WHITEPAPER

ATTIVO NETWORKS® THREATDEFEND® PLATFORM AND THE MITRE ENGAGE MATRIX™

INTRODUCTION

The MITRE Corporation Engage Matrix is a framework for planning and discussing adversary engagement operations that empower organizations to engage their adversaries and achieve their cybersecurity goals.

MITRE Engage seeks to help the defender, the frontline innovator, by lowering the barrier to entry while raising the ceiling of expertise for those seeking to use adversary engagement technologies. Unlike many other defensive technologies, MITRE believes that cyber deception technologies are not "fire and forget." Instead, organizations should deploy deception technologies as part of an intentional strategy that drives toward well-understood goals. As such, Engage is designed to help defenders:

- **Safely and effectively engage in denial, deception, and adversary engagement (AE).** Engage seeks to provide the community with the resources they need to understand how to effectively and safely use adversary engagement technologies to meet their goals, whether they are AE experts or novices.

- **Drive future progress and innovation.** Engage hopes to build a unified community of professionals contributing expertise and sharing insights to grow and mature the technology space.

- **Build a sharing community of adversary engagement practitioners.** Engage hopes to facilitate information sharing and networking as the AE community grows and matures.

MITRE Engage also aims to help the CISOs, and other security decision-makers, understand how denial, deception, and adversary engagement fit into the organization's current cyber strategy. Engage is designed to help decision-makers:

- **Create policies and procedures for safe network operation and response to incidents.** Engage introduces planning and adapting as fundamental components of the framework. While planning and adapting are CISO functions, the practitioner needs know-how activities like collection, reassurance, and motivation that can lead to the detection of incidents.

- **Reduce risks to information and related technologies.** Engage lays out activities to support detecting, preventing, directing, and disrupting adversaries. MITRE believes that employing these activities can support the mission of risk reduction.

- **Protect information and assets.** While denial activities limit an adversary's access to legitimate information, deception performs an additional protection mechanism. Providing misinformation about systems or data can decrease an adversary's trust or value in those assets. Decreasing value and trust typically will cause an adversary to avoid those objects.

THE MITRE ENGAGE MATRIX

Cyber defense has traditionally focused on using defense-in-depth technologies to deny adversaries access to an organization's networks or critical cyber assets. In this paradigm, whenever adversaries can access a new system or exfiltrate a piece of data from the network, they win. However, when a defender introduces deceptive artifacts and systems, it immediately increases ambiguity for the adversary.

Cyber Denial is the ability to prevent or otherwise impair the adversary's ability to conduct operations. This disruption may limit their movements, collection efforts, or the effectiveness of their capabilities. **Cyber Deception** intentionally reveals deceptive facts and fiction to mislead the adversary. In addition, it conceals critical facts to prevent the adversary from forming correct estimations or taking appropriate actions. When organizations use cyber denial and deception together, they provide the foundation of Adversary Engagement within the context of strategic planning and analysis.

Successful adversary engagement operations break down into four components: **narrative, environment, monitoring,** and **analysis**. The narrative is the deception story the organization intends to portray to its adversary. The engagement environment is the set of carefully tailored, highly instrumented systems designed on an engagement-by-engagement basis as the backdrop to the engagement narrative. These systems may be completely isolated or integrated into the production network. Monitoring refers to the collection system used to observe the adversary as they move through the environment. Monitoring is essential for maintaining operational safety throughout an operation. Finally, analysis refers to the actions the organization takes to turn the outputs of its engagement operation into actionable intelligence. The organization's operational objective, the ultimate goal of the engagement, connects everything. This objective can include any of the following: to expose adversaries on the network, to affect the adversary by impacting their ability to operate, and to elicit intelligence to learn about adversary Tactics, Techniques, and Procedures (TTPs). Adversary engagement operations allow the defender to demonstrate tools, test hypotheses, and improve their threat models, all with the benefit of negatively impacting the adversary.

Adversary engagement is an iterative, goal-driven process, not merely the deployment of a technology stack. It is not enough to deploy a decoy and declare success. Instead, the organization must think critically about its defensive goals and how it can use denial, deception, and adversary engagement to drive progress towards these goals. Unlike other defensive technologies, such as antivirus (AV), adversary engagement technologies cannot be considered "fire and forget" solutions. Adversary engagement is a thinking game; it is as much about the organization's mindset as what tools it uses. The Engage 10-Step Process helps evaluate engagement activities within the scope of this mindset.

The ten steps cover three phases: Prepare, Operate, and Understand. In the Prepare phase, the organization defines its operational objective. It then constructs an engagement narrative to support this objective, which then informs the design of the engagement environment and all operational activities. Additionally, the organization gathers relevant stakeholders to define the acceptable level of operational risk. By setting this level of risk at the forefront, the organization can construct clear Rules of Engagement (RoE) to serve as guardrails for operational activities. Its monitoring and analysis capabilities should be sufficient to ensure that its activity remains within these bounds. In the Operate phase, the organization implements and deploys its designed activities. Finally, the Understand phase guides the organization in turning operational outputs into actionable intelligence to assess whether or not it met its operational objective. Additionally, this evaluation allows it to capture lessons learned and refine future engagements.

The Engage Matrix is divided vertically into two categories of actions – Strategic and Engagement. Strategic actions bookend the Matrix and ensure that defenders appropriately drive operations with strategic planning and analysis. These actions map to the Prepare and Understand phases of the 10-Step Process.

Engagement actions are the traditional cyber denial and deception activities used to drive progress towards the objectives. These actions map to the Operate phase of the 10-Step Process.

Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

The Engage Matrix further subdivides horizontally into Goals, Approaches, and Activities. Across the top of the Matrix are the Engage Goals. Goals are the high-level outcomes the operation should accomplish.

The Prepare and Understand Goals focus on the inputs and outputs of an operation. While the Matrix is linear, just like the 10-Step Process, one should view it as cyclical. As the operation proceeds, the organization constantly aligns and realigns its actions to drive progress towards its Engagement Goals. The Engagement Goals are Expose, Affect, and Elicit. These goals focus on actions taken against the adversary.

The organization can Expose adversaries on the network by using deceptive activities to provide high fidelity alerts when adversaries are active in the engagement environment.

The organization can Affect adversaries by negatively impacting their operations. Affect activities are ultimately about changing the cost-value proposition in cyber operations for the adversary to increase the adversary's cost to operate or drive down the value derived from attack operations. It is important to note that all Affect activities stay within the defender's network. It is NOT hacking back or any activities in the adversary's space. This distinction is essential to ensure that the organization's defense activities are legal.

The organization can Elicit information about the adversary to learn about their TTPs. By creating an engagement environment uniquely tailored to engage with specific adversaries, the defenders can encourage them to reveal additional or more advanced capabilities. Observing adversaries as they operate can provide actionable cyber threat intelligence (CTI) data to inform the defender's other defenses.

The next row contains the Engage Approaches, which let the organization progress towards its selected goal. Strategic Approaches help the organization focus on the steps it must complete before, during, and after an operation to ensure that its activities align with the overall strategy. Engagement Approaches help identify what actions the organization would like to take against its adversary and helps it drive progress towards that impact.

The remainder of the Matrix is composed of the Engage Activities. These are the concrete techniques to use in the approach. Activities can adapt to fit a spectrum of use cases and objectives based on implementation. Additionally, actual adversary behavior drives them. When adversaries engage in specific behaviors, they are vulnerable to exposing unintended weaknesses. Engage looks at each MITRE ATT&CK® technique to examine the weaknesses revealed and identify engagement activities to exploit them. By mapping the engagement activities to ATT&CK, the organization can better plan which activities will enable it to reach its strategic objectives.

ATTIVO NETWORKS SUPPORT FOR THE MITRE ENGAGE MATRIX

The Attivo Networks ThreatDefend® Platform provides extensive capabilities to implement many of the activities outlined in the Engage Matrix. The ThreatDefend Platform identifies risks, provides least privileges access to data, and detects threat lateral movement 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.

Expose		Affect			Elicit	
Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate
API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity
Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity
Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation
System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities
		Security Controls	Malware Detonation		Information Manipulation	Malware Detonation
			Network Manipulation		Network Diversity	Network Diversity
			Peripheral Management		Peripheral Management	Personas
			Security Controls		Pocket Litter	
			Software Manipulation			

In evaluating the ThreatDefend Platform against the Engage Matrix, Attivo Networks compared the solution against activities to identify how the solution would implement each one. The table below contains the analysis as of the initial release of the Engage Matrix in 2022, mapping to the activities the ThreatDefend Platform can successfully implement.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	How Attivo Implements the Activities
Expose	Collect	API Monitoring	The ADSecure solution for endpoints monitors key APIs and console commands to understand the adversary's malicious intent. The solution detects and alerts adversary attempts to collect information on running services on the endpoints. The EDN ThreatStrike® solution also deploys deceptive credentials. Attackers stealing credentials will also collect decoy accounts that expose and redirect them to the decoys for engagement when used.
Expose	Collect	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 decoys can capture data an adversary produces 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.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	How Attivo Implements the Activities
Expose	Collect	Software Manipulation	The ADSecure solution monitors, collects intelligence, and observes the adversaries' TTPs. The solution can manipulate or alter the output of commonly used Active Directory discovery commands to influence an attacker's next choice of actions. It can also hide critical assets from such recon attempts to protect from malicious activity.
Expose	Collect	System Activity Monitoring	The ThreatDefend platform captures the adversary's malicious activities and collects deep forensic data for investigation. The solution provides detailed session activities for attacker actions on the compromised endpoint and decoy servers.
Expose	Detect	Introduced Vulnerabilities	The BOTsink server hosts full Operating System decoys with real applications and services. The solution supports hundreds of applications such as SSH, RDP, MSSQL, Active Directory, VPN gateway, Hadoop, MySQL, MongoDB, video cameras, IoT applications, ICS/SCADA, etc. to motivate the adversary to target specific resources. Attackers trying to exploit vulnerabilities on the targetted resource can engage and reveal tactics, techniques, and procedures.
Expose	Detect	Lures	The EDN ThreatStrike solution deploys decoy artifacts such as deceptive credentials, accounts, files, etc. The BOTsink server can deploy decoys mimicking production infrastructure. Adversaries attempting to use decoy artifacts engage with these decoys. Additionally, the detection capability produces a high-fidelity alert and provides deep forensic data for investigation.
Expose	Detect	Malware Detonation	The BOTsink server includes a malware sandbox to detonate malware 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.
Expose	Detect	Network Analysis	The BOTsink server deploys network decoys across multiple remote and branch locations. The solution captures data and analyzes network traffic to help defenders detect exposed adversary activity, such as C2 or data exfiltration traffic. Additionally, the ADSecure solution for domain controllers detects attacks targeting AD, identifies suspicious user behaviors using deep packet inspection, and delivers high-fidelity alerts.
Affect	Prevent	Baseline	The BOTsink server offers adaptive cybersecurity defenses using machine learning to create deception campaigns that create authentic decoys to reduce the attack surface and provides authentic deception for every possible attack. Afterward, it reverts the environment to a baseline configuration by redeploying decoys with new IP addresses, MAC addresses, hostnames, SMB shares, etc., to maintain the deception fabric's freshness and increase the likelihood of surprising attackers.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	How Attivo Implements the Activities
Affect	Prevent	Isolation	The EDN Deflect function alerts on attacker reconnaissance scans to find 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	Prevent	Network Manipulation	The BOTsink server offers a unique capability of providing proxy internet access that allows watching interactions between decoys and the Command and Control (C2) servers. The solution captures how the adversary communicates, 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 for engagement.
Affect	Prevent	Security Controls	The ThreatDefend platform alters Windows security controls by adding decoy SYSVOL Group Policy objects in the production Active Directory. Adversaries harvest privileged credentials from SYSVOL shares to gain access to all systems. A decoy SYSVOL policy will prevent such attempts by misdirecting the adversary from compromising all the systems and revealing them.
Affect	Direct	Attack Vector Migration	The BOTsink server supports malware analysis and denies the adversary from conducting their operation as intended. The solution detects and moves phishing/suspicious emails to a decoy system to prevent further damage by the adversary.
Affect	Direct	Email Manipulation	The EDN ThreatStrike solution provides decoy email objects as a collection of fake email addresses and passwords. Additionally, the BOTsink server supports malware analysis features and dynamically analyzes suspicious emails with URLs and supported file attachments.
Affect	Direct	Introduced Vulnerabilities	The BOTsink server hosts full Operating Systems decoys with real applications and services. The solution supports hundreds of applications such as SSH, RDP, MSSQL, Active Directory, VPN gateway, Hadoop, MySQL, MongoDB, video cameras, IoT applications, ICS/SCADA, etc. to motivate the adversary to target specific resources. Attackers trying to exploit vulnerabilities on the targetted resource can engage and reveal tactics, techniques, and procedures.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	How Attivo Implements the Activities
Affect	Direct	Lures	The EDN ThreatStrike solution deploys decoy artifacts such as deceptive credentials, accounts, files, etc. The BOTsink server can deploy decoys mimicking production infrastructure. Adversaries attempting to use decoy artifacts engage with these decoys, further derailing them from conducting their operation as intended.
Affect	Direct	Malware Detonation	The BOTsink server includes a malware sandbox and high-interactive decoys to detonate malware. The solution can reveal high-fidelity interactive information to identify IoCs for a broader detection and protection strategy.
Affect	Direct	Network Manipulation	The BOTsink server offers a unique capability of providing proxy internet access that allows watching interactions between decoys and the Command and Control (C2) servers. The solution captures how the adversary communicates, possibly exposing additional C2 information. Additionally, the EDN Deflect function triggers alerts on suspicious network activity and redirects the traffic to decoys for engagement, impacting the adversary's intended operations.
Affect	Direct	Security Controls	The ThreatDefend platform alters Windows security controls by adding decoy SYSVOL Group Policy objects in the production Active Directory. Adversaries harvest privileged credentials from SYSVOL shares to gain access to all systems. A decoy SYSVOL policy will prevent such attempts by misdirecting the adversary from compromising all the systems and revealing them.
Affect	Direct	Software Manipulation	The ADSecure solution monitors, collects intelligence, and observes the adversaries' TTPs. The solution can manipulate the output of commonly used discovery commands and hide critical assets from such recon attempts. As a result, the solution derails the adversary from conducting its intended operation.
Affect	Disrupt	Isolation	The EDN Deflect function alerts on attacker reconnaissance scans to find 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	Disrupt	Lures	The EDN ThreatStrike solution deploys decoy artifacts such as deceptive credentials, accounts, files, etc. The BOTsink server can deploy decoys mimicking production infrastructure. Adversaries attempting to use decoy artifacts engage with these decoys, further derailing them from conducting their operation as intended.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	How Attivo Implements the Activities
Affect	Disrupt	Network Manipulation	The EDN Deflect function alerts when adversaries scan 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.
Affect	Disrupt	Software Manipulation	The ADSecure solution can monitor adversary queries or scripts to discover a diverse set of accessible resources. The solution can alter the results of typical reconnaissance commands to influence an attacker's next choice of actions.
Elicit	Reassure	Application Diversity	The BOTsink server offers decoys for over a hundred different services and applications. These decoys are entirely customizable to mimic production services and applications. Additionally, the EDN suite adds authenticity to deceptive components for realistic user accounts, credentials, files to attackers, etc. Attackers following this decoy data can engage with the decoys, thereby revealing tactics, techniques, and procedures.
Elicit	Reassure	Artifact Diversity	The BOTsink server offers deployment of decoy systems with varying Operating Systems and software configurations. The EDN ThreatStrike solution deploys deceptive credentials on production endpoints. The solution helps detect attackers compromising fake credentials and redirect them to decoys for engagement. The diversity of artifacts allows the organization to elicit and gain more information from the adversary.
Elicit	Reassure	Burn-In	The EDN suite periodically refreshes deceptive artifacts deployed on endpoints to make them appear in use or recently created. Adversaries have a higher probability of targeting artifacts that seem to be in current use using compared to others. The solution redirects adversaries using deceptive artifacts to decoys that capture their tactics, techniques, and procedures when they engage.
Elicit	Reassure	Email Manipulation	The EDN ThreatStrike solution provides decoy email objects as a collection of fake email addresses and passwords. These assets can reassure and convince an adversary that the decoys are part of the production environment. Additionally, the BOTsink server supports malware analysis features and dynamically analyzes suspicious emails with URLs and supported file attachments.
Elicit	Reassure	Information Manipulation	The EDN suite deploys deceptive credentials, accounts that look real and can easily make adversaries believe them. Additionally, the ADSecure solution prevents attackers from accessing information in Active Directory by efficiently concealing the production objects and returning fake data to an attacker's query. The solution detects and alerts when adversaries collect decoy data, revealing their tools and techniques.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	How Attivo Implements the Activities
Elicit	Reassure	Network Diversity	The BOTsink server projects a diverse set of 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 trick attackers into engaging, providing the advantage of early detection and the ability to gather extensive data for attack analysis.
Elicit	Reassure	Pocket Litter	The ThreatDefend platform deploys convincing decoy documents and browser artifacts on endpoints to reassure an adversary that they are part of the production environment. The platform also offers controls to ensure the content of such documents or artifacts mimics the patterns as seen at the endpoint. The platform enables the defender to create target-rich environments and has a variety of artifacts. Any adversaries using them would reveal their tactics, techniques, and procedures
Elicit	Motivate	Application Diversity	The BOTsink server offers decoys for over a hundred different services and applications. These decoys are entirely customizable to mimic production services and applications. Additionally, the EDN suite provides authentic, high-interaction decoys to trick attackers into engaging, providing the advantage of early detection and gathering extensive data for attack analysis.
Elicit	Motivate	Artifact Diversity	The ThreatDefend platform provides a target-rich environment to encourage an adversary to conduct part or all of their mission. The EDN ThreatStrike solution deploys deceptive credentials on production endpoints. The solution helps to detect attackers compromising deceptive credentials and redirects them to decoys systems for engagement.
Elicit	Motivate	Information Manipulation	The EDN suite periodically refreshes deceptive artifacts deployed on endpoints to make them appear in use or recently created. Adversaries have a higher probability of targeting artifacts that seem to be in current use using compared to others. The solution redirects adversaries using deceptive artifacts to decoys that capture their tactics, techniques, and procedures when they engage.
Elicit	Motivate	Introduced Vulnerabilities	The BOTsink server hosts full Operating Systems decoys with real applications and services. The solution supports hundreds of applications such as SSH, RDP, MSSQL, Active Directory, VPN gateway, Hadoop, MySQL, MongoDB, video cameras, IoT applications, ICS/SCADA, etc. to motivate the adversary to target specific resources. Attackers trying to exploit vulnerabilities on the targetted resource can engage and reveal tactics, techniques, and procedures.
Elicit	Motivate	Malware Detonation	The BOTsink server includes a malware sandbox to detonate malware and understand its behavior. The sandbox is a controlled environment that allows defenders can collect new IoCs during dynamic analysis and study the adversary's malicious intent.

MITRE Engage Goals	MITRE Engage Approaches	MITRE Engage Activities	How Attivo Implements the Activities
Elicit	Motivate	Network Diversity	The BOTsink server projects a diverse set of network decoys such as Switches, Routers, Printers, and Server Decoys like Windows Active Directory Domain Controllers. These decoys appear indistinguishable from production assets to encourage an attacker to interact with them. For authenticity, decoys run full Operating Systems and services and can be customized 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 the interaction methods reveal the tools, techniques, and procedures.
Elicit	Motivate	Personas	The ThreatDefend platform enables the defender to create target-rich environments of planted data. The BOTsink server supports deploying decoy documents on endpoints that detect and alert when attackers exfiltrate them. The EDN suite can hide and deny access to sensitive data from the local system. An adversary using the artifacts or attempting to access the concealed data would reveal their tactics, techniques, and procedures.

SUMMARY

The ThreatDefend platform provides extensive coverage for operational activities within the Engage Matrix. By adding the Attivo Networks® ThreatDefend® platform to the security stack, organizations can implement many Engage Activities to detect, deny, and derail attack activities while engaging with the attackers to collect TTPS and develop threat intelligence to strengthen defenses. These, in turn, can progress their engagement operations to fulfill their goals.

ABOUT ATTIVO NETWORKS®

Attivo Networks®, the identity detection and response leader, delivers a superior defense to prevent privilege escalation and lateral movement. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical attack points, including at endpoints, in Active Directory, and cloud environments. Data concealment technology hides critical AD objects, data, and credentials, eliminating attacker theft and misuse, particularly useful in a Zero Trust architecture. Bait and misdirection efficiently steer attackers away from production assets, and deception decoys obfuscate the attack surface to derail attacks. Forensic data, automated attack analysis, and automation with third-party integrations serve to speed threat detection and streamline incident response. ThreatDefend® capabilities tightly align to the MITRE ATT&CK Framework, and deception and denial are now integral parts of NIST Special Publications and MITRE Engage adversary engagement strategies. Attivo has 180+ awards for technology innovation and leadership. www.attivonetworks.com