

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

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

| Builds | | | |
|---|---|--|---|
| Build Definitions | | | |
| Mine | All Definitions | Queued | |
| Folder / Name ↑ | Default branch summary | Queued | Running |
|  VSO.Compliance.CredScan |  1921 •  46 |  1 |  1 |
|  VSO.Compliance.FxCop |  1 |  10 | |

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

| | |
|---|-------------------------|
| src/MyHealth.Web/Project_Readme.html | |
| <input type="checkbox"/> Replace this tag by . See Rule | 2 years ago ▾ L133 🔗 🗑️ |
| 🐛 Bug ▾ 🟡 Minor ▾ 🔵 Open ▾ Not assigned ▾ 2min effort Comment | 🔗 accessibility ▾ |
| src/MyHealth.Web/Views/Home/Index.cshtml | |
| <input type="checkbox"/> Add an "alt" attribute to this image. See Rule | 2 years ago ▾ L16 🔗 🗑️ |
| 🐛 Bug ▾ 🟡 Minor ▾ 🔵 Open ▾ Not assigned ▾ 5min effort Comment | 🔗 accessibility ▾ |
| <input type="checkbox"/> Add an "alt" attribute to this image. See Rule | 2 years ago ▾ L22 🔗 🗑️ |
| 🐛 Bug ▾ 🟡 Minor ▾ 🔵 Open ▾ Not assigned ▾ 5min effort Comment | 🔗 accessibility ▾ |
| <input type="checkbox"/> Add an "alt" attribute to this image. See Rule | 2 years ago ▾ L23 🔗 🗑️ |
| 🐛 Bug ▾ 🟡 Minor ▾ 🔵 Open ▾ Not assigned ▾ 5min effort Comment | 🔗 accessibility ▾ |
| <input type="checkbox"/> Replace this tag by . See Rule | 2 years ago ▾ L96 🔗 🗑️ |
| 🐛 Bug ▾ 🟡 Minor ▾ 🔵 Open ▾ Not assigned ▾ 2min effort Comment | 🔗 accessibility ▾ |
| <input type="checkbox"/> Replace this tag by . See Rule | 2 years ago ▾ L106 🔗 🗑️ |
| 🐛 Bug ▾ 🟡 Minor ▾ 🔵 Open ▾ Not assigned ▾ 2min effort Comment | 🔗 accessibility ▾ |
| <input type="checkbox"/> Replace this tag by . See Rule | 2 years ago ▾ L117 🔗 🗑️ |
| 🐛 Bug ▾ 🟡 Minor ▾ 🔵 Open ▾ Not assigned ▾ 2min effort Comment | 🔗 accessibility ▾ |

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

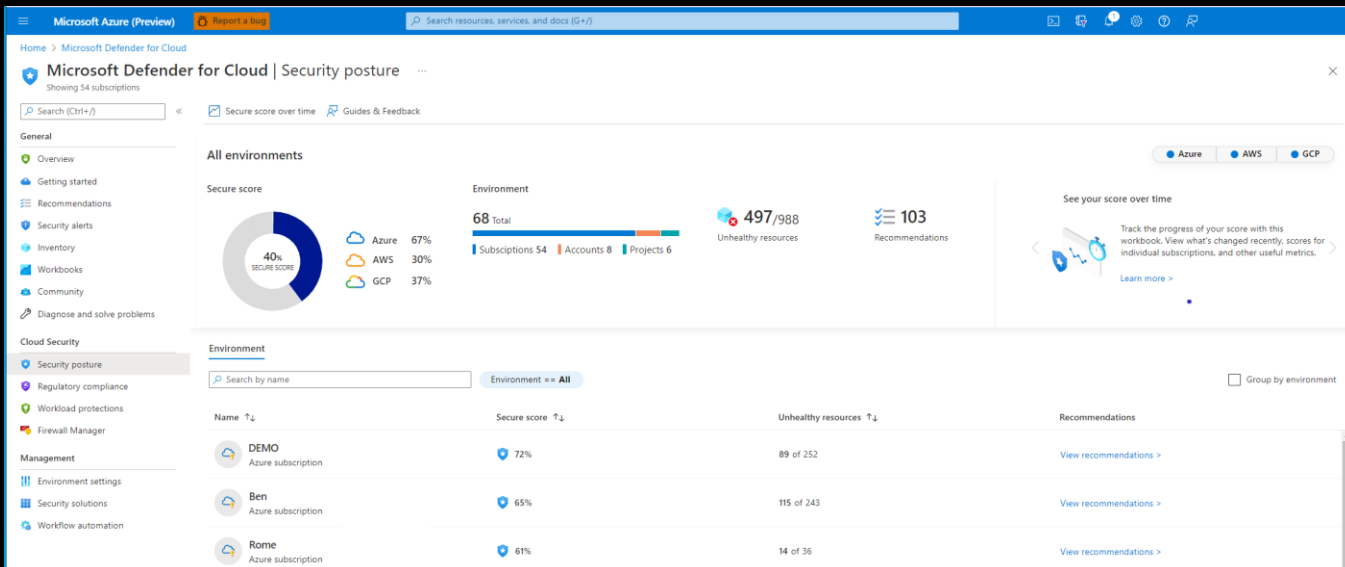
The screenshot shows the NIST National Vulnerability Database (NVD) homepage. It features a navigation menu on the left with links to General, Vulnerabilities, Vulnerability Metrics, Products, Developers, Contact NVD, and Other Sites. The main content area includes a header with the NIST logo and the text 'NATIONAL VULNERABILITY DATABASE'. Below the header, there are three circular icons representing 'New 2.0 APIs', '2022-23 Change Timeline', and 'New Parameters'. A section titled 'Last 20 Scored Vulnerability IDs & Summaries' lists several CVEs with their CVSS severity scores. The CVEs listed are: CVE-2023-4439 (IBM Cloud Private 3.1.0, 3.1.1, and 3.1.2), CVE-2023-45061 (NetCDF through 5.7.3), CVE-2023-4415 (IBM Cloud Private 3.1.1 and 3.1.2), and CVE-2023-4430 (IBM Maximo Asset Management 7.6).

The screenshot shows the CVE Details page for CVE-2022-45932. The page header includes the CVE logo and navigation links for CVE List, CNAs, WGs, Board, About, and News & Blog. The main content area displays the CVE ID, a search bar, and a list of search results. The search results table has columns for Name and Description. The first result is CVE-2022-45932, which describes a SQL injection issue discovered in AAA in OpenDaylight (ODL) before 0.16.5. The page also includes a notice about the transition to the new CVE website at www.cve.org.

The screenshot shows the GitHub Advisory Database. The header includes the title 'GitHub Advisory Database' and a subtitle 'Security vulnerability database inclusive of CVEs and GitHub originated security advisories from the world of open source software.' The main content area is divided into two sections: 'GitHub reviewed advisories' and 'Unreviewed advisories'. The 'GitHub reviewed advisories' section lists several advisories with their severity levels and CVE IDs. The advisories listed are: '10,042 advisories', 'phpxmllrpc vulnerable to argument injection', 'XBlock vulnerable to Cross-Site Scripting (XSS)', 'Prometheus Exporter-Toolkit is vulnerable to authentication bypass', 'GuardDog vulnerable to arbitrary file write when scanning a specially-crafted PyPi package', 'kube-httpcache is vulnerable to Cross-Site Request Forgery (CSRF)', 'Authenticated OpenRedirect Vulnerability', 'Sinatra vulnerable to Reflected File Download attack', and 'Zenario CMS is vulnerable to Remote Code Execution (RCE)'.

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

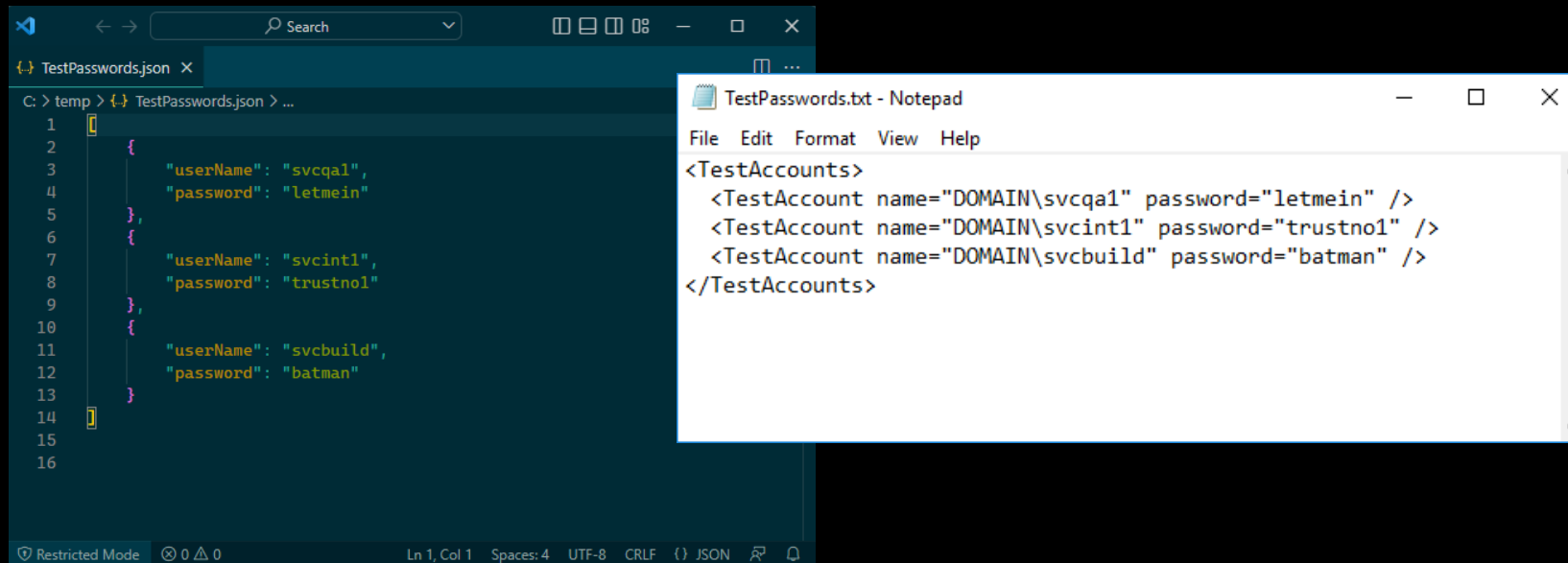


Secure DevOps Culture

- 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

Managing secrets

Plaintext credentials in files



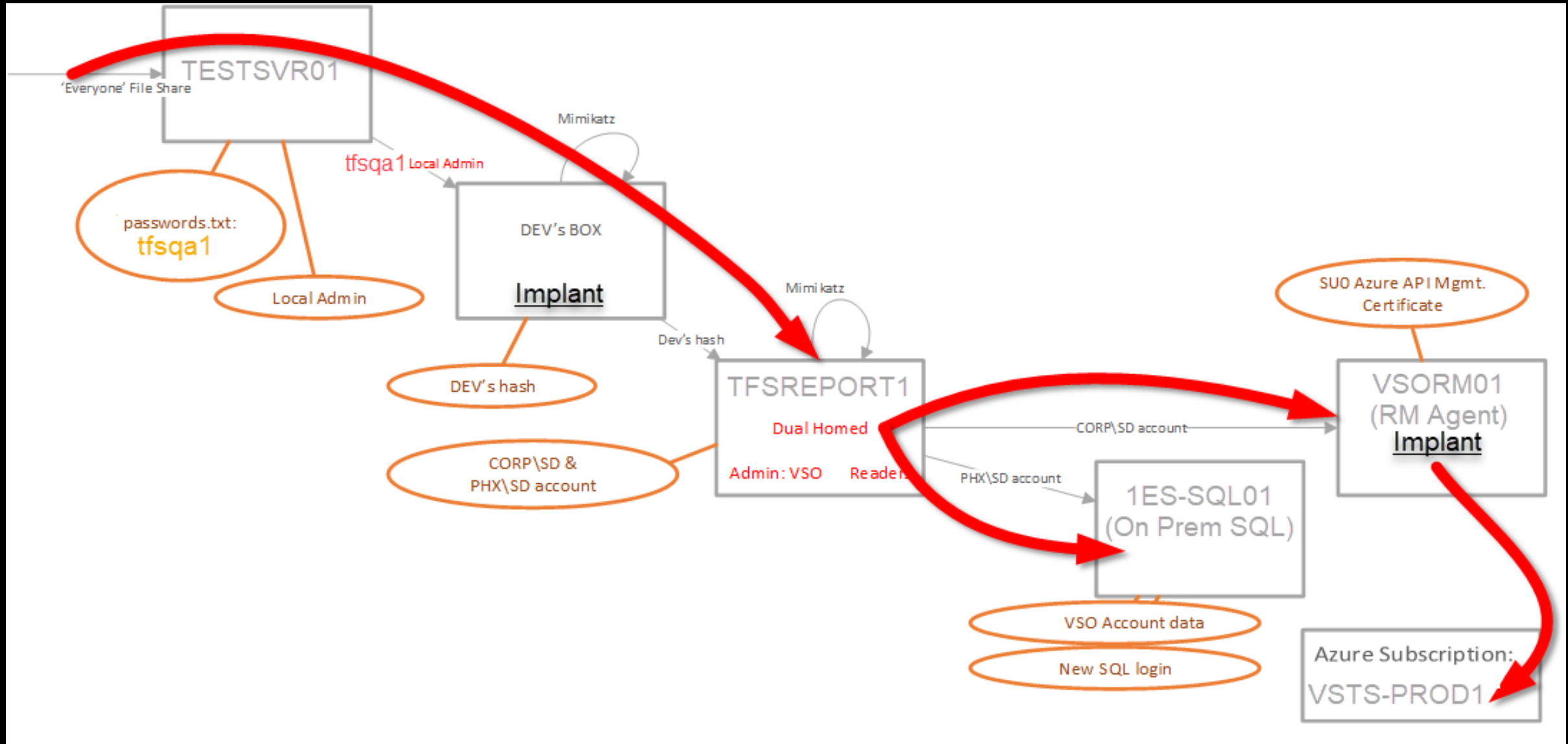
The image shows two windows side-by-side. The left window is Visual Studio Code (VS Code) with a file named 'TestPasswords.json' open. The file contains a JSON array of three objects, each representing a test account with a 'userName' and a 'password'. The right window is a Notepad application with a file named 'TestPasswords.txt' open. The file contains an XML document with a root element 'TestAccounts' and three child elements 'TestAccount', each containing 'name' and 'password' attributes.

```
1 {
2   {
3     "userName": "svcqa1",
4     "password": "letmein"
5   },
6   {
7     "userName": "svcint1",
8     "password": "trustno1"
9   },
10  {
11    "userName": "svcbuild",
12    "password": "batman"
13  }
14 }
15
16
```

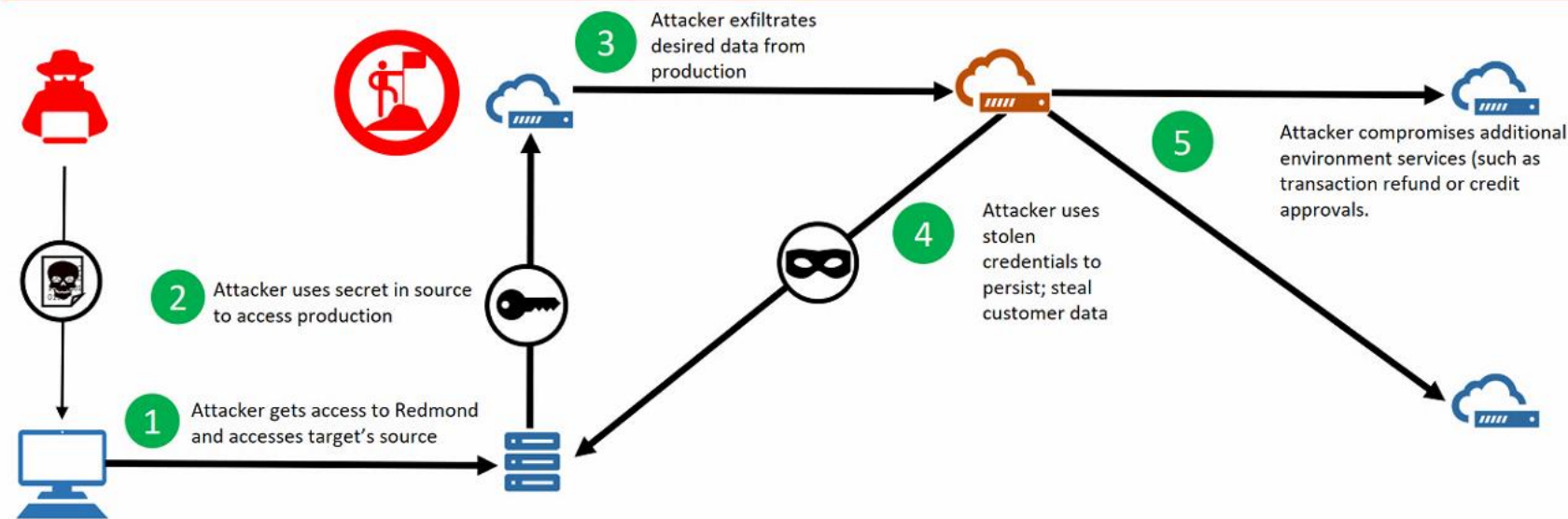
```
<TestAccounts>
  <TestAccount name="DOMAIN\svcqa1" password="letmein" />
  <TestAccount name="DOMAIN\svcint1" password="trustno1" />
  <TestAccount name="DOMAIN\svcbuild" password="batman" />
</TestAccounts>
```

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 |
|--|--|---|--|
| <ul style="list-style-type: none">Target's source code was pulled as part of standard recon activities and analyzedProduction Keyvault information was discovered inside source repositoryProduction Keyvault was accessed; all targets employees' usernames and password hashes were discovered and cracked outCustomer information was accessed, and read-write access was validatedCertificates for managing targets Azure subscriptions and targets Fabric were discovered and validated | <ul style="list-style-type: none">No actions were detected while on this engagementIncident Response is engaged for cleanup of employee credentials and customer data | <ul style="list-style-type: none">Due to no detections; no response actions have been taken | <ul style="list-style-type: none">Implementation of automated credential scanning for places where high value data is a mustEnvironment separation between pre-production and production also is a mustA 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

Protect this branch

- Setting a Required policy will enforce the use of pull requests when updating the branch
- Setting a Required policy will prevent branch deletion
- Manage permissions for this branch on the [Security page](#)

☐ **Require a minimum number of reviewers**
Require approval from a specified number of reviewers on pull requests.

☐ **Check for linked work items**
Encourage traceability by checking for linked work items on pull requests.

☐ **Check for comment resolution**
Check to see that all comments have been resolved on pull requests.

☐ **Limit merge types**
Control branch history by limiting the available types of merge when pull requests are completed.

Build validation
Validate code by pre-merging and building pull request changes

+ Add build policy

Require approval from additional services
Require other services to post successful status to complete pull requests. [Learn more](#)

+ Add status policy

Automatically include code reviewers
Include specific users or groups in the code review based on which files changed.

+ Add automatic reviewers



Add build policy ✕

Build pipeline *
MyHealthClinic-PRBuild ▼

Path filter (optional) ⓘ
No filter set

Trigger
☒ Automatic (whenever the source branch is updated)
☐ Manual

Policy requirement
☒ Required
Build must succeed in order to complete pull requests.
☐ Optional
Build failure will not block completion of pull requests.

Build expiration
☐ Immediately when master is updated
☒ After 12 hours if master has been updated
☐ Never

Display name
Build with CredScan

[Source Code Analysis Tools | OWASP Foundation](#)
[About GitHub Advanced Security - GitHub Docs](#)

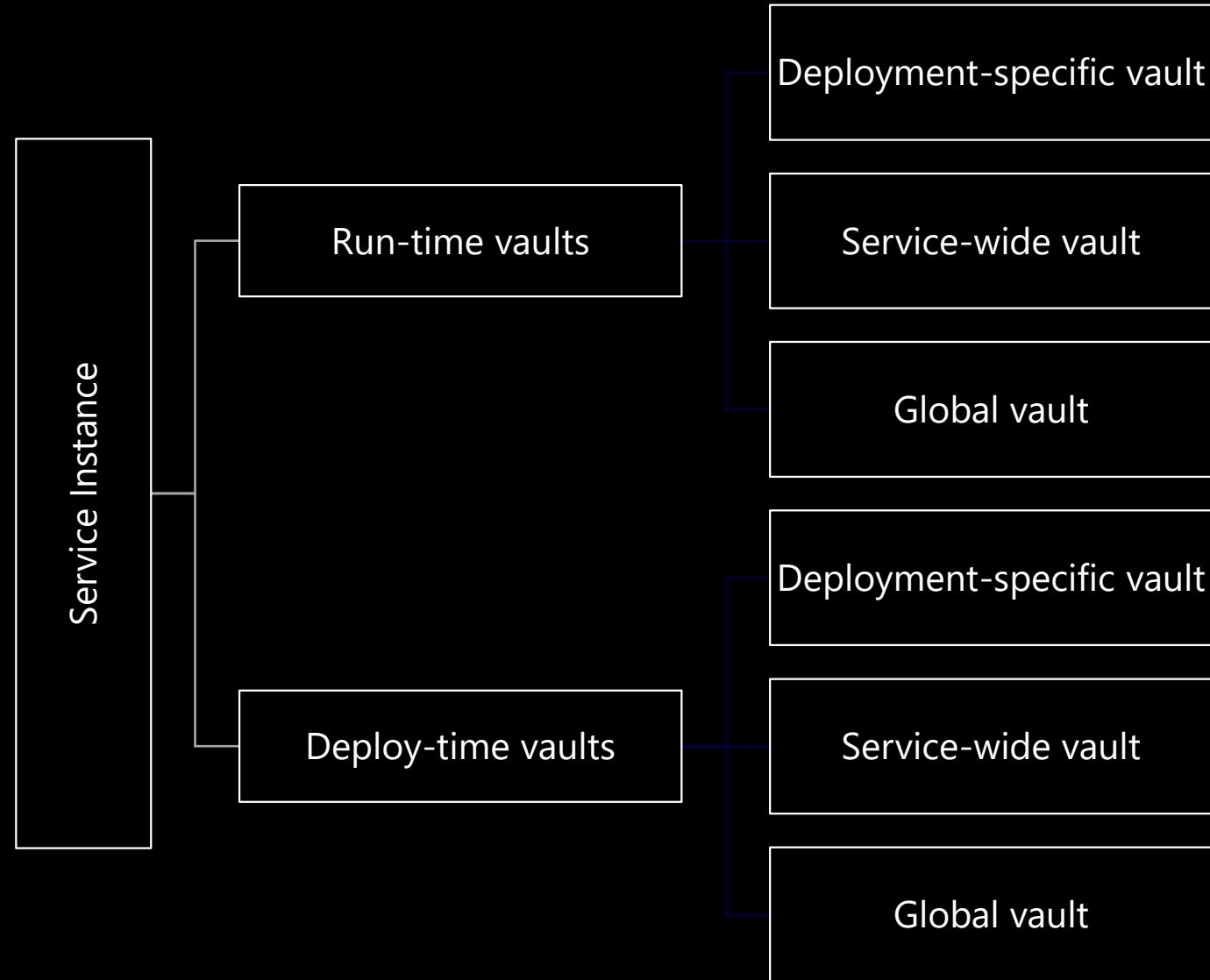
Azure Key Vault (AKV)

All secrets must be stored in AKV:

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

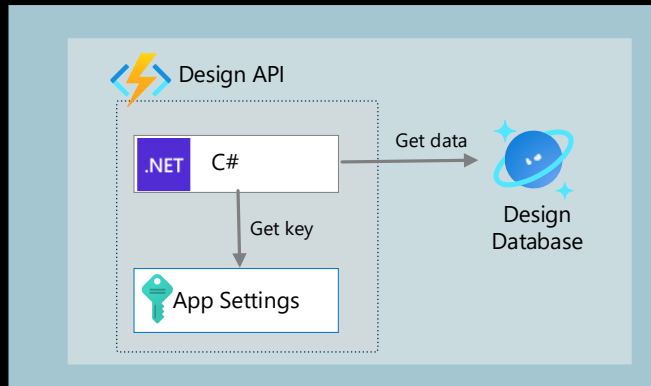
Hierarchy of vaults to eliminate duplication of secrets.

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

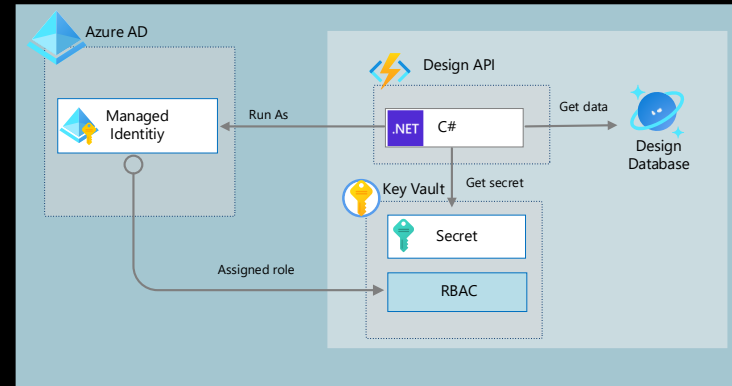


Is a secret really needed?

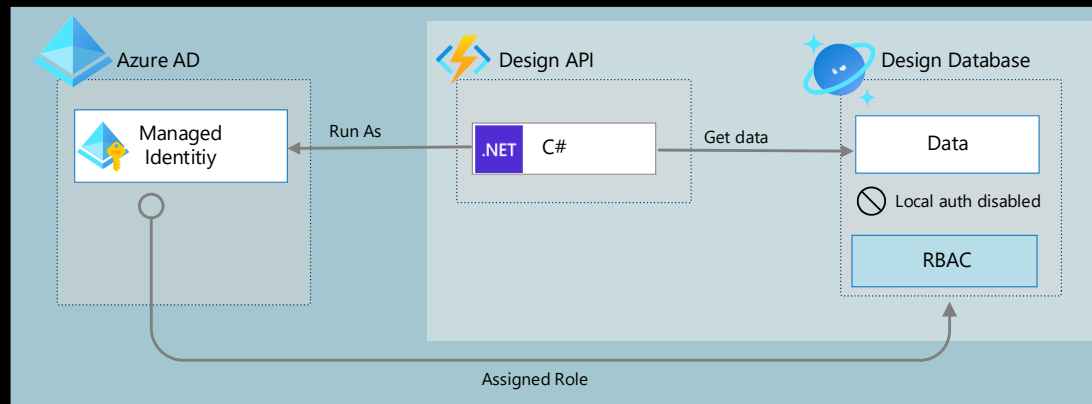
Option 1 – secret in app settings



Option 2 – secret in Azure Key Vault



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



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?



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



Identity Management

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

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.

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)

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.'

Download PDF

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 | <p>Understand your GDPR requirements and consider engaging with a Microsoft GDPR Advisory Partner.</p> <ul style="list-style-type: none">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. <p>Start discovering the types of personal data you are storing and where it resides to comply with DSRs.</p> <ul style="list-style-type: none">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 | <p>Start implementing compliance requirements using Microsoft 365 data governance and compliance capabilities.</p> <ul style="list-style-type: none">Assess and manage your compliance risks by using Microsoft Purview Compliance Manager.Help users identify and classify personal data, as defined by the GDPR. <p>Use Microsoft 365 security capabilities to prevent data breaches and implement protections for personal data.</p> <ul style="list-style-type: none">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 | <p>Use Microsoft 365 advanced data governance tools and information protection to implement ongoing governance programs for personal data.</p> <ul style="list-style-type: none">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

Learn / Security / Benchmark /

Microsoft cloud security benchmark documentation


Learn how to secure your cloud solutions with our best practices and guidance.

About the Microsoft cloud security benchmark (MCSB)

 OVERVIEW


- Microsoft cloud security benchmark introduction
- Overview of MCSB controls (v1)
- Overview of the MCSB security baselines

AI + Machine Learning security baselines

 OVERVIEW

- Azure Databricks
- Azure Machine Learnings
- Azure Cognitive Search


Databases security baselines

 OVERVIEW

- Azure Cache for Redis
- Azure Database for MySQL
- Azure Database for MariaDB
- Azure Database for PostgreSQL - Single Server
- Azure Database for PostgreSQL - Hyperscale
- Azure SQL Database
- Cosmos DB


Networking security baselines

MCSB v1 controls

 OVERVIEW


- Network security
- Identity management
- Privileged access
- Data protection
- Asset management
- See more

Analytics security baselines

 OVERVIEW


- Azure Data Explorer security baseline
- Azure Data Factory security baseline
- Data Lake Analytics security baseline
- Event Hubs security baseline
- HDInsight security baseline
- Stream Analytics baseline
- Azure Synapse Analytics security baseline

Integration security baselines

 OVERVIEW


- API Management
- Event Grid
- Logic Apps

More Azure security resources

 TRAINING


- Azure Security Fundamentals
- Shared responsibility in the cloud
- Microsoft Defender for Cloud
- Azure Security Benchmark Foundation blueprint sample

Compute security baselines

 OVERVIEW

- Azure Functions
- Batch
- Container Instances
- Container Registry
- Service Fabric
- Azure Storage
- Virtual Machine Scale Sets
- Virtual Machines Linux
- Virtual Machines Windows

Management and Governance security baselines

 OVERVIEW

- Automation
- Azure Backup
- Azure Monitor
- Azure Policy

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

