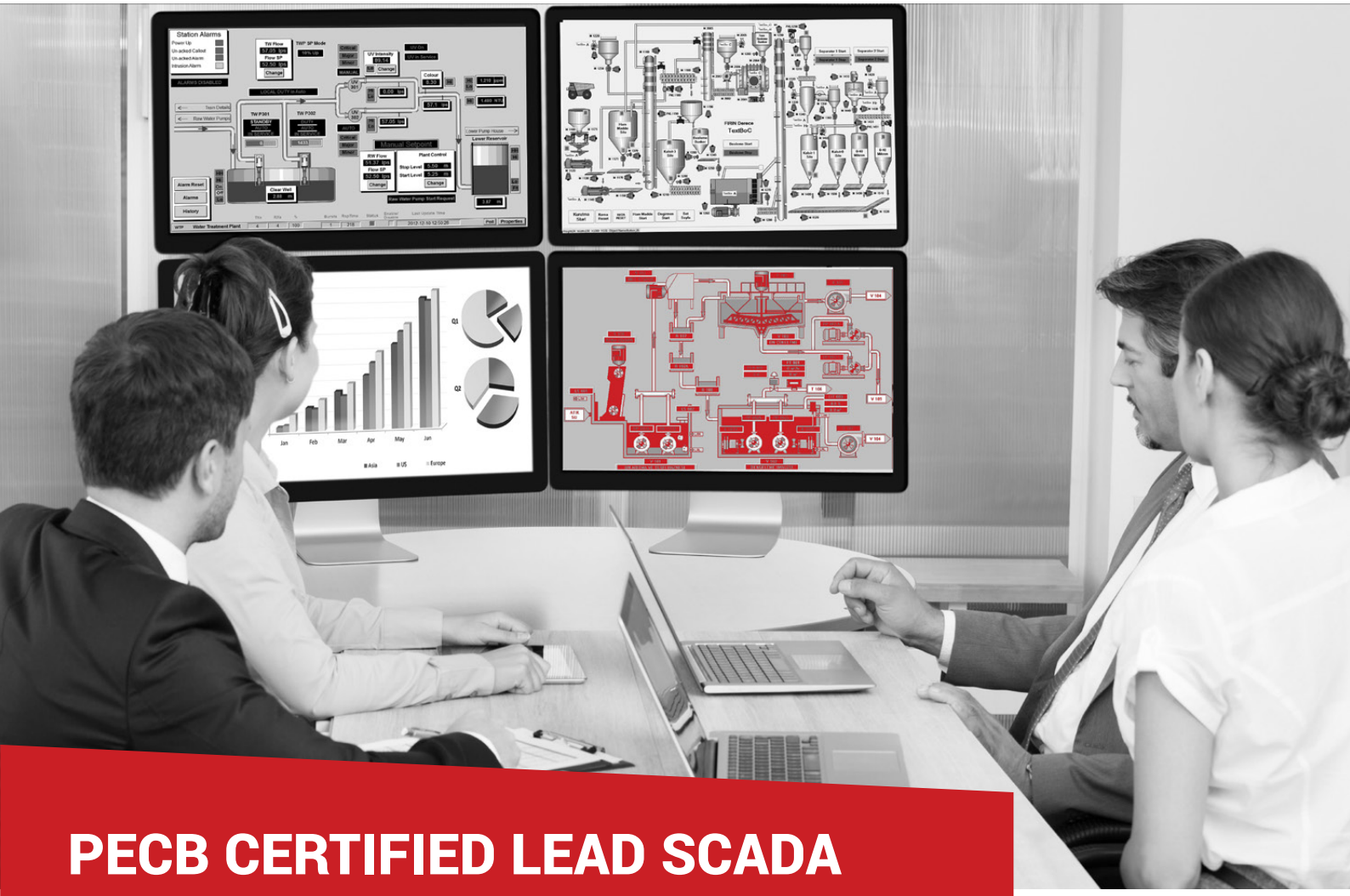
SPARTAN Allied Services
Deliver Results - Create Value

PECB



PECB CERTIFIED LEAD SCADA SECURITY PROFESSIONAL

MASTERING THE SKILLS OF A SCADA SECURITY PROFESSIONAL

SUMMARY

This five-day intensive course enables participants to develop the necessary expertise to plan, design, and implement an effective program to protect SCADA systems. Participants will be able to understand common Industrial Control System (ICS) threats, vulnerabilities, and risks related to ICS systems and how they can be managed. This training focuses on a mix of knowledge and skills related to SCADA/ICS security.

The course has been designed by industry experts with in-depth experience in SCADA and Industrial Control Systems Security. Unlike other certifications, this course focuses specifically on the knowledge and skills needed by a professional looking to advice on, or manage risks related to SCADA environments and systems. Given the high profile nature, and the significant impacts associated with such environments, a holistic professional approach to security is needed and that is exactly what this course is designed to provide.

In addition to presenting the theoretical knowledge needed by a SCADA Security Professional, a comprehensive methodology for the implementation is presented. Thus, at the end of this course, participants will gain knowledge on how to effectively implement a security program for SCADA/ICS systems.

WHO SHOULD ATTEND?

- Security professionals wanting to gain SCADA security professional skills
- IT staff looking to enhance their technical skills and knowledge
- IT and Risk Managers seeking a more detailed understanding of ICS and SCADA systems
- SCADA system developers
- SCADA Engineers and Operators
- SCADA IT personnel

COURSE AGENDA

DURATION: 5 DAYS

DAY 1

Introduction to SCADA and ICS with Fundamental Principles

- Course objective and structure
- Fundamental principles and concepts of SCADA and SCADA Security
- Industrial Control Systems (ICS) characteristics, threats and vulnerabilities

DAY 2

Designing a Security Program and Network Security Architecture

- SCADA Security Program, design, development and implementation
- Risk assessment
- Network security architecture for SCADA Systems

DAY 3

Implementing ICS Security Controls, Incident Management and Business Continuity

- Development and implementation of security controls for SCADA Systems
- Incident management in relation to SCADA
- Business Continuity and Disaster recovery
- Monitoring, measurement analysis and evaluation of SCADA security

DAY 4

Security testing of SCADA systems

- Testing principles
- Legal and ethical issues
- Penetration testing approaches
- Security testing of ICS
- Management of a penetration test
- Documentation of the test, quality review and report
- Maintaining a testing program

DAY 5

Certification Exam

LEARNING OBJECTIVES

- To understand and explain the purpose and risks to SCADA Systems, Distributed Control Systems and Programmable Logic Controllers.
- To understand the risks faced by these environments and the appropriate approaches to manage such risks.
- To develop the expertise to support a pro-active SCADA security program including policies and vulnerability management.
- To define and design network architecture incorporating defense in depth security controls for SCADA.
- To explain the relationship between management, operational and technical controls in a SCADA security program.
- To improve the ability to design resilient high availability SCADA systems.
- To be able to manage a program of effective security testing activities.

EXAMINATION

The "Certified Lead SCADA Security Professional" exam fully meets the requirements of the PECB Examination and Certification Programme (ECP). The exam covers the following competence domains:

1

Domain 1: Fundamental principles and concepts of SCADA and SCADA Security

Main objective: To ensure that the Certified Lead SCADA Security Professional candidate can understand, interpret and illustrate the main concepts and principles related to SCADA Systems and associated security concepts.

2

Domain 2: Industrial Control Systems (ICS) characteristics, threats and vulnerabilities

Main objective: To ensure that the Certified Lead SCADA Security Professional candidate can understand, the common threats and vulnerabilities related to ICS systems and how they can be managed.

3

Domain 3: Designing and Developing an ICS Security Program based on NIST SP 800-82

Main objective: To ensure that the Certified Lead SCADA Security Professional candidate can plan, design and implement an effective program to protect SCADA systems.

4

Domain 4: Network Security Architecture for SCADA Systems

To ensure that the Certified Lead SCADA Security Professional candidate can implement the processes of a SCADA required for its certification.

5

Domain 5: Implementation of Security Controls for SCADA Systems

Main objective: To ensure that Certified Lead SCADA Security Professional Candidate can understand the possible controls that can be applied to manage SCADA security risks along with the challenges, benefits and issues to be considered.

6

Domain 6: Developing Resilient and Robust Systems

Main objective: To ensure that the Certified SCADA Security Professional has a complete understanding of how SCADA systems should be resilient and recoverable in the event of an incident or major business interruption.

7

Domain 7: Security testing of SCADA Systems

Main objective: To ensure that the Certified Lead SCADA Security Professional candidate can organise and lead an effective program of security testing for key SCADA systems.

- The “Certified Lead SCADA Security Professional” exam is available in different languages (the complete list of languages can be found in the examination application form)
- Duration: 3 hours
- For more information about the exam, please visit: www.pecb.com

CERTIFICATION

- After successfully completing the exam, participants can apply for the credentials of Certified Lead SCADA Security Professional.
- A certificate will be issued to participants who successfully pass the exam and comply with all the other requirements related to the selected credential.

Exam	Professional Credential	Professional Experiencele	Testing Experience
Certified Lead SCADA Security Professinal	Provisional SCADA Security Professional	None	None
	Certified SCADA Security Professional	**Two years** One year of Information security work experience	200 hours
	Certified Lead SCADA Security Professional	**Five years** Two years of Information security work experience	300 hours

GENERAL INFORMATION

- Certification fees are included in the exam price.
- A student manual containing over 450 pages of information and practical examples will be distributed to participants.
- A participation certificate of 31 CPD (Continuing Professional Development) credits will be issued to participants.
- In case of failure of the exam, participants are allowed to retake the exam for free under certain conditions.