THE SEPIO PLATFORM: ENHANCING HARDWARE SECURITY FOR THE US ARMY SECURITY OPERATIONS CENTER

INTRODUCTION

The US Army Security Operations Center (SOC) faces a complex and evolving threat landscape, tasked with safeguarding critical national security assets and information in an increasingly interconnected and digital world. While traditional cybersecurity measures focus on software and network layers, a significant and often overlooked vulnerability exists at the hardware level. This white paper explores how the Sepio Platform, a leading asset visibility solution, directly addresses these critical hardware security gaps, providing zero-trust visibility and control, essential for protecting Army operations and maintaining compliance.

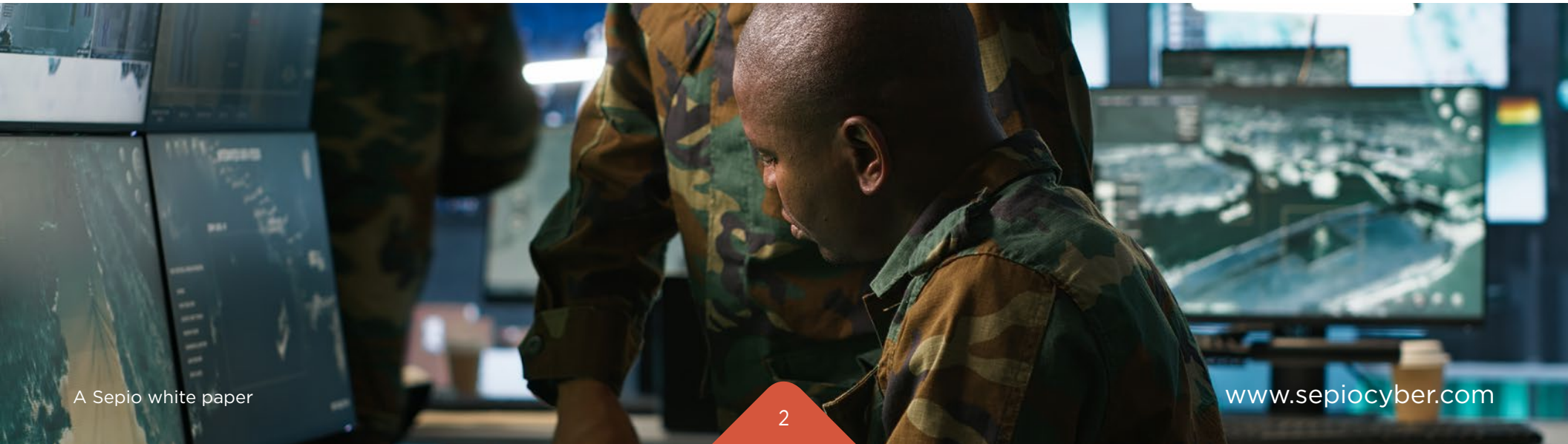
CHALLENGES FACED BY THE US ARMY SOC

US Army SOCs, like other critical infrastructure and government entities, contend with a unique set of challenges that hardware-level security can uniquely address:

- **Advanced Persistent Threats (APTs):** Government agencies are primary targets for sophisticated, state-sponsored APTs aimed at espionage or sabotage, which can persist undetected for long periods. Such attacks often leverage hidden hardware.

WHILE TRADITIONAL CYBERSECURITY MEASURES FOCUS ON SOFTWARE AND NETWORK LAYERS, A SIGNIFICANT AND OFTEN OVERLOOKED VULNERABILITY EXISTS AT THE HARDWARE LEVEL

- **Supply Chain Vulnerabilities:** The global supply chain introduces significant risks, including counterfeit hardware, unauthorized modifications, and embedded malicious components from original equipment manufacturers (OEMs). Regulations like NDAA Section 889 specifically prohibit the use of equipment from certain foreign manufacturers, requiring frequent validation of hardware origin and integrity.
- **Proliferation of IT, OT, and IoT Devices:** Modern military operations extensively integrate IT (Information Technology), OT (Operational Technology), and IoT (Internet of Things) devices, including Industrial IoT (IIoT). This convergence expands the attack surface significantly, as many of these devices, particularly older OT systems, were not designed with robust cybersecurity in mind and lack sufficient security features.



- **Physical Layer ("Layer 1") Blind Spots:** Existing security solutions, such as Network Access Control (NAC), Intrusion Detection Systems (IDS), Endpoint Protection Solutions (EPS), and IoT Network Security, operate at higher network layers (Layer 2 and above). This creates a critical "blind spot" at the physical layer, allowing undetectable hardware attacks to bypass security protocols.
- **Rogue Device Exploitation:** Malicious actors exploit this Layer 1 blind spot using Rogue Devices, hardware attack tools like spoofed USB peripherals (e.g., a mouse acting as a keyboard) or covert network implants. These devices appear as "trusted devices" to traditional security software or have no network presence (no IP/MAC address), enabling them to go completely undetected. This includes devices like Raspberry Pis, which are small, inexpensive, and can be configured to carry out malicious clandestine activities, often going unnoticed.
- **Insider Risk:** Whether through malicious intent or carelessness, employees can unwittingly or wittingly introduce vulnerabilities, including connecting compromised personal devices or rogue hardware, especially in Bring Your Own Device (BYOD) or remote work scenarios.
- **Compliance Requirements:** Adherence to cybersecurity frameworks like the Cybersecurity Maturity Model Certification (CMMC) and National Institute of Standards and Technology (NIST) require rigorous, continuous asset management and protection, spanning practices from basic cyber hygiene to advanced/proactive measures against APTs. Full visibility and risk identification of hardware assets is crucial for meeting these requirements.

THE SEPIO PLATFORM SOLUTION

The Sepio Platform, a leading asset visibility and risk management solution, provides a comprehensive answer to these challenges by focusing on the fundamental layer of hardware security. It enables SOC teams to achieve ultimate visibility and control over all hardware assets, ensuring no device goes unmanaged or undetected.

HERE'S HOW SEPIO PROVIDES CRITICAL CAPABILITIES FOR THE SOC:

› Zero-trust Physical Layer Visibility:

- Sepio is the only company in the world to undertake Physical Layer data source. It calculates a unique digital AssetDNA from the electrical characteristics and device descriptors of all connected peripherals and network devices.
- This capability provides true identity validation of devices, regardless of their claimed identity or traffic patterns. It addresses the fundamental "blind spot" that traditional security solutions miss and is the only hardware zero- trust solution on the market.

• Sepio detects network devices that do not emit traffic or network characteristics and might otherwise go unnoticed. Sepio's visibility ensures a complete inventory of all IT, OT, and IoT assets, managed or unmanaged.

› Robust Rogue Device Detection and Mitigation:

• By comparing a device's digital AssetDNA against a known set of malicious devices and utilizing Machine Learning to analyze device behavior for abnormalities (e.g., a mouse acting as a keyboard), Sepio can automatically detect and block attacks.

• Sepio's Asset DNA, derived from electronic characteristics, provides the unique ability to identify spoofed peripherals and hidden network implants that operate covertly above layer 1.

• Once a rogue or threatening device is detected, Sepio enforces predefined policies to automatically block it, preventing unauthorized access and mitigating threats in real-time.

› Enhanced Zero Trust Hardware Access (ZTHA):

• Sepio integrates with and strengthens existing Zero Trust Architectures by extending the "never trust, always verify" principle to the hardware level.

• It allows SOC teams to implement strict or granular hardware access control rules based on a device's true characteristics and risk score. This prevents malicious devices from bypassing traditional identity-based authentication or micro-segmentation controls.

> Supply Chain Security and Compliance:

• By providing complete, real-time device visibility, Sepio enables SOCs to proactively identify and prevent supply chain intrusions. It can detect when a device has been manipulated or contains components from prohibited manufacturers, directly supporting NDAA Section 889 compliance.

• Sepio's comprehensive asset inventory and continuous monitoring also align with CMMC and NIST requirements for asset management, physical protection, and system integrity, providing crucial data for certification and ongoing adherence.

> Non-intrusive and Rapid Deployment:

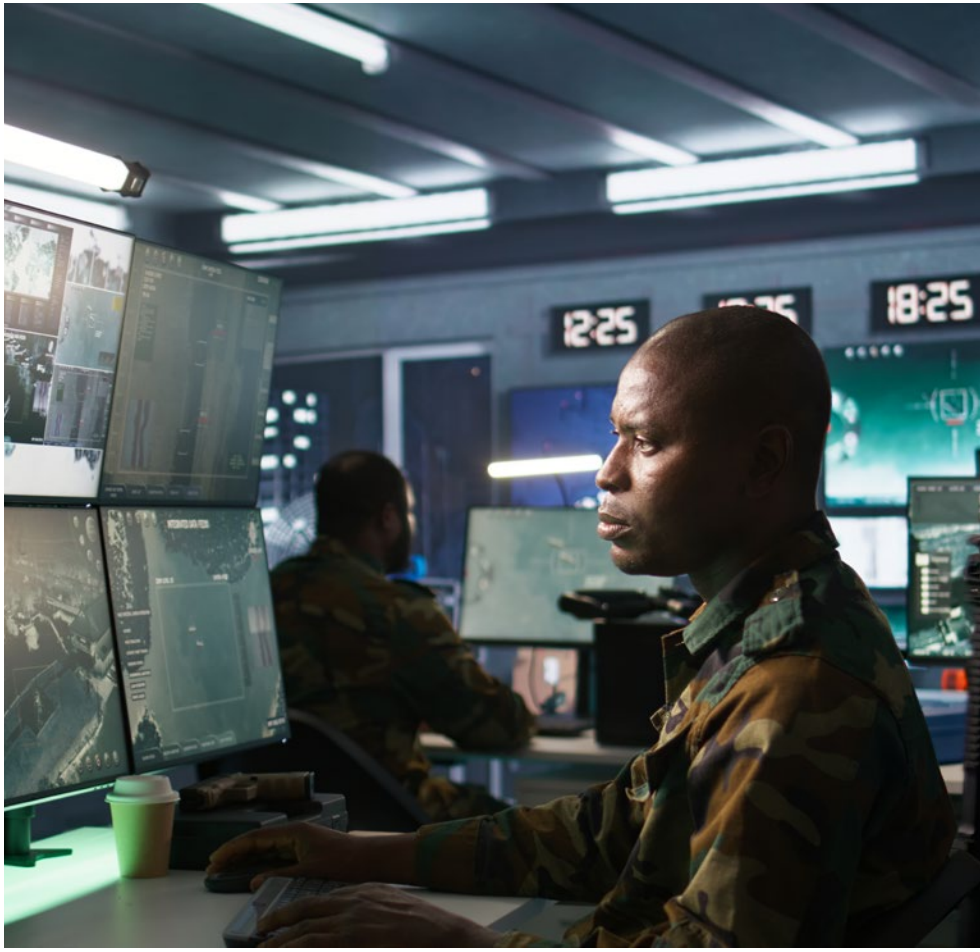
• The Sepio Platform does not monitor user traffic and requires only read-only SSH access to network switches, making it suitable for sensitive and operational environments like those found in sensitive environments.

• It can be deployed agentless or cloud-based (with optional on-prem components) and provides complete asset visibility within 24 hours, with no prior baselining or whitelisting required. This allows for immediate security enhancement without disrupting critical operations.

BENEFITS FOR THE US ARMY SOC

Implementing the Sepio Platform can provide several profound benefits for the US Army SOC:

- **Eliminates Hardware Blind Spots:** Gains 100% visibility into all hardware assets, including those previously invisible to traditional security tools.
- **Proactive Threat Mitigation:** Moves beyond reactive responses by automatically detecting and blocking rogue devices at the earliest point of entry—the physical layer—before they can cause damage or move laterally.
- **Strengthens Supply Chain Security:** Provides the crucial ability to verify the true identity and integrity of hardware acquired through complex supply chains, directly supporting NDAA Section 889 compliance and mitigating the risk of embedded malicious hardware.
- **Enhances Compliance Posture:** Directly aids in achieving and maintaining compliance with stringent regulations like CMMC, ensuring that all hardware assets are managed, monitored, and protected according to DoD standards.



- **Bolsters Zero Trust Architecture:** Provides the foundational hardware-level visibility and control necessary for a robust Zero Trust security model, ensuring that every device accessing the network is explicitly verified and appropriately privileged.
- **Protects Critical IT/OT/IoT Infrastructure:** Safeguards vital operational technologies and the growing number of IoT devices used in military environments from hardware-based attacks, preventing disruptions to critical functions.
- **Reduces Insider Risk:** Identifies unauthorized or compromised devices introduced by insiders, whether intentional or accidental, providing critical oversight into hardware access.

CONCLUSION

The dynamic nature of modern warfare and the increasing sophistication of cyber adversaries demand a security posture that accounts for every potential attack vector, including the often-overlooked hardware layer. The Sepio Platform offers a unique and essential capability for the US Army SOC by providing ultimate visibility and control over all hardware assets through its innovative Physical Layer AssetDNA and Machine Learning. By addressing blind spots and enabling robust Rogue Device Mitigation, Sepio not only strengthens an organization's overall cybersecurity posture but also ensures compliance with critical regulations, directly contributing to the security and operational resilience of the US Army.