EC-Council ICS/SCADA Cybersecurity + Voucher d'examen

Durée: 3 Jours **Réf de cours: EICS-SCADA** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

Le cours ICS/SCADA Cybersecurity est un module de formation pratique qui enseigne les bases de la sécurité et de la défense des architectures réseau contre les attaques. Les participants apprendront à penser comme un pirate informatique malveillant pour défendre leurs organisations.
ICS/SCADA enseigne des méthodes puissantes pour analyser les risques possédés par l'infrastructure réseau dans les espaces informatiques et d'entreprise. Une fois que les concepts de base sont clairs, vous apprendrez un processus systématique d'analyse des intrusions et des logiciels malveillants. Après cela, vous découvrirez le processus d'investigation numérique et les techniques de réponse aux incidents lors de la détection d'une violation.

Cette formation interactive peut être suivie depuis n'importe quel site, votre bureau ou votre domicile. Global Knowledge vous enverra toutes les informations nécessaires avant le début du cours et vous pourrez tester les connexions.

Mise à jour : 03.03.2023

Public visé:

This course is designed for IT professionals who manage or direct their organization’s IT infrastructure and are responsible for establishing and maintaining information security policies, practices, and procedures. The focus in the course is on the Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) Systems.
- SCADA Systems personnel.
- Business System Analysts who support SCADA interfaces.
- System Administrators, Engineers, and other IT professionals who are administering, patching, securing SCADA, and/or ICS.
- Security Consultants who are performing security assessments of SCADA and/or ICS.

Pré-requis:

- Linux operating system fundamentals, including basic command line usage.
- Conceptual knowledge of programming/scripting.
- Solid grasp of essential networking concepts (OSI model, TCP/IP, networking devices, and transmission media).
- Understanding of basic security concepts (e.g., malware, intrusion detection systems, firewalls, and vulnerabilities).
- Familiarity with network traffic inspection tools (Wireshark, TShark, or TCPdump) is highly recommended.

Contenu:

Module 1: Introduction to ICS/SCADA Network Defense

- IT Security Model
- ICS/SCADA Security Model

LAB: Security Model

- Security Posture
- Risk Management in ICS/SCADA
- Risk Assessment
- Defining Types of Risk
- Security Policy

LAB: Allowing a Service

Module 2: TCP/IP 101

- Introduction and Overview
- Introducing TCP/IP Networks
- Internet RFCs and STDs
- TCP/IP Protocol Architecture
- Protocol Layering Concepts
- TCP/IP Layering
- Components of TCP/IP Networks
- ICS/SCADA Protocols

Module 3: Introduction to Hacking

- Review of the Hacking Process
- Hacking Methodology
- Intelligence Gathering
- Footprinting
- Scanning
- Enumeration
- Identify Vulnerabilities
- Exploitation
- Covering Tracks

LAB: Hacking ICS/SCADA Networks Protocols

- How ICS/SCADA Are Targeted
- Study of ICS/SCADA Attacks
- ICS/SCADA as a High–Value Target
- Attack Methodologies In ICS

Module 4: Vulnerability Management

- Challenges of Vulnerability Assessment
- System Vulnerabilities
- Desktop Vulnerabilities
- ICS/SCADA Vulnerabilities
- Interpreting Advisory Notices
- CVE
- ICS/SCADA Vulnerability Sites
- Life Cycle of a Vulnerability and Exploit
- Challenges of Zero-Day Vulnerability
- Exploitation of a Vulnerability
- Vulnerability Scanners
- ICS/SCADA Vulnerability Uniqueness
- Challenges of Vulnerability Management Within ICS/SCADA

LAB: Vulnerability Assessment

- Prioritizing Vulnerabilities
- CVSS
- OVAL

Module 5: Standards and Regulations for Cybersecurity

- ISO 27001
- ICS/SCADA
- NERC CIP
- CFATS
- ISA99
- IEC 62443
- NIST SP 800-82

Module 6: Securing the ICS network

- Physical Security
- Establishing Policy – ISO Roadmap
- Securing the Protocols Unique to the ICS
- Performing a Vulnerability Assessment
- Selecting and Applying Controls to Mitigate Risk
- Monitoring
- Mitigating the Risk of Legacy Machines

Module 7: Bridging the Air Gap

- Do You Really Want to Do This?
- Advantages and Disadvantages
- Guard
- Data Diode
- Next Generation Firewalls

Module 8: Introduction to Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

- What IDS Can and Cannot Do
- Types IDS
- Network
- Host
- Network Node
- Advantages of IDS
- Limitations of IDS
- Stealthing the IDS
- Detecting Intrusions

LAB: Intrusion Detection

- Log Analysis
- ICS Malware Analysis

LAB: ICS Malware Analysis

- Essential Malware Mitigation Techniques
- ICS/SCADA Network Monitoring
- ICS/SCADA IDS

Méthodes pédagogiques :

The EC-Council Advantage
With EC-Council, you'll get a chance to learn ICS/SCADA from industry experts. The training program is spearheaded by renowned SCADA expert, Kevin Cardwell. EC-Council's SCADA training uses multimedia learning with interactive formats such as lectures, illustrations, and simulations.
Apart from this, the training program is interactive, and the learning module is activity-focused, which is helpful for skill development.

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.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est 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 vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.