AZR101 - DEFENDING AZURE

Course Learning Objectives

This course is part of the line of defending against threats to cloud. Defending Azure builds on the foundations of cloud security but in the context of Azure.

In seven modules, we'll explore identity management in Azure Active Directory, monitoring logs and potential threats in Azure Security Center, configuring network traffic in Azure Layered Security Architecture, protecting against common exploits with the Web Application Firewall, identifying vulnerabilities with Azure Web Application Vulnerability Scanning, detecting malware, and centralizing storage with Azure Key Vault.

Description

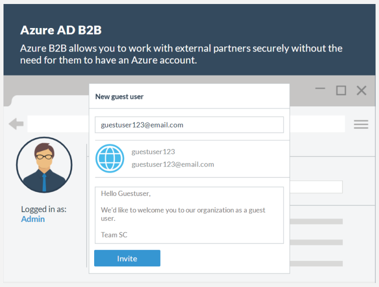
Defending Azure was created for DevOps and Ops Engineers who have experience using Microsoft Azure and familiarity with application security. This course focuses on configuring Azure to defend against the most common security threats.

Audience

DevOps/Ops Engineers

Time Required

Tailored learning - 60 minutes total



Azure AD B2B

Azure B2B allows you to work with external partners securely without the need for them to have an Azure account.

New guest user

guestuser123@email.com

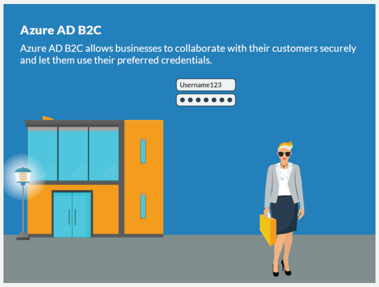
guestuser123
guestuser123@email.com

Hello Guestuser,

We'd like to welcome you to our organization as a guest user.

Team SC

Logged in as:
Admin



Azure AD B2C

Azure AD B2C allows businesses to collaborate with their customers securely and let them use their preferred credentials.

WAF monitoring

After configuring your WAF, it's important to monitor its health and operational states.

SecurityCompass

AZR101 - DEFENDING AZURE

Course Outline

1. Azure Active Directory

- Active Directory overview
- External identities in AD
- Azure AD B2B
- Azure AD B2C
- Conditional Access policies
- Building conditional access
- Role-based Access Control

2. Azure Security Center

- Azure Security Center overview
- Security baselines
- Secure score
- Security policies and compliance
- Azure Defender
- Azure Defender features
- Enabling Azure Defender
- Automated Asset Discovery solution
- Asset Metadata

3. Layered Security Architecture

- Segmentation patterns definition
- Segmentation patterns components
- Single virtual network segmentation pattern
- Multiple virtual networks
- The hub and spoke model
- Network Security Groups

4. Web Application Firewall

- Front Door
- WAF on Front Door
- Custom WAF rules
- WAF on Azure CDN
- WAF on Azure Application Gateway
- WAF monitoring

5. Web Application Vulnerability Scanning

- Vulnerability scanning overview
- Scanner deployment
- At-scale scanner automation
- View and remediate findings
- Disable findings

6. Antimalware Configuration

- Overview
- Antimalware architecture
- Deployment Workflow
- VM deployment: security extension
- VM deployment: server explorer
- Antimalware configuration

7. Azure Key Vault

- Intro to Azure Key Vault
- Secret storage
- Authenticate apps and users
- Configure Key Vault Firewall
- Azure Key Vault soft-delete

SecurityCompass