ICS-SCADA Cybersecurity

CODICE	**DT0244**
DURATA	**3 gg**
PREZZO	**2.100,00 €**
EXAM	

DESCRIZIONE

A causa del potenziale impatto di un attacco sulla sicurezza fisica delle comunità, dei dipendenti o dei clienti, la sicurezza ICS/SCADA è importantissima. I criminali informatici hanno già sviluppato minacce malware come Triton/TRISIS e Stuxnet che possono interrompere la tecnologia operativa industriale (OT).

Il corso ICS/SCADA Cybersecurity si concentra sui sistemi di controllo industriale (ICS) e sui sistemi di controllo di supervisione e acquisizione dati (SCADA).

Il corso di formazione ICS/SCADA Cybersecurity fornisce una formazione pratica che vi permetterà di apprendere le basi della sicurezza e di difendere le infrastrutture dagli attacchi. Verrà affrontato il concetto di "thinking like a hacker/pensare come un hacker" per apprendere le tecniche di difesa dai tipi di attacchi che vengono comunemente condotti contro le reti aziendali e di controllo IT del settore petrolifero e del gas.

Imparerete metodi efficaci per analizzare il rischio della rete IT e aziendale. Una volta poste le basi, si analizzeranno le best practice e le raccomandazioni per colmare il divario. Imparerete un processo sistematico di analisi delle intrusioni e delle minacce informatiche. Una volta acquisita la padronanza del processo di analisi, si verrà introdotti al processo di digital forensic e a come rispondere agli incidenti quando viene rilevata una violazione.

TARGET

Questo corso è stato progettato appositamente per i professionisti IT che sono coinvolti nella gestione o nella direzione dell'infrastruttura IT della loro organizzazione e che sono responsabili della definizione e del mantenimento di politiche, pratiche e procedure di sicurezza delle informazioni.

PREREQUISTI

- 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.

CONTENUTI

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