email : techcenter@trainocate.com.my
contact : +603-2281-1111

DevSecOps Foundation

Course Code: DSOF
Duration: 2 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Topics covered in the course include how DevSecOps provides the business value of DevOps and the ability DevOps has to enable the business and support an organizational transformation with the ultimate goal of increasing productivity, reducing risk, and optimizing cost in the organization.

This course explains how DevOps security practices differ from other security approaches and provides the education needed to understand and apply data and security sciences. Participants learn the purpose, benefits, concepts, and vocabulary of DevSecOps; particularly how DevSecOps roles fit with a DevOps culture and organization. At the end of this course, participants will understand using "security as code" with the intent of making security and compliance consumable as a service.

The course is designed to teach practical steps on how to integrate security programs into DevOps practices and highlights how professionals can use data and security science as the primary means of protecting the organization and customer.

SKILLS COVERED

On completion of this course, the following learning outcomes will be achieved:

- The purpose, benefits, concepts, and vocabulary of DevSecOps
- How DevOps security practices differ from other security approaches
- Business-driven security strategies
- Understanding and applying data and security sciences
- The use and benefits of Red and Blue Teams
- Integrating security into Continuous Delivery workflows
- How DevSecOps roles fit with a DevOps culture and organization.

WHO SHOULD ATTEND?

- Anyone involved or interested in learning about DevSecOps strategies and automation
- Anyone involved in Continuous Delivery toolchain architectures
- Compliance Team
- Delivery Staff
- DevOps Engineers
- IT Managers
- IT Security Professionals, Practitioners, and Managers
- Maintenance and support staff
- Managed Service Providers Project & Product Managers
- Quality Assurance Teams
- Release Managers
- Scrum Masters
- Site Reliability Engineers
- Software Engineers
- Testers

PRE-REQUISITES

Participants should have baseline knowledge and understanding of common DevOps definitions and principles

MODULES

Module 1: Realizing DevSecOps Outcomes

- Origins of DevOps?
- Evolution of DevSecOps?
- CALMS?
- The Three Ways

Defining the Cyberthreat Landscape?

- What is the Cyber Threat Landscape?
- What is the threat?
- What do we protect from?
- What do we protect, and why?
- How do I talk to security?

Building a Responsive DevSecOps Model

- Demonstrate Model
- Technical, business and human outcomes?
- What's being measured? ?
- Gating and thresholding?

Module 4: Integrating DevSecOps Stakeholder

- The DevSecOps State of Mind?
- The DevSecOps Stakeholders?
- What's at stake for who??
- Participating in the DevSecOps model?

Module 5: Establishing DevSecOps Best Practices

- Start where you are?
- Integrating people, process and technology and governance?
- DevSecOps operating model?
- Communication practices and boundaries?
- Focusing on outcomes ?

Module 6: Best Practices to get Started

- The Three Ways?
- Identifying target state?s
- Value stream-centric thinking?

Module 7: DevOps Pipelines and Continuous Compliance

- The goal of a DevOps pipeline?
- Why continuous compliance is important?
- Archetypes and reference architectures?
- Coordinating DevOps Pipeline construction?
- DevSecOps tool categories, types and examples?

Module 8: Learning Using Outcomes

- Security Training Options?
- Training as Policy?
- Experiential Learning?
- Cross-Skilling?
- The DevSecOps Collective Body of Knowledge?

END OF PAGE