QualityThought®
Transforming Dreams! Redefining Future!

CELEBRATING
15 YEARS

CYBER SECURITY

Cyber Lab
Access for
Hands-on Training

Direct Training
from Top
CISOs

Video Access
through LMS

qualitythought.in

88974 86382, 88858 78710

Offered Programs

TRAINING (Offline / Online)

1. Any Graduate
2. By Realtime Practitioners
3. Realtime Scenario Projects
4. LMS Access for 6 Months
5. Resume Preparation
6. Doubts Clarification
7. 1 Mock Interview
8. Interview Questions
9. Placement Referral Support
10. Course Completion Certificate

Price
40K+18% GST

(JOIP) Intensive

1. Full Day Training
2. LMS Access for 8 Months
3. Soft Skills & Aptitude Classes
4. Monthly Placement Screening Tests
5. Assignments / Mock Tests
6. Interview Readiness Sessions
7. Mega Drive Selection Mandatory For Placements
8. Placement Assistance for 12months
9. Realtime Scenario Projects
10. By Realtime Practitioners
11. weekly 1 mock interview

Price
50K + 18% GST

(JOIP) Intensive & Internship

1. Internship @IT Company-Ramana Soft
2. By Realtime Practitioners
3. No Mega Drive Selection
4. 3Hrs.- Internship/3Hrs.-Training
5. Interview Questions & Readiness Sessions
6. Monthly Placement Screening Test
7. Personalised Assistance for Complex Tasks
8. 6 - 8 Hrs Daily
9. LMS Access Upto 1Year
10. 100% Placement Assistance - Until you're Hired
11. Internship Completion Certificate-6 Months from Ramana Soft or Client
12. Realtime Scenario Projects
13. Soft Skills & Aptitude Classes

Price
70K + 18% GST

Introduction to Cyber security

- Evolution of Cyber security
- Cyber security & Situational Awareness
- The Cyber security Skills Gap
- Difference between Information Security & Cyber security
- Cyber security Objectives
- Cyber security Roles and Career Paths

Network Fundamentals (Prerequisites)

- Evolution of Cyber security
- Cyber security & Situational Awareness
- The Cyber security Skills Gap
- Difference between Information Security & Cyber security
- Cyber security Objectives
- Cyber security Roles and Career Paths
- Infrastructure Terminology
- Security-Focused Network Design
- Network Topology & Architecture
- OSI Layers & TCP/IP Model
- IPv4 & IPv6 Addressing
- Essential Ports & Protocols
- Firewalls & Intrusion Prevention Systems
- VPNs and VPN Concentrators
- Intrusion Detection & Prevention Systems
- Proxy Servers & Load Balancers
- Network Access Control (NAC) & Zero Trust Architecture
- Secure Mail Gateways

Ethical Hacking Content

- Introduction to CyberSecurity
- Introduction to Ethical hacking
- Computer & Networking Basics
- Lab setup for Virtual Machines
- Foot Print/Information Gathering
- Scanning
- Vulnerability Analysis
- Sniffing & Man-In-Middle
- System Hacking
- Metasploit Attacks.
- Malware Threats
- Phishing Attacks
- Social Engineering Attacks
- Hacking webserver & Web Applications
- SQL Injection
- Wireless Attacks
- Firewalls
- IDS/IPS
- Honeypots
- Cloud Computing
- IOT Hacking
- Cryptography
- Penetration Testing
- Identity Theft
- Security Compliances
- Steganography
- Risk Management
- Mobile Hacking
- DOS/DDOS Attacks
- Proxies & VPn's
- Computer Forensic
- OSIntframework
- Information Gathering with Maltego Tool
- DNS Spoofing
- MAC Spoofing
- Web Application with Nessus Vulnerability Scanner
- Kon Boot for password Breaking
- Countermeasures for Local Systems

Bugbounty

- Introduction to Bug Bounty
- Basic Terminology on Bug Bounty
- Information Gathering
- Lab setup for Bug Bounty
- Installation of Burp Suite Tool
- Bug Bounty Platforms
- Report Writing for Bugs
- Vulnerability Scanner Tools
- Web Application Vulnerabilities
- Cross Site Scripting
- Host Header Injection
- URL Redirection Attack
- Parameter Tampering
- File Upload Vulnerability
- SQL Injection
- Bypass Authentication
- Sensitive Information Disclosure Vulnerability
- CSRF Attack Vulnerability
- Word Press Sensitive information disclosure
- XML Vulnerability in Word Press Vulnerability
- Missing SPF Records vulnerability
- OTP Bypass Technique Vulnerability
- IDOR Vulnerability
- No rate Limit Vulnerability
- Session Hijacking Vulnerability
- Long Password Attack Vulnerability

Security Operations Center (SOC)

- SOC Overview
- SOC Team Structure
- Tier 1 Responsibilities
- Tier 2 Responsibilities
- Tier 3 Responsibilities
- SOC Workflow and Escalation Path
- Alert Lifecycle Stages
- Incident Response Phases
- Types of Alerts Handled in SOC
- Daily SOC Monitoring Activities
- KPIs and Metrics for SOC
- Log Collection Strategy
- Log Parsing and Normalization
- Key SOC Log Sources
- Firewall Logs
- IDS/IPS Logs
- DNS Logs
- Endpoint Logs (Sysmon/EDR)
- Active Directory Logs
- Cloud Logs (CloudTrail, Azure Activity)
- Use Case Design in SIEM
- Rule Writing – SPL (Splunk), AQL (Qradar)
- MITRE ATT\&CK Mapping to Alerts
- Threat Hunting Basics
- Alert Enrichment Techniques
- Alert Suppression & False Positive Handling
- Ticketing Systems (ServiceNow, JIRA) Integration
- Shift Handover Protocols

SIEM and EDR Focus

- Introduction to SIEM
- Overview of Splunk Architecture
- Splunk Ingestion and Indexing
- Writing SPL Queries
- Splunk Dashboards and Alerts
- QRadar Architecture and Flow Collection
- QRadar Rule Creation using CRE
- AQL Querying in Qradar
- Introduction to EDR
- SentinelOne Architecture
- SentinelOne Agent Capabilities
- Remote Response Actions (Kill, Quarantine, Rollback)

Malware Analysis

- Introduction to Malware Analysis
- Malware Categories
  - a. Virus
  - b. Worm
  - c. Trojan
  - d. Ransomware
  - e. Spyware
  - f. Rootkit
  - g. Fileless Malware
- Malware Behavior and Infection Chain
- Static Analysis Fundamentals
- File Header and Metadata Check
- String Extraction (strings, FLOSS)
- PE Header Inspection
- Hashing (MD5, SHA256) and Use Cases
- Dynamic Analysis Overview
- Sandbox Analysis (Any.run, Cuckoo)
- Tools for Monitoring Behavior
  - a. ProcMon
  - b. RegShot
  - c. Wireshark
  - d. TCPView
- Reverse Engineering Introduction
- Disassemblers (Ghidra, IDA Free)
- Debuggers (x64dbg, OllyDbg)
- Packers and Obfuscation
- IOC Extraction Process
- Types of IOCs
- File Hashes
- Registry Keys
- IPs and Domains
- Filenames

Email Security

- Overview of Email-Based Threats
- Anatomy of a Phishing Email
- Spear Phishing vs Generic Phishing
- Business Email Compromise (BEC)
- Malware Delivery via Email
- Spoofing and Lookalike Domains
- Email Header Components
- SPF Record Validation
- DKIM Signature Verification
- DMARC Policy Enforcement
- Email Flow and Received Headers
- Tools for Email Security
  - a. Microsoft Defender for O365
  - b. Cisco ESA
  - c. Proofpoint
  - d. Mimecast
- Email Sandbox Solutions
- SOC Response to Phishing
- IOC Search in Mailboxes
- Quarantining and Purging Emails
- User Awareness and Reporting Channels

Threat Intelligence

- Threat Intelligence Fundamentals
- Intelligence Lifecycle Stages
- Strategic vs Tactical vs Operational vs Technical TI
- IOC Formats (IP, Hash, URL, Domain)
- TI Sources and Feeds
  - a. VirusTotal
  - b. AlienVault OTX
  - c. Recorded Future
  - d. Shodan
  - e. URLScan.io
- MITRE ATT&CK Overview
- IOC Enrichment in SIEM

Digital Forensics (Basic)

- Introduction to Digital Forensics
- Forensics in Incident Response
- Evidence Identification
- Disk Imaging with FTK Imager
- File Recovery and Analysis
- Windows Registry Artifact Locations
- Browser History and Cache Inspection
- Event Log Collection
- Timeline Analysis Basics
- Memory Analysis using Volatility
- Chain of Custody Requirements
- Legal Considerations for Evidence
- Role of Forensics in Root Cause Analysis

Cloud Security

- Cloud Security Fundamentals
- Shared Responsibility Model
- Cloud Infrastructure Threats
- Misconfigured Storage Buckets (e.g., S3)
- Cloud Resource Exploitation
- Unmonitored API Calls and Access Keys
- Credential Theft from Repositories
- Cloud Identity Attacks
- Lateral Movement in Cloud Environments
- Lack of Visibility and Logging

Mobile Security – Threats Only

- Cloud Security Fundamentals
- Shared Responsibility Model
- Cloud Infrastructure Threats
- Misconfigured Storage Buckets (e.g., S3)
- Cloud Resource Exploitation
- Unmonitored API Calls and Access Keys
- Credential Theft from Repositories
- Cloud Identity Attacks
- Lateral Movement in Cloud Environments
- Lack of Visibility and Logging

Internship Topics

Penetration Testing Internships

- Hands-on testing of networks, web applications, APIs
- Working with Metasploit, Burp Suite, Nmap, and Kali Linux
- Companies offering internships: Security firms, ethical hacking teams, and bug bounty programs

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 MITREATT&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 Virus Total, Any. Run, Hybrid Analysis

Threat Intelligence & Threat Hunting Internships

- Investigating Indicators of Compromise (IoCs)
- UsingThreatIntelligencePlatforms(TIPs)suchasMISPand 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)

Career Opportunities after this Course

- SOC Analyst (L1/L2)
- Threat Intelligence Analyst
- Incident Responder
- Cyber security Analyst
- SIEM Engineer
- SOC Analyst (Tier 1, Tier 2, Tier 3)
- Threat Hunter
- Security Operations Engineer
- Incident Responder
- Cyber Threat Intelligence Analyst
- Network Security Engineer
- Firewall & Perimeter Security Administrator
- SOC Analyst (Network Security Focus)
- Threat Detection Engineer
- Cloud Network Security Engineer
- Penetration Tester (Web, Network, Wireless, Cloud)
- Red Team Operator / Adversary Emulation Specialist
- Bug Bounty Hunter & Security Researcher
- Offensive Security Consultant
- Exploit Developer & Malware Analyst
- Career Opportunities after this Course
- Cloud Security Engineer
- Cloud Security Architect
- DevSecOps Engineer
- Container Security Specialist
- Kubernetes Security Engineer
- Cloud Compliance & Risk Analyst

Our Students Are Placed In

	tcs TATA CONSULTANCY SERVICES	vsoft	Cognizant	Microsoft	ENVISION	sunseaz Technologies Pvt Ltd	wipro	VSOFT	amazon
PrimeSoft	statista	Practera	PIERSOFT	KELLTON TECH	Capgemini	KENSIUM	SOLIX	sumtotal A Skillsoft Company	MIRABEL TECHNOLOGIES
VALUEMOMENTUM	PERVACIO	Apollo	LARSEN & TOUBRO	STIC Soft	Advi	NOOR	servicenow	ValueLabs	erwin
CyberTech	BLACK KNIGHT	Micron	highradius	HEXAWARE	NextSphere	GLOBAL	splashBI	archents	techforce.ai
Nendrasys	magnasoft	Innominds Powering the Digital Next	High Noon Consulting.	JRD SYSTEMS	Medtronic	MAXO	PTW	Uber	techolution
SOLUGENIX	Collabera	iPrism Technologies	meslova	{actlogica}	S&P Global	Fission	SOLIGENIX	TechnoFacts	SAHASYA

QualityThought®
Transforming Dreams! Redefining Future!

| ☎ 88974 86382, 88858 78710

Quality Thought Infosystems India (P) Ltd.

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