Defending Against Cyber Threats: Full Spectrum Approach

It’s hard dealing with the full spectrum of cyber threats. The threat landscape is constantly evolving and, to further compound the challenge of defending our enterprises, we continue to roll out new technologies and extend security boundaries into the cloud and Work From Home environments to support the “new COVID normal” and our digital transformation initiatives. The bottom line here is that threats continue to evolve, and our environments are getting more complex and harder to defend.

So, what can be done to better defend our enterprises against the full spectrum of cyber threats in this constantly shifting environment?

I intentionally used a pretty open-ended statement of “full spectrum cyber threats” to characterize threat because in reality we need to be prepared to rapidly respond to whatever the attackers throw at us. This could include continually evolving Phishing and Ransomware threats from cyber criminals, sophisticated and stealthy attacks from nation state attackers, insider threat, exposure through 3rd party partners, supply chain threat, and a whole host of other things.

The keys to defending against these cyber threats.

Early detection and validation of anomalous activity

This allows us to identify adversary Indicators of Compromise (IOCs) and stop the adversary before significant damage is done. If we take Ransomware as an example, stopping a ransomware attack as systems are being encrypted is too late in the game.

At this point, the adversary likely owns your environment and has exfiltrated sensitive data from the environment. We need to detect and block ransomware early on during the initial exploit (the Phishing attempt) and as they begin to move laterally to other systems.

Being really good at cyber hygiene

Fidelis’ Threat Research Team is continually tracking evolving threats and the attackers “go to” techniques continue to be Phishing and social engineering attacks, exploitation of unpatched vulnerabilities in systems, and exploitation of weak logon credentials. The key here is understanding what are your most critical and most exposed assets and then prioritizing cyber hygiene efforts against these assets.

So, what do I mean by being good at cyber hygiene and where do I think you will get the biggest bang for the buck?

Proactive Cyber Defense: Stay Ahead of Threats Reacting to attacks is not enough—prevention is key. In this free guide, discover:

- Assessing Your Security Posture Prior to an Incident
- How Can Decision Makers Use the MITRE ATT&CK Framework?
- Beyond the MITRE Evaluation

[Download the Free Guide Now!]

- Knowing the terrain you are defending (what are your critical data sets, business-critical workflows, and avenues of attack and the high-risk assets associated with those)
- Diligent patching (particularly for those high-risk assets and for systems that support work-at-home users)
- Good account and password management (ensuring employees are using complex, hard-to-guess passwords backed with two-factor authentication where possible)
- Robust endpoint protection – particularly for work-at-home users as many of these systems are exposed to the Internet through insecure home networks. For endpoint protection, I recommend a combination of automated vulnerability management software (such as Desktop Central) to keep endpoints up to date with the latest software and patches, anti-virus software to catch signature-based threats, and Endpoint Detection and Response (EDR) capabilities to catch the stealthier attacks.

EDR adds additional benefits for remote employees by enabling your security operations team to quarantine a device that misbehaving, remotely diagnose the device to determine if and how it was compromised, return the device to a secure state, and apply global policy updates to all your remote devices to ensure other devices are not compromised in a similar way.
- Finally, you need to continually reinforce security best practices with your employees to include best practices for detecting and reporting Phishing and Social Engineering attacks.

This blog post will lean a little more into my federal background and experience (spoiler alert – I'm a huge fan of automation, Big Data analytics, and Machine Learning) but the key takeaway that I want to leave you with for both the private and public sector is – traditional reactive based defenses are insufficient to protect us against the full spectrum of cyber threats and need to be augmented with proactive security capabilities.

Moving to a proactive security posture requires:

- Integrated cyber capabilities to give your security operations personnel holistic visibility of the cyber terrain they are defending and the ability to detect, correlate, and investigate anomalous activity occurring throughout your enterprise;
- The context provided through an attack framework and threat intelligence to allow your security analysts to understand how anomalous events fit into a broader attack kill chain;
- High confidence, integrated, prioritized, and actionable alerts – events independently firing from silo'd security tools just don't cut it here; and
- Automation, analytics, and machine learning to increase the efficiency and effectiveness of your limited security operations personnel to help them find the "needle in the haystack".

It is through these proactive security capabilities that you can move your organization beyond a preventative and reactive defense posture and truly address the full spectrum of cyber threats targeting your organization. As an added bonus, moving into a more proactive cyber posture can help address other challenges we face including alert fatigue, analyst overload, and the impacts of limited cyber personnel.

Moving into proactive defense does require an investment in skilled security analysts to perform the necessary investigation and cyber hunt activities; however, this investment will pay dividends in reducing your enterprise risk and helping you to keep your mission operations moving forward.

If you don't have the skilled analysts needed to move you to proactive defenses or aren't in a position to make the investment needed to build that expertise – not to worry, as there are lots of great Managed Detection and Response (MDR) and Incident / Response (I/R) service providers out there and we can help pair you up with a skilled provider that is trained in proactive defense.

Let's dive a bit deeper into proactive security capabilities…

Leverage an Attack Framework

I mentioned use of an attack framework above, and I see this providing two benefits to an organization – helping to identify gaps, redundancies, and inefficiencies in your enterprise security architecture and helping your analysts better understand and anticipate attacker tactics, techniques and procedures (TTPs). If you are not familiar with attack frameworks, I would recommend taking a look at this infographic demonstrating how Fidelis Deception® maps and correlates with the MITRE ATT&CK Framework®.

Securing the enterprise has traditionally focused on the acquisition of multiple security tools to meet the differing needs of enterprise and in response to new and evolving threats. This approach leads to a complex security stack that is managed in silos without any integration, automation, or correlation amongst the tools and data within the security stack. Use of a cooperative cyber security framework such as the MITRE ATT&CK Framework to drive security stack consolidation ensures that complementary tools are selected that can cover the full range of TTPs employed by adversaries. The framework can be used to essentially measure the effectiveness of your existing security stack and help you identify gaps and redundancies in your stack.

Mapping anomalous activity against an attack framework is also a good way to piece together seemingly unrelated events and demonstrate that they are part of a broader attack. The ATT&CK framework identifies the techniques used by adversaries and the sequencing of those techniques into broader attack campaigns.

A single activity is strange and can be explained away – a string of anomalous activity in a particular sequence is a signature and can provide valuable clues as to what's coming next when evaluated against an attack framework. This provides the critical attack context needed by security analysts to uncover attacks not picked up by reactive defensive capabilities.

Increase Alert Accuracy and Actionability

Once you have analyzed your environment against an attack framework, the next step in moving to proactive defense is increasing the accuracy, integration, prioritization, and actionability of alerts. Traditional threat detection based on attack signatures and flagging anomalous events contained in logs (i.e. firewall logs, application and proxy logs, process event logs, and AD logs) lack the visibility and contextual understanding of the processes, behaviors, network actions, and content needed to detect sophisticated attacks and to weed out false positives.

When an alert fires, the primary things that security teams want to know are:

1. Is this a real incident?
2. What data and systems have been potentially exposed or compromised?
3. How should I respond?
4. Was I successful in mitigating the attack?

Answering these questions effectively, and (most importantly) in cyber relevant time, requires the ability to correlate anomalous events and activity across multiple points in your enterprise using analytics, automation, and Machine Learning. As you look across multiple data sets, patterns begin to emerge which help to fuel new threat hunting hypotheses and uncover hidden threats – both internal and external.

Automation and analytics also allow alerts to be enriched with additional information to provide value-added context for the analyst; automate the mundane task of collecting the necessary data to fully analyze the alert; help the analyst prioritize alerts; and enable the analyst to easily dive into the communications surrounding the alert, pivot to other potentially affected assets, and quickly validate whether the alert is something to be concerned about. I found this Big Data approach to correlating and analyzing alerts to be very powerful in my previous job as CISO of the NSA and I'm excited to be working with Fidelis to move this forward in the commercial sector.

Deception technology can also play an important role in increasing the accuracy of alerts. There is no legitimate reason for your enterprise users and systems to interact with the deception environment and therefore, activity detected by deception decoys provides a high-confidence

indication of an ongoing attack.

Taking this a bit further, deception decoys are used to not only identify that an adversary has breached your defenses but enables you to capture their tools, track their actions (reconnaissance, initial infiltration, lateral movement, …), understand their attack objectives, and block further exploitation. As a side benefit of having higher confidence in your alerts, you will feel more comfortable implementing automated responses. Given the speed of attacks, automated responses can block attackers before they have had the opportunity to do significant damage to your enterprise.

So how do you get there? The key is to break down the silos present within your security stack, pull together metadata and telemetry collected across agents and sensors deployed throughout your enterprise (Internet gateways, internal network communications, endpoints, e-mail servers, web servers, deception decoys, and cloud workflows), and analyze and cross-correlate anomalous events to flag anomalous activity for investigation by your analysts. The correlation of activity across multiple points in your enterprise enables you to increase the confidence of your alerts, and the enrichment of alerts with value-added information enables you to produce more actionable alerts.

The Fidelis Elevate® extended Detection and Response (XDR) platform takes exactly this approach by collecting rich metadata from across the enterprise and correlating anomalous activity through detection rules and analytics to enable your security operations team to identify potential threats early in the attack kill chain and remediate those threats before significant damage can be done.

Enhance the Efficiency of Security Analysts with Automation

Investigation of security alerts has traditionally been performed manually by analysts using data sourced across multiple security tools, leading to extremely labor-intensive and time-consuming analysis of anomalous events – many of which turn out to be false positives. The manual processes for analyzing and fusing data across multiple security tools also leads to significant delays in identifying, verifying, and responding to security incidents. Security teams need to shift focus from manual alert triage to reducing dwell time; stopping attacks before sensitive data is stolen or mission operations are disrupted.

Introducing automation helps ease the analyst workload and frees up their time from manually analyzing, validating, and responding to alerts (a reactive security posture) to active hunting (proactive defense). This allows security analysts to detect adversary TTPs much earlier in the attack kill chain by automating the verification of alerts to produce a prioritized list of high confidence alerts – what Fidelis calls “attack conclusions”.

Threat intelligence comes into play here as it gives your security analysts insights into the changing TTPs used by attackers, provides analysts with a head start in where to hunt for adversary TTPs, and generates updated detection rules to ensure defenses can detect new and evolving threats with high confidence. These updated detection rules coupled with retrospective analysis capabilities, which automatically “replay” stored communications metadata against updated detection rules, enable your organization to determine if systems have been compromised in the past by a newly discovered threat.

This capability provides a powerful tool that allows security teams to look back at what has transpired on their systems, identify how cyber security defenses were penetrated, identify the specific data and systems that were breached, and identify what needs to be done to recover from the attack.

Advanced Threat Detection with Fidelis Elevate®

Don’t let threats go unnoticed. See how Fidelis Elevate® helps you:

- Identify and neutralize threats faster
- Gain full visibility across your attack surface
- Automate security operations for efficiency

Download Now

Making the Shift from Reactive to Proactive Defenses

If you are considering making this shift within your organization and would like a demonstration of our Fidelis Elevate® extended Detection and Response (XDR) capabilities, schedule a demo now.