Red Hat
Summit

Connect

DevSecOps

What does it mean for me as a developer?

Ben Taljaard
Solution Architect

Red Hat | intel.

About me

Ben Taljaard

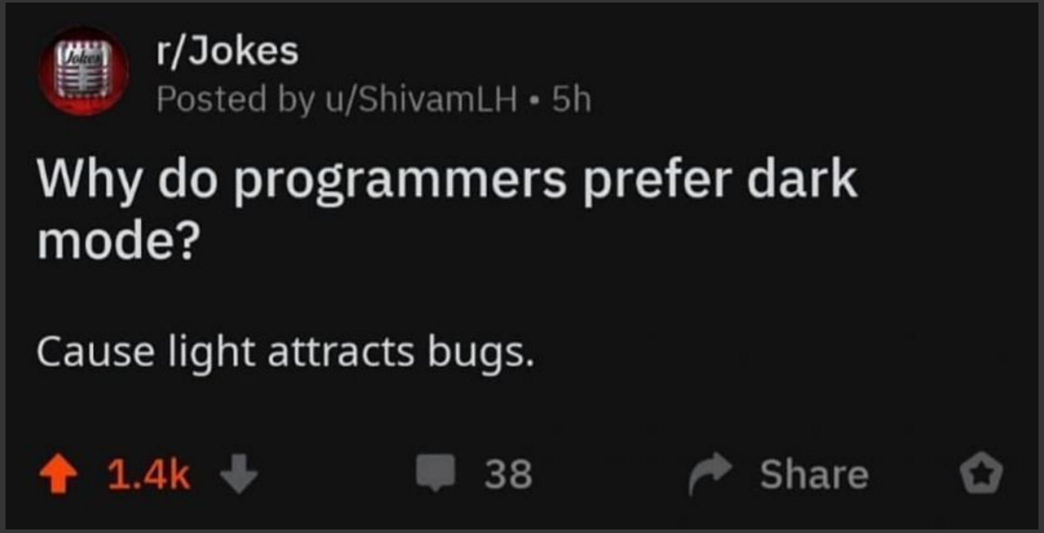
Based in Den Haag, Netherlands
Works for Red Hat
Role: Solution Architect

Self-professed technology geek, with a passion for cloud native application development

Hobbies: Playing guitar, tinkering in my workshop, helping my wife raise 2 boys

Email: ben.taljaard@redhat.com

#JoinTheDarkSide



r/Jokes

Posted by u/ShivamLH • 5h

Why do programmers prefer dark mode?

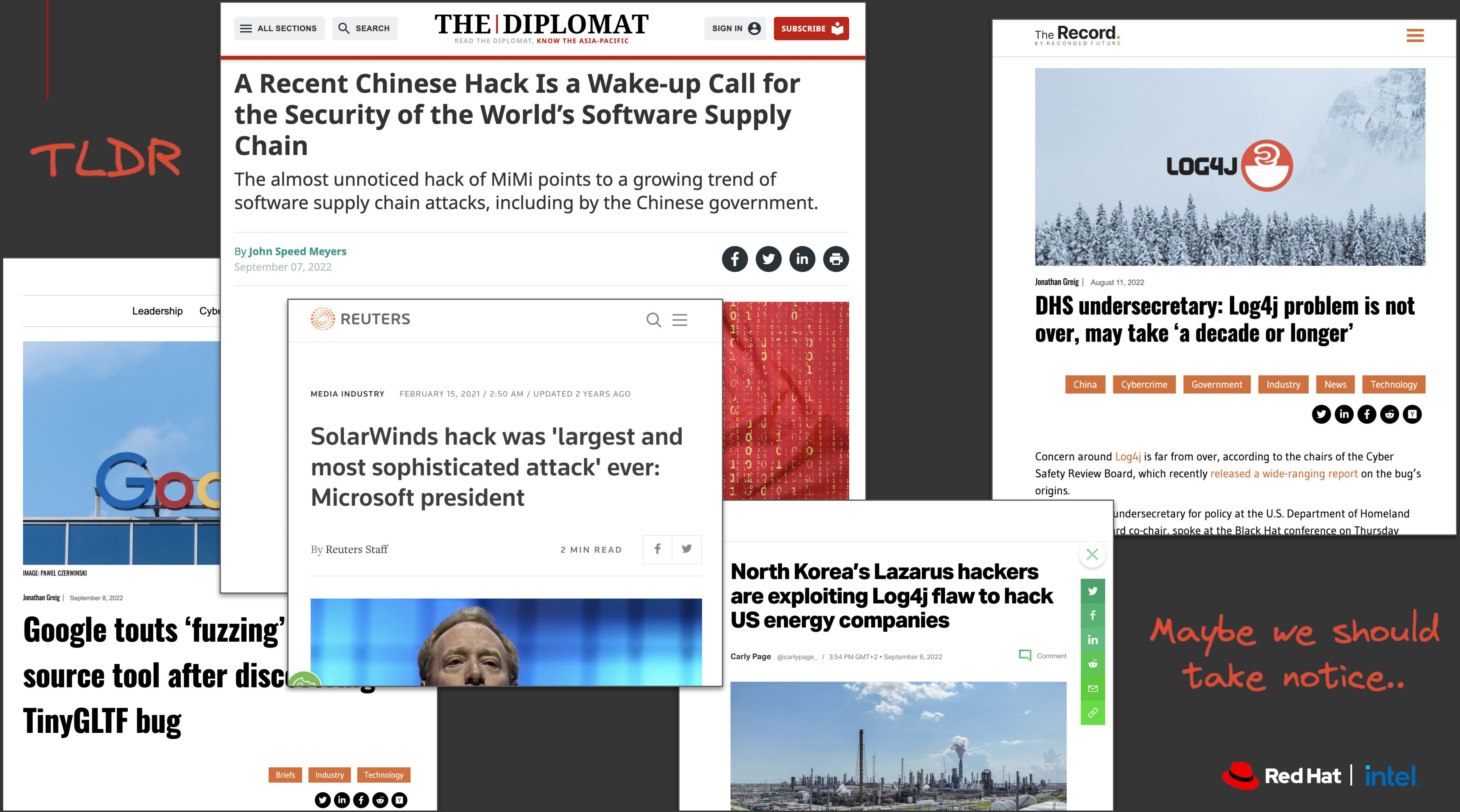
Cause light attracts bugs.

How many of you develop code?

How many of you do DevOps?

How many of you check for security issues in your code?

TLDR



THE DIPLOMAT
READ THE DIPLOMAT, KNOW THE ASIA-PACIFIC

A Recent Chinese Hack Is a Wake-up Call for the Security of the World's Software Supply Chain

The almost unnoticed hack of MiMi points to a growing trend of software supply chain attacks, including by the Chinese government.

By John Speed Meyers
September 07, 2022

IMAGE: PAWEL CZERWINSKI

Jonathan Greig | September 8, 2022

Google touts 'fuzzing' source tool after disc TinyGLTF bug

Briefs Industry Technology

REUTERS

MEDIA INDUSTRY FEBRUARY 15, 2021 / 2:50 AM / UPDATED 2 YEARS AGO

SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president

By Reuters Staff 2 MIN READ

The Record. BY RECORDED FUTURE

Jonathan Greig | August 11, 2022

DHS undersecretary: Log4j problem is not over, may take 'a decade or longer'

China Cybercrime Government Industry News Technology

Concern around Log4j is far from over, according to the chairs of the Cyber Safety Review Board, which recently released a wide-ranging report on the bug's origins.

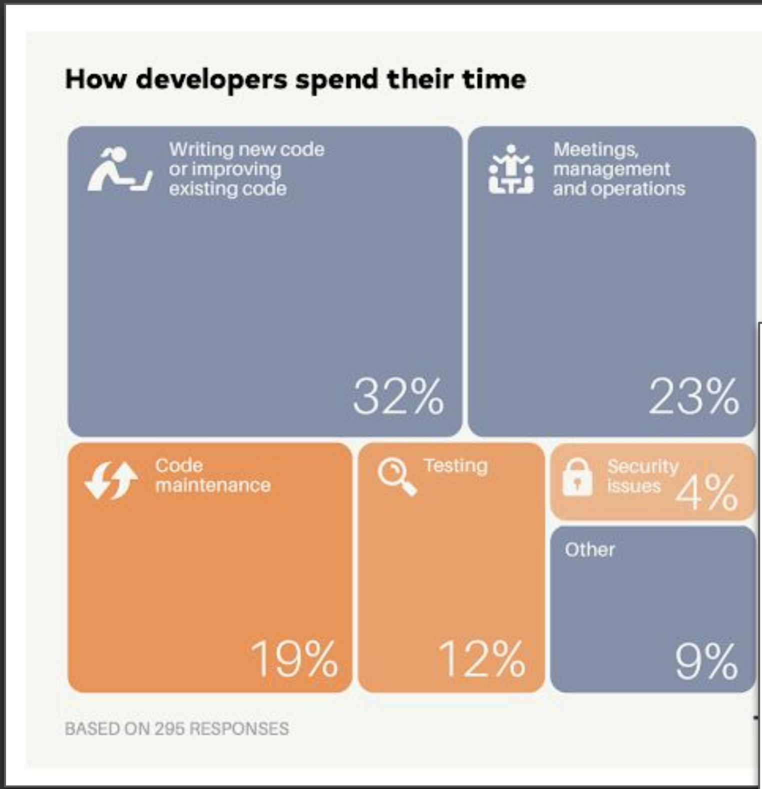
undersecretary for policy at the U.S. Department of Homeland rd co-chair, spoke at the Black Hat conference on Thursday

North Korea's Lazarus hackers are exploiting Log4j flaw to hack US energy companies

Carly Page @carlypage_ / 3:54 PM GMT+2 • September 8, 2022

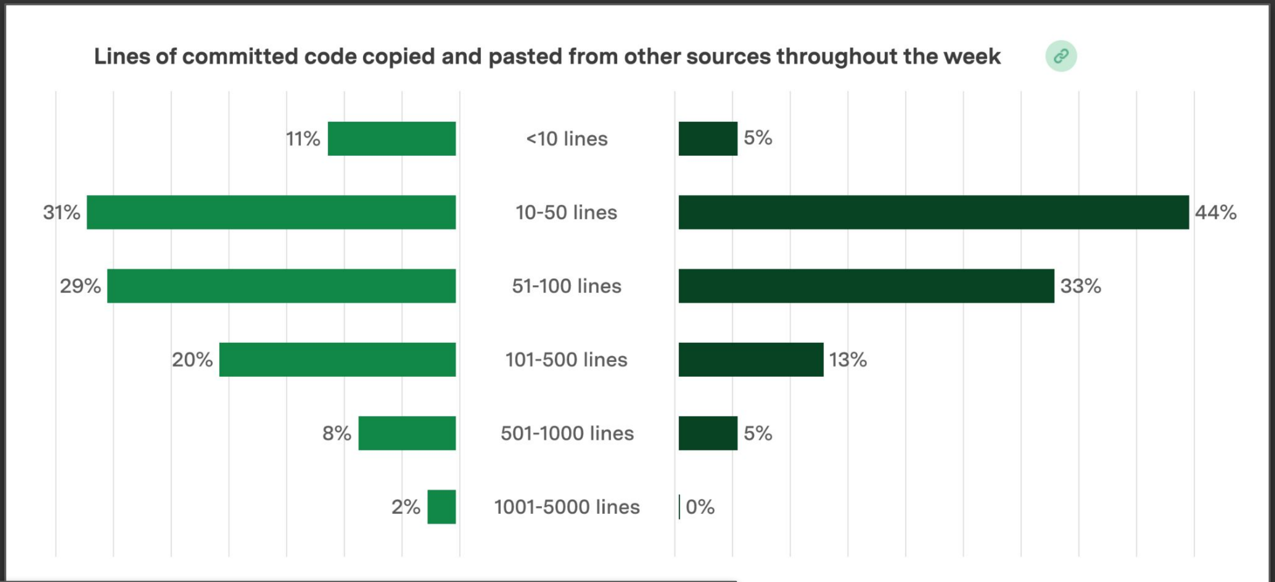
Maybe we should take notice..

What do developers spend their time on?

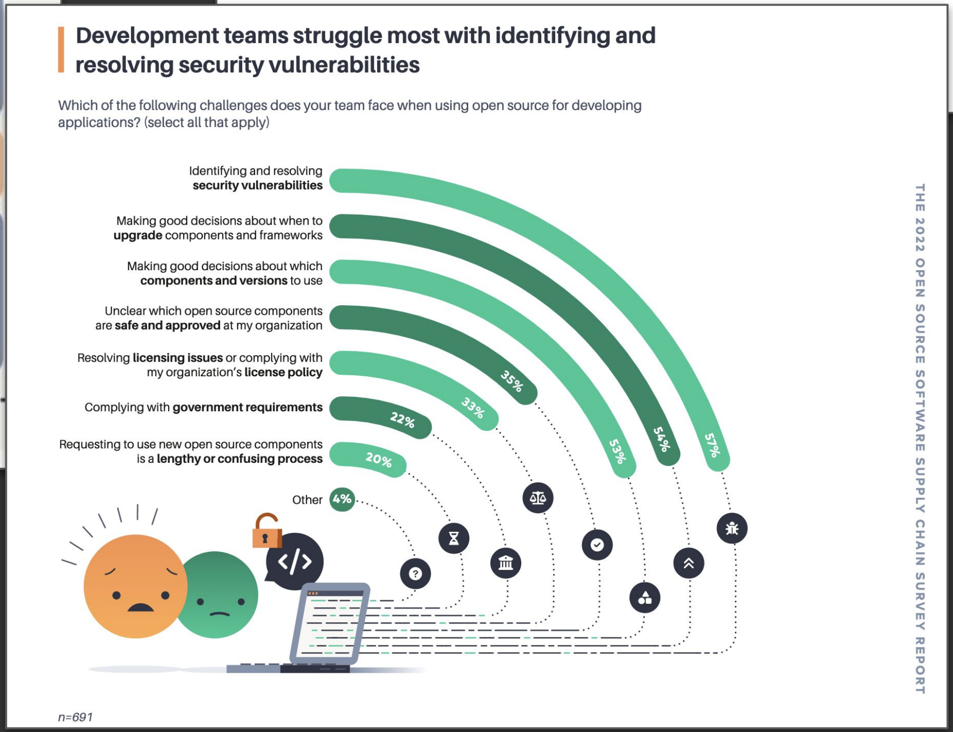


How developers spend their time

BASED ON 295 RESPONSES



Lines of committed code copied and pasted from other sources throughout the week



Development teams struggle most with identifying and resolving security vulnerabilities

Which of the following challenges does your team face when using open source for developing applications? (select all that apply)

n=691

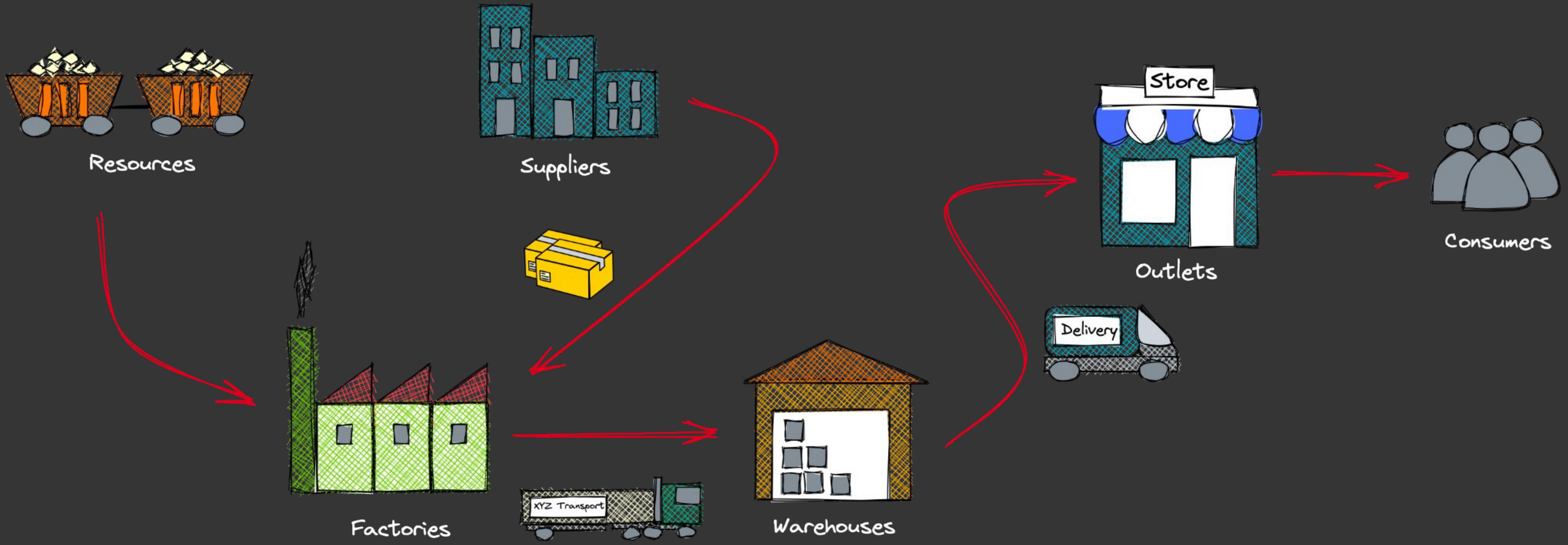
THE 2022 OPEN SOURCE SOFTWARE SUPPLY CHAIN SURVEY REPORT

Should we maybe think about things differently?

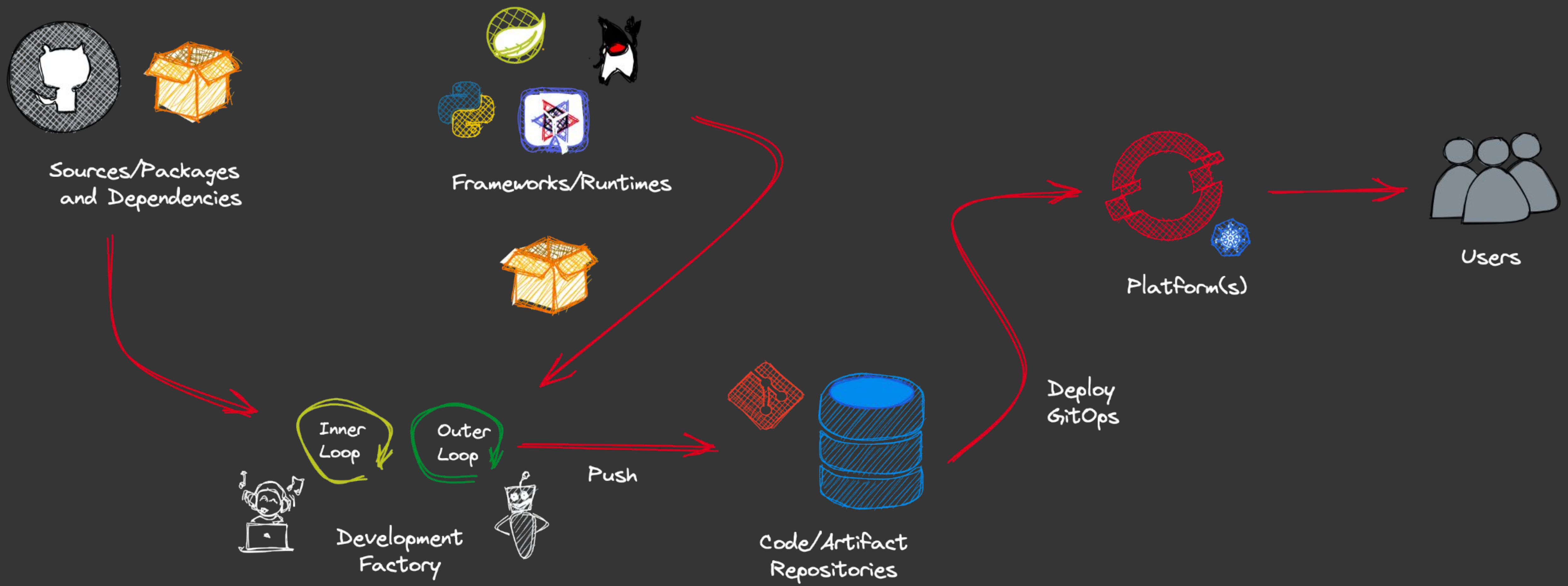
https://tidelift.com/subscription/managed-open-source-survey
https://retool.com/reports/state-of-engineering-time-2022/
https://explore.tidelift.com/survey-results/2022-open-source-software-supply-chain-survey

Why is security so important for me as a developer?

A Product Supply Chain

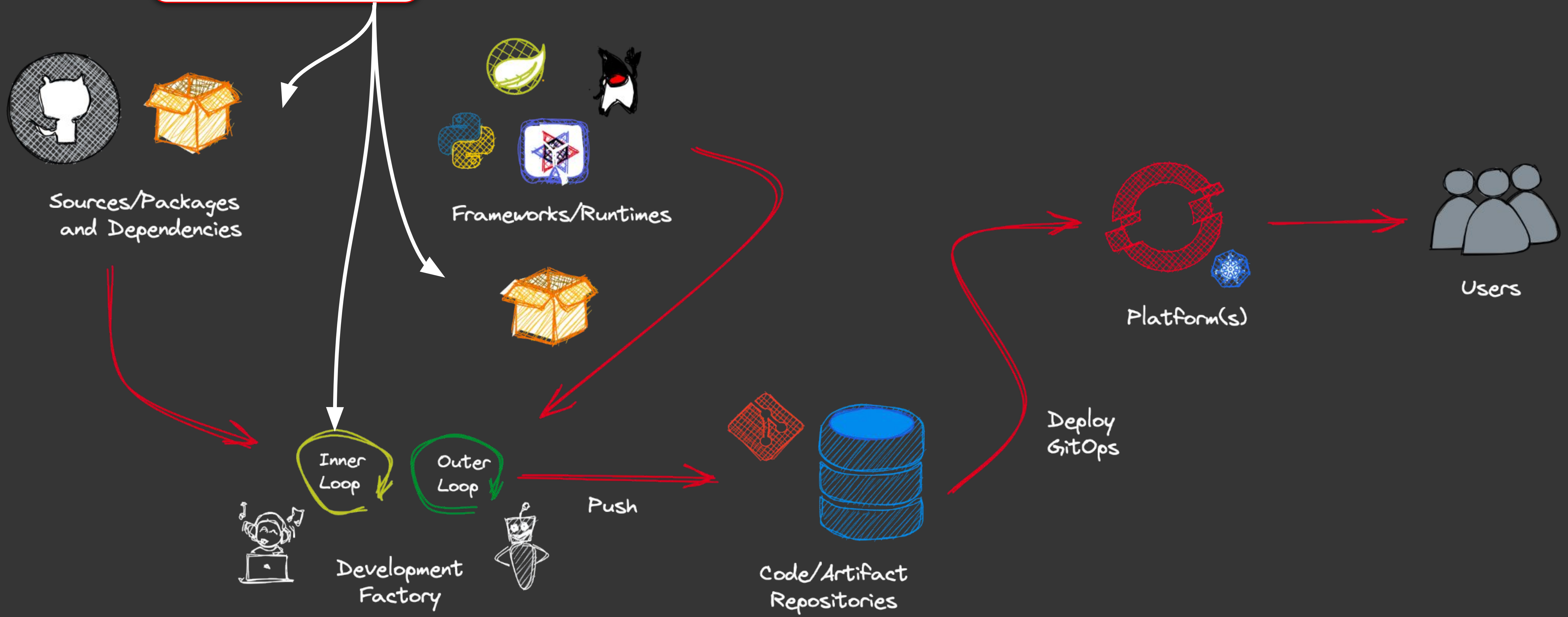


Software as a Product

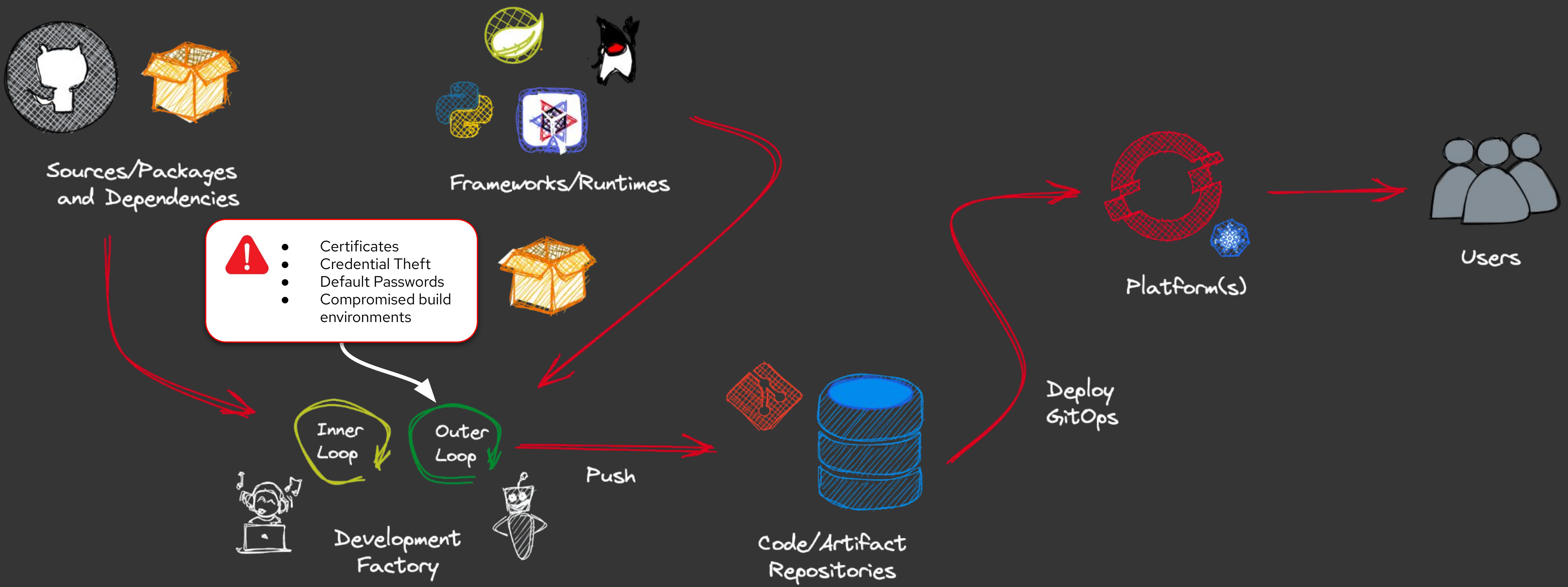


- Compromised Dependencies
- Malicious Code
- Vulnerable Code

Points of Compromise

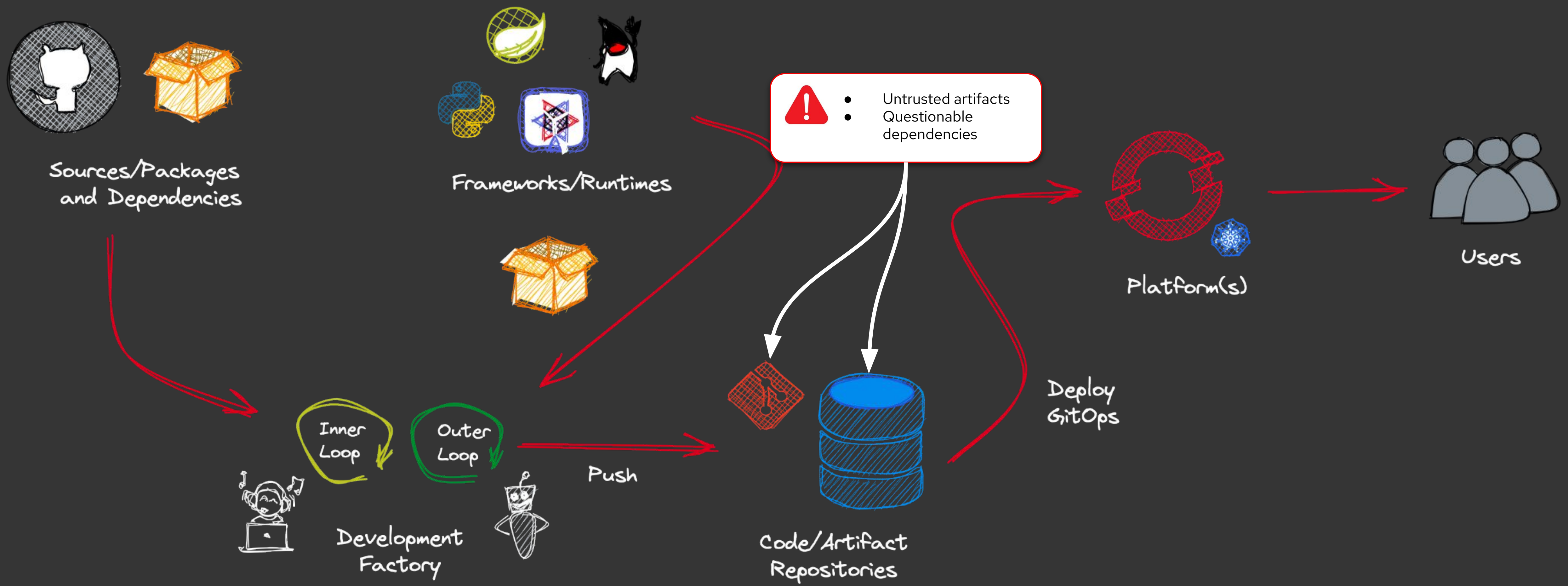


Points of Compromise



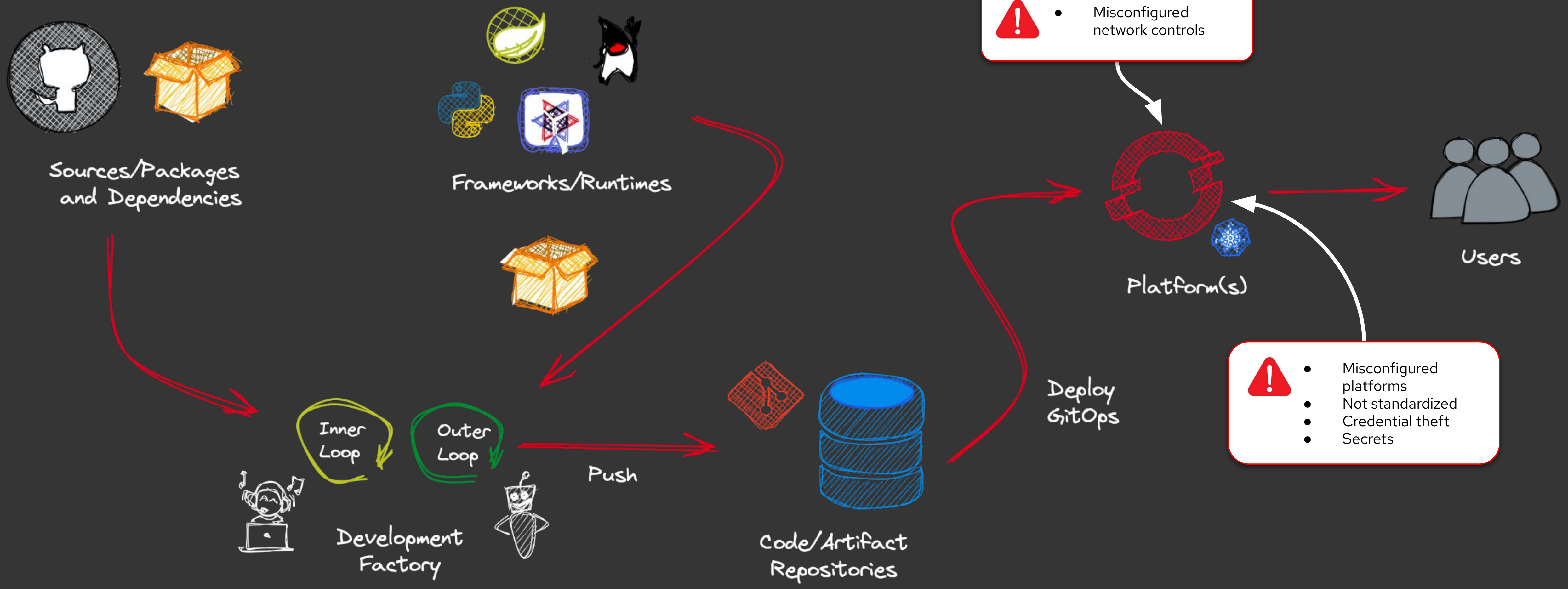
- Certificates
- Credential Theft
- Default Passwords
- Compromised build environments

Points of Compromise



- Untrusted artifacts
- Questionable dependencies

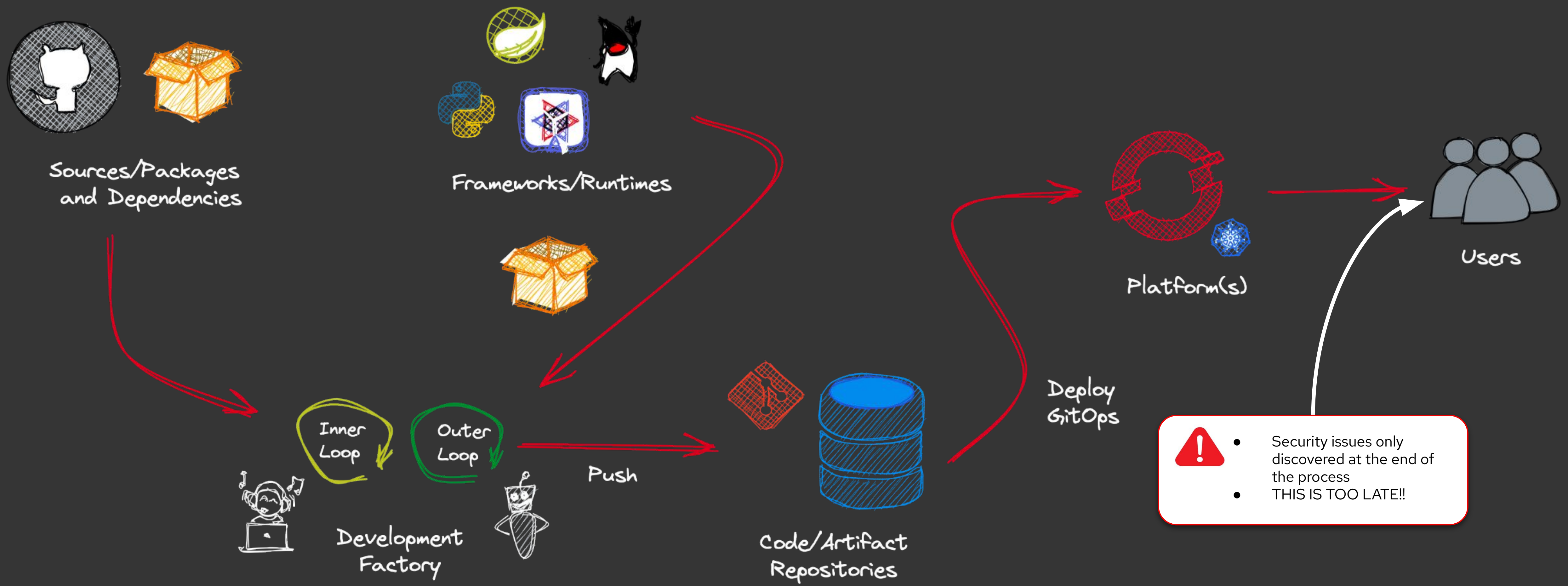
Points of Compromise



- Misconfigured network controls

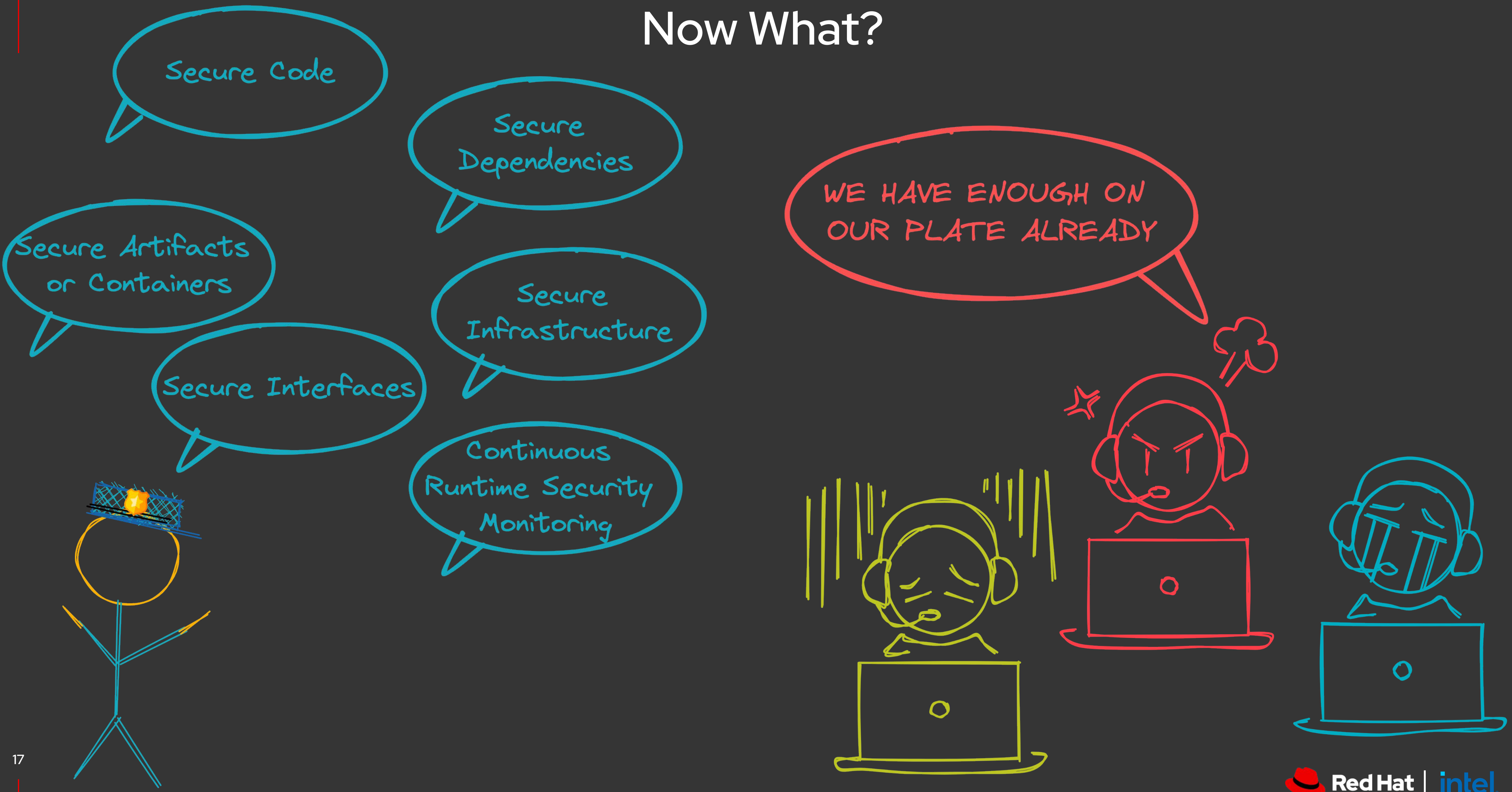
- Misconfigured platforms
- Not standardized
- Credential theft
- Secrets

Points of Compromise

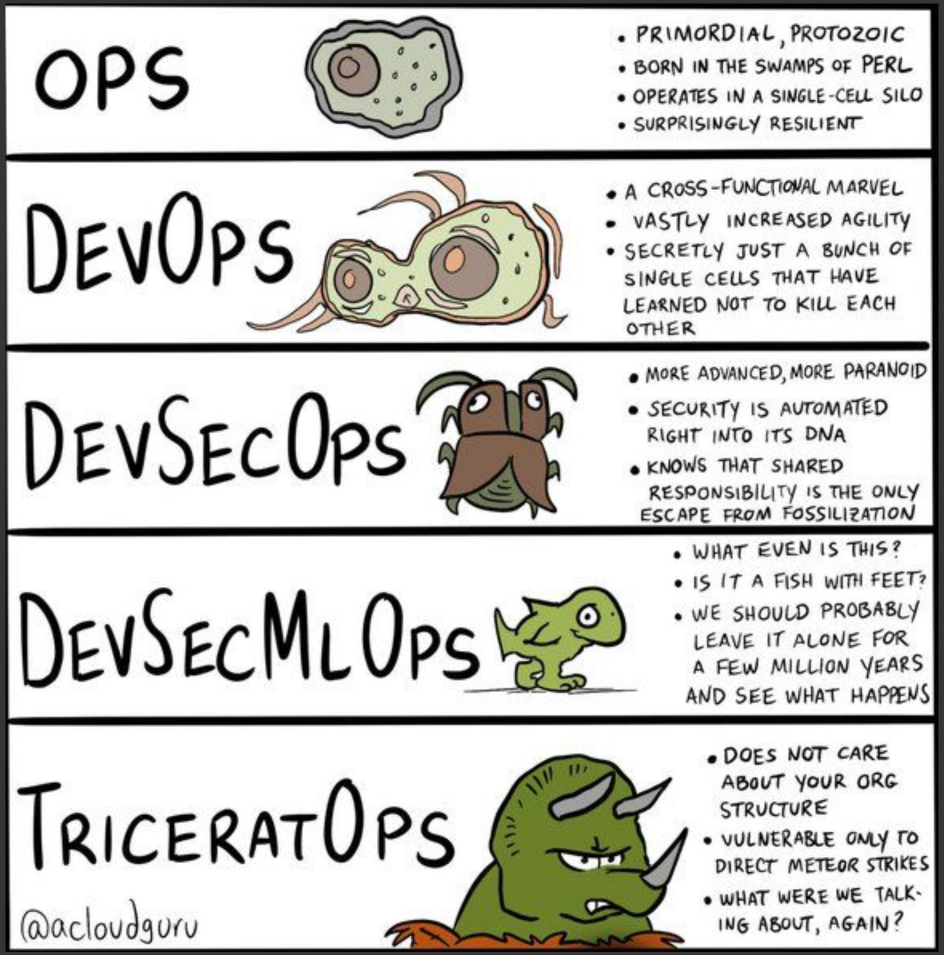


- Security issues only discovered at the end of the process
- THIS IS TOO LATE!!

Now What?

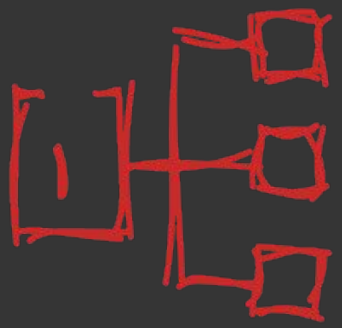

Secure Code
Secure Dependencies
Secure Artifacts or Containers
Secure Infrastructure
Secure Interfaces
Continuous Runtime Security Monitoring
WE HAVE ENOUGH ON OUR PLATE ALREADY

So, time to evolve...DevSecOps???

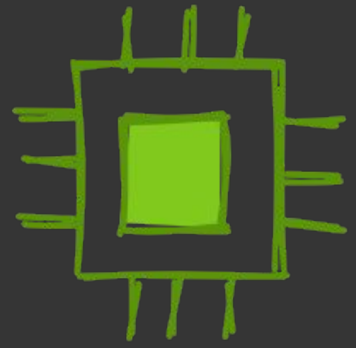

OPS
• PRIMORDIAL, PROTOZOIC
• BORN IN THE SWAMPS OF PERL
• OPERATES IN A SINGLE-CELL SILO
• SURPRISINGLY RESILIENT
DEVOPS
• A CROSS-FUNCTIONAL MARVEL
• VASTLY INCREASED AGILITY
• SECRETLY JUST A BUNCH OF SINGLE CELLS THAT HAVE LEARNED NOT TO KILL EACH OTHER
DEVSECOPS
• MORE ADVANCED, MORE PARANOID
• SECURITY IS AUTOMATED RIGHT INTO ITS DNA
• KNOWS THAT SHARED RESPONSIBILITY IS THE ONLY ESCAPE FROM FOSSILIZATION
DEVSECMLOPS
• WHAT EVEN IS THIS?
• IS IT A FISH WITH FEET?
• WE SHOULD PROBABLY LEAVE IT ALONE FOR A FEW MILLION YEARS AND SEE WHAT HAPPENS
TRICERATOPS
• DOES NOT CARE ABOUT YOUR ORG STRUCTURE
• VULNERABLE ONLY TO DIRECT METEOR STRIKES
• WHAT WERE WE TALKING ABOUT, AGAIN?
@acloudguru

No Really, DevSecOps

People



Process

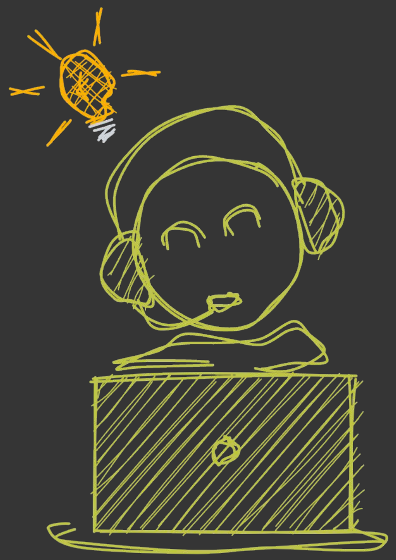


Technology

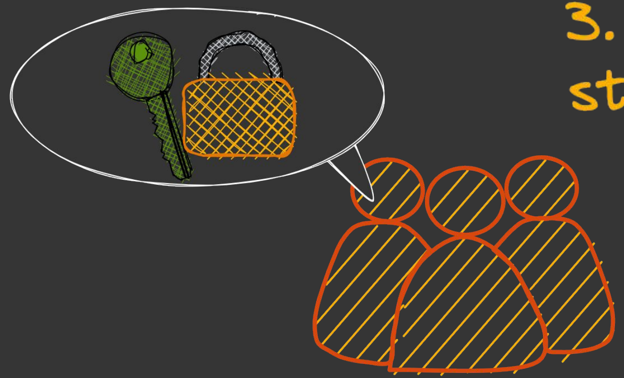
Doing DevSecOps

People

1. Set realistic goals, together

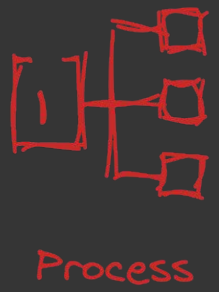


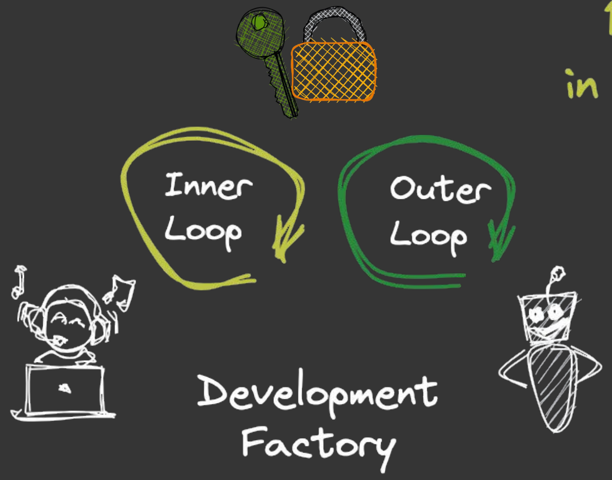
2. You code it, you own it



3. Integrate security staff into your team

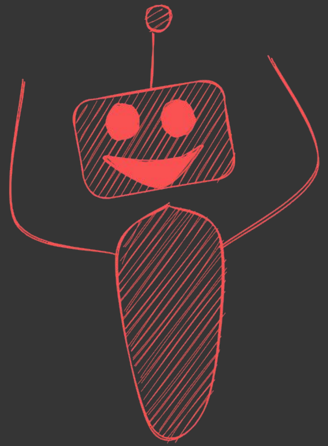
Doing DevSecOps





1. Integrate security in all phases of DevOps Lifecycle

3. Feedback Loops

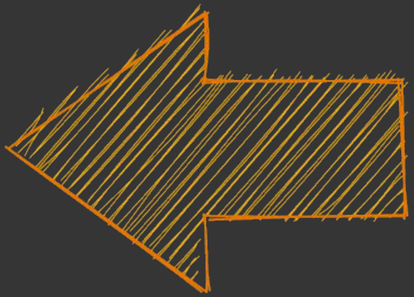


2. Automate Security, Compliance Testing

Doing DevSecOps

Technology

1. Tools should help you balance Speed, Accuracy, Efficiency



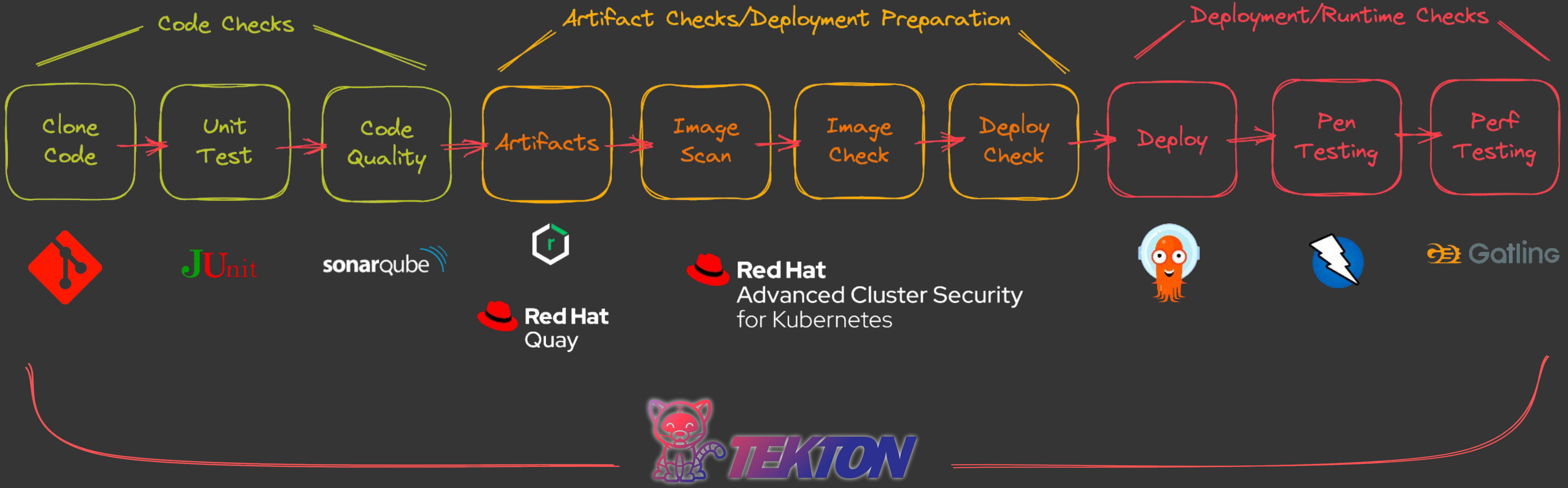
3. Shift Left

2. Single Source of Truth

Show me an example?

What does a secure pipeline look like?

Technology



Code Checks

Clone Code → Unit Test → Code Quality

Artifact Checks/Deployment Preparation

Artifacts → Image Scan → Image Check → Deploy Check

Deployment/Runtime Checks

Deploy → Pen Testing → Perf Testing

JUnit

sonarqube

Red Hat Quay

Red Hat Advanced Cluster Security for Kubernetes

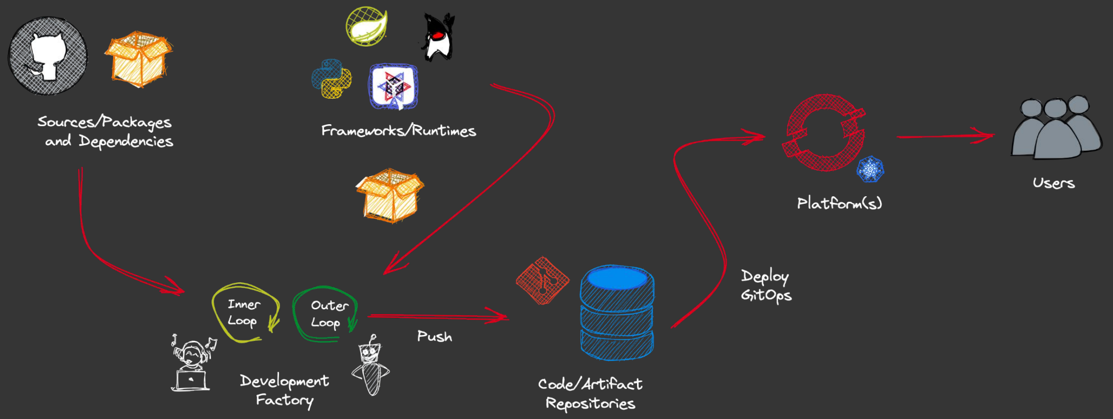
Gatling

TEKTON

What does this look like in real life?

You told me to shift-left?

Doing DevSecOps



1. Think about your whole software supply chain, from build to runtime

2. DevSecOps is more than just a tool or a team

Red Hat Summit

Connect

Thank you

in linkedin.com/company/red-hat

f facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat | intel.