UNIVERSE'24

Enterprise code security 101

Getting started with GitHub Advanced Security

Cuno Reijman - @equalizer999

Customer Success Architect | GitHub

Daniel Meppiel - @danielmeppiel

Senior Customer Success Architect | GitHub

Cuno Reijman

Customer Success Architect | GitHub

cunoreijman

Based in NL Beusichem

Microsoft

Dev stack experience

PADI DIVEMASTER

Daniel Meppiel

Senior Customer Success Architect | GitHub

danielmeppiel

Based in CH Geneva

SAST tooling market experience

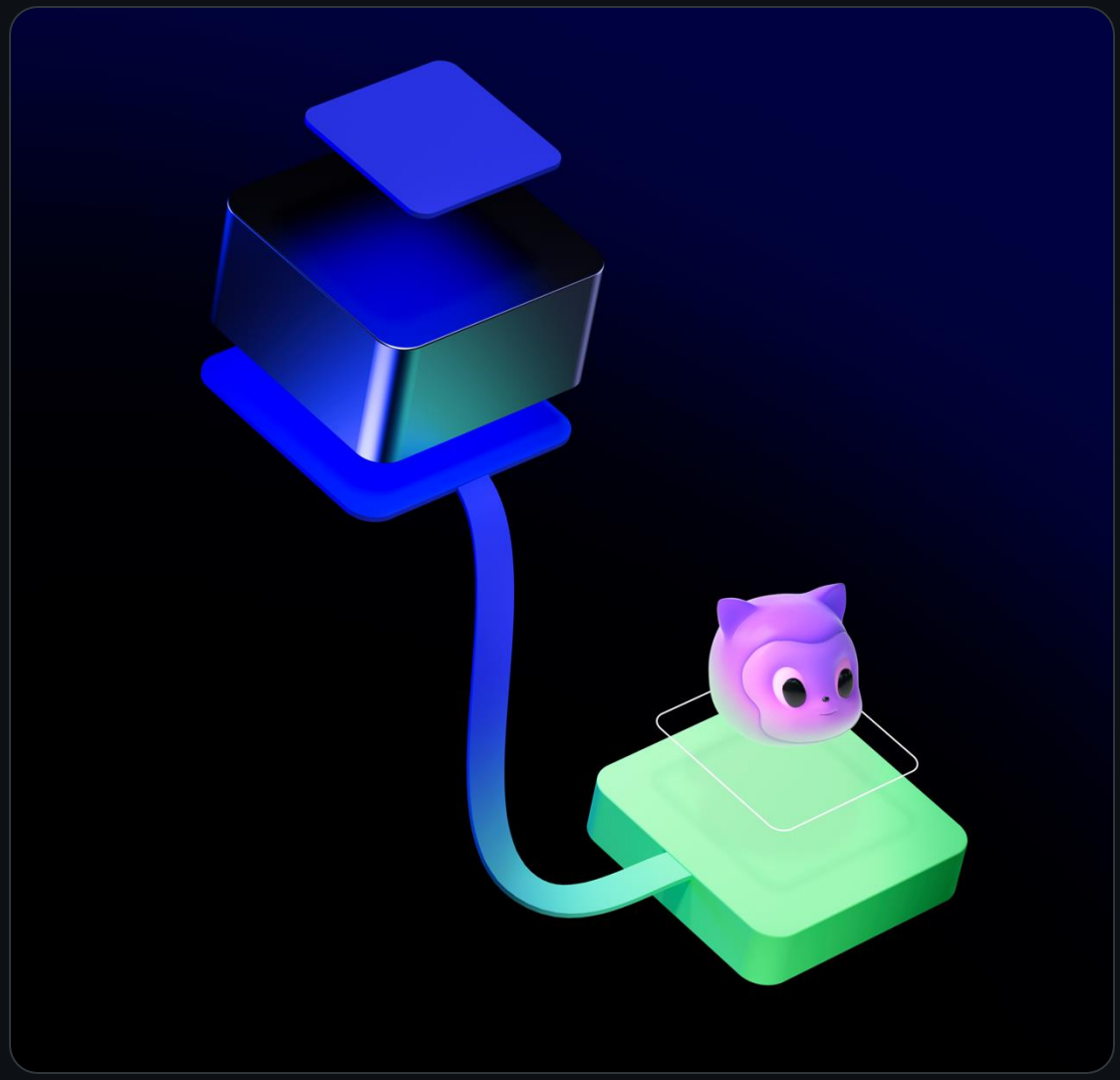
Agenda

01 **Intro** 10 min

02 **Hands-on** 60 min

- Learn and understand how to configure GitHub Advanced Security for a repository
- Learn how to block vulnerable code before it reaches production
- Discover how to scale GitHub Advanced Security setup and policies for thousands of repositories

03 **Closure** 20 min



How are we going to run this?

- As much hands-on as possible
- Interactive!
  - Nobody falls asleep here 😅
- Exercises 🏋️
- Have fun 😃 !

Interactive!

Keep your phone 📱 close!

gh.io/AAsr0sz

Timer: 10-min

Exercises 

1. Demos first

2. Dedicated time for you to do the  exercises yourself 👌

Workshop environment

- Surface machine 💻 – *Only available during workshop*
- Surface machine account – *Username and password*
- Microsoft login account - *Email address and password*
- GitHub sandbox environment - *GitHub organization*

Poll question

Are you up and running?

Please wait 🙇

Troubleshooting 😱 :

1. Check if you have entered the correct username and password

2. Help your neighbour out! 🙇

3. If all fails: 🖐 Raise your hand

gh.io/AAs4awo

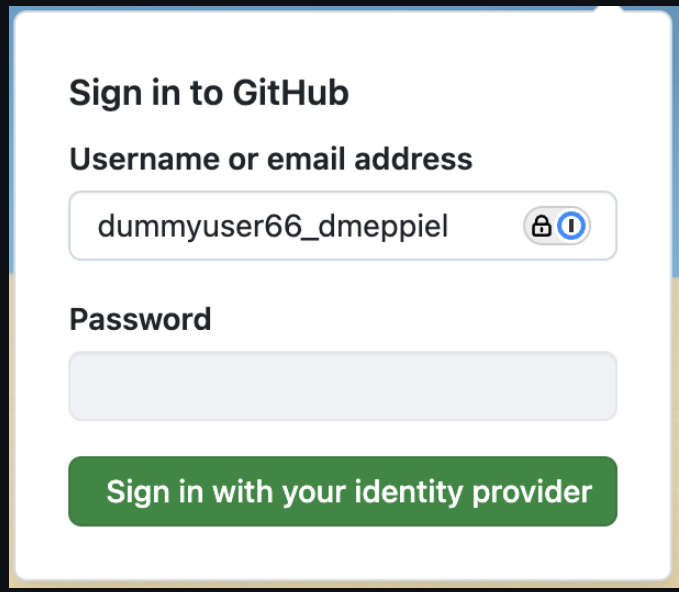
Try it out!

1. Login on your machine with the **Surface** credentials, open a browser

2. Go to: https://github.com/**org-dummyuser<X>-dmeppiel**
   Example: https://github.com/**org-dummyuser66-dmeppiel**

3. Put in your GitHub handle
   Example: dummyuser66_dmeppiel

4. Use the provided **Microsoft** credentials to login
   Example: dummyuser66@dmeppielorg.onmicrosoft.com



2-min

Scan the QR or use link to join

https://forms.office.-com/r/LA4GR23s55

Copy link

20 responses submitted

Are you up and running?

100%

Yep, all good to go!

Treemap | Bar

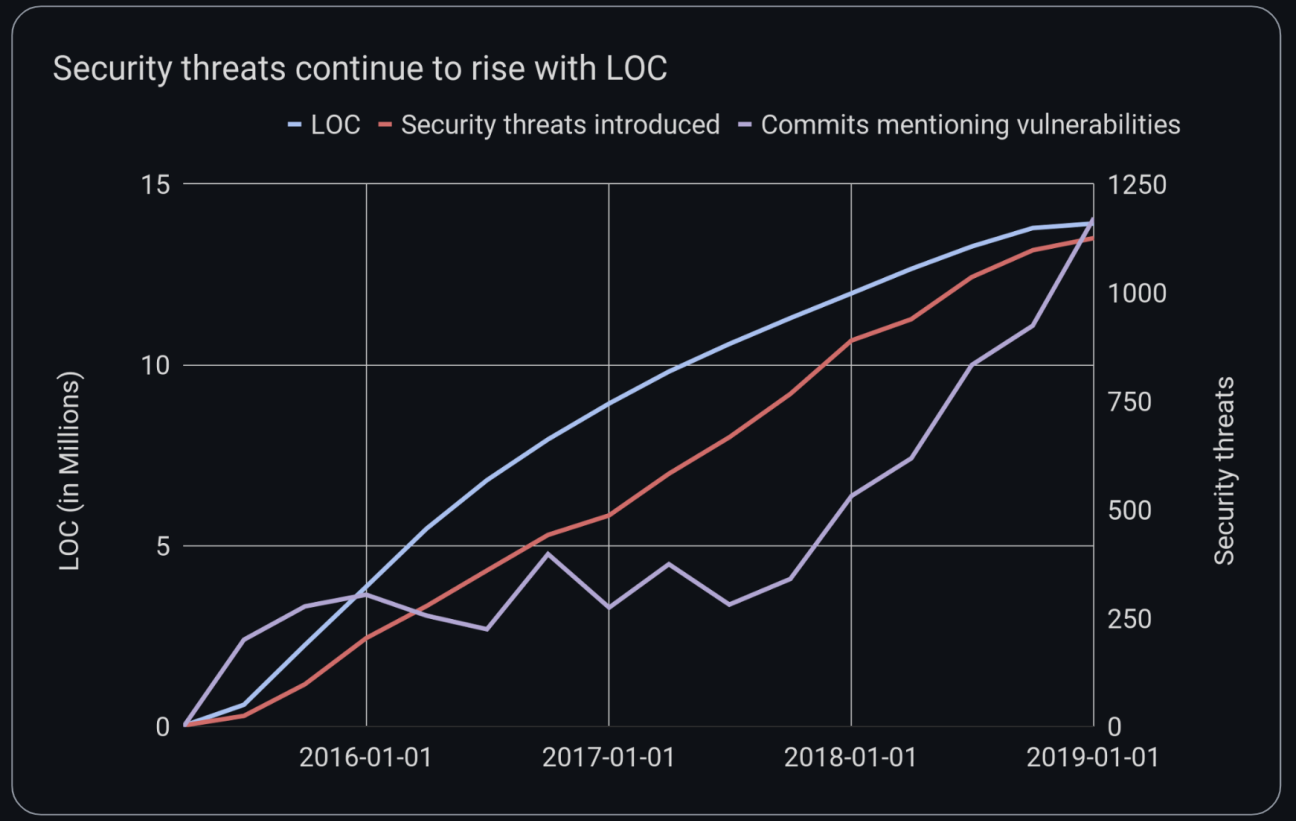
1 of 1

Why are you here?

- Learn what **GitHub Advanced Security** is!
- Learn and understand how to configure GitHub Advanced Security for a repository
- Learn how to block vulnerable code before it reaches production
- Discover how to scale GitHub Advanced Security setup and policies for thousands of repositories

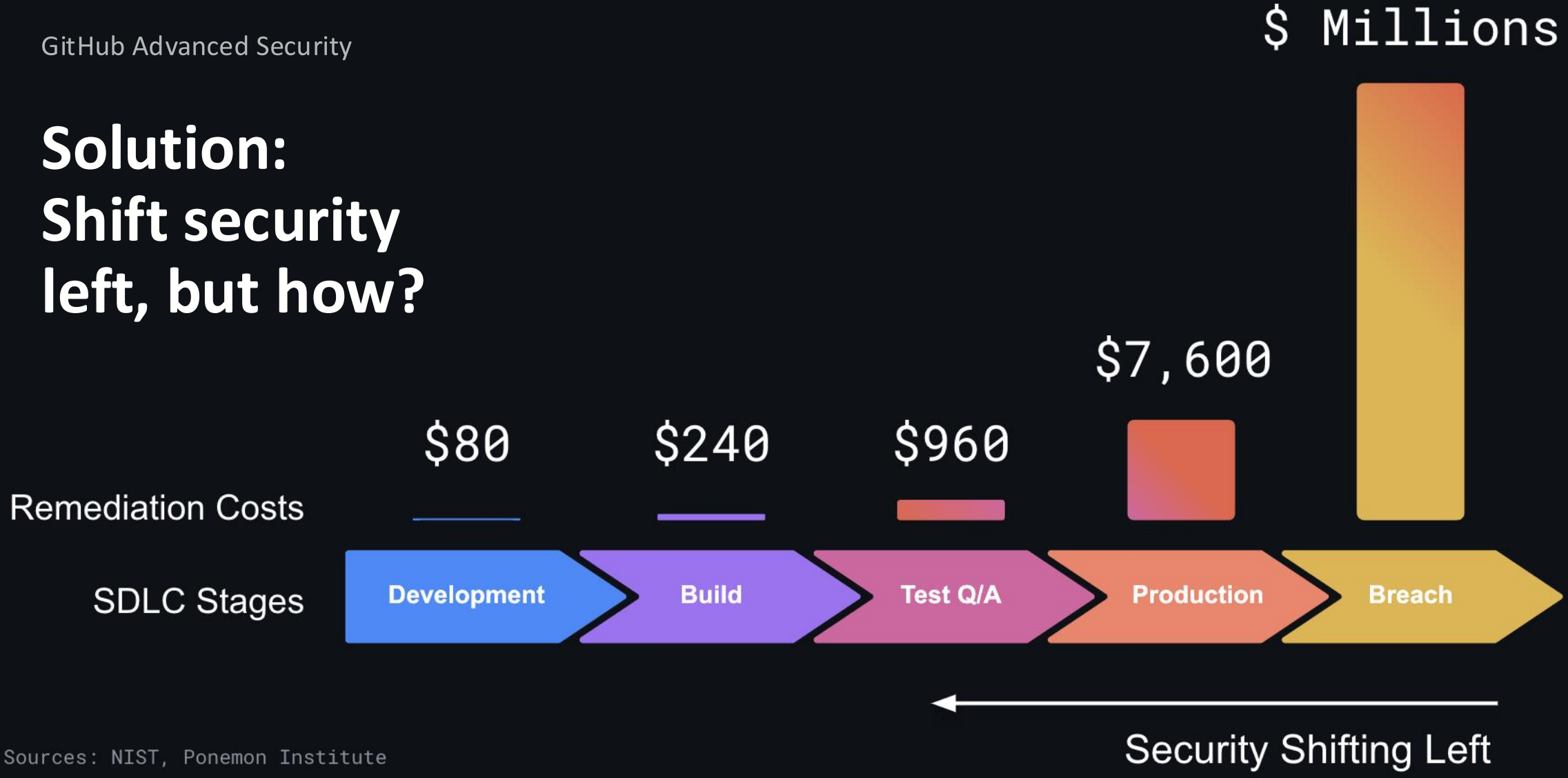
GitHub Advanced Security

Despite increasing developer awareness, security threats continue to rise



GitHub Advanced Security

Solution: Shift security left, but how?



Sources: NIST, Ponemon Institute

Solution: GitHub Advanced Security

Community-powered & AI-powered security and compliance

Dependency insights

Real-time inventory

License compliance

Vulnerability alerting

Vulnerability Management

Automated code scanning

Private secret scanning

Secrets push protection

Largest vulnerability database

Automated security updates

CodeQL

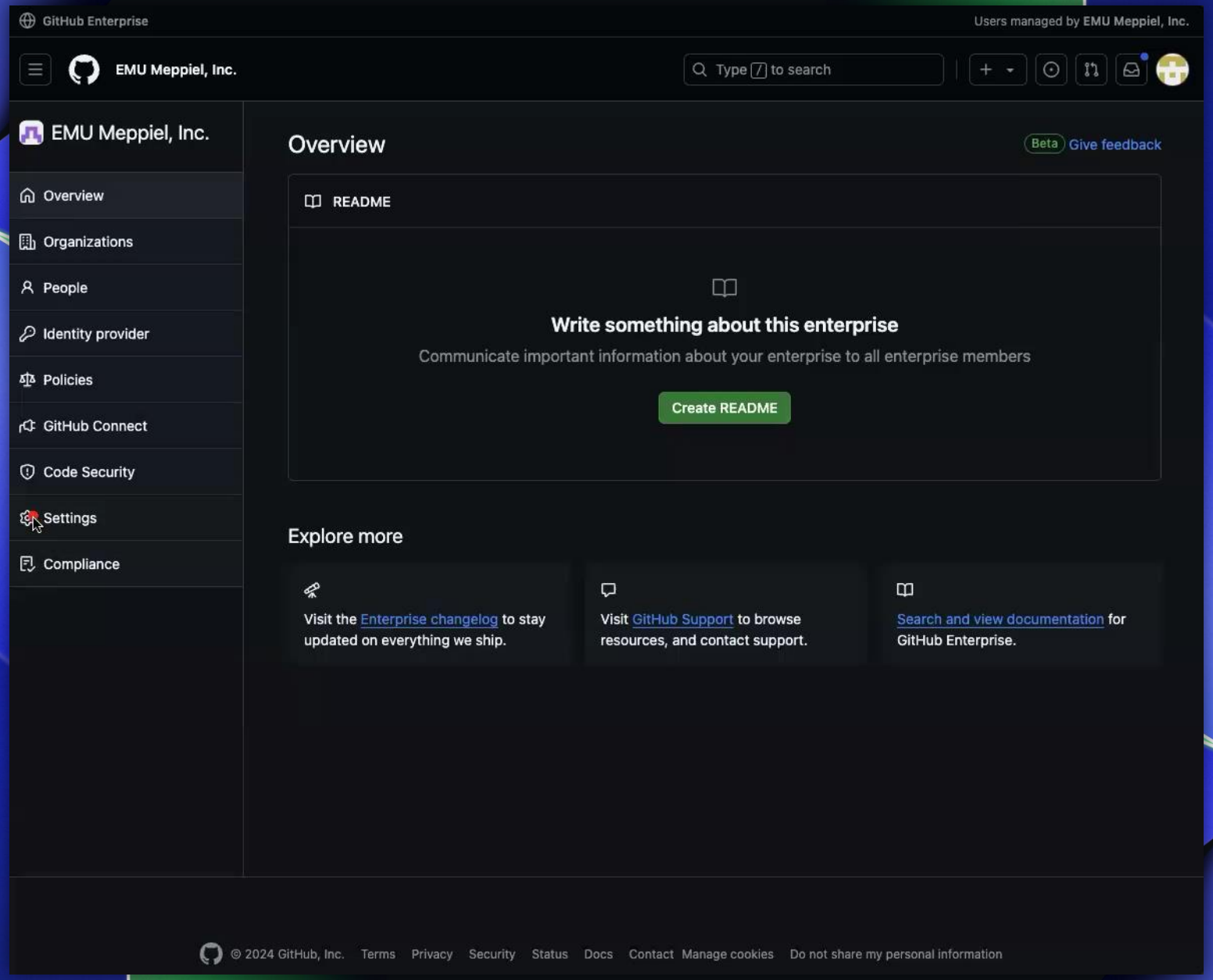
World’s most advanced code analysis

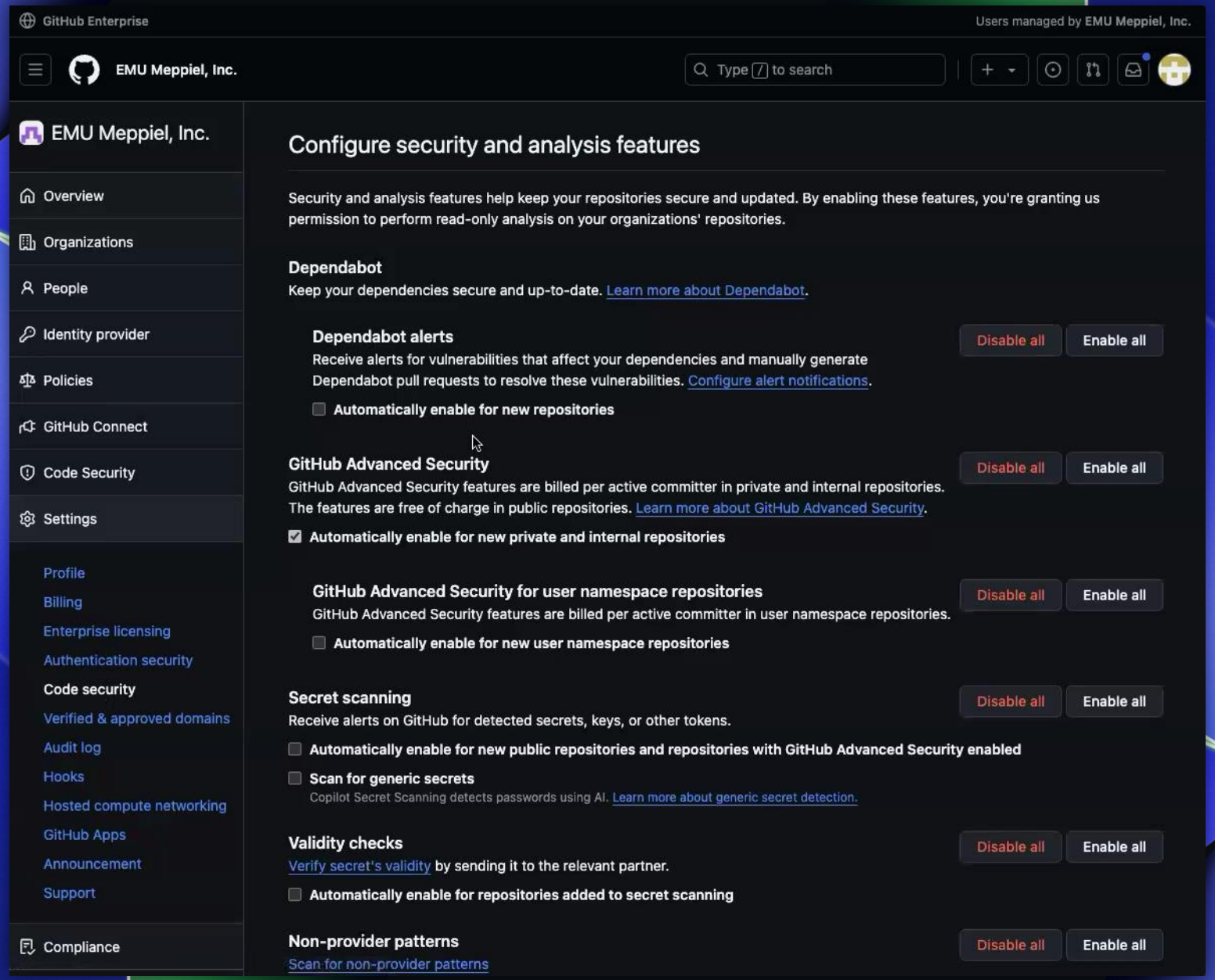
Vulnerability hunting tool

Community of top security experts

Enabling at Enterprise Level

Already done for you in the workshop environments!


GitHub Enterprise
Users managed by EMU Meppiel, Inc.
EMU Meppiel, Inc.
Type / to search
EMU Meppiel, Inc.
Overview
Organizations
People
Identity provider
Policies
GitHub Connect
Code Security
Settings
Compliance
Overview
Beta
Give feedback
README
Write something about this enterprise
Communicate important information about your enterprise to all enterprise members
Create README
Explore more
Visit the Enterprise changelog to stay updated on everything we ship.
Visit GitHub Support to browse resources, and contact support.
Search and view documentation for GitHub Enterprise.
© 2024 GitHub, Inc.
Terms
Privacy
Security
Status
Docs
Contact
Manage cookies
Do not share my personal information


GitHub Enterprise
Users managed by EMU Meppiel, Inc.
EMU Meppiel, Inc.
Type / to search
EMU Meppiel, Inc.
Overview
Organizations
People
Identity provider
Policies
GitHub Connect
Code Security
Settings
Profile
Billing
Enterprise licensing
Authentication security
Code security
Verified & approved domains
Audit log
Hooks
Hosted compute networking
GitHub Apps
Announcement
Support
Compliance
Configure security and analysis features
Security and analysis features help keep your repositories secure and updated. By enabling these features, you're granting us permission to perform read-only analysis on your organizations' repositories.
Dependabot
Keep your dependencies secure and up-to-date. Learn more about Dependabot.
Dependabot alerts
Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. Configure alert notifications.
Disable all
Enable all
Automatically enable for new repositories
GitHub Advanced Security
GitHub Advanced Security features are billed per active committer in private and internal repositories. The features are free of charge in public repositories. Learn more about GitHub Advanced Security.
Disable all
Enable all
Automatically enable for new private and internal repositories
GitHub Advanced Security for user namespace repositories
GitHub Advanced Security features are billed per active committer in user namespace repositories.
Disable all
Enable all
Automatically enable for new user namespace repositories
Secret scanning
Receive alerts on GitHub for detected secrets, keys, or other tokens.
Disable all
Enable all
Automatically enable for new public repositories and repositories with GitHub Advanced Security enabled
Scan for generic secrets
Copilot Secret Scanning detects passwords using AI. Learn more about generic secret detection.
Validity checks
Verify secret's validity by sending it to the relevant partner.
Disable all
Enable all
Automatically enable for repositories added to secret scanning
Non-provider patterns
Scan for non-provider patterns
Disable all
Enable all

Learn how to configure GitHub Advanced Security for a Repository

Exercise coming up!

Poll question

How difficult do you find it to configure security protections for your repos?

30-sec

gh.io/AAs60mr

Scan the QR or use link to join

https://forms.office.-com/r/39isdApkR3

Copy link

23 responses submitted

How difficult do you find it to configure security protections for your repos?

2.87

13% 21% 39% 17% 8%

1 of 1

Watch and chill 

Try it out!

- Go to the exercise file

Done already 🥳 ?

→ Help your neighbour out! 🤷

gh.io/u24-exercise-1

10-min

Learn how to configure GitHub Advanced Security for a Repository

What have we done

1. **Enabled Dependabot**

2. **Added security measures on the pull request**
   - Created a workflow including the `Dependency review` action

3. **Enabled Code Scanning**
   - Default setup

4. **Enabled Secret Scanning**

Detecting vulnerabilities in production is too late; breaches may have occurred and fixing them is exponentially costlier

NIST, Ponemon Institute

Understand ways to block vulnerable code before it reaches production

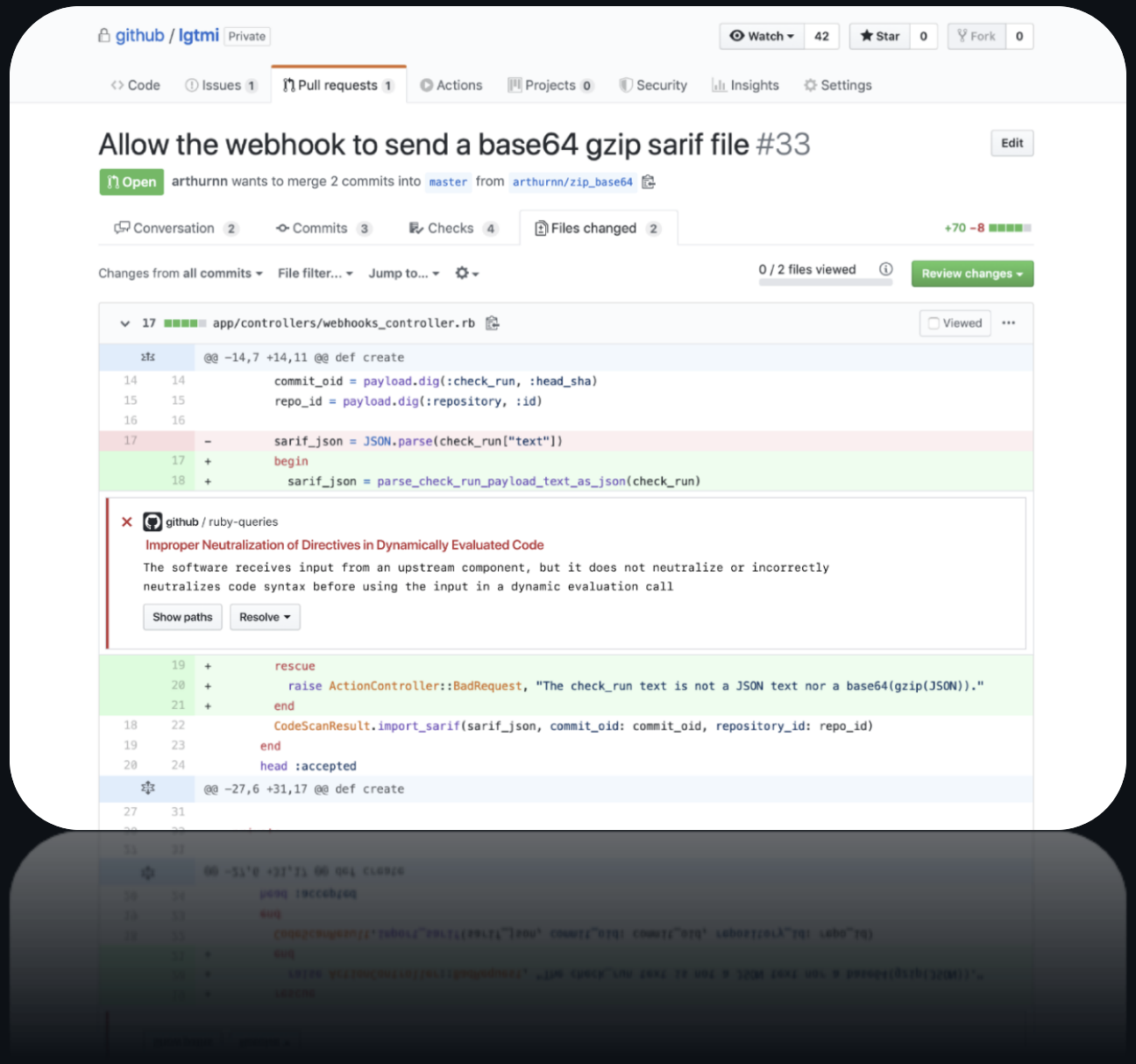
Exercise coming up!

GitHub Advanced Security

Security built into the Developer Lifecycle

“

It is all about keeping your code secure through a Pull Request – or earlier



Cuno Reijman

Customer Success Architect | GitHub

Poll question

What ‘**bad**’ or ‘**dirty**’ things did you do (or found) in code that made it all the way into **production**?

30-sec

gh.io/AAs4awp

Scan the QR or use link to join

https://forms.office.-com/r/CPMNDp6PbS

Copy link

25 responses submitted

What ‘bad’ or ‘dirty’ things did you do (or found) in code that made it all the way into production?

Scan the QR or use link to join

https://forms.office.-com/r/CPMNDp6PbS

Copy link

25 responses submitted

Which had the most impact to remediate / fix those in production?

- Hardcoded Secrets or Configuration values
- Implemented Anti Patterns / Bad practices (intentional/ unintentional)
- Use of Unknown or Old/Unsafe Packages

Watch and chill 

Try it out!

- Go to the exercise file →

Done already 🥳 ?

→ Help your neighbour out! 🙇

gh.io/u24-exercise-2

10-min

Understand ways to block vulnerable code before it reaches production

What have we done

1. **Repository branch ruleset**
    - Protect the `main` branch
    - Require a *Pull Request* before merging
    - Require succesfull `*Status Checks*`
    - Require successfull `*Code Scanning*` results
        - No vulnerabilities

2. **Enabled Secret Push Protection**

Discover how to scale GitHub Advanced Security to thousands of Repositories

Exercise coming up!

Poll question

Do enterprise-wide code security policies generally make developers unhappier?

30-sec

gh.io/AAs6g28

0 response submitted

Do enterprise-wide code security policies generally make developers unhappier?

Treemap Bar

1 of 1

Watch and chill 

Try it out!

- Go to the exercise file →

Done already 🥳 ?

→ Help your neighbour out! 🤷

gh.io/u24-exercise-3

15-min

What have we done

1. **Code security configurations:** Applied GitHub' recommended to be used as the default on *new* and *existing* repositories

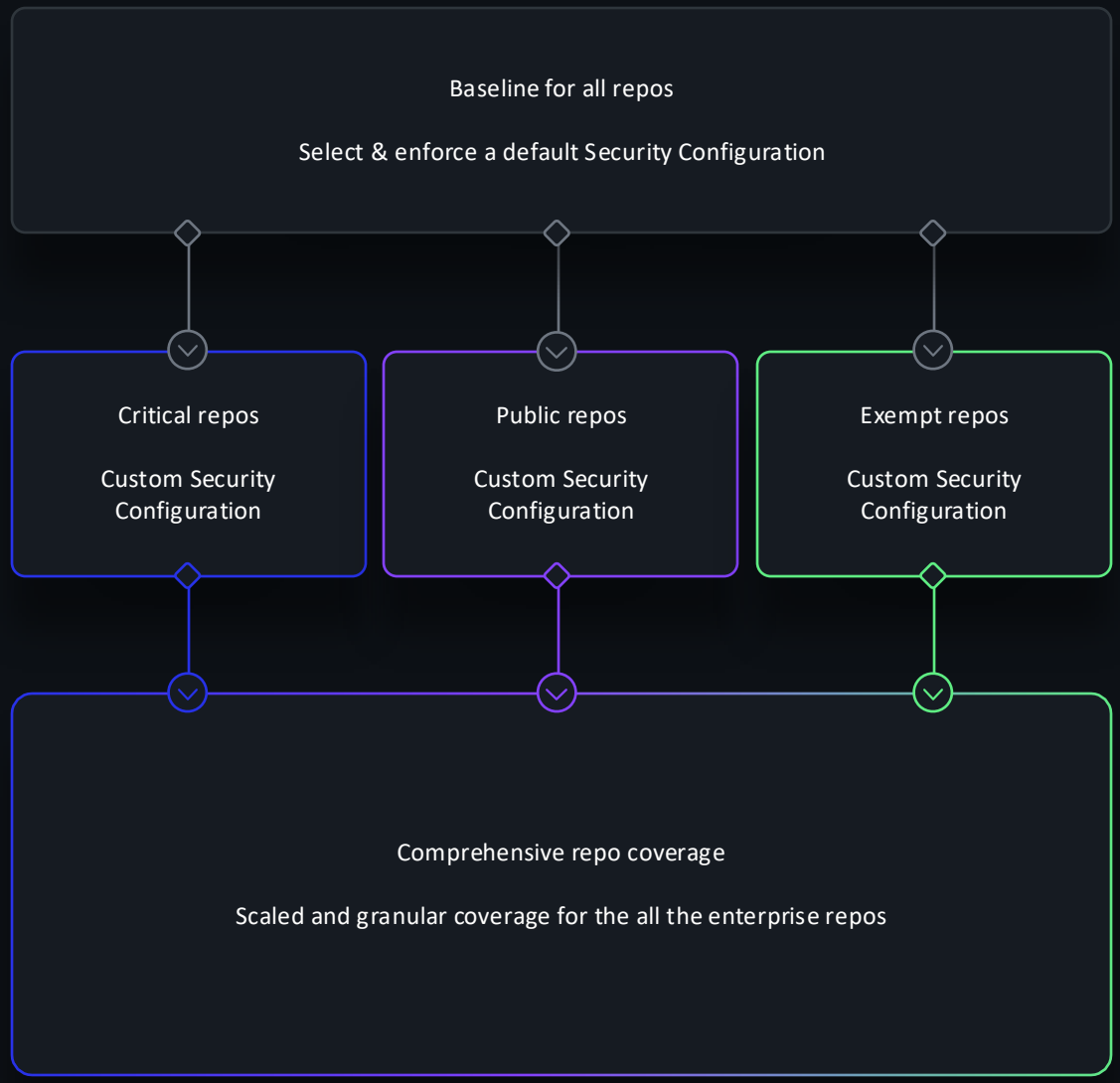
2. **Repository custom properties:** Created and applied to classify a repository and/or a group of repositories

3. **Organization ruleset:** Created and applied an organization ruleset to enforce checks standards to a classified set of repositories through repository custom properties

Scaling code security

At-scale code security meets flexibility

Security configurations and Repo Custom Properties allow tuning code security setups to the needs of each organization, dev team and codebase.



What have we done - Overall

Learn and understand how to configure GitHub Advanced Security for a repository

1. Enabled Dependabot
2. Added dependency review to the pull request
3. Enabled Secret Scanning

Learn how to block vulnerable code before it reaches production

1. Repository branch ruleset
2. Enabled Secret Push Protection

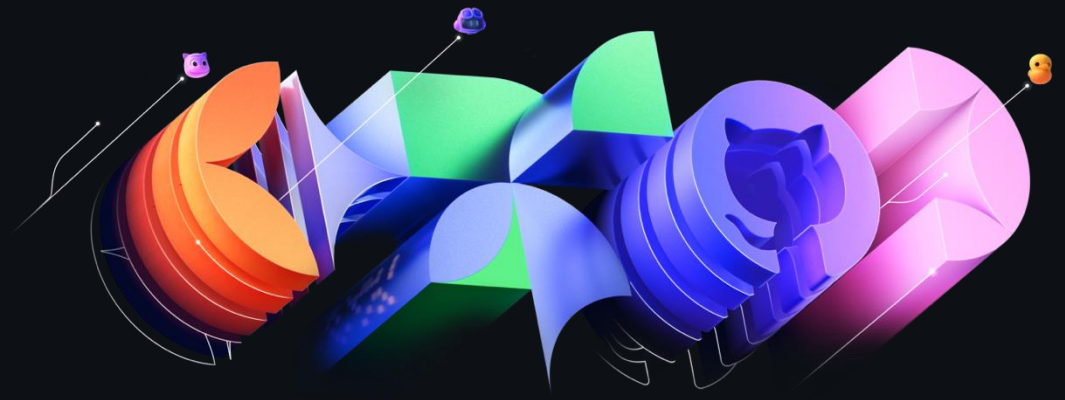
Discover how to scale GitHub Advanced Security setup and policies for thousands of repositories

1. Code security configurations
2. Repository custom properties
3. Organization ruleset

Workshop environment

- Leave the Surface 💻 in the room!
- Not available anymore after today!

UNIVERSE'24



Getting Ready for GitHub Certifications

Enterprise code security 101: Getting started with GitHub Advanced Security

GitHub Certifications

resources.github.com/learn/certifications

Prepare with Confidence

- Study guides for each exam
- Exam doimain breakdown
- Domain learning objectives
- Links to learning content
- Practice exams (coming soon)

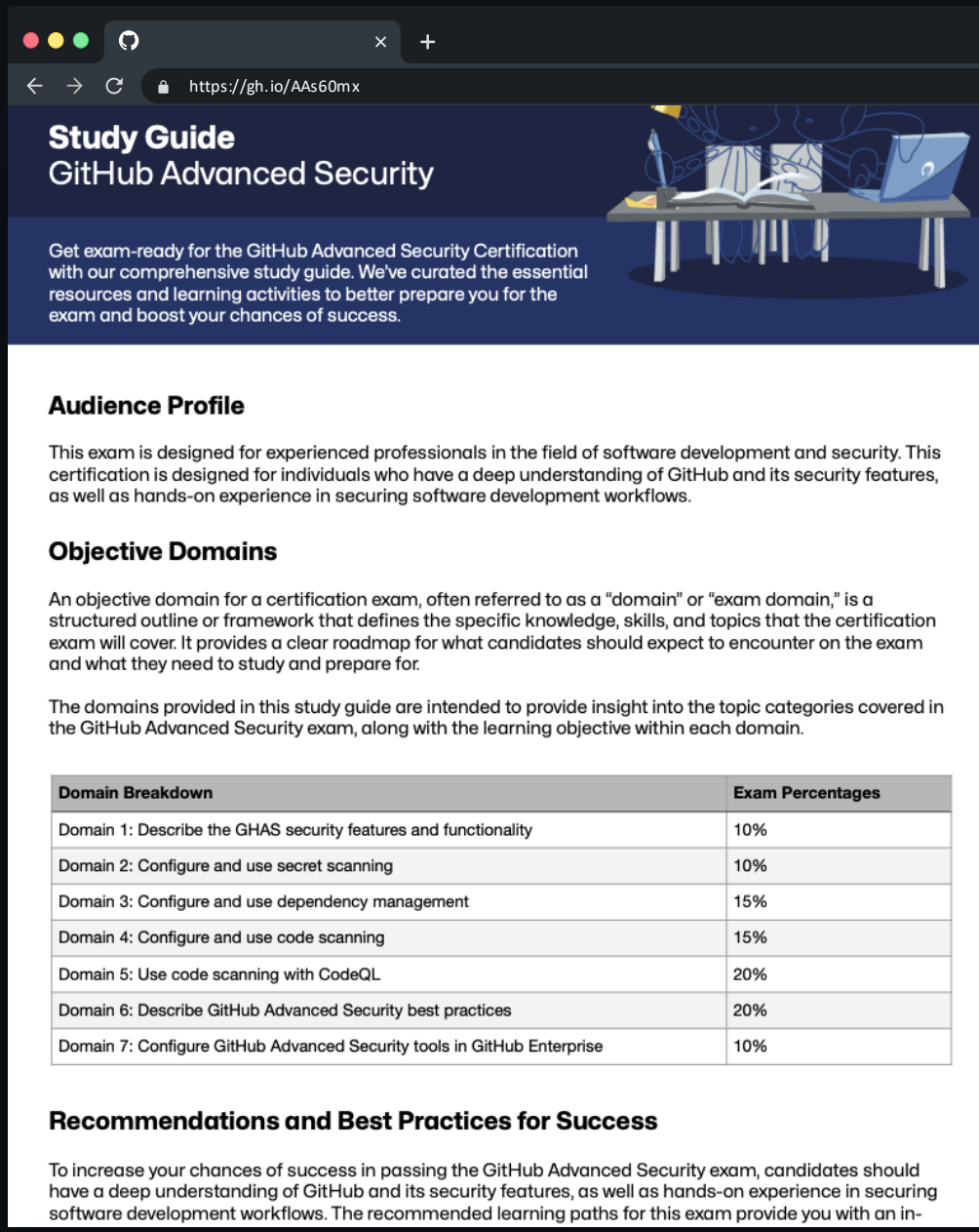
gh.io/AAs4awp

Enterprise code security 101: Getting started with GitHub Advanced Security

Certification: GitHub Advanced Security

gh.io/AAs60mv

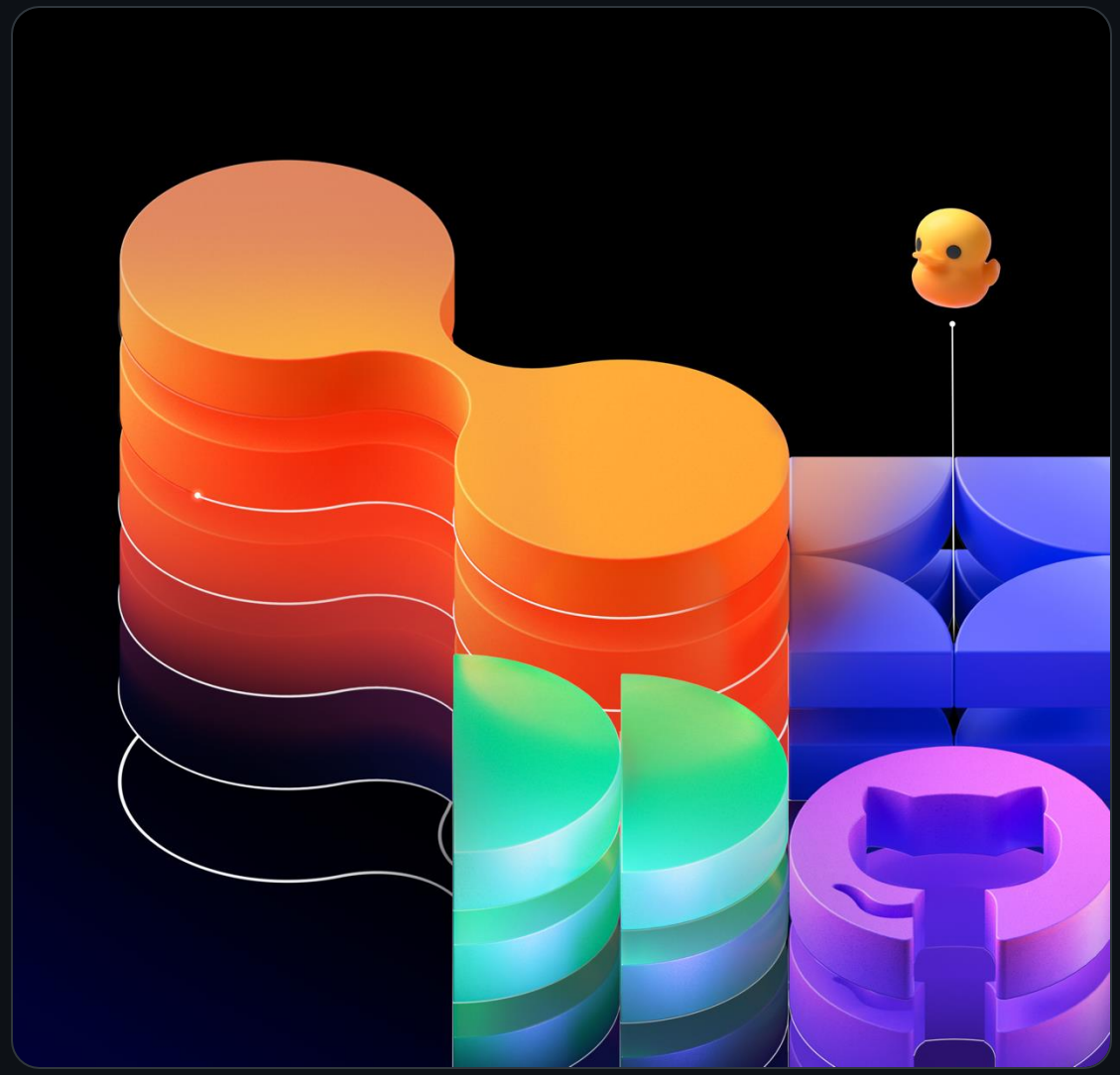
gh.io/AAs5sx4



Certification participation

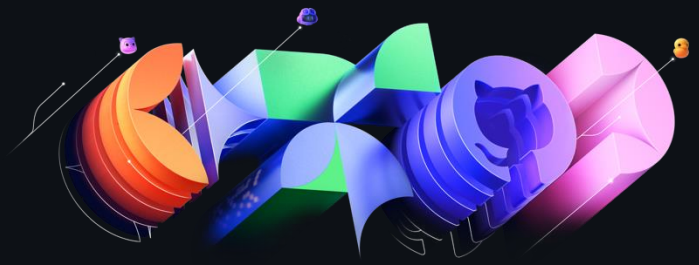
Unlock your GitHub Certification

- Purchase today at a discounted rate: Only $49 to test in-person at Universe or remotely
    - Remote exams: Must be scheduled by December 31, 2024



Certification: GitHub Advanced Security

- ✅ Domain 1: Describe the GHAS security features and functionality
- ✅ Domain 2: Configure and use secret scanning
- ✅ Domain 3: Configure and use dependency management
- ✅ Domain 4: Configure and use code scanning
- ⚠️ Domain 5: Use code scanning with CodeQL
- ✅ Domain 6: Describe GitHub Advanced Security best practices
- ✅ Domain 7: Configure GitHub Advanced Security tools in GitHub Enterprise



We want to hear from you!

Take the session survey by visiting the attendee portal so we can continue to make your Universe experience cosmic!

Thank you!

Cuno Reijman - @equalizer999

Customer Success Architect | GitHub

Daniel Meppiel - @danielmeppiel

Senior Customer Success Architect | GitHub