Cyber Incident Response Specialist

Certification Plan

CYBERGYM

EXPECT THE UNEXPECTED

Cyber Incident Response Specialist

DESCRIPTION

Being a critical, multi-disciplinary and demanding role, the Incident Responder must have significant experience and knowledge in order to cope with all the complexities involved.
The "Incident Responder" training program, provided by Cybergym, allows a Cyber Guardian (or any security specialist with a relevant background), to upgrade his/her skills to become an effective and advanced provider of "the first line of defense" for the respective organization.

TARGET AUDIENCE

- Cyber Guardian
- Having solid background in the field of Cyber Security concepts and methodology
- Being familiar with the essential principles of Cyber Security – malware, APT, risk assessment, mitigation, etc.
- Mastering the basic principles of systems' and networks' security assessment and forensics
- Being familiar with basic concepts and methods of cyber crisis management
- Being familiar with basic concepts and methods of cyber crisis management

OUTCOMES

- Get familiar with the advanced tools, skills and work methods utilized by an Incident Response team in an enterprise, and train their actual usage in the Cyber Arena environment.
- Learn the theory and get hands-on experience with the tools and methods of advanced Incidence Response management.
- Learn about advanced tools, methods and principles of Cyber Incident detection – including analysis and investigation of Linux Operating Systems-based environments.
- Undergo high-intensity hands-on experience, executing actual APT scenarios in the Cyber warfare Arena environment.

CERTIFICATE TRAININGS

1

Incident Response - Principal Tactics

Main Goals:

A comprehensive training program that includes the theoretical principles and practical exercises required to manage and lead organizational cyber incident response processes. Trainees will gain in-depth knowledge of critical concepts and tools in the field of incident response.

The training program's content, case studies, tools, hands-on experiences, and methods are targeted explicitly for managing, investigating, and analyzing organizational cybersecurity and incidents, including:

- Managing corporate security policies and ensuring compliance with standards and regulations
- Developing and updating organizational policies and procedures
- Evaluating the extent of damage and assigning responsibilities
- Detecting and mitigating real-life APTs

Outcome:

Acquire the necessary expertise, methodology and practical experience required to become a skilled First Responder or Incident Response team member in organizations of all sizes

2

Incident Response - Advanced Tactics

Main Goals:

Getting familiar with the advanced tools, skills and work methods utilized by an Incident Response team in an enterprise, and training their actual usage during an actual Cyber Attack in the Cyber Arena environment.

Outcome:

The trainee will learn the theory and get hands-on experience with the tools and methods of advanced Incidence Response management.

3

Graduation Boot Camp

Main Goals:

Intensive, multi-disciplinary experience, summarizing all the skills, the tools, the concepts, and the techniques learned during the course of the "Zero to Hero" program. The participants will be required to real-life-like Cyber Security Incident, use the tools and skills acquired during the program in order to collect evidence, prevent attacks from spreading, analyze the security situation and react in real-time.

The successful completion of the Boot Camp will allow each participant to effectively execute all the knowledge gained during the program, be prepared for the role of real-life Cyber Guardian, and receive the program's Certificate of Completion as a proof of the professionalism and experience acquired.

Outcome:

The trainee will bring to complete use and implementation the complete set of knowledge, methods, tools and experience gained during the course of the "Zero to Hero" program, achieving the final certification as a professional Cyber Guardian.