SYLLABUS

INCIDENT HANDLING & RESPONSE PROFESSIONAL VERSION 1

The most practical and comprehensive training course on incident handling & response

eLearnSecurity
Forging security professionals

eLearnSecurity has been chosen by students in over 140 countries in the world and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto security to be free

COURSE GOALS

The Incident Handling & Response Professional course (IHRP) is an online, self-paced training course that provides all the advanced knowledge and skills necessary to:

- Professionally analyze, handle, and respond to security incidents on heterogeneous networks and assets;
- Understand the mechanics of modern cyber-attacks and how to detect them;
- Effectively use and fine-tune open source IDS, log management, and SIEM solutions; and,
- Detect and even (proactively) hunt for intrusions by analyzing traffic, flows and endpoints, as well as utilizing analytics and tactical threat intelligence.

Thanks to the extensive use of Hera Lab and the coverage of the latest research in the incident handling & response field, the IHRP course is not only the most practical training course on the subject but also the most up to date.

Penetration Testers and Red Team members can also benefit from this course; this is due to the fact that the IHRP course provides invaluable and in-depth information regarding detection tactics and procedures, that, if studied, could result in stealthier penetration testing or red teaming activities. More specifically, the course covers detection tactics and procedures against all stages of the cyber kill chain.

COURSE ORGANIZATION

The training course is entirely self-paced with interactive content that students can access online without any limitation. Students have lifetime access to the training material and can also study from home, the office, or anywhere an internet connection is available.

The Incident Handling & Response Professional v1 course is integrated with Hera Labs, the most sophisticated virtual lab in IT Security. A minimum of 60 hours is advised. For more intensive use, 120 hours may be necessary. Hera Lab provides a dedicated and isolated environment where a student can practice topics seen in the course.

TARGET AUDIENCE AND PRE-REQUISITES

The IHRP training course benefits the career of SOC Analysts, CSIRT members, Incident Handlers, Incident Responders, Red Team members who want to understand blue team tactics and deliver stealthier penetration tests, and IT Security personnel in charge of defending their organization's assets.

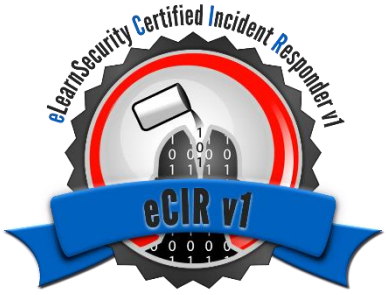
This course allows organizations of all sizes to effectively and timely analyze and respond to recurring alerts and incidents by building strong, practical in-house skills.

Organizations can now train their teams with a comprehensive and practical training course without having to deploy internal labs that are often outdated and not backed by solid, theoretical material.

A student who wants to enroll in the course must possess a solid understanding of networking, protocols, operating systems and security devices.

No programming skills are required. However, snippets of code will be used during the course.

WILL I GET A CERTIFICATE?



The IHRP course leads to the eLearnSecurity Certified Incident Responder v1 (eCIRv1) certification.

The certification can be obtained by successfully completing the requirements, which is a practical incident response exam that consists of a complex, real-world infrastructure hosted in our eLearnSecurity Hera Labs.

An eCIRv1 voucher is included in all the plans of the IHRP course.

ORGANIZATION OF CONTENT

The student is provided with a suggested learning path to ensure the maximum success rate at the minimum effort.

SECTION 1 – INCIDENT HANDLING OVERVIEW

The Incident Handling Overview section will introduce you to the Incident Handling Process. Specifically, the **Preparation** -> **Detection & Analysis** -> **Containment, Eradication & Recovery** -> **Post-Incident Activity** cycle will be covered in detail. Additionally, Incident handling procedures, activities and best practices for maximizing efficiency and performance, as well as reducing important security metrics such as *time to detect*, *time to respond* and *points of risks per host* are also covered.

- Module 1: Incident Handling Process

SECTION 2 – NETWORK TRAFFIC & FLOW ANALYSIS

The Network Traffic & Flow Analysis section will cover how you can detect intrusions or intrusion attempts by analyzing network traffic and network flows. This section consists of three modules that are accompanied by both the required theory and numerous hands-on labs, where you will be tasked with detecting real-world attacks and malware. More specifically, this section's modules are:

- Module 1: Intrusion Detection by Analyzing Traffic – Part 1
- Module 2: Intrusion Detection by Analyzing Traffic – Part 2
- Module 3: Intrusion Detection by Analyzing Flows

SECTION 3 – PRACTICAL INCIDENT HANDLING

The Practical Incident Handling section will cover how you can prepare and defend against each stage of the cyber kill chain. The goal of this section is to first educate you on the techniques, tactics, and procedures that modern adversaries use and then, make you capable of preparing and defending against them, using a variety of detection techniques, tools, logs, and events. More specifically, this section's modules are:

- Module 1: Preparing & Defending Against Reconnaissance & Information Gathering
- Module 2: Preparing & Defending Against Scanning
- Module 3: Preparing & Defending Against Exploitation
- Module 4: Preparing & Defending Against Post-Exploitation

SECTION 4 – SOC 3.0 OPERATIONS & ANALYTICS

The focus of the Practical Incident Handling Section was to educate you on the techniques, tactics, and procedures that modern adversaries use, as well as teach you how to detect them. Now, it is time to scale things up…

The SOC 3.0 Operations & Analytics Section first introduces you to the world of SIEM so you can become comfortable with working with some of the most effective and open-source SIEM solutions. You will then witness how common protocol analytics can greatly increase your network visibility in an attempt to detect abnormal and probably malicious actions at scale. Endpoint analytics are up next, covering the most important logs/events, correlation strategies and SIEM queries that you can leverage to detect adversaries on your network and endpoints. As usual, modules will be accompanied by hands-on labs, where you will be tasked with detecting real-world attacks and malware. As this section progresses, you will also see how tactical threat intelligence and adversary simulation can help you upgrade your detection capabilities.

- Module 1: SIEM Fundamentals & Open Source Solutions
- Module 2: Logging
- Module 3: SMTP, DNS & HTTP(S) Analytics
- Module 4: Endpoint Analytics
- Module 5: Creating a Baseline & Detecting Deviations

MODULE 1: INCIDENT HANDLING PROCESS

The Incident Handling Process module will introduce you to the **Preparation** -> **Detection & Analysis** -> **Containment, Eradication & Recovery** -> Post-Incident Activity cycle (a.k.a incident response life cycle).

Additionally, Incident handling procedures, activities and best practices for maximizing efficiency and performance, as well as for reducing important security metrics such as time to detect, time to respond and points of risks per host are also covered.

1.1 Incident Handling Definition & Scope
1.2 Incident Handling Process
- 1.2.1 Incident Handling Process – Preparation
- 1.2.2 Incident Handling Process – Detection & Analysis
- 1.2.3 Incident Handling Process – Containment, Eradication & Recovery
  - 1.2.3.1. Before Containment
  - 1.2.3.2. Short-term Containment
  - 1.2.3.3. System Back-up
  - 1.2.3.4. Long-Term Containment
  - 1.2.3.5. Eradication
  - 1.2.3.6. Recovery
- 1.2.4 Incident Handling Process – Post-Incident Activity

1.3 The Course's Scope
1.4 Incident Handling Forms
1.5 Appendix
- Windows Cheat Sheet
- Linux Cheat Sheet

MODULE 1: INTRUSION DETECTION BY ANALYZING TRAFFIC – PART 1

In this module, you will first learn to detect attacks in the IEEE 802.x Link and IP layers. Both IPv4 and IPv6 are covered.

1.1 Network Concepts & Analysis
- 1.2.1 Communication Models
- 1.2.2 TCP / IP
- 1.2.3 Request for Comments (RFC)
- 1.2.4 Traffic Analysis Tools

1.2 Analyzing & Detecting IEEE 802.x Link Layer Attacks
- 1.2.1 The Network Access / Link Layer
- 1.2.2 ARP's Security Shortcomings
  - 1.2.2.1 ARP Attacks & Detection
  - 1.2.2.2 ARP Spoofing Prevention
- 1.2.3 Other Sniffing Attacks & Detection
- 1.2.4 802.11 Wireless

1.3 Analyzing & Detecting IP Layer Attacks
- 1.3.1 The IP Layer
- 1.3.2 Important IPv4 Fields
  - 1.3.2.1 Abusing Fragmentation & Detection
- 1.3.3 IPv6
  - 1.3.3.1 Important IPv6 Fields
  - 1.3.3.2 IPv6 Fragmentation
  - 1.3.3.3 Abusing IPv6 Fragmentation & Detection
- 1.3.4 IPv6 Tunneling
- 1.3.5 ICMPv6
- 1.3.6 IPv6 Security Shortcomings

MODULE 2: INTRUSION DETECTION BY ANALYZING TRAFFIC – PART 2

This module starts by covering how to analyze common application protocols for suspicious behavior or abnormalities. Then, you will learn how to effectively leverage open-source IDS solutions to detect real-world attacks and also how to fine-tune them. Snort, Bro and Suricata will be covered.

- Analyzing common application protocols for suspicious behavior or abnormalities
- Effectively using open source IDS solutions
  - Snort
  - Bro
  - Suricata

2.1 Analyzing & Detecting Transport Layer Attacks

2.2.1 TCP
- 2.2.1.1 Suspicious TCP Traffic
- 2.2.1.2 Sequence Number Prediction & SYN Scanning
- 2.2.1.3 Source Port Abnormalities
- 2.2.1.4 Destination Port Abnormalities
- 2.2.1.5 TCP RST Attack
- 2.2.1.6 TCP Session Hijacking
- 2.2.1.7 TCP Options Abuse
  - 2.2.1.7.1 TCP Timestamps Option
  - 2.2.1.7.2 Leveraging TCP Option Support & Ordering

2.2.2 UDP

2.2.3 ICMP
- 2.2.3.1 ICMP Abuse
  - 2.2.3.1.1 ICMP Address Mask Request / Reply
  - 2.2.3.1.2 ICMP Timestamp Request / Reply
  - 2.2.3.1.3 Smurf Attack
  - 2.2.3.1.4 ICMP Tunneling
  - 2.2.3.1.5 Abusing ICMP Redirect

2.2 Analyzing Common Application Protocol Traffic & Attacks

2.2.1 Microsoft-specific Protocols
- 2.2.1.1 NetBIOS
- 2.2.1.2 SMB
- 2.2.1.3 MSRPC
  - 2.2.1.3.1 MSRPC Over TCP Session

2.2.2 HTTP(S)
2.2.2.1 HTTP
2.2.2.2 HTTPS
2.2.3 SMTP
2.2.4 DNS

2.3 Effectively Using Open Source IDS (Lab-based)

MODULE 3: INTRUSION DETECTION BY ANALYZING FLOWS

In this module, you will learn about intrusion detection by analyzing flows. For example, volumetric discovery, anomalous DNS discovery, SMB anomalies and visualizing flows will be leveraged to detect intrusions, lateral movement, malware beacons, etc.

- Volumetric discovery
- Anomalous DNS discovery
- Anomalous SMB discovery
- Visualization to support detection

3.1 Network Flows: Definition, Strengths & Limitations
3.1.1 Definition & NetFlow Overview
3.1.2 Strengths & Limitations

3.2 Network Flow Analysis Toolkit
3.2.1 YAF
3.2.2 SiLK
3.2.3 FlowViewer

3.3 Practical Flow Analysis
3.3.1 Case 1 – Beaconing Malware
3.3.2 Case 2 – Enriching Network Flow Data
3.3.3 Case 3 – Detecting Anomalous DNS Activity
3.3.4 Case 4 – Detecting Anomalous SMB Activity
3.3.5 Case 5 – Visualizing Network Flow Data (iSiLK)

MODULE 1: PREPARING & DEFENDING AGAINST RECONNAISSANCE & INFORMATION GATHERING

In this module, you will learn all of the techniques attackers use to perform reconnaissance and information gathering activities, as well as how to prepare and defend against them.

The techniques to be detected range from Google/Shodan "hacking" to DNS interrogation and reconnaissance through exposed OWA, JavaScript injection, SSL certificates, etc.

1.1 Reconnaissance/Information Gathering: Definition
1.2 Reconnaissance Techniques & Defense
- 1.2.1 Whois information analysis
- 1.2.2 SSL certificate information analysis
- 1.2.3 Utilization of search engines, internet-wide scanners & other sites
- 1.2.4 DNS interrogation
- 1.2.5 Abusing exposed OWA
- 1.2.6 Reconnaissance through JavaScript Injection

MODULE 2: PREPARING & DEFENDING AGAINST SCANNING

In this module, you will learn all the techniques attackers use to perform scanning activities, as well as how to prepare and defend against them.

The techniques to be detected range from war dialing and war driving to nmap/nessus scans and WebRTC-based scans.

2.1 Scanning: Definition
2.2 Scanning Techniques & Defense
- 2.2.1 War Dialing
- 2.2.2 War Driving
- 2.2.3 Nmap/Masscan/Nessus Scans
- 2.2.4 WebRTC-based Scans

MODULE 3: PREPARING & DEFENDING AGAINST EXPLOITATION

In this module, you will learn all the techniques, tactics and procedures that attackers use to gain an initial foothold into a network, as well as how to prepare and defend against them.

The attacks to be detected range from Passive/Active sniffing and remote/web attacks to misusing/brute-forcing Microsoft authentication.

3.1 Exploitation: Definition
3.2 Exploitation Techniques & Defense
- 3.2.1 BGP Hijacking
- 3.2.2 Passive & Active Sniffing
  - 3.2.2.1 SSL Stripping
    - 3.2.2.1.1 Sslstrip+
- 3.2.3 Remote Exploits
- 3.2.4 NetNTLM Hash Capturing & Relaying
- 3.2.5 Remote Linux Host Attacks
  - 3.2.5.1 Password Spraying
  - 3.2.5.2 Samba Vulnerabilities & Misconfigurations
    - 3.2.5.2.1 CVE-2007-2447
    - 3.2.5.2.2 Samba Symlink Directory Traversal
  - 3.2.5.3 Shellshock
  - 3.2.5.4 Heartbleed
  - 3.2.5.5 Java RMI Registry Exploitation
  - 3.2.5.6 Exploiting Insecure Java Deserialization
- 3.2.6 Denial of Service Attacks
  - 3.2.6.1 DNS Amplification Attacks
  - 3.2.6.2 Botnet-based Attacks
- 3.2.7 Malicious Macros

MODULE 4: PREPARING & DEFENDING AGAINST POST-EXPLOITATION

In this module, you will learn all the techniques, tactics and procedures that attackers employ in order to escalate their privileges and move laterally as well as vertically after an initial foothold is gained.

Detecting RATs, rootkits, possible attack path identification attempts, and credential reuse are covered, alongside detection techniques such as privileged access monitoring/privilege escalation detection, abnormal system interaction monitoring, log editing detection, covert channels detection, and persistence detection. The whole spectrum of Kerberos attacks (overpass-the-hash, kerberoasting, etc.) is also covered.

4.1 Post-exploitation: Definition
4.2 Post-exploitation Techniques & Defense
- 4.2.1 Privilege Escalation
  - 4.2.1.1 Windows Privilege Escalation
    - 4.2.2.1.1 Stored Credentials
    - 4.2.2.1.2 Insufficiently Secure Service Registry Permissions
    - 4.2.2.1.3 Unquoted Service Path
    - 4.2.2.1.4 Insufficiently Protected Service Binary
    - 4.2.2.1.5 Always Install Elevated
    - 4.2.2.1.6 Exploiting the Windows Kernel and 3rd-Party Drivers for Privilege Escalation
    - 4.2.2.1.7 Abusing Windows Privileges for Privilege Escalation
  - 4.2.1.2 Linux Privilege Escalation
- 4.2.2 Credential Theft & Cracking or Reuse (for Lateral Movement)
  - 4.2.2.1 Windows Authentication Weaknesses
    - 4.2.2.1.1 LM / NTLMv1
    - 4.2.2.1.2 NTLMv2
  - 4.2.2.2 SMB Relay
    - 4.2.2.2.1 Responder & Inveigh
  - 4.2.2.3 Pass the Hash
  - 4.2.2.4 Pass the Ticket
  - 4.2.2.5 Overpass the Hash
  - 4.2.2.6 Forged Kerberos Tickets
    - 4.2.2.6.1 Golden Tickets
    - 4.2.2.6.2 Silver Tickets

4.2.2.7 Keberoast
4.2.2.7.1 SPN Scanning
4.2.2.8 DCSync
4.2.2.9 DCShadow
4.2.2.10 Password Spraying
4.2.3 Remote User Enumeration
4.2.4 Lateral Movement
4.2.4.1 Remote File Copy over SMB
4.2.4.2 Remote Execution
4.2.4.2.1 Remote Execution Through WMI
4.2.4.2.2 Remote Execution Through WinRM
4.2.4.2.3 Remote Execution Through PS Remoting
4.2.5 Persistence
4.2.5.1 Registry Persistence
4.2.5.2 Scheduled Tasks / Cron Jobs
4.2.5.3 WMI
4.2.5.3.1 Empire WMI Persistence
4.2.5.4 Linux Rootkits

MODULE 1: SIEM FUNDAMENTALS & OPEN SOURCE SOLUTIONS

In this module, you will get accustomed to working with some of the most effective and open-source SIEM solutions such as Customized ELK Stacks and Splunk.

1.1 SIEM: Definition, Benefits & Solutions
1.2 SIEM Components, Architecture & Capabilities
1.3 SOC 3.0 Operations
- 1.3.1 State of the SOC
- 1.3.2 SOC 3.0 Operations

MODULE 2: LOGGING

This module will cover actionable Windows logging, including additional auditing.

2.1 Windows Logging
- 2.1.1 Account Management Events
- 2.1.2 Account Logon and Logon Events
- 2.1.3 Access to Shared Objects
- 2.1.4 Scheduled Task Logging
- 2.1.5 Object Access Auditing
- 2.1.6 Audit Policy Changes
- 2.1.7 Process Tracking
- 2.1.8 Auditing PowerShell

MODULE 3: SMTP, DNS, & HTTP(S) ANALYTICS

In this module, you will witness how common protocol analytics can greatly increase your network visibility, in an attempt to detect abnormal and probably malicious actions. More specifically, you will see how you can extract actionable intrusion-related information by performing SMTP, DNS, HTTP, and HTTPS analytics.

3.1 **SMTP Analytics**
- 3.1.1 Phishing Domain Identification
- 3.1.2 Malicious Attachment Identification

3.2 **DNS Analytics**
- 3.2.1 Detecting DNS Tunneling

3.3 **HTTP(S) Analytics**
- 3.3.1 HTTP Analytics
- 3.3.2 HTTPS Analytics

MODULE 4: ENDPOINT ANALYTICS

In this module, you will learn about the most important logs/events, correlation strategies, regex usages, and SIEM queries that you can leverage to detect adversaries on your endpoints at scale. You will also see how tactical threat intelligence and adversary simulation software can help you upgrade your endpoint adversary detection capabilities. Effectively using Osquery to interrogate endpoints (at scale) is also covered.

4.1 Endpoint Analytics
- 4.1.1 Attackers Leveraging Native Windows Binaries
- 4.1.2 Remote Privileged User Enumeration
- 4.1.3 PowerShell Executing an Encoded Script
- 4.1.4 Mimikatz (Binary)
- 4.1.5 PSExec
- 4.1.6 rundll32
- 4.1.7 Beaconing Malware
- 4.1.8 Malicious PowerShell Activity
- 4.1.9 Unauthorized DNS Server Interactions
- 4.1.10 SQL Injection
- 4.1.11 WMI Persistence
- 4.1.12 UAC Bypass Through Windows Event Viewer
- 4.1.13 net.exe Accessing an Administrative Share
- 4.1.14 Lateral Movement via Scheduled Tasks

MODULE 5: CREATING A BASELINE & DETECTING DEVIATIONS

In this module, you will witness how baselining your environment can result in easier, more efficient and more effective intrusion detection. A basic baselining methodology will also be provided.

5.1 Baselining & Deviation Detection Example
- 5.1.1 RDP Activity Baselining
- 5.1.2 RDP Lateral Movement Detection

ABOUT US

We are eLearnSecurity.

Based in Santa Clara, California, with offices in Pisa, Italy, and Dubai, UAE, Caendra Inc. is a trusted source of IT security skills for IT professionals and corporations of all sizes. Caendra Inc. is the Silicon Valley-based company behind the eLearnSecurity brand.

eLearnSecurity has proven to be a leading innovator in the field of practical security training, with best of breed virtualization technology, in-house projects such as Coliseum Web Application Security Framework and Hera Network Security Lab, which has changed the way students learn and practice new skills.

Contact details:

www.elearnsecurity.com
contactus@elearnsecurity.com

2040 Martin Ave.
Santa Clara, CA, USA

Via Gian Battista Queirolo
Pisa, Italy

Apricot Tower, Dubai Silicon Oasis
Dubai, UAE