Certified CyberDefender (CCD) Syllabus

Module	Topics	Lessons
Module 1: Security Operations (SecOps) Fundamentals	Security Operations Fundamentals and CIA Triad	● Security Operation Centers (SOC) - Overview
		● Protecting Business with Efficient SOC
		● SOC Deployment Models: Dedicated vs. Virtual
		● Deploying a SOC: When to Consider?
	SOC components - tools and technologies	● Network Firewall - Protecting Communication and Data
		● Network-Based Intrusion and Prevention Systems (NIDS/NIPS)
		● Host-Based Intrusion and Prevention Systems (HIDS/HIPS)
		● Web Application Firewalls (WAFs): Protecting Web Apps
		● Endpoint Detection and Response (EDR/XDR)
		● Web Proxy Servers: An Overview
		● Understanding Vulnerability Management Process
		● Security Information and Event Management (SIEM): Core Component of SOC
		● Automating Security Incident Response with SOAR (Security Orchestration, Automation, and Response)

		● Malware Analysis: Static vs. Dynamic Approaches and Sandboxing
		● Using Honeypots and Decoys for Defense
		● Understanding Cloud Computing and CASB
		● Threat Intelligence: Mitigating and Defending
		● Using Machine and Deep Learning for Security
		● Ticketing Systems for Incident Response
		● The Importance of Asset Inventory in Security
	SOC components - people	● Organizational Chart and SOC Roles
		● Creating Effective Cybersecurity Training Plans
		● Challenges and Solutions for SOC Jobs
		● Avoiding Burnout: Tips for SOC Analysts
	SOC components - processes	● Effective Policies: Business Protection Through Documentation
		● Efficient SOC Procedures: The How-To
		● Security Standards: Compliance is Mandatory
		● Security Guidelines and Benchmarks: Best Practices
		● Perform Windows Security Assessments with CIS-CAT Lite

Module 2: Incident Response	Incident Response (IR) - Overview	● Understanding Key Concepts for Incident Response
		● Continuous Incident Response: Before, During, After
		● Remote Incident Response: Challenges and Benefits
		● Structured Approach to Incident Response Phases
	Preperation	● Effective Incident Prevention Strategies and Controls
		● Effective Incident Communication Planning in IR
		● IR Architecture: Defense and Zero Trust
		● IR Policy, Plan, and Procedure
		● Efficient Incident Resolution with Management Platforms
	Detection & Analysis	● Detection Engineering: Building Effective Detectors
		● Network Perimeter-level Detection
		● Endpoint Perimeter Detection: Catching Threats In and Out
		● Achieving System-Level Detection with EDR
		● Application-Level Detection: Prioritize, Monitor, Parse
	Containment, Eradication, and Recovery	● Effective Incident Containment Strategies in IR

	Attack Remediation: Eliminating Vulnerabilities and Artifacts	
	System Recovery: Restore, Validate, Monitor	
	Post-Incident Activity	● Post-Incident Review: Lessons Learned Meeting
		● IR Report: Guidelines for Effective Writing
Module 3: **Perimeter Defense -** **Email Security**	Email Spoofing	● Email Attack Prevention: Spoofing & DMARC
		● Understanding SPF: Email Authentication Protocol
		● DKIM: Email authentication with digital signatures
		● Protecting Against Email Spoofing with DMARC
	Malicious Attachments	● Malicious Attachments: Risks and Responses
		● Secure Email Attachments: Best Practices
		● Activity - Cuckoo Sandbox Deployment
	Malicious URLs	● Malicious URLs: A Growing Threat
		● Protecting Users from Malicious URLs
		● Activity – Detect Lookalike Domains
	Extra Mile Controls	● User Education: Key to Email Security
		● Measuring User Awareness with Phishing Simulators
		● Activity - GoPhish Deployment
		● Early Phishing Detection Using Honeypots Tokens

		• Activity - Canary Token Deployment
		• Secure Accounts with Multi-Factor Authentication
		• Conditional Access: Location-Based Access Control
		• Email reconnaissance: How attackers gather intel
		• Mail Server Hardening: DISA & CIS
		• Activity - Evaluate your organization's exposed internal mail headers
	Responding to Email Attacks	• Email defenses: Validate, Mitigate and Remediate
Module 4: Forensics Evidence Collection	Memory Acquisition: Live & Dead Systems	
	Disk Acquisition: Encryption & Write-Blocking	
	Triage Image: Efficient Evidence Collection	
	Acquiring Disk Images: Windows and Linux Systems	
	Mounting Forensic Images: Analysis Tools & Techniques	
Module 5: Disk Forensics	Windows Event Logs: structure & Analysis	
	Windows Registry: Structure and Analysis	
	Profiling Windows Systems	
	Collecting Network connections, and devices	
	Tracking User Activity	
	Tracking File Activities: NTFS Forensics	
	Linking User Actions to Files/Folders	
	Detecting USB Device Intrusions	

	Analyzing Installed Applications	
	Analyzing Execution Activities	
Module 6: Memory Forensics	Collecting OS Info	
	Processes Analysis	
	Network Artifact Analysis	
	Detecting Persistence Techniques	
	Collecting NTFS Artifacts	
Module 7: Network Forensics	Traffic Statistics	
	Conversations & Streams	
	Files' Extraction	
Module 8: Threat Hunting and Emulation	Comprehensive Threat Hunting Techniques	● Proactive Human-driven Threat Hunting
		● The Importance of Proactive Threat Hunting
		● Essential Requirements for Effective Threat Hunting
		● Stages of Threat Hunting in Detail
	Elastic SIEM, Kibana, and Advanced Threat Detection	● Elastic SIEM: Modern, Scalable Threat Detection
		● Elastic SIEM: Components and Architecture
		● Starting and Accessing Elastic Stack and Kibana
		● Elastic Agent and Fleet Management Overview
		● Enroll Elastic Agent via Fleet in Kibana

		• Exploring Kibana Concepts and Filtering Data
		• Dashboards and Data Visualization in Kibana
		• Creating a Custom Detection Rule with MITRE ATT&CK Framework
	Proactive Endpoint Threat Hunting and Analysis	• Endpoint Threat Hunting: Proactive Security Measures
		• Endpoint Hunting for Persistence
		• Endpoint Hunting for Lateral Movement
		• Endpoint Hunting for Credential Dumping
	Network Threat Hunting and Intrusion Detection	• Proactively Detecting Threats: Network Hunting Fundamentals
		• Network Hunting for Lateral Movement
		• Network Hunting for Data Exfiltration

Module 9: Malware Analysis	Static Analysis	• Fingerprinting Malware with Hashes
		• Antivirus Scanning to Confirm Maliciousness
		• Analyzing Packed Malware
		• Analyzing Obfuscated Strings
		• Automating Malware Analysis
	Dynamic Analysis	• Malware Execution Techniques
		• Monitoring Malware's Process Activity
		• Monitoring Malware's File Activity
		• Monitoring Malware's Registry Activity

		● Monitoring Malware's Network Activity
		● Sandboxes
	Microsoft Office files analysis	● VBA Macros Analysis
		● XLM Macros Analysis
		● RTF Macros Analysis
		● Automating the whole process
	PDF files analysis	● Extract Malicious Code from PDFs
		● JS - Static Analysis
		● JS - Dynamic Analysis
	Fileless Malwares	● PowerShell Analysis
		● Debug PowerShell Code: using PowerShell ISE