Essential Elements of Network Security II

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

Education & Training Services

About this workshop

Network security isn't a one-size-fits-all strategy. Dive into the various segments of network security, and learn how they overlap and interact with each other.

IT has changed considerably, moving from a client-server environment to one driven by digital transformation, which increases the interaction of mobile devices, cloud resources such as SaaS and IaaS, and IoT. All this innovation has greatly expanded the ability of people and devices to communicate. What remains constant, however, is that the network, no matter what form it takes, must protect the usability and integrity of network resources.

Target Audience for this workshop

Network teams, Business Technology professionals, audit, risk and compliance, information security, IT operations, Project Management, Cybersecurity professionals, Enterprise Architects, Technical Writers, and fresh network professionals who want to;

- Learn essential networking security trends in information and cybersecurity.
- Understand Network Access Control and Cloud Access Security Broker.
- Learn about Distributed Denial-of-Service Mitigation and Software Defined WAN Security and their use-cases and best practices.

After completing this workshop, you will be able to:

Network security is not one-size-fits-all, as it typically comprises seven different elements. In this workshop, we explore four elements of network security and their roles in a security strategy.

Workshop details:

Unit 1 - Network Access Control

- What do your device know about you?
- Assess and mitigate vulnerabilities in mobile systems.
- Describing the need for having a solution based on Network Access Control.
- Understand Network Access Control.
- How NAC Secures your Network.
- Exploring the types of Network Access Control.
- Key components of Network Access Control.
- Key advantages of Network Access Control.
- Why is it important to have a NAC solution?
- Understand Network Access Control.
- A layered Cyber Defense Approach – The bigger picture.
- Best practices to implement Network Access Control.
- Industry Use Cases for Network Access Control.
- The path to next-generation secure network access.
- Unit 1 Assessment

Unit 2 - Cloud Access Security Broker

- Cloud Computing Defined.
- Service Oriented Architecture (SOA) and Web Services.
- Technologies that enable Cloud Computing Framework.
- Cloud deployment models and workloads.
- Understand Cloud Access Security Broker.
- Security features offered by CASB.
- How Cloud Access Security Broker work.
- Requirements of a CASB Solution.
- 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 for Cloud Access Security Broker.
- Unit 2 Assessment.

Unit 3 - Distributed Denial-of-Service Mitigation

- Distributed Denial-of-Service (DDoS) Attack defined.
- DDoS Mitigation and Mitigation Stages and DDoS attack categories details.
- DoS Verses DDoS Attack and understand How does a DDoS attack work?
- Differentiate between the 3 major categories of DDoS attacks.
- Layer 7 Attacks: Bot Management Solution.
- Layer 4 Attacks: Use Per-Client Throttling.
- Ransom DDoS Attacks – Stages and What should you do.
- Common myths about ransom DDoS attacks.
- Addressing Ransom DDoS Efficiency – Do's and Don'ts.
- Are you prepared for a ransom DDoS attack?
- What to do during a DDoS attack?
- Strategy to prevent DDoS attacks – Best Practices.
- Five steps to mitigate data breach risks.
- Strategy to prevent DDoS attacks – Best Practices.
- Unit 3 Assessment.

Unit 4 – Exploiting SD-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.
- Main components that make up the basic structure of an SD-WAN.
- Main types of SD-WAN Architectures.
- MPLS defined and difference between SD-WAN and MPLS.
- MPLS Vs SD-WAN – Pros and Cons.
- SD-WAN Architecture and understand 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 and SD-WAN Use-cases.
- SD-WAN and MPLS – Differentiating between the two technologies.
- Describe SD-WAN Orchestration – Orchestration Vs. Cloud Automation.
- Unit 4 Assessment.

Detail Information

Course Code : TN228-II
Course Duration : 2 Day
Course Location : TLC, online and Customer On-site.
Terms & Conditions :100% payment in advance.
Course Deliverable : Comprehensive Student Guide and Course Certificate

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

Opportunities are made, not found