RED ALERT LABS
IoT Security

COMMON CRITERIA

TRAINING PROGRAM

03 January 2018

TABLE OF CONTENTS

CHAPTER

1 - INTRODUCTION

This document provides an overview of the Common Criteria (CC) Training Program.

It includes a general presentation of the Security Certification Standard (ISO/IEC 15408), a detailed training program and the Keys of CC Project Management.

1.1 - Overview

Common Criteria is an international standard defining a framework for IT security evaluation and certification. It is used specifically to ensure that IT products meet standard security requirements for government or specific market deployments.

In summary, the end user needs a sort of trust that the products they purchase and use will meet their security requirements. CC certification provides value to that user by having independent third party examining and validating the claimed security requirements against recognized industry standard metrics and criteria. Moreover, the confidence increases if that third party is credible and accredited by a government certification scheme which is the case in the CC.

And finally the greatest benefit in Common Criteria is that it is indeed common to 26 different countries in the world. Meaning that a product could be evaluated once in one country and have that evaluation recognized and accepted in anyone of the 26 supporting countries and that is a huge benefit.

1.2 - Training Audience

IT product developers, engineering managers, product managers, consultants are all concerned in the CC certification process. In fact, CC could be viewed like a security vocabulary so that all these parties can communicate with the evaluators and certification schemes using the same terms. CC being a common language intended to describe products security characteristics.

The full training program targets mainly people involved directly in the CC evaluation process and a subset of it could also aim at those indirectly involved in the CC such as marketing/sales team, and final users.

1.3 - Training Goals

The intent of this training program is to provide useful information generic to all the parties involved in the CC certification process helping them understand all the key aspects of the CC evaluation process. It gives the beginners a good start and the experienced ones new techniques and best practices to improve the efficiency of CC evaluations.

After completing this training, the participant will have all the keys concepts to:

- define the Target of Evaluation (TOE) and Security Assurance Level (EAL).
- manage efficiently a CC evaluation project from A to Z.

- communicate efficiently with the involved third parties
- write evidence documentation

1.4 - Training Duration and Style

The complete CC Training Program requires 5 full days in duration and it could be split into the following 3 parts depending on the need:

- **CC (2 days)**
  - **Introduction to CC**
  - **Certification process**
  - **Best Practices and Lessons Learned**
- **CC+ (2 days)**
  - **CC Project Management in Practice**
- **CC++ (1 or 2 days depending on the product's type)**.
  - **Product Specifics (Workshop and Handout Materials)**

The training will follow a workshop style including presentations, interactive discussions, hands-on exercises and project's simulation.

[redacted]

CHAPTER

2 - TRAINING PROGRAM

This chapter provides the outline of the training program.

2.1 - Introduction to CC (1/2 day) – CC TRAINING PROGRAM

- What is CC?
    - Definition
    - History
    - International Organization
    - ICCC
    - Standard Structure
- CC facts
    - International Technical Committees
    - Collaborative Protection Profiles
    - CCMC Vision Statement
    - CCRA Transition Plan
    - Benefits
    - Costs
    - Schedule
    - Competition
    - Business Value
- CC Key definitions
    - Evaluation
    - Certification
    - Protection Profile
    - Security Functional Requirements
    - Security Assurance Requirements
    - Security Target
    - Evaluation Assurance Level
- Documentation
    - Security Target
    - Development Evidence
    - Lifecycle Support
    - Tests
    - Guidance
    - General Tips

2.2 - CC Certification Process (1 day) – CC TRAINING PROGRAM

- PHASE 1: PREPERATION
    - Get Started
    - Business Case
    - Resource Allocation
    - Managing Project Scope
    - Third Party Selection
    - Roles and Responsibilities
    - Defining the Target of Evaluation
    - Reading a collaborative Protection Profile
    - Writing a Security Target
- PHASE 2: CONDUCT
    - Create and Submit evidence documents
        - Development
            - Functional Specifications
            - Design
            - Implementation Representation
            - TSF Internals
            - Security Architecture
        - Testing
            - Functional Tests
            - Testing Coverage Analysis
            - Depth Testing
        - Guidance
            - Operational User Guide
            - Preparation User Guide
        - Life-Cycle
            - Life-cycle definition
            - Tools and Techniques
            - Life-cycle support
            - Configuration Management
- PHASE 3: RECOVER and/or FINALIZE
    - Evaluator’s Observation Reports
    - ETR
    - Receive Certificate
    - Re-Certification

2.3 - Best Practices and lessons learned (1/2 day) – CC TRAINING PROGRAM

- Choose the Country to Perform the Evaluation
- Allocate Time
- Minimize Changes to the Plan

- Meet Minimum Requirements
- Reuse Certification Materials
- Weekly Status Call with Evaluators
- Dedicated Technical Writer
- Synchronize Evaluation with Development
- The limits of Products Evaluation

2.4 - CC Project Management in Practice (2 days) – CC+ TRAINING PROGRAM

- Project's Scope
- Project Initiation
- Project Objectives
- Tasks Separation
- Team Organization & Resource Allocation
- Budget Estimation
- Consultants, Partner & Evaluation Lab selection
- Negotiations
- Evaluation work plan and Schedule (PERT, GANTT, AGILE)
- Risks
- Meetings
- Progress Status Control
- Conflicts & Reactions
- Reports & Control Chart

2.5 - Product Specifics (1 or 2 days) – CC++ TRAINING PROGRAM

- Workshop
    - cPP study
    - Applied SFRs
    - Semi-Formal Description
    - Use case study
    - Evidence Developments
- Handouts Materials
    - Example TOE
    - Evidence documents templates including guidelines
        - ASE
        - ADV
        - AGD
        - ATE
        - ALC

CONTACTS

Red Alert Labs

contact@redalertlabs.com

+33 9 53 55 54 11

www.redalertlabs.com

RED ALERT LABS
IoT Security