CBL101 – DEFENDING COBOL

Course Learning Objectives

Learn about how the confidentiality, integrity, and availability of your COBOL applications are affected by vulnerabilities such as injection attacks, column truncation, broken access control, logic errors, bypassed audit trails, debug code, and unsafe functions.

Description

This course is designed as an introduction to safeguarding mainframes that use the COBOL programming language.

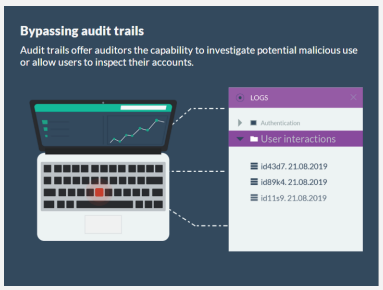
While COBOL implementations may vary extensively based on their platforms and environments, this course aims to provide an implementation-agnostic overview of COBOL's most common vulnerabilities.

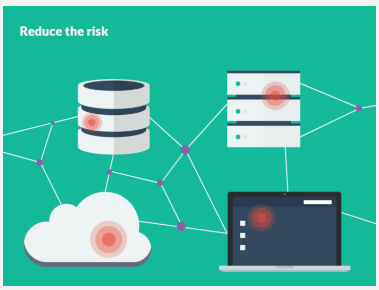
Audience

Developers

Time Required

Tailored learning - 30 minutes total





CBL101 – DEFENDING COBOL

Course Outline

1. Secure Coding - Part 1

- Reducing the risk
- CIA Triad
- The COBOL language
- COBOL program structure
- Common vulnerabilities in COBOL
- SQL injection
- Command injection
- Column truncation
- Broken access control

2. Secure Coding - Part 2

- Logic errors
- Bypassing audit trails
- Debugging in production code
- Segregation of privilege
- Static analysis tools
- Unsafe functions
- Analyzing COBOL programs

SecurityCompass