Cybersecurity Specialization: Incident Handler

Duration: 2 Days   Course Code: GK840101

Overview:

Gain the knowledge and skills needed to manage and mitigate cybersecurity incidents effectively.
This course is designed to equip cybersecurity professionals with the essential knowledge and skills required to effectively manage and mitigate cybersecurity incidents. Learn various components and phases of incident response frameworks, explore state-of-the-art tools and techniques, and engage in practical exercises to hone their incident response capabilities.
By the end of this course, students will gain hands-on experience with industry-leading tools and techniques used in malware analysis, incident response, and threat hunting, and be equipped with the tools, techniques, and methodologies required to protect your organization from evolving cyber threats and ensure a resilient cybersecurity posture.
Our Cybersecurity Specialization courses follow the 9 pillars of Cybersecurity, providing key skills necessary to be successful as a cybersecurity professional.

Target Audience:

Strong technical skills and a desire to mitigate cyber attacks (Min. 2+ yrs exp. in security).This is an intermediate to advanced level course designed for:
- IT Security Analysts
- Network Administrators
- Forensic Analysts
- Security Operations Center (SOC) Team Members
- Information Security Managers
- Cybersecurity Consultants
- Incident Response Team Members

Objectives:

- Identify key components and phases of advanced incident response frameworks.
- List the tools and techniques used in malware analysis, incident response, and threat hunting.
- Explain the importance and function of each phase in an incident response framework.
- Describe the process and methodologies behind static and dynamic malware analysis.
- Demonstrate the use of advanced tools like SIEM, EDR, and forensic analysis software in handling cybersecurity incidents.
- Perform threat hunting exercises using industry-standard tools and techniques.
- Analyze complex incident scenarios to determine the root cause and impact.
- Compare different incident response frameworks and their application in various organizational contexts.
- Evaluate the effectiveness of incident response strategies and frameworks using predefined metrics.
- Assess emerging threats and trends to determine their potential impact on cybersecurity defenses.
- Design a customized incident response framework tailored to specific organizational needs.
- Develop comprehensive incident reports and documentation based on real-world incident simulations.

Prerequisites:

- A security background looking to specialize in incident handling.
- Basic Knowledge of Cybersecurity Concepts
- Familiarity with Networking Fundamentals
- Experience with Operating Systems
- Introduction to Incident Handling
- Basic Knowledge of Malware Analysis
- Familiarity with Security Tools

- Understanding of Threat Landscape
- 9701 - Cybersecurity Foundations

Content:

Incident Response Frameworks and Advanced Techniques

- Advanced Incident Response Frameworks
- Progressive Cyber Incident Analysis Approaches
- Leading-Edge Malware Analysis Practices
- Threat Hunting and Proactive Defense
- Hands-on Practice:
- Advanced malware analysis exercise
- Threat hunting exercise
- Case studies: Discuss complex incident response scenarios and lessons learned

Incident Handling Tools and Emerging Trends

- Advanced Incident Handling Tools
- Emerging Threats and Trends
- Incident Response Automation and Orchestration
- Incident Response Metrics and Reporting
- Hands-on Practice:
- Incident response automation exercise
- Incident reporting exercise

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/