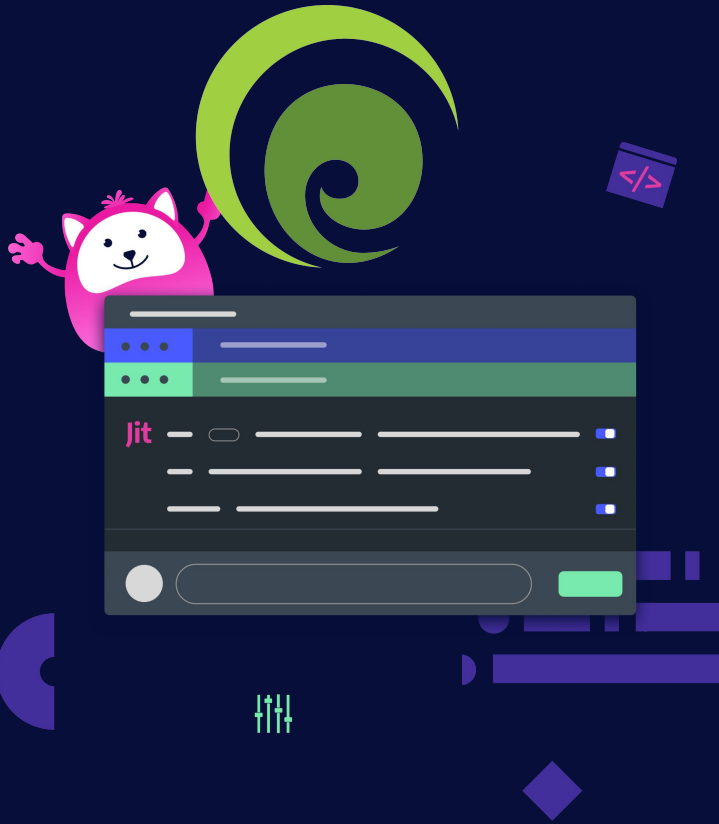
Jit

OWASP NEW ZEALAND DAY 2022



Minimum Viable Security

for Microservices

David Melamed, Co-Founder & CTO at Jit

7 July, 2022

Jit

I'm David Melamed

Co-Founder and CTO at Jit
Continuous Security Platform for Developers

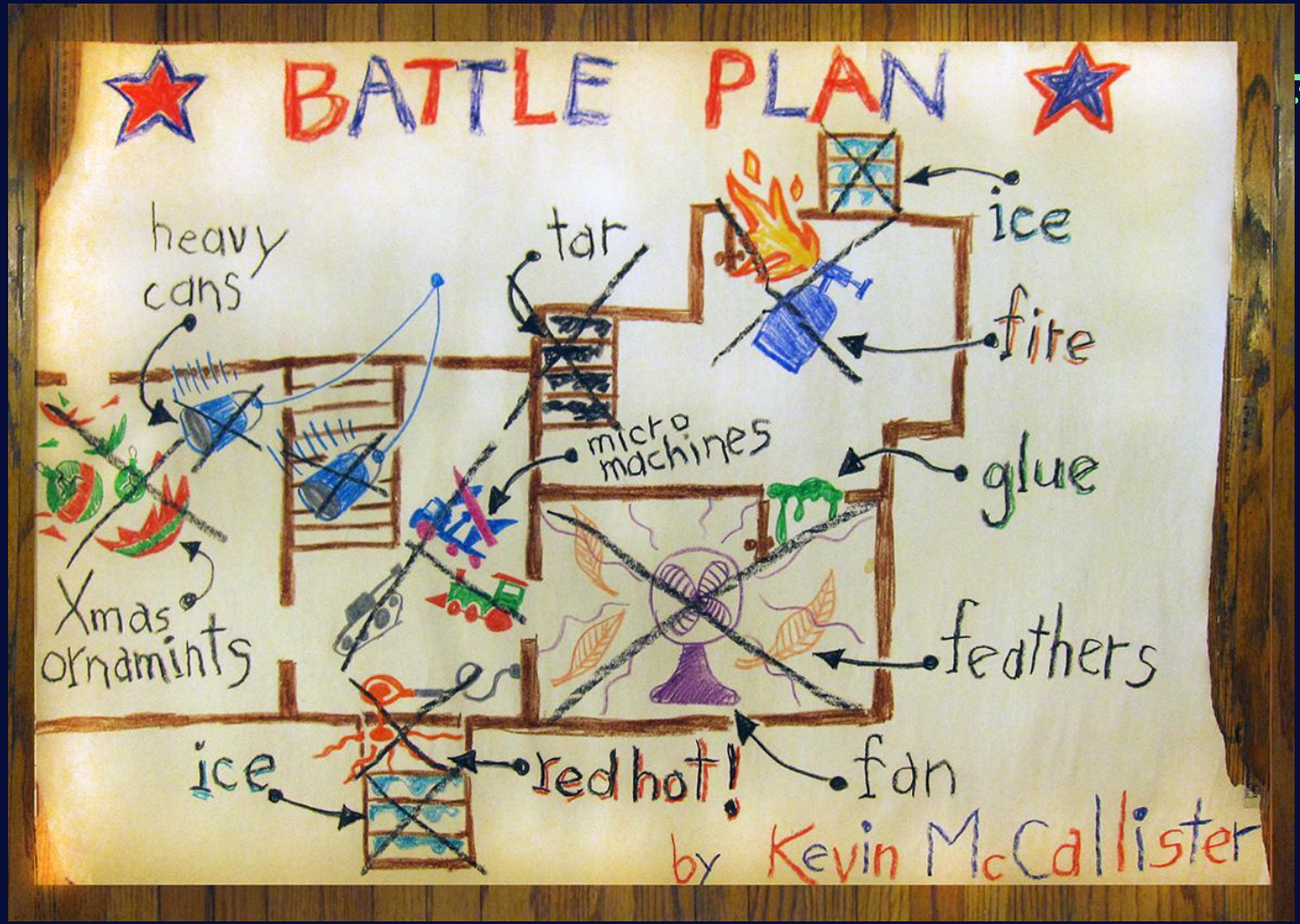
Tech & Automation Addict

@dvdmelamed

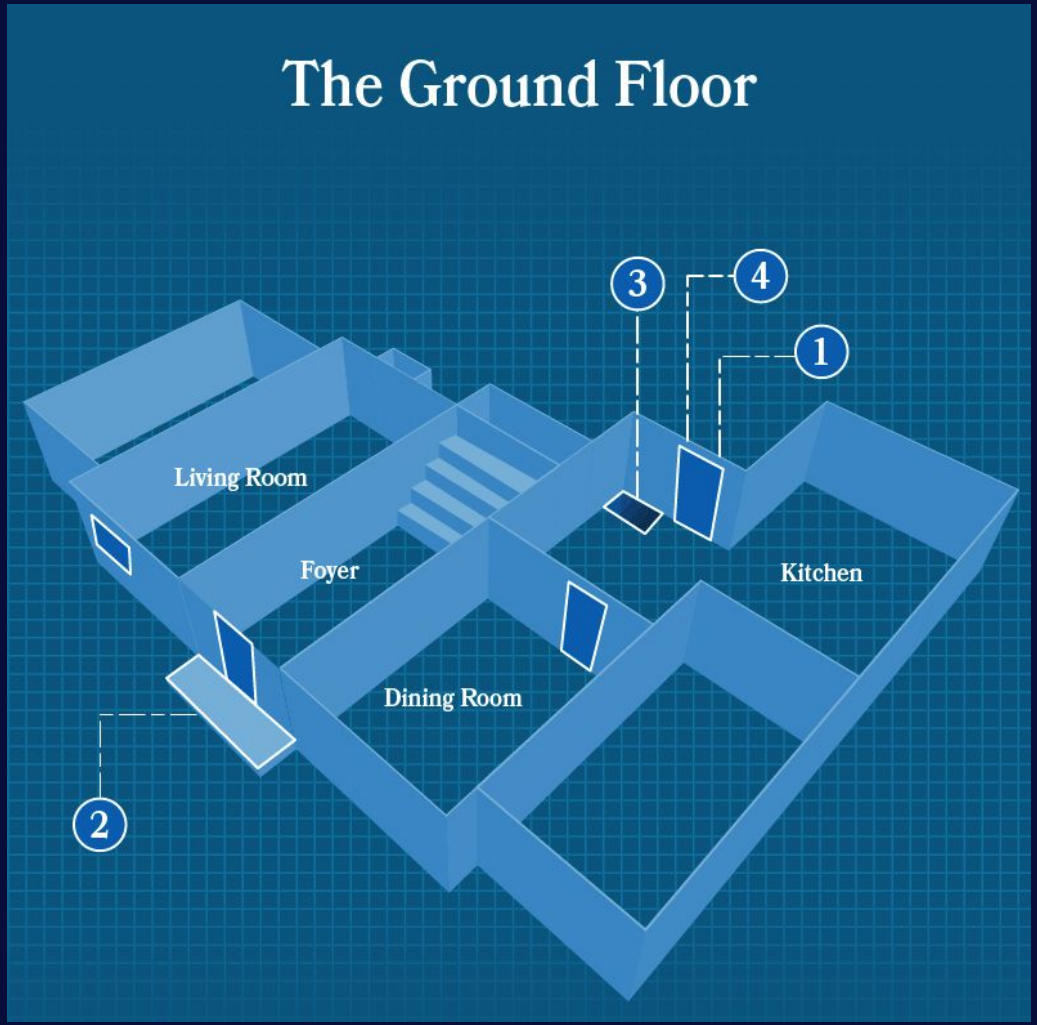
Jit

Source: https://visual.ly/community/Infographics/entertainment/protecting-your-house-home-alone-style

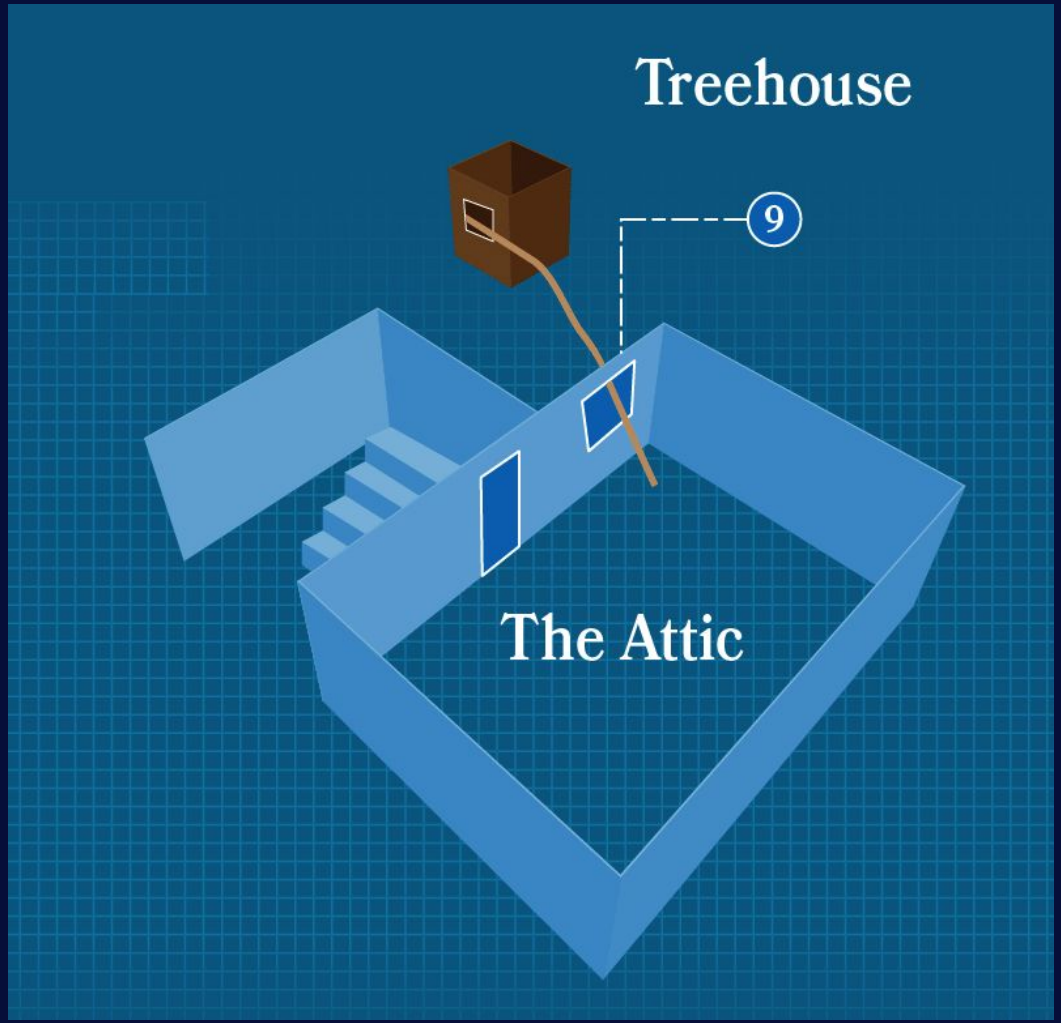
Jit

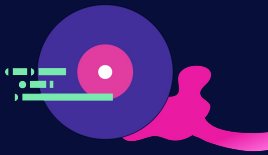

BATTLE PLAN
heavy cans
tar
ice
fire
micro machines
glue
Xmas ornamints
feathers
ice
red hot!
fan
by Kevin McCallister

Jit


The Ground Floor
3
4
1
Living Room
Foyer
Kitchen
Dining Room
2

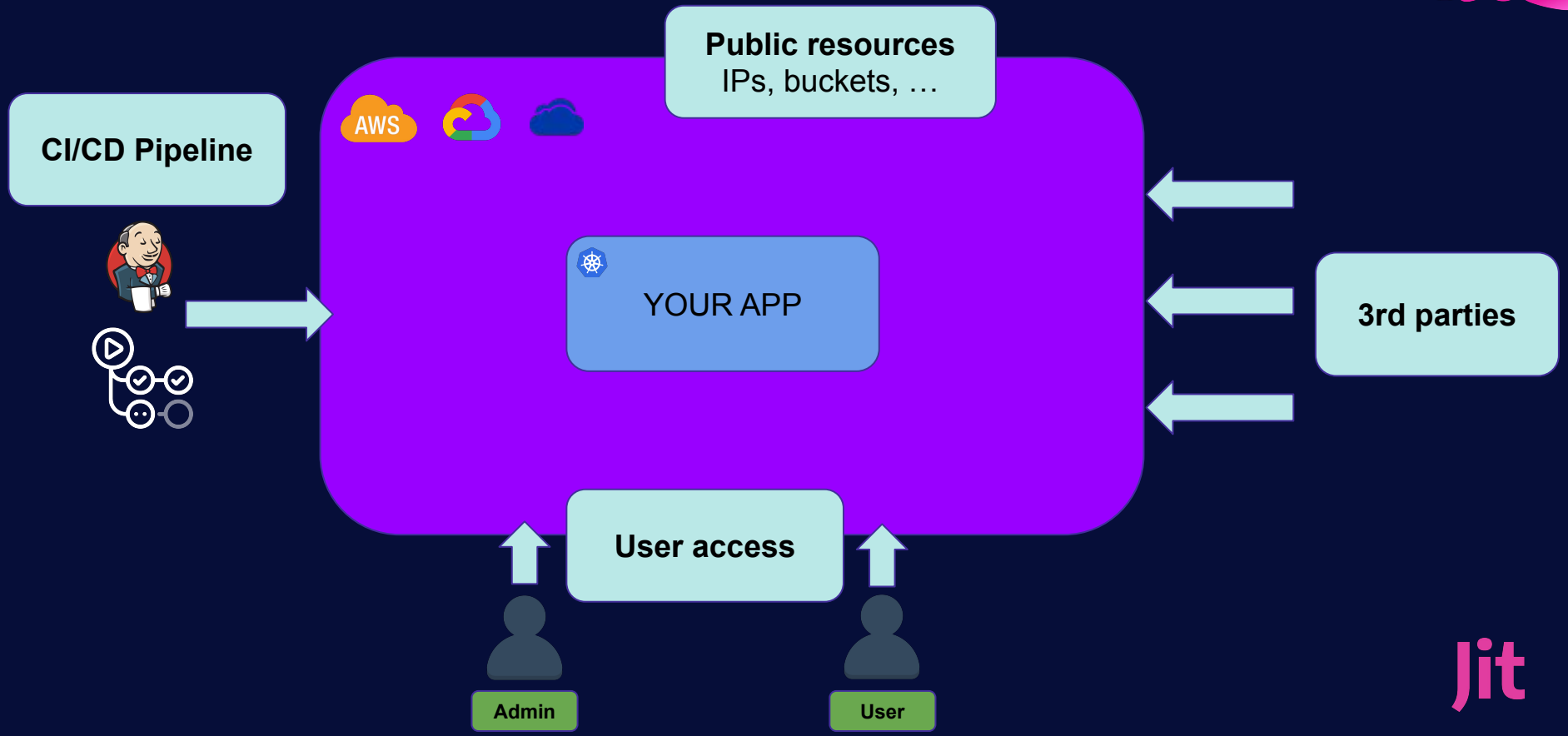
Jit





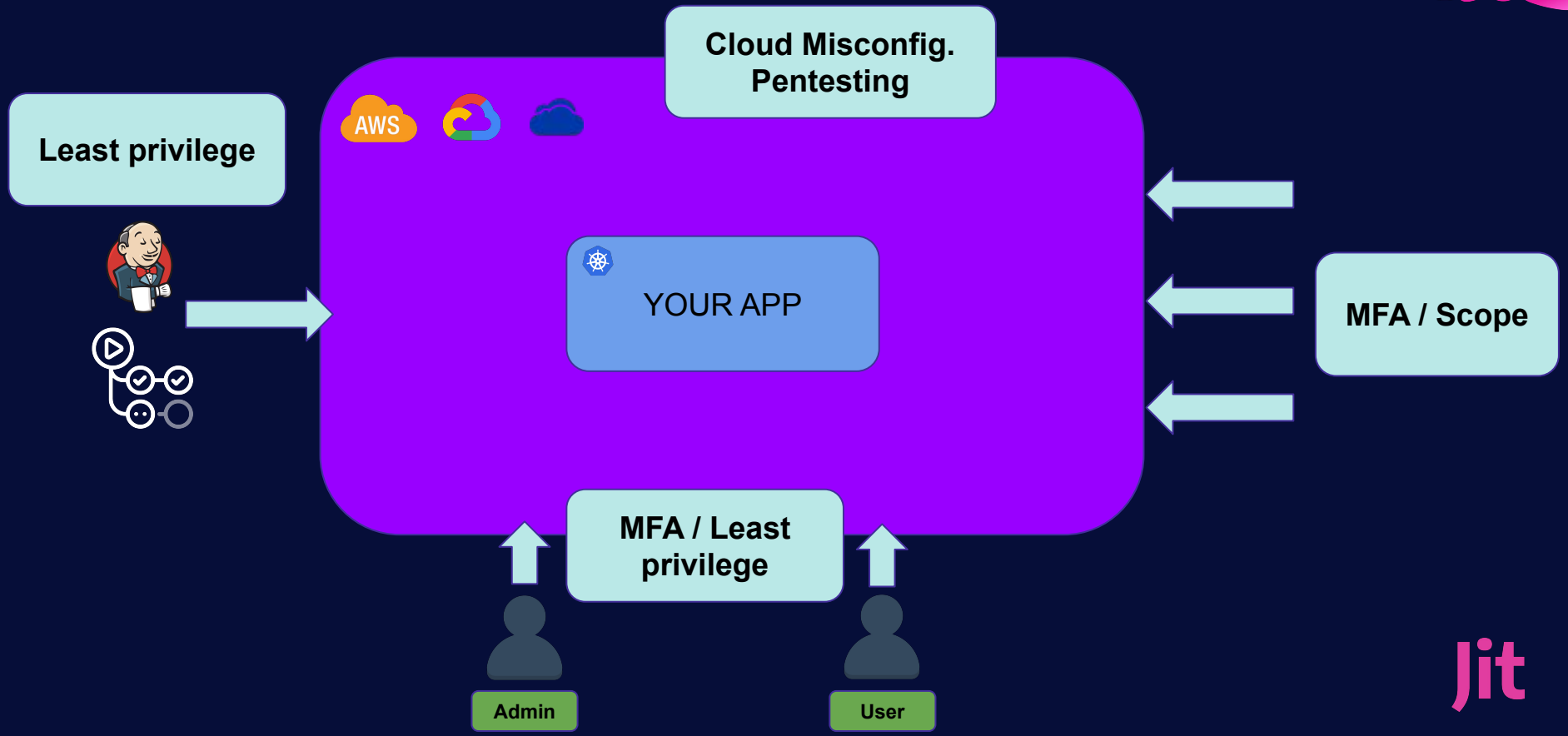
Jit

Protecting your perimeter

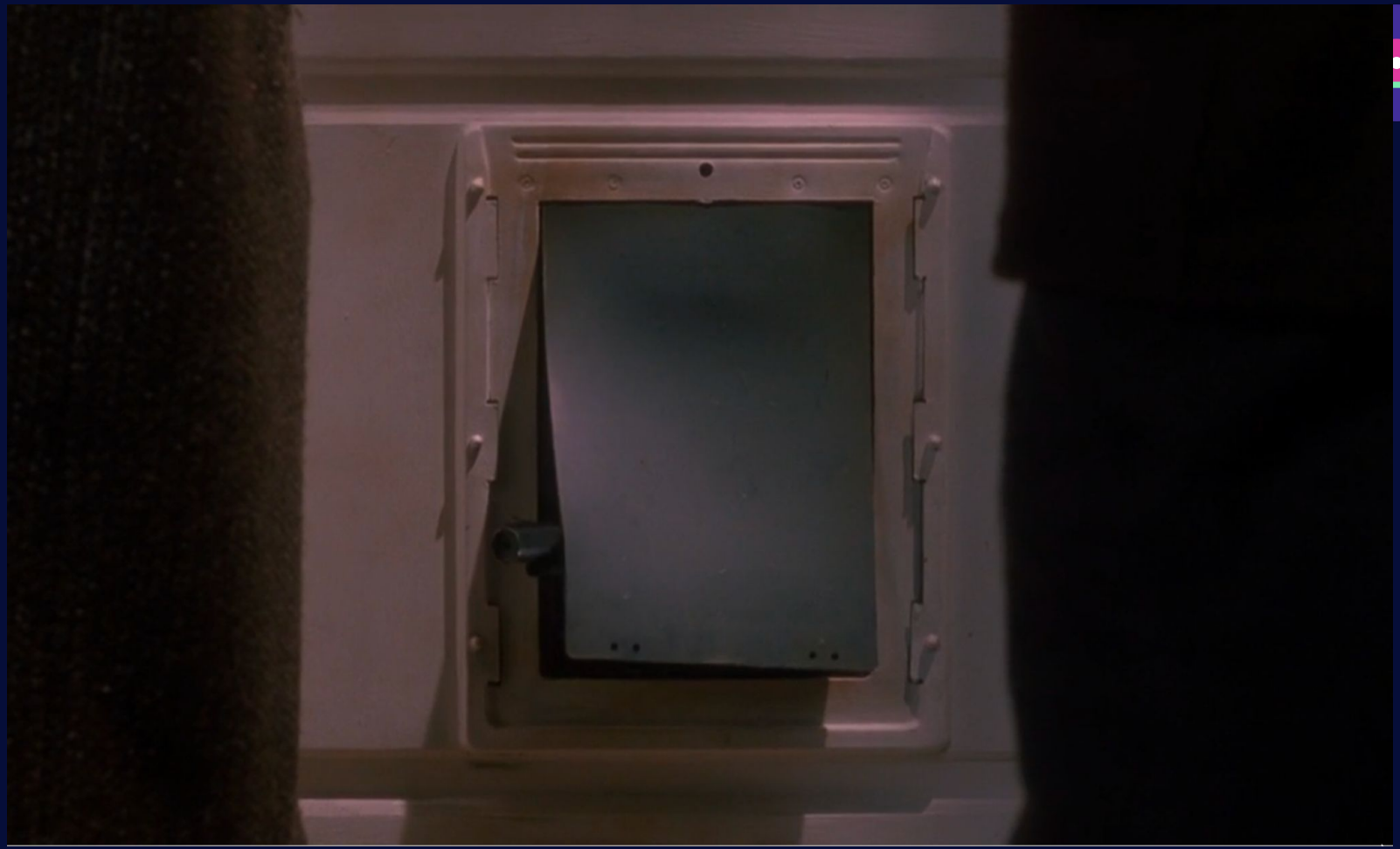


Jit

Controls to protect your perimeter

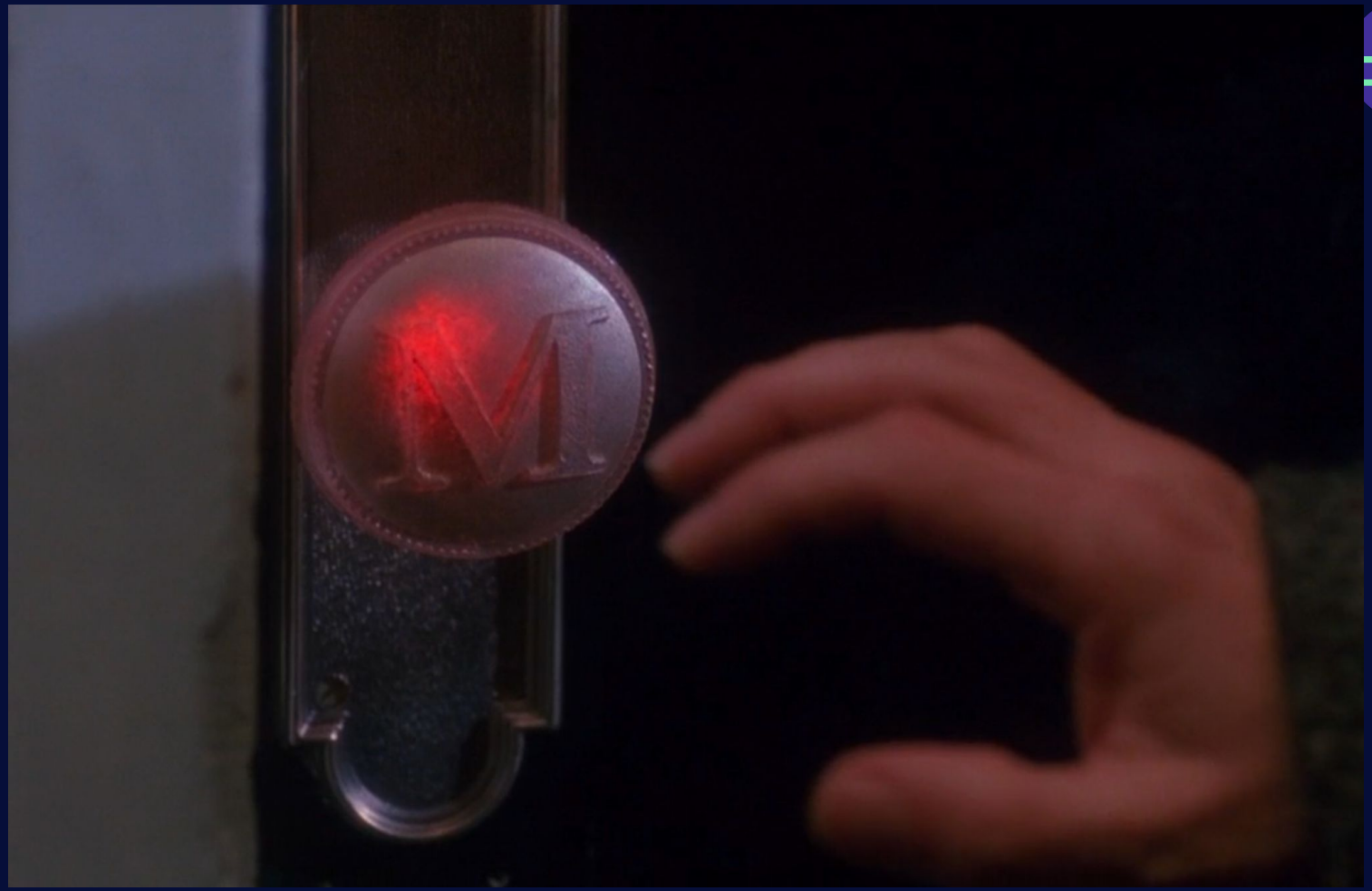


Jit



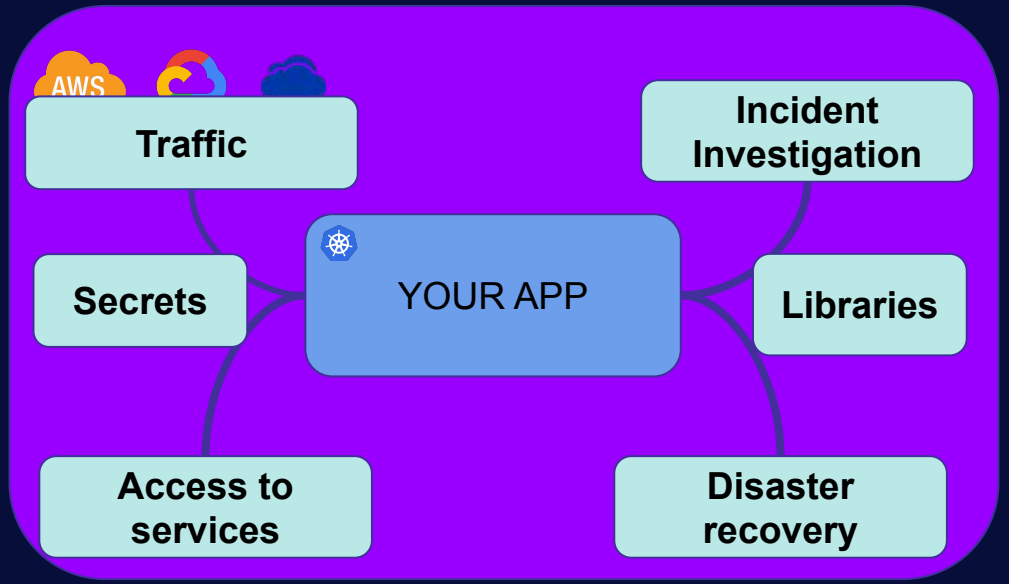
Jit

Jit



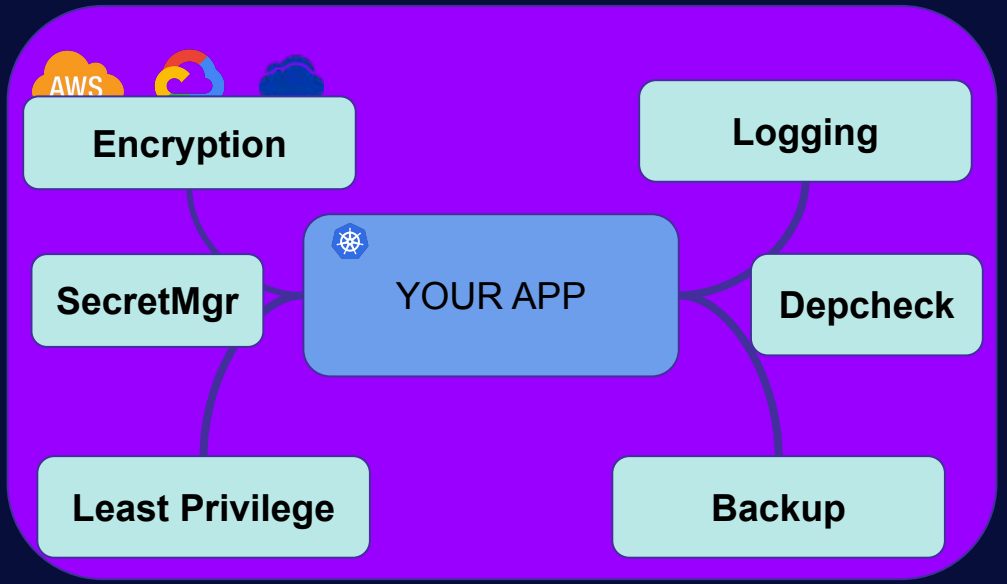
Jit

Protecting your app and its data



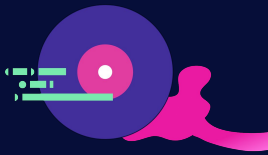
Jit

Controls to protect your app

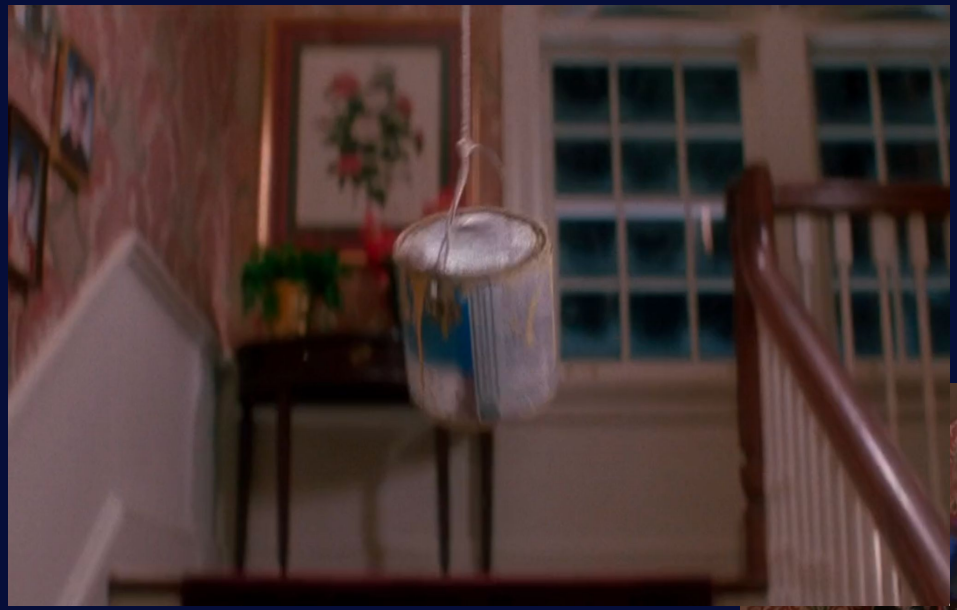


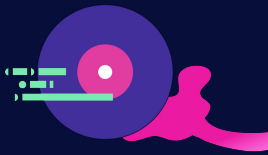
Jit

Jit



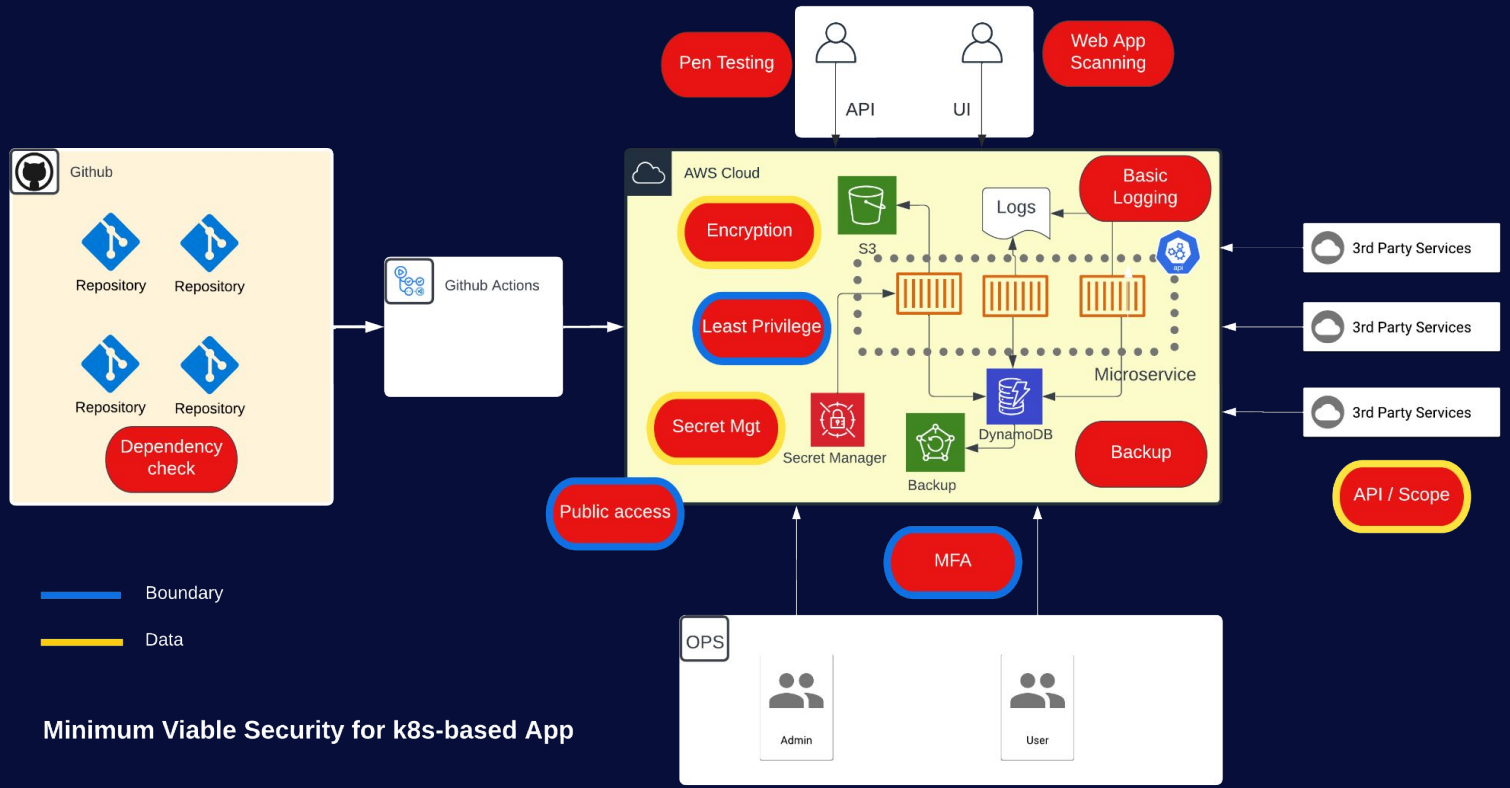
Jit





Jit

Minimum Security Controls



Minimum Viable Security for k8s-based App

Jit

Securing a sample microservice

Example for a Python-based app

- Simple FastAPI-based app to display movies information
- Data persistence: SQLite
- SCM: Github / CI: Github Actions
- Goal: integrate the 7 tools that are part of the MVS in the CI pipeline
- Demo repository
  https://github.com/dvdmelamed/owasp-nz-2022

Jit

Code vulnerabilities

Your Code

- Ensure you don’t have vulnerabilities in your code
- Use a Static Application Security Testing (SAST) scanner to detect vulnerabilities based on existing patterns
- Demo: Bandit
  - Security open-source linter for Python source code
  - Includes 35 rules for detecting vulnerabilities

Jit

Secrets

Your Code

- Make sure there are no hard-coded secrets
- Use a scanner that both searches for regexes of well known secret patterns like PAT, Slack token, AWS keys...
- Demo: Gitleaks
  - Supports multiple types of secrets: API keys, AWS credentials, SSH keys...
  - Supports detecting secrets in git history

Jit

Vulnerable Dependencies

Your Code

- Track 3rd parties libraries with disclosed vulnerabilities (CPE / CVE)
- Use a scanner that will track down those vulnerable libraries
- Demo: dependency-check
  - OWASP OSS project
  - Detects publicly disclosed vulnerabilities contained within a project's dependencies

Jit

Infrastructure misconfiguration

Your Infrastructure

- When the infrastructure is expressed as code, it is possible to detect misconfigurations early by scanning the code
- Use a scanner that will look for IaC misconfigurations
- Demo: KICS
  - OSS by Checkmarx supporting many infrastructure types: CloudFormation, Terraform, Ansible, Kubernetes, Helm, Docker, Ansible, ARM...
  - Include 2000+ checks

Jit

Pentesting

Your Runtime

- ➔ Simulate attacks on your frontend to ensure it is safe

- ➔ Use a pentest / Web Application Scanner
- ➔ to test the security of your SaaS

- ➔ Demo: ZED Attack Proxy (ZAP)
  - ◆ Free web app scanner by OWASP
  - ◆ Includes 17 built-in rules
  - ◆ Supports also API Scanning using OpenAPI or Swagger for endpoint discovery

Jit

Vulnerable container images

Your Pipeline

- When building your container images, make sure there is no vulnerability in the base image
- Use a scanner that will scan your container images and enforce your image trust (Notary)
- Demo: Trivy
  - OSS by Aqua supporting OS packages and language-based packages
  - Supports also IaC misconfigurations

Jit

Multi-Factor Authentication (MFA)

Your 3rd Parties

- ➔ Ensure you enforce MFA for all 3rd party access
- ➔ Make sure MFA is used (custom tool)
- ➔ Demo: MFA on Github

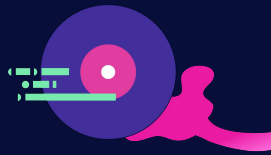
Jit

Securing a sample microservice: the tools

Example for a Python-based app

SAST	SAST (Secrets)	IAC	SCA	Containers	DAST	MFA
						
Bandit	Gitleaks	KICS	OWASP Dependency-check	Trivy	OWASP ZAP	Custom

A Minimum Viable Security plan (1)



01

Your code

Code vulnerability
Secrets
Logging
Vulnerable libraries

02

Your infra

Cloud Misconfiguration
Least Priv. Remote access

03

Your runtime

Pentesting
API Security

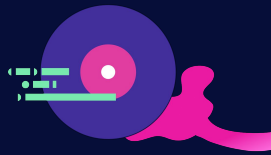
04

Your pipeline

Vulnerable containers
Least priv. access

Jit

A Minimum Viable Security plan (2)



05

Your data

Data encryption
Secrets storage

06

Your 3rd parties

Multi-Factor Auth
Secured access

07

Your people

Password manager

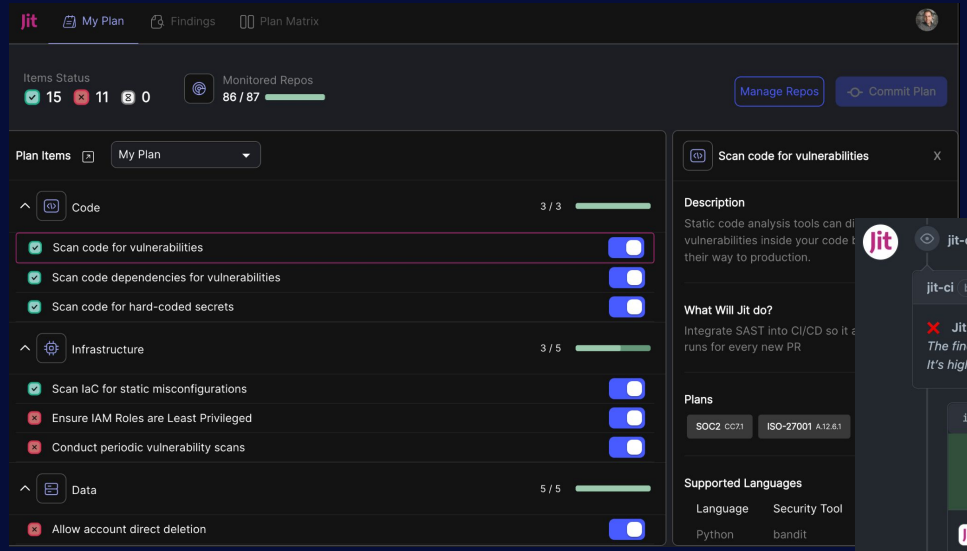
08

Your operations

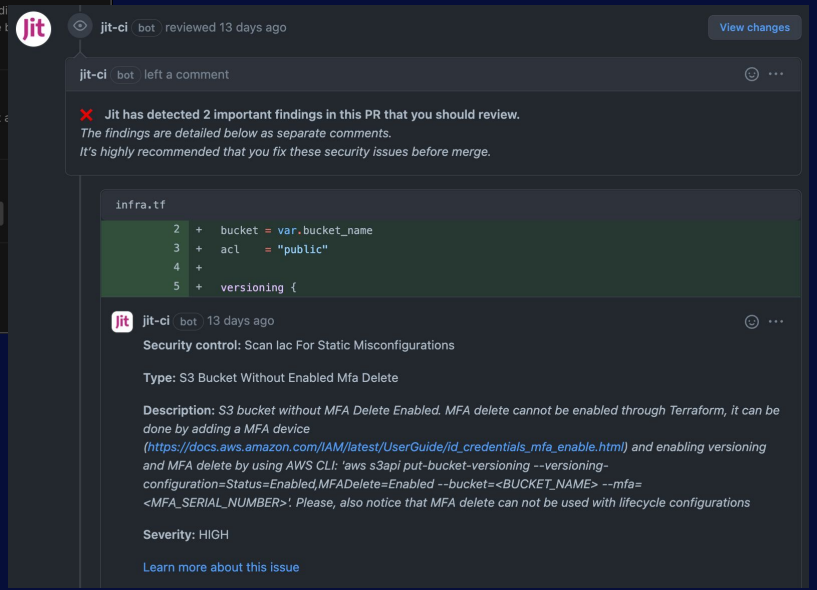
Audit
Backup

Jit

Improving dev-first experience: Jit



Customized MVS plan



Dev-native experience using PR comments

Jit

Your next step on the security journey

Jit

Jit

OWASP NEW ZEALAND DAY 2022

Thank you

Intrigued? Try our free **beta** at **jit.io**

Inspired? Join us! **We are hiring!**

Questions? Contact me at **david@jit.io**