EC – Council Certified Incident Handler (ECIH)

Course Overview

This latest iteration of EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe.

It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

Following a rigorous development which included a careful Job Task Analysis (JTA) related to incident handling and incident first responder jobs, EC-Council developed a highly interactive, comprehensive, standards-based, intensive 3-day training program and certification that provides a structured approach to learning real-world incident handling and response requirements.

The E|CIH program includes hands-on learning delivered through labs within the training program. True employability after earning a certification can only be achieved when the core of the curricula maps to and is compliant with government and industry-published incident and response frameworks.

E|CIH is a method-driven program that uses a holistic approach to cover vast concepts concerning organizational incident handling and response from preparing and planning the incident handling response process to recovering organizational assets after a security incident. These concepts are essential for handling and responding to security incidents to protect organizations from future threats or attacks.

Course Objectives

- To enable individuals and organizations with the ability to handle and respond to different types of cybersecurity incidents in a systematic way.
- To ensure that organization can identify, contain, and recover from an attack.
- To reinstate regular operations of the organization as early as possible and mitigate the negative impact on the business operations.
- To be able to draft security policies with efficacy and ensure that the quality of services is maintained at the agreed levels.
- To minimize the loss and after-effects breach of the incident.
- For individuals: To enhance skills on incident handling and boost their employability.

Upon Completion, students will:

- Understand the key issues plaguing the information security world
- Learn to combat different types of cybersecurity threats, attack vectors, threat actors and their motives
- Learn the fundamentals of incident management including the signs and costs of an incident
- Understand the fundamentals of vulnerability management, threat assessment, risk management, and incident response automation and orchestration
- Master all incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Decode the various steps involved in planning an incident handling and response program
- Gain an understanding of the fundamentals of computer forensics and forensic readiness
- Comprehend the importance of the first response procedure including evidence collection, packaging, transportation, storing, data acquisition, volatile and static evidence collection, and evidence analysis
- Understand anti-forensics techniques used by attackers to find cybersecurity incident cover-ups
- Apply the right techniques to different types of cybersecurity incidents in a systematic manner including malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents

Who should attend?

- Penetration Testers
- Vulnerability Assessment Auditors
- Risk Assessment Administrators
- Network Administrators
- Application Security Engineers
- Cyber Forensic Investigators/ Analyst and SOC Analyst
- System Administrators/Engineers
- Firewall Administrators and Network Managers/IT Managers

Course Outline

Module #	Module Topic
Module 01	Introduction to Incident Handling and Response
Module 02	Incident Handling and Response Process
Module 03	Forensic Readiness and First Response
Module 04	Handling and Responding to Malware Incidents
Module 05	Handling and Responding to Email Security Incidents
Module 06	Handling and Responding to Network Security Incidents
Module 07	Handling and Responding to Web Application Security Incidents
Module 08	Handling and Responding to Cloud Security Incidents
Module 09	Handling and Responding to Insider Threats

Exam Details:

Exam Details	EC|IH® (MCQ Exam)
Number of Questions/Practical Challenges	100
Test Duration	4 Hours
Test Format	Multiple Choice Questions
Test Delivery	ECC EXAM, VUE
Exam Prefix	212-89(ECC EXAM), 312-50 (VUE)
Passing Score	70%

RF, Principal Security Consultant

Experience and Skills Summary:

RF has over 11 years of Information Security and technology experience providing latest security and infrastructure technologies delivery, solutions and services to different clients, implementing mid to high end solutions for enterprise customers.

RF has good knowledge in Security Operations Center Operations. In addition to that RF has extensive experience in SIEM, SOAR Platforms, two factor authentication, systems encryption, operating systems (UNIX, Linux and windows), enterprise software solutions, IT infrastructure solutions (Storage Systems, Servers, Backup) and other specialized security solutions.

Main Tasks and Expertise

- Project and Program Management
- Resource Management and Team Leading
- SOC Operations.
- SOC Assessment and Roadmap Definition.
- SOC Processes & Procedures Development.
- System Hardening.
- Incident Handling.
- Designing, Implementing and Maintaining Information Security Solutions.
- Developing Custom Security Training and Awareness Courses.
- Implementation and Configuration of RSA Envision SIEM RSA Security Analytics implementation and Operation.
- Implementation, Configuration and Operation of IBM Resilient SOAR Platform.
- Security Solutions Include: SIEM, Endpoint Security, Encryption, Firewalls, and Email Security, Two-Factor Authentication.
- Deployment and Configuration of Security Related Products & Solutions Including: RSA, SafeNet, Trend Micro, Symantec and IBM.
- Designing, Implementing and Maintaining Servers Infrastructure: Oracle, Dell, HP.
- Designing, Implementing and Maintaining Storage Systems: Oracle, EMC.
- Designing, Implementing and Maintaining Internet Services Applications: Apache, Bind, SendMail, Oracle Sun Internet Applications.
- Designing, Implementing and Maintaining Clustering Software: Oracle Sun, Symantec.

- Designing, Implementing and Maintaining Multiple Virtualization Platforms: EMC, Oracle Sun, and Microsoft.
- Implementing and maintaining different OSs: Solaris UNIX, RedHat and CentOS Linux, Microsoft Windows.

Accreditation and Certifications:

- Bachelor of Computer Engineering.
- RSA Security Analytics Analyst, *RSA.*
- Oracle Certified Professional, Oracle Solaris 10 System Administrator, *Oracle*.
- Oracle Certified Expert, Oracle Solaris 10 Network Administrator, *Oracle*.
- Microsoft Certified System Administrator, *Microsoft*.
- CIHE, Certified Incident Handling Engineer – Mile2.
- CPTE, Certified Penetration Testing Engineer – Mile2.
- Symantec Advanced Threat Protection Administration – ATP.
- Vectra Certified Implementation Engineer (VCIE).
- Vectra Pre-Sales Engineers (VPSE).
- EC-Council Certified Incident Handler (ECIHv2).
- ISO/IEC 27001:2013 Information Security Management Systems: Lead Implementer (BSI).

Key Projects Experiences:

1. **Technical Consultation:**

Client	Telecom – Saudi Arabia
Project Name	IBM SOAR Implementation
Team Size	1
Role	***Consultant***
Brief Project Description	IBM Resilient SOAR implementation, playbooks configurations, devices integration, incident response automation planning and implementation

2. **Technical Consultation:**

Client	Telecom – Morocco

Project Name	Managed Security Services Provider Development
Team Size	3
Role	***Consultant***
Brief Project Description	Security Operations Center Processes and Procedures development, covering Incident Handling, Monitoring, Cyber Forensics and Security Reporting.

3. **Technical Consultation:**

Client	Telecom – Turkey
Project Name	Security Operations Center Development
Team Size	2
Role	***Consultant***
Brief Project Description	Security Operations Center Processes and Procedures development, covering Incident Handling, Monitoring, Cyber Forensics and Security Reporting.

4. **Technical Consultation:**

Client	Airline – United Arab Emirates
Project Name	Security Operations Center Development
Team Size	2
Role	***Consultant***
Brief Project Description	Security Operations Center Processes and Procedures development, covering Incident Handling, Monitoring, Cyber Forensics and Security Reporting.

5. **Technical Consultation:**

Client	Banking – Saudi Arabia
Project Name	Security Operations Center Development
Team Size	3
Role	***Consultant***

Brief Project Description	Security Operations Center Processes and Procedures development, covering Incident Handling, Monitoring, TI, VM and SIEM administration processes.

6. **Technical Consultation:**

Client	Power – Saudi Arabia
Project Name	Security Operations Center Development
Team Size	3
Role	***Consultant***
Brief Project Description	Security Operations Center Processes and Procedures development, covering Incident Handling, Monitoring, TI, VM and SIEM administration processes.

7. **Technical Consultation:**

Client	Telecommunication – Saudi Arabia
Project Name	Security Operations Center Development
Team Size	4
Role	***Consultant***
Brief Project Description	Security Operations Center Processes and Procedures development, covering Incident Handling, Monitoring, TI, VM and SIEM administration processes.

Client	
Project Name	IT Security Assessment
Team Size	4
Role	***Sr. Cybersecurity Consultant***
Brief Project Description	• Minimum Security Baseline Development. • High Level Architecture Review. • Low Level Configuration Review.

8. **Security Solutions:**

Client	Oil – Saudi Arabia
Project Name	RSA Security Analytics for Packets and Logs Content Development
Team Size	1
Role	***Project Owner, Technical***
Brief Project Description	Consultation and professional services duties, Upgrade for old RSA SA, parsers creation and fixing for unsupported event sources, devices integration, new Rules and alerts creation in ESA (event stream analysis) and reporting engine, Dashboards and reports tuning and creation and use cases development.

Client	Banking – Saudi Arabia
Project Name	RSA Security Analytics for Packets and Logs Content Development
Team Size	3
Role	***Project Owner, Technical***
Brief Project Description	Consultation and professional services duties, New HW deployment, parsers creation and fixing for unsupported event sources, devices integration, new Rules and alerts creation in ESA (event stream analysis) and reporting engine, Dashboards and reports tuning and creation and existing Rules tuning.

Client	Multiple Clients – Saudi Arabia
Project Name	RSA Security Analytics SIEM.
Team Size	8
Role	***SOC Supervisor, Technical***
Brief Project Description	Oversee 8 SOC Analysts monitoring client RSA Security Analytics (SA) SIEM.

Client	Banking – Saudi Arabia

Project Name	RSA Security Analytics for Packets Upgrade
Team Size	1
Role	***Project Owner, Technical***
Brief Project Description	Oversee 8 SOC Analysts monitoring client RSA Security Analytics (SA) SIEM.

Client	Telecommunication – Jordan
Project Name	RSA Security Analytics SIEM.
Team Size	1
Role	***Project Owner, Technical***
Brief Project Description	Install, configure, device integration and maintenance tasks related to RSA SA.

Client	Telecommunication – Jordan
Project Name	RSA Envision SIEM.
Team Size	2
Role	***Project Owner, Technical***
Brief Project Description	Install, configure, device integration and maintenance tasks related to RSA envision.

Client	Government Hospital – Jordan
Project Name	RSA Envision SIEM.
Team Size	1
Role	***Project Owner, Technical***
Brief Project Description	Install, configure, device integration and maintenance tasks related to RSA envision.

Client	Banking – Jordan
Project Name	RSA Envision SIEM.
Team Size	3
Role	***Project Owner, Technical***

Brief Project Description	Install, configure, device integration and maintenance tasks related to RSA envision.

Client	Military
Project Name	RSA Envision SIEM.
Team Size	3
Role	***Project Manager, Technical***
Brief Project Description	Install, configure, device integration and maintenance tasks related to RSA envision.

Client	Banking - Jordan
Project Name	Vasco Two Factor Authentication – Identikey Server
Team Size	1
Role	***Project Manager, Technical***
Brief Project Description	Install, configure and support Vasco Identikey Server to be used for external VPN connections --- PCI Req.

Client	Banking - Jordan
Project Name	Symantec Encryption Server
Team Size	1
Role	***Project Manager, Technical***
Brief Project Description	Install, configure and support Symantec Encryption Server to be used to encrypt a file server --- PCI Req.

Client	Banking – Jordan
Project Name	RSA Envision SIEM.
Team Size	2
Role	***Project Owner ,Technical***
Brief Project Description	Install, configure, device integration and maintenance tasks related to RSA envision.

Client	Private Company – Jordan
Project Name	RSA Envision SIEM.
Team Size	1
Role	***Project Owner ,Technical***
Brief Project Description	Install, configure, device integration and maintenance tasks related to RSA envision.

9. **Enterprise Infrastructure Solutions:**

Client	Telecommunication – Jordan
Project Name	Oracle Sun Java Communications Suite
Team Size	1
Role	***Project Owner ,Technical***
Brief Project Description	This Project Consists Of Two Phases: 1- Install: This mean to install it as distributed solution. 2- Migration: migrate users (22000) from an old setup to the new one.

Client	Banking Sector – Jordan
Project Name	Oracle LDOMs Virtualization
Team Size	2
Role	***Project Owner ,Technical***
Brief Project Description	This Project ensured the delivery of entire needed virtualized infrastructure to be ready for Banking System.

Client	Education/University – Jordan
Project Name	EMC Storage System
Team Size	2
Role	***Project Owner ,Technical***
Brief Project Description	By This project; we Installed and fully configured a EMC VNX Storage with 4 DAE attached, so it then used for virtualization servers and DB servers.

Client	Government – Jordan
Project Name	Oracle Solaris Cluster
Team Size	2
Role	***Project Owner ,Technical***
Brief Project Description	By This project; we Installed Solaris OS, Updates, and then Solaris Cluster Binaries with needed configs to create HA cluster on the Oracle DB service.