Zero Trust Security Architecture Framework

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

TLC Education & Training Services

About this workshop

In recent years, organizations are increasingly moving towards zero trust principles for their remote access needs. With workforces around the world now leveraging remote or hybrid working scenarios, there is a greater emphasis on access to cloud and application deployment environments.

This course will review the history of many popular terms for security best practices as well as how the industry developed the term Zero Trust. We will review Zero Trust Architecture and Framework in details with enterprise use cases. Topics will include network, endpoint and cloud security concepts. We will also discuss misconceptions, such as how Zero Trust best practices can't be achieved by simply acquiring a technology such as a Firewall, Identity Management solution or Network Access Control offering. Expect many real-world examples, demos and definitions of topics that you can relate to as well as evaluate with open source or enterprise technology.

Target Audience

- Customers who want to build their knowledge in the space of new security technology and want to understand how to smartly tackle the growing security challenges associated with businesses and how to address complex problems by using the Zero Trust framework as a part of their enterprise strategy.
- CIO/CTO/CISO/CDO, IT Directors/GM IT, Risk and Business Technology Leaders, IT Managers, Strategic Technology Planners, Project Managers, Solution/IT/Systems Architects, Enterprise Architects, Network Operations and SOC teams.

For additional information, please write to us at:
info@tlcpak.com

Unit 1 – Unified Threat Management Principles

- Threats and security challenges faced today.
- Why do we need to make cybersecurity a priority?
- Threat hunting and indicators of compromise (IoC's).
- Understand threat management and knowing security threats and their channels.
- Threat management and threat hunting tools
- Explaining categories of Risks.
- Understand Threat Modeling and procedure how to perform threat modeling exercise.
- Threat Hunting Methodologies and key steps.
- Fileless Malware Attack Process and Fileless Lifecycle.
- Describe Threat hunting Maturity Model.
- Understand Unified Threat Management.
- Understand how Unified Threat Management works?
- Unified Threat Management vs. Next-Generation Firewalls How to avoid the catch – Unified Threat Management.
- UTM – Advantages and Disadvantages.
- Best practices for a modern threat management strategy.
- Exploring UTM Managed Cloud Services – Key Features.
- UTM Performance and Throughput.
- Unit 1 Assessment

Unit 2 – Advanced Network Threat Prevention

- Understand Zero-day Attack.
- The critical issue with Zero-day vulnerability.
- Suggestions for Mitigating the effects of a Zero-day attack.
- Describe Advanced Network Threat Prevention.
- Issues addressed by Advanced Network Threat Prevention.
- Describe Digital Signatures and their distinct goals.
- Signatureless Malware Deduction technology.
- Attack Vector, Attack Surface & Malicious Actors.
- How Does Advanced Network Threat Prevention Work?
- Understand Advanced Network Threat Prevention Engine framework.
- Understand malware features like whitelisting, blacklisting, security services provided by third parties, sandboxing, honeypots, honeynets and anti-malware.
- Understand Penetration Testing.
- MITRE ATT&CK framework, benefits, challenges and .
- Tactics and Techniques use by MITRE ATT&CK.
- The role of Read Team and Blue Team.
- Unit 2 Assessment.

Unit 3 – Exploiting Network Threat Detection and Prevention Tools

- Evaluate the effectiveness of your IDS and IPS systems.
- Firewall and Network-based IPS/IDS & IPS Capacity Planning.
- Best practices for deploying an IPS in your enterprise.
- A features Comparison Matrix – Firewall Vs IDS Vs IPS.
- Critical issue with Zero-day vulnerability.
- Understand SIEM and log management.
- How to select a right SIEM tools for your business.
- Differentiating Continuous and Egress Monitoring.
- Understand Network Access Control.
- Secure network components – NAC devices.
- Best practices to implement Network Access Control.
- Industry Use Cases for Network Access Control.
- The path to next-generation secure network access.
- Vulnerabilities in mobile systems – MDM Features.
- Unit 3 Assessment

Unit 4 – Zero Trust Architecture Framework

- Understanding Zero Trust Architecture.
- Describe Segmentation Gateway.
- Deploying Zero Trust and Zero Trust scenarios.
- Zero Trust scope and phases.
- Zero Trust architecture services – An Example.
- Implementing Zero Trust Identity Management Principles.
- Zero Trust Implementation Methodology.
- How do you approach Zero Trust governance?
- Key steps to Risk Management for Zero Trust.
- Recommendations for starting a Zero Trust Journey.
- Digital Enterprise based on Zero Trust adoption.
- Zero Trust Architectural Framework and Zero Trust Best Practices.
- VPN Vs Zero Trust networks.
- Difference between SDP, VPN and Zero-Trust Networks.
- Unit 4 Assessment.

Detailed Information

Course Code : TN224
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