NS3EDU.

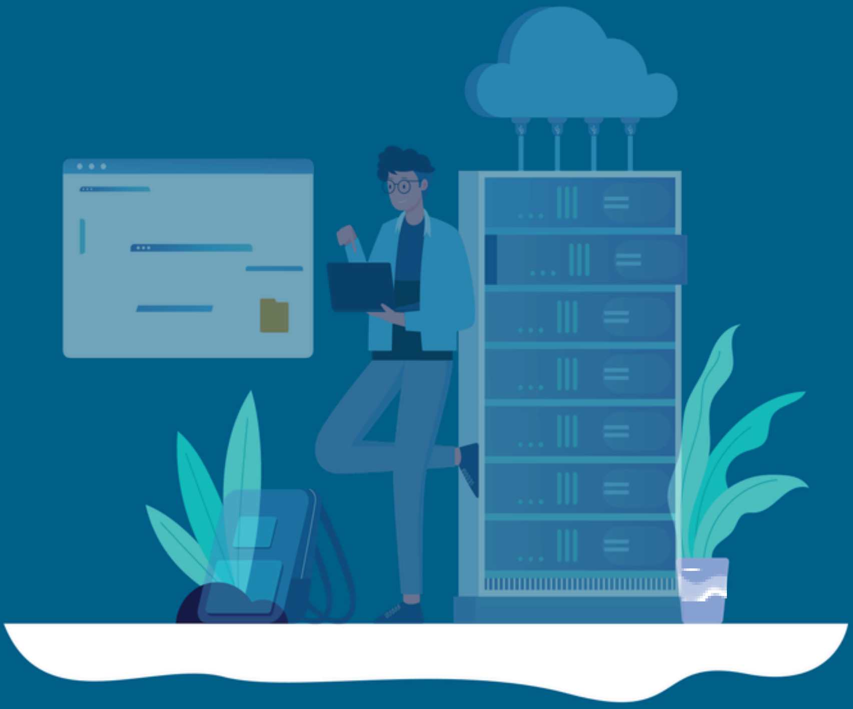
Learn Today Earn Tomorrow

SOC (Security Operations Center)

COURSE OUTLINE

TABLE OF CONTENT

NS3EDU: BRIDGE YOUR IT DREAMS TO REALITY



EMPOWERING CAREERS THROUGH KNOWLEDGE

Lookingto makeitbigin 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

Themissionof NS3Eduisto

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.

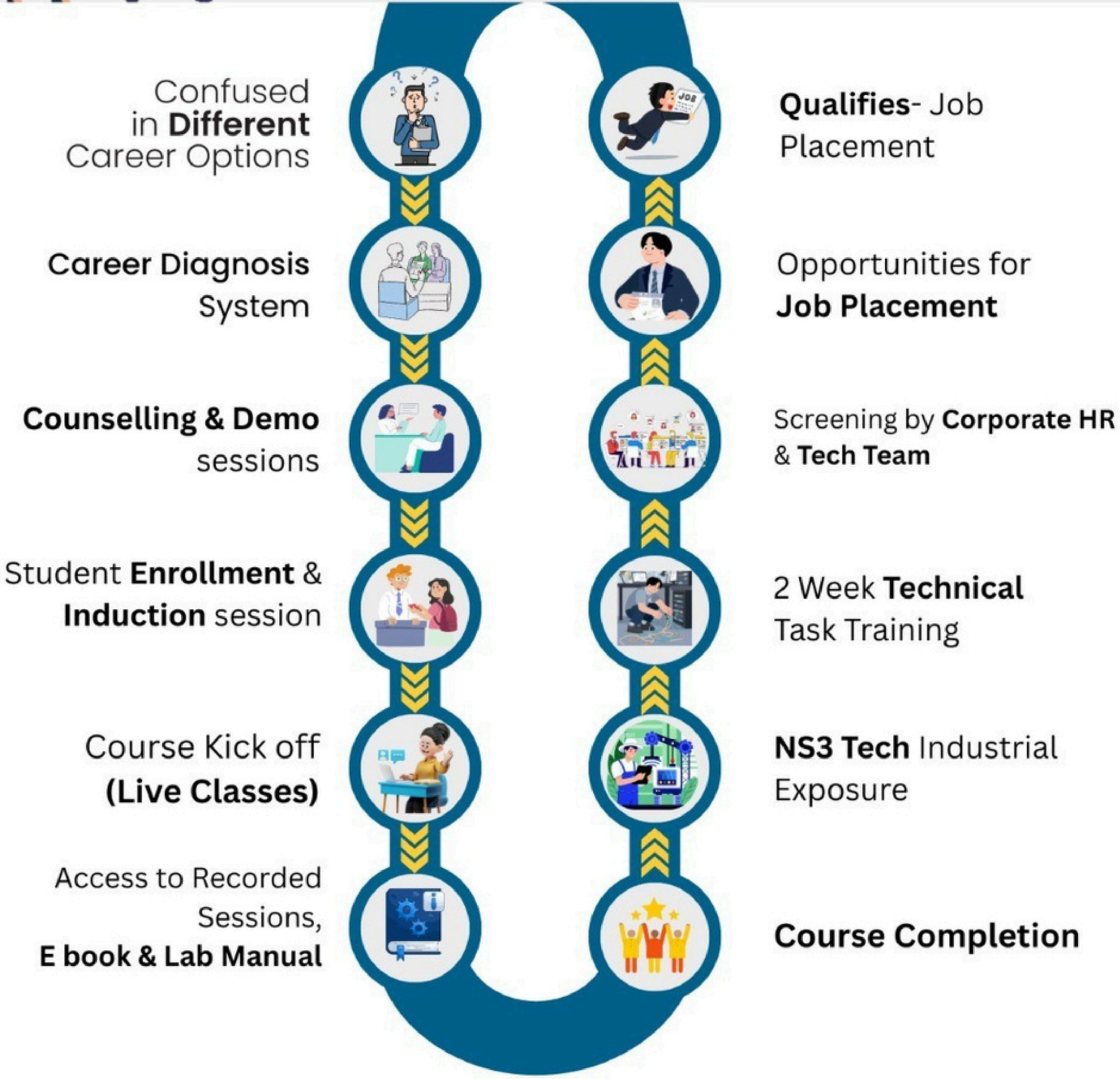
VISION

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

CERTIFICATES

Cisco Certified Internetwork Expert
Cisco Certified Internetwork Expert
Cisco Certified Internetwork Expert
Cisco Certified Internetwork Expert

ROADMAP OF JOB PLACEMENT



- Confused in **Different** Career Options
- **Career Diagnosis** System
- **Counselling & Demo** sessions
- Student **Enrollment** & **Induction** session
- Course Kick off **(Live Classes)**
- Access to Recorded Sessions, **E book & Lab Manual**
- **Course Completion**
- **NS3 Tech** Industrial Exposure
- 2 Week **Technical** Task Training
- Screening by **Corporate HR** & **Tech Team**
- Opportunities for **Job Placement**
- **Qualifies**- Job Placement

WHAT MAKES US UNIQUE?

USP'S

Industry Demand & Customized Courses

Smart Classrooms

100% Job Placement

Offline/Online Classroom Mode

Lifetime Membership

Recorded Sessions & Mock Interviews

Employability Enhancement Program

100% Industry Fit

24*7 Lab Access & Real-time Troubleshooting

Certified Trainers & Advance Lab

Course Outline

LEVEL 1: SOC Foundations (Beginner Level)

Part 1: Introduction to SOC

- What is SOC
- Role of SOC in Cyber Security
- SOC Team Structure (L1, L2, L3)
- SOC Tools & Technologies Overview
- Blue Team vs Red Team

Part 2: Cyber Security Fundamentals

- CIA Triad
- Common Threats & Attacks
- Malware Types
- Social Engineering
- Network Basics for SOC

Part 3: Logs & Monitoring Basics

- What are Logs
- Types of Logs (System, Network, Application)
- Log Collection & Centralization
- Importance of Log Analysis

LEVEL 2: SIEM & Threat Detection (Intermediate Level).

Part 4: SIEM Fundamentals

- What is SIEM
- SIEM Architecture
- Log Ingestion & Parsing
- Correlation Rules
- Alerts & Events

Part 5: Security Monitoring & Alert Handling

- Alert Investigation Process
- False Positive vs True Positive
- Incident Categorization
- Ticketing System Basics
- Escalation Procedures

Part 6: Network & Endpoint Security Monitoring

- Firewall Logs Analysis
- IDS/IPS Alerts
- Endpoint Detection & Response (EDR)
- Suspicious Activity Detection

Part 7: Threat Intelligence

- Threat Intelligence Basics
- IOC (Indicators of Compromise)
- Open-Source Threat Feeds
- Threat Hunting Concepts

LEVEL 3: Incident Response & Advanced SOC Operations (Professional Level)

Part 8: Incident Response Lifecycle

- Incident Identification
- Containment & Eradication
- Recovery
- Post-Incident Review

Part 9: Malware & Attack Analysis

- Basic Malware Analysis
- Phishing Email Analysis
- Log-Based Attack Investigation
- Brute Force & Lateral Movement Detection

Part 10: Digital Forensics Basics

- Forensics Concepts
- Evidence Collection
- Chain of Custody
- Memory & Disk Forensics (Intro)

Part 11: Cloud & Modern SOC

- Cloud Log Monitoring
- Cloud Security Alerts
- Hybrid SOC Environment
- Zero Trust Monitoring

Part 12: SOC Reporting & Documentation

- Incident Reporting
- Executive Summary Writing
- Root Cause Analysis
- SLA & KPI Tracking

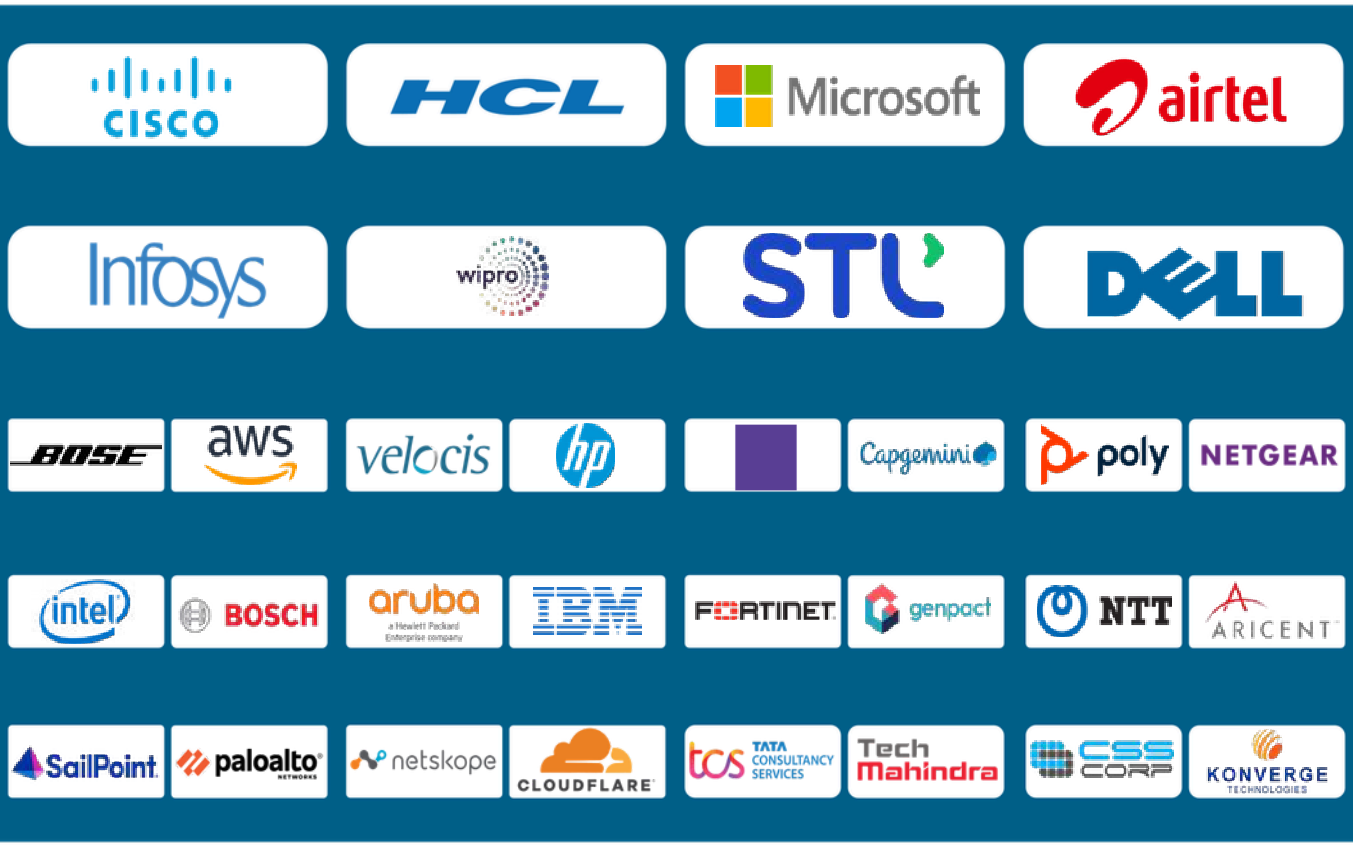
Part 13: Real-World SOC Labs & Case Studies

- Live Log Investigation
- Malware Alert Simulation
- Phishing Attack Response
- Insider Threat Scenario
- Ransomware Case Study

Part 14: Career & Certification Preparation

- SOC Analyst Roles (L1, L2)
- Interview Questions & Scenarios
- Resume & Portfolio Guidance
- Security+ / CEH / SOC Career Path
- Mock Interviews

OUR PLACEMENT **PARTNERS**



YOUR FUTURE OUR RESPONSIBILITY

Free consulting

Get trained with certified trainers

24X7 Lab access

Employability enhancement program

info@ns3edu.com

www.ns3edu.com

+91-9821442746

3rd Floor, B9, Block B,
Old DLF Colony, Sector 14,
Gurugram, Haryana 122007

NETWORK SECURITY

CYBER SECURITY

CLOUD SERVICE

FULL STACK DEVELOPMENT

DIGITAL MARKETING

DATA SCIENCE

AI ML LEARNING