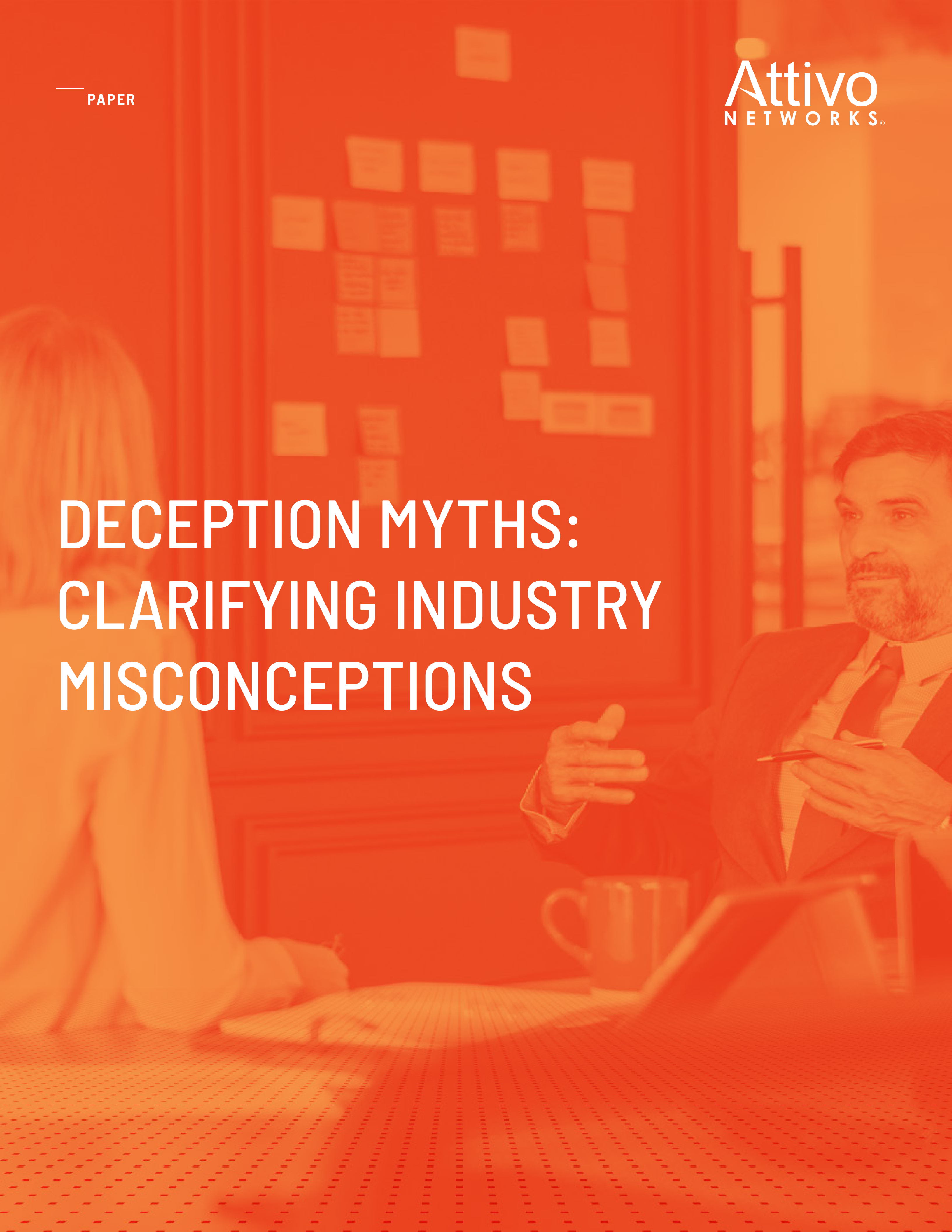


PAPER

DECEPTION MYTHS: CLARIFYING INDUSTRY MISCONCEPTIONS

EXECUTIVE SUMMARY

Deception has seen use in the contexts of law enforcement, military action, and survival settings for centuries. It is only recently that it has evolved from its earliest forms to become a useful tool in computer and network defense contexts.

The earliest deception systems were used primarily for research and they were difficult to set up and maintain. Those preliminary experiences have led to some myths and misconceptions about deception. This paper will address and debunk those myths, while detailing how deception has evolved into an invaluable asset for organization's Defense in Depth postures.

Various forms of deception technology have been around a while. With the evolution of the technology also comes misconceptions related to what challenges really exist, and which ones have been removed.

BACKGROUND: EARLY DECEPTION TECHNIQUES

Deception is one of the earlies concepts known to man. Fishermen and hunters have used lures, bait, and decoys, for centuries. Law enforcement has used various deception-based techniques to catch and convict wrongdoers. For the military, deception has played a key role for generations: from soldiers using camouflage to blend in with their surroundings, to elaborate ruses involving faked plans fed to an opponent, backed by entire staging areas and fake airfields, complete with inflatable aircraft and tanks to fool aerial reconnaissance into believing what they were seeing was real.

Deception in the computing realm is a much more recent application, with the first honeypots appearing in the late 1980's . These early efforts at tricking intruders were primarily in place for research purposes, dealing with specific security threats and providing insight into attack techniques used in the wild. Honeypots then evolved into honey nets, where multiple honeypots formed a dedicated network. The early honey net was also primarily for research purposes and positioned on the edge or as a standalone network.

Other techniques, such as Honeytokens and Honeydocs, appeared and offered more granular targets to potential attackers, as using, distributing, or altering the tokens, was easy to identify and track. However, these early techniques all shared characteristics that made them difficult to scale for use in an enterprise security context.

Manually configuring and deploying these early solutions was inefficient and impractical to manage at scale given the existing load on system, network, and security

> Attacker dwell time in 2018 was 191 days according to Ponemon & IBM. Deception Technology addresses the dwell time dilemma and shifts the power back to the defender with early detection and accelerated incident response.

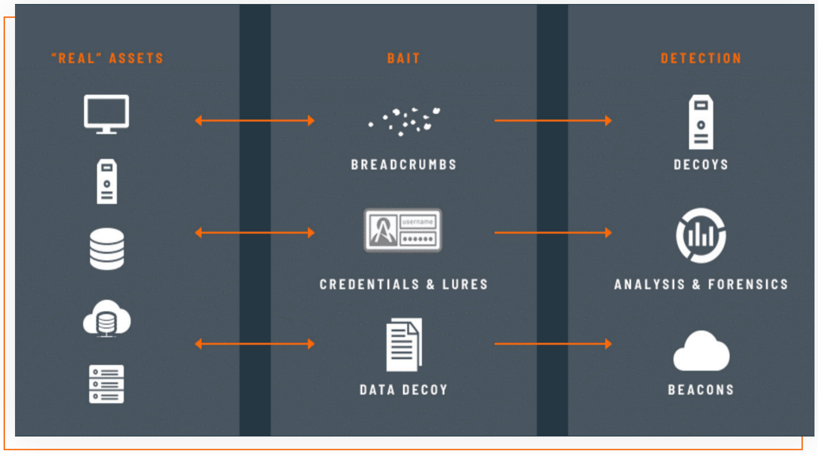
administrators. The earliest efforts to solve the deployment issue involved dedicated Linux distributions that were preconfigured as honeypots, but they were still impractical for larger deployments or for those with less skilled security teams.

The introduction of commercial, enterprise scale, deception solutions altered the landscape to make deception technology a practical solution for information security practitioners.

CATEGORIES OF DECEPTION

DECOYS AND LURES

Deception in information security covers a broad range of techniques that fall into two main categories: Network and Endpoint Deception. While these categories are designed to work together, each presents different benefits and is based on offering different types of targets or enticements to a potential attacker. Modern deception solutions now offer a way to centrally manage the deployment and consolidate reporting from the decoys in the field, which was missing in older deception-based technologies. That lack of central management and reporting was a legacy of the early honeypot and honeynet efforts, where it wasn't seen as an obstacle to a purely research-oriented effort.



NETWORK DECEPTION

In this context, network deception refers to any decoy, lure, or other form of deception that appears on, and is reached from, within the network. These are decoy assets that respond as if they were a real system or service, whether it is an entire host or just a single service.

When an attacker is doing reconnaissance or otherwise exploring for additional targets, network decoys give them viable targets to draw them away from production assets. These decoys can offer a range of interactions from simple emulation to presenting live services and operating systems and can often duplicate non-conventional assets . The most sophisticated decoys will use a "gold disk" image to perfectly duplicate live assets on the network, making it impossible for an attacker to tell the difference between a decoy and a real asset or service.

During a reconnaissance scan, the attacker will see a range of decoys in addition to real assets. This makes the threat surface appear much larger than it is, making their job much more difficult as they try and find a valid target. More important for the defender is that any interaction with a decoy is an event, since normal users should never be touching these assets.

> Where the original paradigm was "the defender needs to be right every time, while the attacker only needs to be right once," deception turns that on its head.

This is an important point for shifting the balance of power on the attacker. Where the original paradigm was "the defender needs to be right every time, while the attacker only needs to be right once," deception turns that on its head. Adversaries can no longer assume that "what they see is what they get" and now the attacker needs to be right every time or risk discovery.

Against malicious automated attacks, such as ransomware, worms, cryptojacking attacks, etc., deceptive network assets can provide accurate and early warning. Additionally, advanced decoy systems can be configured to slow down these automated attacks and give the information security team time to react to the attack. This allows them to quickly contain the infection and remediate the effected systems.

ENDPOINT DECEPTION

Here, endpoint deception refers to any lure, breadcrumb, or other kind of deception that is placed on an endpoint, such as a server, workstation, or individual user systems. Endpoint deception, as the name implies, is focused on deceptive assets on a system. These deceptions are placed primarily to attract and engage an in-network attacker looking to harvest credentials or find mapped shares.

Endpoint deceptions are deployed based on the assumption that attackers are seeking to gain access to a host. By providing lures and breadcrumbs at the points of entry, detection occurs early in the attack cycle. This quickly diverts the attackers from production assets into the deception environment where they can be observed and contained.

Examples of endpoint deceptions are deceptive credentials that appear as valid administrative, network, or user credentials, all of which are often early targets for an attacker set on elevating their privileges.

Gathering credentials, ideally administrative credentials, from a local machine is a common technique used by attackers to escalate privileges and move closer to their ultimate target. Compromising an authentication server could, with stolen credentials, be considered the attacker's "holy grail," as it can give them unrestricted access to the entire organization. This makes deceptive administrator credentials especially effective bait.

The ideal deceptive credentials follow the same format as production credentials and can be integrated with Active Directory to provide additional verification and authenticity to these lures.

MODERN DECEPTION

Early deception efforts could provide some of the features explained above, but they were not able to scale effectively in breadth or depth of the offerings. Modern deception systems solve that problem by offering levels of scalability, ease of use, control, and automation, that early systems simply couldn't match. Ideally, a modern deception system offers a full range of deception, both on the network and endpoints, that can efficiently scale to meet an enterprise's needs. To be fully effective, the solution can't stop with just deception.

Production environments require practical solutions, which leads to several basic expectation: the platform should be easy to deploy, easy to manage, provide useful and actionable information, and fit within an organization's security budget. The best solutions will include all the decoys and lures described above and backed by the complete enterprise-ready features described here.

From an infrastructure administrator's perspective, resources are often in short supply, so the solution must be easy to deploy and easy to manage on both the network and endpoints. It needs to gracefully scale across the organization and be able to adapt to changes and growth in an evolving environment. From a security administrator's perspective, the solution must be easy to work with, effective, and provide accurate and actionable information. It needs to compliment the rest of the security tools the enterprise has in place.

From a user's perspective, as an administrator or operator, the solution needs a user interface that is versatile and easy to use. To be most efficient, operation and configuration information must be easy to access and simple to interpret regardless of the user's role on the system.

Modern information security systems are a system, meaning they are not just single components working in isolation. The different components of the system must work together to provide effective and efficient protection, making integration a vital piece of the puzzle. Thus, a deception solution should work seamlessly with the other facets of a defense-in-depth strategy. Ideally, integration includes a high degree of automation, so attacks discovered by deception can be isolated, blocked, and remediated by the other security controls.

> A modern deception system should offer a full range of deception, both on the network and endpoints, that can efficiently scale to meet an enterprise's needs.

Modern deception technologies, unlike their ancestral honeypots and honeynets, are complete solutions that are easy to use, easy to deploy, and fully integrate with the rest of an organization's security tools to support a fully realized defense in depth posture.

DECEPTION MYTHS

Several myths remain in circulation about deception technology, largely based on its origin in research-oriented honeypots and honeynets. In some cases, the myths can be traced to vendors in the industry who focused only on one aspect of deception and want to steer buyers towards what they have to offer.

Some skepticism is common with any new technology and, in this context, deception at enterprise scale is still comparatively new. This leads to myths driven by a lack of understanding of what deception is or what it is capable of.

Below, we address some of the most common myths and explain the facts behind them.

"DECEPTION IS THE SAME THING AS A HONEYPOT" - FALSE.

Honeypots, some of the earliest deception systems, are very limited in capabilities and are extremely difficult to manage and operate. Commercial grated deception technology has evolved considerably since then to incorporate a full range of high-interaction decoys, lures, and deception techniques. Modern deception technologies are part of a full system that scales to cover an enterprise environment and take additional measures to ensure believability against a sophisticated attacker. Deception technology has also conquered the operational issues seen with honeypots through the use of machine-learning and automations.

"YOU ONLY NEED DECEPTION ON THE ENDPOINTS" - FALSE.

Deception on the endpoint is valuable for quickly misdirecting attacks. Deceptive credentials and lures can efficiently divert an attacker away from production resources, but endpoint deception alone is not enough. There are a range of activities that endpoint deception alone won't catch, including reconnaissance and lateral movement when an attacker tries to extend their foothold.

"YOU ONLY NEED DECEPTION ON THE NETWORK" - FALSE.

Network decoys are a hallmark of deception, providing inviting targets to draw an attacker's attention, but network decoys alone are not enough. Many attacks start on a compromised endpoint and much of an attacker's initial strategy is based on what they find on the that compromised endpoint. This makes endpoint deception a crucial piece of the puzzle. A high interaction decoy will also be able to provide deeper engagement and adversary intelligence.

“YOU ONLY NEED DATA DECOYS OR HONEYDOCS” - FALSE.

Honey-docs are a range of documents that appear inviting to an attacker but are tagged so they can be tracked if they are exfiltrated from the company. They are useful to identify where “stolen” assets are going, but do not provide the full scope of deception necessary to effectively detect and derail, an attacker. Honey-docs can be very useful for counterintelligence, but they only represent a subset of deception techniques.

“DECEPTION IS HARD TO DEPLOY” - FALSE.

In the early days of honeypots and honeynets, each system was built individually and customized for each specific deployment. This was acceptable in a research environment where resources were available, but this type of technology definitely couldn’t scale to enterprise levels. Modern, comprehensive, deception solutions, on the other hand, are designed with easy deployment in mind. Deploying decoys and pushing deception to the endpoints from a modern system is only a few simple steps, and automation with machine learning can make the process even faster and more efficient.

“DECEPTION IS HARD TO MANAGE” - FALSE.

When honeypots and honeynets were all custom builds, managing them was a challenge both from a technical and resource standpoint. With modern deception solutions, easy management is built in from the start. A complete deception solution offers easy maintenance, a comprehensive user interface, automation, and integration with the rest of an organization’s data security systems. These modern deception solutions are easy to deploy and easy to manage.

“DECEPTION IS EASY TO SPOT” - FALSE.

Modern deception solutions are designed with authenticity and believability as core tenants, blending cleanly into a production environment without leaving any easily identified clues they are anything but authentic assets. Decoys relying on emulation, will have some success when they are leveraging the element of surprise. For full authenticity, the decoy should us real operating systems and services that will make them appear as identical to production devices. This makes it extraordinarily difficult for an attacker to identify, and evade, deceptive defenses.

THE ATTIVO SOLUTION

The Attivo Networks® ThreatDefend™ platform offers a state-of-the-art Deception Technology solution for commercial grade deployments. Based on the premise that malicious actors will manage to get in past the perimeter, Attivo’s deception solution provides unparalleled detection on both the network with host and service decoys, and on the endpoints with authentic looking credentials and other bait to lure and misdirect attackers away from valuable production assets.

The ThreatDefend platform starts with the BOTsink® server that directly hosts the full range of network and service decoys, generates the endpoint decoys, and provides the comprehensive user interface that provides the security operations team visibility into the environment and attacks occurring within the deception environment. The BOTsink server is available as a physical or virtual appliance, or as a Cloud instance, providing the deployment flexibility modern environments require.

BOTsink decoys can be configured using machine learning to observe the organization's live environment, making the deception assets indistinguishable from real production servers and services.

BOTsink decoys can be configured using machine learning to observe the organization's live environment, making the deception assets indistinguishable from real production servers and services. Machine learning will automate the preparation, deployment and ongoing management of the deception environment for simplified operations. Fully customized decoys can also be created by loading in golden images that match the production environment perfectly. The architecture of the BOTsink solution is unique in that all deceptions are centrally managed and then projected onto the network. This removes any complexity and per license costs, keeping deployments simple while upholding the highest authenticity standards.

To provide deception on the endpoints, the ThreatDefend platform includes the ThreatStrike® solution. This component features deceptive credentials that are indistinguishable from real production credentials, which direct an attacker to a BOTsink hosted decoy rather than a production asset. It also places deceptive documents, mapped shares, and other assets, that can derail an attack by directing the threat into the decoy environment. This protects the production environment from live attackers and automated threats, including malware – ransomware, cryptomining, keyloggers, etc. ThreatStrike's "bundle" is compatible with multiple operating systems and can leverage a broad range of management tools to simplify and automate deployment.

ThreatDirect™ gives organizations the ability to project decoys into remote locations without the need for an actual deception device. By efficiently extending the BOTsink's capabilities into remote sites, for both network and endpoint decoys, the organization gains full coverage without increasing the workload on their security operations team.

The ThreatPath® system can give the security team visibility into potential pathways based on exposed or orphaned credentials, RDP, or misconfigurations that an attacker could use to gain access to their targets. This topographical or table-based visualization can be invaluable, providing SecOps with the visibility to set up and enforce policies, permissions, and relationships that minimize the attack surface and an attacker's options.

The BOTsink appliance has an evidence collection capability that delivers real-time forensics with enhanced visibility and aligns to the NIST Cybersecurity Framework. By providing a more complete view of attacks, the capability delivers immediate attack data for accelerated remediation. During the attack, the collection function captures memory, registry changes, network activity, originating endpoint, lateral movement, C&C addresses, file changes, exposures, and more, all displayed in a central dashboard. Additionally, organizations can safely let the attack play out in the deceptive environment to collect adversary intelligence, TTPs and IOCs, and is easily shared with other security controls to remediate the threat and for root cause analysis. This is especially useful for quickly detecting, containing, and gathering intelligence to remediate and hunt for sophisticated and determined attackers.

The ThreatDefend platform also includes advanced malware analysis tools that let an organization easily identify new attacks, whether they are identified as a payload in the deception environment or manually sent to the system for analysis. Further, the solution includes native integrations with a broad range of 3rd party security solutions. Integration allows the Security Operations team to automate their response to isolate or quarantine infected hosts, start forensic analysis, generate advanced reports, and initiate service tickets, improving their efficiency and effectiveness.

SUMMARY

Myths about deception are often based on misconceptions or information that's simply out of date. The technology's origin in research honeypots and honeynets, combined with inaccurate information, has created a certain level of FUD about what deception can do and how it works.

Modern deception technology provides an organization with unparalleled detection capabilities that other solutions cannot provide. Deception is easily deployed, accurate, and fills in the gaps other solutions leave open. With improved detection, an organization gains tighter security, faster response times, and better efficiency from their security operations team.

Attivo's approach to deception technology offers the most complete solution available on the market, with deception on the network and endpoints that is easy to deploy, easy to operate, and fully integrates into a modern defense in depth strategy.

ABOUT ATTIVO NETWORKS

Attivo Networks®, the leader in deception technology, provides an active defense for early detection, forensics, and automated incident response to in-network attacks. The Attivo ThreatDefend™ Deception Platform provides a comprehensive and customer-proven platform for proactive security and accurate threat detection within user networks, data centers, clouds, and a wide variety of specialized attack surfaces. The portfolio includes expansive network, endpoint, application, and data deceptions designed to efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning makes preparation, deployment, and operations fast and simple to operate for organizations of all sizes. Comprehensive attack analysis and forensics provide actionable alerts, and native integrations automate the blocking, quarantine, and threat hunting of attacks for accelerated incident response. The company has won over 65 awards for its technology innovation and leadership.
For more information, visit www.attivonetworks.com.