

Compliance-Kosten in den Griff bekommen

Entwickler glücklich
und produktiv machen

» Continuous Lifecycle «



13.–14. November 2024, Continuous Lifecycle Conference, Mannheim
Schlomo Schapiro, Associate Partner / Principal Engineer, Tektit Consulting

 @schlomo@floss.social
 [@schlomoschapiro](https://twitter.com/schlomoschapiro)



The Golden Path to Golden State

How to Keep Developers Happy & Productive

» Continuous Lifecycle «



13.–14. November 2024, Continuous Lifecycle Conference, Mannheim
Schlomo Schapiro, Associate Partner / Principal Engineer, Tektit Consulting



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

What happened before...

©forto

The Role of GitOps In IT Strategy

The GitOps Journey to Hands-Off Operations

18.11.2021 | Schlomo Schapiro | Principal Engineer, Forto GmbH

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License (with the exception of the stock images with copyright notice)



All Mountain Photos: Schlomo Schapiro / CC-BY-SA

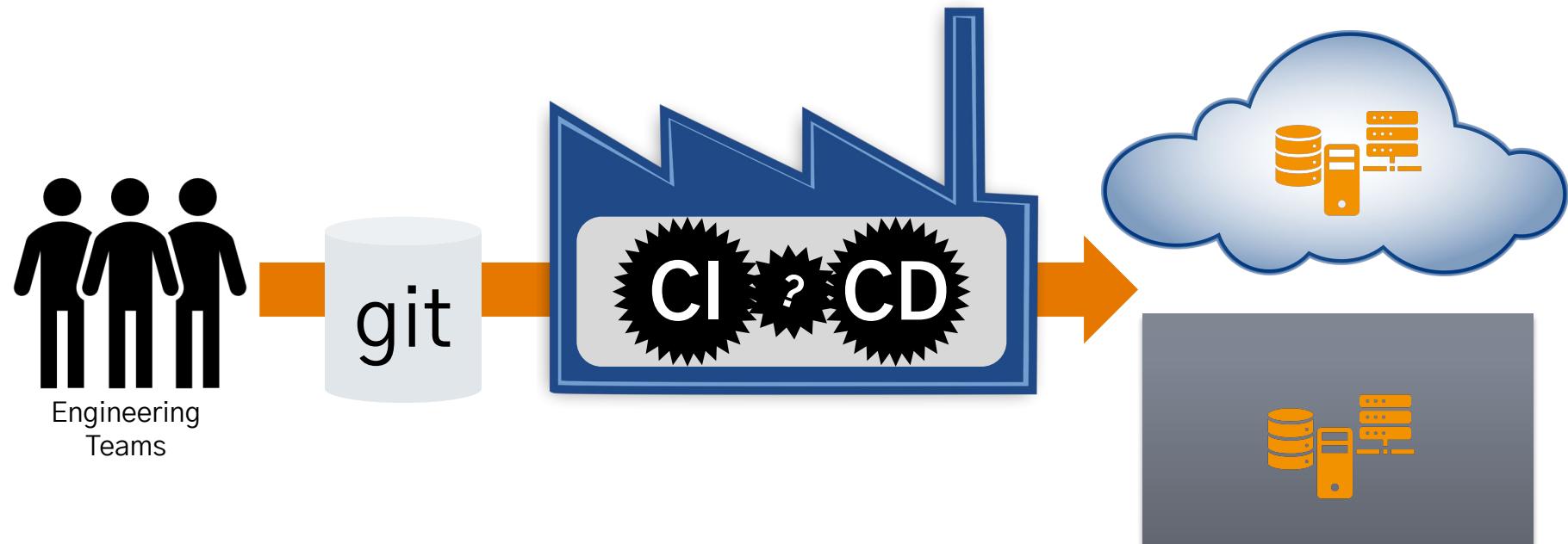
Schlomo Schapiro,
Continuous Lifecycle 2021
18.11.2021



Agenda

1. Context: DevOps
2. What is Compliance?
3. Why is it an **Expensive** Problem?
4. Total Cost of Compliance
5. Golden Path to Golden State
6. Developer Experience

Happy DevOps Campers



DevOps is

- ... if every person uses the same tool for the same job
- ... codified knowledge – everybody contributes his part to common automation
- ... if all people have the same privileges in their tooling
- ... if human error is equally possible for Dev and Ops
- ... replacing people interfaces by automated decisions and processes 

bit.ly/5devops

... a result

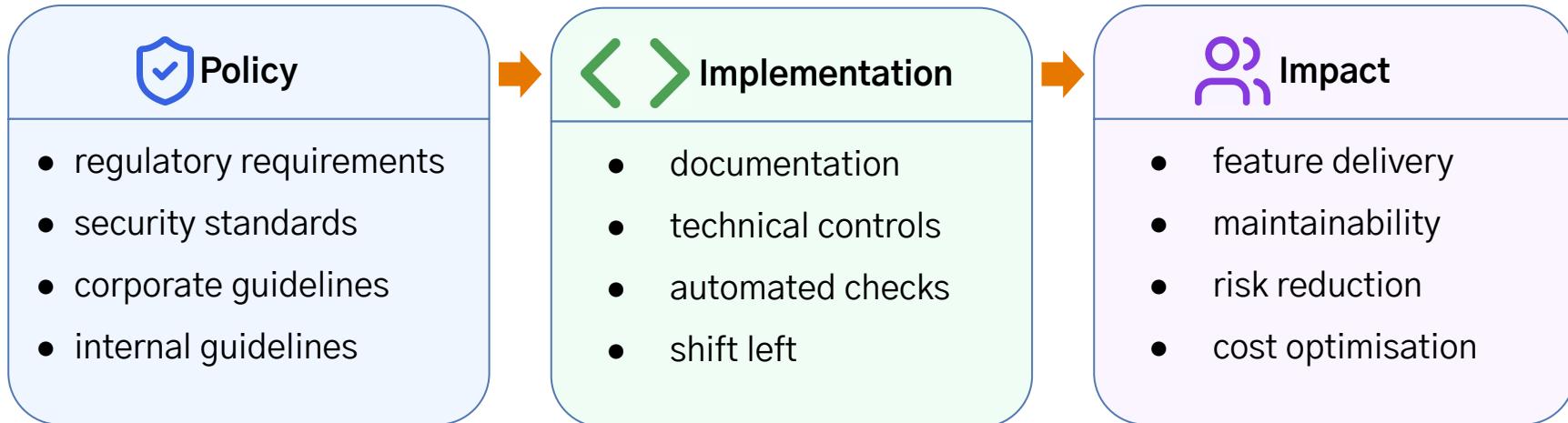
Compliance

Compliance: Where Policy Meets Practice

“The process and state of adhering to internal policies, industry standards, and regulatory requirements while developing and maintaining software systems. It encompasses both the technical implementation of security controls and the organizational processes to ensure these controls are consistently applied and documented.”



Compliance: Where Policy Meets Practice



Compliance is not just about following rules — it's about finding the **optimal balance** between security & regulatory requirements and development efficiency.

Compliance: A roadmap for success

The **process** and **state** of adhering to **internal policies, industry standards,**

Our work

Result

Write them!

IT-Grundschutz, CIS Controls, ISO27K1

and **regulatory requirements** while **developing** and **maintaining** software

KRITIS, NIS2, DORA, GDPR, BAIT ...

New from templates

Existing (the majority)

systems. It encompasses both the **technical implementation** of security

Think holistically end-end

Automate! Solve problems with code, not paper

controls and the organizational **processes** to ensure these controls are

Verify, not trust

Stick to the rules, lead by example

consistently applied and documented.

Everywhere the same!

Make your auditors happy



Cost of Compliance



How much did you pay for fixing those?

Vulnerability	Year	Affected Systems	CVSS	Global Cost Estimate
Spring4Shell CVE-2022-22965	2022	Widespread Spring Framework	9.8	?
Log4Shell CVE-2021-44228	2021	Widespread Java ecosystem	10.0	\$90B+ estimated (Allianz Risk Barometer 2022)
WannaCry MS17-010	2017	230,000+ systems Windows SMB	8.1	\$4-8B estimated (Cyence Risk Analytics)
Shellshock CVE-2014-6271	2014	Widespread Unix/Linux Bash	10.0	\$2.1B estimated (Bloomberg Government analysis)
Heartbleed CVE-2014-0160	2014	17% of HTTPS servers, OpenSSL	7.5	\$500M+ for certificates (Ponemon Institute)

Example: Java

Version	Release Date	End of Life	Paid Support EOL	Migration Considerations
Java 21 (LTS)	Sept 2023	Sept 2028	Sept 2031	Current LTS version
Java 17 (LTS)	Sept 2021	Sept 2026	Sept 2029	Most common upgrade target from Java 8/11
Java 11 (LTS)	Sept 2018	Sept 2023	Sept 2026	Still widely used in enterprise
Java 8 (LTS)	March 2014	Jan 2019	Dec 2030	Most deployed version in enterprises
Java 7	July 2011	April 2015	July 2022	End of Extended Support, critical to upgrade

Example: Java - How much does it cost to upgrade?

- **Large Enterprise** (10,000+ Apps):

"Average cost of \$2.3M for Java 8 to 11 migration"

Source: Forrester Research, 2021 survey of Fortune 500 companies

- **Medium Enterprise:**

"\$300K–\$800K per major version upgrade"

Source: IDC Technology Spotlight, 2022

- **Java 7 to 8 Migration:**

"Average of \$2.2M for large enterprises (>1000 apps)"

Source: Oracle Customer Survey, 2016

- **OpenLogic Survey 2023:**

"37% of organizations reported spending >\$100K on Java upgrades"

Source: OpenLogic State of Open Source Report 2023

Example: OWASP DevSecOps Guideline - v-0.2

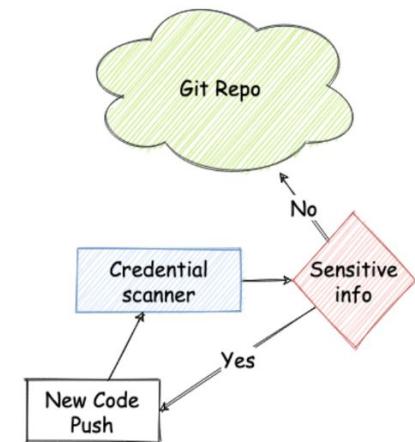
[Home](#) > [Latest](#)

Take care secrets and credentials in repositories

How can you ensure that sensitive information are not pushed to a repository?

This is one of the [OWASP Top Ten issues](#) and several bug bounties write-ups are related to this kind of issue, eg hard-coded credentials pushed by mistake.

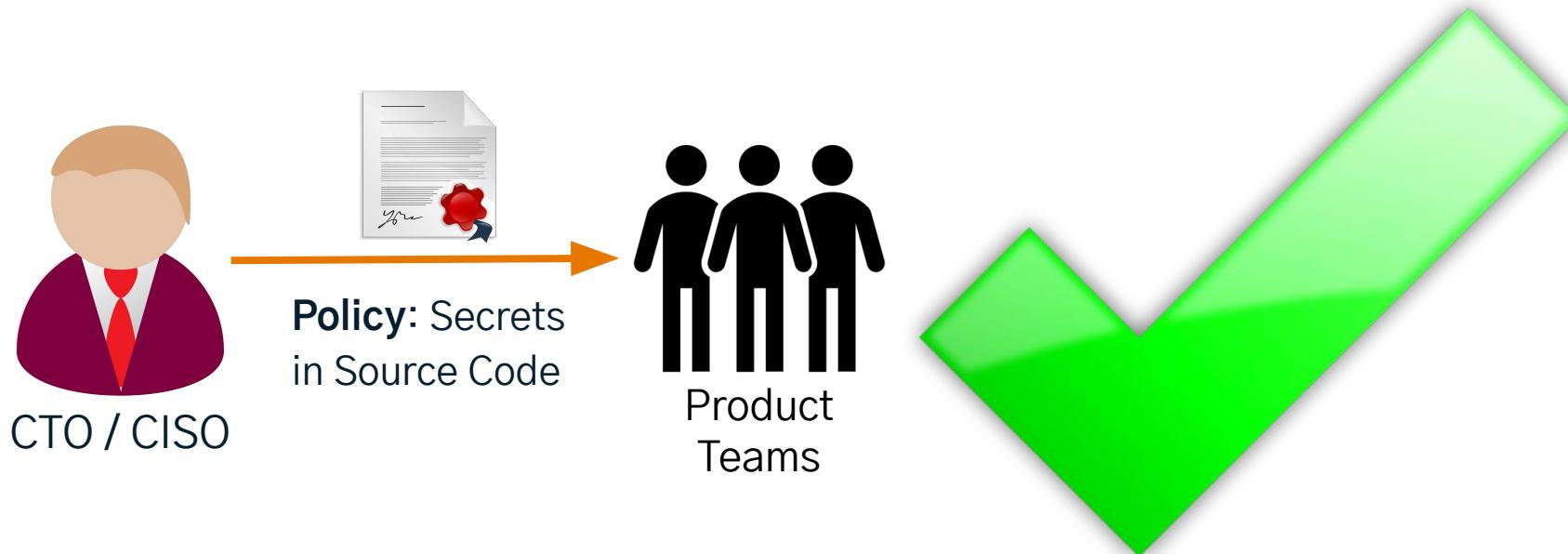
You should scan your commits and your repository, and detect any sensitive information such as password, secret key, confidential, etc. following the process shown in the picture.



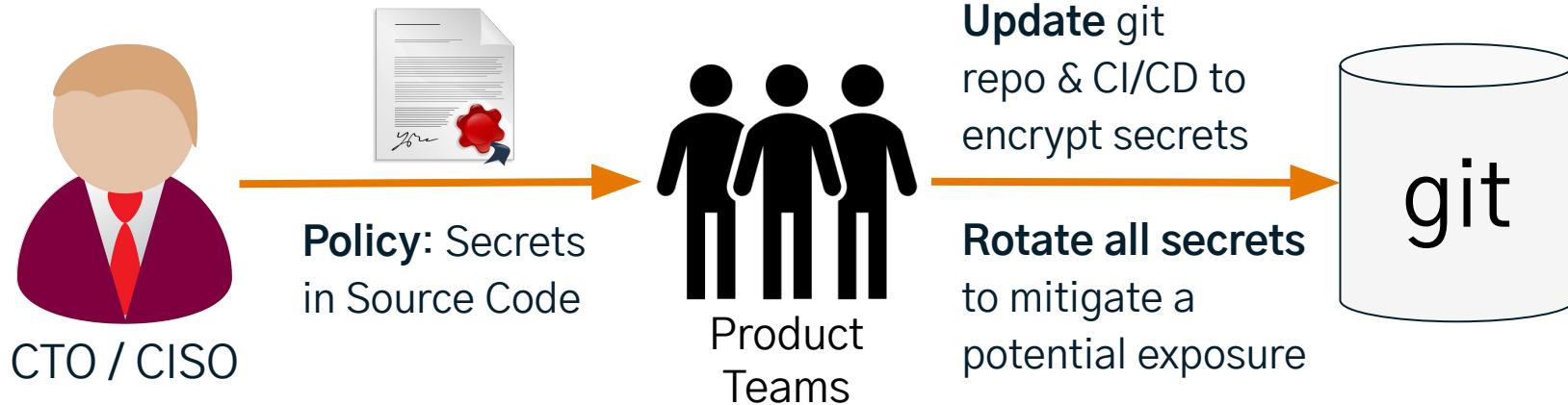
Example: Securing Secrets in Source Repositories

- Status Quo: Git repos contain unencrypted credentials or other secrets
- Risk: Lost or exploited developer laptop leaks **all** operational secrets
 - Impact: Traumatic, credentials allow stealing/changing all data and harming operations
 - Probability: High, developers have admin access on their laptops, go to conferences and all the time try out software downloaded from the Internet
 - **Risk Level / Prio: Very High**
- Evidence:
 - Every year 1 developer laptops is somehow lost
 - Malicious software scanner on developer laptops disabled due to too many false positives
- **Goal: Mitigate risk via ensuring that all secrets in repos are encrypted**

CISO Perspective on Securing Secrets

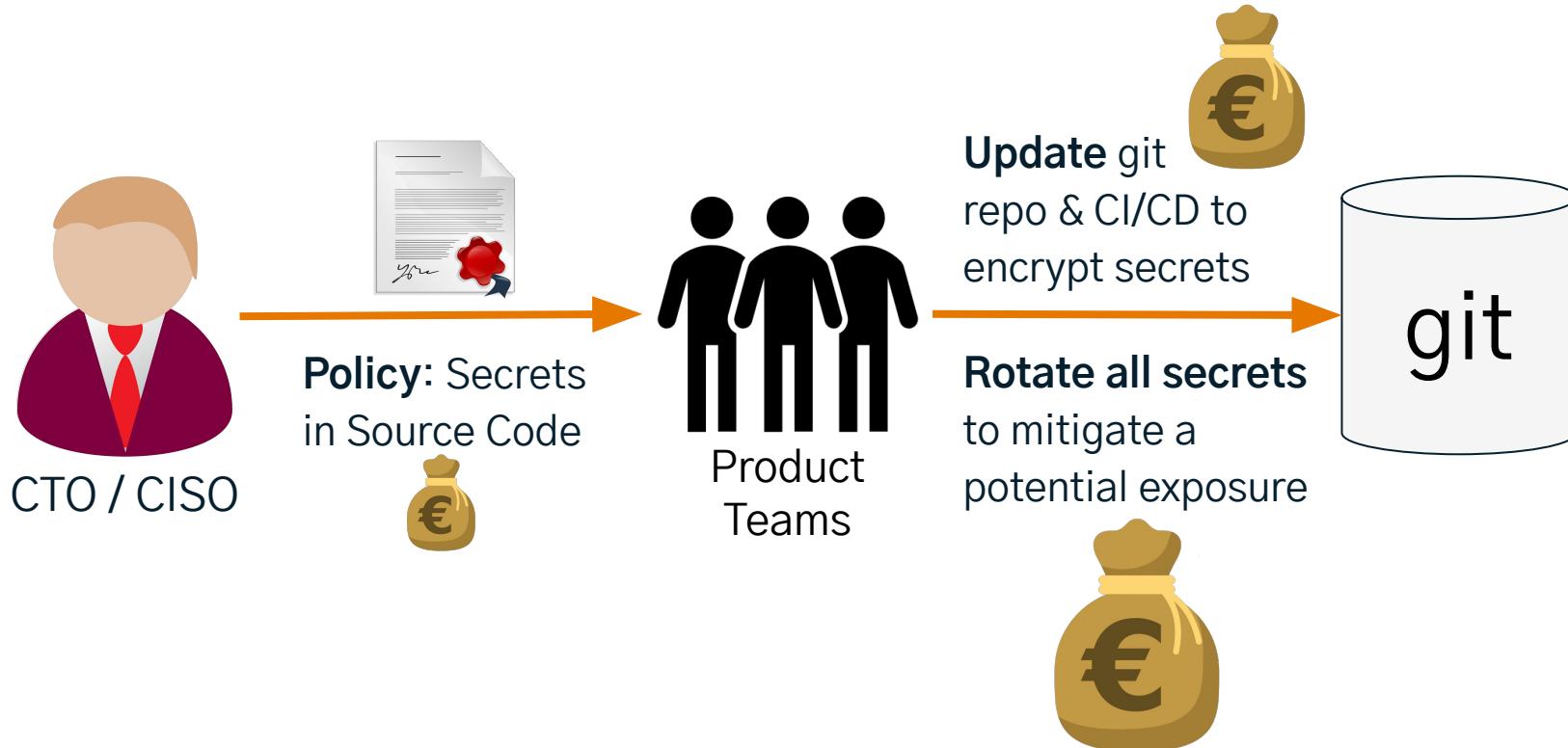


Developer Team Perspective on Securing Secrets

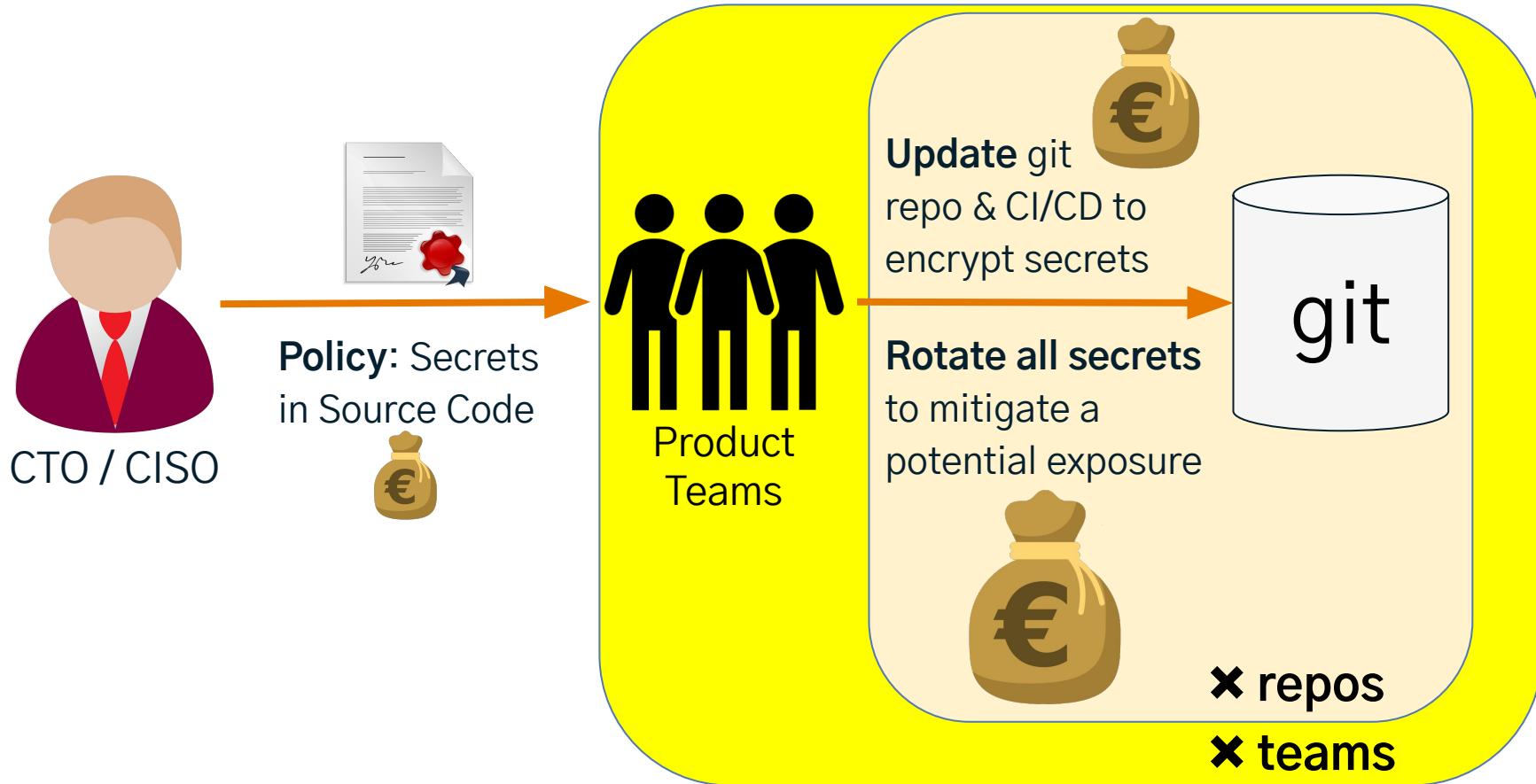


How much does this cost?

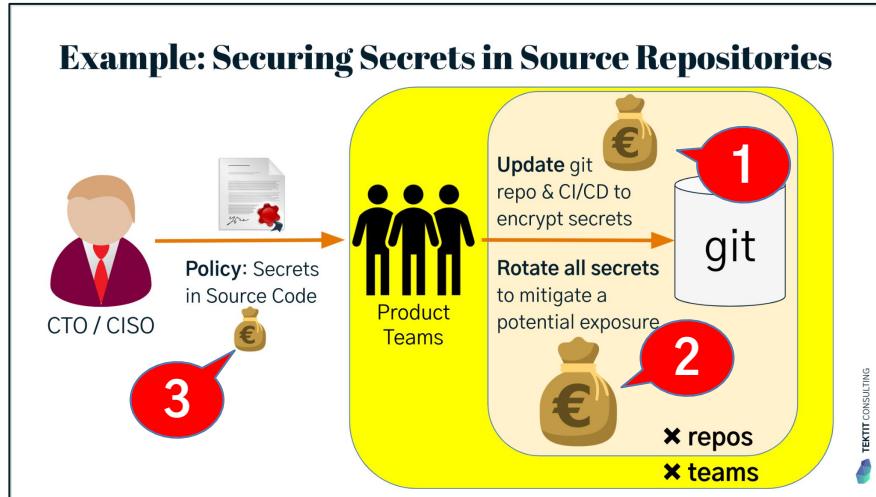
Example: Securing Secrets in Source Repositories



Costs of Securing Secrets in Source Repositories



Total Cost of “Secrets in Source Code” Compliance



PD = Person-Day

Assumptions (average)

- 10 repos per team
- 10 teams in company

Effort (estimated on average)

- 3 PD CISO writing policy
- (1 PD CISO support per team)
- (3 PD per team per repo)
- (31 PD per team incl. support)
- 310 PD for all 10 teams
- **313 PDs in total**

What about continuous prevention?

Did you warn Product about the reduced feature delivery capacity?



Secrets Management: Let Tektit help with that 😊

@forto

Cloud & Offline Secrets Management

Managing operational secrets with SOPS

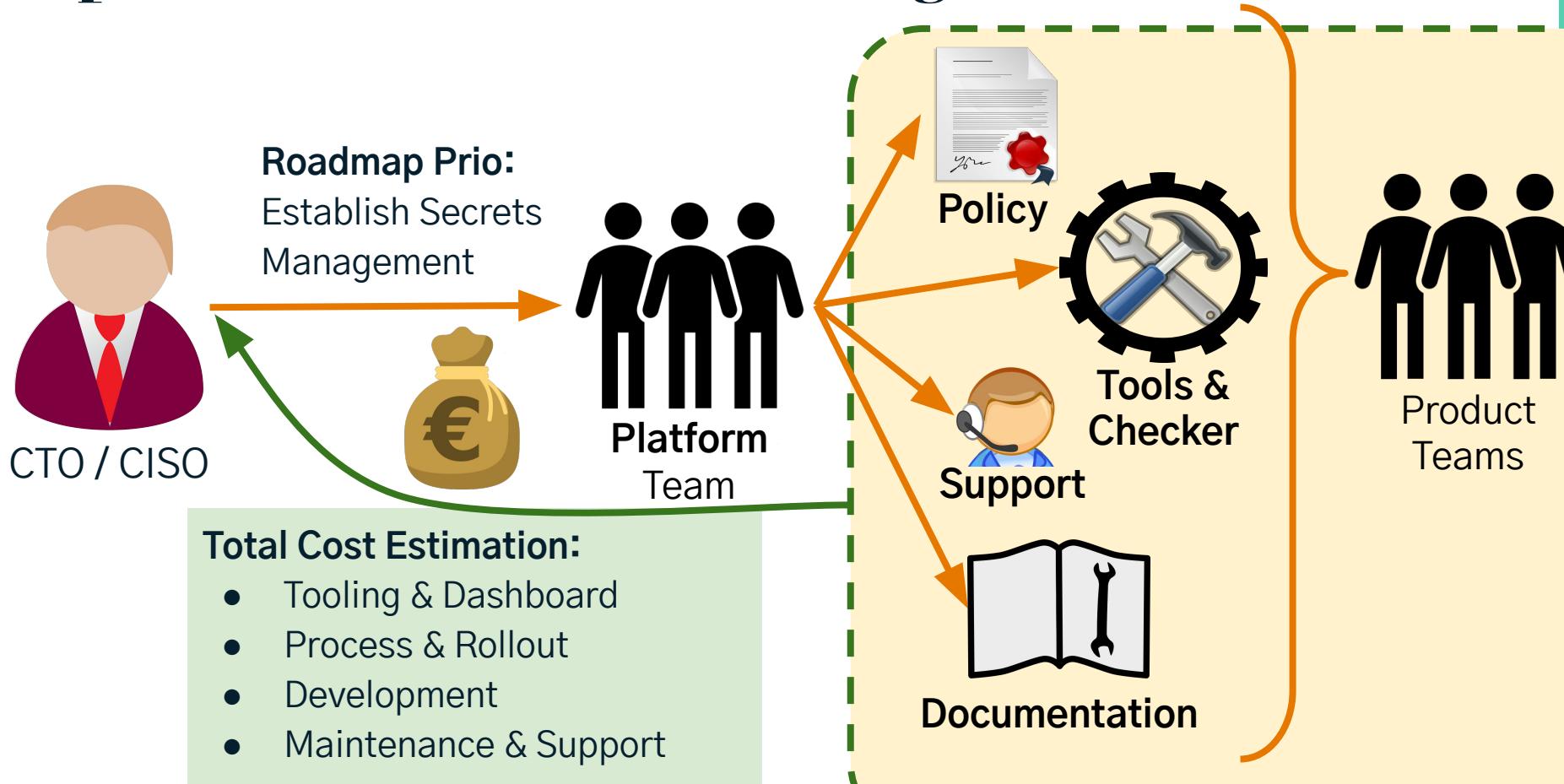
15./16. November 2023, Continuous Lifecycle Conference, Mannheim
Schlomo Schapiro, Principal Engineer, Forto GmbH



This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

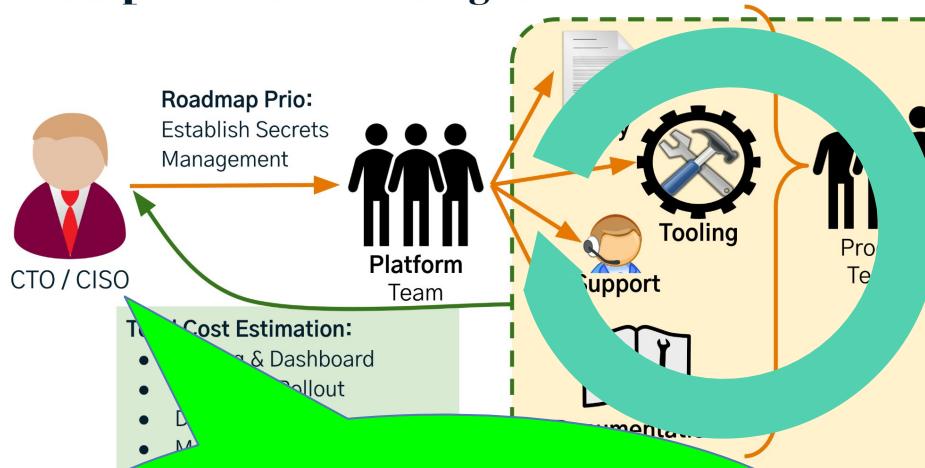


Optimize Total Cost of Securing Secrets in Sources



Benefits for “Total Cost” of Compliance

Example: Total Cost Management



Platform Team:

- End – 2 – end ownership
- Optimize for long term instead of short term, for entire company
- Care about Developer Experience and Developer Happiness
- **“Compliance by Default”**

Stakeholders

- Balance total cost vs. risk mitigation
- Enable holistic company-wide perspective



The Golden Path to the Golden State



Golden State:



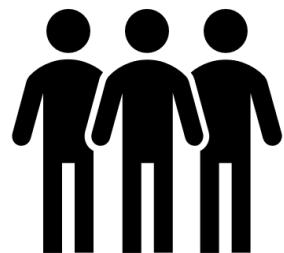
Everything secure, compliant and up-to-date

- Spotless audits
- Comply with all security, compliance & company policies
- Complete documentation
- Software is maintainable
- Developers spend 99% of their time on features
- Developer happiness is 100%
- ...

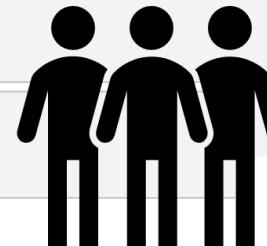
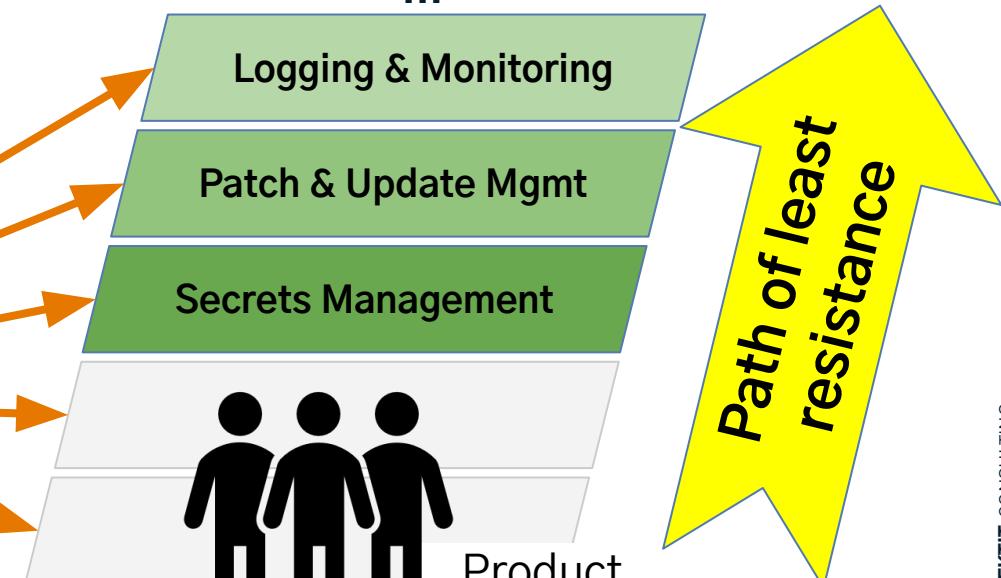
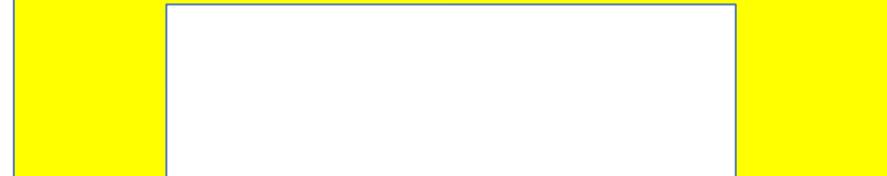
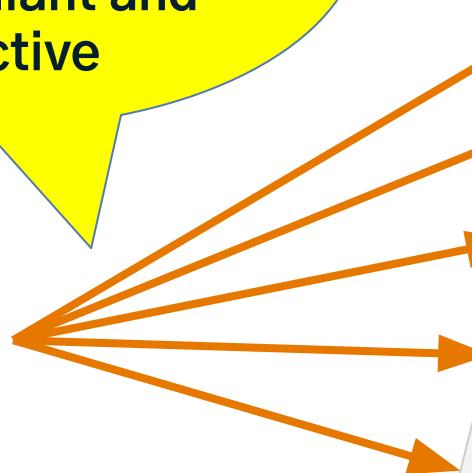
Golden Path

to

Golden State



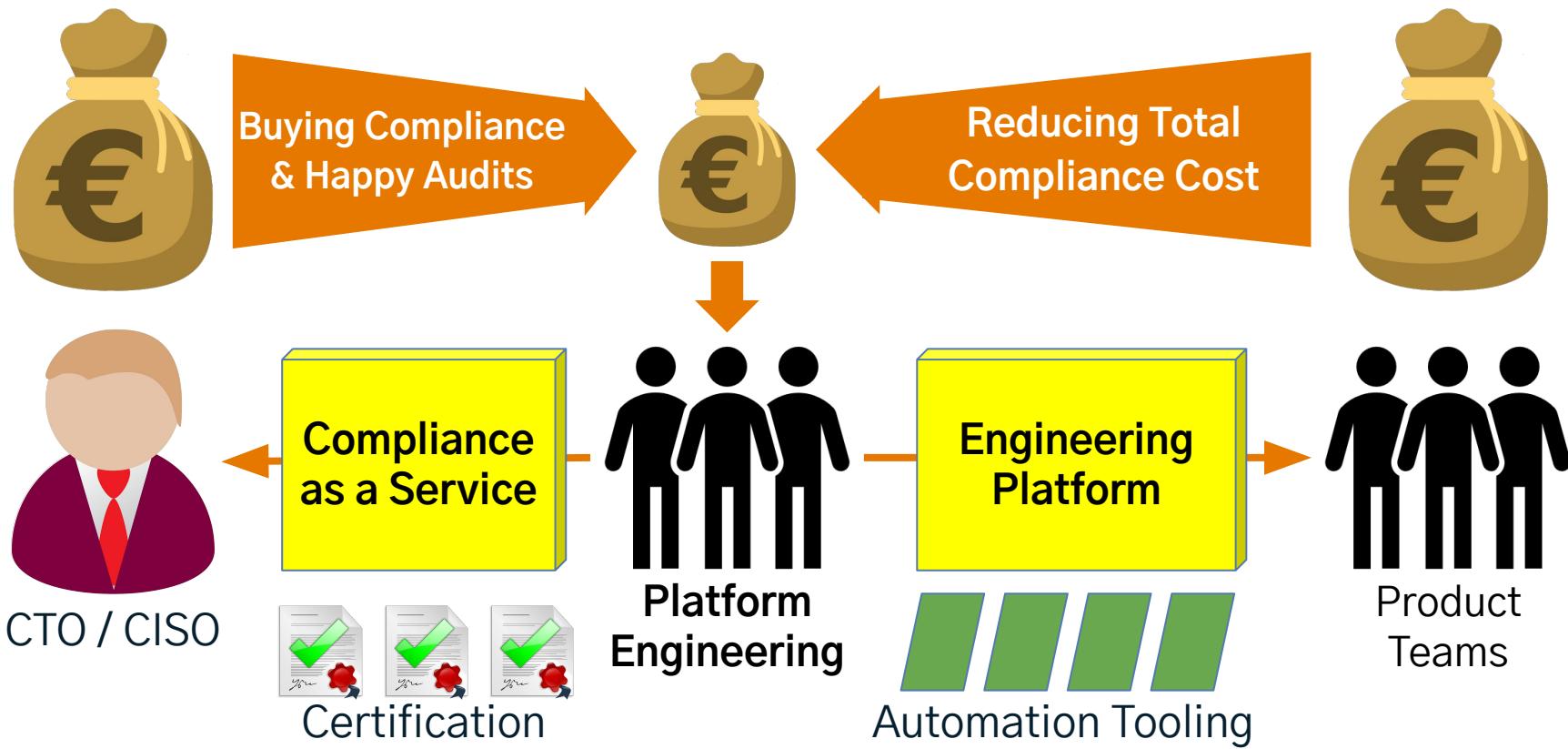
Platform
Engineering



Product
Teams



Internal Economics to Fund Platform Engineering



How does this work in practice?

Quick Recap: The Role of GitOps in IT Strategy



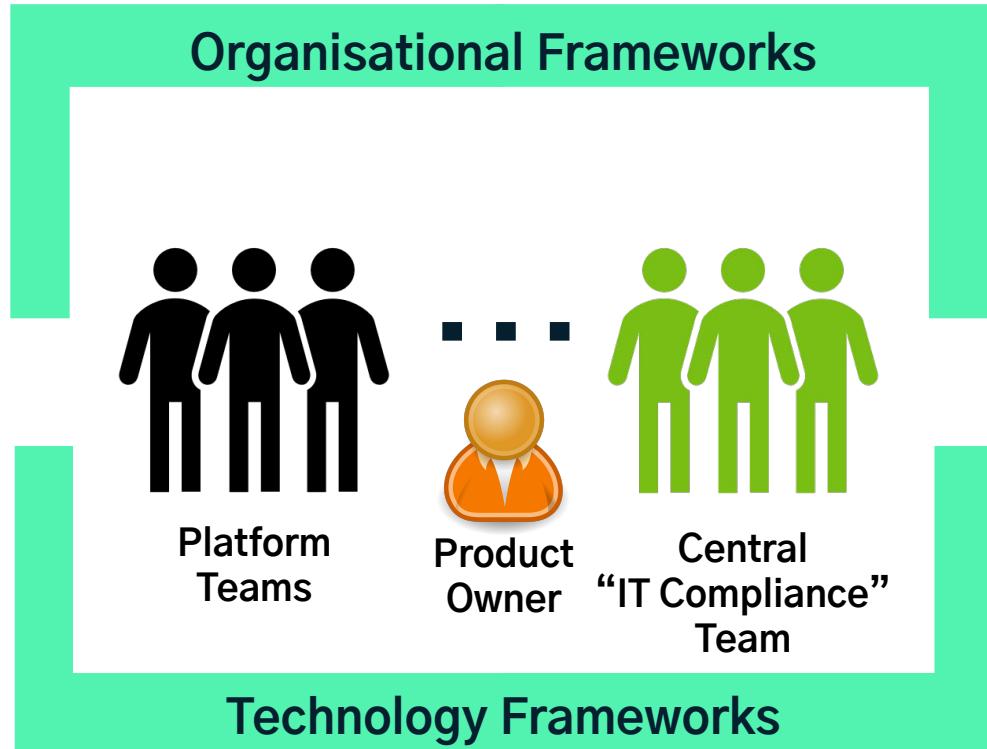
schlomo.schapiro.org



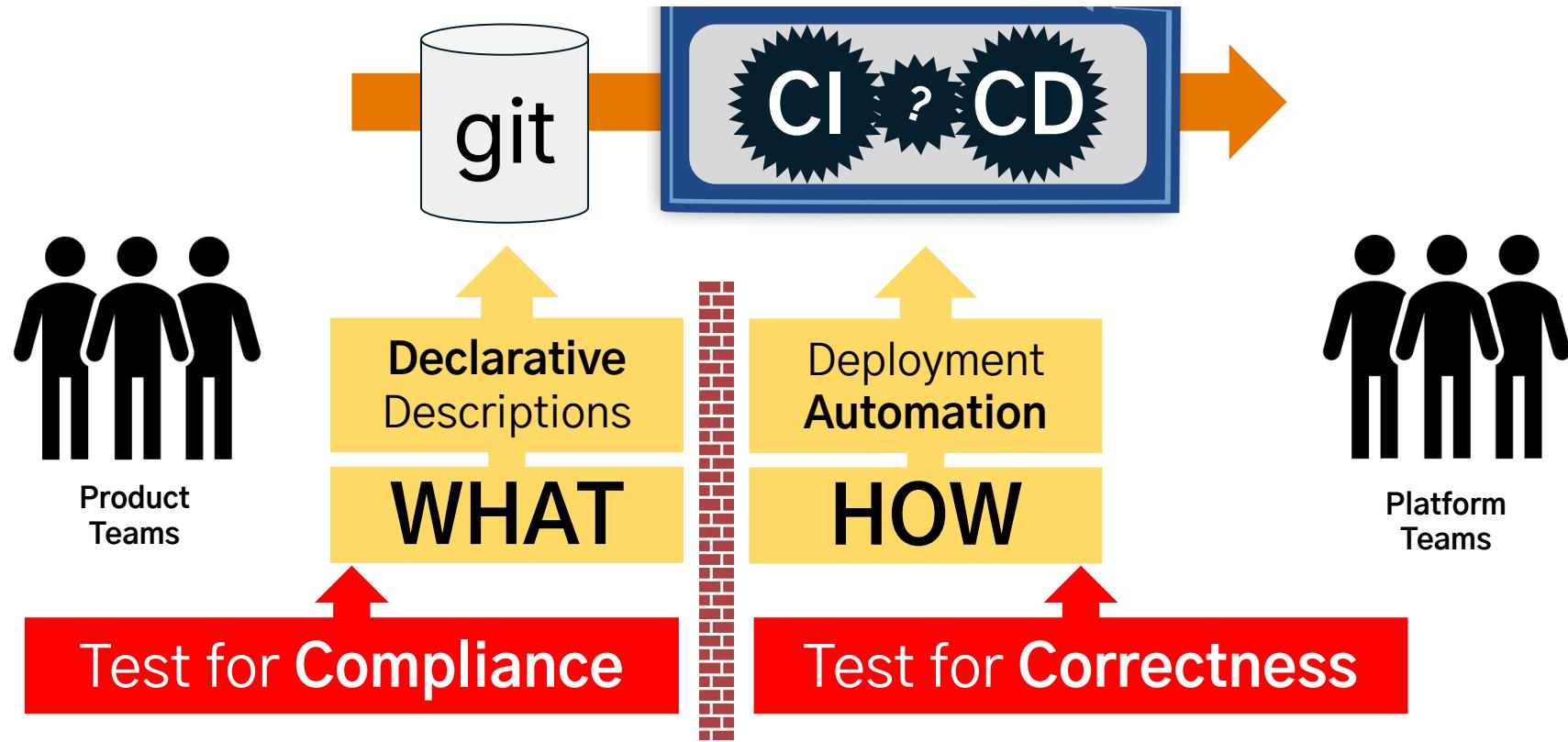
Platform & Compliance Engineering Org

Mission: Compliant-by-Default IT platforms

- Create & maintain standardized tooling for common IT tasks
- Tools are user friendly, integrate automated compliance checks
- Educate & coach teams in tool usage & best practices
- Cost center
- Main KPIs:
 - Productivity of product engineering teams
 - Balancing IT compliance risks and costs



GitOps to the Rescue



Fixing the basics is really hard → Hands-Off Ops

- No manual changes in production
- Dev & Ops have same permissions in production: None by Default
- Automate the **hard** stuff:
 - Compliance & governance
 - Distributed rolling upgrades
 - Consistent Backup & Disaster Recovery
 - Everything in your stack
- Test Driven Everything
- Standardized Tooling
- Remove static credentials
- **Fix the Basics!**



GitOps

The Role of
GitOps in IT
Strategy v2

Schlomo Schapiro, 21.09.2022, DevOpsDays 2022



schlomo.schapiro.org

Developer Happiness #1

1. Treat developers as valued customers
2. Talk with developers, chat over ☕
3. Check frustrating tasks, e.g. internal bureaucracy, forms to fill in, reports ...
4. Ask agile coaches and scrum masters
5. Ask also their managers
6. Surveys, but not too often
7. Ask developers which technical metrics would correlate with their happiness
8. ...



Developer Happiness #2



Deployment Frequency — How often an organization successfully releases to production

Lead Time for Changes — The amount of time it takes a commit to get into production

Change Failure Rate — The percentage of deployments causing a failure in production

Time to Restore Service — How long it takes an organization to recover from a failure in production

The Golden Path to Golden State

*Use the
Total Cost of Compliance
to introduce
Platform Engineering
and make your
Developers HAPPY!*

Q&A — How may I help you?



schlomo.schapiro.org

*We are not consultants. We are Partners, Coaches, Humans, Enablers, Catalysts, Sparring Partners, Experts
... and sometimes a little annoying.*

I focus on **IT strategy**, IT governance, technology and architecture management, security and compliance automation, related organisational changes, business continuity, open source and cloud technologies – and I'm available as a Principal Engineer or Technical Product Owner for short-term / interim support.

Examples:

- **Business-IT alignment & leveraging**, developing required skills and abilities for 21st century IT, leverage AI
- **SaaS compliance & governance**, data possession vs. ownership, IAM, integrations, backup & DR, shadow IT
- **Compliance Automation**, finding the “golden path” to a “golden state” via **Platform Engineering**
- **Secrets Management** for Datacenter, Cloud Infrastructure, IaaS/PaaS/SaaS
- **Open Source**, from usage to contribution, writing policies, using SBOM, establishing Open Source Stewardship
- **Good Engineering Practices**, GitOps, test driven development, good architecture decisions, known tech strategy
- **Business Continuity and Disaster Recovery** for office, Cloud infrastructure, data center & SaaS, with quality assurance, emergency communication & collaboration, hot & cold standby, no-restore solution, ransomware protection, Linux Disaster Recovery / Bare Metal Restore with “Relax and Recover ([rear](#))” Open Source tooling

schlomo.schapiro@tektitconsulting.com

