The State of DevSecOps

Adopted from DevSecOps Day Singapore 2019 Presentation
by Stefan Streichsbier (CEO - GuardRails)

What do these companies have in common?

GO JEK

traveloka

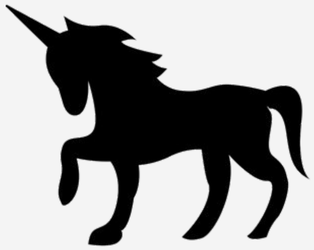
tokopedia

BukaLaPak

Grab

Garena

<10 years



Tech Startups in Asia – #10YearChallenge

tokopedia Garena

2009

V

S

2019

How is that possible?

1. Existing solutions are no longer adequate

Many industries have not been innovated in decades

Software and services provide a terrible user experience

95% of the 1955 Fortune 500 don’t exist anymore

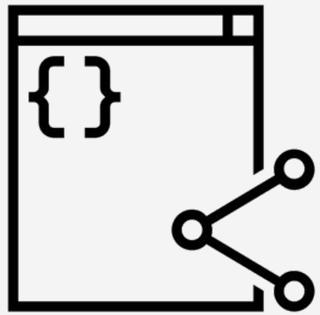
2. Internet enables wide-spread distribution

No Need To Go
To A Physical Location

Customers Are
Everywhere

Digital Marketing Scales
Better Than Sales Teams

3. Cheaper to create & operate Software



Open Source Software
Provides Building Blocks

Cloud Computing Provides
Low Barrier of Entry

Startup Ecosystems
Empower Entrepreneurs

To summarize

Creating new technology solutions was never faster, easier, and cheaper

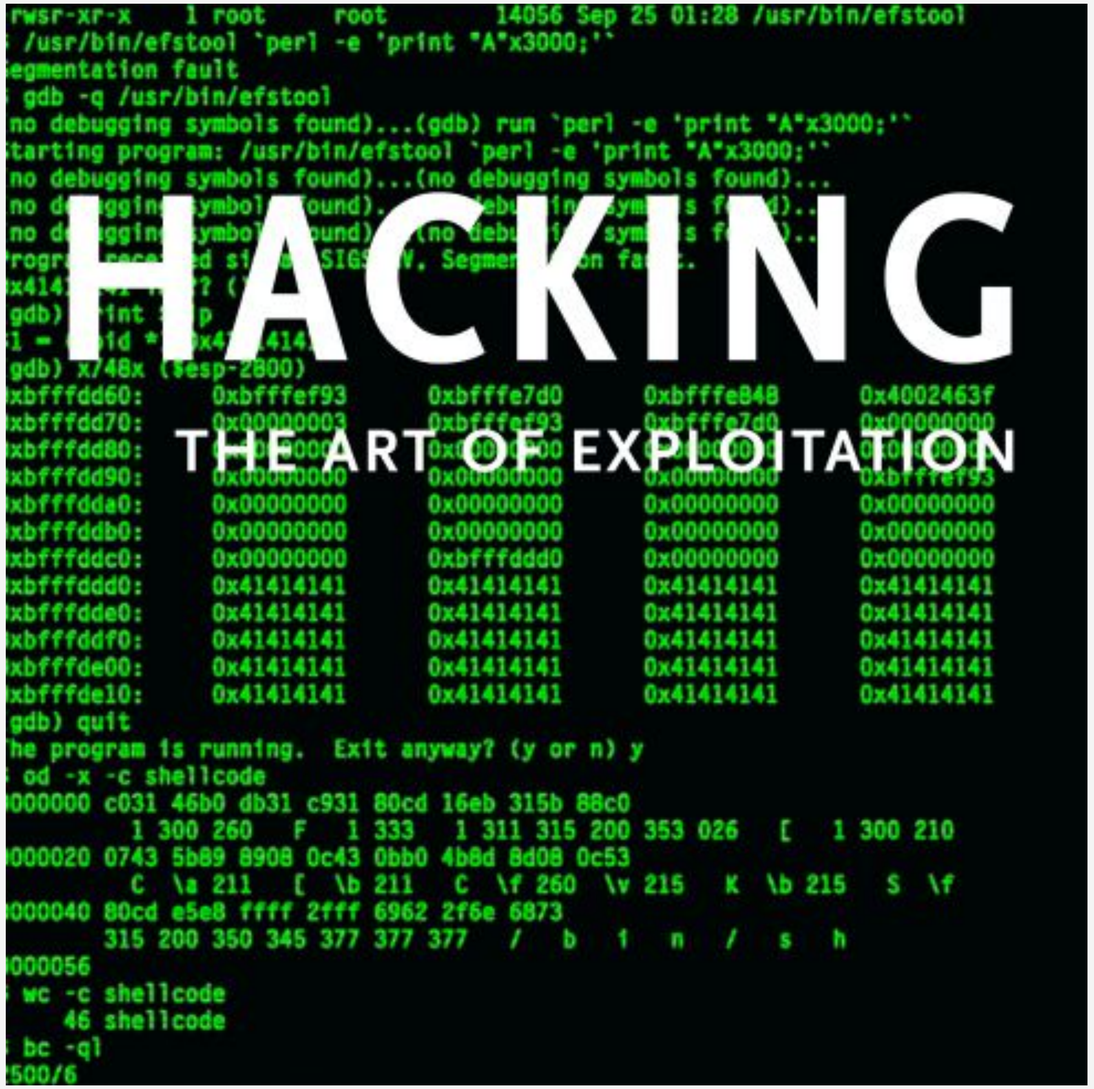
Software can be distributed globally

Existing solutions are ripe for replacement

DevSecOps:
How important is it really?

- Agile took us from months to days to develop value
- DevOps took us from months to minutes to ship value
- Applications are mission critical for every business
- Security remains one of the speed bumps for value realization

The real impact of hacks & breaches



News is full of high-profile breaches that get widespread attention.

EQUIFAX HBO YAHOO! SONY

But they are not the only target of hackers

43% of all **cyber attacks** target **small businesses.**

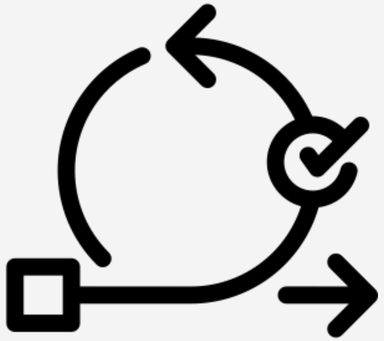
1/5 **data breaches** are the **result** of attackers abusing **insecure web applications.**

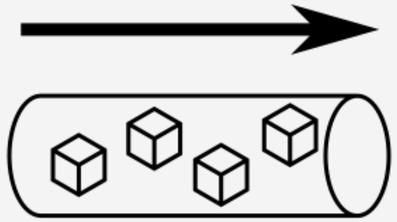
60% of **small businesses** that are **Hacked** go **out of business** within **6 months.**

DevSecOps:
Who is responsible?

The Evolution of Security Tools

Duration 2-4 weeks | 1-2 weeks | Continuous and Real-time





Penetration Testing

Tools
- Port Scanners
- Vulnerability Scanners
- Exploitation Tools

Audience
- Security Professionals

Secure SDLC

Tools
- Code Security Scanners
- Dynamic Security Scanners
- Vulnerability Scanners

Audience
- Security Professionals in Enterprise Security Teams

DevSecOps

Tools
- Code Security Scanners
- Interactive Security Scanners
- Runtime Application Self Protection

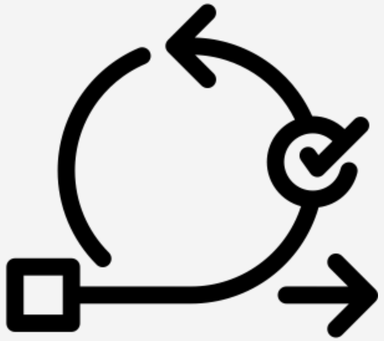
Audience
- Developers in Product Teams

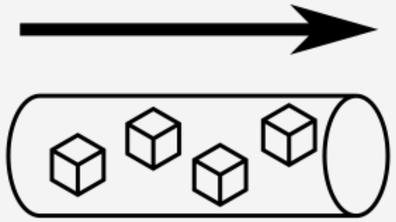
The Evolution of Security Teams

"Department of NO"

"Let's work together"

"How can we help you succeed?"





Penetration Testing

Security
Development
Operations

Secure SDLC

Security
Development
Operations

DevSecOps

Security
Development
Operations

Dev	:	Ops	:	Sec
100	:	10	:	1

Looks like we have a scale problem

Modern security teams
can only empower dev teams!


“ You build it, you run it.
- Werner Vogels (CTO, Amazon)

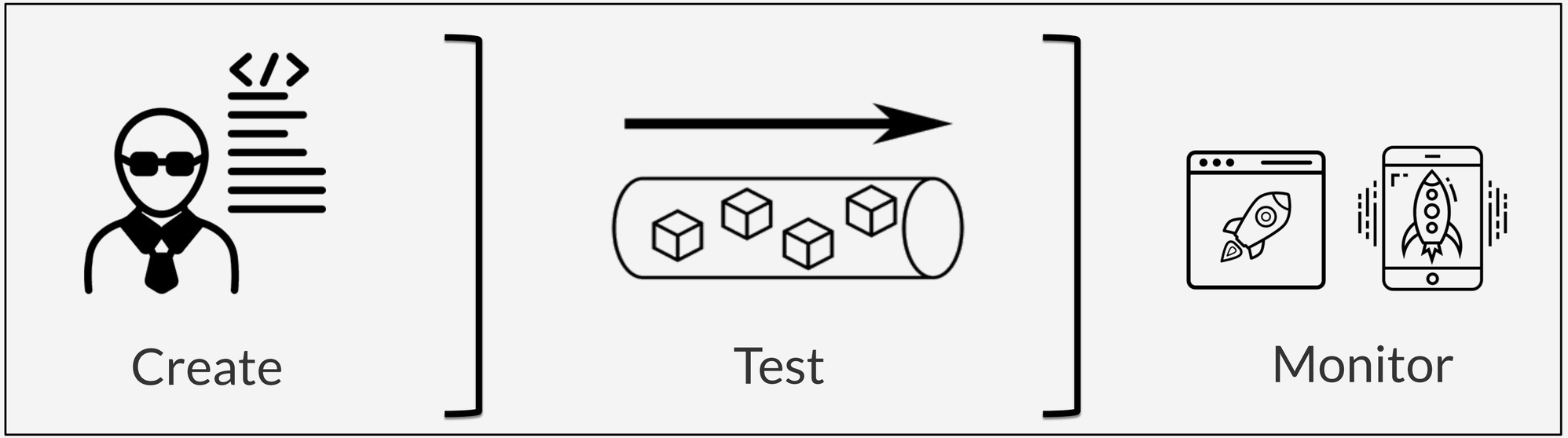
You build it, you secure it.

- John Willis

Think Responsibility vs. Accountability

Leveraging DevSecOps Principles

Understanding benefits of security controls



Challenges
- Changing human behavior
- Difficult to enforce
- People churn

Benefits
- Reduce new vulnerabilities

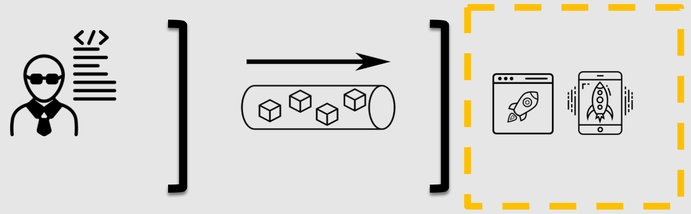
Challenges
- Vulnerability Noise
- Fixing issues
- Coverage of issues

Benefits
- Enforceable
- Provide Metrics

Challenges
- Coverage of issues

Benefits
- Enforceable
- Provide Metrics
- Prevent attacks

DevSecOps - Monitor



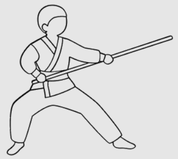
Available Technologies

- Micro Segmentation
- Runtime Application Self Protection (RASP)
- Bug Bounties

Questions you should be able to answer

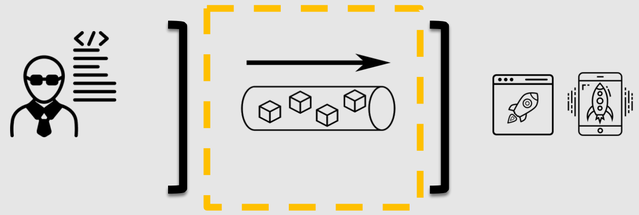
Are your applications currently under attack?

What are attackers going after?



Are we automatically defending against this attack?

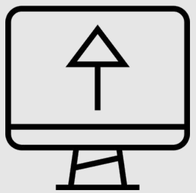
DevSecOps - Test



Available Technologies

- Static Application Security Testing (SAST)
- Sensitive Information Scanners (SIS)
- Software Composition Analysis (SCA/CCA)
- Dynamic Security Scanning (DAST)
- Interactive Application Security Testing (IAST)

Questions you should be able to answer

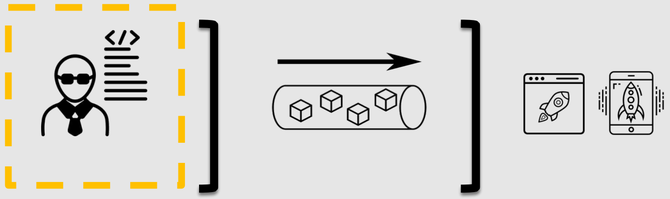


Do the latest changes introduce new security issues?

Do any of our 3rd party libraries have known security issues?

Does our code contain hard-coded secrets?

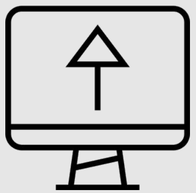
DevSecOps - Create



Available Options

- Security Awareness
- Secure Coding Training
- Shared Knowledge Base
- Security Focused Hackathons
- Security Champion Program

Questions you should be able to answer

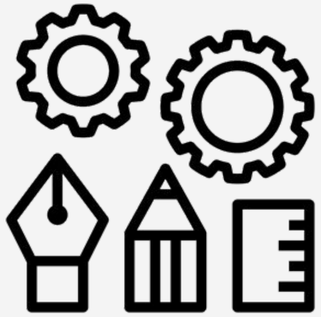


Do your teams know the most common successful attacks?

Do your teams know how to detect and prevent them?

Who is the dedicated security contact in a team?

State of DevSecOps - Conclusion



Technologies

- Tools have improved
- Choose them wisely
- Solve technology problems
- Cover the whole portfolio
- Start acting on data in prod

Security Team

- Department of YES
- Use scarce resources wisely
- Empower product teams

Product Team

- Knowledge is power
- Turn developers into security champs
- Accountable to build it, run it, secure it
- Be mindful that change takes time

DevSecOps
Do we really need it now?

There are some compelling statistics

- It's **30 times cheaper** to fix security defects in development vs production
- An **average data breach** costs an organization **5M USD**
- DevOps **high-performers include security** in their delivery process

Security is a Competitive Advantage

Thank you