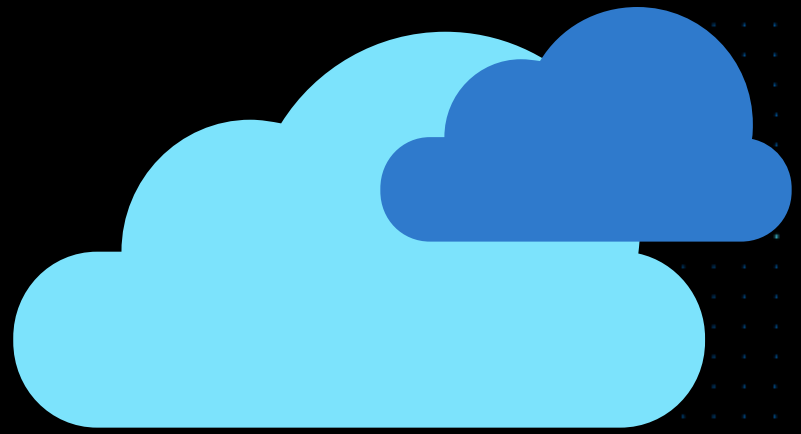
Microsoft Azure

Secure DevOps：應用安全原則與實踐

簡介



課程概述

- Module 1：Secure DevOps 的演進
- Module 2：Secure DevOps 原則與實踐
- Module 3：應用安全原則
- Module 4：自動化安全且合規的流水線
- Module 5：威脅建模
- Module 6：手動安全驗證

Microsoft Azure

Workshop context

Microsoft Azure 優秀架構框架

架構提供指導和最佳實踐，專為架構師、開發人員和解決方案負責人創建，旨在基於五個相互關聯的支柱提升其工作的品質

成本優化

運營卓越

性能效率

可靠性

安全性

https://aka.ms/wellarchitected/framework

雲端採用框架（CAF）

Plan and Develop

- ☐ Threat modelling
- ☐ IDE Security plugins
- ☐ Pre-commit hooks
- ☐ Secure coding standards
- ☐ Peer review

Commit the code

- ☐ Static application security testing
- ☐ Security unit and functional tests
- ☐ Dependency management
- ☐ Secure pipelines

Build and test

- ☐ Dynamic application security testing
- ☐ Cloud configuration validation
- ☐ Infrastructure scanning
- ☐ Security acceptance testing

Go to production

- ☐ Security smoke tests
- ☐ Configuration checks
- ☐ Live Site Penetration testing

Operate

- ☐ Continuous monitoring
- ☐ Threat intelligence
- ☐ Penetration testing
- ☐ Blameless postmortems

DevSecOps 控制 - 雲端採用框架 |Microsoft Learn

定義

軟體漏洞：軟體代碼中發現的安全漏洞、故障或弱點，可能被攻擊者利用（威脅來源）

攻擊面：應用程式中任何可被人類或其他程序訪問的部分

攻擊面減少：盡量減少惡意使用者可能發現並試圖利用的暴露攻擊面數量

隱私：賦予使用者控制其個人資訊收集、使用和分發的能力

安全：建立防禦敵對行為的保護措施

零日漏洞：惡意行為者在專家發現之前就已經知道並利用了該漏洞

信任邊界：

信任邊界違規：

軟體供應鏈：任何第三方或開源軟體的依賴關係和集成

指揮與控制：攻擊者在目標網路中控制已被入侵的資產並與之建立連接的過程

CVE：一個公開披露資訊安全問題的資料庫。 由 MITRE 組織啟動

CWE：社區開發的軟體和硬體漏洞類型清單

剩餘風險：在通過風險控制減少了自然或固有風險之後，某個行動或事件所剩餘的風險或危險程度

工具

Whitesource/Mend

SonarQube

Azure Tenant Security Solution (AzTS)

CodeQL

Microsoft DevSkim

BinSkim

Attack Surface Analyzer

GitHub Dependabot

GitHub Advisory Database

GitHub Dependency Graph

GitHub Code scanning

GitHub Secret scanning

PREfast

FXcop

MiniFuzz

攻擊與漏洞示例

Love Bug：2000

Nimda：2001年

CodeRed：2001

Log4j：2021

SolarWinds：2020

Equifax： 2017，資料庫泄露個人資訊（PII）。 利用了 Apache Struts 中的漏洞

Heartbleed：OpenSSL

Struts：

WannaCry： 2017，勒索軟體，影響了150個國家的30萬台計算機