Programme on

Intelligent SOC : Behind the Scenes of Threat Detection and Response

(November 12 - 14, 2025)

Administrative Staff College of India

(accredited as उत्कृष्ट by Capacity Building Commission, GoI)

PROGRAMME OVERVIEW

Welcome to the Intelligent Security Operations Center (iSOC) Training Program, a dynamic 3-day course designed to empower technical professionals with the skills to excel in modern cybersecurity. In today's fast-evolving threat landscape, an iSOC is the cornerstone of proactive defense, leveraging AI, automation, and threat intelligence to outsmart cyber adversaries. This program immerses participants in hands-on labs, real-world attack simulations, and cutting-edge tools to master threat detection, incident response, and automated workflows. Tailored for IT professionals, network engineers, and security enthusiasts looking to upskill, pivot, or cross-skill into SOC analyst roles, this course serves as a powerful stepping stone toward SOC certification and a thriving cybersecurity career.

💡 Why Take This Course?

- Get a career-launching SOC skillset in just 3 days
- Transition-ready knowledge + hands-on exposure
- Ideal launchpad for advanced SOC Analyst Certifications
- Be future-ready with AI + SOAR-powered defense skills

OBJECTIVES

By the end of the program, participants will be able to:

- **Understand how a modern SOC works**
  Learn about SOC roles, tools, and processes used in cybersecurity operations.
- **Detect and respond to real cyber threats**
  Practice identifying and handling attacks like phishing, ransomware, and insider threats.
- **Use the MITRE ATT&CK framework**
  Map and analyze cyberattacks using this widely used threat model.
- **Automate security tasks with SOAR**
  Create playbooks to quickly respond to alerts and reduce response time.
- **Handle complete incident scenarios with confidence**
  Take part in hands-on simulations to manage full cyber incidents from start to finish.

These objectives are designed to create a focused and impactful training program that addresses key aspects of cybersecurity preparedness and leadership by leveraging the unique environment of Cyber Theme Park (CTmP).

CONTENT

Day 1: The Intelligent SOC (iSOC)

Theme: From Legacy to Legendary – The SOC Reimagined

Topics
🔷 **Welcome Address – Rise of the Intelligent SOC**

Cyber defense is evolving – move from traditional monitoring to intelligent response.
🔷 **Understanding Cyber Threat Landscape** *Today's attackers are faster and smarter. Know your APTs, ransomware, insider threats, and zero-days.*
🔷**SOC 360° – Roles, Tools, and Technologies** *Tiered analyst roles, essential SOC tools (SIEM, SOAR, EDR), and modern workflows decoded.*
🔷**Incident Response: Be First, Fast, and Fearless** *Preparation, detection, and containment in high-stakes incidents.*
🔧 **CTmP Experiences & Activities** • Phishing Email Detection & Credential Hijack • Trace phishing trails using SIEM and user behavior analytics. • Insider Threat Simulation • Correlate after-hours log access to detect unauthorized activity. • Ransomware Outbreak Drill

Day 2: SOC in Action – Tools, Tactics and Automation

Theme: Hunt. Correlate. Automate.

Topics
🔷 **Behind the Scenes: Data Collection & Normalization** *Turn raw logs from firewalls, endpoints, and cloud into intelligence.*
🔷 **Threat Hunting in the SOC** *Manual detection is passé. Use patterns, IOCs, and tactics from MITRE ATT&CK.*
🔷**SOAR: Automate to Accelerate** *Cut your incident response time. Build and test playbooks with SOAR workflows.*
🔷 **Credential Compromise Detection** *Detect brute force, login anomalies, and suspicious access.*
🔧 **CTmP Experiences & Activities**

- Data Exfiltration Attempt – Real-Time Case
- Stop hidden data theft via DNS tunnelling or HTTPS leaks
- Activity: Attack Detection with SIEM & SOAR
- Correlate alerts, visualize ATT&CK coverage, and execute real-time response

Day 3: Red vs Blue – Analyst in Command

Theme: Simulate. Defend. Win.

Topics
🔷 **SOC Live-Fire Exercise: Run the Show** *Real-world simulation where participants detect and respond to a coordinated cyberattack.*
🔷 **MITRE ATT&CK Navigator in Action** *Visualize gaps in detection and map alerts to attack tactics.*
🔷 **Red Teaming Fusion: From Alert to Action** *From exploitation to containment using integrated SOC tools.*
🔷 **SOAR Playbook Lab: Response on Autopilot** *Create automated response pipelines for common alerts (e.g., phishing, brute force).*
🔧 **CTmP Experiences & Activities** • **Capstone Simulation: Full Incident Lifecycle** Detect, analyze, contain, and report a multi-stage cyberattack. • **Activity: SOC Tabletop & Presentation** Collaborate, report findings, and demonstrate readiness as a future SOC analyst.
Valedictory & Feedback

Participant Profile:

The iSOC 3-day training program is designed for:

- IT professionals (e.g., network engineers, system admins) from government or private sectors
- Technical individuals wanting to switch to or grow in cybersecurity as SOC analysts
- System administrators, network engineers, software developers, or QA/testers seeking cybersecurity roles
- Security enthusiasts with technical skills aiming to upskill or cross-skill
- Professionals seeking a foundation for SOC certifications

Organisational sponsorship is essential

VENUE

The programme is fully residential and the participants will be accommodated in air-conditioned single occupancy rooms. The college does not provide accommodation for the family. The college is Wi-Fi enabled in a comprehensive way.

DURATION

The programme duration is 3 days starting from **November 12 - 14, 2025.** The participants are expected to arrive a day before commencement and may leave after the conclusion of the programme.

PROGRAMME FEE

Residential Fee: **Rs. 43,700/-** (US $683 for foreigners) plus GST as applicable (presently 18%) per participant. The fee covers tuition, board and lodging, courseware (in electronic form) and other facilities of the College including internet usage.

Non-Residential Fee: **Rs. 37,700/-** plus GST as applicable (presently 18%) per participant. The fee covers tuition, course ware (in electronic form) working lunch and other facilities of the College including internet usage.

A discount of 10% on the Programme fee for three or more participants from the same organisation will be given, provided the payment is credited into our Bank account before **November 10, 2025.**

Note: Kindly forward us the details of the Bank/ Wire transfer of the programme fee through email to: poffice@asci.org.in for confirmation.

Bank details are given below:

For Indian Participants:

Bank Account Number	62090698675
Beneficiary Name	Administrative Staff College of India
IFSC Code	SBIN0020063
Bank Name	State Bank of India
Branch Address	Bellavista Branch, Raj Bhavan Road, Somajiguda, Hyderabad - 500 082

For Foreign Participants:

Bank Account Number	62090698675
Beneficiary Name	Administrative Staff College of India
Swift Code	SBININBB327
Bank Name	State Bank of India
Branch Address	Bellavista Branch, Raj Bhavan Road, Somajiguda, Hyderabad - 500 082.
Country	India

MEDICAL INSURANCE

The nominees are requested to carry with them the proof of Medical Insurance. The sponsoring agency is required to endorse the nominees' medical coverage in the event of hospitalization

LAST DATE FOR NOMINATION

Please use the prescribed/attached form. Last date for receiving nominations is **November 05, 2025.** Kindly contact Programmes Officer for further details (contact details are given at the end of the nomination form).

LAST DATE FOR WITHDRAWAL

November 07, 2025. Any withdrawals after this date will entail forfeiture of fee paid, if any.

ASCI ALUMNI ASSOCIATION

Participants of the College programmes will automatically become members of the ASCI alumni association.

CERTIFICATE OF PARTICIPATION

The College issues a Certificate of Participation on conclusion of the programme.

Programme Director

Dr Madhusoodanan PR

Email: mpr@asci.org.in

Administrative Staff College of India (ASCI) is taking all the precautionary measures and following all the norms (in light of COVID 19) to provide a safe environment for the participants who are visiting our Campus to attend the Training Programmes.

ABOUT ASCI

"I need not tell you how important I feel this institution is, not because it is the first in Asia or third in the world, but because obviously,
it performs a task which is of high importance in the present state of our country, perhaps of other countries too."
-- Pandit Jawaharlal Nehru, the First Prime Minister of India during his visit to the College on 23 Oct. 1958

Established in 1956, it is the first and foremost institution of its kind in the country. Set up as an institution with a difference at the joint initiative of both the Government of India and the industry, it is an autonomous, self-supporting, public-purpose institution with the objectives of being a think- tank for policy inputs and to build the capacities of practicing professionals in the management of government and business enterprises.

ASCI is an institution of excellence and national importance, and a registered society by constitution. At the apex of its governance structure is a policy-setting, oversight body, the Court of Governors (CoG). It is a virtual who's who of eminent professionals, public figures and industry leaders who have distinguished themselves in their respective fields of specialization in education, enterprise, administration, management and governance spanning a wide variety of sectors like agriculture, banking, engineering, economics, judiciary, law, manufacturing, science and technology and public administration.

Capacity building and applied research assignments constitute the bedrock of the activities of ASCI. They have larger societal benefit and public good as the key cornerstones. ASCI integrates economic, social, cultural, financial, technological, regulatory, human, organizational, and environmental aspects into its management training and action-research initiatives for addressing issues of topical interest and current concern to the government and the industry. With its focus on policy, strategy, management, governance, regulation and socio-economic impact evaluation, ASCI brings knowledge inputs, informed advice, best practice and innovative ideas to bear on its training, policy advocacy, advisory and implementation-assistance services. In the process, it provides opportunities to State and Central Government Departments and Ministries in India and abroad as well as the industry, to develop sustainable policies, devise inclusive strategies and deploying robust plans towards improved economic performance, human development and social progress.

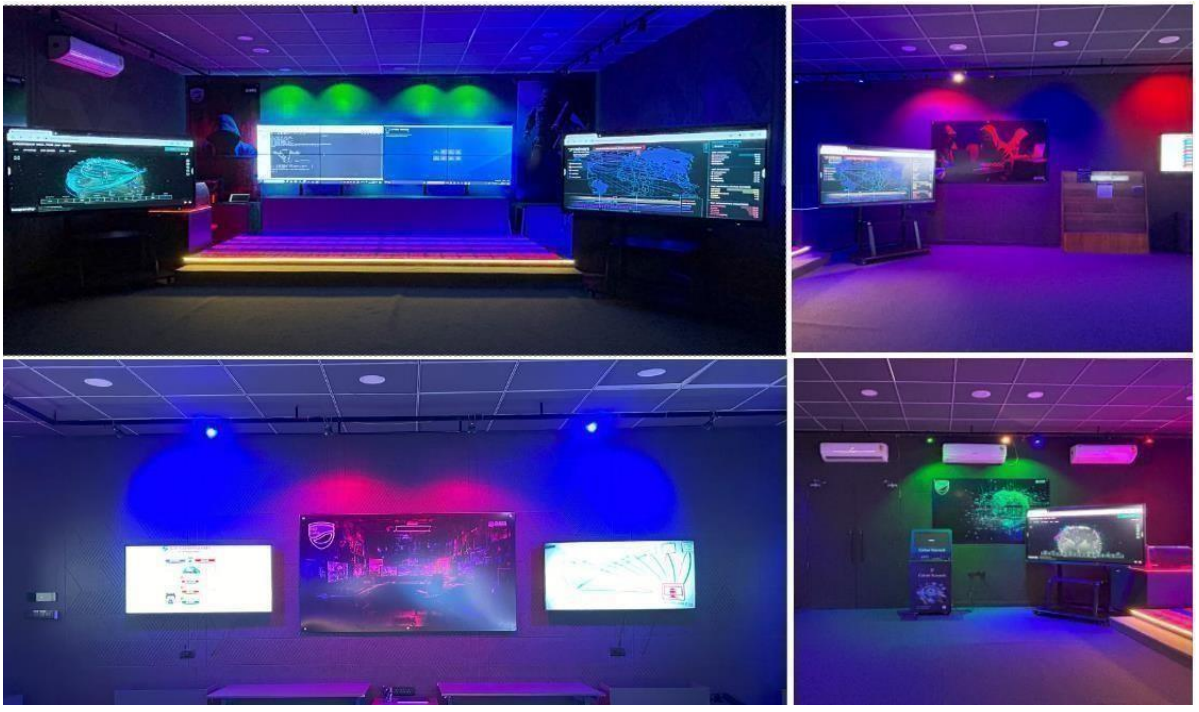
As a result, ASCI enjoys the trust and confidence of the government and industry and is relied upon and entrusted with assignments of varied scale, scope, sweep, spread and specialization.

ABOUT ESF LABS LIMITED

"ESF Labs Limited brings cyber resilience with innovation and excellence."

ESF Labs is a recognized Cyber Security and Digital Forensics Research Centre with over a decade of experience, focusing on delivering effective and innovative solutions and capacity building to clients. As a CERT-INDIA empanelled entity, ESF Labs, aims at assisting its customers to combat the various cyber threats they face through training/capacity building and solutioning. As a trusted partner, ESF Labs, works closely with corporations, law enforcement agencies, and governments to provide consultation services that enhance the client's cybersecurity and digital forensic capabilities. The solutions delivered are designed to minimize the risk exposure of organizations and also providing a strong foundation in cybersecurity and digital forensic posture.

ABOUT CYBER THEME PARK (CTmP) AN EXPERIENCE CENTRE



Cyber Theme Park is an experience centre that transforms theoretical knowledge into practical wisdom. It is a dynamic environment where individuals come together to engage in meaningful interactions, exchange ideas, and challenge their existing perspectives. We believe that true learning occurs when theoretical knowledge is applied and tested in real-life scenarios & situations. Our aim is to bridge the gap between theory and practice by creating an immersive experience with 4 distinct mindsets Attacker, Protector, Defender, and Overseer that transforms abstract concepts into tangible outcomes. The programme seamlessly blends theory with practical, immersing you in the world of attacker and defender techniques.

ADMINISTRATIVE STAFF COLLEGE OF INDIA
Bella Vista, Raj Bhavan Road, Hyderabad - 500 082, India

Nomination Form

Programme on
Intelligent SOC : Behind the Scenes of Threat Detection and Response
(November 12 - 14, 2025)

Nominee's Contact Information

Name (Mr/Ms) : _____ Date of Birth: _____
Designation : _____ Qualification: _____
Organisation : _____
Address : _____
Phone(s) : Office: _____ Mobile: _____ Home: _____
e-mail : _____ Fax: _____

Sponsors Details

Name of the Sponsoring Authority: _____ : Designation: _____
Organisation : _____
GSTIN Number: _____
Address : _____
_____ Pincode: _____
Phone(s) : Office: _____ Mobile: _____
e-mail : _____ Fax: _____

Fee particulars

Amount Payable :	Mode of Payment (DD/Ch/NEFT):
Name of the Bank :	Date of Instrument/Transfer:
Instrument Number:	UTR Number for NEFT

Medical Insurance:

Name of the Insurance Agency	Policy Number	Validity upto
Note: Coverage should be available in Hyderabad, India.		

Signature and Official Seal of the Sponsoring Authority:

NOTE: Forward nomination form to: **Mr. G. Sreenivasa Reddy, Programmes Officer,** Administrative Staff College of India, Bella Vista, Hyderabad-500 082. Phone: 0091-40-66534247, 66533000, Mobile: 9246203535, Fax: 0091-40-66534356, e-mail: **poffice@asci.org.in**