HEBESEC TECHNOLOGIES
PRIVATE LIMITED

Security Operations Centre (SOC) Syllabus

HebeSec Technologies Private Limited provides the Security Operations Centre (SOC) in the field of Cyber Security. In this SOC, Students / Professionals will learn about Networking Concepts, SOC Concepts, Cyber Threat Intelligence, Network Security and Traffic analysis, Endpoint, SIEM and Digital Forensics

Guidelines:

- SOC Skill training is apt for everyone.
- This is one month duration course and every Saturday and Sunday will be the instructor – led training.
- TryHackme Premium Voucher will be provided for One Month
- Before Starting the class, Non - Disclosure Agreement (NDA) should be Filled out, Signed by the candidates
- Classes will be in Online Mode with Live Practical and Theoretical.
- After completion of training, there will be an assessment for certification
- Certificate will be given only after completion of the assessment.
- Students must have a laptop to attend the class.

AGENDA.

Modules	Topics
Introduction to Networking	1. OSI Model 2. TCP/IP Model 3. DNS 4. Connection vs Connectionless Protocols 5. Networking appliances
Introduction to SOC:	1. Pyramid of pain 2. MITRE 3. ISO 27001 4. NIST 5. Cyber kill chain 6. Unified kill chain (In,Through,Out)

Cyber threat Intelligence	1. Introduction to CTI 2. Threat intelligence tools 3. OSINT 4. MISP 5. YARA
Network Security and Traffic analysis:	1. Snort 2. Wireshark 3. Network miner
Endpoint:	1. Intro to EDR 2. Difference between EDR & XDR 3. Core windows process 4. Sysinternals 5. Winevent logs 6. Sysmon
SIEM:	1. Introduction to SIEM 2. Difference between SIEM and SOAR 3. Deploying ELK 4. Incident handling 5. Splunk
Digital Forensics:	1. Intro to Digital forensics 2. Windows forensics 3. Linux forensics 4. Autopsy 5. Volatility 6. The hive project

Note: * GST Will be added overall in the Invoice.