

Description:

IS20 controls are the Top Twenty Most Critical Security Controls in Information Technology. This 4 day training course covers proven tools and methodologies needed execute and analyze the Top Twenty Most Critical Security Controls. Nearly all organizations that maintain sensitive information are adopting these Security Controls



These controls were chosen by leading government and private organizations who are experts on how attacks work and what can be done to prevent them from happening. The controls were selected as the best way to block known attacks as well as help search for and alleviate any damage from the attacks that are successful. This course allows the security professional to see how to implement controls in an existing network through highly effective and economical automation. For management, this training is the best way to distinguish how you will assess whether these security controls are effectively being administered.



Annual Salary Potential \$92,662 AVG/year

Key Course Information

Live Class Duration: 4 Days

CEUs: 32

Language: English

Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:

- Broad Understanding of Multiple Networking and Security Technologies

Modules/Lessons

- Module 1 - Introduction
- Module 2 - Critical Control 1
- Module 3 - Critical Control 2
- Module 4 - Critical Control 3
- Module 5 - Critical Control 4
- Module 6 - Critical Control 5
- Module 7 - Critical Control 6
- Module 8 - Critical Control 7
- Module 9 - Critical Control 8
- Module 10 - Critical Control 9
- Module 11 - Critical Control 10
- Module 12 - Critical Control 11
- Module 13 - Critical Control 12
- Module 14- Critical Control 13
- Module 15 - Critical Control 14
- Module 16 - Critical Control 15
- Module 17- Critical Control 16
- Module 18 - Critical Control 17
- Module 19 – Critical Control 18
- Module 20 – Critical Control 19
- Module 21 – Critical Control 20

Who Should Attend

- Information Assurance Managers/Auditors
- System Implementers
- IT Administrators
- Auditors
- Federal Agencies
- Security Vendors and Consulting Groups

Accreditations



Upon Completion

Upon completion, the IS20 Security Controls candidate will be able to not only competently take the IS20 Controls exam but will also have an understanding of how to implement the top 20 most critical controls in the work place.

Exam Information

The IS20 Controls exam is taken online through Mile2's Learning Management System and is accessible on your Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

- 1) Pass the most current version of the exam for your respective existing certification
- 2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options



Detailed Outline:

Course Introduction

- I. Critical Control 1: Inventory of Authorized and Unauthorized Devices
- II. Critical Control 2: Inventory of Authorized and Unauthorized Software
- III. Critical Control 3: Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- IV. Critical Control 4: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- V. Critical Control 5: Boundary Defence
- VI. Critical Control 6: Maintenance, Monitoring, and Analysis of Audit Logs
- VII. Critical Control 7: Application Software Security
- VIII. Critical Control 8: Controlled Use of Administrative Privileges
- IX. Critical Control 9: Controlled Access Based on Need to Know
- X. Critical Control 10: Continuous Vulnerability Assessment and Remediation
- XI. Critical Control 11: Account Monitoring and Control
- XII. Critical Control 12: Malware Defences
- XIII. Critical Control 13: Limitation and Control of Network Ports, Protocols, and Services
- XIV. Critical Control 14: Wireless Device Control
- XV. Critical Control 15: Data Loss Prevention
- XVI. Critical Control 16: Secure Network Engineering
- XVII. Critical Control 17: Penetration Tests and Red Team Exercises
- XVIII. Critical Control 18: Incident Response Capability
- XIX. Critical Control 19: Data Recovery Capability
- XX. Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps