THE DARK SIDE OF DEVSECOPS
GHOST IN THE DEPLOYMENT PROCESS

EasyStack open cloud computing AMD

datacomm flexi WOWRACK ZConverter Cloud SIVALI CLOUD TECHNOLOGY

boer technology NASHTAGROUP nevacloud

Yogyakarta, 19 July 2025

INTRODUCTION

ANANDA FIKRI IJLAL AKBAR (MAS NAN)

DevSecOps Consultant @i3

Community Founder @Boxsploit Ecosystem

in Ananda Fikri

AfiIskandar

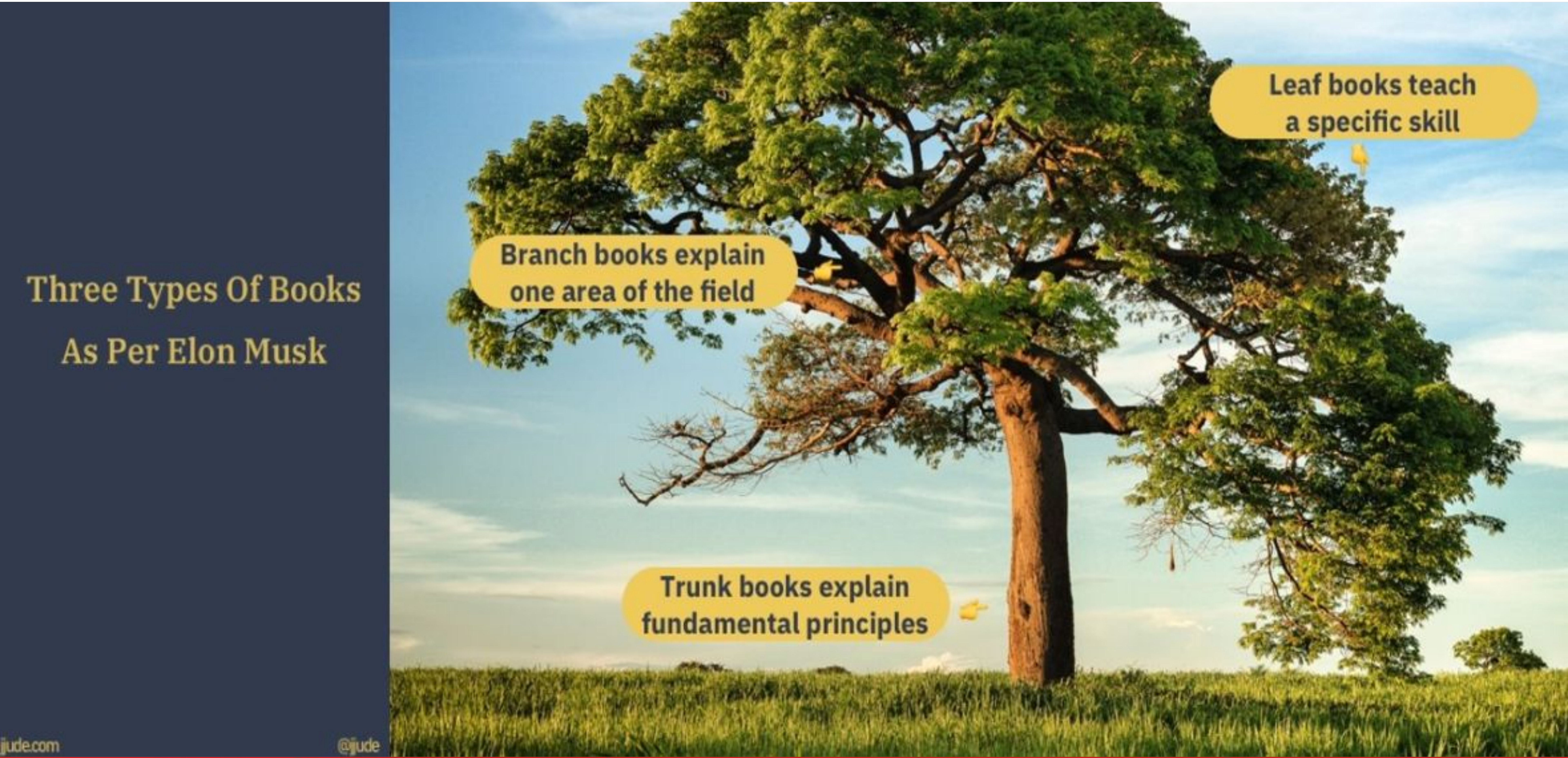
kd.leaf

EasyStack open cloud computing · AMD · datacomm · flexi · WOWRACK · ZConverter Cloud · SIVALI CLOUD TECHNOLOGY · boer technology · NASHTAGROUP · nevacloud

Yogyakarta, 19 July 2025

"It is important to view knowledge as a sort of semantic tree. Make sure you understand the fundamental principles, the trunk and big branches, before you get into the leaves, or there is nothing for them to hang on to."

– Elon Musk



Three Types Of Books As Per Elon Musk

Leaf books teach a specific skill

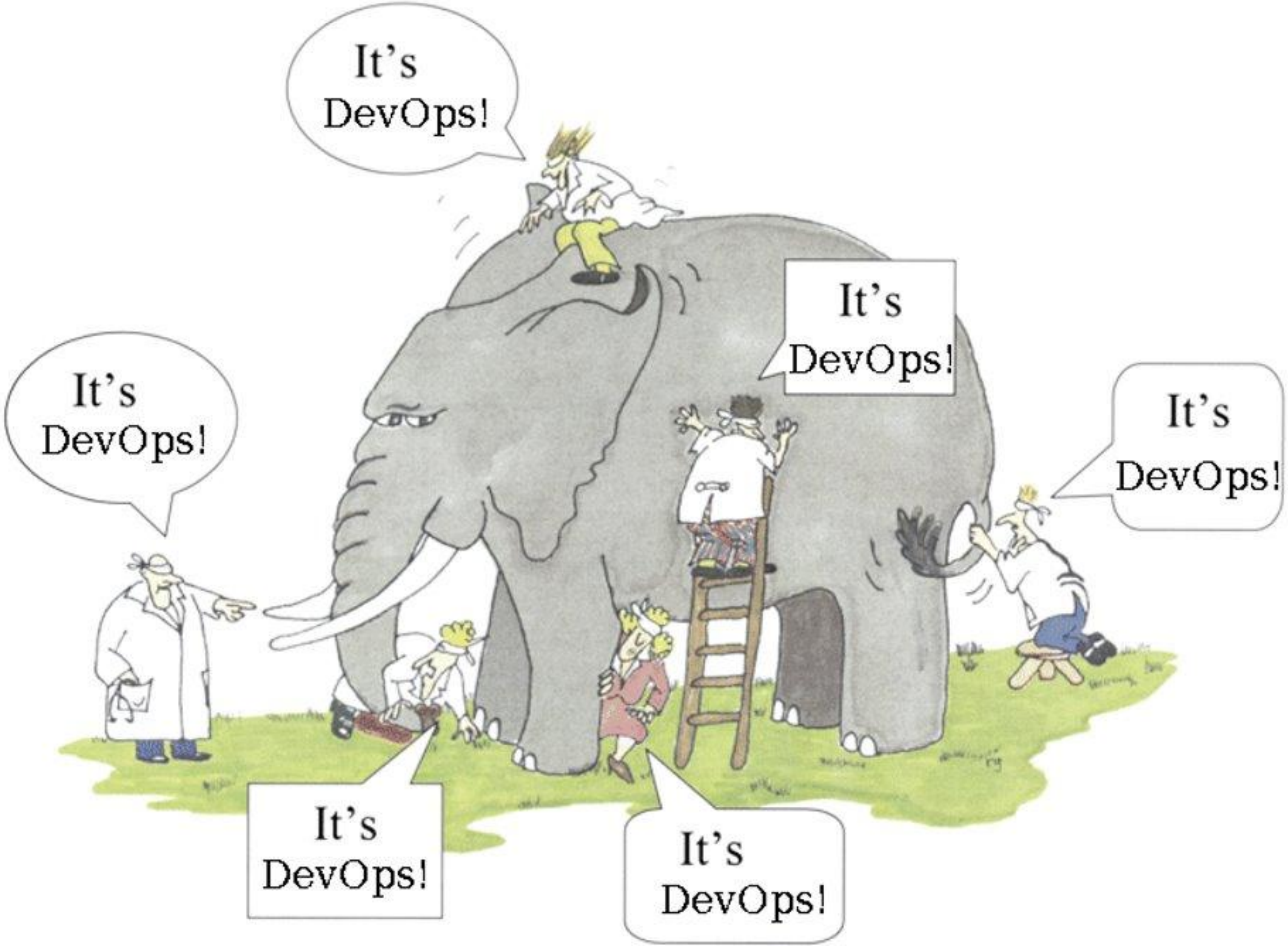
Branch books explain one area of the field

Trunk books explain fundamental principles

ijude.com

@ijude

THE DEVSECOPS BACKGROUND


It's DevOps!
It's DevOps!
It's DevOps!
It's DevOps!
It's DevOps!
It's DevOps!

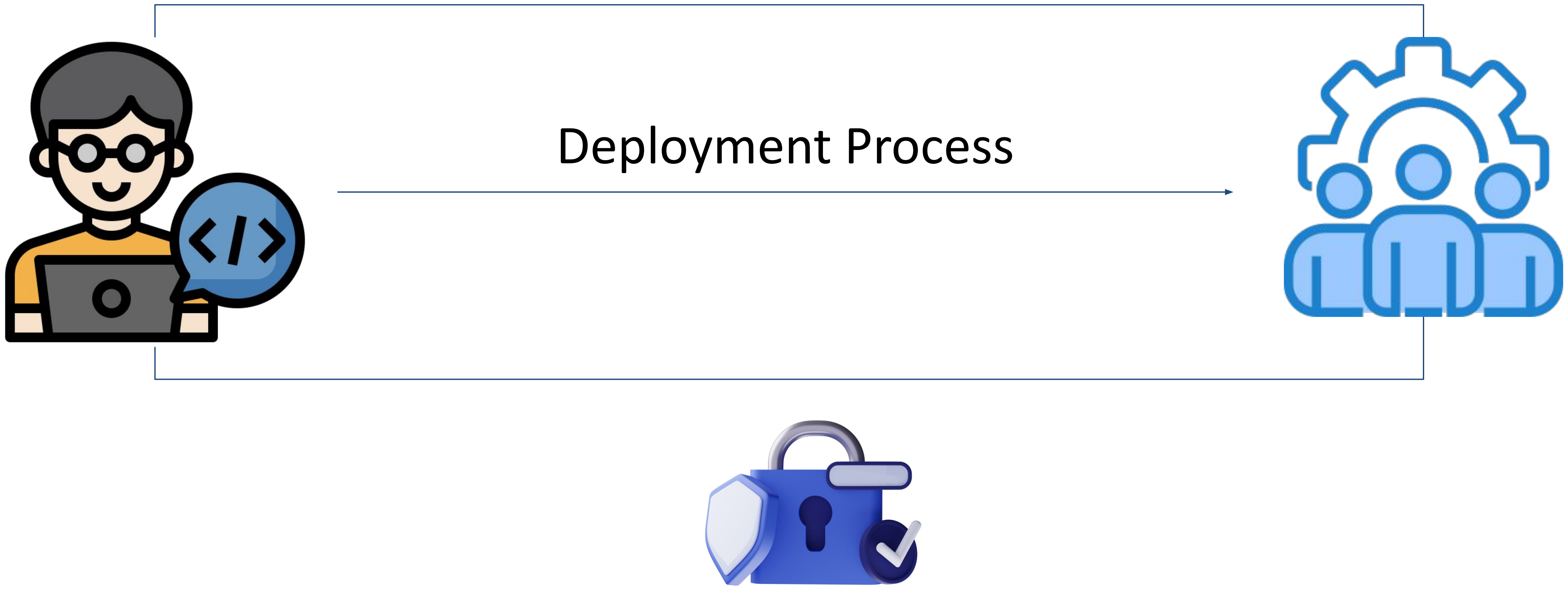
YOU **FOOL**!

It's not about the tools, it's about the CULTURE!!!!

WHAT IS DEVOPS?

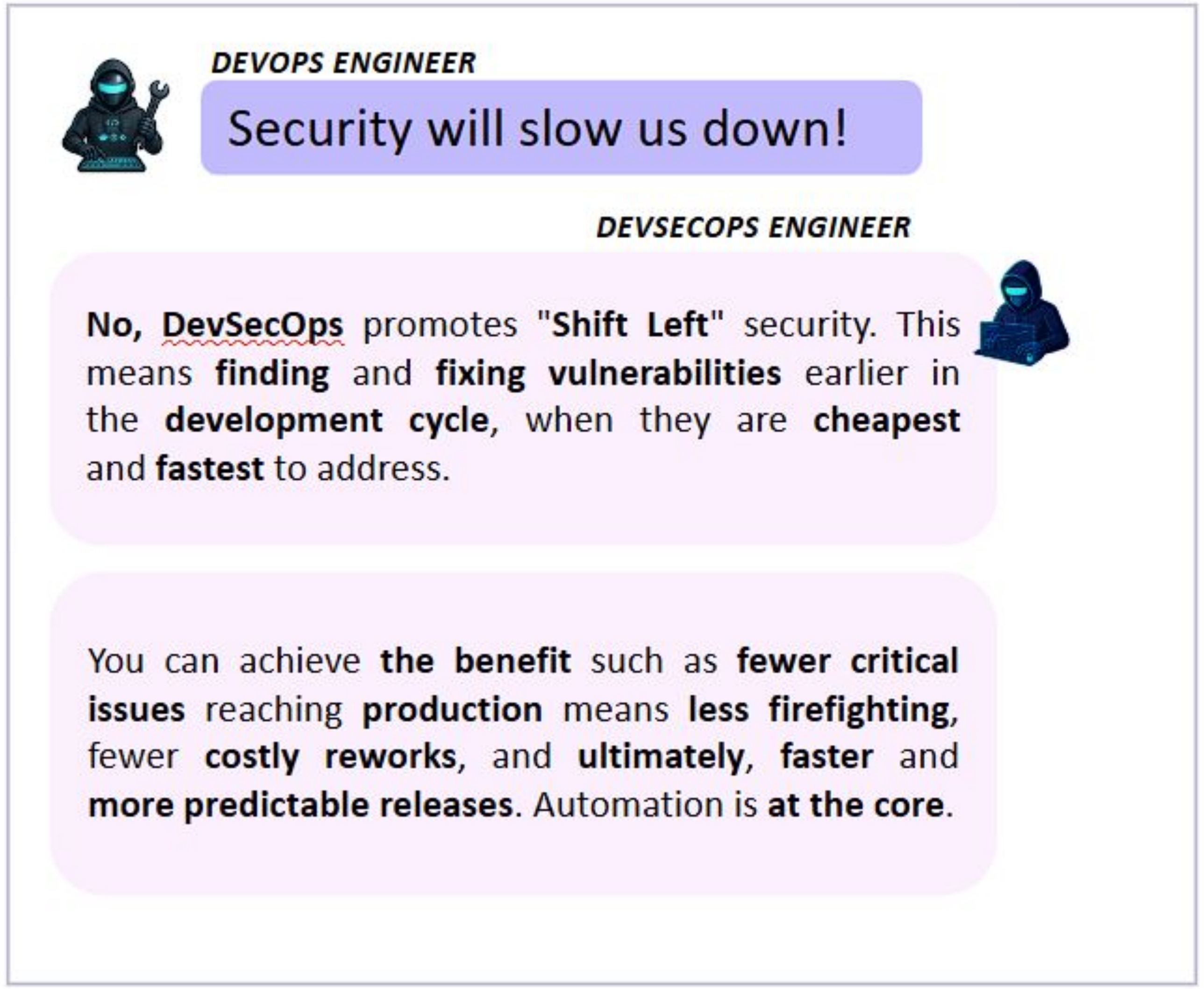
A culture and **professional** movement that stresses communication, collaboration and integration between software developers and IT operations professionals while automating the process of software delivery and infrastructure changes.

DEVSECOPS: ENHANCEMENT OF DEVOPS



Deployment Process

PERSPECTIVE OF DEVSECOPS



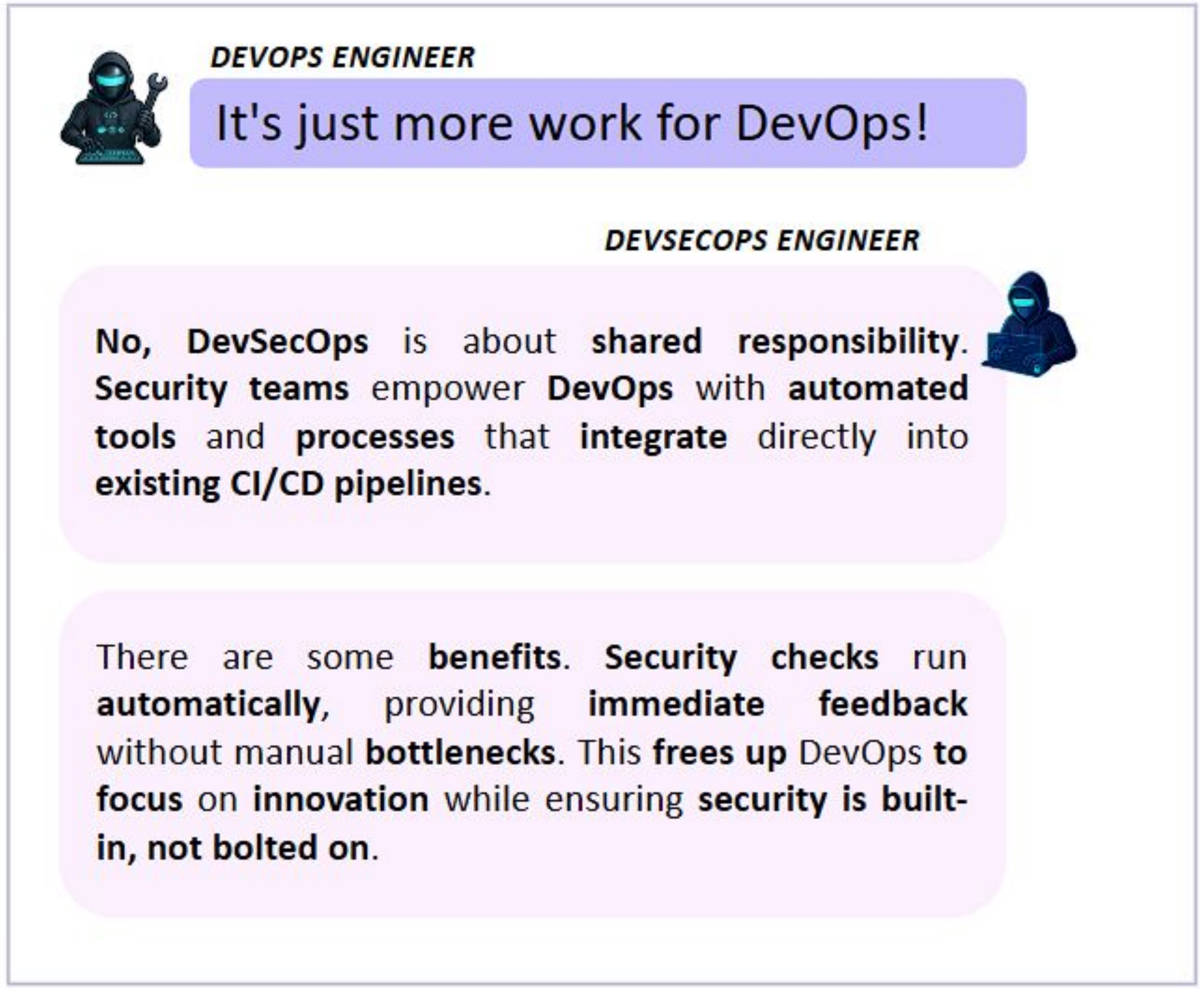
DEVOPS ENGINEER

Security will slow us down!

DEVSECOPS ENGINEER

No, DevSecOps promotes **"Shift Left"** security. This means **finding** and **fixing vulnerabilities** earlier in the **development cycle**, when they are **cheapest** and **fastest** to address.

You can achieve **the benefit** such as **fewer critical issues** reaching **production** means **less firefighting**, fewer **costly reworks**, and **ultimately**, **faster** and **more predictable releases**. Automation is **at the core**.



DEVOPS ENGINEER

It's just more work for DevOps!

DEVSECOPS ENGINEER

No, DevSecOps is about **shared responsibility**. **Security teams** empower **DevOps** with **automated tools** and **processes** that **integrate** directly into **existing CI/CD pipelines**.

There are some **benefits**. **Security checks** run **automatically**, providing **immediate feedback** without manual **bottlenecks**. This **frees up** DevOps **to focus** on **innovation** while ensuring **security is built-in, not bolted on**.

THE DEVSECOPS FOMO

PEOPLE IN INDONESIA, HAS ALREADY KNOWN ABOUT DEVOPS.

PEOPLE IN INDONESIA, ALSO KNOW ABOUT CYBER SECURITY.

DEVSECOPS CONCEPT IN THE WORLD = ABOUT 2015 (HYPE)

DEVSECOPS CONCEPT IN INDONESIA = ABOUT 2021 (HYPE)

We do DevSecOps now

KIND OF FOMO

We always think, DevSecOps is as a simple implementing these:

- Only use the tools (viral) but not implementing the proper decisions of **why we use that tools specifically; how about other tools; what are the powers for the product concern.**
- The Environment variables are still hardcoded.
- Create complex pipeline as they think => Complex == Secure
- Calling a lot of Vendor to help in their security work (They secure the system, but not securing the human as main concern)
- Only think about tools, but not implementing about the nice cultures
- Just Automate the security tools, but ignore the detailed agile actions

IN REALITY

- Fast deployment ≠ secure deployment
- Complexity ≠ Secure Ecosystem
- Automation exposes everything
- Supply chain is now a prime attack vector

SIMPLE DEPLOYMENT

- **Branch**: Development + Production
- **Jobs**: SCA, SAST, IaC, Build, DAST, Deploy

ADVANCE DEPLOYMENT

- **Branch**: Dev + QA + Bug Fix + FrontEnd + Feature + UAT + Production
- **Jobs**: SCA, SAST, IaC, Build, DAST, Deploy

Every Company in Indonesia has security mindset, but they currently are still trapped in the old *bureaucracy*

STAGE WHERE GHOST HIDES

Development

Build

Distribution

Supply Chain

THE LEAK OF DEVSECOPS PROCESS

GHOST IN DEVELOPMENT

The Development Security Scanning: SCA & SAST

Leaked creds via git

Dependency confusion

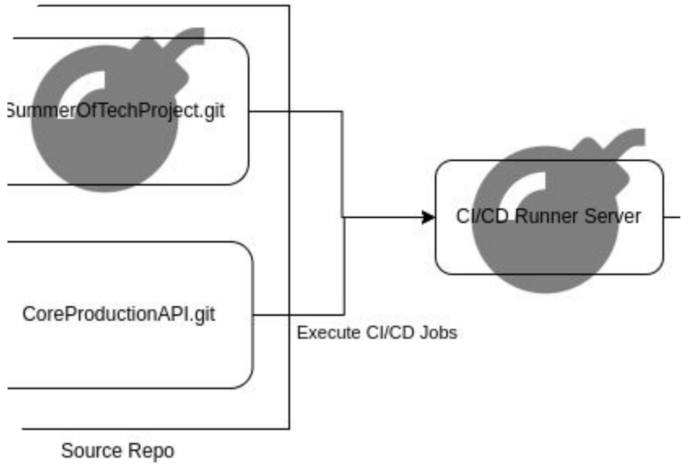
Insecure Git settings

Further Additional Implementation:

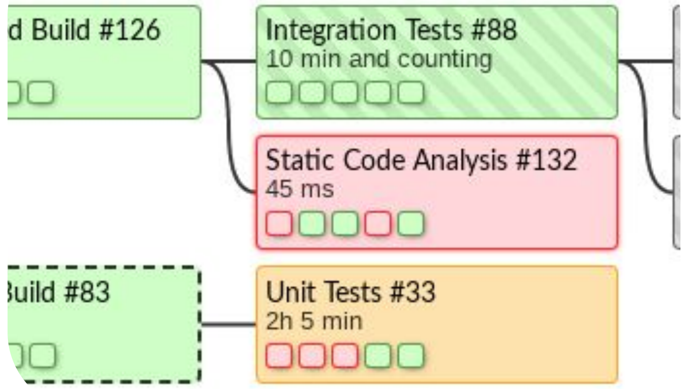
- Git Scanning
- Advanced SCA Analysis (Multi-SCA = General + Specific Language)
- Source Code Management (Taking Out Unused Code)

GHOST IN BUILD

The Build Security Scanning: DAST, ArtifactSec, Secret Management



Compromised Runners



Evil build plugins

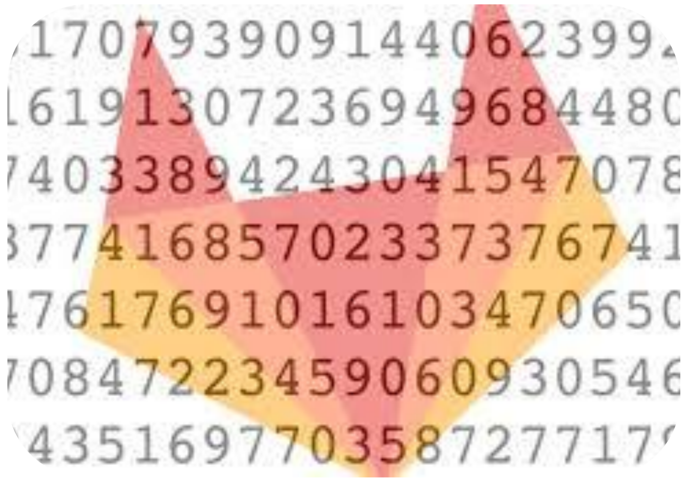
Misconfigured scripts

Further Additional Implementation:

- Plugin Usage Awareness
- RBAC for CI/CD Runner and Firewall Setting
- CI/CD Pipeline Script awareness

GHOST IN DISTRIBUTION

The Distribution Security Action: Artifact Signing, Secret Management



Repository Hijacking

Man-in-the-Middle (MitM) on Artifact Transport

Unsigned Packages

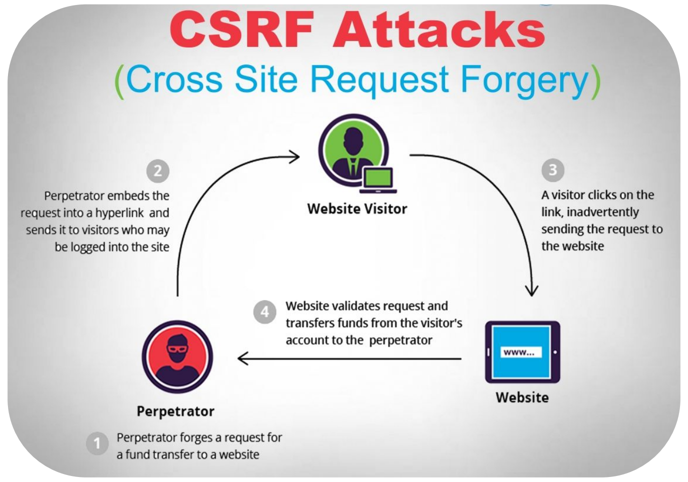
Further Additional Implementation:

- Artifact Signing Implementation
- Secure Transport from Trusted URL
- Integrity Check Before Deployment
- Git Commit Analysis and PR/MR Management

GHOST IN DEPLOYMENT CIRCLE

The Deployment Security Action: Security Compliance, IAST, RASP

Information Disclosure


CSRF Attacks
(Cross Site Request Forgery)

1 Perpetrator forges a request for a fund transfer to a website

2 Perpetrator embeds the request into a hyperlink and sends it to visitors who may be logged into the site

3 A visitor clicks on the link, inadvertently sending the request to the website

4 Website validates request and transfers funds from the visitor's account to the perpetrator

Request Forgery

Code Injection

Further Additional Implementation:

- Enhanced the firewall system with strong rules
- Improved the SRE activity (Monitoring and Alerting) with proper SLAs
- Automated Compliance Scanning Implementation and Automated Hardening based on PCI/DSS or other standards through Production Server (Not only Firewall)

IN CONCLUSION, WE ARE NOT ONLY AWARE OF REGULAR SECURITY, WE ALSO SHOULD BE AWARE OF SUPPLY CHAIN AND HUMAN BRAIN

ADVANCE DEVSECOPS SUGGESTION

- Zero Trust Implementation
- Balancing both Automated Scanning and Regular Analysis
- Manage the Deployment with the proper SLAs
- Arrange the Branching Model into the proper core of branches
- Proxy or Firewall Access Setup for Proper Server or VM Communication
- Supply Chain Attack Training
- Threat Intelligence Education
- Weekly Pipeline Audit
- Human Security Education
- Not Complex, but Proper Security Management for Application or Product Runtime and Deployment

KEY TAKEWAYS

💡 DevSecOps ≠ Set and Forget
👻 Ghosts love automation
🔒 Secure each process properly with automation and human initiation
🔎 Never trust… verify.

IN THE DEVSECOPS PARADOX, WE SHOULD FOCUS ON THE MATURITY, NOT ABOUT THE TOOL QUANTITY, BUT ABOUT THE CULTURE

THANK YOU

EasyStack open cloud computing

AMD

datacomm flexi WOWRACK

ZConverter Cloud

SIVALI CLOUD TECHNOLOGY

boer technology

NASHTAGROUP

nevacloud

Yogyakarta, 19 July 2025