Reducing the Cost of Cyber Attacks with Deception Technology

“Never attempt to win by force what can be won by deception.”

Niccolò Machiavelli, The Prince

Cyber criminals continue to phish, bait, deceive, and lure users so they become victims of attacks. Their methods are increasingly sophisticated and damaging to an organization. According to a 2021 study conducted by The Ponemon Institute, the cost of resolving a malware attack now averages $807,506, an increase from $338,098 in 2015. The average annual cost of phishing attacks has also tripled in the same amount of time to a staggering $14.8 million.

Meanwhile, security teams spend their energies chasing down false alarms, fighting fires, and detecting attackers long after the initial breach. The same study revealed that 52% of security teams spend anywhere from 2500 to more than 10,000 hours per year just evaluating evidence of attacks, and they spend even more time gathering intelligence and planning for the next attack. And that’s only after the attacker is discovered. Recent reports show that the average dwell time of an attacker—meaning the time from initial breach to detection—is over 100 days.

Notice the issue? Reactive security is a never-ending fire drill that keeps you one step behind your adversary.

The Best Cyber Defense Requires a Proactive Approach

It’s time to think (and act) like your adversaries. A proactive cyber defense approach enables you to turn tables on your cyber adversaries so you can reclaim your advantage.

Deception technologies allow security teams to easily bait, lure and deceive cyber criminals, and trap them with decoys, giving security valuable time to study and neutralize threats. Most importantly, deception automates threat detection and alerting, which reduces detection from months to minutes!

Engaging human attackers with decoys occupies adversary time with false assets and diverts their attention away from your production assets, resources, and data. In capture the flag simulations and exercises, the emulation of decoy services proves very effective, often engaging attackers for hours in high interaction.

Deception Technology Empowers Security Teams

Some believe deception is out of reach because it would take too much effort from already strapped security teams. Cyber defenders are already expected to do more with fewer resources than ever before. In reality, modern deception defenses use automation and phased implementation, which gives security teams time back in their day.

Effective deception technology monitoring and management requires less than one hour per day for a tier-1 security analyst at most companies. And with high-fidelity and custom-configurable alerts, security teams spend less time chasing down false alarms and more time eradicating attackers and configuring stronger defenses that hold up to future attacks.

Configuring Deception Technology the Easy Way

With an automated deception tool, the initial discovery phase conducts an initial inventory and analysis automatically learn an environment, and then continuously adapts to changes and additions. Decoys and breadcrumbs get created automatically, based on high-value targets, so that deception layers match the environment, even as it changes. This makes deception layers as realistic and dynamic as possible.

As the deception system runs, decoys, services, and associated breadcrumbs are deployed automatically. These fake assets take a negligible amount of system resources, yet they act as convincing lures that attract and convince adversaries. And with automated detection and alerts that include network and traffic analysis, cyber defense teams start investigations with aggregated intelligence and deep visibility into the attack patterns and lateral movements of the adversaries which accelerates time to remediation. This means security teams spend less time chasing false alarms and more time shutting down post-breach attacks before they can do damage to the organization.

Change the Game with Fidelis Deception

Fidelis Deception® turns the tables on attackers by altering the cyber terrain, with intelligent, automated creation of decoys, breadcrumbs, and lures that slowdown attackers and increase their cost of doing business.

With Fidelis Deception, external and insider threats can no longer move laterally undetected for months on end, ultimately stealing sensitive data or impacting business operations. Instead, they are lured and trapped at the deception layer, where they are discovered quickly and automatically, which prevents damage to your company and reduces the cost of the breach. Armed with intelligence and empowered with insights, your security teams can continually improve your proactive defense, so your cyber defense grows stronger with each attack.