Zero Trust Security Implementation for the Hybrid Enterprise

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC Education & Training Services

About this Workshop

In a nut-shell, the concept of a Zero Trust Security Architecture has been around for more than a decade, but adoption did not really begin to take hold until the past couple of years. Zero Trust is a framework for securing organizations in the cloud, on-premises and mobile world that asserts that no user or application should be trusted by default. Following a key zero trust principle, least-privileged access, trust is established based on context (e.g., user identity and location, the security posture of the endpoint, the app or service being requested) with policy checks at each step.

Target Audience

- Customers who want to build their knowledge in the space of Zero Trust security technology and are in the process of planning and implementing Zero Trust Security Architecture Framework in their organization.
- CIO/CISO/CTO, CRO, IT Directors/GM IT, C-SOC Manager, Risk and Business Technology Leaders, IT Managers, L1 Monitoring Teams, L2/L3 SOC Analysts, Incident Responders, Service Desk, Forensic Specialists, SIEM Administrators, Threat Intelligence teams, Threat Hunters, Strategic Technology Planners, Project Managers, Solution/IT/Systems Architects, Enterprise Architects, Network Operation teams , Information Security and Cybersecurity team and Technical Writers.

To view the list of our new and popular courses, please visit: www.tlcpak.com

Zero Trust Architecture is an alternative security model that addresses the fundamental flaw of traditional strategies that data only needs to be protected from outside of an organization. The **Zero Trust** model views data security through a new lens, enabling parameters that dictate access and restrictions.

Understand how **segmentation gateway** provides granular visibility into traffic and enforces additional layers of inspection and access control with granular Layer 7 policy based on the **Kipling Method.**

Zero Trust is an augmentation of your existing architecture, it does not require a complete technology overhaul. Rather, it can be deployed iteratively while allowing you to take advantage of the tools and technologies you already have.

Unit 1 – Zero Trust Security Architecture Framework and Implementation Strategy

- Understanding the Common IT Challenges.
- A Framework for Zero Trust – Three Key Phases, and the importance of Feedback Loop.
- Certain Myths and Confusions that need Attention from ZT Point-of-View.
- Understanding Zero Trust Architecture.
- Zero Trust architecture services – An Example.
- Putting Zero Trust Architecture into Practice.
- Differentiating between Untrusted Zone and Implicit Trust Zone.
- Zero Trust Architecture – Logical Components.
- Zero Trust Architectural Framework.
- Unleash the role of TCP/IP Session Layer and ZT Implementation.
- The Principles behind Zero Trust Security.
- How to achieve a Zero Trust Architecture.
- Describe Segmentation Gateway – An essential component of Zero Trust.
- Deploying Zero Trust using Kipling Method.
- Implementing Zero Trust Identity Management Principles.
- Following the Zero Trust Model.
- High-level Zero Trust Maturity Model Overview.
- Identity Governance and Administration Strategy.
- Implementing Zero Trust Identity Management Principles.
- ZT Architecture Implementation Example – Before and After.
- A layered Cyber Defense Approach – The bigger picture.
- Recommendations for starting a Zero Trust Journey.
- Digital Enterprise based on Zero Trust adoption – A Bigger View.
- Five Stages Determined Maturity Level for Zero Trust.
  - Mapping People, Process and Technology following SANS, ISO27001 and CMMI to measure enterprise security models.
- A Checklist to take you from Theory to Zero Trust reality.
- What are the threats to Zero Trust Architecture?
- Steps towards Zero Trust implementation strategy summary.
- Unit 1 Assessment.

Unit 2 – User and Entity Behavior Analytics Fundamental Principles

- UEBA – User and Entity Behavior Analytics Defined.
- Understanding UEBA Engines.
- Three pillars of UEBA – Use Cases, Data Sources, and Analytics.
- Exploring main components of UEBA.
- Convergence of UEBA and SIEM.
- UEBA and SIEM comparison and UEBA integration with SIEM.
- Similarities and Dissimilarities between SIEM and UEBA solution.
- Why do organizations need UEBA and How UEBA works and UEBA Threat Workflow.
- Enterprise Data Sources analyzed by UEBA.
- Facts for a successful implementation of UEBA solution.
- UEBA for Enterprise Security – A layered-wise approach.
- UEBA Risk Scoring and Threat Indicator Signs.
- UEBA for Enterprise Security for threat hunting and incident investigation.
- Critical Devices of UEBA Systems.
- Best Practices for building a baseline of User Behavior – Define Use case, Define Data Source, Define Behaviors, Establish the Baseline, Update Policies and Training Awareness Program, Conduct Testing, Rebuild Baseline.
- Unit 2 Assessment.

Security and networking teams globally have implemented or plan to implement Zero Trust, SASE, and SD-WAN soon – Are you ahead of the curve? – *A Ponemon Institute Survey*

62% are familiar with Zero Trust

45% are familiar with SASE

38% are familiar with SD-WAN

Over half of companies are already taking steps to deploy Zero Trust solutions

Zero Trust		SASE		SD-WAN	
20% have deployed	**37%** plan to deploy	**10%** have deployed	**39%** plan to deploy	**11%** have deployed	**34%** plan to deploy

Zero Trust Security Implementation for the Hybrid Enterprise

Skills and expertise to help you increase your knowledge in the field of digital technologies

TLC Education & Training Services

The need for having a SDP, CASB and SASE

When organizations shifted toward accelerated digital transformation to the cloud, the VPN became a bottleneck that was impossible to scale. This is where the need for having a Software Defined Parameter (SPD) arises.

In this massive shift to cloud applications and digital transformation, Cloud Access Security Brokers emerged. CASBs aim to mitigate risks around cloud assets when users access those assets from inside the organization's perimeter.

Choosing Between CASB and SASE

- CASB vs. SASE both offer benefits to enterprises depending on the situation and conditions.
- A CASB solution can be deployed as a standalone framework that easily integrates into an enterprise's existing security architecture.
- However, SASE is increasingly seen as the preferred option as it builds on CASB capabilities while simplifying security and maximizing the efficiency of a company's IT and security architecture under an Hybrid Model.

Hybrid Enterprise

Your hybrid enterprise needs secure network access that streamlines administration and enables business agility. Moreover, your remote, in-office and third-party users need simple, secure connections across wildly diverse on-premises, legacy and cloud environments. That's why you need Zero Trust Network Access (ZTNA) because traditional network access solutions are not built on the principles of Zero Trust.

Unit 3 – The Role of CASB and SASE in Implementing Zero Trust Security

- Cloud Management Components and Cloud Architecture.
- Cloud Computing Reference Architecture – CCRA.
- NIST Cloud Computing Reference Architecture.
- Pillars of Robust Cloud Security and Top Cloud Application Security Threats.
- Understand Cloud Access Security Broker.
- Security features offered by Cloud Access Security Broker.
- How Cloud Access Security Broker work?
- Requirements of a CASB Solution and why do I need a CASB solution?
- Cloud Access Security Broker Solution Deployment Models.
- Three key considerations for choosing a CASB.
- Multi-Mode Next-Gen CASB Architecture.
- Use Cases and Best Practices for Cloud Access Security Broker implementation.
- Cloud Access Security Broker Vs. Secure Access Service Edge.
- Privileged Access Management Defined.
- Unprivileged to Privileged Access Management using Zero Trust Architecture.
- Understand Secure Access Service Edge (SASE).
- SASE Architecture – CASB within SASE.
- Pros and Cons of SASE & CASB– Advantages and challenges for enterprises.
- Comparative Analysis on SASE Vs. CASB.
- Unit 3 Assessment.

Unit 4 – Exploiting Software Defined WAN Security

- Business Challenges that develop the need for considering an SD-WAN.
- What business problems does SD-WAN solve?
- Software-defined Wide Area Network (SD-WAN) Defined.
- Planning for your SD-WAN solution.
- SD-WAN Key Characteristics and benefits.
- Zero-Touch Provisioning – An impressive capability of SD-WAN.
- Main components that make up the basic structure of an SD-WAN.
- Main types of SD-WAN Architectures.
- MPLS defined and key difference between SD-WAN and MPLS.
- MPLS Vs SD-WAN – Pros and Cons.
- SD-WAN Architecture – Flexibility and Scalability.
- How does SD-WAN work?
- Build an effective SD-WAN security strategy at the branch.
- Three Models for an SD-WAN Deployment.
- Evaluate where to deploy the SD-WAN controller.
- Assess connectivity choices for SD-WAN deployment.
- SD-WAN Policy Types.
- Five Common SD-WAN Challenges.
- Five Steps to follow when Migrating MPLS to SD-WAN.
- SD-WAN and MPLS – Differentiating between the two technologies.
- Describe SD-WAN Orchestration – Orchestration Vs. Cloud Automation.
- SD-WAN Use-cases and key Checkpoints.
- Unit 4 Assessment.

Remote work has driven the demand for increased security and networking solutions. Zero Trust, SD-WAN, CASB, and SASE architectures hold the promise of:

Weaving security from edge to cloud

Providing secure access to enterprise applications from wherever they are accessed

Prioritizing business application traffic that dominates the branch WAN

Three things to get started on your Zero Trust journey

- Build a Zero Trust "Center of Excellence"
- Do a Zero Trust workshop
- Start with something low-risk

Detailed Information

Course Code : TN280
Course Duration : 2 Day Workshop
Course Location : TLC, Customer On-site & Online.
Terms & Conditions : 100% payment in advance.
Course Deliverable : Comprehensive Student Guide and Course Certificate