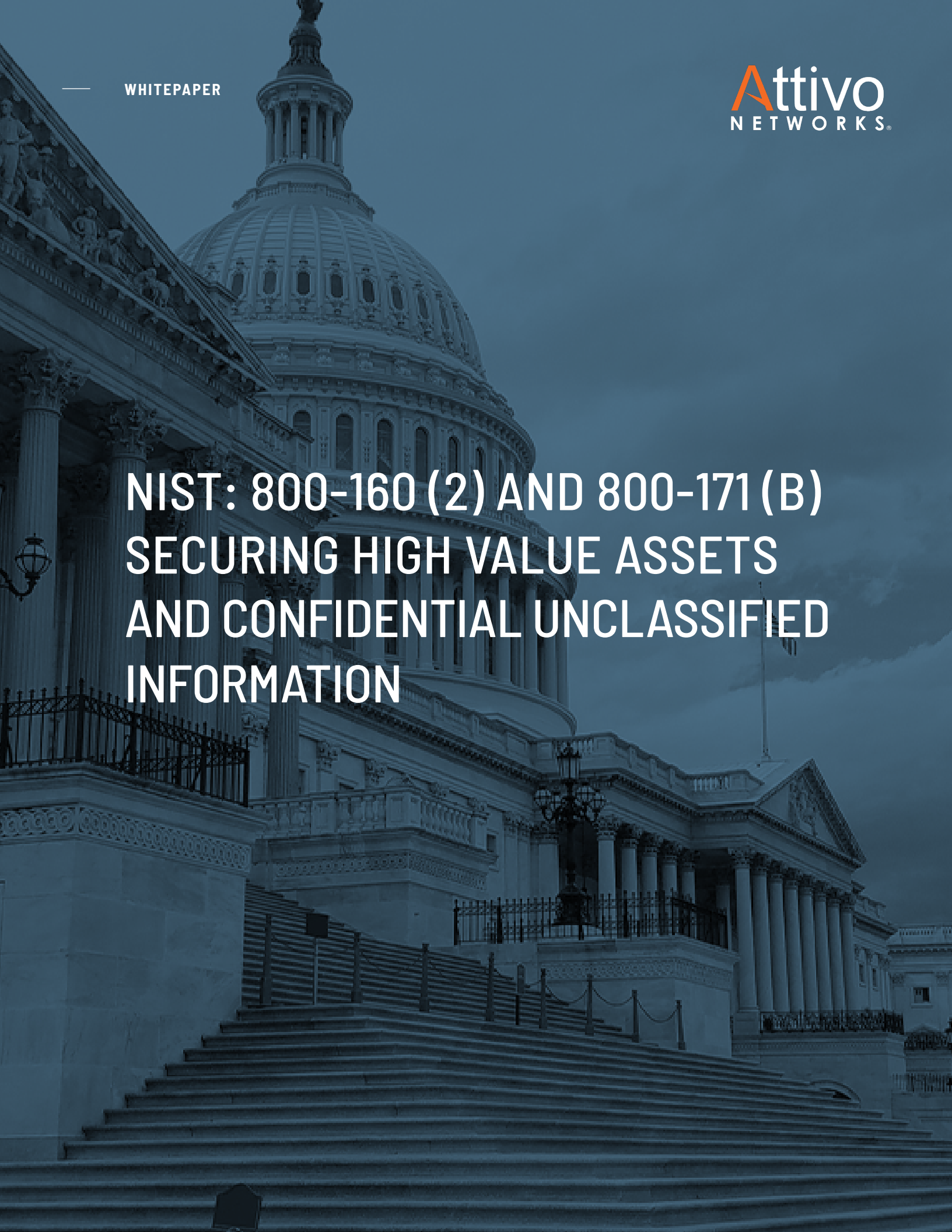
WHITEPAPER

Attivo NETWORKS®



NIST: 800-160 (2) AND 800-171 (B) SECURING HIGH VALUE ASSETS AND CONFIDENTIAL UNCLASSIFIED INFORMATION

EXECUTIVE SUMMARY

The NIST publications 800-160 Volume 2[1] and 800-172[2] deal with developing cyber-resilient systems and protecting controlled unclassified information in non-federal systems and organizations, respectively. These documents give an organization clear guidance on implementing secure systems from the policy, process, personnel, and technical perspectives. This paper briefly summarizes these NIST publications, introduces deception and concealment technologies, and shows how they fit within the NIST guidelines to support regulatory compliance and enhanced security.

NIST 800-160 VOL 2 AND NIST 800-172

NIST 800-160, released November 2016, goes into depth from a systems engineering perspective into how organizations can design, develop, and deploy trustworthy and secure systems that are dependable and resilient against compromise. The document is not a specific "how-to" guide. Instead, NIST 800-160 provides advice on implementing consistent and repeatable security and sets standards for systems engineering best practices.

NIST 800-160 has several notable objectives.

1. Create a formalized, disciplined basis for Systems Security Engineering that emphasizes principles, concepts, and activities.
2. Promote a standard security development paradigm that applies to any system regardless of size, scope, complexity, or stage in its operational life cycle.
3. Demonstrate ways organizations can apply these principles and concepts within the systems engineering process.
4. Foster growth in the study, development, and application of secure systems engineering practices.
5. Serve as the basis for education and training programs that can evolve into professional assessment criteria and individual certifications.

The security model presented in NIST 800-160 does not focus on specific threats. Instead, the model emphasizes recognizing the consequences of a potential breach, designing to minimize risk, enabling mitigation post-breach, and reducing the damage resulting from the loss of critical assets.

NIST 800-172 focuses on Controlled Unclassified Information (CUI). The National Archives define CUI as "information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended."[3] NIST 800-172 is a subset of requirements defined in NIST 800-53 and applies specifically to CUI shared by the federal government with a non-federal organization or entity. The controls protect this information on non-federal systems from unauthorized disclosure.

1 https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final

2 https://csrc.nist.gov/publications/detail/sp/800-172/final

3 https://www.archives.gov/cui/about

Providing a detailed analysis of these NIST documents is beyond the scope of this paper. However, both documents extensively reference using deception techniques within the context of cybersecurity and its particular use as a foil against sophisticated Advanced Persistent Threats (APT). This inclusion clearly shows that deception technology has reached the maturity needed for NIST recognition as an effective and recommended security control.

INTRODUCTION TO DECEPTION AND CONCEALMENT

Generations have used deception and concealment techniques in hunting, gaming, law enforcement, and the military domains. Adding deception and concealment technology to Defensive Cyber Operations (DCO) changes the status quo in cybersecurity from asymmetry in favor of the attacker to one that favors the defender. These strategies utilize decoy assets, breadcrumbs, and lures while hiding production assets and data to derail attacks and engage attackers. Deceptive assets placed throughout the network and on the endpoints make the entire production environment a trap for adversaries. These deceptive assets mirror-match the production environment, so even a skilled attacker will not recognize them for what they are without actively engaging. By that time, they have already revealed themselves. Meanwhile, concealment technology hides and denies access to sensitive or critical data and accounts to prevent attackers from targeting or compromising them.

Deceptive defenses range between network-, host-, and cloud-based deceptive assets, such as decoy file shares, serverless functions, and similar objects. On the network, deception technology provides decoy computing hosts and networked devices (that accurately reflect the production network environment and are indistinguishable from production assets. A live attacker or automated process can not determine the true nature of the deceptive assets without taking a closer look. The solution immediately detects any active effort to observe these devices or gain, sending a high-fidelity alert to the incident response team.

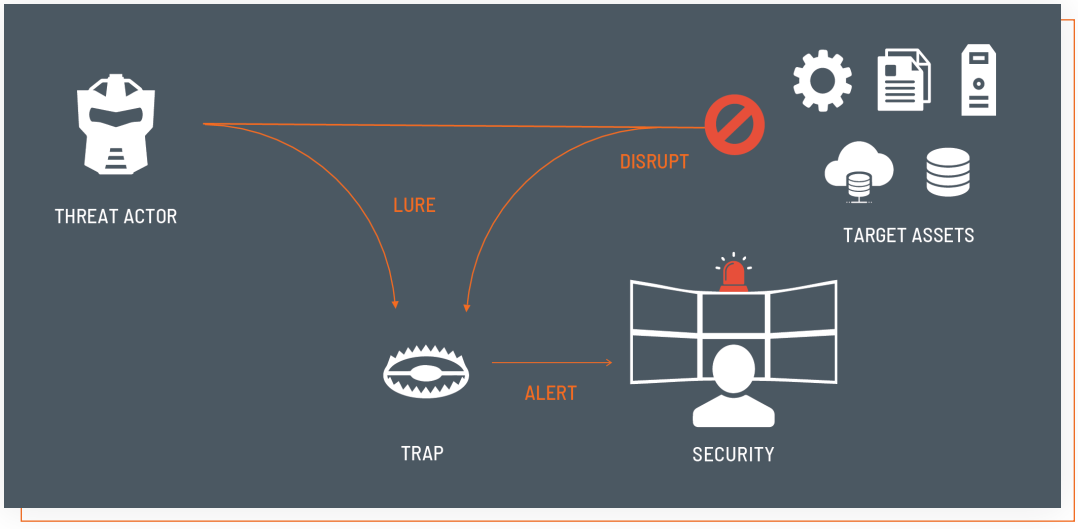


FIGURE 1: HOW DECEPTION WORKS

Deception and concealment solutions defend the endpoints by placing decoy credentials, hidden file shares mapped to decoy servers, and a range of other deceptive breadcrumbs and lures. These assets deflect an attacker away from the production environment into the deception environment for monitoring and containment. Concealment technology protects sensitive or critical local files, folders, network or cloud mapped shares, removable storage, and credentials stored on endpoints by preventing attackers from enumerating or accessing them. The technology is effective for human attackers and malicious software such as ransomware.

For example, when attackers query Active Directory for admin accounts or other intelligence from a compromised system, a host-resident deception and concealment solution can intercept the communication, hide the accurate query results, and return false objects. These results misdirect the attacks away from production systems and to decoys while disrupting attacker intelligence gathering.

Similarly, a ransomware 1.0 attack that encrypts or destroys files on network shares would engage with the deception shares[4] which identifies the attack and slows it to a crawl, feeding it fake data to keep the attacker occupied in the deception environment. This capability is invaluable for giving the incident response team time to react and contain the infection before it can spread. Meanwhile, the technology is effective against ransomware 2.0 attacks that seek to steal credentials and move laterally to compromise critical systems such as AD servers or production databases. The deception and concealment technologies detect credential theft, lateral movement, privilege escalation, target acquisition, and Active Directory attacks that the ransomware attempts to execute, preventing the attack from finding privileged accounts and objects or targeting critical assets.

In addition to deflecting reconnaissance, credential theft, AD queries, and man-in-the-middle attacks, modern deception and concealment systems can also redirect scans or connection attempts to closed ports and services on endpoints to decoys for engagement. The decoys respond to the attackers, disrupting the attack while alerting the cybersecurity team to the event.

In total, deception and concealment technology makes an attacker's job much more complex and gathers company-centric threat intelligence. It reverses the conventional paradigm, "An attacker only needs to be right once, while the defender needs to be right every time." Now, the attacker must be right every time or risk early detection and removal from the target network. Deception and concealment have proven to be unique resources for leveling the playing field in favor of cyber defenders, who typically are at a significant disadvantage.

USING DECEPTION AND CONCEALMENT TO MEET NIST 800-160 VOL 2 AND 800-172 REQUIREMENTS

NIST 800-160 Volume 2 mentions deception multiple times, focusing on its use in against adversarial threats while defining four areas of deception: The Attivo Networks ThreatDefend® platform provides coverage for each of these domains.

- Obfuscation
- Disinformation
- Misdirection
- Tainting

The Attivo Networks ThreatDefend® platform provides coverage for each of these domains.

In the context of the NIST document, "Obfuscation" refers to hiding, transforming, or otherwise obfuscating information from an adversary. Host and endpoint deception assets and concealment technologies obscure the apparent threat surface by vastly manipulating how it appears to a threat actor. Attackers will not know which targets are real and which are decoys or lures. Conventional security doctrine has held that "obscurity is not security." However, obfuscation is a valuable defensive tactic, especially when paired with attack interception and redirection while feeding the attacker disinformation to derail their efforts further.

4 **Mapped drives that are not normally visible to a user, but are available to automated tools and manual discovery.**

"Disinformation" in this context refers to deliberately providing misleading information to an adversary using any of a variety of techniques. One of the methods explicitly mentioned is the introduction of false credentials and tokens into the environment. The ThreatDefend platform achieves this with deceptive credentials and authentication tokens on endpoints, intercepting efforts to enumerate directory controllers and substituting false and misleading credentials. Any usage of these fake credentials quickly sends a high-fidelity alert to the cyber defense teams providing the option to trigger a fully automated response.

NIST defines "Misdirection" as maintaining deception resources or environments and directing an adversary to those resources or environments. This capability is a core function of the ThreatDefend platform. It creates and maintains a comprehensive set of decoy systems (computers, IoT, telecom, SCADA, etc.) indistinguishable from other assets in the production environment. These capabilities closely interrelate with disinformation functions that a threat actor away from the production assets into the deception environment.

Finally, "Tainting" involves embedding covert capabilities into resources. The ThreatDefend platform integrates deceptive elements into otherwise regular services or assets, such as adding entries into an organization's DNS and network caches that point to deceptive assets and hosts. These entries increase the perceived authenticity of decoy systems while giving an attacker potential targets that are themselves traps. Another example of tainting is the process of embedding carefully crafted beacons into a variety of commonly encountered file types (office documents, etc.) and strategically distributing them as deceptive targets of opportunity for data exfiltration or insider threat actors. The embedded beacons serve as a "phone home" capability that immediately identifies when anyone opens one of these "decoy documents" and can provide GeoIP information for context.[5] Tainting can also affect attacks on Active Directory by intercepting their queries and feeding back information that directs them into the deception environment, feeding them misinformation that slows and misdirects their attack activity.

The ThreatDefend platform allows an organization to address each of the recommendations outlined in NIST 800-160 Volume 2, providing additional security measures that let an organization meet compliance while reinforcing the rest of its security stack.

NIST 800-160 deals with systems engineering, while NIST 800-172 deals specifically with protecting controlled unclassified information (CUI) held on non-federal systems. Like NIST 800-160, it makes specific reference to using deception as a method to meet the goal of safeguarding CUI on relevant systems. NIST 800-172 3.13.3e specially deals with employing "technical and procedural means to confuse and mislead adversaries through a combination of misdirecting, tainting, or disinformation."[6]

This document describes the same methods and goals for deception detailed in NIST 800-160 Volume 2. It includes a reference to that publication to provide guidance on developing cyber-resilient systems and system components. This similarity also means that a solution such as the Attivo Networks ThreatDefend platform lets an organization meet the requirements in both publications.

5 **GeoIP information received from outside a known environment may not be reliable.**

6 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-172.pdf#page=36

The following table lists Attivo coverage maps based on NIST 800-160 and 800-172 requirements for the listed MITRE ATT&CK techniques.

F-3 Reconnaissance	F-4 Resource Development	F-5 Initial Access	F-6 Execution	F-7 Persistence	F-8 Privilege Escalation	F-9 Defense Evasion
Active Scanning (T1595)	Acquire Infrastructure (T1583)	Drive-by Compromise (T1189)	Command and Scripting Interpreter (T1059)	Account Manipulation (T1098)	Abuse Eleveation Control Mechanism (T1548)	Abuse Eleveation Control Mechanism (T1548)
Gather Victim Host Information (T1592)	Compromise Accounts (T1586)	Exploit Public Facing Application (T1190)	Container Adminsitration Command (T1609)	BITS Jobs (T1197)	Access Token Manipulation (T1134)	Access Token Manipulation (T1134)
Gather Victim Identity Information (T1589)	Compromise Infrastructure (T1584)	External Remote Services (T1133)	Deploy Container (T1610)	Boot or Logon Autstart Execution (T1547)	Boot or Logon Autostart Execution (T1547)	BITS Jobs (T1197)
Gather Victim Network Information (T1590)	Develop Capabilities (1587)	Hardware Addtions (T1200)	Exploitation for Client Execution (T1203)	Boot or Logon Initialization Scritps (T1037)	Boot or Logon Initialization Scritps (T1037)	Build Image on Host (1612)
Gather Victim Org Information (T1591)	Establish Accounts (T1585)	Phishing (T1566)	Inter-Process Communication (T1559)	Broswer Extensions (T1176)	Create or Modify System Process (T1543)	Deobfuscate/Decode Files or Information (T1140)
Phishing for Information (T1598)	Obtain Capabilities (T1588)	Replication Through Removable Media (T1091)	Native API (T1106)	Compromise Client Software Binary (T1554)	Escape to Host (T1611)	Deploy Containter (T1610)
Search Closed Sources (T1597)	Stage Capabilities (T1608)	Supply Chain Compromise (T1195)	Scheduled Task/Job (T1053)	Create Account (T1136)	Event Triggered Execution (T1546)	Direct Volume Access (T1006)
Search Open Techical Database (T1596)	Supply Chain Compromse (CM1162)	Trusted Relationship (T1199)	Shared Modules (T1129)	Create or Modify System Process (T1543)	Exploitation for Privilege Escalation (T1068)	Execution Guardrails (T1480)
Search Open Websites or Domains (T1593)		Valid Accounts (T1078)	Software Deployment Tools (T1072)	Event Triggered Execution (T1546)	Group Policy Modification (T1484)	Exploitation for Defense Evasion (T1211)
Search Victim-Owned Websites (T1594)			System Services (T1569)	External Remote Services (T1133)	Hijack Execution Flow (T1574)	File and Director Permissions Modification (T1222)
			Windows Management Instrustmentation (T1047)	Hijack Execution Flow (T1574)	Process Injection (T1055)	Group Policy Modification (T1484)
				Implant Container Image (T1525)	Scheduled Task/Job (T1053)	Hide Artifacts (T1564)
				Office Application Startup (T1137)	Valid Accounts (T1078)	Hijack Execution Flow (T1574)
				Pre-OS Boot (T1542)		Impair Defenses (T1562)
				Scheduled Task/Job (T1053)		Indicator Removal on Host (T1070)
				Server Software Component (T1505)		Indirect Command Execution (T1202)
				Traffic Signaling (T1205)		Masquerading (T1036)
				Valid Accounts (T1078)		Modify Authentication Process (T1556)
						Modify Cloud Compute Infrastructure (T1578)
						Modify Registry (T1112)
						Modify System Image (T1601)
						Network Boundary Bridging (T1599)
						Obfuscated Files of Information (T1027)
						Pre-OS Boot (T1542)
						Process Injection (T1055)
						Rogue Domain Controller (T1207)
						Rootkit (T1014)
						Signed Binary Proxy Execution (T1218)
						Signed Script Proxy Execution (T1216)
						Subvert Trust Controls (T1533)
						Template Injection (T1221)
						Traffic Signaling (T1205)
						Trusted Developer Utilities Proxy Execution (T1127)
						Unused/Unsupported Cloud Regions (T1535)
						Use Alternate Authentication Material (T1550)
						Valid Accounts (T1078)
						Virtualization/Sandbox Evasion (T1497)
						Weak Encryption (T1600)
						XSL Script Processing (T1220)

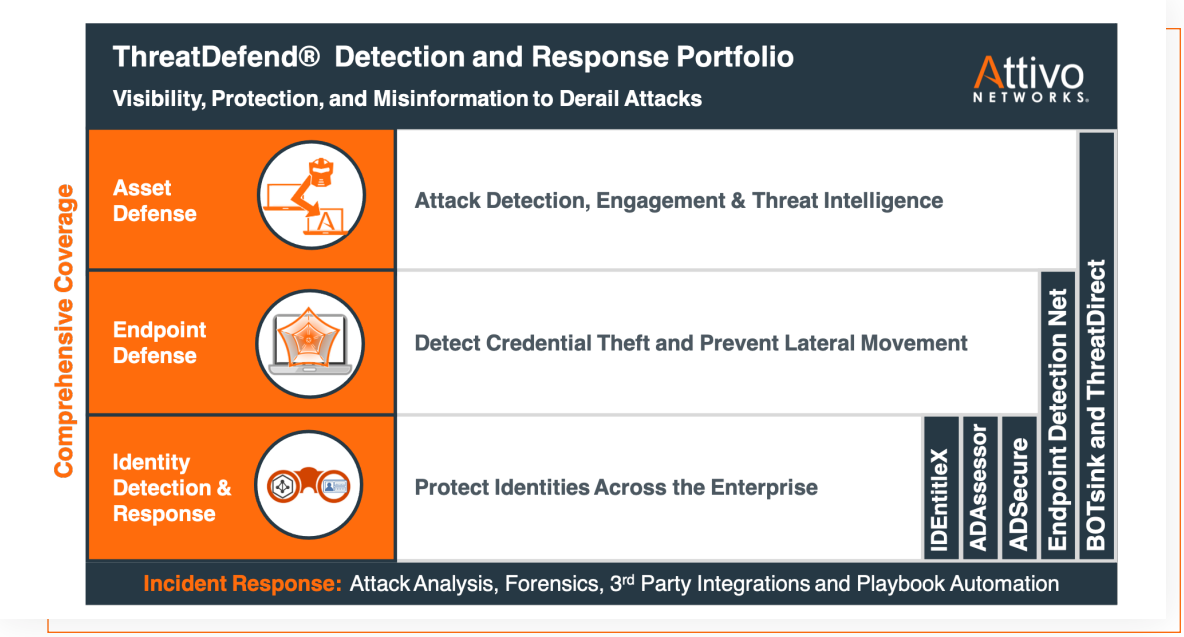
F-10 Credential Access	F-11 Discovery	F-12 Lateral Movement	F-13 Collection	F-14 Command and Control	F-15 Exfiltration	F-16 Impact
Brute Force (T1110)	Account Discovery (T1087)	Exploitation of Remote Services (T1210)	Archive Collected Data (T1560)	Application Layer Protocol (T1071)	Automated Exfiltration (T1020)	Account Access Removal (T1531)
Credentials from Password Stores (T1555)	Application Window Discovery (T1010)	Internal Spear-Phising (T1534)	Audio Capture (T1123)	Communication Through Removable Media (T1092)	Data Transfer Size Limits (T1030)	Data Destruction (T1485)
Exploitation for Crendential Access (T1212)	Browser Bookmark Discovery (T1217)	Lateral Trool Transfer (T1570)	Automated Collection (T1119)	Data Encoding (T1132)	Exfiltration Over Alternative Protocol (T1048)	Data Encrypted for Impact (T1486)
Forced Authentication (T1187)	Cloud Infrastructure Discovery (T1580)	Remote Service Session Hijacking (T1563)	Clipboard Data (T1115)	Data Obfuscation (T1001)	Exfiltration Over C2 Channel (T1041)	Data Manipulation (T1565)
Input Capture (T1056)	Cloud Service Dashboard (T1538)	Remote Services (T1021)	Data from Cloud Storage Object (T1530)	Dynamic Resolution (T1568)	Exfiltration Over Other Network Medium (T1011)	Defacement (T1491)
Man-in-the-Middle (T1557)	Cloud Service Discovery (T1526)	Replication Through Removable Media (T1091)	Data from Configuration Repository (T1602)	Encrypted Channel (T1573)	Exfiltration over Physical Medium (T1052)	Disk Wipe (T1561)
Modify Authentication Process (T1556)	Container and Resource Discovery (T1613)	Software Deployment Tools (T1072)	Data from Information Repositories (T1213)	Fallback Channels (T1008)	Exfiltration Over Web Service (T1567)	Endpoint Denial of Service (T1499)
Network Sniffing (T1040)	Domain Trust Discovery (T1482)	Taint Shared Content (T1080)	Data from Local System (T1005)	Ingress Tool Transfer (T1105)	Scheduled Transfer (T1029)	Firmware Corruption (T1495)
OS Credential Dumping (T1003)	File and Directory Discovery (T1083)	Use Alternate Authentication Material (T1550)	Data from Shared Network Drive (T1039)	Multi-Stage Channels (T1104)	Transfer Data to Cloud Account (T1537)	Inhibit System Recovery (T1490)
Steal Application Access Token (T1528)	Network Service Scanning (T1046)		Data from Removable Media (T1025)	Non-Application Layer Protocol (T1095)		Network Denial of Service (T1498)
Steal of Forge Kerberos Tickets (T1558)	Network Share Discovery (T1135)		Data Staged (T1074)	Non-Standard Port (T1571)		Resource Hijacking (T1496)
Steal Web Session Cookie (T1539)	Network Sniffing (T1040)		Email Collection (T1114)	Proxy (T1090)		Service Stop (T1489)
Two-Factor Authentication Interception (T1111)	Password Policy Discovery (T1201)		Input Capture (T1056)	Remote Access Software (T1219)		System Shutdown/Reboot (T1529)
Unsecured Credentials (T1552)	Peripheral Device Discovery (T1120)		Man-in-the-Browser (T1185)	Traffic Signaling (T1205)		
	Permission Group Discovery (T1069)		Man-in-the-Middle (T1557)	Web Service (T1102)		
	Process Discovery (T1057)		Screen Capture (T1113)			
	Query Registry (T1012)		Video Capture (T1125)			
	Remote System Discovery (T1018)					
	Software Discovery (T1518)					
	System Information Discovery (T1082)					
	System Local Discovery (T1614)					
	System Network Configuration Discovery (T1016)					
	System Network Connections Discovery (T1049)					
	System Owner/User Discovery (T1033)					
	System Service Discovery (T1007)					
	System Time Discovery (T1124)					

SUMMARY

The capabilities of deception and concealment technology to meet the requirements outlined in NIST publications 800-160 Volume 2 and 800-172 indicate that these new solutions can provide a high level of security to any organization.

These technologies improve security by making an attacker's mission more difficult, expensive, and time-consuming. Deception and concealment technology changes the asymmetry and economics of system compromise regardless of the type of attack, target, methodology, or source. Deception and concealment techniques are also effective against both organic and automated attack tools.

The ThreatDefend platform from Attivo Networks gives an organization a comprehensive set of tools that enables compliance with the NIST guidelines while improving their overall security posture and improving their incident response team's efficiency and effectiveness.



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