

The Role of SOC Analysts in Managing Enterprise Security

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

About this workshop

This course is the first step to joining a security operations center (SOC) and is especially designed for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

As the security landscape is expanding, a SOC team must offer high-quality IT-security services to detect potential cyber threats/attacks actively and quickly respond to security incidents. Organizations need skilled SOC Analysts who can serve as the front-line defenders, warning other professionals of emerging and present cyber threats.



This two-day online workshop will help the candidate acquire trending and in-demand technical skills through instruction by one of the most experienced trainers in the industry. The course focuses on creating new career opportunities through extensive, thorough knowledge with enhanced level capabilities for dynamically contributing to a SOC team. In this session, we will be covering the key fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response using SOAR will also be discussed. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need and develop the strategy for building an automated Cybersecurity SOC Playbook.

After completing this workshop, you will be able to:

Handle sophisticated threats landscape, enterprises using advanced cybersecurity solutions along with traditional methods of defense. Practicing good cybersecurity hygiene and implementing an appropriate line of defense. This session will enable SOC Analysts with a reasonable knowledge in smartly managing continuous 24x7 coverage for performing security monitoring, security incident management, vulnerability management, security device management, and network flow monitoring. In a nut shell, this course will develop a SOC Analyst who can continuously monitor and detect potential threats, triage the alerts, and appropriately escalating them to the next level, if required.

Workshop details:

Unit 1 – SOC Fundamentals and NICE 2.0 Framework

- Threats and security challenges and their solutions.
- Assess and mitigate vulnerabilities in mobile systems.
- Tactics used by the Attackers.
- Why you need to make cybersecurity a priority?
- Understanding Security Elements – Knowing security threats and their channels.
- Attack Progression Model used by Cybercriminals.
- How cognition works – A behavior-based security.
- Understand Attacker Profiles.
- Security Operations Center Defined.
- How to make you SOC responsive?
- Understand Security Operations Center operations.
- Understand Cyber Incident Recovery Tools.
- SOC Team Structure.
- Challenges every Security Operations Center faces.
- Components of Security Operations Center.
- Understanding NICE Framework and its components.
- How the NICE Framework can be used.
- What Top-Performing SOC Teams have in Common.
- Unit 1 Assessment.

Unit 2 - Enhanced Incident Detection with Unified Threat Management

- What is a Security Operations Center (SOC) Analyst?
- Why do we need SOC Analysts?
- Prerequisites for becoming a SOC Analyst.
- The general training and skills that a SOC Analyst will need.
- SOC Analyst Roles and Responsibilities.
- Sizing your SOC Analysts team size.
- What Operations carried out in Security Operation Center?
- Typical SOC Tool Architecture.
- SOC Operation Workflow and design criteria.
- Threat Hunting defined.
- Threat hunting and Indicators of Compromise (IoCs).
- Exploit Threat Management and Threat Modeling.
- 7 Steps to Threat Modeling.
- Threat Hunting Methodologies
- Key Threat Hunting Steps.
- Mandatory requirements for having an effective Threat Hunting program.
- Threat Hunting Maturity Model.
- Understand Unified Threat Management.
- How Unified Threat Management works.
- Unified Threat Management vs. NGFW – A smart comparison.
- Unified Threat Management – Advantages and Disadvantages.
- Best practices for a modern Threat Management Strategy.
- UTM Managed Cloud Services – Key Features.
- Defending the SOC with open gates – The Biggest Challenge.
- Top 8 vulnerabilities affecting most organizations.
- Unit 2 Assessment.

Prepare for compliance audits and reports before an attack – because you won't have much time after it happens



The Role of SOC Analysts in Managing Enterprise Security

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

The first step for organizations is to establish a common security language

Recent years have witnessed the evolution of cyber risks, creating an unsafe environment for organizations across major business sectors.

To handle sophisticated threats, enterprises need advanced cybersecurity solutions along with traditional methods of defense. Practicing good cybersecurity hygiene and implementing an appropriate line of defense, and incorporating a security operations center (SOC) has become reasonable solutions. SOC Analysts requires continuous 24x7 coverage for performing security monitoring, security incident management, vulnerability management, security device management, and network flow monitoring. This course will develop a SOC Analyst who can continuously monitors and detects potential threats, triages the alerts, & appropriately escalates them.



About the instructor

Training will be delivered by an experienced trainer with 25+ years of career experience imparting education and training services both locally and internationally and have served international enterprise technology vendors including IBM, Fujitsu, and ICL.

Our instructor holds various industry professional certifications in the space of enterprise servers and storage technologies, Information Security, Enterprise Architecture, ITIL, Cloud Computing, Virtualization, Green IT, and a co-author of 10 IBM Redbooks.

The training course flow will be a mix of lectures & classroom discussions and videos so that participants can have a detailed understanding of various components and technologies used to combat against cyber attacks.

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

Unit 3 - Log Collection, Threat Detection and SOC Monitoring Tools

- The SOC at the Highest-Level.
- 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 and Response.
- Evaluate the effectiveness of your IDS and IPS systems.
- Network Traffic Analysis.
- Understanding critical components of SIEM Solution & 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.
- Describe Egress Monitoring.
- The need for having a solution based on Network Access Control.
- Understand NAC and how NAC secures your network.
- Exploiting Next-Generation Firewall.
- Unit 3 Assessment.

Unit 4 - Building a SOC Playbook for IR Automation

- Understanding Incident Response.
- The Role of Computer Security Incident Response Team – CSIRT.
- The importance of Incident Response Plan.
- Incident Management and Categorization.
- Seven key phases of an Incident Response Plan.
- Computer Forensics (Cyber Forensics).
- Cyber Incident Management Framework.
- Understanding SOC Playbook.
- Why there is a need for developing a Cybersecurity Playbook.
- Five key steps for developing a Cybersecurity Playbook.

- SOC Automation Playbook – User Containment Sample Workflow.
- Benefits of a Security Operations Center.
- Unit 4 Assessment.

Target Audience for this course:

- SOC Analysts (Tier I and Tier II).
- Network and Security Administrators, Network and Security Engineers, Network Defense Analyst, Network Defense Technicians, Network Security Specialist, Network Security Operator, and any security professional handling network security operations.
- Cybersecurity Analyst.
- Entry-level cybersecurity professionals.
- Anyone who wants to become a SOC Analyst.

Network security is not one-size-fits-all

Worldwide, IT organizations spend more than \$20 billion per year on hardware and software across a wide variety of network security components. Research from Doyle Research and Security Mindsets forecasted that this spending will reach nearly \$25 billion by 2024. Dozens of suppliers focus on unique security capabilities, and most large organizations use multiple vendors and various elements of network security for in-depth defense.

Detail Information

Course Code	: TN220
Course Duration	: 2 Day Online Instructor Led Workshop
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*