ICDL Arabia

SYLLABUS

ICDL Module

Cyber Security for Military & Law Enforcement

Syllabus Version 1.0

Purpose

This document details the syllabus for the Cyber Security for Military & Law Enforcement module. The syllabus describes, through learning outcomes, the knowledge and skills that a candidate for the Cyber Security for Military & Law Enforcement should possess. The syllabus also provides the basis for the theory and practice-based test in this module.

Cyber Security for Military & Law Enforcement Module

This syllabus is recommended for military, law enforcement, university students, government organisations, or individuals who are interested in examining the best practices of network security methods.

Module Goals

Upon completion of this programme, participants should be able to:

- Describe the key security requirements of confidentiality, integrity, and availability.
- Understand the different types of security threats people face today and provide examples that apply to the different categories of computers and network assets.
- Explain the fundamental security design principles.
- Understand the procedures of attack surfaces, including the principal aspects of a comprehensive security strategy.
- Discuss the four general ways of authenticating a user's identity.
- Discuss the issues and approaches involved in remote user authentication.
- Explain how access control fits into the broader scheme of things, including authentication, authorisation, and audits.
- Understand the need for cloud and database security.
- Present an overview of the common attack methods, such as a denial-of-service/ distributed denial of service, TCP Session Hijacking, and Man-in-the-Middle (MITM) attacks.
- Describe broad mechanisms that malware uses to propagate and understand the basic operation of malicious codes along with the different threats posed by bots, spyware, and rootkits.
- Understand the basic principles of network/computer security protection.
- Distinguish between the various types of protection, such as Intrusion Detection/ Prevention Systems (IDS/IPS), and Firewalls.
- Describe strategies, management, security design, and policies of cyber security.
- Present an overview of the current and future technological attacks.
- Explain the basic concepts and operations of smart security based on Artificial Intelligence (AI), Machine Learning (ML), and "deep learning."

CATEGORY	SKILL SET	REF.	TASK ITEM
1 Cyber Security Key Terms for Military & Law Enforcement	*1.1 Information Accepts of Military and Law Enforcement*	1.1.1	Identify the Term Information
		1.1.2	Identify the Term Information Security
		1.1.3	Identify the Term Information Warfare
		1.1.4	Define the Concepts of Information
		1.1.5	Define the Military Information Sources
		1.1.6	Recognise the Law Enforcement Information Sources
		1.1.7	Recognise the Key Principles of Information Security
		1.1.8	Define the Information Classifications

CATEGORY	SKILL SET	REF.	TASK ITEM
	1.2 Main Cyber Players and Their Motives	1.2.1	Identify Cybercrime
		1.2.2	Define Cyberespionage
		1.2.3	Identify Hacktivist
		1.2.4	Define Cyber Sabotage
		1.2.5	Define the Cyberwarfare
	1.3 National Security	1.3.1	Define Cyber Terrorism
		1.3.2	Be aware of Organised Criminal Groups in Cyber Space
		1.3.3	Define the term Cybersecurity for Military and Law Enforcement
		1.3.4	Identify Who Might Be Attacking You
		1.3.5	Identify Cyber/ Physical Threat Scenarios
		1.3.6	Recognise the Cyber Threat Spectrum
2 An Overview of Computer Security Concepts	*2.1 Preface to Computer Security*	2.1.1	Define the term Computer Security
		2.1.2	Identify the Key Security Concepts
		2.1.3	Recognise the Levels of Impacts
	2.2 Computer Security Terminology	2.2.1	Identify Assets of a Computer System
		2.2.2	Recognise Internet Security Keys
	2.3 Understanding Vulnerabilities, Threats and Attacks	2.3.1	Define the term Vulnerability
		2.3.2	Recognise the Dangerous of Threats
		2.3.3	Identify the term Countermeasure
		2.3.4	Be Aware of Threat Sources
		2.3.5	Be Aware of Threats from Insiders
		2.3.6	Recognise System Administration Threats
		2.3.7	Recognise Security Risk
		2.3.8	Classify the Types of Threats & Attacks
		2.3.9	Identify the Risks to Network Monitoring
		2.3.10	Extranets Information-Assurance Goals
	2.4 Issues on P2P, IM, SMS and Collaboration Tools	2.4.1	Identify the term Peer-to-Peer (P2P)
		2.4.2	Define Instant Messaging (IM)
		2.4.3	Define Short Message Service (SMS)
		2.4.4	Identify Collaboration Tools
		2.4.5	Understand P2P, Abusing Resources & Illegal Content Organisations
		2.4.6	Be aware if Instant Messages (IM) are not allowed
		2.4.7	Understand why SMS cannot be Used
		2.4.8	Recognise the Dangers of Collaboration Tools
		2.4.9	Define the ways to prevent P2P, IM, SMS, and Collaboration tools
	2.5 Data Loss Prevention System (DLP)	2.5.1	Understand Data Loss Prevention (DLP)
		2.5.2	Understand how to Protect Data Loss Prevention (DLP)
		2.5.3	Understand the Six (6) Essential Security Element Losses
		2.5.4	Understand why Email and Internet is not Allowed

CATEGORY	SKILL SET	REF.	TASK ITEM
	2.6 Cyber Security Governance & Risk Management	2.6.1	Understand the term Governance
		2.6.2	Understand Threat Analysis: Acts and Suggested Controls
		2.6.3	Define the Key Functions of Vulnerability Management
		2.6.4	Recognise the Vulnerability Assessment Strategy & Techniques
		2.6.5	Understand Risk Management
		2.6.6	Understand Event Recovery
		2.6.7	Understand the Guidelines for Recovery Events
		2.6.8	Define Information Assurance Considerations
3 Rapid Advances in Technology & Cybercrimes	*3.1 Cloud Computing*	3.1.1	Define Cloud Computing
		3.1.2	Understand the Cloud Computing Service Types
		3.1.3	Distinguishing between SaaS, PaaS, and IaaS
	3.2 Internet of Things (IoT)	3.2.1	Identify Internet of Things
		3.2.2	Internet of Things: Phases of Evolution
		3.2.3	Recognise Some Major Domains of the IoT (Internet of Things)
		3.2.4	Internet of Things (IoT) Characteristics
	3.3 Fog Computing	3.3.1	Understand the Importance of Fog Computing
		3.3.2	Define the Characteristics of Fog Computing
	3.4 Big Data and Data Lakes	3.4.1	Understand the meaning of Big Data
		3.4.2	Recognise the Current Data Volumes
		3.4.3	Identify the term Data Lakes
	3.5 Issues on Darknet, Deep and Dark Web	3.5.1	Define the Relationship between Internet, Deep Web and Dark Web
		3.5.2	Identify Surface Web
		3.5.3	Define The Deep Web
		3.5.4	Understand The Dark Web and Darknets
		3.5.5	Understand the Browser of Darknet
		3.5.6	Define what is inside The Hidden Web (Deep Web)
		3.5.7	Distinguish between The Surface Web, The Deep Web & The Dark Web
	3.6 Darknet and Cybercrimes	3.6.1	Understand how Dark Net helps Organised Crime
		3.6.2	Be Aware of Digital Money (Bitcoin) and Related Cybercrimes
		3.6.3	Sample Cases of Organised Crimes
		3.6.4	Identify the Techniques used by Cyber Terrorists
4 Computer/ Network Attacks	*4.1 Key Terms of Attacks*	4.1.1	Identify the term Port Number
		4.1.2	The Basics of a Network
		4.1.3	Recognise the Importance of Data Packets
		4.1.4	Distinguishing between Identity Theft & Identity Fraud
		4.1.5	Identify the possible Active Attacks
		4.1.6	Identify the possible Passive Attacks
		4.1.7	Be Aware of Cookies

CATEGORY	SKILL SET	REF.	TASK ITEM
	4.2 Common Cybercrime Attacks	4.2.1	Identify Classification of Threads
		4.2.2	Define the term Attack Surfaces
		4.2.3	Threats to Network Security
		4.2.4	Be aware of the Computer Network Risks
		4.2.5	Threats to Workstations and Home Personal Computer Security
		4.2.6	Define the term Intruder
		4.2.7	Identify what an Intruder Can Do
		4.2.8	Understand the Activities of Intruders
	4.3 Denial of Service (DoS) Attacks	4.3.1	Define the Types of Denial of Service Attacks
		4.3.2	Be Aware of Specific DoS Attacks
		4.3.3	Define Distributed Denial-of-Service (DDoS) Terminology
	4.4 Fiber Channel Weakness and Exploits	4.4.1	Identify Man-in-the-Middle Attacks (MIMA)
		4.4.2	Understand TCP Session Hijacking
		4.4.3	Recognise Name-Server Corruption Attacks
	4.5 SQL Injection Attacks	4.5.1	Understand the Need for Secure Databases
		4.5.2	Be Aware of SQL Injection
	4.6 Spam, Phishing, and Trojan Attacks meant to Fool	4.6.1	Recognise the Common Elements between Spam, Phishing and Trojans
		4.6.2	Identify the Purpose Of Spam
		4.6.3	Define the Problems behind Spams
		4.6.4	Understand what Phish Looks Like
		4.6.5	Define the Trojans Tricks that Fool Users
	4.7 The Broad Classification of Malicious/ Malware Software	4.7.1	Understand the term Virus
		4.7.2	Identify the terms Spyware and Adware
		4.7.3	Recognise the effects of Worms
		4.7.4	Understand why Trojans are Dangerous
		4.7.5	Recognise Rootkits
		4.7.6	Define IRC Bots
		4.7.7	Recognise Malicious Mobile Code
		4.7.8	Define Downloaders and Drive by Download
		4.7.9	Identify Logic Bombs
		4.7.10	Understand Polymorphic and Cryptographic Viruses
	4.8 The Terminology for Malicious Software (Malware)	4.8.1	Be Aware of Tool Kits
		4.8.2	Recognise the Attack Sources
		4.8.3	Be Aware of Advanced Persistent Threats (APT)
		4.8.4	Understand why Macro and Scripting Viruses are Dangerous
		4.8.5	Understand Client-Side (XSS) and Drive-by Download Attacks
		4.8.6	Be Aware of Clickjacking Attack
		4.8.7	Understand Payload Attack Agents – Zombie and Bots
		4.8.8	Understand Remote Control Facility Attacks
	4.9 Email Attacks	4.9.1	Phishing and Identity Theft
		4.9.2	Identify the Other Types of Phishing

CATEGORY	SKILL SET	REF.	TASK ITEM
	4.10 Social Engineering	4.10.1	Identify why Social Engineering is Dangerous
		4.10.2	Define other ways an Attacker can use Social Engineering
		4.10.3	Be Aware of Social Engineering Networks and Voice Methods
	4.11 Internet based applications and social media Platforms	4.11.1	Understand the Concept of Social Media Platforms
		4.11.2	Be aware of Common Risks Typical to Various Internet-Based Applications & Social Media Platforms
	4.12 Wireless and Mobile Attacks		
	4.13 Domain Name System (DNS) Attacks		
	4.14 Top Threats, & Mechanisms Exploited		
	4.15 Cyber ways to Physical Attacks	4.15.1	Recognise how most Physical to Cyber-Attacks
		4.15.2	Understand the Illegal Penetration of ICT Systems
	4.16 Authentication Vulnerabilities	4.16.1	Identify Authentication Process
		4.16.2	Define the means of Authentication
		4.16.3	Recognise the Risk Assessment for User
		4.16.4	Understand Password Authentication
		4.16.5	Recognise Password Vulnerabilities
		4.16.6	Be Aware of Popular ways to Steal the Encrypted Passwords
		4.16.7	Identify Remote User Authentication
		4.16.8	Understand Authentication Security Issues
5 Network Defense and Counter Measures	*5.1 Intrusion Detection and Prevention Systems*	5.1.1	Define the term Security Intrusion
		5.1.2	Identify Intrusion Detection Systems (IDS)
		5.1.3	Define the need for Intrusion Detection and Prevention Systems
		5.1.4	Identify the IDS Classifications
		5.1.5	Recognise the Strategies used in Performing Intrusion Detection
		5.1.6	Define the Information Sources of the Intrusion Detection Process
		5.1.7	Define a List of Guidelines when IDS is Implemented
		5.1.8	Understand How IDS Analyse Sensor Data to Detect Intrusion

CATEGORY	SKILL SET	REF.	TASK ITEM
		5.1.9	Distinguish Between the Anomaly and Signature Heuristic Approaches
		5.1.10	Define the term Intrusion Prevention Systems (IPS)
		5.1.11	Recognise How IPS Work
	5.2 Honeypot System	5.2.1	Define the term Honeypot
		5.2.2	Identify the Classifications of Honeypot
		5.2.3	Be Aware of Honeypot Deployment
	5.3 Firewall	5.3.1	Define the term Firewall
		5.3.2	Understand the Need for Firewall
		5.3.3	Define the Firewall Goals
		5.3.4	Recognise Firewall Filter Characteristics
		5.3.5	Understand Firewall Capabilities and Limitations
		5.3.6	Understand the term Demilitarised Zone (DMZ) Network
	5.4 Proxy Server	5.4.1	Define the term Proxy Server
		5.4.2	Identify the Fundamentals of Proxying
		5.4.3	Define Advantages of Proxy Firewalls
		5.4.4	Define Disadvantages of Proxy Firewalls
		5.4.5	Identify Web Proxy
		5.4.6	Understand Reverse Proxies
		5.4.7	Define Anonymising Proxies
	5.5 Encryption Algorithms	5.5.1	Identify Encryption Terminology
		5.5.2	Define the Term Encryption
		5.5.3	Identify how the Encryption Works
		5.5.4	Understand the Need for Encryption of Sensitive Data
		5.5.5	Symmetric-Key Cryptography
		5.5.6	Identify the term Asymmetric Key
		5.5.7	Understand the Need for Encryption
	5.6 Steganography	5.6.1	1 Identify the term Steganography
		5.6.2	Define the Basic Steganography Techniques
		5.6.3	Understand how Steganography Works
		5.6.4	Distinguish between Steganography and Cryptography
	5.7 Network Protection Principles	5.7.1	Understand why Uniform Access Management is Important
		5.7.2	Be aware of Secure Communications
		5.7.3	Identify Variable Depth Security or Zoning Security
		5.7.4	Recognise the Importance of Defence in Depth
		5.7.5	Define the term Network Survivability
		5.7.6	Identify why IT System Configuration is Necessary?
		5.7.7	Know the Protection Principles, Prevent, Detect, React and Deter

CATEGORY	SKILL SET	REF.	TASK ITEM
		5.7.8	Understand how to Reduce Network Exposure
		5.7.9	Recognise how Monitoring Network Risks can be managed
		5.7.10	Recognise the Tools that can Detect Incidents
	5.8 Defending Against Malware/Malicious Codes	5.8.1	Understand how to Prevent Malicious Code Attacks
		5.8.2	Know how to Prohibit Malicious Codes by using Technical Controls
		5.8.3	Define how to Fight Trojans
	5.9 Defending Against Fooling Attacks	5.9.1	Recognise the Defence & Mitigation of Social Engineering
		5.9.2	Define how to Fight Spam
		5.9.3	Understand Fighting Phishing
		5.9.4	Identify how to Protect against Cyber Threats: “Fake” Profiles & Toxic Emails
		5.9.5	Define Protection against Cyber Threats- Spyware & Password Hacks
		5.9.6	Identify the XSS Cross-Site Scripting “Cyber Threat Protection
	5.10 Defending Against Denial of Service Attacks	5.10.1	Understand how to Protect Computers after a Zombie Attack
		5.10.2	Recognise the Basic Security Controls to Detect and Avoid Zombies
		5.10.3	Define how to Prevent Denial of Service Attacks
		5.10.4	Identify the Defence against Distributed Denial of Service Attacks
		5.10.5	Exploited Software Defensive Actions
	5.11 Cloud Computing Security	5.11.1	Define Guidelines on Cloud Security and Privacy Issues
		5.11.2	Identify The Cloud Security Alliance Categories
		5.11.3	Define Guideline Techniques for Web Filtering
	5.12 Authentication Protection	5.12.1	Define the Four Principles of Authentication
		5.12.2	Define the major risks of password Use and Mitigation by Technical, Social, and Procedural Means
		5.12.3	Define the Types of Biometric Technology
		5.12.4	Identify Password Selection Strategies
		5.12.5	Define Persistent ways to Protect Password
	5.13 Secure Stored Data		

CATEGORY	SKILL SET	REF.	TASK ITEM
	5.14 Operating Systems Protection	5.14.1	Define the Principles of Security in Operating Systems
		5.14.2	Identify the Categories of Security and Protection to Operating Systems
		5.14.3	Understand the Requirements for Operating Systems Security
		5.14.4	Understand the Design Principles of Security for Threats against Computer Systems
		5.14.5	Understand the Protection Mechanisms of Multiprogramming
		5.14.6	Understand the Security Aspects of File Sharing
		5.14.7	Define Network Operating Systems Issues
	5.15 Virtual Private Network (VPN) & Secure Remote Access	5.15.1	Identify the VPN
		5.15.2	Identify the Extranet
		5.15.3	Define the Remote Access (VPN)
		5.15.4	Distinguish between IPSec and TLS/SSL
6 Smart Security	*6.1 The need for Smart Security*	6.1.1	Recognise IOT Cyber Attacks
		6.1.2	Be aware of the term Market Zero-Day Exploits
		6.1.3	Understand Integrated Security
		6.1.4	Understand Adaptive Security
		6.1.5	Identify Cyber-Physical Threats from the IoT
		6.1.6	Understand Traditional “Physical Security” Defences of “Cybersecurity
	6.2 The Road towards better Automotive Cybersecurity- Smart Security	6.2.1	Understand the Need for Adaptive & Intelligent Cybersecurity
		6.2.2	Identify the Cyber Security Market
		6.2.3	Recognise the Transition to “Machine Learning” Cybersecurity Applications & Tools (Learning Security)
		6.2.4	Identify the need for Self-Learning Security
	6.3 Intelligent Security	6.3.1	Understand Cybersecurity: Created around Artificial Intelligence Tools
		6.3.2	Recognise the Motivation towards “Neural Society”
		6.3.3	Define ways to Defend against Cyber Terrorists
		6.3.4	Understand Military/Law Enforcement’s Smart Security
		6.3.5	Recognise Cyber Integration with Physical Security Operations
		6.3.6	Identify Smart Security for Military/Law Enforcement

CATEGORY	SKILL SET	REF.	TASK ITEM
7 Network/ Computer Cyber Security Management	*7.1 Management of Network Security Risks*	7.1.1	Define the Factors of Computer Security Strategy
		7.1.2	Define the necessary Typical Cybersecurity skills, for Management, Information Assurance and Technical
		7.1.3	Identify the term Vulnerability Management
		7.1.4	Define the Risk Management Approach
		7.1.5	Define Dynamic Approaches to Manage the Cybersecurity Risks
	7.2 Creating a Cyber Security Strategy	7.2.1	Understand the Main Cybersecurity Challenges
		7.2.2	Be Aware of Top Cyber Defense Actions must be taken
		7.2.3	Define the Criminal Activities
		7.2.4	Identify the Cybersecurity Executive Roles
		7.2.5	Define the Importance of Telecommunications Infrastructure, Holders and Vendors
		7.2.6	Be Aware of Employees in Cybersecurity Concepts
		7.2.7	Define the General Cyber Security Strategies
	7.3 Key Elements of Cybersecurity Security Requirements	7.3.1	Be Aware of Awareness and Training
		7.3.2	Define Audits and Accountability
		7.3.3	Define the Certification, Accreditation, and Security Assessments
		7.3.4	Identify the Management Configuration
		7.3.5	Identify the Incident Response
		7.3.6	Understand the Importance of Maintenance
		7.3.7	Be Aware of Media Protection
		7.3.8	Define the Personnel Security
		7.3.9	Identify the Risk Assessment
		7.3.10	Define System, Communications and Information Integrity Protections
		7.3.11	Access Control Context
	7.4 Guidelines of Cyber Security Policies	7.4.1	Identify the term Policy
		7.4.2	Understand Information Security Policy
		7.4.3	Identify the term Controls
		7.4.4	Define the Meaning of Standards in Computing
		7.4.5	Identify the Term Procedures
		7.4.6	Define the Major Resources for Policy Writers
		7.4.7	Define the Contents when Organising the Policies
		7.4.8	Define a Special-Purpose Documents Organisational Policy
		7.4.9	Define Access Control Policies
		7.4.10	Define the Risks can Occur when using Removable Media at work.
		7.4.11	Understand how to Overcome Removable Media Risks
		7.4.12	Information Security Incident Management Policy

CATEGORY	SKILL SET	REF.	TASK ITEM
	7.5 Human Resources Practices and Policies	7.5.1	Define the Aspects of Management to Pursue the Security Policies
		7.5.2	Understand why Security Awareness, Training, and Education are Recommended
		7.5.3	Define the Goals of Employee Security Awareness
		7.5.4	Understand what kind of Threats may happen from Employment Practices and Policies
		7.5.5	Be Aware of Security Principles during Employment
		7.5.6	Define a Procedure upon Termination of Employment
	7.6 Cyber Security Design	7.6.1	Fundamentals of Security Design
		7.6.2	Understand the Importance of User Authentication
		7.6.3	Identify the Physical Characteristics Used in Biometric Applications
		7.6.4	Define Token-Based Authentication
	7.7 Overview of Cybercrime Laws		