Common Criteria Developer Training Course Outline

Common Criteria version 3.1

atsec information security corporation
9130 Jollyville Road, Suite 260
Austin, TX 78759
Tel: +1 512 615 7300
Fax: +1 512 615 7301
www.atsec.com

Course Audience

This course is aimed at software development team members who will be involved in a Common Criteria evaluation in the NIAP CCEVS evaluation scheme.

Prerequisites: Basic knowledge of software development life cycle.

Course Goals

After completing this course, the developer will have the knowledge and skills to:

- understand and use the CC Parts 1,2, 3, the CEM, and additional CCEVS guidance
- understand his or her responsibilities in an evaluation process
- contribute to evaluation projects as a member of the evidence development team
- contribute to authoring a Security Target and provide other evaluation evidence

Course Objectives

Knowledge of CC history

Knowledge of CC organizations

- International
- U.S.

General knowledge of the overall CC standard structure

- Knowledge of the functional assurance paradigm
- Knowledge of how functional components cover functional requirements
- Knowledge of Evaluation Assurance Levels

Ability to understand security functional components as described in CC Part 2

- Knowledge of the functional requirements paradigm
- Knowledge of SFR class structure
    - Ability to describe the purpose of each SFR class
- Knowledge of SFR family structure
    - Ability to describe the purpose of each SFR family
    - Ability to navigate component hierarchy
    - Ability to trace Management requirements
    - Ability to trace Audit requirements
- Knowledge of SFR component structure
    - Ability to describe purpose of each SFR component
    - Ability to describe purpose of each SFR element
    - Ability to trace Dependencies
- Knowledge of component operations

Knowledge of CC evaluation process

- Understand the assurance concept

- Understand the information flow
- Understand the general certification process

Ability to apply security assurance components as described in CC Part 3

- Knowledge of the functional assurance paradigm
- Knowledge of SAR class structure
    - Ability to describe the purpose and application of each SAR class
- Knowledge of SAR family structure
    - Ability to describe the purpose of each SAR family
    - Ability to navigate component hierarchy
- Knowledge of SAR component structure
    - Ability to describe purpose & application of each SAR component
    - Ability to trace Dependencies
    - Ability to identify and describe application of assurance elements
    - Ability to trace Dependencies
- Knowledge of Evaluation Assurance Levels
    - Ability to describe the application of an EAL
    - Ability to differentiate the EALs

Course Duration and Style

This course is targeted for two full days in duration.

This course will be taught in workshop style, with presentations, instructor-led discussions, and hands-on exercises.

Course Outline

1. Statements of course
2. Brief Introduction to evaluations
   - 2.1. Business value of CC
3. International standard and documents
   - 3.1.1. History
   - 3.1.2. International CC organization
   - 3.1.3. CC documentation
4. U.S. National Scheme
   - 4.1. U.S. CCTL
   - 4.2. NVLAP
     - 4.2.1. Handbook 150
   - 4.3. NIAP, NSA
   - 4.4. CCEVS organization
     - 4.4.1. Definition
     - 4.4.2. CCTL
     - 4.4.3. Key resources within NIAP – Director, Deputy Director
     - 4.4.4. CCEVS publications
       - 4.4.4.1. Guidance documents
       - 4.4.4.2. Policy letters
5. Evaluation process overview
6. CC structure overview
   - 6.1. CC documentation
   - 6.2. Key documents produced for evaluation
     - 6.2.1. TOE overview
     - 6.2.2. ST overview
     - 6.2.3. PP overview
7. Evaluation of Protection Profiles and Security Targets
   - 7.1. Functional assurance paradigm
   - 7.2. Previews of simple development life cycle and class example TOE
   - 7.3. Discussion of PP and ST
     - 7.3.1. Purpose
     - 7.3.2. Dissection of document structures
       - 7.3.2.1. Introduction
       - 7.3.2.2. TOE description
       - 7.3.2.3. TOE security environment
         - 7.3.2.3.1. Threats
         - 7.3.2.3.2. OSPs

