CyberadAPT

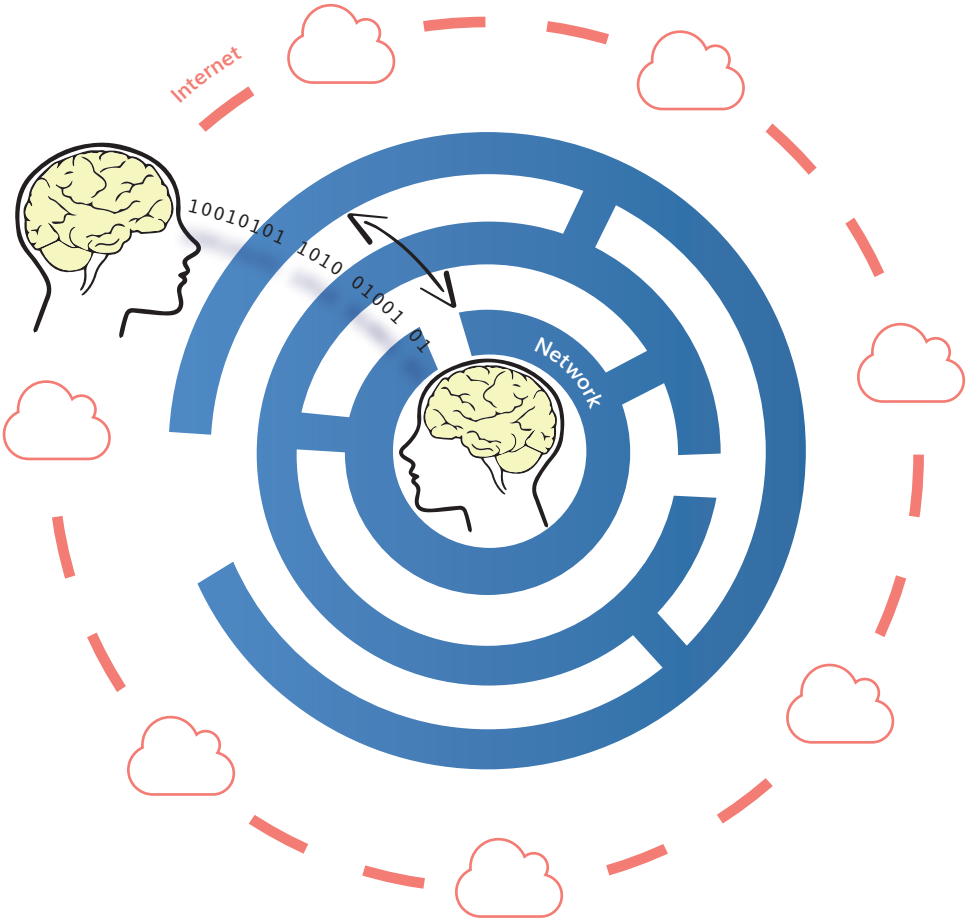
Network Detection: What Is It Really?

Introduction

Network detection is now the hottest area of growth for cyber security. Verizon's 2015 Data Breach Investigations Report notes that the volume of breaches has increased by 55% in the last year and that it takes more than 200 days for these breaches to be discovered. According to The 2015 Global State of Information Security Survey, in the last year alone financial services organizations saw financial losses tied to cyber security incidents jump by 24%. In response, vendors are labeling their products as 'the answer to the latest cyber threats.' Although these solutions come equipped with various tools, the vendors aren't fundamentally upgrading their approach to cyber security, thus their products do little to address the growing problem.

Most approaches are incomplete. While attempting to tackle a complex issue with many layers, many so called cutting-edge solutions address one or two layers at best leaving the rest vulnerable to attack. One of the most widely promoted techniques in detection today is network behavior analysis (NBA). This technique can be excellent at dissecting network traffic in search of malicious activity. That being said, it does fall short when used in isolation.

An individual technique on its own will not solve the problem of identifying hackers inside the network perimeter. However, a change in approach, from a singular focus to a multi-dimensional view of the network, is a great place to start. When the moment-to-moment state of a network is both an object of observation and a point of reference in comparison to the outside world, the methods used to track the health of a network become simpler, yet more robust. In other words, two viewpoints working in tandem enhance the power of each.



Security analysts must have a detailed understanding of what is 'normal' within their network, what we call *inside-out awareness*, for them to be able to identify when someone is trying to disguise malicious traffic inside the millions of good packets. Additionally, a clear understanding of known threatening domains and IP addresses provides a basis for potential issues or what we consider an *outside-in* perspective. The crucial new element of this '*inside-out and outside-in*' approach is advanced detection, which identifies protocol and application specific messages, out of the millions of packets per second, where threatening behaviors can be seen.

Network Traffic Analysis = Context + Advanced Detection

The Intersection of NTA & Threat Analytics

Many network security techniques are becoming less popular with cyber security organizations due to excessive false positives and meaningless events. Two of these misused techniques are behavior analysis and threat intelligence; in isolation they produce sub-par solutions but when used together they are capable of producing a truly advanced product.

Network traffic analysis (NTA) in particular is a term that is often misunderstood and can be confused with network behavior analysis (NBA). NBA is a subset of NTA and denotes a rather fluid set of events that occur on the network, which over time are pooled into baseline reports indicating what is considered 'normal.' This data can, and often does, provide internal context for a breach as it relates to a specific network. For example, if an endpoint user, typically active during normal business hours, deviates from that norm and accesses the network in the middle of the night from a remote location and begins to export massive loads of data, most NBA systems will catch that obvious anomaly. That said, there are flaws within this approach. As an organization adds new employees, policies, and offices, what has been considered 'normal' will need to evolve. In fact, even having a 'baseline' is a misnomer because it can never be static – network behavior is always changing! Furthermore, a solution purely based on NBA is very limited in scope as its main focus is what is inside and/or coming in through the perimeter of an organization's network. It does not take into consideration outside variants that together weave a larger story, helping point the lens toward a threatening target.

Another misunderstood technique within network security is threat intelligence. To put it simply, threat intelligence feeds serve a specific purpose in building the context around a security event. It is a dynamic database that adds and removes IP addresses when their status as 'suspect' changes. This suspicion could be caused by a hack that hijacks a domain or server temporarily, but is then discovered, remediated, and removed. External threat intelligence was once 'the latest thing' in security but lost its luster as security analysts struggled to understand how to use it. Domains are compromised in limited time windows in many cases and suspect threats move on and off of threat intelligence feeds making false alarms very common.

Like NBA, threat intelligence is an excellent source of context and can provide an Indicator of Compromise (IoC) from external information, but on its own, it is not effective in identifying an attack. Taking this into account, combining external context from threat intelligence, with internal context from network behavior analysis ensures that alarms occur only when the threat is real.

Context & Detail: The Holistic Solution

The most significant network security evolution today is threat detection. Industry analysts have identified detection as a crucial element to protecting digital business. But what does it mean exactly?

Detection is currently only a network security marketing term that is loosely defined within the context of any vendor solution. In other words, the term is rapidly becoming meaningless. To remedy this, we looked at real world scenarios from Cyber adAPT clients, to define the actual needs driving the use of detection technology. We found that companies need to:

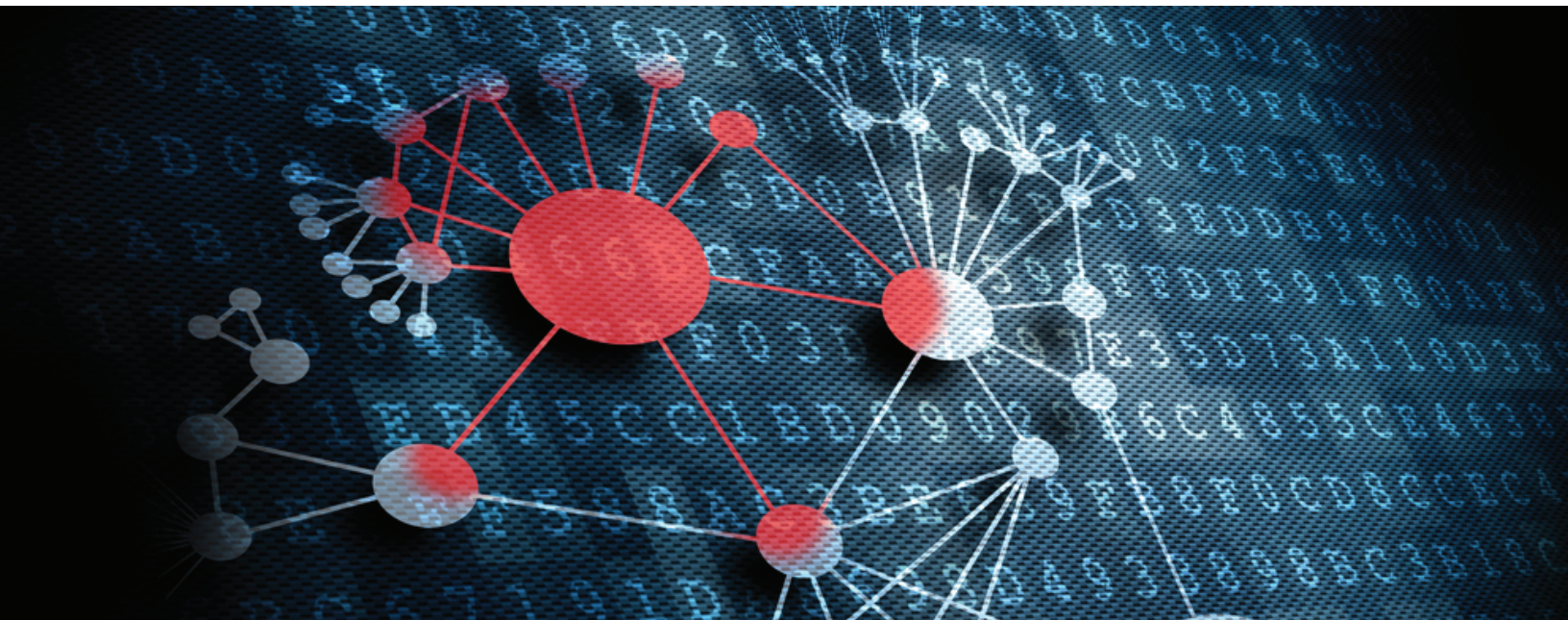
- Find attacks that make it inside the network,
- Reduce false positive alarms,
- Prioritize workflow,
- Develop an informed response.

Many vendors claim to have behavior-based detection, with deep packet inspection at line speed, and predictive analytics. Unfortunately, the systems advertised are rarely 'real-time.' The challenge with delivering advanced threat detection is that there have not been any products that correlate real-time protocol and application events with internally developed threat intelligence unique to the organization. Without consolidating customized baselines and evidence sources, there is no context to identify modern threats.

The Inside-Out & The Outside-In

The industry needs a holistic solution that integrates disparate components of network behavior and threat intelligence to create truly advanced detection. To do this, both network behavior and threat intelligence must be included. To effectively surface the adversary, especially when their intrusion and negative activity are masked to appear as good traffic, both techniques are crucial. The reason these persistent attacks are called advanced is because the attackers are well aware of the current alerting systems and know exactly how to make their behavior appear perfectly 'normal' and thus gain entrance undetected.

The attacker's favorable position significantly wanes with advanced detection, which controls how data is correlated to tell a larger story. Think of a night watchman. A human guard strolling the premises in the evening can notice seemingly unrelated incidents and tie them together. For instance, a security light that has gone dark is not necessarily a cause for alarm, but it could be if there is broken glass where the bulb was broken and not merely burned out. Such clues are invaluable when building context around specific events and recognizing malicious activity from seemingly disparate actions.



Cyber adAPT's latest advanced detection technology allows for the production of context-based mapping of internal network traffic, to provide a high fidelity view of security breaches. Such technology facilitates the understanding of **both the inside-out and the outside-in of a network** environment. By using context in partnership with detection, one can identify subtle commands, requests, responses and protocol errors buried in millions of packets and connect them to the broader 'normal' behavior of network operations. Cyber adAPT is the tool that shines a light on those subtle, yet potentially devastating network events – for the sake of your network's protection.

Detection As The Core

Many organizations continue to struggle with what they should include in their security stack to make it 'bulletproof.' Besides continuing to bolster their defenses and strengthening the perimeter in order to avoid initial intrusions, organizations must look beyond to accept the critical fact that most networks have already been breached by very smart intruders. Consequently, to keep pace with the adversary, organization analysts need access to clear and concise data sets that point straight to what needs attention; they cannot and should not be overwhelmed by the roar of false alarms. Therefore, the 'smart stack' must be built on detection, not prevention. Only when an ecosystem of integrated security tools contains a real-time monitoring tool, can it effectively know and crunch the data. Such analysis is impossible without the right initial information. Signature systems are old, sandboxing is too narrow in scope, and pure NBA systems miss the big picture and often the malicious actor posing as a benign host.

The Cyber adAPT solution takes the guesswork out of the security professional's daily life. By monitoring the network in real time, correlating live data with multiple intelligence variants, and building context that gets smarter over time while eliminating false positives, this crucial portion of the security stack is more than just a detection tool.

Learn More About Cyber adAPT

FACT: Advanced threat actors assault seemingly secure systems from all around the world, every day.

Unfortunately, this grim truth is not going away anytime soon. While organizations will not be able to completely eliminate advanced targeted attacks directed at their critical assets, with the right security approach and strategy, they can build a comprehensive system that is more effective at catching the intruders.

Cyber adAPT breach analytics does just that and more, by:

- Quickly finding attacks that make it inside the network,
- Reducing false positive alarms,
- Prioritizing workflow,
- Developing an informed response,
- Maintaining a cost-effective platform.

Connect with Cyber adAPT Today to learn how to enhance your security strategy and feel more confident in the strength of your network.

sales@cyberadapt.com www.cyberadapt.com (224) 385-3901