ALL SAFE
CYBERSECURITY & TECHNICAL ACADEMY

OFFICIAL CERTIFICATION BLUEPRINT & CURRICULUM GUIDE

ACADEMY DEFENSIVE SECURITY & INCIDENT RESPONSE PROGRAM

Certified SOC Analyst Certification

Security Operations Center Workflows, Enterprise SIEM Architecture (Splunk, QRadar, Sentinel), Threat Detection & Hunting, Endpoint Forensics, and Incident Response.

Core SOC Competencies & Practical Mastery

INDUSTRY ALIGNED

01
Enterprise SIEM Engineering
Master log ingestion, parsing, normalization, and advanced correlation rule creation across IBM QRadar, Splunk Enterprise, and Microsoft Sentinel.

02
Threat Detection & Hunting
Execute hypothesis-driven threat hunting frameworks, map adversary TTPs to the MITRE ATT&CK matrix, and uncover stealthy in-network persistence.

03
Endpoint Security & Forensics
Deploy modern EDR telemetry, inspect volatile memory & process trees, triage filesystem artifacts, and execute host containment actions.

04
Incident Handling & Cloud Response
Lead complete incident response lifecycles following NIST & SANS standards, automating playbooks with SOAR, and securing AWS & Azure cloud assets.

Live Online	100+ Hours	Multi-SIEM	SOC Tier 1/2
Practical Classes Interactive Real-Time Sessions	Live Hands-On Cyber Range Real Unscripted Attack Scenarios	QRadar, Splunk & Sentinel Industry Gold-Standard Platforms	Career Job Role Readiness Global Certification Alignment

AUTHORIZED ACADEMIC CURRICULUM
ALL SAFE Academy • Cybersecurity Operations Division

Document Ref: AS-CSA-2026-V1
www.allsafeinnovate.com

MODERN DEFENSIVE SECURITY ENGINEERING

Security Operations Center Architecture & The ALL SAFE Advantage

Equipping frontline defenders with enterprise SIEM engineering, proactive threat hunting capabilities, digital forensics, and end-to-end incident containment playbooks.

The Enterprise SOC Defense Ecosystem & Analyst Mission

Enterprise Tier 1 & 2 Blueprint

Modern enterprise organizations operate in an adversarial landscape where continuous security visibility, rapid incident triage, and proactive containment are critical survival capabilities. A Security Operations Center (SOC) serves as the nerve center for detecting intrusions, mitigating zero-day exploits, and stopping ransomware campaigns before data exfiltration occurs.

The ALL SAFE Certified SOC Analyst curriculum bridges the gap between academic theory and high-stress security operations. Analysts-in-training build end-to-end telemetry pipelines, ingest multi-source event logs, configure custom correlation rules, and triage live-fire attack campaigns across on-premises enterprise networks and cloud environments.

IBM QRadar Architecture | Splunk SPL Search Language | Microsoft Sentinel & KQL | MITRE ATT&CK Matrix | EDR & Memory Forensics | SOAR Automated Playbooks

THE 6 ALL SAFE INSTITUTIONAL ADVANTAGES

Standard Across All Career Programs

1. Live Practical Sessions

100% instructor-led live interactive labs simulating active SOC command centers, realistic alert pipelines, and live breach investigations.

2. 24/7 Mentorship Support

Direct one-on-one technical support from senior SOC Tier 2/3 Leads and active Incident Responders whenever you face technical roadblocks.

3. Free International Certs

Structured syllabus mapped to global defensive certifications (CSA, CompTIA CySA+, SC-200) with complete practice exam vouchers and prep.

4. International Experts Community

Lifetime access to the private ALL SAFE professional network of security analysts, SOC engineers, and alumni across Fortune 500 firms.

5. Securiti AI Pro — Free

Complimentary access to proprietary AI tools for automated correlation rule generation, KQL query assistance, and threat intelligence.

6. Career-Oriented Learning

Technical CV optimization, SOC analyst mock technical interviews, scenario-based defense tests, and direct employer referral pipelines.

COMPREHENSIVE 12-DOMAIN CURRICULUM

Certified SOC Analyst Modules

Official enterprise-aligned curriculum covering foundational networking, operating system hardening, multi-SIEM monitoring, threat hunting, digital forensics, and cloud defense.

01. Networking

Foundation

- Network fundamentals and core enterprise architecture
- TCP/IP and OSI reference models in depth
- IP addressing, subnetting and traffic routing
- Network protocols, standard ports and packet flows

02. Operation Systems Security

OS Hardening

- Windows security fundamentals and event auditing
- Linux security hardening and baseline configurations
- File system security, ACLs and integrity monitoring
- User and access management, privilege escalation defense

03. Linux Administration

Linux CLI

- Linux command line essentials for security operators
- System monitoring, centralized syslog and log analysis
- Process management, service inspection and daemons
- Network configuration, firewall rules and socket auditing

04. Cyber Security Attacks

Threat Landscape

- Common attack vectors and MITRE ATT&CK tactics
- Malware types, behaviors and execution lifecycles
- Phishing, credential harvesting and social engineering
- Adversary attack methodologies and weaponization chains

05. SIEM Monitoring

SIEM Core

- SIEM fundamentals, architecture and event ingestion
- Log collection, parsing and data normalization
- Correlation rule creation, thresholding and tuning
- Alert triage, severity scoring and incident queue management

06. IBM QRadar & Splunk

Enterprise SIEM

- IBM QRadar architecture, DSMs and rule deployment
- Splunk Search Processing Language (SPL) and correlation
- Enterprise SOC dashboard creation and trend visualization
- Advanced querying, lookup tables and alert automation

07. Microsoft Sentinel

Cloud SIEM

- Sentinel workspace setup and Log Analytics architecture
- Data connectors configuration (Defender, O365, Syslog, CEF)
- KQL (Kusto Query Language) syntax for threat hunting
- Automation with incident trigger playbooks and Logic Apps

08. Threat Detection & Hunting

Threat Hunting

- Threat hunting methodologies, maturity models and cycles
- IOC-based hunting using threat intelligence feeds
- Behavioral anomaly analysis, network and endpoint baselining
- Hypothesis-driven hunting across multi-host environments

09. Endpoint Security

EDR Telemetry

- EDR solutions architecture, telemetry streams and agents
- Endpoint detection techniques, process parentage and DLLs
- Live endpoint forensics, memory inspection and artifact capture
- Automated response strategies and host isolation procedures

10. Incident Response

Incident Handling

- Incident response lifecycle following NIST SP 800-61 & SANS
- Triage, scoping, impact assessment and chain-of-custody
- Containment strategies, eradication and system restoration
- Post-incident review, remediation roadmaps and reporting

11. Digital Forensics

DFIR Lab

- Digital forensic fundamentals, evidence handling and hashing
- Disk image analysis, filesystem artifacts, MFT and registry
- Volatile memory acquisition, RAM analysis and code injection
- Network forensics, PCAP reconstruction and malware triage

12. Cloud Security Monitoring

Cloud SOC

- Cloud security principles and shared responsibility model
- AWS security monitoring with CloudTrail, GuardDuty and VPC flows
- Azure security monitoring with Defender for Cloud and activity logs
- Cloud incident response, compromised identity and storage triage

CAREER TRANSFORMATION & ROADMAP

SOC Analyst Career Scope, Roadmap & Admissions

How certified SOC analyst capabilities accelerate high-paying defensive cybersecurity careers, program cohort specifications, and official enrollment details.

6 High-Demand Defensive Cybersecurity Career Roles

Tier 1 SOC Analyst
Alert triage, incident logging, initial severity qualification, false-positive elimination, and escalation.

Tier 2 Incident Responder
Deep-dive incident investigation, host containment, memory forensics, and eradication execution.

Cyber Threat Hunter
Proactive hunting, hypothesis formulation, threat intelligence integration, and MITRE mapping.

Enterprise SIEM Engineer
Log onboarding, custom parser writing, correlation rule synthesis, and health monitoring.

DFIR Specialist
Post-breach forensic analysis, timeline reconstruction, evidence preservation, and root-cause analysis.

Cloud Security Analyst
Monitoring AWS and Azure workloads, identity protection, cloud audit logging, and automated playbooks.

The 7-Step Student SOC Analyst Learning Journey

STEP 01	STEP 02	STEP 03	STEP 04	STEP 05	STEP 06	STEP 07
Baselines	**Attacks**	**SIEM Core**	**Cloud SIEM**	**Hunting**	**Response**	**Placement**
Network, TCP/IP, OS hardening & Linux	Threat landscape, malware & MITRE	Splunk SPL & QRadar rules	Sentinel KQL & SOAR playbooks	Hypothesis hunting & EDR telemetry	Incident triage, DFIR & cloud recovery	Mock interviews, cert prep & hiring

Program Specifications & Academic Cohort Details

Program Duration	2 Months (8 Weeks Intensive)	**Delivery Mode**	Live Interactive Instructor-Led Labs
Hands-On Lab Hours	100+ Live Hours on Cyber Range	**Instruction Language**	English • Urdu (Bilingual Support)
Prerequisites	Basic networking & OS knowledge	**Certification Alignment**	Certified SOC Analyst (CSA) Aligned

START BUILDING YOUR DEFENSIVE CYBERSECURITY CAREER WITH ALL SAFE

Join Pakistan's premier cybersecurity academy and gain real-world SOC experience on enterprise SIEM platforms.

Direct WhatsApp: +92 321 2077222 Admissions Email: allsafeus@gmail.com Portal: www.allsafeinnovate.com

Contact ALL SAFE Today to Enroll in the Certified SOC Analyst Program.