Cyber adAPT

New Approach to Cyber Security

Part I: Begin with the right questions

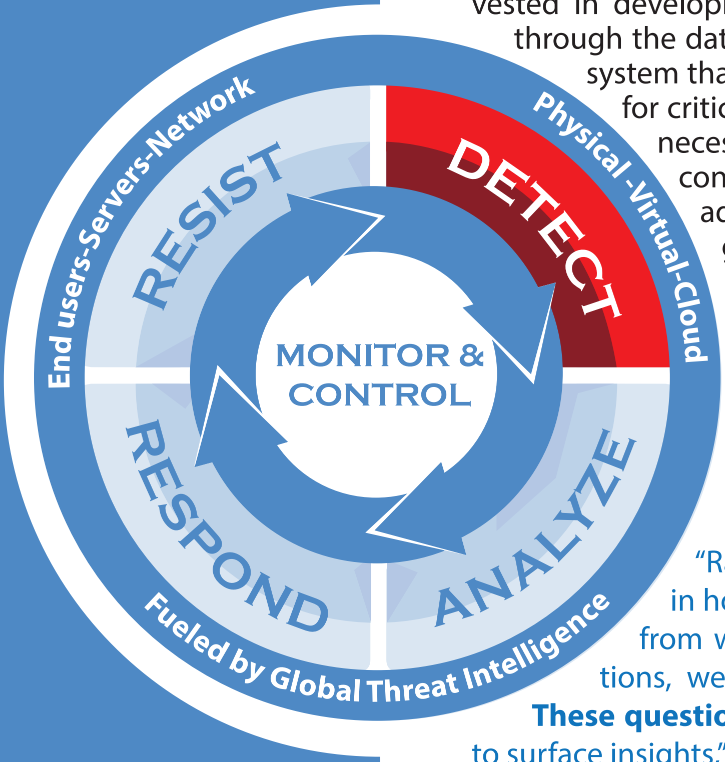
An inside-out approach to intelligence

Each day, an overwhelming volume of data traffic, which only grows over time, floods network pipes. As big data analytics becomes a household term, this new approach to intelligence is steadily making its way into cyber security, with companies promising to crack the evolving patterns of malicious behavior, giving rise to a next generation defense solutions. The problem with "big data" is that most of the data isn't relevant. The ability to narrow data down is both essential to capturing the critical metadata needed and to reduce the footprint for the storage of the critical information.

But there is a very significant component that is still missing in our sophisticated equations: the moment-to-moment activity inside the network. The emphasis continues to be on the bombardment of networks from the outside. It seems that we've been approaching the problem in an unbalanced fashion by giving an uneven amount of weight to one side of the equation: the perimeter. Therefore, we must enrich our intelligence by taking a closer look inside the dark corners of the network that we suspect has already been breached with no ability to see in the malicious activity in real-time.

> **"The problem in the intelligence world is that everyone is trying to surface answers to predefined questions. Instead, we need to surface the ability to help us define what questions we should ask."**
>
> **– Kirsten Bay,**
> **President & CEO of**
> **Cyber adAPT**

For maximum protection, traditional security must embrace real-time detection



A glance at a handful of recent cyber security reports and current approaches to solving the growing problem of system breaches reveals that finding the relevant data to analyze could be a complex and tedious undertaking that would take a lot of time to refine and perfect. Many companies are heavily vested in developing mathematical formulas that help sift through the data noise and inject those algorithms into a system that claims to have next generation solutions for critical network protection. It is absolutely the necessary thing to do, especially as attacks continue to increase with the exponential adaptation of cloud and mobility technologies. However, this data intelligence & analytics approach of tomorrow is still incomplete as long as it lacks the ability of real-time detection. Once true detection is embraced, a new paradigm can emerge and the chasm can be crossed laying a foundation for a much more comprehensive enterprise solution.

"Rather than sorting through **random data** in hopes of stumbling upon a valuable pattern from which one can then distill pertinent questions, we must **begin with the right questions. These questions** are then injected into the data stream to surface insights," says Bay.

What is that question that can help data analysts cross this chasm? The simple assumption that a network has already been penetrated helps save time and cut through the noise while aiming resources at locating the adversary in order expose their footsteps with pertinent forensics technology. According to the 2015 Mandiant report, advanced threat actors continue to evolve their tools and tactics and thus evade detection. And while in 2014 some organizations made progress in protecting unauthorized access to their critical assets, "attackers still had a free rein in breached environments far too long before being detected—a median of 205 days in 2014 vs. 229 days in 2013."

Monitoring activity from “within”

Gathering information and tuning it into intelligence by putting it through an analytical framework is absolutely crucial, but only after the right data has been collected and the right analytic model is used. To have an effective foundation for the sophisticated technology tools of tomorrow, we need to include the still largely missing component: real-time observation of the data movement on the network over long periods of time while capturing notable behavior patters that reveal information about what is and is not considered normal. Only then can a system that contains intelligence, gathered from the perimeter as well as inside of a network, support a security infrastructure that is truly robust and complete.

About Cyber adAPT®

Cyber adAPT® is a non-signature based, agent-less detection product that scans packets on the wire in real-time, looking for and alerting on malicious network behavior already present inside the perimeter. Layering threat feeds and host behavior data to increase its fidelity, Cyber adAPT® provides behavior detection capabilities at line speed with the precision required to avoid the all too common false alarms. Furthermore, Cyber adAPT®’s multi-variant approach to analytics provides a clear picture of the nature of traffic inside the network that otherwise cannot be seen.

Headquarters
337 Mirada Road, Second Floor
Half Moon Bay, CA 94019

Dallas Location
14755 Preston Road, Suite 405
Dallas, TX 75254

Chicago Location
135 Park Avenue, Suite 201A
Barrington, IL 60010

Email
info@cyberadapt.com