System Forensics and Incident Handling

Duration: 3 Days **Course Code: FOR** **Delivery Method: Virtual Learning**

Overview:

Forensics and Incident Handling are constantly evolving and are crucial topics in the area of cybersecurity. In order to stay on top of the attackers, the knowledge of the individuals and teams responsible for collecting digital evidences and handling the incidents has to be constantly enhanced and updated. This advanced training provides the necessary knowedge and skills required to find, collect and preserve data in a correct manner, analyze it and get to know as much about the incident as possible. This is an intense hands-on course covering the general approach to forensics and incident handling, network forensics, important aspects of Windows internals, memory and storage analysis, detecting indicators of compromise and the correct ways of reporting.

Target Audience:

IT professionals, Forensics and Incident Handling Specialists, Security Consultants, Enterprise administrators, infrastructure architects, security professionals, systems engineers, network administrators, IT professionals, security consultants and other people responsible for implementing network and perimeter security.

Objectives:

- **After completing this course you should be able to:**
- Understand the steps of the incident handling process
- Detect malicious applications and network activity
- Recognise common attack techniques that compromise hosts
- Detect and analyze system and network vulnerabilities
- Implement continuous process improvement by discovering the root cause of incidents

Content:

Module 1: Introduction to Incident Handling

- Types of Computer Security Incidents
- Signs of an Incident
- Incident Prioritization
- Incident Response and Handling Steps
- Procedures and Preparation

Module 2: Windows Internals

- Introduction to Windows Internals
- Fooling Windows Task Manager
- Processes and threads
- PID and TID
- Information gathering from the running operating system
- Obtaining Volatile Data
- A deep dive to Autoruns
- Effective permissions auditing
- PowerShell get NTFS permissions
- Obtaining permissions information with AccessChck
- Unnecessary and malicious services
- Detecting unnecessary services with PowerShell

Module 3: Memory Dumping and Analysis

- Introduction to memory dumping and analysis
- Creating memory dump - Belkasoft RAM Capturer and DumpIt
- Utilizing Volatility to analyze Windows memory image
- Analyzing Stuxnet memory dump with Volatility
- Automatic memory analysis with Volatile

Module 4: Indicators of compromise

- Yara rules language

Module 5: Storage Acquisition and Analysis

- Introduction to storage acquisition and analysis
- Drive Acquisition
- Mounting Forensic Disk Images
- Introduction to NTFS File System
- Windows File System Analysis
- Autopsy with other filesystems
- Building timelines

Module 6: Reporting – Digital Evidence

- This module covers the restrictions and important details about digital evidence gathering. Moreover, a proper structure of digital evidence report will be introduced.

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/