DevSecOps, day 1

3. Lab: Azure DevOps

What will you need?

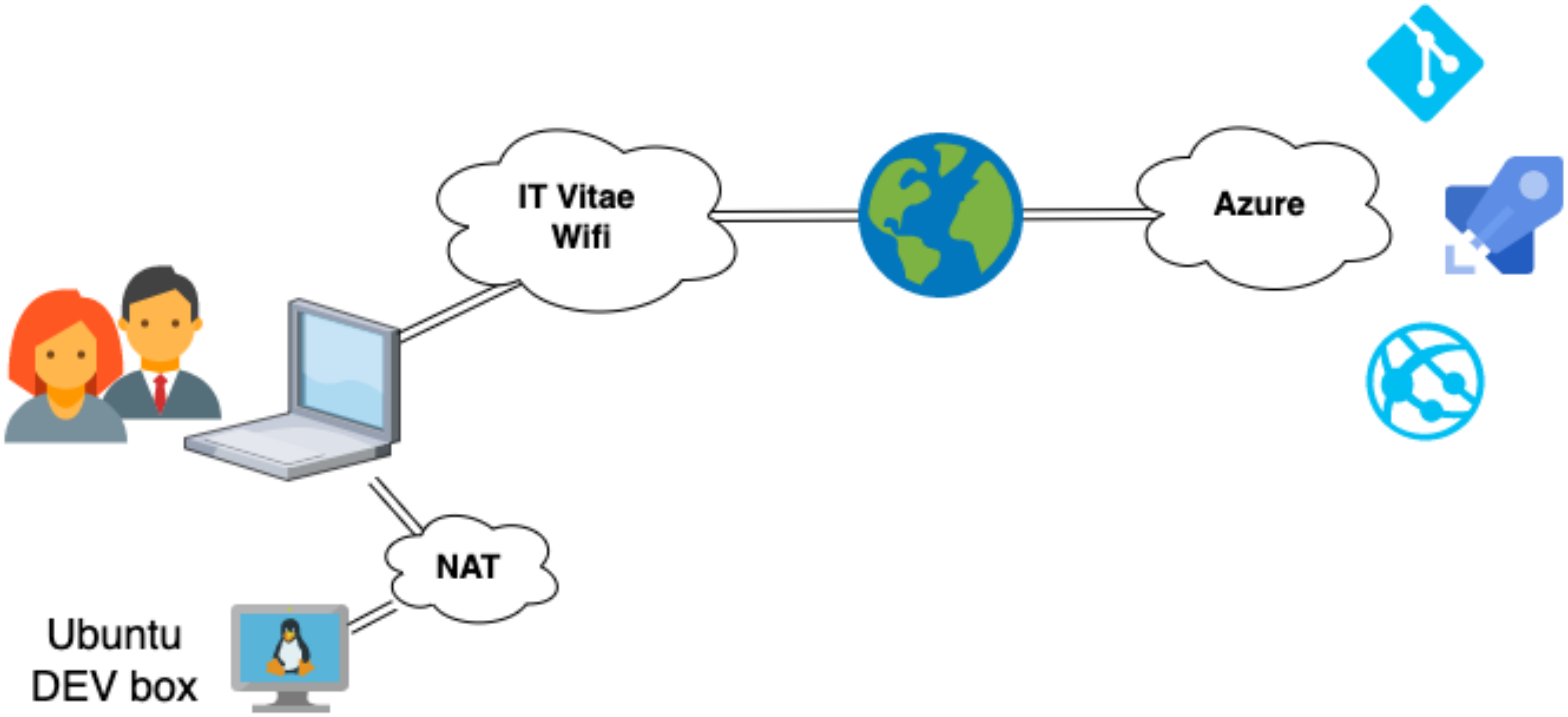
- A semi-recent (5 years) laptop, or PC.
  - Intel i5/i7, AMD Zen2, Apple Silicon (ARM)
  - At least 8GB RAM
  - At least 60GB of storage space

What will you need?

- VirtualBox
- A *Vagrantfile* is available.
  - It makes a Debian 11 VM, with all tools.

- The *Vagrantfile* gives 2 CPU cores and 4GB RAM.
  - If you can spare it, give the VM more!

Our working environment



Our working environment

- Use a browser on your host OS.
- Use Git, etc on your DEV box.
- Use SSH to login to your DEV box.
  - *vagrant ssh devsecops*

Let's start "work"!

- I have invited all of you to a new project.
  - We have Scrum boards, Git repos and more.

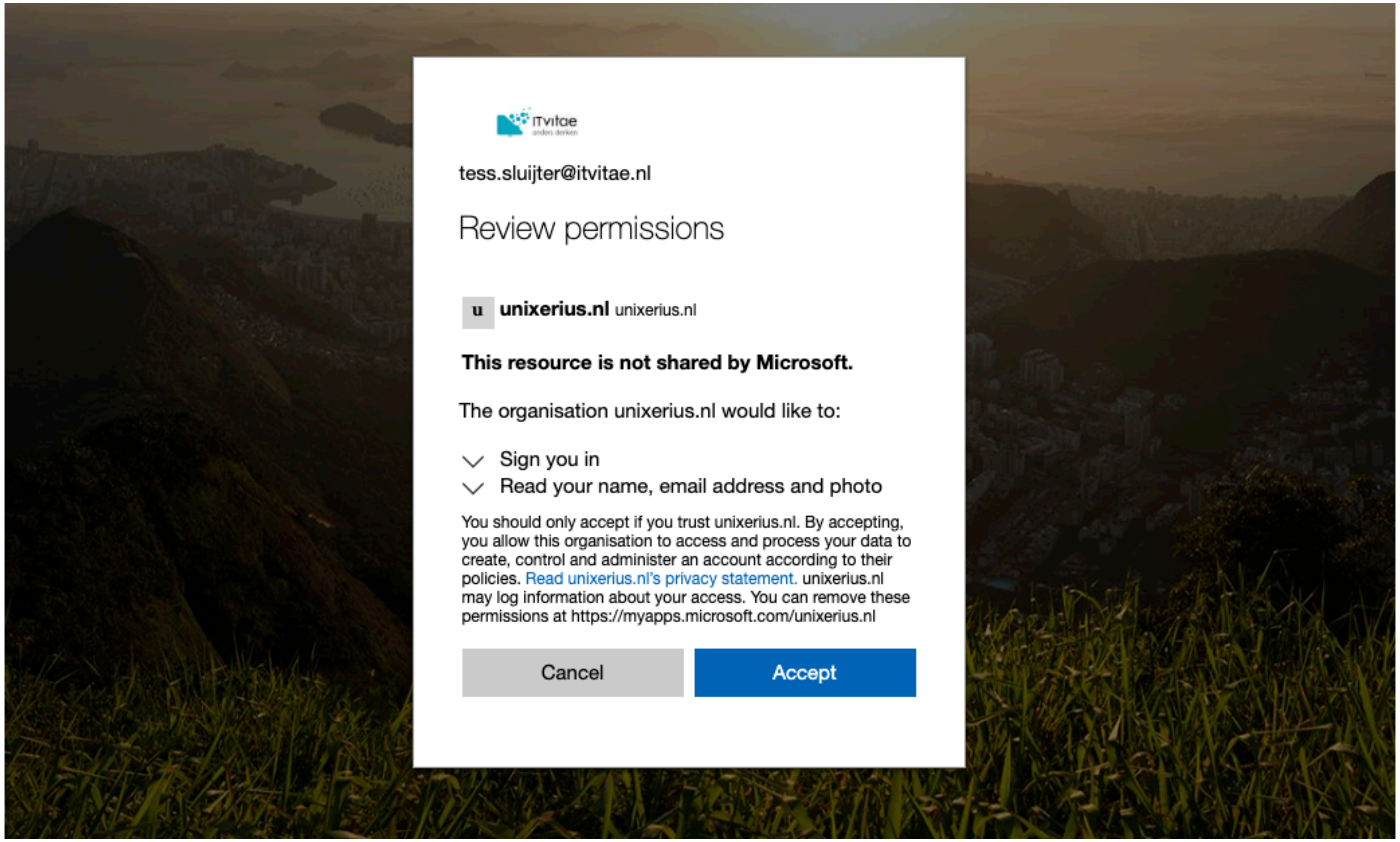
- You will work in teams of 2-3, on the same project.

Logging in

- Go to https://dev.azure.com/Unixerius-learning/
- Login using your ITVitae credentials.
  - You will be asked to setup MFA.
  - Use MS Authenticator app, or your mobile number.*

*: Information will be deleted after the class. I will not look at your number.

Logging in



tess.sluijter@itvitae.nl

Review permissions

u **unixerius.nl** unixerius.nl

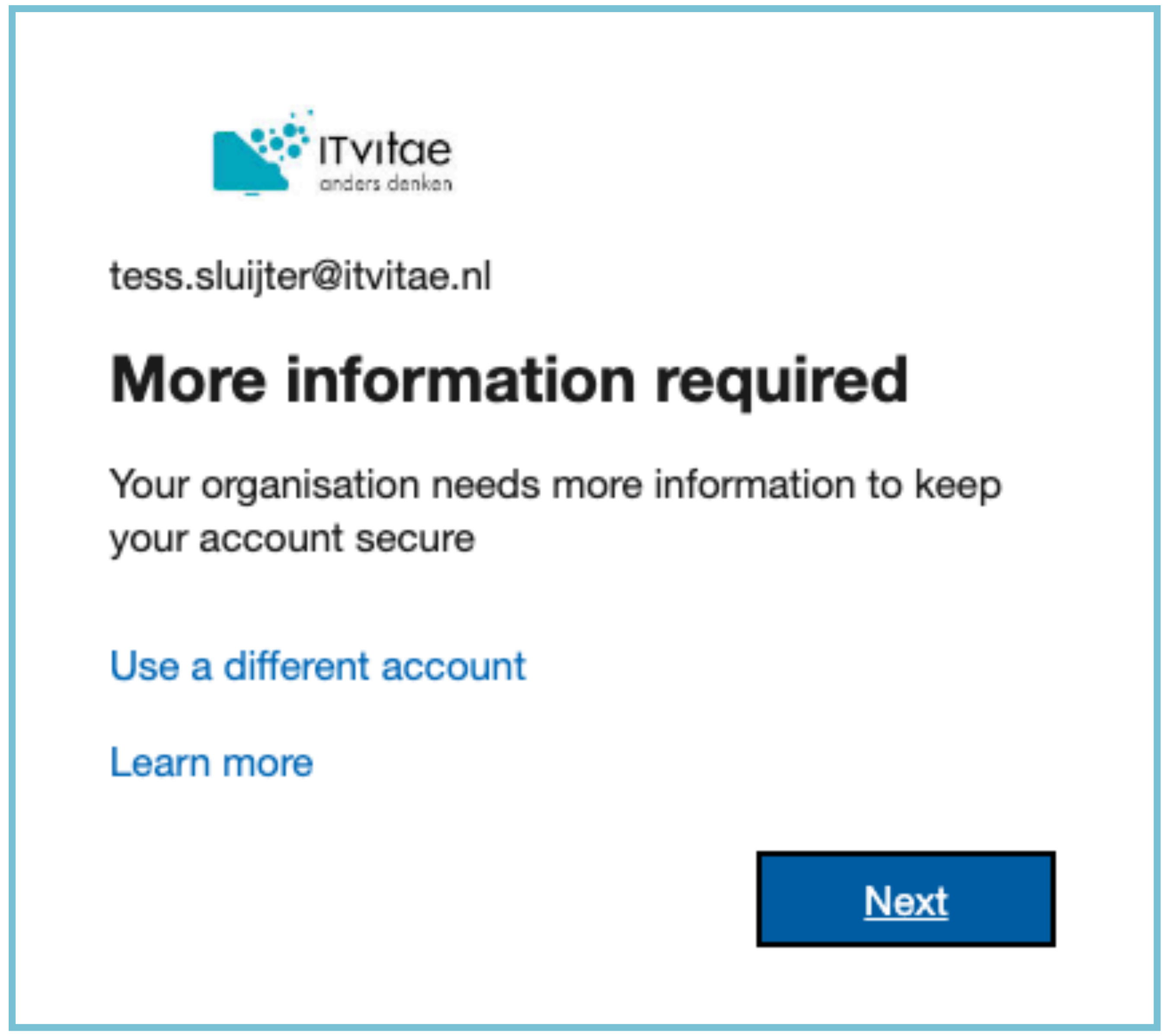
This resource is not shared by Microsoft.

The organisation unixerius.nl would like to:

- Sign you in
- Read your name, email address and photo

You should only accept if you trust unixerius.nl. By accepting, you allow this organisation to access and process your data to create, control and administer an account according to their policies. Read unixerius.nl's privacy statement. unixerius.nl may log information about your access. You can remove these permissions at https://myapps.microsoft.com/unixerius.nl

Logging in



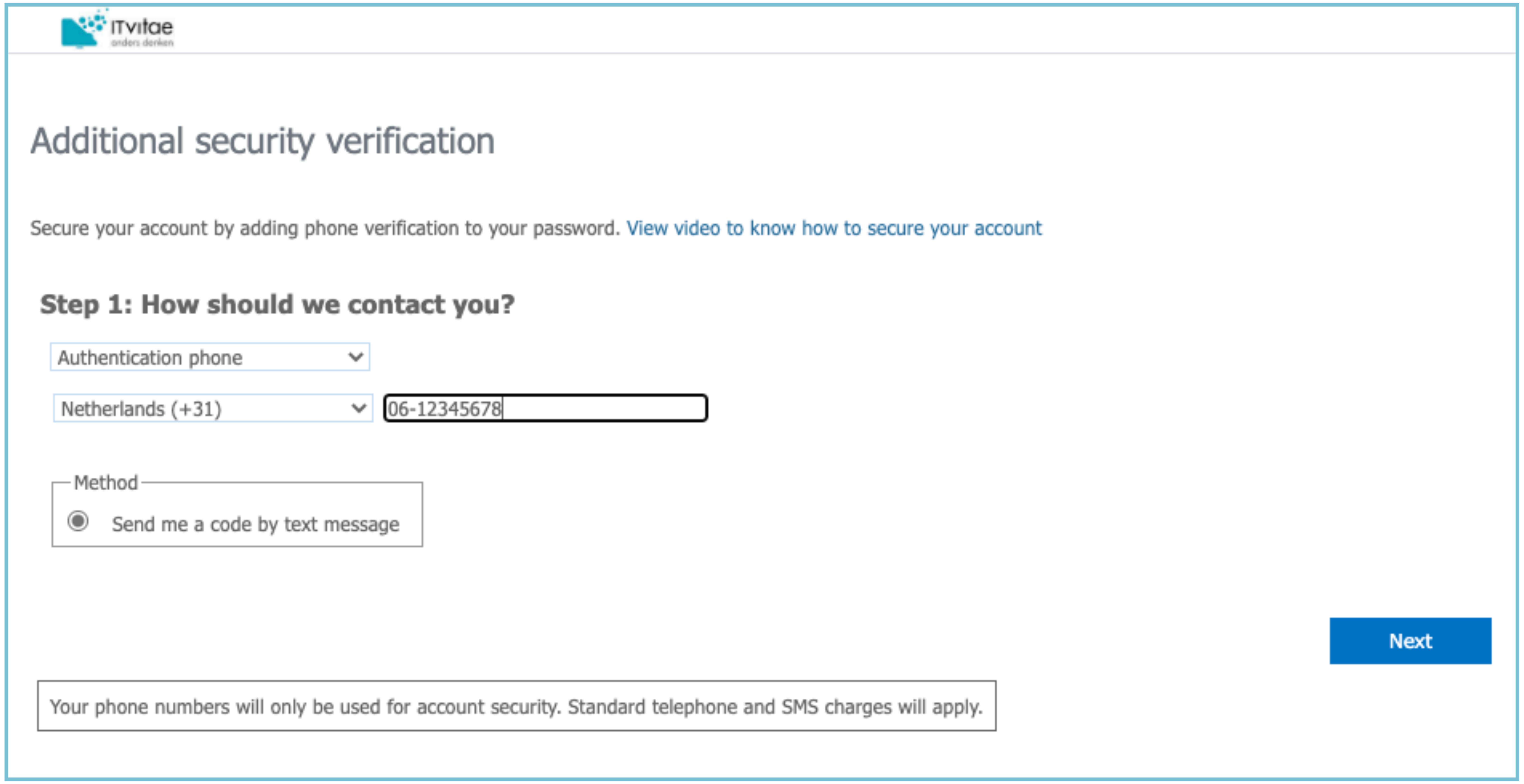
tess.sluijter@itvitae.nl

More information required

Your organisation needs more information to keep your account secure

Use a different account

Learn more



Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

Authentication phone

Netherlands (+31) 06-12345678

Method

● Send me a code by text message

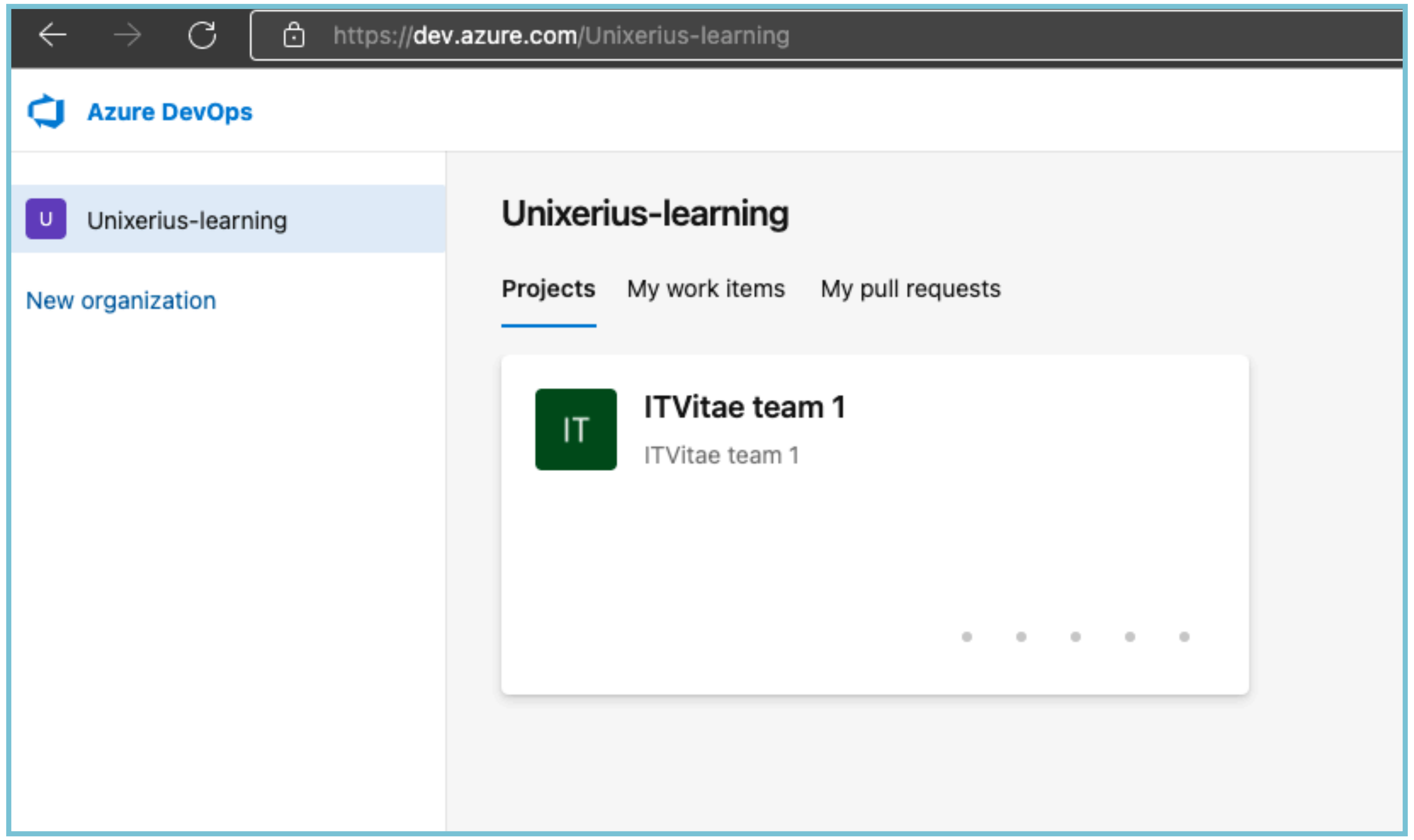
Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply.

Multi-factor authentication

- Azure DevOps and the Azure Portal:
  - Admin-level access to your project and infra!
  - Very serious target for phishing!
  - Case study: *SchizoDuckie vs Belastingdienst*.

Welcome!

- You have been assigned to a team.
- Your team has 1 project.



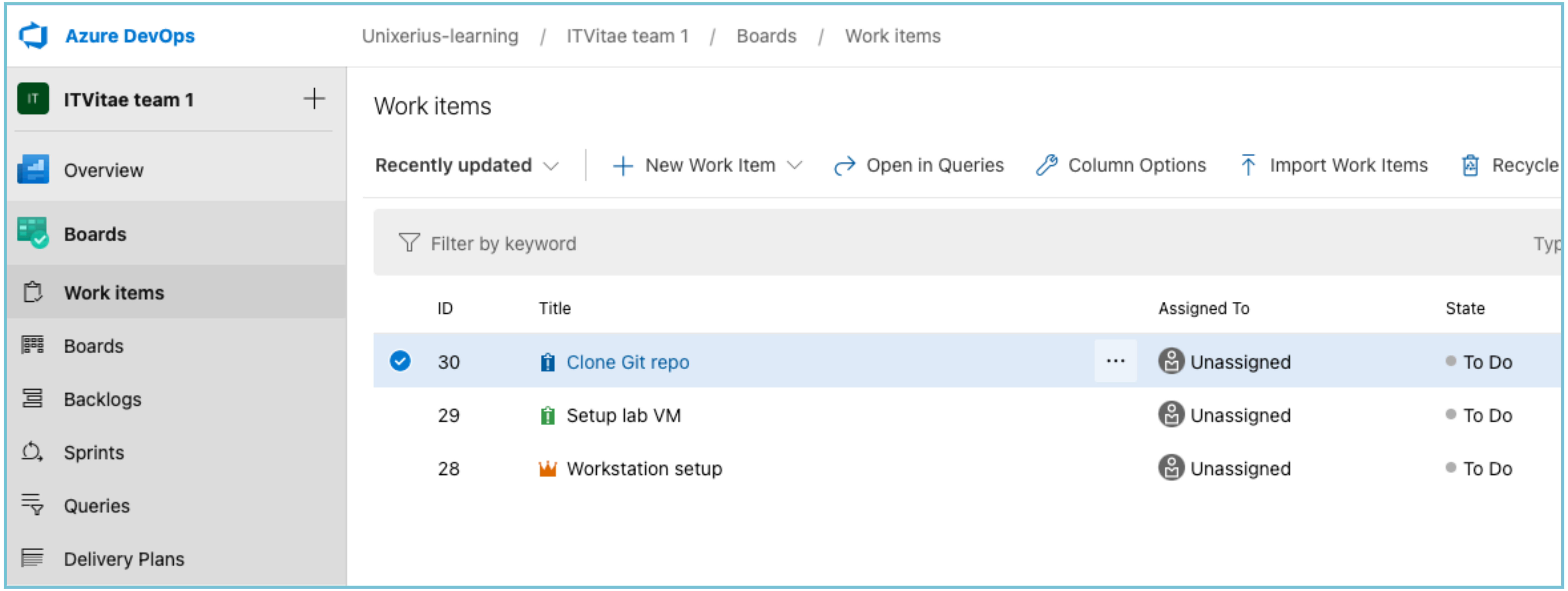
https://dev.azure.com/Unixerius-learning

Unixerius-learning

IT ITVitae team 1
ITVitae team 1

Welcome!

- Your team has a task board.

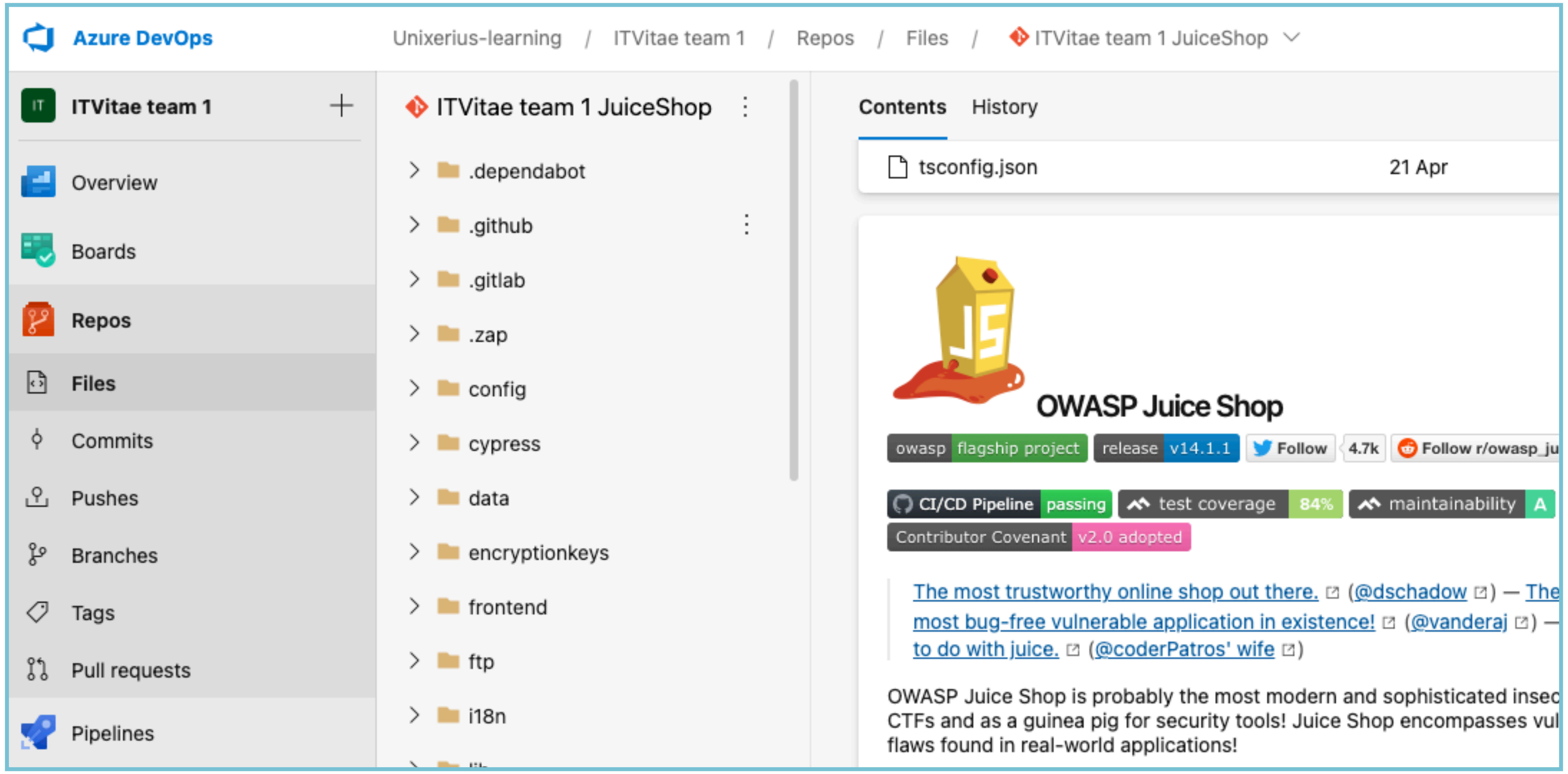


Work items

ID	Title	Assigned To	State
30	Clone Git repo	Unassigned	To Do
29	Setup lab VM	Unassigned	To Do
28	Workstation setup	Unassigned	To Do

Welcome!

- Your team has a Git repo.



Azure DevOps   Unixerius-learning / ITVitae team 1 / Repos / Files / ITVitae team 1 JuiceShop

ITVitae team 1

- Overview
- Boards
- Repos
- Files
- Commits
- Pushes
- Branches
- Tags
- Pull requests
- Pipelines

ITVitae team 1 JuiceShop

- .dependabot
- .github
- .gitlab
- .zap
- config
- cypress
- data
- encryptionkeys
- frontend
- ftp
- i18n

Contents   History

tsconfig.json   21 Apr

OWASP Juice Shop

owasp flagship project | release v14.1.1 | Follow 4.7k | Follow r/owasp_ju

CI/CD Pipeline passing | test coverage 84% | maintainability A | Contributor Covenant v2.0 adopted

The most trustworthy online shop out there. (@dschadow) — The most bug-free vulnerable application in existence! (@vanderaj) — to do with juice. (@coderPatros' wife)

OWASP Juice Shop is probably the most modern and sophisticated insec CTFs and as a guinea pig for security tools! Juice Shop encompasses vul flaws found in real-world applications!

4. Lab : Setting up Git

Assignment: setup Git

- Each team will be cloning *their own* repo.

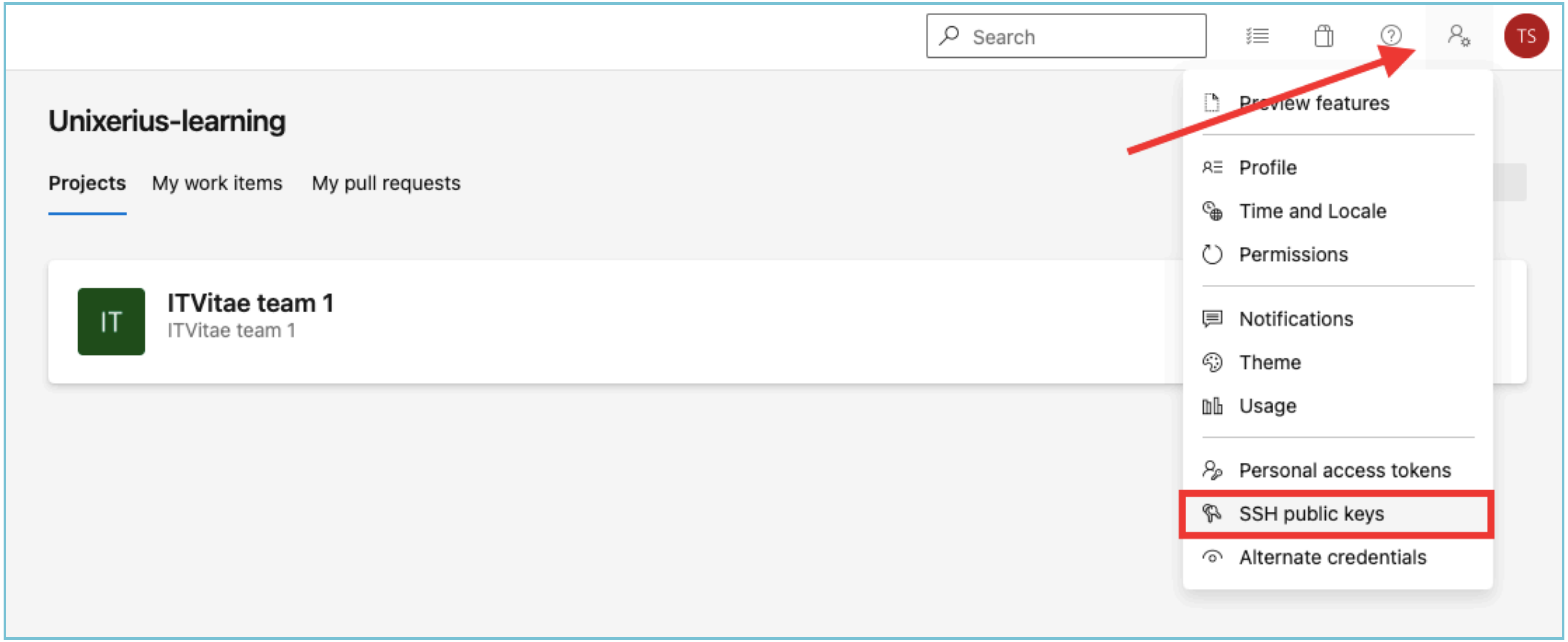
- On your dev VM, make a new SSH RSA key pair.
- You will link your SSH public key,
  - To your Azure DevOps account.

Assignment: setup Git

- Please *do* set up a password for your key pair.

```
$ ssh-keygen -t rsa
   # Use the default location
   # Set a password

$ cat ~/.ssh/id_rsa.pub
```

Assignment: setup Git



Search

TS

Unixerius-learning

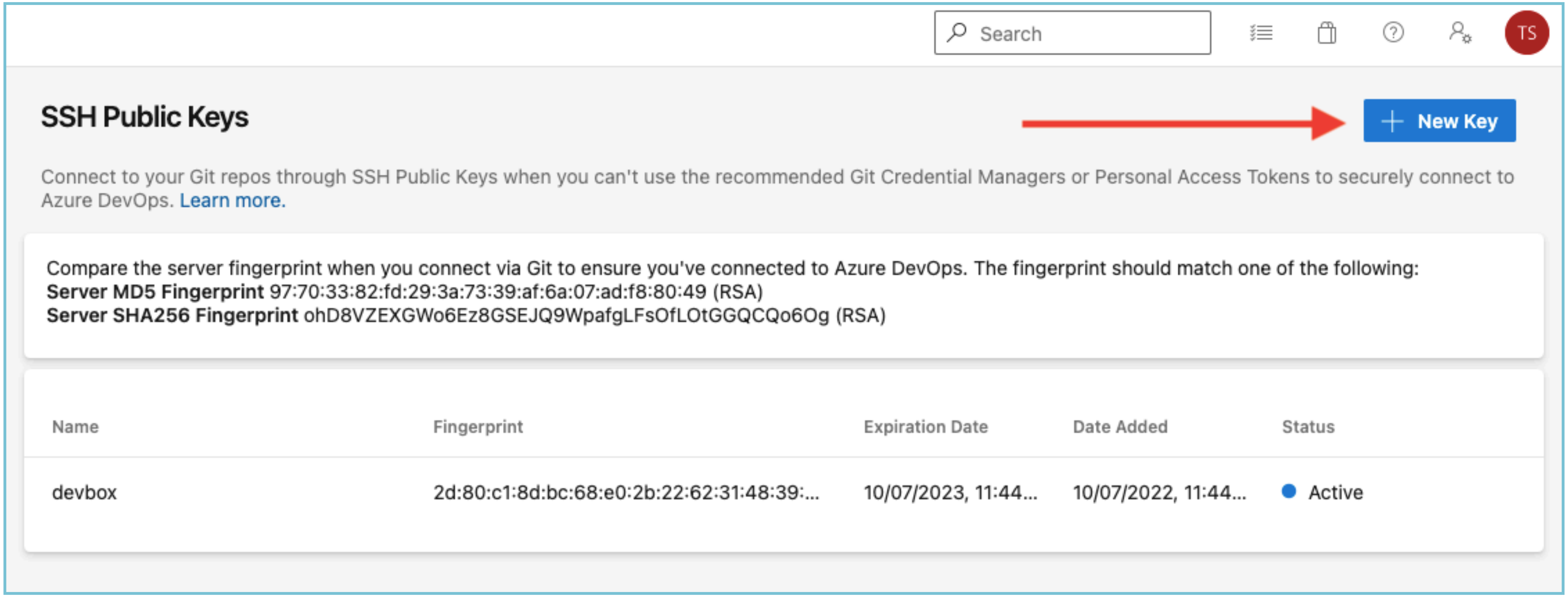
Projects My work items My pull requests

IT

ITVitae team 1

ITVitae team 1

Assignment: setup Git



SSH Public Keys

Connect to your Git repos through SSH Public Keys when you can't use the recommended Git Credential Managers or Personal Access Tokens to securely connect to Azure DevOps. Learn more.

Compare the server fingerprint when you connect via Git to ensure you've connected to Azure DevOps. The fingerprint should match one of the following:
Server MD5 Fingerprint 97:70:33:82:fd:29:3a:73:39:af:6a:07:ad:f8:80:49 (RSA)
Server SHA256 Fingerprint ohD8VZEXGWo6Ez8GSEJQ9WpafgLFsOfLOtGGQCQo6Og (RSA)

Name	Fingerprint	Expiration Date	Date Added	Status
devbox	2d:80:c1:8d:bc:68:e0:2b:22:62:31:48:39:...	10/07/2023, 11:44...	10/07/2022, 11:44...	● Active

Assignment: setup Git

- Also, let's configure your Git client.

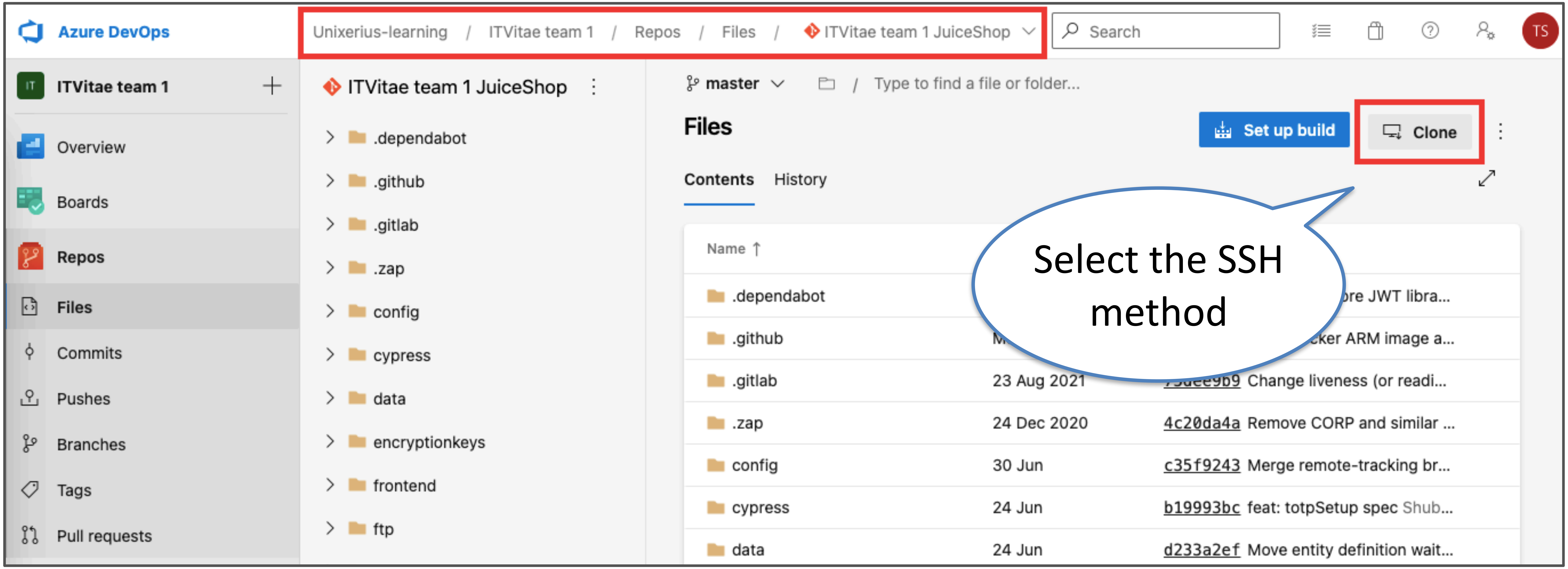
```
$ git config --global user.name \
  "Tess Sluijter"

$ git config --global user.email \
  "tess@itvitae-learning.nl"
```

Assignment: setup Git

- Specify your own Git directory name.
  - Do not just clone the repo.
  - Clone it into *"~/Team1JS"*, for example.

- Otherwise, NPM will complain about "*node-pre-gyp*".

Assignment: setup Git



Name ↑			
.dependabot			...re JWT libra...
.github	M...		...cker ARM image a...
.gitlab	23 Aug 2021	75dee9b9	Change liveness (or readi...
.zap	24 Dec 2020	4c20da4a	Remove CORP and similar ...
config	30 Jun	c35f9243	Merge remote-tracking br...
cypress	24 Jun	b19993bc	feat: totpSetup spec Shub...
data	24 Jun	d233a2ef	Move entity definition wait...

Select the SSH method

Assignment: setup Git

- For me, that gives:

```
$ git clone git@ssh.dev.azure.com:v3/
Unixerius-learning/ITVitae%20team%201/
ITVitae%20team%201%20JuiceShop ~/Team1JS
```

Checkpoint!

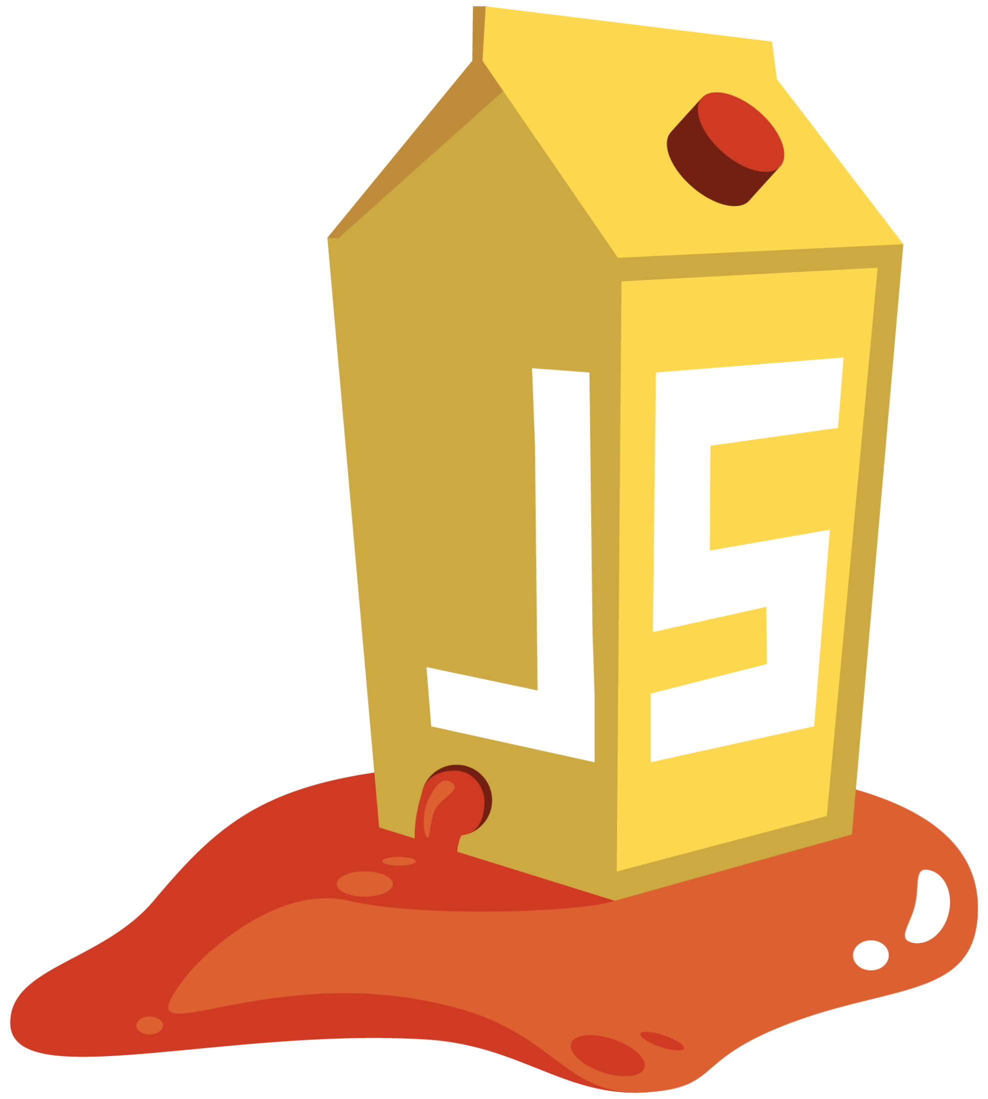
- Does everyone have:
  - Their DEV VM up and running?
  - A local clone of their team's repo?

STOP
SECURITY CHECKPOINT AHEAD
SmartSign.com • 800-952-1457 • K2-4293

6. Lab: Juice Shop

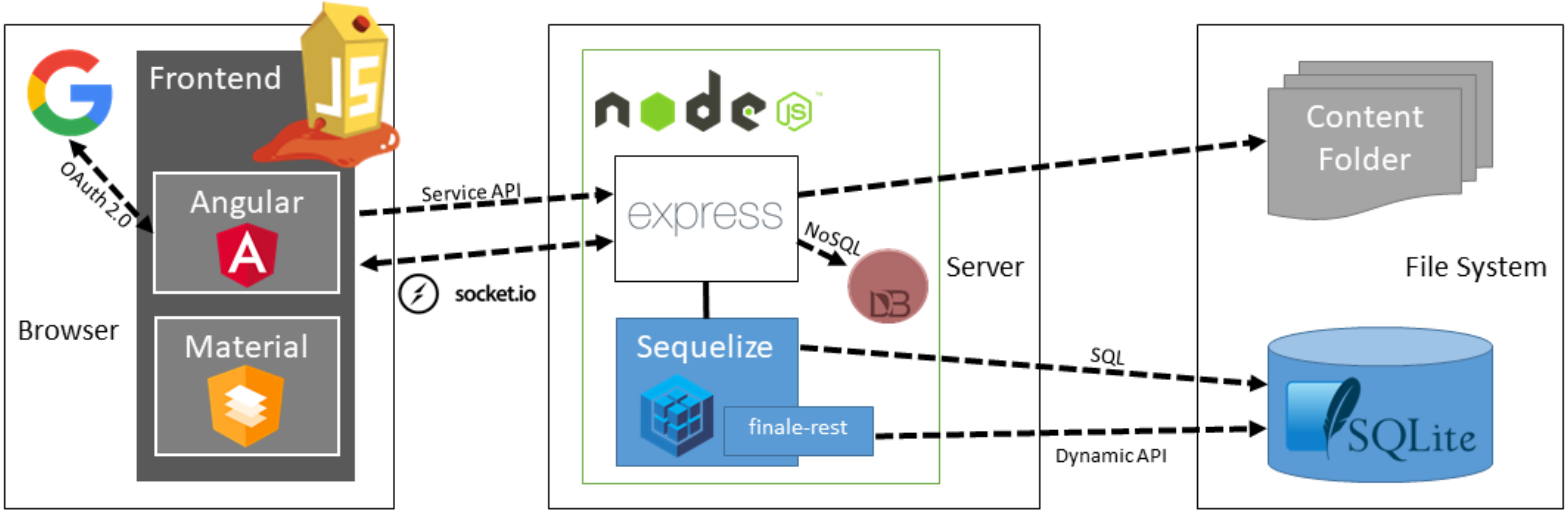
What is Juice Shop?

- An OWASP flagship project.
  - A demo webshop, that works!
  - Built in TypeScript and NodeJS.
  - Frontend, backend, APIs.
- Learning tool for security!



See: OWASP's most broken flagship

From the manual



See: JS Codebase 101

Why is it useful for us?

- Training tool for pen-testers.
- Testing tool for DevSecOps.
- Teaching tool for developers.
- Demo tool for business people.

What will we do?

- We will build and run it on the DEV VM.
- We will run the project's test cases.
- We will build a Docker container.

But how?? RTFM

- Every project should have proper documentation.
  - We already saw the architecture docu.

- The project includes instructions for building.
  - The developer guide has test instructions.

Assignment: build locally

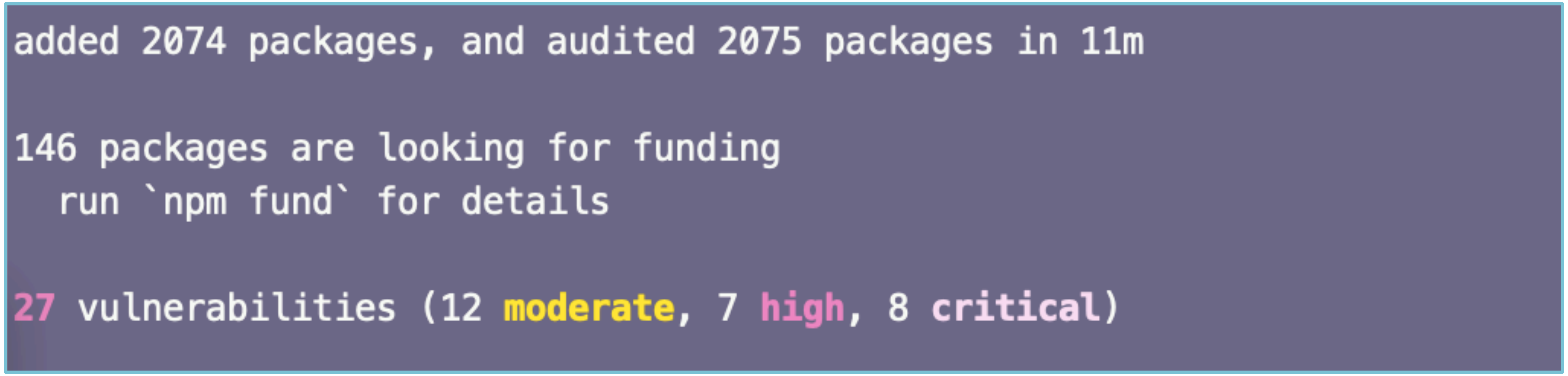
```
$ cd ~/Team1JS

$ npm install
```

Fetching dependencies takes *long.* 6 to 20 minutes.

See: Juice Shop README.md

Assignment: build locally

- This shows a lot of warnings!
  - We'll talk about this on day 3.



```
added 2074 packages, and audited 2075 packages in 11m

146 packages are looking for funding
  run `npm fund` for details

27 vulnerabilities (12 moderate, 7 high, 8 critical)
```

Assignment: run locally

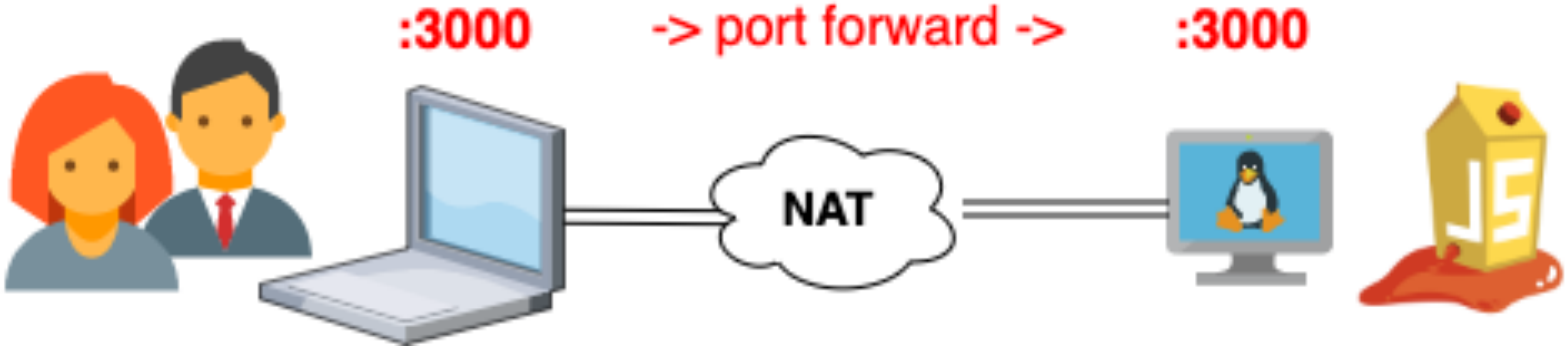
- The following starts the web app services.
  - Access it on http://localhost:3000

```
$ cd ~/Team1JS

$ npm start
```

See: Juice Shop README.md

Assignment: run locally

- Either use your host OS' browser.
  - Or test with *curl* on the DEV VM.



Assignment: test locally

- Every application should include a full set of tests.
  - First stop the running webapp. Then:

```
$ npm test                   # functionality

$ npm run frisby             # integration
```

See: Juice Shop developer contributions

Checkpoint!

- Does everyone have:
  - Working tests?
  - A working running local app?

STOP
SECURITY CHECKPOINT AHEAD
SmartSign.com • 800-952-1457 • K2-4293

Closing

What have we achieved?

- We started work as DevOps engineer!
- We got access to our project.
- We setup our development workstation.
- We built, tested and ran the software locally.

Tomorrow

- We will freshen up our Git skills.
- Dive into virtualization and containers again.
- Get started on CI/CD.

Relevant reading

Topic	Book
Days 003 and 008 of Linux+ track: Git, Docker, Vagrant.	n.a.
The SDLC, Agile and security	Ch 4
Risk assessment for Agile teams	Ch 7
Building secure software	Ch 9
Security culture	Ch 15

Reference materials

Resources

- MIT 6.858 - Computer Systems Security
- PDSO Certified DevSecOps Professional
- "The Phoenix Project"
- "Make DevOps valuable" - Sasha Rosenbaum
- "Agile vs Scrum"
- "Agile, Waterfall, Kanban, Scrum"
- "Kanban vs Scrum"
- A threat modeling journey - B. Schoenfield

Resources

- https://dev.azure.com/Unixerius-learning/
- SchizoDuckie vs Belastingdienst
- FFFO, what it really means
- Juice Shop Codebase 101
- Juice Shop README.md
- Juice Shop developer contributions