

A fluffy white dog is lying on a light-colored wooden desk. In the foreground, a portion of a laptop is visible. The background is blurred, showing what appears to be a living room or office setting.

Developing secure software with GitHub

Laura Kokkarinen & Thomas Vochten

Who are we?



Technology Evangelist, MVP

Thomas Vochten

De Cronos Groep, Belgium

@ThomasVochten



Software Architect, MVP

Laura Kokkarinen

Sulava, Finland

@LauraKokkarinen

Agenda

Protect against what?

Secure Software Development Lifecycle

Automating code security checks

Protecting source code and repositories

Defender for Cloud integration

What about Azure DevOps?

```
import java.util.ArrayList;
import java.util.Scanner;
import java.util.List;
import java.io.File;
import java.io.IOException;
import java.util.Arrays;
import java.io.IOException;

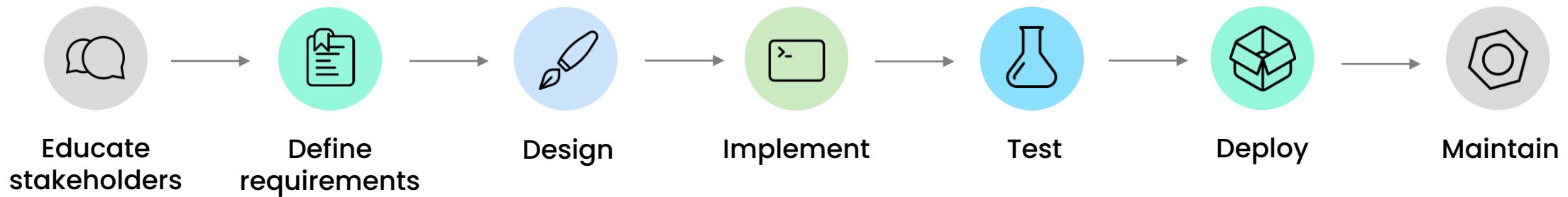
public class AirlineProblem {
    public static void main(String[] args){
        Scanner scannerToReadAirlines = null;
        try{
            scannerToReadAirlines = new Scanner(new File("airlines.txt"));
        } catch(IOException e){
            System.out.println("could not connect to file: " + e);
            System.exit(0);
        }
        if(scannerToReadAirlines != null){
            Scanner scannerFromKeyboard = new Scanner(System.in);
            ArrayList<Airline> airlinesPartnersNetwork = new ArrayList<Airline>();
            Airline newAirline;
            String lineFromFile;
            try{
                while( scannerToReadAirlines.hasNext() ){
                    lineFromFile = scannerToReadAirlines.nextLine();
                    airlineNames = lineFromFile.split(",");
                    newAirline = new Airline(airlineNames);
                    if(airlineNames != null){
                        airlinesPartnersNetwork.add( newAirline );
                    }
                }
            } catch(IOException e){
                System.out.println("could not read file: " + e);
            }
            System.out.println(airlinesPartnersNetwork);
            Scanner keyboard = new Scanner(System.in);
            System.out.print("Enter a new airline name: ");
            String newAirlineName = keyboard.nextLine();
            newAirline = new Airline(newAirlineName);
            airlinesPartnersNetwork.add( newAirline );
            System.out.println(airlinesPartnersNetwork);
        }
    }
}
```

OWASP Top 10

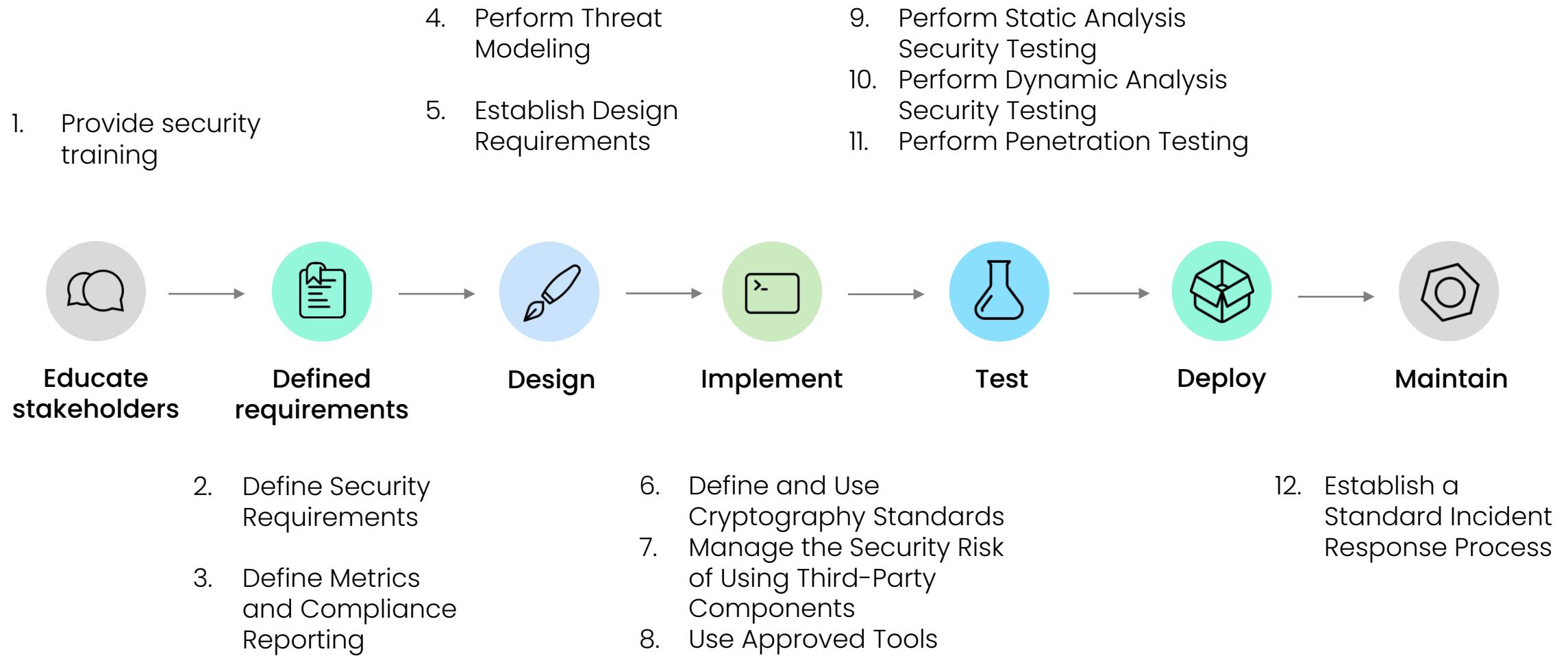


Secure Software Development Lifecycle (s-SDLC)

- Software development process that prioritizes security at every stage
- Framework



Microsoft Security Development Lifecycle (SDL)



Why is it important and what will you gain?

- Attacks targeting apps become ever more prevalent and sophisticated
- Initially requires additional resources but has ROI over long term



Reduced number of security vulnerabilities



Improved overall quality



Compliance with regulations and standards



Reduced development costs



Competitive advantage through reputation and customer trust



Improved customer satisfaction



When is it feasible to implement?

- Viable for all projects
- Ideally adopted from the very beginning



Business,
enterprise or
infrastructure
environment



Sensitive
information



Communicates
over a network

What steps can be automated?

- Often some manual work is combined with automation



Threat modeling



Code analysis



Security testing



Configuration scanning



Continuous
integration and
deployment



Incident response

UP NEXT

How can GitHub help us automate
steps during SDLC?

- **Automated testing is key**
 - Provide a baseline quality check
 - Avoid common mistakes or anti-patterns
 - Awareness of vulnerabilities
 - Consistency through CI/CD integration



- **Manual tests are still valuable**
 - Reviewing pull requests
 - Validation of design decisions
 - Applying common sense



GitHub to the rescue!



Secret
Scanning



Code
Scanning



Dependency
Scanning

Secret Scanning – What?



- Prevents exposing tokens, private keys or other secrets

- Scanning across all branches and git history

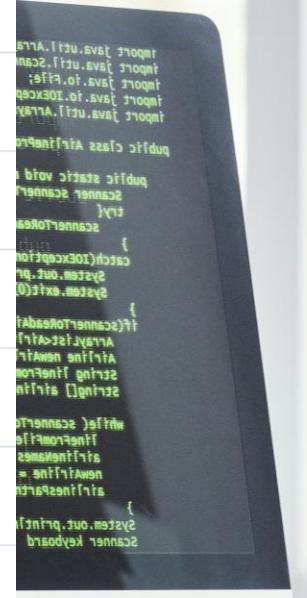
- Looks for patterns provided by the vendors

- Reported as alerts in the repository's Security tab

- Free for public repositories

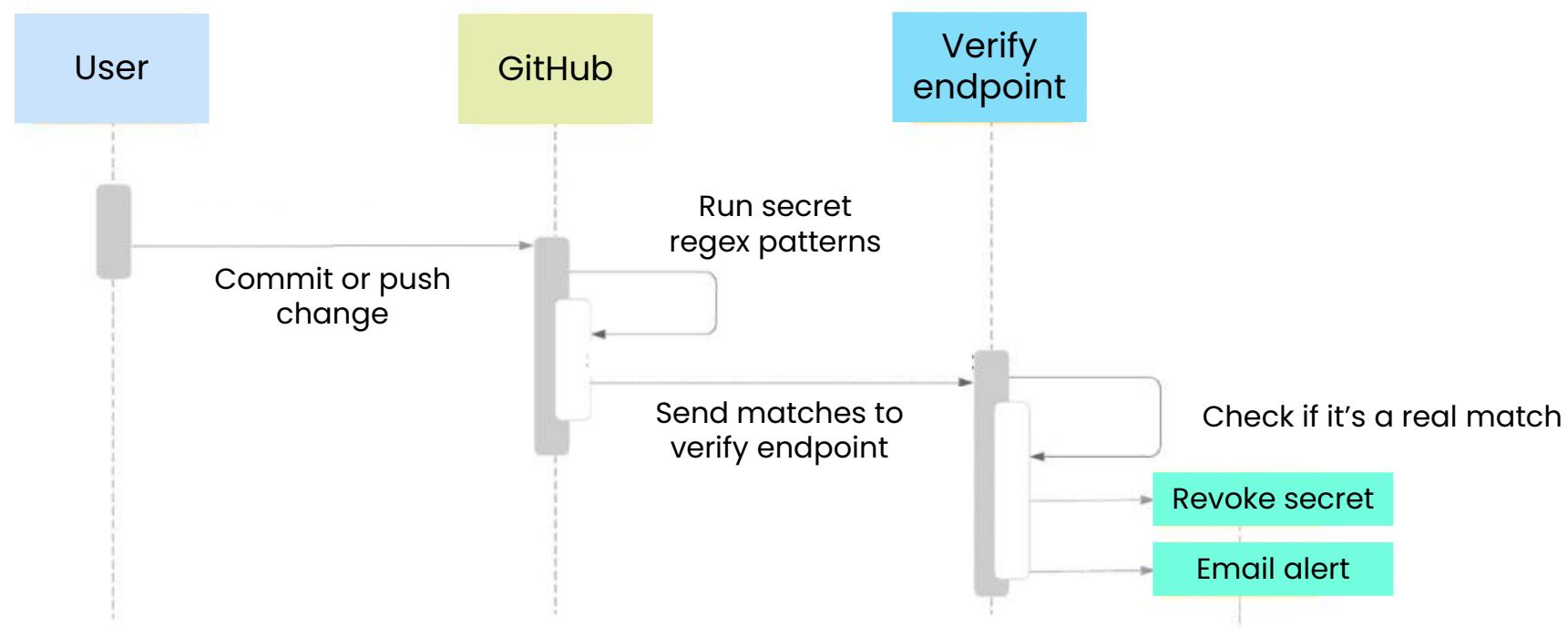
Secret Scanning Patterns

Azure	azure_active_directory_application_secret
Azure	azure_batch_key_identifiable
Azure	azure_cache_for_redis_access_key
Azure	azure_cosmosdb_key_identifiable
Azure	azure_devops_personal_access_token
Azure	azure_function_key
Azure	azure_ml_web_service_classic_identifiable_key
Azure	azure_sas_token
Azure	azure_search_admin_key
Azure	azure_search_query_key
Azure	azure_management_certificate
Azure	azure_sql_connection_string
Azure	azure_storage_account_key



Secret Scanning – Partner Program

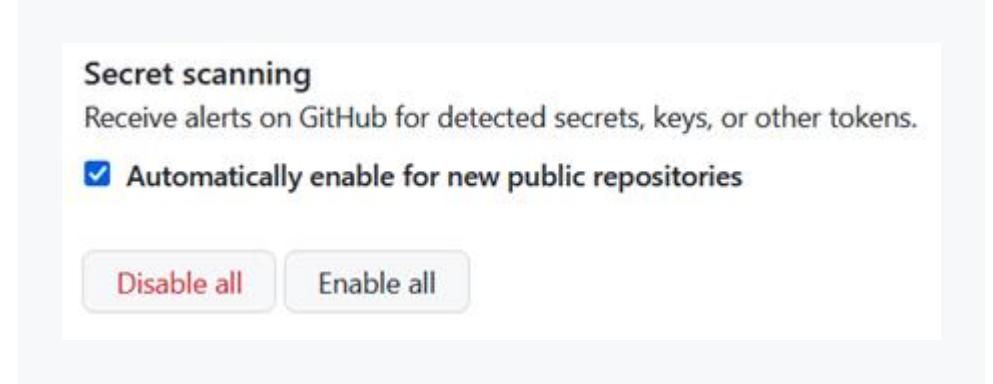
- Contributed by partners such as Microsoft
- Offers additional intelligence and automatic revoking of secrets (!)



Secret Scanning - Configuration

Scope

Enable secret scanning
for a single repository,
or on an account level



The screenshot shows the 'Secret scanning' configuration page on GitHub. It includes a checkbox for 'Automatically enable for new public repositories' which is checked, and buttons for 'Disable all' and 'Enable all'.

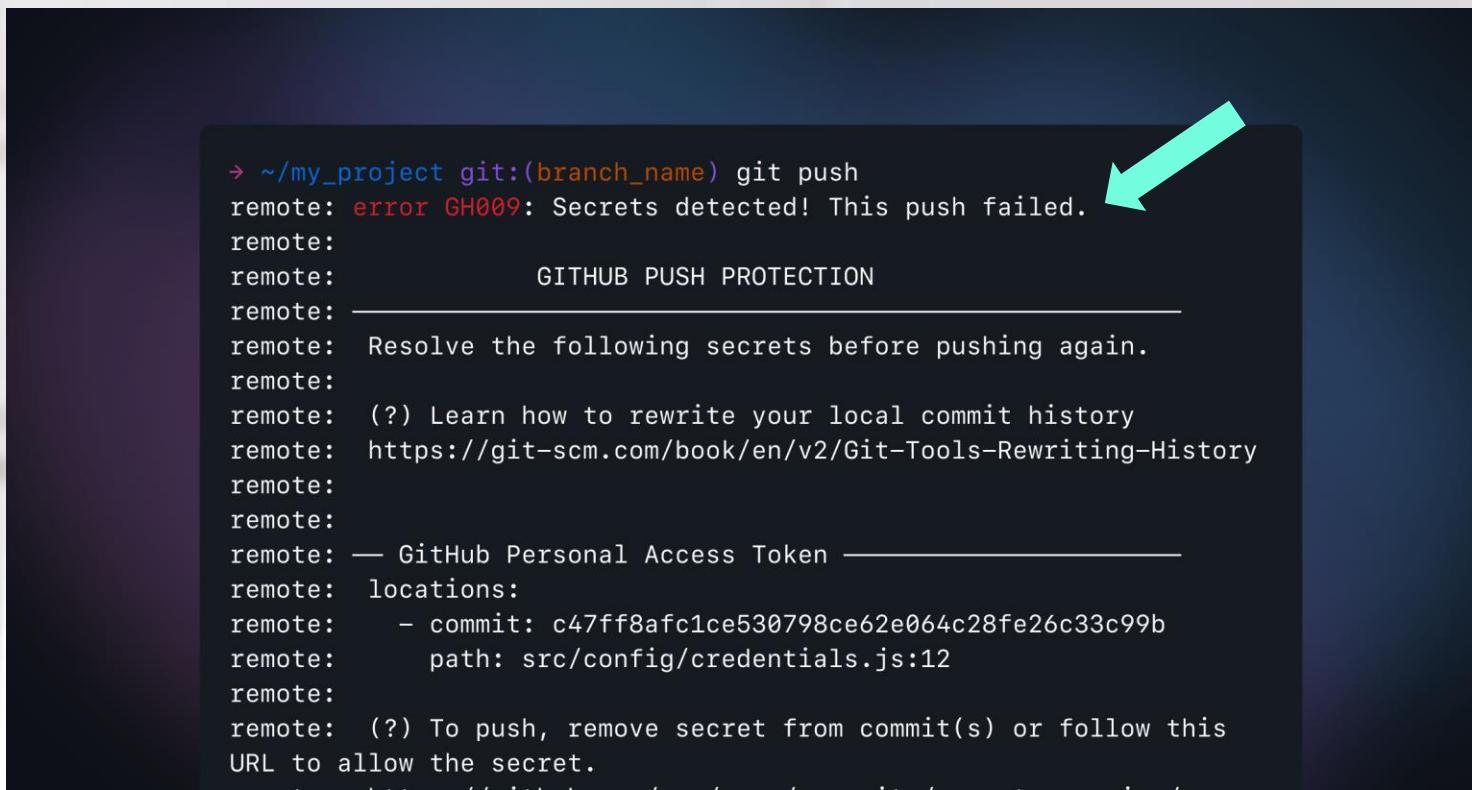
```
paths-ignore:
- "foo/bar/*.js"
```

Exclusions

You can exclude
directories through a
.github/secret_scanning
.yml file

Secret Scanning – Push Protection

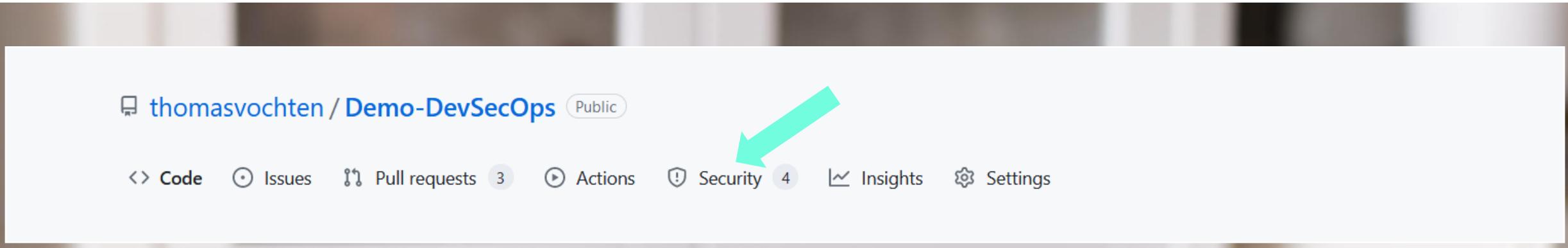
- Free for public repositories



```
→ ~/my_project git:(branch_name) git push
remote: error GH009: Secrets detected! This push failed. ←
remote:
remote:          GITHUB PUSH PROTECTION
remote: -----
remote: Resolve the following secrets before pushing again.
remote:
remote: (?) Learn how to rewrite your local commit history
remote: https://git-scm.com/book/en/v2/Git-Tools-Rewriting-History
remote:
remote:
remote: — GitHub Personal Access Token —
remote: locations:
remote:   - commit: c47ff8afc1ce530798ce62e064c28fe26c33c99b
remote:     path: src/config/credentials.js:12
remote:
remote: (?) To push, remove secret from commit(s) or follow this
remote: URL to allow the secret.
```

Secret Scanning – Alerting

- Alerts are sent to
 - Contributor who committed the secret
 - Repository administrators
 - Organization owners
- Only admins can dismiss secret scanning alerts



Secret Scanning – Alerting

Azure Storage Account Access Key

[Open](#) GitHub detected a secret 1 minute ago [Beta](#) Give us feedback

Possibly active secret

```
+eAwigsvbNxLb7Zc0xvgrHjuXE0oliYfNQb21rpeuFkENfuJ/abfDw1eOaSwIGOR1CIHWYGIXZx+AstJb4kqA==
```

Remediation steps
Follow the steps below before you close this alert.

- 1 Rotate the secret if it's in use to prevent breaking workflows.
- 2 Revoke this Azure Storage Account Access Key through Azure to prevent unauthorized access. [Learn more about Azure tokens](#).
- 3 Check security logs for potential breaches.
- 4 Close the alert as revoked.

Detected in 1 location

Program.cs

```
33 }  
34  
35 // Deliberately hardcoded secrets  
36 BlobServiceClient blobServiceClient = new BlobServiceClient("DefaultEndpointsProtocol=https;AccountName=thisivulnerablestorage;AccountKey=+eAwigsvbNxLb7Zc0xvgrHjuXE0oliYfNQb21rpeuFkENfuJ/abfDw1eOaSwIGOR1CIHWYGIXZx+AstJb4kqA==");  
37 blobServiceClient.GetBlobContainerClient("demo-devsecops").GetBlobClient("demo-devsecops.txt").DownloadTo("demo-devsecops.txt");  
38  
39
```

On a roll! [0e7a41d](#) 1 minute ago

GitHub opened this alert 1 minute ago

Secret Scanning – What now?

- How do I remove secrets from git history?
- Examples:

```
$ bfg --delete-files YOUR-FILE-WITH-SENSITIVE-DATA  
$ bfg --replace-text passwords.txt  
  
$ git push --force
```



Code Scanning – What?

Identify and fix security vulnerabilities and coding errors

Scheduled scans or trigger on certain events (push)

Creates an alert (and closes it automatically)

Uses GitHub Actions

Free for public repositories

Code Scanning – How?

- CodeQL
- Or through a 3rd party tool that supports the Static Analysis Results Interchange Format (SARIF)

The image shows a grid of 15 GitHub Actions cards, each representing a different tool for code scanning. The tools are arranged in a 5x3 grid. Each card includes the tool name, developer information, a brief description, and two buttons: 'Configure' and 'Code scanning'.

- CodeQL Analysis** By GitHub: Security analysis from GitHub for C, C++, C#, Go, Java, JavaScript, TypeScript, Python, Ruby and Kotlin developers.
- zScan** By Zimperium: The zimperium-zscan GitHub action scans your mobile app binary (iOS or Android) and identifies security, privacy, and compliance-related vulnerabilities.
- NowSecure** By NowSecure: The NowSecure Action delivers fast, accurate, automated security analysis of iOS and Android apps coded in any language.
- Bandit Scan** By abirismyname: Bandit is free software designed to find common security issues in Python code, maintained by PyCQA.
- Datre** By Datre: Detect misconfigurations in your Kubernetes manifests and present them in GitHub code scanning.
- Fortify on Demand Scan** By Micro Focus: Integrate Fortify's comprehensive static code analysis (SAST) for 27+ languages into your DevSecOps workflows to build secure software faster.
- Snyk Infrastructure as Code** By Snyk: Detect vulnerabilities in your infrastructure as code files and surface the issues in GitHub code scanning.
- Detekt** By Detekt: Static code analysis for Kotlin.
- Red Hat CodeReady Dependency Analytics** By Red Hat: Scan your project's dependencies with CodeReady Dependency Analytics.
- OSSAR** By GitHub: Run multiple open source security static analysis tools without the added complexity with OSSAR (Open Source Static Analysis Runner).
- Semgrep** By Returntocorp: Continuously run Semgrep to find bugs and enforce secure code standards. Start with 1k+ community rules or write your own in a few minutes.
- Veracode Static Analysis** By Veracode: Get fast feedback on flaws with Veracode Static Analysis and the pipeline scan. Break the build based on flaw severity and CWE category.
- Trivy** By Aqua Security: Scan Docker container images for vulnerabilities in OS packages and language dependencies with Trivy from Aqua Security.
- Frogbot Scan Pull Request** By JFrog: Automatically scans new pull requests for security vulnerabilities. Uses JFrog Xray to scan the project. Included as part of JFrog's free subscription.
- EthicalCheck** By APsec: EthicalCheck provides the industry's only free & automated API security testing service that uncovers security vulnerabilities using OWASP API list.
- lintr** By GitHub Actions: lintr provides static code analysis for R.
- CodeScan** By CodeScan Enterprises, LLC: CodeScan allows for better visibility on your code quality checks based on your custom rulesets.
- SOOS DAST Scan** By SOOS: SOOS DAST is the easy-to-integrate no-limit web vulnerability scanner. Integrate SOOS DAST with your CI pipeline to find vulnerabilities by scanning a web app or APIs.



Code Scanning – CodeQL

CodeQL is a code analysis engine to automate security checks.



Database

You generate a CodeQL database to represent your codebase



Queries

You run CodeQL queries on that database to identify problems in the codebase



Alerts

The query results are shown as code scanning alerts in GitHub when you use CodeQL with code scanning.

Code Scanning – CodeQL

- CodeQL code scanning automatically detects code written in the supported languages:

Language	Variants	Compilers	Extensions
C/C++	C89, C99, C11, C18, C++98, C++03, C++11, C++14, C++17, C++20 [1]	Clang (and clang-cl [2]) extensions (up to Clang 12.0), GNU extensions (up to GCC 11.1), Microsoft extensions (up to VS 2019), Arm Compiler 5 [3]	.cpp, .c++, .cxx, .hpp, .hh, .h++, .hxx, .c, .cc, .h
C#	C# up to 10.0	Microsoft Visual Studio up to 2019 with .NET up to 4.8, .NET Core up to 3.1 .NET 5, .NET 6	.sln, .csproj, .cs, .cshtml, .xaml
Go (aka Golang)	Go up to 1.20	Go 1.11 or more recent	.go
Java	Java 7 to 20 [4]	javac (OpenJDK and Oracle JDK), Eclipse compiler for Java (ECJ) [5]	.java
Kotlin [6]	Kotlin 1.5.0 to 1.8.20	kotlinc	.kt
JavaScript	ECMAScript 2022 or lower	Not applicable	.js, .jsx, .mjs, .es, .es6, .htm, .html, .xhtm, .xhtml, .vue, .hbs, .ejs, .njk, .json, .yaml, .yml, .raml, .xml [7]
Python [8]	2.7, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11	Not applicable	.py
Ruby [9]	up to 3.2	Not applicable	.rb, .erb, .gemspec, Gemfile
TypeScript [10]	2.6-4.9	Standard TypeScript compiler	.ts, .tsx, .mts, .cts

Code Scanning – CodeQL

Code scanning
Automatically detect common vulnerabilities and coding errors.

Tools

CodeQL analysis
Identify vulnerabilities and errors with [CodeQL](#) for [eligible](#) repositories. Last scan 1 hour ago [Set up](#) [...](#)

Other tools
Add any third-party code scanning tool.

Protection rules

Pull request check failure
Define which code scanning alert severity should cause a pull request to fail. This applies to analysis results uploaded via the API.

Default
Languages detected in this repository are not compatible with this setup type at this time. Use the advanced setup instead.

Advanced
Customize your CodeQL configuration via a YAML file checked into the repository.

Code Scanning – Alerting

Code scanning

 All tools are working as expected

 Tool status 2 + Add tool

 is:open branch:main

 3 Open ✓ 1 Closed

Tool ▾ Branch ▾ Rule ▾ Severity ▾ Sort ▾

 Azure Storage Account Keys should not be disclosed  Critical

main

#2 opened 1 hour ago • Detected by SonarCloud in Program.cs:34

 Constant condition  Warning

main

#4 opened 1 hour ago • Detected by CodeQL in Program.cs:29

 Useless assignment to local variable  Warning

main

#3 opened 1 hour ago • Detected by CodeQL in Program.cs:34

Code Scanning

Pull request integration

More silly stuff 😎 #2

Open thomasvochten wants to merge 1 commit into main from testbranch

Conversation 1 Commits 1 Checks 3 Files changed 1



thomasvochten commented last month

No description provided.



More silly stuff 😎

Owner ...

Verified ✅ 1d6a69a



sonarcloud (bot) commented last month

SonarCloud Quality Gate failed. Failed

0 Bugs
0 Vulnerabilities
1 Security Hotspot
1 Code Smell

0.0% Coverage
0.0% Duplication



Add more commits by pushing to the testbranch branch on thomasvochten/Demo-DevSecOps.



Review required

At least 1 approving review is required by reviewers with write access. [Learn more](#).



Some checks were not successful

[Hide all checks](#)

✓ DevSecOpsDemo - Sonarcloud / SonarCloud (pull_request) Successful in 1m [Details](#)

✗ SonarCloud Code Analysis Failing after 31s — Quality Gate failed [Details](#)

✓ Code scanning results / SonarCloud Successful in 2s — No new alerts [Details](#)

Dependabot – What?



Alerts

GitHub creates alerts when a vulnerable dependency or malware is detected



Scans

Scans when a new advisory is published or when you change the dependencies of your project



Fixes

Dependabot can fix vulnerable dependencies for you by raising pull requests with security updates.



Updates

You can use Dependabot to keep the packages you use updated to the latest versions.



PR integration

Can also integrate as a pull request (PR) check



Free

Free for all repositories



Dependabot

GitHub security alert digest

thomasvochten's repository security updates from the week of **Nov 21 - Nov 28**

💻 thomasvochten's personal account

⚠️ thomasvochten / Demo-DevSecOps

Known security vulnerabilities detected

Dependency **System.Data.SqlClient** Version `<= 4.8.4` Upgrade to `~>`
4.8.5

Defined in **DevSecOpsDemo.csproj**

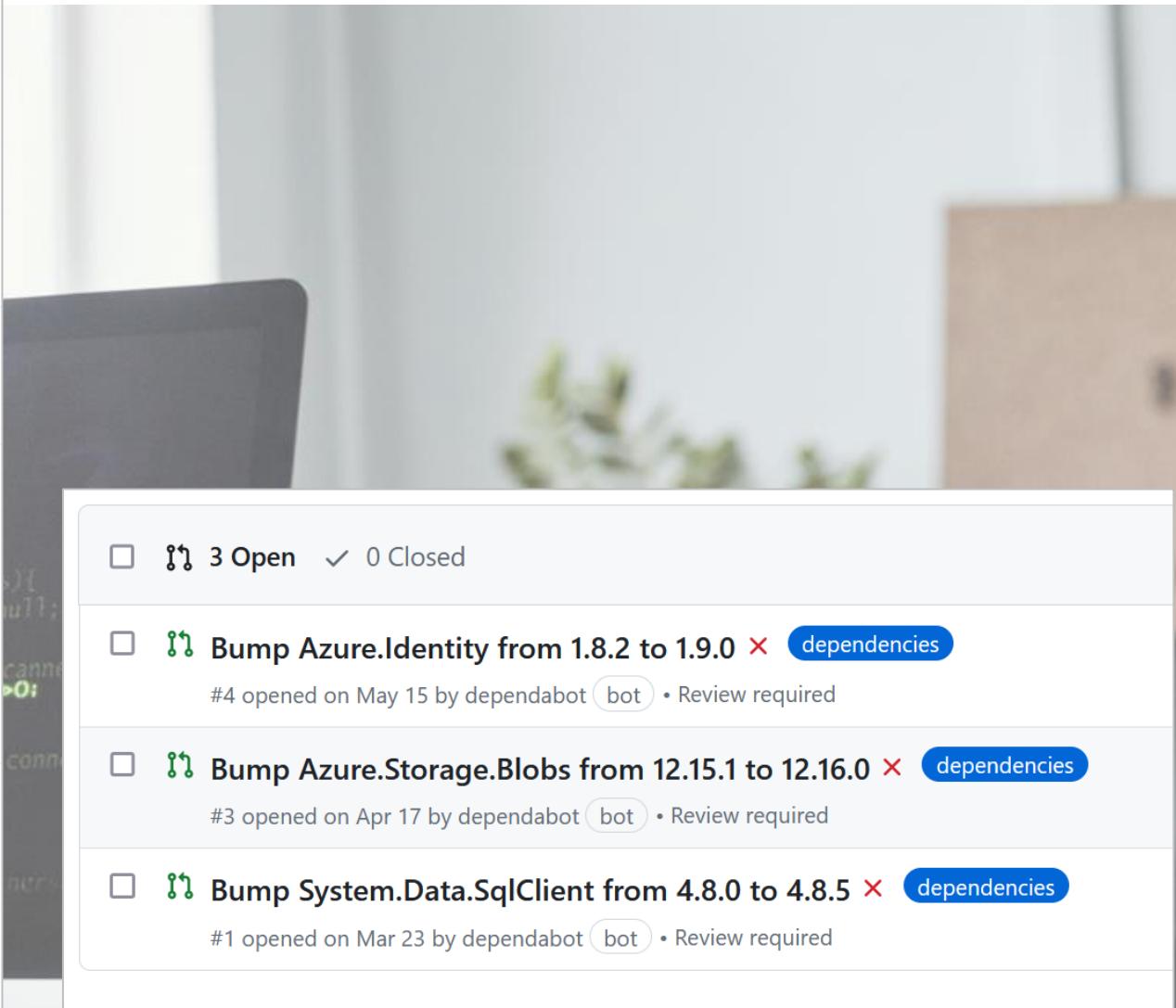
Suggested update
[#1](#)

Vulnerabilities
CVE-2022-41064 Moderate severity

Dependency **Azure.Identity** Version `< 1.10.2` Upgrade to `~>`
1.10.2

Defined in **DevSecOpsDemo.csproj**

Vulnerabilities
CVE-2023-36414 High severity



Dependabot dashboard showing four open pull requests:

- 3 Open ✓ 0 Closed
- Bump Azure.Identity from 1.8.2 to 1.9.0 X dependencies
#4 opened on May 15 by dependabot bot • Review required
- Bump Azure.Storage.Blobs from 12.15.1 to 12.16.0 X dependencies
#3 opened on Apr 17 by dependabot bot • Review required
- Bump System.Data.SqlClient from 4.8.0 to 4.8.5 X dependencies
#1 opened on Mar 23 by dependabot bot • Review required

Dependabot – Alerting

.NET Information Disclosure Vulnerability #1

Open Opened last month on System.Data.SqlClient (NuGet) · DevSecOpsDemo.csproj

Fix Bump System.Data.SqlClient from 4.8.0 to 4.8.5
Merging this pull request would fix 1 Dependabot alert on System.Data.SqlClient in DevSecOpsDemo.csproj.

Review security update

Package	Affected versions	Patched version
System.Data.SqlClient (NuGet)	<= 4.8.4	4.8.5

Microsoft is releasing this security advisory to provide information about a vulnerability in .NET, .NET Core and .NET Framework's System.Data.SqlClient and Microsoft.Data.SqlClient NuGet Packages.

A vulnerability exists in System.Data.SqlClient and Microsoft.Data.SqlClient libraries where a timeout occurring under high load can cause incorrect data to be returned as the result of an asynchronously executed query.

Mitigation factors

If you are not talking to Microsoft SQL Server from your application you are not affected by this vulnerability.

How do I know if I am affected?

.NET has two types of dependencies: direct and transitive. Direct dependencies are dependencies where you specifically add a package to your project, transitive dependencies occur when you add a package to your project that in turn relies on another package.

Dismiss alert

Severity
Moderate 5.8 / 10

CVSS base metrics

Attack vector	Adjacent
Attack complexity	High
Privileges required	Low
User interaction	None
Scope	Changed
Confidentiality	High
Integrity	None
Availability	None

CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

Tags
Direct dependency Patch available

Weaknesses
No CWEs

CVE ID
CVE-2022-41064

Dependabot – Pull Request

Bump System.Data.SqlClient from 4.8.0 to 4.8.5 #1

[Edit](#) [Code](#)

[Open](#) dependabot wants to merge 1 commit into [main](#) from [dependabot/nuget/System.Data.SqlClient-4.8.5](#)

Merging this pull request will resolve a **moderate** severity [Dependabot alert](#) on System.Data.SqlClient.

Conversation 0 Commits 1 Checks 3 Files changed 1 +1 -1

 **dependabot** (bot) commented on behalf of github on Mar 23 • edited

Bumps [System.Data.SqlClient](#) from 4.8.0 to 4.8.5.

▶ Release notes
▶ Commits

 compatibility unknown

You can trigger a rebase of this PR by commenting `@dependabot rebase`.

▶ Dependabot commands and options

Note
Automatic rebases have been disabled on this pull request as it has been open for over 30 days.



  dependabot (bot) added the [dependencies](#) label on Mar 23

Reviewers 
 thomasvochten Request
At least 1 approving review is required to merge this pull request.

Still in progress? [Convert to draft](#)

Assignees 
No one—[assign yourself](#)

Labels 
[dependencies](#)

Projects 
None yet

Milestone 



GitHub to the rescue!



Secret
Scanning



Code
Scanning



Dependency
Scanning

GitHub Account Security

- Username/Password with MFA
 - Time-based one-time password (TOTP)
 - GitHub Mobile
 - Security Key
 - Passkey
- Personal Access Token (PAT)
- SSH Key



Verified Commits

Using GPG, SSH, or S/MIME, you can sign tags and commits locally. These tags or commits are marked as verified on GitHub so other people can be confident that the changes come from a trusted source.

A screenshot of a GitHub commit page for a repository named 'thomasvochten'. The commit was made by the user 'thomasvochten' and is marked as 'committed now' with a green 'Verified' badge. The commit message is 'This commit was signed with the committer's **verified** signature.' Below the message, it shows 'Showing 1 changed file' with a single file named '.github/ISSUE_TEMPLATE.md' which is described as 'Empty file.'. On the right side of the commit card, there is a profile picture of Thomas Vochten, his name 'thomasvochten Thomas Vochten', and his SSH Key Fingerprint: 'DyL8JbAWYsN59CNfjAOAka9M7sQZE7pPRGFxfcUbbtY'. There is also a link to 'Learn about vigilant mode.'

Verified
commits

1Password Access Requested



Allow All Applications to use SSH key



Github Signing Key

Approve for all applications

Deny

Authorize

Defender for Cloud integration

Demo-DevSecOps

GitHub repository

3 Active recommendations | 0 Active alerts

Resource information

Subscription	Resource Group
Visual Studio Ultimate wit...	githubdefender
Environment	Connector
Azure	githubdefender
Resource type	
GitHub repository	

Recommendations

Alerts

Search More (2)

Severity ↑↓	Description
High	Code repositories should have secret scanning findings resolved Preview
Medium	GitHub repositories should have code scanning enabled Preview
Medium	GitHub repositories should have Dependabot scanning enabled Preview
Medium	Code repositories should have infrastructure as code scanning findings resolved Preview
Medium	Code repositories should have code scanning findings resolved Preview
Medium	Code repositories should have dependency vulnerability scanning findings resolved Preview

< Previous Page 1 of 1 Next >

Defender for Cloud integration

Code repositories should have secret scanning findings resolved ...

[Open query](#)

Severity High	Freshness interval  60 Min	Tactics and techniques  Initial Access +1
-------------------------	--	---

Description
Secrets have been found in code repositories. This should be remediated immediately to prevent a security breach. Secrets found in repositories can be leaked or discovered by adversaries, leading to compromise of an application or service. For Azure DevOps, the Microsoft Security DevOps connector is used to scan repositories. Therefore, results may not reflect the complete status of secrets in your repositories.

Remediation steps
Manual remediation:
To resolve discovered secrets:
1. Review the secret found by the scan.
2. Click on each finding to view details.
3. Invalidate the secret, tokens, and/or passwords.
4. Navigate to the repository using the Html URL or Build URL.
5. Refactor your code to remove the secret.
6. Check-in the remediated project.
7. Review scan results for the repository to verify the secret no longer exists.

Security checks

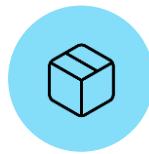
Findings

Search to filter items...

ID	Security check	Category	Severity
2da861e0-2b22-a473-cc3c-36646028e104	azure_storage_account_key	Secrets	 High



What about Azure DevOps?



Similar
features?



Something
missing?



Something
more?

Secret scanning

- Microsoft Defender for DevOps (preview; currently free, future cost unknown)

Microsoft Defender for Cloud | DevOps Security (Preview) Showing 2 subscriptions | PREVIEW

Search Add environment Refresh DevOps workbook Guides and Feedback Getting Started Configure

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Cloud Security Explorer (Preview)
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager
- DevOps Security (Preview)

Management

- Environment settings
- Security solutions
- Identity solutions

Security Overview

DevOps security vulnerabilities 234 VULNERABILITIES

High	Medium	Low
39	195	0

DevOps security results

Code scanning vulnerabilities	Exposed Secrets	OSS vulnerabilities	Recommendations
169	18	31	28

DevOps coverage

Github Connectors	Azure DevOps Connectors
1	1

Total 30 Total

Github repositories 27 Azure DevOps repositories 3

Search Subscriptio... == Contoso Hotels Tenant - Production, CyberSec... Resource Types == Github Repository, Azure DevOps Repository

Name	Pull request status	Total exposed secrets	OSS vulnerabilities	Total code scanning vulnerabilities
ASE_SG_Demo	N/A	Unhealthy (1)	1	65
RS_ramontest	N/A	Unhealthy (1)	0	65
DfDDemo	N/A	Unhealthy (4)	17	16
Toy-Website	N/A	Unhealthy (2)	0	0
Contoso Hotels	On	Unhealthy (1)	N/A	0
RepositoriesSampleContent	N/A	Healthy	0	0
Toy-Website	On	Healthy	N/A	0
DfD Demo	On	Healthy	N/A	0

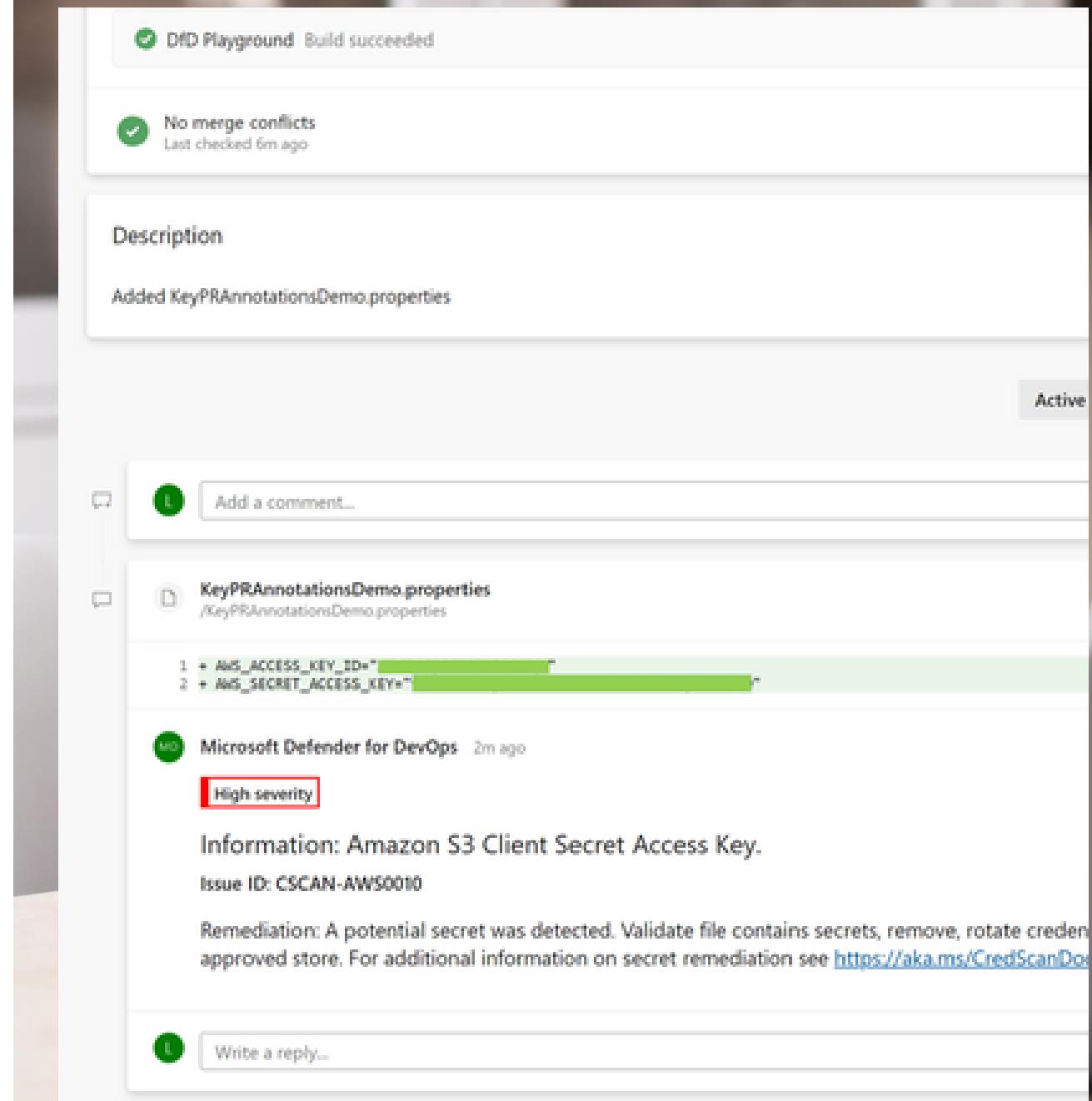
Secret scanning

- Enable Microsoft Defender for DevOps on Azure Portal
- Add Microsoft Security DevOps task to pipeline
- Needs to be run for every repo/branch you want to scan

```
6   trigger:
7     - main
8
9   pool:
10    vmImage: ubuntu-latest
11
12  steps:
13    Settings
14    - task: NodeTool@0
15      inputs:
16        versionSpec: '16.x'
17        displayName: 'Install Node.js'
18
19    - script: |
20      npm install
21      npm run build
22      displayName: 'npm install and build'
23
24    Settings
25    - task: MicrosoftSecurityDevOps@1
26      inputs:
27        categories: 'secrets, code, artifacts'
28        languages: 'javascript, typescript'
29        tools: 'credscan, eslint'
30
31    Settings
32    - task: Npm@1
33      displayName: 'Publish package to feed'
34      continueOnError: true
35      inputs:
36        command: 'publish'
37        publishRegistry: 'useFeed'
38        publishFeed: '3236f8cd-1ab2-47cd-9e49-f395927f206b/13954e39-73a7'
```

Secret scanning

- Results show in Azure Portal, build results, pull requests (if enabled)
- Combine pull request annotations with a branch policy that requires resolving all comments on a pull request
- Promote the usage of git pre-commit hooks



Code scanning

- Many third-party tools available
- SonarCloud
- 10\$/month
- Requires pull request build pipeline configuration

```
1 trigger: none
2
3 pool:
4   - vmImage: ubuntu-latest
5
6 steps:
7   - checkout: self
8   - fetchDepth: 0
9   Settings
10  - task: NodeTool@0
11    inputs:
12      - versionSpec: '16.x'
13      - displayName: 'Install Node.js'
14    Settings
15  - task: SonarCloudPrepare@1
16    inputs:
17      - SonarCloud: 'SonarCloud'
18      - organization: 'sulava'
19      - scannerMode: 'CLI'
20      - configMode: 'manual'
21      - cliProjectKey: 'Sulava.Common'
22      - cliProjectName: 'Sulava.Common'
23      - cliSources: '.'
24    - script: |
25        - npm install
26        - npm run build
27    - displayName: 'npm install and build'
28    Settings
29  - task: SonarCloudAnalyze@1
30    Settings
31  - task: SonarCloudPublish@1
32    inputs:
33      - pollingTimeoutSec: '300'
```

Code scanning

- Require build pipeline execution and resolving comments via branch policies

Laura Kokkarinen completed the pull request May 27

TS May 27

```
^ 248 250      : null}
249 251      { editMode ?
250 252          <div>
251 -          <PrimaryButton className={styles.saveButton} text={strings.Save} onClick={async () => await saveItem()} />
253 +          <PrimaryButton className={styles.saveButton} text={strings.Save} onClick={() => saveItem()} />
252 254          <DefaultButton className={styles.cancelButton} text={strings.Cancel} onClick={() => cancelEdit()} />
253 255      </div>
254 256      : null }
```

KB Kimmo Bergius May 27 Active

Bug: Promise-returning function provided to attribute where a void return was expected. ([typescript:S6544](#))
[See it in SonarCloud](#)

Write a reply... Resolve

Dependency scanning

- Many third-party tools available
- Snyk (free)
- Requires build pipeline configuration
- Config when to fail the build

```
6 trigger:
7 - main
8
9 pool:
10 | .vmImage: ubuntu-latest
11
12 steps:
13   Settings
14   --task: NodeTool@0
15   | .inputs:
16   | | .versionSpec: '16.x'
17   | | .displayName: 'Install Node.js'
18   | .script: |
19   | | .npm install
20   | | .npm run build
21   | | .displayName: 'npm install and build'
22
23   Settings
24   --task: SnykSecurityScan@1
25   | .inputs:
26   | | .serviceConnectionEndpoint: 'Snyk'
27   | | .testType: 'app'
28   | | .monitorWhen: 'always'
29   | | .failOnIssues: true
30   | | .additionalArguments: '--fail-on-all'
31
32   Settings
33   - task: Npm@1
34   | .displayName: 'Publish package to feed'
35   | .continueOnError: true
36   | .inputs:
37   | | .command: 'publish'
38   | | .publishRegistry: 'useFeed'
39   | | .publishFeed: '3236f8cd-1ab2-47cd-9e49-f395927f206b/13954e39-73a7-4799'
```

Dependency scanning

- Direct and transitive
- Detailed report
- Sends out email alerts about discovered vulnerabilities

The screenshot shows a software interface for dependency scanning. On the left is a vertical toolbar with icons for different functions: a gear (Reports), a crown (Dependencies), a shield (Security), a magnifying glass (Search), a bar chart (Metrics), a funnel (Poc), and a document (Details). The main area is titled "Reports" and displays a "Snyk Test for npm (report-2023-05-27 16:04:31) | Found 5 issues". Below this, it shows the package "validator@8.2.0". The "Overview" section states that "validator" is a library of string validators and sanitizers. It notes that affected versions are vulnerable to Regular Expression Denial of Service (ReDoS) via the `isSlug` function. The "PoC" (Proof of Concept) section contains a snippet of JavaScript code demonstrating the vulnerability:

```
var validator = require("validator")
function build_attack(n) {
  var ret = "111"
  for (var i = 0; i < n; i++) {
    ret += "a"
  }

  return ret+"_";
}
for(var i = 1; i <= 50000; i++) {
  if (i % 10000 == 0) {
    var time = Date.now();
    var attack_str = build_attack(i)
    validator.isSlug(attack_str)
    var time_cost = Date.now() - time;
    console.log("attack_str.length: " + attack_str.length + ":" + time_cost+" ms")
  }
}
```

The "Details" section defines Denial of Service (DoS) as a family of attacks aimed at making a system inaccessible to its original and legitimate users. It mentions various types of DoS attacks, including generating a large volume of traffic from many machines (a Distributed Denial of Service).

GitHub Advanced Security for Azure DevOps

- GA on September 20, 2023
- Secret, code and dependency scanning
- Enable for individual repositories under Project Settings -> Repositories
- Project Collection Admin

The screenshot shows the GitHub repository settings page for 'Fabrikam'. The 'Settings' tab is selected. A red box highlights the 'Advanced Security' section, which is currently turned off. Below it, the 'Repository Settings' section contains several other toggle switches, all of which are also off. These include 'Forks', 'Commit mention linking', 'Commit mention work item resolution', 'Work item transition preferences', 'Permissions management', and 'Strict Vote Mode'.

Fabrikam

Settings Policies Security

Off **Advanced Security**
Protect your repositories with security and analysis features like dependency scanning, code scanning, and secret scanning. [View billing](#) | [Learn more](#)

Off **Forks**
Allow users to create forks from this repository.

Off **Commit mention linking**
Automatically create links for work items mentioned in a commit comment.

Off **Commit mention work item resolution**
Allow mentions in commit comments to close work items (e.g. "Fixes #123").

Off **Work item transition preferences**
Remember user preferences for completing work items with pull requests.

Off **Permissions management**
Allow users to manage permissions for the branches they created

Off **Strict Vote Mode**
Enable Strict Vote Mode for repository which requires Contribute permission to vote in Pull Requests.

Secret scanning

- Automatically enabled with push protection(!)

The screenshot shows the Microsoft CloudHub interface for managing repositories. On the left, there's a sidebar with project settings for 'Contoso'. The main area displays 'All Repositories' with three listed: 'AdventureWorks', 'Fabrikam' (which is selected), and 'TailSpin'. The 'Fabrikam' repository page is shown in detail, featuring tabs for 'Settings', 'Policies', and 'Security'. A red box highlights the 'Advanced Security' section, which contains a toggle switch set to 'On', a description about protecting repositories with security features like dependency scanning and secret scanning, and a checked checkbox for 'Block secrets on push' with a sub-description about scanning pushes and blocking secrets. Below this, another red box highlights the 'Repository Settings' section, which includes toggles for 'Forks' (off) and 'Commit mention linking' (off). The 'Forks' setting allows users to create forks from the repository.

CloudHub / Contoso / Settings / Repositories

Search

Project Settings

Contoso

General

- Overview
- Teams
- Permissions
- Notifications
- Service hooks
- Dashboards

Boards

- Project configuration
- Team configuration
- GitHub connections

Pipelines

All Repositories

Filter by keywords

- AdventureWorks
- Fabrikam
- TailSpin

Fabrikam

Browse Rename

Settings Policies Security

Advanced Security

Protect your repositories with security and analysis features like dependency scanning, code scanning, and secret scanning. [View billing](#) | [Learn more](#)

Block secrets on push

Scan all pushes to the repository and block pushes containing secrets.

Repository Settings

Forks

Allow users to create forks from this repository.

Commit mention linking

Automatically create links for work items mentioned in a commit comment.

Secret scanning

- GitHub Advanced Security team maintains the default secret scanning patterns

The screenshot shows the Azure DevOps interface for the Contoso organization under the Advanced Security section. The 'Secrets' tab is selected. A search bar at the top right contains the word 'Search'. On the left, a sidebar lists various repository-related options: Overview, Boards, Repos (which is selected), Files, Commits, Pushes, Branches, Tags, Pull requests, Advanced Security (which is also selected), and Pipelines. In the main content area, the title 'Advanced Security' is displayed above three tabs: Dependencies, Code scanning, and Secrets. Below these tabs is a search bar with the placeholder 'Filter by keywords' and dropdown filters for 'State: Open' and 'Type'. A single alert is listed: 'Alert' for 'Azure DevOps personal access token (PAT) ...uo4kta' was introduced 'Just now'. The alert is labeled 'Critical' and is located in file '#146 in src/secrets.txt:1'.

Secret scanning

- Close the alert after revoking the secret, accepting the risk or if false positive

Azure DevOps CloudHub / Contoso / Repos / Advanced Security / Fabrikam

Search

Contoso

Overview

Boards

Repos

Files

Commits

Pushes

Branches

Tags

Pull requests

Advanced Security

Pipelines

#146 [Open](#) in 41b9a93b • detected Just now

← Azure DevOps personal access token (PAT)

Location

src/secrets.txt:1 @ 41b9a93b

Reason

Revoked
The secret has been revoked.

Risk accepted
Risk is tolerable or irrelevant (e.g., only used in tests or not exploitable in your implementation).

False positive
This alert is inaccurate or incorrect.

Comment (optional)

Cancel Close

Push protection

- Push protection is available on both the command line and the web interface

The screenshot shows the Azure DevOps web interface for a repository named 'Fabrikam'. The left sidebar includes links for Contoso, Overview, Boards, Repos (selected), Files, Commits, Pushes, Branches, Tags, Pull requests, Advanced Security, and Pipelines. The main area displays the repository structure under 'main': 'src' (containing 'app.js' and 'index.html'), 'secrets.txt', '.gitignore', 'azure-pipelines.yml', 'package-lock.json', 'package.json', and 'README.md'. A tooltip over 'secrets.txt' indicates it contains secrets. A 'Commit' modal is open, showing a warning message: 'VS403654: The push was rejected because it contains one or more secrets. Resolve the following secrets before pushing again. For help, see https://aka.ms/advancedsecurity/secret-scanning/push-protection. Secrets: commit: 1dcf26a75cbbd0f189f76af2e9aefff1daee24fc paths: /src/secrets.txt (1,1-53) : SEC101/102 : AdoPat'. The modal also has fields for 'Comment' (containing 'Added secrets.txt'), 'Branch name' (set to 'main'), and 'Work items to link' (with a placeholder 'Search work items by ID or title').

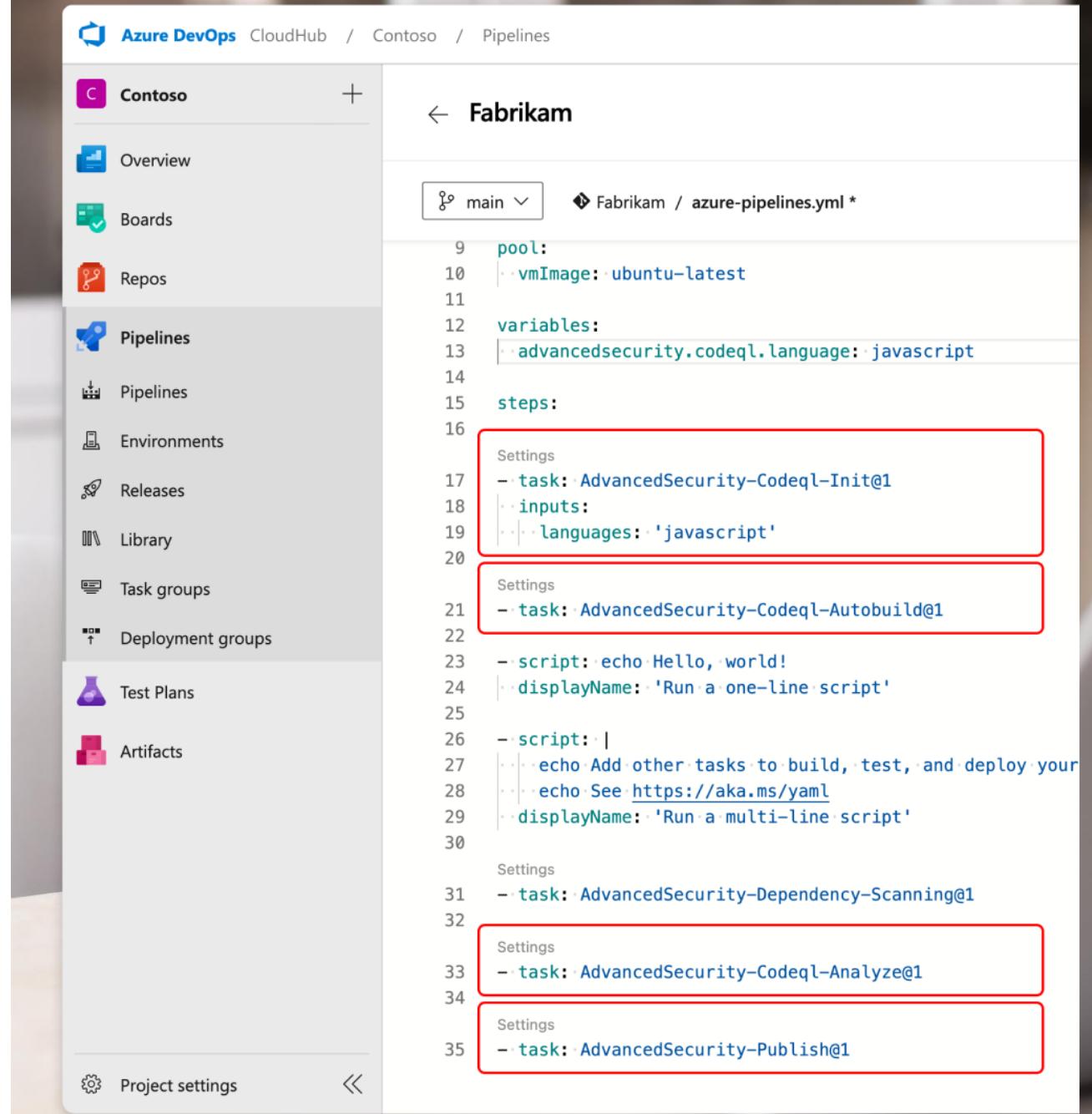
Code scanning

- CodeQL identifies security vulnerabilities
- Code analysis engine
- Queries are open source
 - C/C++
 - C#
 - Go
 - Java,
 - JavaScript/TypeScript
 - Kotlin (beta)
 - Python
 - Ruby



Code scanning

- Add the required actions to the build pipeline
- Pros:
 - Easier to setup than SonarCloud
- Cons:
 - Does not find as many issues (esp. quality)



The screenshot shows the Azure DevOps Pipelines interface. On the left, a sidebar lists various project management and pipeline-related sections: Overview, Boards, Repos, Pipelines (which is selected), Environments, Releases, Library, Task groups, Deployment groups, Test Plans, and Artifacts. At the bottom of the sidebar are Project settings and a back arrow icon.

The main area displays a YAML file named "azure-pipelines.yml" for the "Fabrikam" pipeline. The file defines a pipeline with a pool, variables, and several steps. The steps are highlighted with red boxes:

```
9  pool:
10  vmImage: ubuntu-latest
11
12  variables:
13    advancedsecurity.codeql.language: javascript
14
15  steps:
16
17    - task: AdvancedSecurity-Codeql-Init@1
18      inputs:
19        languages: 'javascript'
20
21    - task: AdvancedSecurity-Codeql-Autobuild@1
22
23    - script: echo Hello, world!
24      displayName: 'Run a one-line script'
25
26    - script: |
27      echo Add other tasks to build, test, and deploy your
28      echo See https://aka.ms/yaml
29      displayName: 'Run a multi-line script'
30
31    - task: AdvancedSecurity-Dependency-Scanning@1
32
33    - task: AdvancedSecurity-Codeql-Analyze@1
34
35    - task: AdvancedSecurity-Publish@1
```

Code scanning

- Automatically closed when no longer detected; can also be accepted or marked as FP

The screenshot shows a detailed view of a code scanning alert in the Azure DevOps interface. The alert is for a vulnerability titled "DOM text reinterpreted as HTML (js/xss-through-dom)" in repository "Fabrikam" under project "Contoso". The alert was detected today at 11:22 AM.

Overview: The alert is marked as an "Open" issue (#145). The "Detections" tab is selected, showing the location as "src/index.html:41 @ 258d2fd1".

Description: The alert describes the vulnerability as follows:
Extracting text from a DOM node and interpreting it as HTML can lead to a cross-site scripting vulnerability.
A webpage with this vulnerability reads text from the DOM, and afterwards adds the text as HTML to the DOM. Using text from the DOM as HTML effectively unescapes the text, and thereby invalidates any escaping done on the text. If an attacker is able to control the safe sanitized text, then this vulnerability can be exploited to perform a cross-site scripting attack.

Recommendation: To guard against cross-site scripting, consider using contextual output encoding/escaping before writing text to the page, or one of the other solutions that are mentioned in the References section below.

Reason: A modal dialog box is open, asking if the alert should be marked as a "False positive". The "False positive" option is selected, with the reason being "This alert is inaccurate or incorrect." There is also an optional comment field and buttons for "Cancel" and "Close".

Details: The alert is identified by the ID "js/xss-through-dom". It is associated with "Weaknesses" such as "CWE-079" and "CWE-116".

Code scanning

- Closed alerts can be viewed via the filtering options

Contoso

Overview

Boards

Repos

Files

Commits

Pushes

Branches

Tags

Pull requests

Advanced Security

Pipelines

Test Plans

Advanced Security

Dependencies Code scanning Secrets

Filter by keywords

Branch: main State: **Closed** Pipeline Package Severity

Alert

Alert	First detected
Regular Expression Denial of Service in ms (CVE-2015-8315) High #7318931	9m ago
Prototype Pollution Protection Bypass in qs (CVE-2017-1000048) High #7318932	9m ago
qs vulnerable to Prototype Pollution (CVE-2022-24999) High #7318933	9m ago
Prototype Pollution Protection Bypass in qs (CVE-2017-1000048) High #7318936	9m ago
qs vulnerable to Prototype Pollution (CVE-2022-24999) High #7318937	9m ago
qs vulnerable to Prototype Pollution (CVE-2022-24999) High #7318938	9m ago

Open

- ✓ All closed
- Risk accepted
- False positive
- Fixed

All closed

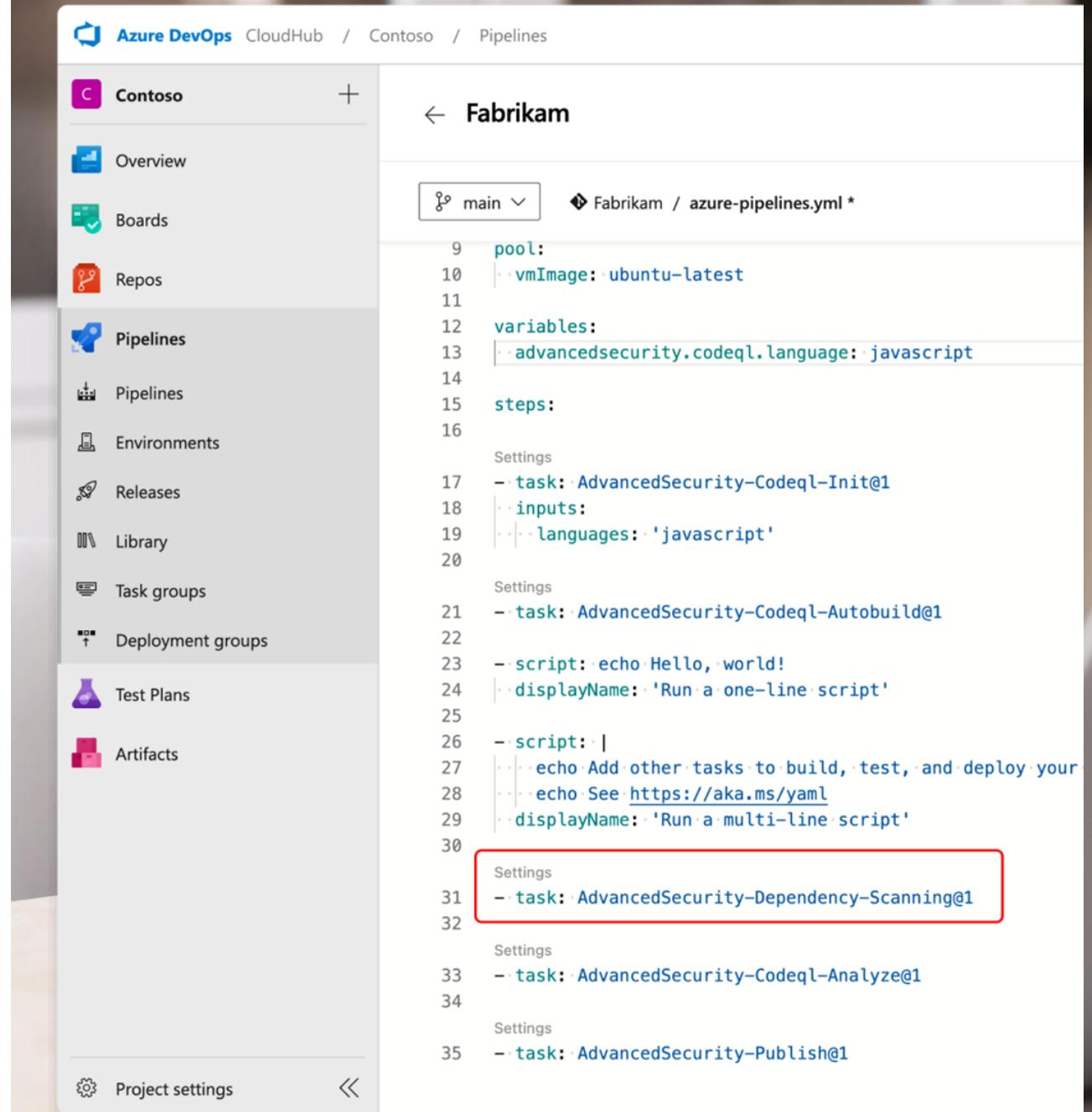
Dependency scanning

- Checks if open-source components used in your source code have associated vulnerabilities
- Direct and transitive
- GitHub Advisory Database



Dependency scanning

- Add the required action to the build pipeline
- Pros:
 - Finds more issues than Snyk
- Cons:
 - No inheritance path
 - No email alerts
 - No break build option



The screenshot shows the Azure DevOps CloudHub interface for the Contoso organization. The left sidebar is open, showing options like Overview, Boards, Repos, Pipelines (which is selected), Pipelines, Environments, Releases, Library, Task groups, Deployment groups, Test Plans, and Artifacts. The main area displays the contents of the azure-pipelines.yml file for the Fabrikam project. The file defines a pool, variables, and steps. A red box highlights the step at line 31, which is the 'AdvancedSecurity-Dependency-Scanning' task. The file also includes other steps for echo commands and codeql analysis.

```
pool:
vmImage: ubuntu-latest

variables:
advancedsecurity.codeql.language: javascript

steps:
- task: AdvancedSecurity-Codeql-Init@1
  inputs:
    languages: 'javascript'

- task: AdvancedSecurity-Codeql-Autobuild@1
  script:
    - echo Hello, world!
    - displayName: 'Run a one-line script'

    - script: |
      echo Add other tasks to build, test, and deploy your
      echo See https://aka.ms/yaml
      displayName: 'Run a multi-line script'

- task: AdvancedSecurity-Dependency-Scanning@1

- task: AdvancedSecurity-Codeql-Analyze@1

- task: AdvancedSecurity-Publish@1
```

Dependency scanning

- How to override transitive vulnerable “acorn” package in a Node project:

```
{  
  "name": "npm-overrides",  
  "version": "1.0.0",  
  "license": "MIT",  
  "dependencies": {  
    "axios": "0.19.2",  
    "eslint  },  
  "overrides": {  
    "eslint      "espree": {  
        "acorn": "6.4.1" // patched, non-vulnerable version  
      }  
    }  
  }  
}
```

Dependency scanning

- How to override transitive vulnerable “Http.Connections” package in a .NET project:

```
<Project Sdk="Microsoft.NET.Sdk.Web">
  <PropertyGroup>
    <TargetFramework>netcoreapp3.1</TargetFramework>
    <RootNamespace>NuGet.Dependencies</RootNamespace>
  </PropertyGroup>
  <ItemGroup>
    <PackageReference Include="Microsoft.AspNetCore.App" Version="2.2.8" />
  </ItemGroup>

  <ItemGroup Label="Dependency Resolutions">
    <!-- Microsoft.AspNetCore.App -->
    <PackageReference Include="Microsoft.AspNetCore.Http.Connections"
Version="[1.0.15,1.1.0)" />
  </ItemGroup>
</Project>
```

Price and billing

- 49\$ per *active committer* per month
- Billed via the Azure sub connected to the ADO org
- If the same sub has multiple orgs, committers are deduplicated

The screenshot shows the Azure DevOps CloudHub Organization Settings page. The left sidebar lists various settings categories: General (Overview, Projects, Users, Billing), Security (Policies, Permissions), Boards, Repos, Pipelines (Agent pools, Settings, Deployment pools), and Parallel jobs. The 'Billing' category is selected and highlighted in grey. The main content area is titled 'Billing' and displays the 'Azure Subscription ID' (12345678-abcd-abcd-abcd-12345678abcd). It also provides usage details for pipelines, boards, repos, and test plans, and information about advanced security and unique active committers.

Azure DevOps CloudHub / Settings / Billing

Organization Settings
CloudHub

Search Settings

Billing

Azure Subscription ID
12345678-abcd-abcd-abcd-12345678abcd

Pipelines for private projects	Free	Paid parallel jobs
MS Hosted CI/CD	10	
Self-Hosted CI/CD	1	10

Visit [parallel jobs](#) for full details on free pipelines and public concurrency

Boards, Repos and Test Plans	Free
Basic users	5
Basic + Test Plans	

This organization is enabled for user assignment based billing and daily pro-rated charges, instead of monthly committed purchases.
[Learn more](#)

Advanced Security	Used
Unique active committers	123

Advanced Security is billed based on the number of unique active committers in repositories. Active committers are users that have committed to an Advanced Security enabled repository in the last 90 days. [Learn more](#)

Which way to go?

- Currently the different third-party tools seem more capable
- Hopefully, GitHub Advanced Security for Azure DevOps will improve
- Ideally, use both
- Costs



Azure DevOps vs GitHub

- GitHub for open source, Azure DevOps for the enterprise
- What about GitHub Enterprise? What is keeping people on Azure DevOps?



Project management and collaboration

- Planning
- Collaboration
- Analytics and reports



Tracing and auditing

- Work item links



More granular access control management

- Levels
- Features
- Permissions



Flexible licensing

- Stakeholder
- Basic
- Basic + Test Plans



More mature pipelines

- Microsoft
- Release pipeline features



Other features

- Test Plans
- Printable Wikis
- Etc.

Future

- What is the point of having two products for the same purpose?
- Migration from Azure DevOps to GitHub Enterprise – eventually



Recap

Protect against what?

Secure Software Development Lifecycle

Automating code security checks

Protecting source code and repositories

Defender for Cloud integration

What about Azure DevOps?

```
import java.util.ArrayList;
import java.util.Scanner;
import java.util.List;
import java.io.File;
import java.io.IOException;
import java.util.Arrays;
import java.io.IOException;

public class AirlineProblem {
    public static void main(String[] args){
        Scanner scannerToReadAirlines = null;
        try{
            scannerToReadAirlines = new Scanner(new File("airlines.txt"));
        } catch(IOException e){
            System.out.println("could not connect to file: " + e);
            System.exit(0);
        }
        if(scannerToReadAirlines != null){
            Scanner scannerFromfile = null;
            ArrayList<Airline> airlinesPartnersNetwork = new ArrayList<Airline>();
            Airline newAirline;
            String lineFromFile;
            try{
                scannerFromfile = new Scanner(new File("airlinesPartnersNetwork.txt"));
                while(scannerFromfile.hasNextLine()){
                    lineFromFile = scannerFromfile.nextLine();
                    airlineNames = lineFromFile.split(",");
                    newAirline = new Airline(airlineNames);
                    if(airlineNames != null){
                        airlinesPartnersNetwork.add(newAirline);
                    }
                }
            } catch(IOException e){
                System.out.println("could not connect to file: " + e);
            }
            System.out.println(airlinesPartnersNetwork);
        }
    }
}
```





Questions?