of cyberattack proliferate and morph with increasing speed. Therefore, today's approaches must be smart and adaptable enough to identify previously unknown threats in real time before they manifest into malicious behaviors that cause harm. This can be done with a combination of advanced streaming capabilities that ingest network traffic in real time, novel approaches to identify meaningful anomalies in that traffic, and predictive analysis to diagnose likely attacks in progress - including previously unknown attacks.

An Evolution in Intrusion Detection

By incorporating unparalleled processing speeds and advanced analytical capabilities, intrusion detection becomes far more accelerated, efficient, and broader in reach. This active network defense capability, called StreamEngine, quickly creates a baseline profile of a network's activity at the individual data packet and port level and then responds to abnormal deviations from that baseline with further inspection and analysis. After pinpointing abnormal activity, StreamEngine continuously monitors the probability that the ongoing sequence of activity is proceeding toward a malicious outcome and, as that probability escalates to a certain threshold, intervenes with an alert. The exceptional speed and advanced analytics of this approach thus combine to create a powerful predictive capability that leads to far faster, more accurate outcomes so malicious activity can be prevented.

No longer is intrusion detection focused on finding the specific markers of past threats - it now is focused on analyzing anomalous patterns of digital activity at the data packet level that appear to signal malicious intentions, regardless of whether that activity is generated by known threats.

With rapid ingestion of large volumes of data and application of in-memory analytics, StreamEngine evolves traditional signature detection from a capability narrowly focused on discovering past threats to one that wields a much wider aperture in patrolling for potential danger. The state-of-the-art advances from what has been a diagnostic analytics capability (that is, identifying sequences or patterns of discreet activities known to cause harm) to a predictive analytics capability (developing models and probabilities of future actions based on analysis of large sets of diagnostic data).

This combination of data processing speed and predictive analytics is not only far more effective than traditional IDS capability at blocking malicious activity, but also at weeding out false positives. To understand this better, consider that any intrusion detection capability must categorize anomalies into one of three buckets: clearly problems, clearly not problems, or uncertain if they are problems or not. The larger the collection of uncertain problems is, the more expensive it is for an organization to address. Considerable staff time and resources must be dedicated to deciding whether those anomalies are potential dangers and must be mitigated. With its robust ability to apply data analytics to network activity of concern in real time, StreamEngine is uniquely suited to dramatically and

quickly reduce the uncertainty surrounding detected anomalies, thereby enabling organizations to redirect those resources toward higher-priority needs. In short, StreamEngine enhances current capability by automating the time-consuming task of discerning the intentions of suspicious network activity.

Finally, this advance in intrusion detection is far superior than traditional approaches in finding the most challenging type of cyber nemesis: APTs. These highly sophisticated threats – often programmed and executed by state-sponsored adversaries – are designed to hide their tracks and lurk within a target network for months, carrying out their assigned duties while disguised as mundane files. Today, detection of APTs still tends to be accidental. With StreamEngine's active network defense capability, the slightest deviations from a network's baseline activity – such as activity on a network socket during off hours or the erasure of log file entries, a tactic many APTs use to hide themselves – could trigger further inspection and analysis.

PROPOSED APPROACH: MIGRATING TO AN ACTIVE NETWORK DEFENSE

The options for how DoD organizations might deploy and leverage an active network defense capability will vary depending on each organization's specific mission sets, use cases, IT environments, and architectures. Organizations must first understand their threat environment and objectively examine their own capability gaps to realize the benefits of an active network defense capability. To better position themselves for success, DoD organizations should address the following key questions:

- What are the operational requirements at the DoD organizations where StreamEngine would be deployed?
- What are the underlying components that comprise StreamEngine from an architectural perspective?
- How could existing tools and technologies support these underlying components?
- What are the most appropriate capabilities to test in a Proof of Concept (POC)?
- What use cases can the organization explore to quickly and accurately assess the technical feasibility of StreamEngine?

We recommend a three-step process as the most tangible way to assess, demonstrate and implement a StreamEngine active network defense capability:

1. Assess the AS IS State. Working with the organization, Booz Allen network defense experts review publicly available and internally sourced data to assess current and future cybersecurity threats and operations. We also evaluate the organization's current tools and capabilities to identify those components of an active network defense capability that already reside within the organization.

Using a diagnostic approach, our experts systematically assess all factors that will contribute to an active network defense capability through a series of interviews, observations, and document reviews. We also take time to thoroughly understand the client organization's culture and design, as well as ascertain stakeholder and leadership views on resources, constraints, and goals. Having this comprehensive picture of the organization is essential for providing the best options to move forward.

2. Determine the TO BE State. With the diagnostic as a guide, we then develop a conceptual TO BE architecture for an active network defense based on understanding of the organization's risk and operations environment, their high-level gaps for building an active network defense capability, the associated components that comprise this solution, and the tools and technologies that could be used to implement it.

From a technical perspective, the TO BE state of an active network defense capability can be decomposed into a series of distinct proofs of concept (POCs) that

build on each other. These POCs might assess feasibility, for example, of the primary architectural components relating to cyber analytics, threat intelligence, data fusion, and automated response. In this step, we develop and execute POCs to evaluate capabilities that comprise the active network defense solution, employing use cases for each POC to enable quick execution and follow-up evaluation. POCs will be used to test deployment of an active network defense by demonstrating end-to-end capability, evaluating the technical performance of the underlying components, and measuring scalability, suitability, cost, and other factors to determine how the capability could be delivered to the entire organization.

3. Define a MIGRATION STRATEGY to get to the TO BE State. In the last step, Booz Allen network defense experts work together with organization leaders to implement and manage the StreamEngine active network defense capability, based on recommendations informed by the previous assessments and POC results. The focus in this step is on scaling the capabilities that were validated by the POCs, integrating those capabilities across the enterprise to appropriate stakeholders and systems, and then monitoring operational metrics to ensure the capability is optimized. The new architecture must be stress-tested, practiced, and regularly updated as the threat and operational environments adjust. Leaders also must ensure the new capability is well integrated with the organization's policies, operations, personnel, technology and management approaches.

BOOZ ALLEN: YOUR ESSENTIAL PARTNER IN ACTIVE NETWORK DEFENSE

Booz Allen Hamilton is uniquely positioned to bring the required skill sets and expertise together to assist defense and intelligence clients in standing up active network defense capabilities. Our unparalleled expertise in cybersecurity and data analytics, has enabled us to create some of the most advanced solutions for some of the most advanced clients in the Defense and Intelligence sector and beyond. Our deep experience as a major service provider has enriched us with a level of insight into their operations that is difficult to replicate.

We are strategists and analysts, engineers and operators embedded in the world's biggest missions, and trusted to advance them. We know the policies, architectures and intelligence that define cyber enterprises and operations, both in the U.S. and internationally - because our people pioneer them. Our project teams rely on established cyber analytics platforms and protocols to guide how the advanced cyber solution capabilities can be structured to best deliver near real-time cyber threat detection, correlation, and defense.

NOTES

1. *"7 Ways to Filter Out Cyber Alert False Positives," GCN, Jan. 18, 2017:* https://gcn.com/articles/2017/01/18/filtering-false-positives.aspx
2. *"DoD Plans to Bolster APT Security," C4ISRNet, Dec. 7, 2016:* https://www.c4isrnet.com/2016/12/07/dod-plans-to-bolster-apt-security/
3. *Vice Adm. Michael Gilday testimony before the Senate Armed Services Subcommittee on Cybersecurity, May 23, 2017:* https://www.armed-services.senate.gov/imo/media/doc/Gilday_05-23-17.pdf

OUR EXPERTS

Contact our experts below for more information.

Richard Shaheen, *Senior Associate*
shaheen_richard@bah.com

Donald Leuschner III, *Senior Lead Technologist*
leuschner_donald@bah.com

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that—together—we will find the answers and change the world. To learn more, visit BoozAllen.com.

 |