Building an Effective Security Operations Center Framework

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

Education & Training Services

About this workshop

Security teams are hard at work on the front lines: identifying, analyzing and mitigating threats facing their organization. But despite their best efforts, incident backlogs continue to grow. The reality is that there simply aren't enough skilled professionals to analyze the volume of incidents that most organizations face.

Security Operation is the continuous operational practice for maintaining and managing a secure IT environment through the Implementation and execution of certain services and process its main purpose is to detect, prevent, prioritize and respond to security incidents. This course is specially designed with all necessary information that can help security professionals for building an effective Security Operations Center and associated tools for building a SOC framework.

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.

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

Unit 1 – SOC Fundamentals

- Things that you cannot ignore – Your Devices.
- Assess and mitigate vulnerabilities in your endpoint devices.
- Threats and security challenges faced today and their solutions.
- Assess and mitigate vulnerabilities in mobile systems.
- Tactics used by the Attackers to compromise your security.
- Why you need to make cybersecurity a priority?
- How cognition works – A behavior-based security.
- SOC Defined & how to make your SOC responsive?
- Understand Cyber Incident Recovery Tool and its importance.
- Main components of SOC and SOC Team Structure.
- Challenges faced by every Security Operations Center.
- What Top-Performing SOC Teams have in Common.
- Understanding SOC Playbook and the need for developing it.
- Key Steps for developing a SOC Cybersecurity Playbook.
- SOC Automation Playbook – User Containment Sample Workflow.
- Unit 1 Assessment.

Unit 2 – SOC Design Criteria and Flow

- Organizations must consider questions related to SOC Assessment.
- Encountering types of supported Data Sources.
- Prerequisites to establishing a SOC Design.
- Why SOC Projects Fails? Reasons SOC Projects Fail and Succeed.
- The SOC at the Highest-Level.
- Core SOC and Auxiliary Activities Diagram.
- Common mistakes that should be avoided in SOC designing phase.
- Log Management/Analytics – A critical aspect of SOC.
- Capacity planning and capacity planning guidelines.
- Selecting the right tools for your Security Operations Center.
- Knowing key challenges of your SOC Design phase.
- Recommendations for selecting SOC tools.
- Strategic Planning Assumption – The right and wrong approach.
- Reasons SOC Tooling Projects Fail and Succeed.
- SOC Design Criteria and Flow.
- Build SOC Approach.
- Security Operations Centers: One size does not fit all.
- Unit 2 Assessment.

Unit 3 – SOC Maturity Assessment and Design Framework

- Key SOC Metrics and KPIs: How to define your KPIs and use them.
- A complete list of tasks carried out in Security Operations Center?
- The three Big Challenges for managing the SOC.
- Align the tool selection process.
- Security Target Operating Reference Model.
- Technologies needed to achieve a Maturing SOC.
- Endpoint Detection & Response and Network Traffic Analysis.
- Understand critical components of SIEM Solution and SIEM Process.
- How to select a right SIEM tools for your business.
- Problem solved by SIEM Solution and SIEM sizing guidelines.
- Security Orchestration, Automation and Response – SOAR.
- Understanding the difference between SOAR and SIEM.
- Understanding the important capabilities of a SOAR based solution.
- Egress Monitoring & solution based on Network Access Control.
- Understand NAC to secure your network and Next-Generation Firewall.
- Measuring Capability & Maturity levels in SOCs.
- SOC Capability Maturity Assessment Model.
- A Modern SOC Maturity Level and Capabilities – An Example.
- What exactly is required by SOC Framework? and SOC Framework Architecture.
- Building a Security Operations Center involves multiple domains.
- Multiple layers of protection – High Level Summary.
- An Effective SOC – Resource Availability & Non-Availability Matrix.
- Generic Security Operations Center Framework.
- Unit 4 Assessment.

Unit 4 – Incident Response

- Understanding Incident Response.
- The Role of Computer Security Incident Response Team – CSIRT.
- The importance of Incident Response Plan.
- Seven key phases of an Incident Response Plan.
- Computer Forensics (Cyber Forensics).
- Cyber Incident Management Framework.
- Incident Management and Categorization.
- The role of Service Desk in Incident Management.
- Challenges associated with Incident Categorization.
- Incident categories, subcategories, and categorizing incidents.
- Incident Response Planning and Severity of Incident.
- Timeline from Security incident to Business Continuity.
- Critical Incident Recovery Plan and Cyber Attack Quick Response.
- Preparing for a Security Breach.
- Important consideration from Data Recovery point of view
- Zero-day and your Security Strategy.
- Mitigating the effects of a Zero-day attack – Recommendations.
- Unit 4 Assessment.

Detailed Information

Course Code	: TN222
Course Duration	: 2 Day
Course Location	: TLC, Customer On-site & Online
Terms & Conditions	: 100% payment in advance
Course Deliverable	: Comprehensive Student Guide and Course Certificate