SOC Analyst Professional – Foundations

About TrainSec Academy

TrainSec is an online learning hub for current and aspiring cybersecurity pros who understand the need for excellence. Level up or change career using skill-expanding modular learning way. We turn beginners into experts and experts into masters. TrainSec is designed for those who are serious about being at the vanguard of the latest knowledge, skills and trends. We're already working with the best.

Course Overview

This beginner-friendly course covers essential IT fundamentals to build the critical skills every cybersecurity professional needs. It's the perfect stepping stone to our SOC Analyst Professional – Level 2 and other advanced hands-on courses at TrainSec Academy.

Course Objectives

By completing this course, you will be able to:

- Understand **core computer hardware architecture** and system operation
- Analyze **Windows system processes**, threads, and baseline activities
- Master **Linux basics essential** for cybersecurity environments
- Grasp **networking fundamentals**: OSI model, TCP/IP, and routing principles
- Capture and **analyze network traffic** using Wireshark and NetworkMiner
- Configure and **manage virtualized environments** with VMware Workstation
- **Deploy and manage Windows** 10 and Windows Server in a cybersecurity lab
- Build and **administer Active Directory domains**, users, and groups
- Troubleshoot **firewall settings, network configurations**, and service connectivity
- Baseline **skills for SOC analyst and cybersecurity operations roles**

Course Format

- **URL**: https://trainsec.net/courses/soc-analyst-professional-level-1/
- **Scope and Mode**: 90 Learning materials, spanning on around 10 hours of online videos and presentations.
- **Format**: Pre-recorded Videos and Presentations, discussion group and personal trainer support.
- **Pace**: Self-paced

The contents of this document and the associated course materials are protected by copyright law and may not be reproduced or distributed without explicit permission from TrainSec.net.

- **Platform**: TrainSec.net Learning Platform, Discord server.

Course Content

TrainSec's SOC Analyst Foundations course provides a hands-on introduction to cybersecurity fundamentals. Students learn computer hardware basics, networking protocols, Linux essentials, packet sniffing, virtualization setup, Windows server deployment, and Active Directory management—developing the technical skills required for effective cybersecurity operations and incident response.

Why this course is important for TrainSec students:

Building a professional cybersecurity career requires more than knowing how to use tools—it demands understanding systems, thinking critically, and anticipating threats. This course ensures TrainSec students develop both the technical skills, and the strategic mindset needed to excel as future cybersecurity analysts.

Labs & Resources

- Course Presentation - SOC Analyst Professional - Level 1.pdf
- Labs Deployment Guidance
- 404 Not Found.pcap
- monitor_sudo.sh

Computer Fundamentals

The Computer Fundamentals section builds a complete technical foundation essential for cybersecurity professionals by exploring how computers operate from the ground up. Students learn about key hardware components such as the motherboard, CPU, RAM, storage devices, GPU, and PSU, and how they interact to support system operations. The course then covers the startup sequence, including BIOS/UEFI functions, boot processes through MBR, GPT, and OS bootloaders, and transitions into understanding system operations through processes and threads. Practical work with tools like Process Explorer deepens students' ability to analyze and validate running processes. Additional topics include managing the Windows Registry, understanding service configurations, recognizing the role of Windows Updates in patching vulnerabilities, and working with file systems like NTFS. This foundational knowledge is critical for TrainSec students because it enables them to analyze system behaviors accurately, detect anomalies, understand system vulnerabilities, and build the deep technical expertise required for more advanced cybersecurity analysis and defense.

- SOC Analyst Professional Course Intro • 4 mins

The contents of this document and the associated course materials are protected by copyright law and may not be reproduced or distributed without explicit permission from TrainSec.net.

- Introduction to Computer Hardware • 7 mins
- BIOS in a Nutshell • 5 mins
- Operating System Boot Order • 3 mins
- Process & Thread • 4 mins
- Windows Baseline Processes - Part 1 • 7 mins
- Windows Baseline Processes - Part 2 • 5 mins
- Process Explorer - Part 1 • 6 mins
- Process Explorer - Part 2 • 7 mins
- Windows Registry • 14 mins
- Windows Services - Part 1 • 3 mins
- Windows Services - Part 2 • 5 mins
- Windows Update • 4 mins
- Introduction to File Systems • 6 mins

Networking Fundamentals

The Networking Fundamentals section provides a complete introduction to how devices communicate across networks, a foundational skill for any cybersecurity professional. Students start by understanding the difference between LANs and WANs, explore data transmission types (simplex, half-duplex, full-duplex), and learn about key communication methods like unicast, multicast, and broadcast. They are introduced to the OSI and TCP/IP models and walk through the roles of each network layer—from the physical transmission of data, MAC addressing at the data link layer, IP addressing at the network layer, to ports and protocols at the transport layer. Critical concepts such as ARP protocol operations, NAT translation, and the TCP three-way handshake are covered with practical examples. By mastering these fundamentals, TrainSec students gain the technical depth needed to understand network structures, identify anomalies, investigate incidents, and effectively secure communications in real-world cybersecurity environments.

- LAN vs WAN • 6 mins
- Transmission Types • 3 mins
- Communication Methods • 2 mins
- OSI Model vs TCP-IP Model • 7 mins
- Physical Layer • 4 mins
- Data Link Layer • 10 mins
- Network Layer - Part 1 • 10 mins
- Network Layer - Part 2 • 4 mins
- Network Layer - Part 3 • 13 mins
- The ARP Protocol • 9 mins
- Transport Layer • 14 mins
- NAT & TCP Three-way Handshake • 6 mins
- Layers 5-7 and Encapsulation-Decapsulation Process • 6 mins

The contents of this document and the associated course materials are protected by copyright law and may not be reproduced or distributed without explicit permission from TrainSec.net.

Packet Sniffing & Analysis

The Packet Sniffing & Analysis section introduces students to critical tools and techniques for monitoring and analyzing network traffic, essential for detecting malicious activities and conducting incident investigations. Students learn to use Wireshark for live traffic capture and detailed inspection, applying powerful filters to isolate relevant packets and protocols. The section covers real-world examples such as DHCP handshakes, Telnet and FTP cleartext vulnerabilities, and contrasts them with secure protocols like SSH. Students explore DNS behavior, triage network issues using netstat, and enhance analysis with tools like NetworkMiner for extracting artifacts. Additionally, students are introduced to active network reconnaissance with Nmap and NetBIOS scanning using NBTscan. By mastering packet analysis, TrainSec students develop the practical skills needed to investigate security incidents, identify network anomalies, and gain visibility into the communications underpinning modern cybersecurity threats.

- Introduction to Wireshark • 7 mins
- Wireshark Filters • 5 mins
- DHCP 4-way Handshake • 8 mins
- Telnet • 4 mins
- FTP • 2 mins
- SSH • 4 mins
- DNS • 7 mins
- Using Netstat for Triage • 5 mins
- Network Miner • 3 mins
- Nmap and NBTscan • 6 mins

Introduction to Virtualization

The Introduction to Virtualization section builds a complete understanding of virtualization technologies, focusing on both concepts and practical deployment critical for cybersecurity professionals. Students explore the differences between hypervisor types (Type 1 vs. Type 2), learn how solutions like VMware Workstation and ESXi operate, and understand the underlying architecture involving hypervisors, virtual NICs, and networking models (Bridged, NAT, and Host-Only). The section dives into essential tools like the Virtual Network Editor for network management and troubleshooting, discusses best practices for secure lab setups, and walks through creating virtual machines with optimized storage strategies. Students also examine VMX configuration files, virtual disks (VMDK), snapshots, and memory files (VMEM), gaining hands-on insight into how virtualization operates under the hood. By mastering these foundations, TrainSec students strengthen their ability to build secure labs, simulate complex environments, and support real-world cybersecurity operations with agility and technical precision.

The contents of this document and the associated course materials are protected by copyright law and may not be reproduced or distributed without explicit permission from TrainSec.net.

- Introduction - Hypervisor Type 1 vs Type 2 • 5 mins
- VMware NICs and Services • 9 mins
- Bridged vs NAT vs VMnet • 14 mins
- Virtual Network Editor & Bridged Mode Troubleshooting • 10 mins
- Creating a Virtual Machine - Part 1 • 9 mins
- Creating a Virtual Machine - Part 2 • 8 mins
- VMX file and other Components • 8 mins

Windows & Active Directory

The Windows & Active Directory section provides a practical and detailed foundation for managing enterprise environments, an essential skill set for cybersecurity professionals. Students start by installing and configuring Windows 10 and Windows Server environments, focusing on critical tasks such as disabling unnecessary features for performance, managing power settings, setting up network configurations, and enabling secure communication between systems. They then progress into building a full Active Directory domain, learning about the structure of forests, domains, organizational units (OUs), users, and groups. Key topics such as FSMO roles, DNS integration, DHCP basics, firewall configurations, and troubleshooting network services are also covered with hands-on exercises. By mastering these elements, TrainSec students develop the necessary ability to work confidently within real-world enterprise networks, investigate security incidents in Active Directory environments, and lay the groundwork for advanced threat detection and incident response.

-
- Deploying Win 10 and Windows Server - Part 1 • 14 mins
- Deploying Win 10 and Windows Server - Part 2 • 11 mins
- Initial Configuration - Part 1 • 7 mins
- Initial Configuration - Part 2 • 9 mins
- Disabling Sleep Mode • 1 min
- ICMP, Firewalls and more - Part 1 • 12 mins
- ICMP, Firewalls and more - Part 2 • 4 mins
- Taking Snapshots • 3 mins
- Introduction to Active Directory • 4 mins
- The Incredible Five - The 5 FSMO Roles • 6 mins
- Active Directory Installation - Part 1 • 10 mins
- Active Directory Installation - Part 2 • 9 mins
- Joining computer to the domain • 8 mins
- Domain Users and Groups • 8 mins
- DNS - Domain Name System • 11 mins
- DHCP - Dynamic Host Configuration Protocol • 11 mins
- Kerberos - Part 1 • 11 mins
- Kerberos - Part 2 • 9 mins

The contents of this document and the associated course materials are protected by copyright law and may not be reproduced or distributed without explicit permission from TrainSec.net.

- Group Policy - Part 1 • 7 mins
- Group Policy - Part 2 • 7 mins
- GPO Bypass & Hardening • 7 mins

Linux Essentials

In this class, we explore one of the most critical pillars of cybersecurity: Linux. As a free and open-source operating system, Linux is deeply integrated into servers, cloud environments, enterprise networks, and various types of devices such as DVRs, routers, switches, and even satellites. Security analysts often encounter Linux when dealing with servers, security appliances, and log sources. Understanding Linux is essential for analyzing system behaviors, hardening environments, and investigating incidents. We introduce popular Linux distributions such as Debian, Ubuntu, Kali Linux (widely used by security professionals and attackers alike), as well as Red Hat-based and Arch-based systems. While different distributions have their own tools and paths, they all share a core set of commands that every cybersecurity professional must master.

- Introduction • 2 mins
- Installing Kali Linux • 9 mins
- Linux File System - Part 1 • 8 mins
- Linux File System - Part 2 • 3 mins
- File & Directory Management - Part 1 • 11 mins
- File & Directory Management - Part 2 • 3 mins
- File System Permissions - Part 1 • 7 mins
- File System Permissions - Part 2 • 8 mins
- Users & Groups - Part 1 • 9 mins
- Users & Groups - Part 2 • 2 mins
- Users & Groups - Part 3 • 5 mins
- The find and locate Commands • 4 mins
- Linux Processes • 7 mins
- The top and htop Commands • 2 mins
- Linux Network Commands • 7 mins
- Linux Package Management • 2 mins
- Logs Monitoring • 4 mins

Required Materials

- **Prerequisites**:
    - Basic experience operating a computer (Windows preferred)
    - A PC with at least 16 GB RAM and virtualization support
    - Comfort with installing and using new software tools
    - Good understanding of English for technical learning
- **Additional Resources:** https://discord.com/invite/qugcNyWdaU

Instructor Information

- **Name**: Uriel Kosayev
- **Email**: uriel@TrainSec.net
- **Trainers Biography**:
  Uriel: Security researcher, consultant, and the author of the "*Antivirus Bypass Techniques book"* who lives both on the offensive and defensive fronts. Passionate about malware research, and red teaming while providing real-world security solutions.

Contact & Support

For any course-related or billing-related inquiries, please contact info@TrainSec.net

The contents of this document and the associated course materials are protected by copyright law and may not be reproduced or distributed without explicit permission from TrainSec.net.