TER201 - DEFENDING TERRAFORM

Course Learning Objectives

This course is part of the line of defending against threats to Infrastructure as Code (IaC). Defending Terraform builds on the foundations of cloud security.

In four modules, we'll explore modern practices for provisioning infrastructure, how Terraform implements IaC, moving system state information to a remote backend, using a secret manager to manage configuration file secrets, using short-term credentials, limiting access to your cloud provider, using Terraform Teams for role-based security, validating configuration files with a linter, writing and testing Sentinel policies, and how you can use Terraform to shift security left.

Description

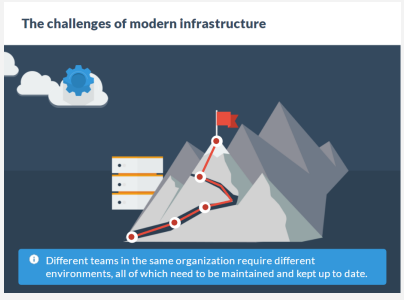
Defending Terraform is for DevOps and DevSecOps professionals who have some familiarity with cloud security fundamentals. This course focuses on best practices for using Terraform to securely configure and deploy cloud infrastructure.

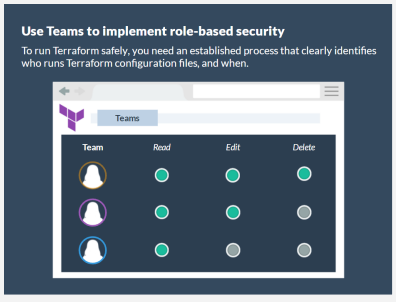
Audience

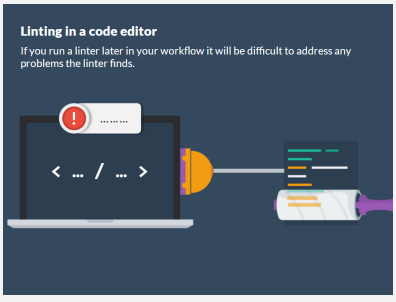
DevOps Engineers
DevOps Managers

Time Required

Tailored learning - 60 minutes total







TER201 - DEFENDING TERRAFORM

Course Outline

1. Introducing Terraform

- The challenges of modern infrstructure
- Use official Terraform providers
- The Terraform Registry
- Understand how Terraform implements IaC
- Don't hard-code authentication credentials
- The key advantages of Terraform configuration
- Understand the Write-Plan-Apply workflow
- Use Terraform to shift security left

2. Protecting Secrets and State

- Terraform state and its protection techniques
- The backend block
- Store secrets with a secret manager
- AWS Secrets Manager
- The benefits of a secrets manager
- Short-lived credentials generation
- Mark sensitive variables for log redaction
- The limits of sensitive variables

3. Strengthening Terraform Security Practices

- Restrict direct access to your cloud provider
- A safe Terraform workflow
- Use Teams to implement role-based security
- Terraform workspaces
- Creating a team
- Best practices for Teams
- Monitor the audit logs for problems
- Retrieving audit logs for analysis
- Audit log information
- Catch common security mistakes with a linter
- Terraform linters
- Using Checkov
- Linting in a code editor

3. Enforcing Policy with Sentinel

- How policies improve your security posture
- The Sentinel workflow
- Write Sentinel policies to limit security risks
- Choosing a Sentinel import
- A sample Sentinel policy
- Use the Sentinel CLI to test policies
- Creating test cases
- Apply Sentinel policies in your Terraform workflow
- Creating a policy set
- Assigning a policy set
- Implement CIS Benchmarks with the Terraform Foundational Policy Library

SecurityCompass