Microsoft Azure

Secure DevOps：應用安全原則與實踐

Secure DevOps 原則與實踐

模組概述

- Secure DevOps 原則
- 軟體組成分析
- 運營安全保障
- 實踐與標準的一致性

Microsoft Azure

Secure DevOps 原則與實踐

假設並防止洩露

防止洩露

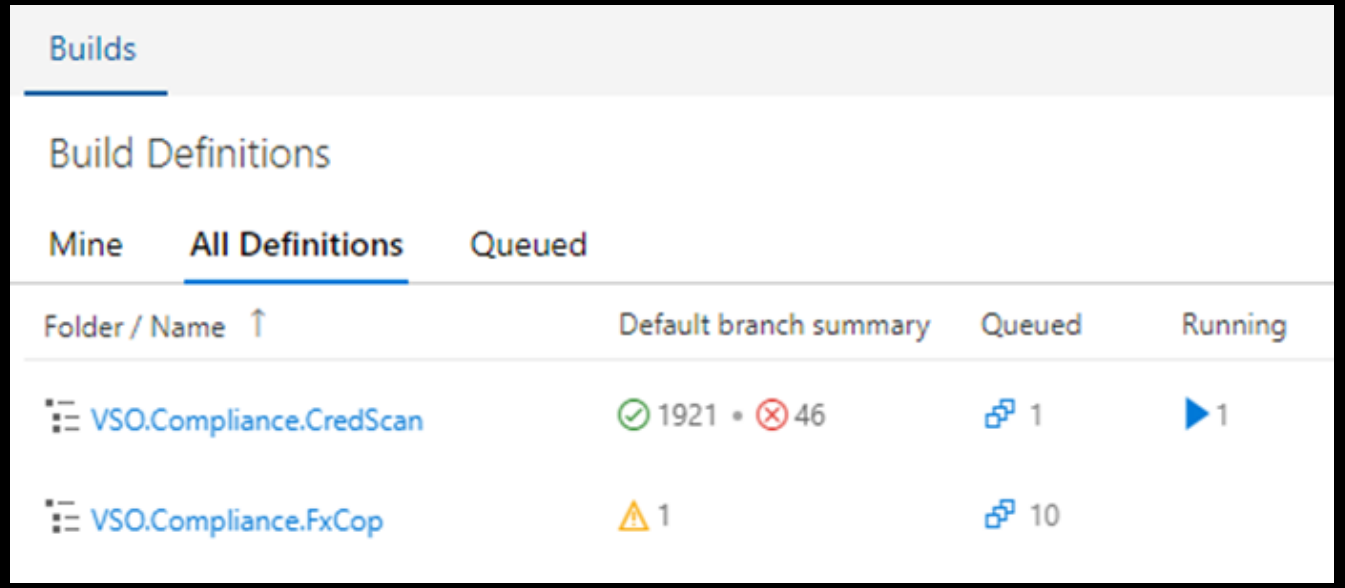
- 威脅模型
- 代碼審查
- 憑證保護
- 靜態應用安全測試（SAST）
- 動態應用程式安全測試（DAST）

假設洩露

- 紅隊和藍隊
- 對抗演習
- 中央安全監控
- 網站滲透測試

左移並實現自動化

- 利用工具分析基礎設施設定錯誤（GitHub 進階安全）
- 定期更新基礎設施
- PaaS 和從 IaC（基礎設施即代碼）進行常規部署，會刷新基礎設施並清除隱藏的角落
- 預設在「傳輸」和「靜止」時加密
- 利用管道安全工具

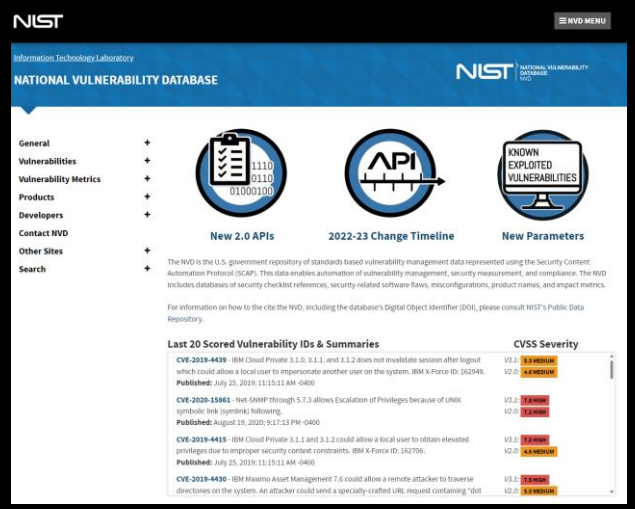


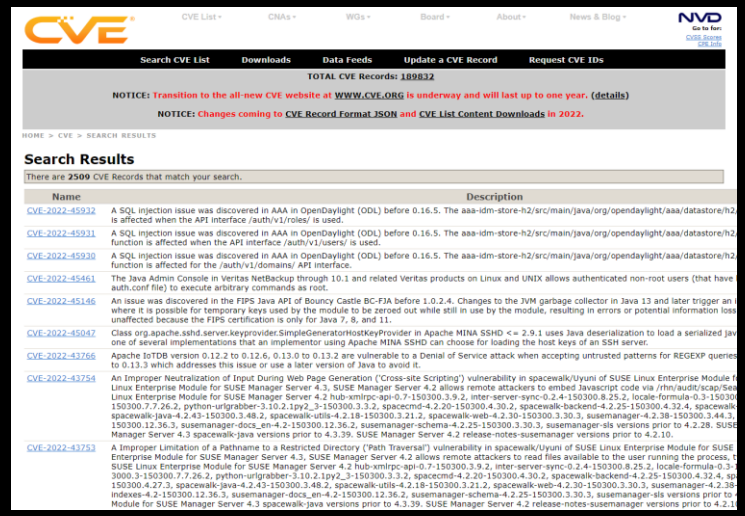
選擇高可信的工具

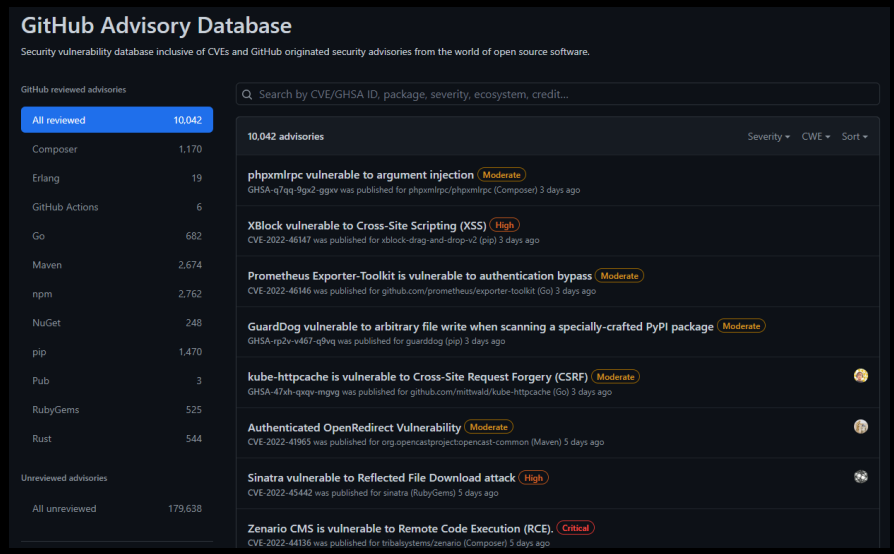
- 集成到管道中的工具不要求安全專業知識
- 結果必須準確且重要
- 團隊必須對工具和流程報告的結果有信心

保持最新動態

- 保持最新的補丁更新
- 更新你的框架
- 保持关注国家漏洞数据库（National Vulnerability Database）
- 及時瞭解監管和合規變化
- 減少技術債務

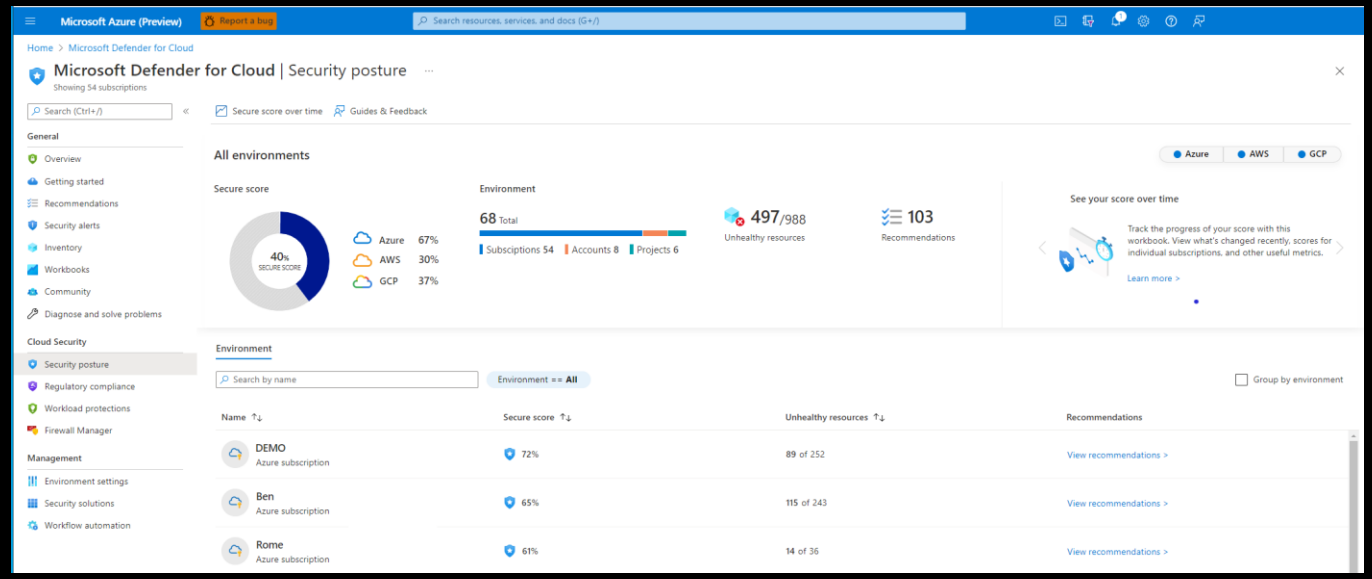






持續監控與學習

- 持續且不懈地提升可用性
- 監控流水線和部署
- 構建和部署輸出結果的匯總
- 監控環境以確保安全性和穩定性



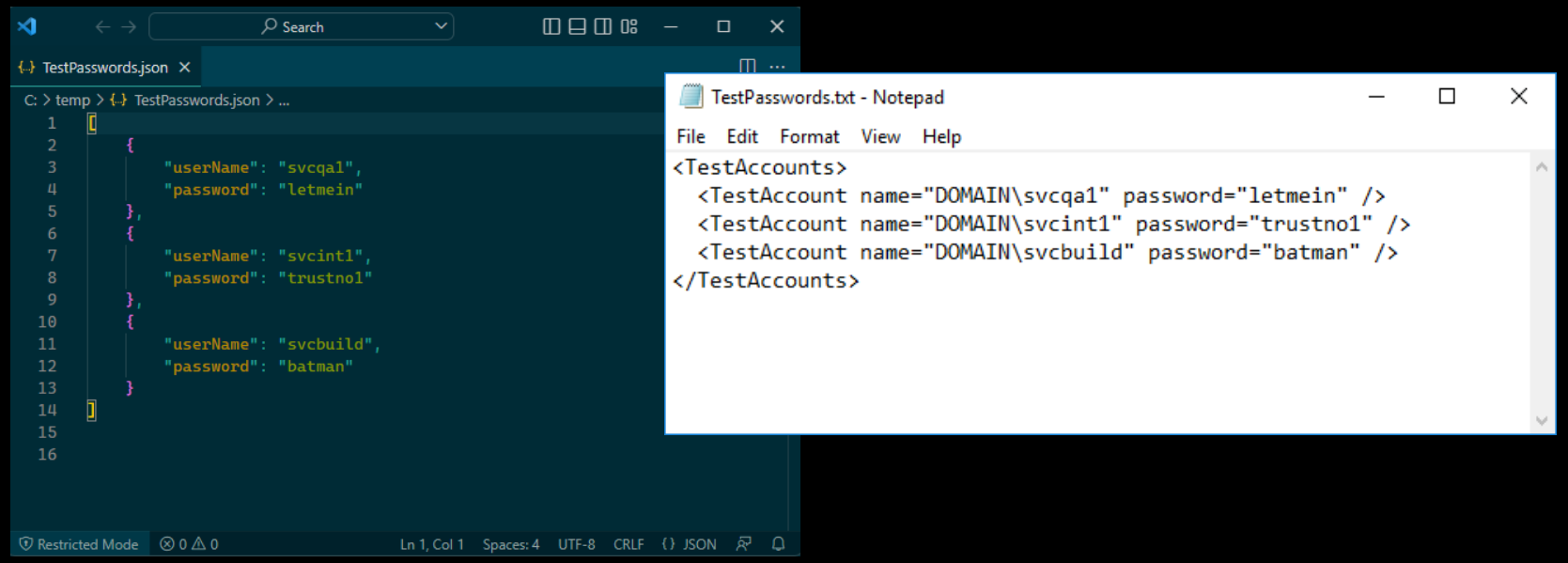
Secure DevOps 文化

- 對所有主要功能進行安全審查（但不是所有功能）
- 資訊安全應整合進軟體交付流程
- 賦予開發者在日常工作中構建安全的能力
- 安全是每個人的責任，把安全、開發和運營整合在一起

Microsoft Azure

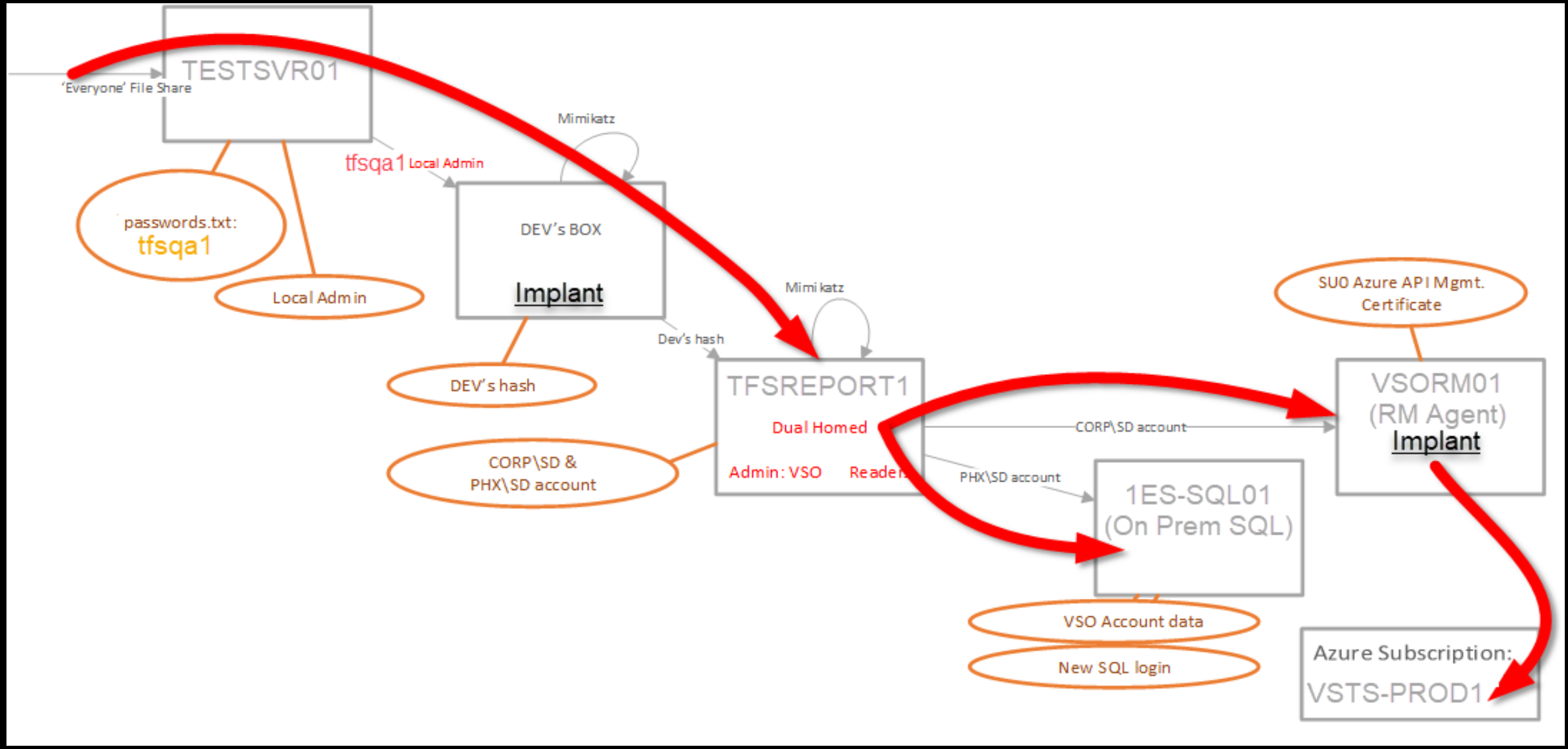
管理機密

檔中的明文憑證

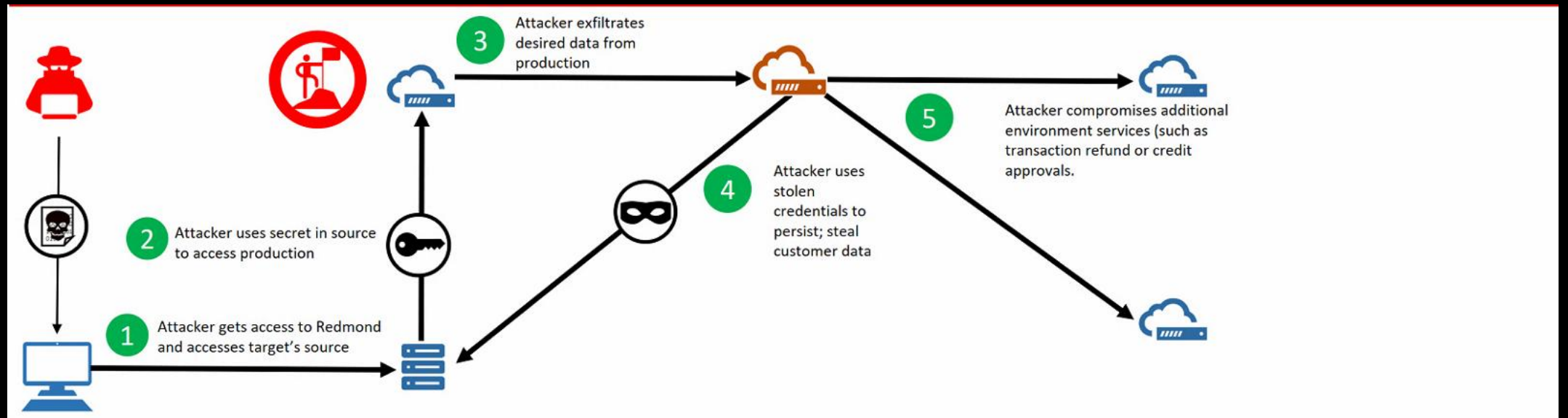


每個隊伍似乎在一開始都會經歷這種情況

示例：紅隊攻擊並伴隨橫向移動



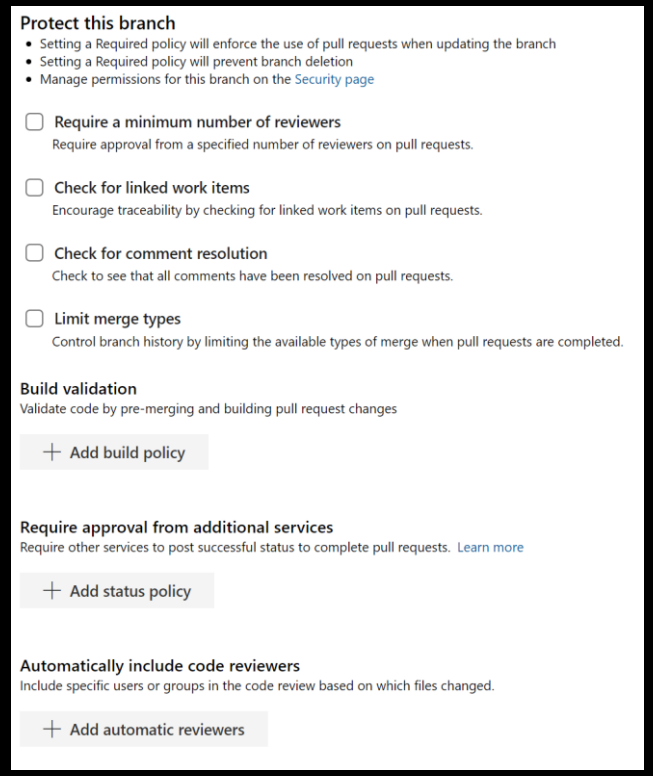
橫向移動攻擊

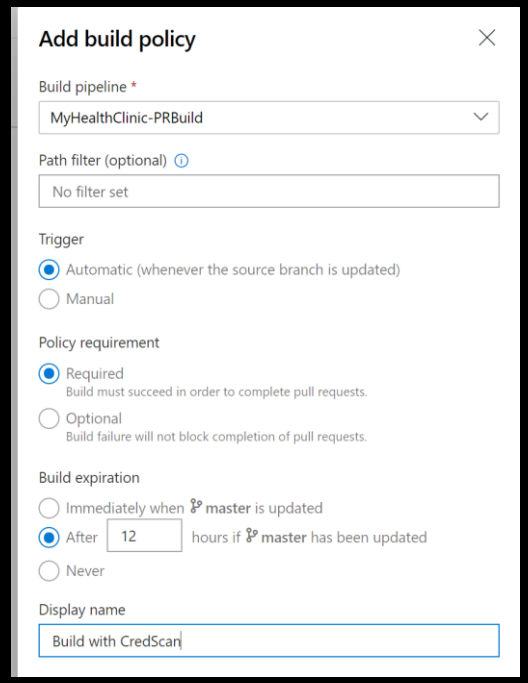


Event	Detection	Response	Impact & Lessons Learned
• Target's source code was pulled as part of standard recon activities and analyzed • Production Keyvault information was discovered inside source repository • Production Keyvault was accessed; all targets employees' usernames and password hashes were discovered and cracked out • Customer information was accessed, and read-write access was validated • Certificates for managing targets Azure subscriptions and targets Fabric were discovered and validated	• No actions were detected while on this engagement • Incident Response is engaged for cleanup of employee credentials and customer data	• Due to no detections; no response actions have been taken	• Implementation of automated credential scanning for places where high value data is a must • Environment separation between pre-production and production also is a must • A second look at target environment might be warranted at some time in the future (this was not planned or part of the roadmap)

自動化憑證掃描

合併代碼前進行憑證掃描





[原始碼分析工具 | OWASP基金會]

[關於GitHub高級安全 - GitHub文檔]

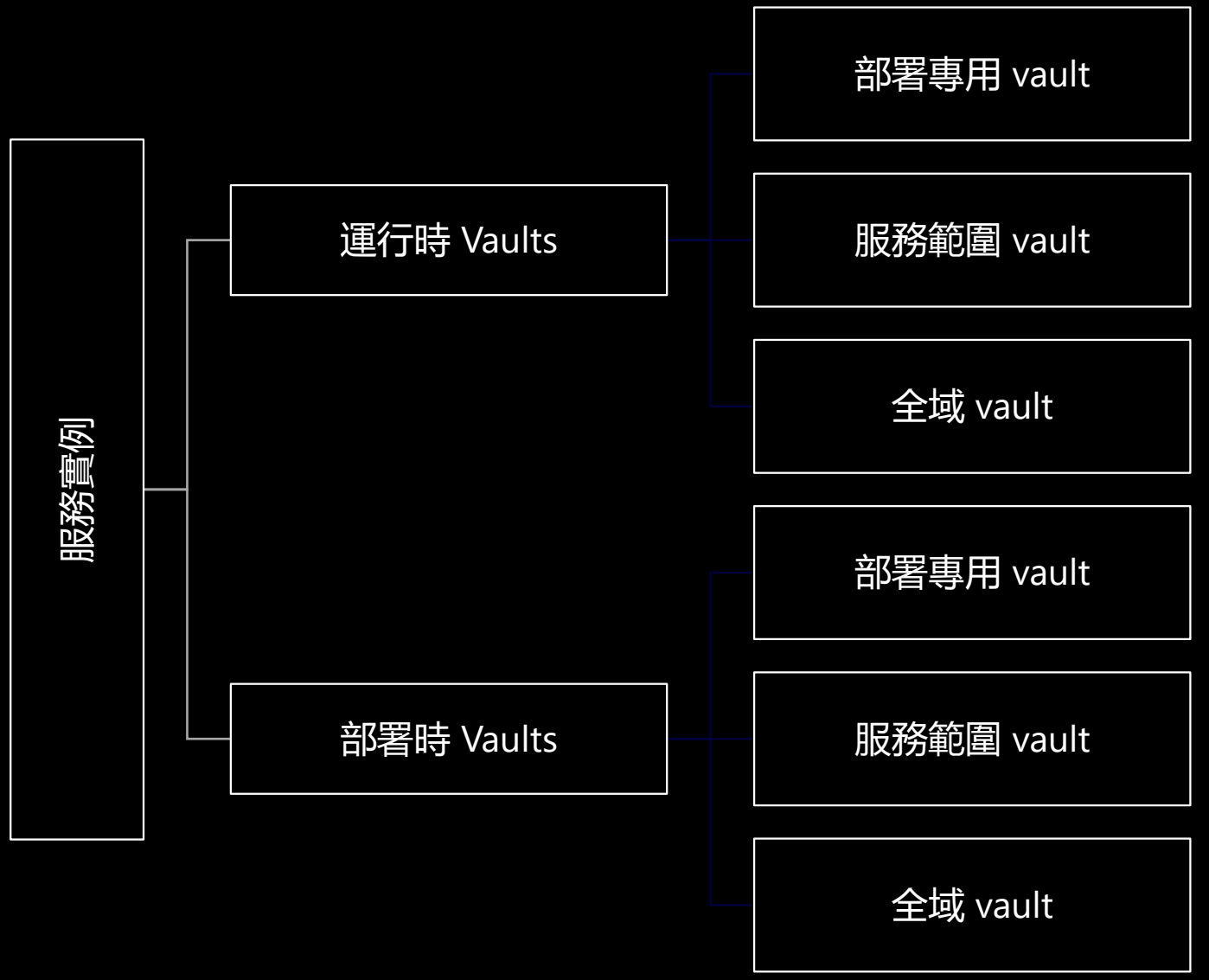
Azure Key Vault （AKV）

所有機密必須儲存在 AKV 中：

- 密碼、金鑰、令牌
- 存儲帳戶金鑰
- 證書
- 測試中使用的憑證

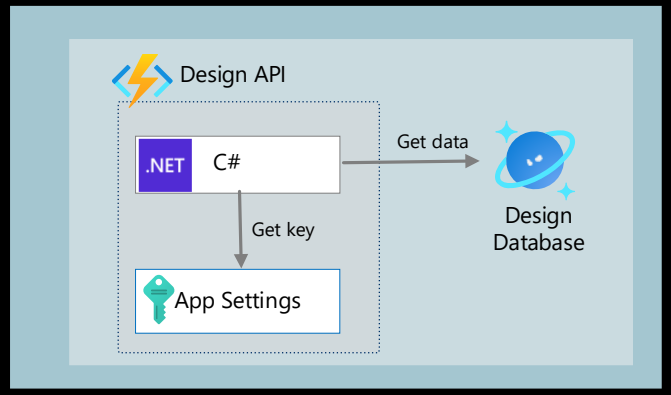
Vault 的分層結構，用於消除金鑰的重複

運行時 Vault，使金鑰更改能夠即時傳播

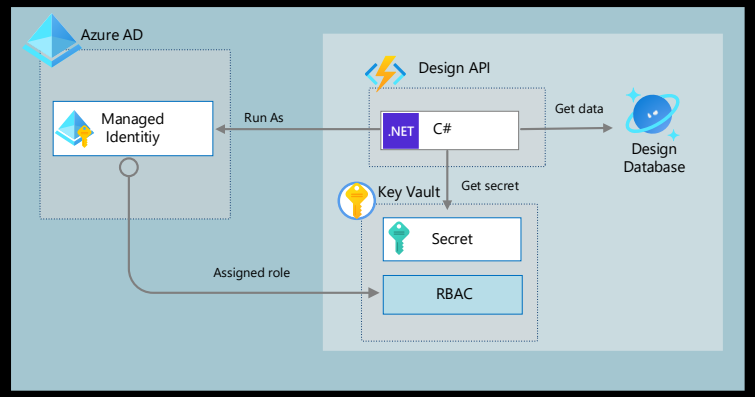


真的需要機密嗎?

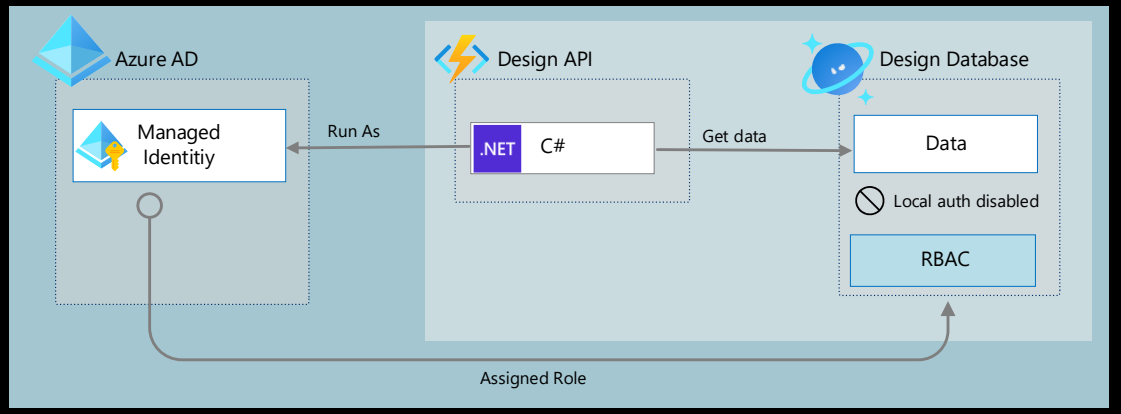
Option 1 – 應用設置中的機密



Option 2 – secret in Azure Key Vault



選項3 – No secret - Managed identitiess and Azure AD RBAC



Microsoft Azure

運營安全保障

解決方案運作中的常見問題

機密管理

連接字串、密碼和私鑰
它們存放在哪裡？
誰可以訪問這些資訊？
它們什麼時候更換/輪換，怎麼更換？

身份管理

用戶認證
使用者是如何獲得授權的
用戶和服務分配的許可權
機密訪問

數據保護

靜止數據
- 授權
- 透明加密與用戶端加密
- 金鑰管理

數據的使用方式
- 記憶體隔離
- 輸入驗證

傳輸中的數據
- HTTPS 品質
- 認證與授權

GDPR 刪除權

- 歐盟居民可以申請從資料庫中刪除個人數據
- 必須是永久且不可逆的
- 在應用設計階段採用匿名化技術以降低成本
- 提供與 FPE 一致的數據掩碼效果，但不可逆

Art. 17 GDPR

Right to erasure ('right to be forgotten')

(1) The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

隱私與安全

隱私

- 賦予使用者控制其個人資訊的收集、使用和分發的能力
- 隱私需要安全

安全

- 建立防護措施以防範攻擊行為
- 安全並不確保隱私

隱私和安全是構建可信應用的關鍵因素

Microsoft Azure

實踐與標準的一致性

OWASP 前十名

OWASP 2021 年度基線安全標準 Top 10

- OWASP Top 10 是達到安全基線的一種有效方法
- 客戶要求遵循十大最佳實踐並不罕見

這是一個低但實用的門檻

不僅僅是針對網頁應用

- API OWASP API Security Project |OWASP 基金會
- DevOps OWASP 十大 CI/CD 安全風險 |OWASP基金會

OWASP Top 10 的替代方案

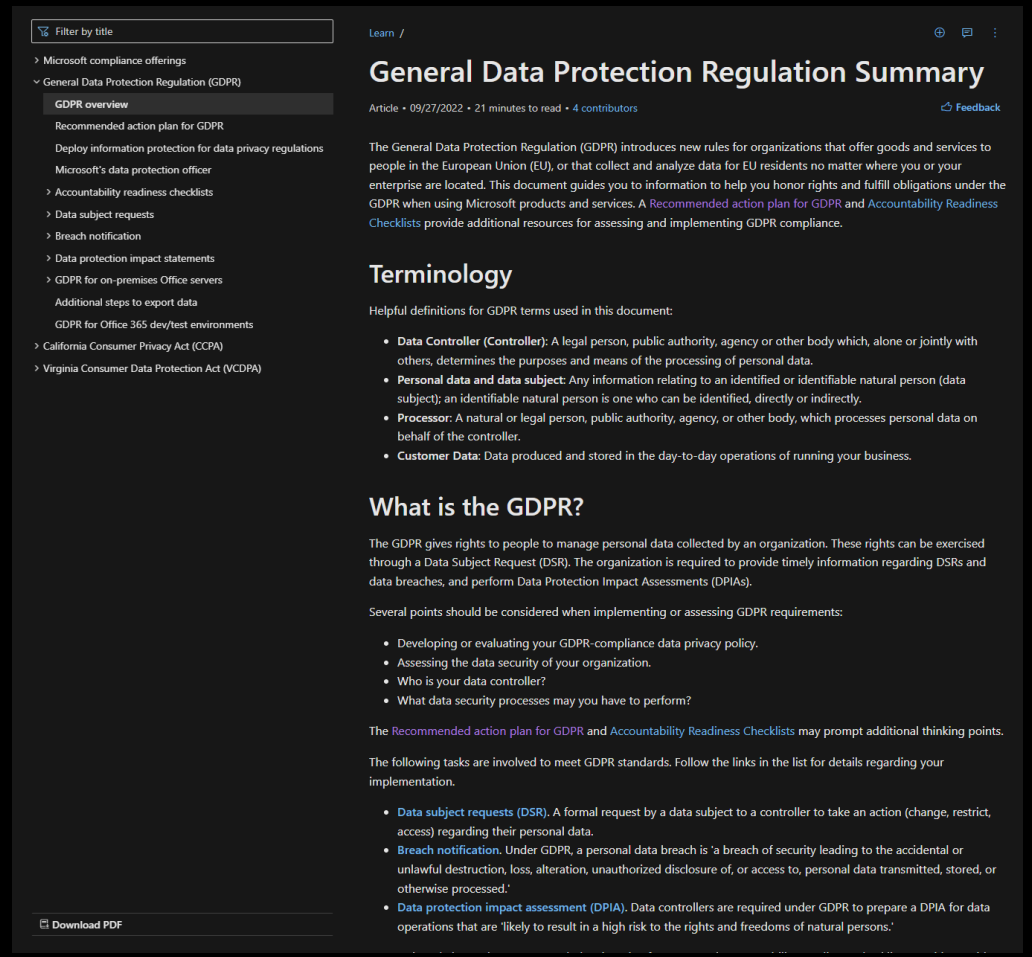
最常見的替代方案是 CWE/SANS 的 Top 25

- CWE 是通用弱點枚舉（Common Weakness Enumeration），是一份全面的安全漏洞清單
- 然而，CWE/SANS Top 25 更新頻率還不夠

CWE 本身是漏洞類別的知名“標準”

- 這是一種表達漏洞的好方法
- 常用於代碼審查和滲透測試結果

合規檔



Filter by title

- Microsoft compliance offerings
- General Data Protection Regulation (GDPR)
  - GDPR overview
  - Recommended action plan for GDPR
  - Deploy information protection for data privacy regulations
  - Microsoft's data protection officer
  - Accountability readiness checklists
  - Data subject requests
  - Breach notification
  - Data protection impact statements
  - GDPR for on-premises Office servers
  - Additional steps to export data
  - GDPR for Office 365 dev/test environments
- California Consumer Privacy Act (CCPA)
- Virginia Consumer Data Protection Act (VCDPA)

Download PDF

Learn /

General Data Protection Regulation Summary

Article • 09/27/2022 • 21 minutes to read • 4 contributors

Feedback

The General Data Protection Regulation (GDPR) introduces new rules for organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents no matter where you or your enterprise are located. This document guides you to information to help you honor rights and fulfill obligations under the GDPR when using Microsoft products and services. A Recommended action plan for GDPR and Accountability Readiness Checklists provide additional resources for assessing and implementing GDPR compliance.

Terminology

Helpful definitions for GDPR terms used in this document:

- **Data Controller (Controller)**: A legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- **Personal data and data subject**: Any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly.
- **Processor**: A natural or legal person, public authority, agency, or other body, which processes personal data on behalf of the controller.
- **Customer Data**: Data produced and stored in the day-to-day operations of running your business.

What is the GDPR?

The GDPR gives rights to people to manage personal data collected by an organization. These rights can be exercised through a Data Subject Request (DSR). The organization is required to provide timely information regarding DSRs and data breaches, and perform Data Protection Impact Assessments (DPIAs).

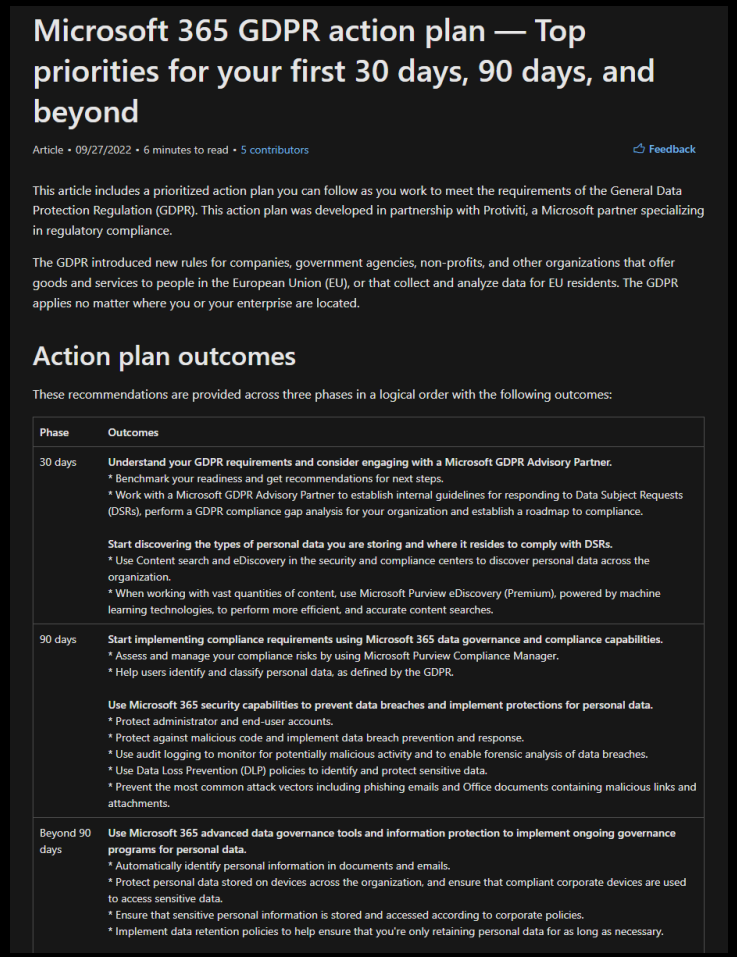
Several points should be considered when implementing or assessing GDPR requirements:

- Developing or evaluating your GDPR-compliance data privacy policy.
- Assessing the data security of your organization.
- Who is your data controller?
- What data security processes may you have to perform?

The Recommended action plan for GDPR and Accountability Readiness Checklists may prompt additional thinking points.

The following tasks are involved to meet GDPR standards. Follow the links in the list for details regarding your implementation.

- Data subject requests (DSR). A formal request by a data subject to a controller to take an action (change, restrict, access) regarding their personal data.
- Breach notification. Under GDPR, a personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.'
- Data protection impact assessment (DPIA). Data controllers are required under GDPR to prepare a DPIA for data operations that are 'likely to result in a high risk to the rights and freedoms of natural persons.'



Microsoft 365 GDPR action plan — Top priorities for your first 30 days, 90 days, and beyond

Article • 09/27/2022 • 6 minutes to read • 5 contributors

Feedback

This article includes a prioritized action plan you can follow as you work to meet the requirements of the General Data Protection Regulation (GDPR). This action plan was developed in partnership with Protiviti, a Microsoft partner specializing in regulatory compliance.

The GDPR introduced new rules for companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data for EU residents. The GDPR applies no matter where you or your enterprise are located.

Action plan outcomes

These recommendations are provided across three phases in a logical order with the following outcomes:

Phase	Outcomes
30 days	**Understand your GDPR requirements and consider engaging with a Microsoft GDPR Advisory Partner.** * Benchmark your readiness and get recommendations for next steps. * Work with a Microsoft GDPR Advisory Partner to establish internal guidelines for responding to Data Subject Requests (DSRs), perform a GDPR compliance gap analysis for your organization and establish a roadmap to compliance. **Start discovering the types of personal data you are storing and where it resides to comply with DSRs.** * Use Content search and eDiscovery in the security and compliance centers to discover personal data across the organization. * When working with vast quantities of content, use Microsoft Purview eDiscovery (Premium), powered by machine learning technologies, to perform more efficient, and accurate content searches.
90 days	**Start implementing compliance requirements using Microsoft 365 data governance and compliance capabilities.** * Assess and manage your compliance risks by using Microsoft Purview Compliance Manager. * Help users identify and classify personal data, as defined by the GDPR. **Use Microsoft 365 security capabilities to prevent data breaches and implement protections for personal data.** * Protect administrator and end-user accounts. * Protect against malicious code and implement data breach prevention and response. * Use audit logging to monitor for potentially malicious activity and to enable forensic analysis of data breaches. * Use Data Loss Prevention (DLP) policies to identify and protect sensitive data. * Prevent the most common attack vectors including phishing emails and Office documents containing malicious links and attachments.
Beyond 90 days	**Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.** * Automatically identify personal information in documents and emails. * Protect personal data stored on devices across the organization, and ensure that compliant corporate devices are used to access sensitive data. * Ensure that sensitive personal information is stored and accessed according to corporate policies. * Implement data retention policies to help ensure that you're only retaining personal data for as long as necessary.

針對 Microsoft 365、Azure 及其他 Microsoft 服務的合規服務。|Microsoft Learn

Azure 安全基準

[Microsoft 雲端安全基準測試 | Microsoft Learn]

Azure Security Benchmark 文件提供了如何在 Azure 上保護雲解決方案的最佳實踐和指導。

安全控制：Azure 安全基準的建議按安全控制進行分類。安全控制代表高級別的、與供應商無關的安全要求，例如網路安全和數據保護。 每個安全控制都有一組安全建議和實施這些建議的指導說明。

服務推薦：在可用的情況下，針對 Azure 服務的基準建議將包括專門針對該服務量身定製的 Azure 安全基準建議。

謝謝！