

Cybersecurity & Network Security Foundations

Build the practical security foundation needed for SOC, security operations and cloud-security pathways through hands-on labs.



8 weeks

DURATION

70 hours

GUIDED LEARNING

2 projects

PORTFOLIO

ABOUT THE ACADEMY

Practical learning. Work you can demonstrate.

Brightnest AI Academy brings live instruction, guided practice and career preparation together for individuals and teams.

23

FOCUSED COURSES

6

FLAGSHIP PROGRAMMES

Noida

ACADEMY LOCATION

Our approach

1

Learn

Understand concepts through live instruction and current examples.

2

Build

Apply learning through labs, assignments and guided projects.

3

Explain

Document decisions, results, trade-offs and limitations.

4

Prepare

Connect completed work with CVs, interviews and workplace conversations.

PEOPLE BEHIND THE ACADEMY

Meet Ranjeet Kumar



ACADEMY ADVISER

Ranjeet Kumar

Innovation & Growth Leader

15+ years

Experience in data, artificial intelligence and machine learning leadership.

Areas of expertise

- Data science and machine learning solution leadership
- AI product strategy and scalable data platforms
- Technology team leadership and mentorship
- Practical AI and data adoption for business transformation

Education

Master of Information Systems, Anna University, Chennai
Bachelor of Computer Science Engineering



COURSE OVERVIEW

Build your next set of skills

Build foundations in security concepts, networks, identity, risk, vulnerabilities, and defensive practices. Progress from Cybersecurity Foundations and Risk to Incident Response, Resilience and Capstone through guided labs, assessed projects, and portfolio evidence.

Who this is for

Beginners, IT support/network professionals and graduates entering cybersecurity.

Before you begin

No prior cybersecurity experience is required. Basic computer literacy and an interest in networking are sufficient.

Security foundations become job-relevant when learners can understand networks, identities, vulnerabilities, risk, controls, and incident response as one connected discipline.



LEARNING OUTCOMES

What you will be able to do

01

Perform a basic risk assessment for a small organisation and prioritise controls.

02

Analyse packet captures and map normal versus suspicious network behaviour.

03

Harden Windows/Linux hosts and document baseline deviations.

04

Design an IAM model and test role-based access in a lab environment.

05

Scan a lab environment, validate findings and create a remediation backlog.

06

Ingest sample logs, identify suspicious activity and document triage steps.

07

Run a tabletop breach simulation and produce an incident report plus recovery plan.



CURRICULUM

Course curriculum

8 modules · 8 weeks · 70 hours of guided learning

01 Cybersecurity Foundations and Risk

6 hours

TOPICS

CIA triad · Threats/vulnerabilities/risk · Attack surface · Security controls · Governance basics · Policies · Ethics · Security careers

PRACTICAL WORK

Perform a basic risk assessment for a small organisation and prioritise controls.

Tools: Risk templates, Security lab environment

Assessment: Risk case and quiz

Portfolio evidence: Risk register and control plan

02 Networking for Cybersecurity

10 hours

TOPICS

OSI/TCP-IP · IP/subnetting · DNS · HTTP/TLS · Routing · Ports/protocols · Packet flow · Firewalls · VPN concepts · Network segmentation

PRACTICAL WORK

Analyse packet captures and map normal versus suspicious network behaviour.

Tools: Wireshark, tcpdump

Assessment: Network practical

Portfolio evidence: Packet analysis notebook/report



CURRICULUM

Course curriculum

8 modules · 8 weeks · 70 hours of guided learning

03 Operating System and Endpoint Security

8 hours

TOPICS

Windows/Linux fundamentals · Permissions · Processes · Services · Patching · Hardening · Endpoint telemetry · Malware persistence concepts

PRACTICAL WORK

Harden Windows/Linux hosts and document baseline deviations.

Tools: Windows/Linux VMs, Sysmon concepts

Assessment: Hardening lab

Portfolio evidence: Endpoint hardening checklist

04 Identity, Access and Authentication

8 hours

TOPICS

Authentication factors · IAM · RBAC/ABAC · Least privilege · Password security · MFA · SSO/federation concepts · Privileged access

PRACTICAL WORK

Design an IAM model and test role-based access in a lab environment.

Tools: Directory/IAM lab

Assessment: IAM design review

Portfolio evidence: Access-control matrix



CURRICULUM

Course curriculum

8 modules · 8 weeks · 70 hours of guided learning

05 Vulnerability Management and Security Testing

8 hours

TOPICS

CVE/CVSS concepts · Scanning · Patch prioritization · Configuration issues · Exposure validation · Remediation workflow · Reporting

PRACTICAL WORK

Scan a lab environment, validate findings and create a remediation backlog.

Tools: Nmap, Vulnerability scanner in lab

Assessment: Vulnerability report

Portfolio evidence: Remediation-focused vulnerability assessment

06 Cryptography and Data Protection

6 hours

TOPICS

Symmetric/asymmetric cryptography · Hashing · PKI · Certificates · TLS · Encryption at rest/in transit · Key management · Data classification

PRACTICAL WORK

Inspect TLS certificates and design encryption/key-management controls for sample data.

Tools: OpenSSL concepts, Browser/dev tools

Assessment: Crypto quiz and lab

Portfolio evidence: Data protection design



CURRICULUM

Course curriculum

8 modules · 8 weeks · 70 hours of guided learning

07 Security Operations and Monitoring

10 hours

TOPICS

Logs · SIEM concepts · Detection · Alert triage · Endpoint/network telemetry · Baselineing · Threat intelligence basics · Escalation

PRACTICAL WORK

Ingest sample logs, identify suspicious activity and document triage steps.

Tools: SIEM lab, Log sources

Assessment: SOC lab

Portfolio evidence: Security monitoring case file

08 Incident Response, Resilience and Capstone

14 hours

TOPICS

IR lifecycle · Evidence handling · Containment · Eradication · Recovery · Communication · Business continuity · Disaster recovery · Lessons learned

PRACTICAL WORK

Run a tabletop breach simulation and produce an incident report plus recovery plan.

Tools: IR templates, Security lab

Assessment: Capstone tabletop and report

Portfolio evidence: Cybersecurity foundations capstone

APPLIED PORTFOLIO

Projects you will build

Two portfolio projects supported by guided module work.

PORTFOLIO PROJECT 1

Small Business Security Baseline

Assess network, endpoints, IAM, vulnerabilities and monitoring and create an improvement roadmap.

DELIVERABLES

Risk register · Hardening checklist · Monitoring plan · IR playbook

PORTFOLIO PROJECT 2

Security Operations Starter Lab

Build a small monitored environment and investigate a simulated incident.

DELIVERABLES

Logs · Alerts · Incident timeline · Lessons learned

LEARNING EXPERIENCE

Learn, practise and present

- Live instructor-led sessions that connect concepts to real workplace decisions.
- Guided labs and workshops in every module.
- Assignments, checkpoints and practical feedback.
- Portfolio documentation, demonstrations and capstone review.
- Access to recordings and LMS resources according to the published batch policy.
- Career preparation based on completed work and target roles.

Tools you will work with

Risk templates · Security lab environment · Wireshark · tcpdump · Windows · Linux VMs · Sysmon concepts · Directory · IAM lab · Nmap · Vulnerability scanner in lab · OpenSSL concepts · Browser · Dev tools · SIEM lab · Log sources

CAREER PREPARATION

Build confidence for interviews

A structured process to connect your learning with your next career step.

01**Role clarity**

Identify roles that fit your background, interests and current skills.

02**Profile readiness**

Review your CV, LinkedIn, GitHub and project summaries.

03**Project proof**

Prepare to demonstrate completed work and explain your decisions.

04**Interview practice**

Practise technical questions, project walkthroughs and interviews.

05**Opportunity updates**

Receive relevant job openings and employer requirements, subject to availability and learner readiness.

Career support helps you prepare. Employment outcomes depend on experience, project quality, interview readiness and market conditions.

LEARNER JOURNEYS

Companies where our learners have been hired

Across the Brightnest AI Academy learner community



Learner employment history across the academy; not a placement guarantee for this course. Names and logos identify employers; they do not imply endorsement or a hiring partnership.

BEFORE YOU ENROL

Your questions, answered

Is the Cybersecurity Foundations course suitable for beginners?

This is a foundation-level course. No prior cybersecurity experience is required. Basic computer literacy and an interest in networking are sufficient.

What will I build during the course?

You will complete guided labs in every module and build two portfolio projects: Small Business Security Baseline and Security Operations Starter Lab. Deliverables include working files or code, documentation, testing or evaluation evidence, and a final presentation.

Which tools and platforms are covered?

Key tools include Risk templates, security lab environment, Wireshark, tcpdump, Windows, Linux VMs, Sysmon concepts, and Directory. Additional platforms are introduced in relevant modules through practical tasks, and the toolset may evolve as industry practice changes.

How long does the course take?

The course includes approximately 70 guided learning hours across 8 modules, delivered over 8 weeks.

Which career paths can this course support?

The curriculum supports the development of skills relevant to roles such as Cybersecurity Analyst, Junior SOC Analyst and security operations roles. Career outcomes depend on prior experience, project quality, interview readiness and market conditions; employment is not guaranteed.

BEFORE YOU ENROL

Your questions, continued

Will I receive mentor and career support?

The course includes live instruction, lab support, assignment feedback, project reviews and career preparation covering portfolio development, CV writing, LinkedIn profile improvement, and interview guidance.

FEES & ADMISSIONS

Plan your next step

COURSE FEE

INR 35,000 + GST

EMI and easy instalments available

Duration	8 weeks
Level	Foundation
Learning format	Live mentor-led learning
Batch starts	Expected Saturday / Sunday starts

Check the live Batches page for the next expected weekend. Confirm the exact date, class times and availability with admissions.

Book a free demo class >

+91 73030 11395

brightnestaiacademy.com/batches

A-56, Sector-64, Noida, Uttar Pradesh - 201301