Securing SCADA

Course Outline - 4 days

1.Differences in Deployments of Industrial Control Systems (ICSs)
- 1.1. Describe critical sectors and their importance.
- 1.2. Define industrial control system.
- 1.3. Identify the different types of processes and their dependencies.
- 1.4. Recognize the types of facilities that support critical infrastructure

2.Influence of Common Information Technology (IT) Components on Industrial Control Systems (ICSs)
- 2.1. Describe common IT components.
- 2.2. Identify where IT components are located within the IT infrastructure.
- 2.3. Explain common IT vulnerabilities.
- 2.4. Describe network model components and how they apply to IT communications.

3.Common Industrial Control System (ICS) Components
- 3.1. Describe common ICS components.
- 3.2. Discuss data flow in an ICS.
- 3.3. Identify ICS architectures.
- 3.4. Recognize ICS communication topologies, methods, and physical media.
- 3.5. Discuss common protocols used in ICS.

4.Cybersecurity within Information Technology (IT) and Industrial Control System (ICS) Domains
- 4.1. Identify security concerns created by the integration of IT and ICSs.
- 4.2. Describe IT and ICS communication differences.
- 4.3. Describe IT and ICS operations differences.
- 4.4. Describe IT and ICS support differences.

5.Cybersecurity Risk
- 5.1. Describe the elements of the risk equation including threat, vulnerability, consequence, and likelihood.
- 5.2. Discuss the cultural and technical factors that have recently contributed to and caused an elevation in risk to ICSs.
- 5.3. Explain the security issues created by integrating IT systems with ICSs.

6.Current Trends (Threats)
- 6.1. Describe the three components of human threat.
- 6.2. Differentiate between the three categories of threat actors: main stream, organized, and terrorist and nation state threats.
- 6.3. Explain the risk curve as it relates to threat groups.
- 6.4. Describe intentional versus unintentional "insider" cyber threats.
- 6.5. Discuss threat trends for ICSs.
- 6.6. Describe attacker tools and techniques.

7.Current Trends (Vulnerabilities)
- 7.1. Identify the items that are vulnerable in an ICS.
- 7.2. Discuss the factors that contribute to ICS vulnerabilities.
- 7.3. Describe the four root causes of cyber vulnerabilities.
- 7.4. Describe existing DHS programs that assist asset owners and vendors in identifying ICS vulnerabilities.
- 7.5. Discuss device programming trends that could introduce vulnerabilities.

8.Determining the Impacts of a Cybersecurity Incident
- 8.1. Explain the three tenants of information security.
- 8.2.Discuss events that can lead to disruptions.
- 8.3. Describe loss of view, loss of control, and denial of service (DoS).

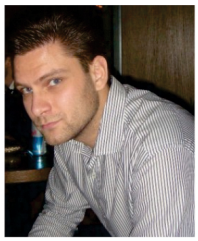
9.Attack Methodologies in IT and ICS
- 9.1. Describe the six most common elements in the life cycle of a cyber attack.
- 9.2. Explain cyber exploitation and how certain attack methods can apply to control systems.

10.Mapping IT Defense-in-Depth Security Solutions to ICS
- 10.1. Define defense in depth.
- 10.2. Create a baseline for defending your ICS.
- 10.3. Describe the first layer of defense: security management.
- 10.4. Describe the second layer of defense: physical security.
- 10.5. Describe the third layer of defense: network security.
- 10.6. Describe the fourth layer of defense: hardware security.
- 10.7. Describe the fifth layer of defense: software security.

centrul de strategii avansate

Heavy transports KIRS Forwarding Never out of transport solutions

www.sandline.ro | www.scada-security.ro | www.cyberguard.ro



SANDLINE IT CORE SECURITY

Radu Stănescu

CEO, Sandline

Radu Stanescu has over 10 years of experience in the IT Sec industry, focused on network and web application penetration testing and training services. He worked as an IT Security Consultant for several large companies from the public sector and among his certifications you can find CEH, ECSA, LPT, CEI,Security+, ISS, CCNA, CCAI and APT and custom Exploit Development.
Radu makes speaking appearances and gives seminars at security events such as HackerHalted, Hacktivity and DefCamp.

In early 2007 he started "Sandline" - an IT Security company focused on penetration testing and consultancy services.