Implementer's Guide to Deception Technologies

Kyle Dickinson

SANS

A SANS Whitepaper

Implementer's Guide to Deception Technologies

Written by **Kyle Dickinson**
Advisor: **Kevin Fiscus**

January 2020

Sponsored by:

Acalvio Technologies
Attivo Networks
Fidelis Cybersecurity

Deception is a word that has a stigma associated with it, beginning with its very definition—"to mislead by a false appearance or statement."[1] Deception has been used throughout history to gain a strategic advantage. As an example, the First United States Army Group was actually a fiction created during World War II to deceive the enemy about the location of the Allies' invasion in France.[2] Through the use of dummy (often inflatable) tanks, airplanes and ships, combined with fake military radio traffic, photographs, documents, and even public radio and news broadcasts, the Allies were able to persuade Germany to believe that the D-Day invasion would occur north of the actual invasion target. This forced the enemy to spread its defenses across a larger area, effectively weakening them.

While we aren't creating a fake military, we can use deception technologies—or "tricky threat detection capabilities," as we like to call them—to gain a better understanding of security attacks and more effectively protect against them. On today's digital battlefield, organizations essentially deploy decoy lures, misdirections, and systems to attract and snare attackers.

In this paper we focus on how deception technologies can significantly improve an organization's ability to quickly and accurately detect attackers while collecting sufficient threat intelligence and attack attribution information to improve response effectiveness. The detection of threats on the network is the primary purpose and most

[1] www.dictionary.com/browse/deceive

[2] "FUSAG: The Ghost Army – Patton's D-Day Force That Was Only a Threat in the Enemy's Imagination," www.warhistoryonline.com/world-war-ii/fusag-the-ghost-army-pattons-d-day-force-that-was-only-a-threat-xb.html

mature benefit of cyber deception, though many organizations also leverage deception data for gathering company-centric attack information.

Deception Technologies 101

Historically, deception technologies relied on decoys consisting of emulated services and low levels of interaction for the attacker. This meant that deceptive resources would be obvious to a skilled attacker, standing out from the environment. Coverage in early implementations of such technologies was limited in terms of the types of deceptive resources that could be used and the overall attack surface that could be covered. Today things have changed. Deceptive technologies can be implemented as network-accessible resources, on endpoints and even in cloud implementations—with all major attack surfaces covered, including but not limited to websites, servers, workstations, IoT devices, ICS and point-of-sale (POS) devices.

The Problem

Attackers are using techniques known to subvert traditional detections by using deceptive methods themselves. For example, if attackers know or suspect that an organization's IDS is looking for a specific pattern match to issue an alert, they will be sure to modify their attack to avoid that pattern and then proceed to move laterally throughout the organization's environment.

Similarly, other techniques, such as stealing credentials and account information from host systems, can be employed to evade antivirus, firewalls, application whitelisting and many other common security technologies. This is largely because most traditional security technologies focus on trying to look for "evil." Evil, in the case of the previous IDS example, would be the pattern the IDS was configured to look for. As a result, all an attacker needs to do to avoid detection is to appear "not evil." This, in a nutshell, is the problem with traditional detection technologies and the reason deception technologies are an important part of any cybersecurity arsenal.

There are also other approaches for detecting attackers on our networks. Instead of looking for evil, we can look for *abnormal*. If we know what happens on our networks normally, we can identify abnormal behavior and investigate it as suspicious. Unfortunately, normalizing an entire network can be challenging. For example, it may be normal for Bob in Accounting to access his computer between 8:00 a.m. and 6:00 p.m., so any access outside of those times would be suspicious. But what if Bob is on vacation in a different time zone? That abnormal behavior becomes normal based on an understanding of context. A simpler approach is necessary.

By placing resources (e.g., open port, service, server, URL, credential, etc.) on the network that are not intended to be used or accessed by anyone, we define normal as no interaction. If anyone or anything attempts to interact with those resources, that is, by definition, abnormal and, therefore, suspicious.

Deception technologies can take many forms, including the following:

- **Token-based deception—**Uses deceptive files, tokens and similar resources in production systems.
- **Appliance-based deception—**Uses small, relatively inexpensive appliances to act as various types of emulated decoy systems.
- **Enterprise-level deception—**Uses a centralized command and control infrastructure, typically installed with visibility into one or more network trunk ports on the network. These solutions generally support virtual appliances, full OS virtual machine decoys and token-based solutions, and often include the benefits of AI and machine learning.

These technologies are not intended to operate on their own. They work best when leveraging and integrating with existing security solutions as part of a comprehensive security program.

Deception Technologies Can Reduce Risk

Once an attacker is inside the network, deception involves creating deceptive resources or assets that are attractive to an attacker, with the intent of allowing or even encouraging that environment or asset to be attacked. This results in a number of benefits:

- Deception technologies enable security teams to detect attacks more accurately by generating alerts whenever a deceptive resource is touched. The quality of the alert also removes the risk of alerts being lost in the noise and alert fatigue.
- Earlier detection reduces the time an attacker can remain on a network, thereby decreasing the cost of a compromise and remediation.
- Depending on implementation, deception technologies can also enable defenders to collect company-centric information about the attacker's behavior. This threat intelligence allows defenders to respond to the incident more effectively, further decreasing the time required for triage and the impact.

Understanding how the attacker got into the environment is critical because it gives teams the ability to disrupt attacks by creating new controls and alerting the organization based on the intelligence they gathered while observing the attack. In other words, the more we know about the attacker's techniques, tools and procedures, the more effective our defenses, including detective controls, can be.

To assist in protecting an organization's environments, deception technologies enable security teams to:

- Detect and respond more quickly
- Analyze threats
- Prevent attacks

We discuss these topics in more detail in the following sections.

Detect and Respond More Quickly

Perhaps the biggest benefit of deception technologies is attack detection. While no technology is guaranteed to detect every attack, the use of deception makes most attacks significantly easier to identify. The reason is simple. An attacker who manages to compromise an environment typically has little or no knowledge of what that environment looks like and has to learn about it. If deception is done correctly, the fake resources placed throughout the environment look identical to the real resources. By placing a sufficient quantity of deceptive resources throughout the environment, the likelihood that an attacker will interact with at least one of them is significant.

Fortunately, deception does not rely entirely on luck. Security teams can create deceptive resources that attackers find more interesting and with which they are more likely to interact. Creating more interesting resources could involve naming a system something that draws attention, making deceptive systems slightly more vulnerable than production systems, or even planting "breadcrumbs" that point to the deceptive resources. To increase the likelihood of attacker interaction, place deceptive resources where you know attackers are going to focus. For example, an attacker who compromises a PC is extremely likely to attempt to pull credentials from the LSASS process in memory. By placing fake credentials directly into memory, deception planners can use the attackers' methodology against them.

Understanding attacker methodology can be both time-consuming and involved, but there are resources available to help, including Lockheed Martin's Cyber Kill Chain,[3] the Unified Kill Chain[4] and the MITRE ATT&CK Matrix.[5]

Cyber deception provides both specific and measurable benefits not found in most other solutions available today, including achieving a significant reduction in dwell time, low false-positive results, and the capability of interacting with security orchestration, automation and response (SOAR) technologies.[6]

Being faster is not always better. Accuracy is also critically important. Most traditional detection technologies attempted to balance rates of false-positive results with false-negative results. False negatives are a significant problem because attackers remain undetected for a prolonged period. False positives are also a problem in that they represent "noise" that distracts defenders from real incidents. Cyber deception significantly reduces false positives because, under normal circumstances, no interaction with deceptive resources should occur. If an interaction occurs, it should be investigated.

Organizations also need to respond effectively and efficiently. Because deceptive resources can be highly interactive, they can collect significant amounts of intelligence about the threat. Such intelligence is not necessarily a simple notification that "something bad happened." Rather, it can include detailed information about where the attacker came from and what was done. This information makes incident response easier and far more effective. While deception technologies can generate these benefits by themselves, understanding the complete picture is always best. Additionally, the intelligence is specifically relevant to the organization, rather than based on a feed that includes information not applicable to the organization or the industry vertical.

A false positive is when an alert is generated although nothing bad actually occurred. A false negative is when no alert is generated, but something bad did indeed occur.

Deception technologies, in most cases, can integrate with existing security detection solutions such as SIEM and other SOAR technologies. This means that cyber deception does not need to replace any legacy technology, nor does it require any specific legacy technology. Cyber deception can be implemented as the first step in a security program, the last step or any step in between. It can integrate with legacy technology but doesn't require it, giving it amazing flexibility and making it an option for organizations of literally any size.

---

[3] www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html; Cyber Kill Chain is a registered trademark of Lockheed Martin Corp.

[4] www.csacademy.nl/en/csa-theses/february-2018/104-the-unified-kill-chain

[5] https://attack.mitre.org/; MITRE ATT&CK Matrix is a trademark of The MITRE Corp.

[6] "A Definitive Market Guide to Deception Technologies," August 2019, http://info.enterprisemanagement.com/a-definitive-market-guide-to-deception-technology-webinar-ws [Registration required.]

Analyze Threats

Simple detection is a fantastic goal, but relying on it solely relegates many organizations to a "swat the mosquito" approach to security. If a mosquito bites you, you swat it, thereby eliminating it as a threat. Applying this approach to an attacker involves removing the attacker from the environment. Unlike with the mosquito, however, kicking the attacker off the network does not eliminate that attacker as a threat. In fact, the opposite is likely to be the case. By detecting and then removing an attacker, the attacker becomes aware of the detection. Skilled attackers will use this knowledge to change their source IP address and their tactics, giving them an additional advantage.

Cyber deception not only allows for rapid attack detection but also facilitates the collection of threat intelligence. Consider this simple deception tactic: the creation of a listening port with no service or application behind it for the attacker to interact with. The attacker can establish a connection to the listening port but cannot interact with it. While the threat intelligence collected in this case will be minimal, security teams will be able to identify the attacker's IP address. As long as that IP address continues to interact with deceptive resources, it does not pose a threat. But should the attacker begin interacting with valuable production resources, that attacker can be dealt with accordingly. A simple port listener is, however, not the limit of what deceptive resources are capable of.

As the level of interaction increases, the ability for the attacker to "play" with the resources also goes up. Higher interaction gives the attacker a more realistic experience and also provides significantly more opportunities for defenders to analyze attacker activity.

When discussing deception, the term *honeypot* frequently comes up. Honeypot technology serves as the foundation of deception. When discussing honeypots, terms like *high*, *medium* and *low interaction* are common. The level of interaction describes how detailed and realistic the honeypot appears to an attacker. The following list includes examples.

- **Low interaction—**A simple port listener would be considered extremely low interaction because, after establishing the connection, the attacker cannot do anything else.
- **Medium interaction—**An emulated service where attacker communications are analyzed and simulated responses designed to replicate a real service are returned would be slightly higher on the interaction scale.
- **Higher interaction—**This can involve the use of real, but deceptive services, fully operational hosts or even complete deceptive networks.

As the level of interaction increases, the ability for the attacker to "play" with the resources also goes up. Higher interaction gives the attacker a more realistic experience and also provides significantly more opportunities for defenders to analyze attacker activity. Not only does a better understanding of attacker activity allow security teams to respond more effectively, but it also enhances their ability to design improved deception scenarios.

Prevent Attacks

Deception is all too often portrayed as a reactionary technology, but it can be used to prevent attacks and even reduce the risk that a production system will be compromised. All else being equal, if an organization has 50 production systems and 50 deceptive systems on its network, an attacker is 50% likely to interact with a deceptive resource first. The inclusion of breadcrumbs and other deceptive mechanisms at the endpoints increases the density of the deception and the odds of the attacker interacting with the deception environment. This extends to matters like fake credentials or fake network directory services (such as Active Directory) or altering AD query results to include deceptive information that leads to decoys. If security teams deploy deceptive breadcrumbs on endpoints, then the ratio of attackers interacting with the decoys increases significantly, depending on how many decoy breadcrumbs are deployed compared to production credentials cached on the endpoint. If security teams detect and respond quickly, they could prevent a breach of production systems. As mentioned previously, making deceptive resources more attractive to attackers increases the probability of an attacker interacting with them.

Organizations don't need to wait for attackers to execute an exploit or to gain a foothold on their networks for deception to be effective. Deception can be implemented in public-facing IP addresses or even pushed further out of the network. Deception planners can leverage fake social networking accounts to talk about fake projects supported by fake technology to plant ideas in the minds of the attackers. This practice can help to deter attacks (by creating the impression of a stronger security posture) or direct attacker behavior (by informing attackers where the good stuff is before they get on the network).

When implemented, one goal of a cyber deception program is not to be detected by attackers. Once deception is detected, attackers have a few options: keep on attacking, leave or change tactics. If the attacker simply ignores the deception, the defender can respond as appropriate. If the attacker simply stops the attack assuming the target is too well-protected, defenders win. In most cases, even if the attacker changes tactics based on knowledge of the deception, the new tactics will be much slower and more cautious. This means the attacker will take more time to compromise the network and the defenders gain an advantage.

Understanding Attacker Activities and Leveraging Deception Technologies to Combat Them

Attackers develop new techniques and tools on a daily basis. With new technologies being used, it's essential that security analysts have the ability to extend their "tricky threat detection" practices beyond traditional network attacks to modern applications, such as containers, and cloud service providers (CSPs) to address a variety of attacker activities. Simply understanding attacker techniques, however, does not stop attacks, prevent breaches or reduce harm. That knowledge must be put to use. By designing deception plans around expected attacker activity, deception planners can increase the likelihood that a deceptive "trap" will be triggered, shift the focus of an attacker toward deceptive resources and away from production, or even stop the attack in its tracks.

Although each organization is unique, it is important to know that similarities in technological and security programs across different organizations tend to be far more significant than their differences. Even if the differences are significant, the attacker remains the common variable. Attackers behave in fairly consistent ways, and by understanding them, both security teams and the plans they implement can be more effective.

By designing deception plans around expected attacker activity, deception planners can increase the likelihood that a deceptive "trap" will be triggered, shift the focus of an attacker toward deceptive resources and away from production, or even stop the attack in its tracks.

One of the biggest advantages of cyber deception is the fact that while knowledge of attacker techniques is beneficial, it is not required. Unlike many traditional detection methods, deception does not look for signatures of attacks or attempt to pattern match; thus there are many deception concepts and benefits that don't directly address individual techniques but rather provide broad benefits. By placing deceptive resources (files, URLs, credentials, shares, ports, services, hosts, etc.) throughout the network, any interaction by any attacker generates an alert. This can help detect not only known attacks but also zero-day threats that would otherwise avoid detection by more signature-based solutions.

Network Asset Discovery

Prior to attempting a compromise, attackers will attempt to learn something about the target environment using approaches such as ping sweeps, port scans, sniffing network traffic and even vulnerability scanning. The attacker's goal is to find targets and identify likely means to attack those targets. By creating deceptive ports, services, systems or even full networks, defenders create an environment where, when attackers start scanning the network, they will, in all likelihood, interact with one of these fake resources and generate an alert. This gives responders an early warning combined with threat intelligence that allows them to triage the incident more effectively.

Active Directory Reconnaissance

Attackers are continually interacting with Active Directory (AD) because it's one of the most common IT control systems in use. Being able to interrogate AD can allow attackers to identify hosts and users and to understand group membership and permissions. Because AD is so tightly integrated with authentication and access control, attackers can use an understanding of AD to affect direct compromise by stealing credentials (e.g., password cracking, pass-the-hash, etc.). By placing deceptive users, groups and computers in AD, deception planners provide additional opportunities to detect and distract attackers.

Account and Credential Hijacking

This type of attack occurs when an attacker steals an account associated with a service or a computing device to obtain security credentials such as usernames/passwords, tokens and access keys. Attackers with access to target systems can extract credential hashes from the hard drive (e.g., Security Account Manager [SAM] database, **`ntds.dit`**, **`passwd/shadow`** files) or directly out of memory. To attackers, credentials are "gold," enabling them to leverage legitimate credentials when moving through a network instead of attempting exploits, making them less likely to be detected and more likely that their attack will work. By placing fake credentials in memory, in the **`passwd/shadow`** files, in the SAM database and other locations, the deception planner creates additional traps for attackers. If those deceptive credentials are slightly easier to crack, or if those credentials are accidentally sent or stored in the clear, they serve as high-value targets for attackers. Once the attacker attempts to use those credentials, an alert is generated.

With account hijacking, security teams have multiple ways to leverage deception technology. One that comes to mind—because it's a rising issue—is access keys to a CSP environment. These keys may be accidentally pushed to source code repositories or found in plain text files on a workstation. An attacker gaining access to these keys gains access to the environment. Using this knowledge, a security team can place CSP keys in locations attackers are likely to discover. When fake keys are used, the team knows there is a problem. If different keys are placed in different locations, the use of a specific key also provides defenders with an understanding of the attacker's location on the network. With full OS decoys, the organization can stand up a fake code repository that will detect any misuse or unauthorized access, as well as create credentials and other access tokens that lead to the decoy server's gaining awareness of attackers stealing credentials to target the code repository.

Phishing

According to the 2018 Internet Crime Report,[7] phishing and related attacks are the fifth most common form of attack. In a phishing scam, the attacker sends an email that appears to be legitimate to a target to persuade that target to provide sensitive or confidential information, such as passwords, banking information and ATM card details. In the case of phishing, attackers are generally indiscriminate when it comes to targets. Any and all users are viable targets because—once attackers manage to compromise a single host on most networks—they can use other techniques to move throughout the network.

Phishing is one of the greatest threat vectors organizations face. Cyber deception can help combat that threat. Creating decoy mailboxes to incite an attacker or implementing a fictitious direct phishing campaign can provide organizations with insight as to how an attacker is attempting to solicit information from various types of audiences. Security teams can create and closely monitor mailboxes for indications of attempted phishing. A simple deception approach would be to create a few unused email accounts and monitor those accounts for activity. Complexity can be added depending on the goal of the deception. For example, the existence of the fake email accounts can be publicized by placing the email addresses on obscure or even unlinked pages on websites. Email addresses that are similar to those used by important personnel can be used to identify attacks targeted against those users. Fake social networking accounts can be created that leverage the fake email accounts to create a more realistic picture for potential attackers.

By creating fake email accounts, deception planners create early warning systems for phishing attacks. If an email account is truly fake, it should never receive an email. Any email received by these fake accounts should be investigated. Deception planners can simply create fake email in the hope that an attacker will stumble across it, or they can place references to those email addresses in places likely to be discovered by attackers. As soon as a phishing email hits one of the fake addresses, an alert is generated, and incident handlers can begin their work.

Containerized Applications/Functions-as-a-Service

Container and serverless technologies have been rapidly gaining popularity. Using containerized applications or serverless technologies allows businesses to modularize their applications for reliability and scalability—and match running resources to the demand that the application is experiencing. Like other technologies, containerized applications are subject to attack. For example, attackers have abused container orchestration platforms to load malicious containers for cryptocurrency mining operations.[8] As organizations begin to create new applications that leverage containers,

[7] 2018 Internet Crime Report, https://pdf.ic3.gov/2018_IC3Report.pdf

[8] "Tesla cloud resources are hacked to run cryptocurrency mining malware," https://arstechnica.com/information-technology/2018/02/tesla-cloud-resources-are-hacked-to-run-cryptocurrency-mining-malware/

or functions-as-a-service, attackers look to adapt their methodologies to include these new technologies. It's important that security detections can aid in defending them.

A decoy can be set up in a cloud environment to detect attacks that target them. Deception platforms can also create decoy serverless functions to extend the deception capabilities further.

Vulnerable Applications and Libraries

Here, the attacker takes advantage of a legitimate business application, or a library that an application leverages to run, that has an unintended bug in the code. These bugs can cause different attacks to succeed, depending on the vulnerability. These honeypots come in virtually any technology format desired. It is possible to create a honeypot that looks like a Linux server running SSH, but it is also possible to create deceptive web servers, IoT, ICS/SCADA systems and many others.

Consider the situation of a hospital that uses network-connected medical devices. Hackers regularly attempt to compromise medical devices in an attempt to steal medical records. These devices often use older technology, which frequently consists of "closed" systems that cannot be easily modified to ensure U.S. Food and Drug Administration (FDA) compliance. As embedded computing devices, it is also difficult to determine that a compromise has occurred, as long as it continues to function properly. Placing deceptive medical devices on a hospital network can provide an effective early warning system for detecting attacks or attempts to tamper with these devices. This same paradigm applies in industrial settings, power generation plants and anywhere embedded computing devices are used.

When implementing cyber deception, creating intentionally vulnerable systems is a way not only to detect attackers and help defenders understand how attackers exploit the vulnerabilities, but also to distract them from production systems and delay them until an effective response can be implemented.

Ransomware

Ransomware is a topic we see on the news—at what seems to be at a common rate of occurrence. The issue with ransomware is its effectiveness. Those that are attacked often pay the ransom to get their data back.

With ransomware, attackers use malware or another mechanism to hold the victim's data hostage. In most cases, once attackers gain access to the target system, they use asymmetric encryption to encrypt all files not critical to the functioning of the operating system. In the past, ransomware affected individual computers. Today, ransomware often slowly and quietly compromises an environment, infects every system, and deletes or corrupts backups prior to demanding the ransom. Because ransomware generally involves encrypting or otherwise altering files of various types, deception planners can create an early warning system by placing files of various types on systems throughout the environment and then regularly checking the integrity of these files. Because these files should never be accessed, they should also never be changed. Any change would generate an alert, which could mean the difference between a minimal ransomware outbreak and a significant breach.

Deception technologies can aid in early detection of a ransomware attack by placing "bait files," similar to honey tokens, throughout the network. If security analysts detect that one of these files is being altered on the endpoint, they can look to isolate the host that may have been the entry vector for the ransomware attack or at a minimum, identify a list of compromised systems.

With ransomware attacks, the trick is limiting the "blast radius" to reduce the effectiveness of attack. This is achieved primarily via early detection. In many cases, ransomware is spread via a worm or similar malware. Even if implemented manually by an attacker, time is of the essence to avert widespread infection. If defenders can detect ransomware infection early, they can take steps to stop its spread and in doing so, reduce the amount of harm.

Implementing Deception Technologies

Organizations have multiple ways to incorporate these types of detection methods into their security programs. Both open source and commercial alternatives are available. Whether to use open source or commercial solutions is a significant decision that will have long-term consequences, so it is important to understand the advantages and disadvantages of each.

Before making such a decision, it is critical that organizations fully understand their goals and objectives when it comes to cyber deception:

- Are you looking specifically to detect compromise earlier and more effectively?
- Are you looking to collect threat intelligence?
- Are you looking to collect evidence about the attackers?
- Does the organization possess the resources for operationalizing open source tools?

Deception technologies can aid in early detection of a ransomware attack by placing "bait files," similar to honey tokens, throughout the network.

It is also important to assess the prevalence and effectiveness of existing security controls and technologies. Deception can integrate with and/or leverage existing security controls. Not only can deception technologies report to centralized detection solutions (e.g., SIEM), they can also benefit from the use of other protective and detective technologies such as firewalls or endpoint detection and response (EDR) controls, because such controls reduce the attacker's freedom of movement. When integrating with existing or legacy technology, commercial solutions may be more desirable because they are built to support such integration, whereas open source or other free solutions will likely require more effort to integrate.

With an understanding of deception goals and how deception technologies could integrate with existing security controls, security analysts should evaluate the various deception methods. Some questions to consider include:

- Given identified goals, will a token-based, appliance-based or enterprise-class solution work best?
- How many deceptive resources do you want to place throughout the network?
- Do you want to use "bare-metal" hosts or virtualization?
- When considering virtualization, do you want to use full virtualization or a containerized solution?
- Do you want to build everything or buy?

The answers to these questions will be based on available budget and personnel.

Organizations vary in the amount of resources and the skill sets they have available to dedicate to any given effort. There are also considerations in terms of flexibility and customization. These differences are important in deciding whether to pursue open source or commercial options.

With open source tools, organizations have the capability to leverage a wide variety of projects, mold them to their specific use cases and requirements, and/or to craft the tools they need. This, however, comes with both cost and risk. With commercial tools, there may be a lack of complete flexibility and limitations in terms of customization. Both approaches have advantages and disadvantages, as described in Table 1.

By understanding their specific deception goals, budgets, technical capabilities and constraints, security integration requirements, and the advantages and disadvantages of different solutions, organizations can make the best possible decisions.

Table 1. Advantages and Disadvantages of Open Source and Commercial Deception Technologies

Category of Solution	Advantages	Disadvantages
Open Source Tools	Lower startup costs Ability to deploy extremely small, focused, targeted solutions Flexibility and customization Ability to leverage operational budget	Hidden initial and ongoing operational costs associated with learning, deploying and managing the solution Lack of dedicated customer support systems No SLAs Potential for open source projects to be discontinued Difficulty in migrating to a commercial solution, if desired
Commercial Tools	Comprehensive solution for all networked environments Well-developed documentation and customer service Defined SLAs Ease of configuration and deployment Automation through built-in third-party integrations Ability to leverage capital and/or operating expense (OPEX) budget	Higher startup costs Some lack of flexibility Not cost-effective for extremely small environments

Summary

It is often stated that "defenders need to be right 100% of the time while attackers only need to be right once." Although this statement isn't technically true, it does articulate the problem defenders face. Mistakes rarely hurt attackers, but they can cripple defenders. It's time to turn that paradigm on its head. All it takes for defenders to take back the advantage is for the attacker to touch one deceptive resource. With deception, the attackers now need to be right 100% of the time to avoid detection, while the defenders must be right only once. Deception technologies give organizations the capability of creating better detection capabilities at every "layer," as well as giving them better insight into attacks that are being executed in their environment—all while limiting the damage the attacker can do.

To be truly effective, deception is not something you can simply throw on your network in an afternoon. Particularly with commercial solutions, the technology is fairly simple, but it must be implemented with a designed intent. For this to happen, organizations must:

- Understand their goals and objectives when it comes to deception
- Understand their current technological infrastructure
- Understand attacker techniques, tactics and methods
- Design their deception solution by incorporating the identified goals, technology and attacker tactics
- Implement and test the solution
- Review and update the solution on a regular basis to address new considerations, constraints, goals and tactics

It should also be noted that cyber deception is largely a detection method. Detecting attacks without the ability to respond effectively provides little real value. Thus the development of a robust, documented incident-handling process should be considered mandatory when deploying cyber deception, if such a process does not already exist.

Computer security has been an issue that organizations have needed to address for decades. Unfortunately, while defenders have gotten significantly better at defense, attackers have outpaced their developments and continue to have an advantage. To reverse that trend, security programs must go beyond traditional detection solutions such as IDS/IPS, SIEM, antivirus and log monitoring that identify "evil," and must instead identify and react to "abnormal" activity. Fortunately, the task of normalizing network activity can be simplified by creating "fake" resources on our network that serve no other business function and thus should never be interacted with. As a result, any interaction with these resources is considered abnormal and should be investigated. This is the core of cyber deception, and this is what will allow defenders moving forward to take back the advantage.

About the Authoring Team

Kyle Dickinson teaches SANS SEC545: Cloud Security Architecture and Operations and has contributed to the creation of other SANS courses. He is a cloud security architect for one of the largest privately held companies in the United States. As a strategic consultant in his organization, Kyle partners with businesses in various industries to better understand security and risks associated with cloud services. He has held many roles in IT, ranging from systems administration to network engineering and from endpoint architecture to incident response and forensic analysis. Kyle enjoys sharing information from his experiences of successes and failures.

Kevin Fiscus (advisor), a principal instructor for the SANS Institute, regularly teaches SANS SEC504: Hacker Tools, Techniques, Exploits and Incident Handling and SEC560: Network Penetration Testing and Ethical Hacking and is the author of an upcoming class on cyber deception. Kevin has founded two consultancies through which he conducts security and risk assessments, compliance gap analysis, penetration testing, security policy development, security program design, and security roadmap development, including planning and implementing cyber deception as part of a larger security program, for client organizations. Kevin currently holds multiple SANS certifications, including the prestigious GIAC Security Expert, and was named a SANS Cyber Guardian for both red and blue teams.

Sponsors

SANS would like to thank this paper's sponsors:

ACALVIO

Attivo NETWORKS

Fidelis Cybersecurity

Last Updated: February 14th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Cairo February 2020	Cairo, EG	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS Brussels February 2020	Brussels, BE	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS Scottsdale 2020	Scottsdale, AZUS	Feb 17, 2020 - Feb 22, 2020	Live Event
SANS San Diego 2020	San Diego, CAUS	Feb 17, 2020 - Feb 22, 2020	Live Event
Open-Source Intelligence Summit & Training 2020	Alexandria, VAUS	Feb 18, 2020 - Feb 24, 2020	Live Event
SANS Training at RSA Conference 2020	San Francisco, CAUS	Feb 23, 2020 - Feb 24, 2020	Live Event
SANS Zurich February 2020	Zurich, CH	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Secure India 2020	Bangalore, IN	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Manchester February 2020	Manchester, GB	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Jacksonville 2020	Jacksonville, FLUS	Feb 24, 2020 - Feb 29, 2020	Live Event
ICS Security Summit & Training 2020	Orlando, FLUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Secure Japan 2020	Tokyo, JP	Mar 02, 2020 - Mar 14, 2020	Live Event
Blue Team Summit & Training 2020	Louisville, KYUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Northern VA - Reston Spring 2020	Reston, VAUS	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Munich March 2020	Munich, DE	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Jeddah March 2020	Jeddah, SA	Mar 07, 2020 - Mar 12, 2020	Live Event
SANS St. Louis 2020	St. Louis, MOUS	Mar 08, 2020 - Mar 13, 2020	Live Event
SANS Paris March 2020	Paris, FR	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Prague March 2020	Prague, CZ	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Dallas 2020	Dallas, TXUS	Mar 09, 2020 - Mar 14, 2020	Live Event
Wild West Hackin Fest 2020	San Diego, CAUS	Mar 10, 2020 - Mar 11, 2020	Live Event
SANS Doha March 2020	Doha, QA	Mar 14, 2020 - Mar 19, 2020	Live Event
SANS San Francisco Spring 2020	San Francisco, CAUS	Mar 16, 2020 - Mar 27, 2020	Live Event
SANS Norfolk 2020	Norfolk, VAUS	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS SEC504 Nantes March 2020 (in French)	Nantes, FR	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS London March 2020	London, GB	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS Secure Singapore 2020	Singapore, SG	Mar 16, 2020 - Mar 28, 2020	Live Event
SANS Kuwait March 2020	Salmiya, KW	Mar 21, 2020 - Mar 26, 2020	Live Event
SANS Seattle Spring 2020	Seattle, WAUS	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS SEC560 Lyon March 2020 (In French)	Lyon, FR	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Oslo March 2020	Oslo, NO	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Madrid March 2020	Madrid, ES	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Dubai February 2020	OnlineAE	Feb 15, 2020 - Feb 20, 2020	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced