Xebia | Microsoft Services

Shift Left on Security with GitHub and Azure DevOps

Randy Pagels
DevOps Architect | Trainer
Randy.Pagels@Xebia.com

PagelsR

Randy-Pagels

Agenda

- The State of Security Today
- Dependency Chain
- GitHub Advanced Security
- Securing your Supply Chain
- Secret Scanning
- Push Protection
- Code Scanning
- Microsoft Defender for DevOps

The State of Security Today

Some interesting facts…

- ✓ **Over 8,000 vulnerabilities were published in Q1 of 2022**
- ✓ Half of internal-facing web application vulnerabilities are considered high risk
- ✓ **The mean time to remediation (MTTR) is around 180 days**
- ✓ The oldest vulnerability discovered in 2020 was 21 years old
- ✓ **75% of attacks in 2020 used vulnerabilities that were at least two years old**
- ✓ 31% of companies detected attempts to exploit software vulnerabilities
- ✓ **Information leakage flaws are the most common**
- ✓ Frequent scanning correlates to much faster remediation time
- ✓ **Over 75 percent of applications have at least one flaw**
- ✓ The global IT security market is set to reach almost $400 billion by 2028
- ✓ **Unpatched vulnerabilities were involved in 60% of data breaches**

25+ Cyber Security Vulnerability Statistics and Facts of 2023 (comparitech.com)

4 years

On average, vulnerabilities go undetected for four years before being identified.

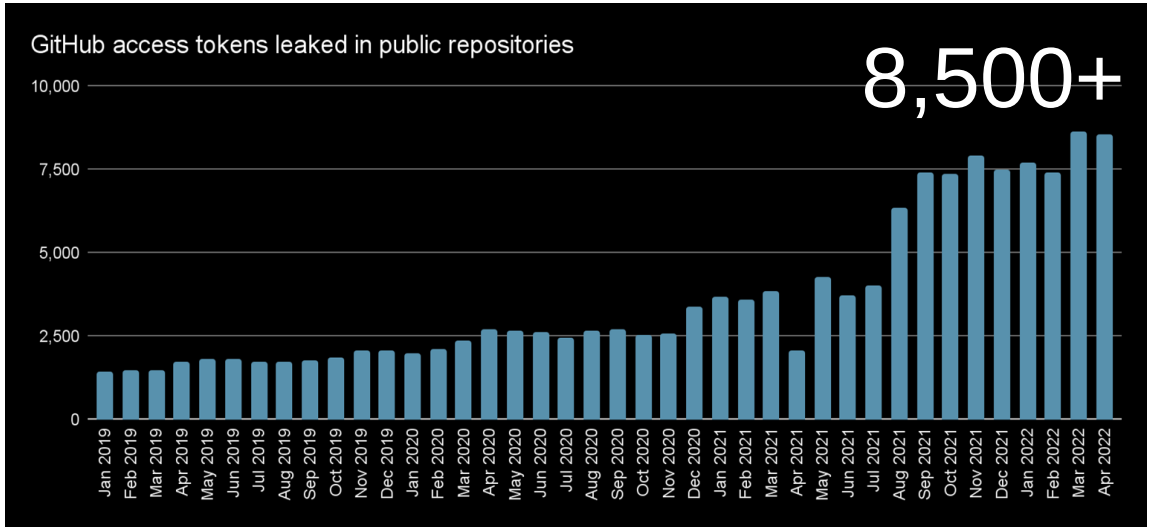
7 years

Sometimes, even longer than that:

- Log4j was vulnerable for ~7 years

Leaked Secrets

GitHub is seeing more credential leaks than ever



Source: GitHub data

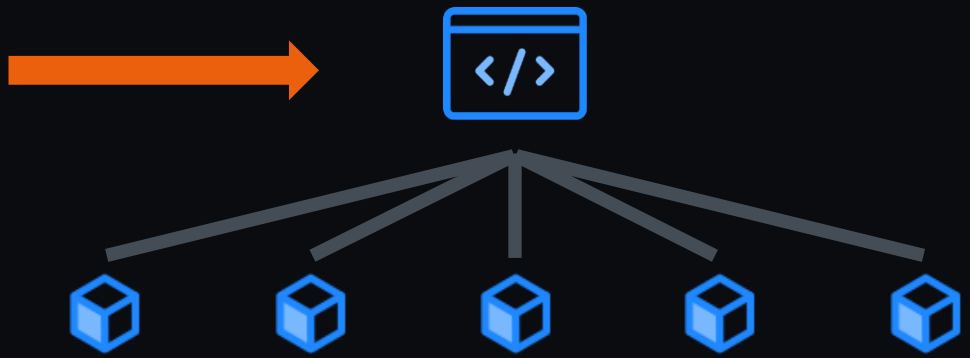
Secret Leaked exposing 38 TB of Data

GitGuardian reported in **2023** GitHub users accidentally exposed approximately **12.8 million** secrets in more than **3 million** public repositories

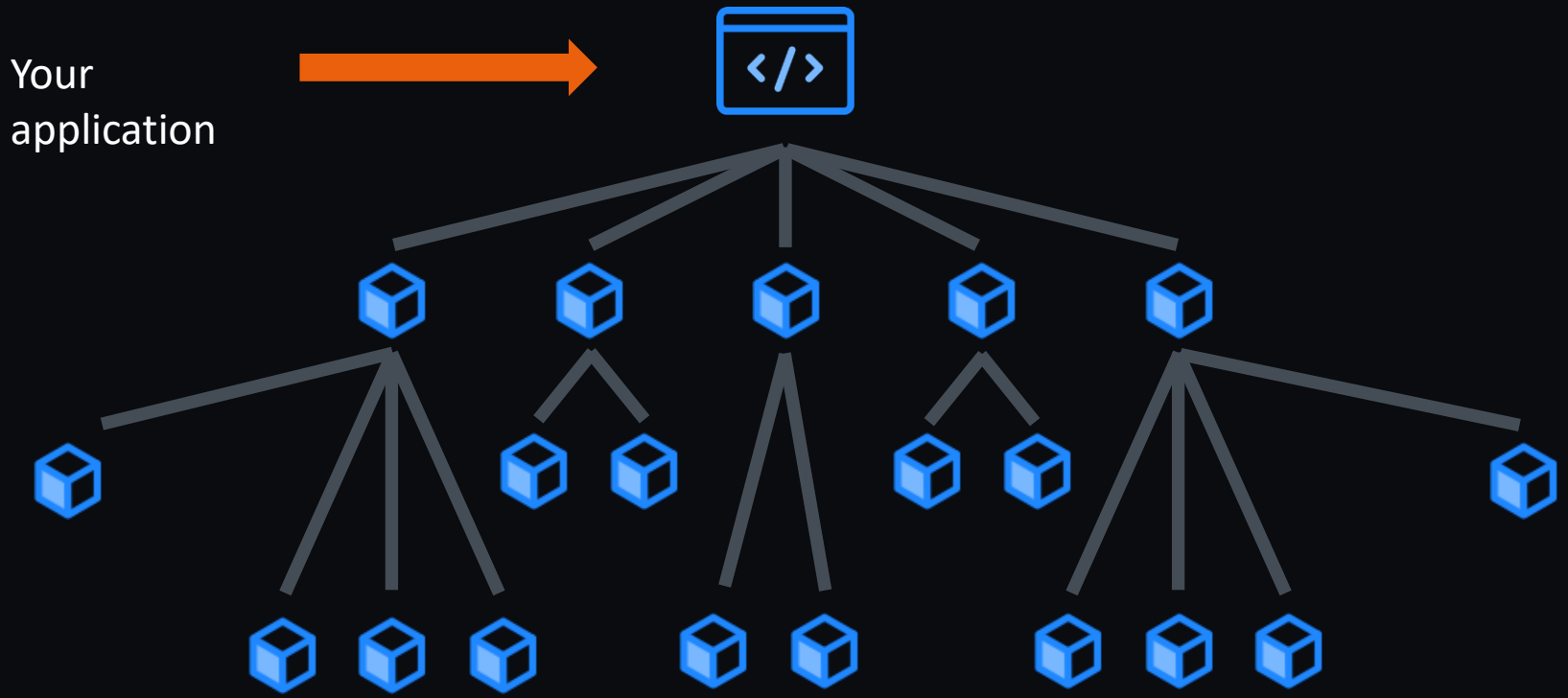
https://www.sisainfosec.com/weekly-threat-watch/12-8-million-auth-secrets-leaked-by-github-users-in-2023/

80-90% of all code in distributed applications is Open Source

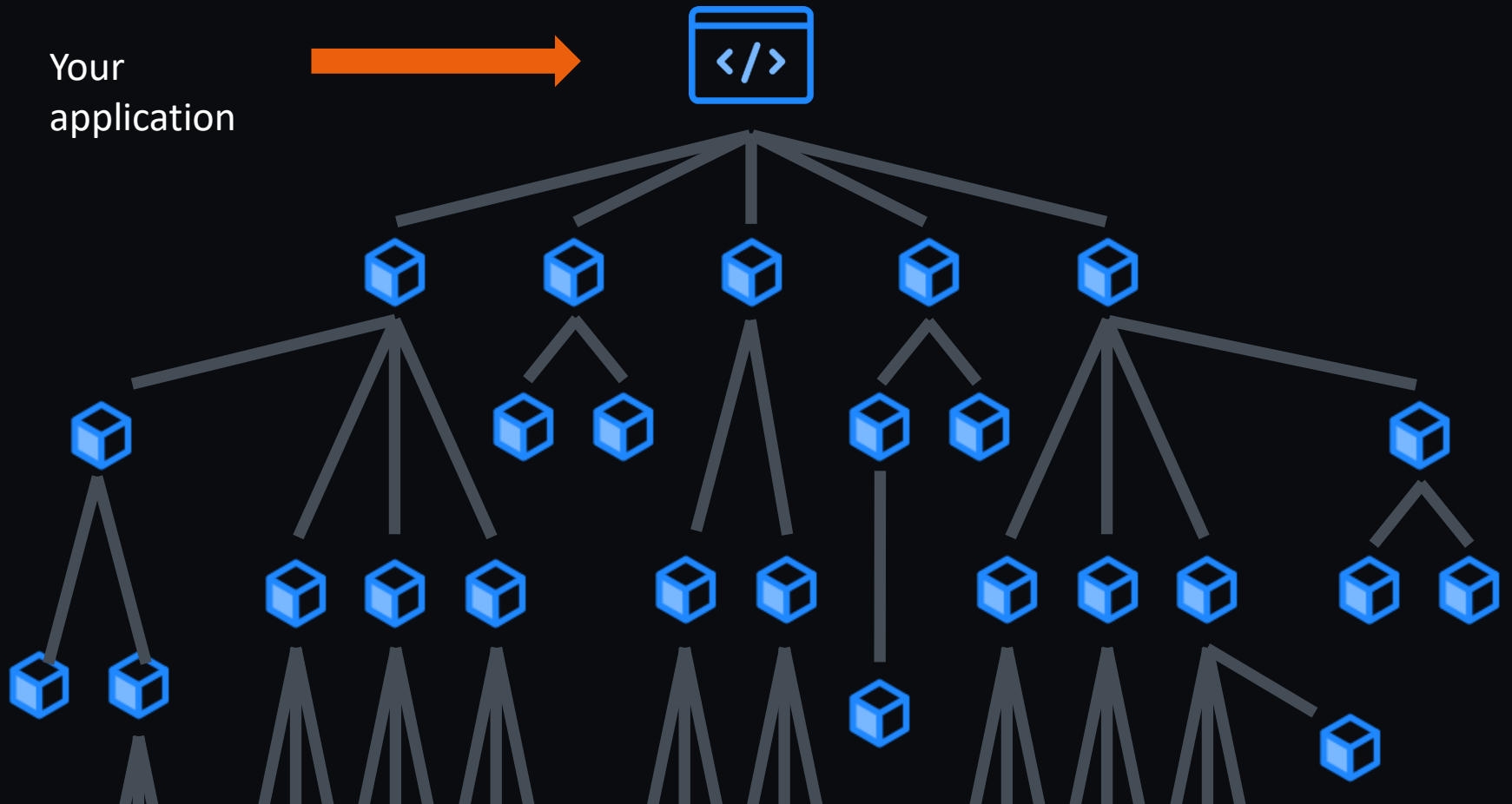
Your application

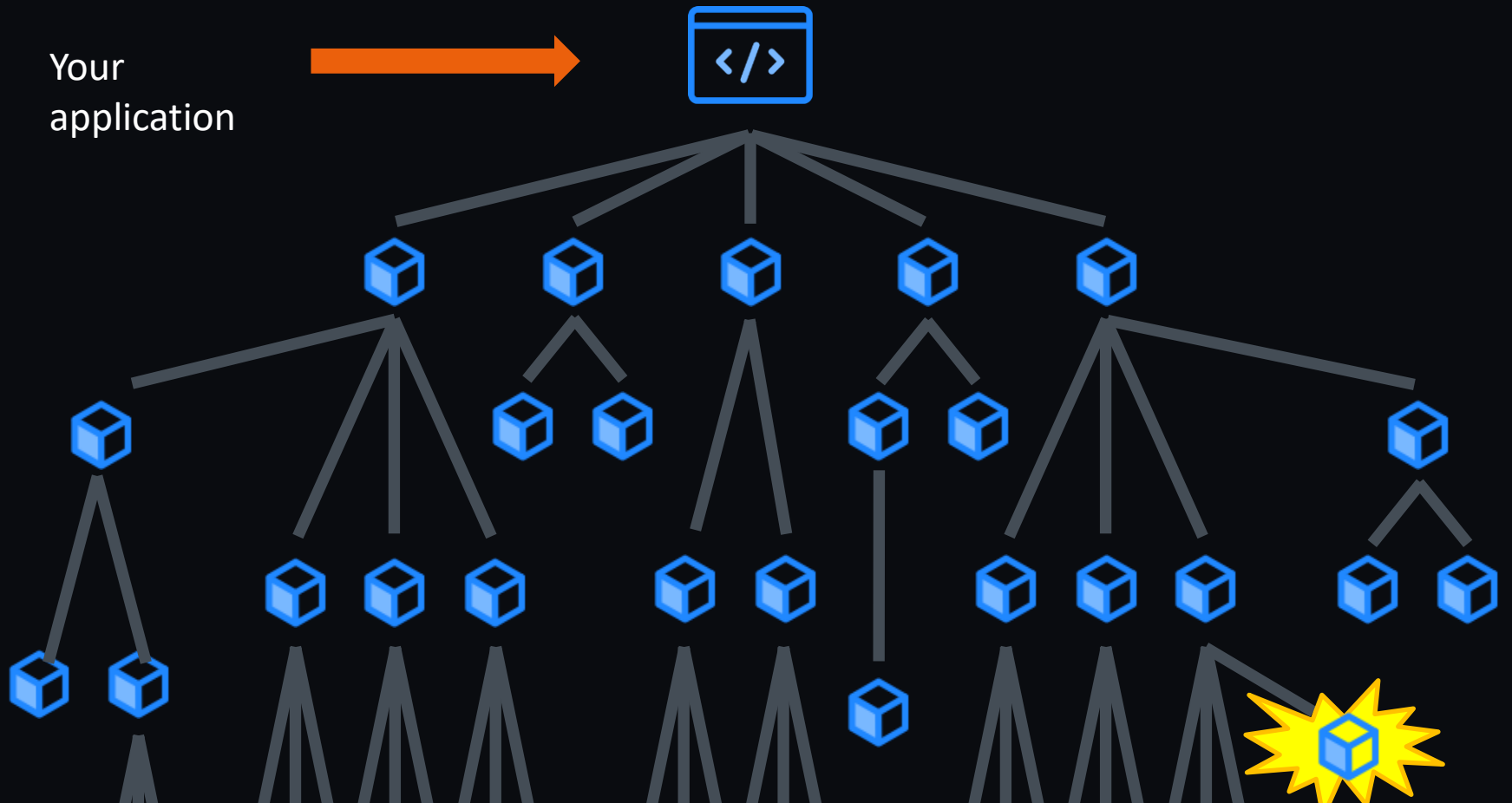


Dependency Chain starts with Top-Level Dependencies



Supply Chain of Dependencies


Your
application


Your
application


180+ days
Mean time to remediate (MTTR)
Industry norm

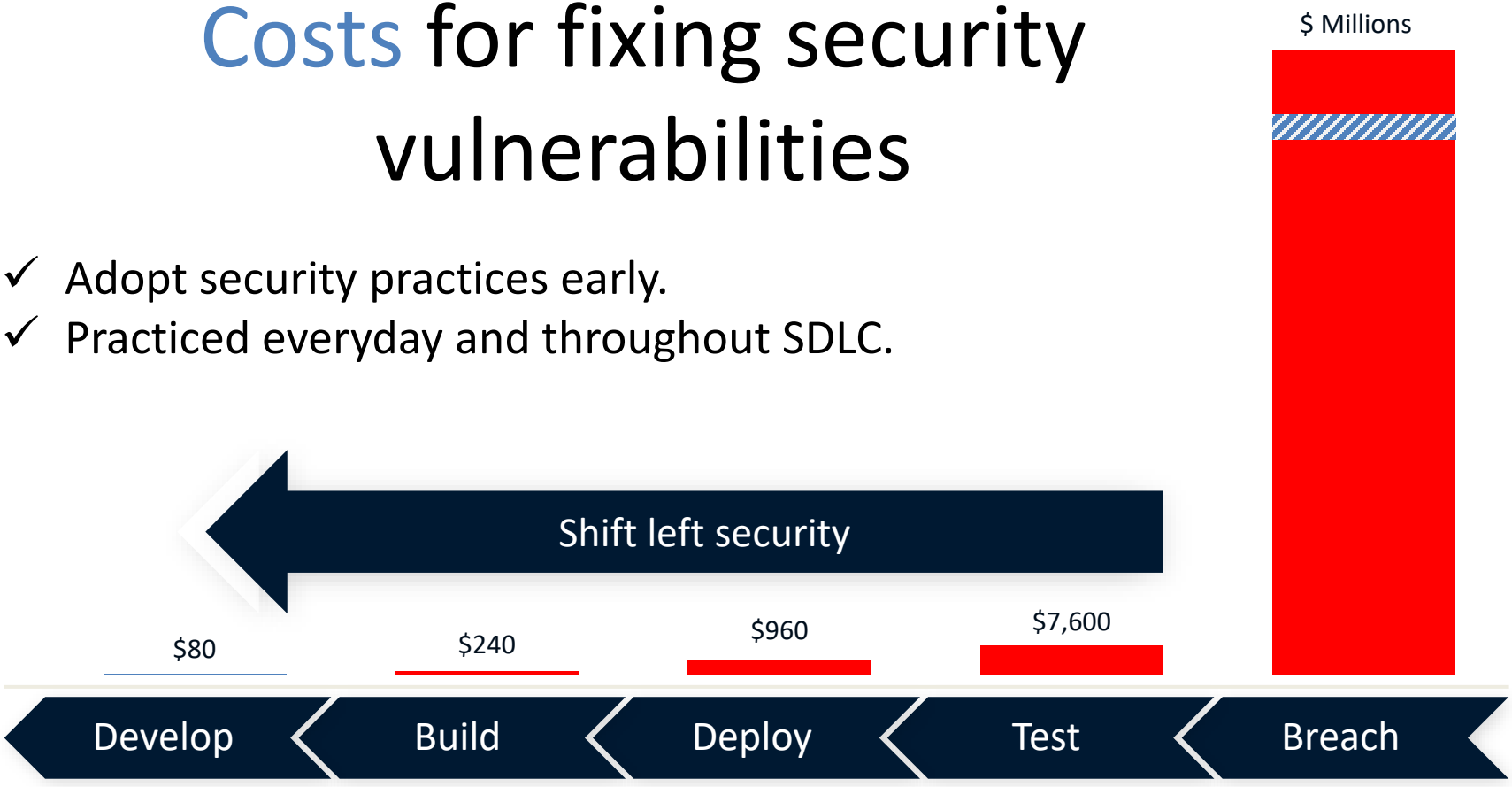

Mistakes Happen
Some of those become a security risk!

GitHub Advanced Security

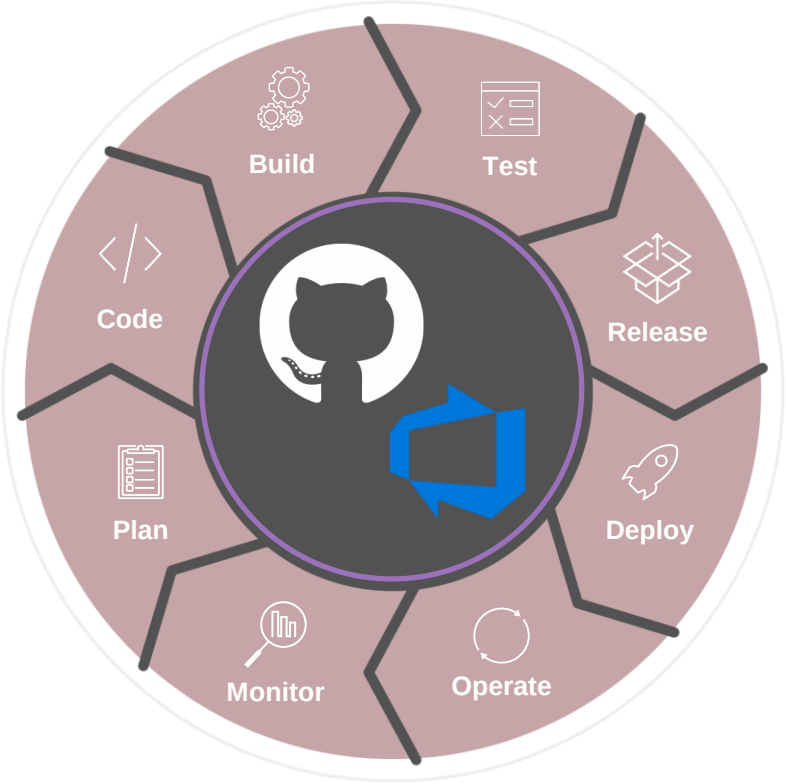
GitHub believes that making this shift requires a developer-first approach to all their security products

Costs for fixing security vulnerabilities

- ✓ Adopt security practices early.
- ✓ Practiced everyday and throughout SDLC.

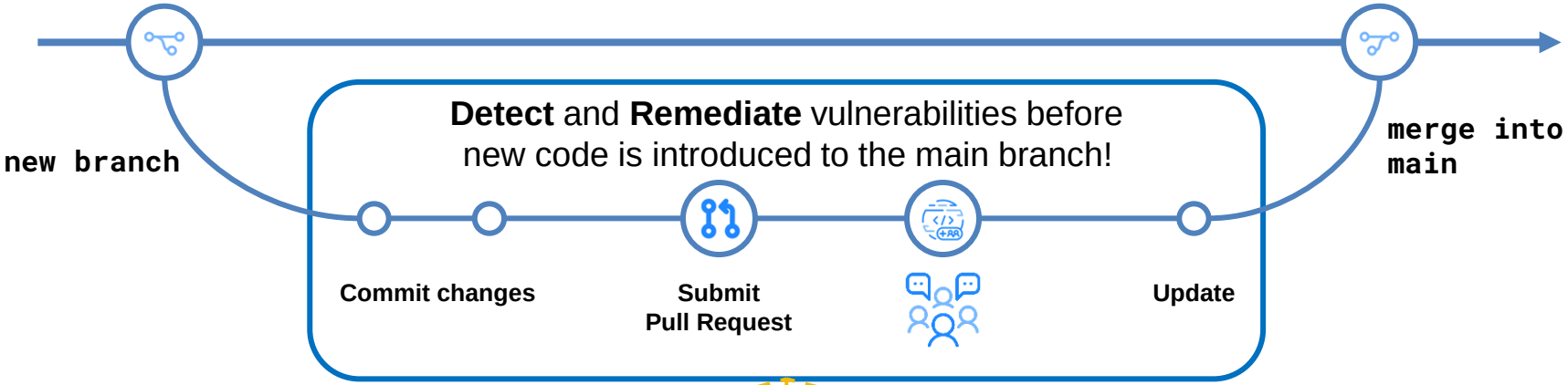


Security Built into the GHAS Developer Lifecycle



Xebia | Microsoft Services

Developer First Security – Shift Left



Dependency Scanning and Dependabot: automatic CVE identification & remediation

GHAS

Secret Scanning: locate and invalidate exposed tokens.

- **Push Protection**: prevent unauthorized changes

GHAS

CodeQL for Code Scanning: find & warn about risky patterns in code

Auto-Fix: AI (Copilot) during PR's covers 90% of alert types

GitHub Advanced Security

Dependency scanning

Know your dependencies

Secret scanning

Find API tokens or other secrets exposed anywhere in your git history or issues / pull requests

Push Protection will Proactively protect against leaked secrets in your repositories

Code scanning

Static analysis of every git push, integrated into the developer workflow and powered by CodeQL

Licensing

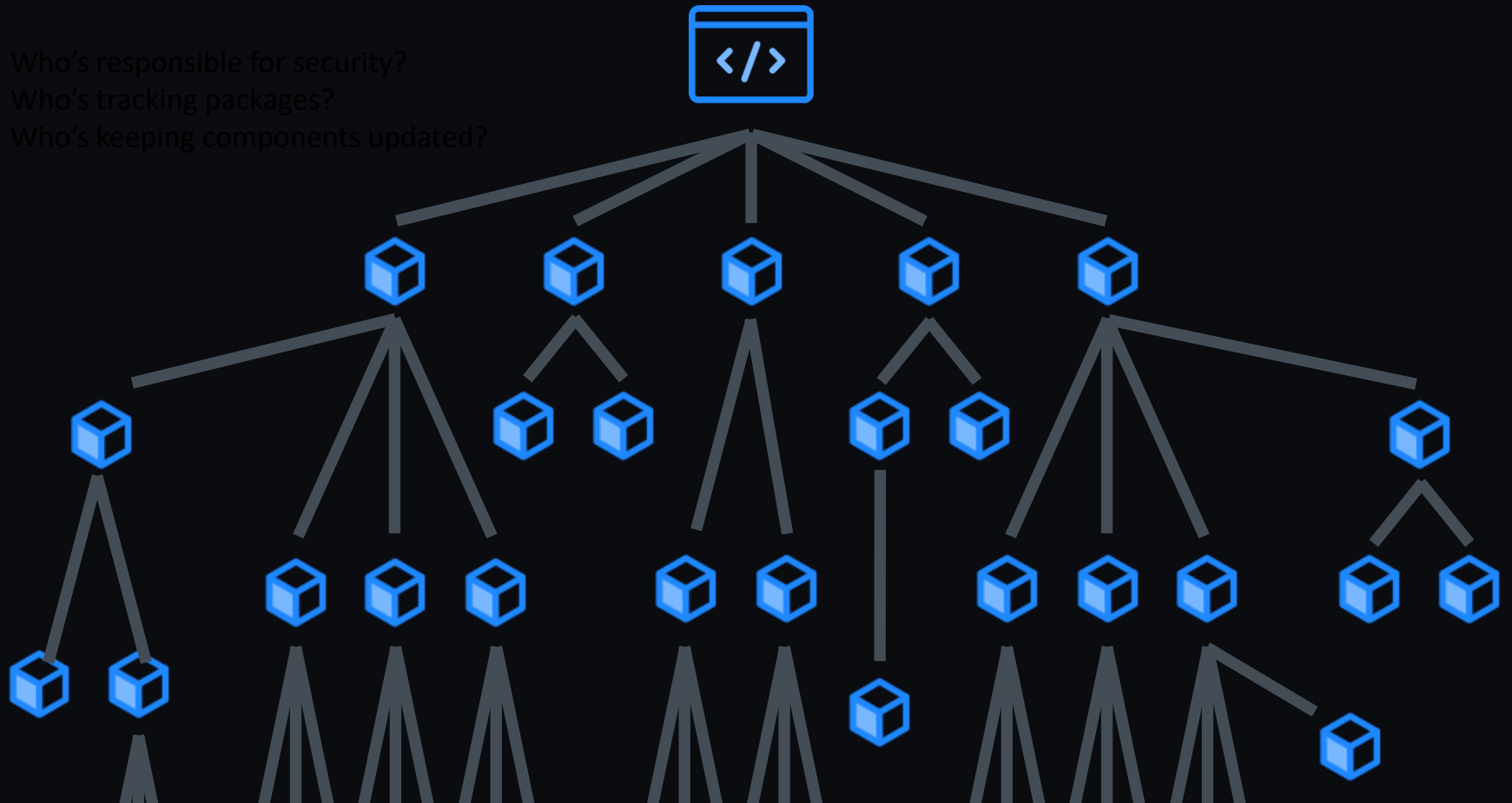
GitHub: Public Repos are Free / $49 for Private Repos

ADO: Additional license - $49 / contributor / month

- Contributor = active committer in the last 90 days
- Deduplicated on the Organization level
- Metered billing through your Azure Subscription
- Pro-rated on a daily basis

Securing your Supply Chain

Who's responsible for security?
Who's tracking packages?
Who's keeping components updated?




Setup +
Dependency
Scanning
Demo

GitHub Advanced Security

Dependency scanning

Know your dependencies

Secret scanning

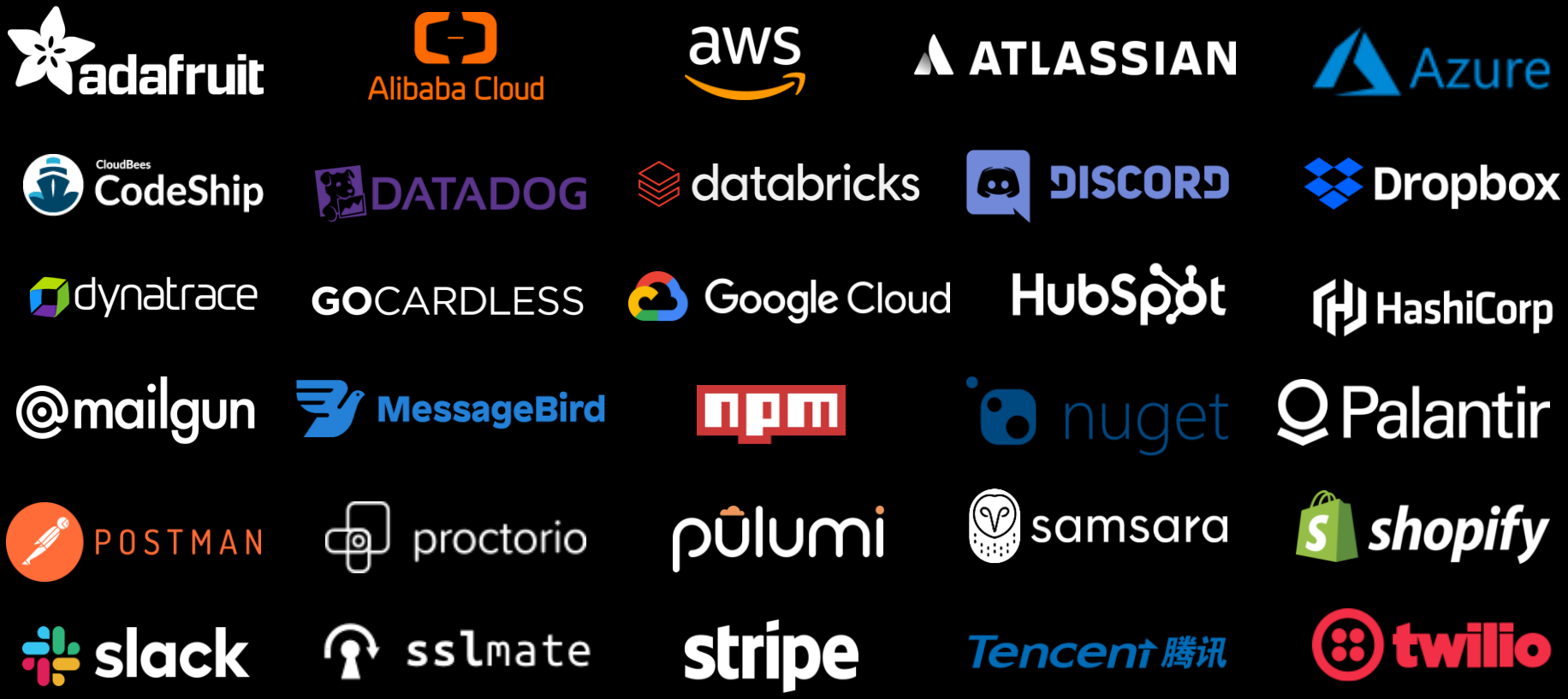
Find API tokens or other secrets exposed anywhere in your git history or issues / pull requests

Push Protection will Proactively protect against leaked secrets in your repositories

Code scanning

Static analysis of every git push, integrated into the developer workflow and powered by CodeQL

Secret Scanning Partners (120+)



Secret Scanning Demo

GitHub Advanced Security

Dependency scanning

Know your dependencies

Secret scanning

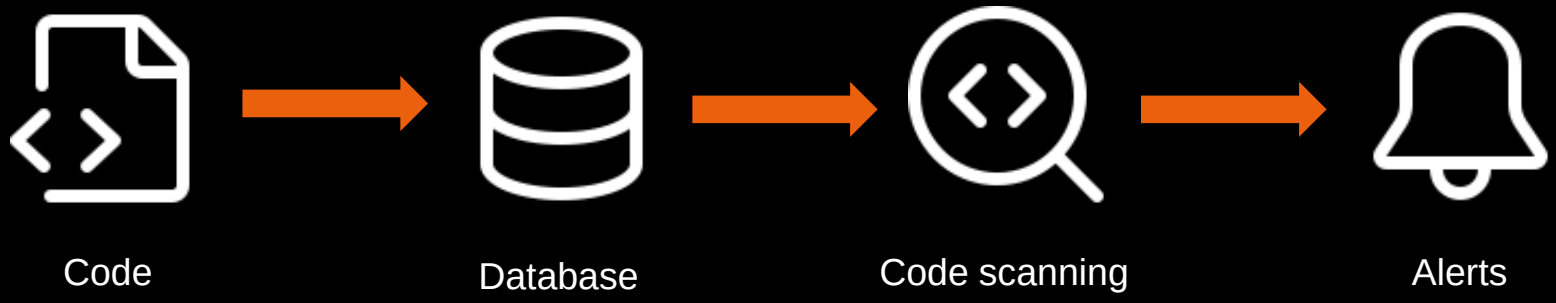
Find API tokens or other secrets exposed anywhere in your git history or issues / pull requests

Push Protection will Proactively protect against leaked secrets in your repositories

Code scanning

Static analysis of every git push, integrated into the developer workflow and powered by CodeQL

What is code scanning with CodeQL?



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

1,700+

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

72%

fix rate for potential vulnerabilities flagged in open source projects

15%

fix rate after 7 days

45%

fix rate after 90 days

24%

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

Code Scanning Demo

Similarities to GHAS

- Both have Secret Scanning
  - Get-clean (repo scanning)
  - Stay-clean (push protection)
- Same list of supported security partners
- Both have CodeQL
- Both are tightly integrated, native features in their respective platforms
- ADO bills at $49 per active committer per month (pro-rated)
- GHAS free for public repos

Differences to GHAS

- GHAS is always first
- Missing functionality on GHAzDo:
  - Numbers on alerts
  - PR blocking / Annotations not there yet
  - Dependabot PR’s (on roadmap no ETA)
  - No Security Overview. (Use DevOps extension by Rob Bos)
  - No pipeline failure on errors
- GitHub is more engineer centered (alerts)
- GHAzDo pushes overview to Defender for DevOps
- Custom secret scanning pattern
- Dependency graph visualization
- Custom CodeQL queries (ETA is early CY2024)

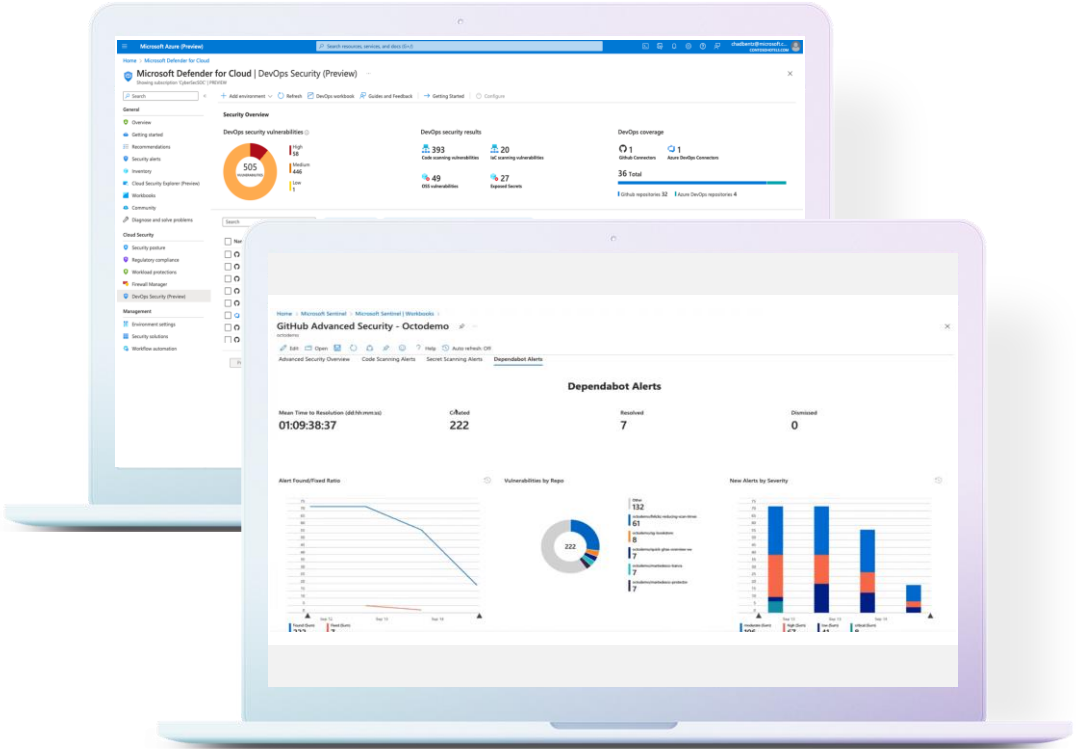
Defender for DevOps and Azure Sentinel

Defender for DevOps

Empower security teams with unified DevOps security management across multi-pipeline and multi-cloud environments, with unified visibility into DevOps security posture and strengthened cloud resource configurations.

Azure Sentinel

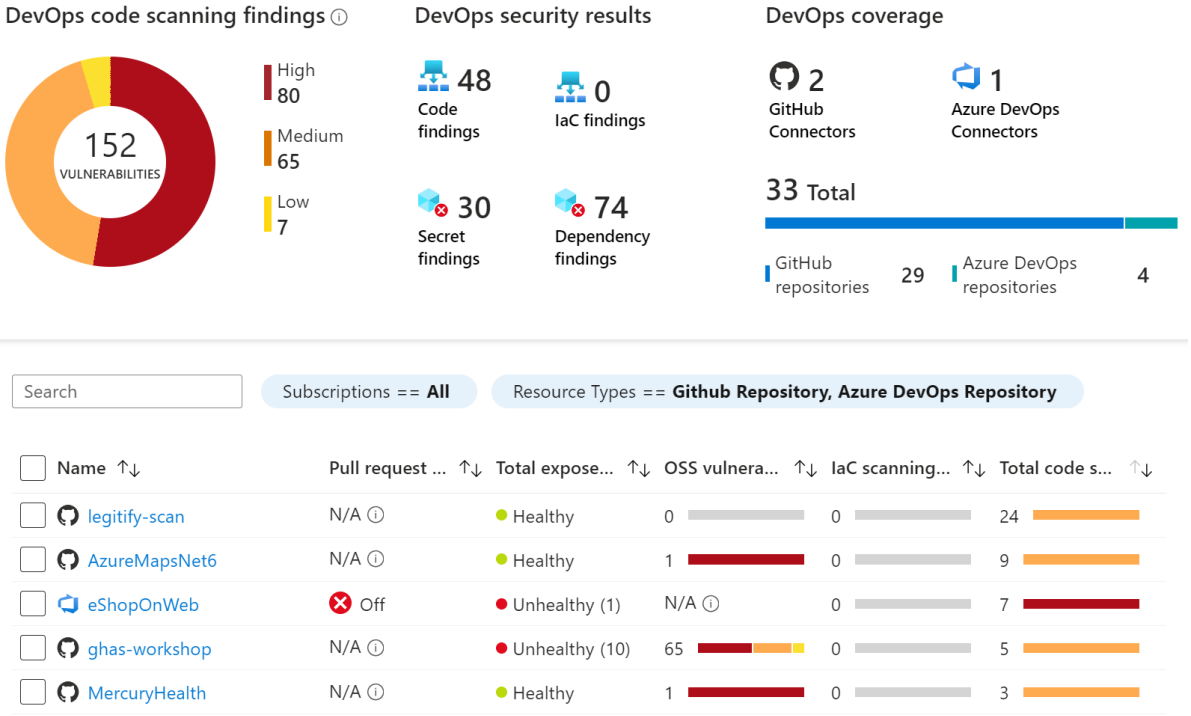
Aggregate your data and monitor your ecosystem, while detecting and monitoring threats. Automate and integrate security intelligence and enrich your detection and investigation with AI.



Microsoft Defender for Cloud

DevOps Security - Insights across multi-pipeline environments to prioritize remediation and apply security guardrails

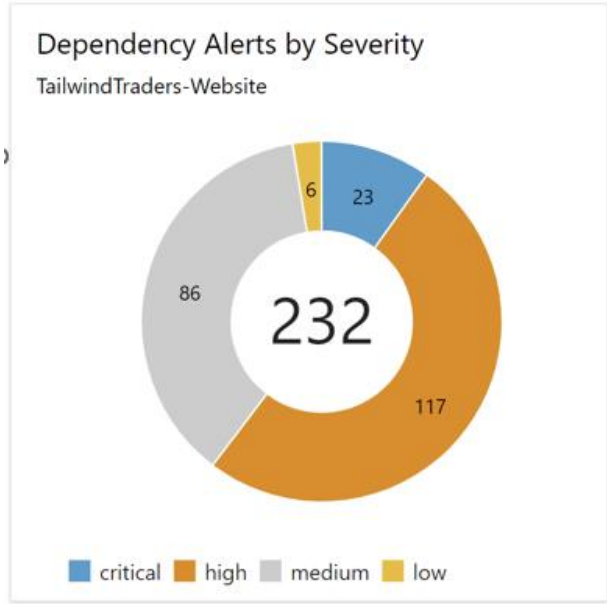
- Strengthen configuration of cloud resources throughout SDLC
- Provide unified, end-to-end visibility across departments
- Prioritize remediation of critical code issues using actionable feedback

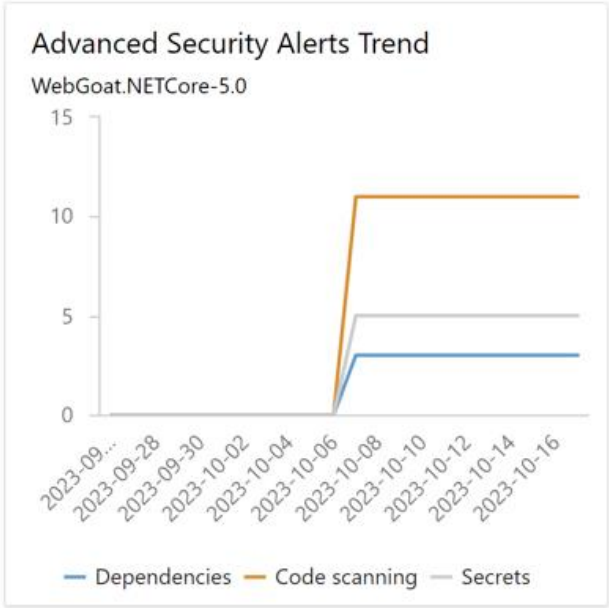


https://www.microsoft.com/security/business/cloud-security/microsoft-defender-devops & https://mslearn.cloudguides.com/guides/Unify DevOps security management with Microsoft Defender for Cloud

Advanced Security dashboard Widgets

Marketplace: https://marketplace.visualstudio.com/items?itemName=RobBos.GHAzDoWidget
Repo: https://github.com/rajbos/ghazDo-widget/






Defender for
DevOps
Demo

Resources

Slide Deck: https://github.com/PagelsR/Talks

Secure at every step
https://resources.github.com/learn/pathways/security

Blog Post on GHAzDO
GitHub Advanced Security for ADO

GitHub Advisory Database
https://github.com/advisories

Code Scanning
https://codeql.github.com/

GHAS dashboard widgets for GHAzDO
https://marketplace.visualstudio.com/items?itemName=RobBos.GHAzDoWidget

Xebia | Microsoft Services

Thank you!

Randy Pagels
DevOps Architect | Trainer
Randy.Pagels@Xebia.com

PagelsR

Randy-Pagels