Quality Thought
Transforming Dreams ! Redefining Future!

Celebrating 16 Years | A gateway to Your Bright Future

Real-Time SOC Analyst & SIEM Practical Training Program

(Splunk + QRadar + Microsoft Sentinel + ELK Stack)
Industry-Oriented Practical Cybersecurity Training Program

Quality Thought

Offered Programs

TRAINING (Offline / Online)

Any Graduate
By Realtime Practitioners
Realtime Scenario Projects
LMS Access for 6 Months
Resume Preparation
Doubts Clarification
1 Mock Interview
Interview Questions
Placement Referral Support
Course Completion Certificate

Price – ₹40,000

(JOIP) Intensive

Full Day Training
LMS Access for 8 Months
Soft Skills & Aptitude Classes
Monthly Placement Screening Tests
Assignments / Mock Tests
Interview Readiness Sessions
Mega Drive Selection Mandatory for Placements
Placement Assistance for 12 Months
Realtime Scenario Projects by Realtime Practitioners
Weekly 1 Mock Interview

Price – ₹50,000

(JOIP) Intensive & Internship

Internship @ IT Company – Ramana Soft
By Realtime Practitioners
No Mega Drive Selection
3 Hrs Internship / 3 Hrs Training
Interview Questions & Readiness Sessions
Monthly Placement Screening Test
Personalised Assistance for Complex Tasks
6–8 Hrs Daily
LMS Access Up to 1 Year
100% Placement Assistance – Until You're Hired
Internship Completion Certificate – 6 Months from Ramana Soft or Client
Realtime Scenario Projects
Soft Skills & Aptitude Classes

Price – ₹1 Lakh

qualitythought.in
88974 86382, 88858 78710

Program Overview

This program is designed to prepare students for real-time SOC Analyst, SIEM Operations, Security Monitoring, Threat Hunting, and Incident Investigation roles with strong practical exposure on enterprise security tools and real-world attack scenarios.

The course focuses on:

- Real-time log analysis
- SIEM monitoring
- Threat detection
- Security investigations
- Incident response
- Threat hunting
- Practical Splunk implementation
- Use-case development
- Real-world SOC operations

Module 1: Networking & Cybersecurity Foundations

Networking Fundamentals

- OSI Model & TCP/IP Model
- IPv4 & IPv6
- Public vs Private IPs
- Subnetting & CIDR
- Ports & Protocols
- DNS / DHCP / HTTP / HTTPS
- FTP / SMTP / IMAP
- SSH / Syslog
- VPN Concepts
- Proxy Servers
- Firewalls
- IDS/IPS
- NAC Basics
- Packet & Traffic Analysis
- NAC Basics

Packet & Traffic Analysis

- Packet Structure
- Headers & Payloads
- Network Traffic Analysis
- Wireshark Overview
- TCP Handshake
- DNS Flow Understanding

Quality Thought

Cybersecurity Foundations

- CIA Triad
- Cyber Kill Chain
- MITRE ATT&CK Framework
- Threats vs Vulnerabilities vs Risks
- Security Operations Center (SOC)
- SOC Workflow
- Roles & Responsibilities of L1 / L2 / L3 Analysts

Module 2: Windows & Linux Security for SOC

Windows Security

- Windows Architecture Basics
- Windows Event Viewer
- Security Event IDs
- Authentication Logs
- Sysmon Overview
- PowerShell Monitoring
- Process Monitoring
- User Activity Investigation
- Registry Basics
- Task Scheduler Investigation

Linux Security

- Linux File System
- Linux Commands for SOC
- SSH Logs
- Authentication Logs
- Cron Jobs
- Process Monitoring
- Linux Security Logs
- User Monitoring
- Service Monitoring

Module 3: SIEM & Splunk Fundamentals

SIEM Fundamentals

- What is SIEM?
- SIEM Architecture
- Log Collection & Normalization
- Correlation Concepts
- Event Lifecycle
- Alerting & Monitoring

qualitythought.in
88974 86382, 88858 78710

Quality Thought

Splunk Fundamentals

- Splunk Architecture
- Universal Forwarders
- Heavy Forwarders
- Indexers
- Search Heads
- Deployment Basics
- Data Flow in Splunk
- Splunk UI & Navigation
- Data Onboarding

Log Onboarding

- Windows Logs
- Linux Logs
- Firewall Logs
- DNS Logs
- Proxy Logs
- EDR Logs
- Cloud Logs

Module 4: Splunk SPL & Dashboarding

- search | table |replace | rename
- stats | chart | timechart
- sort | fields
- where | eval
- rex | regex
- top | rare
- lookup | append | appendcols | joins
- transaction | eventstats | streamstats
- tstats | mstats

Field Extraction & Parsing

- Regex Basics
- Basic Field Extractions
- Search-Time Parsing Concepts
- Lookup Enrichment

Dashboards & Alerts

- Dashboard Creation
- Panels & Visualizations
- Reports
- Alerts
- Scheduled Searches
- Basic Correlation Searches

Module 5: Splunk Administration for SOC Engineers

Splunk Administration

- Splunk Installation (Windows/Linux)
- Basic Linux Deployment
- inputs.conf Basics
- props.conf Basics
- transforms.conf Basics
- outputs.conf Basics
- Index Management
- Bucket Concepts
- License Basics

Forwarder Management

- Universal Forwarder Configuration
- Heavy Forwarder Concepts
- Deployment Server Basics
- Monitoring Forwarders

Splunk Clustering

- What is Clustering?
- RF & SF Concepts
- Single-Site Indexer Clustering Overview
- Search Head Clustering Overview
- High Availability Concepts
- Enterprise Architecture Awareness

Module 6: Real-Time Log Analysis & Security Investigation

Practical Log Analysis

- Firewall Logs Investigation
- Windows Security Logs Analysis
- Linux Logs Investigation
- DNS Logs Analysis
- Proxy Logs Investigation
- VPN Logs Monitoring
- IDS/IPS Logs Analysis
- Antivirus Logs Investigation
- EDR Logs Investigation
- Cloud Logs Investigation
- Active Directory Log Analysis

Investigation Scenarios

- Brute Force Attacks
- Malware Activity
- Suspicious Authentication
- PowerShell Attacks
- Data Exfiltration
- DNS Tunneling
- Beaconing Activity
- Insider Threat Detection
- Privilege Escalation Investigation
- Lateral Movement Detection

Module 7: Threat Hunting & Detection Engineering

Threat Hunting

- IOC Hunting
- Behavioral Analysis
- MITRE ATT&CK Mapping
- Threat Correlation
- Suspicious Activity Detection
- Baseline vs Anomaly Detection

Quality Thought

Detection Engineering

- Correlation Search Development
- Detection Rule Logic
- Alert Tuning
- False Positive Reduction
- Real-Time Detection Use Cases

Real-Time Security Use Cases

- Failed Login Detection
- VPN Abuse Detection
- Malware Communication Detection
- DNS Threat Detection
- Web Attack Detection
- Insider Threat Monitoring
- Data Exfiltration Detection

Module 8: QRadar, Sentinel & ELK Stack

QRadar

- QRadar Architecture Overview
- Offense Investigation
- Log Source Concepts
- AQL Basics
- Rule Concepts
- Event Correlation

Microsoft Sentinel

- Sentinel Architecture
- KQL Basics
- Analytics Rules
- Incident Investigation
- Hunting Queries
- Workbooks Overview

ELK Stack

- Elasticsearch Basics
- Logstash Basics
- Kibana Dashboards
- Beats Overview
- Log Analysis using ELK

Quality Thought

Module 9: Incident Response & SOC Operations

Incident Response

- Incident Lifecycle
- Alert Triage
- Severity Classification
- Escalation Process
- Malware Investigation
- Phishing Investigation
- IOC Extraction
- Root Cause Analysis
- Timeline Investigation

SOC Operations

- Shift Handling
- Ticketing Workflow
- Case Management
- SOC Reporting
- Analyst Documentation
- Security Metrics & KPI Basics

Module 10: Cloud Security Monitoring

Cloud Fundamentals

- AWS Basics
- Azure Basics
- Cloud Security Concepts
- Shared Responsibility Model

Cloud Monitoring

- AWS CloudTrail Logs
- Azure Activity Logs
- Cloud Threat Monitoring
- IAM Threats
- Suspicious API Activity
- Misconfigured Storage Buckets

Module 11: Real-Time Projects & Attack Simulations

Real-Time SOC Projects

- SOC Monitoring Lab
- Firewall Investigation Lab
- Threat Hunting Lab
- Malware Investigation Lab
- Phishing Investigation Lab
- EDR Investigation Lab
- Cloud Threat Investigation Lab

Attack Simulations

- Brute Force Simulations
- Malware Simulations
- Insider Threat Simulations
- DNS Attack Simulations
- Data Exfiltration Simulations
- Website Attack Investigations

BOTS V1 / V2 / V3 Attack Data Analysis

- Multi-Stage Attack Investigation
- Correlated Security Event Analysis
- End-to-End Incident Investigation

Module 12: Dashboarding, Reporting & Automation

Dashboarding

- SOC Dashboards
- Security Monitoring Dashboards
- Threat Intelligence Dashboards
- KPI Dashboards

Reporting

- Incident Reports
- Security Reports
- Executive Reporting
- Automated Reports

Automation

- Email Alerting
- Basic SOAR Concepts
- ServiceNow Overview
- Jira Overview
- Webhook Basics

Quality Thought

Module 13: Interview & Career Preparation

Career Preparation

- Resume Building
- LinkedIn Optimization
- Mock Interviews
- HR Preparation
- Technical Interview Preparation

Real-Time Interview Scenarios

- SOC Analyst Scenarios
- Splunk SPL Scenarios
- Log Investigation Scenarios
- Threat Hunting Scenarios
- SIEM Investigation Scenarios

Tools Covered

- Splunk Enterprise
- QRadar
- Microsoft Sentinel
- ELK Stack
- Wireshark
- Sysmon
- NXLog
- Winlogbeat
- VirusTotal
- Any.Run
- AWS CloudTrail
- Azure Monitoring
- ServiceNow (Overview)
- Jira (Overview)

Key Highlights

- Real-Time Practical Training
- SOC Analyst Practical Exposure
- SIEM Monitoring & Investigation
- Splunk Practical Implementation
- Real-Time Log Analysis
- Threat Hunting Scenarios
- Detection Rule Development
- Incident Response Workflows
- V1 / V2 / V3 Attack Data Analysis
- Real-Time Attack Simulations
- Dashboard Development
- Cloud Threat Monitoring
- Mock SOC Environment
- Interview Preparation

Quality Thought

Outcomes After Completion

- Become Job-Ready SOC Analyst
- Perform Real-Time Log Investigations
- Work on Enterprise SIEM Platforms
- Build Detection Rules & Alerts
- Investigate Security Incidents
- Perform Threat Hunting Activities
- Analyze Multi-Source Logs
- Work with Splunk, QRadar, Sentinel & ELK
- Crack SOC & SIEM Interviews Successfully

Career Opportunities after this Course

- Red Team Operator / Adversary Emulation Specialist
- Bug Bounty Hunter & Security Researcher
- Offensive Security Consultant
- DevSecOps Engineer
- Container Security Specialist
- Kubernetes Security Engineer

QualityThought – Internship Topics

Security Operations Center (SOC) Internships

- Real-time security monitoring using SIEM tools (Splunk, QRadar, Devo, Elastic)
- Log analysis, threat detection, and incident escalation
- Exposure to MITRE ATT&CK Framework and cyber defense strategies

Malware & Phishing Email Analysis Internships

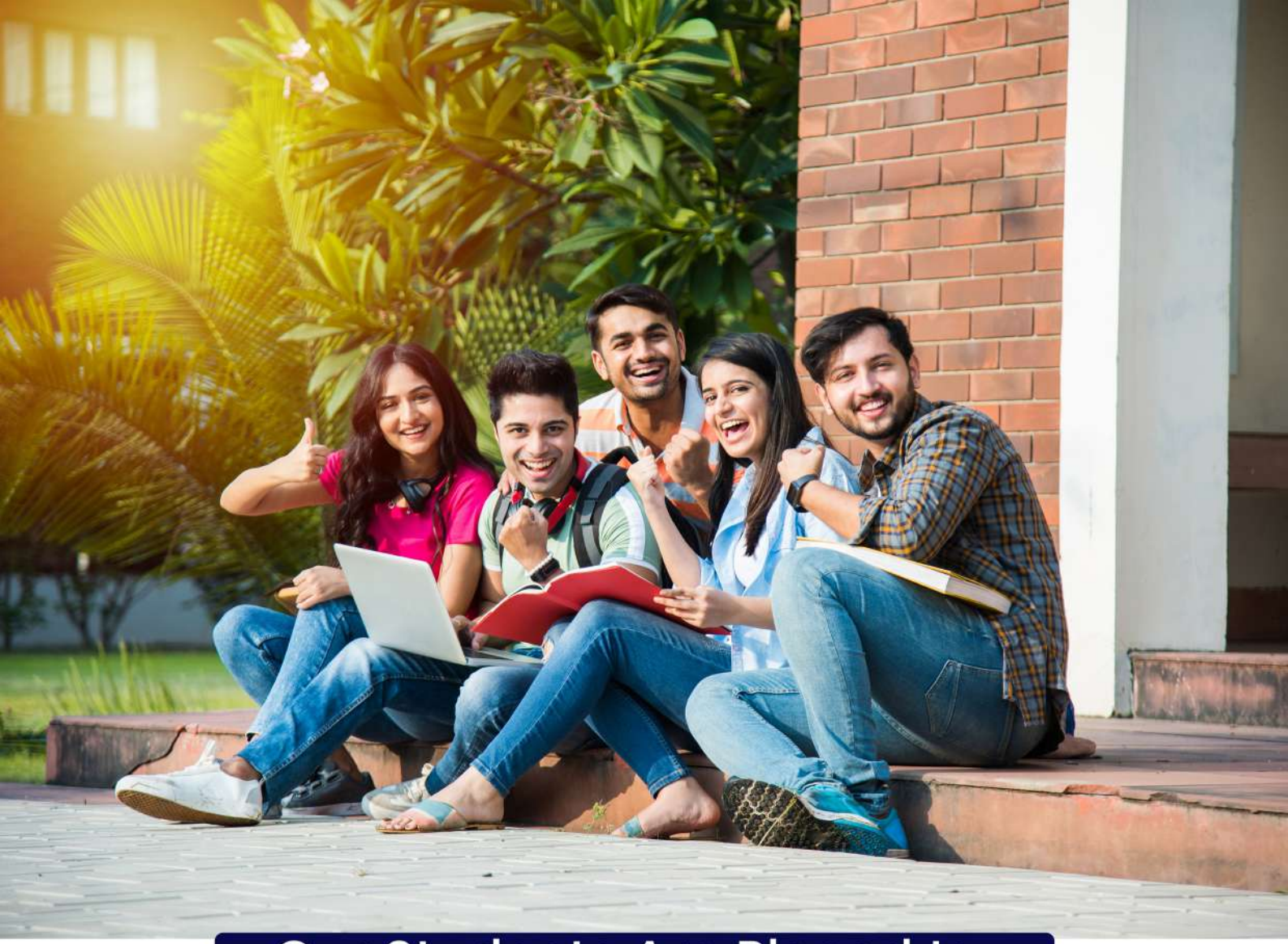
- Analyzing email headers & identifying phishing attempts
- Reverse engineering malware and working in sandbox environments
- Exposure to tools like VirusTotal, Any.Run, Hybrid Analysis

Threat Intelligence & Threat Hunting Internships

- Investigating Indicators of Compromise (IOCs)
- Using Threat Intelligence Platforms (TIPs) such as MISP and OpenCTI
- Monitoring cybercriminal activities on the dark web

Recommended Certifications for Entry-Level Roles

- CompTIA Security+ (Foundational security knowledge)
- Certified SOC Analyst (CSA) (For SOC-related roles)
- Certified Ethical Hacker (CEH) (For penetration testing roles)
- GIAC Security Essentials (GSEC) (General cyber security skills)
- Cyber Threat Intelligence Analyst (CTIA) (For threat intelligence roles)



Our Students Are Placed In

tcs | vsoft ingenuity at work | cognizant | Microsoft | ValueLabs | wipro

amazon | Practera | V-SOFT CONSULTING | erwin | statista | MARBLE TECH

PIERSOFT | SOLIX Empowering Data Management | PrimeSoft | ENVISION | BLACK KNIGHT | CyberTech

Capgemini | sumtotal | archents | servicenow | KENSIUM | KELLTON TECH

LARSEN & TOUBRO | Micron | meslova | splashBI | highradius | PERVACIO

Magnasoft | iPrism Technologies | S&P Global | HEXAWARE | nextsphere TECHNOLOGIES | SOLUGENIX

{actlogica} Actuarial | Finance | Technology | Medtronic | Innominds Engineering Intelligence. Responsibly | Apollo HOSPITALS | Uber | PTW

JRD SYSTEMS always ahead | techolution | techforce.ai | SOLIGENIX | Collabera Value. Accelerated | Fission URANIUM CORP.

Quality Thought Infosystem India (P)Ltd.

#302,Nilgiri Block,Ameerpet,Hyderabad-500016 I www.qualitythought.in I info@qualitythought.in