AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 07/06/2024

Sign up

PVID Training

2 days (14 hours)

Presentation

Our PVID (Remote Identity Verification Provider) training course will familiarize you with modern authentication techniques. You'll be able to identify and choose the different identity verification systems to integrate into your system.

Our program will start with an introduction to PVID, so you'll know what a successful identity check is all about, and the strengths and weaknesses of different authentication systems.

We'll take a closer look at the concepts of official document verification, fraud detection and biometric verification. You'll learn how to recognize the main techniques of identity theft, and how to identify flaws in your verification systems.

In conclusion, we'll teach you the criteria for choosing a PVID integration, so you'll know which PVID to select, thanks to a clear overview of the current leaders.

Objectives

- Detailed knowledge of the different types of identification
- Assess the reliability of an authentication technology
- The essential criteria for choosing a PVID

Target audience

- AI Engineers
- System administrators
- CISO

Prerequisites

Knowledge of IT security.

Our PVID training program

Introduction

- What is identity verification?
- What is PVID?
- What are the different methods of identity verification?
  - Official documents
  - Facial recognition
  - Digital recognition
  - Voice recognition
  - Iris identification
  - Questionnaires
  - Multi-factor authentication
  - Passwords
  - Behavioral analysis
- The advantages and disadvantages of different methods

Document authentication

- The benefits of automated authentication
- Design a reliable database of documents to verify authenticity
- Good scanning practices
- Data extraction vs. OCR recognition
- List of data to check
- Read the RFID chip

Biometric verification

- Active verification
- Passive verification
- How can you ensure the reliability of your biometric control system?

Fraud detection

- Types of fraud and how to avoid them
  - Skimming
  - Social engineering
  - Deep fakes
  - Synthetic identity theft
  - Credential stuffing
  - SIM swapping
  - Data breach
- Common practices of identity thieves

Choosing the right supplier

- Compliance with security and data protection standards
- Precision rate
- Geographical coverage
- Ease of integration
- Customer support
- Ease of use

Introducing the main players

- IDnow
- Onfido
- Jumio
- Sumsub
- Idenfy
- Veriff
- Idemia

Keycloak training

OpenCV training

Computer Vision training

Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.