C|SOCA

Certified SOC Analyst

The role of a **Security Operation Centre (SOC) Analyst** can be a wide and varied one.

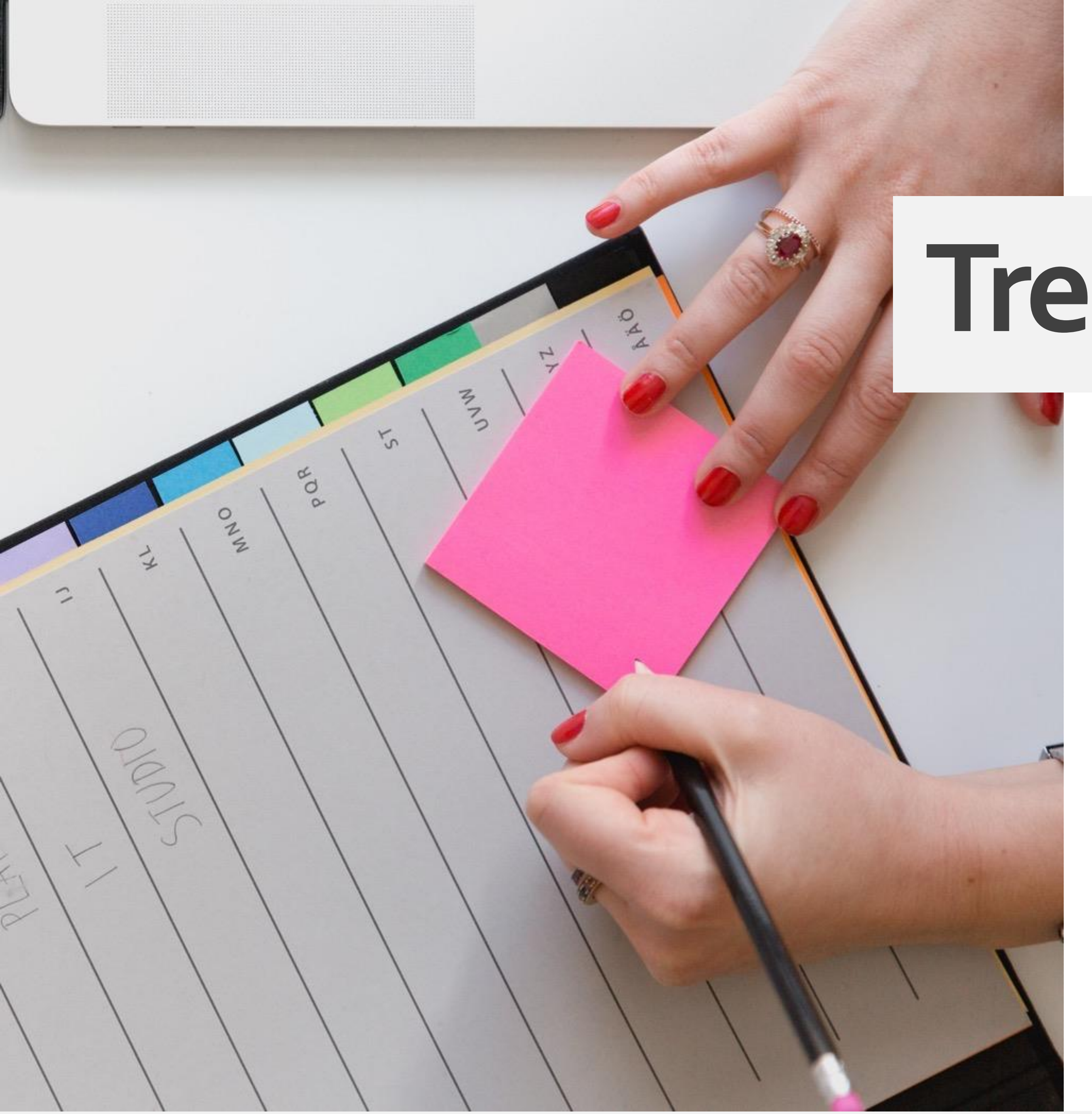
The job covers everything from responding to immediate security requests and incidents to management of threats and vulnerabilities as they develop.

Network and Vulnerability Assessments may need to be carried out together with hands on technical support.

The most effective **SOC Analysts** will have likely learnt key skills on Security Operation Centre focused Courses.

Why C|SOCA?

A SOC Analyst will usually need to be fully up to date with a variety of different SIM and SEM tools in order to carry out their responsibilities effectively.



Trends Today

- As a security operations center analyst your primary duty is to ensure that the organization’s digital assets are secure and protected from unauthorized access.
- That means that you are responsible for protecting both online and on-premise infrastructures, monitoring metrics and data to identify suspicious activity, and identifying and mitigating risks before there is a breach.

Objective

Gain the knowledge and skills needed to effectively operate in the cloud and become an expert in cloud services administration.

In this training you will learn about –

- Working of devices, protocol, ports and services.
- SIEM tool for monitoring and analysis of cyber-attack.
- Learn about the real-world cyber-attacks and investigating on attacks with the help of network packet and device log.
- TCP/IP Protocol Suites with the Detailed summary of Headers in Data Packet.
- Network and Security Device Working, Cyber-attacks and Remediation.
- SIEM Architecture and Correlation Rule.
- SIEM Dashboard creation and usage in the investigation.

Who's for this course?

- Security Officers/Auditors
- Security Professionals
- Site Administrators
- SOC Analysts

Duration: 24Hrs

Target Audience

Course Outline

Topics Covered in Course

1. Basics of Network
2. Understanding of Bit/ Bites in Packets
3. Internet Layer, Transport layer & Cyber Security
4. UDP,ICMP Protocol and Cyber Attack
5. Network Ports , Protocols & Services
6. Security Operation USECASES For Cyber -attack on Networks
7. Working of Windows Domain Controller & Linux
8. System Infection, Brute Force & Vulnerability

9.
- Security Operations Centre USECASE on User Account & System

10.
- Web Application Working

11.
- Cyber Attacks on Web Application / Servers

12.
- Security Operation Center USERCASE on Web Application

13.
- Antivirus Working, Types & USECASES

14.
- IDS- Working , Detection & Evasion

15.
- Firewall Working , Types & Reporting

16.
- Attacking Phases

17
- SIEM

Ducara Info Solutions (P) Ltd.

Discover More

info@ducarainfo.com

www.ducarainfo.com

With our live and online training solutions, we can help you get the skills you need to succeed in the Cyber Security domain.