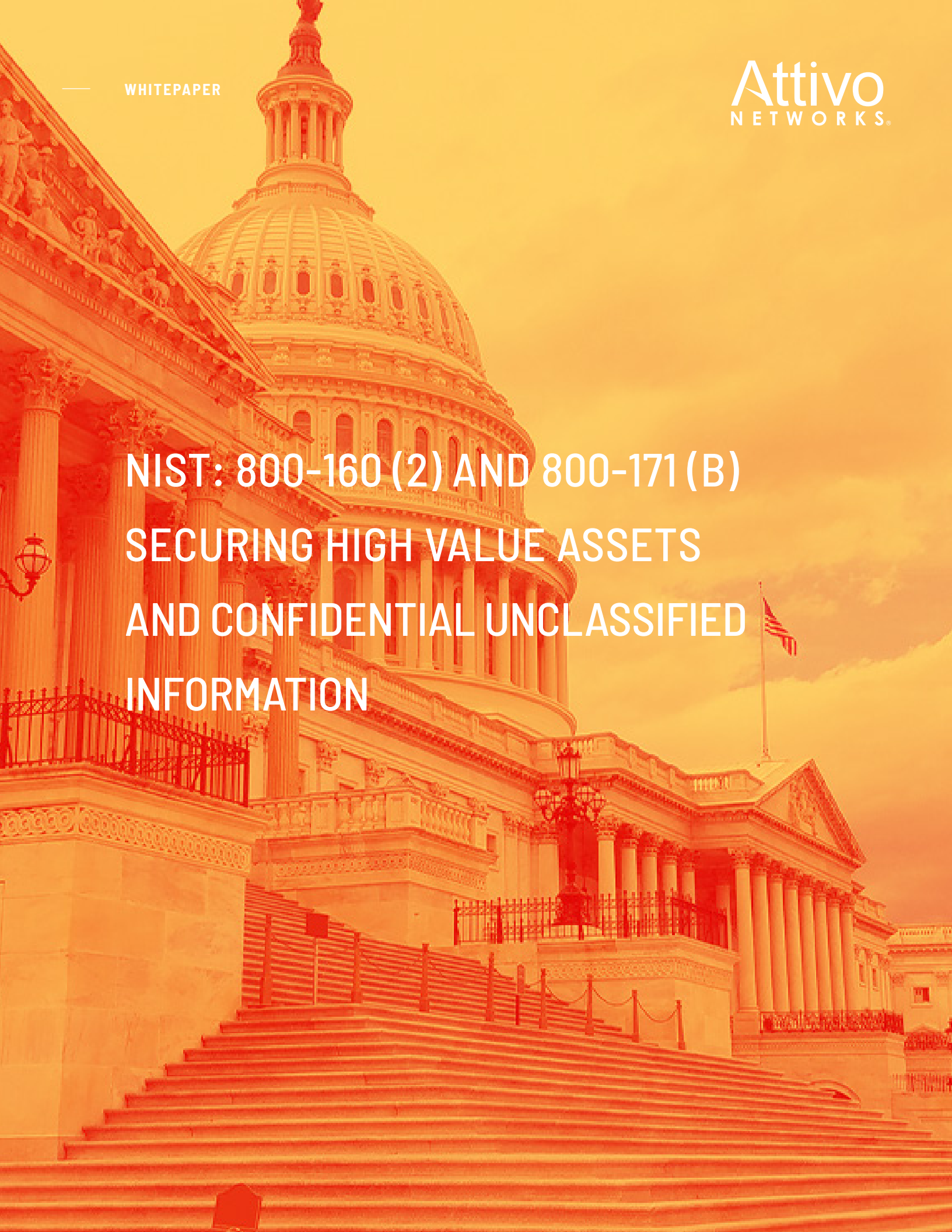
WHITEPAPER

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 800-171[2] deal with developing cyber-resilient systems and protecting controlled unclassified information in nonfederal 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 will very briefly summarize these NIST publications, introduce deception technology, and show how deception technology fits within the NIST guidelines to support regulatory compliance and enhanced security.

NIST 800-160V2 AND NIST 800-171

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's emphases are on 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 800-171 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 800-171 is a subset of requirements defined in NIST 800-53 and applies specifically to CUI that is shared by the

1 https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft-fpd.pdf

2 https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-draft-ipd.pdf

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

federal government with a non-federal organization or entity. The controls are designed to protect this information on non-federal systems from unauthorized disclosure.

Providing a detailed analysis of these NIST documents is beyond the scope of this paper. However, both documents make extensive reference to 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 level of maturity needed for NIST recognition as an effective and recommended security control.

INTRODUCTION TO DECEPTION

Generations have used Deception techniques in hunting, gaming, law enforcement, and the military domains for years. For example, deception played a crucial part in the largest military operation in history[4] . The introduction of deception technology into Defensive Cyber Operations (DCO) changes the status quo in cybersecurity from one of asymmetry in favor of the attacker to one that favors the defender. Cyber deception strategies utilize decoy assets (networked servers and hosts, IoT devices, routers/switches, POS terminals, etc.), as well as breadcrumbs, and lures (deceptive artifacts that reside on real production endpoints). Deceptive assets placed throughout the network 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 which time they have already revealed themselves.

Modern deception evolved from earlier "honeypot" efforts but has matured into a reliable and easy-to-manage system that scales to the enterprise and provides reliable high-fidelity indications of attacker activity. Original honeypot systems were designed and deployed primarily for research and placed on the network's edge, requiring a great deal of technical skill and administrative effort to use. Modern deception technology suites are designed to be easy to manage at scale and easy to deploy, and also differ in purpose.

Research honeypots frequently deployed outside the production environment. They were easy for an attacker to see and access and provided insight into external scanning and exploit activity targeted at the organization. They served a similar purpose when used within the environment but could become a springboard for an attacker who managed to breach the tool. Although sometimes still deployed in the DMZ or perimeter, modern deception systems are now enhanced so they can reliably detect and derail threats that are inside the network. Additionally, advanced architectures now direct an attacker into a sandboxed deception environment, removing the danger of the decoy itself becoming a pivot point or risk.

Deceptive defenses range between network- and host-based decoys and other deceptive assets, such as decoy file shares, serverless functions, and similar objects. On the network, deception technology provides decoy computing hosts (server, workstation) and networked devices (IoT, medical, IoT, ICS, telecom, networking, POS, etc.) that accurately reflect the production network environment. These decoys are indistinguishable from production assets, and a live attacker or automated process will not be able to determine the true nature of the deceptive assets without taking a closer look. Any active effort to observe these devices or gain access is immediately detected, sending a high-fidelity alert to the incident response team.

4 https://www.pbs.org/show/ghost-army/

To provide defense on the endpoints, deception solutions place deceptive assets in the form of false credentials for domain and website logins, hidden file shares mapped to decoy servers, and a range of other deceptive breadcrumbs and lures (serverless functions, keys, buckets, etc.)that deflect an attacker away from the production environment into the deception environment for monitoring and containment.

These endpoint deceptions are effective against both live attackers and their automated tools. For example, threat actors frequently try and glean credentials from the system they've initially breached to raise their privileges and move across the network. Domain controllers are a high-value target which, if compromised, give an attacker "the keys to the kingdom." Gaining access to a domain controller through stolen credentials is a common attack vector. In contrast, deceptive credentials will lead an adversary to a decoy domain controller, deflecting the attacker away from the real target.

Similarly, when an attacker uses a compromised host to query Active Directory for admin accounts or other intelligence, a host-resident deception solution can intercept the communication, hide real information, and return false account identities and relationships. This deception further confuses their perception of the environment, and because they can no longer trust their tools, their task becomes more complex, and they are more likely to make critical mistakes.

Endpoint deception is equally effective against an attacker's automated tools and hostile malware. For example, a ransomware attack that encrypts or destroys files on network shares would engage with the deception shares[5] , 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.

In addition to deflecting reconnaissance, credential, AD queries, and man-in-the-middle attacks, modern deception systems can also defend against attacks on unused ports and services by deflecting scans or connection attempts and responding to an attacker realistically while alerting the cybersecurity team to the event.

In total, deception technology makes an attacker's job much more complex and can gather 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 has proven to be a unique resource for leveling the playing field in favor of cyber defenders who are typically at a significant disadvantage.

USING DECEPTION TO MEET NIST 800-160 AND 800-171 REQUIREMENTS

NIST 800-160 Volume 2 mentions deception multiple times, focusing on its use in against adversarial threats while defining four areas of deception:

- Obfuscation
- Disinformation
- Misdirection
- Tainting

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

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. Both host and endpoint deceptions serve to obscure the apparent threat surface by vastly expanding how it would appear to a threat actor. An attacker 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 useful defensive tactic, especially when paired with the ability to intercept attacks and feed the attacker disinformation that will further derail their efforts.

"Disinformation" in this context refers to providing deliberately 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, by intercepting efforts to enumerate directory controllers, and by 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, where it creates and maintains a comprehensive set of decoy systems (computers, IoT, telecom, SCADA, etc.) that are indistinguishable from other assets in the production environment. These capabilities are closely interrelated to disinformation functions, which serve to lead a threat actor away from the production assets into the deception environment.

Finally, "Tainting" involves embedding covert capabilities into resources. In this context, it relates to activities that integrate 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, for example. 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[6] information for context. 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 gives an organization the ability 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.

Where NIST 800-160 deals with systems engineering, NIST 800-171 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 800-171B 3.13.3e specially

deals with employing "technical and procedural means to confuse and mislead adversaries through a combination of misdirecting, tainting, or disinformation[7]."

---

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

7 https://csrc.nist.gov/CSRC/media/Publications/sp/800-171b/draft/documents/sp800-171B-draft-ipd.pdf#page=79&zoom=100,0,400

This document describes the same methods and goals for deception detailed in NIST 800-160 Volume 2 and 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 laid out in both publications.

SUMMARY

The inclusion of deception technology in NIST publications 800-160 Volume 2 and 800-171B as a recommended addition to an organization's security stack indicate that deception has achieved a high level of maturity and acceptance.

These documents recognize several fields of deception and outline how it should be deployed into an organization's security stack to improve their security by making an attacker's mission more difficult, expensive, and time-consuming. Deception changes the asymmetry and economics of system compromise regardless of the type of attack, target, methodology, or source. Deception 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®, 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 offers comprehensive and accurate threat detection for user networks, data centers, clouds, and a wide variety of specialized attack surfaces. A deception fabric of network, endpoint, application, and data deceptions efficiently misdirect and reveal attacks from all threat vectors. Advanced machine-learning simplifies deployment and operations for organizations of all sizes. Automated attack analysis, forensics, actionable alerts, and native integrations accelerate and streamline incident response. The company has won over 100 awards for its technology innovation and leadership.

www.attivonetworks.com