SEC440: Critical Security Controls: Planning, Implementing, and Auditing

2 Day Course	12 CPEs	Laptop Not Needed

Author Statement

"As we've had the opportunity to talk with information assurance engineers, auditors, and managers over the past ten years we've seen frustration in the eyes of these hardworking individuals trying to make a difference in their organizations by better defending their data systems. It's even come to the point where some organizations have decided that it's simply too hard to protect their information, and many have started to wonder, is the fight really worth it, will we ever succeed? We see companies and agencies making headway, but the offense keeps pushing. The goal of this course is to give direction and a realistic hope to organizations attempting to secure their systems.

The Critical Security Controls: Planning, Implementing, and Auditing offers direction and guidance as to what security controls will make the most impact, from those in the industry that think through the eyes of the attacker. What better way to play defense than by understanding the mindset of the offense? By implementing our defense methodically and with the mindset of a hacker, we think organizations have a chance to succeed in this fight. We hope this course helps turn the tide."

— James Tarala

"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**

Course Preview
available at: **sans.org/demo**

This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security (CIS). These Critical Security Controls, listed below, are rapidly becoming accepted as the highest priority list of what must be done and proven before anything else at nearly all serious and sensitive organizations. These controls were selected and defined by the US military and other government and private organizations (including NSA, DHS, GAO, and many others) who are the most respected experts on how attacks actually work and what can be done to stop them. They defined these controls as their consensus for the best way to block the known attacks and the best way to help find and mitigate damage from the attacks that get through. For security professionals, the course enables you to see how to put the controls in place in your existing network though effective and widespread use of 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. SEC440 does not contain any labs. If the student is looking for hands on labs involving the Critical Controls, they should take SEC566.

You will find the full document describing the Critical Security Controls posted at the Center for Internet Security at **cisecurity.org/controls**.

One of the best features of the course is that it uses offense to inform defense. In other words, you will learn about the actual attacks that you'll be stopping or mitigating. That makes the defenses very real, and it makes you a better security professional.

Section Descriptions

SECTION 1: Introduction and Critical Controls 1–9

Section one will cover Critical Controls 1–9 in depth:

- **Critical Control 1:** Inventory of Authorized and Unauthorized Devices
- **Critical Control 2:** Inventory of Authorized and Unauthorized Software
- **Critical Control 3:** Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- **Critical Control 4:** Continuous Vulnerability Assessment and Remediation
- **Critical Control 5:** Controlled Use of Administrative Privileges
- **Critical Control 6:** Maintenance, Monitoring, and Analysis of Audit Logs
- **Critical Control 7:** Email and Web Browser Protections
- **Critical Control 8:** Malware Defenses
- **Critical Control 9:** Limitation and Control of Network Ports, Protocols, and Services

SECTION 2: Critical Controls 10–20 and Conclusion

Section two will cover Critical Controls 10–20:

- **Critical Control 10:** Data Recovery Capability (validated manually)
- **Critical Control 11:** Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- **Critical Control 12:** Boundary Defense
- **Critical Control 13:** Data Protection
- **Critical Control 14:** Controlled Access Based On Need to Know
- **Critical Control 15:** Wireless Device Control
- **Critical Control 16:** Account Monitoring and Control
- **Critical Control 17:** Security Skills Assessment and Appropriate Training to Fill Gaps (validated manually)
- **Critical Control 18:** Application Software Security
- **Critical Control 19:** Incident Response and Management (validated manually)
- **Critical Control 20:** Penetration Tests and Red Team Exercises (validated manually)

Available Training Formats

Live Training

Live Events
sans.org/information-security-training/by-location/all

Summit Events
sans.org/cyber-security-summit

Private Training
sans.org/private-training

Online Training

OnDemand
sans.org/ondemand

Simulcast
sans.org/simulcast