Updated on 27/11/2023

Sign up

Zero Trust Security training

3 days (21 hours)

PRESENTATION

Zero Trust Security is a strategic cybersecurity model designed to protect all of an organization's digital assets and environments. Increasingly heterogeneous, these ecosystems are typically made up of mixed public and private clouds, SaaS applications, DevOps environments and automated robotic processes (APR).

Based on the principle of "Never Trust, Always Verify", it aims to protect digital environments by relying on four pillars: network segmentation, prevention of lateral movements, prevention of threats on the L7 layer and simplification of granular user access control.

Based on BeyondCorp software, it's one of the most effective ways for companies to control access to their networks, applications and data.

It incorporates a wide range of prevention techniques, including authentication and behavioral analysis, micro-segmentation, endpoint security and least privilege controls, to deter potential attackers and limit their access in the event of a breach.

Following our Zero Trust Security training course, you'll be able to assess a company's existing security model and implement a new zero-trust network within the organization.

OBJECTIVES

- Identify the challenges of traditional network design
- Understanding the need for network access to Zero Trust
- Describe the implications of the changing environment and the Cloud
- Identify Zero Trust network access features
- How to implement Zero Trust network access

TARGET AUDIENCE

- Developers
- IT security engineers
- Cybersecurity professionals

Prerequisites

- Basic knowledge of networking concepts
- Basic knowledge of corporate security
- Basic knowledge of information technology (IT)

Zero Trust Security training program

Zero-Trust fundamentals

- What is Zero Trust?
- Some definitions of Zero Trust
- Never trust, always check
- Zero Trust principles
- Zero Trust pillars
- Background to Zero Trust

Why do we need Zero Trust?

- Perimeter security pitfalls
- Digital transformation
- The state of Zero Trust
- Case study : From SolarWinds to Zero Trust

Zero Trust Architecture

- The NIST Zero Trust Architecture (ZTA) model
- Example of real ZTA solutions
- Approaches to the NIST ZTA architecture
- NIST ZTA deployment models

Zero Trust architectural pillars

- User and identity security pillar
- Securing Pillar appliances
- Securing the Network and Environment Pillar
- Application and workload security pillar
- Securing the data pillar
- Basic components

- Bringing everyone together
- Case study: Colonial Pipeline Colonial Pipeline

Zero Trust architecture design

- There's no easy way to reach Zero Trust
- Zero Trust design principles
- Zero Trust's five-step design methodology
- Forrester's five steps to Zero Trust

Migration to Zero Trust

- Building a business case for Zero Trust
- The challenge of change
- Creating a Zero Trust team
- Leveraging the Zero Trust implementation curve

Exploring ZTA use cases

- VPN-Less implementation
- East-West segmentation
- Secure access From anywhere
- Conditional authentication and authorization
- Microsoft ZTA step by step
- Exploring Cloudflare's Zero Trust roadmap

Zero Trust maturity models

- NSA Zero Trust Maturity Model
- Microsoft Zero Trust maturity model
- CISA Zero Trust maturity model
- Dod Target and advanced Zero Trust activities

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 confirmed, 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 with regard to the training to come, within the limits imposed by the format selected. This

The questionnaire also enables us to anticipate any connection or internal security problems (intra-company or virtual classroom) that 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.