

{ From AppSec to DevSec }

Shift left with GitHub Advanced Security



Losses caused by **cyber attacks** reported to IC3

2020

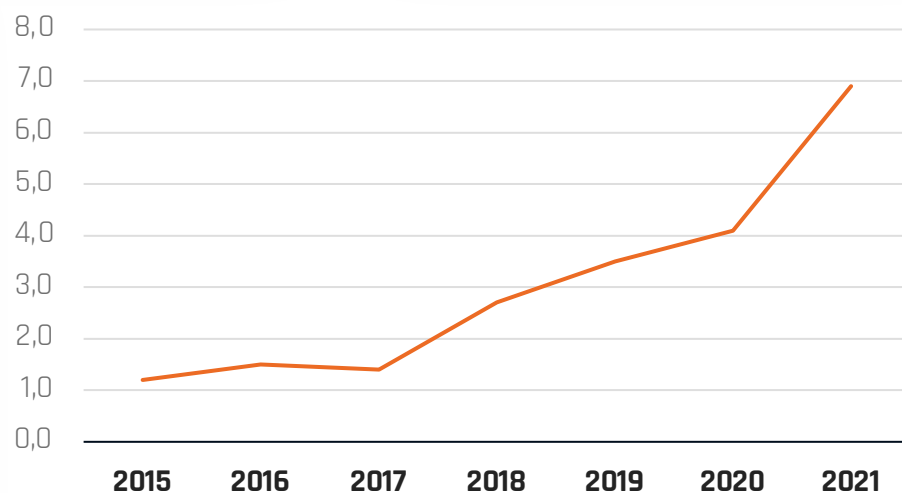
\$ 4.100.000.000

2021

\$ 6.900.000.000



Loss caused
by reported
cyber crime
(in billion
USD)



Top 5 crime types:

- > Phishing
- > Non-Payment / Delivery
- > Data Breach
- > Identity Theft
- > Extortion



Trends

- > Confidence fraud / Romance scams
- > Cryptocurrency
- > Ransomware
- > Tech support fraud



Joseph Lister directing the use of carbolic acid spray in one of his earliest antiseptic surgical operations, circa 1865. Bettmann Archive

Adoption of **anaesthesia** and **antiseptics** in 19th century



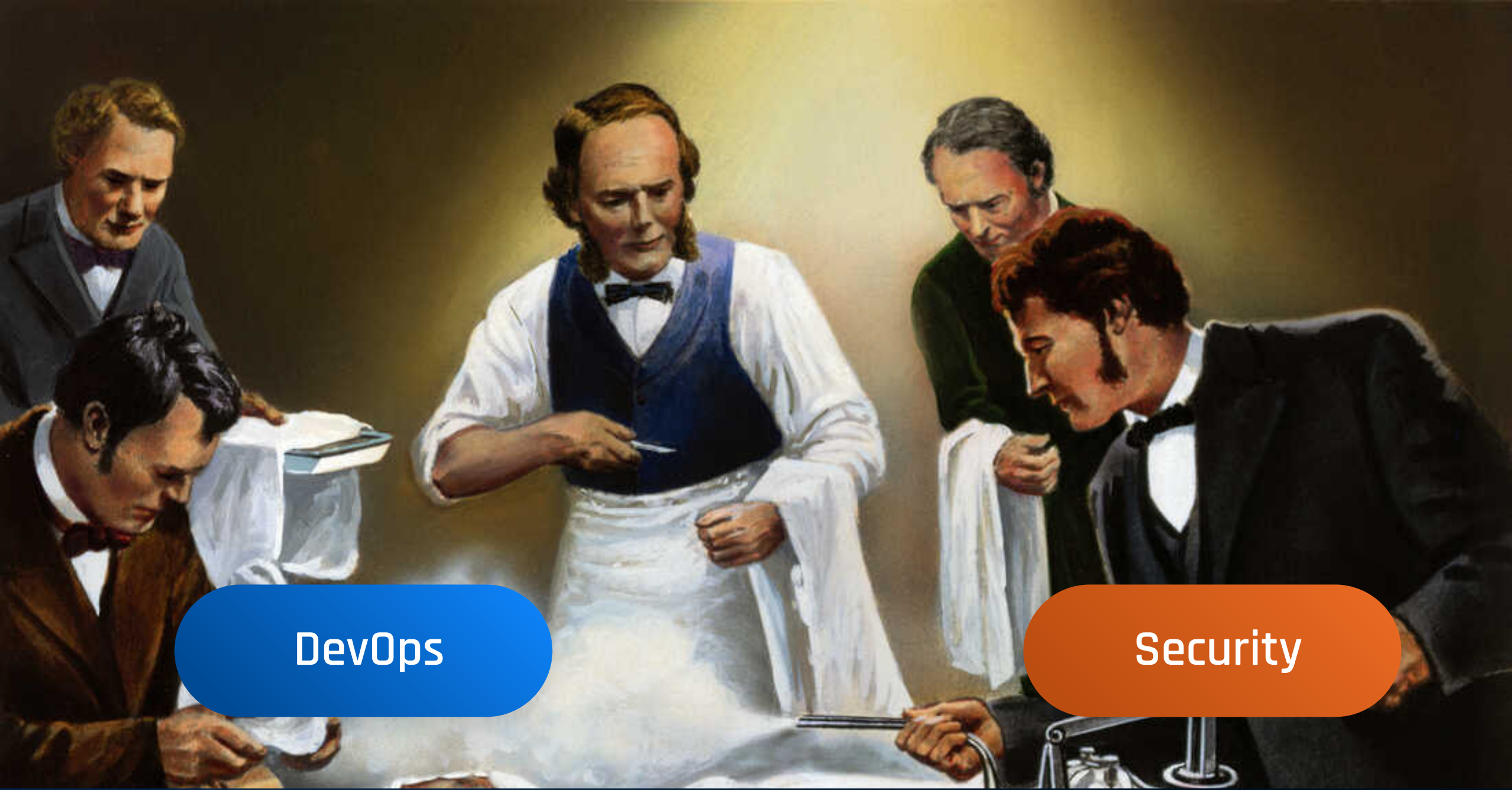
Anaesthesia

- › First discovered in 1846
- › Used worldwide within a year
- › Ubiquitous within 7 years



Antiseptics

- › First discovered in 1865
- › Highly divisive
- › Half-heartedly adopted by mid 1880s
- › Now considered the foundation of modern medicine



DevOps

Security

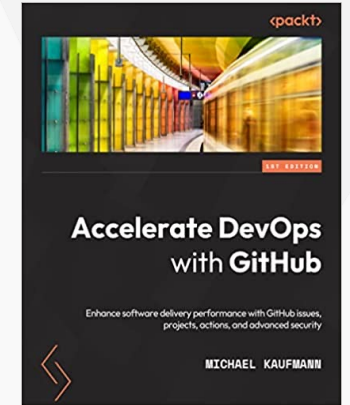
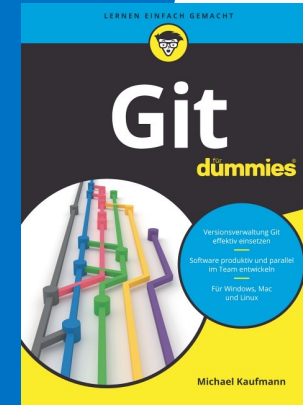
Joseph Lister directing the use of carbolic acid spray in one of his earliest antiseptic surgical operations, circa 1865. Bettmann Archive

Michael Kaufmann

Founder & Managing Director, Xpirit Germany



Microsoft®
Most Valuable Professional



@mike_kaufmann



@wulfland



<https://writeabout.net>



> 20 years software developer

> 15 years ALM & DevOps

> 10 years Git and GitHub

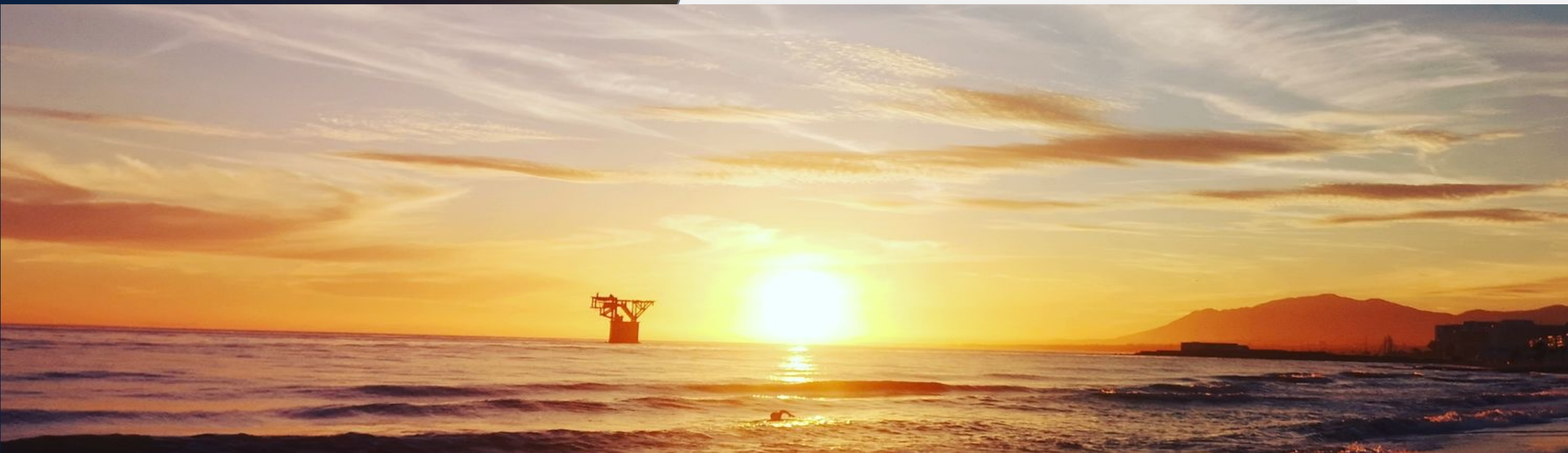
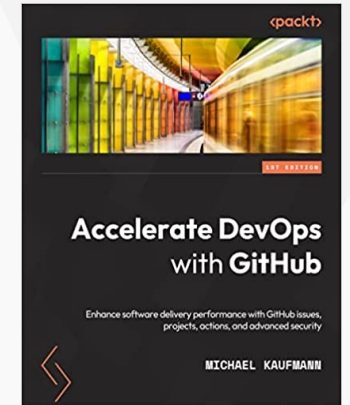
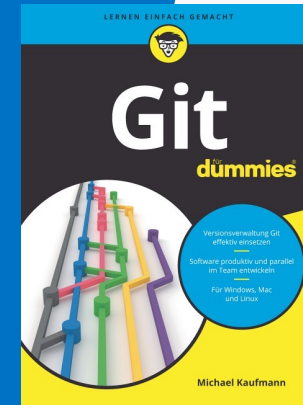
> Microsoft Regional Director & MVP

Michael Kaufmann

Founder & Managing Director, Xpirit Germany



Microsoft®
Most Valuable Professional



The event-stream incident



Social engineering attack



Supply chain attack:
event-stream@3.3.6 -> flatmap-stream@0.1.1



Code execution in build process
targeting copay



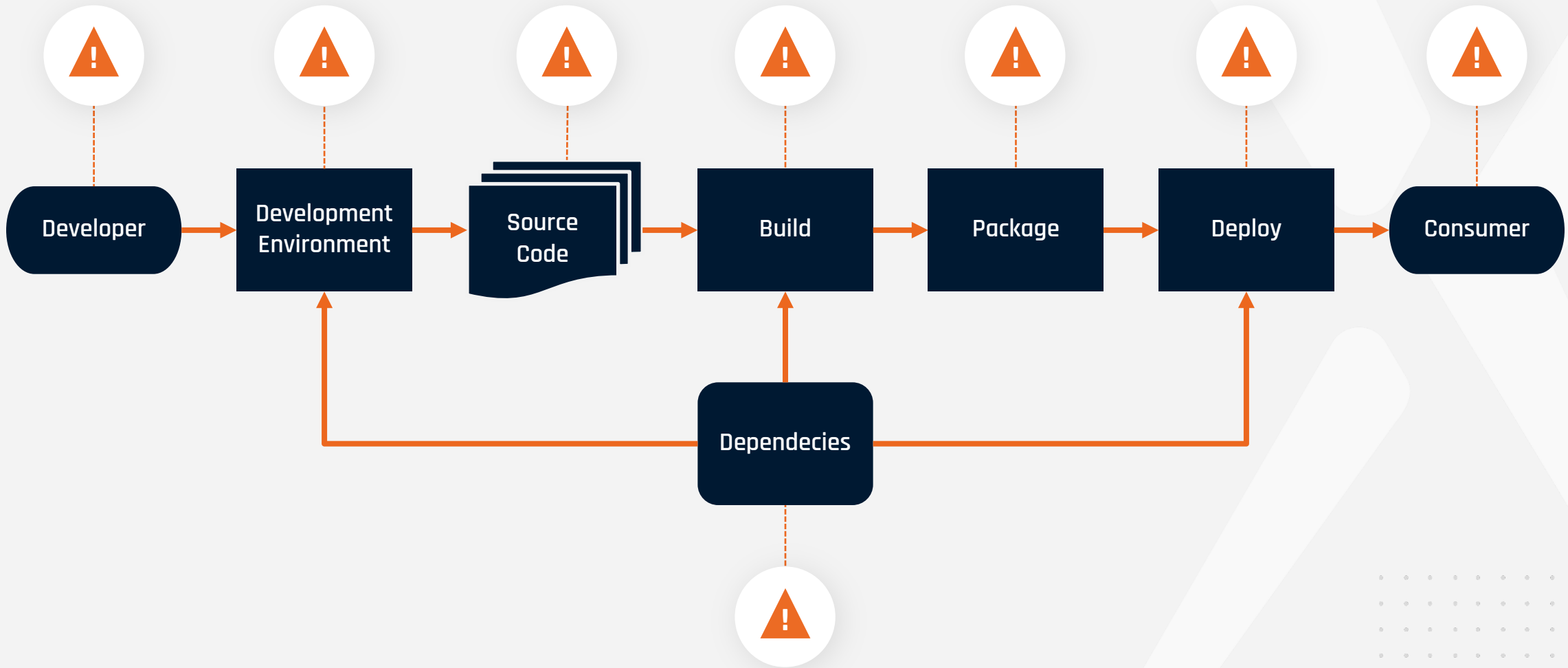
Harvest the user's bitcoin and
private keys

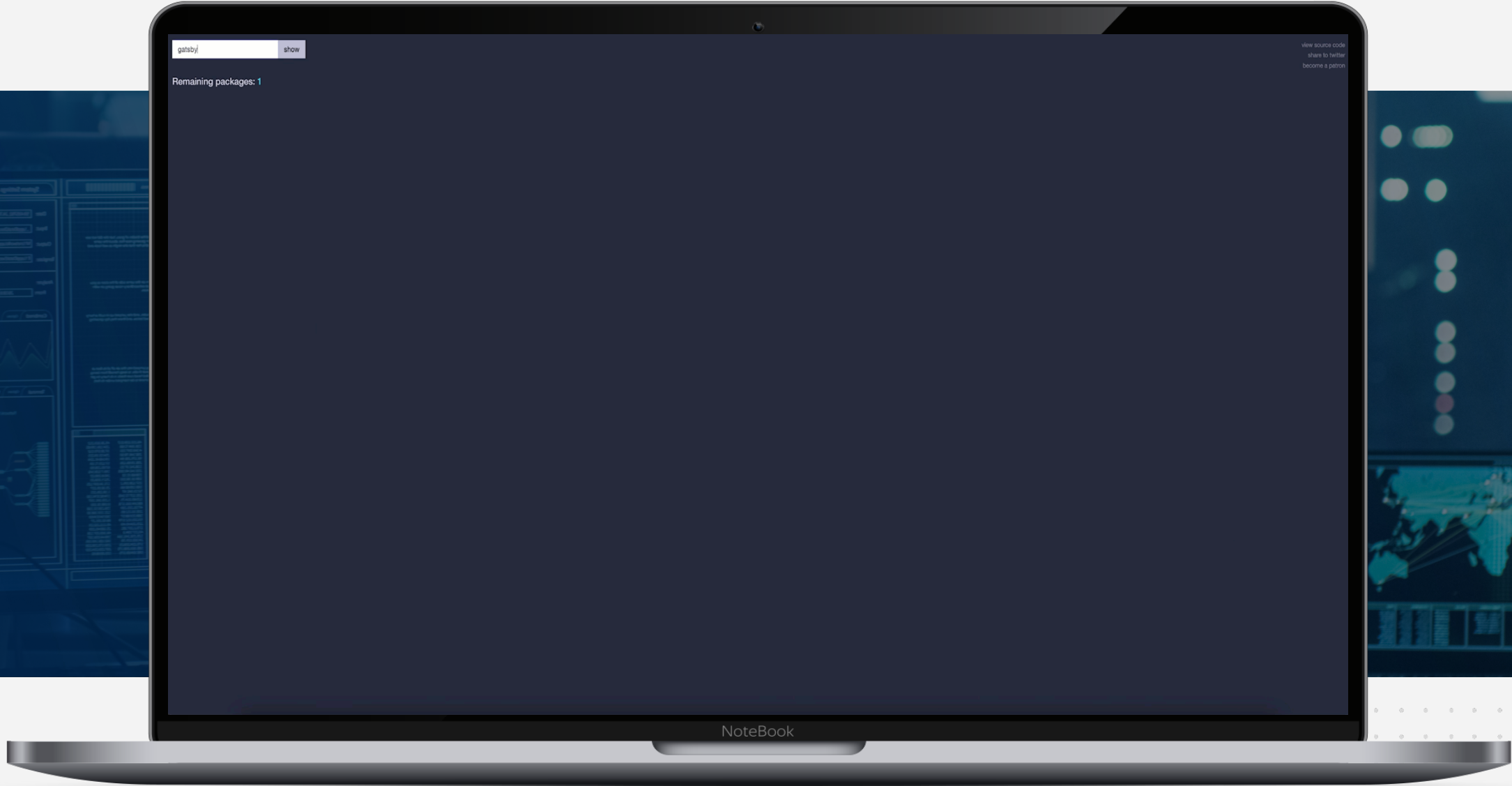
The screenshot shows a GitHub vulnerability advisory for the package `flatmap-stream` (npm). The advisory is titled "Malicious Package in flatmap-stream" and is marked as "Critical severity". It was published on 1 Sep 2020 and updated on 1 Oct 2021. The affected version is 0.1.1. The advisory describes a malicious package that targets a very specific application, `copay`, and because they shared the same description it would have likely worked for `copay-dash`. The injected code performs several actions: it reads in AES encrypted data from a file disguised as a test fixture, grabs the npm package description of the module that imported it, and uses the package description as a key to decrypt a chunk of data pulled in from the disguised file. The decrypted data was part of a module, which was then compiled in memory and executed. This module performed the following actions: it decrypted another chunk of data from the disguised file, concatenated a small, commented prefix from the first decrypted chunk to the end of the second decrypted chunk, performed minor decoding tasks to transform the concatenated block of code from invalid JS to valid JS (we believe this was done to evade detection by dynamic analysis tools), and wrote this processed block of JS out to a file stored in a dependency that would be packaged by the build scripts. The chunk of code that was written out was the actual malicious code, intended to be run on devices owned by the end users of Copay. This code would do the following:

- Detect the current environment: Mobile/Cordova/Electron
- Check the Bitcoin and Bitcoin Cash balances on the victim's copay account
- If the current balance was greater than 100 Bitcoin, or 1000 Bitcoin Cash:
 - Harvest the victim's account data in full
 - Harvest the victim's copay private keys
 - Send the victim's account data/private keys off to a collection

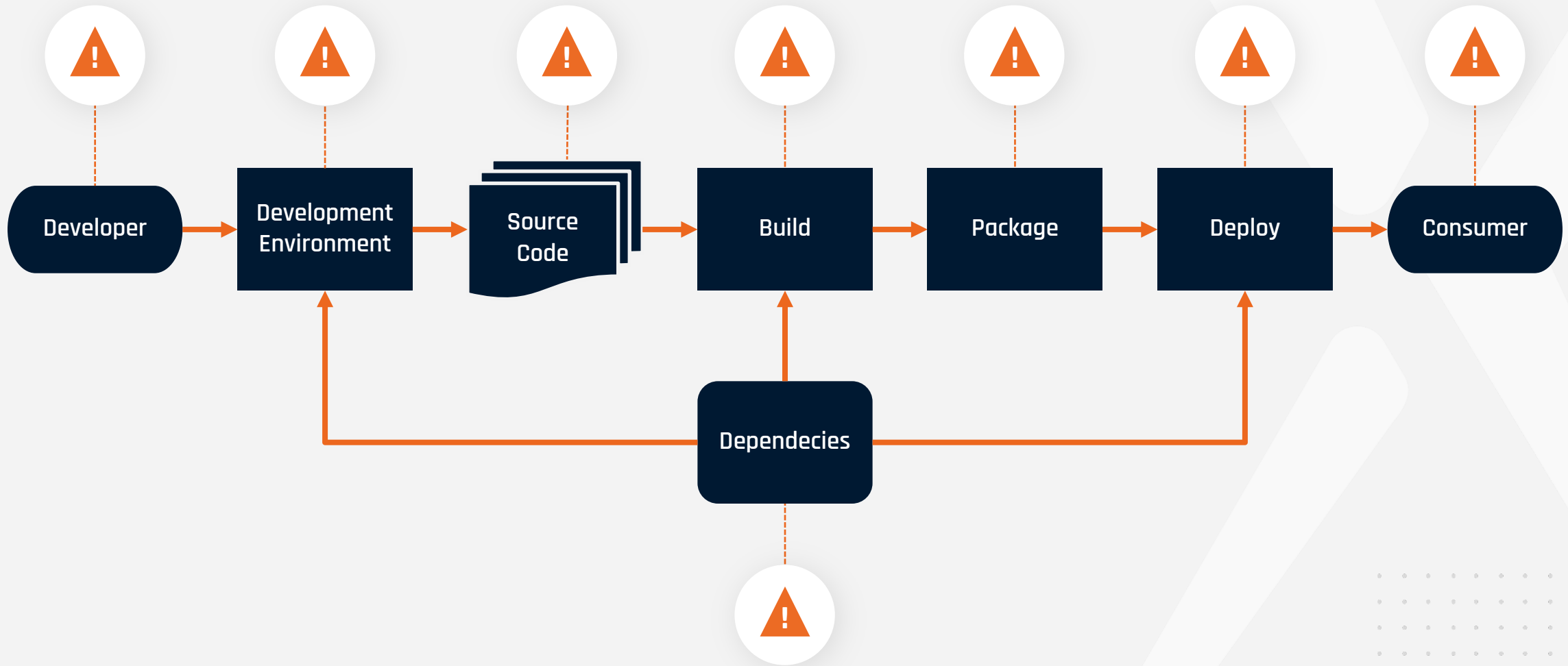
Additional details from the screenshot include: the user `right9ctrl` (located in Tokyo, Japan) committed to this repository; the GHSA ID is `GHSA-9x64-5r7x-2q53`; the CWE is `CWE-506`; and the CVSS Score is 9.8 Critical (`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H`). The advisory has been edited, and there is a link to see the history. A suggestion to contribute is also present.

Attack vectors

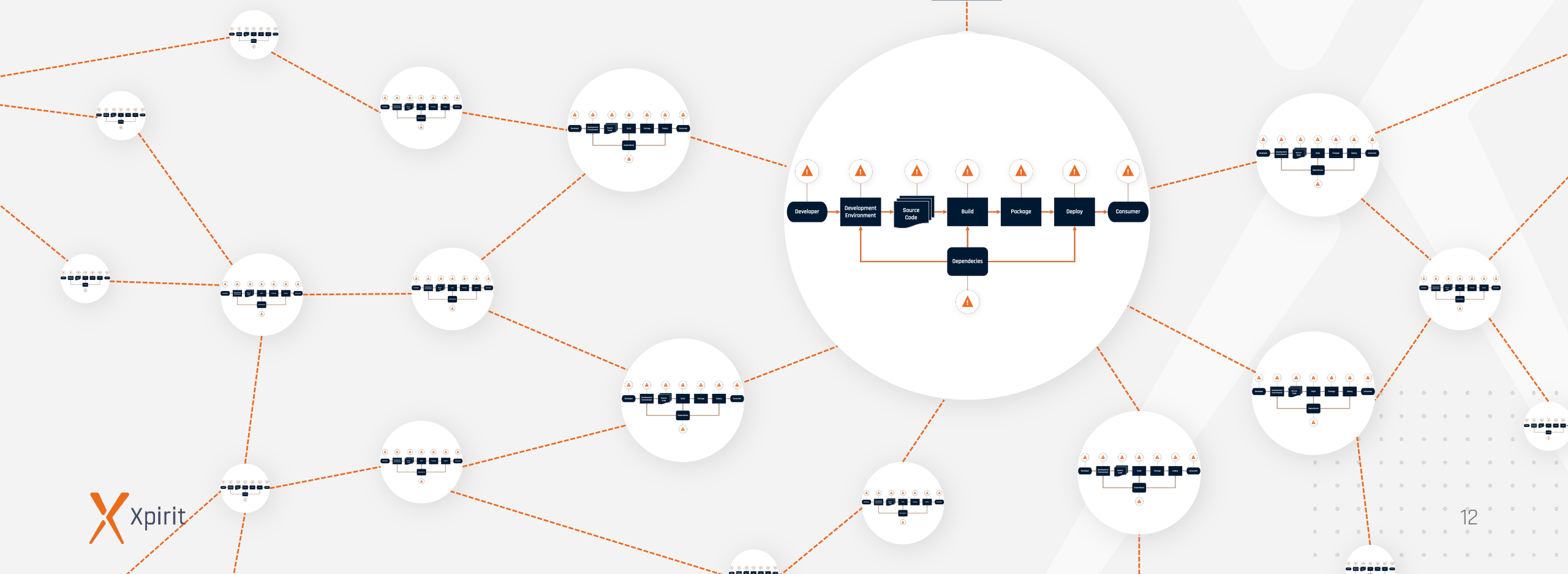
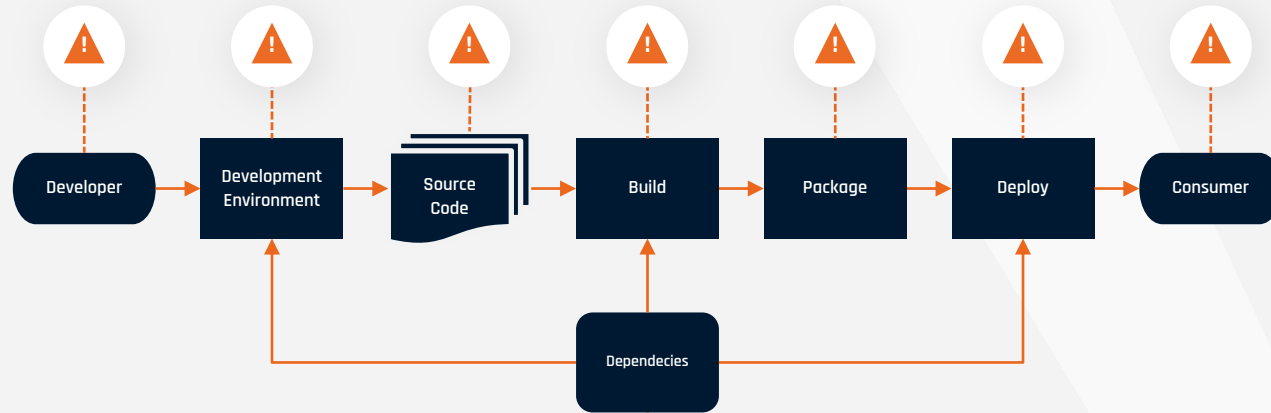




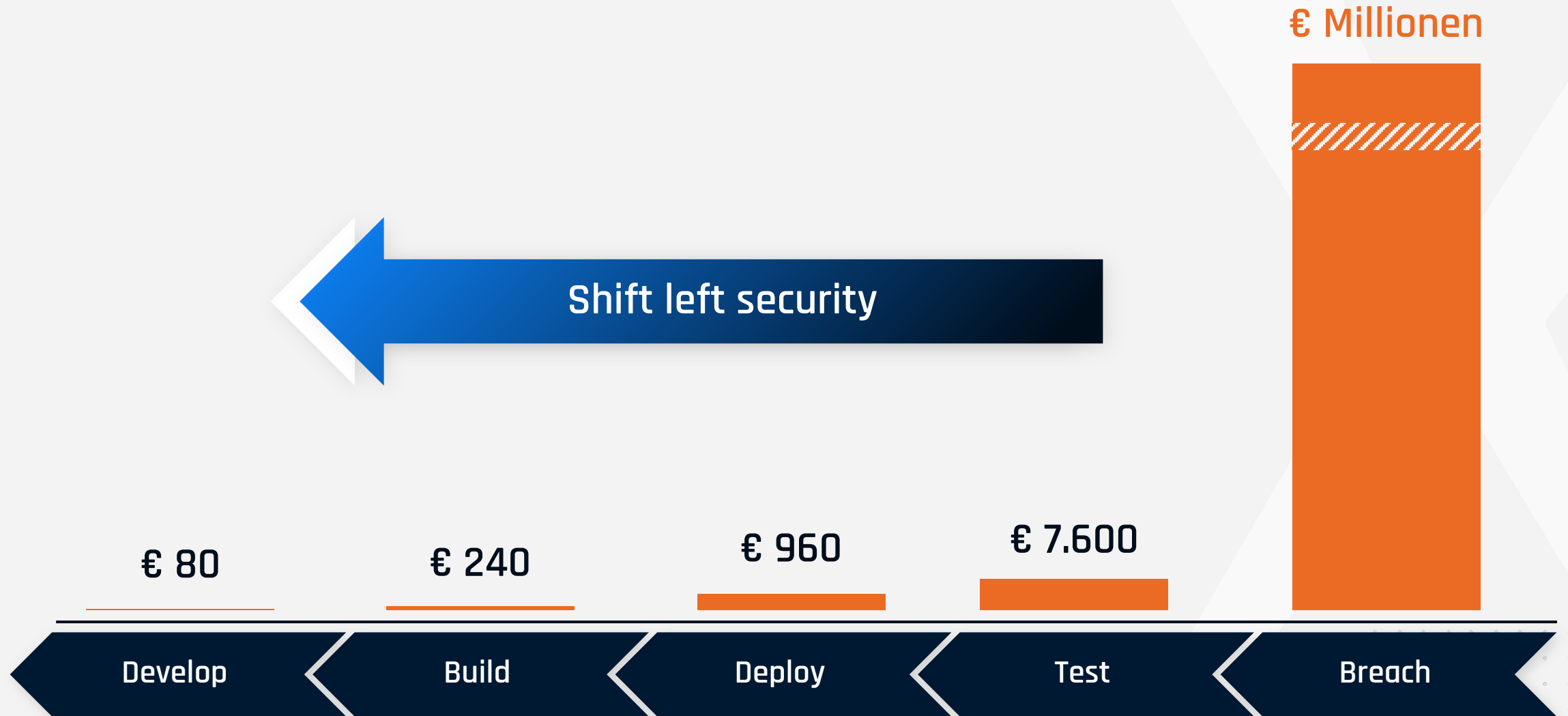
Attack vectors



Attack vectors



Costs for fixing a security vulnerability



Developer Security

Attacking developers

Phishing / Spear Phishing

Social engineering

Unsecured connections to test systems

“A developer is just a normal employee - that works as local admin, can push and execute code on various systems in minutes, and often runs unsecured web servers.”

Phishing



Cgi [STAFF] shared "file" with you.

Cgi [STAFF] <dlawler@oakassociates.com>
Mon 6/14, 1:33 PM
Kaufmann, Michael

Deleted Items

This message was sent with high importance.

EXTERNAL SENDER: Do not click any links or open any attachments unless you trust the sender and know the content is safe.
EXPÉDITEUR EXTERNE: Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe à moins qu'ils ne proviennent d'un expéditeur fiable, ou que vous ayez l'assurance que le contenu provient d'une source sûre.

Message from Cgi server.

Ho mes Limited.

Cgi Share Document on SharePoint Groups

1 of your groups has new document for you

All Company

@cgi.com at 2hrs +
#contest

[Follow below to review this important document]

[Preview Cgi Documents](#)

Urgent information about your April 2019 Deposit

Payroll Accounting <info@paymentreturn.com>
Tue 5/25, 10:12 AM
Kaufmann, Michael

EXTERNAL SENDER: Do not click any links or open any attachments unless you trust the sender and know the content is safe.
EXPÉDITEUR EXTERNE: Ne cliquez sur aucun lien et n'ouvrez aucune pièce jointe à moins qu'ils ne proviennent d'un expéditeur fiable, ou que vous ayez l'assurance que le contenu provient d'une source sûre.

Dear Michael,

Unfortunately, we noticed during an internal review that there was an error in the last salary payment in April, this error was caused by an internal technical error which we have already corrected.

We apologize for the inconvenience caused.

Please check in the tool you know [Payroll Accounting](#), if your payment received matches the data on your statement. The adjusted payroll and the document for the following additional payment are available under the following link: [Payroll Accounting](#)

We apologize again for the error and wish them all the best and stay healthy.

Regards,
Your payroll team

Attacking **developers**

Typo squatting



Namespace shadowing



Typo squatting

```
$ npm install crossenv
```



Steals all
your
environment
variables

```
$ npm install cross-env
```



Normal
package



Namespace shadowing

```
$ npm install @azure/core-tracing
```



Normal
package

```
$ npm install core-tracing
```



Upload data to
a control server



Credentials **Developer**

E-Mail	→	Spear phishing
Access machines	→	Log on, Mimikatz
Source	→	Inject code
Pipeline	→	Execute code / scripts
Access test environment	→	Test against prod?
Access prod?		



What to do?



Security Awareness Trainings



Security Games



Red team | blue team simulations



Virtualized dev-environments

Capture the **flag**

▶ Red team | blue team simulations

▶ Insider attacks

▶ Create awareness

▶ Think like attackers



Demo: GitHub Codespaces





Code Security





4 years

On average, vulnerabilities go undetected for four years before being identified.
Sometimes, even longer than that - Log4j was vulnerable for ~7 years

CodeQL: a revolutionary semantic code engine



Advanced code analysis engine based on 13 years of research by a 30 person team from Oxford University



Allows you to query your code's logic to find vulnerabilities



Queries can be quickly customized to adapt to your specific threat topology



Community-driven query set powers every project with a world-class security team

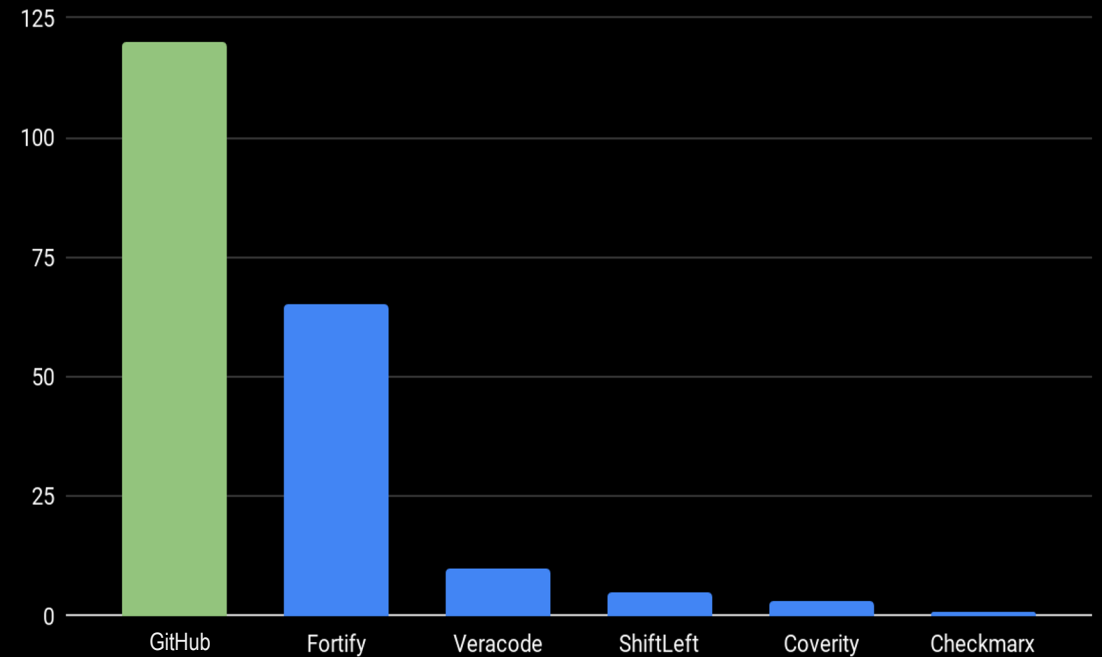
Security researchers find more vulnerabilities with CodeQL

- › More CVEs than any other SAST vendor team
- › 50 CVEs in the last 3 months
- › Testimonials from top security teams, including Microsoft and Uber

Examples

- › Zip Slip at Microsoft
- › Bug bounty at Uber

CVEs discovered, by vendor, 2018 - 2019



Combining CodeQL with the world's largest developer community gives next generation SAST performance

20,000

public repos have enabled automated code review using CodeQL (before it's native!)

1,700+

open source queries with contributions from Microsoft, Google and many others



72%

fix rate for potential vulnerabilities flagged in open source projects

24%

of recent JS CVEs would have been identified by a default CodeQL query

Infrastructure Scanning

Container Vulnerability Analysis (CVA) / Container Security Analysis (CSA)

Open source:

- > Anchore gryp
<https://github.com/anchore/grype/>
- > Clair
<https://quay.github.io/clair/>

Commercial:

- > WhiteSource
<https://www.whitesourcesoftware.com/solution-for-containers/>
- > Aqua
<https://www.aquasec.com/products/container-security/>

```
- name: Anchore Container Scan
  uses: anchore/scan-action@v3.2.0
  with:
    image: ${ env.REGISTRY }}/${ env.IMAGE_NAME }}
    debug: true
```

<https://github.com/wulfland/container-demo/actions/runs/2179243137>



build-and-push-image failed 3 minutes ago in 22s

Search logs

- > ✓ Set up job 3s
- > ✓ Checkout repository 1s
- > ✓ Log in to the Container registry 0s
- > ✓ Extract metadata (tags, labels) for Docker 0s
- > ✓ Build and push Docker image 4s
- > ✓ Anchore SBOM Action 3s
- ▼ ✗ Anchore Container Scan 8s

```
1 ▶Run anchore/scan-action@v3.2.0
12 /usr/bin/chmod +x /home/runner/work/_temp/ca1e5e61-229a-43b7-b70f-c317932ac1c0
13 /home/runner/work/_temp/ca1e5e61-229a-43b7-b70f-c317932ac1c0 -b
/home/runner/work/_temp/ca1e5e61-229a-43b7-b70f-c317932ac1c0_grype v0.27.3
14 [info] checking github for release tag='v0.27.3'
15 [info] fetching release script for tag='v0.27.3'
16 anchore/grype info checking GitHub for tag 'v0.27.3'
17 anchore/grype info found version: 0.27.3 for v0.27.3/linux/amd64
18 anchore/grype info installed /home/runner/work/_temp/ca1e5e61-229a-43b7-b70f-
c317932ac1c0_grype/grype
19
20 Analyzing: ghcr.io/wulfland/container-demo
21 Executing: grype -vv -o json --fail-on medium ghcr.io/wulfland/container-demo
22 ▶grype output...
163 Error: Failed minimum severity level. Found vulnerabilities with level medium or
higher
```

- > ✓ Post Build and push Docker image 0s
- > ✓ Post Log in to the Container registry 0s
- > ✓ Post Checkout repository 0s
- > ✓ Complete job 0s

Infrastructure Scanning

Infrastructure policies

Open source:

- › Checkov
<https://www.aquasec.com/products/container-security/>
- › OpenVAS

Commercial:

- › Defender for Cloud
<https://azure.microsoft.com/en-us/services/defender-for-cloud>
- › Azure Policy
<https://docs.microsoft.com/de-de/azure/governance/policy/>

```
- name: Checkov GitHub Action
  uses: bridgecrewio/checkov-action@master
  with:
    directory: ch15_sec/
    output_format: sarif

- name: Upload SARIF file
  uses: github/codeql-action/upload-sarif@v1
  with:
    sarif_file: results.sarif
  if: always()
```

Code scanning

[Add more scanning tools](#)

Latest scan	Branch	Workflow	Lines scanned	Duration	Result
10 minutes ago	main	CodeQL	1.45k / 1.39k ⓘ	5m 26s	21 alerts

Filters ▾ 🔍 tool:checkov is:open branch:main

✕ Clear current search, filters and sorts

<input type="checkbox"/>	✓ 2 Open × 0 Closed	Tool	Rule	Branch	Severity	Sort
<input type="checkbox"/>	Ensure that S3 bucket has a Public Access block 🚫 Error			main		
	aws.tf:1 • Detected 15 minutes ago by checkov					
<input type="checkbox"/>	Ensure that S3 bucket has cross-region replication enabled 🚫 Error			main		
	aws.tf:1 • Detected 15 minutes ago by checkov					



Demo: Code analysis

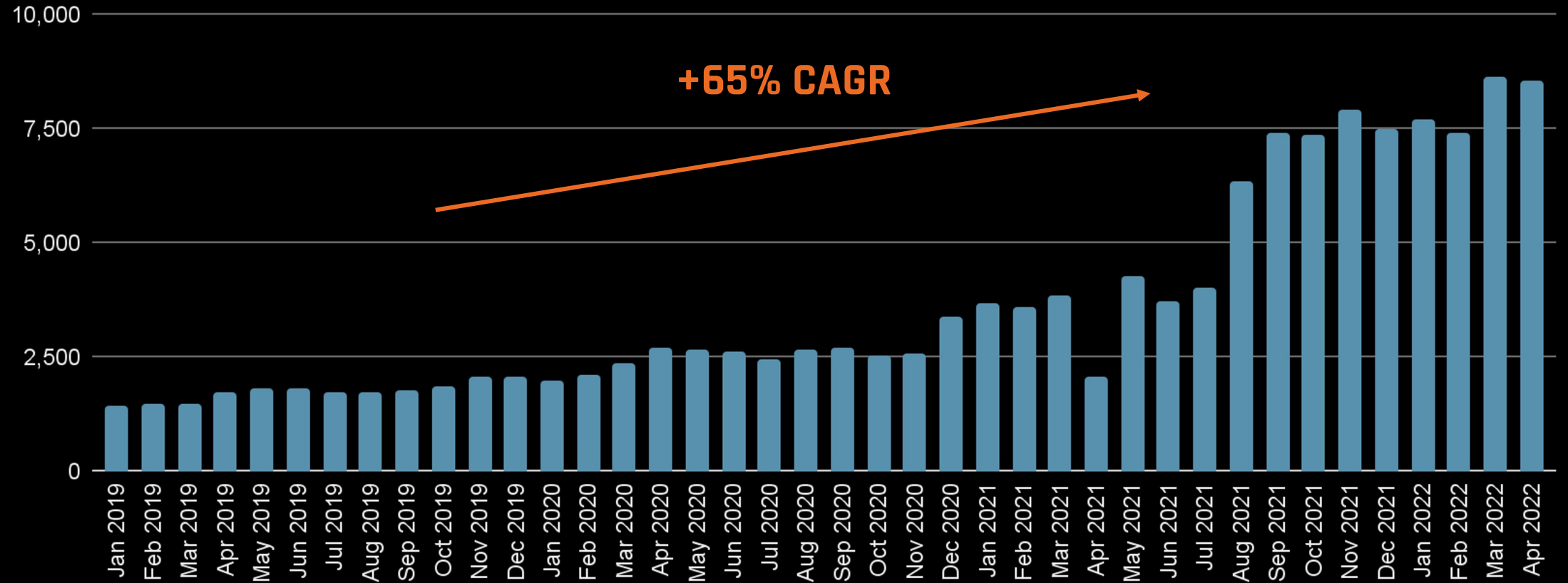


Secret Scanning



We're seeing more credential leaks than ever

GitHub access tokens leaked in public repositories



Secret Scanning

▶ Code

- › GitHub Secret Scanning
- › gitLeaks
- › SpectralOps
- › Git-Secrets
- › Whispers
- › Gittyleaks
- › Git-all-secrets
- › ...

▶ Fileshare

- › Bash/PowerShell
- › Dumpster

Adafruit IO Adafruit IO Key	Dropbox Dropbox Access Token Dropbox Short Lived Access Token	Plivo Plivo Auth Token
Adobe Adobe Device Token Adobe JSON Web Token Adobe Service Token Adobe Short-Lived Access Token	Dynatrace Dynatrace Access Token Dynatrace Internal Token	Postman Postman API Key
Alibaba Cloud Alibaba Cloud Access Key ID and Access Key Secret pair	Finicity Finicity App Key	Proctorio Proctorio Consumer Key Proctorio Linkage Key Proctorio Registration Key Proctorio Secret Key
Amazon Web Services (AWS) Amazon AWS Access Key ID and Secret Access Key pair	Frame.io Frame.io Developer Token Frame.io JSON Web Token	Pulumi Pulumi Access Token
Atlassian Atlassian API Token Atlassian JSON Web Token	GitHub GitHub App Installation Access Token GitHub OAuth Access Token GitHub Personal Access Token GitHub Refresh Token GitHub SSH Private Key	PyPI PyPI API Token
Azure Azure Active Directory Application Secret Azure DevOps Personal Access Token Azure SAS Token Azure Service Management Certificate Azure SQL Connection String Azure Storage Account Key	GoCardless GoCardless Live Access Token GoCardless Sandbox Access Token	RubyGems RubyGems API Key
Clojars Clojars Deploy Token	Google Cloud Google API Key Google Cloud Private Key ID	Samsara Samsara API Token Samsara OAuth Access Token
CloudBees CodeShip CloudBees CodeShip Credential	Hashicorp Terraform Terraform Cloud / Enterprise API Token	SendGrid SendGrid API Key
Databricks Databricks Access Token	Hubspot Hubspot API Key	Shopify Shopify Access Token Shopify App Shared Secret Shopify Custom App Access Token Shopify Private App Password
Datadog Datadog API Key	Mailchimp Mailchimp API Key Mandrill API Key	Slack Slack API Token Slack Incoming Webhook URL Slack Workflow Webhook URL
Discord Discord Bot Token	Mailgun Mailgun API Key	SSLMate SSLMate API Key SSLMate Cluster Secret
Doppler Doppler CLI Token Doppler Personal Token Doppler SCIM Token Doppler Service Token	MessageBird MessageBird API Key	Stripe Stripe Live API Restricted Key Stripe Live API Secret Key Stripe Test API Restricted Key Stripe Test API Secret Key
	npm npm Access Token	Tencent Cloud Tencent Cloud Secret ID
	NuGet NuGet API Key	Twilio Twilio Account String Identifier Twilio API Key
	OpenAI OpenAI API Key	Valour Valour Access Token
	Palantir Palantir JSON Web Token	



Demo: Secret Scanning



Supply Chain Security



Software Composition Analysis (SCA)



GitHub (Dependency-Graph/Dependabot)



anchore (<https://anchore.com/>)



Dependency-Track
(<https://dependencytrack.org/>)

Dependency graph

Dependencies Dependents Dependabot

⚠ We found potential security vulnerabilities in your dependencies.

Dependencies defined in these manifest files have known security vulnerabilities and should be updated:

package.json 7 vulnerabilities found

[View Dependabot alerts](#)

Only the owner of this repository can see this message.

These dependencies are defined in `workshop-2021-learning-journey`'s manifest files, such as `package.json` and `frontend/package.json`.

Dependencies defined in `package.json` 138

>	<code>auth0 / express-jwt</code>	Known security vulnerability in <code>0.1.3</code> ▾
>	<code>auth0 / node-jsonwebtoken</code> <code>jsonwebtoken</code>	Known security vulnerability in <code>0.4.0</code> ▾
>	<code>c58 / marsdb</code>	Known security vulnerability in <code>0.6.11</code> ▾
>	<code>apostrophecms / sanitize-html</code>	Known security vulnerability in <code>1.4.2</code> ▾
>	<code>istanbuljs / istanbuljs</code> <code>@istanbuljs/nyc-config-typescript</code>	^ <code>1.0.1</code>
>	<code>Seally / types-chai</code> <code>@types/chai</code>	^ <code>4.2.14</code>
>	<code>DefinitelyTyped / DefinitelyTyped</code> <code>@types/chai-as-promised</code>	^ <code>7.1.3</code>

Dependabot alerts

Dismiss all ▾

4 Open ✓ 0 Closed

Manifest ▾ Sort ▾

<code>marsdb</code>	critical severity
<code>express-jwt</code>	high severity
<code>sanitize-html</code>	moderate severity
<code>jsonwebtoken</code>	critical severity

Dependency Management

GitHub Dependency graph

▶ Dependabot **alerts**

▶ Dependabot
security updates

▶ Dependabot
version updates

GitHub security alert digest
wulfland's repository security updates from the week of Jul 26 - Aug 2

wulfland's personal account

⚠ wulfland / VisualObjects
Known security vulnerabilities detected

Dependency	Version	Upgrade to
Newtonsoft.Json	< 13.0.1	~> 13.0.1

Defined in packages.config

Vulnerabilities
GHSA-5crp-9r3c-p9vr High severity

[Review all vulnerable dependencies](#)

Security / Dependabot alerts / #71

SQL injection in Django #71

Open Opened 2 months ago on django (pip) - authn-service/requirements.txt

Review security update

Severity
Critical 9.8 / 10

CVSS base metrics	
Attack vector	Network
Attack complexity	Low
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	High
Availability	High

CVSS:3.1(AV:N/A,C:L,PR:N/UI/RS:U/C:H/I:H/A:H)

Weaknesses
CWE-89

pip: bump django from 2.1.0 to 2.2.28 in /authn-service

Merging this pull request would fix 17 Dependabot alerts on django in authn-service/requirements.txt.

Package	Affected versions	Patched version
django (pip)	>= 2.0.0, < 2.2.10	2.2.10

Django 1.11 before 1.11.28, 2.2 before 2.2.10, and 3.0 before 3.0.3 allows SQL Injection if untrusted data is used as a StringAgg delimiter (e.g., in Django applications that offer downloads of data as a series of rows with a user-specified column delimiter). By passing a suitably crafted delimiter to a contrib.postgres.aggregates.StringAgg instance, it was possible to break escaping and inject malicious SQL.

dependabot[bot] opened this from b3540d8..1f0d6dd 2 months ago

Update requirements.txt #13

Open wulfland wants to merge 1 commit into main from wulfland-patch-1

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

Changes from all commits File filter Conversations Jump to 0 / 1 files viewed Review changes

authn-service/requirements.txt

django-piston 0.2.0

High severity vulnerability that affects django-piston and django-tastypie (GHSA-pvhp-v9qp-xf5r)
High severity Patched version: 0.2.2.1

Give feedback on [dependency review](#)

Dependency Management

GitHub Dependency graph

▶ Dependabot **alerts**

▶ Dependabot
security updates

▶ Dependabot
version updates

```
jobs:  
  dependabot:  
    runs-on: ubuntu-latest  
    if: ${{ github.actor == 'dependabot[bot]' }}  
    steps:  
      - name: Dependabot metadata  
        id: dependabot-metadata  
        uses: dependabot/fetch-metadata@v1.1.1  
        with:  
          github-token: "${{ secrets.GITHUB_TOKEN }}"  
      - name: Enable auto-merge for all patch versions  
        if: ${{ steps.metadata.outputs.update-type == 'version-update:semver-patch' }}  
        run: gh pr merge --auto --merge "$PR_URL"  
        env:  
          PR_URL: ${{ github.event.pull_request.html_url }}  
          GITHUB_TOKEN: ${{ secrets.GITHUB_TOKEN }}
```

Bump terser from 4.8.0 to 4.8.1 in /frontend #50

dependabot wants to merge 1 commit into `main` from `dependabot/npm_and_yarn/frontend/terser-4.8.1`

Conversation 0 Commits 1 Checks 6 Files changed 1 +14 -22

dependabot bot commented 14 days ago

Bumps `terser` from 4.8.0 to 4.8.1.

► Changelog

► Commits

compatibility 87%

Dependabot will resolve any conflicts with this PR as long as you don't alter it yourself. You can also trigger a rebase manually by commenting `@dependabot rebase`.

► Dependabot commands and options

Bump terser from 4.8.0 to 4.8.1 in /frontend Verified ✓ 9244552

dependabot bot added `dependencies` `javascript` labels 14 days ago

Reviewers: No reviews. Still in progress? Convert to draft.

Assignees: No one—assign yourself.

Labels: `dependencies` `javascript`

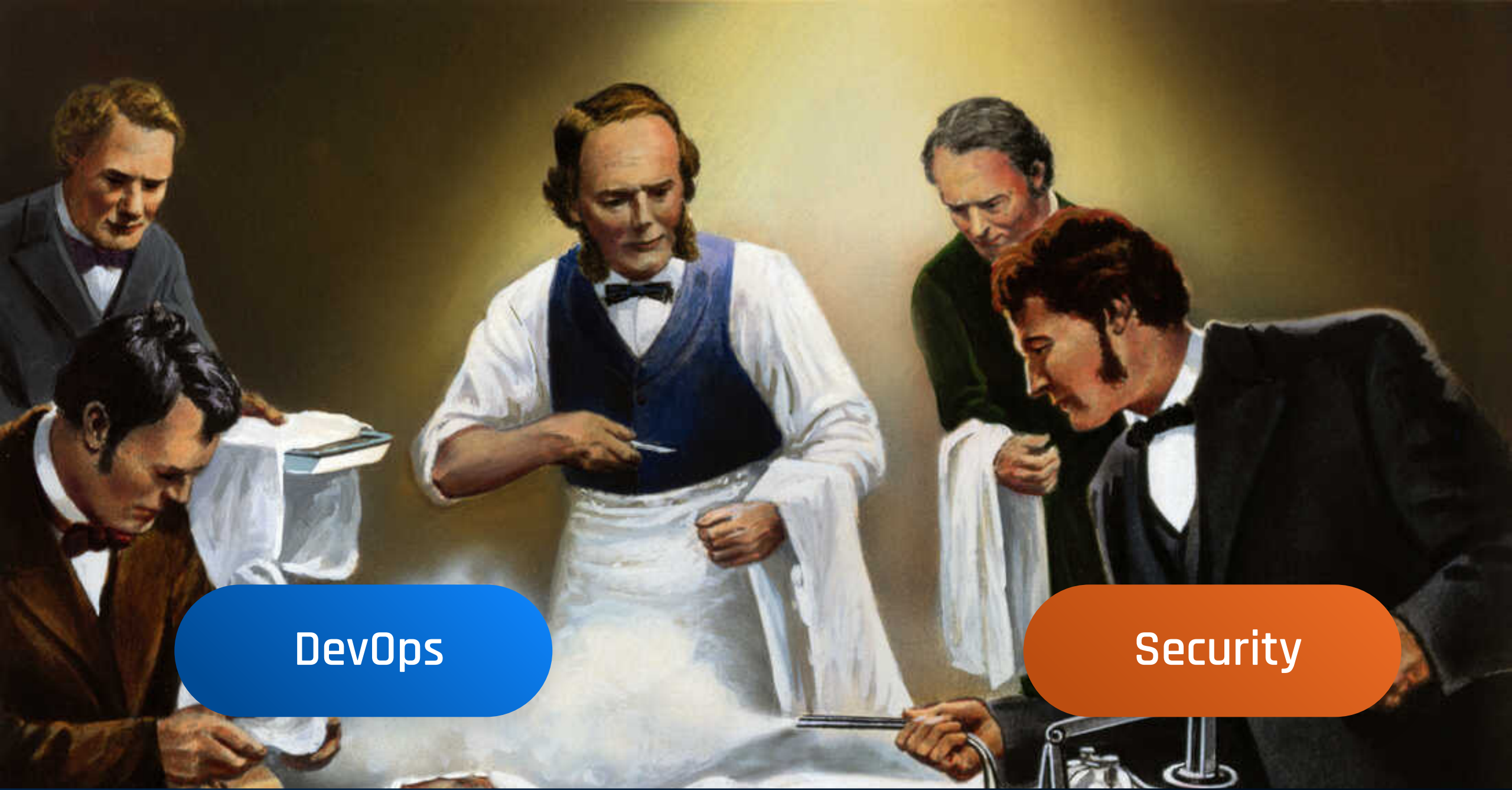
Projects: None yet.

Milestone: No milestone.

Development: Successfully merging this pull request may



Demo: Demo: Dependabot



DevOps

Security

Joseph Lister directing the use of carbolic acid spray in one of his earliest antiseptic surgical operations, circa 1865. Bettmann Archive

Thank you



Blog : <https://writeabout.net>



Twitter : @mike_kaufmann



GitHub : @wulfland



LinkedIn : <https://www.linkedin.com/in/mikaufmann/>