CYBERGYM

Cyber Guardian Certification

Up the game of your in-house security specialists and turn them into multidisciplinary cyber security professionals

// CERTIFICATIONS

Up the game of your in-house security specialists and turn them into multidisciplinary cyber security professionals

Cyber Guardian

The volume and complexity of your security tasks often requires external specialists to supplement your own teams. Our **Cyber Guardian Certification Program** will take your IT professionals to the next level, giving them the skills and knowledge they need to manage and operate the entire incident lifecycle from first response, through mitigation and forensics.

Once certified, your cybersecurity teams, external service-providers, and decision-making executives will be able to rely entirely on your '**Cyber Guardians**' who will have a full understanding of the event, and how to manage it.

The **Cyber Guardian** program includes a Wcomprehensive body of knowledge, hands-on exercises and a live-training experience that covers all the details required to manage a cyber event - in real life.

Participants

- IT Professionals
- Computing and Networking Professionals
- Newly recruited Security Professionals

Results

- The ability to carry out the organization's initial and ongoing risk analysis
- The skills to perform initial analysis of suspicious cyber activity, differentiate between real cyber events and false alarms, as well as the knowledge required to react to ongoing cyber incidents, minimize damage and optimize the mitigation process
- The knowledge, experience and technical ability to perform the initial evidence collection and the forensic investigation of a cyber incident, and provide forensic experts with the required findings
- Competence to act as a single point of contact, as well as manage and liaise between the organization's technical teams, workforce, management and external experts and suppliers
- The knowledge required to correlate the organization's cyber-incident management and attack-mitigation processes with the organization's procedures and policies
- The credentials to act as the organization's leading cyber-defense authority, responsible for maintaining cybersecurity awareness among all employees

Duration

18 Days (in 8-hour training)

Syllabus

1

Network Security Concepts & Methodologies

Introduction to the key architectural and technological concepts of cyber security. Implementations and applications in: networking and communications, computer architecture, software development & execution.

2

Security Monitoring & Management

Tools, concepts and methods used to monitor and manage the network security infrastructure. Gain an essential understanding of the big security picture as well as a cybersecurity incident flow - unfolding within the organization's network.

3

Cybersecurity Awareness - Essentials Workshop

Cybersecurity Key threats, attack-patterns and risks in the cyber world; methods and concepts in protecting and attacking the organizations critical data assets.

4

Essential Tools for Cyber Investigation

Professional tools to investigate an incident, collect initial evidence, and extract the required information for use by the incident response team.

5

⚠ LIVE

Incident Response - Principal Tactics

Tools, skills and work methods utilized by an incident response team, within the organizational context, and during a live cyberattack in one of our Cyberwarfare Arena environment.

6

Cyber Crisis Management

Skills and concepts required for successful management of a major cyber incident and its damage to the organization, based on best practices and actual case studies. Including interfaces with the organization's executives, professionals and the different divisions.

7

⚠ LIVE

Ethical Hacking & Penetration Testing Principles

Principles, methodologies and tools for ethical hacking and penetration testing, covering key concepts such as exploitation, vulnerability, information gathering and more.
Including relevant practices, and hands-on experience within the Cyberwarfare Arena

8

Secure Software Development - A Basic Introduction

Basic principles for designing secure software architecture and developing secure code, utilizing known practices and techniques, such as input validation, authentication strategies, memory access protection and more.

9

⚠ LIVE

Cyber Forensics Overview

Internal processes, mechanisms, and stages of malware execution. Key tools and techniques for cyber evidence collection and initial forensics. Hands-on experience of evidence collection and forensic investigation during cyber attack.

10

Graduation Boot Camp

An intensive experience, summarizing all skills, tools, concepts and techniques covered during the program. The participants will be challenged with a series of live incidents, during which they will demonstrate their skills in collecting evidence, preventing attacks from spreading, analyzing the security situation and reacting in real time.

Upon successful completion of the boot camp, participants will be skilled and qualified for the role of real-life **Cyber Guardian.** They will receive the program's **Certificate of Completion** in recognition of having acquired the required proficiency.

About CYBERGYM

CYBERGYM provides tailored cyber-training solutions to organizations around the world. With the most relevant threat model and an environment configured to your technological setup, we make sure your people gain the experience they need, as individuals and as a team.

In addition to our hands-on training and live attacks, we cover theoretical knowledge, current offensive and defensive methodologies, case studies, and best practices. Trainees get to meet the actual attackers, ex-intelligence and security experts, to understand the hacker state of mind.

CYBERGYM further qualifies yours general workforce and executives, delivering an all-inclusive, organization-wide solution.

Founded in 2013 by experienced veterans of Israel’s prestigious intelligence organizations, CYBERGYM gives you peace of mind knowing that your teams are always ready, and cyber investments are maximized.

The CYBERGYM experience

Maximize The Human Factor

We empower the most critical, yet vulnerable, part of your security - your people

Live Attacks

Hackers run complex attack scenarios in real time, sharing their logic & knowledge with your teams

Teamwork Under Fire

In our realistic environment, your teams maximize their strengths, build effective teamwork, and work together to defend the organization

Tailored for You

Our training programs are created to suit your industry, technologies, policies and a relevant threat model

Industries we serve

Banking & Financial Services // Energy & Utilities // Insurance // Government // Telecommunication // Education

For more details, contact us at :

Sales@cybergym.com | www.cybergym.com