Certified Security Leadership Officer

Description:

Mile2's Certified Security Leadership Officer course is designed for mid and upper-level managers. If you are an engineer, this course will increase your knowledge in the leading information system security teams.

Plus, the C)SLO will give you an essential understanding of current security issues, best practices, and technology. With this knowledge you will then be prepared to manage the security component of an information technology project. As a Security Leadership Officer, you will be the bridge between cybersecurity and business operations.

* This course/certification has been validated by the NSA for: CNSSl-4014, Information Assurance Training Standard for Information Systems Security Officers.

Annual Salary Potential $89,862 AVG/year

Key Course Information

Live Class Duration: 5 Days
CEUs: 32
Language: English
Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:

* 12 months professional experience in IT

or

* 12 months professional experience in systems management

Modules/Lessons

Module 1 - Security Management

Module 2 - Risk Management

Module 3 - Encryption

Module 4 - Information Security Access Control Concepts

Module 5 - Incident Handling and Evidence Module 6 - Operations Security

Module 7 - Network Security

Who Should Attend

* C - Level Managers
* IT Managers
* Cyber Security Personelle
* Engineers
* Information Systems Owners
* ISSO's
* CISSP Students
* ISO's

Accreditations

Upon Completion

Upon completion, the Certified Security Leadership Officer candidate be able to competently take the C)SLO exam. You will be versed in implementing strong security controls and managing an organization with an industry acceptable security posture.

Exam Information

The Certified Security Leas exam is taken online through Mile2's Learning Management System and is accessible on you 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:

Module 1 - Security Management

a. The Role of the CSLO
b. Business Goals and Objectives
c. Overview of Governance
    a. The First Priority for the CSLO
    b. Outcomes of Governance
    c. Performance and Governance
d. Organization of IT Security
e. Security Strategy
f. The Goal of Information Security
g. Defining Security Objectives
h. Security Budget
i. Security Integration
j. Architecture
k. Information Security Frameworks
l. Integration
m. COBIT 4.1
n. Deming and Quality
o. Ethics
p. Fraud
q. Hiring and Employment
r. Intellectual Property
s. Protecting IP
t. Attacks on IP
u. OECD Privacy Principles
v. PII and PHI
w. Awareness Training

Module 2 - Risk Management

a. Risk Management
b. Risk Assessment
c. Quantitative vs Qualitative Risk
d. What Is the Value of an Asset?
e. What Is a Threat/Vulnerability
f. Assess and Evaluate Risk
g. Controls

h. Comparing Cost and Benefit
i. Cost of a Countermeasure
j. Appropriate Controls
k. Documentation

Module 3 – Encryption

a. Encryption
b. Secrecy of the Key
c. Cryptographic Functions
d. XOR Function
e. Symmetric Encryption
f. Asymmetric Algorithms
g. Hashing Algorithms
h. Digital Signatures
i. Digital Envelope
j. Public Key Infrastructure (PKI)
k. Certificates
l. Uses of Encryption in Communications
m. Auditing Encryption Implementations
n. Steganography
o. Cryptographic Attacks

Module 4 - Information Security Access Control Concepts

a. Information Asset Classification
    a. Criticality
    b. Sensitivity
    c. Regulations and Legislation
b. Asset Valuation
c. Information Protection
d. Storing, Retrieving, Transporting and Disposing of Confidential Information
e. Password Policy
f. Password Cracking
g. Biometrics
h. Authorization
i. Accounting/Auditability
j. Centralized Administration
k. Access Control

Module 5 - Incident Handling and Evidence

a. Goals of Incident Management and Response
b. Security Incident Handling and Response
c. Evidence Handling
d. What is an Incident - Intentional
e. What is an Incident - Unintentional
f. Malware
g. Attack Vectors
h. Information Warfare
i. Developing Response and Recovery Plans
j. Incident Response Functions
k. Incident Management Technologies
l. Responsibilities of the CSLO
m. Crisis Communications
n. Challenges in Developing an Incident Management Plan
    a. When an Incident Occurs
    b. During an Incident
    c. Containment Strategies
    d. The Battle Box
    e. Evidence Identification and Preservation
    f. Post Event Reviews
o. Disaster Recovery Planning (DRP) and Business Recovery Processes
p. Development of BCP and DRP
q. Disaster Recovery Sites
r. Recovery of Communications
s. Plan Maintenance Activities
t. Techniques for Testing Security
u. Vulnerability Assessments
v. Penetration Testing

Module 6 - Operations Security

a. Operations Security
b. Specific Operations Tasks
c. Data Leakage – Object Reuse
d. Records Management
e. Change Control
f. Trusted Recovery
g. Redundant Array of Independent Disks (RAID)
h. Phases of Plan
i. BCP Risk Analysis
j. Recovery Point Objective

k. Priorities
l. OWASP Top Ten (2013)
m. Common Gateway Interface
n. How CGI Scripts Work
o. Cookies
p. Virtualization - Type 1
q. Virtualization – Type 2
r. Technologies – Databases and DBMS
s. Facilities
t. Facilities Security
u. Environmental Security
v. Physical Access Issues and Exposures
w. Controls for Environmental Exposures

Module 7 - Network Security

a. Network Topologies– Physical Layer
b. Data Encapsulation
c. Protocols at Each Layer
d. Devices Work at Different Layers
e. Technology-based Security
f. Network Security Architecture
g. Firewalls
h. Unified Threat Management (UTM)
i. UTM Product Criteria
j. TCP/IP Suite
k. Port and Protocol Relationship
l. Network Security
m. Internet Threats and Security
n. Auditing Network Infrastructure Security
o. IPSec - Network Layer Protection
p. Wireless Technologies– Access Point