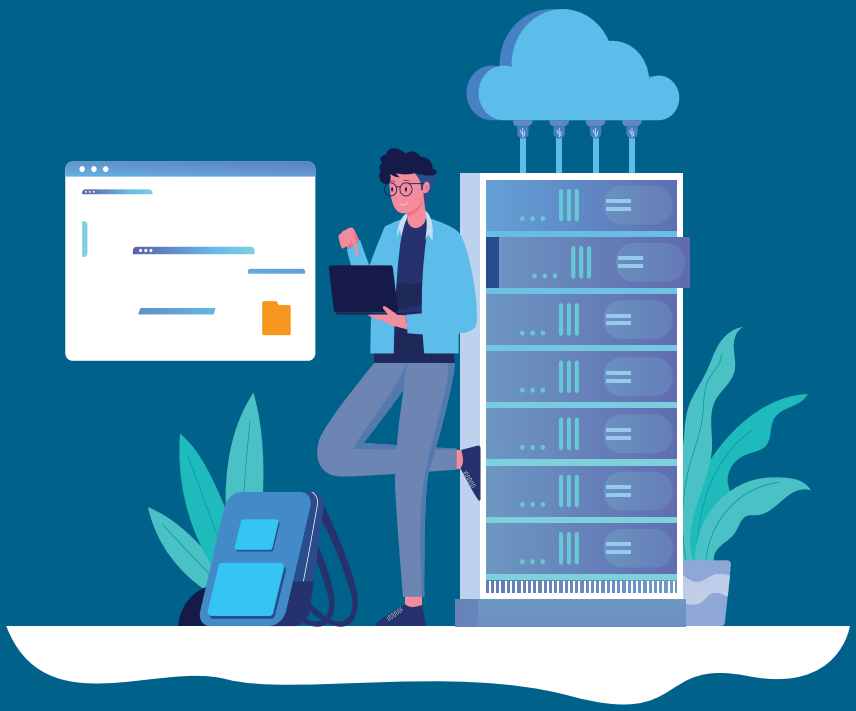
NS3EDU.

Learn Today $ Earn Tomorrow

SECURITY
OPERATIONS CENTER

TABLE OF CONTENT

NS3EDU: BRIDGE YOUR IT DREAMS TO REALITY



EMPOWERING CAREERS THROUGH KNOWLEDGE

Looking to make it big in the world of IT networking? Look no further than NS3Edu! We help beginners learn the ropes & experienced pros master new skills. Come join us and build your dream career!

MISSION

The mission of NS3Edu is to empower our candidates with in-depth knowledge of IT fundamentals along with real-time industry experience and also take 100% responsibility for the placement by making them Industry fit.

CERTIFICATES

VISION

In-depth knowledge + hands-on experience + analytical thinking = placement

ROADMAP OF JOB PLACEMENT

Confused in **Different** Career Options

Counselling & **Demo** sessions

Student Enrollment & Induction **session**

Course **Kick** off (Live Classes)

Access to Recorded Sessions, E book & Lab Manual

Qualifies- Job Placement

Opportunities for **Job** Placement

Screening by Corporate **HR** & **Tech** Team

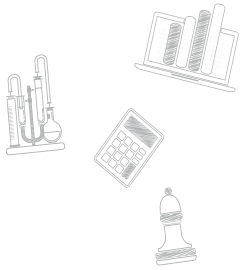
2 Week **Technical Task** Training

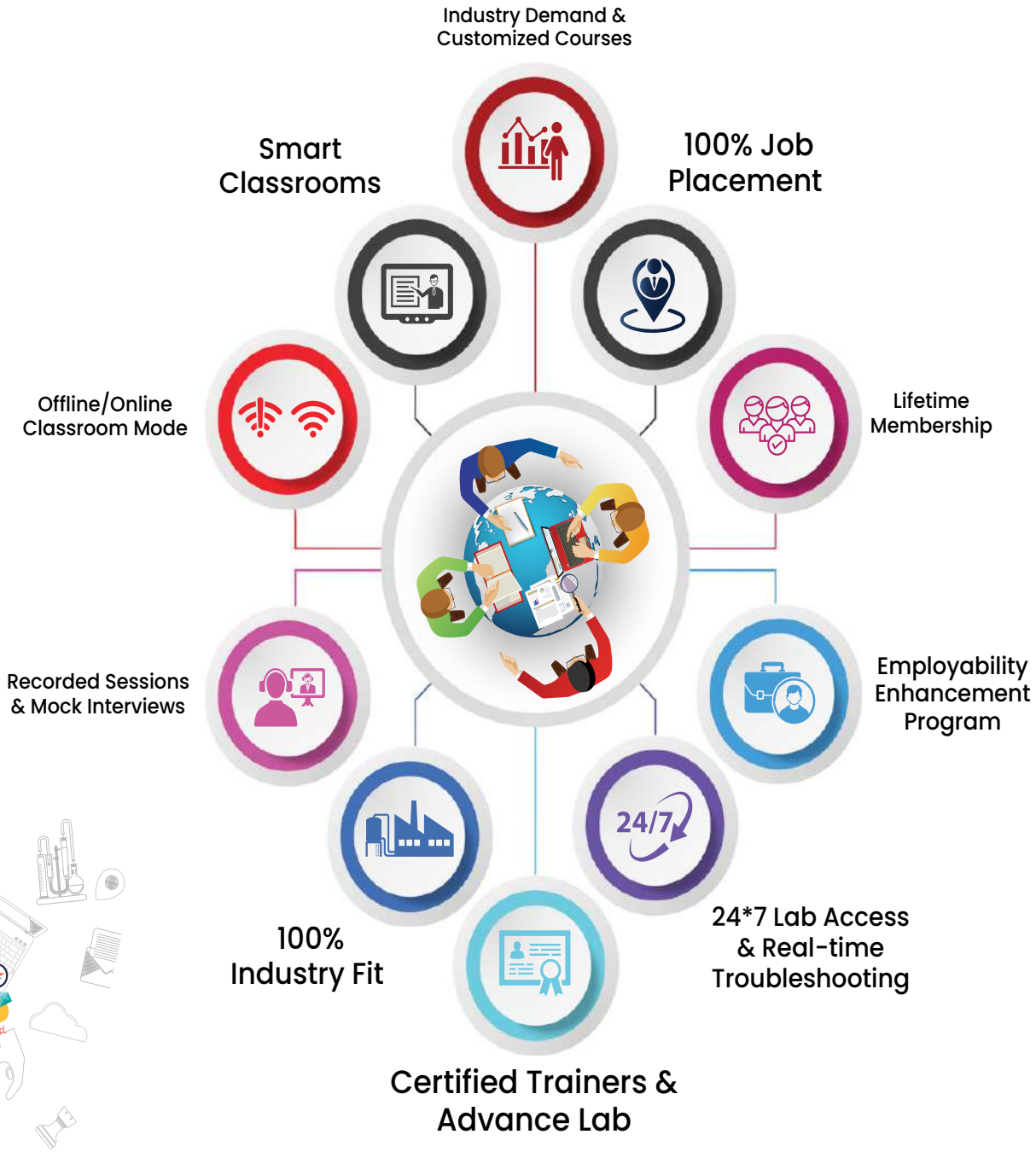
NS3 Tech **Industrial** Exposure

Course **Completion**

WHAT MAKES US UNIQUE?

USP's





SOC ANALYST TRAINING PROGRAM

- Job oriented training
- Get trained on:- Cyber security SOC
- Get Real Time Training Certificate & Hands on tools like Seceon, Splunk, Elastic .
- Duration : 12 weeks training (online).
- What is SOC .

A Security Operations Center (SOC) is a centralized team and facility responsible for monitoring, detecting, responding to, and mitigating cybersecurity threats and incidents within an organization. It acts as the nerve center for maintaining the security of networks, systems, and data in real-time.

SOC ANALYST TRAINING TOPICS:

Day 1

- What is cyber security & information security? Why is it needed?
- Difference between information security and Cyber security?
- What are the advantages of cyber security?
- Research on some of the recent cyber security incidents that happened around the world.
- What is Red Team and Blue Team?
- What is offensive and defensive security?
- What is VA and PT?
- Difference between VA and PT?

Day 2

- Basics of Computer Networking

- Network Traffic Examples
- Network Components-client, server
- Network Resources

Network Geography -WAN, LAN, MAN

Day 3

- OSI model
- TCP/IP model
- IP addressing- IPv4 Addressing
- What is MAC Address.
- Difference of IP and MAC address.

Day 4:

- Classes of IP addresses and CIDR
- Public IP, Private IP, Private IP Ranges
- NAT
- TCP/UDP
- Three-way handshake
- Ports and Protocols
- Find and list out well known Protocols and their port numbers
- Ranges of Port Numbers

Day 5:

- Router
- Switches
- IPS/IDS
- VPN
- Proxy
- Firewall
- Types of firewalls
- Firewall Rules, Rule Types
- Practical with firewalls or UFW:
- 1) install firewalls in VM.
- 2)how to create zones.
- 3)how to add/remove port & IP into created zone.

Day 6:

- What is Active Directory
- What are processes and threads
- What is sysmon
- What is child process , parent process .
- What is critical process.
- What is Alert. What is Event ?
- Dynamic link libraries
- Registry hives
- Operation on Registry.
- WMI

Day 7:

- CIA triangle
- Vulnerability, Threat and Risk, Exploit
- What is Malware and Types of Malware
- What is Zero Day, Patch Tuesday, Exploit Wednesday?
- What is hashing
- What is encryption & decryption
- types of encryption
- difference between hashing and encryption
- difference between symmetric and asymmetric encryption

Day 8:

- What is system hardening and procedure
- What is Zero trust model
- What do you understand by Compliance in cyber security.
- What is cyber kill chain
- What is MITRE attack framework
- Bruteforce Attack
- Phishing , types of phishing
- Social Engineering
- Man in the middle attacks
- Pass the hash
- Denial of Services

Day 9:

- Windows event logs- What are event logs?
- windows logon types
- reasons for login failures for windows login
- Default location of windows logs
- Event IDs
- Practical:
- Event Viewer (GUI-based application)
- Get-WinEvent (PowerShell cmdlet),
- Sysinternal toolset – (Psexec, Sysmon)
- (Using above find out tools find out the event id 4624 and logon type and what is event Id of login failures and simulate the login fail in windows and find out.)

Day 10:

- What is docker ?
- Why we use Docker ?
- Practical :
- Installing docker in Linux
- How to download any container?
- How to run container and how to run container in detached
- How to start, stop and restart the container?
- How to list running and all containers?
- How to check logs of any docker container ?

Day 11:

- Download Oracle VM Virtualbox or VMware, Rocky Linux 9 and Kali Linux 64-bit. (Installation will be tomorrow)

Use the x86_64 version
https://rockylinux.org/download/

Use the 64-bit version
https://www.kali.org/get-kali/#kali-installer-images

- Virtual Machines
- Virtual machine networks
- Practical Task : Set up two Virtual Machines in Oracle VM VirtualBox or VMware with 'Rocky Linux 9' and 'Kali Linux'.
- Practical: Settings up two virtual machines in a virtual network and allowing two machines to communicate each other

Day 12:

- What is SOC
- Need for SOC
- What are SOC Models?
- What is log ingestion.
- What is SIEM
- Capabilities of SIEM
- Raw log vs parse log
- What is use case in SIEM
- What is parsing
- What is aggregation
- What is normalization
- What is correlation

Day 13:

- Working of DNS
- DNS poisoning
- What is the session and cookies.
- What is SSL and TLS
- Working of SSL and TLS
- Difference between SSL and TLS
- How website works
- Http basic
- Difference between http and https
- Https method
- Http codes
- Http request and response

Module A: Roles of L1, L2 & L3

Overview of network support levels (L1, L2, L3)
Responsibilities and tasks of each level
Troubleshooting methodologies
Incident escalation and communication

Network monitoring and management
Documentation and reporting

Module B : Analysis on SIEM

Log and event analysis techniques
Investigation and correlation of security events
Incident response workflow in QRadar
Threat hunting and anomaly detection
Risk and vulnerability assessment
Reporting and visualization of security data

Module C : Real-time Monitoring and Alerting

Real-time event monitoring and dashboards
Creating custom views and reports
Real-time alerting and notifications
Integration

Module D: Incident Response

Introduction to incident response
Incident response life cycle and frameworks
Incident detection and classification
Incident triage and prioritization
Containment and eradication of threats
Post-incident analysis and lessons learned
Incident response tools and automation

Module E: Reporting

Importance of reporting in security operations
Types of security reports (e.g., executive reports, technical reports)
Reporting best practices and templates
Data visualization and dashboard creation
Compliance reporting and auditing
Report automation and distribution

OUR PLACEMENT PARTNERS

ACHIEVEMENTS

1500+ Training Hours

500+ Placements

50+ Corporate Training

200+ International /Domestic Batches

GURUGRAM(H.O)

B9, 3rd Floor, 302, Block B,
Old DLF, Sector 14, Gurugram
Haryana

+91 8800011138
info@ns3edu.com

LUCKNOW

Office space 1, First Floor Omaxe
Avenue Near Omaxe City
Bijnor Rd, Lucknow

+91 7703030320
info_lko@ns3edu.com

DELHI(BADARPUR)

Property No:-3, 3rd Floor Main
Mathura road nearby Badarpur
Police Station, Ch. Dharamvir
Market Badarpur New Delhi 110044

+91 7428080999
info_bpb@ns3edu.com

www.ns3edu.com

+91 8800 0111 38

Follow us for **Job Placement** & Knowledge updates

ns3edu

Ns3eduu

@Ns3eduG

NS3EDUsolutions

ns3edu_