DevSecOps Certified Professional (DSOCP)

About DevOpsSchool

DevOpsSchool is a unit of "Cotocus PVT ltd" and a leading platform which helps IT organizations and professionals to learn all the emerging technologies and trend which helps them to learn and embrace all the skills, intelligence, innovation and transformation which requires to achieve the end result, quickly and efficiently. We provide over 40 specialized programs on DevOps, Cloud, Containers, Security, AI, ML and on Big data that are focused on industry requirement and each curriculum is developed and delivered by leading experts in each domain and aligned with the industry standards.

About Course

These days, every company in the software industry have started pushing code faster and more frequently than ever. Which is raising the rates of vulnerabilities in our systems and products day by day too. Thanks to DevOps which makes it possible to do more with less efforts but we must integrate security into our process as soon as we can to avoid the vulnerabilities. This is the reason DevSecOps concept came into the picture.

“DevSecOps Certified Professional” certification course is especially curated to educate the approach of integrating security into the practices and emphasizes the professional use of security discipline as the principal means of safeguard to the organization and customer.

After attending this training you will have a good understanding and practical knowledge of tools, techniques, technologies which are related to DevSecOps, and you would be able to implement DevSecOps pipeline, culture for your project or product independently.

Co-ordinator – Mantosh Singh
Call/WhatsApp:- +91 700 483 5930
Mail Address:- contact@DevOpsSchool.com

Secondary contact – Biraj Kumar
Call/WhatsApp:- +91 968 682 9970
Mail Address:- contact@DevOpsSchool.com

Duration	72 Hrs
Mode	Online (Instructor-led, live & Interactive)
Projects (Real time scenario based)	1

FEATURES	DEVOPSSCHOOL	OTHERS
Lifetime Technical Support	✔	✖
Lifetime LMS access	✔	✖
Top 30 Tools	✔	✖
Interview KIT (Q&A)	✔	✖
Training Notes	✔	✖
Step by Step Web Based Tutorials	✔	✖
Training Slides	✔	✖
Training + Additional Videos	✔	✖

Training

Upon completion of this program you will get 360-degree understanding of DevSecOps methodology. This course will give you thorough learning experience in terms of understanding the concepts, mastering them thoroughly and applying them in real work environment.

Projects

You will be given industry level real time projects to work on and it will help you to differentiate yourself with multi-platform fluency, and have real-world experience with the most important tools and platforms.

Interview

As part of this, You would be given complete interview preparations kit, set to be ready for the DevSecOps role. This kit has been crafted by 200+ years industry experience and the experiences of nearly 10000 DevOpsSchool's DevOps learners worldwide.

Agenda/Course outline of the DevSecOps Training

SDLC Models & Architecture with Agile, DevOps, SRE & DevSecOps, SOA & Micro services - Concept

- Let's Understand about Software Development Model
- Overview of Waterfall Development Model
- Challenges of Waterfall Development Model
- Overview of Agile Development Model
- Challenges of Agile Development Model
- Requirement of New Software Development Model
- Understanding an existing Pain and Waste in Current Software Development Model
- What is DevOps?
- Transition in Software development model
    - Waterfall -> Agile -> CI/CD -> DevOps -> DevSecOps
- Understand DevOps values and principles
- Culture and organizational considerations
- Communication and collaboration practices
- Improve your effectiveness and productivity
- DevOps Automation practices and technology considerations
- DevOps Adoption considerations in an enterprise environment
- Challenges, risks and critical success factors
- What is DevSecOps?
    - Let's Understand DevSecOps Practices and Toolsets.
- What is SRE?
    - Let's Understand SRE Practices and Toolsets.
- List of Tools to become Full Stack Developer/QA/SRE/DevOps/DevSecOps
- Microservices Fundamentals
- Microservices Patterns
    - Choreographing Services
    - Presentation components
    - Business Logic

- Database access logic
- Application Integration
- Modelling Microservices
- Integrating multiple Microservices

- Keeping it simple
  - Avoiding Breaking Changes
  - Choosing the right protocols
  - Sync & Async
  - Dealing with legacy systems
  - Testing
- What and When to test
- Preparing for deployment
- Monitoring Microservice Performance
- Tools used for Microservices Demo using container

Platform - Operating Systems - Centos/Ubuntu & VirtualBox & Vagrant – 4 Hrs

- Installing CentOS7 and Ubuntu
- Accessing Servers with SSH
- Working at the Command Line
- Reading Files
- Using the vi Text Editor
- Piping and Redirection
- Archiving Files
- Accessing Command Line Help
- Understanding File Permissions
- Accessing the Root Account
- Using Screen and Script
- Overview of Hypervisor
- Introduction of VirtualBox
- Install VirtualBox and Creating CentOS7 and Ubuntu Vms
- Understanding Vagrant
- Basic Vagrant Workflow
- Advance Vagrant Workflow
- Working with Vagrant VMs
- The Vagrantfile
- Installing Nginx

- Provisioning
- Networking
- Sharing and Versioning Web Site Files
- Vagrant Share
- Vagrant Status
- Sharing and Versioning Nginx Config Files
- Configuring Synced Folders

Platform - Cloud - AWS - 4 hrs

- Introduction of AWS
- Understanding AWS infrastructure
- Understanding AWS Free Tier
- IAM: Understanding IAM Concepts
- IAM: A Walkthrough IAM
- IAM: Demo & Lab
- Computing:EC2: Understanding EC2 Concepts
- Computing:EC2: A Walkthrough EC2
- Computing:EC2: Demo & Lab
- Storage:EBS: Understanding EBS Concepts
- Storage:EBS: A Walkthrough EBS
- Storage:EBS: Demo & Lab
- Storage:S3: Understanding S3 Concepts
- Storage:S3: A Walkthrough S3
- Storage:S3: Demo & Lab
- Storage:EFS: Understanding EFS Concepts
- Storage:EFS: A Walkthrough EFS
- Storage:EFS: Demo & Lab
- Database:RDS: Understanding RDS MySql Concepts
- Database:RDS: A Walkthrough RDS MySql
- Database:RDS: Demo & Lab
- ELB: Elastic Load Balancer Concepts
- ELB: Elastic Load Balancer Implementation
- ELB: Elastic Load Balancer: Demo & Lab
- Networking:VPC: Understanding VPC Concepts
- Networking:VPC: Understanding VPC components
- Networking:VPC: Demo & Lab

Platform - Containers - Docker - 4 hrs

- What is Containerization?
- Why Containerization?
- How Docker is good fit for Containerization?
- How Docker works?
- Docker Architecture
- Docker Installations & Configurations
- Docker Components
- Docker Engine
- Docker Image
- Docker Containers
- Docker Registry
- Docker Basic Workflow
- Managing Docker Containers
- Creating our First Image
- Understading Docker Images
- Creating Images using Dockerfile
- Managing Docker Images
- Using Docker Hub registry
- Docker Networking
- Docker Volumes
- Deepdive into Docker Images
- Deepdive into Dockerfile
- Deepdive into Docker Containers
- Deepdive into Docker Networks
- Deepdive into Docker Volumes
- Deepdive into Docker Volume
- Deepdive into Docker CPU and RAM allocations
- Deepdive into Docker Config
- Docker Compose Overview
- Install & Configure Compose
- Understanding Docker Compose Workflow
- Understanding Docker Compose Services
- Writing Docker Compose Yaml file
- Using Docker Compose Commands
- Docker Compose with Java Stake
- Docker Compose with Rails Stake
- Docker Compose with PHP Stake
- Docker Compose with Nodejs Stake

Planning and Designing - Jira & Confluence (2 + 2 = 4 hrs)

JIRA

- Overview of Jira
- Use cases of Jira
- Architecture of Jira
- Installation and Configuraration of Jira in Linux
- Installation and Configuraration of Jira in Windows
- Jira Terminologies
- Understanding Types of Jira Projects
- Working with Projects
- Working with Jira Issues
- Adding Project Components and Versions
- Use Subtasks to Better Manage and Structure Your Issues
- Link Issues to Other Resources
- Working in an Agile project
- Working with Issues Types by Adding/Editing/Deleting
- Working with Custom Fields by Adding/Editing/Deleting
- Working with Screens by Adding/Editing/Deleting
- Searching and Filtering Issues
- Working with Workflow basic
- Introduction of Jira Plugins and Addons.
- Jira Integration with Github

Confluence

- Exploring Confluence benefits and resources
- Configuring Confluence
- Navigating the dashboard, spaces, and pages
- Creating users and groups
- Creating pages from templates and blueprints
- Importing, updating, and removing content
- Giving content feedback
- Watching pages, spaces, and blogs
- Managing tasks and notifications
- Backing up and restoring a site
- Admin tasks
    - Add/Edit/Delete new users
    - Adding group and setting permissions
    - Managing user permissions
    - Managing addons or plugins
    - Customizing confluence site

- Installing Confluence
  - Evaluation options for Confluence
  - Supported platforms
  - Installing Confluence on Windows
  - Activating Confluence trial license
  - Finalizing Confluence Installation

Source Code Versioning - Git using Github - 4 hrs

- Introduction of Git
- Installing Git
- Configuring Git
- Git Concepts and Architecture
- How Git works?
- The Git workflow

- Working with Files in Git
  - Adding files
  - Editing files
  - Viewing changes with diff
  - Viewing only staged changes
  - Deleting files
  - Moving and renaming files
  - Making Changes to Files

- Undoing Changes
  - Reset
  - Revert

- Amending commits
- Ignoring Files
- Branching and Merging using Git
- Working with Conflict Resolution
- Comparing commits, branches and workspace
- Working with Remote Git repo using Github
- Push - Pull - Fetch using Github
- Tagging with Git

Code Analysis & Securing Code (SAST) - SonarQube & OWASP SonarQube - 2 hrs

- What is SonarQube?
- Benefits of SonarQube?
- Alternative of SonarQube
- Understanding Various License of SonarQube
- Architecture of SonarQube
- How SonarQube works?
- Components of SonarQube
- SonarQube runtime requirements
- Installing and configuring SonarQube in Linux
- Basic Workflow in SonarQube using Command line
- Working with Issues in SonarQube
- Working with Rules in SonarQube
- Working with Quality Profiles in SonarQube
- Working with Quality Gates in SonarQube
- Deep Dive into SonarQube Dashboad
- Understanding Seven Axis of SonarQube Quality
- Workflow in SonarQube with Maven Project
- Workflow in SonarQube with Gradle Project
- OWASP Top 10 with SonarQube

Webserver - Apache HTTP & Nginx - 2 + 2 = 4 hrs

- Introduction to web server
- Install Apache on CentOS 7.4
- Enable Apache to automatically start when system boot
- Configure the firewall service
- Where is Apache?

- Directory structure
    - Apache directory structure
    - Configuration file
    - Create your first page
- Virtual hosts
    - Setting up the virtual host - name based
    - Setting up the virtual host - port based
- Using aliases and redirecting
    - Configuring an alias for a url
    - Redirects
- Logging
    - The error log
    - The access log
    - Custom log
    - Log rotation
- Security
    - Basic Security - Part 1
    - Basic Security - Part 2
    - Set up TLS/SSl for free
    - Basic authentication
    - Digest authentication
    - Access Control
    - .htaccess (Administrator Side)
    - .htaccess (User Side)
    - Install and Configure antivirus
    - Mitigate dos attacks - mod_evasive
- Apache Performance and Troubleshooting
    - Apache Multi-Processing Modules (MPMs)
    - Adjusting httpd.conf - Part 1
    - Adjusting httpd.conf - Part 2
    - Troubleshoot Apache (Analyz Access Log) - Part 1
    - Troubleshoot Apache (Analyze Access Log) - Part 2
    - Use Apachetop to monitor web server traffic

- Installation
    - Server Overview
    - Installing with a Package Manager
    - Building Nginx from Source & Adding Modules
    - Adding an NGINX Service
    - Nginx for Windows
- Configuration
    - Understanding Configuration Terms
    - Creating a Virtual Host
    - Location blocks
    - Variables
    - Rewrites & Redirects
    - Try Files & Named Locations
    - Logging
    - Inheritance & Directive types
    - PHP Processing
    - Worker Processes
    - Buffers & Timeouts
    - Adding Dynamic Modules
- Performance
    - Headers & Expires
    - Compressed Responses with gzip
    - FastCGI Cache
    - HTTP2
    - Server Push
- Security
    - HTTPS (SSL)
    - Rate Limiting
    - Basic Auth
    - Hardening Nginx
    - Test your knowledge
    - Let's Encrypt - SSL Certificates

Securing infra & compliance - Chef InSpec - 2 hrs

- About InSpec
  - Orchestration, Configuration Management, Validation to Deployment
  - Automating Security Validation Using InSpec
  - Processing InSpec Results

- Overview
  - InSpec Profile Structure
  - InSpec Controls Structure
  - InSpec Results
    - Failure
    - Pass
    - Multiple Controls

- Environment Setup
  - Download and Install VirtualBox
  - Download and Install Vagrant
  - Clone or Download-Unzip This Course Repository
  - Setup Environments
    - Run Vagrant to install the Virtual Environment
    - Setup network in VirtualBox
  - Vagrant Credentials
  - AWS Credentials

- Studying an InSpec profile
  - Understanding the profile structure
  - Understand a control's structure
  - Understand a describe block's structure
    - file
    - it
    - should
    - be_directory

- Exploring the InSpec Shell
- Enter the shell
- Explore the file resource
- Explore the nginx resource
- Write the InSpec controls

- Refactor the code to use Attributes
    - Multiple Attribute Example
- Running baseline straight from Github/Chef Supermarket
- Viewing and Analyzing Results
    - Syntax
    - Supported Reporters
    - Putting it all together
- Automation Tools
- Additional InSpec tricks
    - rspec Explicit Subject
    - looping file structure
- Create basic profile
    - Download STIG Requirements Here
    - Example Control V-38437
    - Getting Started on the RHEL6 baseline
    - Completed RHEL6 Profile for Reference
- Cleanup Environments

Container Orchestration - Kubernetes & Helm Intro - 4 hrs

Kubernetes

- Understanding the Need of Kubernetes
- Understanding Kubernetes Architecture
- Understanding Kubernetes Concepts
- Kubernetes and Microservices
- Understanding Kubernetes Masters and its Component
    - kube-apiserver
    - etcd
    - kube-scheduler
    - kube-controller-manager

- Understanding Kubernetes Nodes and its Component
    - kubelet
    - kube-proxy
    - Container Runtime

- Understanding Kubernetes Addons
    - DNS
    - Web UI (Dashboard)
    - Container Resource Monitoring
    - Cluster-level Logging
- Understand Kubernetes Terminology
- Kubernetes Pod Overview
- Kubernetes ReplicationContrller Overview
- Kubernetes Deployment Overview
- Kubernetes Servcie Overview
- Understanding Kubernetes running environment options
- Working with first Pods
- Working with first ReplicationContrller
- Working with first Deployment
- Working with first Services
- Introducing Helm
- Basic working with Helm

Infrastructure Coding - Terraform - 4 hrs

- Deploying Your First Terraform Configuration
    - Introduction
    - What's the Scenario?
    - Terraform Components
- Updating Your Configuration with More Resources
    - Introduction
    - Terraform State and Update
    - What's the Scenario?
    - Data Type and Security Groups
- Configuring Resources After Creation
    - Introduction
    - What's the Scenario?
    - Terraform Provisioners
    - Terraform Syntax

- Adding a New Provider to Your Configuration
    - Introduction
    - What's the Scenario?
    - Terraform Providers
    - Terraform Functions
    - Intro and Variable
    - Resource Creation
    - Deployment and Terraform Console
    - Updated Deployment and Terraform Commands

Network configurations and Service Discovery - Consul - 2 hrs

- Why Consul?
    - Modern Ops Challenges
    - An Explosion of Services
    - First Class Service Discovery
    - Distributed Failure Detection
    - Reactive Configuration via Key/Value Store
    - Multi Datacenter Aware
- Monitoring Nodes
    - Nodes and Services
    - What We Will Set Up
    - Defining the consul-server Node
    - Launching the consul-server Node
    - Network Interfaces on consul-server
    - Exercise Consul Is Easy to Install
    - Installing Consul
    - Running the Consul Dev Agent
    - Running Consul Locally to Access the Web UI
    - Interface Web UI
    - Interface HTTP API
    - Interface DNS
    - Interface CLI RPC
    - Client vs. Cluster Address Conventions

- Challenge Spin Up Web and LB nodes
- Defining Web and LB Nodes
- Running Web and LB Nodes
- Consul Agent On Web and LB nodes
- Remote Command Execution Across Cluster
- Graceful Leave vs. Failure

- Service Discovery
  - From Nodes to Services
  - Registering a Web Service
  - Service Definitions
  - Health Checking the Web Service
  - Launching NGINX
  - Consul DNS for Randomized Internal Service Load Balancing
  - HTTP API and Failing Services
  - Exercise Register Load Balancer
  - Maintenance Mode
  - Registration Methods
- Dynamic LB Config with consul-template
  - HAProxy
  - Setup Script for HAProxy
  - Static HAProxy Config
  - Handling Failed Services
  - HAProxy Config Template
  - What Is Consul Template?
  - Installing Consul Template
  - Consul Template Dry Mode
  - Dynamically Regenerate HAProxy Config
  - Rolling Updates with Maintenance Mode
  - Other Tools Like Consul Template
  - Benefits Recap and What Next
- Reactive Configuration via Key/Value Store Why?
  - Creating Keys and Folders in the Web UI
  - Key Value CRUD via the CLI
  - Exercise Get KV Data into HAProxy

- Reactive, Real Time Configuration Files
- Revolutionizing Configuration Management
- Blocking Queries
- Tools to Investigate

- Health Checking
  - Intro
  - Terms Agent, Client, and Server Mode
  - Gossip and Edge Triggered Updates
  - Understanding Serf Health Status
  - Node and Service Level Check Definitions
  - Custom Node Level Health Checks of Disk, Memory, and CPU
  - Self Healing Nodes
  - Health Checking Is the Value at the Last Transition
  - Health Check Recap
  - Don't Forget to Try This Out
  - Consul Docs Overview

Securuing Containers & Kubernetes (RASP) - Falco & Notary - 2 and 2 = 4 hrs

Falco - 2 hrs

- Securing Containers (RASP)- Twistkock
- Falco Components
- Userspace program
- Falco Configuration
- Privilege escalation using privileged containers
- Namespace changes using tools like setns
- Read/Writes to well-known directories such as /etc, /usr/bin, /usr/sbin
- Creating symlinks
- Ownership and Mode changes
- Unexpected network connections or socket mutations
- Securing Containers (RASP)- Falco
- Spawned processes using execve
- Falco drivers
- Falco userspace program

- Executing shell binaries such as sh, bash, csh, zsh, etc
- Executing SSH binaries such as ssh, scp, sftp, etc
- Mutating Linux coreutils executables
- Mutating login binaries
- Mutating shadowutil or passwd executables

Notary – 2 hrs

- What is CNCF Notary
- Why CNCF Notary?
- What is The Update Framework (TUF)?
- Understand the Notary service architecture & Brief overview of TUF keys and roles
- Architecture and components
- Example client-server-signer interaction
- Threat model
- Notary server compromise
- Notary signer compromise
- Notary client keys and credentials compromise
- Run a Notary service
- Notary configuration files

Securing credentials - HashiCorp Vault & SSL & Certificates – 2hrs

- Introduction
- Vault Concepts and Use Cases
- Vault Comparison
- Installing Vault
- Installing Vault Demo
- Starting a Dev Server
- Basic Secret Management
- Managing Secrets Demo
- Working with Secrets
- Introduction
- Key Value Secrets Engines
- Key Value Secrets Lifecycle Demo

- Scenario and General Secrets Engines
- Working with Secrets Engines
- Key Value Secrets Engine Demo
- Database Secrets Engine
- MySQL Secrets Engine Demo
- Dynamic Secrets
- Dynamic Secrets Demo
- Auditing Actions in Vault
- Audit Architecture and Device Types
- Vault Audit Commands
- Vault Audit Scenario
- Vault Enabling Auditing
- Vault Audit Log Review
- Vault Reviewing Audit Logs
- Operating Vault Server
- Overview
- Vault Server Architecture
- Storage Backend Options
- Installation Scenario
- Setting up the Consul Server
- Installing the Consul Agent
- Vault Server Configuration
- Installing Vault Server
- Server Operations
- Unseal and Initialize Vault Server
- Rotating and Updating Keys
- Managing Root Token
- Controlling Access in Vault
- Overview
- Authentication Methods
- Enabling the Userpass Method
- Logging in with Userpass
- Active Directory Authentication
- Vault Policies

- Creating Policies
- Configuring LDAP Authentication
- Client Tokens
- Response Wrapping
- Using Response Wrapping

- **SSL & Certificates**
  - How SSL works
  - Types of SSL
  - Demo with OpenSSL
  - How Certificates based auth works!

Infrastructure Monitoring Tool 1 - Datadog - 4 hrs

- Getting started
  - Integrations
  - Infrastructure
  - Host Map
  - Events
  - Dashboards
- Datadog Tagging
  - Assigning Tags
  - Using Tags
- Agent
  - Datadog Agent Usage
  - Datadog Agent Docker
  - Datadog Agent Kubernetes
  - Datadog Agent Cluster Agent
  - Datadog Agent Log Collection
  - Datadog Agent Proxy
  - Datadog Agent Versions
  - Datadog Agent Troubleshooting

- Datadog Integrations
  - Apache & Tomcat & AWS & MySql

- Datadog Metrics
    - Metrics Introduction
    - Metrics Explorer
    - Metrics Summary
- Datadog Graphing
    - Dashboards and Metrics
- Datadog Alerting
    - Monitors
    - Manage Monitors
    - Monitor Status

Log Monitoring Tool 1 - Splunk - 4 hrs

- What Is Splunk?
    - Overview
    - Machine Data
    - Splunk Architecture
    - Careers in Splunk
- Setting up the Splunk Environment
    - Overview
    - Splunk Licensing
    - Getting Splunk
    - Installing Splunk
    - Adding Data to Splunk
- Basic Searching Techniques
    - Adding More Data
    - Search in Splunk
    - Demo: Splunk Search
    - Splunk Search Commands
    - Splunk Processing Language
    - Splunk Reports
    - Reporting in Splunk
    - Splunk Alerts
    - Alerts in Splunk

- Enterprise Splunk Architecture
    - Overview
    - Forwarders
    - Enterprise Splunk Architecture
    - Installing Forwarders
    - Installing Forwarders
    - Troubleshooting Forwarder Installation
- Splunking for DevOps and Security
    - Splunk in DevOps
    - DevOps Demo
    - Splunk in Security & Enterprise Use Cases
- Application Development in Splunkbase
        - What Is Splunkbase?
        - Navigating the Splunkbase
        - Creating Apps for Splunk
        - Benefits of Building in Splunkbase
- Splunking on Hadoop with Hunk
        - What Is Hadoop?
        - Running HDFS Commands
        - What Is Hunk?
        - Installing Hunk
        - Moving Data from HDFS to Hunk
    - Composing Advanced Searches
        - Splunk Searching
        - Introduction to Advanced Searching
        - Eval and Fillnull Commands
        - Other Splunk Command Usage
        - Filter Those Results! & The Search Job Inspector

    - Creating Search Macros
        - What Are Search Macros?
        - Using Search Macros within Splunk
        - Macro Command Options and Arguments
        - Other Advanced Searching within Splunk

Log Monitoring Tool 2 - ELK stake - 4 hrs

- Introduction to Elasticsearch
- Overview of the Elastic Stack (ELK+)
- Elastic Stack
- Architecture of Elasticsearch
    - Nodes & Clusters
    - Indices & Documents
    - A word on types
    - Another word on types
    - Sharding
    - Replication
    - Keeping replicas synchronized
    - Searching for data
    - Distributing documents across shards
- Installing Elasticsearch & Kibana
    - Running Elasticsearch & Kibana in Elastic Cloud
    - Installing Elasticsearch on Mac/Linux
    - Using the MSI installer on Windows
    - Installing Elasticsearch on Windows
    - Configuring Elasticsearch
    - Installing Kibana on Mac/Linux
    - Installing Kibana on Windows
    - Configuring Kibana
    - Kibana now requires data to be available
    - Introduction to Kibana and dev tools
- Managing Documents
    - Creating an index
    - Adding documents
    - Retrieving documents by ID
    - Replacing documents
    - Updating documents
    - Scripted updates

- Upserts
- Deleting documents
- Deleting indices
- Batch processing
- Importing test data with cURL
- Exploring the cluster

- Mapping
  - Introduction to mapping
  - Dynamic mapping
  - Meta fields
  - Field data types
  - Adding mappings to existing indices
  - Changing existing mappings
  - Mapping parameters
  - Adding multi-fields mappings
  - Defining custom date formats
  - Picking up new fields without dynamic mapping
- Analysis & Analyzers
  - Introduction to the analysis process
  - A closer look at analyzers
  - Using the Analyze API
  - Understanding the inverted index
  - Analyzers
  - Overview of character filters
  - Overview of tokenizers
  - Overview of token filters
  - Overview of built-in analyzers
  - Configuring built-in analyzers and token filters
  - Creating custom analyzers
  - Using analyzers in mappings
  - Adding analyzers to existing indices
  - A word on stop words

- Introduction to Searching
    - Search methods
    - Searching with the request URI
    - Introducing the Query DSL
    - Understanding query results
    - Understanding relevance scores
    - Debugging unexpected search results
    - Query contexts
    - Full text queries vs term level queries
    - Basics of searching
- Term Level Queries
    - Introduction to term level queries
    - Searching for a term
    - Searching for multiple terms
    - Retrieving documents based on IDs
    - Matching documents with range values
    - Working with relative dates (date math)
    - Matching documents with non-null values
    - Matching based on prefixes
    - Searching with wildcards
    - Searching with regular expressions
    - Term Level Queries
- Full Text Queries
    - Introduction to full text queries
    - Flexible matching with the match query
    - Matching phrases
    - Searching multiple fields
    - Full Text Queries
- Adding Boolean Logic to Queries
    - Introduction to compound queries
    - Querying with boolean logic
    - Debugging bool queries with named queries
    - How the “match” query works

Performance & RUM Monitoring - NewRelic - 4 hrs

- Introduction and Overview of NewRelic
  - What is Application Performance Management?
  - Understanding a need of APM
  - Understanding transaction traces
  - What is Application Performance?
  - APM Benefits
  - APM Selection Criteria
  - Why NewRelic is best for APM?
  - What is NewRelic APM? & How does NewRelic APM work?
  - NewRelic Architecture & Terminology
- Installing and Configuring NewRelic APM Agents for Application
  - Register a Newrelic Trial account
  - Installing a JAVA Agent to Monitor your Java Application
  - Installing a PHP Agent to Monitor your PHP Application
  - Installing New Relic Agent for .NET Framework Application
  - Installing a Docker based Agent to Monitor your Docker based Application
  - Understanding of NewRelic Configuration settings of newrelic.yml
  - Understanding of NewRelic Agent Configuration settings
- Working with NewRelic Dashboard
  - Understanding a transactions
  - Understanding Apdex and Calculating and Setting Apdex Threshold
  - Understanding Circuit break
  - Understanding Throughput
  - Newrelic default graphs
  - Understanding and Configuring Service Maps
  - Understanding and Configuring JVM
  - Understanding Error Analytics
  - Understanding Violations
  - Understanding and Configuring Deployments
  - Understanding and Configuring Thread Profiler
  - Depp Dive into Transaction Traces
  - Profiling with New Relic

- Creating and managing Alerts
- Working with Incidents
- Sending NewRelic Alerts to Slack
- Assessing the quality of application deployments

- Monitoring using Newrelic
  - View your applications index
  - APM Overview page
  - New Relic APM data in Infrastructure
  - Transactions page
  - Databases and slow queries
  - Viewing slow query details & External services page
  - Agent-specific UI & Viewing the transaction map
- Deep Dive into Newrelic Advance
  - Newrelic transaction alerts
  - Configure abnd Troubleshoot and Cross Application Traces
  - NewRelic Service Level Agreements
  - Troubleshooting NewRelic
  - Understanding and Configuring NewRelic X-Ray Sessions
  - Deep Dive into NewRelic Agent Configuration
  - Adding Custom Data with the APM Agent
  - Extending Newrelic using Plugins
  - Finding and Fixing Application Performance Issues with New Relic APM
  - Setting up database montioring using Newrelic APM
  - Setting up and Configuring Newrelic Alerts
- Working with NewRelic Performance Reports
  - Availability report
  - Background jobs analysis report
  - Capacity analysis report
  - Database analysis report
  - Host usage report
  - Scalability analysis report
  - Web transactions analysis report
  - Weekly performance report

Emergency Response & Alerting & Chat & Notification - SMTP, SES, SNS, Pagerduty & Slack - Self-learning video

Security Through Logs 1 - Splunk SIEM - 4 hrs

- Module 1 Getting Started with ES
    - Provide an overview of Splunk for Enterprise Security (ES)
    - Identify the differences between traditional security threats and new adaptive threats
    - Describe correlation searches, data models and notable events
    - Describe user roles in ES & Log on to ES
- Module 2 Security Monitoring and Incident Investigation
    - Use the Security Posture dashboard to monitor enterprise security status
    - Use the Incident Review dashboard to investigate notable events
    - Take ownership of an incident and move it through the investigation workflow
    - Use adaptive response actions during incident investigation
    - Create notable events
    - Suppress notable events
- Module 3 – Investigations
    - Use ES investigation timelines to manage, visualize and coordinate incident investigations
    - Use timelines and journals to document breach analysis and mitigation efforts
- Module 4 – Forensic Investigation with ES
    - Investigate access domain events & Investigate endpoint domain events
    - Investigate network domain events & Investigate identity domain events
- Module 5 – Risk and Network Analysis
    - Understand and use Risk Analysis
    - Use the Risk Analysis dashboard & Manage risk scores for objects or users

Security Through Logs 2 - Elastic search with Kibana Security - 4 hrs

- SIEM Introduction
- SIEM Components
- Setup and Configure ELK
- Understanding a types of Threats
- Introduction to threat hunting on an endpoint platform
- Hunt types
- Install Beats shippers
    - Filebeat for forwarding and centralizing logs and files
    - Auditbeat for collecting security events
    - Winlogbeat for centralizing Windows event logs
    - Packetbeat for analyzing network packets
- Data Source in ELK for Security Scanning
- Enable modules and configuration options
- Auditbeat & Discover Anomaly detection
    - System module - Linux, macOS, Win
        - Packages
        - Processes
        - Logins
        - Sockets
        - users and groups
    - Auditd module (Linux Kernel Audit info)
    - File integrity module (FIM) - Linux, macOS, Win
- Filebeat & Discover Anomaly detection
    - system logs (auth logs) – Linux
    - Santa – macOS
- Winlogbeat & Discover Anomaly detection
    - Windows event logs – Windows
- Packetbeat & Discover Anomaly detection
    - Flows
    - DNS
    - other protocols

- Filebeat & Discover Anomaly detection
    - Zeek NMS module
    - Suricata IDS module
    - Iptables/Ubiquiti module
    - CoreDNS module
    - Envoy proxy module (Kubernetes)
    - Palo Alto Networks firewall module
    - Cisco ASA firewall module
- Understanding SIEM UI
    - Timelines
    - Hosts
    - Network
    - Raw Event Data
- Threat Hunting with Kibana
    - Introduction to the threat hunting and the Elastic Stack
    - Network data
    - Host data
    - Data enrichment
    - Threat hunting
    - Guided Hunt
- Elastic Endpoint Security Triage and Response
    - Triage and tune & Alert management
    - Detection and response & Hunting malicious activity
    - Advanced tradecraft analytics

Cloud Security service & Practices - Cloud Security with AWS service - 4 hrs

- Identity & access management
    - AWS Identity & Access Management (IAM)
    - AWS Single Sign-On
    - Amazon Cognito
    - AWS Directory Service
    - AWS Resource Access Manager
    - AWS Organizations

- Detection
  - AWS Security Hub
  - Amazon GuardDuty
  - Amazon Inspector
  - AWS Config
  - AWS CloudTrail
  - AWS IoT Device Defender
- Infrastructure protection
  - AWS Shield
  - AWS Web Application Firewall (WAF)
  - AWS Firewall Manager

Thank you!

Connect with us for more info

Call/WhatsApp:- +91 700 483 5930
Mail:- contact@DevOpsSchool.com
www.DevOpsSchool.com