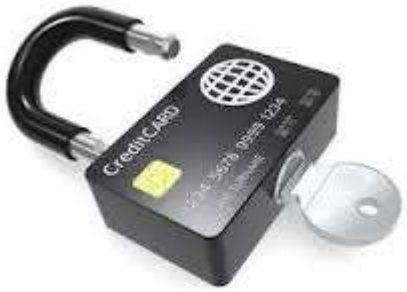
PCI DSS in Essence

Through practical examples



September, 2016
Septia Academy

PCI DSS in Essence

Training program specification

Overview

Introduction

The **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard's requirements are practices performed by many, but mastered by surprisingly few. And yet, the payoff from achieving excellence in these areas is large. This course addresses in detail the specific requirements of the PPCI DSS standard in terms of opening questions revealed from the implementation practice and answers them as effective requirements' specifications and recommendations.

PCI DSS in Essence is a practical one-day interactive program involving guidelines, roadmaps, examples, exercises, case studies and discussions. This training program has been developed to transfer the skills and expertise to those involved in maintaining various parts from the security in corporate networks, overviewed through the prism of the PCI DSS requirements.

Who Should Attend This Course? / Audience

The "PCI DSS in Essence" training course is designed for IT/IS Professionals, Security Officers, IT/IS Managers, who, in any capacity, deal with the PCI DSS requirements and tasks related to it.

Training Methods and Course Materials

For each course attended, you will be provided with:

- comprehensive course specifications, writing guidelines and notes;
- workshop model solutions;
- checklists, forms and charts which you can use immediately in your projects;
- a CD-ROM with extensive documents and resources;
- Information regarding access to web-resources and etc.;
- Post access to the presenter via phone and email for up to 3 months after the completion of the course.

Learning Objectives

Training Objective

The one-day "PCI DSS in Essence" course provides highly effective techniques and resources for understanding and surpassing the standard's requirements, in any predicted scenario or data-processing environment. A workshop-scenario approach is used extensively in this course, to maximize learning and practical application. Effectiveness of the techniques, collectively comprising a complete methodology, is independent of the domain of application, and independent of the specifics of the need.

After completing this course, the student will be able to:

- Describe the role and purpose of the PCI DSS requirements;
- identify a framework for organizing project in terms of fulfilling concrete requirements;
- Describe key steps involved in implementation of particular controls/requirements;
- Explain methods used in terms of accomplishing compliance;
- List tools and techniques for scoping and structuring specifications;
- Describe the methods to prepare system checks, drawings, plans and etc.;
- Determine the scope and adequate segregation of a Card-Holder-Data-Environment.

Key Questions

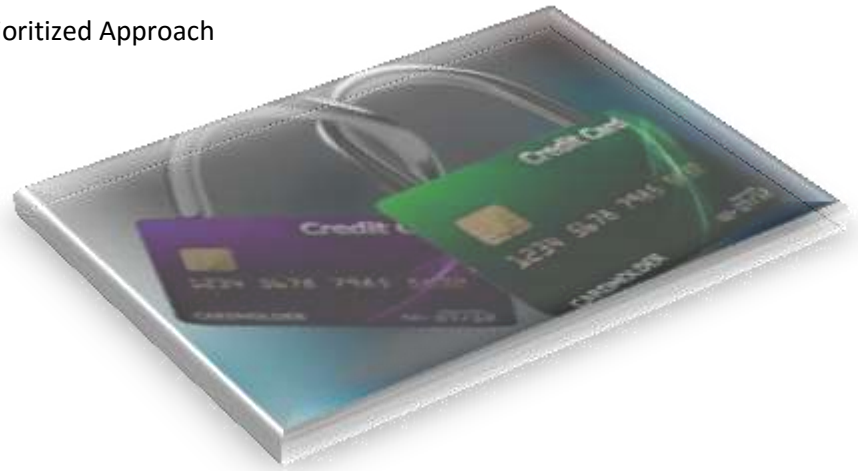
- To whom does PCI apply?
- What are the PCI compliance ‘levels’ and how are they determined?
- What is defined as ‘cardholder data’?
- How does the Prioritized Approach work?
- Can I report on my Prioritized Approach progress instead of producing a Report on Compliance or Attestation of Compliance?
- Are compliance certificates recognized for PCI DSS validation?
- Can a partial PCI DSS assessment be documented in a Report on Compliance (ROC)?
- Can I combine sections from different versions of the PCI DSS?
- Do QSAs and ASVs need to send reports of compliance (ROCs) or scanning results to the PCI Security Standards Council directly?
- What is the PCI DSS Self-Assessment Questionnaire?
- Which Self-assessment Questionnaire (SAQ) should I complete?
- Should service providers demonstrate PCI DSS compliance as part of their client's assessment or in their own separate assessment?

Outline

Day 1

- PCI DSS Overview
  - Attacks and Sources of Risk
  - PCI Tools
  - Goals and Requirements
- What is PCI compliance?
  - What is PCI validation?
  - What is required to become PCI compliant?
  - Security Standards Myths
- Requirements in Depth
- PCI DSS development and (its last version 3.2) Changes: What Your Business Needs to Know, What's New?
  - Multi-factor authentication required in and out the CDE - Security Beyond Passwords
  - Clarifying masking criteria
  - Change management process
  - Service Provider Written Agreement
  - New penetration testing requirements
  - Cryptographic architecture requirements
  - Establish a PCI DSS program
  - Quarterly personnel reviews
  - Timely detection and reporting
- Is Your Business Prepared for the Physical Security Threat?
  - Recognize Social Engineering Techniques
  - Social Engineering Training: What Your Employees Should Know
  - Ways to Social Engineer in Financial Institution
- Getting compliant and PCI DSS Compliance Trends
  - Pen-testing vs Vulnerability Scanning: What's the Difference?
  - Vulnerability Scanners: What, Why, and How to Comply
    - Spotting Vulnerabilities – Is Vulnerability Scanning Antiquated?
  - 10 Qualities to Look For When Selecting an Approved Scanning Vendor
- How to Prepare for a PCI DSS Audit
  - Reduce PCI DSS Scope
  - PCI DSS Risk Assessment Guidelines
  - Implement Data Security Best Practices
  - Role Based Access Control
  - Typical Anti-Virus for True PCI Requirement 5 Compliance
  - Firewalls, IPSs, SIEMs: Things You Should Know
    - How to make compliant configuration of a Firewall/SIEM
  - PCI Council Security Awareness Guidance
  - Internal Regulations and Records
- How Much Does PCI Compliance Cost?
  - Which PCI SAQ is Right for My Business?
  - PCI Compliance Scanning Requirements
  - How Much Does a Pen-test Cost?

- WorkShops
  - Understanding PCI DSS Prioritized Approach
  - Exam Exercise



Presenter / Speaker

Mr. Darko Mihajlovski

About the Presenter

With his 4 years' experience as an IT Systems Engineer, and 6 years hands-on experience in the field of Information Security, besides CISO's operations and governance in the Bank, currently working as responsible for PCI DSS implementation and maintenance in the Bank's Card-Holder-Data-Environment, as well.

Darko's educational status is Master of Science with Master thesis in the field of Industrial Information Security (SCADA Environment). His professional background is accompanied with several certifications in the field of information security, such as: Certified Ethical Hacker, Certified ISO27001:2013 Lead Auditor, BIA Implementer etc.

His resume includes several publications:

- Assessing Industrial Networks,
- Hacking Techniques performed in Industrial Environment,
- Compensation controls as an alternative method for PAN numbers encryption in MS SQL Database (PCI DSS 3.0 Chapter 3.4),
- Attacking IT-Defense Devices,
- Implementation of „SSL for ADO.Net" for Encryption of the Data In Transit in the Corporate Network (PCI DSS 3.1 Chapters 2.3, 4.1).