

SOC Analyst & Incident Response

Train like a SOC analyst: triage alerts, write detections, hunt threats, investigate incidents and automate response workflows.



8 weeks

DURATION

76 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

Detect, investigate and respond to security events using SOC workflows and tooling. Progress from SOC Operations and Alert Triage to SOAR, Metrics and SOC Capstone through guided labs, assessed projects, and portfolio evidence.

Who this is for

Cybersecurity learners and analysts pursuing hands-on SOC, detection and incident response roles.

Before you begin

Learners should understand cybersecurity and networking fundamentals and have basic familiarity with Windows/Linux.

SOC analysts need to interpret telemetry, triage alerts, investigate incidents, document decisions, and improve detections under realistic operational constraints.



LEARNING OUTCOMES

What you will be able to do

01

Triage a queue of simulated alerts and document disposition and escalation decisions.

02

Onboard sample log sources and create normalised fields/searches.

03

Create and tune detections for credential abuse, persistence and suspicious network activity.

04

Investigate a simulated compromise using endpoint and network telemetry.

05

Enrich a set of indicators and convert intelligence into detection/triage actions.

06

Triage phishing and cloud identity incidents using safe artifacts.

07

Build a simple automated enrichment workflow and complete a multi-stage SOC incident capstone.



CURRICULUM

Course curriculum

8 modules · 8 weeks · 76 hours of guided learning

01 SOC Operations and Alert Triage

6 hours

TOPICS

SOC tiers · Incident severity · Alert lifecycle · Escalation · Ticketing · Evidence · False positives · Playbooks · Communication

PRACTICAL WORK

Triage a queue of simulated alerts and document disposition and escalation decisions.

Tools: SIEM lab, Ticketing template

Assessment: Triage assessment

Portfolio evidence: SOC triage workbook

02 Log Sources and SIEM Fundamentals

10 hours

TOPICS

Windows/Linux logs · Authentication · DNS · Proxy · Firewall · Endpoint · Cloud logs · Parsing · Normalisation · Correlation · Retention

PRACTICAL WORK

Onboard sample log sources and create normalised fields/searches.

Tools: Splunk/Elastic/Microsoft Sentinel lab concepts

Assessment: SIEM lab

Portfolio evidence: Log onboarding runbook



CURRICULUM

Course curriculum

8 modules · 8 weeks · 76 hours of guided learning

03 Detection Engineering and Threat Hunting

10 hours

TOPICS

Detection logic · Signatures versus behavior · Baselines · MITRE ATT&CK mapping · Queries · Tuning · Hypothesis-driven hunting · Coverage gaps

PRACTICAL WORK

Create and tune detections for credential abuse, persistence and suspicious network activity.

Tools: SIEM query language, MITRE ATT&CK

Assessment: Detection review

Portfolio evidence: Detection rule pack

04 Endpoint and Network Investigation

10 hours

TOPICS

Process trees · Command lines · Persistence · Connections · Packet/log correlation · EDR concepts · Timeline building · Suspicious binaries

PRACTICAL WORK

Investigate a simulated compromise using endpoint and network telemetry.

Tools: EDR lab concepts, Wireshark, SIEM

Assessment: Investigation case

Portfolio evidence: Incident timeline and evidence pack



CURRICULUM

Course curriculum

8 modules · 8 weeks · 76 hours of guided learning

05 Threat Intelligence and Enrichment

6 hours

TOPICS

Indicators · TTPs · Intelligence lifecycle · Confidence · Feeds · Enrichment · Pivoting · ATT&CK · Intelligence-driven prioritization

PRACTICAL WORK

Enrich a set of indicators and convert intelligence into detection/triage actions.

Tools: Threat intel sources, ATT&CK

Assessment: Intel brief

Portfolio evidence: Threat intelligence brief

06 Incident Response and Digital Evidence

10 hours

TOPICS

Preparation · Identification · Containment · Eradication · Recovery · Evidence handling · Memory/disk concepts · Root cause · Communications

PRACTICAL WORK

Run an incident-response scenario and produce containment/recovery actions.

Tools: IR toolkit concepts, SIEM/EDR lab

Assessment: IR practical

Portfolio evidence: Incident response report



CURRICULUM

Course curriculum

8 modules · 8 weeks · 76 hours of guided learning

07 Phishing, Malware and Cloud Alert Triage

8 hours

TOPICS

Email headers · URLs/domains · Attachment analysis concepts · Sandboxing · Cloud identity alerts
· OAuth abuse concepts · Suspicious sign-ins

PRACTICAL WORK

Triage phishing and cloud identity incidents using safe artifacts.

Tools: Email analysis tools, Sandbox concepts, Cloud logs

Assessment: Triage lab

Portfolio evidence: Phishing/cloud incident case files

08 SOAR, Metrics and SOC Capstone

16 hours

TOPICS

Playbook automation · Enrichment · Containment actions · Human approval · SOC KPIs ·
MTTD/MTTR · Coverage · Backlog · Continuous improvement

PRACTICAL WORK

Build a simple automated enrichment workflow and complete a multi-stage SOC incident capstone.

Tools: SOAR concepts, SIEM, Scripting optional

Assessment: Capstone and metrics review

Portfolio evidence: SOC detection and response portfolio

APPLIED PORTFOLIO

Projects you will build

Two portfolio projects supported by guided module work.

PORTFOLIO PROJECT 1

SOC Detection and Response Challenge

Detect and investigate a simulated attack from endpoint/network/cloud logs.

DELIVERABLES

Detection rules · Timeline · Incident report · Response actions

PORTFOLIO PROJECT 2

Threat Hunting Detection Pack

Develop ATT&CK-mapped detections and hunt hypotheses for a sample environment.

DELIVERABLES

Query pack · Tuning notes · Coverage matrix · Executive summary

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

SIEM lab · Ticketing template · Splunk · Elastic · Microsoft Sentinel lab concepts · SIEM query language · MITRE ATT&CK · EDR lab concepts · Wireshark · SIEM · Threat intel sources · ATT&CK · IR toolkit concepts · EDR lab · Email analysis tools · Sandbox concepts

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 SOC Analyst & Incident Response course suitable for beginners?

This course progresses from intermediate to advanced level. Learners should understand cybersecurity and networking fundamentals and have basic familiarity with Windows/Linux.

What will I build during the course?

You will complete guided labs in every module and build two portfolio projects: SOC Detection and Response Challenge and Threat Hunting Detection Pack. Deliverables include working files or code, documentation, testing or evaluation evidence, and a final presentation.

Which tools and platforms are covered?

Key tools include SIEM lab, ticketing template, Splunk, Elastic, Microsoft Sentinel lab concepts, SIEM query language, MITRE ATT&CK, and EDR lab concepts. 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 76 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 SOC Analyst, Detection Engineer and Incident Response Analyst. 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	Intermediate-Advanced
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