System Forensics and Incident Handling

Durée: 5 Jours **Réf de cours: FOR**

Résumé:

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.

Public visé:

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.

Objectifs pédagogiques:

- **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

Contenu:

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.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form"""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement