مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

دوره Cloud Security و DevSecOps Automation

مروری بر دوره

این دوره بر اساس آخرین سیلابس شرکت SANS طراحی شده است و شامل مفاهیم و تکنیک های مورد نیاز برای امنیت DevOps و Cloud می باشد در این دوره شما با تمامی تکنیک های مورد نیاز برای بالا بردن امنیت چرخه CI/CD در دواپس آشنا شده و با سناریو های کاربردی یاد خواهید گرفت که چطور در محیط های عملیاتی DevOps را به صورت Secure راه اندازی کنید و از حملاتی که ممکن است به زیرساخت یک شرکت انجام شود جلوگیری کنید و از طرف دیگر شما یاد می گیرید که چطور زیرساخت Cloud را که می تواند Azure شرکت Microsoft و یا AWS شرکت Amazon باشد را Secure کنید شما بعد از گذراندن این دوره به متخصصی تبدیل خواهید شد که بازار وسیعی در دنیا خواهید داشت چرا که متخصصین این دوره انگشت شمار بوده و نیاز مارکت به این متخصصین روز به روز بیشتر می شود.

سرفصل ها

SEC۵۴۰.۱: DevOps Security Automation

DevOps and Security Challenges

Understand the Core Principles and Patterns behind DevOps

Recognize how DevOps works and identify keys to success

DevOps Toolchain

Version control and source code management with git

Using GitFlow to manage changes across environments

(Continuous Integration (CI) versus Continuous Delivery (CD

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Continuous Delivery versus Continuous Deployment

GitHub workflows, actions, and secrets storage

GitLab CI workflows, OpenID Connect identity tokens, and HashiCorp Vault integration

CI/CD supply chain attacks, risks, and hardening guidelines

Securing DevOps Workflows

Threat model and secure your build and deployment environment

DevSecOps phases and security controls

How DevSecOps and artificial intelligence (AI) work together

Pre-Commit Security Controls

Conduct effective risk assessments and threat modeling in a rapidly changing environment

Learn how to analyze a git repository and identity key technology stacks

Configure pre-commit git hooks to run required security checks

Install code editor extensions for security and artificial intelligence (AI)

Enable branch protections to require approvals and change control

Enforce high risk code reviews using CodeOwners

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Commit Security Controls

Design and implement automated security tests and checks in CI/CD

Understand the strengths and weaknesses of different automated testing approaches in Continuous Integration

Centralize automated security checks into a dedicated security scanning factory

How to minimize false positives and create custom rules

Parse automated security using the xUnit, JUnit, SARIF, CycloneDX, and SPDX machine readable formats

Learn the toolchain for scanning application source code, dependencies, configuration management code, and infrastructure as code

Secrets Management

Managing secrets for CI/CD workflows

Scan version control repositories for secrets

Prevent secrets from being committed to version control

Register pre-commit hooks to block commits with secrets

Open-source and commercial secrets management systems

Provision secrets in the Azure Key Vault, AWS Secrets Manager, and HashiCorp

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Vault

Exercises

Attacking the DevOps Toolchain

Version Control Security

Automating Code Analysis

Protecting Secrets with Vault

CloudWars (Section ۱): Cloud & DevOps Security Bonus Challenges

SEC۵۴۰.۲: Cloud Infrastructure Security

Cloud Infrastructure as Code

(Introduction to Cloud Infrastructure as Code (IaC

Terraform, OpenTofu, and the pros and cons of multi-cloud IaC

(Create Terraform resources with HashiCorp Configuration Language (HCL

How to choose a Terraform provider for your cloud

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Create shared Terraform modules for your organization

Automate Terraform deployments in CI/CD

Secure Infrastructure as Code (IaC) configurations with Checkov and EasyInfra

Configuration Management as Code

Introduction to configuration management tools

How Ansible templates can help configure a custom virtual machine

Build custom virtual machine images with Packer

Automate golden image configuration test suites with InSpec

Publish golden images using CI/CD workflows

Container Security Lifecycle

Introduction to the Application Container Security Guide

Dockerfile commands, examples, and misconfigurations

Linting container configuration files with Trivy

Eliminating vulnerabilities with minimal base images, trusted suppliers, and multi-stage builds

Writing custom container configuration policies with Conftest

Scanning container images for vulnerabilities with Trivy

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Software Supply Chain Security

Introduction to the software supply chain

Software provenance attestations with Docker BuildKit

(Supply-Chain Levels for Software Artifacts (SLSA

Managing vulnerable dependencies with trusted suppliers

(Create Software Bill of Materials (SBOMs

Sign build artifacts and Software Bill of Materials (SBOMs) with Project Sigstore

Scan SBOM artifacts for vulnerabilities and track results using Vulnerability (Exploitability eXChange (VEX

Exercises

Infrastructure as Code Network Hardening

Gold Image Creation

Container Image Hardening

Container Software Supply Chain Security

CloudWars (Section ۲): Cloud & DevOps Security Bonus Challenges

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

SEC۵۴۰.۳: Cloud Native Security Operations

Kubernetes Architecture, Resources, and Deployments

Introduction to Kubernetes architecture

Interacting with the Kubernetes API server using kubectl

Learn to create Kubernetes resource using YAML configuration

Build Kubernetes ingress, service, and deployment resources for routing traffic to a microservice

Inventory Kubernetes resources using metadata labels, and annotations

Install Kubernetes packages using Helm

Prepare container registry security for deploying Kubernetes pods

Deploy a container image to Kubernetes using GitLab CI

Kubernetes Risks and Security Controls

Understand container runtime and orchestration platforms

Review container orchestrator security risks

Use Kubernetes control plane authentication to access a cluster

Apply role-based access control (RBAC) permissions to a subject

Isolate resources using namespaces

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Store sensitive data in Kubernetes secrets and encrypt secrets storage using cloud managed encryption services

Kubernetes Workload Security

Kubernetes cloud controller manager capabilities

Review Azure Kubernetes Service (AKS) cloud controller manager permissions

Understand how Azure Kubernetes Service (AKS) pod permissions grant access to Azure APIs

Review AWS Elastic Kubernetes Service (EKS) cloud controller manager permissions

Understand how AWS Elastic Kubernetes Service (EKS) pod permissions grant access to AWS APIs

Enable Kubernetes workload identity using OpenID Connect (OIDC)

Deploy Kubernetes workload identity for pods running in both Azure Kubernetes Service (AKS) and AWS Elastic Kubernetes Service (EKS)

Audit pods for least privilege access in both Azure Kubernetes Service (AKS) and AWS Elastic Kubernetes Service (EKS)

Kubernetes Runtime Security

Introduction to pod and container security context options

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Enable host and process namespacing and workload resource limits

Build network policies with Container Network Interface (CNI)

Introduction to Kubernetes admission controllers

Write validating admission controllers with Common Expression Language (CEL) and Open Policy Agent (OPA), Gatekeeper, and Rego

Learn how eBPF enables runtime protection for Kubernetes hosts and containers

Compare runtime security options include Cilium, Falco, KubeArmor

Continuous Security Monitoring

Monitoring and feedback loops from production to engineering

Understand the difference between logs, metrics, and data tracing

Examine Kubernetes cluster, node, container, and event log sources

Enable Azure Kubernetes Service logging with the OMS Agent

Ingest Kubernetes logs in Azure Log Analytics

Analyze logs with Kusto Query Language (KQL) and trigger alerts using Azure Monitor

Enable AWS Elastic Kubernetes Service (EKS) cluster logs and container insights

خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Stream EKS log data to CloudWatch using Fluent Bit

Query EKS log data with CloudWatch Log Insights

Create CloudWatch Dashboards and trigger alerts using Simple Notification Service (SNS) topics

Automate notifications using web hooks to a Discord channel

Test monitoring, alerts, and notifications using automated ZAP scans

Exercises

Container Registry Security

Kubernetes Workload Identity

Kubernetes Admission Control

Continuous Security Monitoring

CloudWars (Section ۳): Cloud & DevOps Bonus Challenges

SEC۵۴۰.۴: Microservice and Serverless Security

Deployment Orchestration using Cloud Native Services

Introduction to blue/green deployment workflows

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Understand blue/green deployments using Azure Application Gateway

Automate blue/green deployments using Azure Kubernetes ingress controller and service resources

Understand blue/green deployments using AWS Route۵۳ and AWS Application Load Balancer (ALB) weighted target groups

Automate blue/green deployments using AWS Elastic Kubernetes Service (EKS) ingress controller and service resources

Secure Content Delivery

(Introduction to cloud content delivery networks (CDN

Evaluate CDN backend origin access control permissions to a storage account

Protect static content and single page applications hosted in cloud CDN services

Configure Azure CDN token authorization policies

(Create an AWS CloudFront Origin Access Identity (OAID

Enable AWS CloudFront Signing policies

Configure secure CDN Cross-Origin Resource Sharing (CORS) policies

Microservice Security

Compare the attack surfaces for traditional and microservice architectures

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Understand the pros and cons when moving to microservices

Protect the perimeter with an API Gateway

Enable API Gateway authentication and authorization with Open ID Connect (OIDC)

Understand how service providers validate identity tokens from OIDC identity providers

Create an Azure API Management gateway to protect a private microservice

Configure an Azure API Management custom security policy to validate custom OIDC identity tokens

Create an AWS API Gateway to protect a private microservice

Configure an AWS API Gateway custom authorizer to validate custom OIDC identity tokens

Verify JSON Web Token (JWT) configurations and claims meet security recommendations

Protect internal service to service communications with mutual TLS

Apply Kubernetes network policy to

Extend Kubernetes network policy intelligence with Calico

Understand how service mesh offerings can control API traffic at scale

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Serverless Security

Introduction to serverless application architectures

Leverage event driven cloud services to host dynamic applications

Build a serverless single page application (SPA) cloud native CDN, storage, identity provider, API Gateway, function (FaaS), and database services

Review the Azure Function service and security options

Review the AWS Lambda service and security options

Introduction to GraphQL managed services and security concerns

How do serverless systems change the security team's responsibilities

Divide serverless deployment responsibilities between development and operations

Build GitLab CI workflows for deploying serverless function packages

Exercises

Automated Patch Deployment using Blue/Green Services

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Content Protection with AWS CloudFront and Azure CDN

Microservice Security using API Gateways, OpenID Connect, and Network Policy

Serverless Security for Cloud Functions as a Service (FaaS) with GitLab CI

CloudWars (Section ۴): Cloud & DevOps Security Bonus Challenges

SEC۵۴۰.۵: Continuous Compliance and Protection

Continuous Compliance

Introduction to Continuous Compliance and Compliance as Code

Modern governance, risk, and compliance for cloud native applications

Mapping DevOps guardrails to ITIL and PCI controls

Automate compliance and security policy scanning using InSpec, AWS Service Control Policies (SCP), and Azure Policy

Automate cloud native Cloud Security Posture Management (CSPM) policy using Microsoft Defender for Cloud, AWS Security Hub, and Prowler

Runtime Security Protection

Automating compliance with cloud native web application firewall (WAF) services

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Protect Kubernetes workloads using the Azure and AWS WAF services

Write WAF as Code custom rules for Azure and AWS WAF services

Learn how the AWS WAF Security Automations Project uses event triggers and serverless to build custom WAF protection

Compare compliance with WAF to RASP and IAST solutions

Automated Remediation

Introduction to automated detection and remediation in the cloud

Learn how Azure Event Grid and AWS EventBridge route events to runbooks for remediation and notifications

Explore CSPM automation capabilities in Microsoft Defender for Cloud and AWS Security Hub

Learn how AWS Security Hub Automated Response & Remediation (SARR) uses playbook automation to close findings

Write policy as code with Cloud Custodian to manage cloud resources

Deploy Cloud Custodian policies to remediate Azure Network Security Group and AWS Security Group firewall rule misconfigurations

Exercises

مؤسسه آموزش عالی آزاد
خیابان ولیعصر، نبش فاطمی، کوچه بوعلی سینا شرقی، پلاک ۱۷
تلفن: ۵۰ – ۸۸۹۹۵۳۴۸ | ۸۸۹۵۷۰۷۵ | فاکس: ۸۸۹۶۹۱۴۲

Cloud Security Posture Management (CSPM) with Prowler and Microsoft Defender for Cloud

Blocking Attacks with Azure and AWS WAF

Automated Remediation with Cloud Custodian

CloudWars (Section ۵): Cloud & DevOps Security Bonus Challenges

مخاطبان دوره

-کارشناسان Cloud

-کارشناسان DevOps

-کارشناسان امنیت

پیش نیاز ها

دوره جامع DevOps