RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **DSO-W02**

CI/CD: Top 10 Security Risks

Daniel Krivelevich
Co-Founder & CTO
Cider Security
@dkrivelev

Omer Gil
Head Of Research
Cider Security
@omer_gil

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

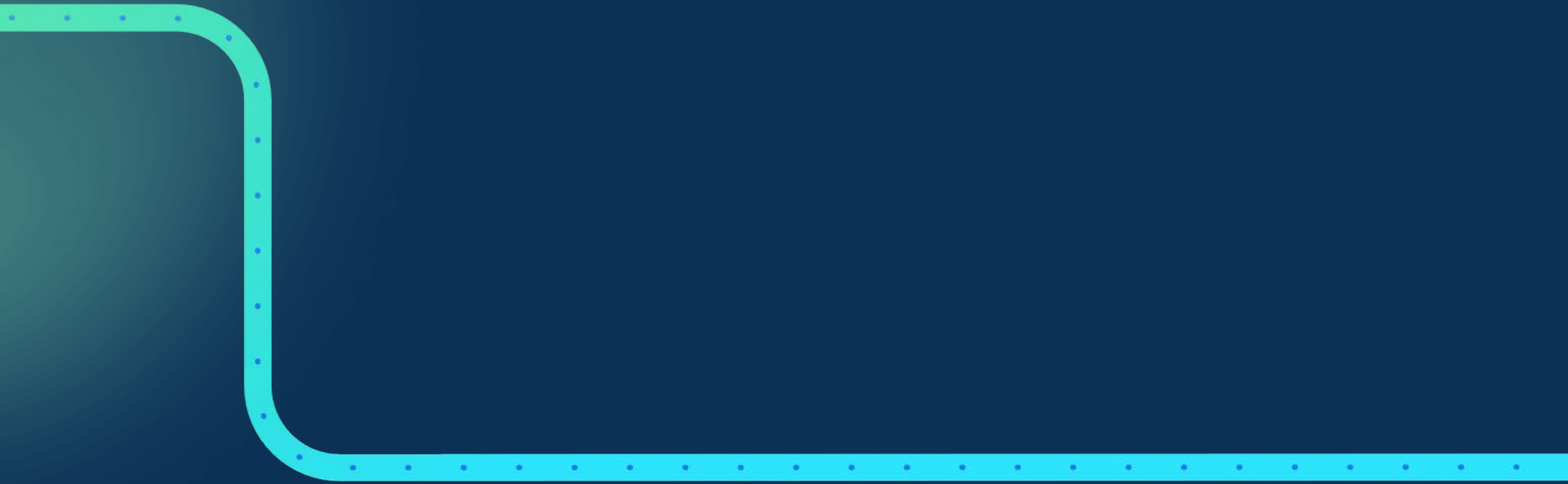
December 2020 – A Pivotal Moment

RSAConference2022

What we will talk about

1. What is CI/CD security?
2. “Top 10 CI/CD Security Risks” initiative
3. Analysis of breach anatomies
4. Takeaways

What is CI/CD security?



Cider

The engineering train **moves faster and faster...**

Shorter time to release

Larger diversity in tech stack

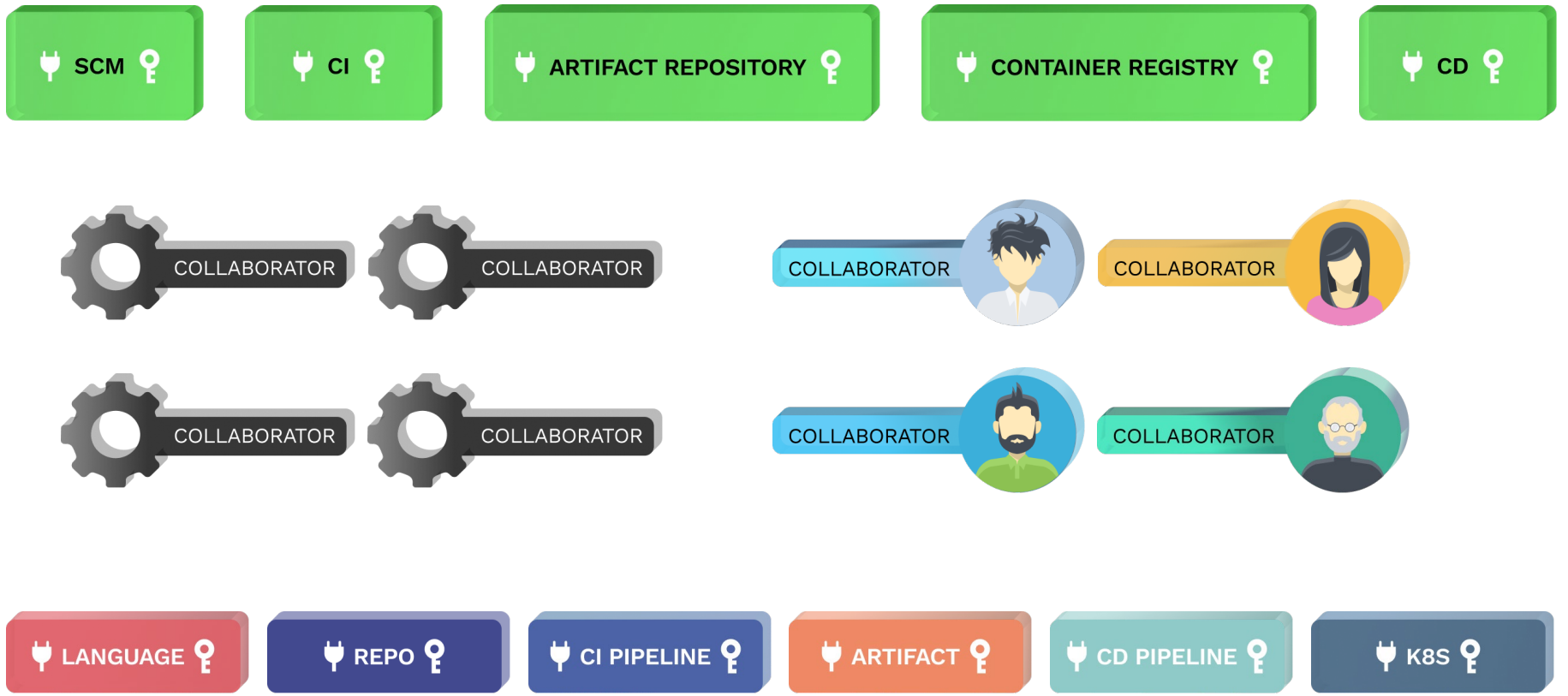
Rapid adoption of new tech

IaC

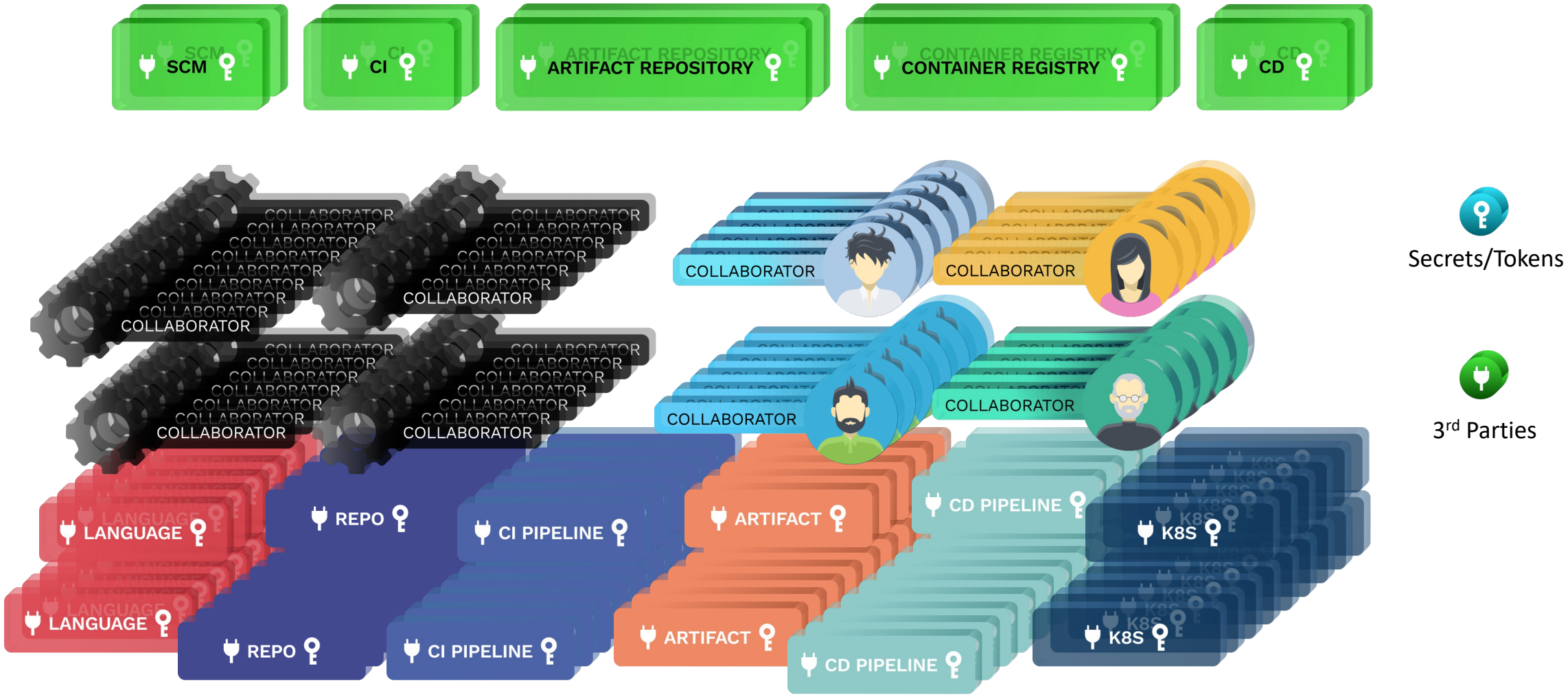
Automation CI/CD

Cider

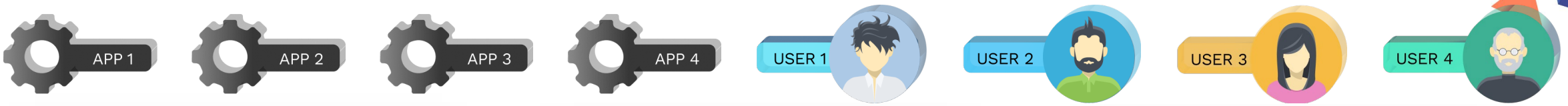
The Engineering Ecosystem

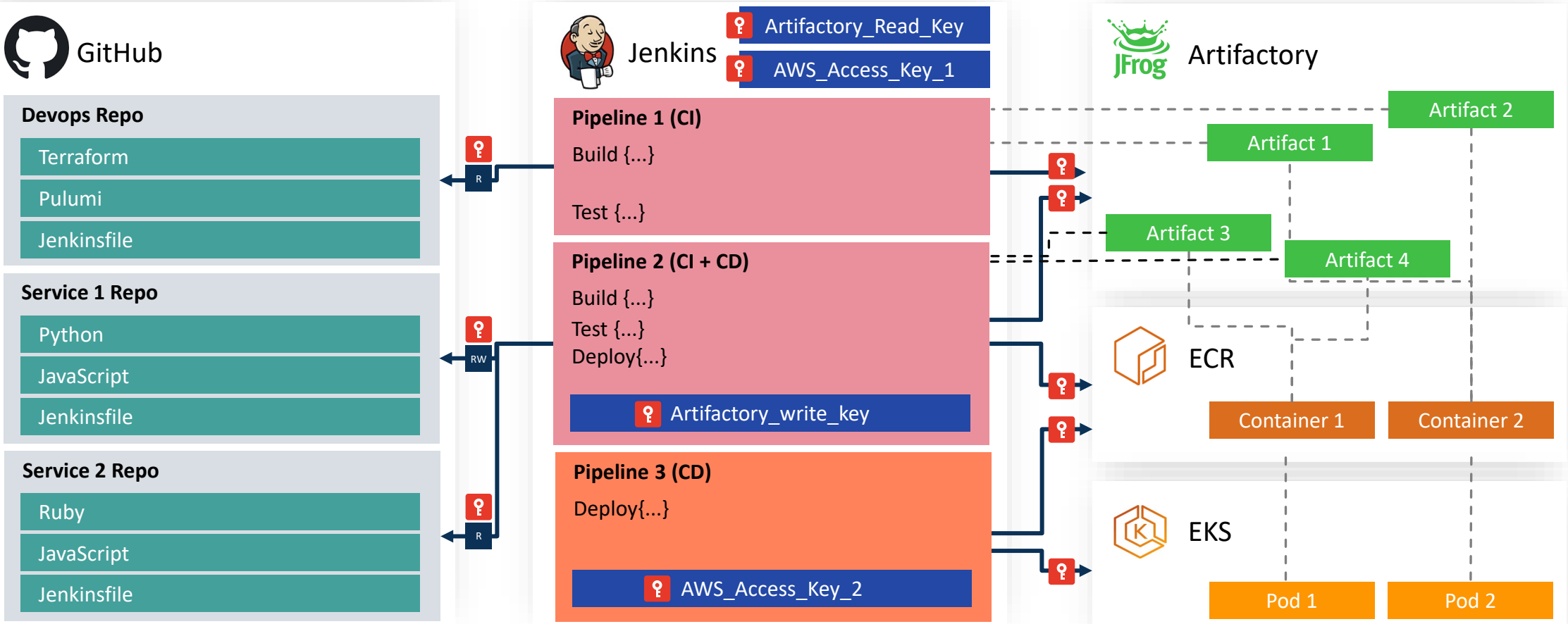


The Challenge



The Security Perspective





CI/CD Security

Building visibility over the engineering ecosystem

Mapping risks and attack paths

Securing the engineering ecosystem – all the way from code to deployment

2021 - The Year of CI/CD Security

- Engineering environments have become **the new attacker's turf**
- **A single insecure step in the CI, or insecure package import** - can expose the organization to critical risks

“Top 10 CI/CD Security Risks” initiative

Cider

https://www.cidersecurity.io/top-10-cicd-security-risks/

Top 10 CI/CD Security Risks

Insufficient Flow Control Mechanisms

Inadequate Identity and Access Management

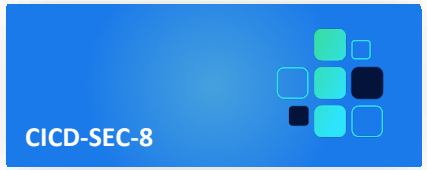
Dependency Chain Abuse

Poisoned Pipeline Execution (PPE)

Insufficient PBAC (Pipeline-Based Access Controls)

Insufficient Credential Hygiene

Insecure System Configuration



Ungoverned Usage of 3rd Party Services

Improper Artifact Integrity Validation

Insufficient Logging and Visibility

Reviewers

Iftach Ian Amit
CSO at Rapid7

Jonathan Claudius
Director of Security Assurance at Mozilla

Michael Coates
CEO & Co-Founder at Altitude Networks, Former CISO at Twitter

Jonathan Jaffe
CISO at Lemonade Insurance

Adrian Ludwig
Chief Trust Officer at Atlassian

Travis McPeak
Head of Product Security at Databricks

Ron Peled
Founder & CEO at ProtectOps, Former CISO at LivePerson

Ty Sbano
CISO at Vercel

Astha Singhal
Director, Information Security at Netflix

Hiroki Suezawa
Security Engineer at Mercari, inc.

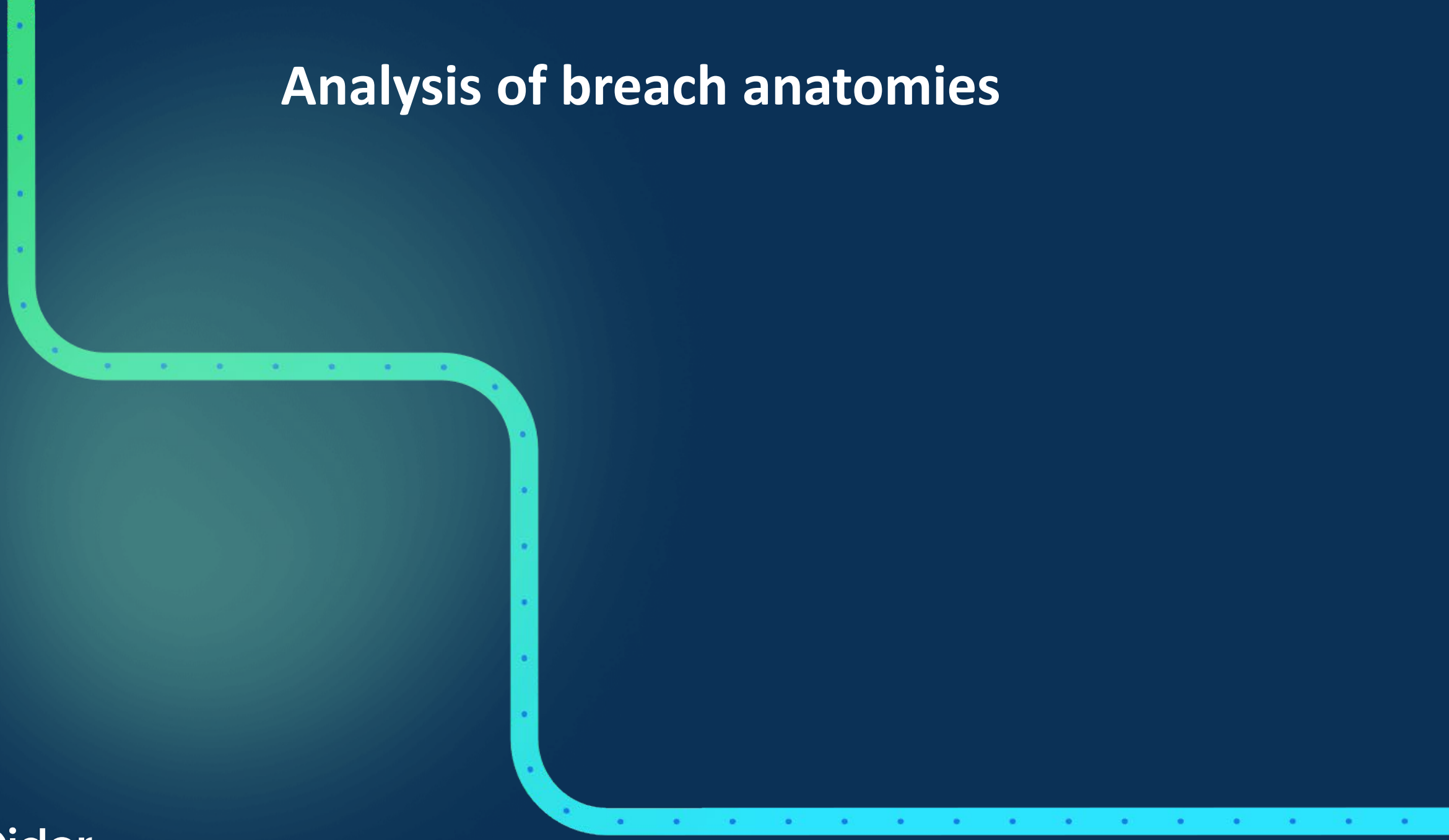
Tyler Welton
Principal Security Engineer at Built Technologies, Owner at Untamed Theory

Tyler Young
Head of Security at Relativity

Noa Ginzbursky
DevOps Engineer at Cider Security

Asi Greenholts
Security Researcher at Cider Security

Analysis of breach anatomies



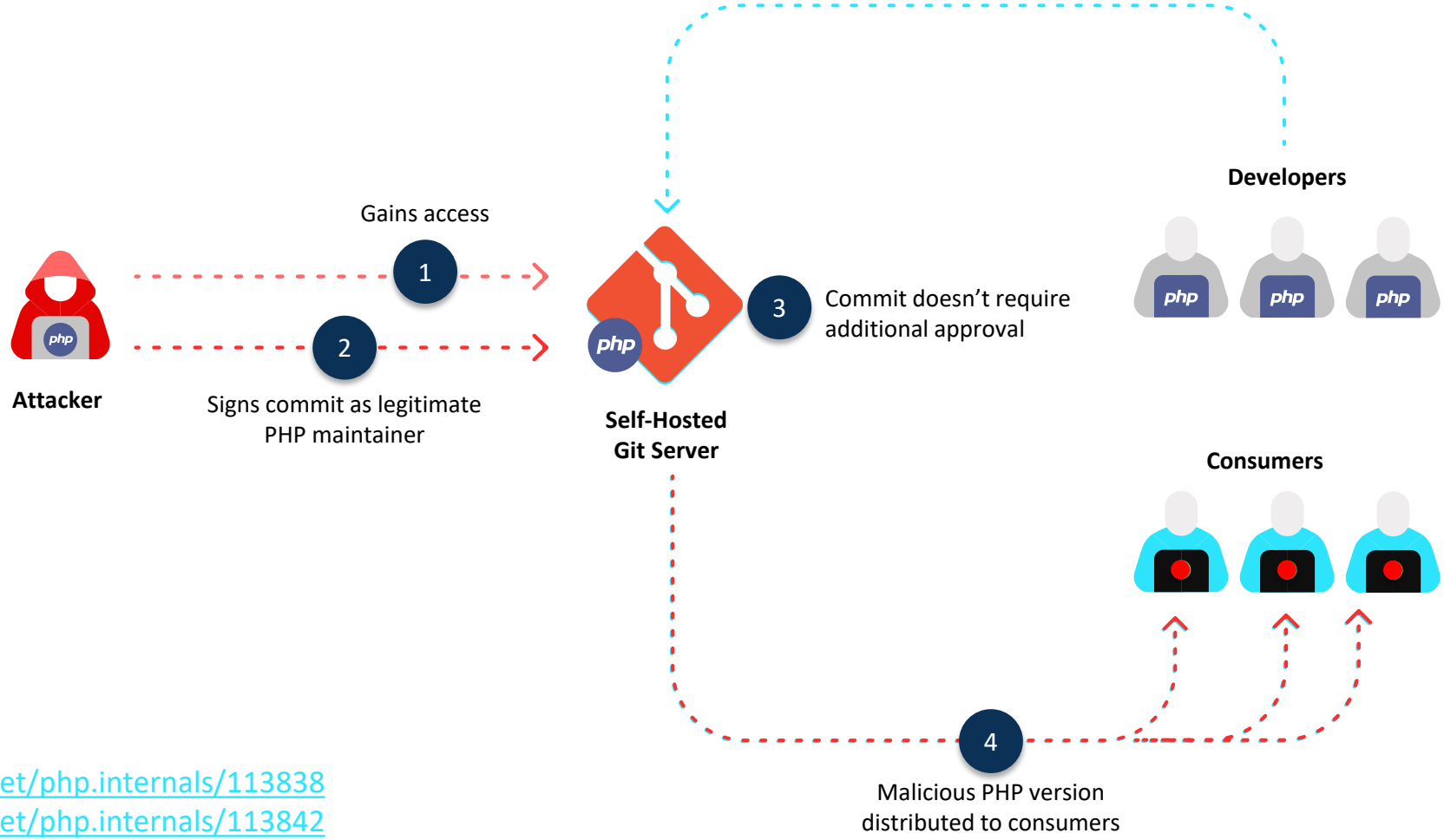
Cider

RSAConference2022

PHP Git infrastructure compromise

Case Study #1

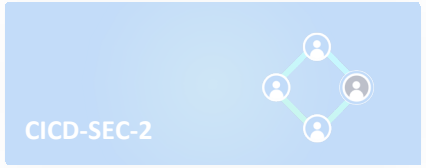
PHP Git infrastructure compromise



https://news-web.php.net/php.internals/113838
https://news-web.php.net/php.internals/113842

Top 10 CI/CD Security Risks

Insufficient Flow Control Mechanisms



Inadequate Identity and Access Management

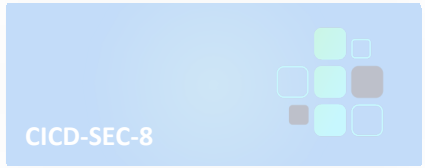
Dependency Chain Abuse

Poisoned Pipeline Execution (PPE)

Insufficient PBAC (Pipeline-Based Access Controls)

Insufficient Credential Hygiene

Insecure System Configuration



Ungoverned Usage of 3rd Party Services

Improper Artifact Integrity Validation

Insufficient Logging and Visibility

CICD-SEC-1
Insufficient Flow Control Mechanisms

Abusing CI/CD misconfigurations to single handedly push unreviewed code or artifacts down the pipeline.

- Prevention / Detection of merging unapproved code

CICD-SEC-7
Insecure System Configuration

Flaws in the security settings, configuration and hardening of the different systems across the pipeline (e.g. SCM, CI, Artifact repository).

- Self-hosted Git with insufficient security hardening

CICD-SEC-9
Improper Artifact Integrity Validation

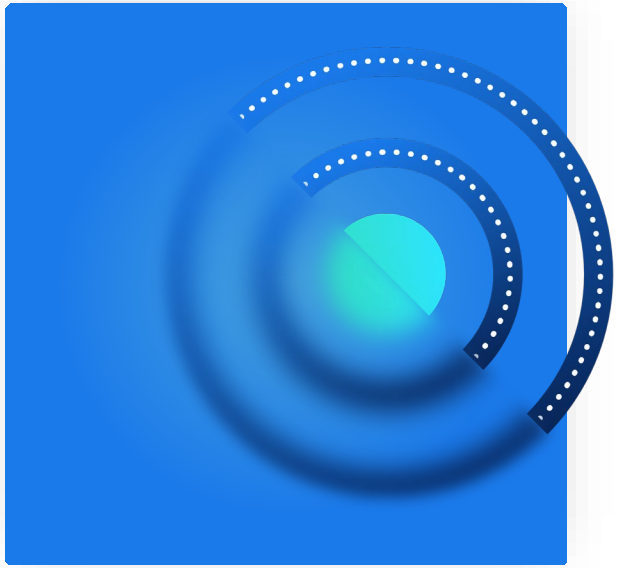
Access to one of the systems in the CI/CD environment can push malicious code or artifacts down the pipeline, due to a lack in mechanisms for validating for the integrity of the code/artifact.

- Signed commits

CICD-SEC-10
Insufficient Logging and Visibility

Malicious activities can be carried out within the CI/CD environment without any correlating detective and investigative capabilities.

Essential base layer for coping with all CI/CD security risks

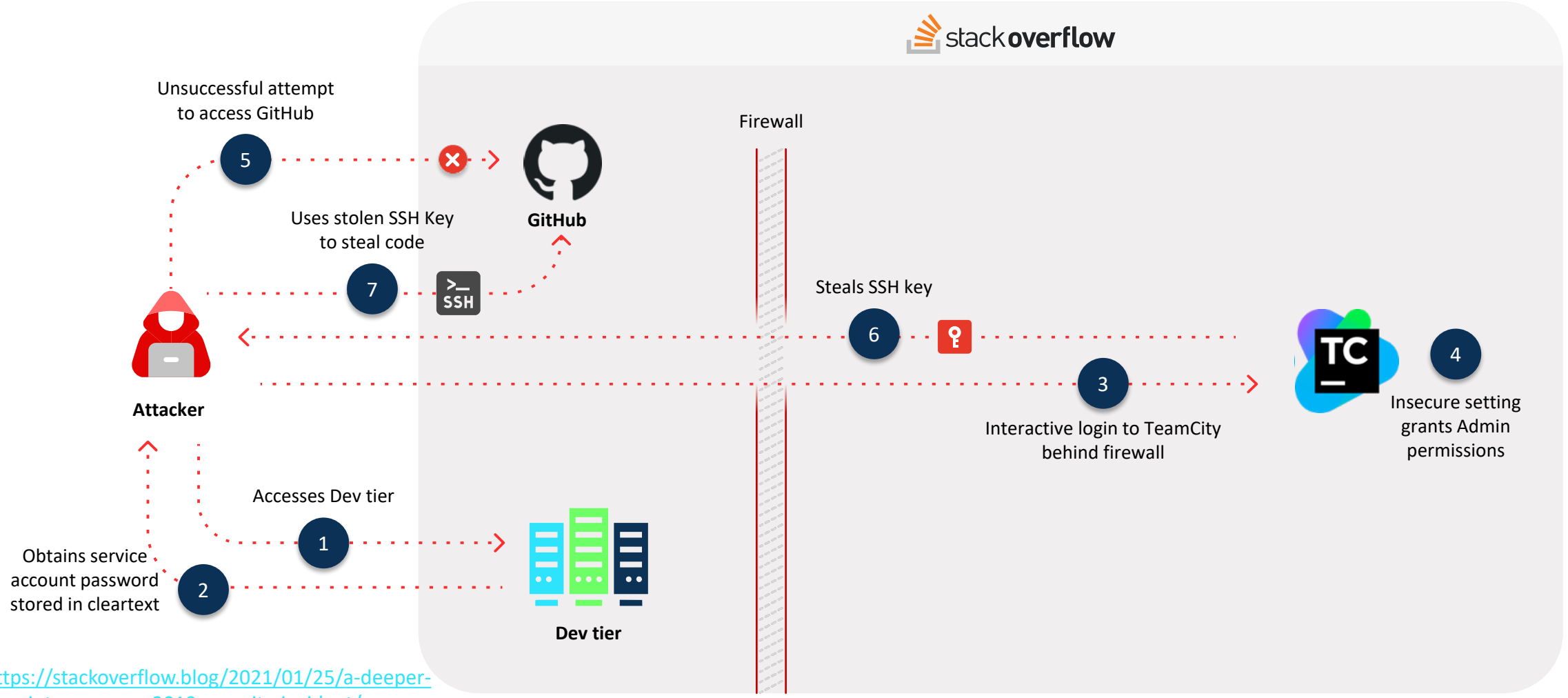


RSAConference2022

Stack Overflow breach

Case Study #2

Stack Overflow breach



https://stackoverflow.blog/2021/01/25/a-deeper-dive-into-our-may-2019-security-incident/

Top 10 CI/CD Security Risks

CICD-SEC-1

Insufficient Flow Control Mechanisms

CICD-SEC-2

Inadequate Identity and Access Management

CICD-SEC-3

Dependency Chain Abuse

CICD-SEC-4

Poisoned Pipeline Execution (PPE)

CICD-SEC-5

Insufficient PBAC (Pipeline-Based Access Controls)

CICD-SEC-6

Insufficient Credential Hygiene

CICD-SEC-7

Insecure System Configuration

CICD-SEC-8

Ungoverned Usage of 3rd Party Services

CICD-SEC-9

Improper Artifact Integrity Validation

CICD-SEC-10

Insufficient Logging and Visibility

CICD-SEC-2
Inadequate Identity and Access Management

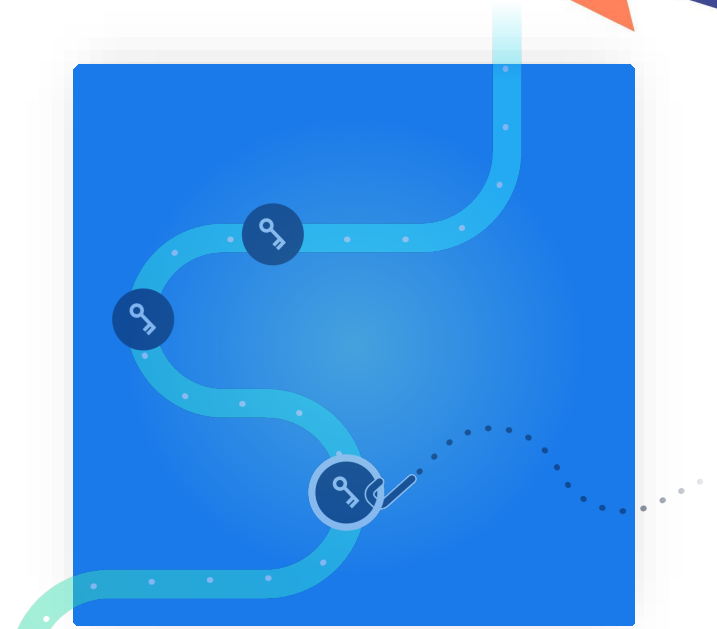
Poorly managed/governed identities – both human and programmatic – across the different systems in the engineering ecosystem.

- Inactive account not revoked
- Service account logs in interactively
- Admin privileges as a base permission

CICD-SEC-6
Insufficient Credential Hygiene

Obtaining and abusing secrets and tokens spread throughout the CI/CD ecosystem due to poor access controls, insecure secret management and overly permissive credentials.

- Static credentials stored in cleartext in the codebase, build system, and configuration files



Additional Risks

Insecure System Configuration

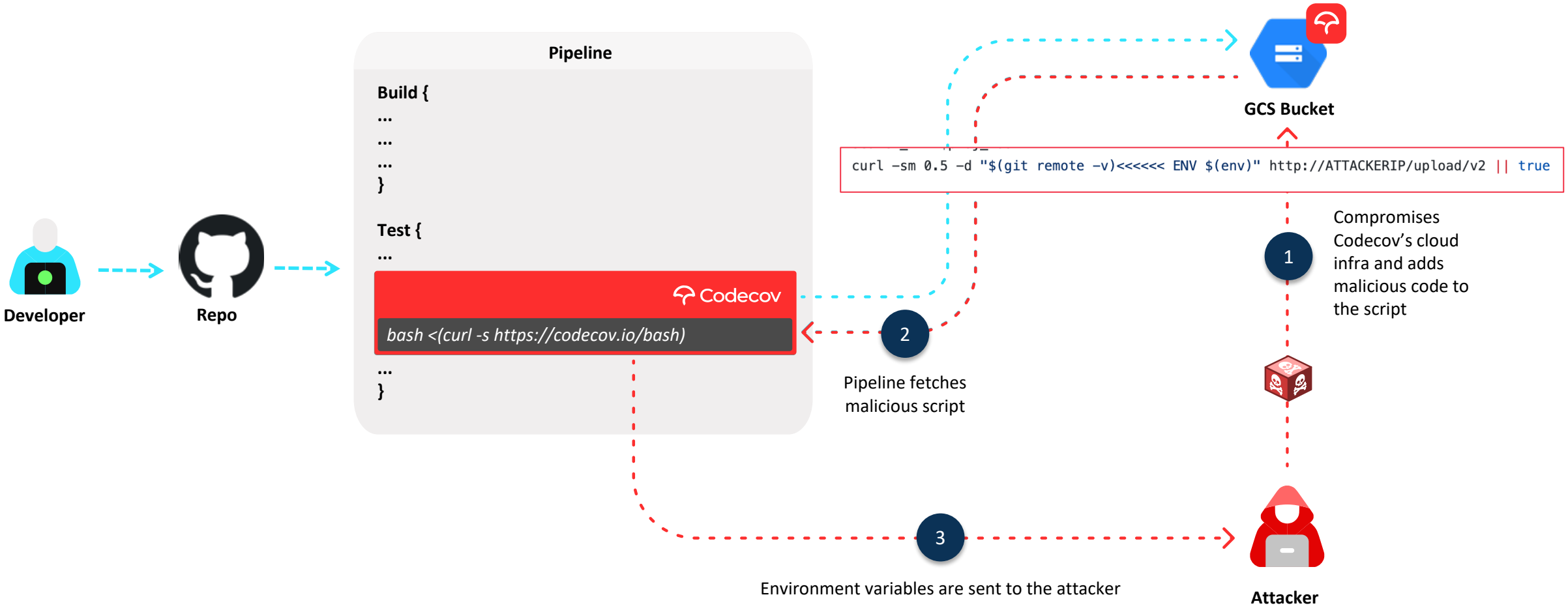
- Self-hosted SCM & CI exposed to the internet

RSAConference2022

Environment variables exfiltration through Codecov

Case Study #3

Environment variables exfiltration through Codecov



https://about.codecov.io/security-update/

Top 10 CI/CD Security Risks

CICD-SEC-1

Insufficient Flow Control Mechanisms

CICD-SEC-2

Inadequate Identity and Access Management

CICD-SEC-3

Dependency Chain Abuse

CICD-SEC-4

Poisoned Pipeline Execution (PPE)

CICD-SEC-5

Insufficient PBAC (Pipeline-Based Access Controls)

CICD-SEC-6

Insufficient Credential Hygiene

CICD-SEC-7

Insecure System Configuration

CICD-SEC-8

Ungoverned usage of 3rd Party Services

CICD-SEC-9

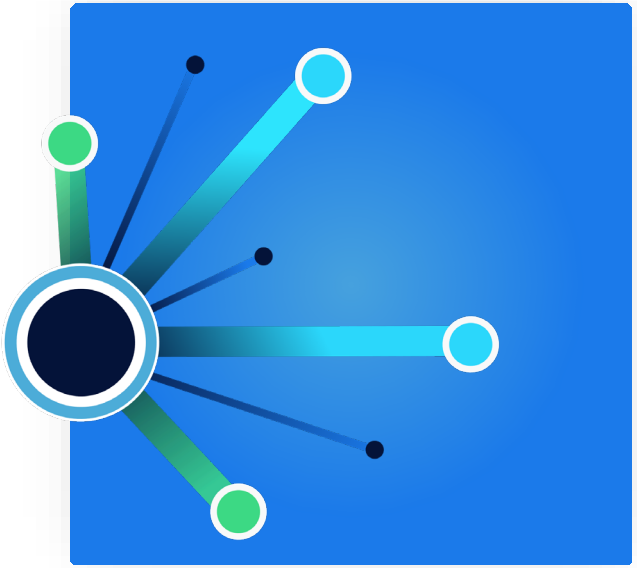
Improper Artifact Integrity Validation

CICD-SEC-10

Insufficient Logging and Visibility

CICD-SEC-5
Insufficient PBAC (Pipeline-Based Access Controls)

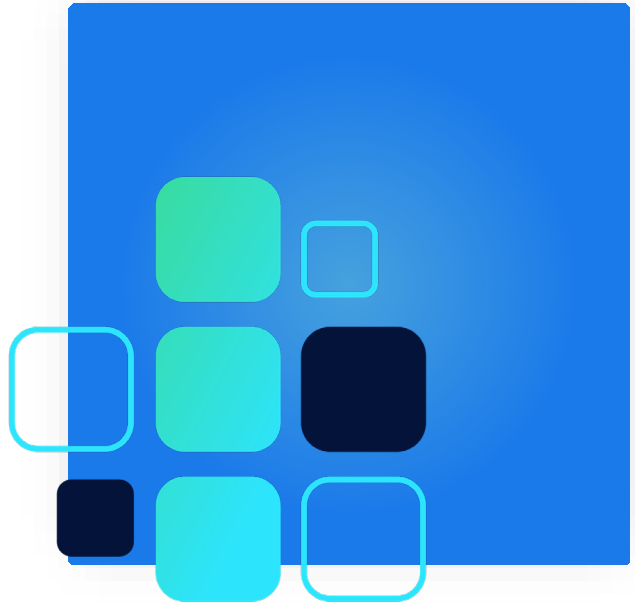
Abusing the excessive permissions/access granted to the pipeline execution nodes for moving laterally within or outside the CI/CD environment.



- Overly permissive pipeline execution environments

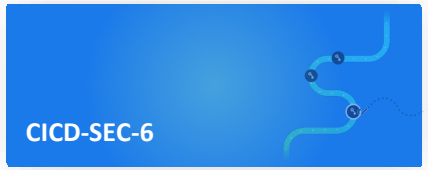
CICD-SEC-8
Ungoverned Usage of 3rd Party Services

Risks which rely on the extreme ease with which a 3rd party service can be granted access to resources in CI/CD systems, effectively expanding the attack surface of the organization.



- Minimal investigative capabilities around existence/permissions of Codecov

Additional risks



Insufficient Credential Hygiene

- Overly permissive secrets stored as environment variables

Improper Artifact Integrity Validation

- Integrity checks not performed prior to executing Codecov script

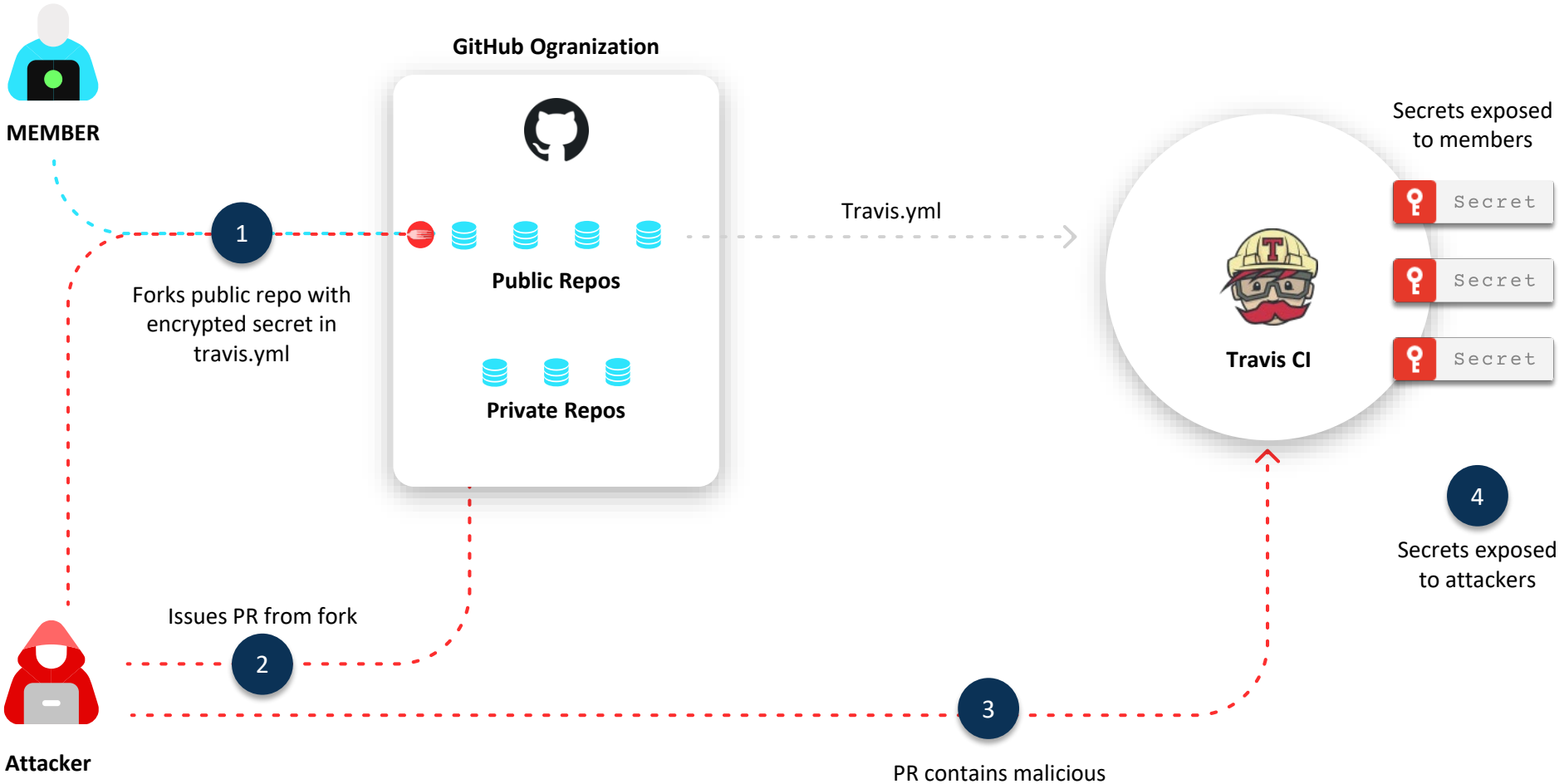
Insufficient Logging and Visibility

RSAConference2022

Travis CI secrets exposure

Case Study #4

Travis CI secrets exposure



https://travis-ci.community/t/security-bulletin/12081

Top 10 CI/CD Security Risks

CICD-SEC-1

Insufficient Flow Control Mechanisms

CICD-SEC-2

Inadequate Identity and Access Management

CICD-SEC-3

Dependency Chain Abuse

CICD-SEC-4

Poisoned Pipeline Execution (PPE)

CICD-SEC-5

Insufficient PBAC (Pipeline-Based Access Controls)

CICD-SEC-6

Insufficient Credential Hygiene

CICD-SEC-7

Insecure System Configuration

CICD-SEC-8

Ungoverned Usage of 3rd Party Services

CICD-SEC-9

Improper Artifact Integrity Validation

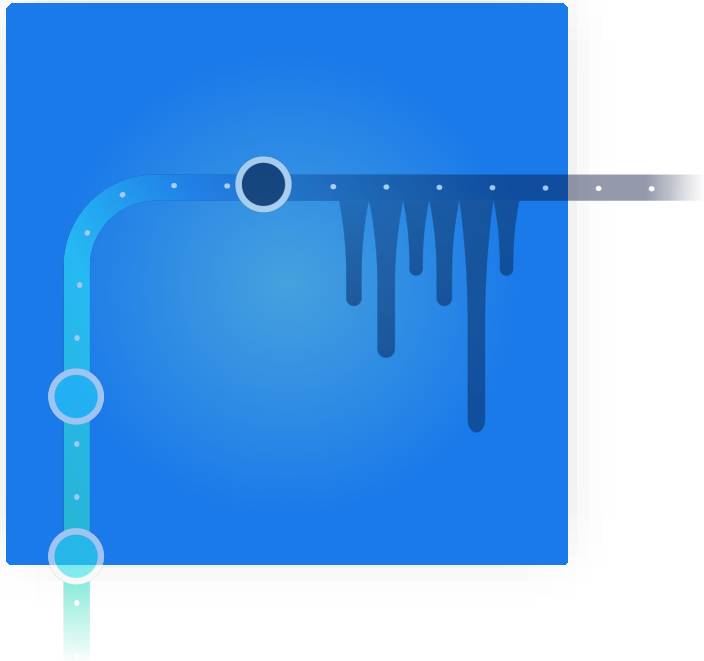
CICD-SEC-10

Insufficient Logging and Visibility

CICD-SEC-4
Poisoned Pipeline Execution (PPE)

The ability of an attacker that has obtained access to an SCM repository, to run malicious code in the CI - despite not having access to it - by manipulating the pipeline configuration.

- Execution of a PPE attack to exfiltrate pipeline secrets



Additional Risks

Insufficient Credential Hygiene

- Secrets the pipeline shouldn't access
- Permissive credentials

Insufficient Logging and Visibility

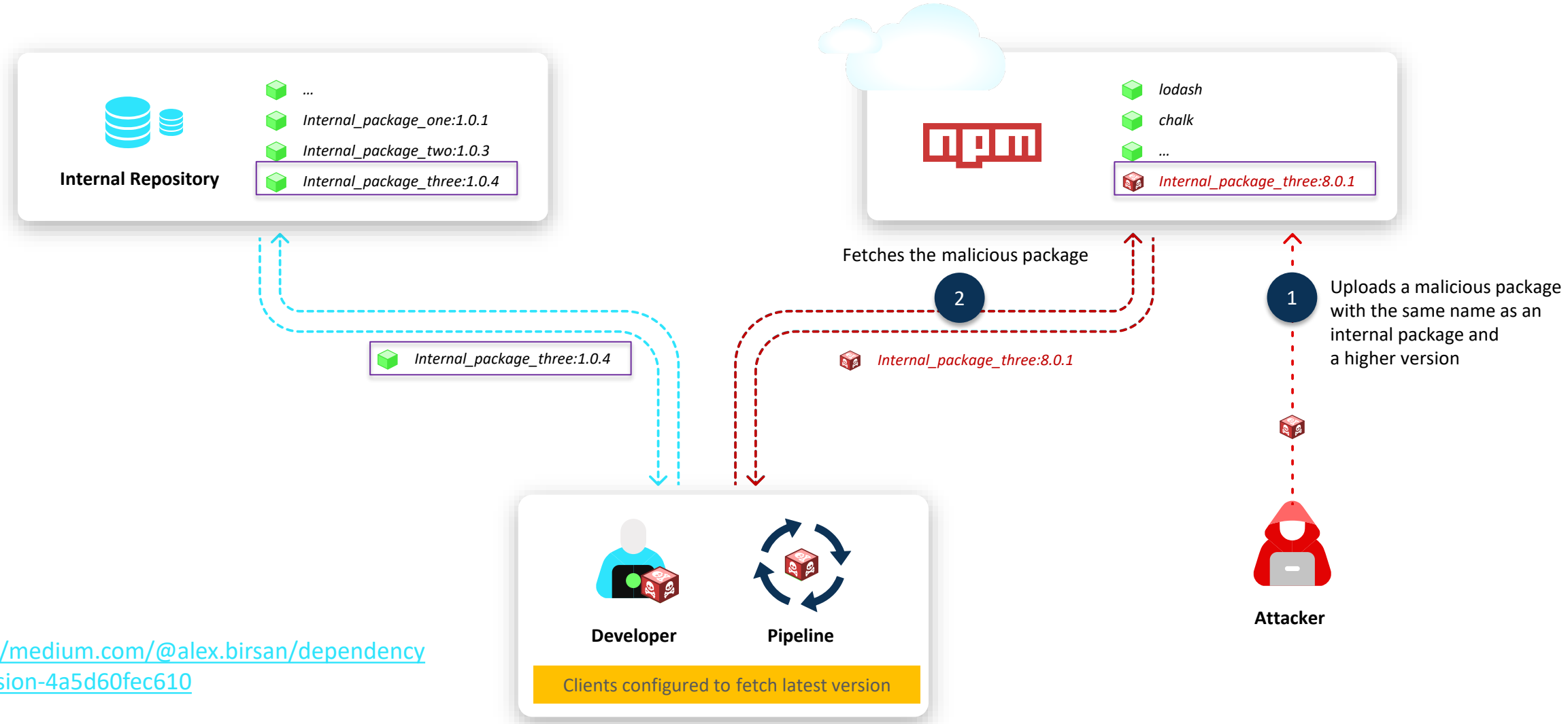
- Identify potentially vulnerable repos
- Identify an actual breach

RSAConference2022

Dependency Confusion

Case Study #5

Dependency Confusion



https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

Cider

Top 10 CI/CD Security Risks

CICD-SEC-1

Insufficient Flow Control Mechanisms

CICD-SEC-2

Inadequate Identity and Access Management

CICD-SEC-3

Dependency Chain Abuse

CICD-SEC-4

Poisoned Pipeline Execution (PPE)

CICD-SEC-5

Insufficient PBAC (Pipeline-Based Access Controls)

CICD-SEC-6

Insufficient Credential Hygiene

CICD-SEC-7

Insecure System Configuration

CICD-SEC-8

Ungoverned Usage of 3rd Party Services

CICD-SEC-9

Improper Artifact Integrity Validation

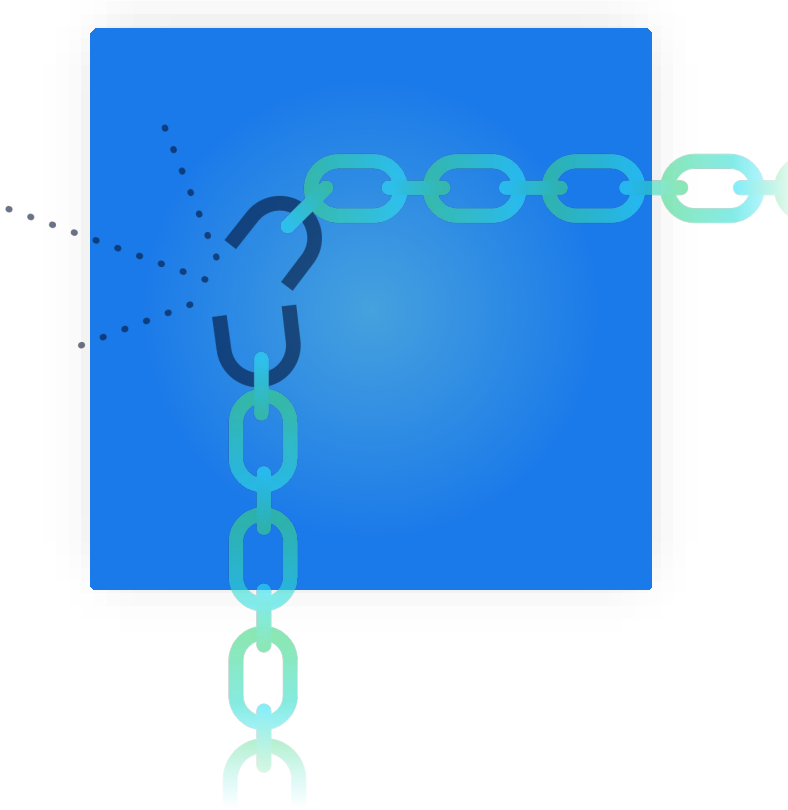
CICD-SEC-10

Insufficient Logging and Visibility

CICD-SEC-3
Dependency Chain Abuse

Abusing code dependency fetching configuration – to cause an unsuspecting client to fetch and execute a malicious package.

- Dependency confusion abuses the dependency chain by taking advantage of misconfigured package fetching processes



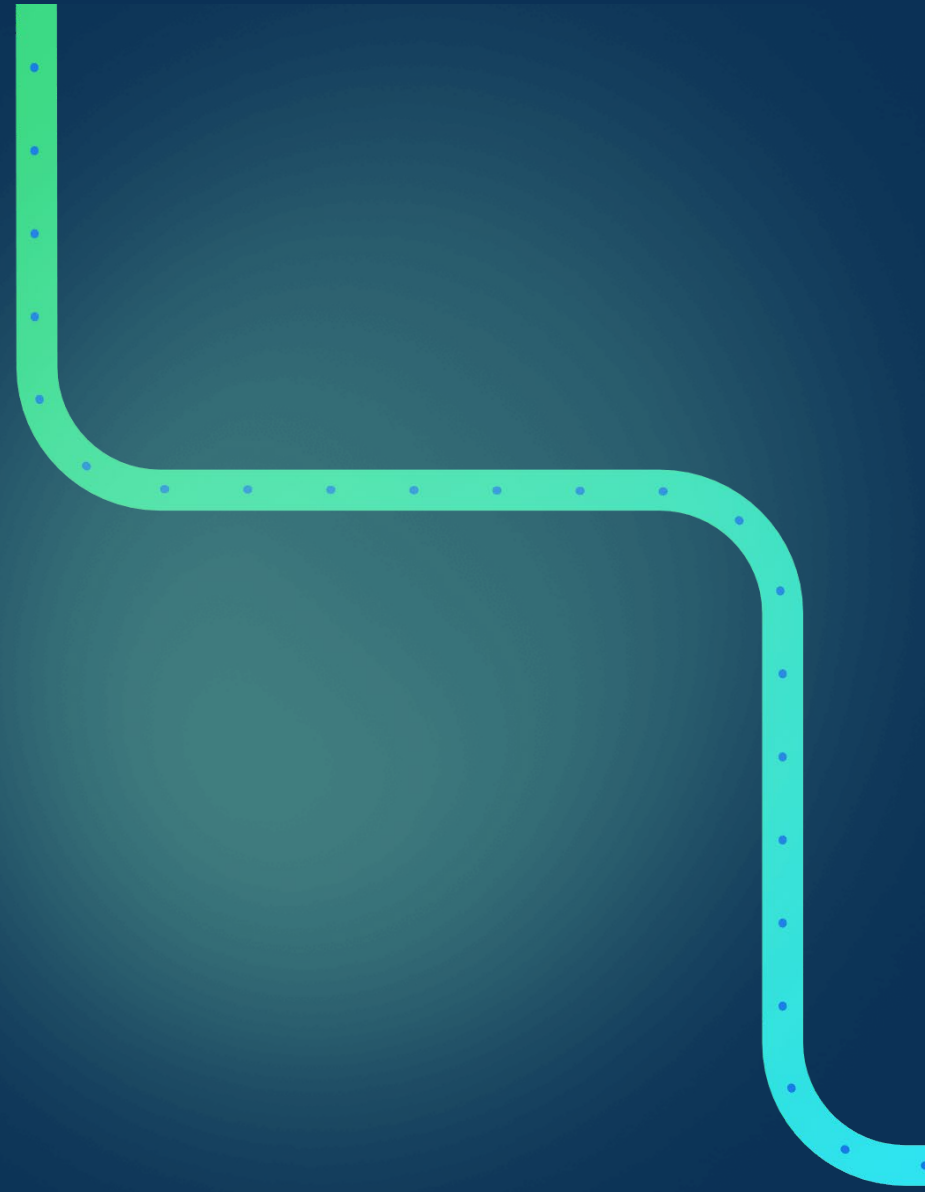
Additional Risks

Insufficient PBAC (Pipeline-Based Access Controls)

- Packages installed and executed on overly permissive execution nodes

Insufficient Logging and Visibility

Takeaways



Cider

Apply to your day-to-day

- A shift in mindset –
  - The changes in the engineering ecosystem have reshaped our attack surface. Engineering environments, systems and processes have become a big part of our attack surface.
- A different approach to AppSec –
  - Application Security extends far beyond securing the code. We need to build an overarching security umbrella over all systems and processes all the way from code to deployment.
- Comprehensive mapping of your engineering ecosystem –
  - Security teams must develop practices and controls to allow them to continuously map the technical elements that comprise their engineering ecosystem.

    A full mapping of the ecosystem – including all 3rd party access – is the only way to have a true understanding of our attack surface.
- Continuous analysis against the attacker's perspective –
  - Once strong visibility over the engineering ecosystem is achieved, an analysis against the attacker's perspective – using the Top 10 CI/CD security risks - is required.
- Build and optimize CI/CD security programs –
  - A continuous effort to optimize CI/CD posture is required to ensure that the velocity and dynamic nature of engineering ecosystem to not increase risk.

Thank you!

Cider