D3B3sh>5!>>o

Acalvio and NIST SP 800-171B:

Raising the Bar for Effective APT Detection and Deception

July 2019

Background: The Never-Ending Battle Against Advanced Persistent Threats

The US government is engaged in a constant battle against well-funded, motivated attackers. The "front line" in this battle extends well beyond government networks: sensitive data is broadly distributed in private organizations such as defense contractors and service providers. To help guide such organizations on how to protect this data, NIST publishes a document known as SP 800-171, which lists security controls that should be implemented in private organizations that transact with the federal government.

While 800-171 provides an adequate security baseline in many situations, NIST recognized that a higher level of security is required to defend against advanced persistent threats (APTs). APTs are sophisticated, persistent attacks designed to exfiltrate information or compromise a mission. They are commonly employed by more capable adversaries, including nation state actors. Therefore, in mid-2019 NIST published a draft of a new security standard: SP 800-171B, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations". The goal of 800-171B is to recommend enhanced security controls to protect particularly sensitive data (Controlled Unclassified Information, or CUI) against APTs. The draft is expected to be finalized in 2020. The new standard does not replace 800-171, but rather builds upon it with additional precautions to be taken by non-federal organizations:

Highlights

- NIST SP 800-171B mandates robust security controls to defend against Advanced Persistent Threats.
- 800-171B applies to the government's sensitive data in non-federal systems, but is relevant for all types of organizations.
- Acalvio ShadowPlex supports eight controls across four control families across the 800-171B standard.
- ShadowPlex is ideally suited to provide the Deception requirement (3.13.3e) in 800-171B
- Acalvio meets the 800-171B requirements in a more cost-effective and operationally efficient manner than alternative approaches.

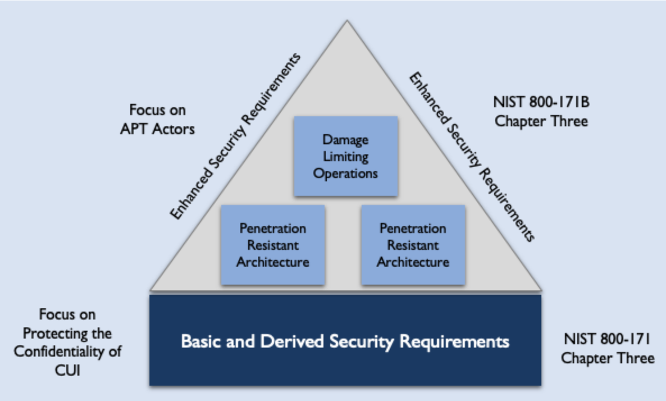

Focus on APT Actors
Enhanced Security Requirements
Damage Limiting Operations
Enhanced Security Requirements
NIST 800-171B Chapter Three
Penetration Resistant Architecture
Penetration Resistant Architecture
Focus on Protecting the Confidentiality of CUI
Basic and Derived Security Requirements
NIST 800-171 Chapter Three

Figure 1. 800-171B builds upon the basic requirements in 800-171 to protect sensitive data and systems from APT actors.

While the official scope of 800-171B is CUI held by private organizations, the recommendations in the document are completely relevant for any company concerned about APTs:

> *"Everyone has high value assets, from small businesses to Fortune 500 companies. These enhanced defenses are great tools for anyone to use. We do our jobs primarily for the federal government, but everyone gets to take advantage of NIST's cybersecurity guidance."*
>
> ***Ron Ross, 800-171B contributor, NIST***

Increasingly, organizations are leveraging federal government security standards to provide frameworks for cybersecurity, even though the organization is not in-scope for compliance. This trend reflects the reality that the federal government has to deal with the most sophisticated attackers, and so the thought is "If it's good enough for them, it's certainly good enough for my organization." The NIST Cybersecurity Framework (CSF) is the best example, and we expect a similar trend for SP 800-171B, as more and more companies come under attack from APTs.

800-171B: Getting Serious About APTs

Successfully countering APTs is not easy: the adversary has both the time and sophistication to probe defenses for months, slowly and methodically recon the internal environment, and progress along the cyber kill chain at a pace designed to go unnoticed. Therefore, 800-171B includes 32 controls across 10 control families, which should be implemented in addition to the baseline of 800-171.

Families	
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Figure 2. 800-171B adds 32 controls across 10 of the 14 control families in 800-171

A major emphasis of the standard is establishing staff, process, and technical controls to support ongoing cybersecurity intelligence and monitoring. "Defense in depth" protections are just the starting point. The assumption must be made that attackers will breach defenses and establish a foothold on the internal network.

> *"This strategy recognizes that despite the best protection measures implemented by organizations, the APT may find ways to breach those primary boundary defenses and deploy malicious code within a defender's system. When this situation occurs, organizations must have access to additional safeguards and countermeasures to confuse, deceive, mislead, and impede the adversary—that is, taking away the adversary's tactical advantage and protecting and preserving the organization's critical programs and high value assets."*
>
> ***NIST 800-171B***

Acalvio and SP 800-171B: A Deception Match Made in Heaven

Acalvio was founded on the premise that perimeter defenses are inadequate against determined attackers, and therefore additional measures are required to detect and retard attacks inside the network. This is exactly the same paradigm as that taken in SP 800-171B, which is why Acalvio's support for the standard is so strong. At the most fundamental level, Acalvio strives to provide three key security controls:

- Detection of an attack, post initial breach;
- Intelligence gathering on attackers tactics, techniques, and procedures (TTP);
- Impeding the attack by obfuscation and deception

The tight alignment between ShadowPlex and SP 800-171B is most obvious in the standard's controls 3.11.2e and 3.13.3e, which spell out the need for detection and deception:

> *"Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls",*
>
> ***NIST 800-171B Requirement 3.11.2e.***

> *"Employ technical and procedural means to confuse and mislead adversaries through a combination of misdirection, tainting, or disinformation. ",*
>
> ***NIST 800-171B Requirement 3.13.3e.***

It is important to note that the standard goes well beyond the rather obvious need to be able to detect and track APTs. It also mandates active measures to delay and disrupt them. Why is this so important? Because NIST understands that once an attacker is on the inside, they can embed themselves broadly and deeply in the environment. Simple attempts to clean up infected laptops will not be sufficient because of the depth of attack penetration. Furthermore, response measures that tip the defender's hand make the problem worse: The adversary will know he's been detected and will take new measures to slow his attack and wait for a better opportunity to proceed. Clumsy responses that drive the attacker to "go deep" also limits the opportunity to monitor the attacker's methods to gain valuable intelligence on his methods and internal footprint. Instead, the superior methodology is to slow the attacker's progression, to allow time to really understand who he is, what he's doing, what his goals are, and what it would take to eradicate him from the environment. In summary, truly effective APT defenses require a totally different level of defender sophistication than what most organizations do today.

Acalvio ShadowPlex is a strong choice to support 800-171B controls, because the capabilities of the solution tightly match the requirements in the NIST standard with respect to detection, obfuscation, and disruption. In total, ShadowPlex supports eight controls across four control families in 800-171B, as detailed at the end of this Solution Brief. It must be noted that NIST specifically recommends deception, rather than specifying the desired results from deceptive actions and leaving it to the organization to decide how to implement the control activity. It is likely that NIST took this step because they wanted to be very specific on the type of controls they felt were necessary to be successful.

SP800-171B and Operational Efficiency: The Acalvio Advantage

Countering APTs is not easy, which suggests it won't be inexpensive either. Investments are required in staffing and tools well beyond typical security controls. However ShadowPlex was designed to be operationally efficient as well effective, bringing advanced APT defenses within reach of a wide range of organizations. The ShadowPlex operational advantage manifests itself in many technical aspects:

- Low False Positives – Highly accurate deception based detection is far more accurate than behavior analytics approaches, drastically reducing resources wasted on spurious alerts;
- AI-Driven Deployment - Automated analysis of production environment drives efficient creation and deployment of high-credibility deception assets (decoys, lures, and breadcrumbs);
- Deception Farms - Centralized decoy farm with projection across the environment reduces the overhead associated with high-scale deployments;
- Fluid Deception - Just-in-time decoy creation minimizes resource and license costs;
- Dynamic Deception – Continuously monitors the environment, adjusts deception assets to maintain credibility

In addition to these advantages, 800-171B itself suggests the operational efficiency of deception. Control 3.13.3e is written to encourage the use of deception, as is made clear in the first sentence of the supporting discussion:

Deception is used to confuse and mislead adversaries regarding the information the adversaries use for decision making; the value and authenticity of the information the adversaries attempt to exfiltrate; or the environment in which the adversaries desire to operate. NIST SP 800-171B

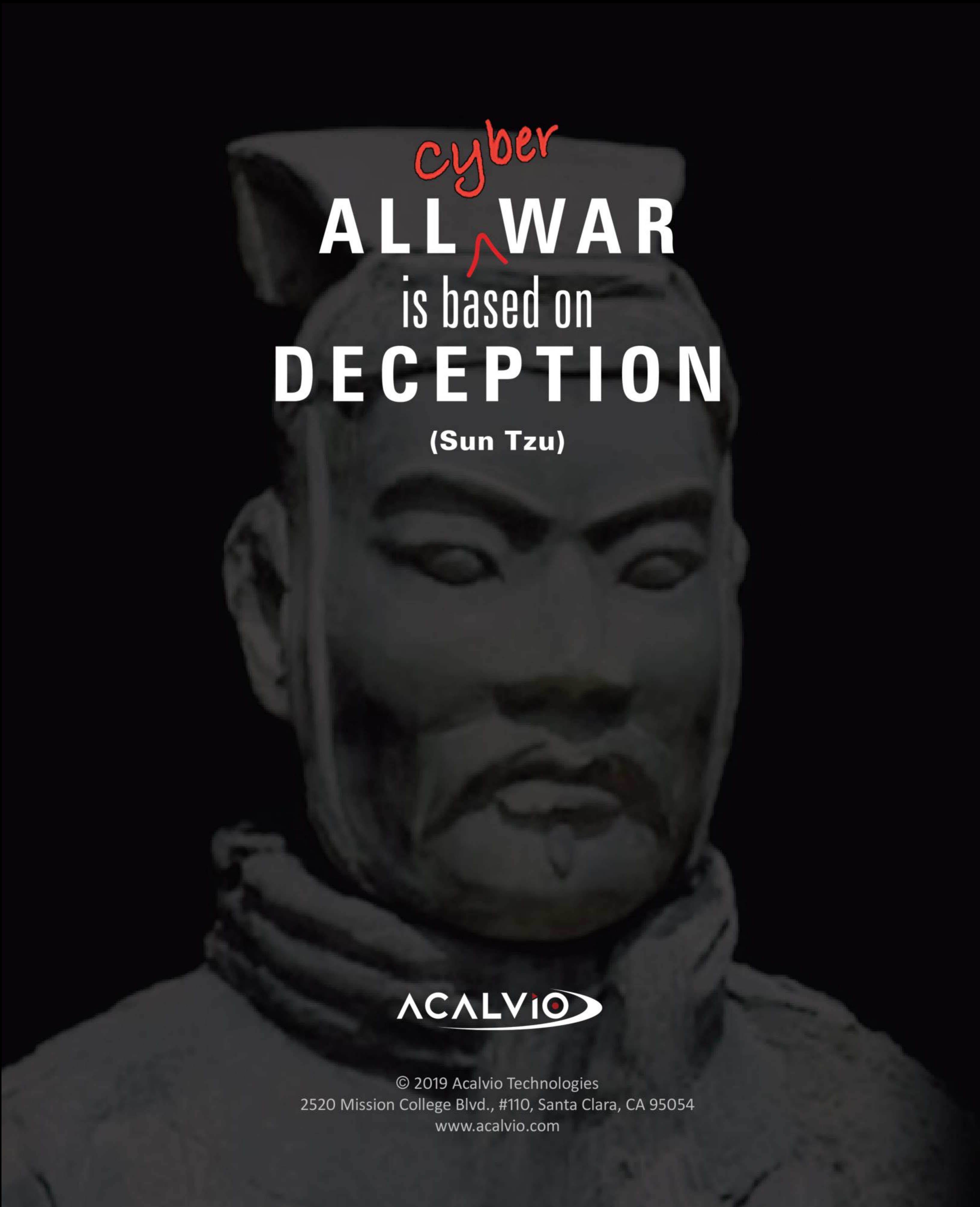
Note that the discussion of this control is centered on impeding the attacker, and not on detection. But if an organization is going to implement a deception solution to meet 3.13.3e, they might as well also leverage it for detection, as required by the preceding control: 3.11.2e. Put another way, only deception can be realistically used to support both controls, making it the most operationally efficient option for meeting the intent of the standard.

Acalvio ShadowPlex: NIST SP800-171B Support Matrix, Including 800-53 Mappings*

800-171B Section	Control Requirement	Acalvio Support	NIST 800-53 Supporting Controls
3.2.2e	Include practical exercises in awareness training that are aligned with current threat scenarios and provide feedback to individuals involved in the training and their supervisors.	The most effective practical exercises are those based on actual attacker TTPs. Acalvio ShadowPlex provides the captured TTPs from real attacks, the ability to quickly build detailed network neighborhoods of decoys using playbooks for the exercises and provides comprehensive information on the activity, to inform effective training for SOC, CIRT, and threat hunting teams.	AT-2(1), AT-2(8)
3.11.2e	Establish and maintain a cyber threat hunting capability to search for indicators of compromise in organizational systems and detect, track, and disrupt threats that evade existing controls.	ShadowPlex enables threat hunting on internal networks by generating IoCs for all deception incidents and by detecting, tracking and containing threats.	RA-10, SI-4(24)
3.11.3e	Employ advanced automation and analytics capabilities to predict and identify risks to organizations, systems, or system components.	ShadowPlex automates risk identification and produces high fidelity alerts to address the intent of this control to avoid SOC information overload. Shadow Network supports deep, continuous attacker engagement.	RA-3(4), SI-4(24)
3.13.1e	Employ diverse system components to reduce the extent of malicious code propagation.	ShadowPlex uses a combination of decoys, breadcrumbs, and baits to identify malicious code. With 60+ decoy types and 30+ breadcrumb types out of the box, ShadowPlex leverages a diverse set of systems and breadcrumbs. ShadowPlex also integrates with a variety of other security software to automatically contain any system identified as compromised.	PL-8, SA-17(9), SC-27, SC-29, SC-29(1), SC-47
3.13.3e	Employ technical and procedural means to confuse and mislead adversaries through a combination of misdirection, tainting, or disinformation.	Deception is ideally suited to confuse and mislead adversaries away from the enterprise network and to decoys. A variety of breadcrumbs can be placed on different types of endpoints (Windows, Linux, MacOS etc), which provide an alternate	SC-8(4), SC-26, SC-30, SC, 30(2), SI-20

800-171B Section	Control Requirement	Acalvio Support	NIST 800-53 Supporting Controls
		reality for the adversary to engage with.	
3.14.2e	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	ShadowPlex monitors systems for anomalous behavior that indicated compromise.	AU-6(6), SI-4(4), SI-4(7), SI-4(11), SI-4(13), SI-4(18), SI-4(19), SI-4(20)
3.14.3e	Ensure that Internet of Things (IoT), Operational Technology (OT), and Industrial Internet of Things (IIoT) systems, components, and devices are compliant with the security requirements imposed on organizational systems or are isolated in purpose-specific networks.	ShadowPlex Service Reflection creates decoys based on specialized hardware such as IoT devices, enabling deception without the need to instrument the IoT devices themselves	AC-3, AC-4, SA-8, SC-2, SC-3, SC-49
3.14.6e	Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	ShadowPlex delivers broad threat indicator information that reflects the actual environment, creating actionable intelligence for detection and hunting teams.	PM-16(1), SI-4(24), SI-5

*: The authors of SP 800-171B used the SP 800-53 standard as source material to derive the controls for APT protections, and are reproduced here for reference.



ALL cyber WAR is based on DECEPTION

(Sun Tzu)

ACALVIO

2520 Mission College Blvd., #110, Santa Clara, CA 95054
www.acalvio.com