Sword & Shield
ENTERPRISE SECURITY

Back to Basics:
Basic CIS Controls

Chad Waddell | Enterprise Consultant

Center for Internet Security

https://www.cisecurity.org/

- Non-profit organization founded in 2000
- Employs closed crowdsourcing model to identify and refine effective security measures
- Members include large organizations, government agencies, and academic institutions

CIS Vision and Mission

The CIS Vision:

Leading the global community to secure our connected world.

The CIS Mission:

- Identify, develop, validate, promote, and sustain **best practice solutions** for cyber defense.
- **Build and lead communities** to enable an environment of trust in cyberspace.

CIS Controls

https://www.cisecurity.org/controls/

- Publication of **best practices guidelines** for computer security.
- Consists of **20 critical security controls** (CSC) that organizations should take to block or mitigate known attacks.
- **No-nonsense**, actionable recommendations for cybersecurity.
- Distributed as **widely and freely** as possible.

Mappings

NIST

PCI DSS COMPLIANT

Information Security Management System
ISO
27001
Certified

HIPAA

CIS Controls V7

CIS Controls™

V7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

CIS Controls

- Basic (CIS Controls 1-6): **Key controls** which should be implemented in every organization for essential cyber defense readiness.

- Foundational (CIS Controls 7-16): The next step up from basic – these **technical best practices** provide clear security benefits and are a smart move for any organization to implement.

- Organizational (CIS Controls 17-20): These controls are different in character from 1-16. While they have many technical elements, CIS Controls 17-20 are more focused on **people and processes** involved in cybersecurity.

Basics

Basic (CIS Controls 1-6)*

Key controls which should be implemented in every organization for essential cyber defense readiness.

*We won’t address every sub-control.

CIS Control 1

Inventory and Control of Hardware Assets

Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

Hardware Inventory

If you don’t know what you have you won’t be able to secure it!

What do you need to inventory?

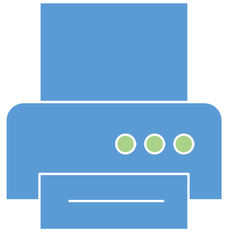
How do you create and maintain an inventory?

Hardware Inventory

What do you need to inventory?

Desktops

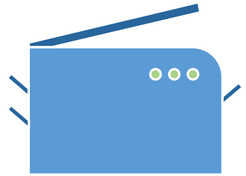
Switches



Printers

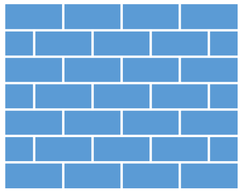
Laptops

Routers

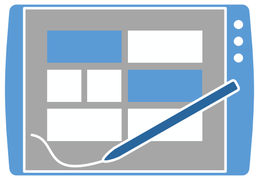


Copiers

SANs/NAS
Servers/VMs



Firewalls



Smartphones/
Tablets

Wireless
Access Points

Hardware Inventory

How do you create and maintain an inventory?

spiceworks

Lansweeper

ALIEN VAULT™

Open-AudIT
Opmantek
What's on your network?

CIS Control 2

Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Software Inventory

déjà vu?

If you don’t know what you have you won’t be able to secure it!

Scan hardware identified with CIS Control 1

What do you need to inventory?

How do you create and maintain an inventory?

Whitelist applications

Software Inventory (All Software!)

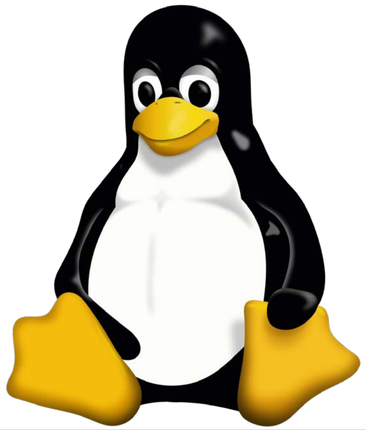
What do I need to inventory?

Operating Systems

Windows 10

Windows Server 2016

macOS



Windows 7

Applications

Office

Java

Hardware Inventory

How do you create and maintain an inventory?

CIS Control 3

Continuous Vulnerability Management

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

Vulnerability Management

Now you know what you have, it’s time to secure it!

How do you manage vulnerabilities?

Scanning and Remediation

Examples of vulnerabilities

Vulnerability Management

How do you manage vulnerabilities?

Nessus™

Qualys®

ALIEN VAULT™

OpenVAS
Open Vulnerability Assessment System

Vulnerability Management

Examples of vulnerabilities

CIS Control 4

Controlled Use of Administrative Privileges

The processes and tools used to **track/control/prevent/correct the use, assignment, and configuration of administrative privileges** on computers, networks, and applications.

Administrative Privileges

Inventory Admin Accounts

Remove Local Admin Rights

Separate Standard and Admin Accounts

Escalate Privileges

Change Default Usernames and Passwords

Multifactor Authentication

CIS Control 5

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

Secure Configurations

Informed by Hardware and Software Inventory from CIS Controls 1 and 2

Configuration Authorities

Windows Tools

Linux Tools

Secure Configurations

- Windows
- macOS
- Linux
- IIS
- VMware
- SharePoint
- iOS
- Android

Secure Configurations

Defense Information Systems Agency (DISA)
Security Technical Implementation Guides (STIGs)

Configuration standards for DOD

- Windows
- macOS
- Linux
- IIS
- VMware
- SharePoint
- iOS
- Android

Patching, Imaging, and Configurations

Windows Server Update Services (WSUS)

Windows Deployment Services (WDS)

System Center Configuration Manager (SCCM)

PowerShell Desired State Configuration (DSC)

Group Policy Object (GPO)

What about Linux?

DevOps…

CHEF

ANSIBLE

kubernetes

CIS Control 6

Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

Logs

Collect, manage, and analyze logs

Security Information and Event Management (SIEM)

Contact Us

Sword & Shield Enterprise Security, Inc.
1431 Centerpoint Blvd, Suite 150
Knoxville, TN 37932-1984

865-244-3500

Social Media
Facebook.com/SwordShieldSec
Twitter.com/SwordShieldSec
Youtube.com/SwordShieldSec

secureme@swordshield.com

www.swordshield.com