Quality Thought®
Transforming Dreams! Redefining Future!

CELEBRATING 15 YEARS

SOC ANALYST

100,000+ Students Trained

1000+ Placement Companies

60,000+ Students Placed

15 Years of Student Trust

88974 86382, 88858 78710

#302, Nilgiri Block, Aditya Enclave, Ameerpet, Hyd.,Telangana-500016

qualitythought.in | ihubtalent.com

QualityThought®
Transforming Dreams! Redefining Future!

CELEBRATING 15 YEARS

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

QualityThought®
Transforming Dreams! Redefining Future!

CELEBRATING 15 YEARS

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

QualityThought®
Transforming Dreams! Redefining Future!

CELEBRATING 15 YEARS

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

Our Students Are Placed In

TCS · Capgemini · LTIMindtree · accenture
CLOUD9 · CloudCover · Coforge · CGI · CISCO · Cloud4C · amazon
databricks · dataflex · DXC TECHNOLOGY · Cognizant · Convergytics · CSS CORP · Medtronic
genpact · HCL · HSBC · Deloitte. · EMIDS · Foray · STIC Soft
Infosys · Legato · MINDGRAPH · Mindtree · motivitylabs · photon · meslova
pwc · quantiphi · RENAULT · SIGMASOFT · SOFTILITY · syren cloud · splashBI
TIGER ANALYTICS · wipro · ENVISION · virtusa · ValueLabs · zensor. · SOLIX
JRD SYSTEMS · ValueLabs · archents · magnasoft · Innominds · techforce.ai · techolution

QualityThought

88974 86382, 88858 78710

Quality Thought Infosystems India (P) Ltd.

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