Microsoft Azure

Secure DevOps: Application Security Principles and Practices

Secure DevOps Principles and Practices

Your name
Your Title
Microsoft

Module Overview

- Secure DevOps Principles
- Software Composition Analysis
- Operational Security Assurance
- Practices alignment with standards

Microsoft Azure

Secure DevOps Principles and Practices

Assume and prevent breach

Prevent breach

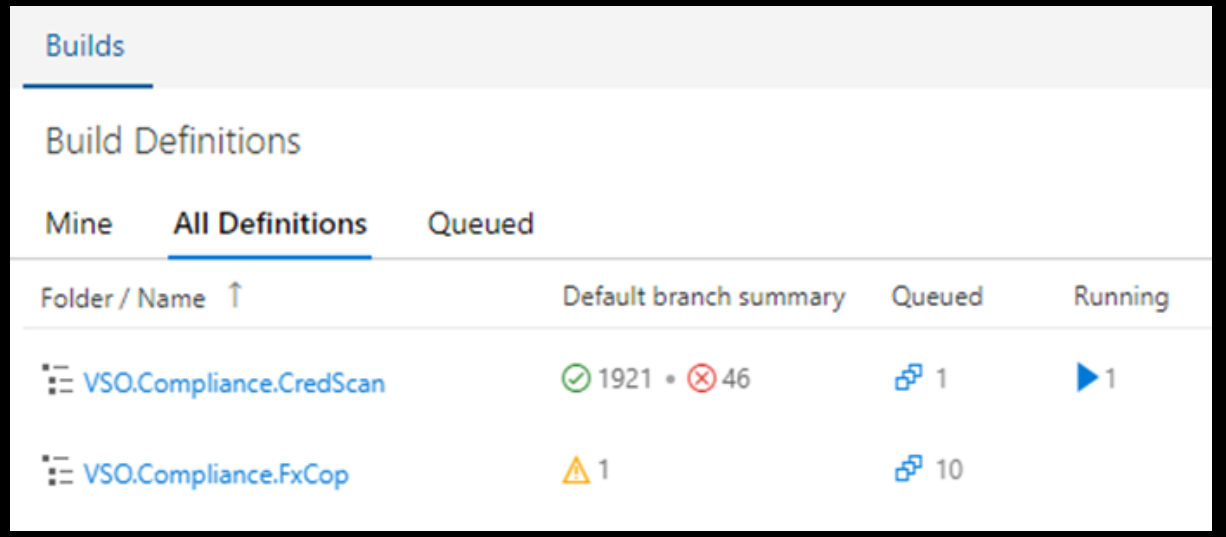
- Threat model
- Code review
- Credential protection
- Static Application Security Testing (SAST)
- Dynamic Application Security Testing (DAST)

Assume breach

- Red and Blue teams
- War game exercises
- Central security monitoring
- Live site penetration test

Shift left and automate

- Utilize tools to analyze misconfiguration of infrastructure (GitHub Advanced Security)
- Refresh the infrastructure regularly
- PaaS and regular deployment from IaC (Infra as Code) refresh the infra and wash out the places to hide
- Encrypt by default in transit and at rest
- Utilize Pipeline Security Tools

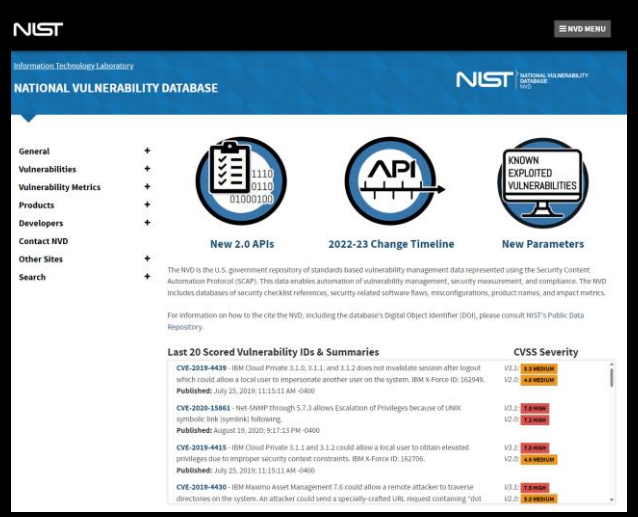


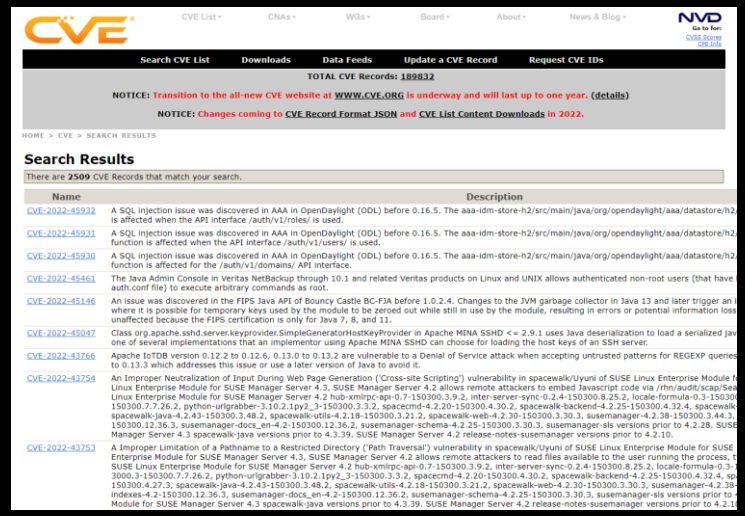
Select tools that provide high confidence

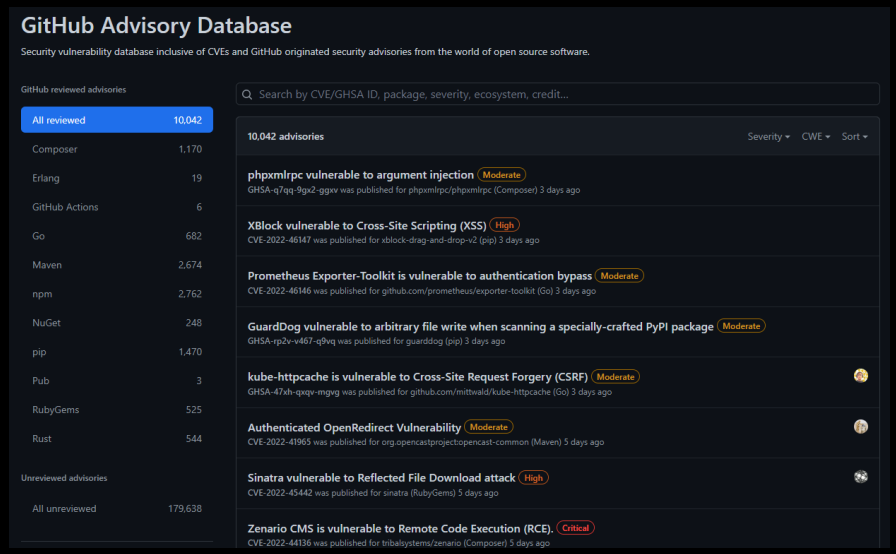
- Tools that are integrated into the pipeline must not require security expertise
- Results must be accurate and important
- The team must have high confidence on the results reported by the tools and the process

Stay Up-to-date

- Keep current on the latest patches
- Update your frameworks
- Keep up to date with **N**ational **V**ulnerability **D**atabase
- Stay current on regulatory and compliance changes
- Reduce technical debt

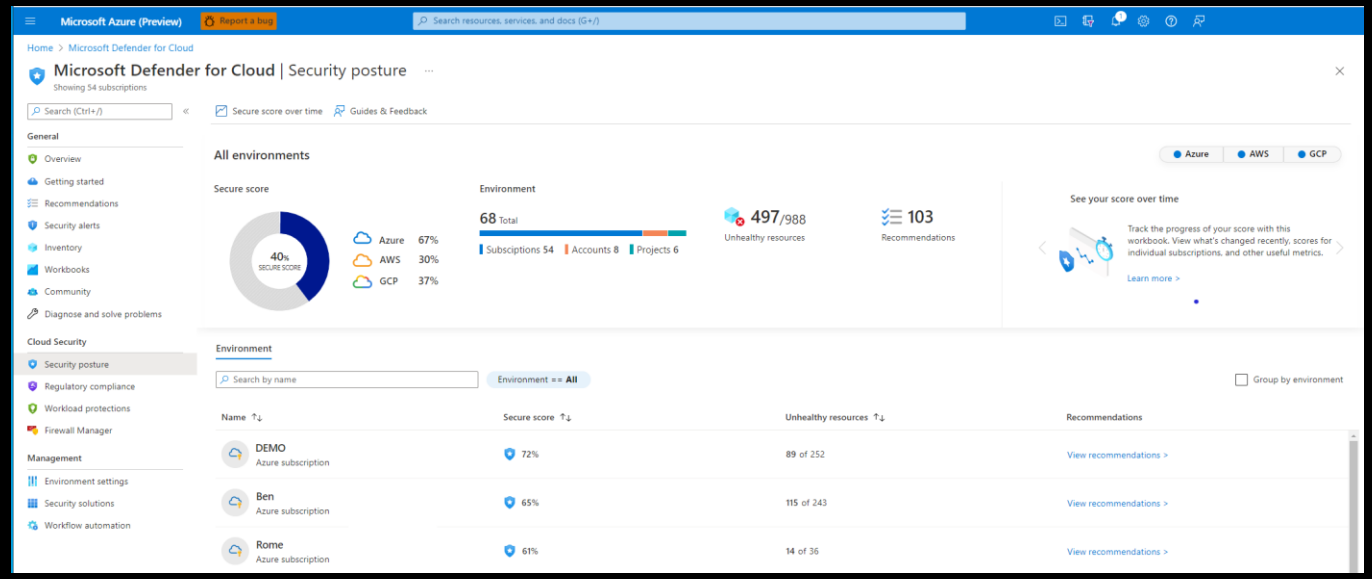






Continuous monitoring and learning

- Continuously and relentlessly improve usability
- Monitoring the pipeline and deployments
- Aggregation of build and deployment output results
- Monitoring environments for security and stability



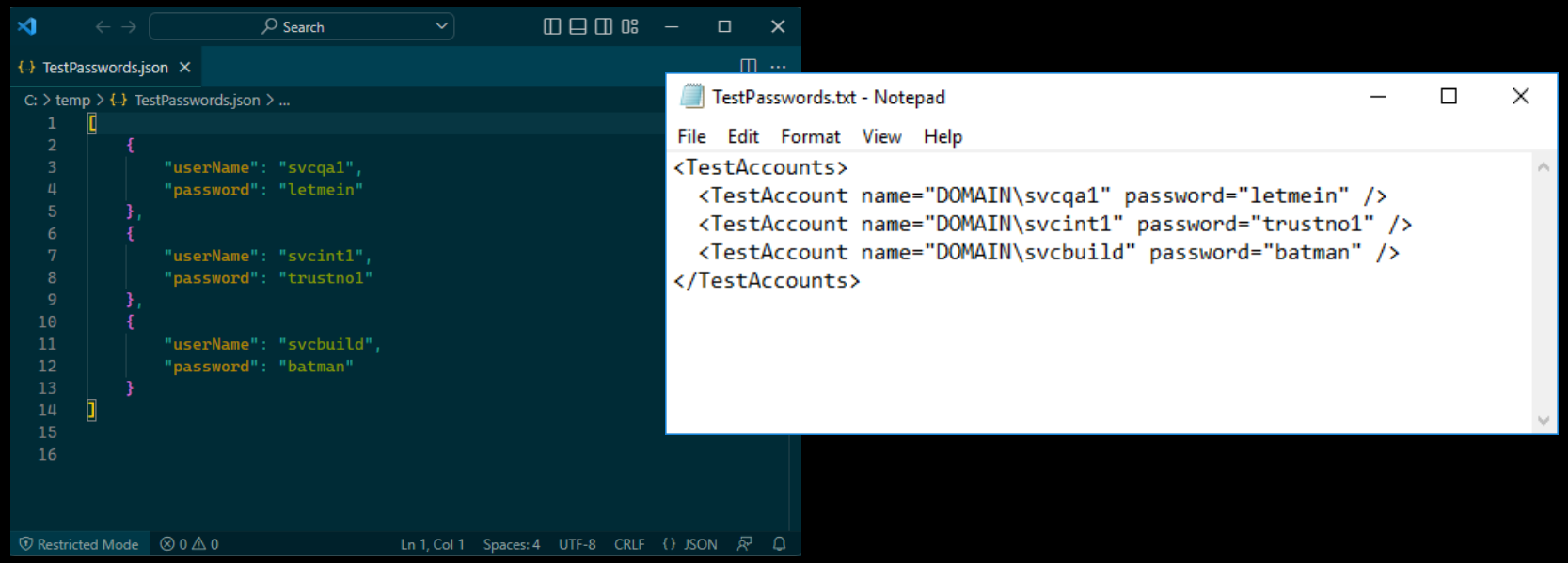
Secure DevOps Culture

- Perform security reviews for all major features (but not all features)
- InfoSec should be integrated into the software delivery process
- Give developers the ability to build security into their daily work
- Security is everyone's responsibility, Bring Security, Development, and Operations together

Microsoft Azure

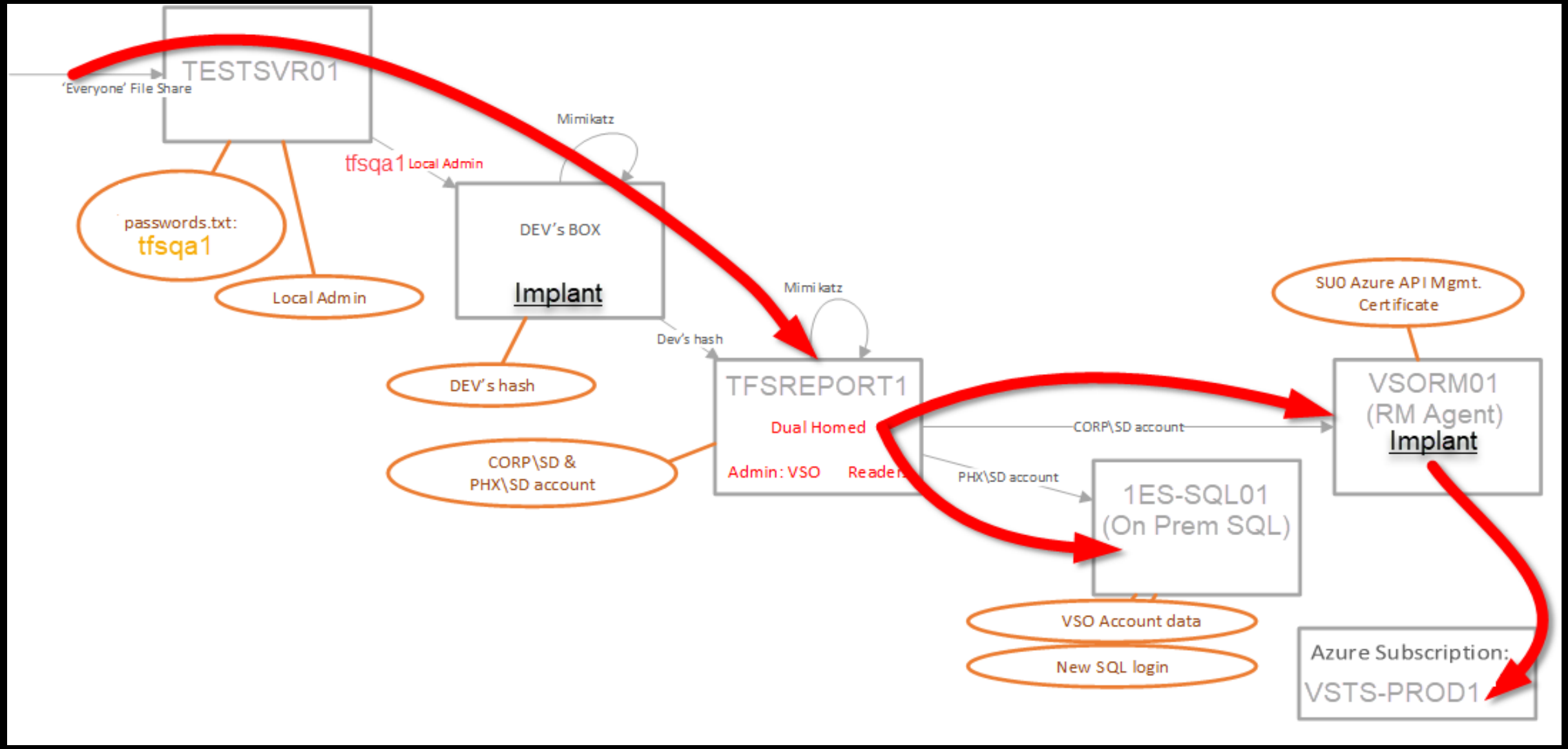
Managing secrets

Plaintext credentials in files

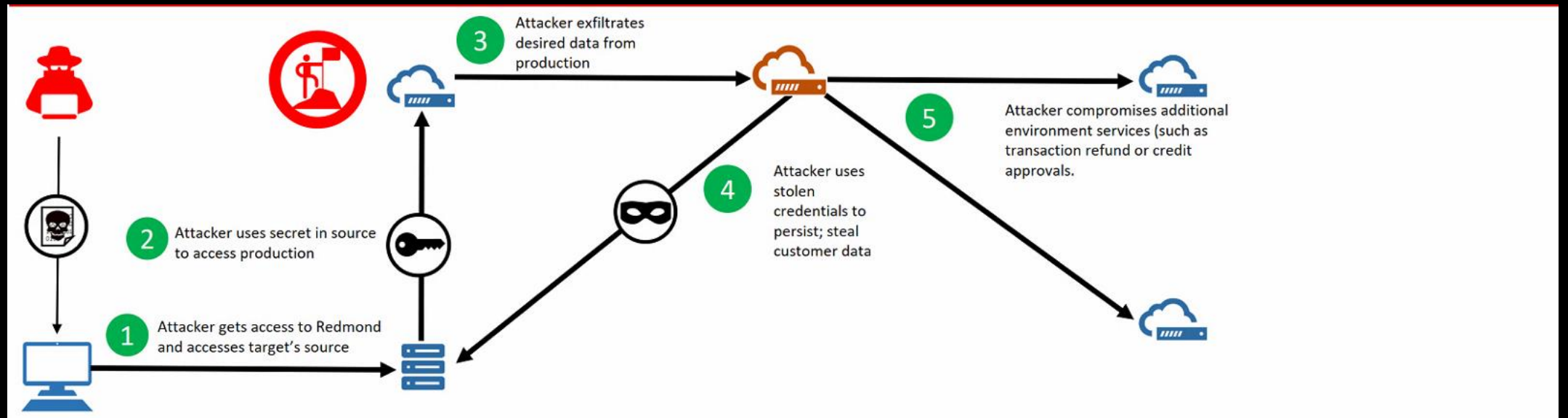


Every team seems to experience this one at the beginning

Example: Red Team Attack with Lateral Movement



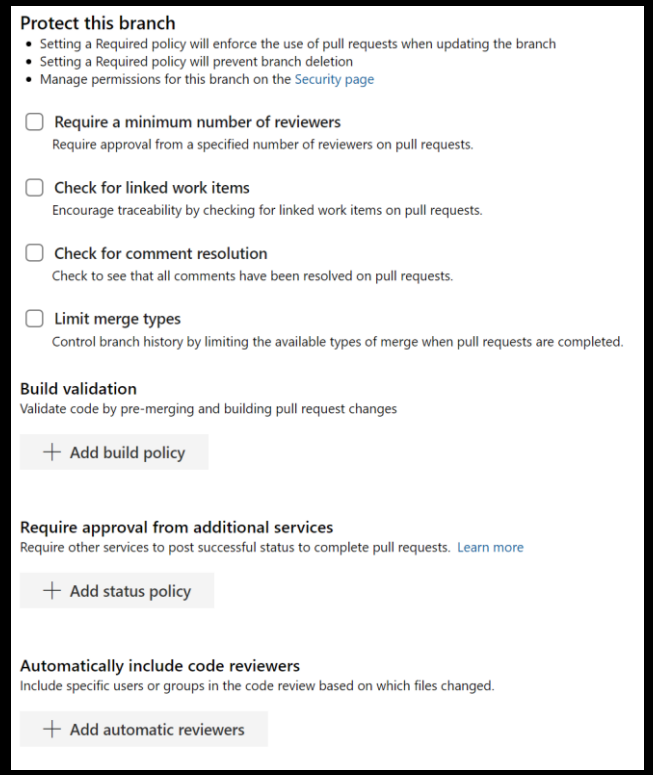
Attack with lateral movement

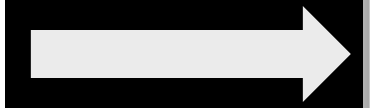


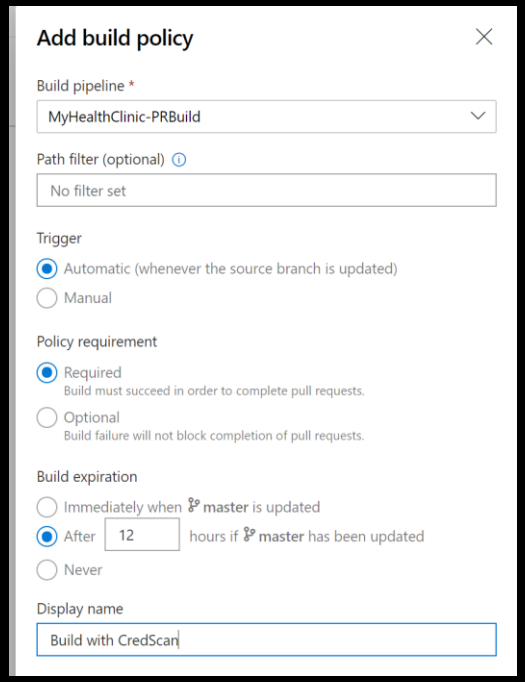
Event	Detection	Response	Impact & Lessons Learned
• Target's source code was pulled as part of standard recon activities and analyzed • Production Keyvault information was discovered inside source repository • Production Keyvault was accessed; all targets employees' usernames and password hashes were 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)

Automate credential scanning

Cred scanning before merging code







[Source Code Analysis Tools | OWASP Foundation]

[About GitHub Advanced Security - GitHub Docs]

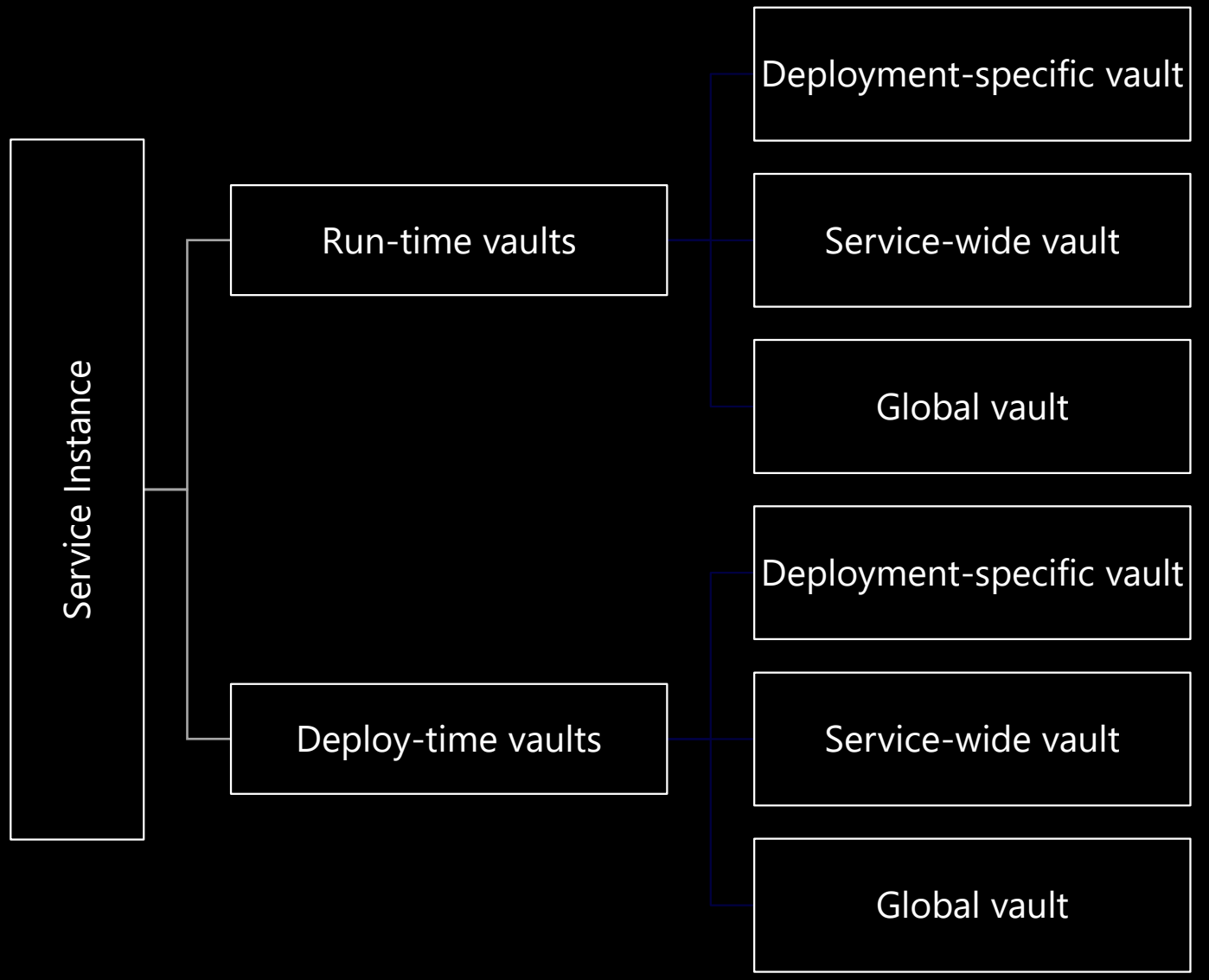
Azure Key Vault (AKV)

All secrets must be stored in AKV:

- Passwords, keys, tokens
- Storage Account keys
- Certificates
- Credentials used in Test too

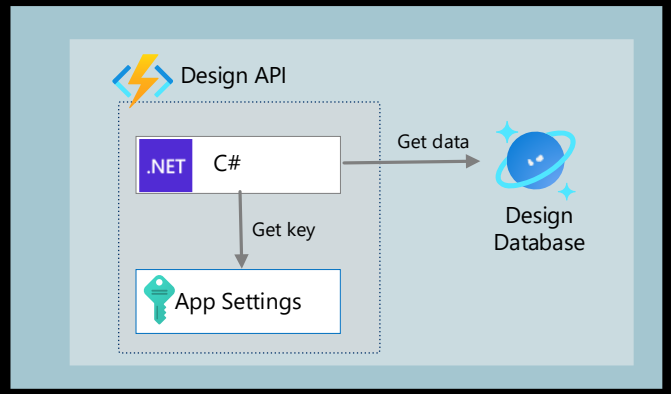
Hierarchy of vaults to eliminate duplication of secrets.

Vaults available at run-time so that secret changes propagate instantly.

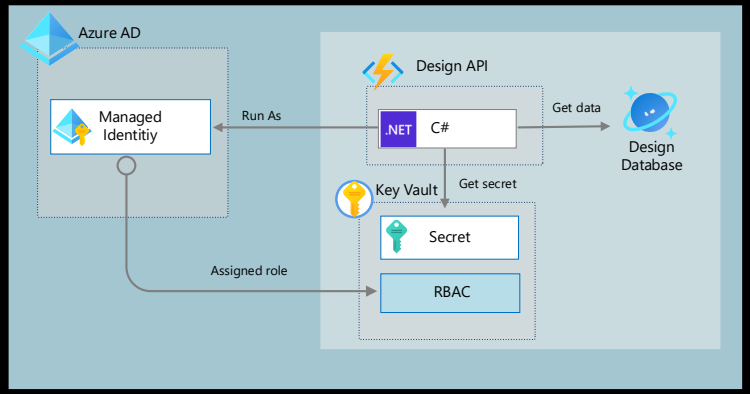


Is a secret really needed?

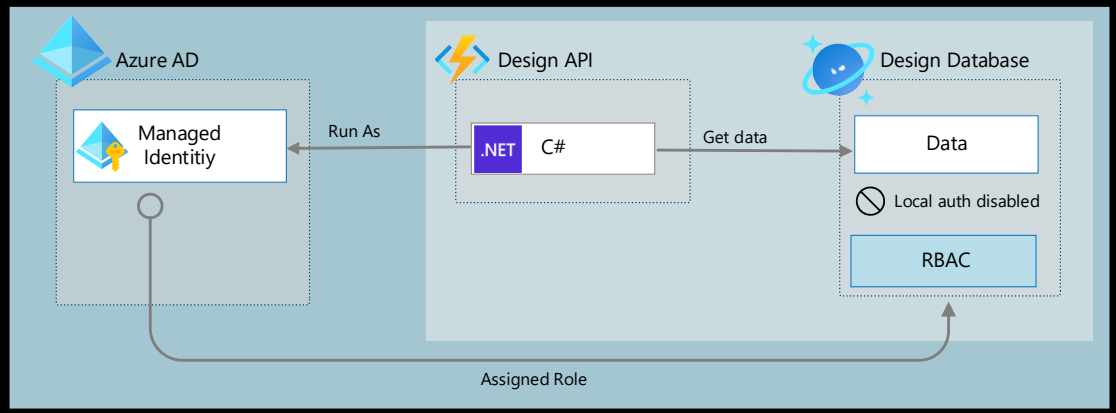
Option 1 – secret in app settings



Option 2 – secret in Azure Key Vault



Option 3 – No secret - Managed identities and Azure AD RBAC



Microsoft Azure

Operational Security Assurance

Common challenges with solution operations

Secret Management

Connection strings, passwords and private keys
Where are they stored?
Who can access them?
When are they replaced/rotated and how?

Identity Management

User Authentication
How are users authorized
Assigned rights for users and services
Secret access

Data protection

Data at rest
- Authorization
- Transparent encryption vs client-side encryption
- Keys management

Data in use
- Memory isolation
- Input validation

Data in transit
- HTTPS quality
- Authentication & authorization

GDPR Right to Erasure

- EU residents can request removal of personal data from databases
- Must be a permanent, irreversible method for GDPR compliance
- Adopt anonymization technique during app design phase to lower the cost
- Delivers consistent data masking benefits as FPE, but irreversible

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).

Privacy versus Security

Privacy

- Empowering users to control collection, use, and distribution of their personal information.
- Privacy requires security

Security

- Establishing protective measures that defend against hostile acts.
- Security does not guarantee privacy

Privacy AND Security are key factors for building trusted applications.

Microsoft Azure

Practices alignment with standards

OWASP Top 10

A Common Baseline Security Standard OWASP Top 10:2021

- The OWASP Top 10 is a well-known way to get to a secure baseline
- It's not uncommon for customers to demand systems that adhere to Top 10 practices

It's a low, but practical bar

Not only for web applications

- API OWASP API Security Project | OWASP Foundation
- DevOps OWASP Top 10 CI/CD Security Risks | OWASP Foundation

Alternatives to OWASP Top 10

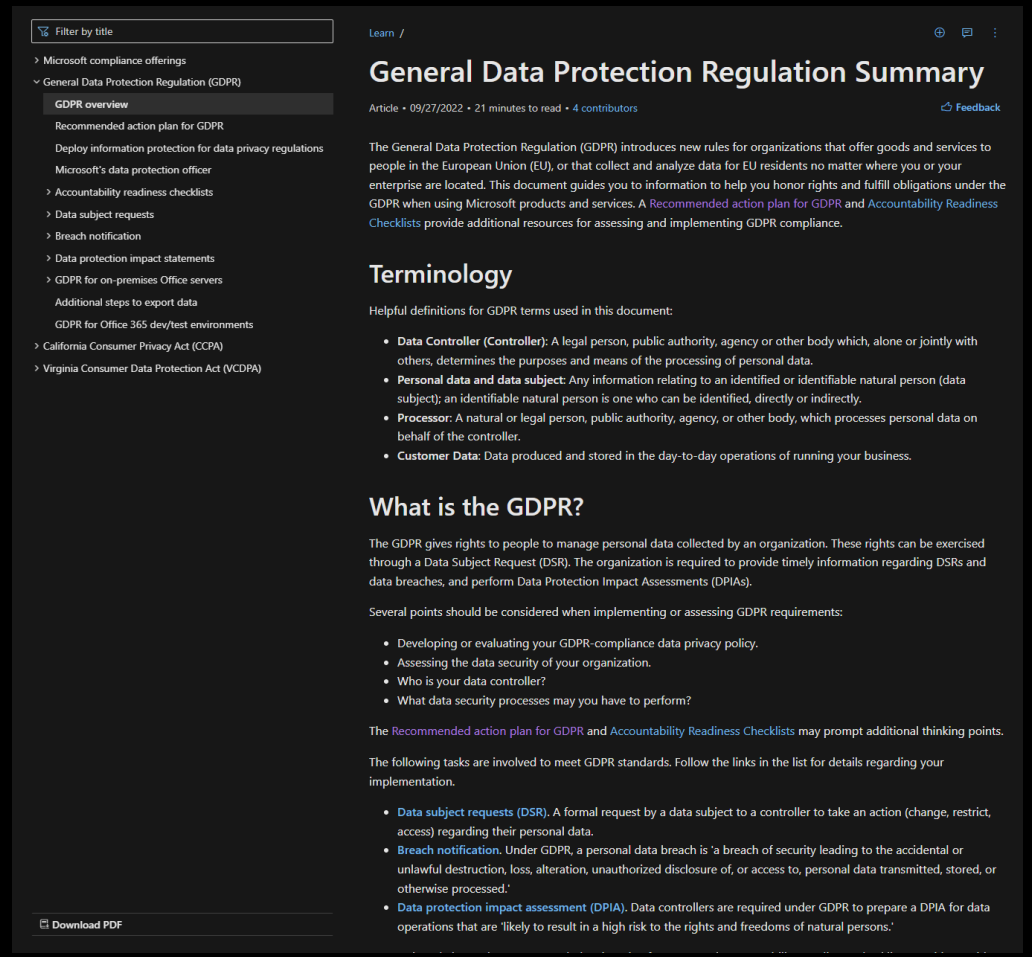
The most common alternative is the CWE/SANS Top 25

- CWE is the Common Weakness Enumeration and is a comprehensive list of security vulnerabilities
- CWE/SANS Top 25 is not updated often enough, however

The CWE itself is a well-known ‘standard’ for vulnerability classes

- It’s a great way to express a vulnerability
- Commonly used on code review and pen-test results

Compliance documentation



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).

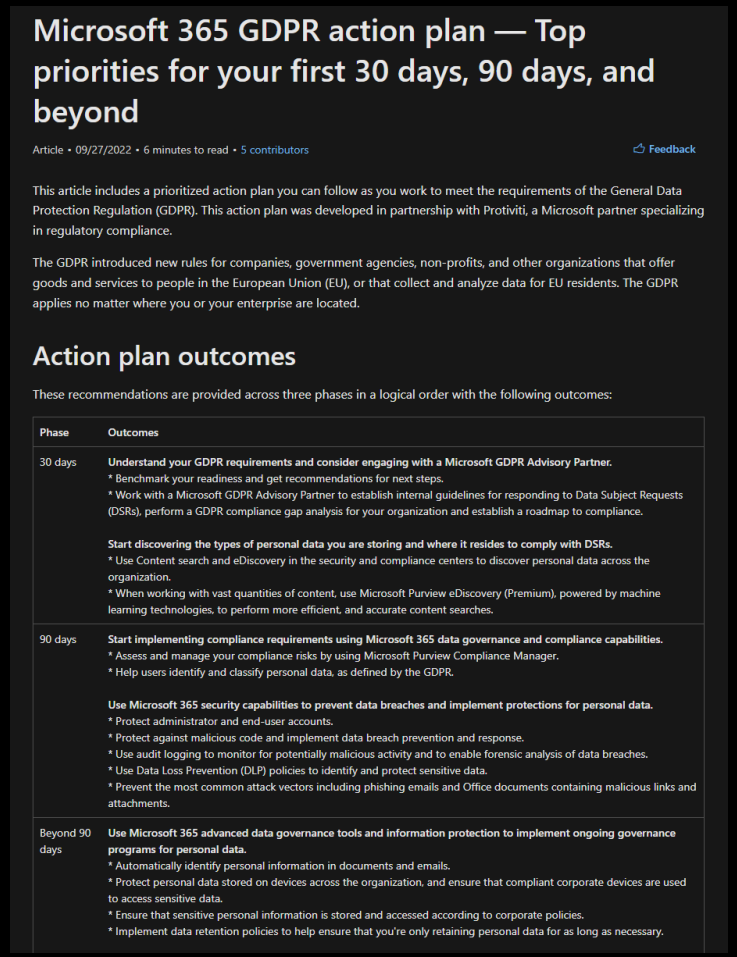
Several points should be considered when implementing or assessing GDPR requirements:

- 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.

[Compliance offerings for Microsoft 365, Azure, and other Microsoft services. | Microsoft Learn]

Azure Security Benchmark

[Microsoft cloud security benchmark | Microsoft Learn]

The Azure Security Benchmark documentation provide guidance for how to secure your cloud solutions on Azure with best practices and guidance.

Security Controls: The Azure Security Benchmark recommendations are categorized by security controls. Security controls represent high-level vendor-agnostic security requirements, such as network security and data protection. Each security control has a set of security recommendations and instructions that help you implement those recommendations.

Service Recommendations: When available, benchmark recommendations for Azure services will include Azure Security Benchmark recommendations that are tailored specifically for that service.

Lab – Credentials Management in pipelines