The Future of Cyber Defense… Going on the Offensive

Angela Messer
Brad Medairy

ABSTRACT

Today, organizations are faced with the overwhelming challenge of protecting their enterprise against threat actors that are well resourced and constantly evolving. While most clients have a traditional Security Operations Center (SOC) to identify vulnerabilities and catch harmful activity on their networks, historical evidence proves that perimeter defense alone is not enough. To combat these evolving threats, traditional approaches to Cyber defense must evolve, and enterprises must go on the offensive. One emerging approach is Advanced Threat Hunting. An approach that pairs best-in-class Cyber Defense tools with trained threat analysts who have a deep understanding of their operating environment and an ability to ask the right questions. Advanced Threat Hunting, in conjunction with the client's current security posture, offers a proactive, defense in-depth solution focused on finding malicious actors.

TODAY'S CYBER SECURITY LANDSCAPE

Does it help you sleep thinking that your cyber team has a plan to respond after you've been hacked? It shouldn't. Your organization may have used a "react-and-defend" approach to cybersecurity for years. However, if you think this strategy is enough to protect your organization from a breach, you're wrong.

Too many organizations wait to be notified that they've been breached. Yet with the increasing number and scale of cyberattacks—and the sophisticated techniques threat actors are using to mask their activities—the traditional approach of "building bigger fences" will no longer suffice.

The hack of Equifax in 2017 posed one of the most significant risks to personally sensitive information in years, potentially exposing data for as many as 143 million

Angela Messer is an Executive Vice President and Chief Transformation Officer (CTO) for Booz Allen Hamilton. Before being named CTO in April 2018, she led the company's Cyber capability, guiding teams of cyber forensics engineers, data scientists, and threat intelligence experts who focus on cyber malware, cyber next gen operations, and incident response. Angela also led the Firm's Army business, which is a global, multi-functional business in the defense and intelligence sector. Prior to joining the company, she was a U.S. Army officer, managed two major commercial businesses and launched a startup software development company. She earned a B.S. in engineering management from West Point Military Academy and an M.S. in management from the Florida Institute of Technology.

Americans, according to the New York Times. [1] High profile, large-scale breaches like the one at Equifax serve as reminders that a defensive cyber approach is no longer sufficient.

Today's Advanced Persistent Threat (APT) actors commonly engage in long-term campaigns to compromise target networks, seeking first to gain, then maintain, a hidden presence. APT actors are skilled at defeating reactive, rule-based cybersecurity defenses by continually evolving their malicious tools, techniques, and procedures (TTPs). Modern polymorphic and obfuscated malware, dynamic infrastructure, file-less malware, and operating system hijacking techniques all evade traditional defenses.

COMMON CHALLENGES WITH EXISTING CYBER DEFENSE APPROACHES

While a tremendous amount of dollars and resources have been invested to secure the enterprise, Cyber defenders struggle to keep pace with sophisticated adversaries that are continually evolving their tactics at little cost. Enterprises are continually looking to the vendor community to provide the "silver bullet" in the form of a security product that will make this problem disappear. Unfortunately, this has further amplified the problem. Security teams are stretched thin monitoring the numerous products necessary to provide traditional perimeter defense. As no single device or platform provides the complete solution, they are stuck with an "eyes on glass" approach.

Most enterprises today have turned to Security Information and Event Management (SIEM) platforms to help analysts better triage and identify high priority events; however, this too is failing. Analysts are either flooded with false positive alerts, known as alert fatigue, or the platform is over tuned and missing true positive alerts. In both scenarios,

Brad Medairy is a McLean, VA-based Senior Vice President and leader in Booz Allen's Strategic Innovation Group (SIG) focused on the delivery of Cyber solutions across Federal and Commercial clients. In this role, Mr. Medairy is responsible for the development and delivery of next generation service offerings that integrate Booz Allen's leading Cyber (e.g., Malware Analysis, APT Hunting, Incident Response, Security Operations Center design & support), Engineering, Systems Development (e.g., Reverse Engineering), and Data Science capabilities. Mr. Medairy engages with clients across the Defense and Intelligence Community, Federal Agencies (e.g., Department of Homeland Security), and commercial market (retail, financial services, automotive, energy/utilities, and pharmaceutical) to understand their current environment, assess the threat landscape, determine their risk posture, and deliver tailored solutions that address their business/mission requirements

critical events are likely to be missed. Most enterprises do not truly know if they are compromised and are unaware if cyber threats are "living off the land." It's often difficult to assess how far a threat actor has crawled across an enterprise. For all they know, advanced actors lay dormant, quietly moving laterally, conducting reconnaissance, and ex-filtrating sensitive data undetected.

GOING ON THE OFFENSIVE

In today's unpredictable environment, filled with rapidly evolving threat actors and emerging technologies, the only way organizations can protect themselves is by unleashing offensive cyber techniques to uncover advanced adversaries on their networks. The most effective approach—**advanced threat hunting**—is essential to any organization that wants to stop and prevent attacks in its networks.

Advanced adversaries live in the noise of networks and defeat reactive, rule-based cybersecurity defenses by constantly developing malicious tactics, techniques, and procedures (TTPs). These developments—such as polymorphic and obfuscated malware, dynamic infrastructure, file-less malware, and hijacking legitimate operating system functions—all evade traditional defenses.

In working with clients on hunt engagements, we have found an average dwell time—that is, the time an advanced adversary lies undetected in a victim's network—of 200-250 days before discovery. Advanced threat hunting involves actively searching for compromises before alarm bells go off by carefully combing through networks and datasets to discover hidden threats. By regularly evaluating their networks for threat activity, organizations can catch attacks in progress—before it's too late. Advanced threat hunting is a proactive approach that relies on sophisticated tools and tradecraft,

such as automation, threat intelligence, threat analytics, and machine intelligence, to gather and analyze vast reams of data. Advanced threat hunting uncovers threats that are generally invisible to the traditional network security, endpoint security, and perimeter defenses at the core of anomaly detection. The focus of threat hunting is to reduce the dwell time (the length of time between initial breach and expulsion of the threat from the network) of APTs that are missed by the client's SIEM, intrusion detection system, and/or Anti-Virus solutions. While threat hunting leverages the client's SIEM, it's important that the data not be filtered so that the high false positive data, where indicators of a skilled APT will exist, can be revealed. Potentially malicious events are identified through Indicators of Compromise (IOCs), hypothesis-based rules that allude to a persistent threat's TTPs, and anomaly detection analytics supported by machine intelligence. Threat hunting is most effective when employed in real-time, but it can be used like a Compromise Assessment to analyze historical data for signs of a breach. These tools can identify and mitigate threats at machine speed using customized delivery models.

It is important to note that not all threats can be detected with automated tools alone. These tools must be paired with trained threat analysts who have a deep understanding of their operating environment and an ability to ask the right questions. Threat analysts can make sense of complex data, develop hunting hypotheses, and test these hypotheses to better identify hidden threats.

Even with trained analysts using the right tools, ad-hoc hunting isn't enough—it must be standardized and measured. Advanced threat hunting requires implementing a repeatable process that's part and parcel of an organization's overarching security strategy. Fusing Security Information and Event Management (SIEM) and Endpoint Detection and Response (EDR) tools intelligently can help to streamline this process.

CONCLUSION

At Booz Allen, we have spent the last decade assembling teams of analysts who can think like the enemy and know how to identify warning signs. Our analysts specialize in global malware hunt operations, anti-malware research, and development of APT countermeasures, and use measurable processes to strengthen network defenses and identify adversary activity.

Incidents like the Equifax hack don't have to be inevitable. Organizations need to take steps now to improve their security posture before the next attack hits. Three elements—analytical tools, talented threat analysts, and a standardized hunt process embedded in a broader security strategy—can be the key to knowing your organization is protected. With advanced threat hunting, you can sleep well at night—or at least a little better.

[1] https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html