Zielbox Level 3 Course - SOC Processes, SOC tools & advance capabilities

Module - 1

Topics Covered – SOC Architecture, SLA, Incidents types, Ticketing tool Service Now tool

Module - 2

Topics Covered – IR (Incident Response), NIST, Playbook

Module - 3

Topics Covered – Advance Phishing Analysis, Email Authentication (SPF, DKIM, DMARC)

Module - 4

Topics Covered – Phishing Email Analysis & Email Authentication Continues …

Module - 5

Topics Covered – Advance Analysis methods of Different types of Attacks

Module - 6

Topics Covered – Types of SOC (In-house & MSSP), SOC interview preparation

Module - 7

Topics Covered – Building SOC - SOC RFP (Release for proposal), SOW (Statement of work), POC (Proof of concept)

Module - 8

Topics Covered - Prepare SOC Weekly Reports

Module - 9

Topics Covered – Threat Hunting, MITRE Attack framework, Heat MAP

Module - 10

Topics Covered – SOC interview preparation & Discussing various Q & A

Module - 11

Topics Covered - SOC interview preparation & Discussing various Q & A continues …

Module - 12

Topics Covered – Hands on best practices on handling Various types of Security Alerts

Module - 13

Topics Covered – SIEM Technical Assessment

Module - 14

Topics Covered – PALOALTO - Next Gen Firewall

Module - 15

Topics Covered – Proof Point – Email Security Solution

Proof point _ Email security solution.do