Attivo NETWORKS®

Checklist for Evaluating Deception Platforms

With over 700 reported breaches occurring annually, a modern day adaptive security defense requires a combination of prevention, detection, response, and prediction technologies. Even the most state of the art prevention solutions have shown time and again, that they cannot keep every attacker out. Having an early detection system for attacks that have bypassed prevention systems and tools that can predict attacker lateral movement are critical in the line of defense for preventing the exfiltration of data, Personally Identifiable Information (PII/PFI/PHI), and/or potential harm to critical infrastructure or a company's brand reputation.

This paper will provide an overview of what deception technology is and how it provides an efficient and effective solution for detecting in-network threats in real-time. A useful checklist is also included, which can be used by organizations to understand the elements of a comprehensive deception platform and how to evaluate both the breadth and depth of deception offerings.

What is deception technology?

Deception technology is designed as a network "motion sensor" that will alert organizations, in real-time, of threat actors that have bypassed cyber security prevention solutions and have made their way to the inside of the network. Deception systems will turn the network into a ubiquitous trap through the usage of deception techniques that are designed to confuse, deceive, and delay attackers by incorporating ambiguity and misdirecting a cyber attacker's operations. This provides an early alert system and the much needed time and visibility to thwart the attack and remediate infected systems.

What does deception technology do?

Deception platforms are based on high interaction engagement servers working in conjunction with decoys and deception lures to deceive, detect, and analyze attacks. Forensic attack analysis can also be used to automate manual processes with integrations that will provide automated blocking of attackers and quarantine of infected devices.

Deception platforms are designed to detect and analyze all threat vectors including reconnaissance, stolen credential, ransomware, man-in-the-middle, and phishing. Unlike a honeypot (an early stage form of deception), which was designed to be a low interaction honeypot for detecting automated scanning tools and worms, deception is designed to detect inside-the-network threats and the lateral movement by human attackers. Deception, by design, is not reliant on signatures or known attack patterns, making it extremely effective for gaining real-time visibility into attacks. Zero-day, stolen credential, and insider threat actors are known to slip by traditional detection methods. With advanced deception platforms the attacker cannot distinguish the deception servers from production assets and deception bait from real credentials and user information, which is then used to cleverly deceive attackers into revealing themselves.

Comprehensive solutions will be able to detect threats in user networks, data centers, cloud, industrial control system (ICS- SCADA), and Internet of Things (IoT) environments. These platforms will turn the entire network into a trap and once the attacker is engaged, the platform will also safely analyze attacks to attain the forensic data required to quarantine an infected device and update prevention systems to block against current and future attacks. Integrations with other detection systems can also strengthen an organization's defense by working together to detect the use of deception credentials and to augment attack information to provide continuous threat management and improve incident response.

Additionally, deception end-point credential information can be used for predictive assessment of attack threat path vulnerabilities and misconfigurations. Organizations can use the deception platform for "continuous" end-point penetration testing to help identify risks associated with credential exposure, open SMB shares, privileged credentials on non-designated computers in addition to software misconfigurations.

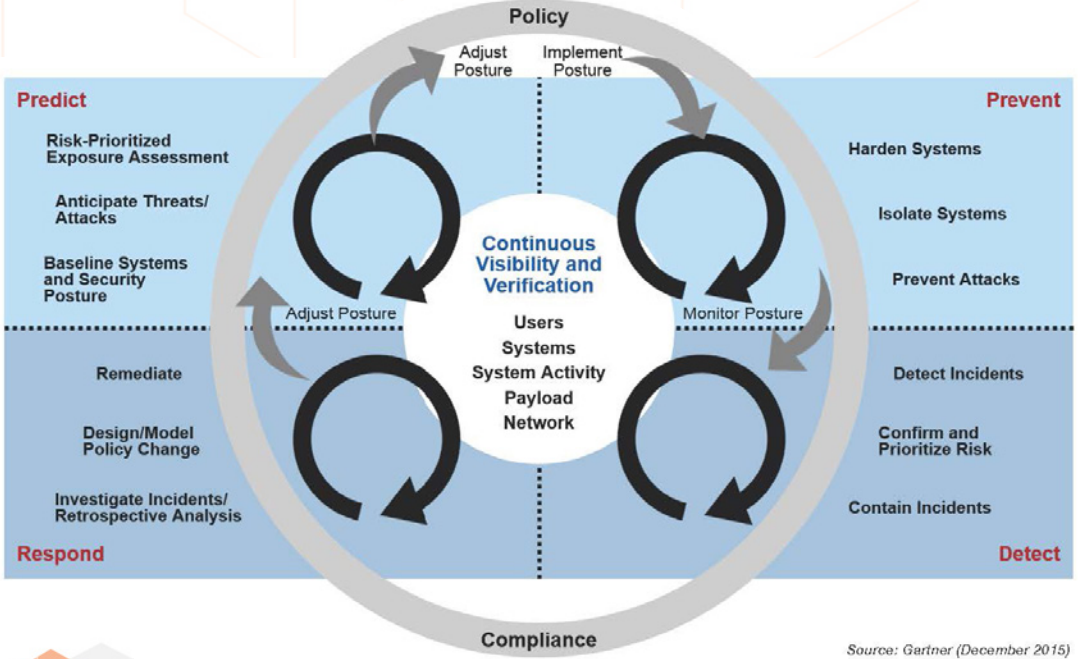
Who uses deception technology?

Organizations across all industries that are concerned with protecting their most critical assets (company data and intellectual property (IP), PII, critical infrastructure, etc.) have started adopting deception as a core element of their adaptive security infrastructure and defense. With the number of breaches that occur on a daily basis, today's secure posture requires an "assumed breached" approach that includes a mix of prevention and detection solutions.

Deception is rapidly being adopted by Fortune and midsize organizations across financial, healthcare, high-tech, retail, entertainment, energy, government, and many other verticals as organizations seek an efficient solution for inside-the-network threat visibility and early detection to augment to their prevention infrastructure.

Why is deception technology important?

Prevention alone has proven unreliable and has allowed attackers on average over 6 months of dwell time before being detected. The reality is that a traditional security posture can't be effective with 12 new attack strains being produced per minute, two out of three attacks come from stolen credentials, 43 percent of data loss coming from insider and 3rd party threat actors, and with the expectation that security operations center (SOC) teams can keep up with an average of 14 alerts per hour .


Policy
Adjust Posture
Implement Posture
Predict
Risk-Prioritized Exposure Assessment
Anticipate Threats/ Attacks
Baseline Systems and Security Posture
Prevent
Harden Systems
Isolate Systems
Prevent Attacks
Continuous Visibility and Verification
Users
Systems
System Activity
Payload
Network
Adjust Posture
Monitor Posture
Remediate
Design/Model Policy Change
Investigate Incidents/ Retrospective Analysis
Respond
Detect Incidents
Confirm and Prioritize Risk
Contain Incidents
Detect
Compliance

Source: Gartner (December 2015)

Organizations are realizing now more than ever that inside-the-network threat detection is a must for early detection and that deception offers the most efficient and cost effective way to quickly detect all types of cyber threats. Paul Proctor, Gartner Analyst, has published a paper titled "Shift Cybersecurity Investment to Detection and Response," which serves as a good reference to why detection is needed in addition to prevention solutions.

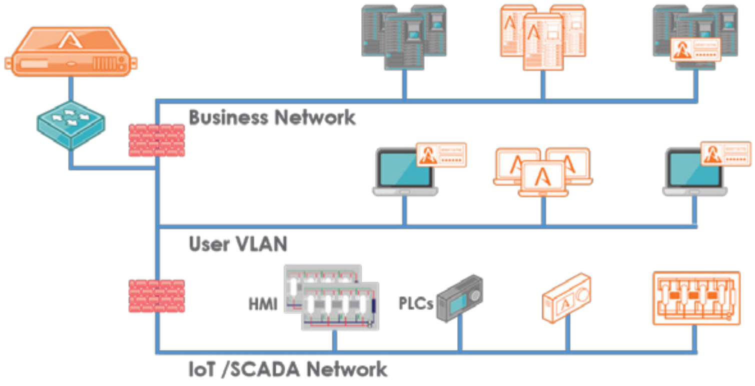
The Gartner model for an Adaptive Defense is also a helpful overview on how these systems can work together for the best cyber security defense. In addition to compatibility, deception providers are going one step further and will also provide automations and integrations to provide continuous threat management and accelerate incident response based on the attack data gathered by its engagement servers and through its forensic analysis process.

How does deception technology work?

It is important to understand that deception is not another layer of prevention. It is also different than Intrusion Detection Systems (IDS/IPS) and big data monitoring, which although they are methods for detecting attacks, are challenged by reliability. Additionally, IDS/IPS are tethered to their need for highly skilled resources to tune the systems, analyze the data, and to manage the number of false alerts that are often generated as a result of pattern matching and anomaly detection techniques.

Deception takes an entirely different approach to cyber defense. Deception is designed to detect what prevention systems have missed and to give organizations real-time visibility to know what is lurking in their network. Deception is inherently efficient since it does not need to be in-line and uses deception vs. monitoring signatures or attack patterns to detect a threat actor. Deployment is friction-less and an "out of the box" configuration can be installed in under 30 minutes. Operational management is extremely efficient with high-fidelity alerts that are substantiated with detailed attack forensics based on actual engagement. Alerts can be viewed in a threat intelligence dashboard, easily reported on or can be set up to integrate with prevention systems to automatically block attacks and quarantine infected devices. Given the simplicity of management and the no false positive design of alerts, additional or highly skilled resources are not typically required to operate a deception platform. Installation wizards and templates will also simplify installation and deployment and ongoing management can be done with platforms such as Microsoft Active Directory, ForeScout, or Casper.

It is important to note that not all deception platforms are alike and there is a wide variance in breadth and depth of solutions. Many providers only have partial solutions such as an engagement server or endpoint deceptions. Moreover, the solutions may not work in a data center, cloud environment, Industrial Control (ICS), or Internet of Things (IoT) environment. Authenticity is critical for a deceptive environment to be successful. The greatest levels of deception are achieved by using real operating systems and come with the ability to customize the services or use a golden image of the production assets. Some vendors will only provide an emulated environment or won't have the ability to appear active with features like the ability to broadcast traffic. It is highly recommended to do your research and understand how complete a vendor's offering is and the depth of deceptions provided.



Here is a checklist for how to evaluate the elements of a comprehensive deception platform, including the criteria, which can be used for your evaluation.

What environments are supported?

- Will the solution support user networks?
- Can the solution scale to operate in a data center?
- Will you need cloud security? AWS, Azure, OpenStack, VMware
- Is GRE /routed network support required?
- Are there ROBO that could benefit from advanced detection without the need for an onsite engagement server?
- Do you need detection for Industrial Control System or IoT environments?
- What system types are needed: Microsoft, Linux, Mac?

How effective is the detection solution for the following threat vectors?

- Reconnaissance
- Stolen Credential
- Man-in-the-Middle
- Ransomware
- Phishing

How comprehensive is the deception?

Deception lures are based on a variety of deception techniques that are placed on endpoints and servers and are used to lure attackers to the engagement server. Deception lures should cover layers 2-7 and regularly refresh for the greatest level of effectiveness.

- What type of deception lures are available?
- End-point
- Server
- Application
- Data
- Active Directory
- Are the deceptions static or do they dynamically update?
- Do they support the OS you need?
- Do they require an agent to maintain?
- How easy are the lures to deploy and update?

How authentic is the deception and how well can the solution lure attackers away from production servers?

- Are the servers running real operating systems or are they emulated?
- How extensive are the services?
- Can you load a "golden image" or customize services to make the deception servers indistinguishable from production servers?
- Can they deceptions be designed to match hospital devices, SCADA, or IOT environments?
- Are the servers static or can they broadcast traffic to appear active?
- How authentic and customizable are the deception credentials?
- Can the deception lures attract ransomware attackers?

How difficult is it to install?

Some deception engagement servers require network integration and monitoring of all traffic while others can reside off of a switch and don't require a network redesign or traffic redirection assessments.

- Is in-line deployment required and if so, what network and compute changes need to be factored in?

How well does the engagement server analyze, identify, and report on attack findings?

- Can the system identify attacks without known attack patterns or signatures?
- How comprehensive, safe, and manageable is the analysis environment? Advanced deception systems can open communications with the Command and Control (C&C) to understand more about attacker methods and tools being used.
- Can the "sandbox" environment be configurable for different lengths of time for attack analysis?
- How comprehensive is the attack information and how is it displayed or information shared?
- Can the attack information be augmented and reporting enhanced with information from threat reputation providers?

How comprehensive is the threat intelligence dashboard/ user interface?

- Clarity of information
- Navigation and detail drill down
- Information Enrichment (I.e. Virus Total)
- Ability to add manual or automated response actions

Report formats

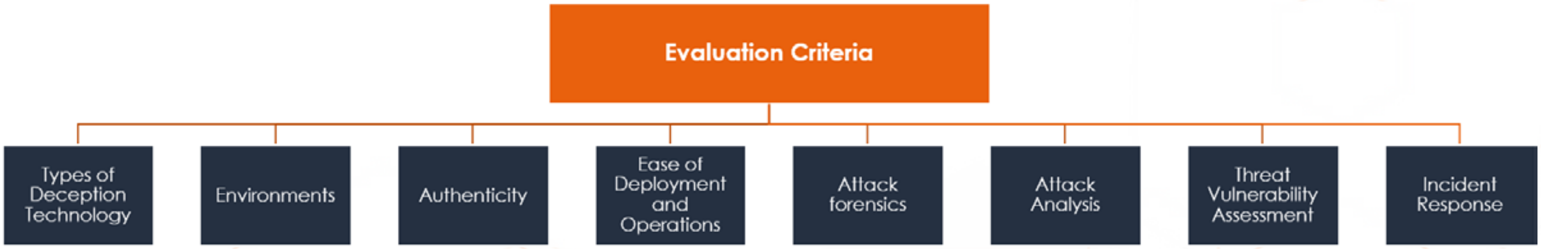
- IOC, PCAP, STIX, CSV, etc.

3rd Party Integrations

- Automated or manual with SIEM, Firewall, NAC, Patch Management, etc.

How accurate and detailed are the alerts?

- Can they be customized based on level of attack finding?
- How clear is it to quickly identify areas of greatest concern?
- Is all the detail required for incident response and infected system quarantining provided?



Evaluation Criteria
Types of Deception Technology
Environments
Authenticity
Ease of Deployment and Operations
Attack forensics
Attack Analysis
Threat Vulnerability Assessment
Incident Response

What else should a person evaluating deception know?

Common Misconceptions

- Deception is only for outside the network – The focus and value of a deception solution is for detecting inside-the-network threats.
- Deception is easy to detect – Deception that runs real operating systems, allows customized images and services, and dynamic deception lures will appear indistinguishable to an attacker.
- Deception is hard to install – Installation and activation of detection solution occurs in less than 30 minutes.
- Deception requires more staff to operate – Alerts are based on actual engagement (zero false positives) with server and have substantiated forensics to make each alert actionable. The environment also auto-rebuilds after each attack. Additional staff is not required to operate the platform given the high quality alerts, depth of reporting, and 3rd party integration that improve overall staff productivity.
- Isn't deception just a honeypot? – No. At the most fundamental level, there is some commonality. They are both designed to confuse, misdirect, and delay the enemy by incorporating ambiguity and misdirecting their operations. Beyond that, however, the technologies are quite different. More information can be found at this blog, which explores the origins of honeypots and explains why comparing a honeypot to a deception platform is like comparing a horse and buggy to a Tesla.

Ultimately, nothing beats seeing a real demo of the deception platform to see the full functionality and user interface of the solution. Attack analysis and reporting will also play a key role in the operations and effectiveness of deception for continuous threat management. Interested parties should also ask for sample reporting to see the depth of information provided and how the information is displayed.

Summary

The Attivo ThreatDefend™ Deception and Response Platform plays a critical role in empowering an adaptive defense with real-time detection of threats, attack vulnerability assessments, attack forensic analysis, and the integrations to dramatically accelerate incident response. Technology integrations with partners serves as a force multiplier effect, which improves existing technologies, process, and resource productivity, making them better and ultimately reducing the time to detect and remediate an exploit or malicious threat actor. Working hand-in-hand with our partners, Attivo Networks will continue to expand its platform and 3rd party integrations to deliver the fastest detection and incident response to stop attackers in their tracks.

About Attivo Networks

Attivo Networks® provides the real-time detection and analysis of inside-the-network threats. The Attivo ThreatDefend™ Deception and Response Platform detects stolen credentials, ransomware, and targeted attacks within user networks, data centers, clouds, SCADA, and IoT environments by deceiving an attacker into revealing themselves. Comprehensive attack analysis and actionable alerts empower accelerated incident response. www.attivonetworks.com