INTRODUCTION

Cyberattacks are occurring at a relentless pace as sophisticated attackers continue to find ways to penetrate perimeter defenses. With each breach, security professionals face mounting pressure to detect and stop threats quickly before attackers can do damage. In addition to compliance expectations, new proposed breach notification laws promise significant fines and potential jail time if organizations do not meet notification expectations. Organizations of all sizes and across all industries are seeking innovation to mature their security models and close detection gaps. They want to understand their adversaries better and prepare to adhere to breach tracking and disclosure requirements. Organizations are now shifting their security strategies from a reactive defense to one of an Active Defense, which is not solely based on reacting to attacks but instead a balanced investment in the early detection and rapid response to threats.

DECEPTION TECHNOLOGY

Deception technology provides the innovation required to non-disruptively evolve to an Active Defense security posture. By deploying a fabric of deception-based detection throughout the network stack, companies can achieve efficient detection for every threat vector in the life-cycle of an attack. Deception tricks attackers into revealing themselves by using high-interaction decoys and lures, thereby alerting on and identifying detection gaps on threats that have evaded other security controls.

With early visibility into threats and actionable alerts for incident handling, deception solutions are rapidly becoming the solution of choice for proactively uncovering and responding to external, internal, and supplier threat actors. Organizations of all security maturity levels are aggressively adopting deception technologies to mitigate risks related to employee credential theft, Active Directory reconnaissance, data exfiltration, ransomware, crypto-mining, and attacks with the intent to disrupt services or impact public safety. The accuracy and ease of use of threat deception have been major drivers in its adoption and wide-spread deployment.

In 2019, analysts continued to recognize deception for its efficiency in detecting advanced threats, and EMA recently published research showing that deception technology users achieved dwell times of 5.5 days, a reduction of over 90% as compared to those who did not use it. A variety of surveys have also recorded the market’s intent to add deception technology to its security controls, given its efficacy and efficiency in deterring attackers.
WITH THE RAPID MIGRATION TO THE CLOUD, IT IS CRUCIAL TO THE DECEPTION FABRIC TO SCALE EASILY THEREBY. THE THREATDEFEND PLATFORM OFFERS EXTERNAL SUPPORT FOR AWS, AZURE, Google, AND OTHER CLOUD ENVIRONMENTS. INTEGRATION DEVICES AND LAUNCHER DEVICES THAT ALLOW USERS TO SELECT AND LAUNCH DECEPTIONS FROM THE TLP DESKTOP APPLICATION.

THE ATTIVO NETWORKS SOLUTION

THE THREATDEFEND® SOLUTION AND RESPONSE PLATFORM TURNS THE ENTIRE NETWORK INTO A TRAP, FORCING THE ATTACKER TO BE RIGHT 100% OF THE TIME. THIS TECHNIQUE REDUCES THE TIME TO RESPONSE AND REMEDIATION, ENHANCES NETWORK VISIBILITY, AND PROVIDES A PREDICTIVE VIEW OF ATTACK PATHS AND POTENTIAL THREATS.

DECEPTION FOR DETECTION AND ATTACK PATH VISIBILITY

THE THREATDEFEND SOLUTION AND RESPONSE PLATFORM PROVIDES UNPRECEDED VULNERABILITY INTO THREATS INSIDE THE NETWORK AND ATTACK PATHS MOVEMENTS AND TACTICS. THE PLATFORM DETECTS ADVANCED THREATS PROPAGATING THROUGHOUT THE NETWORK BY LAYING TRAPS AND DETECTING, DETECTING, AND DEFENDING AGAINST ATTACKS AS THEY OCCUR.

THE INFORMER DASHBOARD DELIVERS A COMPREHENSIVE VIEW OF THE ATTACK PATHS AND THREATS, ALLOWING USERS TO VISUALLY MODEL HOW ATTACKS CAN MOVE LATERALLY TO REACH THEIR TARGETS.

THE DEFENDER DASHBOARD PROVIDES A COMPREHENSIVE VIEW OF THE INCIDENT AND FORENSIC INFORMATION GATHERED DURING AN ATTACK. FORENSIC REPORTS INCLUDE IDENTIFICATION OF INFECTED SYSTEMS AND O365 ADDRESSES, AND EXPORT OF FULL DSC, PAR, AND STIX FORMATS TO ALLOW WIDER SHARING AND ANALYSIS OF ATTACK INFORMATION. THE INFORMER DASHBOARD INCORPORATES ACTIVITY LOGS AND RAISES EVIDENCE-BASED ALERTS TO THE USER.

IN ADDITION TO THE EARLY DETECTION OF ATTACKERS INSIDE THE NETWORK, THE THREATDEFEND PLATFORM’S ACTUALLY ALERTS, AUTOMATED ANALYSIS, AND INTEGRATION WITH THIRD-PARTY RESPONSE ORCHESTRATION PLATFORMS FOR AN EFFICIENT RESPONSE TO THREATS.

THE THREATDEFEND DECEPTION AND RESPONSE PLATFORM OFFERS CUSTOMERS:

• EARLY DETECTION AND FORENSICS TO IMPROVE THEIR SECURITY POSTURE
• AUTOMATED ANALYSIS TO INCREASE THEIR RESPONSE EFFICIENCY
• INTEGRATION WITH THIRD-PARTY RESPONSE ORCHESTRATION PLATFORMS FOR AN INTELLIGENT AND EFFICIENT RESPONSE TO THREATS

DECEPTION IS A STRONG AND EFFECTIVE WAY TO DETECT AND DEFEND AGAINST THE MOST ADVANCED AND UNPREDICTABLE THREATS. THE THREATDEFEND PLATFORM PROVIDES A INTELLIGENT AND EFFECTIVE WAY TO DEFEND AGAINST THE MOST ADVANCED AND UNPREDICTABLE THREATS.