Security Leadership

Posters

CyberPosture Intelligence for the Hybrid Cloud

HALOCK

Premiering Your CIS Controls and Meeting Duty of Care

IBM Security

Delivering Controls with CIS-Certified “Security Through System Integrity”

Qualys

Continued Security

Cavirin

November 14-16, 2017

SANS Conference, San Francisco

CIS Controls™

Cybersecurity + Cloud

CIS Maturity

The NIST Framework & The CIS Controls: Unifying Your Cyberdefense Program

CIS Controls CIS controls the critical data in three different categories:

Basic

Key controls, which should be implemented in any organization for a baseline security posture.

Foundational

Technical best practices to achieve secure infrastructure and the applications running on it.

Organizational

These controls are more focused on access and permissions rather than cybersecurity.

Start by taking care of the basics: build a solid cybersecurity program from the ground up. To build a solid cybersecurity program:

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

For more information, visit our website at sans.org/curricula/management

Cybersecurity Community

When designing the blueprint of a cybersecurity program, we should extensively review the risk posture and risk appetite of an organization. When designing a cybersecurity program, it is critical to ensure that the organization is using the correct controls. To determine the correct controls, we must first understand the following:

1. The NIST Framework
2. The CIS Controls

CIS RAM

CIS RAM is a framework of controls that is designed to help organizations implement and measure their cybersecurity posture. The framework is designed to help organizations prioritize the controls that are most critical to their business and to facilitate the implementation of those controls.

CIS Center for Internet Security

CIS Center for Internet Security (CIS) provides a framework for organizations to implement and measure their cybersecurity posture. The framework is designed to help organizations prioritize the controls that are most critical to their business and to facilitate the implementation of those controls.

Version 7: a prioritized set of actions to protect your organization and data from known cyber attack vectors.
Five Keys for Building a Cybersecurity Program

1. Find Frameworks that Fit
Choose frameworks that guide the work of your security program and, ultimately, simplify the complex world of cybersecurity in a way that can be more easily understood by business leaders.
- Control frameworks describe the security controls that are the foundation of every security program.
- Program frameworks help structure the security program, establish a basis for evaluating program activities, and simplify communication about the program.
- Risk frameworks provide a consistent approach for managing and assessing risk in a way that provides value to the business.

Choose a framework from each of these three categories to mature your program over time. Examples of common frameworks include:

- **Control Frameworks**
  - NIST 800-53
  - CIS Controls
- **Program Frameworks**
  - ISO 27001
  - ISMS 2005
  - CIS RAM
  - FAIR

2. Map Controls to the Framework
Security frameworks can be used together. This shows how the CIS Controls can be mapped to the Categories and Functions of the NIST Cybersecurity Framework (CSF).

3. Manage and Assess Risk
Beyond the activities defined in control or program frameworks, you also need to determine which capabilities to prioritize. What do you do first or not at all? How do you make this determination beyond just a checklist of activities?
ISO 27005 is a commonly referenced standard that defines a systematic approach to manage and assess risk for an organization.

4. Measure Maturity and Progress
Use a risk-based approach to prioritize security controls to reach a desired target state. Developing a roadmap allows you to measure maturity and progress over time.

5. Monitor and Measure Security
To continuously improve security effectiveness:
- Establish and measure meaningful security metrics.
- Monitor those metrics frequently enough to minimize incident impact.
- Take action rapidly and efficiently to effectively improve overall security.

The CIS Controls have proven to be an effective starting point for selecting key security metrics. Establish and measure meaningful security metrics.

SANS Training to Implement the CIS Controls and Build a Security Program

SEC566 Implementing and Auditing the Critical Security Controls – In-Depth
This course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, SOx, and risk officers, this course is the best way to understand how to measure whether the Controls have been implemented effectively.

“Provides greater structure to the basic controls. Good methodology provides in implementing controls.”

SANS Training for Security Strategy Planning, Policy, and Leadership
This course gives you the tools you need to become a security business leader who can build and execute strategic plans that resonate with other business executives, create effective information security policy, and develop management and leadership skills to better lead, inspire, and motivate your teams.

“I moved into management a few years ago and am currently working on a new security strategy roadmap and this class just confirmed the past two months of my life into a one week course and still learned a lot.”

sans.org/mgt514