Xpirit

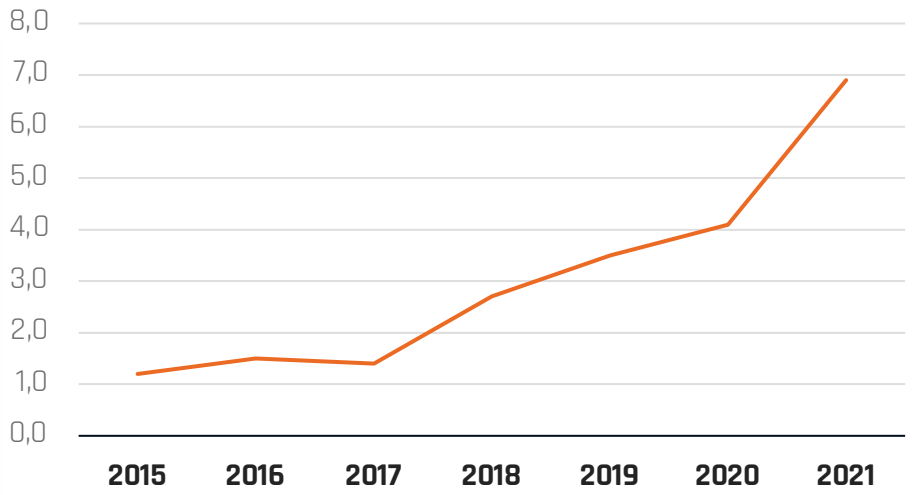
{ From AppSec to DevSec }

Shift left with GitHub Advanced Security

Losses caused by cyber attacks reported to IC3

2020	2021
$ 4.100.000.000	$ 6.900.000.000

Loss caused by reported cyber crime (in billion USD)



Top 5 crime types:

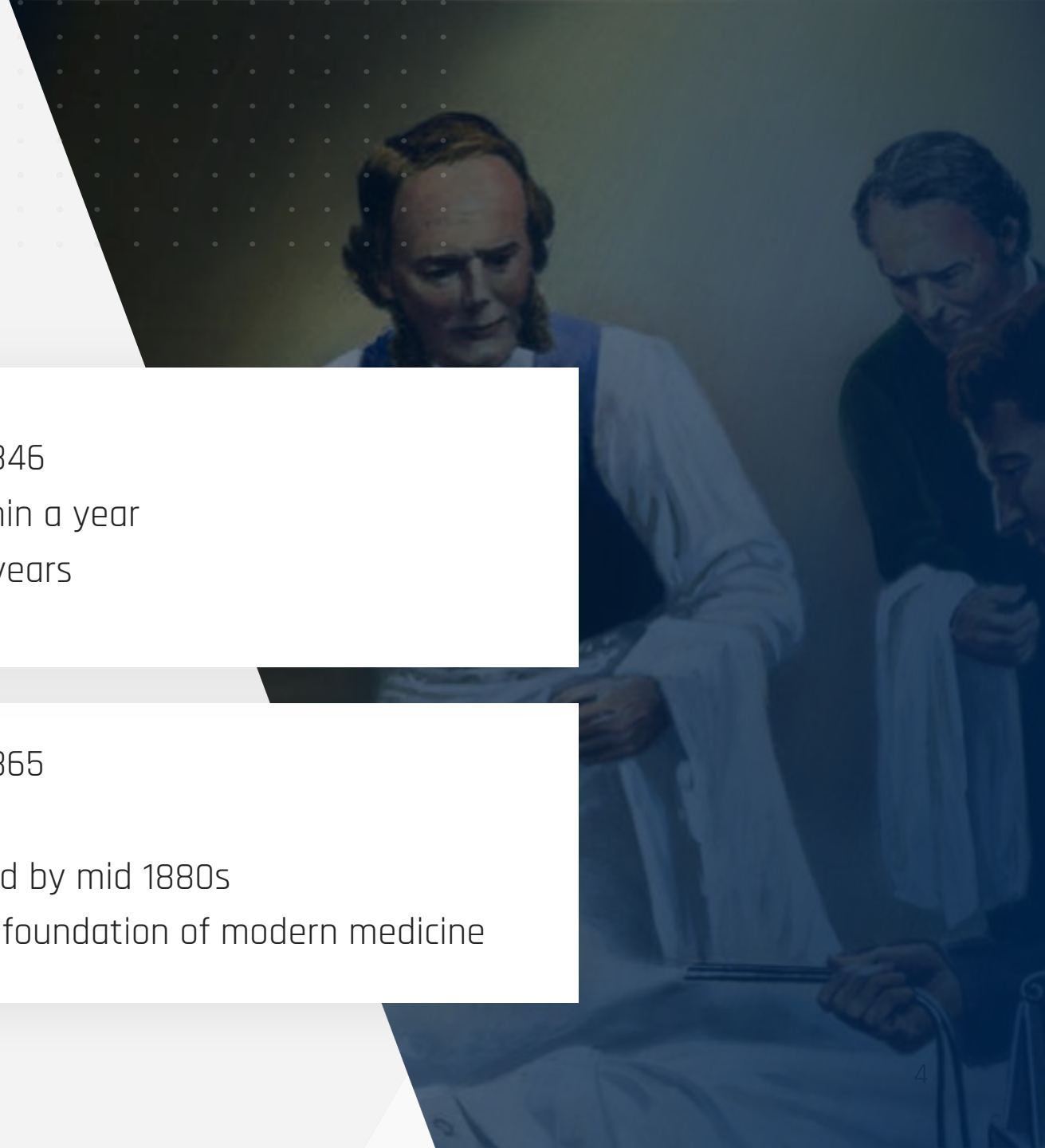
- Phishing
- Non-Payment / Delivery
- Data Breach
- Identity Theft
- Extortion

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-hearted adopted by mid 1880s
- Now considered the foundation of modern medicine

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

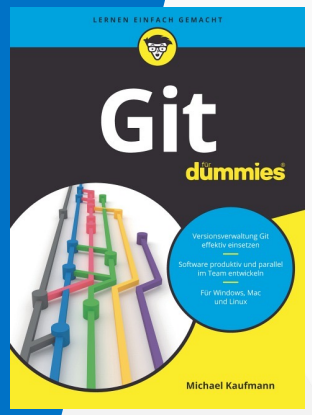
@mike_kaufmann

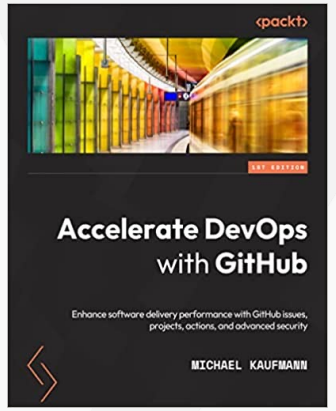
@wulfland

https://writeabout.net

Microsoft REGIONAL DIRECTOR

MVP Microsoft® Most Valuable Professional





- 20 years software developer
- 15 years ALM & DevOps
- 10 years Git and GitHub
- Microsoft Regional Director & MVP

Xpirit

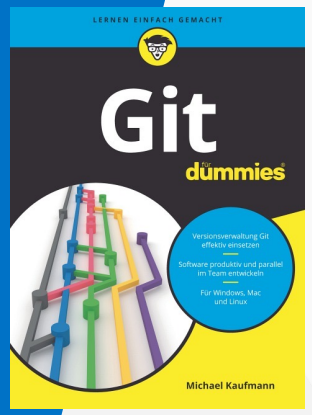
6

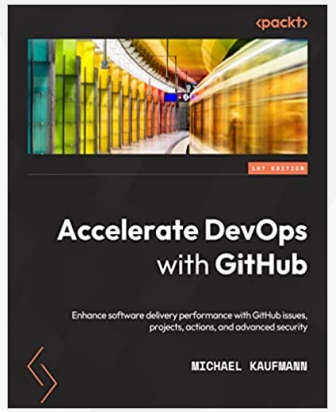
Michael Kaufmann

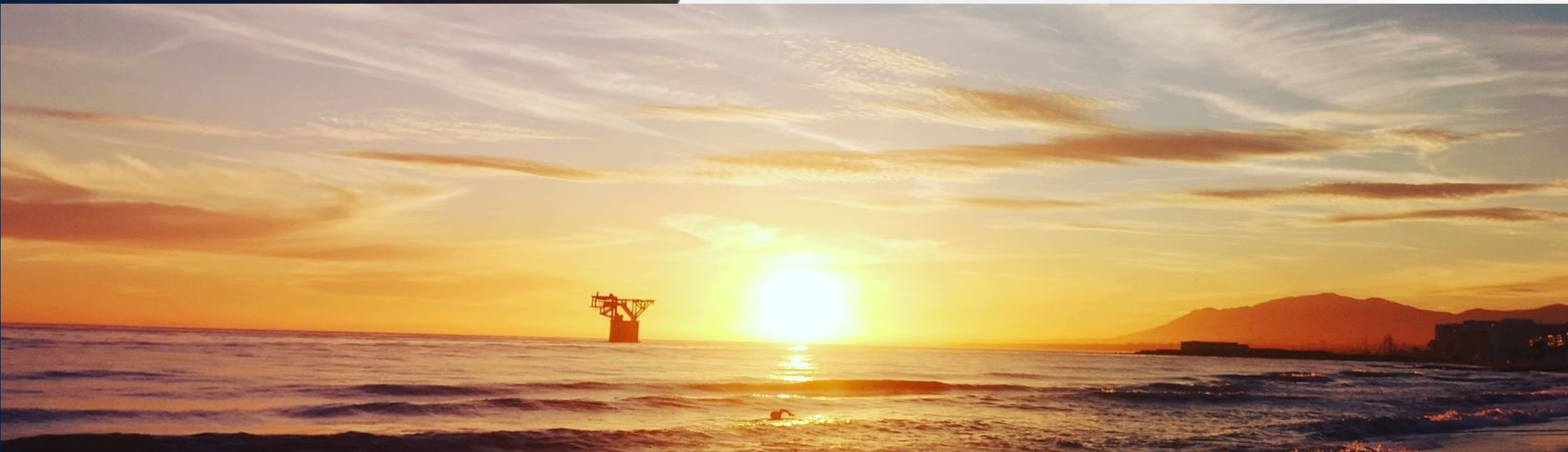
Founder & Managing Director, Xpirit Germany

Microsoft REGIONAL DIRECTOR

MVP Microsoft® Most Valuable Professional







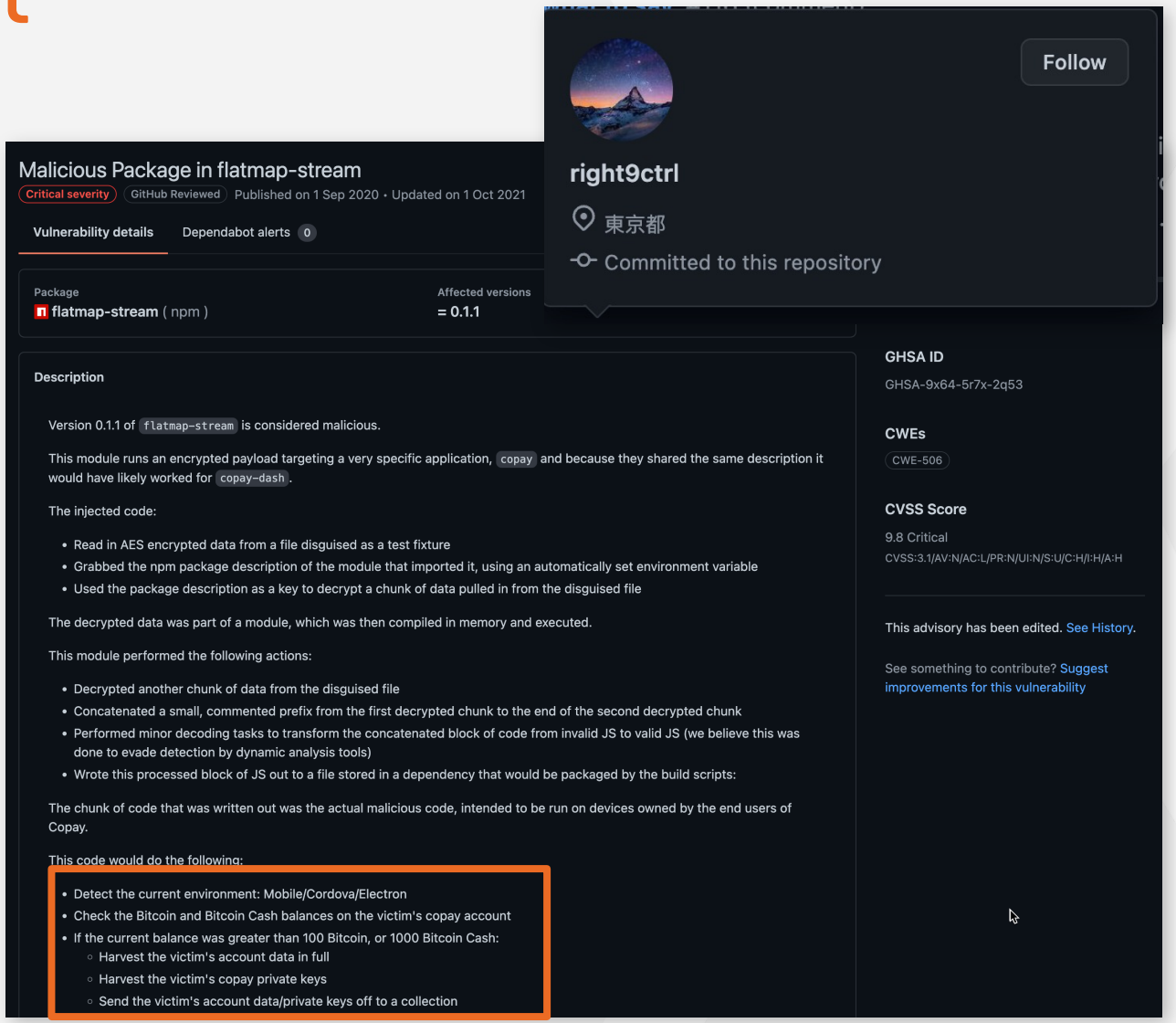
The event-stream incident

Social engineering attack

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

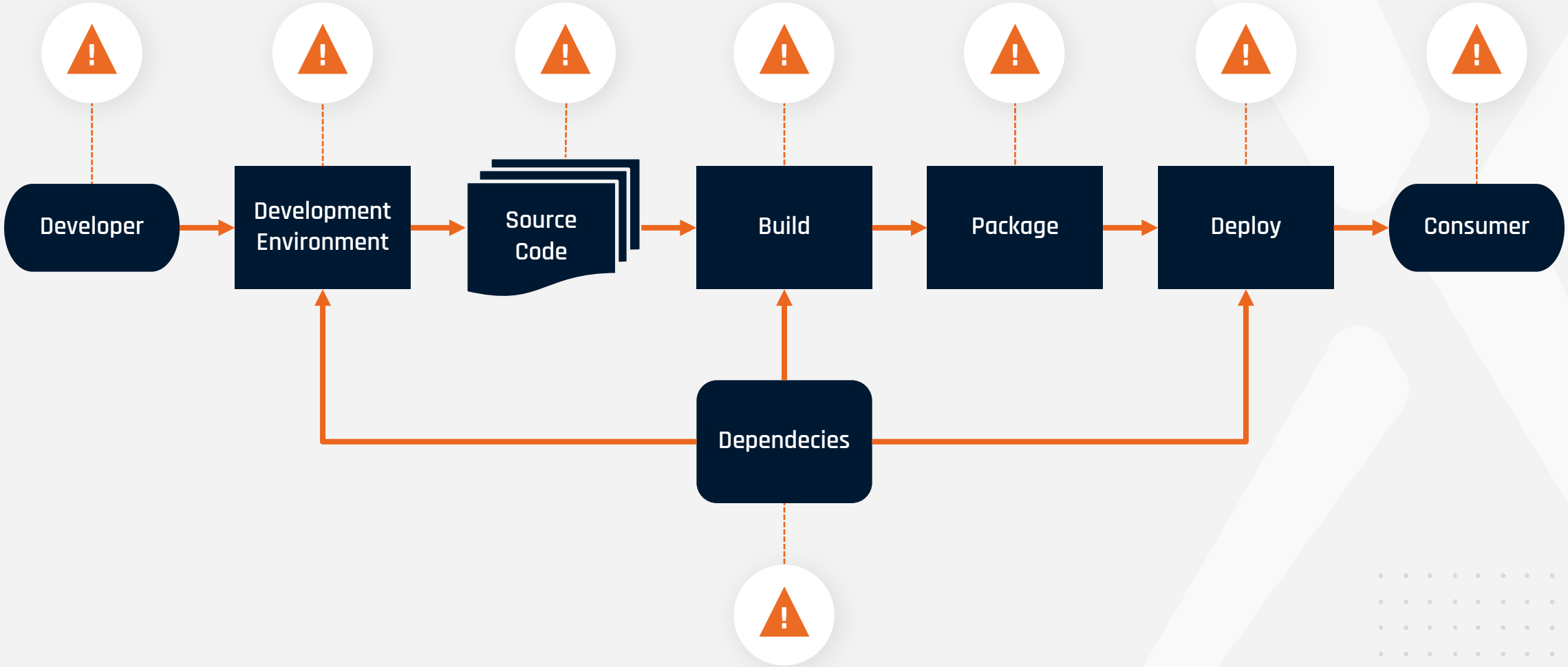
Code execution in build process targeting copay

Harvest the user's bitcoin and private keys



Xpirit

Attack vectors

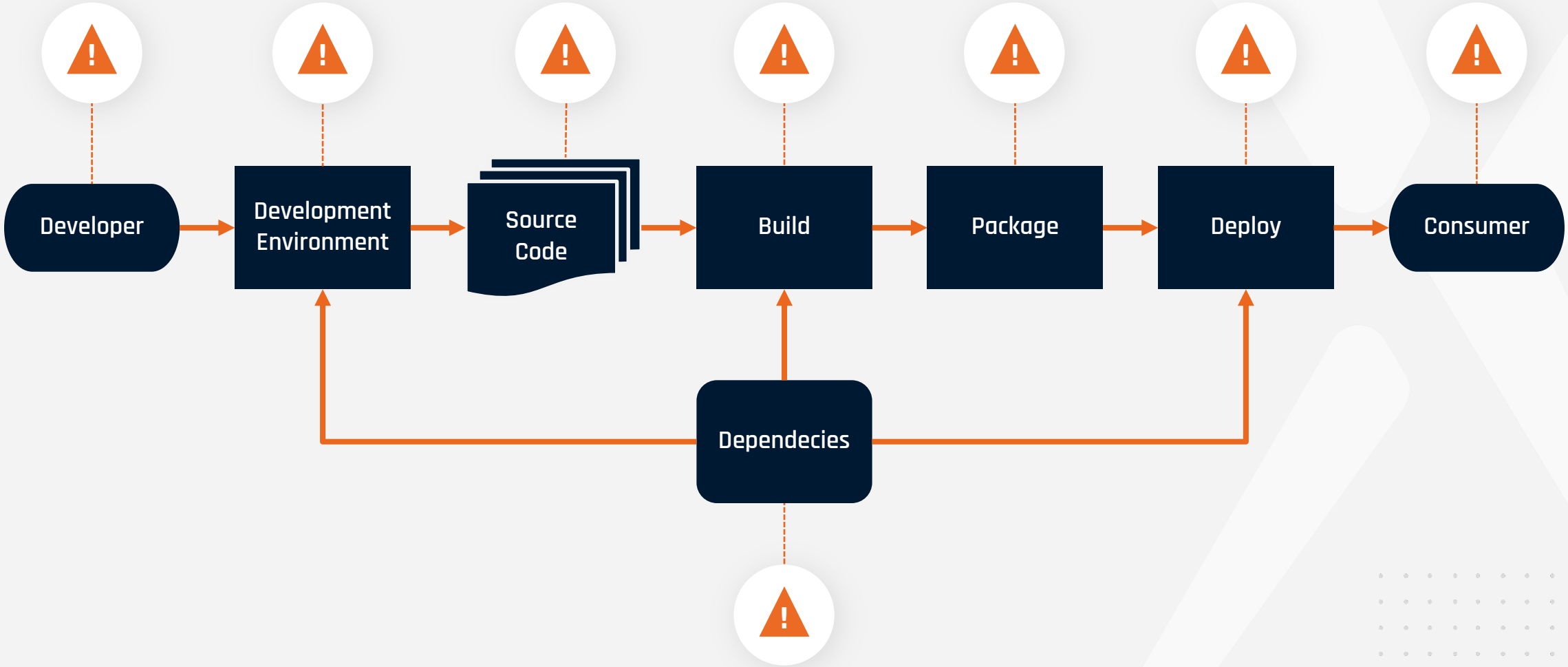


Xpirit

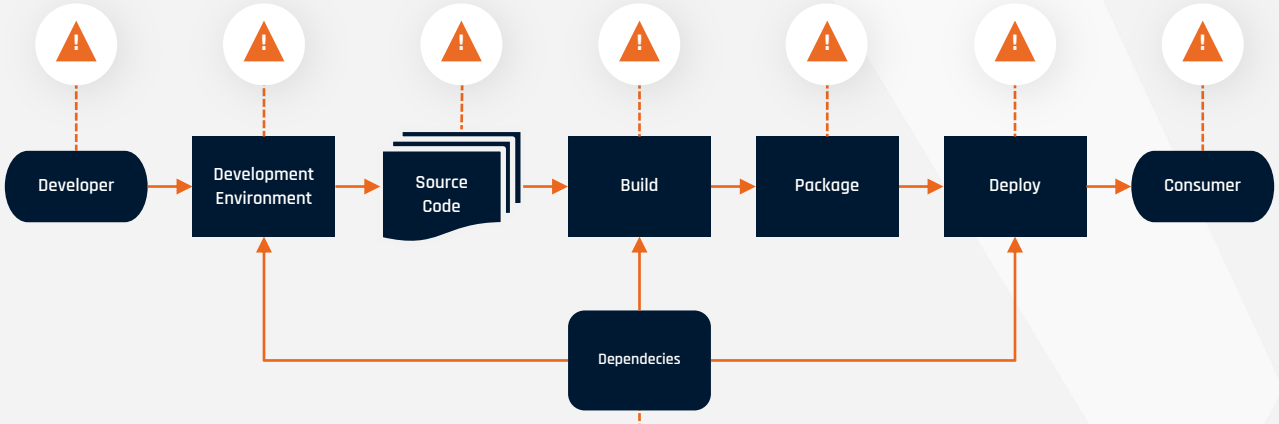

gatsby
show
Remaining packages: 1
view source code
share to twitter
become a patron
NoteBook

Xpirit

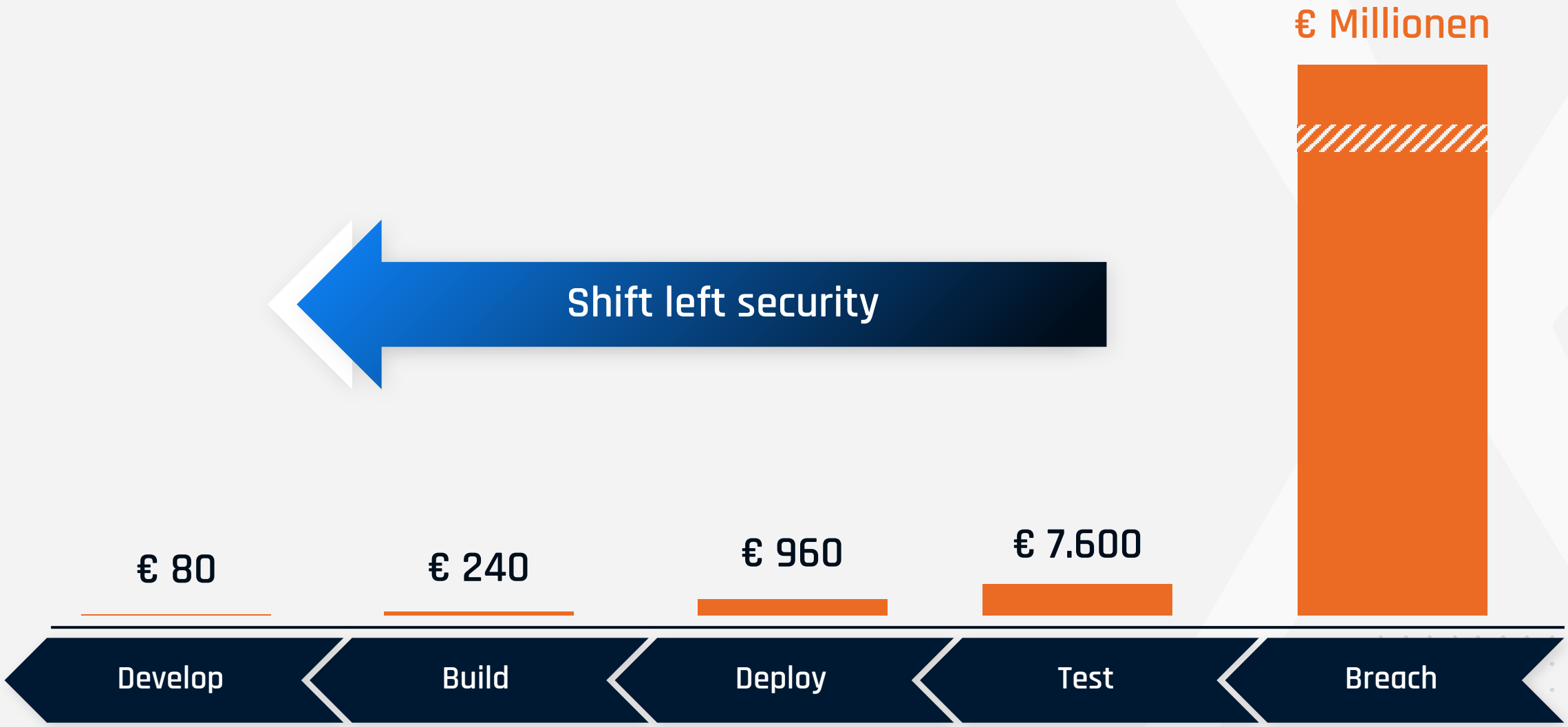
Attack vectors



Attack vectors



Costs for fixing a security vulnerability



Source: Ponemon Institute Cost of a Data Breach 2020

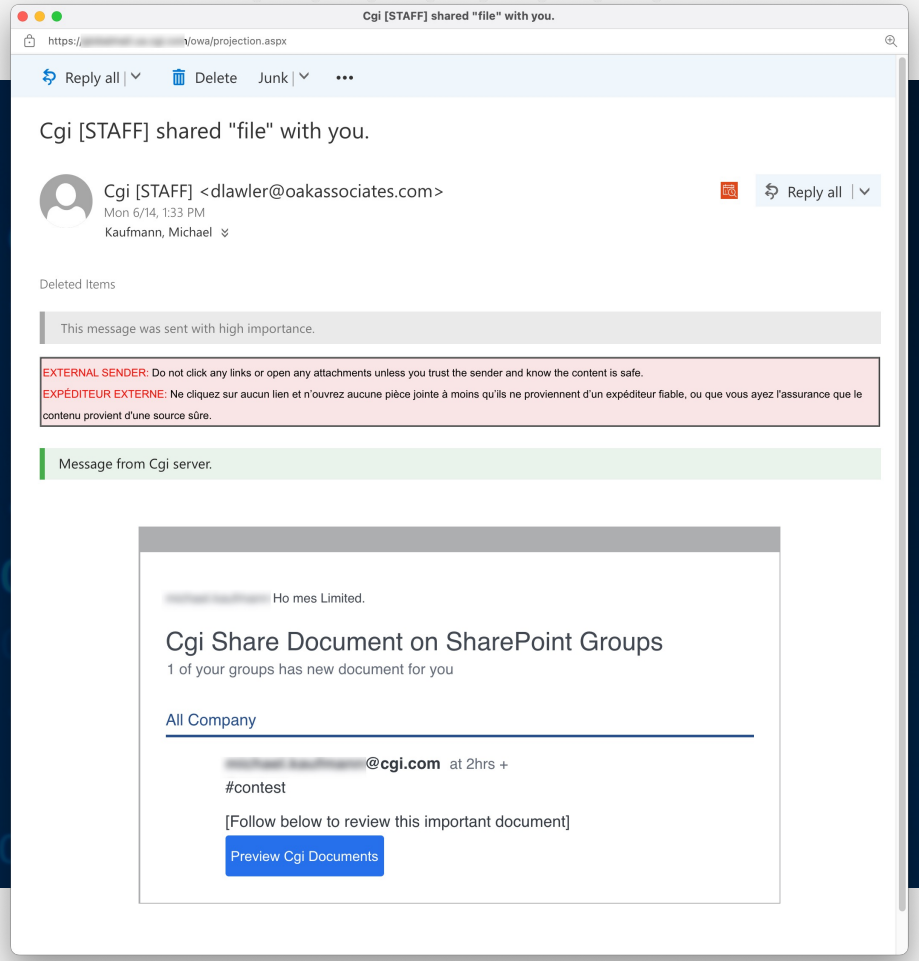
Developer Security

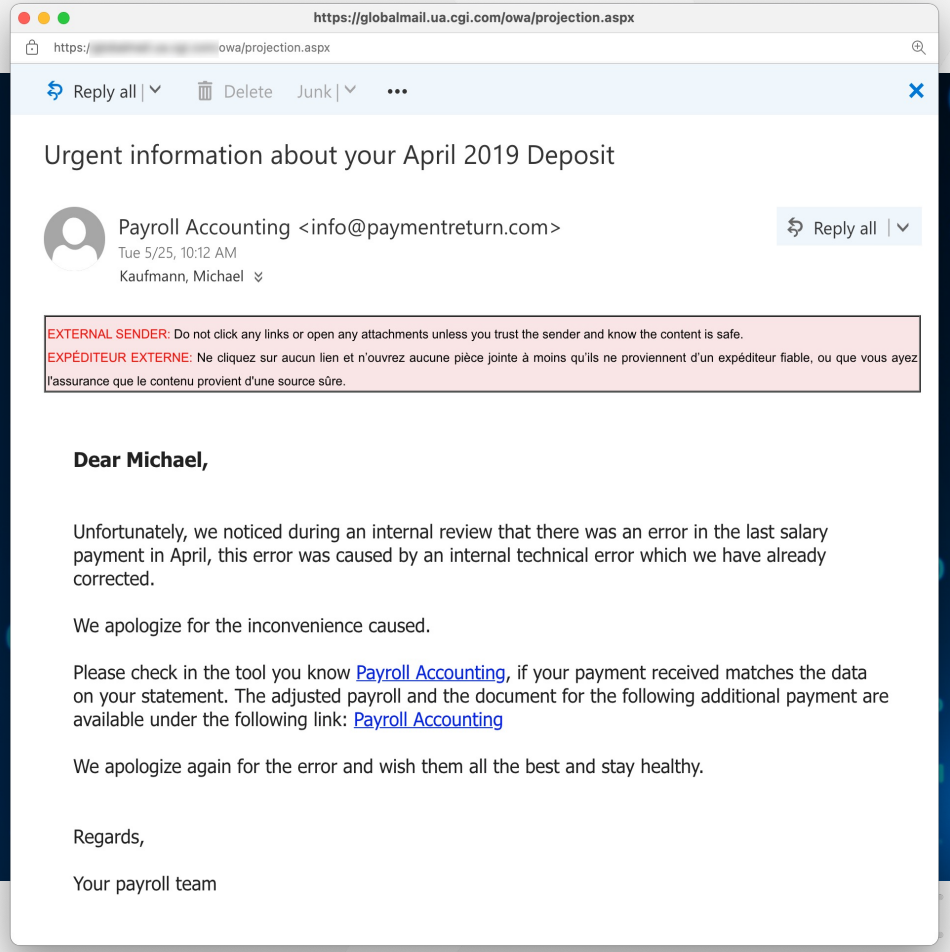
Attacking developers

- 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





Xpirit

Attacking developers

Typo squatting 

Namespace shadowing 

Typo squatting

```
$ npm install crossenv
```

Steals all your environment variables

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

Normal package

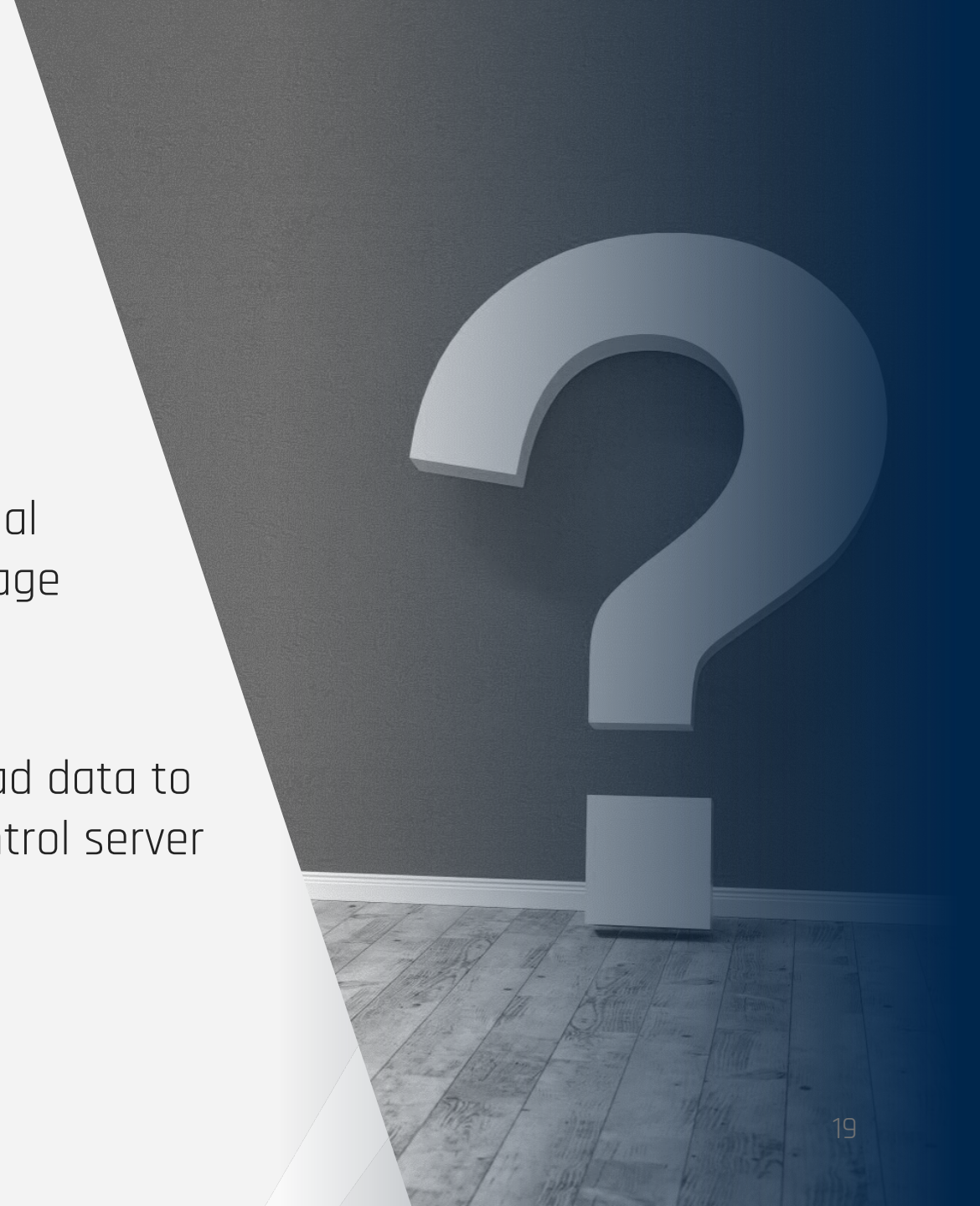
Namespace shadowing

```
$ 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?	

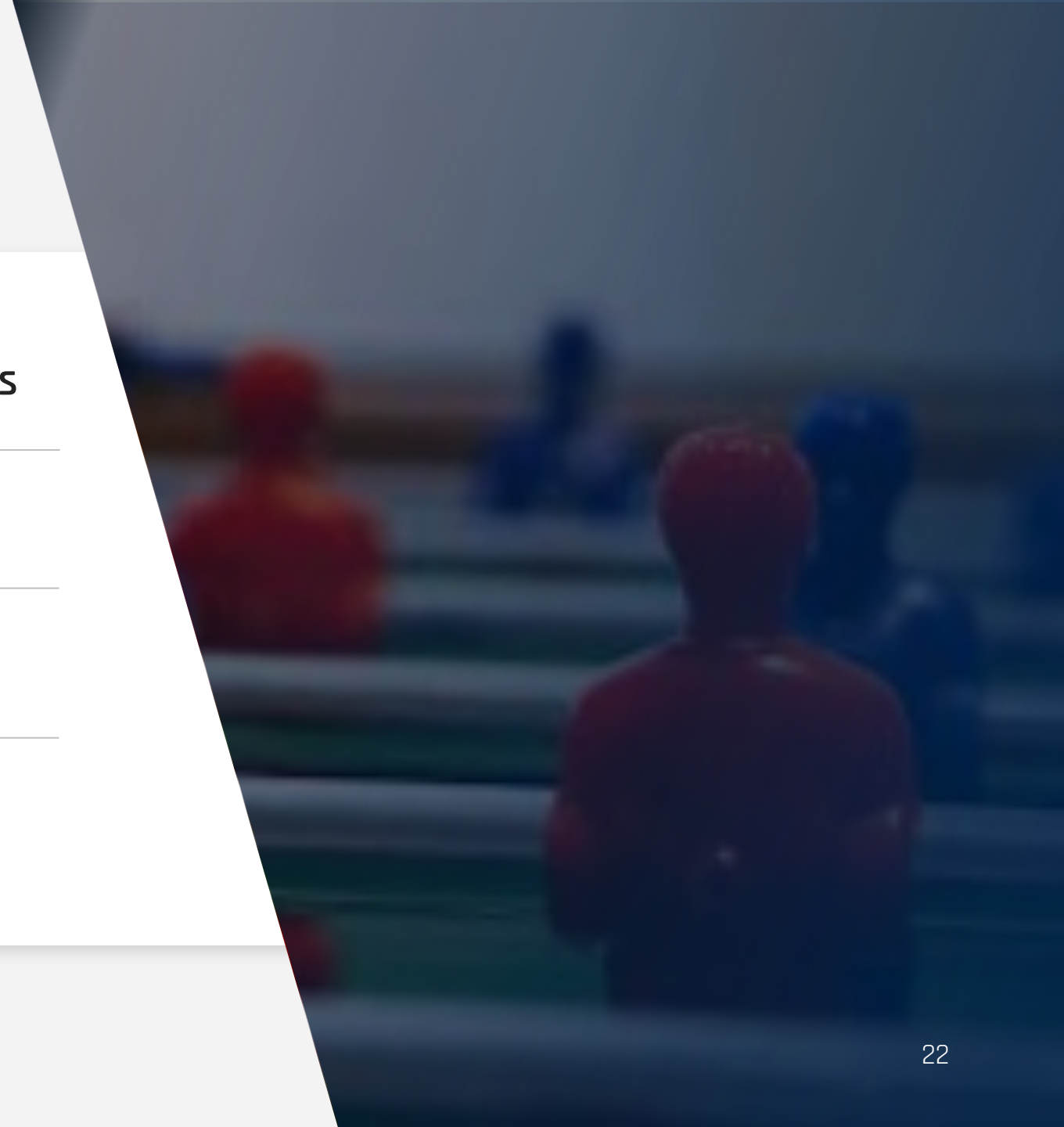
What to do?

- Security Awareness Trainings
- Security Games
- Red team | blue team simulations
- Virtualized dev-environments

Xpirit

Capture the flag

- Red team | blue team simulations
- Insider attacks
- Create awareness
- Think like attackers



Xpirit

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

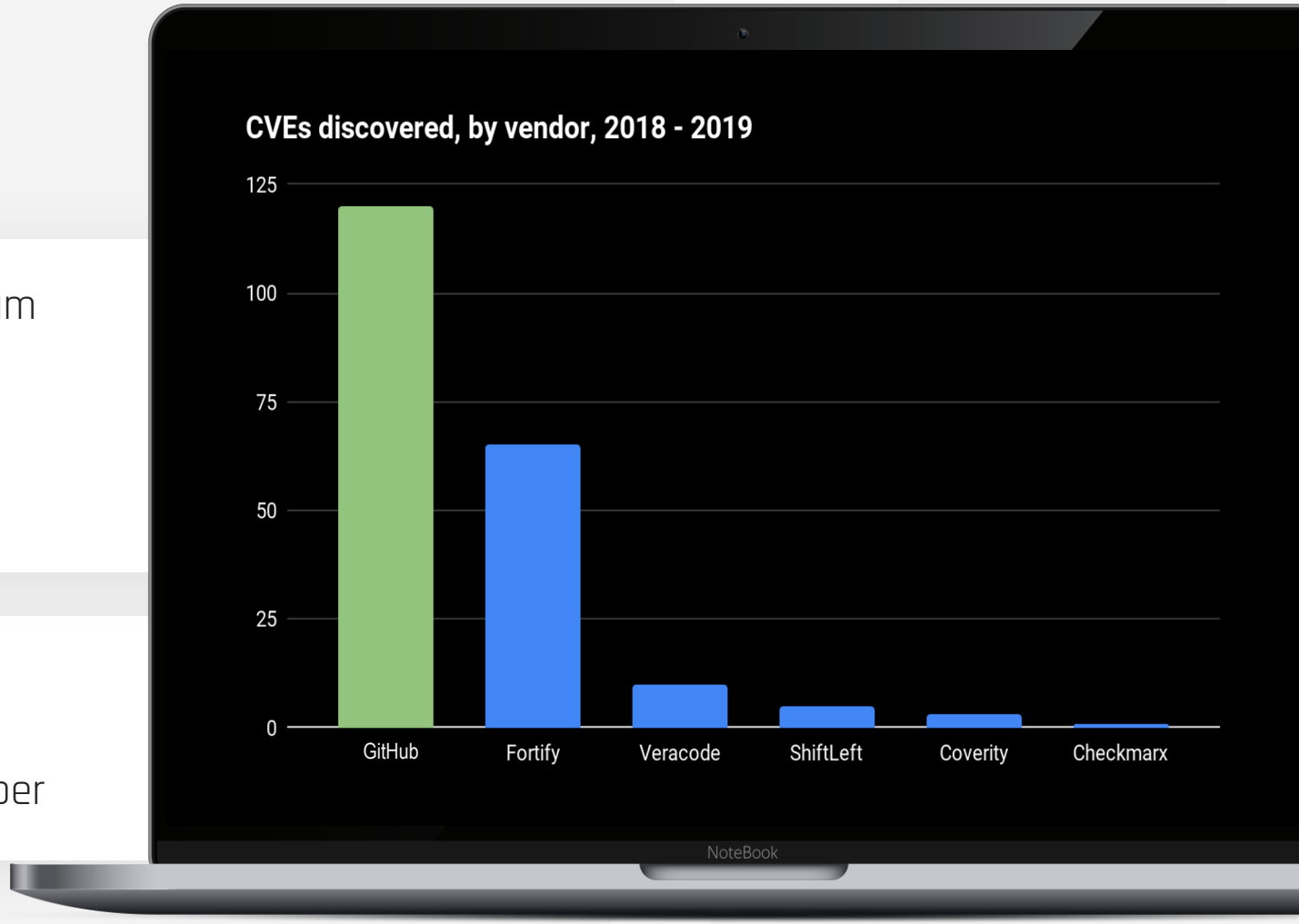
- Advanced code analysis engine based on 13 years of research by a 30 person team from Oxford University
- Allows you to query your code's logic to find vulnerabilities
- Queries can be quickly customized to adapt to your specific threat topology
- Community-driven query set powers every project with 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



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:

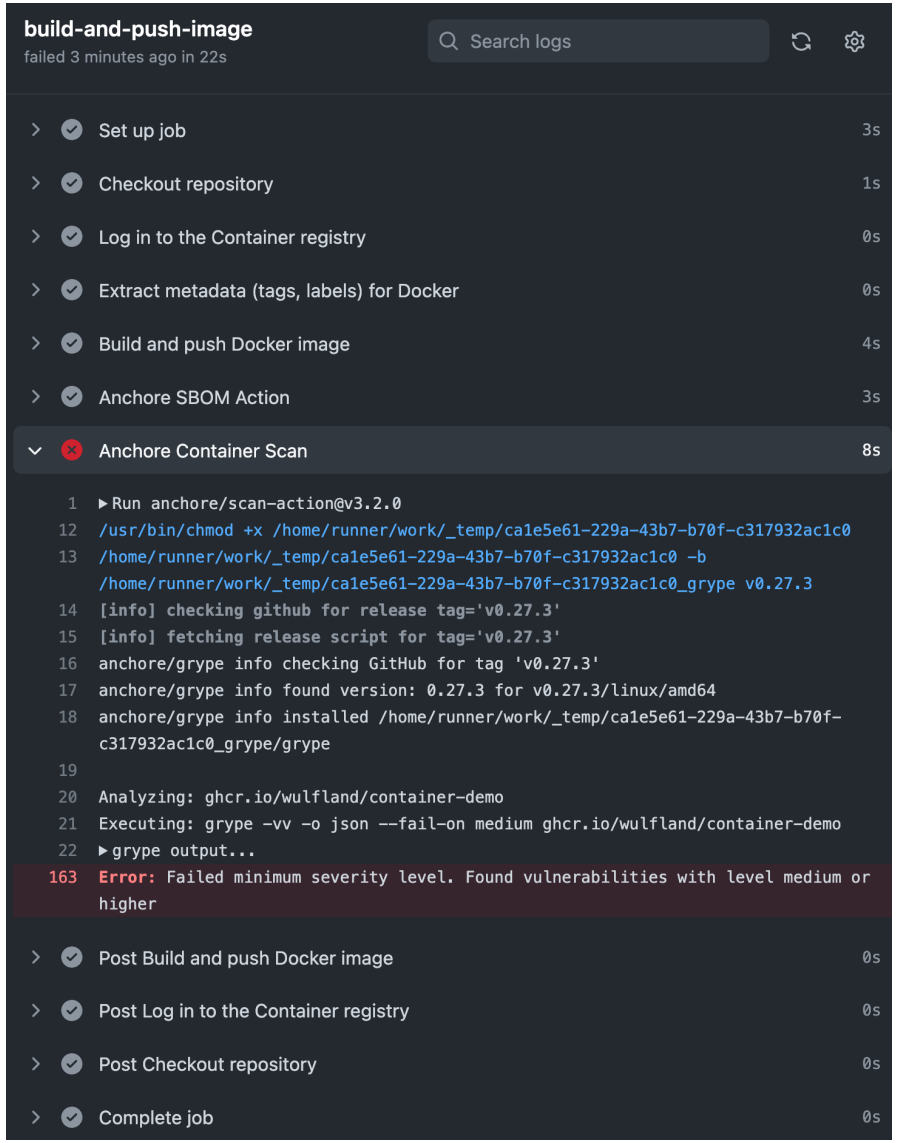
- Anchore gryp
  https://github.com/anchore/grype/
- Clair
  https://quay.github.io/clair/

Commercial:

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

```yaml
- 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



Xpirit

Infrastructure Scanning

Infrastructure policies

Open source:

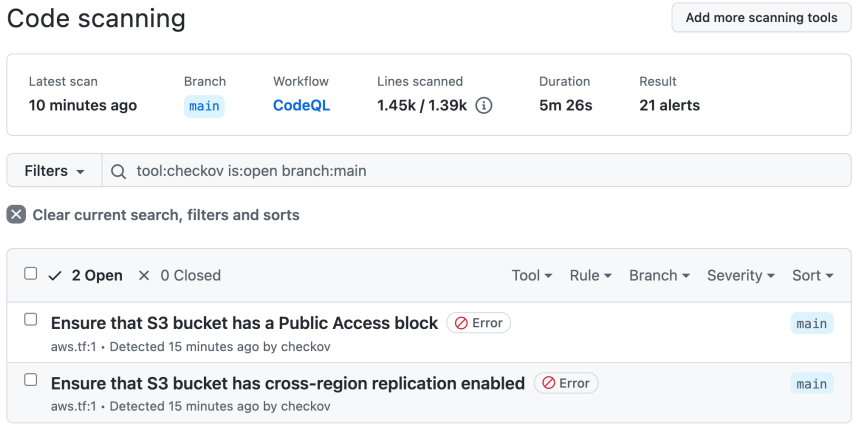
- Checkov
  https://www.aquasec.com/products/container-security/
- OpenVAS

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/

```yaml
- 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()
```

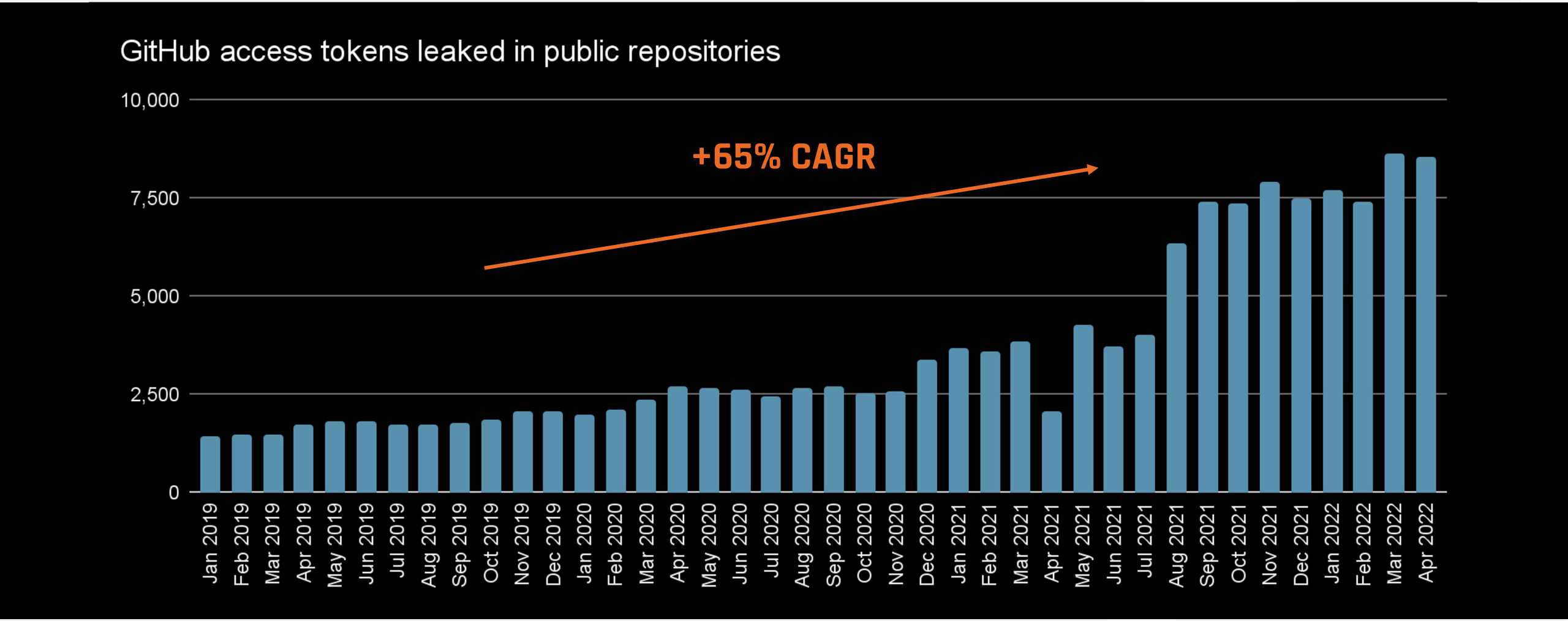


Xpirit

Demo: Code analysis

Secret Scanning

We're seeing more credential leaks than ever



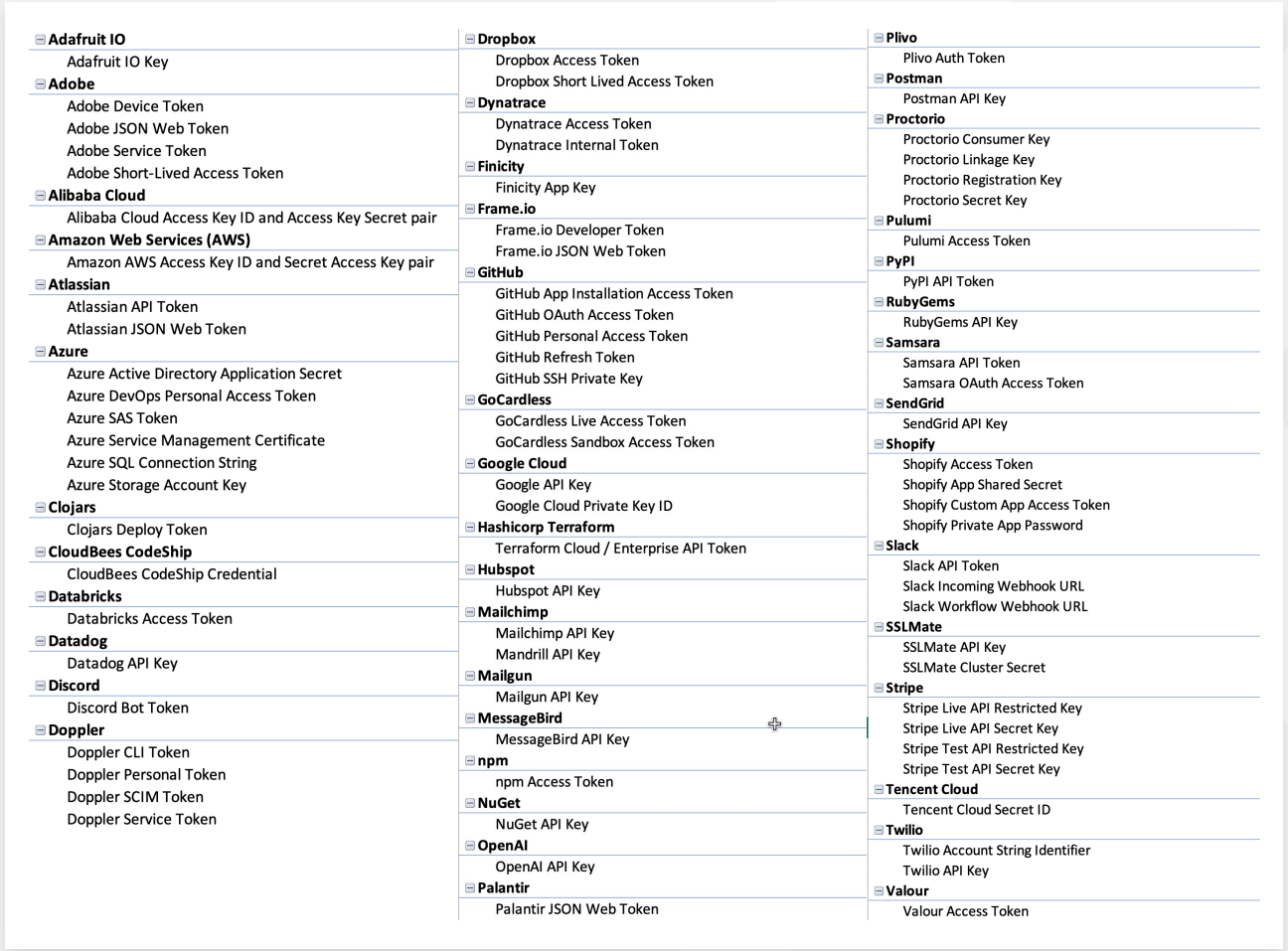
Secret Scanning

Code

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

Fileshare

- Bash/PowerShell
- Dumpster



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

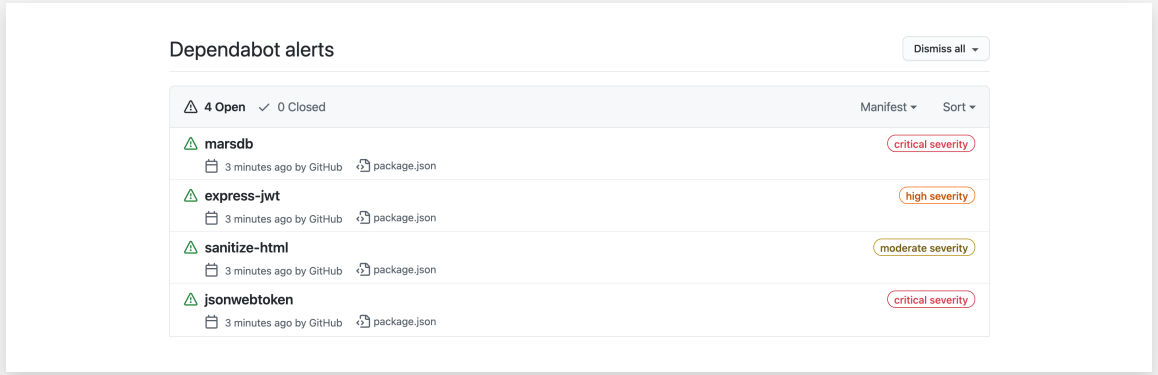
Xpirit

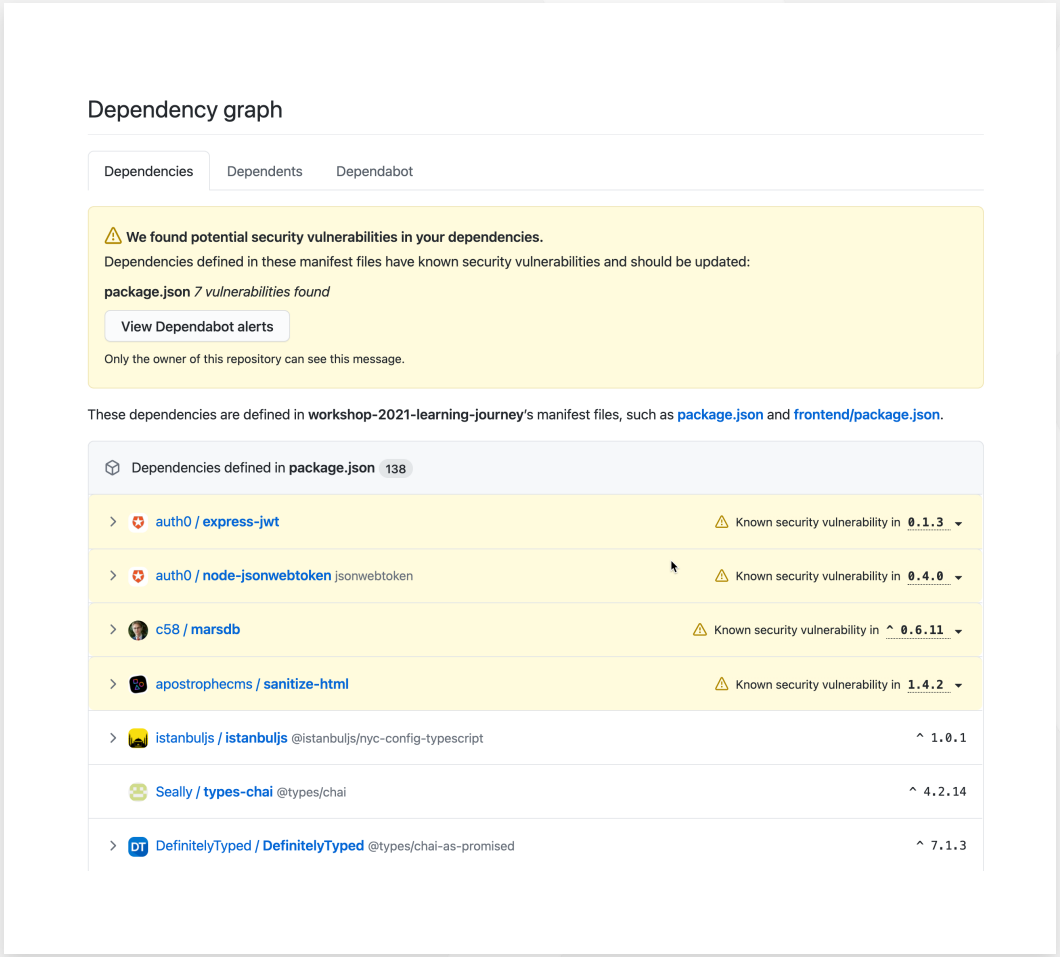
Demo: Secret Scanning

Supply Chain Security

Software Composition Analysis (SCA)

- GitHub (Dependency-Graph/Dependabot)
- anchore (https://anchore.com/)
- Dependency-Track (https://dependencytrack.org/)



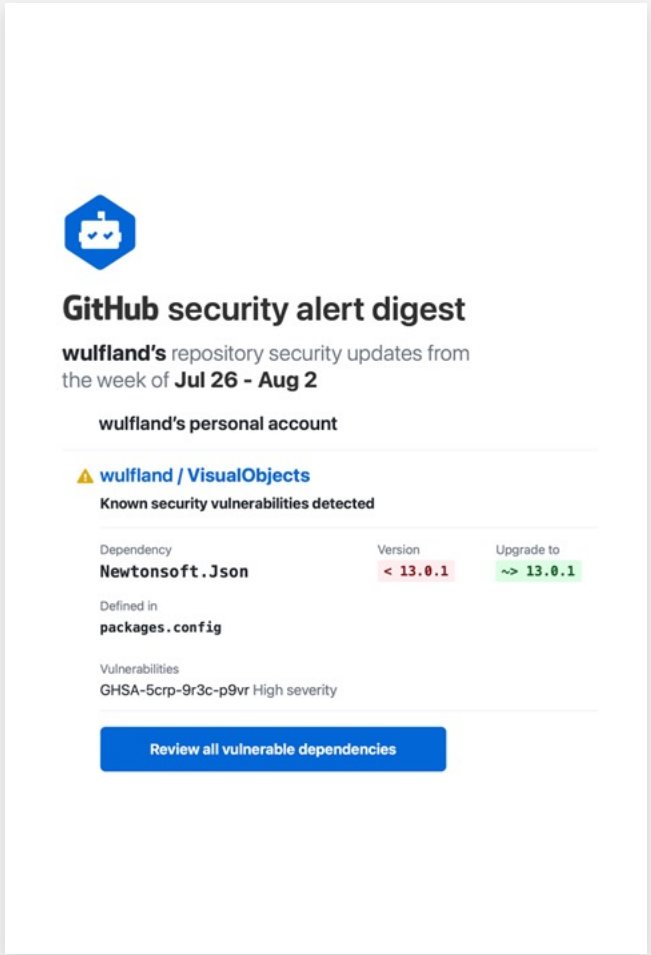


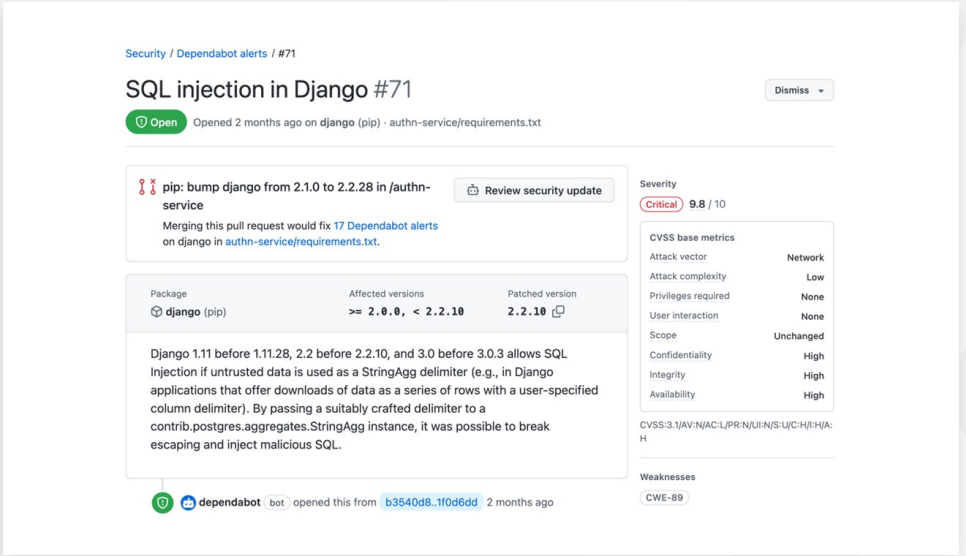
Xpirit

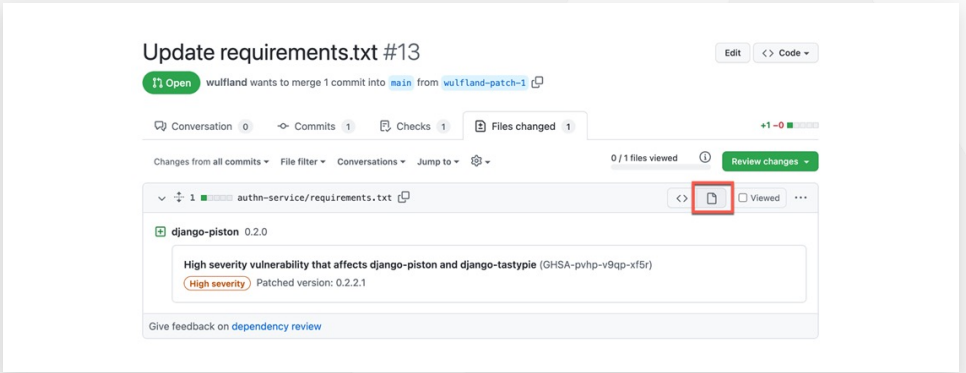
Dependency Management

GitHub Dependency graph

- Dependabot **alerts**
- Dependabot **security updates**
- Dependabot **version updates**







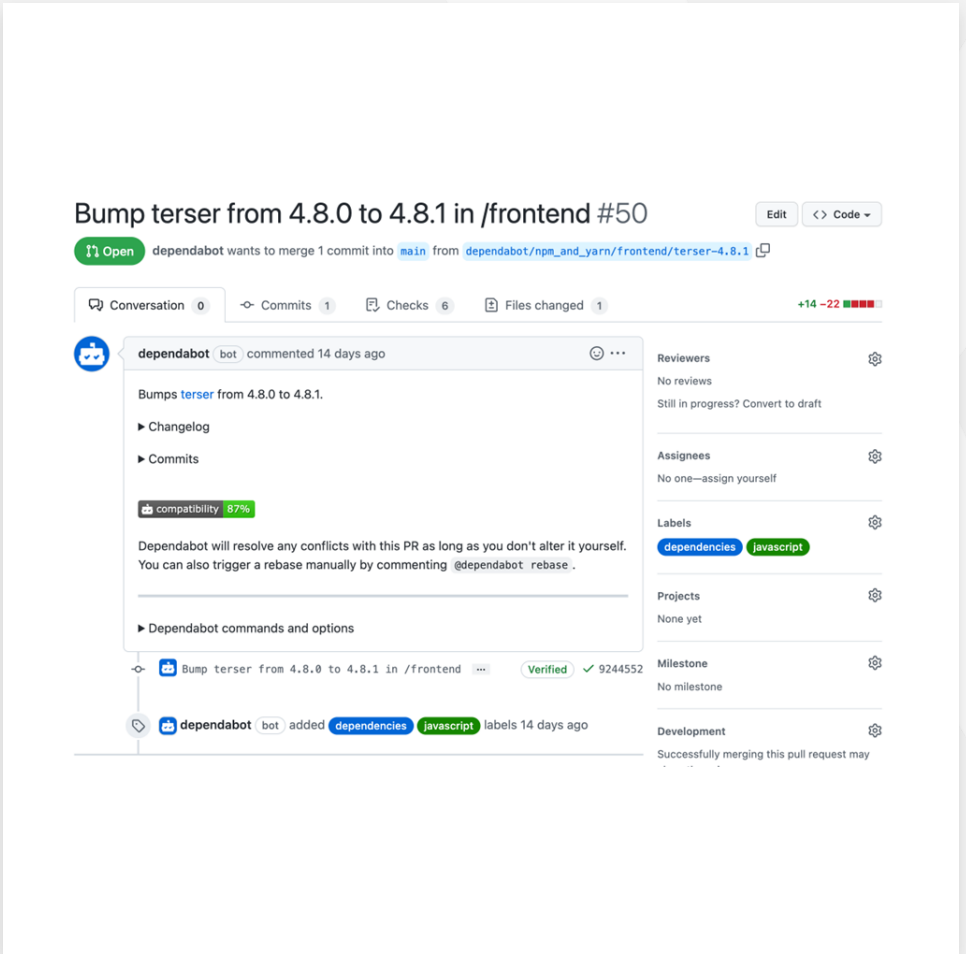
Dependency Management

GitHub Dependency graph

- Dependabot **alerts**
- Dependabot **security updates**
- Dependabot **version updates**

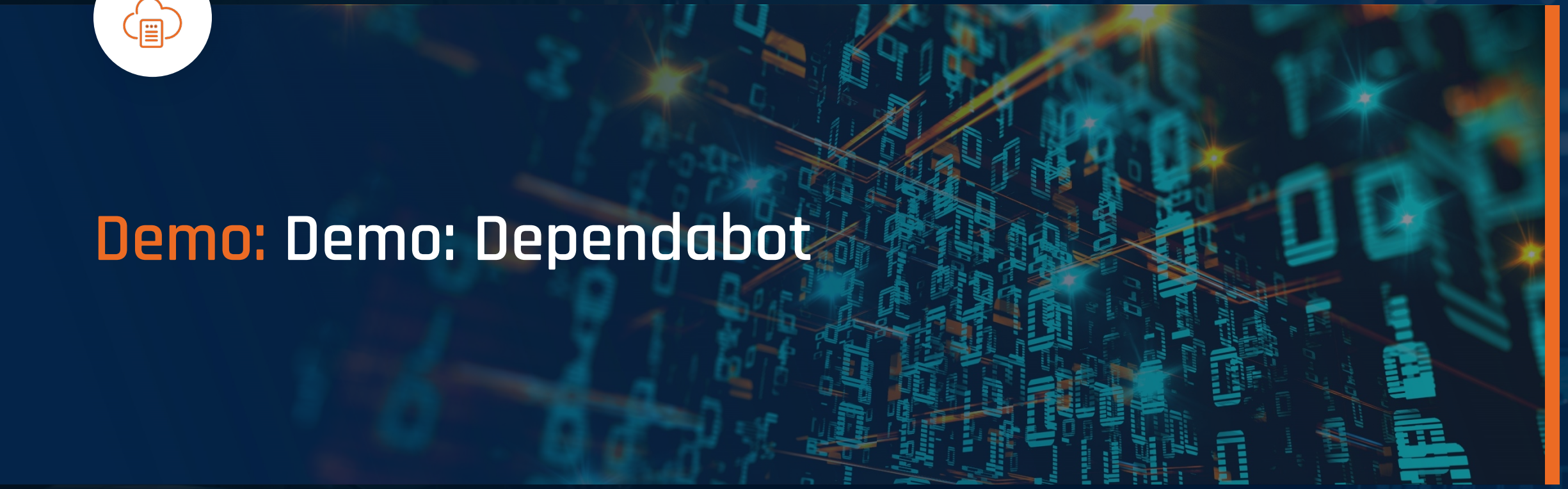
```yaml
jobs:
  dependabot:
    runs-on: ubuntu-latest
    if: ${{ github.actor == 'dependabot[bot]' }}
    steps:
      - name: Dependabot metadata
        id: dependabot-metadata
        uses: dependabot/fetch-metadata@v1.1.1
        with:
          github-token: "${{ secrets.GITHUB_TOKEN }}"

      - 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}}
```



Xpirit

Xpirit



Demo: Demo: Dependabot

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/