Top 10 CI/CD Security Risks

Daniel Krivelevich
Co-Founder & CTO
Cider Security
@dkrivelev

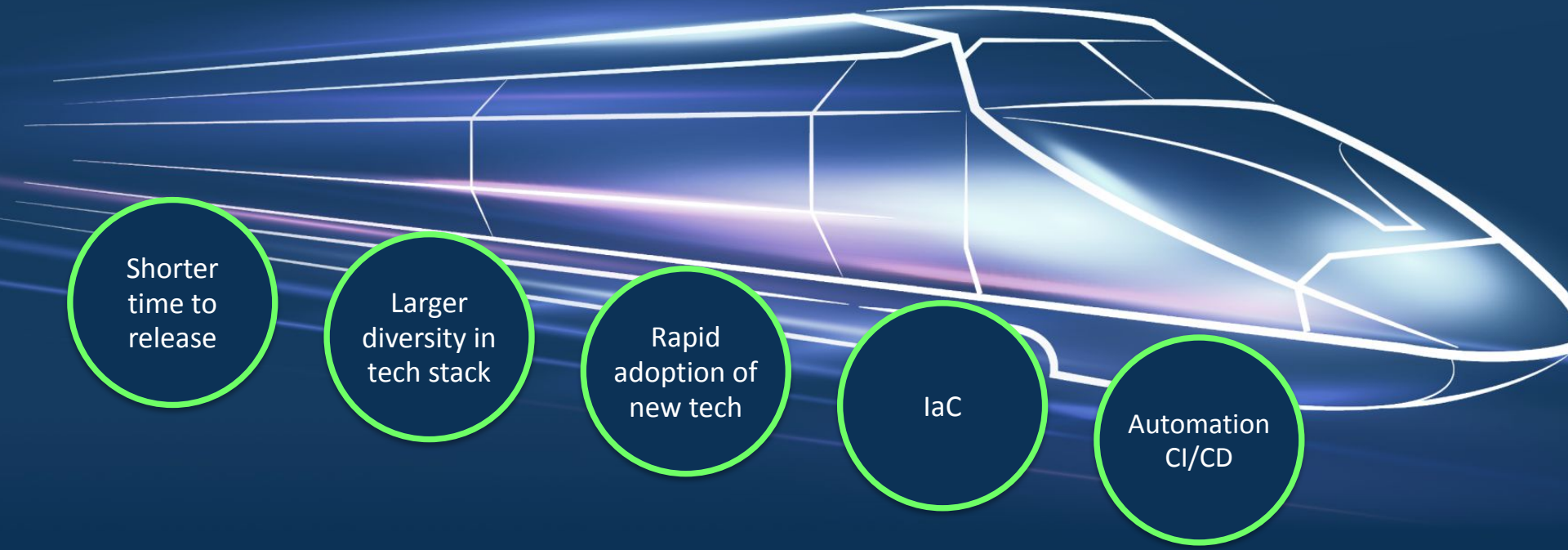
Omer Gil
Head Of Research
Cider Security
@omer_gil

Cider

What is **CI/CD security?**

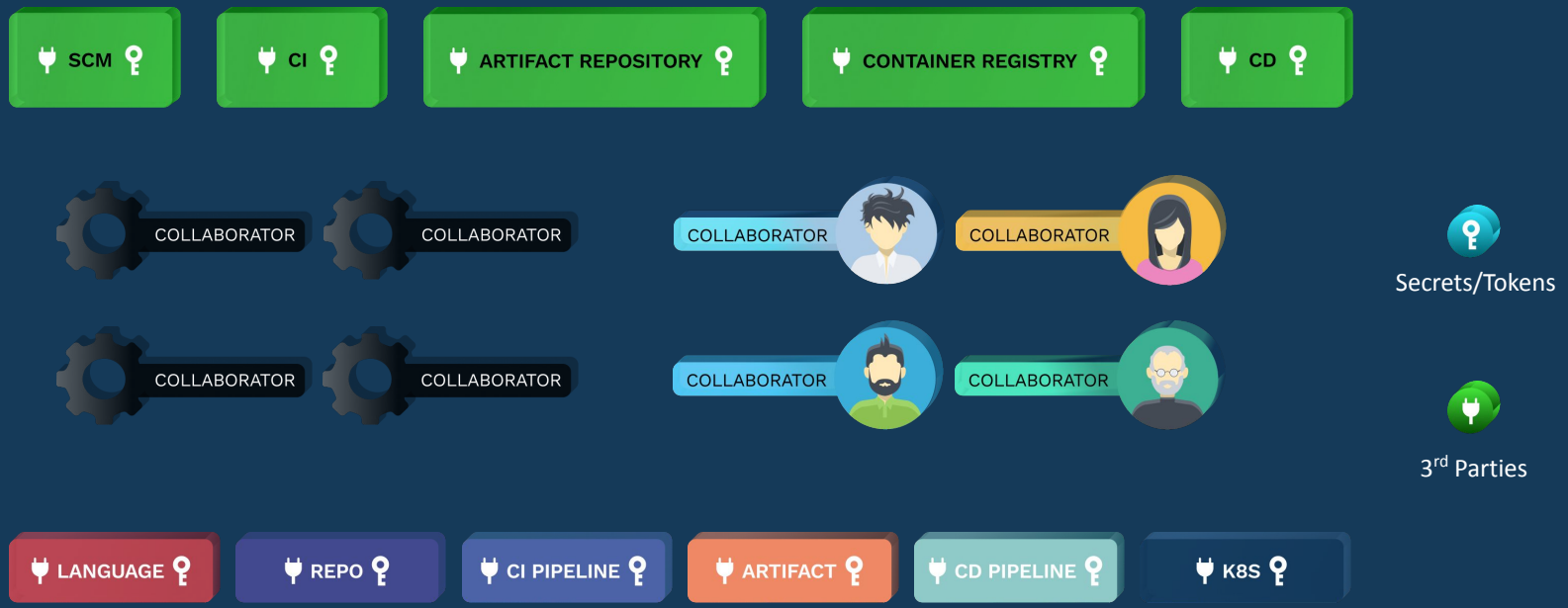
Cider

The engineering train moves faster and faster...



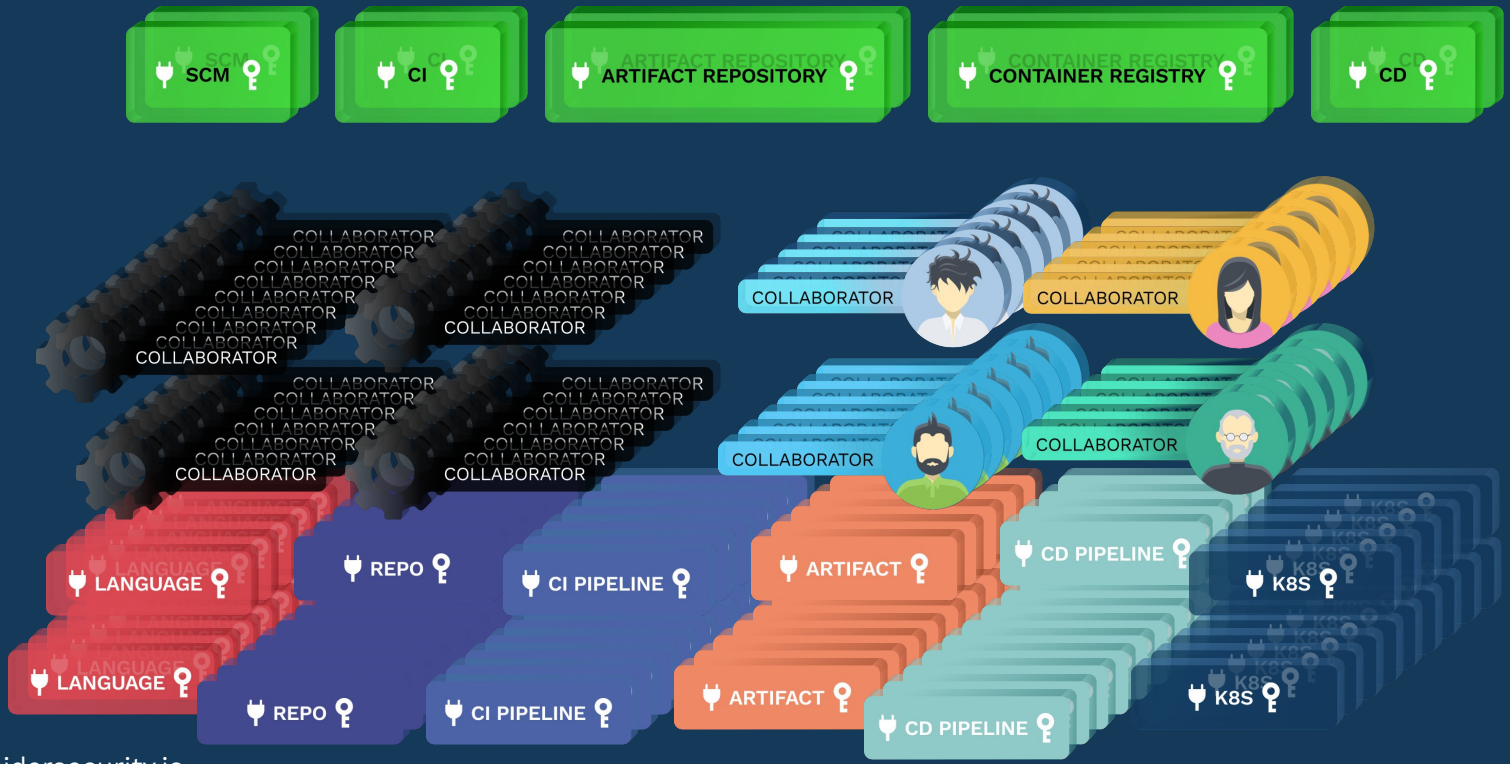
Cider

The engineering ecosystem



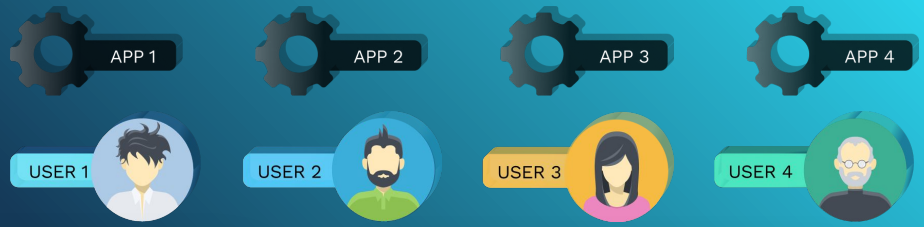
Cider

The challenge



Cider

The Security Perspective



GitHub

Devops Repo
- Terraform
- Pulumi
- Jenkinsfile

Service 1 Repo
- Python
- JavaScript
- Jenkinsfile

Service 2 Repo
- Ruby
- JavaScript
- Jenkinsfile

Jenkins

Artifactory_Read_Key

AWS_Access_Key_1

Pipeline 1 (CI)
Build {...}
Test {...}

Pipeline 2 (CI + CD)
Build {...}
Test {...}
Deploy{...}
Artifactory_write_key

Pipeline 3 (CD)
Deploy{...}
AWS_Access_Key_2

Artifactory

Artifact 2
Artifact 1
Artifact 3
Artifact 4

ECR

Container 1
Container 2

EKS

Pod 1
Pod 2

Cider

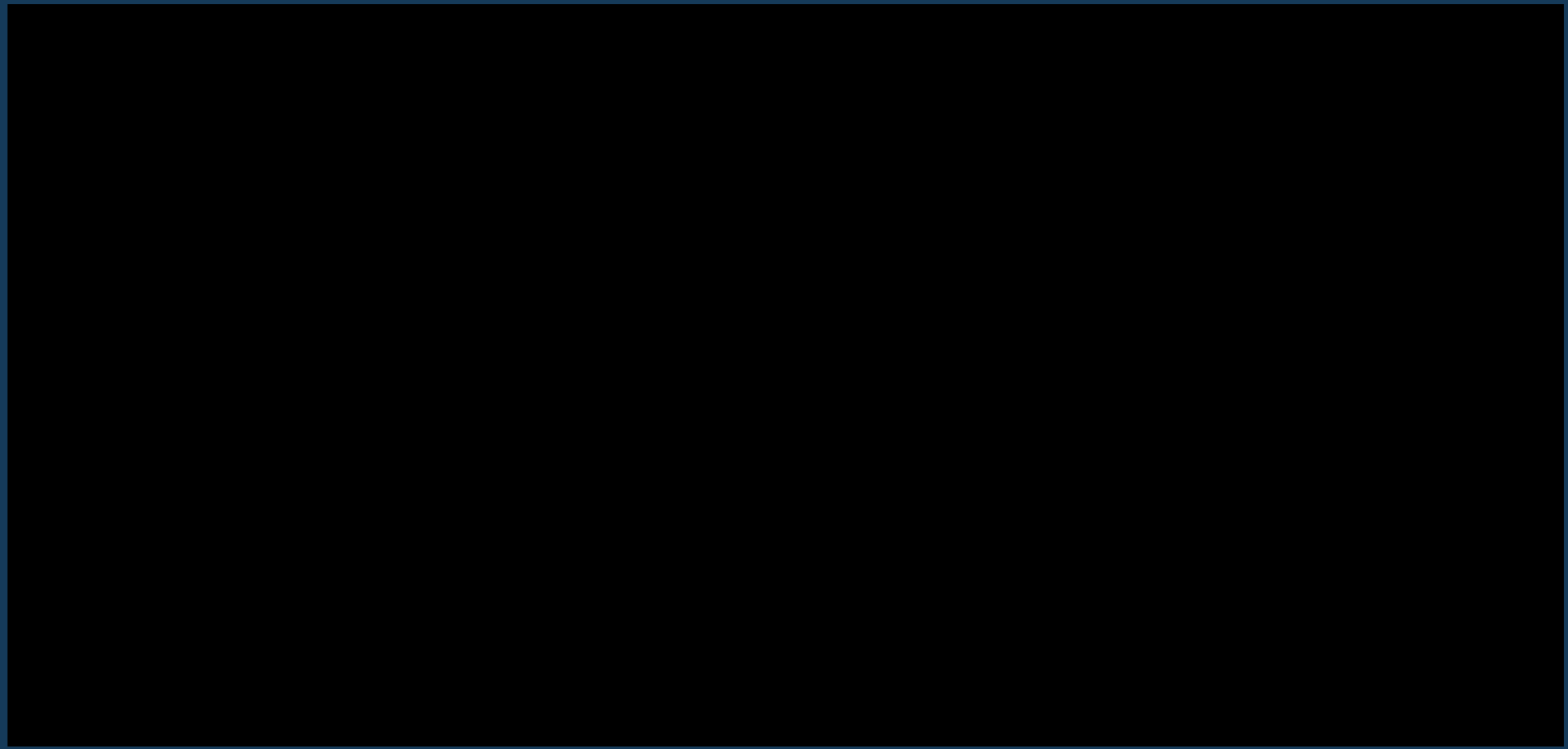
CI/CD Security

- The changes in the engineering ecosystem have changed the way our attack surface looks like
- CI/CD security is about adapting to these changes
- 2021 - A pivotal year for CI/CD security

Cider

“**Top 10** CI/CD Security Risks” initiative

Cider

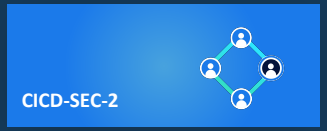


https://www.cidersecurity.io/top-10-cicd-security-risks/

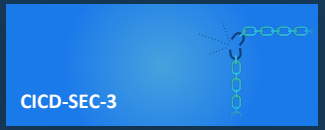
Cider

Top 10 CI/CD Security Risks

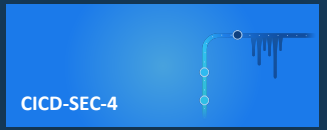
Insufficient Flow Control Mechanisms



Inadequate Identity and Access Management

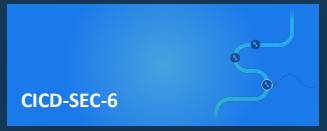


Dependency Chain Abuse



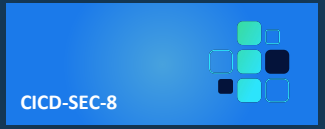
Poisoned Pipeline Execution (PPE)

Insufficient PBAC (Pipeline-Based Access Controls)

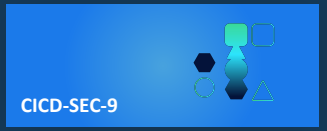


Insufficient Credential Hygiene

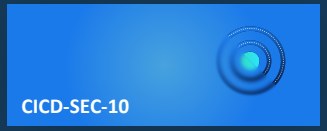
Insecure System Configuration



Ungoverned Usage of 3rd Party Services



Improper Artifact Integrity Validation



Insufficient Logging and Visibility

Reviewers

Iftach Ian Amit
CSO at Rapid7
RAPID7

Jonathan Claudius
Director of Security Assurance at Mozilla
moz://a

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

Jonathan Jaffe
CISO at Lemonade Insurance
Lemonade

Adrian Ludwig
Chief Trust Officer at Atlassian
Atlassian

Travis McPeak
Head of Product Security at Databricks
databricks

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

Ty Sbano
CISO at Vercel
Vercel

Astha Singhal
Director, Information Security at Netflix
NETFLIX

Hiroki Suezawa
Security Engineer at Mercari, inc.
mercari

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

Tyler Young
Head of Security at Relativity
Relativity

Noa Ginzbursky
DevOps Engineer at Cider Security
Cider

Asi Greenholts
Security Researcher at Cider Security
Cider

Cider

Analysis of breach anatomies

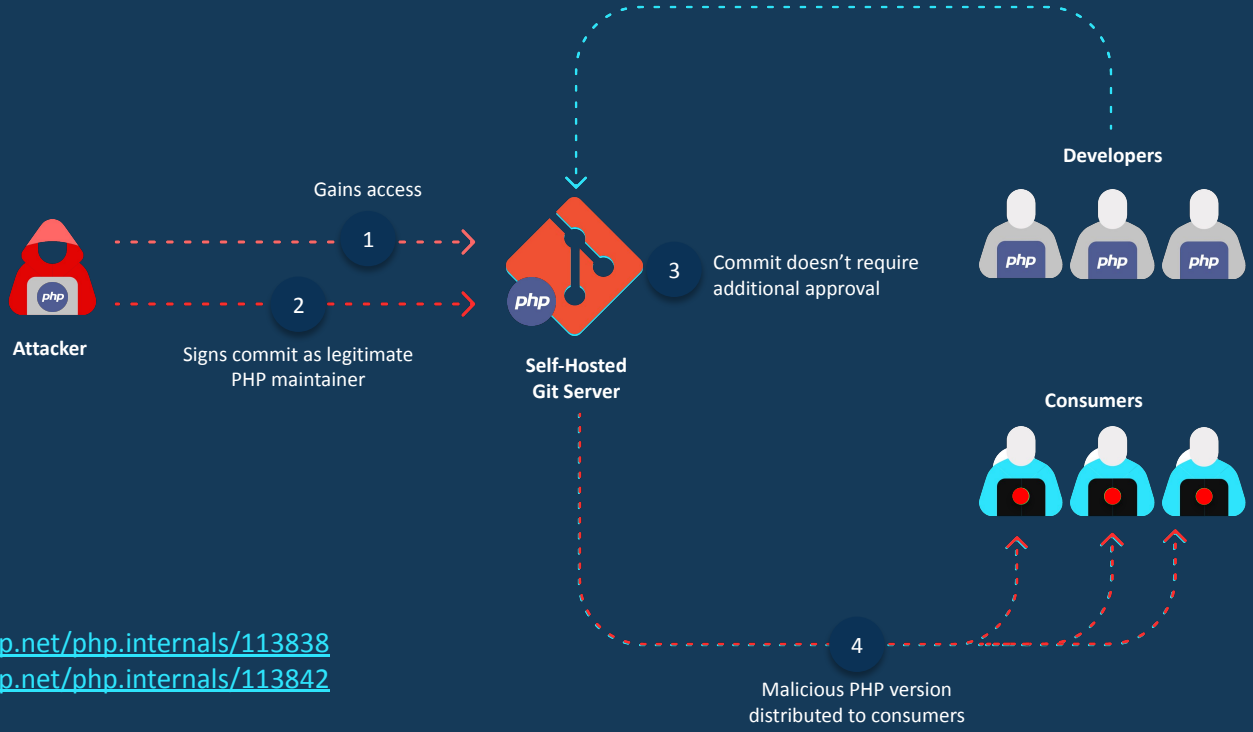
Cider

PHP Git infrastructure compromise

Case Study #1

Cider

PHP Git infrastructure compromise

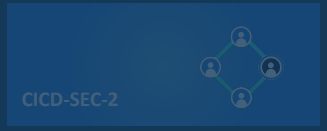


https://news-web.php.net/php.internals/113838
https://news-web.php.net/php.internals/113842

Cider

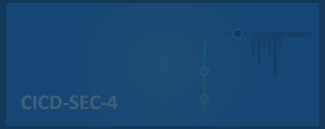
Top 10 CI/CD Security Risks

Insufficient Flow Control Mechanisms

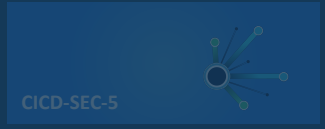


Inadequate Identity and Access Management

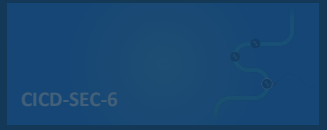
Dependency Chain Abuse



Poisoned Pipeline Execution (PPE)

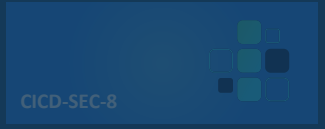


Insufficient PBAC (Pipeline-Based Access Controls)

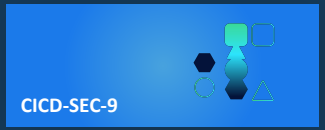


Insufficient Credential Hygiene

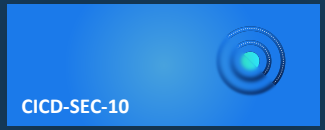
Insecure System Configuration



Ungoverned Usage of 3rd Party Services



Improper Artifact Integrity Validation



Insufficient Logging and Visibility

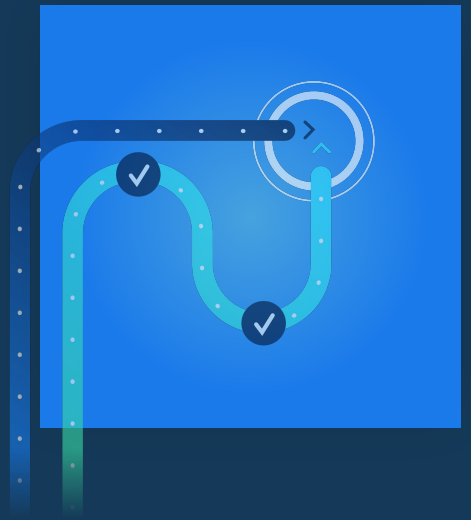
Cider

Insufficient Flow Control Mechanisms

CICD-SEC-1

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

- Prevention / Detection of merging unapproved code



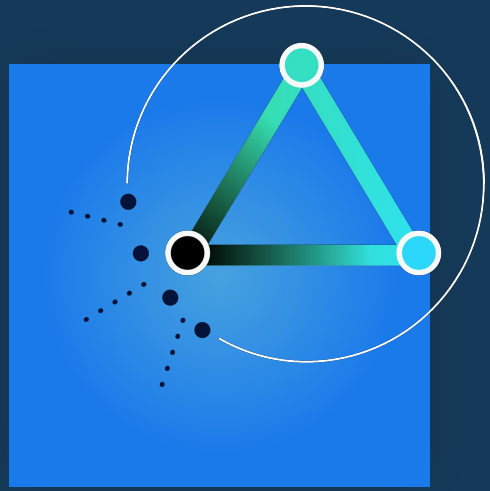
Cider

Insecure System Configuration

CICD-SEC-7

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

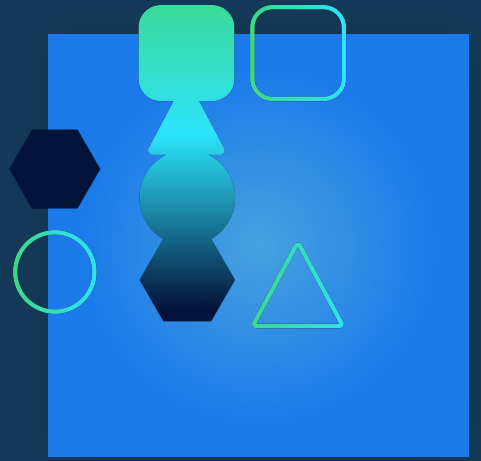
- Self hosted Git with insufficient security hardening



Improper Artifact Integrity Validation

CICD-SEC-9

A lack of mechanisms for validating the integrity of code and artifacts, allows an attacker with access to one of the systems in the CI/CD to push malicious code or artifacts down the pipeline.



- Signed commits

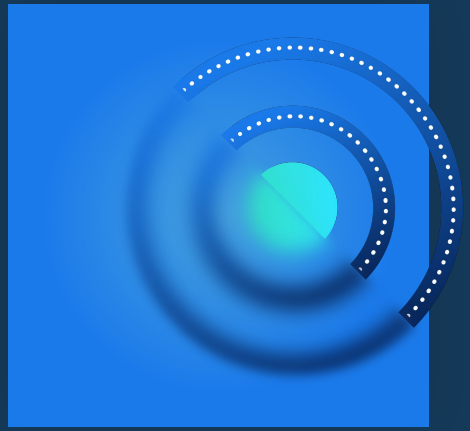
Cider

Insufficient Logging and Visibility

CICD-SEC-10

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

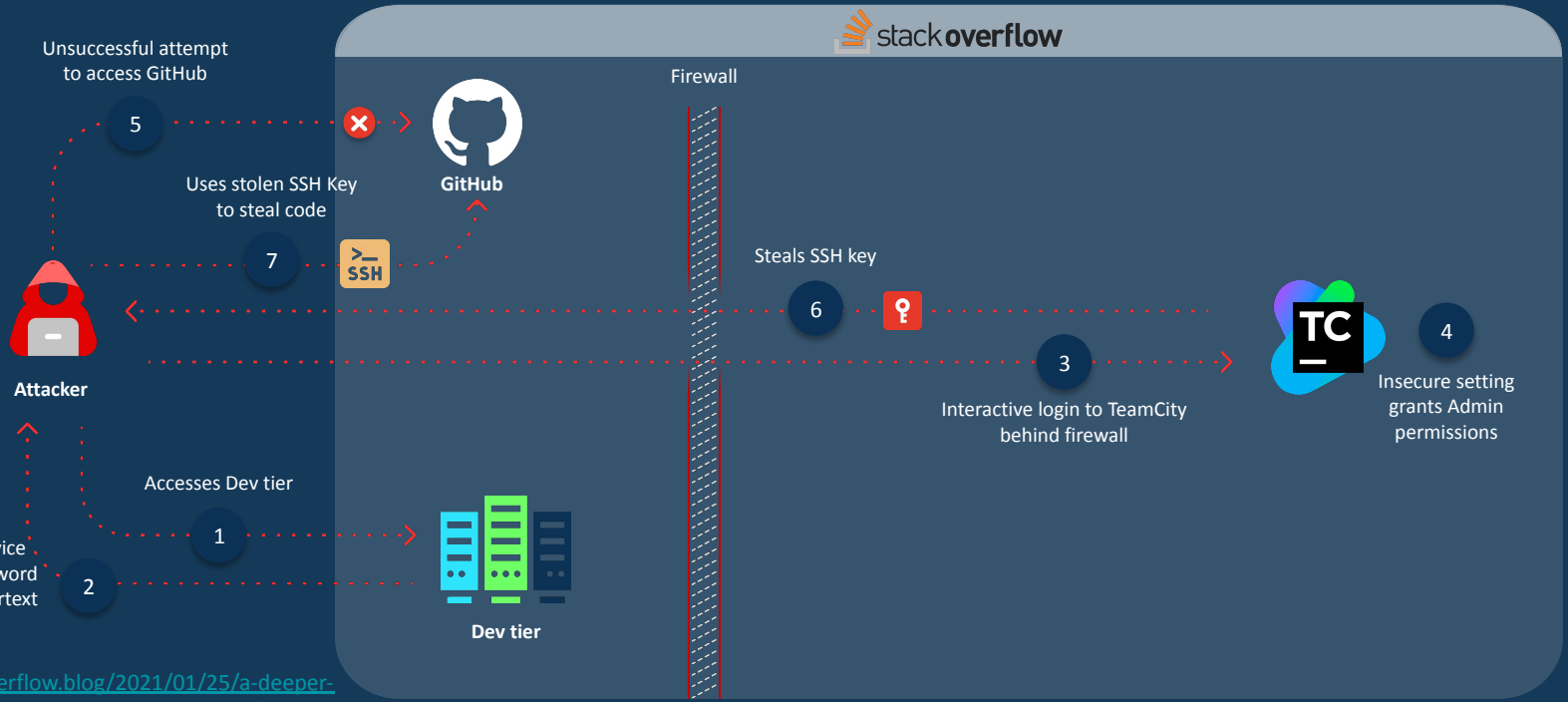


Stack Overflow Breach

Case Study #2

Cider

Stack Overflow breach

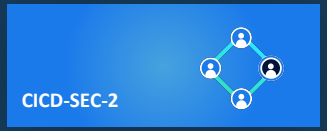


https://stackoverflow.blog/2021/01/25/a-deeper-dive-into-our-may-2019-security-incident/

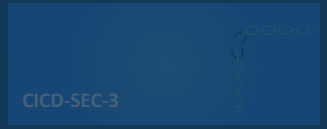
Cider

Top 10 CI/CD Security Risks

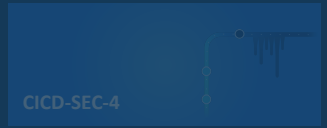
Insufficient Flow Control Mechanisms



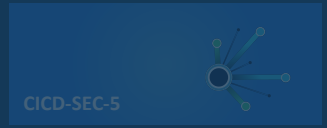
Inadequate Identity and Access Management



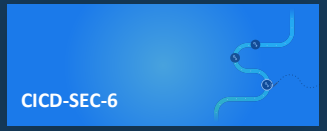
Dependency Chain Abuse



Poisoned Pipeline Execution (PPE)

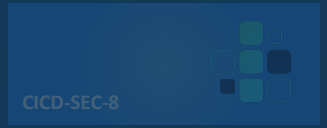


Insufficient PBAC (Pipeline-Based Access Controls)

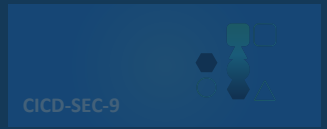


Insufficient Credential Hygiene

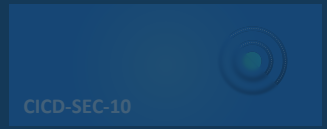
Insecure System Configuration



Ungoverned Usage of 3rd Party Services



Improper Artifact Integrity Validation



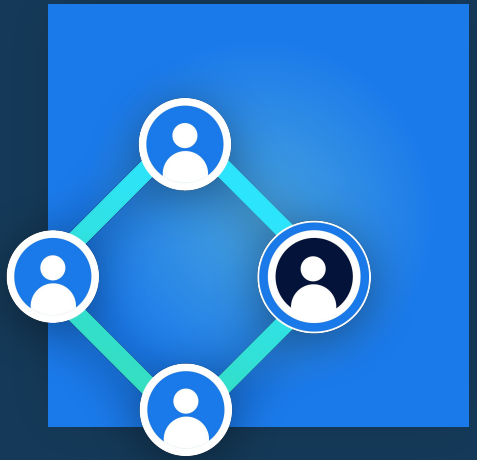
Insufficient Logging and Visibility

Cider

Inadequate Identity and Access Management

CICD-SEC-2

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

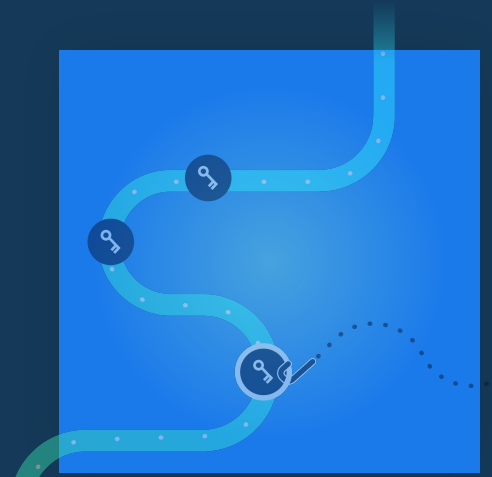
Cider

Insufficient Credential Hygiene

CICD-SEC-6

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



Cider

Additional risks

Insecure System Configuration

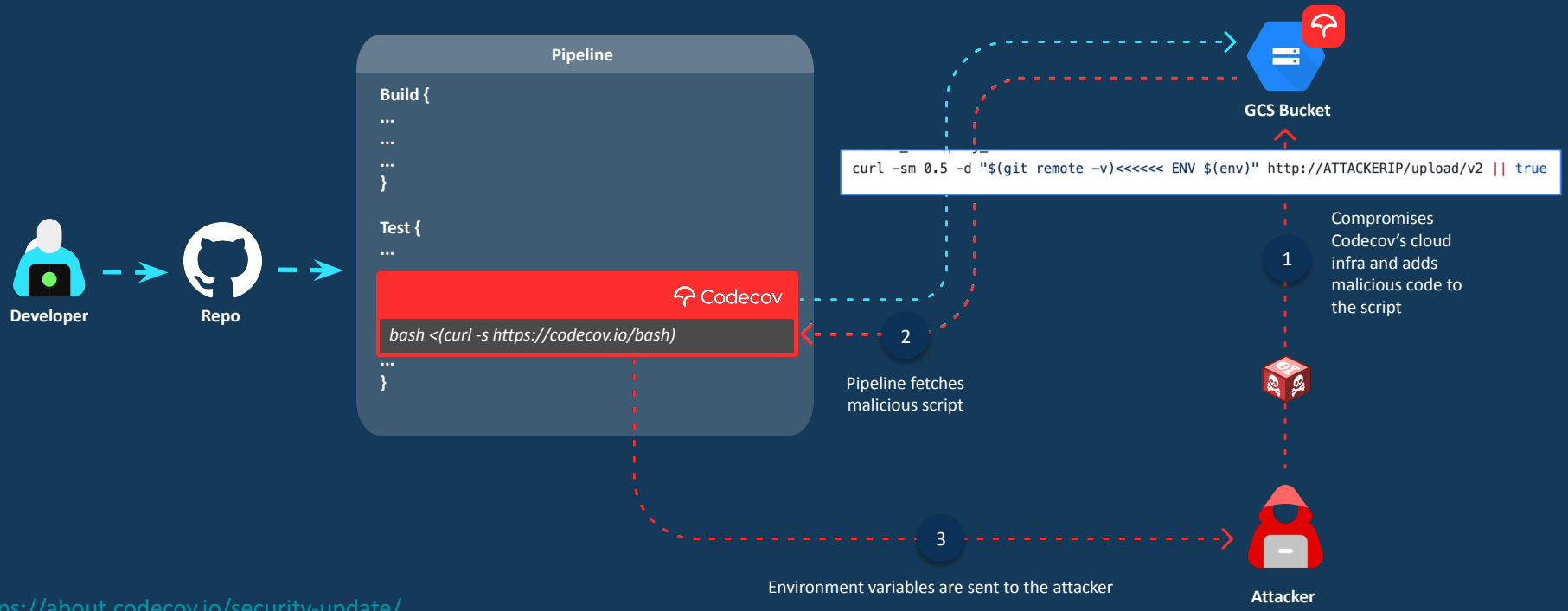
- Self-hosted SCM & CI exposed to the internet

Environment variables exfiltration through Codecov

Case Study #3

Cider

Environment variables exfiltration through Codecov

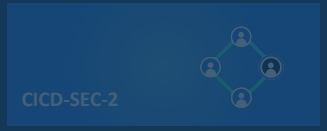


https://about.codecov.io/security-update/

Cider

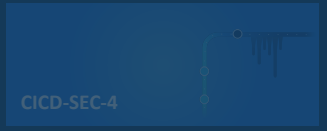
Top 10 CI/CD Security Risks

Insufficient Flow Control Mechanisms



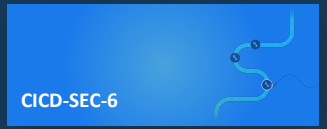
Inadequate Identity and Access Management

Dependency Chain Abuse



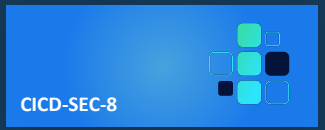
Poisoned Pipeline Execution (PPE)

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

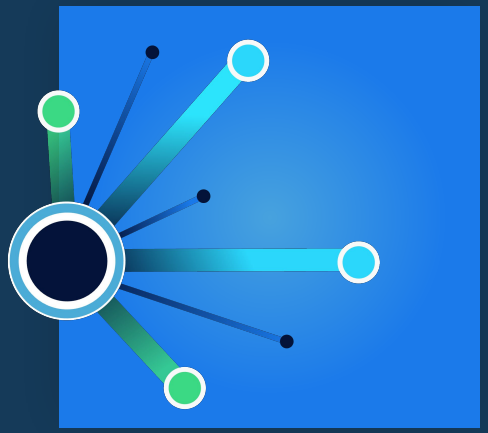
Cider

Insufficient PBAC (Pipeline-Based Access Controls)

CICD-SEC-5

Abusing the permission/access granted to the pipeline execution nodes for moving laterally within or outside the CI/CD system.

- Overly permissive pipeline execution environments

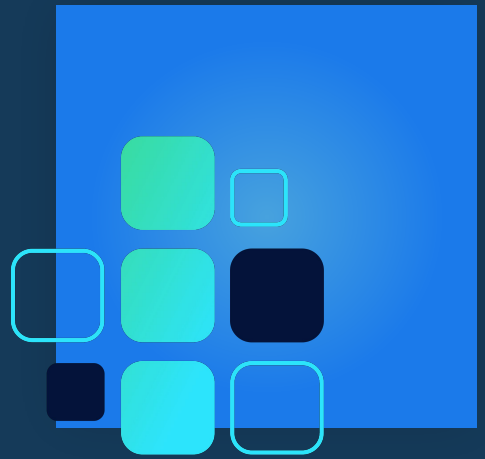


Cider

Ungoverned Usage of 3rd Party Services

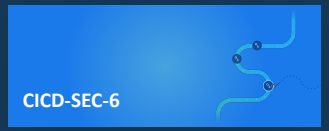
CICD-SEC-8

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.



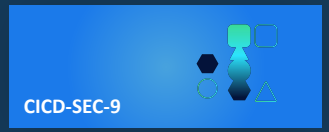
- Minimal investigative capabilities around existence/permissions of Codecov

Additional risks



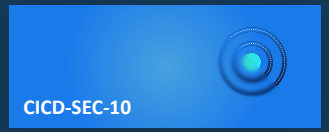
Insufficient Credential Hygiene

- Sensitive secrets stored as global environment variables



Improper Artifact Integrity Validation

- Integrity checks not performed prior to executing Codecov script



Insufficient Logging and Visibility

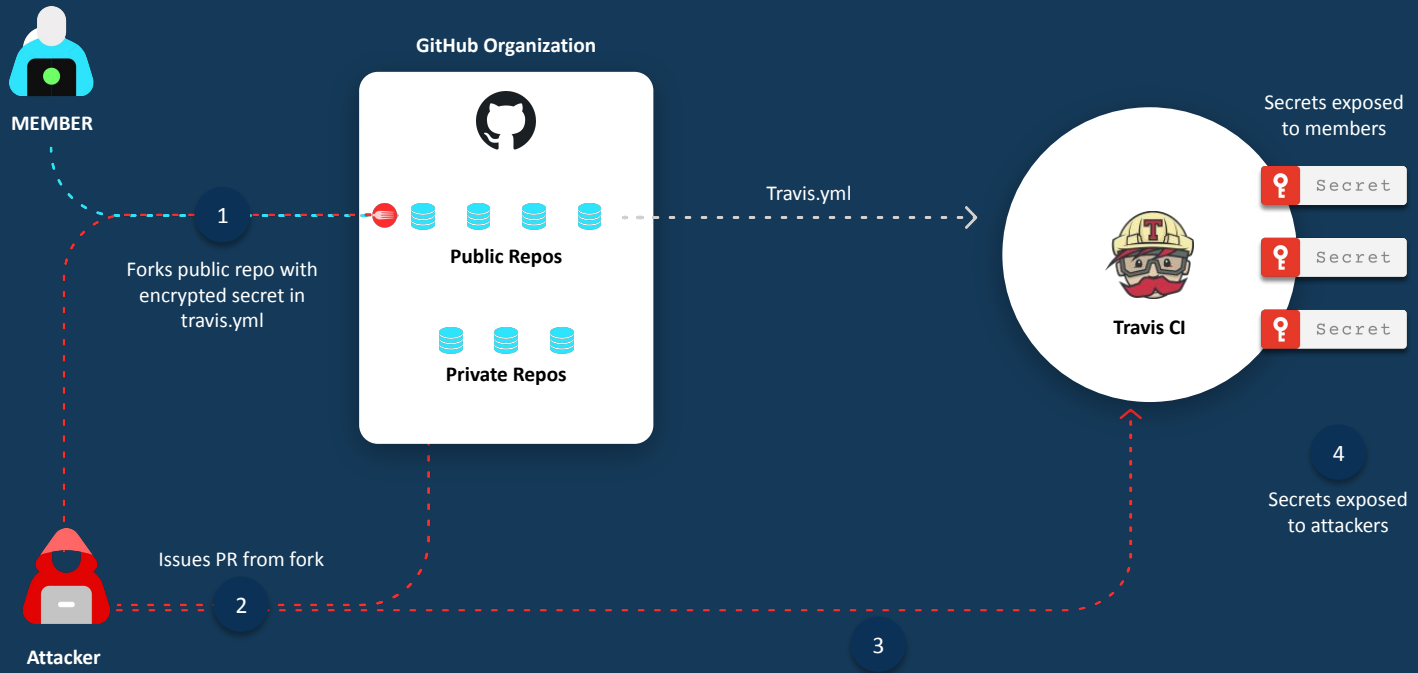
Cider

Travis CI secrets exposure

Case Study #4

Cider

Travis CI secrets exposure

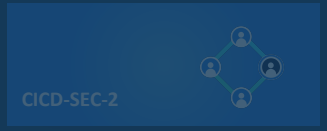


https://travis-ci.community/t/security-bulletin/12081

Cider

Top 10 CI/CD Security Risks

Insufficient Flow Control Mechanisms

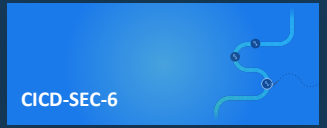


Inadequate Identity and Access Management

Dependency Chain Abuse

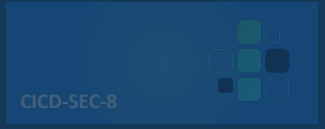
Poisoned Pipeline Execution (PPE)

Insufficient PBAC (Pipeline-Based Access Controls)

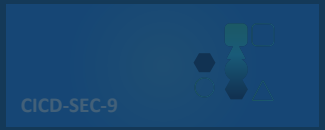


Insufficient Credential Hygiene

Insecure System Configuration



Ungoverned Usage of 3rd Party Services



Improper Artifact Integrity Validation

Insufficient Logging and Visibility

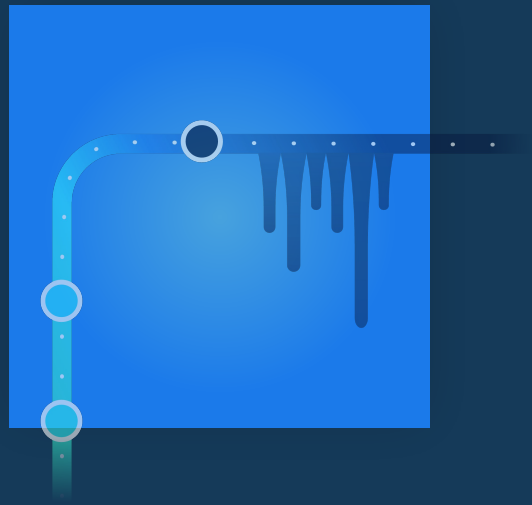
Cider

Poisoned Pipeline Execution (PPE)

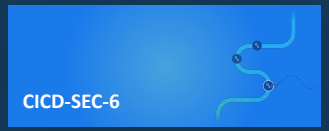
CICD-SEC-4

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

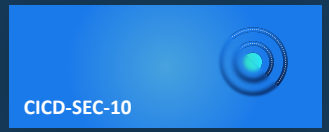


Additional risks



Insufficient Credential Hygiene

- Secrets the pipeline shouldn’t access
- Permissive credentials



Insufficient Logging and Visibility

- Identify potentially vulnerable repos
- Identify an actual breach

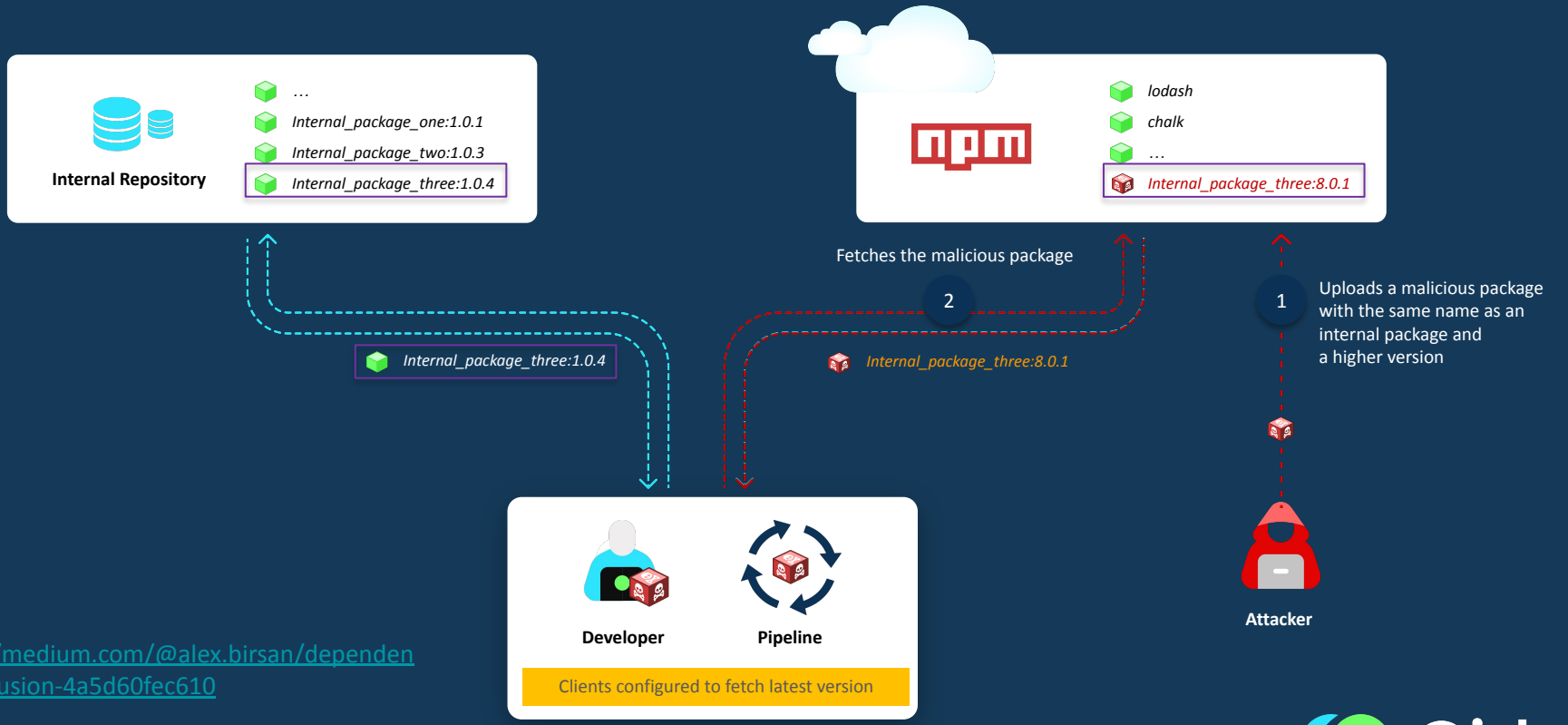
Cider

Dependency Confusion

Case Study #5

Cider

Dependency Confusion

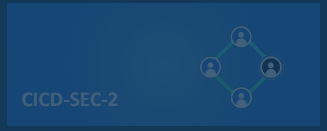


https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610

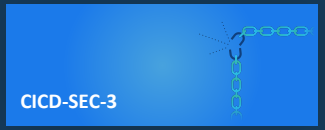
Cider

Top 10 CI/CD Security Risks

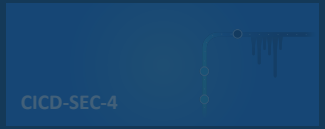
Insufficient Flow Control Mechanisms



Inadequate Identity and Access Management

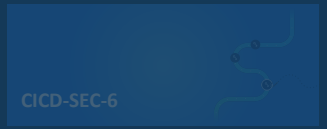


Dependency Chain Abuse



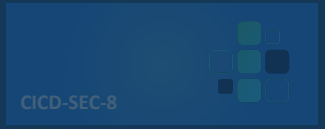
Poisoned Pipeline Execution (PPE)

Insufficient PBAC (Pipeline-Based Access Controls)

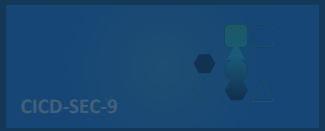


Insufficient Credential Hygiene

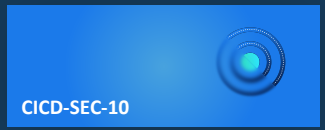
Insecure System Configuration



Ungoverned Usage of 3rd Party Services



Improper Artifact Integrity Validation



Insufficient Logging and Visibility

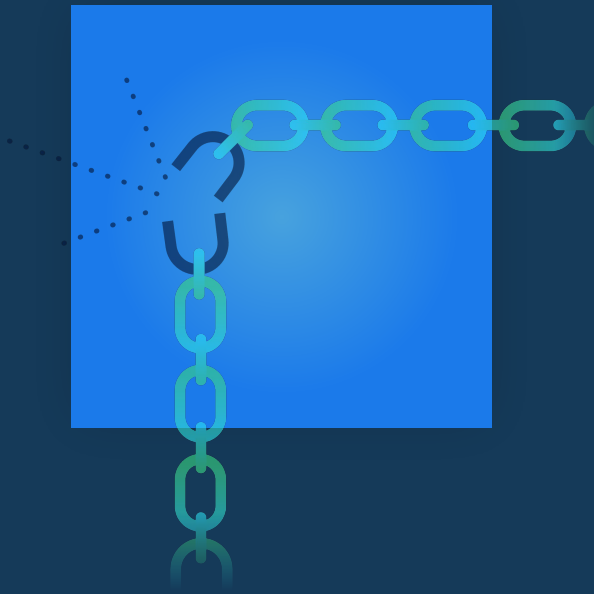
Cider

Dependency Chain Abuse

CICD-SEC-3

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

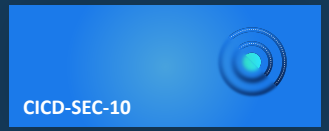
- Dependency confusion abuses the dependency chain by taking advantage of misconfigured package fetching processes



Cider

Additional Risks

Insufficient PBAC (Pipeline-Based Access Controls)



Insufficient Logging and Visibility

- Packages installed and executed on overly permissive execution nodes

Cider

Takeaways

- ## 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 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.

Thanks!

Daniel Krivelevich
Co-Founder & CTO
Cider Security

@dkrivelev

Omer Gil
Head Of Research
Cider Security

@omer_gil

Cider