System Forensics and Incident Handling

Duration: 5 Days **Course Code: FOR**

Overview:

The secure infrastructure configuration should be the most important line of defense in every organization. Unfortunately, people, the most valuable resource, are not always aware of the level of security in their companies, possible points of entry, how operating systems are attacked, and how to protect the infrastructure from successful attacks which are sometimes caused by configuration mistakes. Understanding internal OS protection mechanisms and services/roles completely provides a huge impact on the whole infrastructure security level. Unfortunately, the problem is… rarely anyone has this impact!
This is a deep dive course on security operations: vulnerability management, anomalies detection, discovery of industry attacks and threats, understanding how compromised system or solution looks like, defining the indicators of the attack, incident handling also daily servicing on SIEM platform. We will also walk through the advanced access rights, password mechanisms, windows internals, PowerShell usage for security purposes, gaining unauthorized access, advanced DNS configuration and common configuration mistakes, forensics techniques, Active Directory security, IIS Security, debugging, advanced monitoring and troubleshooting and much more! Topics covered during this training will help you to walk in hackers' shoes and evaluate your infrastructure from their point of view.

The training focuses on detecting, responding, and resolving computer security incidents.:

Target Audience:

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 Response and Handling

- Types of Computer Security Incidents
- Examples of Computer Security Incidents
- Signs of an Incident
- Incident Prioritization
- Incident Response
- Incident Handling

Module 2: System and Network Security Mechanisms

- Integrity Levels
- Anti-malware Firewalls
- Application Whitelisting, Application Virtualization
- Privileged Accounts, Authentication, Monitoring,
- and UAC
- Whole Disk Encryption
- Browser Security
- EMET
- Dangerous Endpoint Applications Session Zero
- Privileges, permissions and rights
- Passwords security (techniques for getting and cracking passwords
- Registry Internals
- Monitoring Registry Activity
- Boot configuration
- Services architecture
- Access tokens
- Web Application Firewall
- HTTP Proxies, Web Content Filtering, and SSL Decryption
- SIMs, NIDS, Packet Captures, and DLP
- Honeypots/Honeynets
- Network Infrastructure – Routers, Switches, DHCP, DNS
- Wireless Access Points

Module 3: Incident Response and Handling Steps

- How to Identify an Incident
- Handling Incidents Techniques
- Incident Response Team Services
- Defining the Relationship between Incident Response, Incident Handling, and Incident Management
- Incident Response Best Practices
- Incident Response Policy
- Incident Response Plan Checklist

Module 4: Handling Network Security Incidents

- Denial-of-Service Incidents
- Distributed Denial-of-Service Attack
- Detecting DoS Attack
- Incident Handling Preparation for DoS
- DoS Response and Preventing Strategies
- Following the Containment Strategy to Stop DoS
- Detecting Unauthorized Access Incident
- Incident Handling Preparation
- Incident Prevention
- Following the Containment Strategy to Stop Unauthorized Access
- Eradication and Recovery
- Detecting the Inappropriate Usage Incidents
- Multiple Component Incidents
- Containment Strategy to Stop Multiple Component Incidents
- Network Traffic Monitoring Tools

Module 5: Handling Malicious Code Incidents

- Count of Malware Samples
- Virus, Worms, Trojans and Spywares
- Incident Handling Preparation
- Incident Prevention
- Detection of Malicious Code
- Containment Strategy
- Evidence Gathering and Handling
- Eradication and Recovery

Module 6: Securing Monitoring Operations

- Industry Best Practices
- Critical Security Controls
- Host, Port and Service Discovery
- Vulnerability Scanning
- Monitoring Patching, Applications, Service Logs
- Detecting Malware via DNS logs
- Monitoring Change to Devices and Appliances
- Leveraging Proxy and Firewall Data
- Configuring Centralized Windows Event
- Log Collection
- Monitoring Critical Windows Events
- Detecting Malware via Windows Event Logs
- Scripting and Automation
- Importance of Automation
- PowerShell

Module 7: Forensics Basics

- Computer Forensics
- Objectives of Forensics Analysis
- Role of Forensics Analysis in Incident Response
- Forensic Readiness And Business Continuity
- Types of Computer Forensics
- Computer Forensic Investigator
- Computer Forensics Process
- Collecting Electronic Evidence
- Challenging Aspects of Digital Evidence
- Forensics in the Information System Life Cycle
- Forensic Analysis Guidelines
- Forensics Analysis Tools
- Memory acquisition techniques
- Finding data and activities in memory
- Tools and techniques to perform memory forensic

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo