SEC440: CIS Critical Controls: A Practical Introduction

2 Day Course | 12 CPEs | Laptop Not Needed

You Will Be Able To

- Understand a security framework and its controls based on recent and evolving threats facing organizations
- Prepare you to interpret a security framework based on data from publicly known attacks, breach reports, and large scare data analytics from the Verizon Data Breach Investigation Report (DBIR), along with data from the Multi-State Information Sharing and Analysis Center (R) (MS-ISAC(R)).
- Understand the importance of each control, how it is compromised if ignored, and explain the defensive goals accomplished with each control
- Identify tools that implement controls through automation
- Learn how to create a scoring tool for measuring the effectiveness of each controls the effectiveness of each control
- Identify specific metrics to establish a baseline and measure the effectiveness of security controls

"The 20 Critical Security Controls provide updated/ current trends in InfoSec. The course provided an excellent explanation of the controls and how to apply them."

— Dan Sherman, **RIC Audit FRB**

Introduction to Critical Security Controls

Cybersecurity attacks are increasing and evolving so rapidly that it is more difficult than ever to prevent and defend against them. Does your organization have an effective method in place to detect, thwart, and monitor external and internal threats to prevent security breaches? Does your organization need an on-ramp to implementing a prioritized list of technical protections?

In February of 2016, then California Attorney General, Vice President Kamala Harris recommended that "The 20 controls in the Center for Internet Security's Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization's environment constitutes a lack of reasonable security."

SANS has designed SEC440 as an introduction to the CIS Critical Controls, in order to provide students with an understanding of the underpinnings of a prioritized, risk-based approach to security. The technical and procedural controls explained in the CIS Controls were proposed, debated and consolidated by various private and public sector experts from around the world. Previous versions of the CIS Controls were prioritized with the first six CIS Critical Controls labeled as "cyber hygiene" and now the CIS Controls are now organized into Implementation Groups for prioritization purposes.

The Controls are an effective security framework because they are based on actual attacks launched regularly against networks. Priority is given to Controls that (1) mitigate known attacks (2) address a wide variety of attacks, and (3) identify and stop attackers early in the compromise cycle.

The course introduces security and compliance professionals to approaches for implementing the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.

Section Descriptions

SECTION 1: Introduction and Critical Controls 1–9

Section 1 will introduce you to Critical Controls 1-9, including the name, purpose, and why each matters in the bigger picture of cybersecurity.

- **CIS Critical Control 1:** Inventory and Control of Enterprise Assets
- **CIS Critical Control 2:** Inventory and Control of Software Assets
- **CIS Critical Control 3:** Data Protection
- **CIS Critical Control 4:** Secure Configuration of Enterprise Assets and Software
- **CIS Critical Control 5:** Account Management
- **CIS Critical Control 6:** Access Control Management
- **CIS Critical Control 7:** Continuous Vulnerability Management
- **CIS Critical Control 8:** Audit Log Management
- **CIS Critical Control 9:** Email and Web Browser Protections

SECTION 2: Critical Controls 10–18 and Conclusion

Section 2 will introduce you to Critical Controls 10-18, including the name, purpose, and why each matters in the bigger picture of cybersecurity.

- **Critical Control 10:** Malware Defenses
- **Critical Control 11:** Data Recovery
- **Critical Control 12:** Network Infrastructure Management
- **Critical Control 13:** Network Monitoring and Defense
- **Critical Control 14:** Security Awareness and Skills Training
- **Critical Control 15:** Service Provider Management
- **Critical Control 16:** Application Software Security
- **Critical Control 17:** Incident Response Management
- **Critical Control 18:** Penetration Testing