Zielbox Level 2 Course - Cyber Security Alert Analysis & SIEM tool Splunk Enterprise

Module - 1

Topics Covered – RAW Log Analysis

Module - 2

Topics Covered – More about Log Analysis, Log sources

Module - 3

Topics Covered – SIEM (Security Information Event Management), SIEM solution - Splunk introduction

Module - 4

Topics Covered - Splunk Architecture, Installing Splunk

Module - 5

Topics Covered - Setting up Splunk Enterprise LAB

Module - 6

Topics Covered – Onboarding various log sources into Splunk Enterprise

Module - 7

Topics Covered - Splunking

Module - 8

Topics Covered - Splunking continues ...

Module - 9

Topics Covered - Building Dashboard in Splunk Enterprise

Module - 10

Topics Covered - Alert Creation in Splunk Enterprise

Module - 11

Topics Covered - Alert Analysis in Splunk Enterprise

Module - 12

Topics Covered - Alert Analysis in Splunk Enterprise continues ...

Module - 13

Topics Covered - Phishing Email Analysis

Module - 14

Topics Covered - SOC CV Preparation