Quality Thought

CYBER SECURITY with AI

90 Live Sessions
Hands on Labs

Direct Training
From Top
CISOs

Video access
throuhg LMS

Quality Thought

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

(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. Realtime Scenario Projects
9. Placement Assistance for 12months
10. By Realtime Practitioners
11. weekly 1 mock interview

Price 50K+30K

TRAINING (Offline / Online)

1. Internship @IT Company-Ramana Soft
2. By Realtime Practitioners
3.Hrs.- Internship/3Hrs.-Training
4. No Mega Drive Selection
5. Interview Questions & Readiness Sessions
6. Monthly Placement Screening Test
7. 6 - 8 Hrs Daily
8. LMS Access Upto 1Year
9. Personalised Assistance for Complex Tasks
10. 100% Placement Assistance - Until you're Hired
11. Internship Completion Certificate-6 Months from Ramana Soft or Client Price 50K 1
2. Realtime Scenario Projec

Price 1 Lakh+30K

88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

Quality Thought

Introduction to Cybersecurity

- The evolution of Cybersecurity
- Cybersecurity & situational awareness
- The Cybersecurity skills gap
- Difference between information security & cybersecurity
- Cybersecurity objectives
- Cybersecurity Roles

Understanding Devices and Infrastructure

- Infrastructure Terminology
- Designing with Security in Mind
- Network Topology
- OSI Layers & TCP/IP Model
- IPv4 & Ipv6
- Ports & protocols
- Port numbers Firewalls
- VPNs and VPN Concentrators
- Intrusion Detection Systems Router
- Switch
- Proxy
- Load Balancer
- Access Point
- Network Access Control (NAC)
- Mail Gateway Br

88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

Quality Thought

Ethical Hacking Bugbounty

- 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
- ocial 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
- Information Gathering with Maltego Tool
- DNS Spoofing
- MAC Spoofing

- Introduction to Bug Bounty
- Basic Terminology on Bug Bounty
- Installation of Burp Suite Tool
- Bug Bounty Platforms
- Report Writing for Bugs
- XML Vulnerability in Word Press Vulnerability
- Missing SPF Records vulnerability
- OTP Bypass Technique Vulnerability
- No rate Limit Vulnerability
- Session Hijacking Vulnerability
- Long Password Attack Vulnerability

Vulnerability Management

- Introduction to Vulnerability Assessment
- Types of Vulnerability Assessment
- Basic Terminology for Vulnerability Assessment
- Vulnerability Assessment life cycle
- Vulnerability Assessment tools (Nessus, Openvas)
- Report analysis
- Risk assessment

88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

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),
- 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.Wireshar 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

88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

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 RecordValidation ن
- DKIM Signature Verification
- DMARC Policy Enforcement
- Email Flow and Received Headers
- Tools for Email Security
  a. Microsoft Defender for O365
  b. Proofpoint
  c. 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 Cloud Security
- 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
- MemoryAnalysis using Volatility
- Chain of Custody Requirements
- Legal Considerations for Evidence
- Roleof 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 Loggin

Module : Identity & Access Management (IAM) with Okta

- IAM Fundamentals: Core Principles, Authentication vs. Authorization, Identity Lifecycle (Joiner–Mover–Leaver)
- Authentication & Federation: MFA, SSO, SAML, OAuth 2.0, OpenID Connect (OIDC)
- Access Control Models: RBAC, ABAC, Least Privilege, Zero Trust
- Identity Governance & Security: PAM, Access Reviews, Compliance, Role Mining
- Okta Administration: User Provisioning & Deprovisioning, SSO Configuration, MFA Policies, Directory Integration (AD, Azure AD, LDAP)
- Hands-on Labs: Okta tool

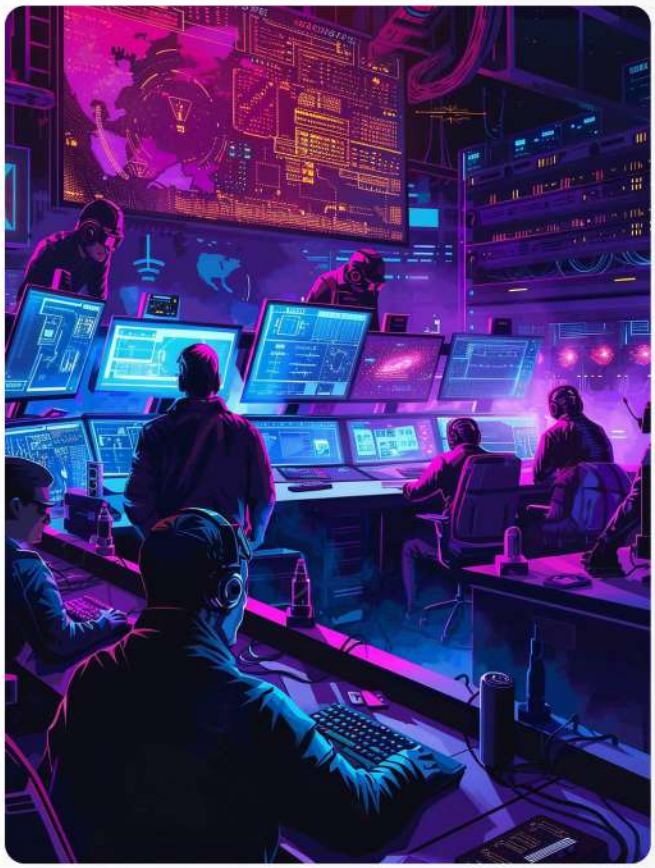
88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

Quality Thought

AI in Cybersecurity

- Introduction to AI in Cybersecurity
- What is Artificial Intelligence (AI) & Machine Learning (ML)
- Difference between AI, ML, and Deep Learning
- Why AI matters in modern cybersecurity
- Generating policy templates using LLMs
- NLP-based review for policy clarity & compliance alignment
- OneTrust AI – Policy automation & compliance tracking
- Open-source AI risk tools: RiskSense, OpenGRC



Governance & Information Security Frameworks

- Overview of Governance in Cybersecurity
- Role of governance in InfoSec
- Key governance principles and policies
- Information Security Management Systems (ISMS)
- Purpose and structure of ISMS
- PDCA (Plan–Do–Check–Act) cycle
- Major Cybersecurity Frameworks
- ISO 27001/27002 Overview
- NIST Cybersecurity Framework (CSF)
- CIS Controls
- COBIT for Information Security Governance
- Security Policies & Standards
- Policy hierarchy (Policies → u Standards → Procedures → Guidelines)
- Writing effective security policies
- Roles & Responsibilities in GRC
- Board, CISO, risk managers, compliance officers
- RACI matrix in security governance

88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

Quality Thought

RED TEAM

(Attack / Offensive Security) Tools

* Kali Linux
* Parrot OS
* Nmap
* Burp Suite
* Metasploit Framework
* SQLmap
* Hydra
* Hashcat
* John the Ripper
* Gobuster
* FFUF
* Nikto
* Aircrack-ng
* Netcat
* theHarvester
* Shodan
* Tor Browser
* Psiphon
* TMAC (Technitium MAC Address Changer)

BLUE TEAM

(Defense / Defensive Security) Tools

* Wireshark
* Tcpdump
* Nessus
* OpenVAS
* OWASP ZAP
* Splunk
* Wazuh
* ELK Stack (Elasticsearch, Logstash, Kibana)
* Microsoft Sentinel
* Snort
* Suricata
* CrowdStrike Falcon
* Microsoft Defender for Endpoint
* Palo Alto Cortex XDR
* Velociraptor
* MISP
* OpenCTI
* VirusTotal
* ANY.RUN
* Cuckoo Sandbox
* YARA
* Autopsy
* Volatility
* Ghidra
* IDA Free
* REMnux
* FLARE VM
* Sysinternals Suite
* Process Explorer
* Process Monitor (ProcMon)
* Sysmon
* Autoruns
* TCPView
* PsExec
* Sigcheck
* Handle
* WinObj
* Strings
* Event Viewer
* Windows Performance Monitor
* Windows Resource Monitor

88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

Quality Thought

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

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 securityskills)
- Cyber Threat Intelligence Analyst (CTIA) (For threat intelligence roles)

88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

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

88974 86382, 88858 78710

#302, 3rd floor, Nilagiri Block
Beside Metro station, Ameerpet, Hyderabad.

Quality Thought

THINK QUALITY • DELIVER EXCELLENCE

More Details
88974 86382

Online
qualitythought.in

100,000+
Students Trained

60,000+
Students Placed

1000+
Placement Companies

16 Years
of Student Trust

OUR STUDENTS ARE PLACED IN

TCS	Microsoft	Cognizant	accenture	Capgemini	wipro	Infosys	amazon	Deloitte.	UBER
Persistent	Tech Mahindra	HCLTech	LTI Let's Solve	Mindtree	Mphasis The Next Applied	HEXAWARE	virtusa	servicenow	freshworks
ZOHO	Adobe	ORACLE	SAP	BYJU'S	INTUIT	paloalto	CISCO	Flipkart	meesho
SAMSUNG	SONATA SOFTWARE	Qualcomm	BOSCH	zscaler	PTW	Micron	NOKIA	Collabera	D-Link
cybertrust	SOUCENEXT	Redington	VALUE LABS	KPIT	opentext	ramco	Globallogic	HITACHI Inspire the Next	HEXAWARE

Quality Thought Infosystems India (P) Ltd.

302, 3rd Floor, Nilgiri Block, Aditya Enclave,
Ameerpet, Hyderabad, Telangana 500016