# Cyber Security and Incident Response

40 hours

## Description

Wawiwa's Cyber Security and Incident Response program is a one of a kind program, specifically aimed to meet the ever growing need of incident response handling aspects in cyber security for people with no cyber experience.

## Expectations and Goals

In this program, students will gain an introduction to incident response, learn how to handle common security incidents, perform malware analysis and digital Forensics investigation during the incident, deep dive into insider threats and malware threats, and get familiar with the cyber threat intelligence world.

## Learning Objectives

By graduation, a student would be able to perform these responsibilities:

- Understand the incident response plan and methodologies
- Detect, identify and contain most common cybersecurity incidents
- Look for suspicious activity of malwares and malicious code on an organization's endpoints
- Analyze malwares with several techniques (static and dynamic)
- Find, collect, and perform a forensics investigation of digital evidence
- Look for cyber threat intelligence feeds with online and Open Source tools

## Target Audience

- IT staff
- Network engineers / administrators
- Incident handlers and leaders of incident handling teams
- System administrators
- IT security practitioners and security architects who want to design, build, and operate their systems to prevent, detect, and respond to attacks
- Students for technological bachelor's degree

# Prerequisites

- Basic knowledge of Microsoft Windows Operating Systems
- Understanding of networks and protocols
- Basic knowledge of monitoring and security devices

# Virtual Lab

***The course uses envario ™ virtual labs , an Israeli based Cyber virtual lab***

Wawiwa provides the center with a unique cloud environment with the following Virtual Machines:

- Clean VM (Win10 64-bit) – For first Lab Installation
- Malware Analysis VM (Win10 64-bit)
- Digital Forensics VM (Win10 64-bit)
- Certificates

Students are expected to bring their own laptops, unless the center has appropriate training classes with computers. Hardware requirements: Intel: i3 or higher, Win 10, Min 8GB RAM

Internet bandwidth at home - minimum base connection speed of 100 Mbps down is required, Internet latency less than 50ms.

# Classroom Facility

A fully equipped classroom, with the required multimedia infrastructure. At list 2 screens of 50” or higher connected to the instructor working station

a. Workstations with internet communication,

b. Minimal requirements for student’s workstation (per student) and 1 for Instructor:

1. Windows 10 OS, MS office
2. Intel: i5 processor or higher
3. x64-compatible 2.0 GHz CPU minimum or higher
4. 8 GB RAM minimum
5. 250 GB SSD available hard-drive space

6. Laptop or stationary computer workstation recommended monitors of 22” or larger

c. Minimum base connection speed of 100 Mbps down is required, Internet latency less than 50ms.

## Practical Learning (Hands-On)

- 25 academic hours of hands-on activities during the program
- Hands-on activities on local environments

## What Graduates Receive

- Wawiwa Graduate Certificate (co-branded with the center)
- Program presentation file (PDF) via an LMS
- Cheat sheet with useful documentation
- Incident Response "Swiss Army Knife" - 3GB of IR tools

## Program Syllabus

| Main Module | Hours + Labs |
|---|---|
| **Module 1 - Event Handling Methodologies (IR)**<br>• Cyber Security Technologies<br>• Cyber Security Operation Center<br>• SOC building Blocks<br>• Common Cyber Security Terminologies<br>• Internal/External communication<br>• Critical assets<br>• Risk assessment<br>• Events VS Incidents<br>• NIST Framework<br>• IR Phases | **4** |
| **Module 2 - Cyber Simulations**<br>• Cyber real life use cases simulations | **2** |

| | |
|---|---|
| **Module 3 - Response to cyber events**<br>• Incident Record and Documentation<br>• Incident Report<br>• Monitoring and Investigation Tolls<br>• Common Security Mitigation Tools<br>• Common Cyber Security Incidents Handling | **4** |
| **Module 4 - Introduction to the world of attack**<br>• Introduction to Cyber Attacks<br>• Threat Actors<br>• Threat Vectors<br>• Attack Cyber Kill Chain<br>• Common Terminologies | **2** |
| **Module 5 - Malware analysis**<br>• Malware Analysis Fundamentals<br>• Types of Malwares<br>• Malware Functionality (Behavior, Persistency, Encoding, etc.)<br>• Armored Malwares (Packing, Entropy, Fileless, etc.<br>• Investigation Techniques (Static and Dynamic)<br>• Basic Static Analysis<br>• Basic and Advanced Dynamic Analysis<br>• Common Investigation Tools<br>• Evasion Techniques<br>• Anti-Reverse-Engineering<br>• Anti-Disassembly<br>• Anti-Debugging<br>• Anti-Virtual Machine Techniques | **8** |
| **Module 6 - Digital Forensics**<br>• Introduction to Digital Forensics<br>• Know Your Lab and Tools<br>• Digital Forensics and Enforcement Of Law<br>• Windows Artifacts<br>• Memory Forensics<br>• Reporting and Clean-Up<br>• Memory Forensics and Registry Forensics | **6** |

| | |
|---|---|
| **Module 7 - Intelligence gathering in the cyber world**<br>• Introduction to CTI<br>• Defining Threats<br>• Tactics and Strategy<br>• Online Tools (Search Engines, Social Network, Pictures, etc.)<br>• OSINT (Maltego, Foca, Shodan, etc.) | **4** |
| **Module 8 - Cyber Challenge (CTF Platform)**<br>• Tailor made CTF<br>• CTF Solution | **4** |
| **Module 9 - Automation Systems and Orchestration - SOAR**<br>• Automation and Orchestration intro<br>• Get to know the TOP technologies<br>• SOAR – “The good, the bad and the ugly” | **2** |
| **Module 10 - Course Final BIT Project**<br>• Hands-On investigation Drill<br>• Bonus - Diving into the “Dark net” | **4** |

* Virtual labs are implemented using classroom facilities or can be provided 100% virtual (no need for facility only Bring Your own laptops)