We are again at the cybersecurity crossroads. Continue in the same direction, it could result in just more of the same, you may lose. You may waste time and resources on the next well-marketed and shiny silver bullet solution, and your environment may be compromised anyway. Many well-known organizations such as Target, Sony, Home Depot, JP Morgan, Chase , Linkedin , Adobe, and even NSA were investing millions of dollars per year on their cybersecurity programs . Many had security forces of hundreds of experts together with capable SOC's and the latest generation sandboxes, firewalls, SIEMS's, EDR but when it mattered, as the news articles inform us, these organizations just didn't know until after they had been compromised. Consider that money and traditional approaches seldom deliver a complete security solution anymore. According to Gartner, the current emphasis on blocking & prevention techniques are failing, leading to programs that cannot truly meet the emerging threats. Currently protection and prevention approaches account for 85% of the total Cyber spending, whereas monitoring, detection, and intelligent response account for only 15%. While robust prevention is still a critical capability and must not be overlooked, it is simply not enough by itself to result in acceptable outcomes, and additional emerging ideas and approaches such as Extended Detection and Response (XDR) should be considered as an additional component to help pave the way towards more acceptable security outcomes.

Our Extensive Research Has Pointed Out Three Serious Pain Points:

Alert fatique:

Only one percent of all attacks are detected through logs. This is an astounding number and SIEM has proven to be a particular failure. Interviews with IT teams delivered this frustrated indictment of SIEM : "Stupidity, Irrelevant, Electronic Messaging" They said SIEMS produce too many alarms, most of which are not actionable and may simply be false positives. A mid-sized organization can receive 200-300 or more alerts per day from their MSSP and many are left with no idea what to do with them.

Lack of breach validation:

The adversaries roam free as companies have no way to accurately confirm if these alerts are actual incidents. It becomes too time consuming & costly to investigate.

Fortress mentality:

Even though it is clear by now that adversaries can more easily penetrate and gain control on the inside, organizations cling to the illusion that cybersecurity means keeping bad things out.

Not only that we live in a networked world built on the weakest of foundations: insecure code leaving everyone with big vulnerabilities. Even if Al magically comes along to patch all the insecure code or plug all the known and unknown security holes, it won’t be able to patch all the insecure people and practices. The human factor. People keep opening phishing emails, they are smart and good at what they do, but are increasingly difficult to train when it comes to cybersecurity.

Bottom Line: Organizations Need To Think Differently About How To Detect And Respond To Threats.

Luckily there is a way forward: Our Active Defense. We are in the business of detecting advanced and unknown threats that bypass existing security controls. After detection, we can reduce attackers dwell time by validating, investigating, containing and responding to threats within minutes or hours and unlike many solutions that send streams of unvalidated alerts. Our Active Defense approach can not only halt active attacks early in the process, it will provide you with the evidence post breach to help you answer questions such as when did the attacker get in, how long were they there, how did they try to move around, what tools did they use, did they try to setup any backdoors, what data did they try to access and what have they done with the data since accessing it.

we think like the attacker and value rapid detection & response. When our technology resides on your network and systems, you cease to be the prey. In effect we turn the tables on to the attackers , shifting the cost to them and changing the economics of cyber defense. We strategically weave illusion into your entire network, coating every end point, server and network component with deceptions , creating an environment naturally hostile to the adversary. When adversaries are inside but are unable to determine what data and resources are real and what is not, their ability to pivot and expand their attack is diminished and their efforts to infiltrate is paralyzed. This is where rapid detection and response helps complement the efforts of protection, which unfortunately can be bypassed in virtually every situation. In this way, those adversaries may be able to find a way in, but once inside are placed in a confusing trap where they can more easily be detected and dealt with.

We call this Active Defense . Active Defense is a validated and integrated threat detection & response architecture that addresses unknown and advanced threats that slip by perimeter controls.

Our methods are unique and powerful, combining advanced network & end point threat detection, deceptions everywhere, anlytics, and global threat intelligence technology. Wrapped around this technology Is continuous monitoring that can be further strengthened by best-in-class threat hunting that is both internal and outward facing , capable of scouring the deep & dark web. In short, our active defense solution is a fully-managed , security analyst delivered service , 24 hours a day, 7 days a week it provides coverage.

Continuous is the key: Adversaries never stop and we don't either. We shift your security mindset from "incident response" to "continuous response" Continuous response assumes that systems will soon be or are already compromised and require ongoing monitoring & remediation. We are always on alert and you are safe.

Our intrusion analysts monitor your networks & endpoints 24X7, applying the latest intelligence & proprietary methodologies to look for signs of compromise . When a potential compromise is detected, the team performs an in-depth analysis on the affected systems to confirm the breach before moving to contain & remediate the endpoint.

Our Active Defense Features

- – 24X7 monitoring
- – End-to-end management
- – End point visibility
- – Network visibility (selective PCAP)
- – Log visibility (on premises & cloud)
- – Deceptions everywhere
- – Deep & dark web intelligence
- – Proactive threat hunting
- – Active threat hunting
- – Forensic investigation
- – False positive reduction
- – Managed remote host tactical threat containment
- – Managed remote network tactical threat containment
- – Managed remote cloud-based threat containment
- – Unlimited Remediation support
- – Automated known threat response
- – Powerful visualizations

Some Of The Use Cases We Solve:

Alert Fatigue and Log overload - (Security monitoring has not changed in 20+ years. This is why companies such as Electronic Arts, CNA Insurance, Capital One, Marriott, Target, Home Depot, Equifax were all in the news with security issues) - Aggregating logs and sending to a SIEM and trying to find the needle in the haystack is a difficult and expensive endeavor, and a challenge to show stakeholders a return on investment. The noise in the SIEM is a big challenge. You may not easily find the advanced actor in the logs. Sending a canned alert to a customer and having an internal team member spend hours trying to find something does not work very well. It is also one of the major reasons no one caught the SolarWinds breach for over 9+ months which affected some very large enterprises including Microsoft, Intel and many critical U.S. government agencies.

Post-Breach detection of malware or non-malware and file-less attacks which has bypassed the perimeter is not always easy. How do you detect the actions of malware or non-malware that has bypassed all security controls? We do this with automated active threat hunting on endpoints and the network packets. We can also build custom hunts at no charge based on feedback from your team.

Post-Breach detection of human adversaries moving laterally across the environment represents a significant challenge. How do find human adversaries (rogue employees or nation-state actors) inside your environment? We also can detect them through similar deceptions.

We can provide post breach full fidelity forensic capability - We can answer the who, what , where, how questions forensically with our Network Hunt sensor which is basically a DVR for the environment at the wire level.