EC-Council Certified DevSecOps Engineer (ECDE) v2 - Course Outline

Module 01 Understanding DevOps Culture

LO#1: Understand the Evolution of the Software Development Life Cycle

- Evolution of Software Development Life Cycle (SDLC)
- Waterfall Methodology
- Drawbacks of Waterfall Methodology
- Agile Methodology
- Drawbacks of Agile Methodology
- DevOps Methodology
- Advantages of DevOps Methodology
- Waterfall vs. Agile vs. DevOps Methodology

LO#2: Understand what DevOps is

- What is DevOps?
- Main Goals of DevOps Methodology
- Benefits of DevOps
- Building Blocks of DevOps
- What is Continuous Integration and Continuous Deployment (CI/CD) in DevOps?
- Phases of the DevOps Pipeline
- DevOps Practices
- On-Premises DevOps Vs. Cloud Native DevOps
- DevOps Tools
- Summary of DevOps Tools

- DevOps Services in the Cloud
- AI Tools used in DevOps

LO#3: Learn to Implement DevOps in an On-Premises Environment

- Project Management Tool: Jira
- Project Management Tool: Confluence
- Project Management Tool: Slack
- IDE for Coding: Eclipse
- IDE for Coding: Visual Studio
- Source-Code Management Tool: GitHub
- Source-Code Management Tool: GitLab
- Build Tool: Maven
- Build Tool: Packer
- Build Tool: Gradle
- Continuous Testing Tool: Selenium
- Continuous Integration Tool: Jenkins
- Continuous Integration Tool: Bamboo
- Continuous Integration Tool: TeamCity
- Infrastructure as Code Tool: Terraform
- Configuration Management Tool: Ansible
- Configuration Management Tool: Chef
- Configuration Management Tool: Puppet
- Container Management Tool: Docker
- Container Management Tool: Kubernetes
- Continuous Monitoring Tool: Splunk
- Continuous Monitoring Tool: Nagios
- Continuous Monitoring Tool: Elastic Stack - ELK

LO#4: Learn to Implement DevOps in an AWS Cloud Native Environment

- Amazon Web Services (AWS) DevOps
- AWS CodeBuild
- AWS CodePipeline

- AWS CodeDeploy
- AWS CodeCatalyst
- Deploying a PaaS Application using CodePipeline
- Deploy an AWS Elastic Beanstalk Application using AWS CodePipeline
- Deploy a Container Based Application using AWS Elastic Kubernetes Services (EKS)
- Integrate Jenkins Pipeline with Amazon Elastic Container Service (ECS)/ Fargate Plugin in Jenkins

LO#5: Learn to Implement DevOps in an Azure Cloud Native Environment

- Azure DevOps
- Azure DevOps Tools and Services
- Azure Boards
- Tracking Work on Backlogs and Boards
- Managing Access Control in Azure DevOps
- Integrate Azure DevOps with Jira Using Exalate
- Azure Repos
- Review and Merge Code Changes with a Pull Request in Azure Repos
- Azure Pipelines
- Configure Azure Build Pipeline for Continuous Integration
- Deploying ARM Project with Azure DevOps Pipeline
- Deploying Azure Kubernetes Services (AKS) in Azure Portal
- Automatic Build and Deployment with Azure Static Web Apps
- Azure Artifacts
- Use Azure Artifacts to Publish and Consume NuGet Packages
- Azure Test Plans
- Running Automated Tests using Azure Test Plans
- Azure Application Insights
- Monitoring Application Performance with Application Insights

LO#6: Learn to Implement DevOps in a Google Cloud Native Environment

- GCP Devops
- Cloud Code
- GCP Cloud Build

- Automate CI/CD Pipelines with Cloud Build
- Cloud Artifact Registry
- Cloud Deploy
- Google Cloud Deployment Manager
- Google Kubernetes Engine (GKE)
- Orchestrate Containers with Kubernetes Engine
- Google Cloud Monitoring
- Monitor Google Cloud Environment using Cloud Monitoring

LO#7: Understand the Frameworks and Maturity Model in DevOps

- DevOps Framework: Culture, Automation, Lean, Measurement, and Sharing (CALMS)
- Devops Framework: DevOps Value Stream Management (DVSM)
- What is the DevOps Maturity Model?
- Measuring DevOps Maturity
- Transformation Stages of the DevOps Maturity Model
- Components of the DevOps Maturity Model
- DevOps Maturing Practices
- Principles for DevOps Success
- Best Practices for Successful DevOps Implementation

LO#8: Evaluate Security Silos in DevOps

- Bottlenecks to the DevOps Process
- DevOps Security Challenges

Module 02 Introduction to DevSecOps

LO#1: Addressing DevOps Process Security Bottlenecks and Challenges

- Fix DevOps Security Bottlenecks by Shifting Security to the Left
- Addressing DevOps Security Challenges

LO#2: Understand DevSecOps

- What is DevSecOps?
- DevSecOps Manifesto
- DevSecOps State of Mind
- Common Misconceptions and Misinterpretations Regarding DevSecOps

- Benefits of DevSecOps
- Steps in the DevSecOps Pipeline
- DevSecOps Pillars
- DevSecOps Areas for a Successful Project
- Metrics for Measuring DevSecOps Success
- DevSecOps Challenges and Mitigation
- Spectrum of DevSecOps Stakeholders
- Important Security Behaviors in DevSecOps

LO#3: Understand DevSecOps Culture

- DevSecOps Culture
- DevSecOps Culture: People
- DevSecOps Culture: Process
- DevSecOps Culture: Technology
- DevSecOps Culture: Governance
- DevSecOps Best Practices

LO#4: Understand Continuous Security in DevSecOps

- Continuous Security in DevSecOps
- Continuous Testing for CI/CD Pipeline Security
- Continuous Application Security Testing
- DevSecOps: Implementing Security as Code

LO#5: Understand the DevSecOps Pipeline

- Role of DevSecOps in CI/CD Pipeline
- DevSecOps Toolchain
- Embracing the DevSecOps Cycle
- DevSecOps Ecosystem
- Key Elements of the DevSecOps Pipeline
- Integrating Security in the DevOps Pipeline
- Implementing Security into the CI/CD Pipeline
- DevSecOps Security Controls
- AWS DevSecOps CI/CD Pipeline Architecture

- Azure DevSecOps CI/CD Pipeline Architecture
- GCP DevSecOps CI/CD Pipeline Architecture

LO#6: Understand DevSecOps Strategy

- Need for DevSecOps Strategy
- Implementing an Effective DevSecOps Strategy
- Need for a Change Management Strategy
- Change Management Strategies
- DevSecOps Maturity Model (DSOMM)

LO#7: Understand DevSecOps Tools

- DevSecOps Tools for Securing Applications
- Summary of DevSecOps Tools Used in On-Premises Environments
- Summary of DevSecOps Tools Used in AWS Environments
- Summary of DevSecOps Tools Used in Azure Environments
- Summary of DevSecOps Tools Used in GCP Environments

LO#7: Leveraging Artificial Intelligence (AI) in DevSecOps

- DevSecOps and Artificial Intelligence (AI)
- AI Powered DevSecOps: GitLab Duo
- AI Powered DevSecOps: Kubiya.Ai
- Challenges in Integrating AI into DevSecOps Pipeline

Module 03 DevSecOps Pipeline-Plan Stage

- Security Activities in the DevSecOps Plan Stage

LO#1: Understand Continuous Threat Modeling in the DevSecOps Pipeline

- Threat Modeling
- DevSecOps Threat Modeling
- Integrate Threat Modeling into DevSecOps
- Threat Model Input for the Entire CI/CD Pipeline
- Automating Threat Modeling with Infrastructure as Code (IaC)

LO#2: Learn to Integrate Threat Modeling Tools

- Threat Modeling Tool: Threat Dragon
- Threat Modeling Tool: Threatspec

- Threat Model Generation using pytm
- Threat Modeling Tool: Threagile
- Threat Modeling Tool: ThreatPlaybook
- Threat Modeling Tool: Microsoft Threat Modeler
- ThreatModeler Integrations with AWS
- ThreatModeler Integrations with Azure
- ThreatModeler JIRA Plugin
- Challenges and Mitigations for Threat Modeling in DevSecOps
- Threat Modeling Best Practices

LO#3: Learn to Gather Security Requirements from Business Functionality

- Gathering Security Requirements
- Gathering Security Requirements from Threat Modeling
- Track Security Requirements of Business Functions using Jira
- Use Jira and Confluence to Manage Security Requirements
- Integrate Jira with Jenkins
- Integrate Jenkins with Jira and GitHub
- Manage Access and Resource Allocation with AI Features of Kubiya.Ai
- Vulnerability and Risk Control using Jira

LO#4: Address Technical Security Debts

- Technical and Security Debts
- Technical Security Debt
- Address Technical Security Debt
- Security Debt from Previous Sprints

LO#5: Learn to Run Pre-Commit Checks in the Plan Stage

- Execute Git Pre-Commit Hooks in Windows
- Execute Git Pre-Commit Hooks in Linux
- Execute Git Pre-Commit Hooks in MacOS
- Implement the Pre-Commit Framework
- Use the git-multimail Tool to Send an Email Notification for Every Push
- Pre-Commit Hook Tool: Talisman

- Integrating GitHub Webhooks with Jenkins: GitHub Configuration
- Integrating GitHub Webhooks with Jenkins: Jenkins Configuration
- GitHub Webhooks: Triggering a Jenkins Job

LO#6: Understand Secure Code Training and Awareness

- Need for Secure Code Training and Awareness for the DevSecOps Team
- Common Security Challenges while Developing a Security Program
- Checklist for a Secure Code Training Program
- Secure Coding Standards
- Secure Coding Principles

LO#7: Understand Security Tools Training

- Significance of Security Tools Training
- Security Tools Training

Module 04 DevSecOps Pipeline-Code Stage

- DevSecOps Code Stage Security Activities

LO#1: Learn to Integrate Security Plugins in IDEs

- Need for Integrating Security Plugin in IDE
- Security Plugin SonarLint
- Integrate SonarLint in Eclipse IDE
- Integrate SonarLint in VS Code IDE
- Integrate SonarLint in Visual Studio IDE
- Integrate SonarLint in IntelliJ IDEA
- JFrog
- JFrog Eclipse IDE Plugin
- JFrog Visual Studio Extension
- Snyk Security Plugin for Visual Studio Code IDE
- Microsoft Code Analysis for Visual Studio IDE
- Fortify Static Code Analyzer Plugin for Visual Studio IDE
- Microsoft DevSkim for Visual Studio IDE
- Cody AI Coding Assistant for Visual Studio IDE
- Use PyCharm Security Plugin to Secure Python Application Code in PyCharm IDE

- Integration of Security IDE Plugin to Cloud Native IDE
- Checkstyle Plugin in Eclipse IDE
- Use Mend Advice to Scan Application Code in Visual Studio Code IDE
- Integrating Mend Advice IDE Security Plugin in VS Code IDE for Microsoft Azure Cloud Environment
- Integrating AWS Account in Snyk's IDE
- AI Powered Intelligent Code Recommendation using Amazon CodeGuru Security
- Additional Security IDE Plugins

LO#2: Learn to Configure and Manage Code Scanning for GitHub Repository

- Setting up Code Scanning in GitHub
- Use GitHub Actions to Set Up Code Scanning
- Setting Up Code Scanning for Multiple Repositories
- Understanding the Pull Request Checks
- Managing Code Scanning Alerts in Git Repository
- Alert Details
- Viewing the Alerts for a Repository
- Searching Code Scanning Alerts
- Fixing an Alert
- Dismissing Alerts
- AI Powered Tool Kubiya.AI for Secure Coding

LO#3: Learn to Integrate and Scan Source Code Repository

- Integrating Bitbucket Repository with Eclipse IDE
- Secure Bitbucket Server Repository by Integrating with SonarQube
- Integrating GitHub Repository with Visual Studio Code
- Scan GitHub Repository using CodeQL
- Integrate and Scan GitHub Repository using Codacy
- Integrate and Scan GitHub Repository using Snyk
- Integrate Azure Repos with Visual Studio Code IDE
- Integrating and Scanning Azure Repos using Snyk
- Integrating CodeQL Security Check Tool in Azure DevOps

LO#4: Learn to Integrate Secret Management Tools

- Need to Integrate Secret Management Tools in CI/CD Pipeline
- HashiCorp Vault Integration with Jenkins
- Conjur Secret Management Tool Integration with Jenkins
- Secrets Management Tool: Vault
- Secrets Management Tool for AWS: AWS Secrets Manager
- AWS Secret Manager Integration with Jenkins
- Secrets Management Tool for Azure: Microsoft Azure Key Vault
- Azure Key Vault Integration with Jenkins
- Secrets Management Tool for Google: Google Cloud Secret Manager
- GCP Secret Manager Integration with Jenkins

LO#5: Learn to Integrate Software Composition Analysis (SCA) Tools

- Integrating Software Composition Analysis Tool in CI/CD Pipeline
- Challenges for Integrating SCA
- SCA Tool Evaluation
- SCA Tools

LO#5.1: Learn to Integrate SCA Tools with IDE

- Sonatype Nexus IQ Plugin for Eclipse IDE
- SCA Tool: Retire.js
- Perform Vulnerability Scanning with Grunt-Retire

LO#5.2: Learn to Integrate SCA Tools with Source Code Repository

- Mend for GitHub.com Integration with GitHub Repository
- Snyk Integration with Bitbucket Cloud Repository
- Debricked SCA Tool Integration with GitHub Actions
- Mend Bolt SCA Tool Integration with GitHub Actions

LO#5.3: Learn to Integrate SCA Tools with Travis CI, Jenkins, and GitLab

- Integrate Trivy in Travis CI to Detect Security issues
- Integrate Debricked SCA tool with Jenkins to Perform Vulnerability Scan
- Using Checkmarx to Perform SCA Scan on GitLab Project Code

LO#5.4: Learn to Integrate SCA Tools with AWS

- Automate Software Composition Analysis on AWS using Snyk

- Black Duck SCA Tool Integration in AWS Cloud
- Mend SCA Tool Integration with AWS CodeBuild

LO#5.5: Learn to Integrate SCA Tools with Microsoft Azure

- SCA Tool for Microsoft Azure: OWASP Dependency-Check
- Use OWASP Dependency Check to Scan Microsoft Azure Cloud Project
- Automate Software Composition Analysis on Azure using Snyk
- Additional SCA Tools

LO#5.6: Learn to Integrate SCA Tools with GCP

- SCA Tool for GCP: Snyk SCA

Module 05 DevSecOps Pipeline-Build and Test Stage

- DevSecOps Build and Test Automation
- Test-Driven Security
- AI Powered Automated Testing using Tricentis Tosca

LO#1: Learn to Integrate SAST Tool

- SAST Tool in Build Phase
- Synopsys Coverity Plugin Integration with Jenkins
- Fortify Static Code Analyzer Integration with Jenkins
- Bandit SAST Tool Integration with Jenkins
- Brakeman SAST Tool Integration with Jenkins
- SonarQube Integration with Jenkins
- Snyk SAST Tool Integration with Bitbucket
- Kiuwan Plugin for Jenkins
- Veracode Jenkins Plugin Integration with Jenkins
- Selecting Suitable SAST Tool
- Best Practices for Implementing SAST
- Challenges for Integrating SAST

LO#2: Learn to Integrate SAST Tool with AWS Cloud

- Integrate SonarCloud with AWS Codepipeline Utilizing AWS CodeBuild
- SonarQube Integration with AWS Pipeline
- PHPStan SAST Integration with AWS Pipeline

- AI Powered SAST: Amazon CodeGuru Security

LO#3: Learn to Integrate SAST Tool with Microsoft Azure

- GitHub Advanced Security (GHAS) for Azure DevOps
- Veracode Static Analysis Tool in Azure DevOps Pipeline
- Another SAST Tool for Azure: Coverity
- Additional SAST Tools

LO#4: Learn to Integrate SAST Tool with Google Cloud

- SNYK Integration with Google Cloud

LO#5: Conducting Manual Secure Code Review

- What is Manual Code Review?
- Manual Code Reviews
- Example: Detecting SQL Injection Vulnerability through Manual Code Review
- Secure Code Review using AI
- AI-based Secure Code Review Tool: Tabnine

LO#6: Learn to Integrate DAST Tool

- Need for Integrating DAST Tools
- Use DAST Security Solution in Testing Stage
- DAST Tools: w3af
- Perform Full Audit on Web Application using w3af
- DAST Tool: Codename SCNR
- Detect Vulnerabilities in a Website Using Codename SCNR
- Acunetix DAST Tool Integration with Jenkins
- Burp Suite DAST Plugin Integration with Jenkins
- Invicti DAST Plugin Integration with Jenkins
- OWASP ZAP DAST Plugin Integration with Jenkins
- Integrate StackHawk DAST Tool with Jenkins
- Scan Web Application using StackHawk DAST Tool in Jenkins Pipeline
- Integrate InsightAppSec DAST Tool with Jenkins
- Integrate InsightAppSec DAST Tool with JIRA
- Web Application Security Scanning using GitHub Actions and OWASP ZAP

- DAST Tool Evaluation
- Challenges for Integrating DAST
- Best Practices of DAST

LO#7: Learn to Integrate DAST Tool with AWS

- Integrate OWASP Zed Attack Proxy (ZAP) with AWS
- Scan AWS Web Application using OWASP ZAP

LO#8: Learn to Integrate DAST Tool with Microsoft Azure

- Invicti and Azure Pipeline
- Scan Microsoft Azure Web Applications Using Invicti
- Integrate AppCheck with Azure Pipeline
- Integrate and Scan Azure Web Application using Acunetix
- Integrate HawkScan with Azure DevOps Pipeline
- Scan Azure Web Application using HawkScan
- DAST Tool for Microsoft Azure: Tenable.io
- Additional DAST Tools

LO#9: Learn to Integrate DAST Tool with Google Cloud

- DAST Tool for GCP: Intruder
- Integrate Intruder with GCP Pipeline

LO#10: Learn to Integrate IAST Tool

- What is Interactive Application Security Testing (IAST)?
- Active IAST vs. Passive IAST
- Key Use Cases of IAST
- Key Vulnerabilities Detected by IAST Security Solution
- Integrate Invicti Enterprise with GitLab
- Secure Web Applications by Deploying Invicti Shark IAST Functionality in Docker
- Integrating CxFlow IAST Tool with Jenkins
- Integrate Veracode IAST Tool with AWS
- Integrate Seeker IAST Tool with Azure App Service
- Integrate Contrast Assess IAST Tool with Azure Pipeline
- HCL AppScan on Cloud

- IAST Tool Evaluation

LO#11: Understand Security Testing Framework

- Gauntlt Security Testing Framework
- BDD-Security Testing Framework

Module 06 DevSecOps Pipeline-Release and Deploy Stage

- DevSecOps Release Stage Security Activities

LO#1: Learn to Integrate RASP Tool

- Runtime Application Self Protection (RASP)
- RASP Example: Preventing SQL Injection
- RASP Example: Preventing Remote OS Command Injection
- RASP Example: Preventing Cross Site Scripting Injection
- Testing using RASP
- Contrast Security Tool Integration with Gradle
- Jscrambler RASP Tool Integration with GitLab
- Dynatrace RASP Tool Integration with AWS
- Datadog Integration with Slack
- Rapid7 tCell Next-Gen Cloud WAF and RASP Tool Integration with AWS CloudFront
- Trend Micro Cloud One RASP Tool Integration with Microsoft Azure
- Additional RASP Tools
- SAST vs DAST vs IAST vs RASP

LO#2: Learn to Conduct Penetration Testing

- Need for Conducting Penetration Testing in CI/CD Pipeline
- GitGraber Tool: Check Sensitive Data in GitHub
- Integrate GitGraber with Slack
- GitMiner Tool: Check Sensitive Data in GitHub
- Gitleaks Tool: Check Leaked Sensitive Data in a Public GitHub Repository
- Burp Suite Integration with Jenkins to Scan Source Code using Command Line Interface (CLI)
- Burp Suite Integration with Jenkins to Scan Source Code using Graphical User Interface (GUI)

- Burp Scanner Integration with Jenkins
- Exploit Jenkins using Metasploit Framework
- Additional Penetration Testing Tools
- Challenges with Pentesting in DevSecOps

LO#3: Learn to Integrate Vulnerability Scanning Tool

- Vulnerability Scanning in CI/CD Pipeline
- Vulnerability Assessment and Remediation using AI
- Vulnerability Assessment and Remediation using AI Tool: Aqua Security
- Acunetix Vulnerability Scanner Integration with GitHub
- Probely Vulnerability Scanner Integration with Jenkins
- NeuVector Vulnerability Scanner Integration with Jenkins
- Vulnerability Management Tool: BeSECURE
- Vulnerability Management Tool: Cisco Vulnerability Management
- Aqua Security Scanner Integration with Jenkins
- Integrate Trivy for Scanning Docker Images for Vulnerabilities
- Integrate Probely Vulnerability Scanning Tool with Jenkins on AWS EC2 Instance
- Amazon Inspector Vulnerability Scanning Tool to Scan AWS Workloads
- Vulnerability Management Tool for AWS: Vulnerability Manager Plus
- Intruder Vulnerability Scanner Integration with AWS
- Vulnerability Management Tool for Azure: Qualys VMDR
- Qualys Vulnerability Scanner to Scan Microsoft Azure Environment
- Nessus Integration with GCP Environment to scan for Vulnerabilities
- Cloud Security Command Center to Scan GCP Environment
- Additional Vulnerability Scanning Tools
- Vulnerability Scanner Evaluation
- Best Practices for Vulnerability Scanning

LO#4: Understand Bug Bounty Program

- Need for Bug Bounty Program
- AWS BugBust Challenge
- Azure Bug Bounty Program

- Microsoft Azure DevOps Bounty Program
- Google Bug Hunters

LO#5: Learn to Integrate Threat Detection Tools

- Threat Intelligence and DevSecOps
- Use Cases of Threat Intelligence
- Benefits of Threat Intelligence in CI/CD Pipeline
- Prisma Cloud Threat Detection Integration with Jenkins
- Threat Detection using AI and DevSecOps
- AI-Based Threat Detection Tool: IBM Qradar SIEM

LO#6: Understand Infrastructure Deployment using Infrastructure as Code (IaC)

- What is Infrastructure as Code (IaC)?
- Components of IaC
- IaC Approaches
- Manage Infrastructure with IaC
- Infrastructure-as-Code Tools
- AI Powered Infrastructure Automation and Deployment using Kubiya.Ai
- Deploy Application Services on Multiple EC2 Instances using Docker Swarm (BCDR)
- Using Amazon Elastic Container Registry (ECR) to Store, Share, and Deploy Containers
- Best Practices for Infrastructure as a Code (IaC)

LO#7: Learn Infrastructure Provisioning as Code (IaC) using Terraform

- Terraform: Infrastructure Provisioning Tool
- Terraform Architecture
- Terraform Configuration Examples
- Building Infrastructure with Terraform: Example
- Integrate Terraform with Jenkins Pipeline
- Integrate Terraform with GitLab CI/CD
- Automate Terraform with GitHub CI/CD Pipeline using GitHub Actions
- Create Docker Images, Containers, and Docker Services with Terraform
- Integrate Terraform Cloud with Kubernetes
- Provision an EKS Cluster with Terraform

LO#8: Learn Infrastructure Provisioning as Code (IaC) using Pulumi

- GitOps with Pulumi and Gitlab
- Managing Infrastructure through GitOps with GitLab and Anthos

LO#9: Learn to Integrate AWS CloudFormation

- AWS CloudFormation
- AWS CloudFormation Template
- AWS CloudFormation Stack
- Configure Jenkins CI/CD Pipeline and Deploy CloudFormation Template
- AWS CloudFormation Best Practices

LO#10: Learn to Integrate Configuration Orchestration Tools: Ansible

- Ansible
- Integrate Ansible Playbook with Jenkins in a CI/CD Pipeline
- Provision an AWS EC2 Instance using Ansible
- Ansible Deploy for Bamboo Plugin
- Provision Docker Container using Ansible
- IaC Example using Jenkins, Ansible, and CloudFormation

LO#11: Learn to Integrate Configuration Orchestration Tools: Chef

- Chef
- Chef Architecture
- Bootstrap using Chef EC2 Instances on AWS using Jenkins Pipeline
- Integrate Chef Automate with AWS CloudFormation
- Integrate Chef Automate with Azure DevOps
- Integrate Chef Automate Workflow GitHub

LO#12: Learn to Integrate Configuration Orchestration Tools: Puppet

- Puppet
- Puppet Components and Elements
- Puppet Code Management using Git Repository
- Use Puppetlabs-IIS Module for Managing IIS Server
- Using Docker with Puppet

LO#13: Learn to Integrate Configuration Orchestration Tools: Azure Resource Management

- Azure Resources Management Templates
- Integrate ARM Templates with Azure Pipelines
- Enable Azure Release Gates to Control Deployments
- ARM Templates Best Practices

LO#14: Learn to Integrate Binary Authorization to Secure GCP Deployment

- Create a Binary Authorization Attestation in a Cloud Build Pipeline
- Secure GKE Deployments with Binary Authorization
- Configure Binary Authorization on Cirecle CI
- Attest an Image Based on a Black Duck Scan

Module 07 DevSecOps Pipeline-Operate and Monitor Stage

LO#1: Understand Security Activities in the Operate and Monitor Stage

- Operate and Monitor Phase
- Maintain Security into Production Operations

LO#2: Learn to Scan Infrastructure as Code (IaC) for Vulnerabilities

- Security Challenges of IaC
- Snyk: Scan Terraform Configuration Files
- Snyk: Scan CloudFormation Files
- Terrascan: Scan Terraform Configurations
- PrismaCloud: Scan Terraform Files in GitHub
- PrismaCloud: Scan CloudFormation Templates
- PrismaCloud: Scan Infrastructure as Code (IaC) Files in Azure Repo
- Checkov: Scan Kubernetes Manifests Templates in Azure Pipelines
- IaC Security Best Practices
- Additional Infrastructure as Code (IaC) Scanning Tools

LO#3: Learn to Scan Infrastructure for Vulnerabilities

- Fugue: Scan Cloud Infrastructure
- Examine AWS Environment using CloudMapper
- Securing AWS Infrastructure by Integrating Serverspec
- Secure Azure Infrastructure using Chef InSpec

- Scan Azure DevOps with Azure DevOps Security Scanner

LO#4: Learn to Secure Containers

- Hardening Docker Containers
- HashiCorp Packer: Build Customize Docker Image
- Deploying Jenkins on the Azure Kubernetes Service

LO#5: Learn to Integrate Container Vulnerability Scanning Tools

- Need for Integrating Container Image Scanning Tools with the CI/CD Pipeline
- Anchore: Scan Container Vulnerabilities
- Integrate Anchore Container Image Scanner with Jenkins and Scan Docker Images
- Integrate Qualys Container Scanner Plugin with Jenkins
- Qualys: Scan Container Image
- Integrate Chef InSpec with AWS to Secure AWS Cloud Infrastructure

LO#6: Learn to Secure Jenkins

- Jenkins Security Management
- Secure Jenkins Configuration
- Secure Jenkins Controller
- Securing Access to Jenkins
- Jenkins: Matrix-Based Security
- Analyze Installed Plugin Usage
- Configure CSRF Protection in Jenkins
- Configure Security in Jenkins
- Jenkins Best Practices

LO#7: Learn to Integrate Compliance as Code (CaC) Tools

- Need for Integrating Compliance as Code Tools in the CI/CD Pipeline
- Compliance as Code Tool: Docker Bench for Security
- Compliance as Code Tool: DevSec Hardening Framework
- Compliance as Code Tool: Cloud Custodian

LO#8: Learn to Integrate Logging, Monitoring, and Alerting Tools

- Role of Logging in DevSecOps
- Logging Tools

- Continuous Monitoring
- Continuous Monitoring Tools
- Logging and Monitoring Tool: Sumo Logic
- Logging and Monitoring Tool: Nagios Log Server
- Monitoring Tool: Splunk
- Integrate Splunk with GitLab to Monitor Source Code
- Monitoring Tool: ElasticSearch (ELK) Stack
- Monitoring Tool: Datadog
- Monitoring Tool: Extrahop Reveal(X)
- Monitoring Tool: SolarWinds Network Performance Monitor
- Monitoring Tool: Paessler PRTG
- Monitoring Tool: Nagios
- AI Powered Predictive Analysis and Monitoring using Dynatrace
- Alerting Tools
- Alerting Tool: OpsGenie
- Integrating OpsGenie with Splunk
- Notify Merge Issues in GitHub using Jira
- Alerting Tool: Alerta
- Configure Alerta to Monitor Nagios Alerts
- Automate Artifacts Deployment to Nexus Repository Manager from Jenkins
- Additional Monitoring and Alerting Tools

LO#9: Understand Monitoring Features in AWS

- AWS Threat Response
- AWS CloudTrail
- Detect and Respond to Application Attacks using AWS Config
- Monitor Server Node using Grafana and Prometheus on AWS EC2 Instance
- Monitor AWS CodeBuild Application with CloudWatch
- Monitoring S3 Repository with AWS Slack Chat
- Monitoring Amazon S3 using Amazon Macie

LO#10: Understand Monitoring Features in Azure

- Azure Governance Features and Services
- Azure Policy
- Azure Blueprints
- Azure Artifacts
- Monitoring Azure Virtual Machine Logs
- Trigger Build Notifications using Slack in Azure Pipeline

LO#11: Understand Monitoring Features in Google Cloud

- GCP Monitoring Features and Services
- Google Cloud Logging
- Google Cloud Profiler
- Google Cloud Error Reporting
- Google Kubernetes Engine (GKE) Monitoring
- Trigger Alert Notifications with Slack
- Monitor Google Cloud Resources using Nagios Core
- Monitor VM Instances with Google Operations Suite

LO#12: Learn to Integrate WAF

- Need for Integrating WAF in the CI/CD Pipeline
- Deploy Web Knight WAF on IIS Web Server
- Web Application Firewall for AWS: AWS Web Application Firewall
- Use AWS Firewall Manager to Secure Web Applications
- Deploying AWS WAF
- Automate AWS WAF Deployment with AWS CloudFormation Pre-Built Templates
- Creating Custom WAF Rules and Conditions in AWS WAF
- Deploying ModSecurity WAF
- Deploy Cloudflare WAF to Analyze Incoming Traffic and Safeguard Web Applications
- Web Application Firewall for Azure: Azure Web Application Firewall
- Web Application Firewall for GCP: Google Cloud Armor
- Additional Web Application Firewall Tools

LO#13: Learn to Integrate Patch Management

- Implement AWS Systems Manager to Automate Patching of AWS EC2 Instances

- Implement Scheduled Patch Jobs in GCP VM Manager to Automate Instance Patching

LO#14: Learn to Integrate Continuous Feedback

- Continuous Feedback
- Creating a Continuous Feedback Loop
- Configure Email Notifications in Jenkins
- AI Powered Chatbot: Atlassian Intelligence
- AI Powered Chatbot: ClickUp
- Integrate Microsoft Teams with Azure DevOps and GitHub to Provide Feedback
- Microsoft Feedback Hub for Providing Feedback
- Integrate AWS Simple Email Service with Jenkins

LO#15: Understand Incident Reponse in DevSecOps

- Incident Response in DevSecOps
- Incident Response Tool: Incident.io
- Integrating OpsGenie with Incident.io for Incident Response
- Incident Reponse Tool: PagerDuty
- Integrating Pager Duty with Datadog for Incident Response
- Integrating Splunk and PagerDuty for Incident Response
- Incident Response with AI

LO#16: Understand High Availability, Fault Tolerance, and Disaster Recovery in DevSecOps

- High Availability, Fault Tolerance, and Disaster Recovery in DevSecOps
- Automated Jenkins Backup: thinBackup plugin
- Automated Git Repository Backup: Git CLI
- Automated GitLab Instance Backup
- Implementing Scheduled Backups in Azure DevOps
- Configure DNS Failover for High Availability with Amazon Route 53
- Configure Azure Traffic Manager for High Availability in Azure
- Configure External Passthrough Network Load Balancer Failure for High Availability in GCP
- Disaster Recovery Testing in Amazon EKS using LitmusChaos
- Example: Disaster Recovery Testing using LitmusChaos
- Automate Replication of Amazon RDS Instances across Services AWS Accounts

- Automate Azure DevOps Data Replication to Azure SQL with CData Sync
- Implement Automated Rollbacks using Spinnaker
- Implementing Blue-Green Deployment with Argo Rollouts and NGINX
- Implement Canary Deployments with Argo Rollouts and Istio Service Mesh
- Deploy Redundant Jenkins Build Agents on Kubernetes for High Availability