Vendor-Neutral Global IT Certifications

Star Incident Handler Expert

Prepare Yourself from Unforeseen Incidents

SIHE

Star Incident Handler Expert

Exam Code : S09-009

LEARN + EXAM = CERTIFIED

www.starcertification.org

info@starcertification.org

Star Incident Handler Expert

The threat of cybercrime is the new reality and major concern for enterprises worldwide. Unfortunately, most organizations, don't have a proactive approach to information security. Alarmingly, 76% of organizations globally do not have an Incident Response plan, making it difficult for them to reliably identify, contain and recover from a cyber-attack. An incident response plan prepares enterprises for both known and unknown threats.

Star Incident Handler Expert is a comprehensive certification training program designed to help learners acquire skills required to manage enterprise security incidents by understanding common attack techniques, vectors and tools, while avoiding common errors; thus, increasing both the effectiveness and efficiency of their incident response efforts.

The program introduces the learners to various incidents related to computer/information security, detailing all the aspects of incident handling from proper incident response management, to risk assessment and mitigation, to the techniques, policies and laws, further, to creating a proper incident response and recovery system for future. The purpose of SIHE is to help the learners master the skills they need to establish a successful career as an Incident Handler.

Audience: Intermediate to Advance. SIHE assumes that the User is already working in the IT Networking Field and Involved in Daily Operations and would like to be Part of Incident Management Operations.

Course Objectives:

In this course, you will learn about:

- How to prepare secure incident response system and understand the threats associated with such systems
- How to implement incident response system to prepare its defence against attacks
- Creating recovery plan based on the past attacks and threats
- Various network security incidents and malicious code incidents
- Internal threats and how to manage them

Course Outcome:

After completing this course, you will be able to:

- Explain incident response in an enterprise environment
- Develop an incident response plan and a response team
- List the policies and laws related to incident handling
- Manage the computer security related incidents and prepare for future risk mitigation, from malicious code attacks and threats associated
- Help organizations built their own Incident Management Systems
- Design a recovery plan and manage internal threats

Course Outline:

- Exploring Incident Response System and Risk Analysis
- Exploring Incident Handling Policies and Law
- Exploring Incident Response Handling and Creating an Incident Response Team
- Creating Incident Recovery Planning Documents
- Use of Forensic Analysis in Incident Response
- Identifying and Controlling Network Security Incidents
- Identifying and Controlling Malicious Code Incidents
- Managing Internal Threats

Labs

- How to implement GNU Privacy Guard (GnuPG)?
- How to perform Network Traffic Monitoring and Auditing using Ntopng and Nessus Home
- How to perform Network Traffic Monitoring and Auditing using Wireshark?
- How to perform Network Auditing using Snort
- How to Protect Network using iptables?
- How to perform Employee Monitoring by SpytechSpyAgent?
- How to Perform Forensic Analysis on Linux using Various Commands?
- How to use Sysinternals Suite to perform Forensic Analysis?

Exam Information:

Exam Code	:	S09-009	Exam Pattern	:	Multiple Choice
Exam Duration	:	2 Hrs	Exam Delivery	:	AEPTC (ACADEMIC EDUCATION & PROFESSIONAL TESTING CENTER)
Passing Score	:	70%			

Course Duration:

40 Hrs