WHITEPAPER

ATTIVO NETWORKS® COVERAGE FOR MITRE® ENGAGE

INTRODUCTION

MITRE has launched a knowledge base named Engage to replace its Shield matrix, available at https://engage.mitre.org/ Engage is a framework for discussing and planning adversary engagement, deception, and denial activities. Engage is informed by adversary behavior observed in the real world and is intended to drive strategic cyber outcomes. Engage was created to help the private sector, government, and vendor communities to plan and execute the use of adversary engagement strategies and technologies.

THE ENGAGE MATRIX

The Engage Matrix displays the relationships between the various Strategic and Engagement Goals, Approaches, and Activities. The top row of Engage lists the Goals, and each Approach and Activity falls under a goal. Approaches are the next row down, and all Activities get assigned to an Approach. Finally, Activities make up the remaining entries in Engage. Strategic Actions are in the far right and far left columns, with Engagement Actions in the central columns. By bookending Engagement Actions with Strategic Planning and Analysis, the goal is that MITRE Engage can help organizations better plan and implement real-world adversary engagement strategies and advance the cybersecurity ecosystem.

Prepare	Expose		Affect			Elicit		Understand
Planning	Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation	Analysis
Define Exit Criteria	API Monitoring	Decoy Artifacts & Systems	Baseline	Decoy Artifacts & Systems	Decoy Artifacts & Systems	Application Diversity	Application Diversity	Distill Intelligence
Develop Threat Model	Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity	Hotwash
Persona Creation	Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware	Inform Threat Model
Strategic Goal	System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation	Refin Operations Activities
Storyboarding			Security Controls	Network Manipulation		Information Manipulation	Personas	
				Peripheral Management		Network Diversity	Network Diversity	
				Security Controls		Peripheral Management		
				Software Manipulation		Pocket Litter		

ATTIVO NETWORKS SUPPORT FOR THE MITRE ENGAGE MATRIX

The Attivo Networks ThreatDefend® Platform offers extensive capabilities that cover Activities listed in the MITRE Engage matrix. The platform capabilities range from simple deception and concealment strategies to a layered prevention strategy. Attivo evaluated the ThreatDefend platform features against all Activities documented per Approach by the MITRE Engage knowledge base. The image below captures the overall coverage the platform provides to any defender. The highlighted cells are the Activities that the Attivo ThreatDefend platform covers.

Expose		Affect			Elicit	
Collection	Detection	Prevention	Direction	Disruption	Reassurance	Motivation
API Monitoring	Decoy Artifacts & Systems	Baseline	Decoy Artifacts & Systems	Decoy Artifacts & Systems	Application Diversity	Application Diversity
Network Monitoring	Detonate Malware	Hardware Manipulation	Detonate Malware	Isolation	Artifact Diversity	Artifact Diversity
Software Manipulation	Network Analysis	Isolation	Email Manipulation	Network Manipulation	Burn-In	Detonate Malware
System Activity Monitoring		Network Manipulation	Migrate Attack Vector	Software Manipulation	Email Manipulation	Information Manipulation
		Security Controls	Network Manipulation		Information Manipulation	Personas
			Peripheral Management		Network Diversity	Network Diversity
			Security Controls		Peripheral Management	
			Software Manipulation		Pocket Litter	

COVERAGE DESCRIPTIONS BY ACTIVITY

This section details how specific Attivo ThreatDefend platform components provide coverages for Activities within MITRE Engage. The Attivo Networks ThreatDefend® Platform identifies risks, provides least privileges access to data, and lateral movement threat detection across endpoints, Active Directory (AD), clouds, and networks. Concealment technology hides critical AD objects, data, and credentials, while misdirection and deception decoys derail attacker lateral movement. Automated intelligence collection, attack analysis, and third-party integrations accelerate incident response. The platform includes BOTsink® deception servers, Endpoint Detection Net Suite, ADSecure, and ADAssessor for Active Directory protection, and the IDEntitleX solution protects cloud identities and entitlements.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	Attivo Coverage
Expose	Collection	API Monitoring	The ADSecure solution monitors key APIs and console commands to understand the adversary's malicious intent. The solution detects and alerts on adversary attempts to collect information on running services on the endpoints. The EDN ThreatStrike solution also deploys deceptive credentials. Attackers stealing locally stored credentials should also collect deceptive accounts that expose and redirect them to the decoys for engagement when used.
Expose	Collection	Network Monitoring	The BOTsink server monitors the network traffic on broadcast and multicast protocols to detect network-based attacks like MITM and DGA attacks. The BOTsink-deployed decoys capture high-fidelity data adversaries produce during their operations. These decoys detect attackers performing reconnaissance and lateral movements. The EDN Deflect function monitors the traffic and identifies anomalous traffic patterns exposing the presence of an adversary at the endpoints.
Expose	Collection	Software Manipulation	The ADSecure solution identifies unauthorized AD queries, collects intelligence, and observes the attacker's TTPs. The solution can manipulate or alter the output of commonly used discovery commands to influence an attacker's next choice of actions. It can also hide away critical assets from such recon attempts to protect from malicious activity.
Expose	Collection	System Activity Monitoring	The ThreatDefend platform captures the attacker's malicious activities and provides deep forensic data for investigation. The solution provides detailed session activities for each attacker's action on the compromised endpoint and decoy servers.
Expose	Detection	Decoy Artifacts and Systems	The EDN ThreatStrike solution deploys decoy artifacts as deceptive credentials, accounts, files, etc. The BOTsink servers can deploy decoys mimicking production infrastructure. Adversaries attempting to use decoy artifacts get directed to these decoys for engagement. Additionally, the detection capability produces a high-fidelity alert and provides deep forensic data for investigation.
Expose	Detection	Detonate Malware	The BOTsink server offers a malware sandbox to detonate malware or ransomware and understand its behavior. The BOTsink server also provides detailed insights for each malicious activity and exposes adversary intelligence, such as how the malware interacts with system resources and its target preferences, etc.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	Attivo Coverage
Affect	Prevention	Isolation	The EDN Deflect function alerts on reconnaissance as attackers scan for ports and services to exploit. It also redirects both inbound and outbound connection attempts to decoys for engagement. The EDN Deflect function makes every endpoint a part of the deception fabric, obfuscating what they look like from the network to disrupt attackers attempting to move laterally. The EDN Deflect function enables native isolation of infected systems to limit their communications to the decoy environment, thus limiting the damage they can do by quarantining them away from production systems.
Affect	Prevention	Network Manipulation	The BOTsink server offers a unique capability of providing proxy internet access that watches interactions between decoys and the Command and Control (C2) servers. This capability provides the intelligence for how an adversary responds, possibly exposing additional C2 information. Additionally, the EDN Deflect function triggers alerts on suspicious network activity and forwards the failed outbound connection attempts on non-existing services to the decoys.
Affect	Prevention	Security Controls	The ThreatDefend platform alters Windows security controls by adding deceptive SYSVOL Group Policy objects in the production Active Directory. Adversaries harvest privileged credentials from SYSVOL shares to gain access to all systems. A deceptive SYSVOL policy can prevent such attempts by misdirecting the adversary from compromising all the systems and revealing them.
Affect	Direction	Decoy Artifacts and Systems	The EDN ThreatStrike solution deploys decoy artifacts as deceptive credentials, accounts, files, etc. The BOTsink server also deploys decoys mimicking production infrastructure. Adversaries stealing decoy artifacts from endpoints can also take these deceptive accounts and get redirected to the decoys for engagement, negatively impacting them from conducting their intended operations.
Affect	Direction	Detonate Malware	The BOTsink server offers a malware sandbox and high-interactive decoys to detonate malware, thereby revealing high-fidelity interactive information to identify IoCs for broader detection and protection strategies.
Affect	Direction	Migrate Attack Vector	The BOTsink server supports malware analysis and adversely affects adversaries from conducting their intended operations. The solution detects and moves phishing or other suspicious emails to a decoy system to prevent further damage.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	Attivo Coverage
Affect	Direction	Network Manipulation	The BOTsink server offers a unique capability of providing proxy internet access that watches interactions between decoys and the Command and Control (C2) servers. This capability provides the intelligence for how an adversary responds, possibly exposing additional C2 information. Additionally, the EDN Deflect function triggers alerts on suspicious activity and redirects the traffic to decoys for engagement, thereby impacting the adversary's intended operations.
Affect	Direction	Security Controls	The ThreatDefend platform alters windows security controls by adding deceptive SYSVOL Group Policy objects in the production Active Directory. Adversaries harvest privileged credentials from SYSVOL shares to gain access to all systems. A deceptive SYSVOL policy can prevent such attempts by misdirecting the adversary from compromising all the systems and revealing them.
Affect	Direction	Software Manipulation	The ADSecure solution identifies unauthorized AD queries, collects intelligence, and observes the attacker's TTPs. The solution can manipulate or alter the output of commonly used discovery commands and hide critical assets from such recon attempts to protect from malicious activity. As a result, the solution disrupts adversaries and their ability to conduct their intended operation.
Affect	Disruption	Decoy Artifacts and Systems	The EDN ThreatStrike solution deploys decoy artifacts as deceptive credentials, accounts, files, etc. The BOTsink server also deploys decoys mimicking production infrastructure. Adversaries stealing decoy artifacts from endpoints can also take these deceptive accounts and get redirected to the decoys for engagement, negatively impacting them from conducting their intended operations.
Affect	Disruption	Isolation	The EDN Deflect function alerts on attacker reconnaissance as they scan for ports and services to exploit. It also redirects both inbound and outbound connection attempts to decoys for engagement. The EDN Deflect function makes every endpoint a part of the deception fabric, obfuscating what they look like from the network to disrupt attackers attempting to move laterally. The EDN Deflect function enables native isolation of infected systems to limit their communications to the decoy environment, thus limiting the damage they can do by quarantining them away from production systems.
Affect	Disruption	Network Manipulation	The EDN Deflect function alerts on attackers scanning for ports and services to exploit. It redirects any attack connection attempt targeting non-existing services on endpoints to network decoys for engagement. The solution disrupts an attacker's ability to discover services and move laterally to other endpoints.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	Attivo Coverage
Affect	Disruption	Software Manipulation	The ADSecure solution identifies adversary use of queries or scripts to discover a diverse set of accessible resources. The solution can manipulate or alter the output of commonly used discovery commands to influence an attacker's next choice of actions.
Elicit	Reassurance	Application Diversity	The BOTsink server offers decoys for over 70 different kinds of services and applications. These decoys are entirely customizable to make them mimic the production services and applications. Additionally, the EDN suite adds authentic deceptive components to create realistic user accounts, credentials, and files. Attackers following such deceptive data can engage with the decoys, thereby revealing tactics, techniques, and procedures.
Elicit	Reassurance	Artifact Diversity	The BOTsink server deploys decoy systems with varying Operating Systems and software configurations. The EDN ThreatStrike solution deploys deceptive credentials on production endpoints. These detect attacker attempts to compromise deceptive credentials and redirect them to decoys for engagement. The diversity of artifacts elicits and gathers more information from the adversary.
Elicit	Reassurance	Burn-In	The EDN suite deploys deceptive artifacts on endpoints and periodically refreshes them to make them appear in use or recently created. Artifacts that appear to be in current use have a higher probability of attackers stealing them than others. Adversaries using these artifacts can engage with decoys that capture their tactics, techniques, and procedures.
Elicit	Reassurance	Information Manipulation	The EDN suite deploys deceptive credentials and accounts that look real and believable to adversaries. Additionally, the ADSecure solution prevents attackers from accessing information from Active Directory by efficiently concealing the actual objects and returning fake information to unauthorized queries. The solution detects and alerts on adversaries collecting deceptive data, thereby revealing their tools and techniques.
Elicit	Reassurance	Network Diversity	The BOTsink server projects diverse network decoys such as switches, routers, printers, and server decoys like Windows Active Directory Domain Controllers. The solution provides authentic, high-interaction decoy technology to engage with attackers, providing the advantage of early detection and the ability to gather extensive data for attack analysis.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	Attivo Coverage
Elicit	Reassurance	Pocket Litter	The ThreatDefend platform deploys decoy documents and browser artifacts on endpoints to convince an adversary that an endpoint is real. The platform also allows defenders to customize the decoy document or artifact contents to mimic the patterns as seen at the endpoint. The platform enables the defender to create environments that are target-rich and have a variety of artifacts. An adversary using them would end up revealing their tactics, techniques, and procedures.
Elicit	Motivation	Application Diversity	The BOTsink server offers a target-rich environment with decoy systems for over 70 different kinds of services and applications. These decoys are entirely customizable to make them mimic the production services and applications. Additionally, the EDN suite provides authentic, high-interaction decoy credentials and other user artifacts to force lead attackers to decoys for engagement, providing the advantage of early detection and the ability to gather extensive data for attack analysis.
Elicit	Motivation	Artifact Diversity	ThreatDefend platform provides a target-rich environment to encourage an adversary to execute part or all of their mission. The EDN ThreatStrike solution deploys deceptive credentials on production endpoints. The solution helps to detect attackers compromising these credentials and redirects them to decoys systems for engagement.
Elicit	Motivation	Detonate Malware	The Ativo BOTsink server provides a malware sandbox to detonate malware and understand its behavior. The sandbox is a controlled environment that defenders can customize to match their infrastructure's OS and other baselines. Defenders can collect new IoCs during dynamic analysis and study the adversary's malicious intent.
Elicit	Motivation	Information Manipulation	The EDN suite deploys deceptive artifacts on endpoints and periodically refreshes them to make them appear in use or recently created. Artifacts that appear to be in current use have a higher probability of attackers stealing them than others. Adversaries using these artifacts engage with decoys that capture their tactics, techniques, and procedures.
Elicit	Motivation	Network Diversity	The BOTsink server projects diverse network decoys such as switches, routers, printers, and server decoys like Windows Active Directory Domain Controllers. The solution provides authentic, high-interaction decoy technology to engage with attackers, providing the advantage of early detection and the ability to gather extensive data for attack analysis. For authenticity, decoys run real operating systems and services that defenders can customize with production "golden images" to better blend in with other network assets. The selection of decoys that an attacker interacts with reveals their intent, and interaction methods reveal the tools, techniques, and procedures.

MITRE ATT&CK

Attivo has also mapped its ThreatDefend capabilities to the MITRE ATT&CK® framework, documentation of which is here. Another paper highlighting how the Attivo Endpoint Detection Net (EDN) suite improves endpoint security by augmenting existing endpoint security controls to boost overall detection performance is here.

Independent research by TAG Cyber validates the performance enhancements seen by adding the Endpoint Detection Net Suite to various EDR solutions using the MITRE ATT&CK DIY methodology. On average, users saw a performance boost of 42%. A summary of that research is here.

CONCLUSION

Deception and concealment technologies are powerful defense mechanisms that bridge gaps attackers can exploit when they successfully penetrate a perimeter defense. By adding the Attivo Networks ThreatDefend Platform to the security stack, organizations gain early and accurate visibility, detection, and prevention of attacks that evade existing controls while gaining capabilities that help them meet the guidance set forth MITRE.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, experts in Identity Detection and Response (IDR), provides an innovative defense to protect against identity compromise, privilege escalation, and lateral movement attacks. The company's solutions deliver unprecedented visibility to security exposures and attack paths and prevent and derail attack escalation activities across endpoints, Active Directory, and cloud environments. A combination of patented data cloaking, misdirections, and cyber deception innovations protects identities and comprehensively detects threats. These solutions are an integral part of NIST Special Publications, MITRE Shield, and its capabilities tightly align to the MITRE ATT&CK Framework. Attivo Networks has won 150+ awards for its technology innovation and leadership.
www.attivonetworks.com