



# Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

---

CyberSecurity Weißwurstfrühstück, Mai 2025



Digital & App Innovation  
Azure

Specialist  
DevOps with GitHub



Data & AI  
Azure

Specialist  
Migrate Enterprise Applications  
to Microsoft Azure

# Wer bin ich?

---



**Nico Meisenzahl**  
**Geschäftsführer | COO**



+49 8031 230159-112



nico.meisenzahl@whiteduck.de



@nmeisenzahl



[www.linkedin.com/in/nicomeisenzahl](https://www.linkedin.com/in/nicomeisenzahl)

- Cloud Solution Architect
- Azure & Developer Technologies MVP

# Ihr Partner für Microsoft Azure & AI



## Cloud Native Entwicklung

Konzeption und Entwicklung von nachhaltigen und intelligenten Anwendungen.



## Platform Engineering

Planung, Implementierung und Betrieb skalierbarer Anwendungsplattformen.



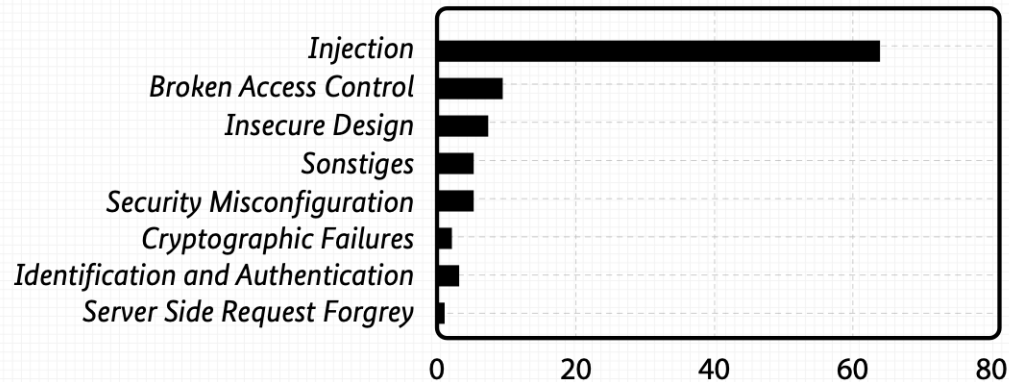
## Developer Productivity

Mehr Produktivität und Sicherheit durch KI und agile Prozesse.

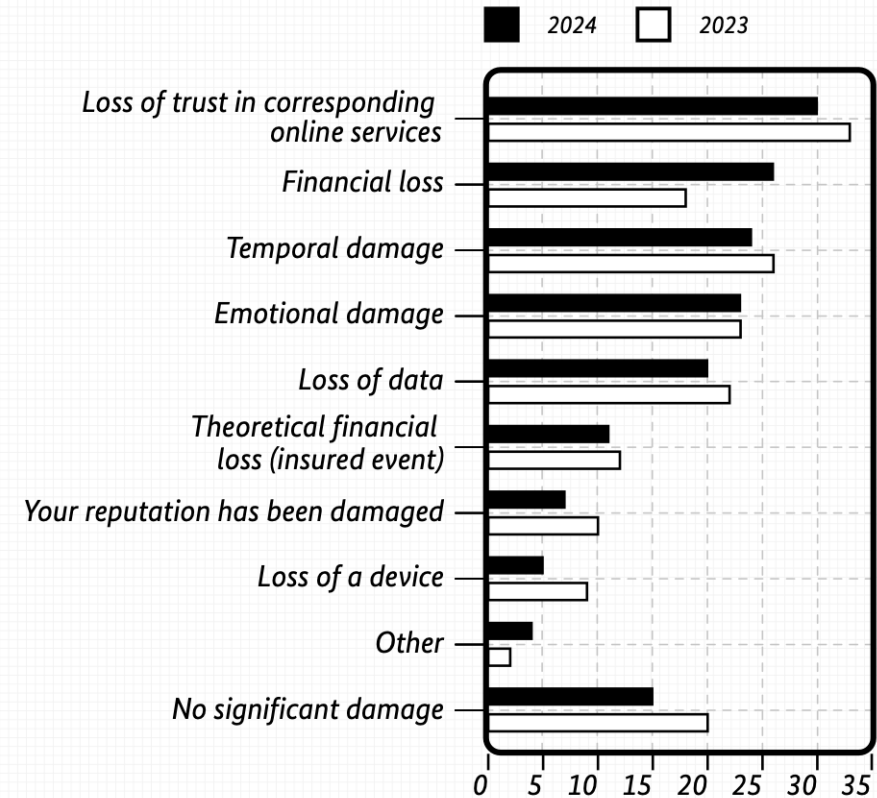
# State of security in Germany

## Notifications of products with vulnerabilities July 2023 to June 2024 by potential harmful impact

Share in %

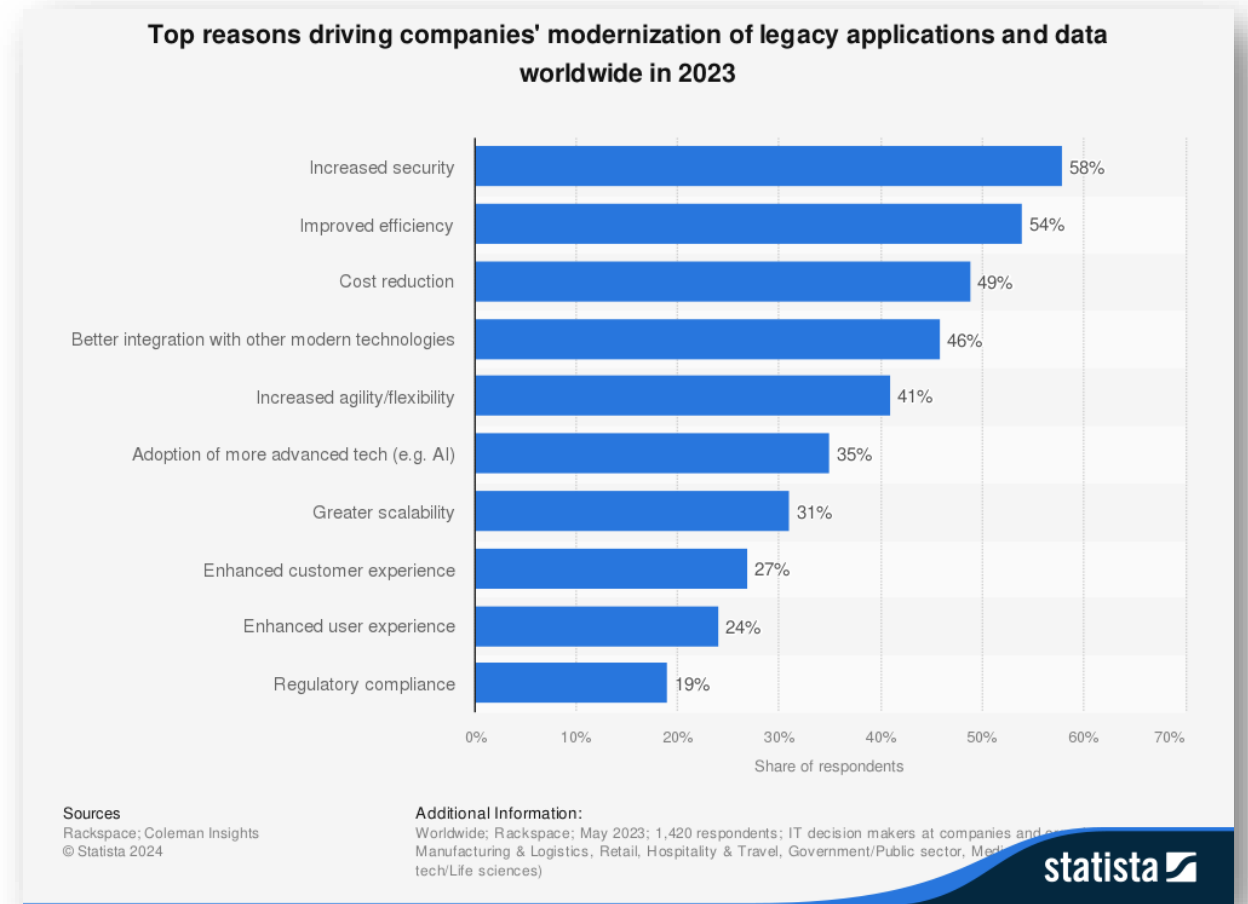


## Share in % of affected consumers



# Cloud-native as the fundamental basis

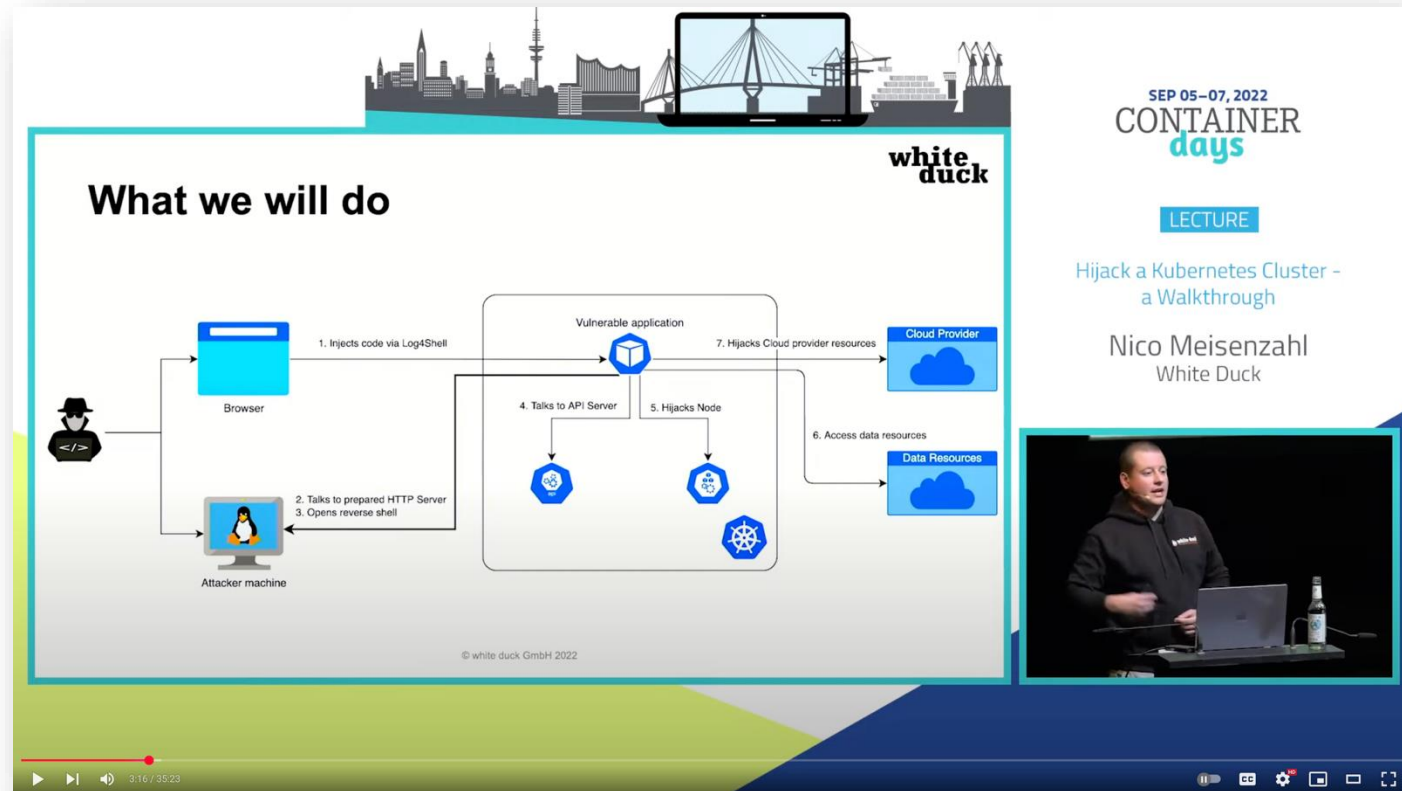
Gartner predicts that **by 2025, more than 95%** of all new digital apps will be delivered on cloud-native platforms, up from 30% in 2021. \*



\* Gartner, "Your Detailed Guide to the 2024 Gartner Top 10 Strategic Technology Trends"

# Example: Log4Shell

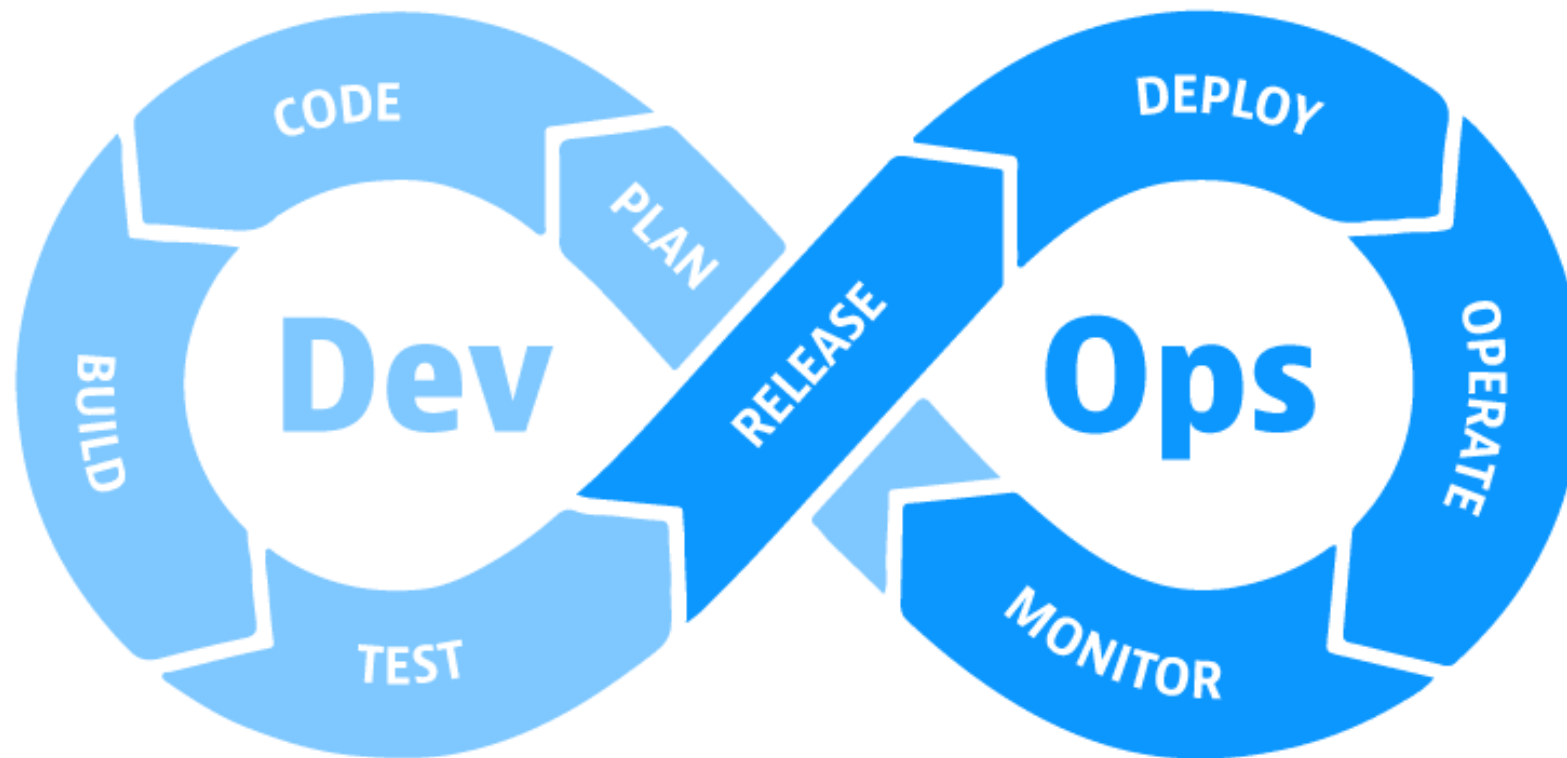
Log4Shell in a shared environment like Kubernetes can lead to gaining access to other applications, data or even unrelated cloud resources!



Hijack a Kubernetes Cluster – a Walkthrough

# DevSecOps

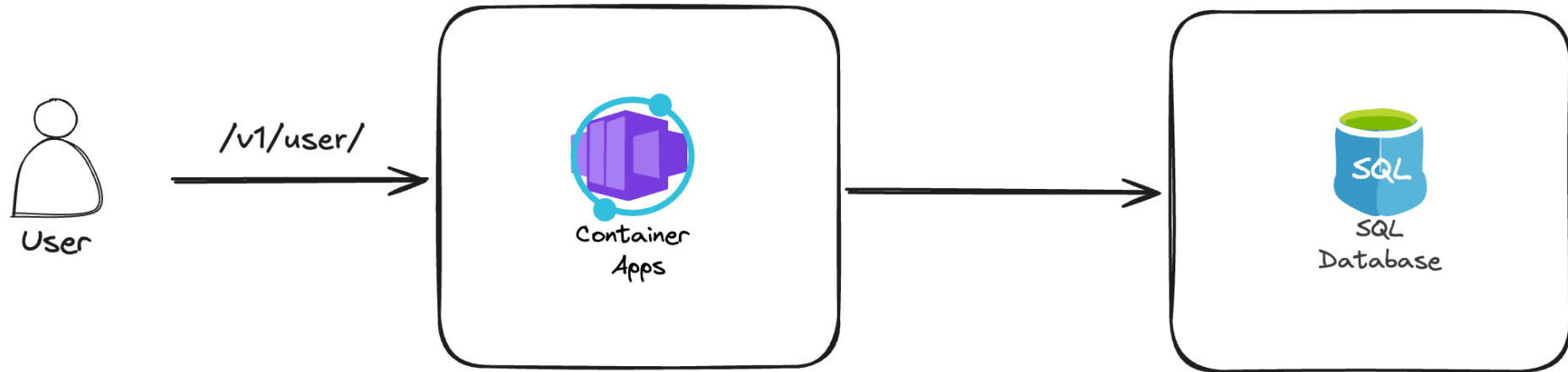
... is the **integration of security** within the whole DevOps process.



Picture source: <https://www.dynatrace.com>



# Today's demo application



# Dependencies

---

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

# Dependency awareness

- Software Bill of Materials (SBOM)
  - “List of ingredients” for all your software and dependencies
  - Baseline for vulnerability and licensing scanning
- SBOMs is the baseline for your dependency tracking
  - and therefore, vulnerability scanning
  - but can also track your dependency licenses
- Without it, you don’t have full visibility

Dependency graph

Dependencies Dependents Dependabot [Export SBOM](#)

Search all dependencies

57 Total Ecosystem

**actions/checkout** 3.\*.\*  
GitHub Actions · .github/workflows/docker-publish.yml · Detected automatically on May 18, 2025

**azure/login** 2.\*.\*  
GitHub Actions · .github/workflows/docker-publish.yml · Detected automatically on May 18, 2025

**docker/build-push-action** 3.\*.\*  
GitHub Actions · .github/workflows/docker-publish.yml · Detected automatically on May 18, 2025

**docker/login-action** 3.\*.\*  
GitHub Actions · .github/workflows/docker-publish.yml · Detected automatically on May 18, 2025

**docker/setup-buildx-action** 2.\*.\*  
GitHub Actions · .github/workflows/docker-publish.yml · Detected automatically on May 18, 2025

**github.com/Azure/azure-sdk-for-go/sdk/azcore** 1.18.0  
Go · src/api/go.mod · Detected automatically on May 18, 2025

**github.com/Azure/azure-sdk-for-go/sdk/azidentity** 1.10.0  
Go · src/api/go.mod · Detected automatically on May 18, 2025

**github.com/Azure/azure-sdk-for-go/sdk/internal** 1.11.1  
Go · src/api/go.mod · Detected automatically on May 18, 2025

**github.com/AzureAD/microsoft-authentication-library-for-go** 1.4.2  
Go · src/api/go.mod · Detected automatically on May 18, 2025

**github.com/bytedance/sonic** 1.11.6  
Go · src/api/go.mod · Detected automatically on May 18, 2025

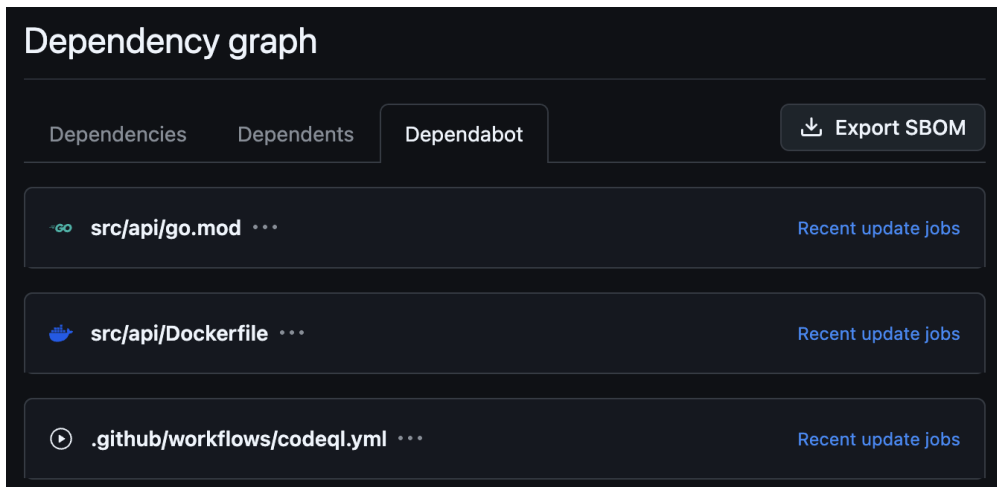
**github.com/bytedance/sonic/loader** 0.1.1  
Go · src/api/go.mod · Detected automatically on May 18, 2025

**github.com/cloudwego/base64x** 0.1.4  
Go · src/api/go.mod · Detected automatically on May 18, 2025

**github.com/cloudwego/iasm** 0.2.0

# Dependency updates

- Dependabot continuously monitoring dependencies
  - It creates pull requests to update outdated or vulnerable packages
- Open source: Renovate
  - <https://github.com/renovatebot/renovate>



The screenshot shows the 'Dependency graph' interface with three tabs: 'Dependencies', 'Dependents', and 'Dependabot'. The 'Dependabot' tab is active, showing a list of dependencies with their respective update jobs. The dependencies listed are:

- `src/api/go.mod` (Go icon) with a 'Recent update jobs' link.
- `src/api/Dockerfile` (Docker icon) with a 'Recent update jobs' link.
- `.github/workflows/codeql.yml` (GitHub Actions icon) with a 'Recent update jobs' link.

There is an 'Export SBOM' button in the top right corner of the graph view.

build(deps): Bump docker/setup-buildx-action from 2

[Open](#) dependabot wants to merge 1 commit into `main` from `dependabot/github_actions/docker/setup-buildx-action`

Conversation 0 Commits 1 Checks 4 Files changed 1



dependabot bot commented on behalf of github 7 minutes ago

Contributor ...

Bumps `docker/setup-buildx-action` from 2 to 3.

► Release notes

► Commits

compatibility 61%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

► Dependabot commands and options



`build(deps): Bump docker/setup-buildx-action from 2 to 3` [Verified](#) [41feccf](#)

dependabot bot added `dependencies` `github_actions` labels 7 minutes ago



✓ All checks have passed

4 successful checks

✓ No conflicts with base branch

Merging can be performed automatically.

Squash and merge

You can also merge this with the command line.

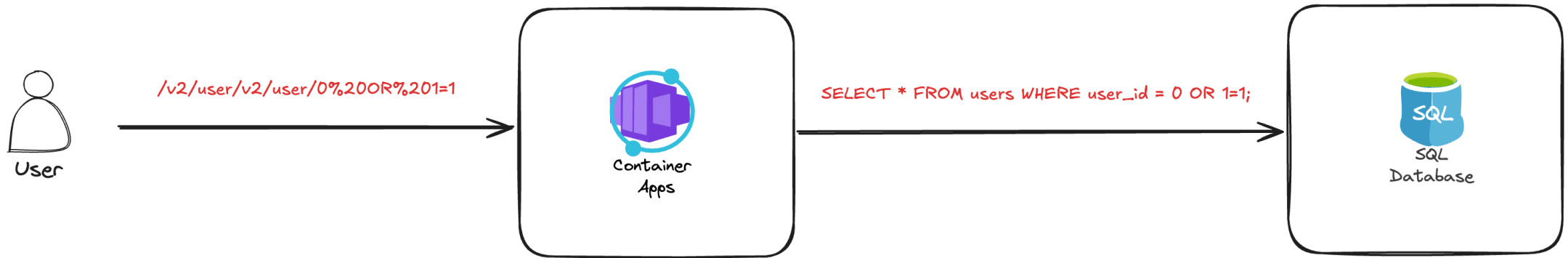
[View command line instructions.](#)

# Shift security left

---

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

# Example: SQL-injection



The `1=1` condition always evaluates to TRUE.  
As a result, the WHERE clause becomes irrelevant  
because of the OR condition.

# Early awareness with code analysis

- Enforce Static Application Security Testing (SAST) in PRs
  - scans your code to identify potential security vulnerabilities and secrets
- Implement automated Dynamic Application Security Testing (DAST)
  - black-box scanning against a running web application
- GitHub Advanced Security brings a fully-integrated SAST code scanning based on CodeQL
  - based on 2000 open-source policies and 13 years of research

feat: adds v2 api endpoint #8

Open nmeisenzahl wants to merge 11 commits into main from app-v2

Conversation 1 Commits 11 Checks 4 Files changed 10

nmeisenzahl commented 20 hours ago

No description provided.

feat: adds v2 api endpoint Unverified e22dd8f

github-advanced-security (bot) found potential problems 20 hours ago View reviewed changes

```
src/api/internal/db/db.go
122 +   utils.LogInfo(fmt.Sprintf("DB: GetUserV2 start idParam=%s", idParam))
123 +   // WARNING: directly concatenating user input into SQL query
124 +   query := fmt.Sprintf("SELECT id, name, email FROM users WHERE id = %s", idParam)
125 +   rows, err := db.conn.Query(query)
```

Check failure

Code scanning / CodeQL

Database query built from user-controlled sources High

This query depends on a user-provided value.

Show more details

Show paths Dismiss alert

Copilot Autofix AI about 21 hours ago

To fix the SQL injection vulnerability, the query should use parameterized queries instead of string concatenation. Parameterized queries ensure that user input is treated as data rather than executable code, preventing SQL injection attacks. Specifically:

1. Replace the `fmt.Sprintf`-based query construction with a query that uses placeholders (`@id`) for parameters.
2. Use `sql.Named` to safely bind the user-provided `idParam` to the query.

The changes will be made in the `GetUserV2` method in `src/api/internal/db/db.go`.

Suggested changeset 1

```
src/api/internal/db/db.go
... @@ -122,5 +122,4 @@
122 122   utils.LogInfo(fmt.Sprintf("DB: GetUserV2 start idParam=%s", idParam))
123 -   // WARNING: directly concatenating user input into SQL query
124 -   query := fmt.Sprintf("SELECT id, name, email FROM users WHERE id = %s",
125 -                       idParam)
125 +   query := "SELECT id, name, email FROM users WHERE id = @id"
126 +   rows, err := db.conn.Query(query, sql.Named("id", idParam))
126 125   if err != nil {
```

Copilot is powered by AI and may make mistakes. Always verify output.

Edit Commit suggestion

Reply...

# Full flexibility with open source

---

- Code scanning (SAST) based on your dev stack
  - [https://owasp.org/www-community/Source\\_Code\\_Analysis\\_Tools](https://owasp.org/www-community/Source_Code_Analysis_Tools)
- Code scanning for DevOps/Platform with trivy & checkov
  - <https://trivy.dev>
  - <https://www.checkov.io>
- Dependency tracking (SBOM) and vulnerability scanning with syft & gype
  - <https://github.com/anchore/syft>
  - <https://github.com/anchore/gype>

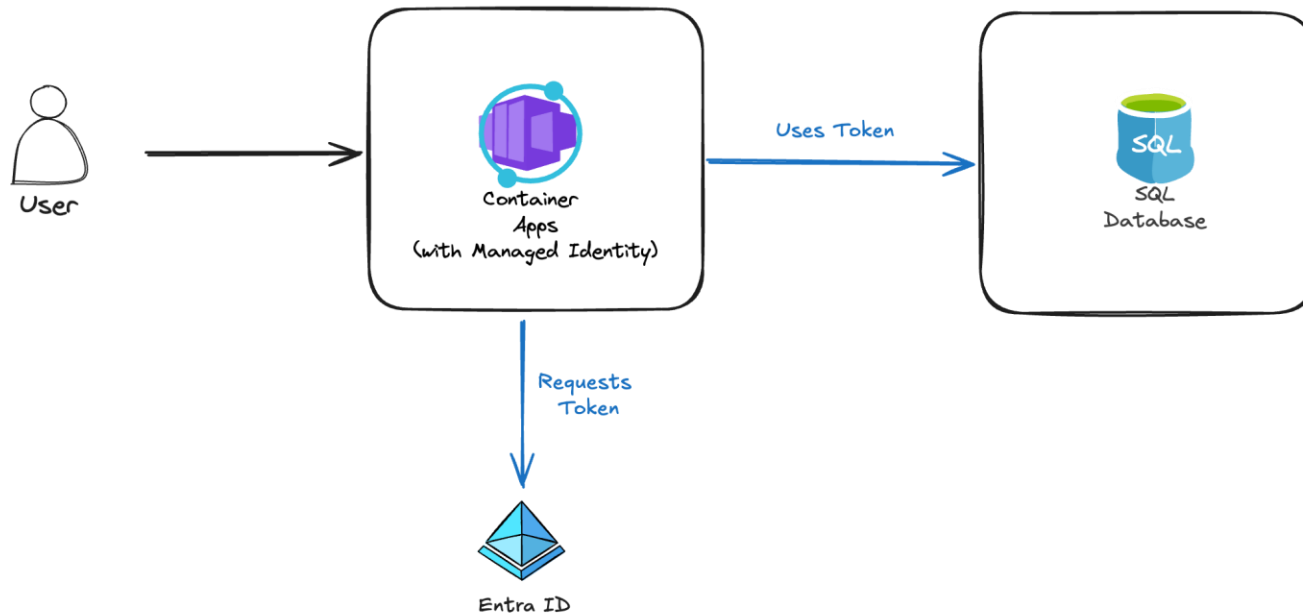


# Cloud-native architecture

---

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

# Managed identity for database access



```
// NewConnection creates a new DB using the provided context and config
func NewConnection(ctx context.Context, cfg *configs.Config) (*DB, error) {
    utils.LogInfo("DB: starting new connection")
    // Use values from external configurations to configure connection properties
    server := cfg.DBServer
    database := cfg.DBDatabase

    // Use Azure's DefaultAzureCredential for authentication
    cred, err := azidentity.NewDefaultAzureCredential(nil)
    if err != nil {
        utils.LogError(err)
        return nil, fmt.Errorf("failed to obtain Azure credential: %v", err)
    }

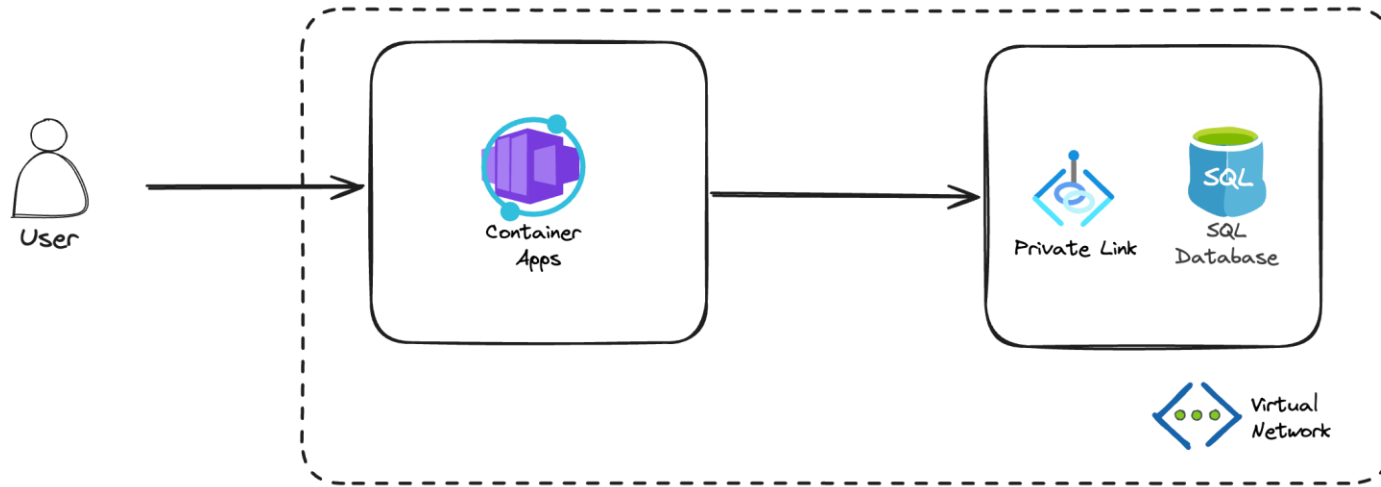
    // Build base connection string with Active Directory token authentication enforced
    baseConnStr := fmt.Sprintf("server=%s;database=%s;encrypt=true;authentication=ActiveD
    // Token provider using DefaultAzureCredential
    tokenProvider := func() (string, error) {
        tok, err := cred.GetToken(ctx, policy.TokenRequestOptions{
            Scopes: []string{"https://database.windows.net/.default"},
        })
        if err != nil {
            utils.LogError(err)
            return "", fmt.Errorf("failed to refresh Azure token: %v", err)
        }
        return tok.Token, nil
    }
    connector, err := mssql.NewAccessTokenConnector(baseConnStr, tokenProvider)
    if err != nil {
        utils.LogError(err)
        return nil, fmt.Errorf("failed to create token connector: %v", err)
    }
    conn := sql.OpenDB(connector)
```

# Authentication between Azure resources

---

- Relying on connection strings isn't the best idea
  - Long living secrets without rotation
  - Connections string needs to be stored and injected
- Managed Identity (Workload Identity) solves this issue
  - It is essentially a managed service principal living in your Entra ID
  - Relies on certificate-based with expiration of 90 days and rollover every 45 days
- There is a system-assigned and user-assigned option
- Abstracted via Azure SDK Azure.Identity library *"DefaultAzureCredential"*
  - Supports all credential types which is helpful for developer inner loop

# Private Link for database access



Enables the private access of Azure services in a vNet

- Public endpoints must be locked down separately!
- Increases security and performance

```
// Private Endpoint for SQL Server to allow private connectivity
You, 22 hours ago | 1 author (You)
resource "azurerm_private_endpoint" "sql_pe" {
  name                = "${var.prefix}-sql-pe"
  resource_group_name = azurerm_resource_group.rg.name
  location            = azurerm_resource_group.rg.location
  subnet_id           = azurerm_subnet.pe_subnet.id
}

You, 22 hours ago | 1 author (You)
private_service_connection {
  name                = "sql-psc"
  private_connection_resource_id = azurerm_mssql_server.sql.id
  subresource_names    = ["sqlServer"]
  is_manual_connection = false
}

// Private DNS Zone for SQL Private Endpoint resolution
You, 22 hours ago | 1 author (You)
resource "azurerm_private_dns_zone" "sql_zone" {
  name                = "privatelink.database.windows.net"
  resource_group_name = azurerm_resource_group.rg.name
}

// Link the Private DNS Zone to the VNet
You, 22 hours ago | 1 author (You)
resource "azurerm_private_dns_zone_virtual_network_link" "dns_link" {
  name                = "link-to-vnet"
  resource_group_name = azurerm_resource_group.rg.name
  private_dns_zone_name = azurerm_private_dns_zone.sql_zone.name
  virtual_network_id   = azurerm_virtual_network.vnet.id
}

// A record for SQL Private Endpoint to resolve server privately
You, 22 hours ago | 1 author (You)
resource "azurerm_private_dns_a_record" "sql_pe_record" {
  name                = azurerm_mssql_server.sql.name
  zone_name           = azurerm_private_dns_zone.sql_zone.name
  resource_group_name = azurerm_resource_group.rg.name
  ttl                 = 300
  records              = [azurerm_private_endpoint.sql_pe.private_service_connection[0].private_ip_address]
}
```

# Federated Credentials for GitHub Action authentication

```
▼ ✓ Azure Login using OIDC 5s
1 ▼Run azure/login@v2
2   with:
3     client-id: ***
4     tenant-id: ***
5     subscription-id: ***
6     enable-AzPSSession: false
7     environment: azurecloud
8     allow-no-subscriptions: false
9     audience: api://AzureADTokenExchange
10    auth-type: SERVICE_PRINCIPAL
11    env:
12      CONTAINER_APP_NAME: devsecops-app
13      RESOURCE_GROUP: devsecops-rg
14  Running Azure CLI Login.
15  /usr/bin/az cloud set -n azurecloud
16  Done setting cloud: "azurecloud"
17  Federated token details:
18  issuer - https://token.actions.githubusercontent.com
19  subject claim - repo:nmeisenzahl/devsecops-25:ref:refs/heads/main
20  audience - api://AzureADTokenExchange
21  job_workflow_ref - nmeisenzahl/devsecops-25/.github/workflows/docker-publish.yml@refs/heads/main
22  Attempting Azure CLI login by using OIDC...
23  Subscription is set successfully.
24  Azure CLI login succeeds by using OIDC.
```

```
// User-assigned identity for GitHub Actions with federated credentials
You, 2 days ago | 1 author (You)
resource "azurerm_user_assigned_identity" "github_actions" {
  name           = "${var.prefix}-uai-gh"
  location       = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
}

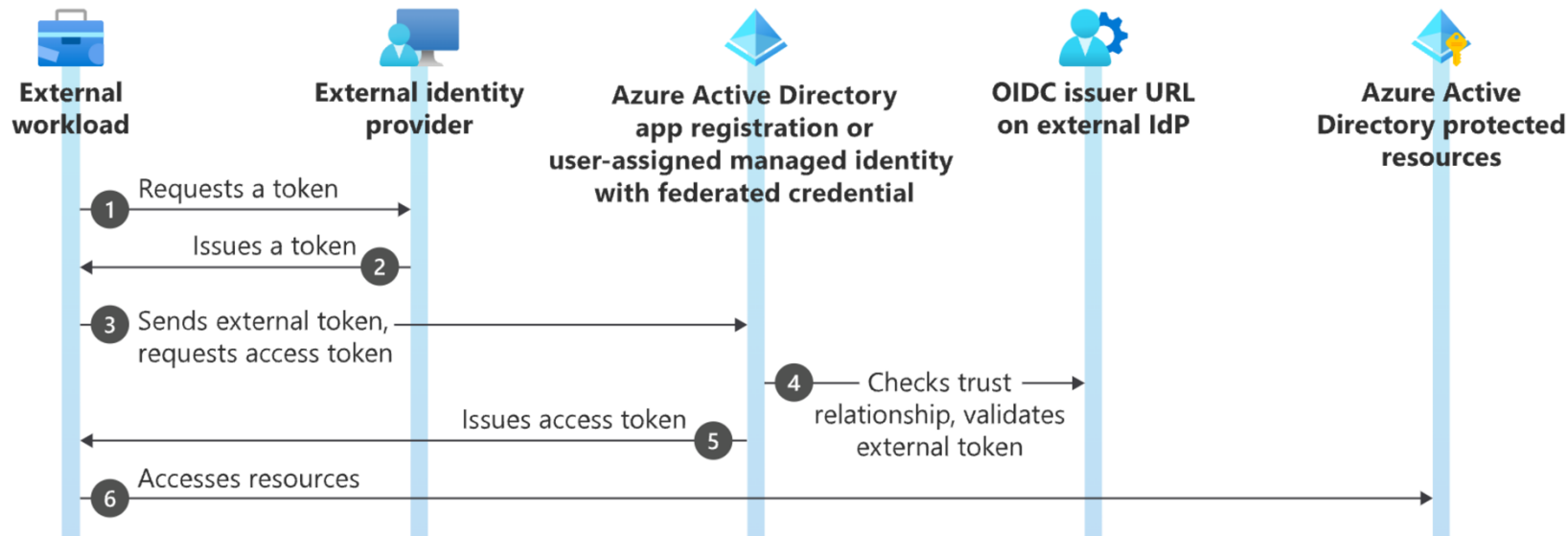
// Federated Identity Credential for GitHub Actions
You, 16 hours ago | 1 author (You)
resource "azurerm_federated_identity_credential" "github_actions" {
  name           = "${var.prefix}-fedcrd-gh"
  resource_group_name = azurerm_resource_group.rg.name
  parent_id      = azurerm_user_assigned_identity.github_actions.id
  audience       = ["api://AzureADTokenExchange"]
  issuer         = "https://token.actions.githubusercontent.com"
  subject        = var.oidc_subject // repo:nmeisenzahl/devsecops-25:ref:refs/heads/main
}

// Role Assignment for GitHub Actions identity in Resource Group
You, 2 days ago | 1 author (You)
resource "azurerm_role_assignment" "github_actions" {
  scope           = azurerm_resource_group.rg.id
  role_definition_name = "Contributor"
  principal_id    = azurerm_user_assigned_identity.github_actions.principal_id
}

// Managed identity for Application Gateway to access Key Vault
You, 17 hours ago | 1 author (You)
resource "azurerm_user_assigned_identity" "appgw_identity" {
  name           = "${var.prefix}-uai-agw"
  location       = azurerm_resource_group.rg.location
  resource_group_name = azurerm_resource_group.rg.name
}
```

# Securely authenticate with Azure services

- Entra ID Federated Credential can be used to authenticate with Azure services from third-party
  - Azure DevOps, GitHub Actions, GitLab, and other CI/CD solutions
  - Workload Identity with Azure Kubernetes Service
  - Basically, everything supporting OIDC (includes other cloud provider)

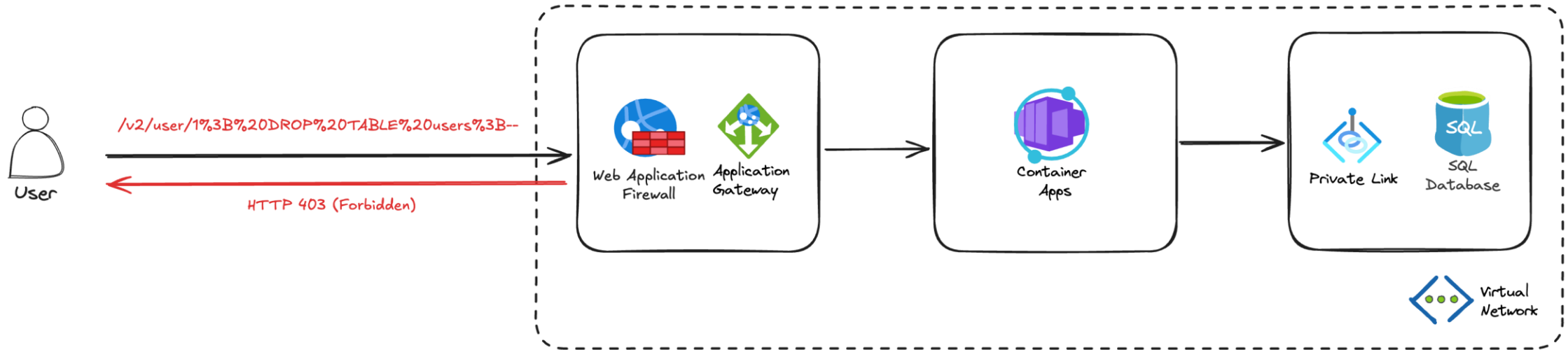


# Runtime security

---

Sichere Anwendungen durch Cloud-Native Technologien und DevSecOps

# Securely exposing the API



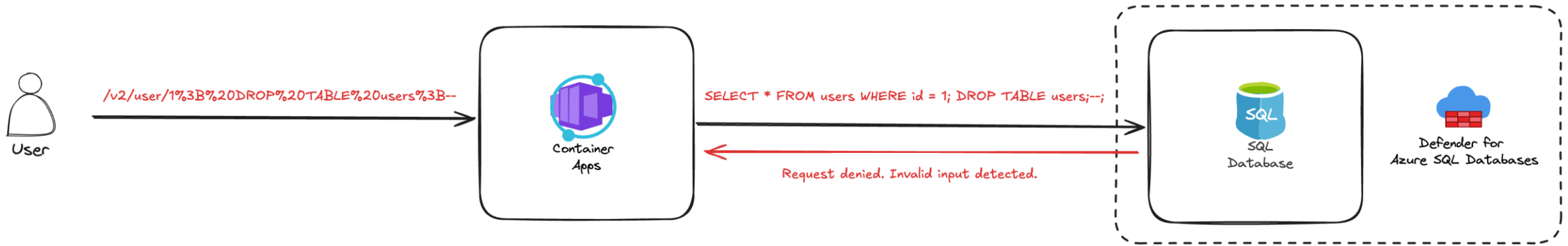


# Azure Web Application Firewall (WAF)

---

- A Web Application Firewall operates on Layer-7 (HTTP) and therefore helps with
  - Threat Detection for web-based attacks such as SQL injection, cross-site scripting (XSS), and other malicious payloads
  - Zero-Day Protection for newly discovered and unpatched vulnerabilities
  - Mitigate Layer-7 DDoS attack & Bot protection
- Managed Rule sets
  - “Core rule set” based on OWASP (Open Web Application Security Project) CRS
  - “Default rule set” based on OWASP and tuned by Microsoft Threat Intelligence team
- Custom rules based on your needs

# SQL runtime security

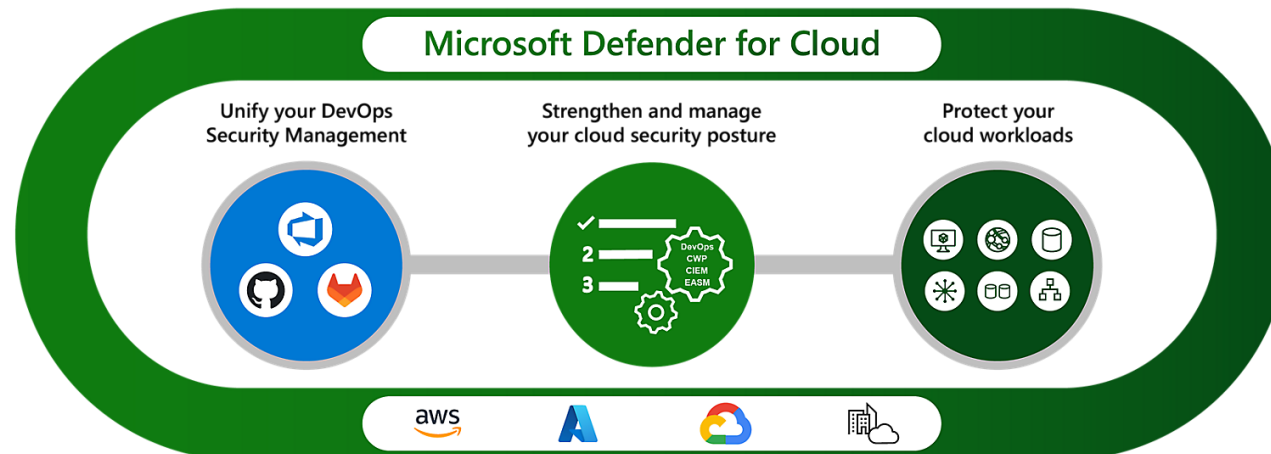


Defender for Azure SQL Databases monitors threats such as:

- Detects vulnerabilities caused by faulty SQL statements (SQL injection)
- Anomalous access patterns: Flags unusual activity like multiple failed sign-ins and brute force attacks

# Microsoft Defender for Cloud

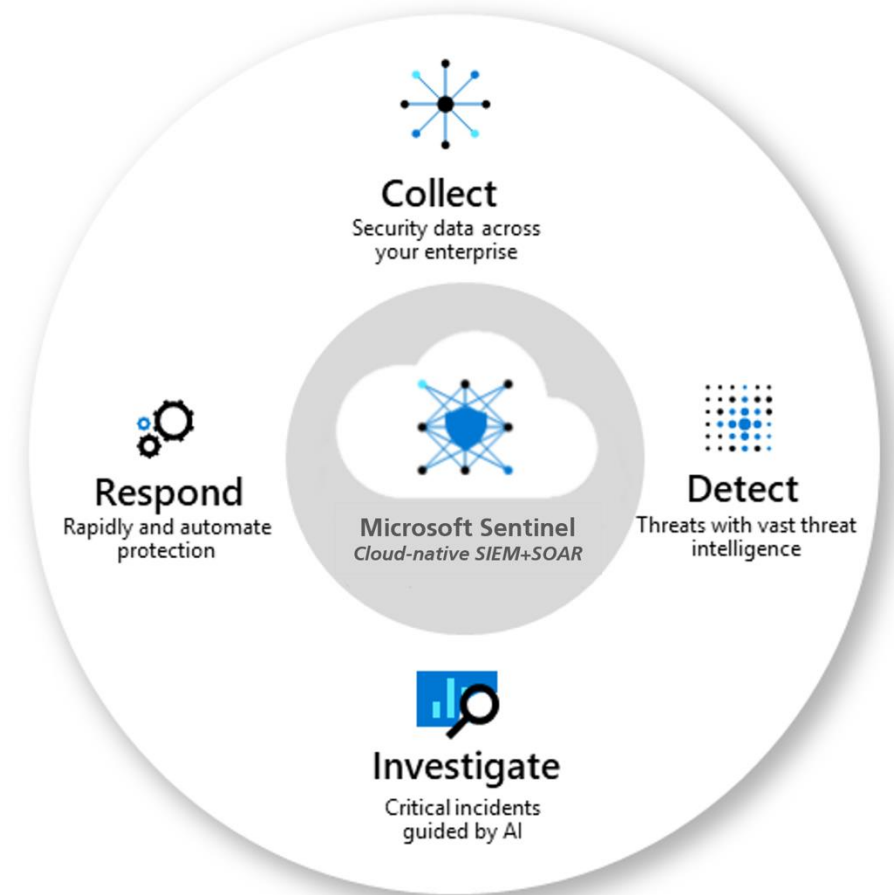
- A cloud-native application protection platform (CNAPP) that secures applications from cyber threats. It includes:
  - Unifies security management across code
  - Identifies preventative actions to avoid breaches (Cloud Security Posture Management)
  - Provides protection for Azure IaaS and PaaS (Cloud Workload Protection Platform)
- Provides a holistic view across multiple clouds and environments



# Microsoft Sentinel

---

- Provides cyberthreat detection, investigation, response, and proactive hunting, with a bird's-eye view across your enterprise
- Is a cloud-native security information and event management (SIEM) with SOAR (security orchestration, automation, and response) capabilities
- Integrates with the whole Microsoft stack as well as others



# How to get started?

- Think big, but start small – then review and iterate
- Enable your team for security awareness
- Abstract security into your CI process and enforce PR reviews
- Implement a zero-trust architecture
- Abstract security into a platform to scale



# Unsere Solution Assessments

*Ganzheitliche Analyse von Softwarelösungen und Cloud-Plattformen.*

## Unsere ersten Schritte bei neuen Kunden oder Projekten

- ✓ Einführung/Überblick und Anforderungserfassung
- ✓ Pain-Point-Analyse und Quick-Win-Implementierung
- ✓ Definition Ihrer Roadmap und weitere Zusammenarbeit



**Cloud-native  
Entwicklung mit KI**



**DevOps &  
Developer Productivity**



**Platform Engineering &  
Kubernetes**



**Nachhaltige  
Anwendungsentwicklung**



**Softwarehersteller &  
SaaS Anbieter**



**DevSecOps & Security**

# Gibt es Fragen?



**Nico Meisenzahl**  
**Geschäftsführer | COO**



+49 8031 230159-112



nico.meisenzahl@whiteduck.de



@nmeisenzahl



www.linkedin.com/in/nicomeisenzahl





**Vielen Dank!**