skillsoft global knowledge™

Cybersecurity Specialization: DevSecOps

Duration: 3 Days **Course Code: GK840102**

Overview:

Learn how to integrate security within DevOps
DevSecOps is designed to empower you with the knowledge and skills necessary to seamlessly integrate security into your DevOps pipeline. You will gain a deep understanding of DevSecOps principles and practices, ensuring that security is an integral part of your software development lifecycle (SDLC). By mastering continuous security testing methods and tools, you will be equipped to identify and address vulnerabilities early, enhancing the overall security posture of your applications.
Learn the knowledge and tools to ensure continuous security and compliance, safeguarding your software solutions from potential threats.
Our Cybersecurity Specialization courses follow the 9 pillars of Cybersecurity, providing key skills necessary to be successful as a cybersecurity professional.

Objectives:

- Understand DevSecOps principles and practices to integrate security within the DevOps pipeline
- Master secure software development lifecycle (SDLC) techniques
- Get familiar with continuous security testing methods and tools to identify vulnerabilities early
- Enhance secure coding practices by understanding common vulnerabilities and how to mitigate them.
- Advanced threat modeling and risk assessment strategies
- Implement best practices for container security using container orchestration tools.
- Leverage Infrastructure as Code (IaC) security to secure infrastructure from the ground up
- Master identity and access management (IAM) principles to manage user identities and permissions securely
- Get hands-on experience with application security testing (AST) tools to uncover and remediate security flaws.
- Utilize security information and event management (SIEM) tools for real-time analysis of security alerts
- Develop strategies for effective incident response and digital forensics
- Understand compliance and regulatory requirements
- Enhancements to secure DevOps toolchains
- Integrate cloud-specific security services provided by major cloud providers to protect cloud-based applications and infrastructure.
- Interact with network security tools to safeguard network communications.
- Design professional scripts to automate security tasks and improve efficiency
- Query databases securely, ensuring data integrity and protection against database-related vulnerabilities.
- Process and protect sensitive data using security measures to ensure compliance with data protection laws and best practices.

Prerequisites:

- Foundational Knowledge of DevOps: Participants should have a basic understanding of DevOps principles and practices.
- Basic Security Concepts: Familiarity with fundamental cybersecurity concepts is required.
- Experience with CI/CD Pipelines: Prior experience setting up and using Continuous Integration/Continuous Deployment (CI/CD) pipelines.
- Scripting Knowledge: Experience writing scripts in languages such as Python, Bash, or PowerShell.
- Operating System Proficiency: A working, user-level knowledge of Unix/Linux, Mac, or Windows.
- 9701 - Cybersecurity Foundations

Content:

Overview of DevSecOps

- DevSecOps principles
- The DevOps lifecycle and security integration
- Key challenges in implementing DevSecOps

Security by Design

- Secure software development lifecycle (SSDLC)
- Threat modeling and risk assessment
- Best practices for secure coding
- Resources: OWASP Top Ten, NIST Cybersecurity Framework

Infrastructure as Code (IaC) Security

- Introduction to IaC and its benefits
- Security considerations for IaC
- Tools to Address : Terraform, Azure Resource Manager (ARM)
- Resources To be used: Terraform: HashiCorp Terraform, Azure ARM: Azure Documentation

Continuous Integration and Continuous Security

Secure CI/CD pipeline design,

- Implementing Zero Trust in CI/CD Pipelines
- Incident Response and Recovery in CI/CD Pipelines"

Integrating security tools into CI/CD pipelines

- Implementing Security Gates in CI/CD Pipelines"
- Tools to Cover: Jenkins, GitHub Actions, Azure DevOps
- Resources to use: Jenkins: Jenkins Documentation, GitHub Actions: GitHub Actions

Application Security Testing

- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)
- Tools: SonarQube, OWASP ZAP, Other SAST Tools (Checkmarx, Veracode), Other DAST Tools (Burp Suite, Acunetix)
- Resources: SonarQube: SonarQube Documentation, OWASP ZAP: OWASP ZAP Documentation

Container Security

- Securing Docker images and containers
- Best practices for container security
- Tools: Docker, Aqua Security. Kubernetes Security
- Resources: Docker: Docker Documentation, Trivy: Aqua Trivy Documentation

Monitoring and Logging

- Importance of monitoring and logging in security
- Tools for monitoring and logging: ELK Stack, Prometheus, Grafana, SIEM (Security Information and Event Management), Grafana for Visualizing Security Metrics
- Resources: ELK Stack: Elastic Documentation, Prometheus: Prometheus

Incident Response and Forensics

- Incident response planning and execution
- Forensic analysis and post-incident review
- Tools: Splunk, Wireshark, SOAR (Security Orchestration, Automation, and Response), Volatility
- Resources: Splunk: Splunk Documentation, Wireshark: Wireshark Documentation

Compliance and Governance

- Understanding security compliance requirements
- Implementing security policies and governance
- Standards: GDPR, HIPAA, PCI-DSS, CCPA (California Consumer Privacy Act)
- Resources: GDPR: EU GDPR Information, HIPAA: HIPAA Journal, PCI-DSS: PCI Security Standards Council

Data Security and Privacy

- Protecting sensitive data
- Encryption techniques and key management
- Tools: Vault by HashiCorp, Azure Key Vault, Google Cloud Key Management Service (KMS), AWS Key Management Service (KMS),
- Resources: Vault: HashiCorp Vault Documentation, Azure Key Vault: Azure

Capstone Project

Further Information:

For More information, or to book your course, please call us on 0800/84.009

info@globalknowledge.be

www.globalknowledge.com/en-be/