DECEPTION-BASED THREAT DETECTION

SHIFTING POWER TO THE DEFENDERS

Carolyn Crandall and Joseph Salazar
WHAT IS THIS BOOK ABOUT?
This book provides a general introduction to deception technology and an overview of use cases from general detection to creating an active defense. You will gain a better understanding of how deception fits within your overall security architecture and the role it plays in detecting, identifying, and responding to threats.

WHO IS THIS BOOK FOR?
This book is for anyone interested in learning not only about the basics of deception technology, but also how deception can be used strategically to stop advanced attackers.
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The cloud</td>
<td>94</td>
</tr>
<tr>
<td>The supply chain: VARs, suppliers, and third-parties</td>
<td>97</td>
</tr>
<tr>
<td>Warehouse: Distribution center, manufacturing location, and more</td>
<td>100</td>
</tr>
<tr>
<td>Advanced deceptions and detection</td>
<td>103</td>
</tr>
<tr>
<td>Benefits across deployment models</td>
<td>106</td>
</tr>
<tr>
<td>Deception Operational and Management Efficiency</td>
<td>107</td>
</tr>
<tr>
<td>Active Defense vs. Cyberwarfare</td>
<td>110</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>114</td>
</tr>
<tr>
<td>Acknowledgments</td>
<td>117</td>
</tr>
</tbody>
</table>
FOREWORD

As founder of the Honeynet Project, I’ve always been fascinated by the world of deception. Deception brings tremendous advantages to the cyber defender, from simplified threat detection and hunting to cyber intelligence gathering and dynamic defenses. Early attempts at deception technologies, including honeynets, were hampered by complexity. However, since those early days, deception has rapidly evolved in efficacy, scalability, and ease of use. This is why I’m thrilled to write a Foreword for this book.

My history with honeynets started when I built my own solution in 1998, which eventually led to the Honeynet Project. In many ways, this is when cyber deception was born. A lot has changed over the last 20 years. Commercial deception has increased its overall efficacy and has dramatically decreased the time it takes to create and manage a deception network from weeks down to what a single systems admin can do during their lunch break.

I’m thrilled to see this book published to help us all better understand what deception is and the value it brings to organizations of all sizes.

Lance Spitzner
Director, SANS Institute

INTRODUCTION

Increased compute power, artificial intelligence, and tools on the Dark Web are equipping cyberattackers with the resources to launch more sophisticated and destructive attacks. Reactive defenses are no longer enough to stop attackers from infiltrating even the best security architectures. Environmental dynamics are also changing and disrupting resiliency with the rapid adoption of cloud infrastructure and the proliferation of IoT devices. The concept of a perimeter as we have known it is disappearing, and the battle against cybercrime has moved inside the network. With this shift, organizations need to rethink their security strategies as well as the tools they have traditionally come to rely on.

A prevention only defense is no longer enough, and organizations are seeking new tools and programs for early detection, faster response, and gaining a better understanding of their adversaries. Cyber deception is serving to meet these needs driven by its simplicity, ease of use, and ability to complement security solutions already in place. The solution uniquely carries the benefit of not only being able to disrupt and derail attacks but also, in its power to shift the asymmetry in the direction of the defenders.
THE IMPACT OF DECEPTION ON CYBER CRIMINALS

WHAT IS CYBER DECEPTION?

For millennia, deception has been used to effectively confuse and outmaneuver opponents in warfare, sports, and gambling. Now deception is being applied to the cyber realm to create uncertainty in the attacker’s mind, to trick them into making mistakes that reveal their presence, and to make the overall attack economics unfavorable. With deception technology, security teams do not need to wait and react to an attack. Instead, they can deploy bait, lures, and decoys designed to derail attacks early and throughout the attack lifecycle.

Attackers typically harvest credentials, conduct reconnaissance, and move laterally to complete their attack. With a deception fabric, organizations create a virtual minefield consisting of credential bait and decoys that mirror the production environment’s operating systems, applications, and data. As soon as an attacker interacts with a deceptive asset, the security team receives a high fidelity, engagement-based alert with the information required to not only stop the threat actor but also understand them.

Unlike other detection tools, a high-interaction deception environment provides defenders the option to safely study their opponent while gathering adversary intelligence. By gaining insight into the attacker’s tools, methods, and intent, the defender is armed with deeper knowledge for strengthening overall defense strategies, leveling the playing field with their opponent.
If an organization says they are not interested in deception, they are fundamentally ill-equipped to address modern adversaries and leave their organization willingly exposed.

- MATT STAMPER, CISO, EXECUTIVE ADVISOR | EVOTEK CO-AUTHOR, CISO DESK REFERENCE GUIDE (VOLUMES 1 AND 2)

**WHY DECEPTION MUST BE A PRIORITY**

Attackers remain undetected in networks for much too long after the initial compromise. Dwell time ranges from 79 days to over 200 days, depending on the region and source of the report. These numbers reinforce that an attacker is afforded far too much time in an enterprise while remaining undetected.

Conversely, even when defenders successfully disrupt and remediate attacks, too often little useful information is gathered about the adversary. This lack of information makes verifying the removal of the attacker’s foothold and preventing a successful return extremely challenging. Unlike attackers, who gain knowledge about the environment each time they attack, defenders do not acquire additional insight, putting them at a distinct disadvantage. As in physical attacks, understanding potential adversaries is critical to countering their next move.
THE EVOLUTION OF DECEPTION:  
FROM HONEYPOTS TO A FULL DECEPTION FABRIC

The first mentions of honeypots appeared in the late 1980s and early 1990s by Cliff Stoll in his book The Cuckoo’s Egg and Bill Cheswick’s paper An Evening with Berferd in his deployment of emulated honeypots. Following this, Marcus Ranum produced the Back Officer Friendly solution in 1998, Neils Provos published Honeyd in 2007, and many other projects followed suit. These were based on low-interaction, emulated deceptions to detect mass network scanning or automated attacks (malware, scripts, bots, scanners), and to track worms.

Honeypots were useful. They were inexpensive, typically set up to detect threats outside the network as well as for general research. However, the use of honeypots was limited because:

- Human attackers could easily identify an emulated system, fingerprint it, and avoid future interaction with them, or even worse fill the honeypots with bogus data.

- Honeypots are generally low-interaction environments, limiting the information that can be collected. As a result, they provide little value for improving incident response or gaining a better understanding of threats.

1 Low-interaction honeypots are used mainly for detection. Attackers can only interact with the honeypot in limited ways. High-interaction honeypots (they do exist) enable attackers to do more with the system but are also vulnerable to attack themselves. In this ebook, the term honeypot refers to low-interaction systems.
• Inline solutions can be used as a pivot point for attackers to continue their attack.

• Honeypots are not designed for scalability. They are complex to deploy, operationally intensive to manage, and require deep expertise to maintain.

Modern enhancements in deception started appearing in 2014 based on the convergence of virtualization, machine learning, and automation. The concept of a deception fabric expanded the technology beyond honeypots and into layers of network, endpoint, application, and data deceptions. This is when the commonality between honeypots and commercial deception diverged. As such, comparing modern deception technology to a honeypot or honeynet is roughly analogous to calling a Tesla a Ford Model T.

“Taken in its totality, ease of setup, ease of management and very low false positives, deception technology creates a layer of detection in the environment that, with very little effort, can analyze topology, explain complex relationships to administrators, suggest recommendations for improving the network and alert only when under attack.

– SIMON GIBSON, GIGAOM
THE ROLE OF MODERN DECEPTION TECHNOLOGY

Deception benefits start by greatly simplifying detection. Security teams gain immediate visibility to attack activities that are traditionally difficult to detect, such as lateral movement, credential theft and reuse, internal threat reconnaissance, man-in-the-middle (MITM) activities, and attacks on directory services such as Lightweight Directory Access Protocol (LDAP) or Active Directory (AD). The visibility and accuracy provided by deception also serve as a force multiplier to existing security controls, adding a critical layer of in-network defense to the security stack.

Enterprises of all sizes should consider adopting deception technology for the following benefits:

- Rounds out a defensive strategy with early and accurate detection
- Almost zero false positives
- Comprehensive and scalable attack surface coverage
- Threat visibility throughout the attack lifecycle
- A real-time inventory of networks, systems, software, and relationships
- Threat intelligence to help correlate traffic with threat indicators
- Requires minimal overhead and delivers value quickly
- Effective detection for both internal and external threat actors

“Attivo is great for both ends of the maturity scale. Security teams that are still in the beginning phases of their security program and are still trying to close the windows and lock the doors, Attivo will give them the confidence that they are recovered for when an attacker makes it inside of the network. For security teams that are much more mature, Attivo gives them visibility for how the attackers are getting in.”

- CISO OF MAJOR ENTERTAINMENT ORGANIZATION
WHERE DECEPTION FITS INTO THE SECURITY STACK

Deception should not be viewed as a “rip and replacement” of existing security controls; it complements and enhances them. The decision to add deception should be based on a need for early and simplified threat detection, closing in-network detection gaps, strengthening security programs across multiple environments and threat vectors, and for its ability to do things that other security solutions cannot do.

Additionally, deception provides visibility into exposed attack paths, attacker activity, and captured threat intelligence. This, paired with forensic recording, enhances and elevates a security team’s ability to prevent an attack and to respond decisively when under attack.

Adding a new capability to a security stack can come with complexity as security teams work to incorporate the solution into their operations. This is generally not the case with a deception platform. Such platforms integrate with existing systems in a way that requires minimal effort to deploy, operate, and manage. Advanced deception platforms won’t disrupt other network functions. They operate out of band and have the flexibility to white-list devices to avoid conflicts. They also don’t require the installation of endpoint agents.

A deception platform’s high-fidelity alerts become a true force multiplier when applied to endpoint detection and response (EDR), network traffic analysis (NTA), and security information and event management (SIEM) solutions for better and more accurate detection. Native platform integrations with existing security infrastructure provide seamless sharing of attack information and facilitate automation. Benefits include automated blocking, isolation, threat hunting, and repeatable playbooks that accelerate incident response. Some solutions also provide integrations with threat orchestration tools for streamlined operations.
5 Days
Average Dwell Time

90%
Performance Improvement

98%
Achieve at or Above Expected Value

- EMA, A DEFINITIVE GUIDE TO DECEPTION TECHNOLOGY

ATTACKERS ARE MOST CONCERNED ABOUT

- 56% IDS/Next Gen Firewalls
- 55% Deception
- 34% EDR/Next Gen AV
- 19% IAM
- 45% Traffic Analysis
- 41% SIEM
- 15% UEBA
- 1% Other

ATTIVO NETWORKS 2018 CYBERSECURITY SURVEY
THE ROLE OF DETECTION IN A SECURITY PROGRAM

Traditionally, security programs primarily focused on prevention-based strategies aimed at stopping attackers from getting into the network. These programs attempt to use hardened perimeters and endpoint defenses by recognizing and blocking malicious activities to detect and stop attackers before they can get in. Most organizations implement such a strategy by fortifying their networks with defense-in-depth through layered prevention controls.

Detection controls are usually placed to augment prevention at the perimeter, and not as consistently deployed for in-network threat detection. This architecture leaves detection gaps that are difficult to fill with existing security controls not specifically designed for that role.

Rather than using prevention alone, a strategy that attackers have consistently succeeded against, defenders are adopting a more balanced strategy that includes detection and response.

Most organizations deploy an intrusion detection system (IDS) or next-generation firewall that picks up known attacks or attempts to pattern match for identification. Other detection tools use monitoring, traffic, or behavioral analysis. These reactive defenses are designed to detect once they are attacked yet often fail. They also have some limitations because they are not designed to catch credential harvesting or attacks based on what appears as authorized access. They are also often seen as complex and prone to false positives, adding to analyst alert fatigue.

The security industry has focused recent innovation in finding more accurate ways to recognize malicious activity with technologies such as user and entity behavioral analytics (UEBA), big data, artificial intelligence (AI), and deception.
SECURITY CONTROLS THREAT ACTORS ARE MOST WORRIED ABOUT

According to security professionals, attackers are most concerned about IDS and deception technology at 56% and 55% respectively. IDS stops known attacks while deception detects those that evade security controls.

UEBA, big data, AI, and other forms of network traffic analysis rely on signatures, database lookup, or pattern matching to identify threats. This requires time for the systems to learn and become effective and will also require ongoing tuning. Throughout this process, security teams often experience excessive false positives that create alert fatigue. The “noise” created by these solutions has limited deployments and been a barrier to usage.
TYPES OF DECEPTION TECHNOLOGY

Today, there are several approaches to threat deception – network, endpoint, application, and data. Deception technology is available as a full deception fabric or platform, as features within a broader platform, and as independent solutions. When choosing a solution, consider factors such as attack surface coverage, scalability, and efficacy against multiple attack vectors.

The following sections describe the different types of deception technology.

ATTACK SURFACE COVERAGE

**Network Decoys**
- User network and datacenter systems and servers
- Active Directory domain controllers and objects

**Virtual Private Cloud (VPC) Decoys**
- Containers, virtual machines (VMs), servers, and serverless functions.

**Non-traditional Decoys**
- Operational technology (OT)
- IoT, medical IoT
- ICS–SCADA (Supervisory Control and Data Acquisition) systems
- Point-of-sale (POS) systems
- Network infrastructure
- And more...
NETWORK DECEPTION

High-interaction decoys that appear identical to production assets are deployed throughout the network and are designed to detect attackers during reconnaissance and lateral movement attempts. The concept is to hide in plain sight by creating a camouflaged environment where the attacker is tricked into believing what is fake is real.

Coverage. For optimal detection and attack surface coverage, deception decoys should be able to mimic and seamlessly blend in with the production asset.

Authenticity. Believability is critical. For full deception authenticity, the decoys should run the same operating systems and services as production assets so that highly skilled attackers cannot discern which assets are decoys and which are real. They should match the other networking characteristics of production devices to be credible to the threat actor. The highest level of authenticity can be achieved if decoys run the same “golden image” that is used in production.

Lateral movement. A dynamic, high-interaction deception environment enables decoys to communicate with each other to capture an attacker’s lateral movement and techniques as they believe they are advancing their attack.

ENDPOINT DECEPTION

In addition to endpoint decoys, genuine-looking and attractive deceptive credentials and lures are placed on existing systems and servers. The solution also provides capabilities to monitor available services on production endpoints, and redirects attempted access into a deception environment. Plus, exposed credential mapping provides for visibility into lateral attack paths.

Credentials. Comprehensive endpoint deceptions cover a wide variety of application and memory credential lures, browser credentials, history, and items such as identity and access management (IAM) access accounts, access keys and tokens, S3 buckets, serverless functions, and Domain Name Service (DNS) entries for cloud environments. Customization of these credentials as well as timestamping keeps them attractive. For authenticity, credentials should be able to validate within AD. Additional AD deceptions can hide high-value objects such as administrator or service accounts and present decoy credentials in their place without altering the production AD environment.

Deployment. Agentless deployment models are generally preferred, as they require less overhead to operate and maintain. Integration with existing endpoint management systems can also provide deployment and management flexibility.

Deflection. Endpoint scan deflection and obfuscation of Active Directory information deflects attacker activities to decoys for engagement and reduces the risk of lateral movement.

Attack Path Visibility. Identify exposed, orphaned, or misused credentials stored at the endpoints for attack surface risk reduction. This also identifies misconfigurations that attackers can leverage to move between systems.
APPLICATION DECEPTION

Application deceptions allow an organization to publish internal decoy applications, such as a SWIFT terminal, a web application with a supporting database backend, or network directory services. Application deception provides additional targets for an attacker to pursue in the deception environment. It is especially useful for learning what attackers are pursuing within the network as well as for identifying external and internal threat actors using valid credentials.

DATA DECEPTION

Database, network, and endpoint data deceptions can be placed strategically, giving attackers the promise of personally identifiable information (PII), intellectual property, AD privileged accounts, or other valuable data. They can also redirect network-enabled malware or ransomware attacks from production systems to the deception environment.

Data deceptions can include decoy file servers and services, fake credentials, decoy documents, server message block (SMB) shared drives, and network shared folders. Adding deceptive files, databases, or decoy document beaconing functionality provides additional insight into what an attacker is seeking to steal and the geolocation of where files are accessed.

Deception involves setting up decoys so as to mislead an adversary. With varying levels of sophistication, deception has been an integral part of the nature of conflict itself, both for attackers and defenders.

When defenders couple effective deception with believable artifacts, attackers are forced to spend significant resources on trying to decipher real from fake. With efficient deception, these artifacts can be created with minimal cost to the defense and can be a powerful tool for a number of detection use cases.

- FERNANDO MONTENEGRO, PRINCIPAL ANALYST AT 451 RESEARCH
CONSIDERATIONS FOR SELECTING DECEPTION TECHNOLOGY

For maximum coverage, an organization should consider a full fabric deception solution. An endpoint solution is useful but does not help with lateral movement or threat detection in the cloud. Similarly, network decoys miss endpoint credential-based attacks and do not offer the ability to place bait for ransomware attacks in the deception environment. Without deploying both endpoint and network decoys, defenders could miss some activity like Man-in-the-Middle (MITM) attacks.

By choosing a deception technology platform that offers network, endpoint, application, and data deceptions that scale across a broad range of attack surfaces, organizations gain the best security posture for early and accurate in-network detection, regardless of attack method or the access point attackers choose to exploit.

Additionally, for Windows environments, one must consider the availability, breadth, depth, and intrusiveness of an AD deception solution. Protecting AD with deception that can divert attackers while hiding critical accounts and objects without altering the production environment offers efficient and unobtrusive defenses.

THE IMPORTANCE OF EARLY DETECTION TO REDUCE DWELL TIME

“More than half (61%) of security professionals say that 100 days of dwell time is representative (or below) what they are seeing.

One-third of respondents expect dwell time to increase, indicating that organizations anticipate attackers to get even better than they are today, and security programs may not be able to keep up.”

- ATTIVO NETWORKS 2018 GLOBAL CYBERSECURITY SURVEY
DECEPTION AND THE ATTACK CYCLE

Deception is an extremely effective detection mechanism throughout various stages of an attack, providing visibility into actions that most organizations cannot easily detect.

Traditionally, most security investments focused either on preventing the attacker from successfully getting in (firewalls, antivirus, intrusion prevention systems, and similar technologies), or detecting attackers who try to leave with any data of value (data loss prevention). However, attackers spend the most time inside the network in the persistence cycle of privilege escalation, internal reconnaissance, lateral movement, and maintaining a presence. Deception excels at providing internal visibility to such activities while denying accurate intelligence to the threat actor through misinformation and misdirection.

<table>
<thead>
<tr>
<th>ATTACK CYCLE PHASE</th>
<th>ATTACKER ACTIVITY</th>
<th>DECEPTION CAPABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish Foothold</td>
<td>Install custom malware, establish command and control (C2), and exploit applications to establish remote access</td>
<td>Network decoys alert on attempts to compromise the system or communicate with C2 servers</td>
</tr>
<tr>
<td>Escalate Privileges</td>
<td>Credential theft, “pass-the-hash,” MitM attacks, or brute force password cracking</td>
<td>Decoy endpoint credentials lead attackers to the deception environment for alerting and activity recording. MitM detection identifies credential theft and vulnerable credentials for lateral movement</td>
</tr>
<tr>
<td>Internal Reconnaissance</td>
<td>Critical system recon; system, AD, and user enumeration; ping sweeps; port/service scans; target identification; internal intelligence gathering</td>
<td>Network decoys with decoy services, decoy user accounts, decoys for cloud services and functions, and AD deceptions to hide real objects while diverting attacks with decoy data and alerting on the activity. Deflection to divert port/service scans to decoys.</td>
</tr>
<tr>
<td>Lateral Movement</td>
<td>Net use commands, reverse shell access, mapped share access, or stolen credential reuse to compromise remote systems</td>
<td>Network and cloud decoys alert on lateral movement and capture forensics on attacker activity for analysis.</td>
</tr>
<tr>
<td>Maintain Presence</td>
<td>Backdoor variants, VPN subversion, sleeper malware, or remote access trojans that allow for re-entry</td>
<td>Network decoys alert on software installation, remote access, or C2 traffic while capturing forensics for analysis</td>
</tr>
</tbody>
</table>
“Deception is about deceiving the threat actor and allowing us a new creativity of “getting in the head of the actor” to slow them down or get better insight.”

- DIRECTOR OF CYBERSECURITY, MAJOR HEALTHCARE PROVIDER
CHANGING THE ASYMMETRY OF CYBERATTACKS

With each attack, the adversary learns more, gaining knowledge of the network architecture and finding accessible attack paths and credentials needed to complete their objectives. In contrast, the defender typically does not gather information on the adversary, even with detection because most systems quickly deflect (and end) the attack. Many detection solutions do not gather in-depth information until much deeper in the attack lifecycle.

These factors make cyberattacks asymmetrical: the attackers have the advantage of time and stealth to gather the information needed to outmaneuver the defender. Deception changes this asymmetry by creating an environment where an attacker cannot tell real from fake and now must also be right 100% of the time or risk being revealed.

The attacker only needs to be right once to get in, while the defender must be right every time to protect their network, assets, and data.

ADVANCED DECEPTION FOR AN ACTIVE DEFENSE

An active defense strategy involves direct defensive actions taken to destroy, nullify, or reduce the effectiveness of cyber threats against an organization’s assets. These defensive activities increase attacker resource expenditures while reducing those of the defender. With deception, the attacker focuses on targets with no corporate production value while the defenders gather information on the attacker’s tools, techniques, and methods.

Deception puts the burden on the attacker to discern real from fake. Network decoys, endpoint breadcrumbs, deceptive applications, and decoy data disrupt the attacker’s advantage of stealth by detecting them early in the attack cycle. When attackers attempt to use deceptive credentials or engage with a network decoy, they spend precious time and resources interacting with an asset that does not advance their attack. Conversely, the defender gains valuable threat and adversary intelligence.

With deception, the attacker cannot gain an accurate picture of the network. Network decoys appear as regular systems and respond to discovery scans, causing uncertainty and polluting the attacker’s information with inaccurate data. Endpoints deflect port and service scans to decoys for engagement, making it appear to attackers that they are engaging with a production system instead of a decoy.
This misinformation alters attackers’ understanding of the network, slows them down, and causes them to make mistakes.

Introducing deception adds uncertainty to the environment that attackers must now factor into their activities. Attackers that suspect or are aware of deception in the environment must now question their discovery scans and whether the system they are targeting is a valid production asset or a decoy that alerts on malicious activities. The attackers can no longer trust their tools or target a system with confidence, increasing their costs as they slow their activities in an attempt to validate information, avoid the decoy systems, and identify real targets.

The known deployment of deception can be a strong deterrent. As attack processes become more complex, there is a higher likelihood that attackers must repeatedly restart their attacks, and the economics are no longer favorable. Collectively, these challenges motivate attackers to seek easier targets.
A critical advantage of deception–based defenses is that they give defenders an edge, a home-field advantage. They can actively feed their adversaries deceptive information that affects the observe and orient phases of a decision–making cycle called the OODA loop.

The OODA loop (Observe, Orient, Decide, and Act) is a cyclic process model proposed by Colonel John Boyd, USAF, from his observations of air combat in the Vietnam War. He found that fighter pilots continuously cycled through four phases while engaged with the enemy: observe what is happening, orient to the situation, decide on a course of action, then act on it. Pilots who cycled through this process faster than their opponent usually won the engagement. To gain the advantage, one must either find a way to cycle through their OODA loop faster or slow the adversary’s loop by adding friction.

Deception inserts significant friction through misdirection and misinformation in the observe and orient phases of the adversary’s OODA loop. The defender gains an edge over the adversary by slowing the attacker’s process, giving themselves more time to decide and act, and providing a clearer understanding of how the adversary is moving and reacting to the deception. Attackers make decisions based on faulty or inaccurate information that clouds their situational awareness and disrupts their OODA loops. With deception, defenders manipulate the adversary’s OODA loop, disrupt the attack cycle, and gain a significant advantage.

During my nearly four decades in enterprise security, I’ve experienced numerous times the incredible power of using deception to protect organizational resources. The primary success factors for deception include proper means for deployment, realism of visible interfaces, and smoothness of integration with the network environment. When these attributes are covered, the results for a security team can be awesome.

- ED AMOROSO, CEO OF TAG CYBER
DECEPTION’S ROLE IN IT ASSET AND DIGITAL RISK MANAGEMENT

Organizations are modernizing their approach to information security. This requires them to move beyond IT risk management and shift towards digital risk management. It is no longer enough merely to protect a particular asset, server, or endpoint. It is about enabling new services for a competitive advantage, cost reduction, and overall reduction in business risk.

As a result, digital risk management models are evolving to address new attack surfaces, limitations in built-in device security, and business models that grant deeper access to insiders, suppliers, and contractors.

Deception technology plays a critical role in an organization’s ability to adapt to these changes by providing ongoing reliability assessments of both security tools and processes. Specifically, deception aligns to how a company can manage their risk tolerance levels, assessment, architectures, and systems.

Deception technology provides metrics for accountability and acting on or assessing achievement of a business’s risk management program. The ability to deliver fast and accurate notifications of malicious activity, policy violations, and misconfigurations allows organizations to venture into new, interconnected, on-demand business models while securing their networks and mitigating risk.

NIST FIVE FUNCTIONS

IDENTIFY
Develop organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. OS, Application, Data Deceptions

PROTECT
Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services.

DETECT
Develop and implement appropriate activities to identify cybersecurity events.

RESPOND
Develop and implement appropriate activities to take action regarding a detected cybersecurity event.

RECOVER
Develop and implement appropriate activities to maintain plans for resilience and restore capabilities or services impaired by a cybersecurity event.
Several factors influence how organizations choose to integrate deception technologies into their operational environments, including their views on IT risk management, strategic risk management, and compliance framework alignment. These can include legal and regulatory compliance, technology changes, and stakeholder, consumer, and competitive pressures. Any solution or strategy must have the necessary metrics to measure success and areas of improvement. When deception is incorporated into one’s risk reduction strategy, it can aid in measuring the reliability of security controls and in reporting on deviations to program risk models. This can be valuable in reporting to the board or management on program efficacy and resiliency.

Mapping deception to the MITRE ATT&CK adversary model and framework can be used to further characterize and describe post-compromise adversary behavior. It both expands the knowledge of network defenders and assists in prioritizing network defense by detailing the tactics, techniques, and procedures (TTPs) cyber threats use to gain access and execute their objectives while operating inside a network.

Baseline security maturity frameworks like NIST\(^2\) and ISO\(^3\) as well as industry-specific models such as PCI-DSS or HIPAA can also be useful in setting baselines for operating practices. Each framework varies in its approach but all are useful in defining how an organization is to behave, implement, integrate, manage, report, and generally measure adherence to the controls being identified.

For example, the NIST Cybersecurity Framework organizes its core material into five Functions, shown below. Deception technology plays a role in over 30 framework subcategories and has a direct and measurable impact in improving an organization’s security posture. In June 2019, NIST issued draft security guidelines that formally include deploying deception technology.

Regardless of the framework you choose, by adding deception as a security control, businesses can mature their overall security posture in ways that can be used for implementing new services, reducing risk, and gaining competitive advantage.
Deception data is more visually usable than data from other tools that we have used for detection. The interface is nice since it drills down and provides the information you need. SIEMs pull in so much that it is overwhelming and takes time. Deception alerting shows that there is clear and immediate need to respond.

- CISO FROM A HEALTHCARE PROVIDER
DECEPTION AND HIGH-FIDELITY ALERTS

Deception virtually eliminates false positives and can have a material impact on increasing a responder’s ability to address a compromise with confidence. Any touch of deception provides an engagement-based alert that is substantiated with attack details, which makes the alert actionable. Whether it be from reconnaissance, credential theft, or engagement with deception lures, even the lightest touch will generate an alert. Since the deception environment has no production value, any interaction will notify the security team of malicious activities or policy violations. In a time where alert fatigue is extreme and staff is limited, these detection alerts cut through the noise so that teams can focus on the most critical alerts instead of chasing false positives.
DECEPTION FOR INTELLIGENCE GATHERING AND FORENSICS

A high-interaction deception environment provides what a low-interaction honeypot cannot: contextual information. The decoys in an interactive deception environment capture and record attacker activity that defenders can analyze. The information becomes forensic evidence the security analyst can process to create tactical and strategic intelligence. Once this intelligence is collected, it can be used internally to strengthen defenses, support administrative action, and share with other industry organizations or law enforcement as necessary.

The deception environment provides a fully functioning synthetic network for capturing forensics. Security teams can safely study attacks without artificial time limits or fear of attackers breaking out or pivoting to attack other systems.

Threat intelligence enables security teams to recognize an attacker’s actions. Indicators of compromise (IOCs) describe specific conditions that may signal the presence of a threat actor, along with relevant contextual information. A deception fabric provides for direct capture of IOC-related forensic artifacts such as packet captures, dropped files, disk changes, and memory contents for analysts to use in developing IOCs that can be shared with others.

Adversary intelligence in the form of tactics, techniques, and procedures (TTPs). Adversary intelligence describes threat actor behavior with TTPs that describe and characterize the “how” and “what” of an adversary (what they are doing and how they are doing it). Analysts extract TTPs from observing specific IOCs within specific alerts to develop contextual understanding across incidents, campaigns, and threat actors. Deception forensic evidence contributes to developing TTPs by capturing the metadata and details surrounding the recorded IOCs in a session and timeline format that an analyst can replay. This gives context that an analyst can use to develop TTPs.

Counterintelligence (CI) covers activities designed to prevent or thwart intelligence gathering, sabotage, or spying by an attacker. Unlike IOCs and TTPs, CI provides information and actions that are taken to identify and protect against an adversary’s intelligence collection activities, operations, or attempts to cause harm through malicious actions within an organization.

Deception is an implementation of CI and the only security technology that provides an in-network CI function. The defender is actively deceiving adversaries and feeding them fake information to defeat their intelligence gathering and manipulate their situational awareness. Security teams also collect intelligence based on the IOCs and TTPs the deception environment captures through attacker engagement with a decoy. This CI information indicates what the attackers are after, and the methods they are using to target their objectives.
Taken together, all of this information aids in developing tactical intelligence for security teams to use in finding and responding to the attacker inside the network. It also helps develop strategic intelligence to gain an understanding of how adversaries may be attacking them, what they could target, and who they may be. In turn, the defenders can use this deeper understanding to adjust their security policies and procedures, improve their defensive posture, and preempt subsequent attacks. As needed, they can share the intelligence with law enforcement and with other organizations to elevate security across their industry.

“Before we had Attivo, we would be spending 4-6 hours dealing with one event, but now with Attivo it’s about 5-10 minutes for us to understand what is going on.”

– DIRECTOR OF CYBERSECURITY
AT A LARGE UNIVERSITY
DECEPTION FOR ACCELERATING INCIDENT RESPONSE

Deception provides support in identifying the extent of a breach and the efficacy of existing security controls. Knowing that an attacker has bypassed the perimeter is a useful first step but gaining visibility into what other systems may be affected, lateral movement paths, and what methods attackers used to bypass defenses provides benefit beyond the immediate alert.

In addition to providing actionable alerts backed by forensics, high-interaction decoys gather information for the defender for post-incident analysis. Any data about the methods or tools attackers leveraged to bypass security on a network decoy aids the analyst in identifying how a security control failed and to mitigate the risk of a returning adversary. The captured data also provides IOCs for the analyst to use in finding other potential victims the attacker may have compromised.

For example, during an attack, the attacker drops an unknown binary onto a decoy that contacts a previously unknown C2 server through an encrypted channel to download a malicious payload. This set of actions provides the security team with information that can be used during and after the incident response process. The security team can add the C2 Internet IP address to the firewall and external

EXAMPLES OF INTEGRATIONS FOR FULLY AUTOMATED RESPONSE

CONTAIN/NETWORK BLOCKING
Check Point, Cisco, Fortinet, Juniper Networks, Palo Alto Networks, Symantec Blue Coat

CONTAIN/ENDPOINT QUARANTINE
Aruba, Carbon Black, Cisco, CounterTack, CrowdStrike, Forescout, McAfee, Tanium

INVESTIGATION/ANALYSIS & HUNTING
Carbon Black, Forescout, IBM QRadar, LogRhythm, McAfee, Micro Focus, ReversingLabs, Splunk, Tanium, ThreatConnect, VirusTotal, Webroot

ORCHESTRATION
Demisto, IBM Resiliency, Splunk Phantom, Swimlane

 TICKETING
Jira and ServiceNow
DNS blocks to increase defenses. This prevents the malware from communicating out and discovers other potential C2 servers IP addresses through malware connection attempts.

Additionally, through native integrations and APIs, response actions can be automated. This often starts by augmenting detection with known threat intelligence, which can include malware identification and domain reputation information. Examples of solutions that integrate with deception platforms include McAfee DXL, ThreatConnect, ReversingLabs, VirusTotal, and Webroot.

In addition to expediting attack analysis and correlation, integrations are available for automated incident response actions such as blocking, isolation, and threat hunting. Advanced deception solutions will offer native integrations with most major firewall, NAC, SIEM, endpoint, and orchestration offerings. Some go as far as automating with ticketing systems to expedite remediation. In particular, the deflection function and Active Directory obfuscation combined with an EDR solution essentially locks down the endpoint, preventing the attacker from moving laterally while remaining undetected.

Companies such as Attivo Networks have expanded beyond simple automation and also offer extensive native integrations and incident response playbooks. These accelerate response, either automatically based on policy or with user intervention. For example, data can be sent to a range of tools to automate forensics, reporting, incident response, isolation at the endpoint, or blocking on the network – and it can handle it in any combination.
Incident response analysts can identify other potential victims by searching the SIEM for systems that had communicated with the C2 IP address or by matching the SHA1 hash of the malicious payload to find infected endpoints. Responders can then expand the scope of their remediation efforts to include these systems. The security team can subsequently check if they have found and remediated all potential victims. The information captured by the deception platform is added intelligence for defenders to use and share as needed to elevate the security posture across multiple organizations.
DECEPTION FOR IDENTIFICATION AND PREVENTION

Other useful deception functionality includes being able to identify and prevent attacks. A deception platform is designed to learn the network so that deceptions can be automatically prepared and deployed. Within this process, the tool gathers information on exposed or orphaned credentials as well as misconfigurations. It will also pick up network changes and show when devices come on and off the network.

This visibility is extremely effective for reducing the attack surface and is not typically achievable with other security tools. Either in the form of tables or topographical maps, defenders can visualize the paths an attacker would take and shut them down before the attacker can exploit them. In some cases, the deception platform can also automate the remediation in addition to passing the information to ticketing systems.

With deception’s ability to hide priority AD objects at the endpoint and present deception in their place, the technology diverts attackers away from critical assets, countering attacks that target AD from gaining accurate information. Additionally, the ability to deflect port and service scans at every endpoint reduces the likelihood that the attacker can move from the initially infected system without touching a decoy. Not only does this prevent attackers from expanding their foothold into the production environment, but also allows for detection earlier in the attack cycle.

During a recent security audit, Attivo detected the auditors on 3 different occasions where they had hit our decoys and spent a total of 8 hours over the course of a week. I had to finally tell them to stop wasting their time. Between this and the success we had detecting activity during a recent pen test, my leadership sees that we are more secure, and are receiving a great return from our investment in Attivo’s solutions.

– ATTIVO CUSTOMER
DECEPTION FOR RED/PURPLE TEAM AND PENETRATION TESTING

Deception is a powerful tool for Blue teams during ongoing security control assessments and when coinciding with a Red Team, Purple Team, or Penetration Test. Deception empowers the Blue team in these Red/Purple team or pen test exercises by detecting when the Red Team or pen tester successfully engages with the deception environment. With the visibility and forensic evidence that the deception platform provides, the Blue team can identify which security controls the attackers bypassed and how they succeeded. Given deception’s ability to validate the resiliency of networks, defenders should not overlook this benefit.
DECEPTION USE CASES

Each organization is unique and faces specific business challenges. However, even with their differences, most organizations find they have multiple concerns in common with industry peers as well as with other organizations across both the public and private sector.

DECEPTION FOR RISK MITIGATION AND COMPLIANCE

- Reduces Risk: Early In-network Threat Detection
- Ongoing Assessment of Security Control Reliability
- Attack Forensics for Root Cause Analysis
- Analysis, Reporting, & Tracking of Cyber Incidents
- Incident Response, Containment, Eradication
- Return Adversary Mitigation
- Asset and Credential Vulnerability Visibility

“...The most important thing you do is provide me alerts based on confirmed activity... you are my eyes and ears on the inside of my network... the nerve center.”

– SENIOR DIRECTOR OF INFORMATION SECURITY AT A TOP 50 RETAIL ORGANIZATION
EARLY IN-NETWORK DETECTION

Threat actors operating within a compromised network are difficult to detect by conventional means. In the NUIX 2018 Black Report\(^4\), two-thirds of attackers indicated that they can breach the perimeter within 10 hours. Attackers are finding innovative ways to bypass traditional detection systems, which are not designed to detect activities such as credential-based attacks. Novel architectures like cloud, IoT, and Internet-connected OT networks also present new attack surfaces to exploit.

Deploying a deception fabric across the network creates a virtual minefield designed to misdirect attacker efforts by detecting early reconnaissance activities, quickly identifying in-network threats, and derailing them with decoys at all levels. This tricks attackers into making mistakes, shrinks their window of opportunity, and slows them down as they are forced to restart their activities.

\(^4\) https://www.nuix.com/black-report/black-report-2018
LATERAL MOVEMENT

Most commonly known as lateral movement, attackers operate “under the radar” as they move to their next system. Identifying attacks that have evaded intrusion detection systems and use “low and slow” movement has proven a consistent concern for many organizations, as indicated by lengthy global dwell times.

The Carbon Black April 2019 Global Incident Response Threat Report noted that 70% of attacks now involve lateral movement. Many organizations are shifting to an “assumed breach” posture, acknowledging that attackers may already be inside the network. Identifying such activity early as they try to move laterally is critical for detecting the compromise but also for preventing an opportunity to create backdoors for an easy return.

CrowdStrike, in its 2019 Global Threat Report, focused on “breakout time,” defined as the window between when an intruder compromises a system and when they move laterally to other systems on the network. The average breakout time is just over 4.5 hours, dropping to less than 20 minutes for highly sophisticated criminal actors. Security teams have minimal time to detect attackers on the initially compromised system before they jump to their next target. Tools that rely on behavioral analysis or pattern matching are not as effective for this level of detection, and as such should not be relied on for finding early lateral movement.

Deception efficiently detects lateral movement through a combination of endpoint deceptive assets, Active Directory deception functions, port scan deflection, and network decoys to obfuscate attack paths and confuse the attacker. Attempts to leverage stolen credentials or query AD lead the attacker into the deceptive environment while conventional as they interact with mirror-match decoy network or port/service scanning activity is detected or deflected systems that are intermingled with production assets.

In the deception environment, attackers unknowingly engage with a decoy, triggering an alert to the defenders. If attackers assume or know that there is deception on the network, they are forced to invest more time in the attack, sacrificing speed and expending additional resources while attempting to avoid detection. With decoys that are indistinguishable from production systems, the attackers won’t know if the next system they move to is real. They are driven to investigate and in doing so make mistakes that spoil their attempts at stealth.

A deception platform efficiently discovers lateral attack paths between systems, revealing misconfigurations and stored credentials that attackers leverage to move deeper into the network. This highlights where security teams should deploy additional deceptive credentials or network decoys, or pre-emptively remove valid stored credentials and remediate misconfigurations before a compromise happens.

Advanced platforms provide the additional benefit of letting the attack play out in the synthetic deception network. This can be invaluable in gaining insight into how the attacker is attempting lateral movement and what techniques and tools they employ.
STOLEN CREDENTIALS

Attackers target user credentials, especially those for privileged accounts, as they seek to compromise a system, escalate their privileges, and extend their reach inside the network, moving closer to their intended target. They also frequently use in-network MITM attacks to collect credentials in transit and query Active Directory for critical accounts. Attackers using these tactics are difficult to detect. Even with UEBA or IAM, an attacker behaving within parameters that appear appropriate, whether external or an insider, does not trigger an alert.

A deception platform generates deceptive credentials for an attacker to steal, seeding them onto all production assets. These deceptive credentials look real and are stored with legitimate credentials but point to a decoy network service. They lead attackers into the deception environment, where defenders can safely record their activities. If threat actors attempt to use deception credentials on other systems, integrations with SIEMs or Active Directory immediately flag the attempt for investigation.

MITM activities can be extremely difficult to detect as they are passive and specific to the virtual local area network (VLAN) they are on. Deception platform decoys provide visibility to threats within the VLANs they are part of. Since they are local to the activity, decoys can quickly detect MITM attacks. Additionally, by generating requests and sending traffic containing deceptive credentials, deception solutions can detect the activity and insert deceptive credentials into the traffic the attacker is collecting.

Active Directory queries fall under the radar as the production environment allows any member system to access the data within as part of normal operations. Attackers that query AD can extract high-value account information to escalate privileges and gain domain access. AD deception can hide these critical accounts while presenting decoy information to attackers regardless of the tool they use.

Collectively, these credential theft detection mechanisms preemptively alert on threat activity at initial compromise and during lateral movement. When combined with a deception application deployment, organizations also can detect the misuse of legitimate credentials when an adversary attempts to use them to log into a decoy environment.
INSIDER AND SUPPLY CHAIN THREATS

Malicious insiders pose a challenge for many organizations. They are difficult to detect and substantiate because they have legitimate access to the environment. These attackers include individual employees, contractors, outside vendors with access to the organization’s systems, and third-party suppliers with access that use their existing authentication infrastructure.

Given the complexity involved in directly targeting an organization with a more mature security posture, attackers instead target small entities that are part of a larger organization’s supply chain as entry points, leveraging the third-party relationship as an attack vector. These attack chains could go several layers deep, with an attacker compromising a seemingly unrelated target and then advancing through the supply chain to their eventual goal.

Deception technology gives defenders a way to disguise the attack surface even to legitimate users. The strategies they employ to combat stolen credentials also apply to insider threats. Additionally, with decoy servers, mapped shares, data, and documents, the deception solution can detect specific “unauthorized access” events, alerting the security team to suspicious insider activity. This seemingly valuable data entices an insider into engaging with the deceptive assets, whether it is a fake development environment, a deceptive preproduction staging area, or a decoy database.

A deception solution arms the security team with the insight required to protect their critical data by detecting and misdirecting insider activity. The solution also provides substantiated proof of policy violation or malicious activity so that organizations can take decisive human resource, administrative, or legal action.

Often the debate is whether to disclose that deception is being used to employees or to conceal the deployment so that additional information on intent can be gathered.

“Deception Technology ranked highest in efficacy for detecting Insider Threats when compared against twelve other security controls”

- EMA, A Definitive Guide to Deception Technology

Insiders have approved access to the network and often know where critical data resides. Because they are authorized users, security teams lack ready visibility into policy violations or malicious actions on systems these users legitimately access. Further, insiders often steal credentials belonging to other users to cover their tracks, making investigations difficult and time-consuming.
Remote datacenters, hybrid cloud deployments, and cloud adoption overall pose a range of new security challenges. Newer technologies, such as serverless applications and containers, introduce additional variables into the security equation. While many conventional security techniques apply to parts of these new deployment models, other aspects call for completely new strategies that address the unique environmental challenges. These strategies must be ubiquitous and scale easily as organizations find themselves supporting a mix of Amazon Web Services, Microsoft Azure, Google, Oracle, and other cloud environments.

As malicious actors develop new techniques to attack these distributed infrastructures, deception technology continues to provide capabilities that other solutions lack. The ability to obfuscate the attack surface is an advantage in datacenters, hybrid cloud, and pure cloud environments alike. Serverless applications present their challenges to conventional security but provide additional opportunities to add layers of deception where an attacker least expects it. Deception technology can provide deceptive applications, mass storage, internal credentials, and serverless applications, among other techniques, that alter the cloud landscape in ways attackers do not expect.
MALWARE AND RANSOMWARE

By encrypting files on individual systems or across network shares, ransomware attacks cause major disruptions, even in cases where organizations can successfully recover their files. The onslaught of new ransomware variants and the availability of ransomware-as-a-service have made it an unrelenting challenge and concern for organizations. The situation is compounded because antivirus efficacy drops against unknown strains of malicious software. Deception, on the other hand, is highly effective at detecting new variants of malware.

An advanced deception implementation goes one step further than early detection. Through a combination of feeding decoy files and metering access to them, the deceptive environment slows the ransomware’s progress dramatically and gives responders time to isolate and remediate the infection. A combination of early detection, automated isolation, and the ability to delay the spread of the infection can mean the difference between losing a single computer or everything on that network segment.

Ransomware isn’t the only malware concern that continues to plague business environments. Resource theft is an ongoing challenge, and cryptomining has led to new families of malware that compromise systems to use their computing power to “mine” for cryptocurrencies. While most cryptomining attacks are not directly destructive, they steal compute, network, and power resources that inflict indirect damage and could be used for other nefarious means.

Deception technology provides early detection of ransomware and other malware that tries to leverage shared filesystems by placing hidden, deceptive shares on endpoint systems. Ransomware and malware rarely discriminate and often aggressively access any available files on any available shares, which quickly reveals their presence when they engage a decoy share.

With cryptomining or related malware, the decoy systems automatically identify the activity and gather forensic data so that incident response teams can efficiently remediate other impacted systems. Deception’s value to incident responders lies in its efficiency in detecting and slowing malware regardless of the variant or strain and limiting the spread of the infection.
The deception project enables the team to efficiently gain knowledge and visibility of the acquired network while adding a much-needed capability for early threat detection to identify any future attacks. By deploying deception, the team accelerated their ability to establish visibility into the subsidiary network, and helped them gain additional insight into any security gaps that could exist.

They now have real time, highly reliable detection of threats inside the network, and have gained an ability to understand the nature and mechanisms of an attack.

-CISO, MAJOR RETAILER

MERGERS & ACQUISITIONS (M&A)

Combining organizational assets and infrastructure during a merger or acquisition presents unique challenges. It is common for the respective organizations to have different security policies, processes, technologies, and levels of operational maturity. After organizations announce a merger or acquisition, attackers often target the smaller company to get into the consolidated network.

To effectively combat attackers, security teams need visibility into these new environments to rapidly determine when attackers have bypassed existing security controls. Additionally, it is important to complete their due diligence to verify there are no preexisting compromises before merging resources. Deception technology is a useful tool in this case, as it works to lure existing malicious actors out of hiding and provides early alerting on policy violations or when controls are not working reliably.
SPECIALIZED ENVIRONMENTS

The widespread adoption of specialized devices into production and Internet-connected environments has altered the threat landscape. IoT devices, SCADA systems, POS terminals, telecom, and medical devices all present increased security challenges. The use of older or stripped-down operating systems, the lack of built-in security controls, or the inability to run antivirus or malware programs makes many of them a relatively easy entry point. Even specialized devices with limited computing power are still inviting targets to threat actors looking to use them individually as entry points or collectively for a more substantial attack.

For example, gaining access to POS terminals is a lucrative target for skimming credit card information or directly interfering with transactions. Compromising supervisory or patch management servers also presents a malicious actor with a significant opportunity to take over distributed environments that include many devices.

Even the most simplistic IoT devices are useful as a springboard to other systems or as a specialized attack platform. Examples of fish tanks, thermostats, and other simplistic device compromises continually surface as the entry point to greater prizes. Although often hard to find, they cannot be ignored, given the risk they present. Organizations should not assume that they are safe even on an air-gapped network. Today’s supply chain carries risk and could still infect these devices by entering the network with malware preloaded during manufacturing or in transit.

By introducing deception into these specialized environments, defenders quickly identify attackers and divert them from their actual targets. Deception technology creates credential lures and authentic looking decoys for individual devices or their control infrastructure, presenting inviting targets that effectively divert an attack. These deceptions provide organizations with the additional visibility and early detection required to mitigate security risks associated with these specialized devices.

“The deception space is also helpful on “trip wire” type detections to help in the “unknown”. For example, trying to pick up on URGENT11 scanning.”

- Director of Cybersecurity, Major Healthcare Provider
THREAT ACTIVITY VISIBILITY AND IMPROVED INCIDENT RESPONSE

It is an all-too-common practice for organizations to contain and remove attackers upon identification to quickly start remediation and minimize damage. However, there is a measurable benefit in analyzing the attack to identify the targets, tactics, techniques, and procedures the attacker is using against the environment.

With the information gleaned by observing an attacker in action, organizations can seek out and address specific issues in their security posture, policies, and infrastructure. It also gives their incident response team insight to more effectively remediate the incident and mitigate future attacks.

Historically, it was a challenge to gather this data without tipping off the attacker. Deception offers a solution by providing a synthetic environment where defenders can safely study the attacker as they attempt to advance their attack.

By diverting malicious actors into a carefully contained, controlled, and instrumented environment, the incident response team can record the attacker’s activity. They acquire full data on every action the attacker performed during the engagement, along with the information needed to understand the incident across its duration. Once analysts address and remediate the incident, they can study the forensic evidence to gain further insight into the adversary.

In addition to providing an attack analysis environment, an advanced platform can open communications to command-and-control servers if desired by defenders. The platform can then collect additional details to understand the attack better. At any time during the deception engagement, security teams can activate blocking, isolation, and threat hunting activities based on their findings, while still letting the attack play out in the controlled deception environment.
Before deploying any new technology, it is critical to set up the criteria for success, how it is measured, and how anticipated advantages are reported. It is also crucial to understand how to deploy and operationalize the technology. This section explores the available components of deception technology, deployment scenarios, and how to achieve benefits within each one.

Deception solutions play a valuable role in being the first alert tripwire to tell an organization that they have been infiltrated. Lures and decoy landmines are camouflaged amongst the systems and are a trigger point for an event. Critical factors for deception efficacy are attack surface coverage, authenticity, and detection regardless of the attack vector.
SETTING DEPLOYMENT GOALS

Deployment goals center on better detection of attackers with the benefits of improved visibility and faster response. Primary goals typically include detection for:

- **Lateral Movement Across Attack Vectors**
  - Network reconnaissance, stolen credentials

- **Reconnaissance**
  - Enumeration, device exploitation of IoT, app servers, etc.
  - Application vulnerability (for example, SQL injection)
  - Default or simple passwords, brute force attacks
  - Misconfigured systems, network share reconnaissance

- **Advanced Attack Techniques**
  - Man-in-the-Middle, Active Directory recon, kerberoasting
  - Group policy preferences, network traffic capture
  - Malware, WMI exploitation, hard-coded credentials
  - Open ports and services reconnaissance
DECEPTION FABRIC PLATFORM
EXAMPLE: ATTIVO NETWORKS

The Attivo Networks® ThreatDefend™ deception solution provides the broadest deception fabric coverage, and for the purposes of this book, is used to illustrate the scenarios and benefits. Here are the components of the solution:

**Deception management platform.** The BOTsink® server provides the central management for the deception environment, including creating and managing decoy systems, services, endpoint and data deceptions, hosting attack analysis, and other core functions.

**Endpoint deceptions.** The ThreatStrike® service places deceptive credentials, hidden shares that link back to decoy services, and other deceptive assets on the endpoint. The solution also adds port scan deflection and the ADSecure module to obfuscate critical AD information.

**Deception forwarding.** The ThreatDirect® system projects code deception functionality into remote locations or segmented parts of the network.

**Attack surface reduction.** The ThreatPath solution provides visibility into attack paths that an attacker could traverse through misconfigured systems, credential exposure, or misuse.

**Visibility.** The BOTsink server provides visibility to network adds and changes, visual attack replays for analysis, and visual lateral attack path mappings for a predictive defense.

**Playbooks.** The ThreatOps solution provides deception-driven repeatable playbooks for manual or automated response actions through native partner integrations.

**Attack simulation.** The ThreatInject tool simulates attack activity to assess deception deployment efficacy.

**Remote management.** The Attivo Central Manager provides a central platform to manage an entire deception deployment across multiple BOTsink servers and environments through a single pane of glass. This is valuable for organizations or service providers looking to aggregate threat data or provide centralized management of large deployments.

Organizations typically deploy a mixture of these components to provide the coverage and capability they need within their environment based on the results of their risk analysis or compliance framework requirements.

Organizations both large and small tend to have common concerns regarding vulnerability visibility, attack vectors, and ability to respond; the primary difference is scale and complexity. Deception solutions are designed to operate effectively across the diversity of vertical markets and their different environments.

There are very similar and common topologies, technologies, protocols, programs, and philosophies when it comes to operationalizing deception. The main difference is in understanding the environment and developing the right density of deception to align with risk models.
Deception technology can have a wide-ranging and immediate impact in reducing risk, adhering to frameworks, meeting audit requirements, and elevating the maturity of the organization when built into the security fabric and operating models of a company. Deception offerings should be able to protect not only business operations but also cover the heating, lighting, and other non-terrestrial communication systems that everyone relies upon.

The deception provider should be considered a long-term, equitable partner to evolve with. An enterprise evolves, grows, and morphs, and any solution the organization implements must be able to do the same. As organizations move towards the cloud, perimeters fade away, and core workforce activities and data move further away from corporate control, a deception solution must flexibly scale with these changes for ongoing protection and continued adherence to an organization’s risk strategies and frameworks.

**DEPLOYMENT SCENARIOS**

The following sections describe common deployment scenarios and how to address deception within them.

**HEAD OFFICE: CORPORATE HEADQUARTERS**

Most security teams understand how to defend a single site such as a headquarters or corporate office from an attack. When considering deception, the head office is usually where a security team starts. A headquarters deception deployment generally involves using deception in production datacenters and on user VLANs.

The security team deploys network decoys and endpoint lures and breadcrumbs throughout the environment for coverage. They often start by deploying deception around their “crown jewels,” on their critical servers and services, or around sensitive departments such as finance, development, legal, and human resources. Organizations may leverage integrations with existing security infrastructure for blocking and quarantine, and create fake applications, databases, or data. They can create fake servers, desktops, file shares, and database servers.
A typical deployment includes:

- BOTsink deception servers and decoys: Engagement server and decoy management. Easily scalable by simply adding additional servers.
  - Decoys customized to servers and endpoints
  - Network infrastructure decoys, including switching, routing, and VOIP

- ThreatStrike Endpoint deception: Windows, Mac, Linux, or cloud credentials; mapped shares; bait placed on endpoint that breadcrumb to the deception server

- Active Directory integrations: For AD reconnaissance and deception credential verification

- ThreatPath visibility tools: View how an attacker would see and traverse the network to get to their target. Automated remediation of exposed credentials.

- Attivo Central Manager: Centrally manage distributed locations on-premises or in the cloud.
Regional offices present unique challenges for a security team, often lacking the space and infrastructure found at a head office. In this case, the security team can use a deception platform that supports remote deployments from a central office or datacenter. The security team can deploy a VM on the remote office’s local VLANs that forwards traffic to a deception server or decoy at the head office. This server or decoy then responds to the traffic as if it were at the remote office, allowing the security team to scale deployments to these remote sites from a central hub.
A typical deployment includes:

- BOTsink deception servers: Engagement server and ThreatDirect Management. Scales through software licensing
- ThreatDirect forwarders: Forward suspicious remote traffic to a central server for investigation
- ThreatStrike Endpoint deception: Windows, Mac, Linux, or cloud credentials; mapped shares; bait placed on endpoint that breadcrumb to the deception server
- Active Directory integrations: For AD reconnaissance and deception credential verification
- ThreatPath visibility tools: View how an attacker would see and traverse the network to get to a target. Automated remediation of exposed credentials
- Attivo Central Manager: Centrally manage distributed locations on-premises or in the cloud

THE CLOUD

Deploying deception to the cloud presents challenges for solutions that favor an endpoint approach or are limited in the types of deception they can provide. A full-featured deception platform can deploy not only network decoys and deceptive credentials for cloud assets but also native cloud technologies such as containers and serverless computing functions.

With a physical deception server at the head office or a cloud-native server, the security team can deploy native cloud decoy systems and services or decoy forwarder VMs; fake credentials that point to cloud assets, databases, or connectors; deceptive storage buckets; serverless functions; and decoy access keys for the cloud. Using native cloud security solutions such as CloudWatch, the security team receives an alert when attackers use high-value real credentials or deceptive credentials for cloud access.
A typical deployment includes:

- **BOTsink deception servers and decoys**: Engagement server and decoy management. Easily scalable by simply adding on additional deceptions in the virtual private cloud (VPC)

- **VPC Decoys**: Containers, VMs, serverless, servers, Lambda

- **Databases, ElastiCache deceptions**

- **ThreatStrike Endpoint deception**: Cloud credentials, mapped, shares, bait placed on endpoint to breadcrumb to deception server

- **Deception credentials**: IAM access accounts, access keys/tokens, SSH keys, S3 buckets, Lambda functions, DNS entries

- **CloudWatch and CloudTrail integration**: For monitoring

- **ThreatPath visibility tools for EC2**: View how an attacker would see and traverse the network to get to a target. Automated remediation of exposed credentials

- **Attivo Central Manager**: Centrally manage distributed locations on-premises or in the cloud
THE SUPPLY CHAIN: VARS, SUPPLIERS, AND THIRD-PARTIES

Organizations that provide third-party access to contractors, suppliers, or partners have an increased attack surface. Similar exposures occur during M&A activity. Attackers leverage these third-party connections to compromise organizations, whether as an insider with access or as an external threat actor using the third-party as an attack vector.

Security teams that want to defend their supply chains and third-party connections can deploy deceptive servers, credentials, and applications such as a decoy development environment, a deceptive preproduction staging area, or a decoy database to detect suspicious activity.

Security teams can gain visibility into the third-party by deploying deception servers, forwarder VMs, and decoys in the partner network that report to their home office. This is also useful for M&A situations where visibility into the acquired network is needed to validate security controls before and after the acquisition.
A typical deployment includes:

- **BOTsink deception servers and decoys**: Engagement server and decoy management. Easily scalable by placing deception servers and decoys in likely attack paths to detect policy violations or activity from misconfigurations.

- **ThreatStrike Endpoint deception**: Windows, Mac, Linux, or cloud credentials; mapped shares; bait placed on endpoint with breadcrumbs to the deception server.

- **Active Directory integrations**: For AD reconnaissance and deception credential verification.

- **ThreatPath visibility tools**: View how an attacker would see and traverse the network to get to a target based on supplier systems. Automated remediation of exposed credentials.

- **Attivo Central Manager**: Centrally manage distributed locations on-premises or in the cloud. Helpful during the M&A process to see who is attacking and whether controls are working.

---

**WAREHOUSE: DISTRIBUTION CENTER, MANUFACTURING LOCATION, AND MORE**

Organizations that use factories, warehouses, distribution centers, or similar facilities commonly use ICS-SCADA and other OT infrastructure for operational automation. Security teams in this space know that IT and OT should have separate networks and security infrastructure, but they have seen them converge for ease of use and sometimes based on accidental inclusion.

Security teams seeking to deploy deception can use VM forwarders or a full deception server whether virtual, physical, or cloud. They can also deploy SCADA and IoT device decoys such as sensors, human/machine interfaces (HMIs), control panels, or management servers alongside their IT decoys and credentials. A full-featured deception platform provides the flexibility to meet both upstream and downstream operational needs.
A typical deployment includes:

- BOTsink deception servers and decoys: Engagement server and decoy management. Easily scalable to all environments by simply adding on additional servers based on segmentation
  - Decoys customized to look like ICS, IoT, and other OT technologies or supervisory control devices
  - Similar strategies can be applied for retail point-of-sale or medical IoT networks
ADVANCED DECEPTIONS AND DETECTION

Security teams can leverage deception for advanced deployments and cases. Using a full-featured deception platform, they can create an entire deceptive Active Directory or LDAP server with associated decoys as part of the environment. They can also choose to deploy deception routers, switches, and VOIP telecom deception, or application and data deceptions specific to their organization, such as a deceptive SWIFT terminal for a bank, or a deceptive gift card web portal with a fake database backend server.

If the security team operates a device network, such as IoT cameras or multifunction printers, they can deploy deception assets that match those as well. Security teams can also create decoy documents that beacon home when exfiltrated, providing information on what attackers are targeting and where the data is accessed.
A typical deployment includes:

- Network deception with engagement server and decoy management. Easily scalable by adding additional servers
  - Customized decoys running the environment’s golden-image software
  - Customized application servers to appear as attractive targets
  - Network infrastructure decoys including routers, switches, telecommunications, surveillance, and more
  - Database deceptions
  - Decoy documents placed strategically on servers to gather counterintelligence

- Endpoint deception with lures, AD obfuscation, and attack deflection along with the ability to intercept attacks, provide attack path visibility, gather forensics, and insider risk scoring
  - Lures: Credentials, file shares, buckets, and serverless functions

- Detection for AD reconnaissance, kerberoasting, and MITM attacks

- Advanced detections: For group policy preferences, network traffic capture and malware, WMI exploitation, hard-coded credentials

- Phishing email attack analysis automation (through built-in sandbox)

---

**BENEFITS ACROSS DEPLOYMENT MODELS**

Regardless of the deployment model, the solution also captures the data that incident response teams, first responders, and other parties need to understand what happened. Critically, the platform also provides analysis on where it happened, what else is infected, what it deployed, and where it came from. Organizations will also gain insight into what must be done to contain the incident, if it has not already done so automatically.

The fact that a well-architected, deployed, and managed deception solution can detect, contain, and manage an incident is critical to strategic risk management and other frameworks. Therefore, as deceptive solutions are evaluated and requirements strengthened, ask vendors to provide the necessary adherence to risk management and various frameworks through the lens of end-to-end lifecycles of deployment and incident response.
DECEPTION OPERATIONAL AND MANAGEMENT EFFICIENCY

There are many use cases and operational benefits of deception. Unfortunately, perceptions remain that it requires highly skilled staff and is difficult to deploy and manage. This misconception stems from legacy technology such as traditional honeypots, deception solutions that deploy inline, and those that require endpoint agents.

It is also a misconception that deception is only for organizations with a mature security infrastructure. Organizations of all sizes and maturity levels find value in using deception technology for early detection, enhanced internal visibility, and accelerated response. Deception deployment information currently indicates while there are many top Fortune 100 deployments, industry estimates state that about 60% of deception customers are midmarket companies.

A modern deception platform does not add friction to the production network or interfere with the operating environment. These platforms are designed to deploy quickly and easily at scale across the entire organization, without interfering with network traffic or requiring an endpoint agent. Advanced platforms also apply machine-learning techniques to automate the preparation, deployment, and management of the deception environment. This reduces the time necessary to maintain authenticity and manage the solution and simplifies operations so that highly skilled resources are not required. A flexible solution also offers a variety of deployment options that fit into existing endpoint management operating tools.

Advanced solutions provide central management for all deception environments, geographically distributed deployments, or when offered as a managed detection service. The central management simplifies the aggregation of information and can be operated in the cloud or on-premises regardless of where deceptions are deployed.

Operational efficiency is gained through high-fidelity alerts. Notifications come from confirmed engagement with deceptive assets or credentials and deliver the attack analysis information needed to decisively respond to the threat. This virtually eliminates false positives, as the deception environment only triggers upon interaction.

There is no employee production value in a deception asset, so any internal interaction serves as notice of policy violations or something more nefarious. Built-in forensic reporting removes many manual steps in correlating attack information and documenting findings. Given the depth of information provided, responding to threats can be reduced from hours of manual correlation down to minutes to respond and provide previously unknown intelligence on the attacker.

Collectively, ease of management combined with actionable, high-fidelity alerts makes advanced deception solutions simple for organizations of all sizes to operate, without the need for adding incremental resources.
ACTIVE DEFENSE VS. CYBERWARFARE

Deception is based on planned, deliberate, and controlled actions to conceal the networks, create uncertainty and confusion in the adversary’s mind, delay and manipulate his efforts to establish situational awareness, and to influence and misdirect perceptions and decision processes, thereby causing them to take or not take actions that are beneficial to the defender’s security posture.

Active defense goes one step further in applying the learnings from attacks to confidently respond to the immediate incident, mitigate risks from a returning adversary, and build pre-emptive defenses.

Cyberwarfare is “the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.”

Deception in information security gives public and private sector organizations the same defensive advantages the military gains from deception in actual warfare: causing an adversary to make mistakes, wasting the opponent’s time and resources as they pursue false targets, and giving the defense valuable intelligence on their adversary and the data they need to confidently stop an attack. How far each organization employs the functionality available directly correlates with the maturity and sophistication of their security posture.
For some, hacking back may immediately come to mind. That is distinctly different; protecting one’s organization with an active defense does not mean warfare or retaliation. Although hacking back may sound like an appealing idea, it is fraught with issues. First, under The Computer Fraud and Abuse Act (CFAA) Title 18 US Code, subsection 1030, knowingly accessing a computer without authorization, exceeding restricted access, and with intent to obtain confidential information or to cause harm is currently illegal in the US. The Active Cyber Defense Certainty Act (ACDC) bill submitted in 2017 proposed making changes, but to date has not been approved, and even if legalized in the US, would still be subject to international laws that predominantly prohibit this type of activity.

Law and ethics aside, attribution is typically not easy, and most organizations simply don’t have the skills or tools to do this successfully. Hacking back also presents a high risk that could result in unintended consequences. This may stem from attacking the innocent or bringing on heightened attacker retaliation, which organization may find themselves ill-prepared for.

Threat deception is a much better option than retaliation. Instead, organizations can use the rich forensic, threat, and adversary intelligence gathered in a deception environment to take pre-emptive measures to fortify their defenses. By better understanding the attacker, an organization can confuse, slow down, and stop an attacker while gathering information on how they are attacking and what they may be targeting.

In addition to threat and adversary intelligence, the use of decoy document beaconing functionality provides counterintelligence on what an attacker is seeking and geolocation of where the document is accessed, inside and outside the network. This capability can be invaluable in understanding what and whether something is stolen and for protecting research, intellectual property, or case files.
KEY TAKEAWAYS

- Deception should not be thought about as a luxury or considered “the final security initiative” to be deployed once everything else is done
- It is inherently early and accurate detection
- Near zero false positives and automation drive high ROI
- Deception technology requires very little overhead to deploy and manage
- Administrators and architects gain an awareness about vectors and vulnerabilities they may have not had without it
- Effective for external and insider threats

EXECUTIVE SUMMARY

Malicious actors have repeatedly proven that they can bypass conventional defenses even when the organization has a mature, well-executed security strategy. Defense-in-depth helps, as does adhering to recommended or required security standards and frameworks. However attackers are crafty, and no solution is 100% foolproof. Deception technology provides a range of advantages that conventional information security solutions cannot match, inclusive of early and accurate detection and the ability to shift the balance of power from the attacker to the defender through the collection of adversary intelligence.

By deploying decoy systems and services that are camouflaged to blend seamlessly into the environment, and placing breadcrumbs and deceptive assets on the endpoints, deception technology disrupts the attack cycle at multiple points and quickly detects an in-network adversary. An attacker gets an unclear picture of the attack surface which slows them down, forces them to make mistakes, expends additional resources, and alters the economics of their attack.

The evolution of modern deception technology platforms makes deployment and management at scale easy. A broad range of use cases makes deception valuable to organizations of all sizes and industries. Deception is unique in that it serves as a force multiplier to an organization’s existing security solutions while reducing information
security team workloads, giving them visibility into unseen threats, lateral movement, and “low and slow” attack techniques that evade existing defenses.

With deception technology, existing security programs benefit from improved intelligence and automation, while the incident response team receives high-fidelity alerts. Teams become more effective and efficient by focusing on actionable threats rather than consuming valuable resources pursuing false positives or manually attempting to correlate or respond to an attack.

Unlike other security controls, with deception, defenders are no longer relegated to being reactive to an attack and can now establish pre-emptive defenses. This shift in the balance of power between attackers and defenders benefits the organization in multiple ways beyond what conventional security solutions were ever designed to provide. In the ever-changing threat landscape and evolution of attack surfaces, it’s now more important than ever to implement a proactive defense that arms the defender with a powerful offense and the tools and intelligence they need to outmaneuver even the craftiest of adversaries.
ACKNOWLEDGMENTS

Writers: Carolyn Crandall and Joseph Salazar

Project Lead: Christina Adams

Graphic Designer: Grace Chen

Core Contributors:

Tony Cole, Chief Technology Officer, Attivo Networks
Bill Ender, CEO, Right Brain Media
Marshall Heilman, Senior Vice President, Managed Defense and TORE, FireEye
George Insko, Director of Cybersecurity, University of Kentucky
Chris Roberts, Chief Security Strategist, Attivo Networks
Lance Spitzner, Director, SANS Institute
The team at Evolved Media

Additional acknowledgments:

Several security professionals provided their input and guidance in the creation of this book. A special thanks to each individual for their feedback, sharing of real-world experiences, and perspectives that collectively made it possible to bring this book to life.