Course Outline

Zero Trust Security Boot Camp
Course ZTSBC: 3 days Instructor Led

About this course
Zero trust security is not a new concept, but 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 doesn't work as well as they need. For example, in mid-2021, the US Federal CISO (Chief Information Security Officer) Chris DeRusha said the White House will push all federal agencies toward a "zero trust paradigm."

Traditionally, organizations would put a lot of 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 to get access to the organization's resources, they would need to gain physical access to the building, which was quite difficult to do.

Now, with the ubiquity of connectivity (direct links with customers and suppliers, Internet of Things, remote work, etc.), everything changes. 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 or their location or the device they are using becomes problematic – especially since all of those things can be spoofed.

Zero trust security is a concept that eliminates trusted locations, people, devices, or anything else. Instead of having unrestricted access to internal networks from certain locations or devices, you require authentication and authorization from everywhere and at all times. This may seem like an unnecessary complication, but it actually makes things simpler. By implementing zero trust security, teams can focus on one solution that works best 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 refers to user access, we can't forget about applications talking to one another. Traditionally, there weren't many security constraints when it came to applications or containers networking. Normally, 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: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 or devise or container needs to access a particular resource, it requests permission to perform a well-defined transaction.

In this course, you'll learn all about zero trust security. We'll teach you the basics starting from understanding what "trust" actually is and where the zero trust model came from. Then, we'll move to design considerations, and, after that, we'll start discussing the actual technical implementation details.

Audience profile
Professionals who may benefit include:

- Anyone in an IT Leadership role
- CIOs / CTOs /CSO
- Security Administrators
- Any Security Staff
- System Administrators
- IT Operations Staff

SHI | TRAINING & ADOPTION

Course Outline

- Release Engineers
- Configuration Managers
- Anyone involved with IT infrastructure
- Developers and Application Team leads
- ScrumMasters
- Software Managers and Team Leads
- IT Project & Program Managers
- Product Owners and Managers

At course completion
After completing this course, students will be able to:

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

Course Outline

Part 1: Zero Trust – What It Is and Is Not

1. What Is "Trust" in Your IT Infrastructure?
2. History of Zero Trust
3. Understanding the Zero Trust Concept
4. Benefits of Zero Trust

Exercise: *Small Group Discussions – How is Zero Trust different from our current approach to security?*

Part 2: Basic Tenets and Concepts of Zero Trust

1. 5 Zero Trust Tenets (US DoD – Zero Trust Ref Arch)
2. 7 Zero Trust Tenets (US NIST – SP 800-207)
3. A Zero Trust View of a Network (US NIST – SP 800-207)
4. Zero Trust Pillars & Capabilities (US DoD – Zero Trust Ref Arch)
5. Macro-Segmentation and Micro-Segmentation

Exercise: *Individuals or teams – Which Tenets would require significant changes for us?*

Part 3: Zero Trust Architectures

1. General Zero Trust Architecture Overview
2. Dynamic Access Control Plane (SOAR – Security Orchestration, Automation & Response)
    - Policy Engine
    - Inputs to the Policy Engine (Analytics & Confidence Scoring, SIEM – Security Information & Event Management, Threat Intelligence, Data Access Policy, etc.)
    - Policy Administration
3. Data Plane
    - Policy Enforcement Points

Course Outline

- Actor Authentication and Authorization (Person & Non-Person)
- Resource Authorization (Applications, Data & Other Resources)
- Logging & Auditing (SIEM – Security Information & Event Management)

Exercise: *Small Group Quiz – Collaborate to answer questions about Zero Trust Architectures*

Part 4: Zero Trust Use Cases

1. Enterprise with Satellite Facilities
2. Multi-Cloud / Cloud-to-Cloud Enterprise
3. Enterprise with Contracted Services and/or Nonemployee Access
4. Collaboration Across Enterprise Boundaries
5. Enterprise with Public- or Customer-Facing Services

Exercise: *Individuals or teams – Which Use Case most closely matches our organization?*

Part 5: Prerequisites to Implementing a Zero Trust Architecture

1. Discovery
    - Identify DAAS – Data, Assets, Applications, Services
    - Review Business Processes & Map Data Flows
    - Inventory Users & Devises
    - Identify Privilege Accounts
    - Log Network Traffic
2. Assessment
    - Determine Existing Compliance State
    - Determine Proper Account Privilege Levels
    - Identify if existing policies are based on “Least Privilege”

Exercise: *Individuals or teams – Which prerequisites do we already have? How can we complete the others?*

Part 6: Growing Maturity in your Zero Trust Implementation

1. Establish the Security Baseline
    - Grant assess to DAAS – Data, Assets, Applications, Services via security policy
    - Segment Networks with Default = Deny Access
    - Manage Devices Compliant with Security Policy
    - Implement Least Privilege Access
    - Use MFA – Multi-Factor Authentication
    - Begin Data Classification & Critical Data Tagging
    - Use Strong Encryption
2. Implement Intermediate Zero Trust Capabilities & Controls
    - Grant Assess to DAAS Based on Fine-Grain User & Devise Attributes
    - Use Micro-Segmentation Across the Majority of the Network
    - Authenticate Users Using an Enterprise Federated Identity Service
    - Enhance Least Privilege with a Privileged Access Management System
    - Begin Implementing DLP – Data Loss Prevention & DRM – Data Rights Management
    - Automate data tagging and classification

Course Outline

- Develop Baseline Security Policies Based on UEBA – User & Entity Behavior Analytics

3. Achieve Advanced Zero Trust Capabilities & Controls
    - Grant Assess to DAAS Dynamically using Robust Real-Time Analytics
    - Complete Micro-Segmentation of the Network
    - Implement Continuous & Adaptive Authentication & Authorization
    - Authenticate Users & Devices Using an Enterprise Federated Identity Service
    - Fully Implement Just-In-Time and Just-Enough Access Policy
    - Use machine Learning to automate most data tagging and classification
    - Complete Implementing DLP & DRM Using Data Tags
    - Automate & Orchestrate Threat Detection via Advanced Analytics

Exercise: *Individuals or teams – How close are we to achieving the Baseline, and what more must we do to get there? Which of the Intermediate and Advanced practices do we already have in place?*

Part 7: Our Path to Zero Trust

Exercise: *Individuals or teams* – Plan your organization's path to Zero Trust

1. Determine your starting point
    - Identify First Steps
    - Discuss strategy with classmates