Shifting from Reactive to Proactive Defenses

Today I wanted to touch on the benefits of a proactive, predictive, and retrospective cybersecurity defense strategy (aka threat hunting) to augment the more traditional protective and reactive defenses in place within most organizations. And I do mean augment, as protective and reactive capabilities are a critical first line of defense for your enterprise.

This topic tracks closely with my earlier blog on mitigating cyber threats with the Full Spectrum, as a proactive, predictive, and retrospective defensive strategy is squarely aimed at defending against the sophisticated and constantly evolving threats discussed in the blog.

The end goal for a proactive, predictive, and retrospective defense strategy is to enable your security operations team to detect and respond to cyber threats before significant damage is done. And here lies what I view as the key difference between protective/reactive defenses and a proactive defense, detecting sophisticated threats with confidence much earlier in the kill chain.

Preventative and reactionary defenses are based on the premise that your perimeter defenses will successfully detect and alert your security operations team of all threats probing your defenses, minimizing impact to your enterprise. The challenge with this strategy is that sophisticated attackers have gotten really good at disguising their attacks to confuse and circumvent preventative detections – enabling them to fly low under the radar and bypass your defenses.

This strategy is further impacted by something I've also touched on in earlier blogs – alert fatigue caused by the overwhelming number of alerts that in many cases turn out to be false positives. Once the perimeter is breached, many organizations lack the internal monitoring and visibility needed to detect an attacker's lateral movements within the enterprise enabling attackers to operate undetected for long periods of time and cause significant and costly damage.

Additionally, many data breaches originate from insider threats – through accidental or intentional malicious actions – and preventative defenses are not particularly useful in detecting insider threats.

A proactive, predictive, and retrospective defense strategy on the other hand is centered around the assumption that the attackers will be successful in breaching perimeter defenses and the added proactive capabilities provide your security team with the threat hunting tools, knowledge, and insights (visibility) necessary to detect the breach early in the attack kill chain, determine how the attackers breached your defenses and what systems have been compromised, take corrective action to eject the attackers from your enterprise, and prevent them from returning (at least using the same attack vector).

With that as a backdrop, let's explore a little deeper why I believe a shift from a preventative to a proactive defense is the rational security strategy and how it can detect and block threats early in the kill chain before significant damage is done.

Proactive, Predictive, and Retrospective – what do these mean?

Proactive defense involves active threat hunting within your enterprise for activities that are

indicative of an ongoing attack and then taking corrective action to mitigate any detected attacks. In this context, active threat hunting can involve human security analysts and/or automated detection and response capabilities that are tipped and tuned through predictive defense analytics, Machine Learning (ML), and Artificial Intelligence (AI) algorithms.

A key aspect of proactive defense is hunting “within” your enterprise; meaning you have the viability within your enterprise to detect, investigate, analyze, mitigate, and track anomalous activity that has breached your perimeter defenses. An important aspect of this is the ability to understand and then manage the perception of your network’s attack surface from the perspective of an attacker – that is, enable your security operations team to view your enterprise through the lens of an attacker.

Proactive and predictive defense requires security analysts that are:

1) knowledgeable in the attack techniques used by cyber criminals and nation-state threat actors and

2) backed by sophisticated analytics, tools, and automation to enable your security team to perform deep inspection and analysis of anomalous activities detected within your networks.

Many of our customers have in-house security analysts with the advanced threat hunting skills necessary to mount a proactive defense; however, we also have plenty of customers that choose to gain this expertise through one of our Managed Detection and Response (MDR) or Incident Response (I/R) service partners.

Predictive defensive capabilities identify interesting events and activities that warrant further investigation and provide threat hunters with the knowledge and insights into an attacker’s behavior necessary for them to detect and investigate anomalous activities early in the attack kill chain, anticipate the attacker’s next moves, track their movements, and ultimately block their advance.

Predictive defense capabilities help to focus and direct where the threat hunters should be looking to enable them to find the proverbial needle in the haystack. For example, predictive analytics are continually churning through network and sensor metadata to correlate and sequence seemingly random pieces of information into interesting anomalies that require a threat hunter’s attention – perhaps a low bandwidth connection to an unusual network address that could be indicative of a beaconing host.

Threat intelligence also comes into play here by keeping the threat hunters and automated attack detection rule sets up to date on the evolving TTPs used by the attackers. Finally, attack frameworks like Mitre ATT&CK® enable your security analysts (and predictive analytics) to understand the attackers TTPs (think like an attacker), string together those seemingly random events, and put those events in the context of a broader attack campaign.

As I’ve said in past blogs, a single activity is strange and can be explained away. A string of anomalous activity in a particular sequence is a signature that can be used for early detection of advanced threats – and this in a nutshell is what proactive and predictive defense is all about.

Retrospective analysis provides security teams with the ability to apply threat intelligence against historical (archived) metadata collected by defensive sensors to determine if the environment has already been compromised by a newly identified threat. Ideally, this analysis is automated and continuously running against stored metadata to quickly flag a past compromise as new threat intelligence becomes available. Security analysts can then apply proactive defense techniques to investigate the details of a past security incident, understand what data and systems have been compromised, and ultimately eradicate the attacker from your

environment.

Shifting Your Security Strategy from a Reactive to a Proactive Posture

A proactive, predictive, and retrospective cybersecurity approach allows you to identify, prioritize, and mitigate urgent threats to your enterprise – generally with greater confidence and earlier in the kill chain. However, despite the clear benefits of active threat hunting, many enterprises remain at a standstill. So how do I get started down the path to proactive, predictive, and retrospective defense?

You can download our whitepaper to learn the role of response in Network Detection and Response, and how machine learning coupled with threat intelligence plays a valuable role in the discovery of threat actors. Artificial Intelligence and Machine Learning capabilities, along with threat intelligence, are the key to being able to respond predictively and proactively, rather than reactively, to advanced threats.

Network Detection and Response (NDR) solutions use machine learning to predict how to adjust its internal detection logic and its response actions by correlating the execution sequence of an attack. Using the techniques detailed in the MITRE ATT&CK framework, you can drive detections and responses to threats and stay one step ahead of attackers.

Getting beyond a reaction-based security paradigm requires enterprises to rethink both their networking and security strategies. Enterprises need to begin to anticipate attacks by implementing zero-trust strategies, leveraging real-time threat intelligence, and tying information back into a unified system that can preempt cyber criminals and sophisticated Nation-state attackers – before significant damage is done.

All of this can be managed through the Fidelis Elevate® Extended Detection and Response (XDR) platform which combines Network Detection and Response (NDR), Endpoint Detection and Response (EDR), and Dynamic Deception into one unified solution – providing integrated, automated, correlated detections to advanced threats.

Fidelis Elevate also combines protective, reactive, proactive, predictive, and retrospective capabilities to deliver Full Spectrum Cyber Defense across the entire MITRE ATT&CK framework® and enables security teams to focus on their mission — identifying the most urgent threats and protecting sensitive data rather than spending time validating and triaging thousands of alerts from multiple point solutions.

Additionally, the Fidelis Elevate® XDR platform provides the core cybersecurity features for Enterprise-Wide Defense — Remote Offices, Corporate Infrastructures, and Cloud Workloads — AND provides the critical features and capabilities to enable Incident Response (I/R), Managed Detection and Response (MDR), and Cyber Threat Hunt professionals.