WHITEPAPER

Attivo NETWORKS

DECEPTION TECHNOLOGY: A CRITICAL COMPONENT OF A MODERN CYBER SECURITY STACK

With hundreds of reported breaches occurring annually, organizations must build a comprehensive and adaptive security defense with a combination of prevention, detection, response, and predictive technologies that work actively together. Whether originating outside or starting as an insider, attackers have proven time and again their ability to evade traditional defenses. Detecting threats early inside the environment is critical to prevent data exfiltration, theft of sensitive information, or damage to an organization's critical infrastructure, brand, or reputation.

This document explains the role deception has played in historical conflicts and highlights why it has become a critical element of a modern cybersecurity stack. Deception technology is a core necessity in any security architecture.

WHAT IS DECEPTION?

Deception has been part of human conflict for as long as human beings have recorded their actions. From Sun Tzu to Niccolò Machiavelli, deception has long been a critical element any commander would use to win. Deception was integral in ensuring the success of the Normandy invasion by the Allies in WWII. Operation Quicksilver diverted German forces away from the actual invasion site to Pas-de-Calais. The Axis forces moved whole battalions north away from Normandy to defend against decoy military forces, reducing their defenses where the allies intended to land.

Similarly, military leaders in ancient China successfully employed the "Empty Fort Strategy," one of the "Thirty-Six Stratagems," to distract and defeat numerous attackers. In "The Romance of the Three Kingdoms", Zhuge Liang was trapped in a city with a small force while a more numerous army led by Sima Yi approached. He ordered all the gates to be opened and told his men to sweep and dust the ground. Sima Yi knew Zhuge Liang's reputation as a very cautious and prudent commander. Seeing this apparent lack of concern displayed by Zhuge Liang, Sima Yi feared an ambush and withdrew his troops. While likely embellished for dramatic purposes, this story shows how valuable deception can be when looking to create confusion and doubt in an adversary's mind.

It is invaluable to misdirect an attacker, making them believe one is strong where one may be weak and luring them into a trap. Attackers who fall for a deceptive strategy will often hesitate for fear of making another mistake. Moreover, it causes them to reveal their strengths and tactics in a manner that causes little risk and harm to the defender.

WHAT DOES DECEPTION MEAN FOR CYBERSECURITY?

Traditional prevention postures have proven inadequate as attackers have repeatedly demonstrated their ability to evade perimeter defenses. The number of breaches continues to increase, and year after year, security research shows that attackers are growing more sophisticated. Dwell times are still unacceptably long, and there is little that traditional security controls can do to detect attackers once they infiltrate the network and move laterally.

Deception is a valuable but, unfortunately, sometimes overlooked tool for anyone building a cybersecurity infrastructure. With its billions of networked devices and millions of applications, the reality of modern cybersecurity is that static defenses no longer suffice.

Adding deception technology increases the difficulty for adversaries to conduct their activities while remaining undetected. With deceptive assets mixed throughout the environment, attackers must now be correct all the time at every stage of the attack cycle or else risk detection. A single scan or access attempt against a deceptive asset or object anywhere in the network or on endpoints trips an alarm. By its very nature, deception does not generate false positives. Decoys, bait, and lures have no production value, and employees would not normally encounter them during regular business activities. The core concept of modern deception technology is that no one should ever interact with any deceptive asset, so any detection indicates suspicious or malicious activity. This concept is instrumental in detecting insider threats who would conduct actions not typically part of their daily processes.

Crafting decoy assets indistinguishable from production systems makes differentiating between them virtually impossible for an attacker.

The next generation of deception takes misleading attackers even further than decoys and bait by hiding and denying access to production files, folders, and storage. This potent tactic restricts the attacker's ability to see production data and storage locations, limiting visibility to decoy assets that force engagement with the deception environment. Furthermore, innovative solutions can misinform and redirect the attackers away from production assets when they attempt to conduct discovery activities, channeling their lateral movements against them by deflecting their attacks to decoys and away from critical systems.

> "Deception and misdirection technology is the only capability at market to single-handedly enable large enterprises to shorten the detection gap to hours or even minutes, protecting sensitive customer and organizational data." – DoD Chief

One other factor to consider is the efficiency gains by using deception technology, as recent research shows. One out of three alerts generated by traditional detection solutions is a false positive. While these can occur with deceptive detection, deception-based alerts also include detailed intelligence about the attack and the attacker, thus significantly increasing the ability to respond more effectively and the time it takes to identify false positives. Compared to the combination of system/device logs, IDS, IPS, DLP, or SIEM technologies, cyber deception is much simpler to design, deploy, and operate. When factoring in time gained from streamlining SOC operations with investigation efficiencies, deception technology can reduce SOC costs by an additional $4,600 per analyst per year for a total per analyst savings of almost $23,000 per year, or a decrease in SOC analyst costs of 32%. Furthermore, when factoring in deception's ability to reduce attacker dwell times by 91-97%, or down to 5.5 days, it can reduce data breach costs by 63%, an average savings of $249 million per incident or $5141 per compromised record.

HOW DOES ATTIVO BRING DECEPTION TO CYBERSECURITY?

Deception platforms detect and analyze internal attack activity, including discovery, credential theft, privilege escalation, lateral movement, and data collection. The Attivo Networks ThreatDefend platform uses fully customizable virtual machines as decoys to mimic production assets ranging from Windows and Linux servers to network infrastructure to IoT and SCADA devices, projecting them throughout the environment.

To an attacker looking for critical systems, credentials, drive share, and data, these decoys appear as tempting targets indistinguishable from production assets and worthy of exploration.

> Attackers on average infiltrate a network within less than five hours, and within fifteen hours they can exfiltrate data.

The ThreatDefend platform provides a much-needed detection solution for today's modern security teams of any size. Current tools such as SIEMs provide large volumes of data that require dedicated time and resources to separate false positives from actual security incidents. Signature-based systems such as anti-virus and endpoint monitoring tools can easily miss zero-day or sophisticated attacks. Behavioral analytics methods generate alert fatigue and routinely overlook advanced attackers and insider threats since human attackers are not fully computable objects. Current security controls cannot effectively detect attackers targeting Active Directory for discovery, data exploitation, lateral movement, and privilege escalation.

The ThreatDefend platform allows security teams to focus on finding and responding to attacks and giving them visibility into new and complex tactics by turning the entire IT environment into a trap. Additionally, the high fidelity and low volume of alerts allow the system to run with low maintenance and overhead while providing incredibly accurate and relevant threat data.

Deception technology is straightforward and quick to deploy. Within hours of installing an Attivo BOTsink or Endpoint Detection Net solution, security teams can project thousands of automatically customized decoys and bait through their network, providing deception and early alerting. With a proper "crawl, walk, run" strategy, this can mature into a fully integrated and authentic deception layer that will fool and catch even the most careful and mature threats.

The Endpoint Detection Net suite of products also allows organizations to create various deceptive credentials, fake objects such as SSH tokens, cloud platform keys, and SMB shares to place on existing production systems that lead attackers back to the decoys. The hidden SMB mapped shares act as lures for ransomware seeking to spread via network drives, stalling the malware by continuously feeding it data while throttling the connection to give security teams time to respond to it. Additionally, the ADSecure module looks for unauthorized Active Directory (AD) queries and intercepts the results, hiding sensitive or critical objects and returning deceptive lures in their place. The Deflect function also makes any production endpoint a decoy that redirects attacks targeting ports and services into the deception environment for engagement, essentially locking down endpoints from attacker lateral movement.

The ThreatPath component identifies credential exposures and misconfigurations on endpoints that allow attackers to move laterally across the network from system to system. The solution maps connections and indexes the data for searching and analysis. By identifying such vulnerabilities, the security team can clean the stored credentials, fix the misconfigured policies, or add decoy credentials to defend endpoints further.

When an attacker engages with the deception environment, the ThreatDefend Platform immediately alerts on the activity for security teams to quickly identify the source of the attack for automated incident response. When the attacker directly accesses a decoy or engages with a webpage or SMB share hosted on it, the platform logs all activity, displaying it to the security team in the dashboard. The platform captures the forensic data providing information for incident response and remediation actions, including

recording all command and control (C2) traffic and conducting memory forensics analysis. For the security team, this is a wealth of organization-specific threat intelligence they can use to improve their defenses further.

The ThreatDirect solution scales across on-premises, remote offices, and cloud environments. The forwarder comes as a VM, endpoint module, or containerized application. It can run on endpoints, servers, VM environments, or switches that contain a hypervisor or can run container applications. This deployment flexibility benefits organizations with extensive and varied network infrastructures.

> Attackers take an average of 4.5 hours to break out of a system.

The DecoyDocs solution creates deceptive files with an embedded beaconing function that notifies security teams of improper access. When alerting within the network, the solution provides the full details of the host accessing it. If the attacker exfiltrates the document, it will beacon home with the geolocation of every IP address that opens it. This capability gives security teams knowledge of what attackers are targeting.

The ThreatOps repeatable playbooks leverage the many native partner integrations built into the platform for a consistent and automated incident response process. This function removes complexity and accelerates incident response, easing workloads for security teams that face resource challenges.

Overall, the ThreatDefend platform provides a comprehensive and easy-to-use threat deception solution that scales across any size network, regardless of location, and accelerates incident response while providing critical adversary intelligence to improve defenses.

SUMMARY

The Attivo ThreatDefend Platform plays a critical role in empowering a threat-informed defense with real-time threat detection, credential and Active Directory vulnerability assessments, attack forensic analysis, and integrations to accelerate incident response dramatically. High fidelity threat information provided by Attivo reduces alert fatigue among security teams.

Technology integrations with partners serve as a force multiplier, which improves existing technologies, process, and resource productivity, making them better and ultimately reducing the time to detect and remediate an exploit or malicious threat actor. Working together with many partners, Attivo Networks continues to expand its platform and 3rd-party integrations to deliver the fastest detection and incident response to stop attackers in their tracks.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the leader in lateral movement attack detection and privilege escalation prevention, delivers a superior defense for countering threat activity. Through cyber deception and other tactics, the Attivo ThreatDefend® Platform offers a customer-proven, scalable solution for denying, detecting, and derailing attackers and reducing attack surfaces without relying on signatures. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, in the cloud, and across the entire network by preventing and misdirecting attack activity. Forensics, automated attack analysis, and third-party integrations streamline incident response. Deception as a defense strategy continues to grow and is an integral part of NIST Special Publications and MITRE® Shield, and its capabilities tightly align to the MITRE ATT&CK® Framework. Attivo has won over 130 awards for its technology innovation and leadership. www.attivonetworks.com