Attivo NETWORKS®

CYBER DECEPTION: HOW TO BUILD A PROGRAM

BY GEOFF HANCOCK

INTRODUCTION

With traditional cybersecurity, companies play a cat-and-mouse game to identify, block, and prevent threats. A deception program changes this by giving defenders the ability to learn about attackers in the same way attackers try to learn about their targets. Once an organization knows an attacker is in the network, it can observe the attacker's behaviors and patterns. This background helps security teams better understand what attackers are after and the best way to respond.

Today's cyber defenders are at a disadvantage. Some tools and methods like whitelisting IP addresses are intended to help them be somewhat proactive. But by and large, today's cyber operations have been designed to respond only after attacks take place. This gives adversaries a significantly asymmetric advantage: They can probe systems, and then prepare and launch attacks within a short period, leaving little opportunity for defenders to defeat them.

A critical change in approach is needed. Cyber deception is an emerging proactive cyber defense methodology that, when done well, can put the defender in the driver's seat. It enables defenders to lead the attacker and gather intelligence on the adversary's tools, methods, and behaviors. In this way, defenders have the upper hand in cyber operations.

Military Deception

Activities intended to deter hostile actions, increase the success of friendly defensive actions, or to improve the success of any potential friendly offensive action.

Cyber Deception

Planned, deliberate, and controlled actions to conceal the network, 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.

3,000 YEARS OF DECEPTION

Deception in warfare is probably as old as armed conflict itself. The logic of confusing an adversary is obvious, and the rewards can be realized very quickly.

According to myth, in the 12th century B.C. the Greeks sent a present to Priam, the king of Troy. Little did the king realize he was about to become well known for letting his guard down and giving his enemy the upper hand. This story has echoed over the past 3,200 years as an example of the first recorded example of deception in battle, and according to the myth, was quite successful.

During Operation Desert Storm in 1991, the U.S. Central Command planned a two-pronged approach to penetrating Iraq. First, coalition forces dropped 12,000 leaflets to warn Iraqis of imminent attacks from the sea. To support this deception, the U.S.

Navy maneuvered in waters just off the Kuwait shoreline, conducting reconnaissance operations while the U.S. Marines practiced invasion drills. Second, the U.S. Army moved troops up to the Kuwait border and broadcast radio signals, indicating the presence of several large army divisions. The ruse fooled the Iraqi army into focusing on Kuwait. Meanwhile, coalition forces swept across the Saudi desert to the west, struck deep into Iraq, and severed all lines of communication, thereby cutting off the Iraqi army.

This deception caused ambiguity and confusion in the eyes of the Iraqi leadership. It influenced them to allocate resources in areas the coalition forces wanted them to focus on. It also caused them to reveal strategies, objectives, and intentions.

CYBER DECEPTION VALUE

The value of having a cyber deception plan is twofold:

1. PLANNING OF THE CAMPAIGN: It reveals the defender's security posture, risks, and business functions likely to be attacked. Properly planning, designing, and implementing a deception campaign can help you identify previously unknown and potentially vulnerable assets along with the paths an attacker could utilize to move through your environment. You need to understand your organization and how your business units use your network and how data flows around it. This will give you a complete view of your network's strengths and weaknesses and identify the areas where the adversary will most likely try to gain access.

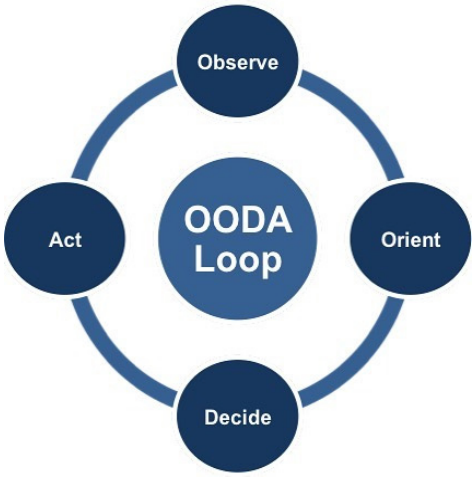
2. DIRECT ACTION: It leads the attacker through the network, revealing motives, techniques, and intentions. By using deceptive techniques, a defender can mislead and confuse attackers, thus enhancing the defensive capabilities over time. The ability to deceive, direct, and guide the adversary away from critical assets, denies him his goals and reveals how he wants to move through your networks. It also holds the benefit of increasing the attacker's cost as they must now decipher what is real from the fake and often must restart their attacks.

Many security controls and technologies create a boundary around computer systems and try to stop any illicit access attempts. Because of the low cost on the adversaries' side, the existence of many automated exploitation tools, and the known defensive technologies and controls, the attackers can continuously conduct reconnaissance on computers until they find a vulnerability to infiltrate undetected. System defenders typically learn nothing about the intruders' targets during this process. Ironically, the quest to instantly deflect an attack also makes the task of defending a computer system harder after every unsuccessful attack.

> "Rouse him and learn the principle of his activity or inactivity. Force him to reveal himself, to find out his vulnerable spots." — Sun Tzu, The Art of War

THE DEFENDER'S EDGE

A critical advantage of deception-based defenses is that they give defenders an edge. They can actively feed adversaries deceptive information that affects the "observe" and "orient" stages of a technique called the OODA loop.



The OODA loop (Observe, Orient, Decide, and Act) is a cyclic process model proposed by John Boyd. It describes how an entity reacts to an event. Winning requires executing this loop faster than the adversary.

The edge is that by using the OODA loop, the defender slows the adversary's process, gives defenders more time to decide and act, and gives a clearer understanding of how the adversary is moving and reacting to your deception. In cyber deception, the use of the OODA loop is crucial to tracking and identifying the adversary's behavior.

TODAY'S BATTLEFIELD

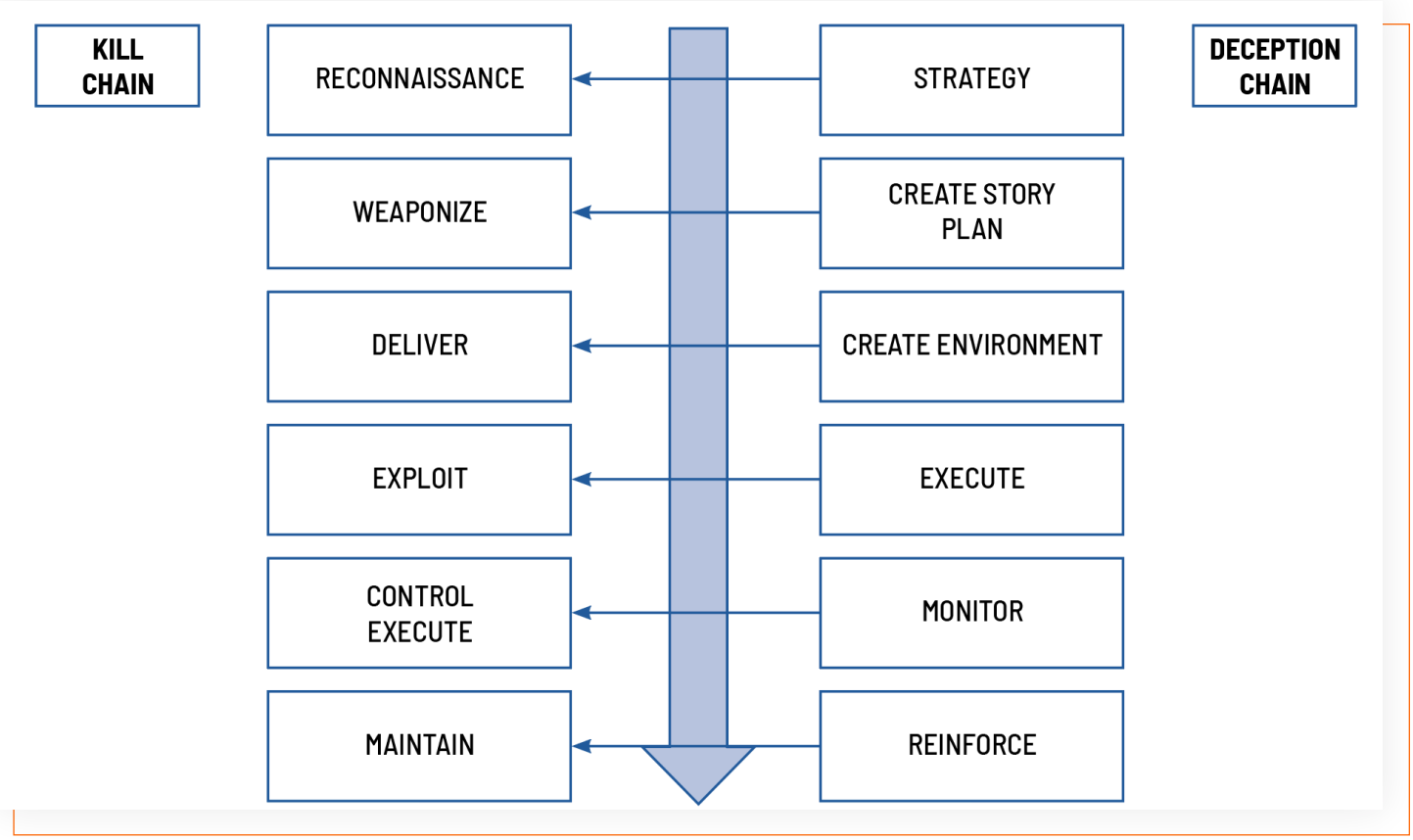
For the past 30 years cybersecurity has been about keeping the bad guys out in a very direct manner. The cyber industry has grown through the creation of such terms such IDS, IPS, firewalls, encryption, anti-virus, Security Information & Event Management (SIEM), cyber threat intelligence, cloud security, Security Automation & Orchestration, and hundreds of other terms. All of these still deliver value and help keep attackers out to some degree. However, with the speed of business and technology growth, cyber defenders are increasingly reacting to changes in their network instead of looking for proactive measures.

> With deception-based security, defenders can focus on the actions or anticipated actions of the adversary. This proactive approach combined with traditional measures can give defenders a greater, more complete and holistic way to manage their networks.

CYBER DECEPTION CHAIN VS. THE KILL CHAIN

The Cyber Kill Chain is a well-known process that attackers go through to penetrate a target network. The Cyber Deception Chain was created to identify and map the stages and procedures needed to implement cyber deception successfully.

The chart on the following page displays how defenders can use the deception chain to disrupt and deny the cyber kill chain.



DECEPTION CHAIN

Applying deception to specific areas of the cyber kill chain can give the defenders an advantage. Being able to control every step of the kill chain process not only protects the network, but it also provides a level of intelligence that the defender can use to be more proactive in defending it.

Applying cyber deception to the kill chain can produce the following results:

RECONAISSANCE: Deception plays a critical role in the early detection of attackers conducting reconnaissance on the network to find their target assets or credentials required to conduct their attack. When defenders identify adversarial reconnaissance, credential harvesting, or lateral movement efforts, they unearth a set of behavior patterns and a digital fingerprint that helps track defensive targeting efforts. These can quickly identify bad actions and provide guidance on how the adversary traverses the network.

WEAPONIZE: Influencing the adversary's conclusions that the organization's vulnerabilities, defense posture, or capabilities are weak helps defend against a weaponized payload. Deception methodology and tools can be used to mislead the attacker's view of the network, thereby influencing what technology he uses to conduct the attack. Additionally, once a payload is released within the deception network, defenders can identify its capabilities and direct its impact.

EXPLOIT: Recognizing exploitation attempts, defenders may redirect the adversary to a deceptive environment, which appears to be part of a network that contains important data, but is isolated and monitored by defenders. The goal is to conceal all deception "tells" or indicators to delay the adversary while providing the defender with powerful insight into the attacker's tactics, techniques, and procedures.

CONTROL: As the adversary is accessing the deception network, provide him a deceptive asset with a variety of information to identify his motives, intentions, and capability maturity. The application of DecoyDocs can also be useful in understanding the types of information the attacker is seeking and the geolocation of where these documents are being accessed.

EXECUTE: Slow the adversary down to collect cyber intelligence, data that you can use to direct his steps, and learn how the tools are used.

MAINTAIN: Keep up the appearance of realism by adding or retiring false information, as well as maintaining existing data and ancillary files, email, password change history, login history, and browser history. Deception and response platforms can also be applied as a preventative tool. The intelligence gathered to learn the network for the deployment of deceptions along with visual maps of attack replays can be applied to understand better when new vulnerable devices are being added, primarily exposed credential and lateral movement attack paths. This knowledge can be collectively applied to address risk and fortify new and current defenses.

CONSIDERATIONS FOR A CYBER DECEPTION PROGRAM

Before starting a deception campaign, defenders must consider several questions:

- Who are my likely adversaries?
- What do my adversaries know about me and what do I know about them?
- Where are my vulnerabilities?
- Does the adversary have the capacity to exploit my vulnerabilities?
- Why would an adversary pick out my organization specifically?
- How could I be manipulated by the adversary?
- What do I have in place to validate the efficacy of my current security controls or compliance with my risk profile across insiders, suppliers, and external adversaries?

Once those questions are answered, moving into the campaign plan is much easier. The first two parts of your plan are the Objectives and Planning portions. These fall under your cyber deception strategy.

OBJECTIVES

- Cause adversary to take action that gives you the advantage.
- Immobilize action, so the adversary wastes time and resources.
- Cause adversary to reveal strengths and intentions.
- Cause adversary to reveal weaknesses and methods.
- Direct the adversary to a particular pattern of behavior.
- Create a reconnaissance process within your network so you can monitor and learn how an adversary will move across it.

PLANNING

- Deception goal. What do you expect to get out of this campaign?
- Desired action. Specify how you want the adversary to act.
- Identify the adversary's bias. The adversary bases every attack on assumptions about your network. Knowing their bias will give your plan more value.
- Determine how deception impacts or adds value to your IT and digital risk management strategies. Deception can inform incident response, information sharing, preventative defense, compliance, and insider and supplier management programs.

In planning a deception program, defenders could map out how adversaries could get into the network and target critical data. Identifying critical assets may be a good place to create a deception program. By approaching it this way, it becomes apparent how the company uses and stores data and if there are higher risk devices that create an increased risk profile. This can also uncover gaps in business processes and can be used for identification of policy violations or gaps. It can also identify new data security risks, such as "Why does Logistics have access to the Accounting system?" or "Why does Sales hold so much IP data?" and it may uncover new ways to provide better services while reducing IT investment costs.

CYBER DECEPTION OPERATIONS

In the Operational component of the program, defenders need to tie together the business structure, processes and information, and all of the underlying technical components that both support the business and manage or introduce risks. Since deception success is based on believability and attack surface coverage, the defender must also build the deceptions to mirror-match the production environment and ensure attractiveness to the adversary. This combination helps create the deception story. Having the most realistic and authentic story not only helps convince the attacker but educates the defender on how better to design the corporate network and how data is protected.

PREPARING

- Build the story. This will require technical data about the defender's network, vulnerabilities, attacks surfaces, and the tools and methods the attacker will use to break in. Good deception platforms can identify all of this data and recommend an implementation strategy.
- Understanding the flow of business data or operations is important as well. Creating a believable story involves mapping and understanding how the business works with other companies and networks in the supply chain, recognizing how employees use and access data, understanding business risks and security posture data, and comprehending the adversary's methods.

From a technical perspective, a deception program can help manage and track all IT assets and how partners and vendors manage unique risks. Additionally, it can help with reducing the cost and increasing the efficiency of the technical architecture; streamline how data flows across the networks; and assist with threat modeling, incident response, and reduce of overall IT risk.

IMPLEMENTATION, MONITORING, MEASURING

As you employ your deception mechanisms (concealment, camouflage, false and planted information, lies, displays, ruses, demonstrations, etc.), the deception network needs to reflect active network data, user interaction and network presence as the live network- authenticity is key. Monitoring in-network threats early and measuring the deception network is where the minute-by-minute interaction takes place. Before implementation, the team needs to be clear how each step of the deception is tracked and integrated into existing processes and policies.

- Believability. It's critical to attracting an attacker and deceptions need to look exactly like a normal part of your network. Design and structure the deceptive network to appear identical to the real network. The decoy's profile needs to reflect the actual business and technical environment for the deception to work. It will require creating a duplicate system with all the same IT and business processes, as well as trigger alerts that substantiate the attack and track and record the data created during an attempted attack.
- Monitor and Measure. Having clear and concise ways to evaluate the effectiveness of your security controls and deception campaigns is crucial. Staff will be able to test the reliability of existing security controls and the accuracy of the story with early detection. Simulation tools can also demonstrate security resiliency. Having the metrics to know what and how to monitor is essential for justifying the resources and identifying just how many attacks are attempted against your organization to build an overall stronger defense.

A deception program is not a stand-alone silver bullet for protecting your organization; in fact, there is no silver bullet. It does, however, represent a new direction of protection. It goes beyond just stopping the attacker. It puts you, the defender, in charge of the action, instead of making you wait for something to happen. When done well, it can impact how the business is run in significant ways, including impact to risk profiles and validation of compliance to set standards.

Companies today use an area-defensive strategy, where the predominant tactics utilized are to block and remediate issues. For this approach to be effective, defenders need to wait for an attack to take place. Deception adds a new strategy to cyber operations. An adversary that penetrates the perimeter is now faced with the dilemma of not knowing what is real from fake, causing confusion, slowing the attack, increasing their costs, and in many cases creating economics that force them to choose an easier target.

With the use of deception programs and tools, defenders can now learn from each attack and update the playing field again to ensure the advantage stays with the home team and is taken away from the attacker.

CONCLUSION

The idea of an organization being secure, based on a rigid perimeter defense, has proven time and time again as simply inadequate, especially as the growth of technology across organizations increases, so does the attack surface.

Deception-based cyber defenses are powerful tools, shown to be effective at imposing cost, increasing dwell time, and otherwise distracting the adversary to allow the defender to gain the upper hand. These mechanisms give defenders the ability to learn more about their attackers, reduce indirect information leakages in their systems, and provide defenders with the advantage.

As organizations continue to face off against attackers and cyber conflict continues to become the new norm, if attackers fully understand and expect the reactive controls, tactics, and responses of defenders, while defenders remain mired in a reactive-only posture, we should not expect to see a tide change in the balance of capabilities between attackers and defenders.

If however, defenders can take a more proactive posture in their security strategies and engage with attackers in unexpected and unpredictable ways, the balance can begin to swing back in favor of the defender. How far it swings is up to the ingenuity of today's and tomorrow's security teams.

> "Organization leaders should make every effort to shorten the time from compromise to detection. Deception and misdirection technology is the only capability at market to single-handedly enable large enterprises to shorten the gap to hours or even minutes, protecting sensitive customer and organizational data." - DoD Official

ABOUT ATTIVO NETWORKS

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