Essential Elements of Network Security I

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 Firewalls and role Unified Threat Management.
- Learn about Advanced Network Threat Prevention following best practices.

After completing this workshop, you will be able to:

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

Unit 1 – Network Firewalls

- Network security at a glance.
- Open System Interconnection Model.
- Key networking protocols.
- Network firewall and their types.
- Fine-tuning Firewall Rules: 10 Best Practices.
- Change Management subject to firewall rules.
- Recommended firewall rules.
- How to choose a firewall.
- Questions that you should ask prior choosing a firewall.
- How to configure a Firewall in 6 Steps.
- Next Generation Firewall Defined.
- Key benefits of Next Generation Firewalls.
- Key security features offered by Next Generation Firewall.
- Inbound traffic vs. outbound traffic.
- Firewall Pros and Cons.
- Unit 1 Assessment.

Unit 2 - Intrusion Detection and Prevention Systems

- Understand Intrusion Detection System and Intrusion Prevention Systems.
- Evaluate the effectiveness of your IDS and IPS systems.
- Intrusion Prevention System (IPS) features, market and vendors.
- Firewall and Network-based IPS/IDS.
- IPS Capacity Planning.
- Best practices for deploying an IPS in your enterprise.
- A basic features Comparison Matrix – Firewall Vs IDS Vs IPS.
- Critical issue with Zero-day vulnerability.
- Understand Security information and event management (SIEM).
- Security Information Management Vs. Security Event Management.
- SIEM Process – Four simple steps.
- How to select a right SIEM tools for your business.
- Problem solved by SIEM Solution.
- Exploiting MDR, EDR and XDR Technologies.
- Egress Monitoring defined.
- Unit 2 Assessment.

Unit 3 – Exploring Unified Threat Management

- Threats and security challenges faced today.
- Threat management and knowing security threats and their channels.
- Step-by-step approach from Incident Detection to Root Cause Report.
- Three categories of Risks.
- Threat Modeling as a part of your threat management strategy.
- Understand Unified Threat Management.
- UTM – A series of solutions all under one roof.
- How UTM works – UTM vs. NGFW – A smart comparison.
- How to avoid the catch – Unified Threat Management.
- UTM – Advantages and Disadvantages.
- Best practices for a modern threat management strategy.
- UTM Managed Cloud Services – Key Features.
- UTM – Performance and Throughput.
- Unit 3 Assessment.

Unit 4 - Advanced Network Threat Prevention

- Understand Zero-day Attack and critical issue with Zero-day vulnerability.
- Suggestions for Mitigating the effects of a Zero-day attack.
- Describe Advanced Network Threat Prevention.
- Problems addressed by Advanced Network Threat Prevention.
- Describe Digital Signatures and their distinct goals.
- Signatureless Malware Deduction technology.
- Signatureless Malware Deduction technology.
- Understand Attack Vector, Attack Surface and Malicious Actors.
- Common Breach Vectors.
- How Does ANTP Work?
- Operate and maintain detective and preventative measures.
- Understand malware features like whitelisting, blacklisting, sandboxing, honeypots, honeynets and anti-malware.
- Unit 4 Assessment.

Detail Information

Course Code : TN228-I
Course Duration : 2 Day
Course Location : TLC 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