netAlly®

How CyberScope® Supports (CIS®) Critical Security Controls®

Application Note

CIS Center for Internet Security® CIS Controls

How CyberScope® Supports (CIS®) Critical Security Controls®

INTRODUCTION

The edge network is an area of escalating challenges for organizations of all sizes —both from cybersecurity and visibility gap perspectives. Of course, cybersecurity breaches are an enterprise-wide threat, but the network perimeter is frequently ground-zero for many hackers, serving as the entry point into the environment. Why is this? Because the edge offers so many attack vectors:

- **Proliferation of endpoints**
- **Increased attack surfaces**
- **Ubiquitous connectivity**
- **Undetected vulnerabilities**
- **Unsecured connections**
- **Misconfigured networks**

"44% cite lack of visibility into all endpoints as the biggest challenges in data protection compliance[1]."

- IDG Connect Survey

THE IMPORTANCE OF SECURITY FRAMEWORKS

Given this, adopting the Center for Internet Security (CIS) Controls (or other security frameworks) is a must-have for a growing number of security teams for the following reasons:

- **Standardization:** These frameworks provide a standardized set of best practices and guidelines that help organizations ensure comprehensive security. This standardization simplifies the implementation of security measures and ensures consistency across the organization.
- **Risk Management:** Security frameworks help organizations identify, assess, and manage risks. By following established guidelines, organizations can better understand their vulnerabilities and take proactive measures to mitigate potential threats.
- **Compliance:** Many industries are subject to regulatory requirements that mandate specific security practices. Frameworks like CIS controls help organizations meet these legal and regulatory requirements, avoiding potential fines and legal repercussions.
- **Improved Security Posture:** Implementing a recognized security framework helps organizations build a robust security posture. This includes protecting against data breaches, cyber-attacks, and other security incidents, thus safeguarding sensitive information, and maintaining business continuity.
- **Resource Allocation:** Security frameworks provide a prioritized approach to security, helping organizations allocate resources effectively. By focusing on high-impact areas, organizations can maximize the effectiveness of their security efforts.
- **Benchmarking and Metrics:** These frameworks allow organizations to benchmark their security practices against industry standards and measure their progress over time. This benchmarking helps identify gaps and areas for improvement.

[1]Survey of IT decision-makers worldwide by IDG Connect

CyberScope
Vulnerability Scanner

- **Enhanced Trust:** Adhering to established security frameworks can enhance trust with customers, partners, and stakeholders. Demonstrating a commitment to security through the adoption of recognized frameworks can improve the organization's reputation and business relationships.
- I**ncident Response:** Security frameworks often include guidelines for incident response, helping organizations prepare for and respond to security incidents effectively. This preparation can minimize damage and facilitate a quicker recovery.
- **Continuous Improvement:** Security frameworks are typically updated regularly to address new threats and vulnerabilities. By following these frameworks, organizations can stay up to date with the latest security practices and continuously improve their security posture.
- **Interoperability:** Standardized security practices facilitate better interoperability with other organizations, especially in sectors that require collaboration and information sharing. This interoperability is essential for integrated security efforts and overall ecosystem protection.

In short, CIS controls and other security frameworks provide a structured and effective approach to managing cybersecurity risks, ensuring regulatory compliance, and protecting organizational assets.

SUMMARY OF CIS CONTROLS

A complete review of all the CIS Controls and associated safeguards are beyond the scope of this application note, but here is a list of the eighteen controls:

- **CIS Control 1** - Inventory and Control of Enterprise Assets
- **CIS Control 2 -** Inventory and Control of Software Assets
- **CIS Control 3** - Data Protection
- **CIS Control 4** - Secure Configuration of Enterprise Assets and Software
- **CIS Control 5** - Account Management
- **CIS Control 6** - Access Control Management
- **CIS Control 7** - Continuous Vulnerability Management
- **CIS Control 8** - Audit Log Management
- **CIS Control 9** - Email and Web Browser Protections
- **CIS Control 9** - Email and Web Browser Protections
- **CIS Control 10** - Malware Defenses
- **CIS Control 11** - Data Recovery
- **CIS Control 12** - Network Infrastructure Management
- **CIS Control 13** - Network Monitoring and Defense
- **CIS Control 14** - Security Awareness and Skills Training
- **CIS Control 15** - Service Provider Management
- **CIS Control 16** - Application Software Security
- **CIS Control 17** - Incident Response Management
- **CIS Control 18** - Penetration Testing

For more detailed information, we recommend checking out the Center for Internet Security® (CIS®) Controls website. Should your organization use another security framework, no worries. Simply click on relevant Safeguard on this website and it will display how it maps to other industry frameworks.

HOW CYBERSCOPE SUPPORTS CIS® CRITICAL SECURITY CONTROL INITIATIVES

One of the key advantages of CyberScope is its handheld form factor. By connecting directly to any perimeter physical port or AP, this "inside the edge" perspective often provides a much more comprehensive view of potential cybersecurity vulnerabilities. Compared with centralized cybersecurity solutions, this makes it uniquely positioned to map to critical **CIS controls and safeguards** at the network edge. Let's see where CyberScope can help:

CIS CONTROL 1 - INVENTORY AND CONTROL OF ENTERPRISE ASSETS		
Safeguard	**CyberScope Features**	**Description**
Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory	• Endpoint & Network Discovery • Wi-Fi Site Survey	Complete inventory of all connected endpoints, infrastructure elements, and their logical or physical location.
Safeguard 1.2: Address Unauthorized Assets	• Rogue AP & Wireless Client Locate • Wi-Fi and Bluetooth/BLE Site Survey • Authorized Device List	Enables a simple process to address unauthorized assets on a proactive basis.
Safeguard 1.3: Utilize an Active Discovery Tool	• Endpoint & Network Discovery • Wi-Fi Site Survey • Bluetooth/BLE Site Survey	Actively discovers wired and wireless assets, configurable to execute on an ongoing basis.
Safeguard 1.5: Use a Passive Asset Discovery Tool	• Wi-Fi Site Survey • Bluetooth/BLE Site Survey	Passively discovers Wi-Fi and BT/BLE endpoints, enables review and results to update asset inventory periodically.
CIS CONTROL 4 - SECURE CONFIGURATION OF ENTERPRISE ASSETS AND SOFTWARE		
Safeguard 4.6: Securely Manage Enterprise Assets and Software	• Automated Discovery Monitoring • Integration of Nmap into AutoTest & Network Discovery • Standalone Nmap App	Validate secure configurations, such as accessing administration interfaces over secure protocols only.
Safeguard 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software	• Automated Discovery Monitoring • Integration of Nmap into AutoTest & Network Discovery • Standalone Nmap App	Perform ongoing auditing of network assets to confirm no unauthorized software or assets are present on the network.
Safeguard 4.9: Configure Trusted DNS Servers on Enterprise Assets	• AutoTest: DNS Validation	Enables efficient and ongoing DNS testing; ensures no rogue DNS servers present.
CIS CONTROL 7 - CONTINUOUS VULNERABILITY MANAGEMENT		
Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets	• Integration of Nmap into AutoTest & Network Discovery • Standalone Nmap App	Complete vulnerability scans of internal enterprise assets as frequently as required.

HOW CYBERSCOPE SUPPORTS CIS® CRITICAL SECURITY CONTROL INITIATIVES - *continued*

CIS CONTROL 12 - NETWORK INFRASTRUCTURE MANAGEMENT		
Safeguard	**CyberScope Features**	**Description**
Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date	• Integration of Nmap into AutoTest & Network Discovery • Standalone Nmap App	Ensures infrastructure is running the latest, stable release of software, review on an ongoing basis.
Safeguard 12.2: Establish and Maintain a Secure Network Architecture	• Automated Network Topology Mapping via Link-Live • Wi-Fi Interference (DOS) Detection • AirWISE® Automated Wi-Fi Security Problem Detection • RF Spectrum Analysis • AutoTest: VLAN ID, Monitoring, Device Reachability • Ethernet Copper - 10/100 Mbps 1/2.5/5/10 Gbps • Ethernet Fiber - 1/10 Gbps • Wi-Fi Connection & Roaming Test • Wiremap & Toner – Cable • AirMapper™ Site Survey • Ping/TCP Connect Utility • iPerf Performance Test • Line Rate Performance Test (up to 10 Gbps)	Allows for validation of a secure network architecture and segmentation baseline, then identify subsequent possible deviations
Safeguard 12.3: Securely Manage Network Infrastructure	• Endpoint & Network Discovery • Automated Discovery Monitoring • Integration of Nmap into AutoTest & Network Discovery • Standalone Nmap App • Path Analysis	Confirm use of secure network protocols, such as SSH and HTTPS; no unauthorized devices or endpoints present.
Safeguard 12.4: Establish and Maintain Architecture Diagram(s)	• Automated Network Topology Mapping via Link-Live	Generate baseline network architecture diagrams, related documentation, create reports, capture, review, and document changes annually.
Safeguard 12.6: Use of Secure Network Management and Communication Protocols	• Discover SSID, AP, & Clients • AirWISE® Automated Wi-Fi Security Problem Detection	Validate on an ongoing basis the use of secure protocols such as 802.1X, WPA2 Enterprise or greater.

HOW CYBERSCOPE SUPPORTS CIS® CRITICAL SECURITY CONTROL INITIATIVES - *continued*

CIS CONTROL 13 - NETWORK MONITORING AND DEFENSE		
Safeguard	**CyberScope Features**	**Description**
Safeguard 13.4: Perform Traffic Filtering Between Network Segments	• Path Analysis • AutoTest: VLAN ID, Monitoring, Device Reachability	Perform network segmentation testing between VLANs to validate proper configuration
Safeguard 13.9: Deploy Port-Level Access Control	• Discover SSID, AP, & Clients • AirWISE® Automated Wi-Fi Security Problem Detection • Wi-Fi Connection & Roaming Test	Confirm ongoing port level access control utilizes 802.1x or related access control protocols.
CIS CONTROL 18 - PENETRATION TESTING		
Safeguard 18.4: Validate Security Measuress	• Automated Discovery Monitoring • Integration of Nmap into AutoTest & Network Discovery • Standalone Nmap App	Upon completion of penetration testing, validate recommended security measures are implemented.

SUMMARY

Because of its distinct design, formfactor and capabilities, CyberScope can aid your larger CIS Controls (and other security framework) initiatives, mapping to key controls and safeguards at the problematic edge network. In the process, CyberScope greatly strengthens your organizations security posture while increasing overall situational awareness at the network perimeter.