CELEBRATING
14 YEARS

QualityThought®

Transforming Dreams! Redefining Future!

Cybersecurity
Splunk/SOC Analyst

Cybersecurity Splunk/SOC Analyst

Cyber Security

- What is Cybersecurity
- What is Hacking
- What is Ethical Hacking
- Types of Hacking attacks
- What is Security
- Network case study
- Enterprise network case study.
- Incident responce and Management (SIEM)
- Incident responce
- Security and Monitoring.

SPLUNK

- What is Splunk
- What is Machine data.
- Prerequisites
- Products of Splunk
- Components of Splunk
- Splunk Architecture
- Setting up Splunk search head, indexer
- Setting up Splunk forwarders
- Splunk Licensing, Configuration files on Linux
- Splunk File Precedence
- Splunk Default Ports
- Configuration files on Windows
- Basic AWS Cloud for Infrastructure usage
- Basic Linux which for Splunk needs
- Difference between Linux and Windows OS in Splunk configuration
- Types of files supported in Splunk
- Common Splunk configuration files:
- inputs.conf, outputs.conf, indexes.conf, server.conf, web.conf,
- deploymentclient.conf, savedsearches.conf.

Types of Forwarders

- Universal Forwarders
- Lighter Forwarders
- Heavy Forwarders

Data On-boarding

- Upload
- Monitor
- Forwarders

Data Stages in Splunk through Queues

- Parsing
- Merging
- Typing
- Indexing
- Null
- Persistent

Field Extraction

- Index-time Field Extraction
- Search-time Field Extraction
- Which is best Practice at Splunk point of view

Types of Searches and Optimization of Searches

- Dense
- Sparse
- Super Sparse
- Rare

Splunk Search Commands and Reporting Commands

Basic search commands-
Ex: Fields, Table, Sort, Rename, Search; Understand time range of search.
Learn reporting and transforming commands in Splunk-
Ex: Top, rare, stats, chart, Timechart, Dedup, Rex, regex fields, table, rename, multikv, tstats, eventstats, streamstats, append, mvappend, loadjob, join etc...
Usage of following commands and their functions: Top, Rare, Stats, Addcoltotals, Addtotals

- Explore the available visualizations
- Creation of charts and timecharts
- Omit null values and format results

Cybersecurity Splunk/SOC Analyst

Managing Users, Indexes, Splunk Admin Roles and Clustering

- User creation and management
- Managing indexes
- Importance of roles
- Different permissions of each indexes
- Splunk development concepts
- Roles and responsibilities of Splunk Developer
- How to configure LDAP authentication in Splunk
- Admin role in managing Splunk
- What is alert?
- Reports and dashboards
- Coordinating with Splunk Support
- Implement Search Head Clustering
- Implement Indexer Clustering

Deployment Process, Alerts, Tags and Event Types

- Deploy Apps using Deployment server
- creating tags and using them in search
- Defining event types and their usefulness
- Creating and using event types in search
- creating and modifying alerts and use of Alerts

Analyzing & Calculating Results Fields Extraction and Lookups

- Using eval command
- Perform calculations
- Understand fields
- Maintain and monitor Logs
- Format values
- Importance of logs
- Filtering calculated results
- Raw Data Manipulation
- Extraction of Fields,
- What are lookups?
- Lookup file example
- Creating a lookup table
- Defining a lookup
- Configuring an automatic lookup
- Using the lookup in searches and reports

Splunk Visualizations, Reports and Dashboards

- Explore the available visualizations
- Creating reports and
- Creating dashboards and adding reports

Splunk Enhanced Solutions

- Save and share search results
- Save searches
- Schedule searches

Single Site Clustering and Multi-Site Clustering

- Deployment server's deep explanation
- [Advance] Splunk Clustering techniques-1
- [Advance] Splunk Clustering techniques-2
- [Advance] Splunk Clustering techniques-3

Data Ageing and Buckets Concept

- Managing Index and indexes
- Buckets like Hot, Warm Cold, Frozen and Thawed

Troubleshooting and Interview Assistance

- Troubleshoot Clustered environment
- Interview discussions/questions/guidance
- Project assignment, doubts and Q/A

Troubleshooting and Interview Assistance

- Troubleshoot Clustered environment
- Interview discussions/questions/guidance
- Project assignment, doubts and Q/A

Cybersecurity
Splunk/SOC Analyst

Security operations center(SOC)

- ➪ What is SOC
- ➪ Tools available in SOC
- ➪ Falcon.Croudstrike
- ➪ Security Posture
- ➪ SIEM
- ➪ End point detection and response- EDR
- ➪ Ticketing system - Servicenow/Jira
- ➪ Threat intelligence plotform - TIP
- ➪ SOAR
- ➪ Types of SOC
- ➪ Internal SOC
- ➪ Distributed SOC
- ➪ Global SOC
- ➪ Co Managed SOC
- ➪ Basic team Hierarchy
- ➪ L1 Analyst
- ➪ L2 Analyst
- ➪ SOC lead or L3 Analyst
- ➪ SOC Manager
- ➪ SIEM Engineer
- ➪ Process
- ➪ End result
- ➪ Series of Actions

Communication Skills

Roots of Communication	LSRW	
	7 Cs of Communication	
Roots of Grammar	Parts of Speech	Mastering Helping Verb And Main Verb
	Sentence Structure Development	
	Tense Logic	
	Worksheet Sessions	
Speech Intelligence	Vocabulary Development	
	Usage of words	
	Group Discussions	
	JAMS	
	Debates	
	Public Speaking	
Personality Development	Imagination and Innovation Training	
	Centralized Brain Storming	
	Problem Solving Skill s	
	Desiion Making	
Mangement Skills	Time Management	
	Team Building	
	Task Management	
	Leadership Skills	
Interview Skills	Employbility	
	Think like a Professional	
	Clearing HR Rounds	
	Salary Negotiation	
	Bond Negotiation	
Presentation Skills	Research Skills	Dream Company Reading Skillls Comprehension Skills
	Public Speaking	
	Visualization	
	White Board Presentation	
	Mastering Powerpoint	
	Content Creation	
Personality Development	Mind Mapping	
	Role plays	
	Mock Interview on the Hot Seat	
	Listening Skills	
	Critical Thinking	
	Thought Analysis	
	SWOT Analysis	

APTITUDE & REASONING

Quantitative

- Basic Maths
- Algebra
- Percentages
- Profit And Loss
- Discounts
- Averages
- Time and Work
- Chain Rule
- Pipes and Cisterns
- Ratios
- Proportions
- Partnerships
- Time and Distance
- Trains
- Boats and Streams
- Simple Interest
- Compound Interest

Data Interpretation

- Bar Charts
- Line Charts
- Pie Charts
- Table Charts

Reasoning

- Directions
- Letter Series
- Number Series
- Coding - Decoding
- Blood Relations
- Statement and Assumption
- Analogy
- Odd Man Out Series
- Venn Diagrams
- Mirror Images
- Water Images
- Arranging in Order
- Paper Folding / Cutting
- Grouping
- Counting the figures
- Clocks
- Calenders
- Seating Arrangements
- Syllogism
- Puzzles

Our Students Are Placed In	tcs TATA CONSULTANCY SERVICES	vsoft ingenuity at work	Cognizant	Microsoft	ENVISION	Sunseaz Technologies Pvt Ltd	wipro	VSOFT	amazon
PrimeSoft	statista	Practera	PIERSOFT	KELLTON TECH	Capgemini	KENSIUM	SOLIX Empowering Data Management	sumtotal A Skillsoft Company	MIRABEL TECHNOLOGIES
VALUE MOMENTUM	PERVACIO	Apollo HOSPITALS	LARSEN & TOUBRO	STIC Soft When you need the results	Aadvi Tech Solutions	NOOR	servicenow	ValueLabs	erwin
CyberTech	BLACK KNIGHT	Micron	highradius	HEXAWARE	NextSphere technologies	GLOBAL Management Services	splashBI	archents	techforce.ai
Nendrasys	magnasoft	Innominds Powering the Digital Next	High Noon Consulting.	JRD SYSTEMS	Medtronic	MAXO	PTW	Uber	techolution
SOLUGENIX	Collabera Value. Accelerated.	iPrism Technologies	meslova	{actlogica} Actuarial | Finance | Technology	S&P Global	Fission Technosolutions	SOLIGENIX	TechnoFacts	SAHASYA GLOBAL SOLUTIONS

QualityThought®
Transforming Dreams! Redefining Future!

| ✆ 73373 44490

Quality Thought Infosystems India (P) Ltd.

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