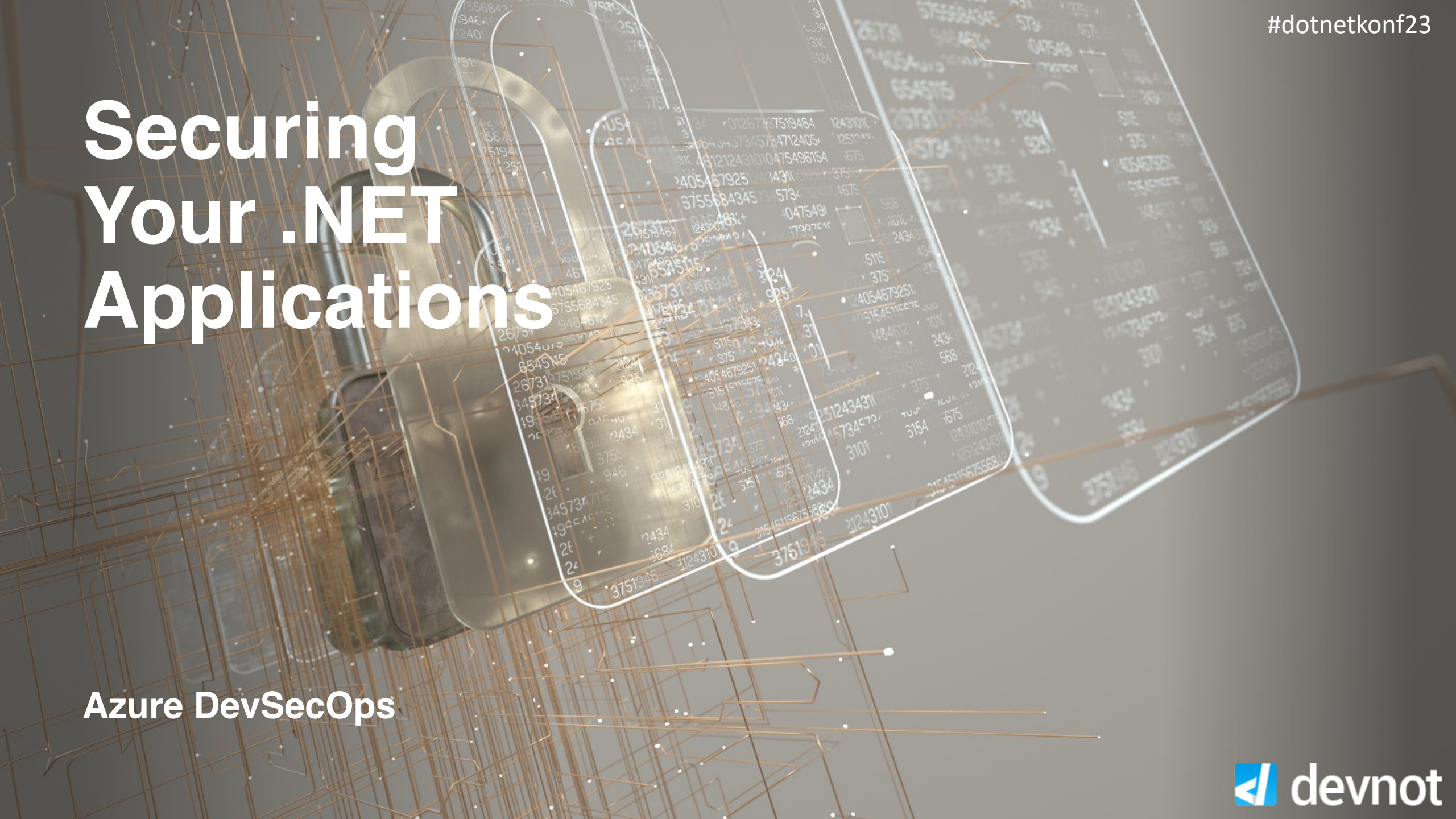
#dotnetkonf23

Securing Your .NET Applications



Azure DevSecOps

devnot

Microsoft® Most Valuable Professional

Mert Yeter

Cloud Solutions Architect

360 Dotnet

Certified Traefik Ambassador

Cloud Community Champion (2020)

@m3rtyeter

/in/mertyeter

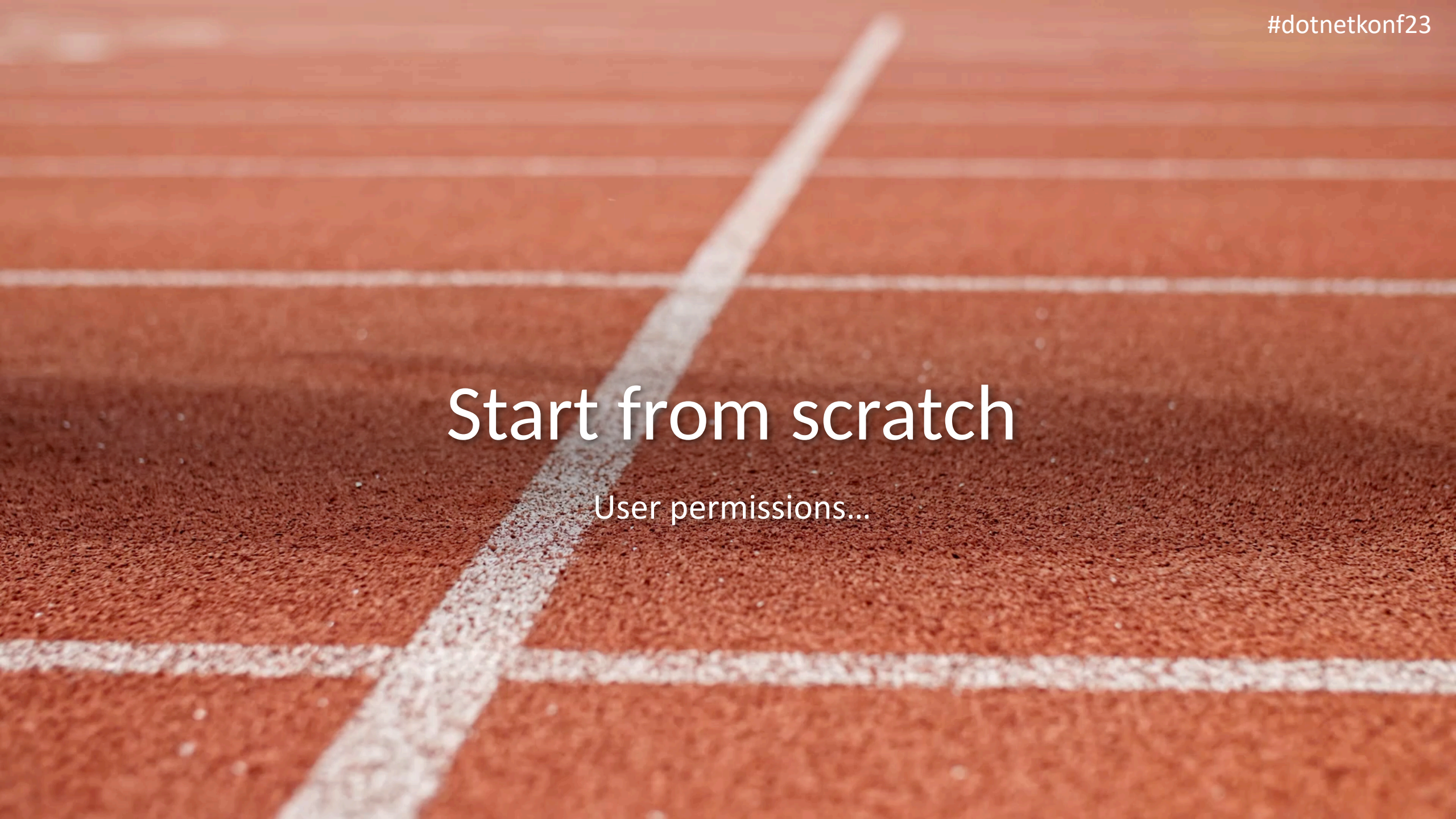
/mertyeter

/azureishlive
/yenimshowto
/TraefikLabsTurkey

/azureishlive
/mshowto
/traefikistanbul

AZUREISH Live!

msHOWTO ÇÖZÜM SANATTIR



Start from scratch

User permissions...

#dotnetkonf23

Project Settings
mshowto-dev

- General
  - Overview
  - Teams
  - Permissions
  - Notifications
  - Service hooks
  - Dashboards
- Boards
  - Project configuration
  - Team configuration
  - GitHub connections
- Pipelines
  - Agent pools
  - Parallel jobs
  - Settings
  - Test management
  - Release retention
  - Service connections
  - XAML build services
- Repos
  - Repositories
- Artifacts
  - Storage
- Test
  - Retention

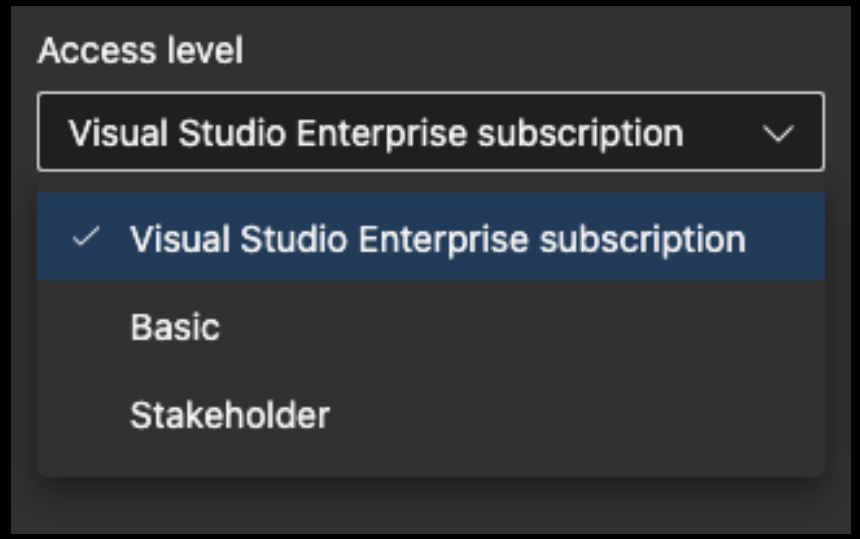
Permissions

Groups | Users

Total 9

Name	Description
BA Build Administrators	Members of this group can create, modify and delete build definitions and manage queued and
C Contributors	Members of this group can add, modify, and delete items within the team project.
EA Endpoint Administrators	Members of this group should include accounts for people who should be able to manage all the
EC Endpoint Creators	Members of this group should include accounts for people who can create service connections.
PA Project Administrators	Members of this group can perform all operations in the team project.
PU Project Valid Users	Members of this group have access to the team project.
R Readers	Members of this group have access to the team project.
RA Release Administrators	Members of this group can perform all operations on Release Management
MT mshowto-dev Team	The default project team.

Organization Settings /
General /
Users



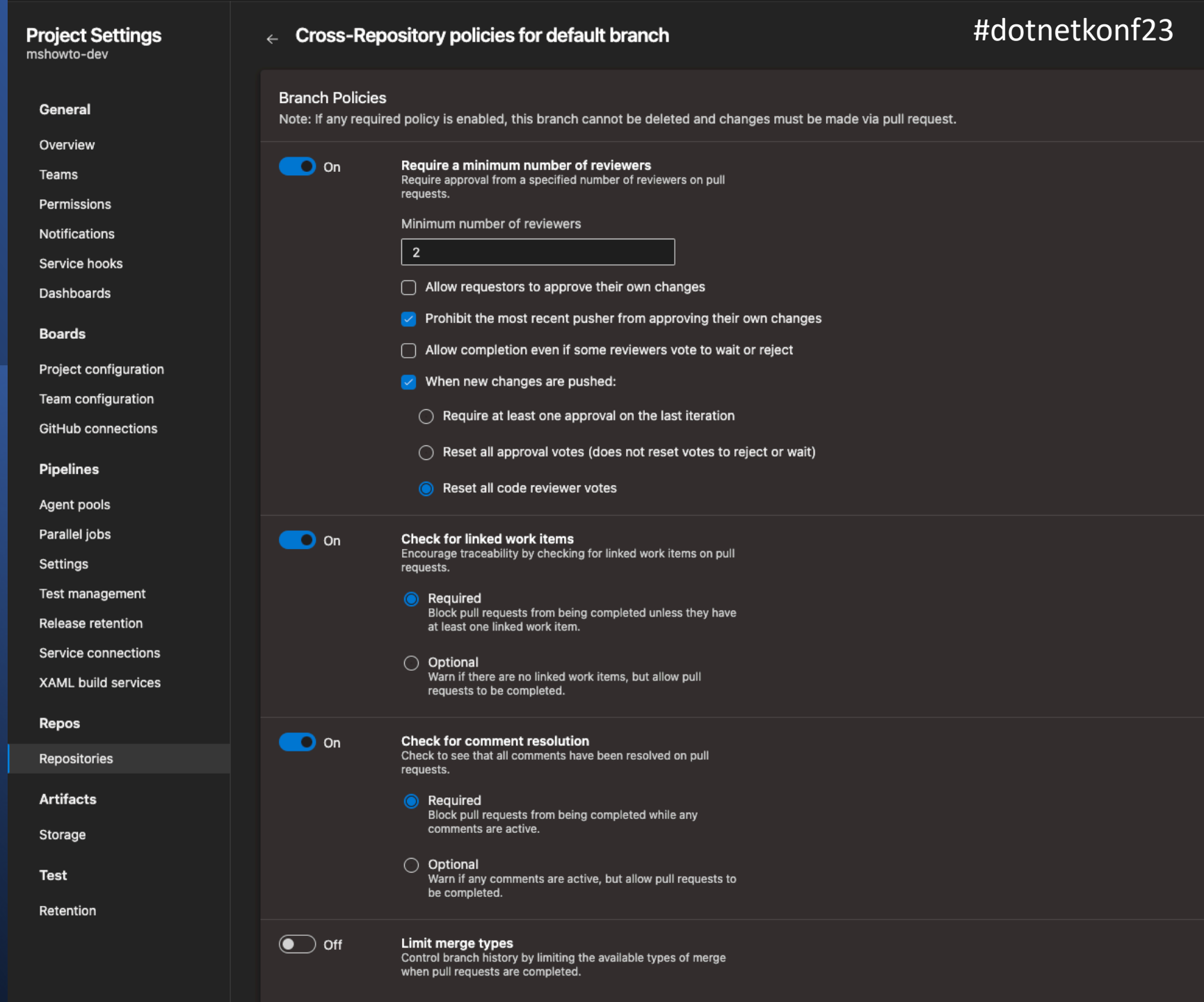
Feature	Stakeholder	Basic & Visual Studio Professional	Basic + Test Plans & Visual Studio Enterprise
Administer organization Can configure resources when also added to a security group or role: team administrator, Project Administrator, or Project Collection Administrator.	✓	✓	✓
Advanced backlog and sprint planning tools Includes full access to all backlog and sprint planning tools.		✓	✓
Advanced home page Includes access to projects, work items, and pull requests defined across projects you work in.		✓	✓
Advanced portfolio management Includes full access to define features and epics from a portfolio backlog or Kanban board.		✓	✓
Agile boards Stakeholders have limited access to Kanban boards and Taskboards. Stakeholders can add work items and update status through drag-and-drop, but can't update fields displayed on cards (except for the work item State) and can't view or set capacity.	✓	✓	✓
Agile Portfolio Management Includes limited access to portfolio backlogs and Kanban boards. Stakeholders can't change the backlog priority order, can't assign items to an iteration, use the mapping pane, or exercise forecasting.	✓	✓	✓
Artifacts Includes full access to all Azure Artifacts features, up to 2 GiB free storage.	✓	✓	✓
Author Release Pipelines and Manage Releases Includes defining release pipelines, multi-stage continuous deployment (CD) pipelines, and using approvals and gates to control deployments; when the **Free access to Pipelines Preview** feature is enabled, Stakeholders gain access to all Azure Pipelines features.		✓	✓
Basic backlog and sprint planning tools Includes limited access to add and modify items on backlogs and sprint backlogs and taskboards. Stakeholders can't assign items to an iteration, use the mapping pane, or forecasting.		✓	✓
Build Includes full access to all features to manage continuous integration and continuous delivery of software.		✓	✓
Chart Authoring Can create work tracking query charts.		✓	✓
Chart Viewing Can only view work tracking query charts. Stakeholders can't view query charts from the Queries page, however can view them when added to a dashboard.		✓	✓
Code Includes full access to all features to manage code using Git repositories or using Team Foundation Version Control (TFVC) Team Foundation Version Control (TFVC).		✓	✓
Delivery Plans Includes full access to add and view Delivery plans.		✓	✓
Request and Manage Feedback Includes full access to request and manage feedback on working software.		✓	✓
Standard Features Includes working across projects, View dashboards, View wikis, and Manage personal notifications. Stakeholders can't view Markdown README files defined for repositories and can only read wiki pages.	✓	✓	✓
Test services in build and release Includes running unit tests with your builds, reviewing, and analyzing test results.		✓	✓
Test Case Management Includes adding test plans and test suites, creating manual test cases, deleting test artifacts, and testing different configurations.			✓
Test Execution and Test Analysis Includes running manual, tracking test status, and automated tests.		✓	✓
Test summary access to Stakeholder license Includes requesting Stakeholder feedback using the Test & Feedback extension.	✓	✓	✓
View My Work Items Access to add and modify work items, follow work items, view and create queries, and submit, view, and change feedback responses. Stakeholders can only assign existing tags to work items (can't add new tags) and can only save queries under My Queries (can't save under Shared Queries).	✓	✓	✓
View Releases and Manage Approvals Includes viewing releases and approving releases; when the **Free access to Pipelines Preview** feature is enabled feature is enabled, Stakeholders gain access to all Azure Pipelines features.	✓	✓	✓

https://learn.microsoft.com/en-gb/azure/devops/organizations/security/access-levels?view=azure-devops

Branch policies

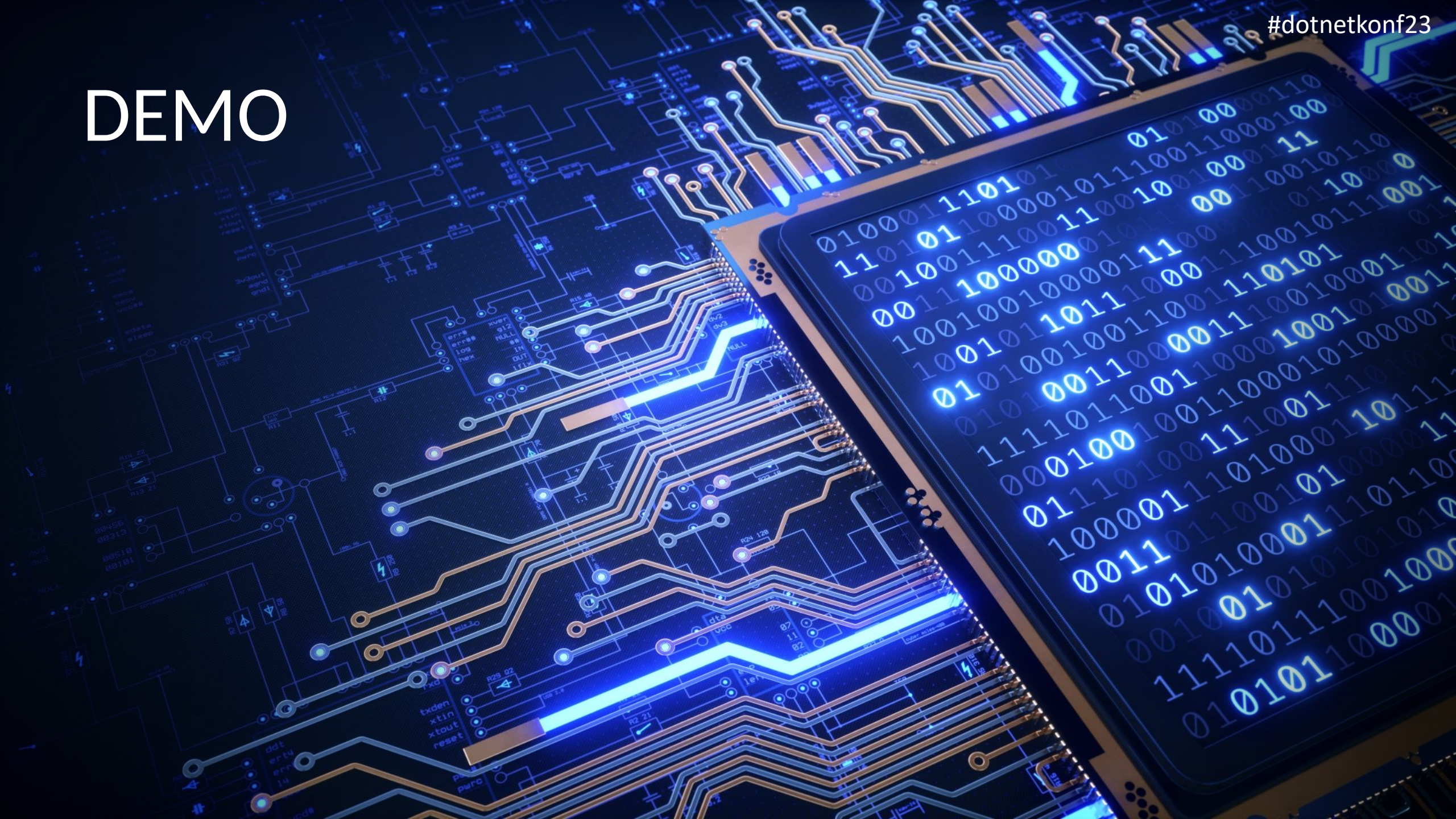
https://github.com/marketplace/actions/reward-for-own-pr-approval

Cross-Repository policies



Pipelines

DEMO



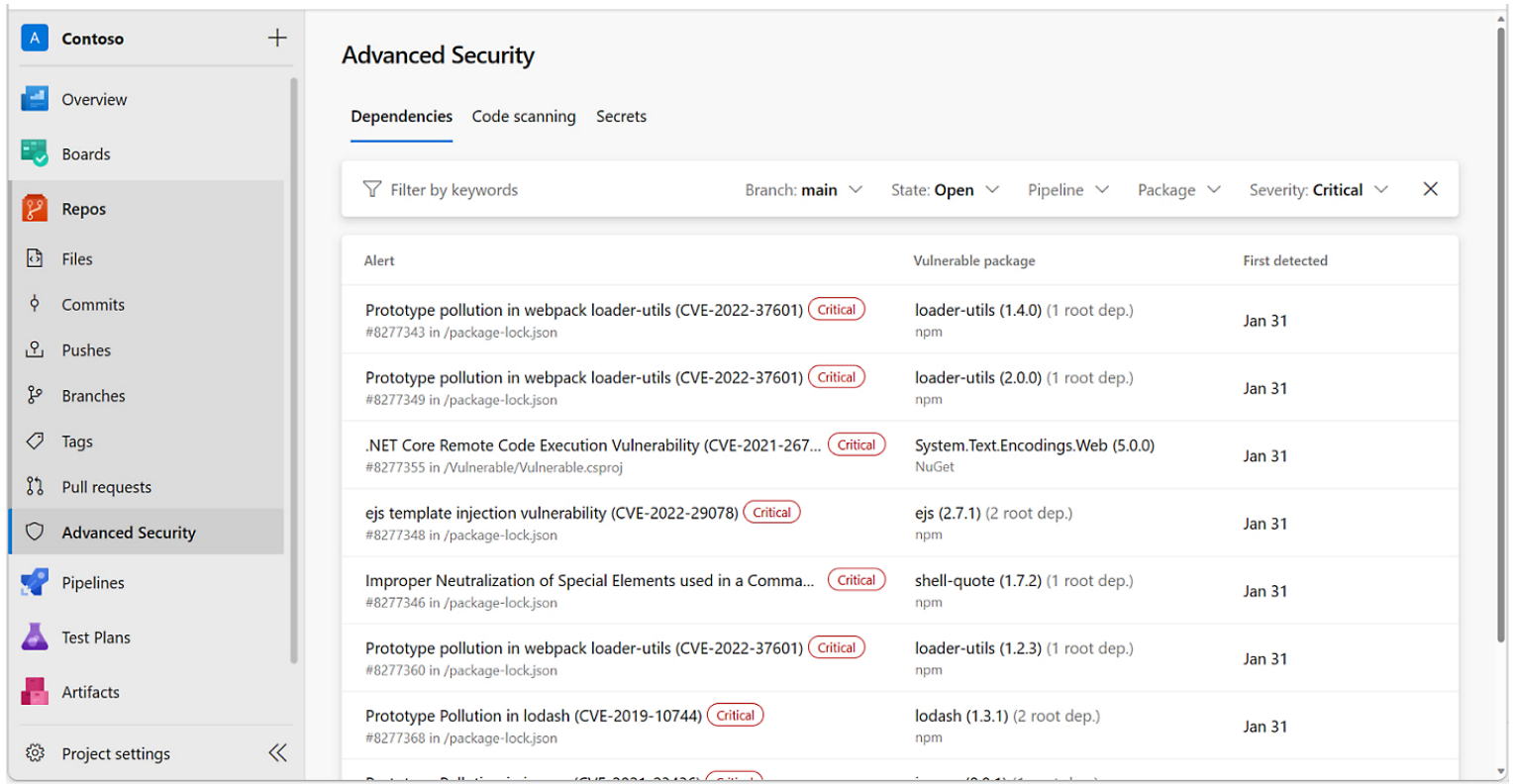
The Microsoft Security DevOps uses the following tools

Name	Language	License
AntiMalware	AntiMalware protection in Windows from Windows Defender, that scans source code and breaks the build if malware has been found	Not Open Source
Bandit	Python	Apache License 2.0
BinSkim	Binary--Windows, ELF	MIT License
Credscan	Credential Scanner (also known as CredScan) is a tool developed and maintained by Microsoft to identify credential leaks such as those in source code and configuration files common types: default passwords, SQL connection strings, Certificates with private keys	Not Open Source
ESlint	JavaScript	MIT License
Template Analyzer	ARM template, Bicep file	MIT License
Terrascan	Terraform (HCL2), Kubernetes (JSON/YAML), Helm v3, Kustomize, Dockerfiles, Cloud Formation	Apache License 2.0
Trivy	container images, file systems, git repositories	Apache License 2.0

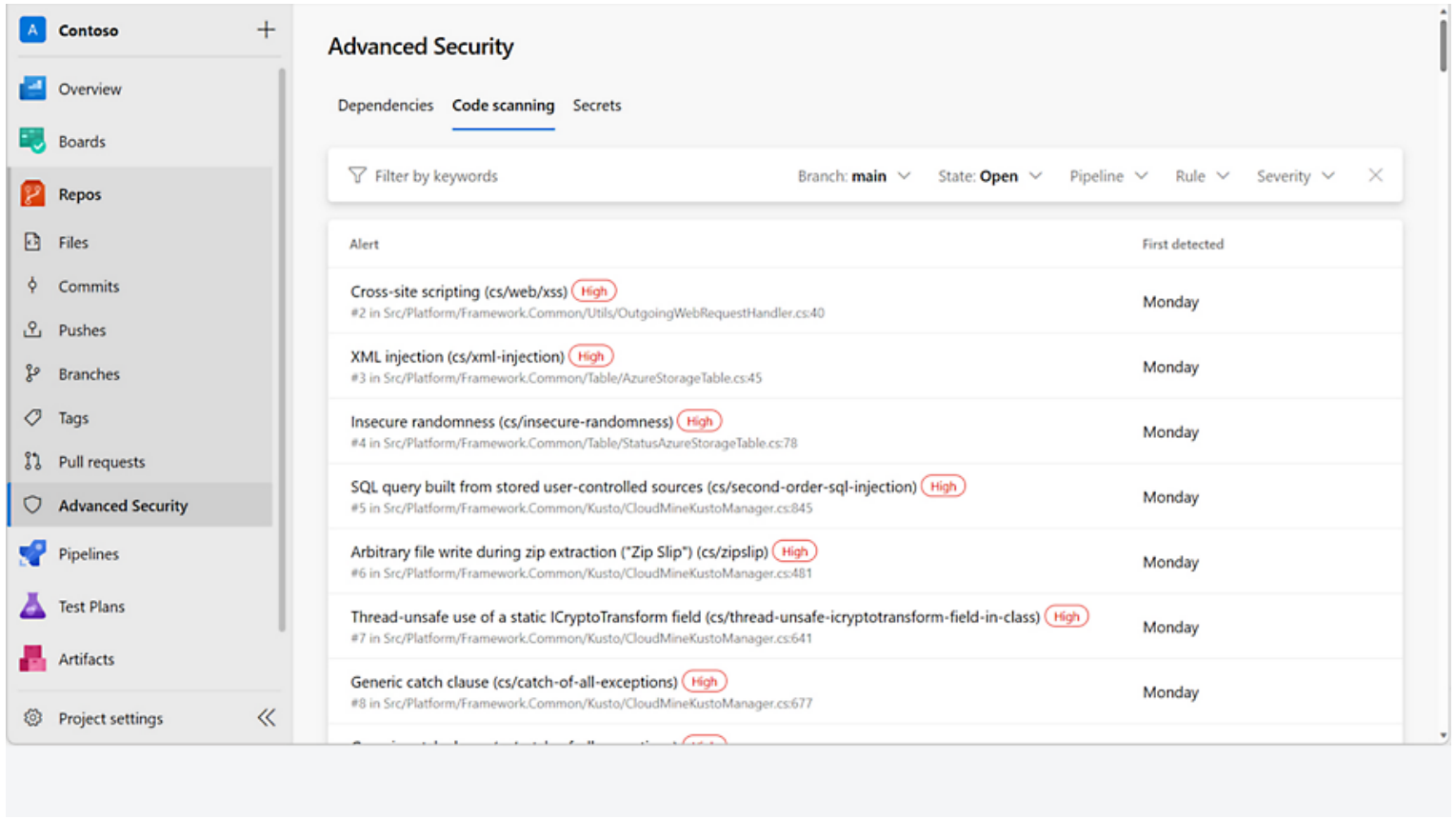
https://learn.microsoft.com/en-us/azure/defender-for-cloud/azure-devops-extension

GitHub Advanced Security for Azure DevOps *Preview*

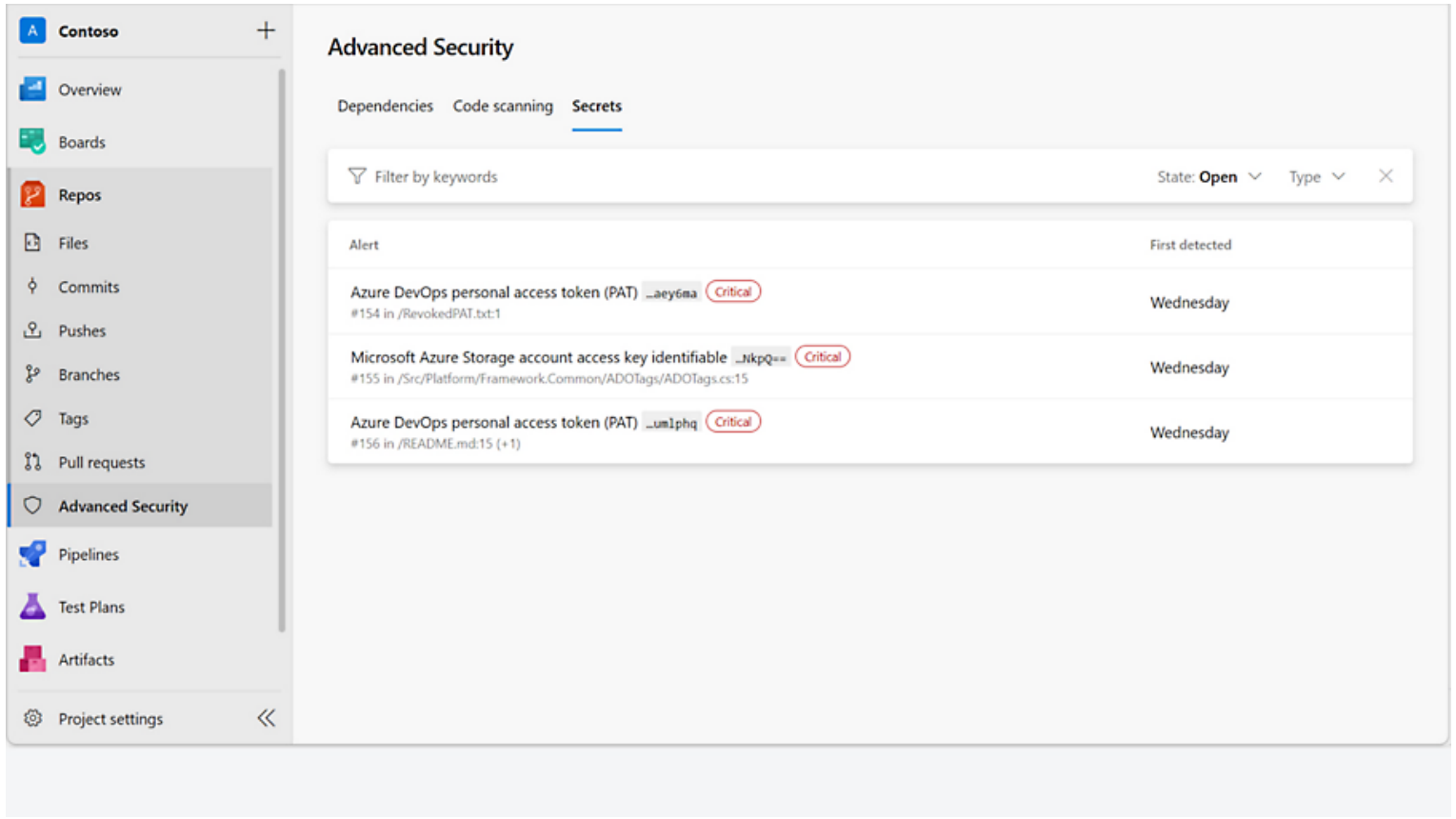
Advanced Security - Dependencies



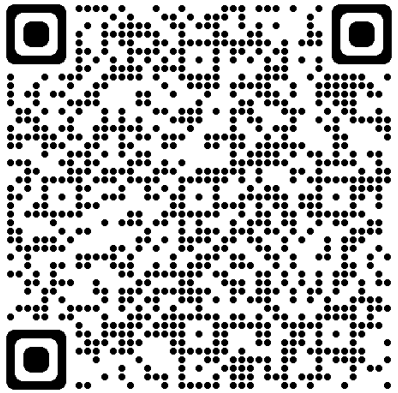
Advanced Security - Code Scanning



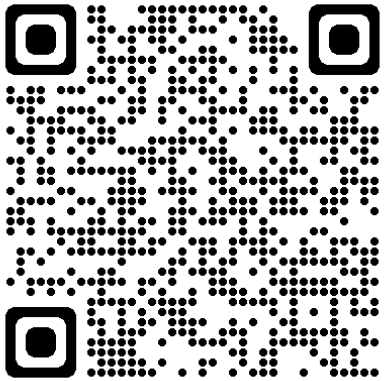
Advanced Security - Secrets



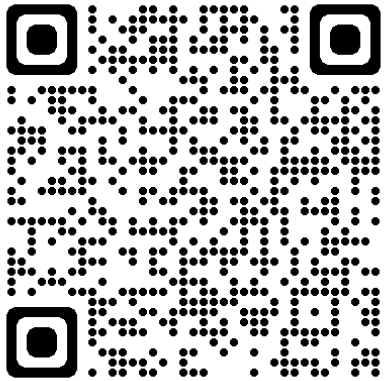
Resources



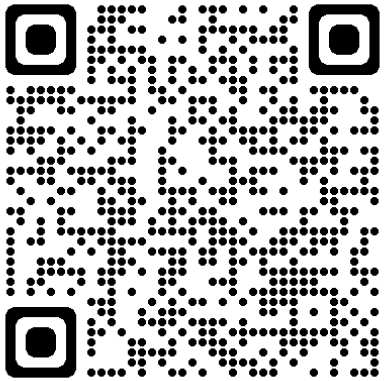
[Security, permissions, access, and billing Azure DevOps]



[Configure the Microsoft Security DevOps Azure DevOps extension]



[SonarQube 10.0]



[GitHub Advanced Security for Azure DevOps]