# Zero Trust Security Boot Camp

Course: **00116**
Filter: **Beginner**
Duration: **20 hours**
Category:: **Cyber Security**
Price: **3000,00 €**

## About Course

Learn what zero trust security is, how it solves typical security issues, and how to implement it in your environment. In this Zero Trust Security Training, you'll learn about zero trust security. First, we'll teach you the basics, starting with understanding what "trust" actually is and from where the zero-trust model comes. Then, we will move to design considerations, and after that, we'll start discussing the actual technical implementation details. Zero trust security is not a new concept. Still, it has gained much more interest in the last couple of years as organizations of all kinds (government, for-profit, nonprofit) realize that their traditional security approach could be better. For example, in mid-2021, the US Federal CISO (Chief Information Security Officer) Chris DeRusha said the White House would push all federal agencies toward a "zero trust paradigm." Traditionally, organizations would put much effort into preventing access to resources from the outside world while leaving internal access relatively open because all their employees were in the same building, using devices managed by the organization. If a malicious person wanted access to the organization's resources, they would need to gain physical access to the building, which was quite challenging. Now, everything has changed with the ubiquity of connectivity (direct links with customers and suppliers, Internet of Things, remote work, etc.). Accessing "internal" resources via the Internet is much easier than gaining physical access to the building. And the "lock 'em out" approach is much less effective. Trusting a user because of who they are, their location, or their device becomes problematic – especially since bad actors can spoof all those things. Zero trust security is a concept that eliminates trusted locations, people, devices, or anything else. So instead of having unrestricted access to internal networks from specific locations or devices, you always require authentication and authorization from everywhere. This may seem like an unnecessary complication, but it makes things simpler. By implementing zero trust security, teams can focus on one best solution in all circumstances. And hackers no longer

get access to everything just because they succeeded in a single exploit. While zero trust sounds like it only refers to user access, we must remember to secure applications talking to one another. Traditionally, there were not many security constraints regarding applications or container networking. Typically, once the firewall rule was open from server A to server B, you could send any type of traffic. In the zero-trust networking model, you change that. Instead of traditional IP (Internet Protocol): PORT combination type firewalls, you implement transaction-level controls. Every necessary transaction is defined, and the access rules for each are defined. Then, when a particular application, device, or container needs to access a particular resource, it requests permission to perform a well-defined transaction.

## What you'll learn

- Implement Zero Trust tenets and concepts in your organization.
- Design Zero Trust Architecture
- Assess your organization's readiness for Zero Trust
- Mature your Zero Trust Implementation

## Targeted audience

- This boot camp does not have an exam, but students can request a certificate of completion.

## Pre-requisites

None

## Curriculum

### Module 1: Introductions

- Brief Evolution of IT (Information Technology) Security

- The Perimeter Model
- Brief Threat Landscape History
- Problems with the Traditional Model
- Brief History of Zero Trust
- Zero Trust AuthN & AuthZ
- Zero Trust Tenants
- Zero Trust Basic Concepts
- Team Knowledge Check

**Module 2: Zero Trust Network Design Part 1**

- Zero Trust 5 Steps of Transformation
- Zero Trust Threats
- Team Knowledge Check
- Zero Trust Access Control
- Mid-Team Quiz
- Zero Trust Risk Management
- Zero Trust Governance
- Zero Trust Vendor Selection
- Team Knowledge Check
- Zero Trust Reference Architecture
- Team Knowledge Check

**Module 3: Zero Trust Network Design Part 2**

- Team Knowledge Check
- Zero Trust Implementation
- Team Knowledge Check
- Zero Trust Migration
- Zero Trust Challenges
- Team Knowledge Check
- Zero Trust Wrap Up
- Final Team Quiz
- Ending - Bonus