

The 3 disciplines of CI/CD security



Daniel Krivelevich
Co-Founder & CTO
Cider Security



@dkrivelev



Intro



Daniel Krivelevich
Co-Founder & CTO
Cider Security
 @dkrivelev



CI/CD

Cyber

Catchy 5-letter word

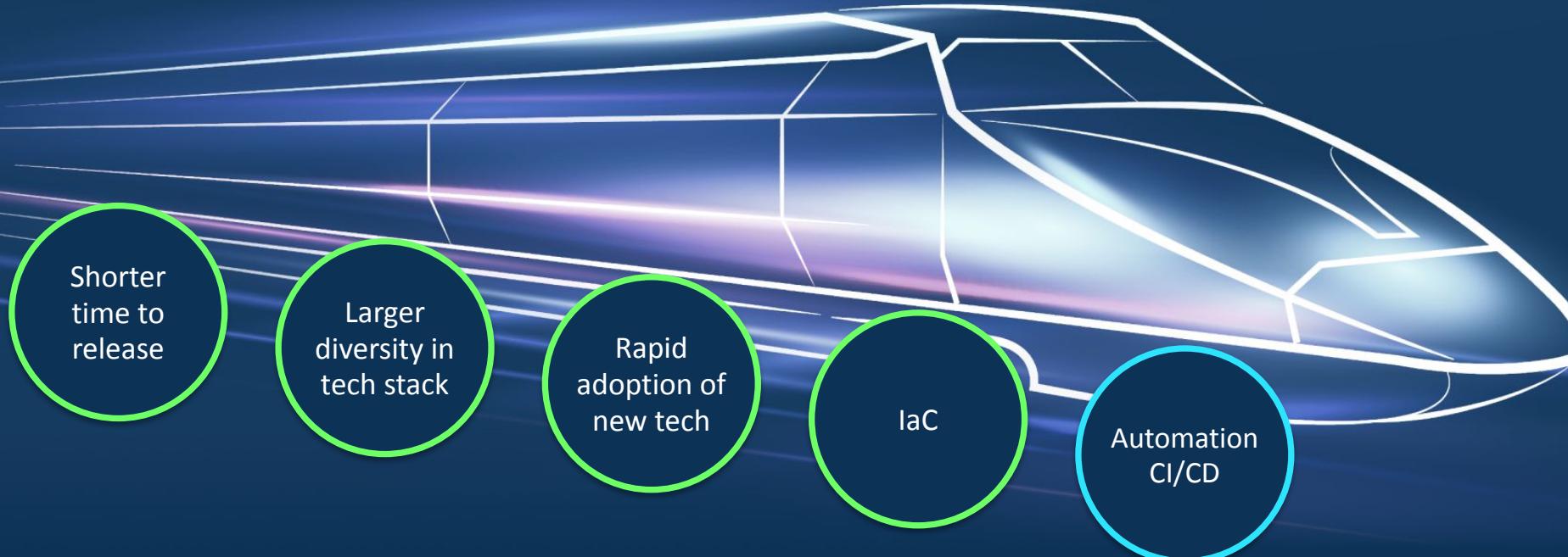
We like Cider





What does
CI/CD security
mean?

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

Monthly executions of CI/CD pipelines worldwide (Jenkins)



How well is security adapting to these changes?



The engineering ecosystem



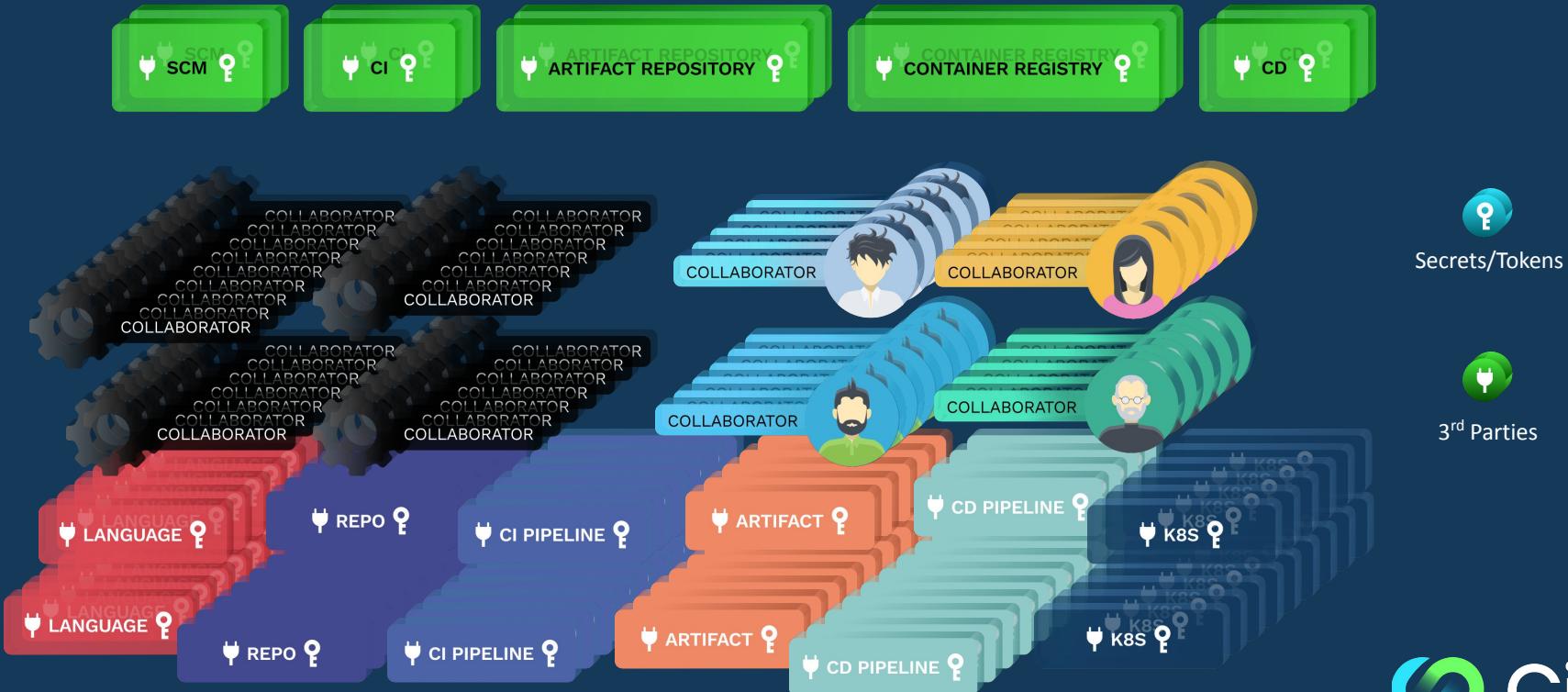
Secrets/Tokens



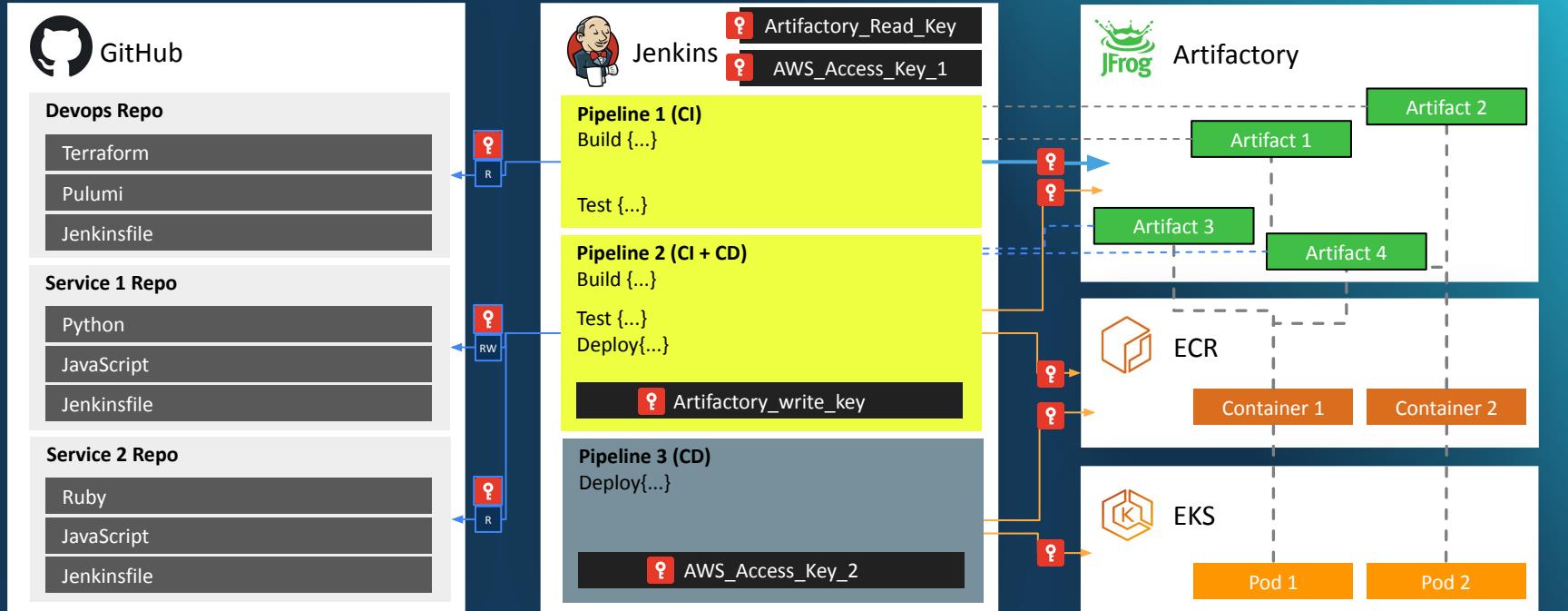
3rd Parties



The challenge



The Complexity



Mapping the environment

For Security, maneuvering through the engineering realm,

**Feels like walking
through New York with a
map of Tokyo**



Today's attack surface

- Engineering environments have become **the new attacker's turf**



- **A single insecure step in the CI, or insecure package import** - can lead to devastating results
- Engineers are also looking for ways to **bridge the gap**



CI/CD security: Adapting AppSec to the modern engineering environment

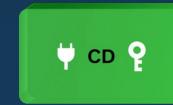
**allowing engineering to
continue to move fast
Without making any
compromises on Security**



SIP
SOP
SAP

SIP / SOP / SAP

Comprehensive Technical DNA of your environment -
from Code to Deployment



COLLABORATOR



COLLABORATOR



COLLABORATOR



COLLABORATOR



COLLABORATOR



COLLABORATOR



COLLABORATOR



COLLABORATOR



Secrets/Tokens



3rd Parties



SIP / SOP / SAP

Comprehensive Technical DNA of your environment - from Code to Deployment



SIP / SOP / SAP

Comprehensive Technical DNA of your environment -
from Code to Deployment

SIP

Security In the Pipeline

Addresses the risk of code
with security flaws flowing
through the pipeline

SIP - Security In the Pipeline



GitHub

Devops Repo

Terraform

Pulumi

Jenkinsfile

Service 1 Repo

Python

JavaScript

Jenkinsfile

Service 2 Repo

Ruby

JavaScript

Jenkinsfile



Gitlab

Devops Repo

Ansible

Chef

Jenkinsfile

Service 3 Repo

Python

JavaScript

Service 4 Repo

Go

JavaScript



BANDIT



BRAKEMAN

checkov
by bridgecrew

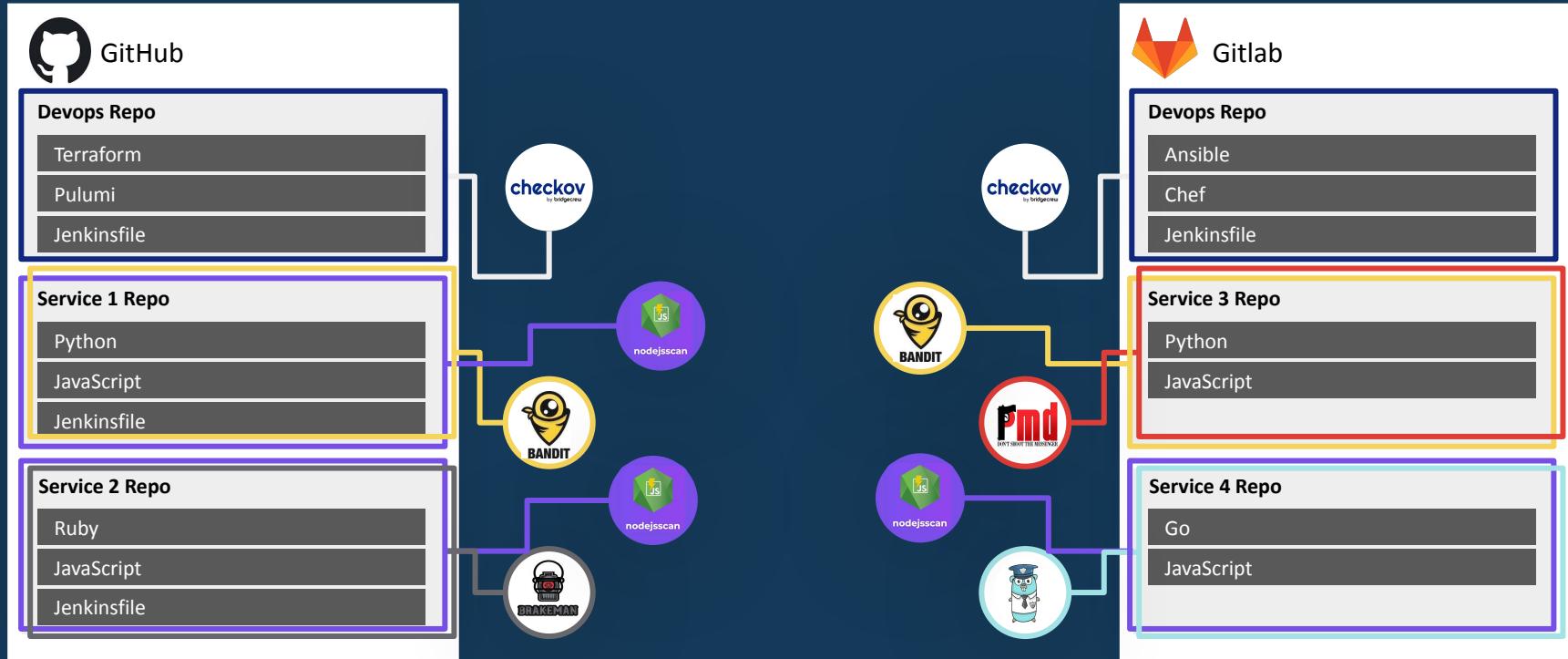


DON'T SHOOT THE MESSENGER



nodejsscan

SIP - Security In the Pipeline



Scanner	Issue	Description	Severity	Repo	Location
Checkov	Bad Stuff	Extremely Bad		Repo 1	Line 01
GoSec	Bad Stuff	Horrible		Repo 1	Line 01
Bandit	Bad Stuff	Very Severe		Repo 1	Line 01
Brakeman	Bad Stuff	Not Good		Repo 1	Line 01
Checkov	Bad Stuff	Fix Now		Repo 1	Line 01
PMD	Bad Stuff	Fix Fast		Repo 1	Line 01
Nodejsscan	Bad Stuff	So So		Repo 1	Line 01
Nodejsscan	Bad Stuff	Doing O.k.		Repo 1	Line 01

SIP / SOP / SAP

Comprehensive Technical DNA of your environment -
from Code to Deployment

SIP

Security In the Pipeline

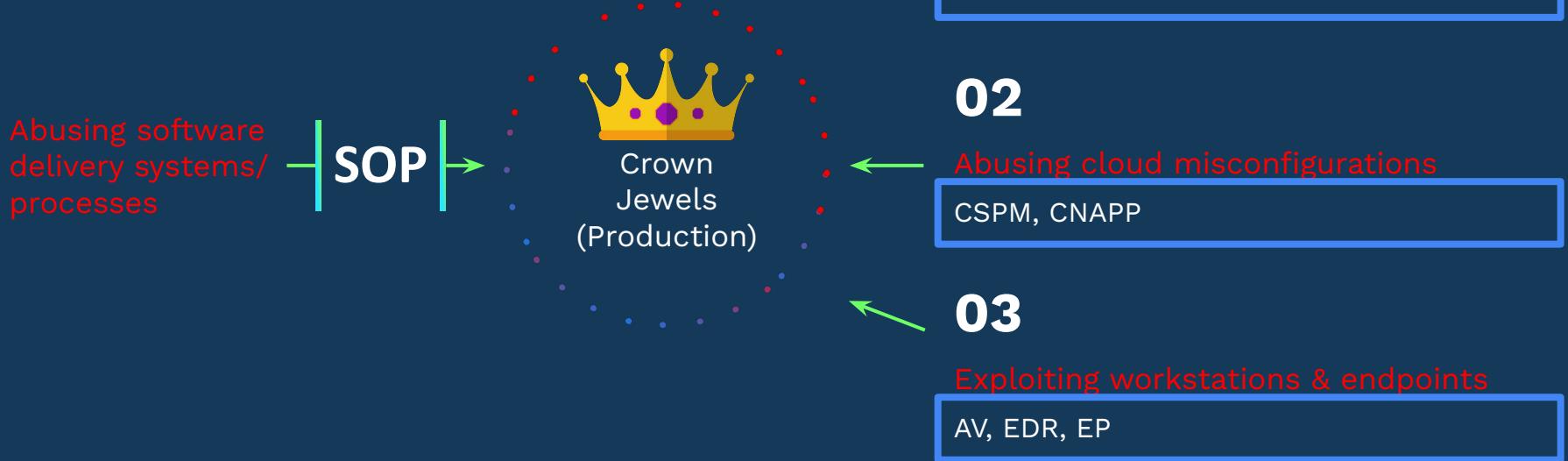
Addresses the risk of code with security flaws flowing through the pipeline

SOP

Security Of the Pipeline

Addresses the risk of the systems in the pipeline being compromised

SOP - Security Of the Pipeline



SIP / SOP / SAP

Comprehensive Technical DNA of your environment -
from Code to Deployment

SIP

Security In the Pipeline

Addresses the risk of code
with security flaws flowing
through the pipeline

SOP

Security Of the Pipeline

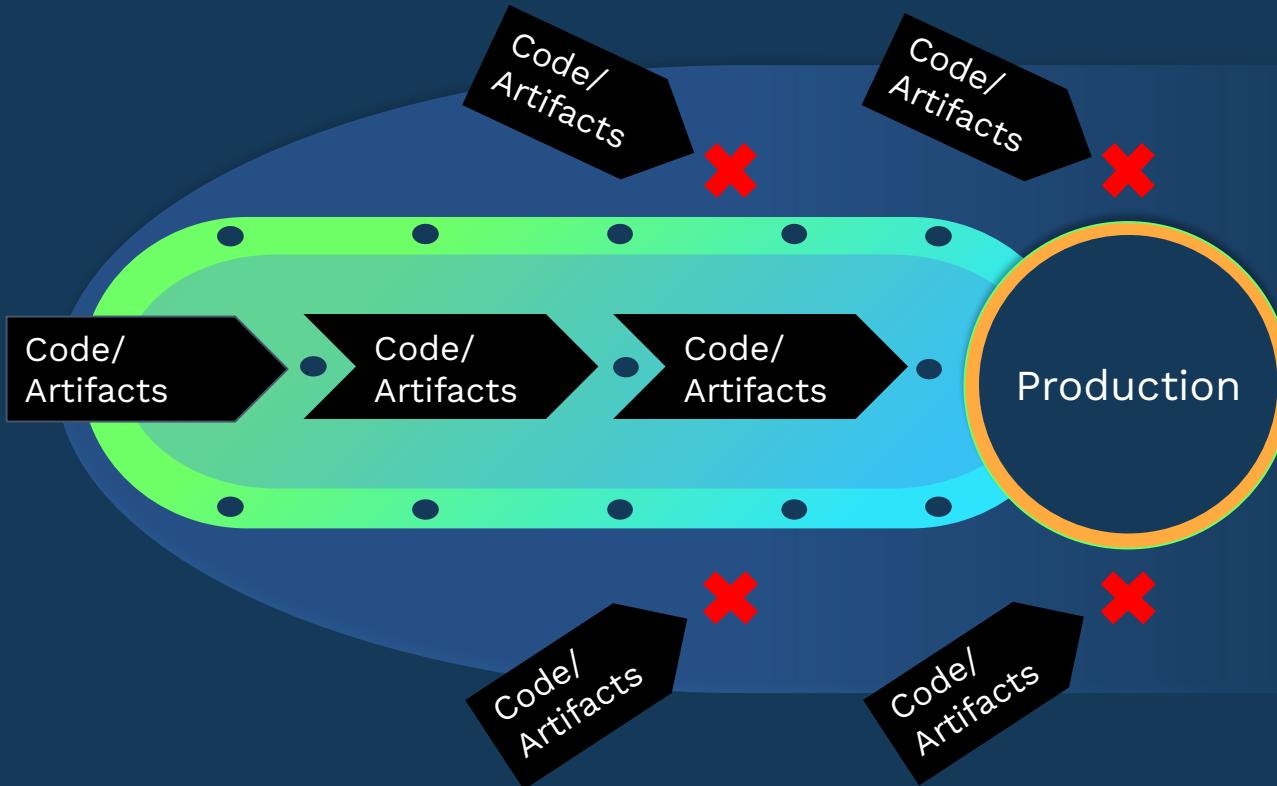
Addresses the risk of the
systems in the pipeline being
compromised

SAP

Security Around the Pipeline

Addresses the risk of the
pipeline being bypassed

SAP - Security Around the Pipeline



SIP / SOP / SAP

Comprehensive Technical DNA of your environment -
from Code to Deployment

SIP

Security In the Pipeline

Addresses the risk of code
with security flaws flowing
through the pipeline

SOP

Security Of the Pipeline

Addresses the risk of the
systems in the pipeline being
compromised

SAP

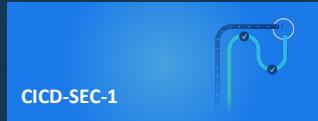
Security Around the Pipeline

Addresses the risk of the
pipeline being bypassed

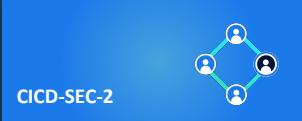


“Top 10 CI/CD Security Risks” initiative

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)



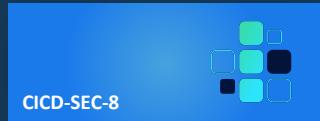
CICD-SEC-5
Insufficient PBAC (Pipeline-Based Access Controls)



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

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

Takeaways

SIP
SOP
SAP

Takeaway #1

For Defenders

The modern engineering environment requires a modern AppSec program

Appsec has extended far beyond the scope of code scanning.

To address today's challenges, we need to be thinking about SIP, SOP and SAP.

Takeaway #2

For Engineers

Bridging the gap between security and engineering requires an effort from both parties

Be patient with your AppSec teams.
We have a lot to catch up on.

Takeaway #3

For Hackers

You've done your fair share of damage for
2021/2022..

Take a break.



Thanks!



Daniel Krivelevich
Co-Founder & CTO
Cider Security

 @dkrivelev