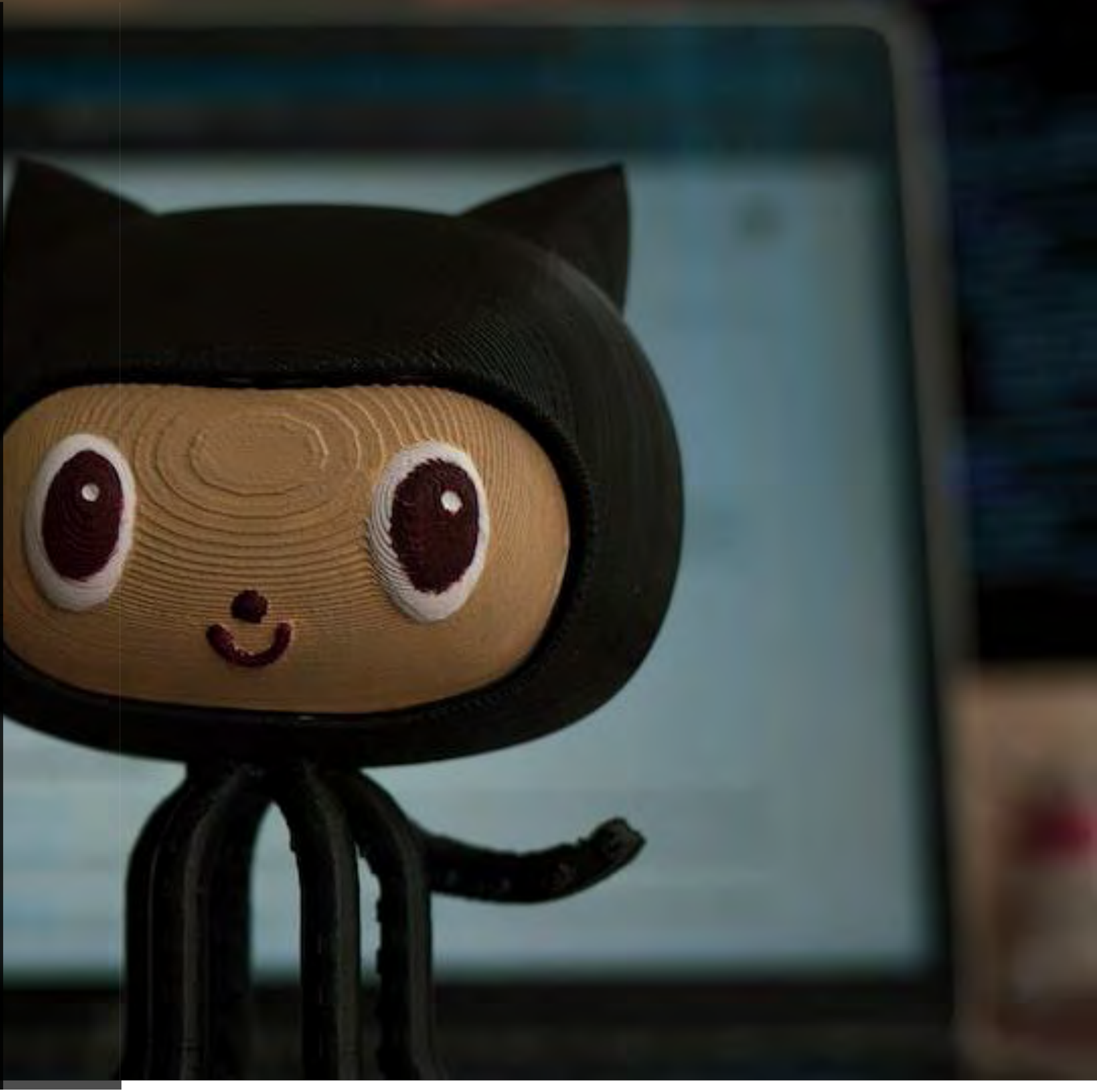
SPS COMMERCE

FORTIFYING YOUR CODEBASE WITH GITHUB

“A YEAR FROM NOW YOU WILL WISH YOU HAD STARTED TODAY.” (KAREN LAMB)



TRAVIS GOSSELIN

DISTINGUISHED SOFTWARE ENGINEER

DEVELOPER EXPERIENCE

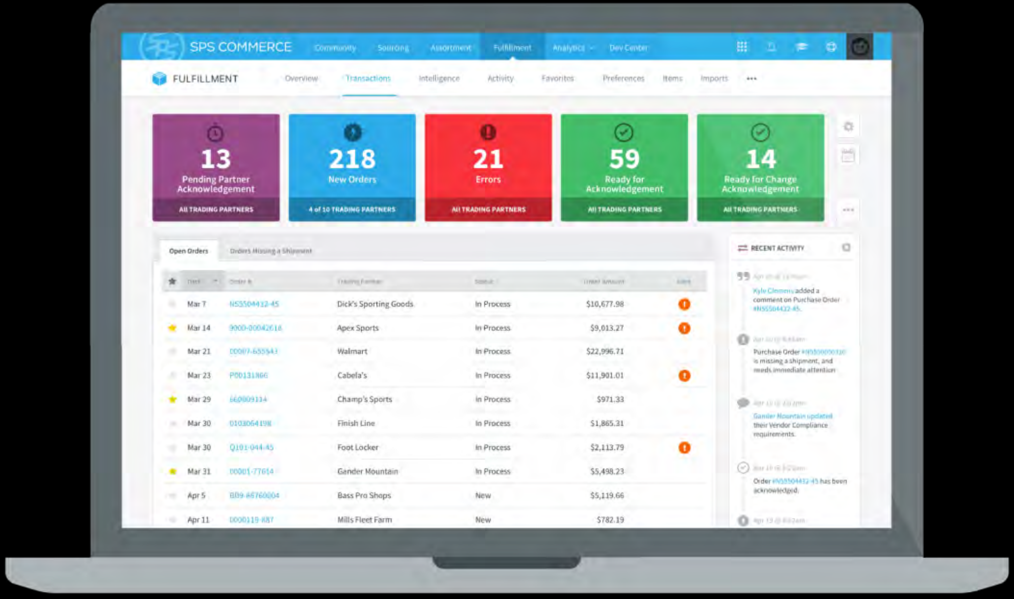
travisgosselin.com

linkedin.com/in/travisgosselin

@travisjgosselin

SPS COMMERCE

INFINITE RETAIL POWER™



★	Date	Order #	Trading Partner	Status	Order Amount	Alert
	Mar 7	NS5504432-45	Dick's Sporting Goods	In Process	$10,677.98	!
★	Mar 14	9000-00042616	Apex Sports	In Process	$9,013.27	!
	Mar 21	00007-655543	Walmart	In Process	$22,996.71	
	Mar 23	P00131866	Cabela's	In Process	$11,901.01	!
★	Mar 29	660009134	Champ's Sports	In Process	$971.33	
	Mar 30	0103064198	Finish Line	In Process	$1,865.31	
	Mar 30	Q101-044-45	Foot Locker	In Process	$2,113.79	!
★	Mar 31	00001-77614	Gander Mountain	In Process	$5,498.23	
	Apr 5	809-A6760004	Bass Pro Shops	New	$5,119.66	
	Apr 11	0000119-887	Mills Fleet Farm	New	$782.19	

Kyle Clemens added a comment on Purchase Order #NS5504432-45.

Purchase Order #NS50000032 is missing a shipment, and needs immediate attention

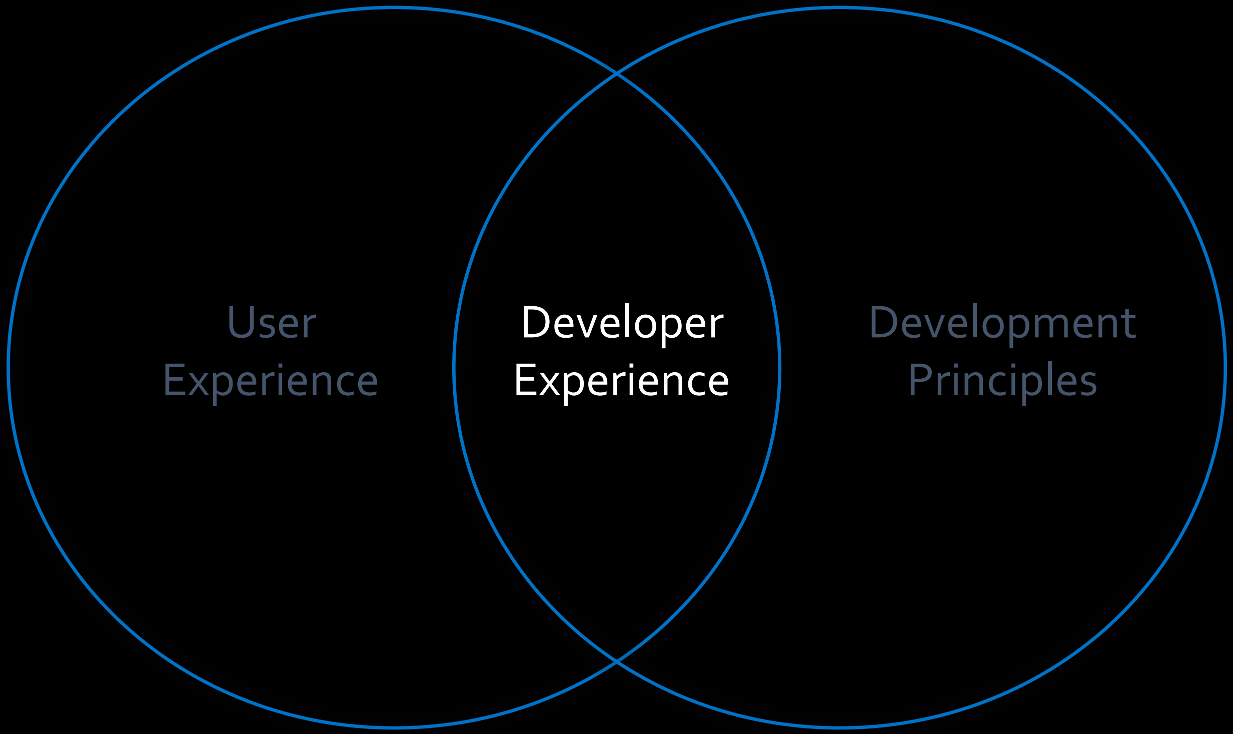
Gander Mountain updated their Vendor Compliance requirements.

Order #NS5504432-45 has been acknowledged.

> "Developer Experience is the activity of studying, improving and optimizing how developers get their work done."
>
> theappslab.com (2017)

DEVELOPER EXPERIENCE

WHAT IS THAT…EXACTLY?



> "Developers work in rainforests, not planned gardens."
>
> [a16z.com](a16z.com)

CODING REALITY

We Need Help

> "Code time is often undervalued, continually interrupted, and almost wholly unmeasured."
>
> Mason Mclead, CTO, Software.com

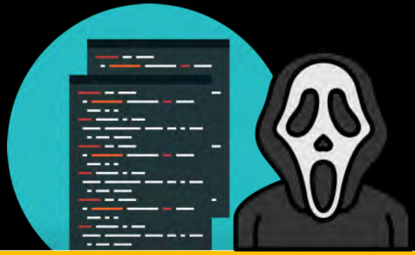
Overhead

- Meetings
- Operational
- Management
- Stuff

Security

- Supply Chain
- SAST
- DAST
- Remediation

Writing New or Updating Existing Coding



Developers Code (Avg): 52 min / Day

Infrastructure

- Configuration
- Dev Environment
- CI/CD
- IaC

Maintenance

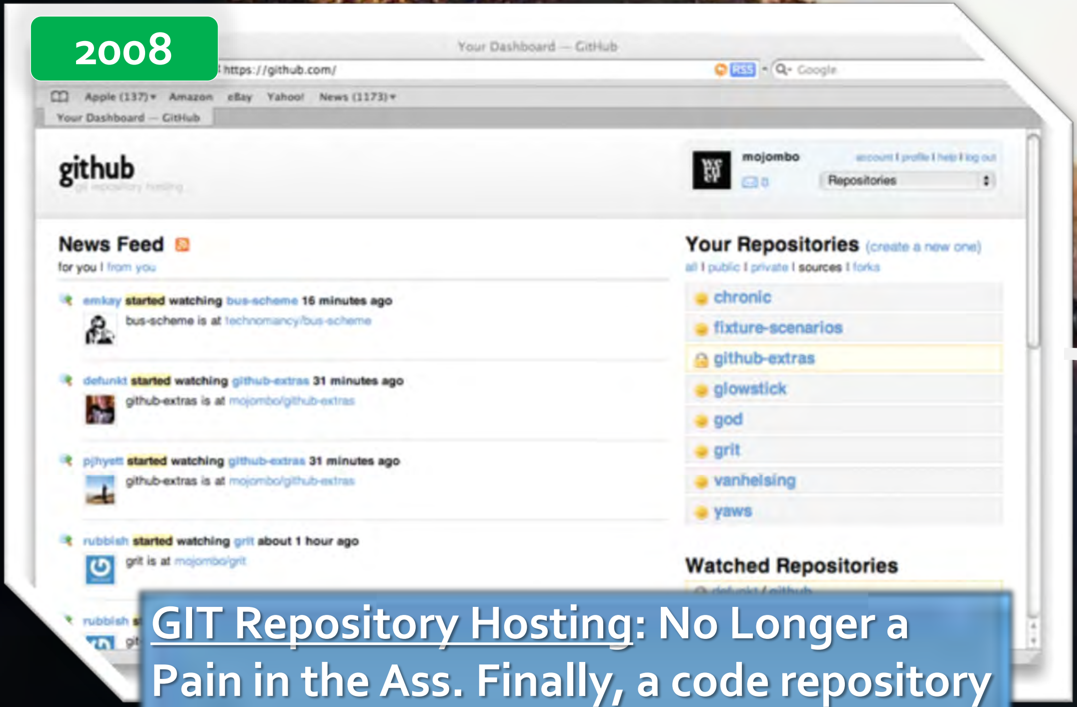
- Code Quality
- Tech Debt
- Feature Flags
- Testing

Improve Daily Work

- **Fix Bottlenecks**
- **More Automation**
- **Reduce Feedback Cycle Duration**
- **Codify Best Practices**
- **Effective Documentation**
- **Streamline Collaboration**

https://www.software.com/reports/code-time-report

2008



Your Dashboard — GitHub

https://github.com/

Apple (137) ▾ Amazon eBay Yahoo! News (1173) ▾

Your Dashboard — GitHub

github
git repository hosting

mojombo account | profile | help | log out
0
Repositories

News Feed
for you | from you

emkay started watching bus-scheme 16 minutes ago
bus-scheme is at technomancy/bus-scheme

defunkt started watching github-extras 31 minutes ago
github-extras is at mojombo/github-extras

pjhyett started watching github-extras 31 minutes ago
github-extras is at mojombo/github-extras

rubbish started watching grit about 1 hour ago
grit is at mojombo/grit

rubbish

Your Repositories (create a new one)
all | public | private | sources | forks

- chronic
- fixture-scenarios
- github-extras
- glowstick
- god
- grit
- vanhelsing
- yaws

Watched Repositories

defunkt / github

GIT Repository Hosting: No Longer a Pain in the Ass. Finally, a code repository that works as well as you do.

2011

We focus on lowering the barriers of collaboration by building powerful features into our products that make it easier to contribute

GitHub

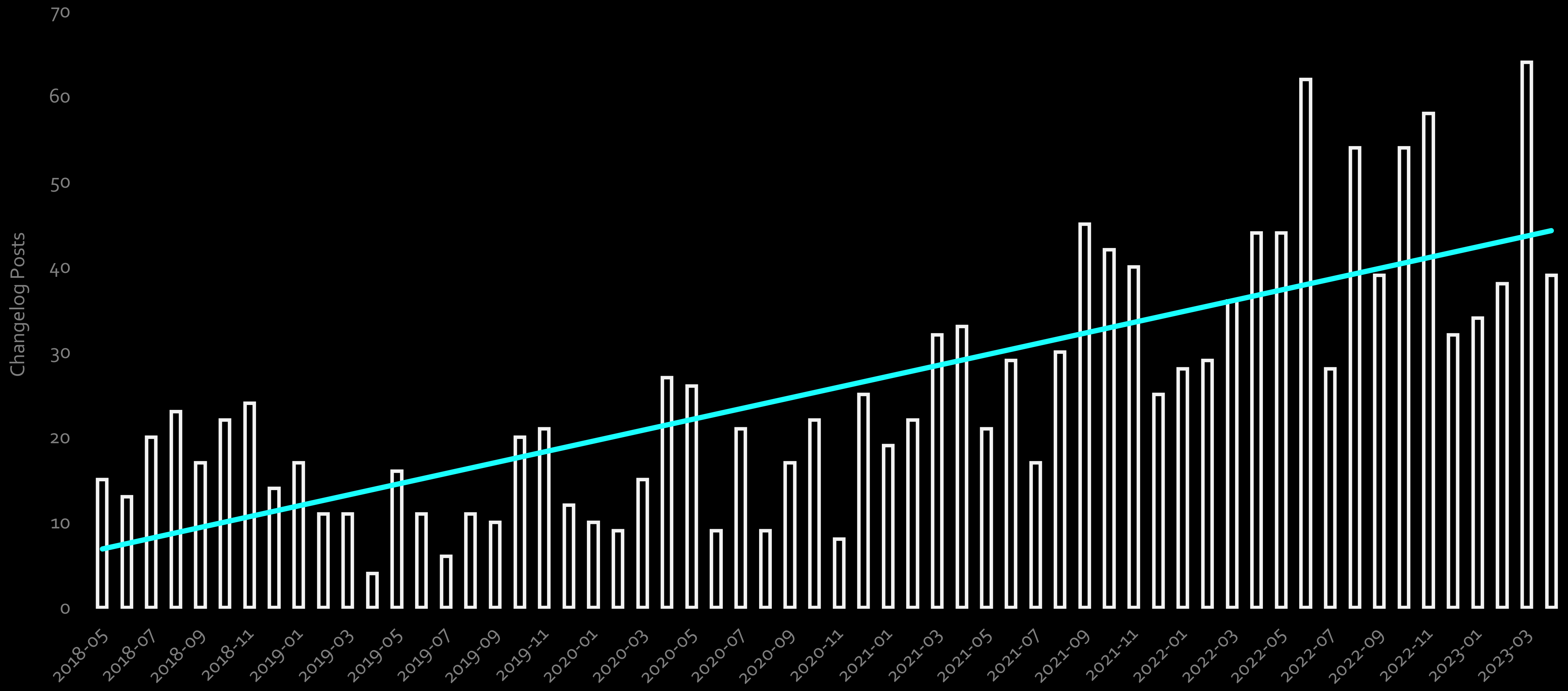
2018 The complete developer platform to build, scale, and deliver secure software.

Now The world's leading AI-powered developer platform.

Universe 2023

GITHUB FEATURE RELEASES

Features Released Per Month



https://twitter.com/ghchangelog

SECURITY & TOOLING

Maximizing Developer Productivity

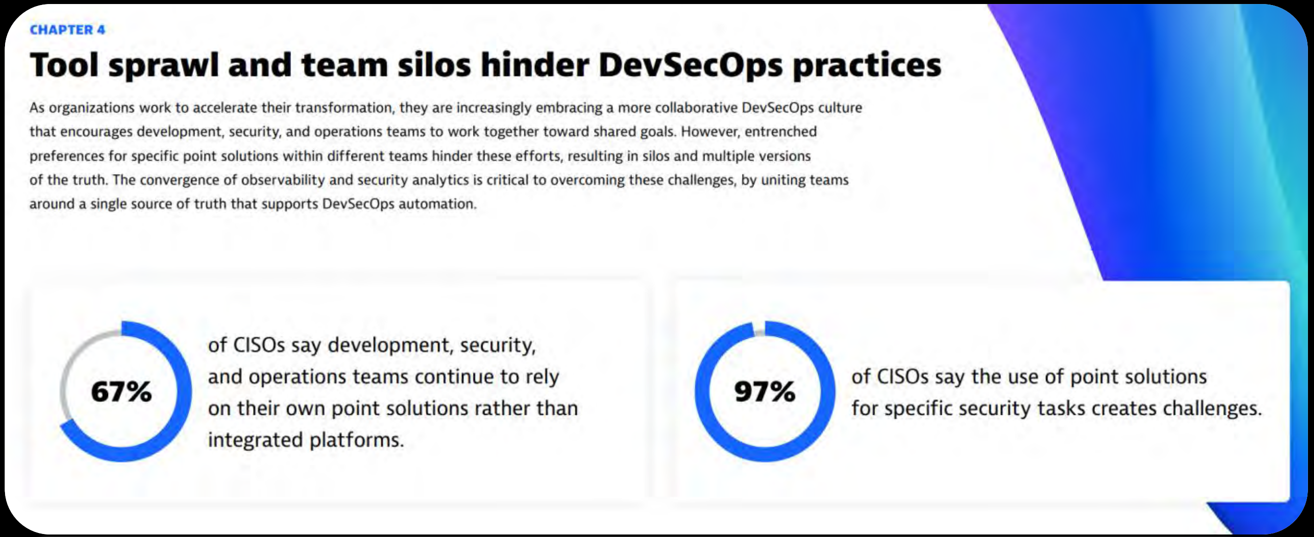
Gartner

2020 29%

Shift towards consolidating security vendors due to operational inefficiencies!

2022 75%

https://www.dynatrace.com/monitoring/platform/application-security/



CHAPTER 4

Tool sprawl and team silos hinder DevSecOps practices

As organizations work to accelerate their transformation, they are increasingly embracing a more collaborative DevSecOps culture that encourages development, security, and operations teams to work together toward shared goals. However, entrenched preferences for specific point solutions within different teams hinder these efforts, resulting in silos and multiple versions of the truth. The convergence of observability and security analytics is critical to overcoming these challenges, by uniting teams around a single source of truth that supports DevSecOps automation.

67% of CISOs say development, security, and operations teams continue to rely on their own point solutions rather than integrated platforms.

97% of CISOs say the use of point solutions for specific security tasks creates challenges.

Dependabot — *Transparency and automation to keep supply chain dependencies up to date.*

Advanced Security — *Centralization and transparency of code security, including static code analysis.*

2021 Over 90% of CVEs not present in most Recent Dependency Versions

DEPENDABOT

SUPPLY CHAIN SECURITY

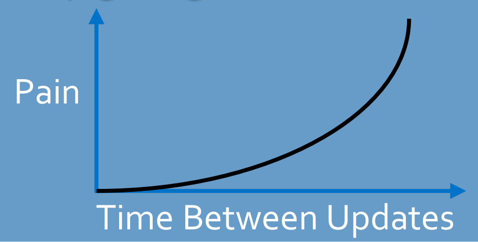
> "Monitor vulnerabilities in dependencies used in your project and keep your dependencies up-to-date with Dependabot."
>
> docs.github.com

Alerts

Security Updates

Version Updates

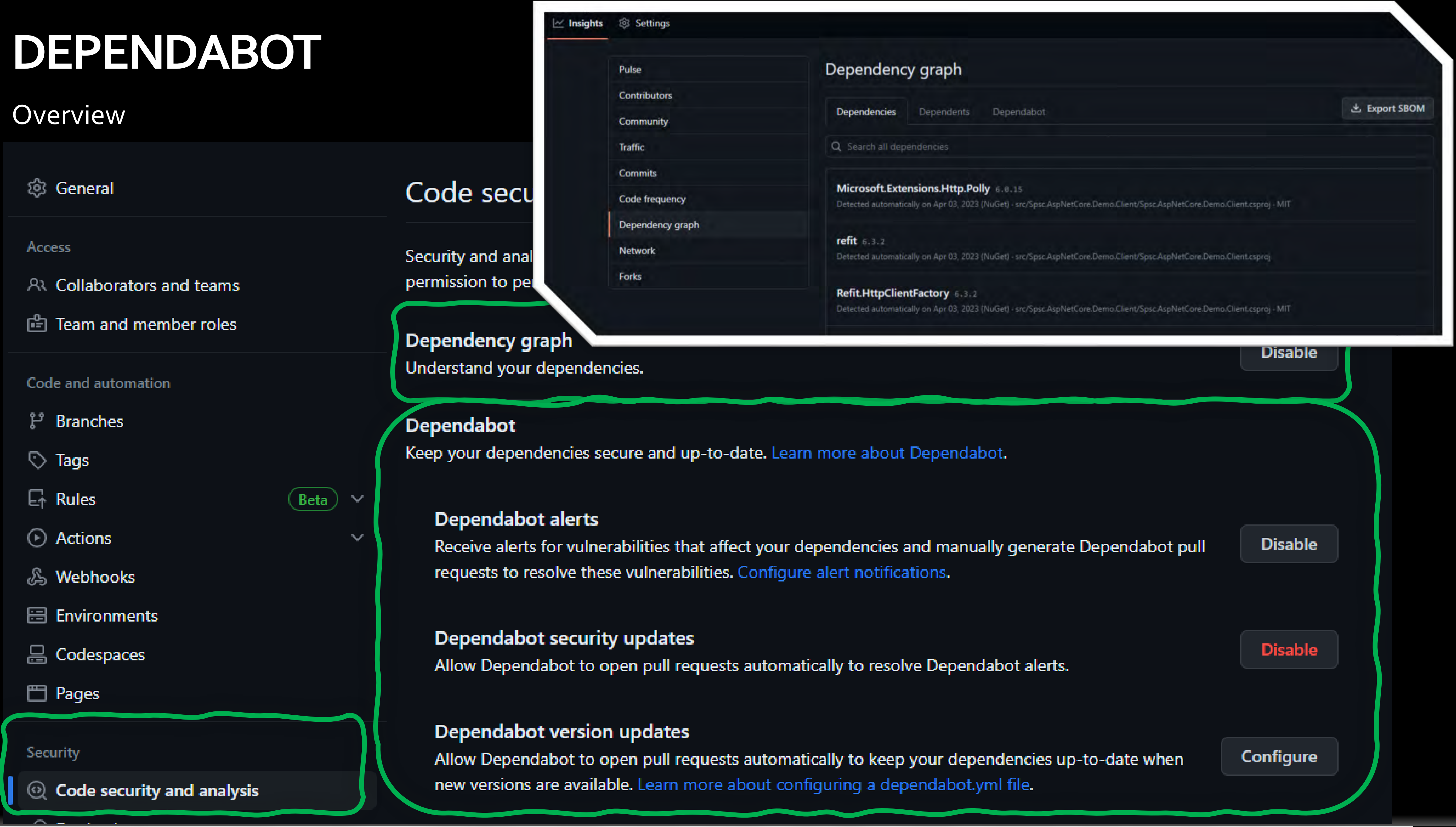
Updating dependencies is like going to the dentist. If you only go once every five years, it's really going to hurt.



mend.io

DEPENDABOT

Overview



Dependency graph

Microsoft.Extensions.Http.Polly 6.0.15
Detected automatically on Apr 03, 2023 (NuGet) · src/Spsc.AspNetCore.Demo.Client/Spsc.AspNetCore.Demo.Client.csproj · MIT

refit 6.3.2
Detected automatically on Apr 03, 2023 (NuGet) · src/Spsc.AspNetCore.Demo.Client/Spsc.AspNetCore.Demo.Client.csproj

Refit.HttpClientFactory 6.3.2
Detected automatically on Apr 03, 2023 (NuGet) · src/Spsc.AspNetCore.Demo.Client/Spsc.AspNetCore.Demo.Client.csproj · MIT

Code secu

Security and anal
permission to pe

Dependency graph
Understand your dependencies. Disable

Dependabot
Keep your dependencies secure and up-to-date. Learn more about Dependabot.

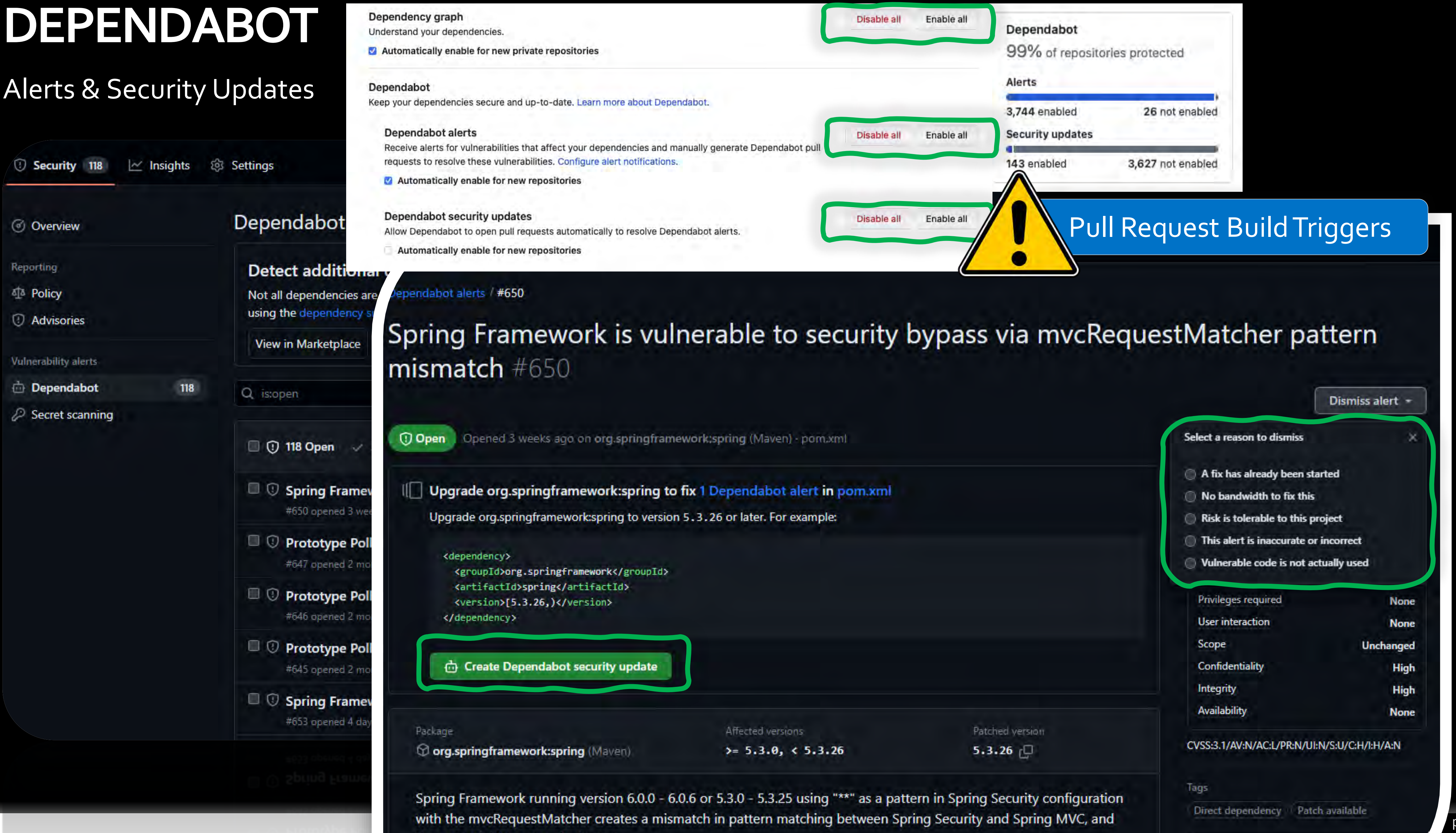
Dependabot alerts
Receive alerts for vulnerabilities that affect your dependencies and manually generate Dependabot pull requests to resolve these vulnerabilities. Configure alert notifications. Disable

Dependabot security updates
Allow Dependabot to open pull requests automatically to resolve Dependabot alerts. Disable

Dependabot version updates
Allow Dependabot to open pull requests automatically to keep your dependencies up-to-date when new versions are available. Learn more about configuring a dependabot.yml file. Configure

DEPENDABOT

Alerts & Security Updates



Dependency graph
Understand your dependencies.
☑ Automatically enable for new private repositories

Disable all | Enable all

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.
☑ Automatically enable for new repositories

Disable all | Enable all

Dependabot security updates
Allow Dependabot to open pull requests automatically to resolve Dependabot alerts.
□ Automatically enable for new repositories

Disable all | Enable all

Dependabot
99% of repositories protected

Alerts
3,744 enabled — 26 not enabled

Security updates
143 enabled — 3,627 not enabled

Pull Request Build Triggers

Dependabot

Detect additional

Not all dependencies are
using the dependency s

View in Marketplace

is:open

□ 118 Open	
□ Spring Framew	#650 opened 3 wee
□ Prototype Poll	#647 opened 2 mo
□ Prototype Poll	#646 opened 2 mo
□ Prototype Poll	#645 opened 2 mo
□ Spring Framew	#653 opened 4 day

Dependabot alerts / #650

Spring Framework is vulnerable to security bypass via mvcRequestMatcher pattern mismatch #650

Dismiss alert

Open Opened 3 weeks ago on org.springframework:spring (Maven) · pom.xml

Upgrade org.springframework:spring to fix 1 Dependabot alert in pom.xml

Upgrade org.springframework:spring to version 5.3.26 or later. For example:

```
<dependency>
  <groupId>org.springframework</groupId>
  <artifactId>spring</artifactId>
  <version>[5.3.26,)</version>
</dependency>
```

Create Dependabot security update

Package	Affected versions	Patched version
org.springframework:spring (Maven)	>= 5.3.0, < 5.3.26	5.3.26

Spring Framework running version 6.0.0 - 6.0.6 or 5.3.0 - 5.3.25 using "**" as a pattern in Spring Security configuration with the mvcRequestMatcher creates a mismatch in pattern matching between Spring Security and Spring MVC, and

Select a reason to dismiss

○ A fix has already been started
○ No bandwidth to fix this
○ Risk is tolerable to this project
○ This alert is inaccurate or incorrect
○ Vulnerable code is not actually used

Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	None

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

Tags
Direct dependency | Patch available

DEPENDABOT

Version Updates

> "Dependabot version updates are automated pull requests that keep your dependencies updated, even when they don't have any vulnerabilities."
>
> docs.github.com

2023 83% of security teams don't have access to a fully accurate SBOM in real time! dynatrace

Supported Ecosystems

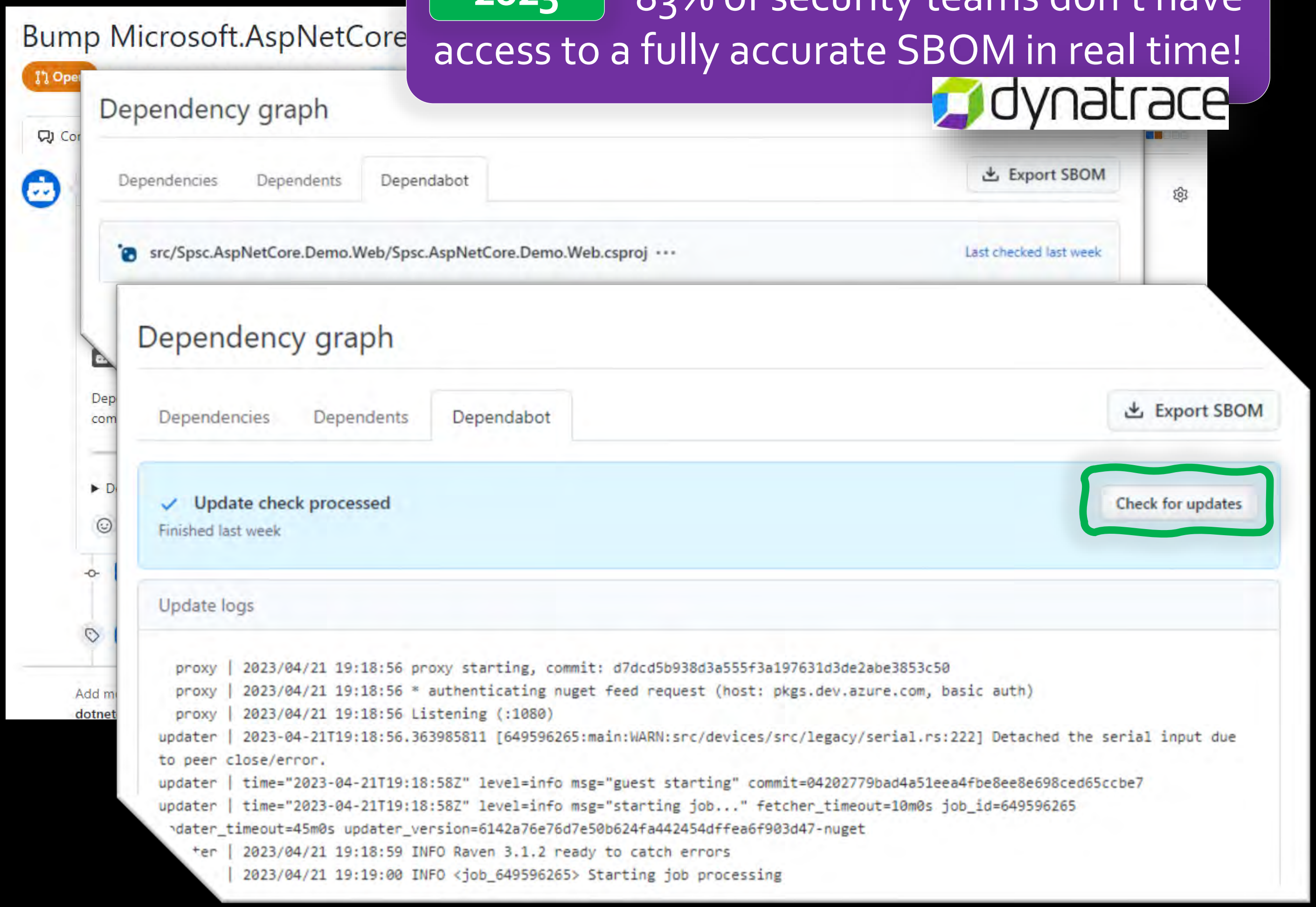
- gomod
- maven
- gradle
- npm
- nuget
- pip
- elm
- ...
- docker
- terraform
- github actions
- git submodule
- helm? dependabot/dependabot-core/issues/2237

Private Feed Configuration with Secrets

Update Schedule

Metadata Configuration

Behavior Configuration



Dependency graph

src/Spsc.AspNetCore.Demo.Web/Spsc.AspNetCore.Demo.Web.csproj ··· Last checked last week

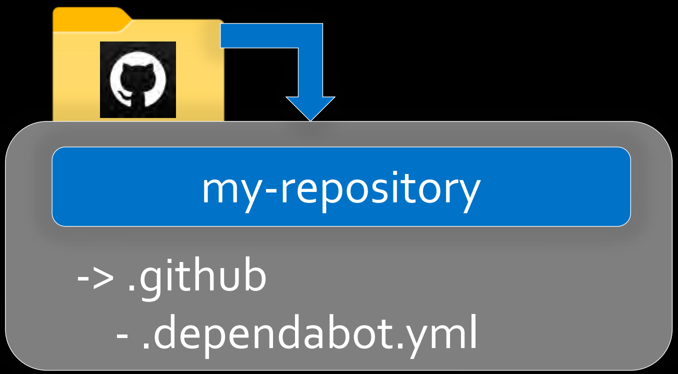
Dependency graph

✓ Update check processed
Finished last week

Update logs

```
  proxy | 2023/04/21 19:18:56 proxy starting, commit: d7dcd5b938d3a555f3a197631d3de2abe3853c50
  proxy | 2023/04/21 19:18:56 * authenticating nuget feed request (host: pkgs.dev.azure.com, basic auth)
  proxy | 2023/04/21 19:18:56 Listening (:1080)
updater | 2023-04-21T19:18:56.363985811 [649596265:main:WARN:src/devices/src/legacy/serial.rs:222] Detached the serial input due
to peer close/error.
updater | time="2023-04-21T19:18:58Z" level=info msg="guest starting" commit=04202779bad4a51eea4fbe8ee8e698ced65ccbe7
updater | time="2023-04-21T19:18:58Z" level=info msg="starting job..." fetcher_timeout=10m0s job_id=649596265
 dater_timeout=45m0s updater_version=6142a76e76d7e50b624fa442454dffea6f903d47-nuget
    ter | 2023/04/21 19:18:59 INFO Raven 3.1.2 ready to catch errors
        | 2023/04/21 19:19:00 INFO <job_649596265> Starting job processing
```

DEPENDABOT



my-repository

-> .github
  - .dependabot.yml

Version Updates: Configuration

```yaml
version: 2

registries:
  nuget-azure-devops:
    type: nuget-feed
    url: https://pkgs.dev.azure.com/index.json
    username: your-user
    password: ${{secrets.NUGET_TOKEN_V1}}

updates:
  # keep NUGET dependencies up to date
  - package-ecosystem: nuget
    directory: "/"
    registries:
    - nuget-azure-devops
    schedule:  # set day, time, timezone, etc
      interval: daily # weekly / monthly
    open-pull-requests-limit: 10
```

```yaml
# metadata
labels:
- custom-label
assignees:
- octocat
reviewers:
- octocat
commit-message:
  prefix: "NUGET: "
  include: "scope"

# dependencies to ignore
ignore:
- dependency-name: AWSSDK.*
  update-types: ["version-update:semver-patch"]
- dependency-name: "Microsoft.Extensions.*"
  versions: ">= 7.0.0"
```

DEPENDABOT

Version Updates: Grouped Pull Requests

```
…
updates:
  - package-ecosystem: nuget
    directory: "/“
    …
    groups:
       test-dependencies:
         patterns:
         - "MSTest.*"
         - "NSubstitute*“
         exclude-patterns:
        - “Other.*"
       core-dependencies:
         patterns:
         - "Spsc.*"
         - "Microsoft.Extensions.*"
         - "Microsoft.AspNetCore.*"
       aws:
         patterns:
         - "AWSSDK.*"
```

Custom Groups

Exclude Patterns

Catch-All

```
groups:
  all-dependencies:
    patterns:
    - "*"
```

Dependency Types

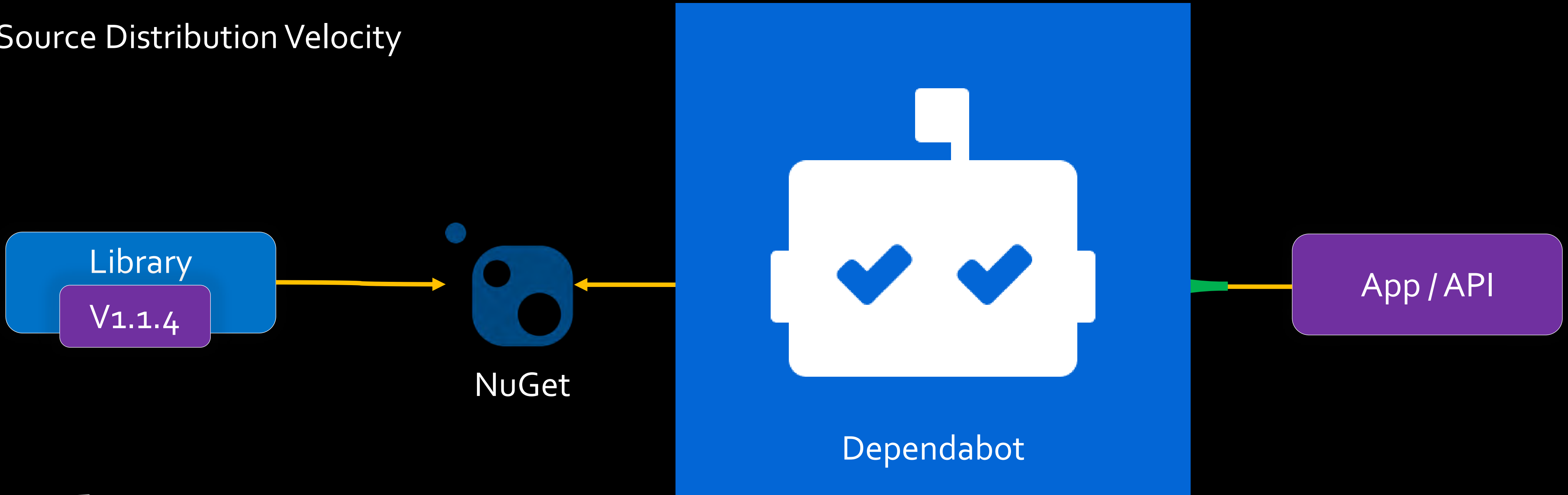
```
groups:
  production-dependencies:
    dependency-type: “production“
  development:
    dependency-type: “development"
```

Update Types

```
groups:
  angular:
    patterns:
    - “@angular*”
    update-types:
    - “minor”
    - “patch*”
```

DEPENDABOT

Inner Source Distribution Velocity



SPS COMMERCE

COMPELLING CODE REUSE IN THE ENTERPRISE

"GOOD PROGRAMMERS KNOW WHAT TO WRITE. GREAT ONES KNOW WHAT TO REWRITE AND REUSE"

ERIC S. RAYMOND

```
# specific dependencies to update
allow:
- dependency-name: "YourOrg.*"
```

DEPENDABOT

Version Updates: Considerations

Pitfalls

- Grouped Updates
- Auto Merge
- Package Maturity

Alternatives

- NuKeeper
- Renovate

Merge Queues

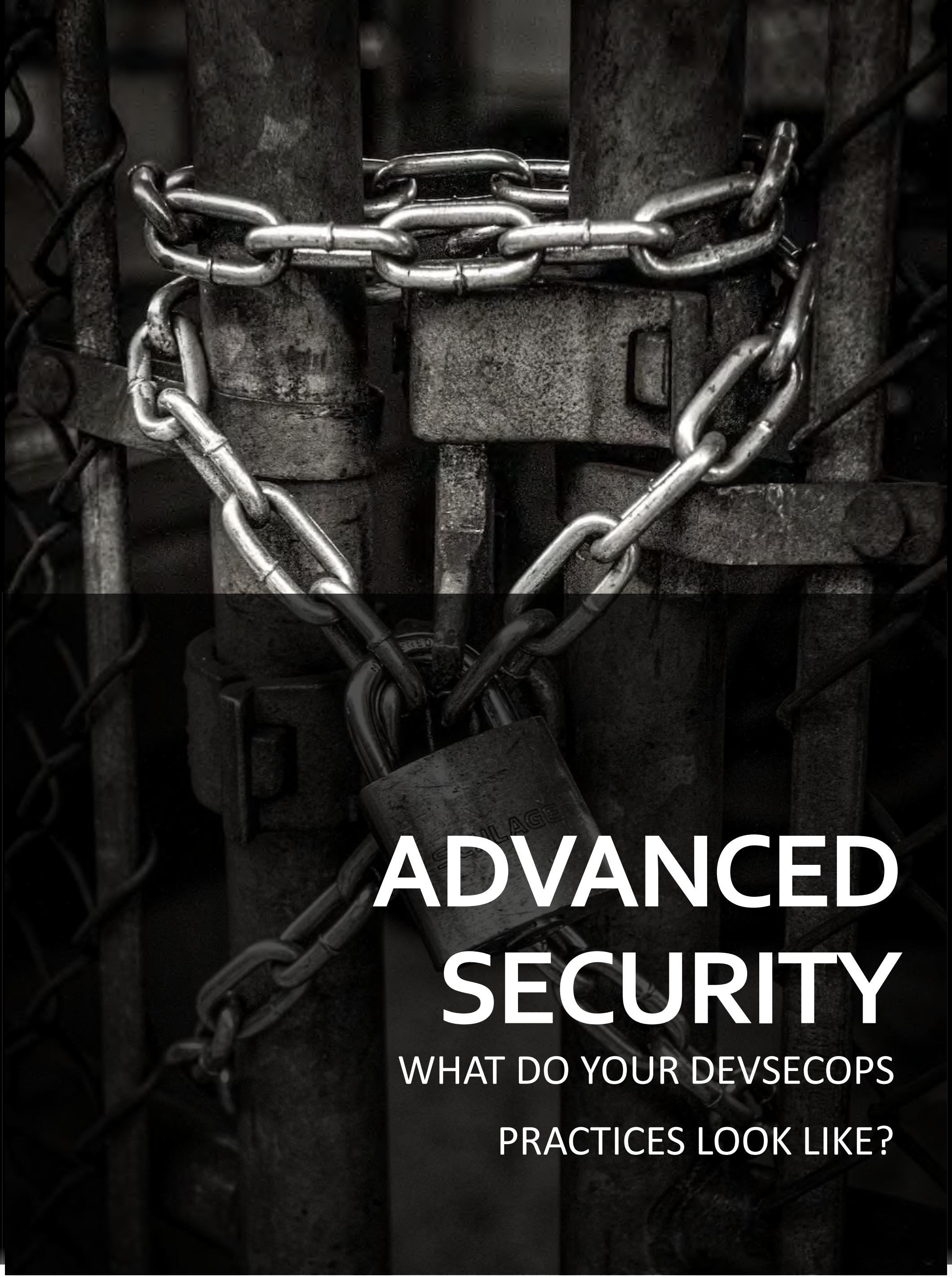
- Coordinate Groups
- Throttle Deploys

Custom Dependencies?

- Proprietary
- Internal

Security Governance

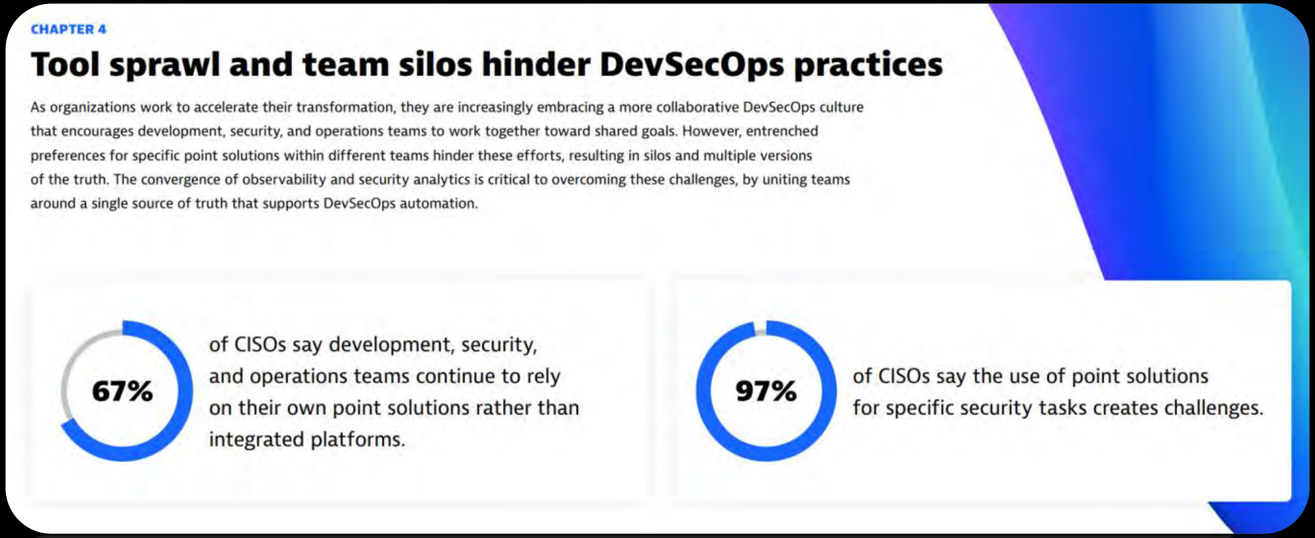
- Enable Defaults
- SBOM
- Assess



ADVANCED SECURITY

WHAT DO YOUR DEVSECOPS PRACTICES LOOK LIKE?

https://www.dynatrace.com/monitoring/platform/application-security/



CHAPTER 4

Tool sprawl and team silos hinder DevSecOps practices

As organizations work to accelerate their transformation, they are increasingly embracing a more collaborative DevSecOps culture that encourages development, security, and operations teams to work together toward shared goals. However, entrenched preferences for specific point solutions within different teams hinder these efforts, resulting in silos and multiple versions of the truth. The convergence of observability and security analytics is critical to overcoming these challenges, by uniting teams around a single source of truth that supports DevSecOps automation.

67% of CISOs say development, security, and operations teams continue to rely on their own point solutions rather than integrated platforms.

97% of CISOs say the use of point solutions for specific security tasks creates challenges.

Overview

Code Scanning

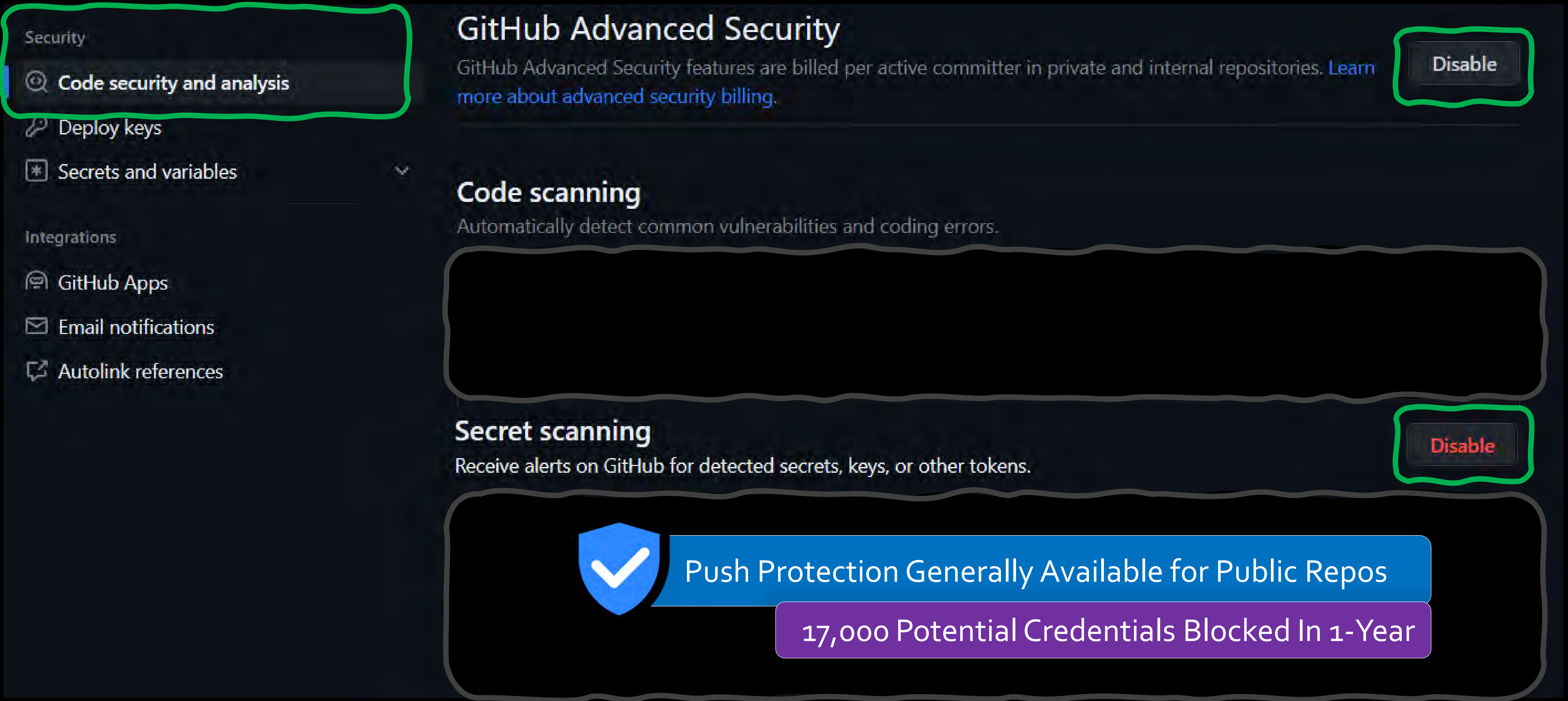
CodeQL (SAST)

ADVANCED SECURITY

Overview

1 License Per User

1 License for Repository Active Committer (90 Days)



GitHub Advanced Security

GitHub Advanced Security features are billed per active committer in private and internal repositories. Learn more about advanced security billing.

Code scanning

Automatically detect common vulnerabilities and coding errors.

[redacted]

Secret scanning

Receive alerts on GitHub for detected secrets, keys, or other tokens.

[redacted]

Push Protection Generally Available for Public Repos

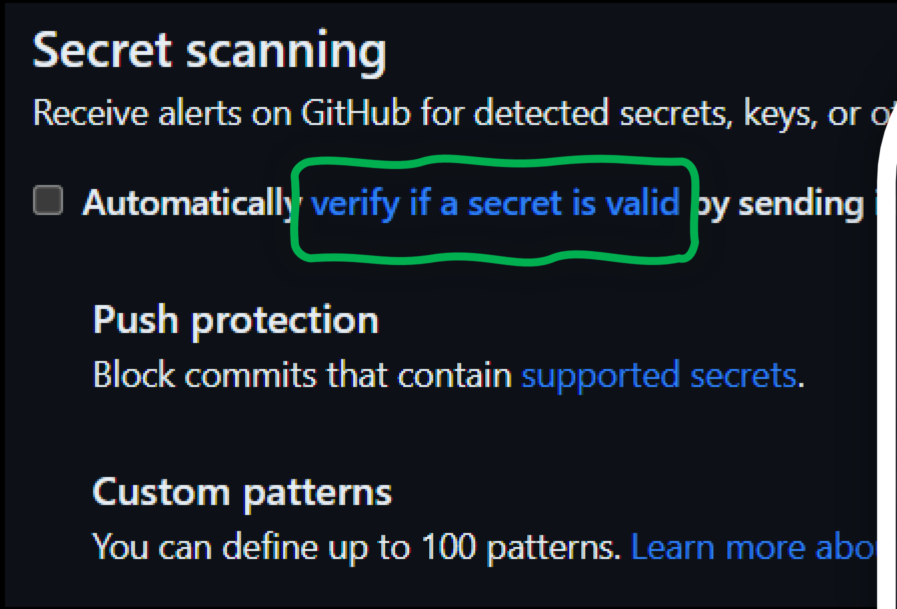
17,000 Potential Credentials Blocked In 1-Year

ADVANCED SECURITY

Secret Scanning

Push Protection Generally Available for Public Repos

17,000 Potential Credentials Blocked In 1-Year



Secret scanning

Receive alerts on GitHub for detected secrets, keys, or o

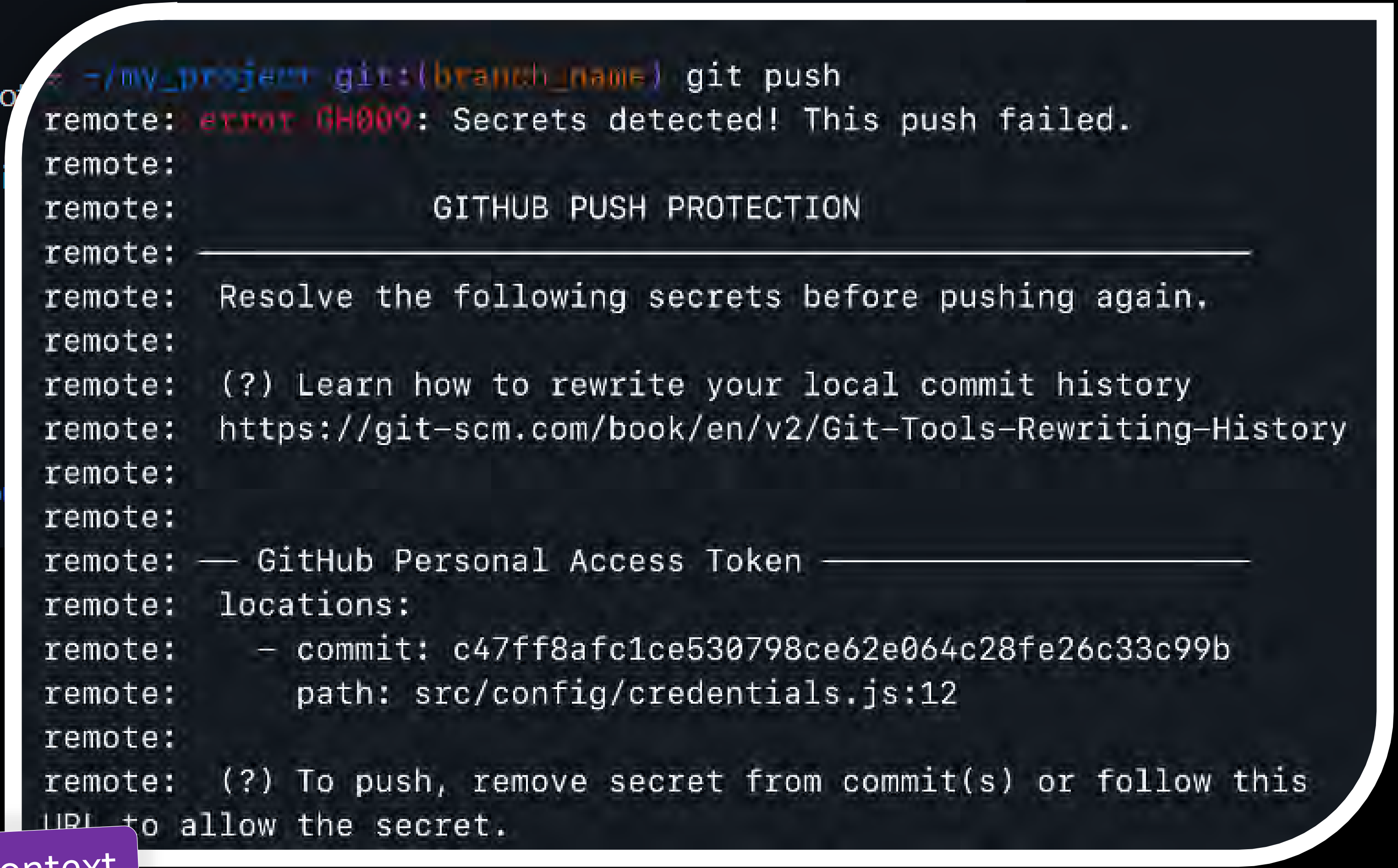
□ Automatically verify if a secret is valid by sending

Push protection

Block commits that contain supported secrets.

Custom patterns

You can define up to 100 patterns. Learn more abo

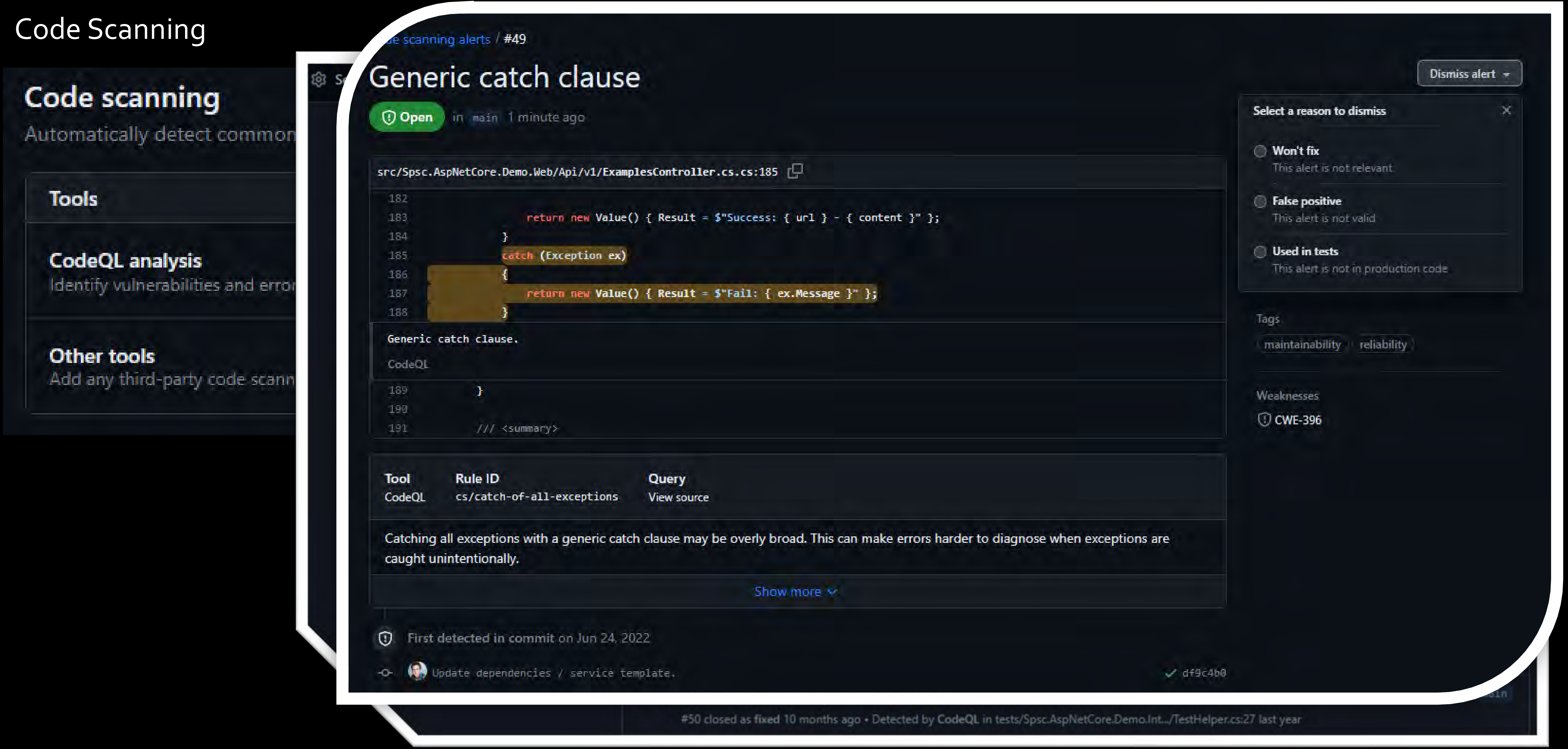


```
→ ~/my_project git:(branch_name) git push
remote: error GH009: Secrets detected! This push failed.
remote:
remote:              GITHUB PUSH PROTECTION
remote: ——————————————————————————————————————————————
remote:   Resolve the following secrets before pushing again.
remote:
remote:   (?) Learn how 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
URL to allow the secret.
```

Auto-Detect Passwords Based on Context

ADVANCED SECURITY

Code Scanning



Code scanning

Automatically detect common

Tools

CodeQL analysis

Identify vulnerabilities and error

Other tools

Add any third-party code scann

de scanning alerts / #49

Generic catch clause

Open in main 1 minute ago

src/Spsc.AspNetCore.Demo.Web/Api/v1/ExamplesController.cs.cs:185

```
                return new Value() { Result = $"Success: { url } - { content }" };
            }
            catch (Exception ex)
            {
                return new Value() { Result = $"Fail: { ex.Message }" };
            }
```

Generic catch clause.

CodeQL

```
        }

        /// <summary>
```

Tool	Rule ID	Query
CodeQL	cs/catch-of-all-exceptions	View source

Catching all exceptions with a generic catch clause may be overly broad. This can make errors harder to diagnose when exceptions are caught unintentionally.

First detected in commit on Jun 24, 2022

Update dependencies / service template. ✓ df9c4b0

Select a reason to dismiss

○ Won't fix
This alert is not relevant

○ False positive
This alert is not valid

○ Used in tests
This alert is not in production code

Tags

maintainability reliability

Weaknesses

CWE-396

#50 closed as fixed 10 months ago • Detected by CodeQL in tests/Spsc.AspNetCore.Demo.Int.../TestHelper.cs:27 last year

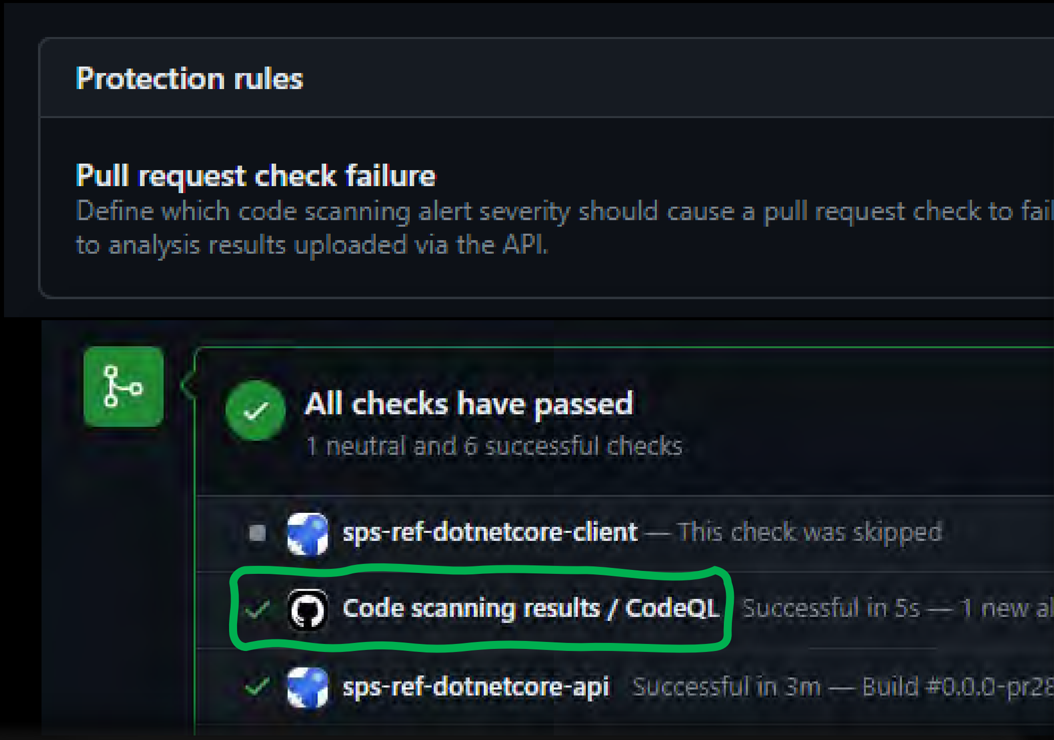
ADVANCED SECURITY

Code Scanning on Pull Requests

Top Challenge: Correlating alerts from different tools is labor-intensive, with many false positives.

2023

dynatrace



Protection rules

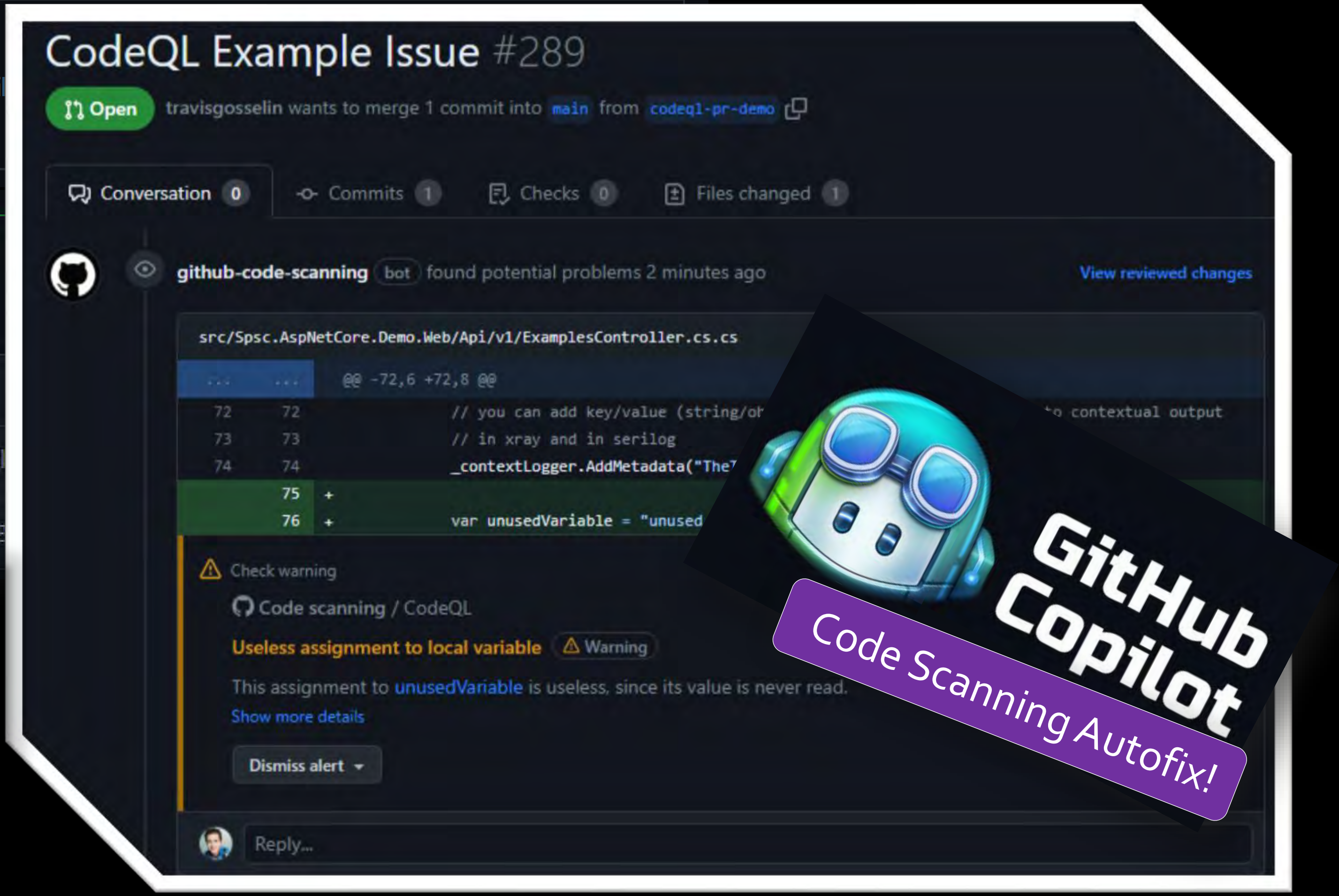
Pull request check failure

Define which code scanning alert severity should cause a pull request check to fai
to analysis results uploaded via the API.

All checks have passed

1 neutral and 6 successful checks

- ■ sps-ref-dotnetcore-client — This check was skipped
- ✓ Code scanning results / CodeQL Successful in 5s — 1 new al
- ✓ sps-ref-dotnetcore-api Successful in 3m — Build #0.0.0-pr28



CodeQL Example Issue #289

Open travisgosselin wants to merge 1 commit into `main` from `codeql-pr-demo`

github-code-scanning bot found potential problems 2 minutes ago

src/Spsc.AspNetCore.Demo.Web/Api/v1/ExamplesController.cs.cs

```
@@ -72,6 +72,8 @@
            // you can add key/value (string/ob                    to contextual output
            // in xray and in serilog
            _contextLogger.AddMetadata("The
+
+           var unusedVariable = "unused
```

⚠ Check warning

Code scanning / CodeQL

Useless assignment to local variable ⚠ Warning

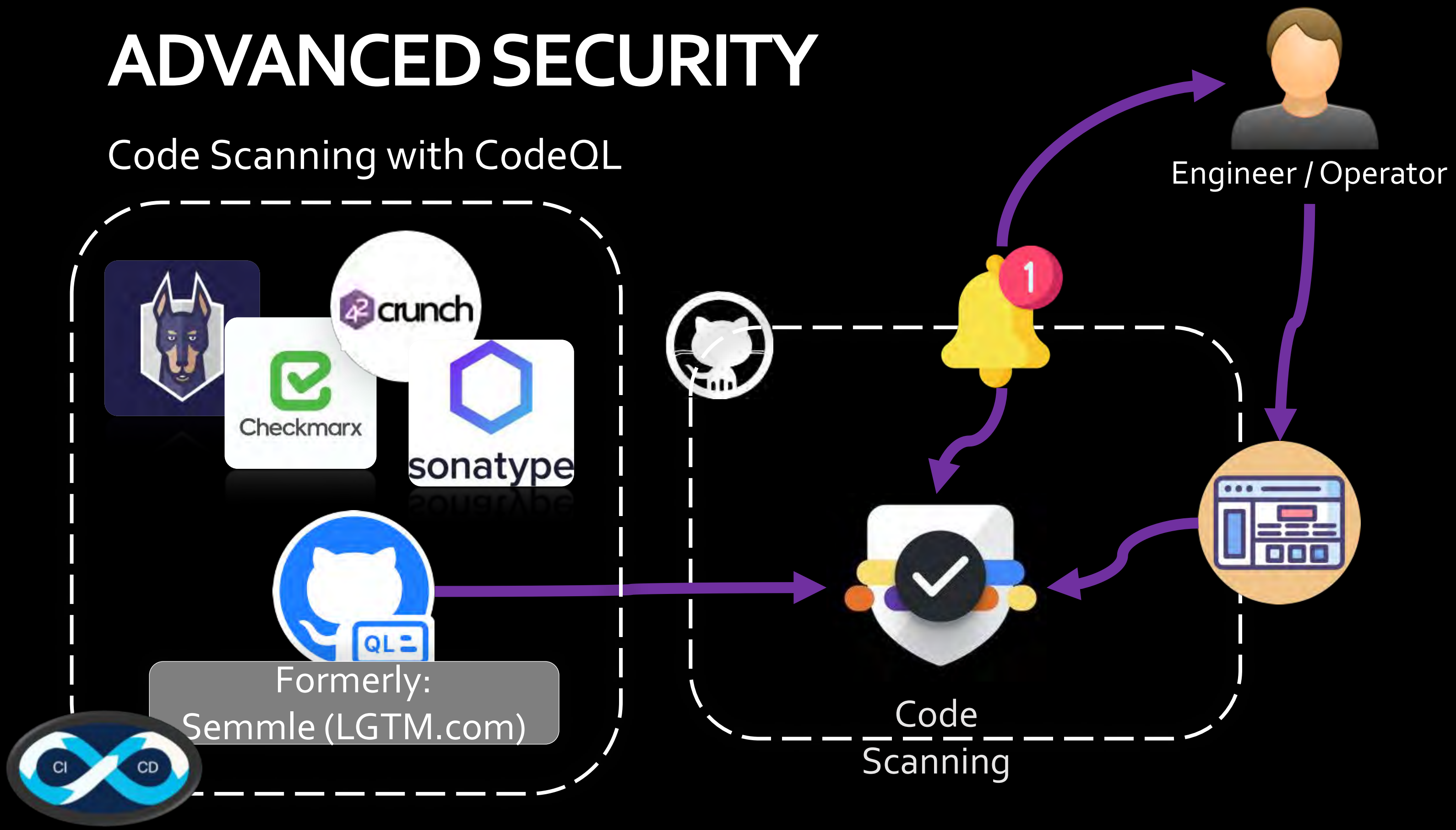
This assignment to unusedVariable is useless, since its value is never read.

Show more details

> It makes no more sense to write code without code scanning tools than it does to write a paper without spell check.
>
> **Mike Lyman (Synopsys)**

ADVANCED SECURITY

Code Scanning with CodeQL

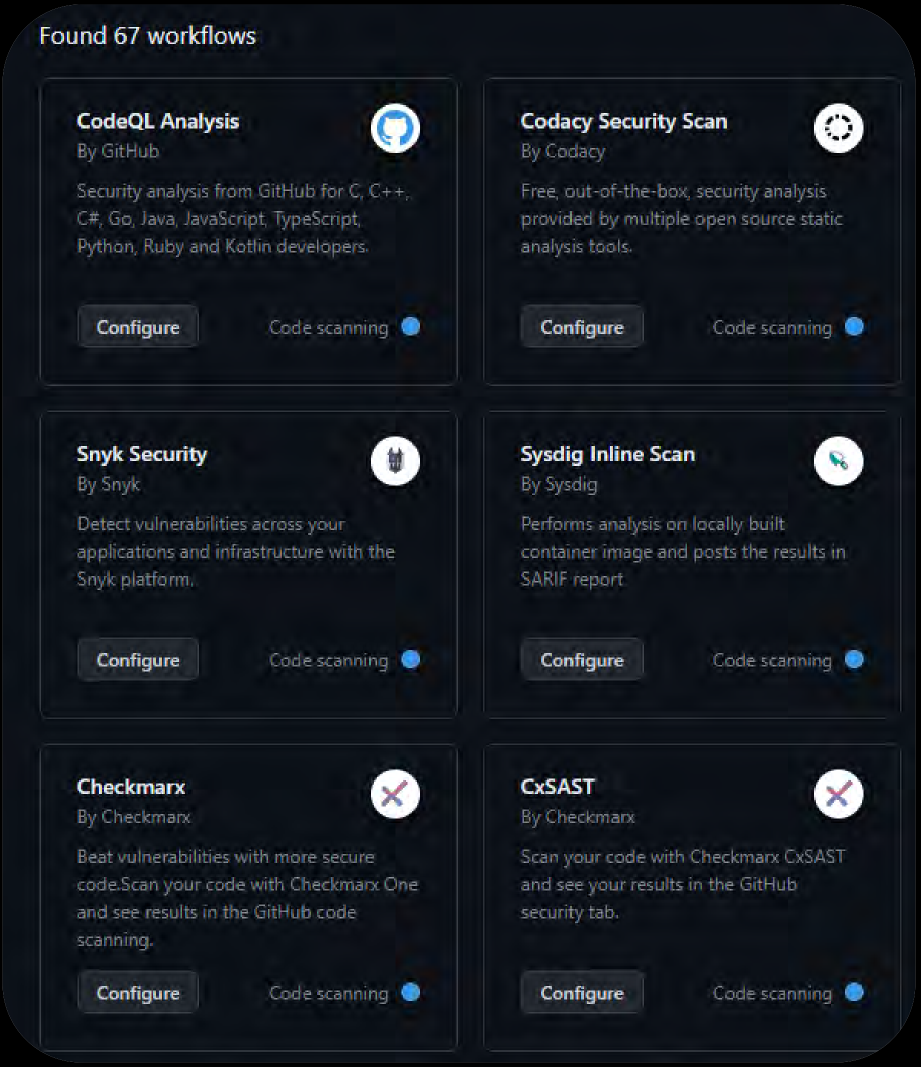


Code Security Analysis

Database / Query Driven

Code Quality Analysis

Maintained Open-Source Queries



Found 67 workflows

CodeQL Analysis
By GitHub
Security analysis from GitHub for C, C++, C#, Go, Java, JavaScript, TypeScript, Python, Ruby and Kotlin developers.
Configure — Code scanning ●

Codacy Security Scan
By Codacy
Free, out-of-the-box, security analysis provided by multiple open source static analysis tools.
Configure — Code scanning ●

Snyk Security
By Snyk
Detect vulnerabilities across your applications and infrastructure with the Snyk platform.
Configure — Code scanning ●

Sysdig Inline Scan
By Sysdig
Performs analysis on locally built container image and posts the results in SARIF report
Configure — Code scanning ●

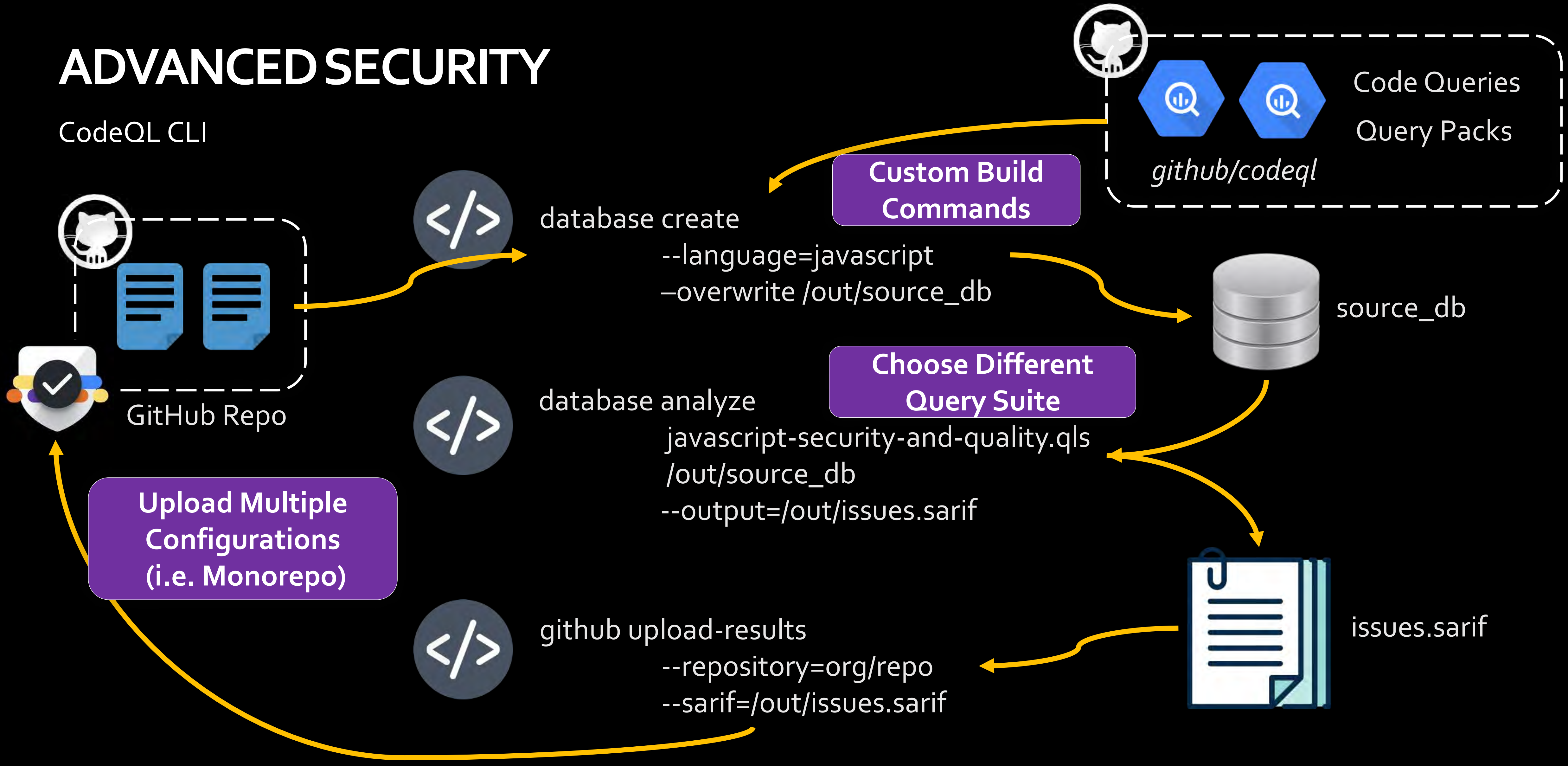
Checkmarx
By Checkmarx
Beat vulnerabilities with more secure code.Scan your code with Checkmarx One and see results in the GitHub code scanning.
Configure — Code scanning ●

CxSAST
By Checkmarx
Scan your code with Checkmarx CxSAST and see your results in the GitHub security tab.
Configure — Code scanning ●

Java

ADVANCED SECURITY

CodeQL CLI



Custom Build Commands

```
database create
        --language=javascript
        –overwrite /out/source_db
```

Choose Different Query Suite

```
database analyze
        javascript-security-and-quality.qls
        /out/source_db
        --output=/out/issues.sarif
```

Upload Multiple Configurations (i.e. Monorepo)

```
github upload-results
        --repository=org/repo
        --sarif=/out/issues.sarif
```

SARIF - Static Analysis Results Interchange Format

Streamlines How Static Analysis Tools Share Results

ADVANCED SECURITY

CodeQL Queries

```
/**
* Query metadata
*/
import /* ... CodeQL libraries or modules ... */
/* ... Optional, define CodeQL classes and predicates ... */
from /* ... variable declarations ... */
where /* ... logical formula ... */
select /* ... expressions ... */
```

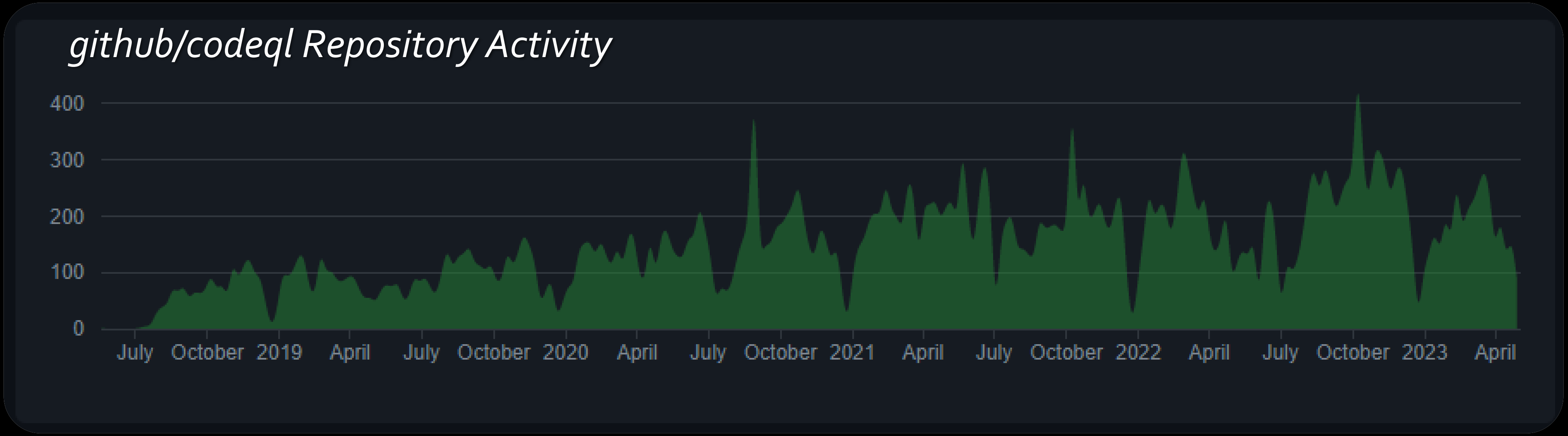
Write Custom Queries

Define Custom Query Packs

Define Custom Query Suites

```
import java

from IfStmt ifstmt
where ifstmt.getThen() instanceof EmptyStmt
select ifstmt, "if statement has an empty then."
```

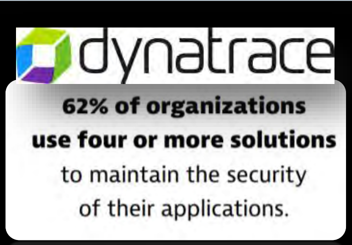

github/codeql Repository Activity

ADVANCED SECURITY

Advanced Security: Considerations

Integrated Experience

- High Setup Cost



dynatrace

62% of organizations use four or more solutions to maintain the security of their applications.

Remote Only

- VSCode Extension
- Pull Requests Workflow

Cost

- Significate Cost
- Comparatively Lower Price

Custom Queries

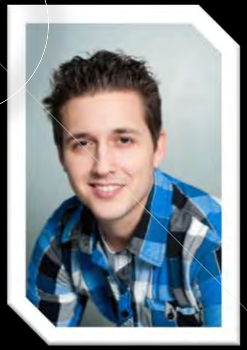
- Bring Your Own
- Need YAML/JSON Capability
- Complexity

Interoperability

- Ecosystem of Tools
- Standard SARIF Format

> "Developers work in rainforests, not planned gardens."
>
> a16z.com

FORTIFYING YOUR CODEBASE WITH GITHUB



TRAVIS GOSSELIN

travisgosselin.com

linkedin.com/in/travisgosselin

@travisjgosselin