Detection: The Emerging Cyber Defense

What's The Meaning Behind the Buzzwords?

According to the latest market research, detection has become the hottest area of growth for cyber security. Statistics show the volume of breaches jumping by 55% and mean time to discovery reaching 200 days[1]. There are numerous security firms in the detection field that claim they have the solution to address this growing problem. But can they really? In order to find out, we must first extract the meaning behind the words that seem to imply the panacea has arrived and examine the claims with relation to the product's performance.

Over the last few years, a plethora of buzzwords have entered the mainstream security space, with detection leading the charge. But what really is 'detection' and perhaps more importantly, what is network traffic analysis (NTA)? Both buzzwords claim to help you find the needle in the haystack. But what does it really mean for an organization to have access to and utilize threat intelligence? As it stands, NTA and threat intelligence seem to be the main cyber security techniques that form the core of true detection, especially when they are coupled with deep packet forensic inspection.

Detection is currently only a network security marketing term that is loosely defined in the context of any vendor solution. In other words, the term is becoming meaningless. However, feedback gathered from vendors and clients has allowed us to define the actual need when referring to detection. Companies need to:

- find attacks that have made it inside their network
- reduce false positive alarms
- prioritize workflow
- develop an informed response

At the moment, none of these needs are applied to the industry definition of detection. The term remains vague and is often used to describe an amalgam of technologies, such as sandboxing and network fortifying tools, that belong to an entirely different class of network protection – prevention. What is really needed at a mainstream level is a specific, actionable definition of what detection technology does, how it works, and the way in which it addresses a customers' problem.

Network traffic analysis (NTA) is a term that can be confused with network behavior analysis (NBA). NBA denotes a fluid set of events that occur on the network, which over time are pooled into baseline reports indicating what is considered 'normal' behavior. The normal baselines aggregated over time are juxtaposed with moment-to-moment activities occurring on the network in order to catch anomalies. NTA looks closely and in real-time at the incoming and outgoing packets crossing the perimeter as well as the traffic within the network. The most recent definition of NTA includes the use of baseline information and threat intelligence in correlation with information discovered using deep packet inspection to identify malicious attacks. Some claim that NTA is a subset of NBA but it is clearly the other way around.

NBA alone poses many challenges related to the variability of established baselines due to the dynamic nature of business, such as network activity related to an urgent sale or customer crisis. These events may be events in time or true baseline shifts, such as increasing or decreasing workforce, that will show anomalies in a baseline but not malicious activity. If taken in isolation, this technique creates too many false alarms. However, baselines can provide powerful context when related to direct evidence in network traffic of activities that cause baseline changes.

Threat intelligence is a technique within network security that is often misunderstood. 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 suspect IP addresses and/or domains as 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 listed threats move on and off of threat intelligence feeds making false positive alarms very common. However, when included in traffic analysis and baseline monitoring, threat intelligence provides an incredibly powerful piece of evidence for a holistic view of NTA.

An individual security breach detection technique on its own will not solve the problem of identifying hackers inside the perimeter. The industry is beginning to realize that combining various information sources about network behavior and activity creates a clearer picture of what is actually going on within network traffic. NTA is how we are beginning to describe the integration of deep packet inspection, network traffic baseline anomaly detection and threat intelligence. This multi-dimensional approach provides high fidelity detection capabilities that are specific enough and worthy of being called **detection**.

To learn more about Network Detection, download our white paper – Network Detection: What Is It Really?

[1] Verizon's Data Breach Investigations Report, 2015