

Securing Your .NET Applications

Azure DevSecOps



@m3rtyeter



/in/mertyeter



/mertyeter



/azureishlive



/yenimshowto

/TraefikLabsTurkey



/azureishlive
/mshowto
/traefikistanbul

Mert Yeter

Cloud Solutions Architect

360 Dotnet



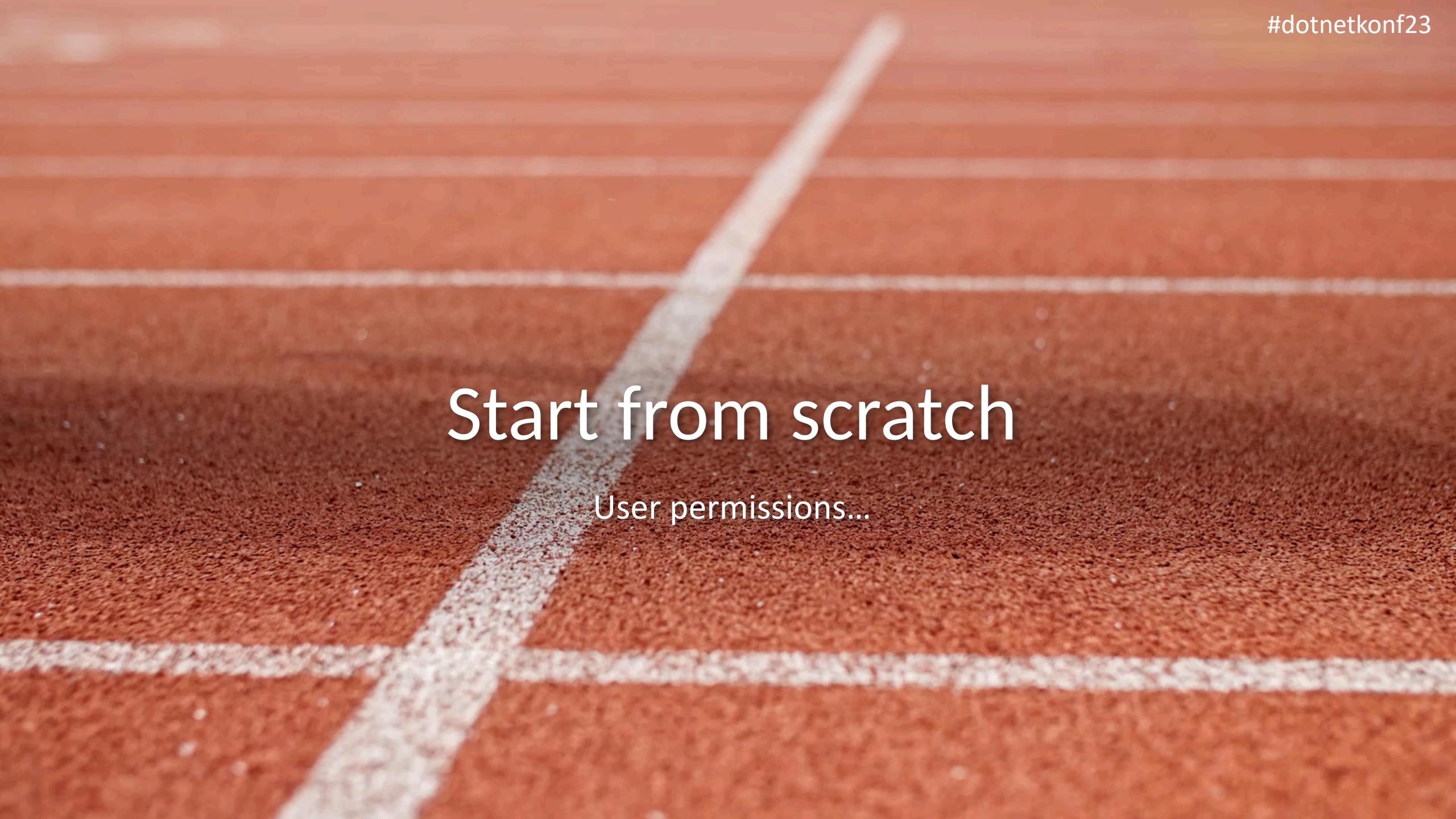
Certified
Traefik
Ambassador



Cloud
Community
Champion (2020)



msHOWTO
COZUM SANATTIR



Start from scratch

User permissions...

M

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

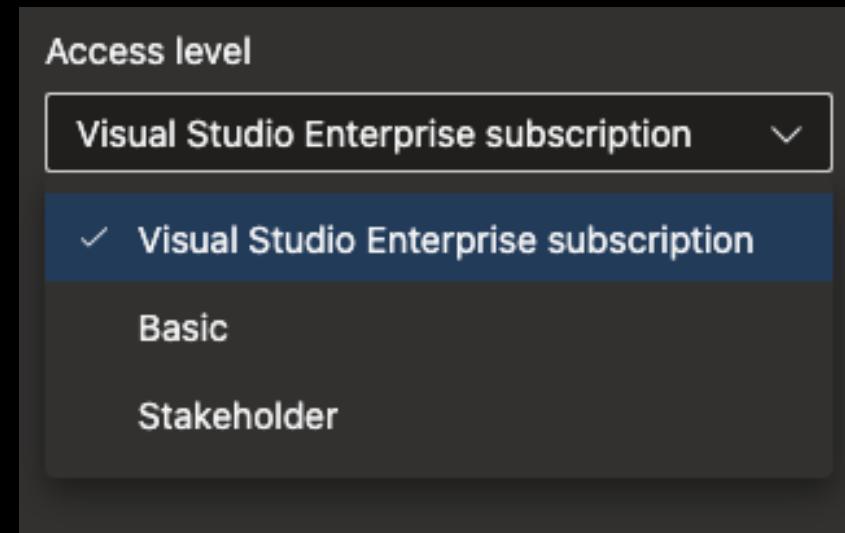
Permissions

Groups Users

Total 9

Name	Description
BA Build Administrators	Members of this group can create, modify and delete build definitions and manage queued and running builds.
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 endpoints used by the team.
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.	✓	✓	✓	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.	✓	✓	Test summary access to Stakeholder license Includes requesting Stakeholder feedback using the Test & Feedback extension .	✓
Advanced backlog and sprint planning tools Includes full access to all backlog and sprint planning tools.	✓	✓	Build Includes full access to all features to manage continuous integration and continuous delivery of software .	✓	✓	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).	✓	✓
Advanced home page Includes access to projects, work items, and pull requests defined across projects you work in .	✓	✓	Chart Authoring Can create work tracking query charts .	✓	✓	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.	✓	✓
Advanced portfolio management Includes full access to define features and epics from a portfolio backlog or Kanban board .	✓	✓	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.	✓	✓			
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 .	✓	✓	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).	✓	✓			
Agile Portfolio Management Includes limited access to portfolio backlog s 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.	✓	✓	Delivery Plans Includes full access to add and view Delivery plans.	✓	✓			
Artifacts Includes full access to all Azure Artifacts features, up to 2 GiB free storage.	✓	✓	Request and Manage Feedback Includes full access to request and manage feedback on working software.	✓	✓			
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.	✓	✓	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 .	✓	✓			

Branch policies



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

Cross-Repository policies

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](#)

← Cross-Repository policies for default branch

Branch Policies

Note: If any required policy is enabled, this branch cannot be deleted and changes must be made via pull request.

 On

Require a minimum number of reviewers

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

Minimum number of reviewers

- Allow requestors to approve their own changes
- Prohibit the most recent pusher from approving their own changes
- Allow completion even if some reviewers vote to wait or reject
- When new changes are pushed:
 - Require at least one approval on the last iteration
 - Reset all approval votes (does not reset votes to reject or wait)
 - Reset all code reviewer votes

 On

Check for linked work items

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

Required

Block pull requests from being completed unless they have at least one linked work item.

Optional

Warn if there are no linked work items, but allow pull requests to be completed.

 On

Check for comment resolution

Check to see that all comments have been resolved on pull requests.

Required

Block pull requests from being completed while any comments are active.

Optional

Warn if any comments are active, but allow pull requests to be completed.

 Off

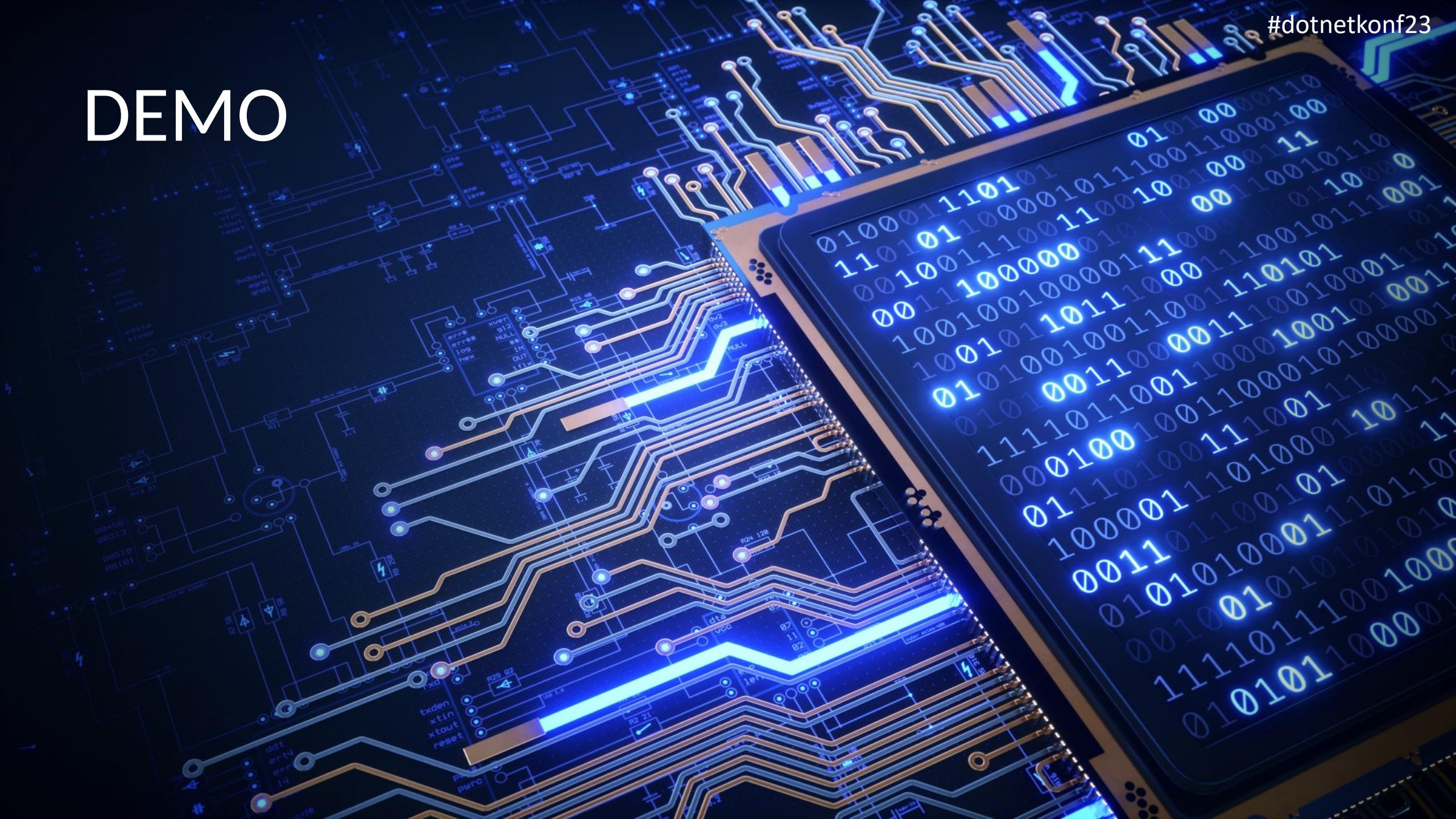
Limit merge types

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

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>

#dotnetkonf23

GitHub Advanced Security for Azure DevOps

Preview



Advanced Security - Dependencies

The screenshot shows the Azure DevOps interface for the 'Contoso' project. The left sidebar includes links for Overview, Boards, Repos, Files, Commits, Pushes, Branches, Tags, Pull requests, Advanced Security (which is selected), Pipelines, Test Plans, Artifacts, and Project settings. The main content area is titled 'Advanced Security' and has tabs for Dependencies, Code scanning, and Secrets. It features a search bar with filters for keywords, branch (main), state (Open), pipeline, package, and severity (Critical). A table lists several critical vulnerabilities:

Vulnerability Description	Severity	Affected Package	Last Detected
Prototype pollution in webpack loader-utils (CVE-2022-37601) #8277343 in /package-lock.json	Critical	loader-utils (1.4.0) (1 root dep.) npm	Jan 31
Prototype pollution in webpack loader-utils (CVE-2022-37601) #8277349 in /package-lock.json	Critical	loader-utils (2.0.0) (1 root dep.) npm	Jan 31
.NET Core Remote Code Execution Vulnerability (CVE-2021-267...) #8277355 in /Vulnerable/Vulnerable.csproj	Critical	System.Text.Encoding.Web (5.0.0) NuGet	Jan 31
ejs template injection vulnerability (CVE-2022-29078) #8277348 in /package-lock.json	Critical	ejs (2.7.1) (2 root dep.) npm	Jan 31
Improper Neutralization of Special Elements used in a Comma... #8277346 in /package-lock.json	Critical	shell-quote (1.7.2) (1 root dep.) npm	Jan 31
Prototype pollution in webpack loader-utils (CVE-2022-37601) #8277360 in /package-lock.json	Critical	loader-utils (1.2.3) (1 root dep.) npm	Jan 31
Prototype Pollution in lodash (CVE-2019-10744) #8277368 in /package-lock.json	Critical	lodash (1.3.1) (2 root dep.) npm	Jan 31

Advanced Security - Code Scanning

The screenshot shows the Microsoft DevOps interface for 'Contoso' under the 'Advanced Security' section. The 'Code scanning' tab is selected. A list of security alerts is displayed, each with a severity level (e.g., High) and a timestamp (e.g., Monday). The alerts include:

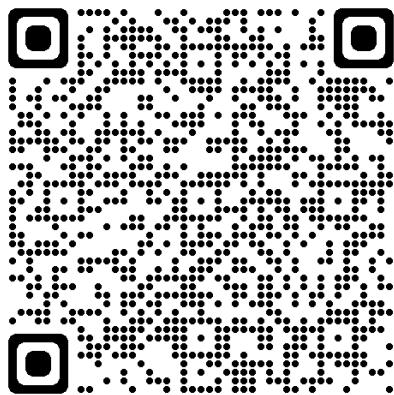
- Cross-site scripting (cs/web/xss) [High] #2 in Src/Platform/Framework.Common/Utils/OutgoingWebRequestHandler.cs:40
- XML injection (cs/xml-injection) [High] #3 in Src/Platform/Framework.Common/Table/AzureStorageTable.cs:45
- Insecure randomness (cs/insecure-randomness) [High] #4 in Src/Platform/Framework.Common/Table/StatusAzureStorageTable.cs:78
- SQL query built from stored user-controlled sources (cs/second-order-sql-injection) [High] #5 in Src/Platform/Framework.Common/Kusto/CloudMineKustoManager.cs:845
- Arbitrary file write during zip extraction ("Zip Slip") (cs/zipslip) [High] #6 in Src/Platform/Framework.Common/Kusto/CloudMineKustoManager.cs:481
- Thread-unsafe use of a static ICryptotransform field (cs/thread-unsafe-icryptotransform-field-in-class) [High] #7 in Src/Platform/Framework.Common/Kusto/CloudMineKustoManager.cs:641
- Generic catch clause (cs/catch-of-all-exceptions) [High] #8 in Src/Platform/Framework.Common/Kusto/CloudMineKustoManager.cs:677

Advanced Security - Secrets

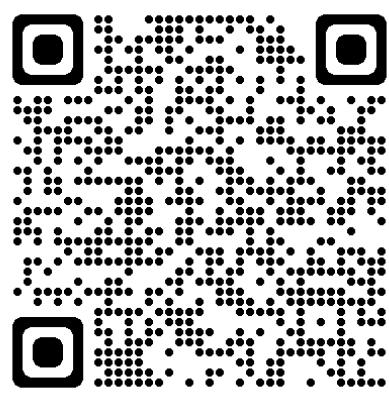
The screenshot shows the 'Advanced Security' page in the Azure DevOps interface, specifically the 'Secrets' tab. The left sidebar lists various project navigation options like Overview, Boards, Repos, and Advanced Security, which is currently selected. The main content area is titled 'Advanced Security' and displays three critical alerts under the 'Alerts' section. Each alert details a found secret, its type, and the date it was first detected.

Alert	First detected
Azure DevOps personal access token (PAT) <code>...aeylema</code> [Critical] #154 in /RevokedPAT.txt:1	Wednesday
Microsoft Azure Storage account access key identifiable <code>...NkpQ==</code> [Critical] #155 in /Src/Platform/Framework/Common/ADOTags/ADOTags.cs:15	Wednesday
Azure DevOps personal access token (PAT) <code>...um1phq</code> [Critical] #156 in /README.md:15 (+1)	Wednesday

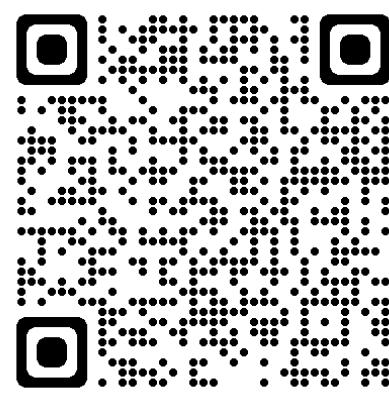
Resources



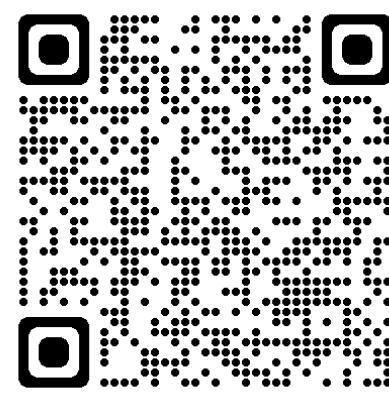
[Security, permissions, access,
and billing
Azure DevOps](#)



[Configure the Microsoft
Security DevOps Azure
DevOps extension](#)



[SonarQube 10.0](#)



[GitHub Advanced
Security for
Azure DevOps](#)