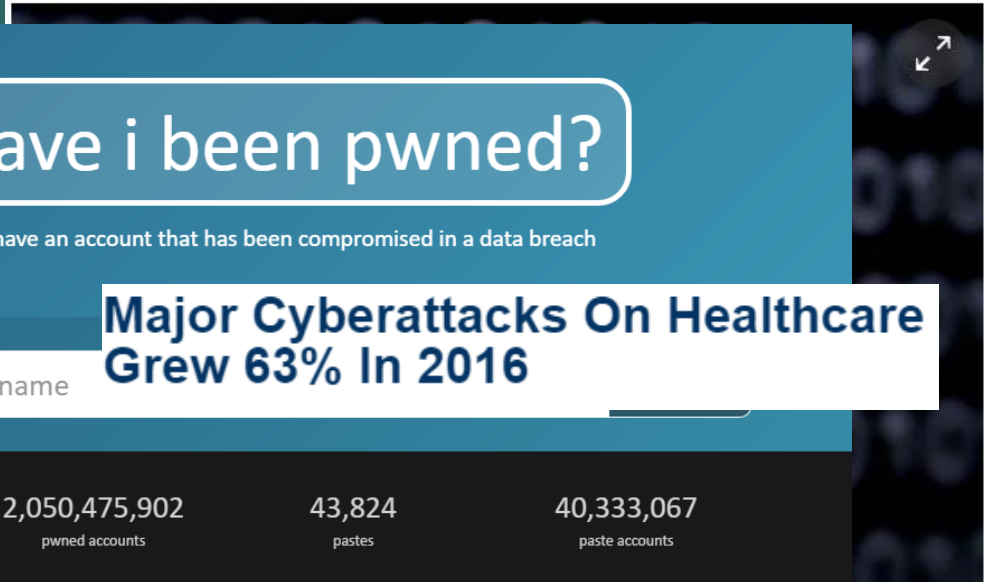
Introduction to DevSecOps

Yahoo hack: 1bn accounts compromised by biggest data breach in history

The latest incident to emerge – which happened in 2013 – is probably distinct from the breach of 500m user accounts in 2014



Red Cross Blood Service data breach: personal details of 550,000 blood donors leaked

KrebsonSecurity
In-depth security news and investigation

21 KrebsOnSecurity Hit With Record DDoS

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

il address or username

Major Cyberattacks On Healthcare Grew 63% In 2016

ars TECHNICA BIZ & IT TECH SCIEN

RISK ASSESSMENT —

Then there were 117 million. LinkedIn password breach much bigger than thought

With a pricetag of $2,200, the new haul came from a 2012 bre

DAN GOODIN - 5/19/2016, 1:10 AM

181 pwned websites

2,050,475,902 pwned accounts

43,824 pastes

40,333,067 paste accounts

The Capgemini leak of Michael Page data via publicly facing database backup

Data Breaches Exposed 4.2 Billion Records In 2016

The 4,149 data breaches reported in 2016 shattered the all-time high of nearly 1 billion exposed records in 2013.

Myspace Breach Reportedly Affects 360M Records

BY ANGELA MOSCARITOLO MAY 31, 2016 01:46PM EST 2 COMMENTS

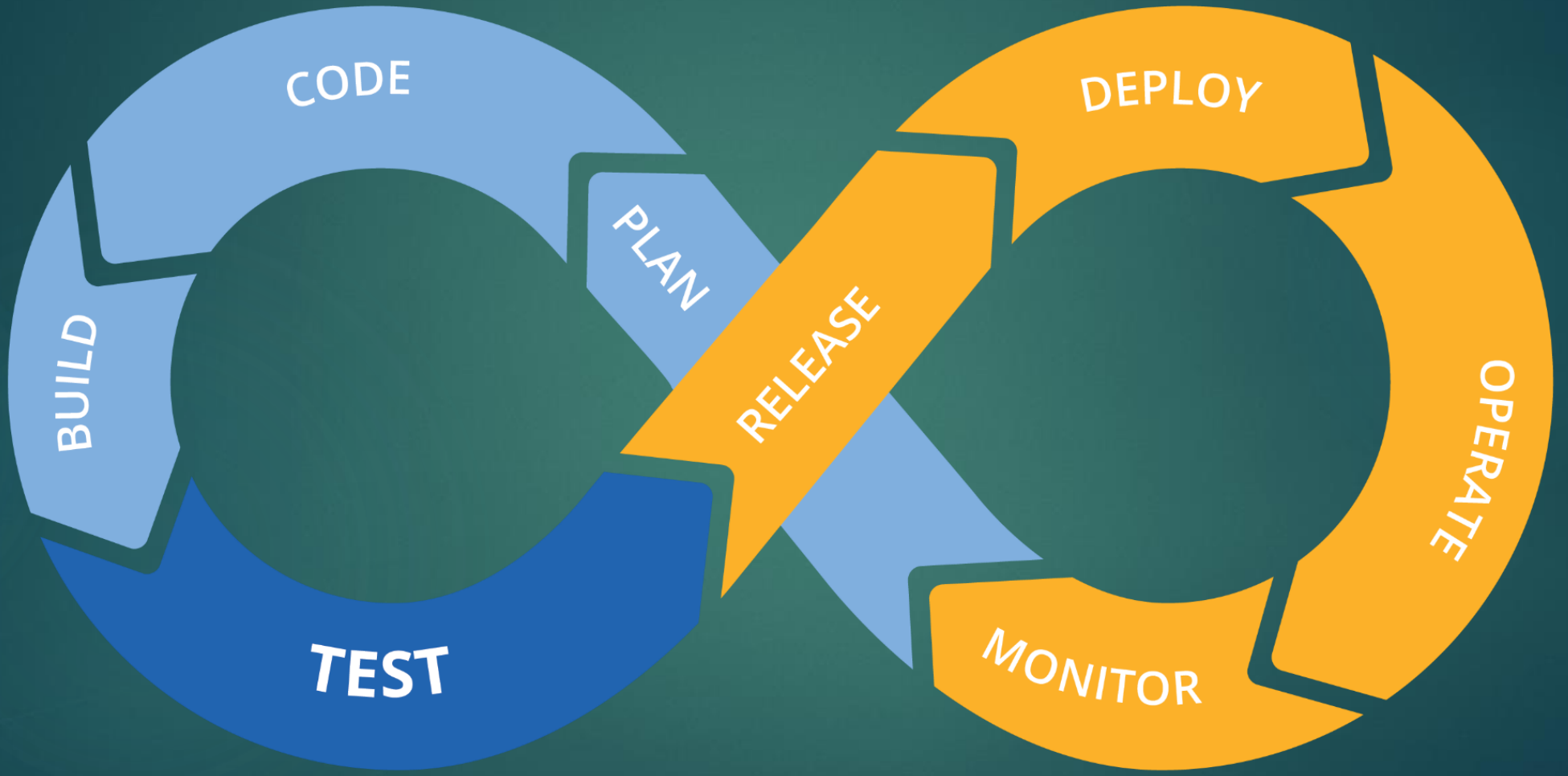
Myspace might be a thing of the past, but if you

Number Of Data Breach Disclosures Jumped 40% in 2016

Major DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline

The sound of silence.

DevOps



But Where Is Security?

DevSecOps

- Clear Communication Pathways
- Streamlined Communication
- Security As Code
- Training
- Integrate Security into DevOps cycle

What is DevSecOps?

DevSecOps is the practice of developing safer software sooner by involving all needed parties in the creative process and practicing continuous improvement from high fidelity actionable feedback with context.

IS

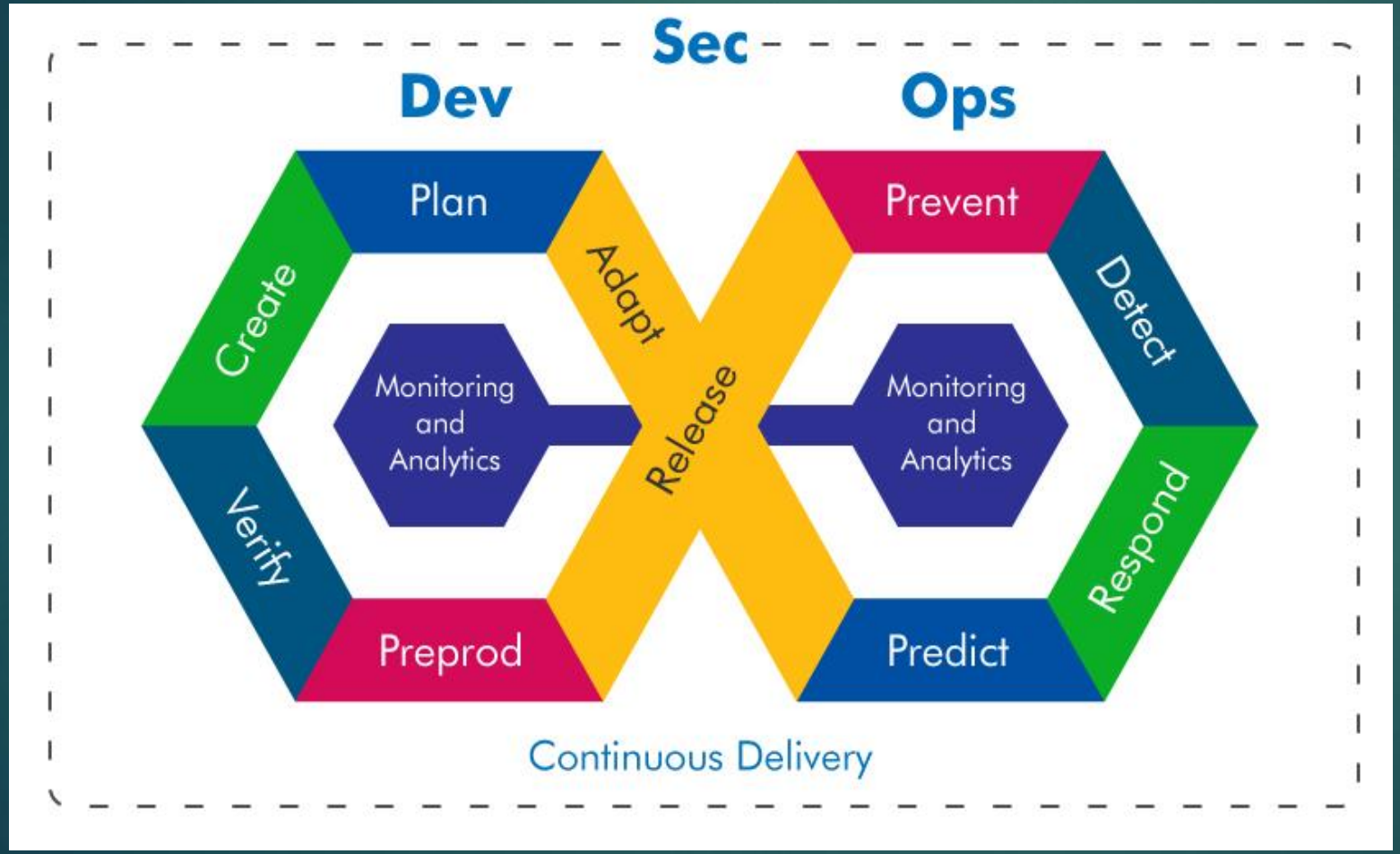
- A Mindset and Holistic Approach
- A Collection of Processes & Tools
- A Means of Building Security and Compliance into Software
- A Community Driven Effort
- A Strategy Driven by Learning and Experiments

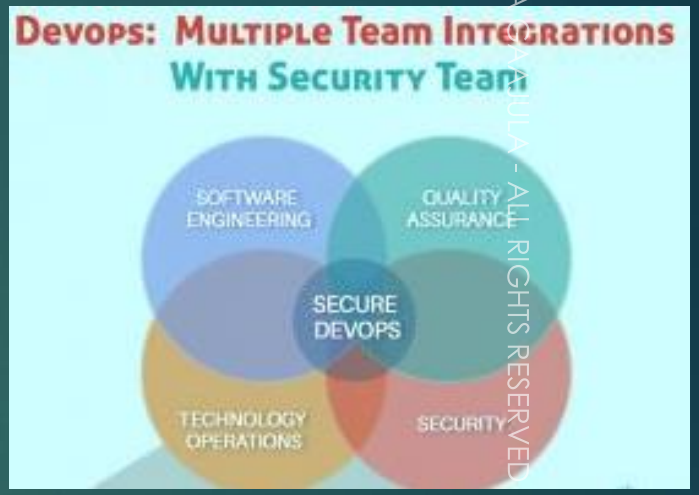
IS NOT

- A One-Size-Fits-All Approach
- A Single Tool or Method
- Just a means of adding Security into Continuous Delivery
- Invented by Vendors
- A Strategy Driven by Perfection and Compliance

Transition from DevOps to DevSecOps

Integrating 'Security as Code' Culture within DevOps





Major Components of DevSecOps Approach

Effective DevSecOps approach requires a consideration of six major components. These include:

- Analysis of code – Enables the quick identification of vulnerabilities through the delivery of code in small fragments
- Change management – Allows users to not only submit changes which can increase the speed and efficiency, but also determine if the impact of the changes is positive or negative.
- Monitoring compliance – Organizations should be compliant with regulations such as General Data Protection Regulation (GDPR) and Payment Card Industry Digital Security Standard (PCI DSS) and be prepared for audits any time by the regulators.
- Investigating threats – Each code update is accompanied by potential emerging threats. It is very important to identify these threats at the earliest and respond immediately.
- Vulnerability assessment – This involves the analysis of new vulnerabilities and the response to them.
- Training – Organizations need to involve their software and IT engineers in security-related training and equip them with the guidelines for set routines.

Adopting DevSecOps Strategy

Making a move from DevOps to DevSecops

There are three key steps that organizations need to consider while adopting DevSecOps.

- Assessment of Current Security Measures
- Merging Security into DevOps
- Integrating DevSecOps with Security Operations

Important DevSecOps Tools

- Visualization Tools: Tools such as CloudWatch , CloudTrail , Kibana and Grafana help in identifying, evolving and sharing security information with operations.
- Automation Tools: Tools like StackStorm help in providing scripted remediation whenever security defects are detected.
- Hunting Tools: These tools help in detecting security anomalies. A few examples include Mirador, OSSEC, MozDef and GRR, among others.
- Testing Tools: Testing is a critical element of DevSecOps with an extensive range of tools such as GauntIt, Spyk, Chef Inspec, Hakiri, Infer and Lynis being used for the purpose.
- Alerting Tools: Tools such as Elastalert, Alerta and 411 provide the alerts and notification upon discovery of security defects requiring remediation.
- Threat Intelligence Tools: These tools capture and collate threat intelligence and include among others OpenTPX, Critical Stack and Passive Total.
- Attack Modeling Tools: These help in operationalizing attack modeling and security defenses.

Implement DevSecOps

- Development and security are no longer two different aspects.
- DevSecOps combined them into a single streamlined process by incorporating security at the level of code, thus ensuring safety of applications and processes at all levels of the process chain.

Five features speak the successful implementation of DevSecOps:

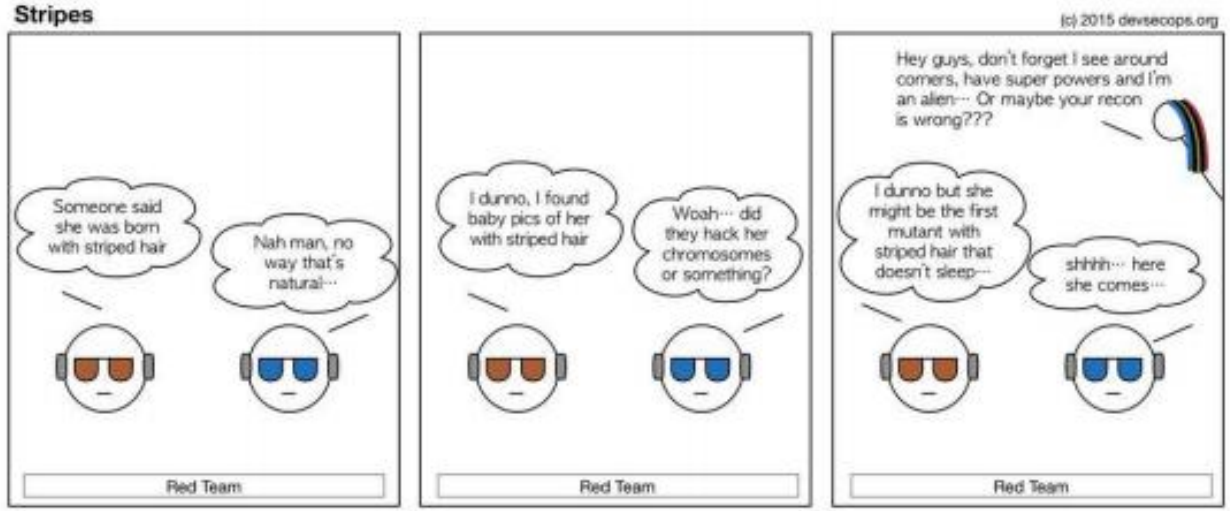
- Mandatory security at every stage
- Thorough Assessment before security
- Security-related changes right at the code level
- Automation of all possible processes
- Continuous monitoring through alerts and dashboards

SAFER
SOFTWARE
SOONER

1984 1989 1996 2001 2011 PRESENT

DEVELOPER
SECURITY
OPERATIONS
"DEVSECOPS"
"RUGGED"

Take Responsibility.
Give Credit.
@seniorstoryteller

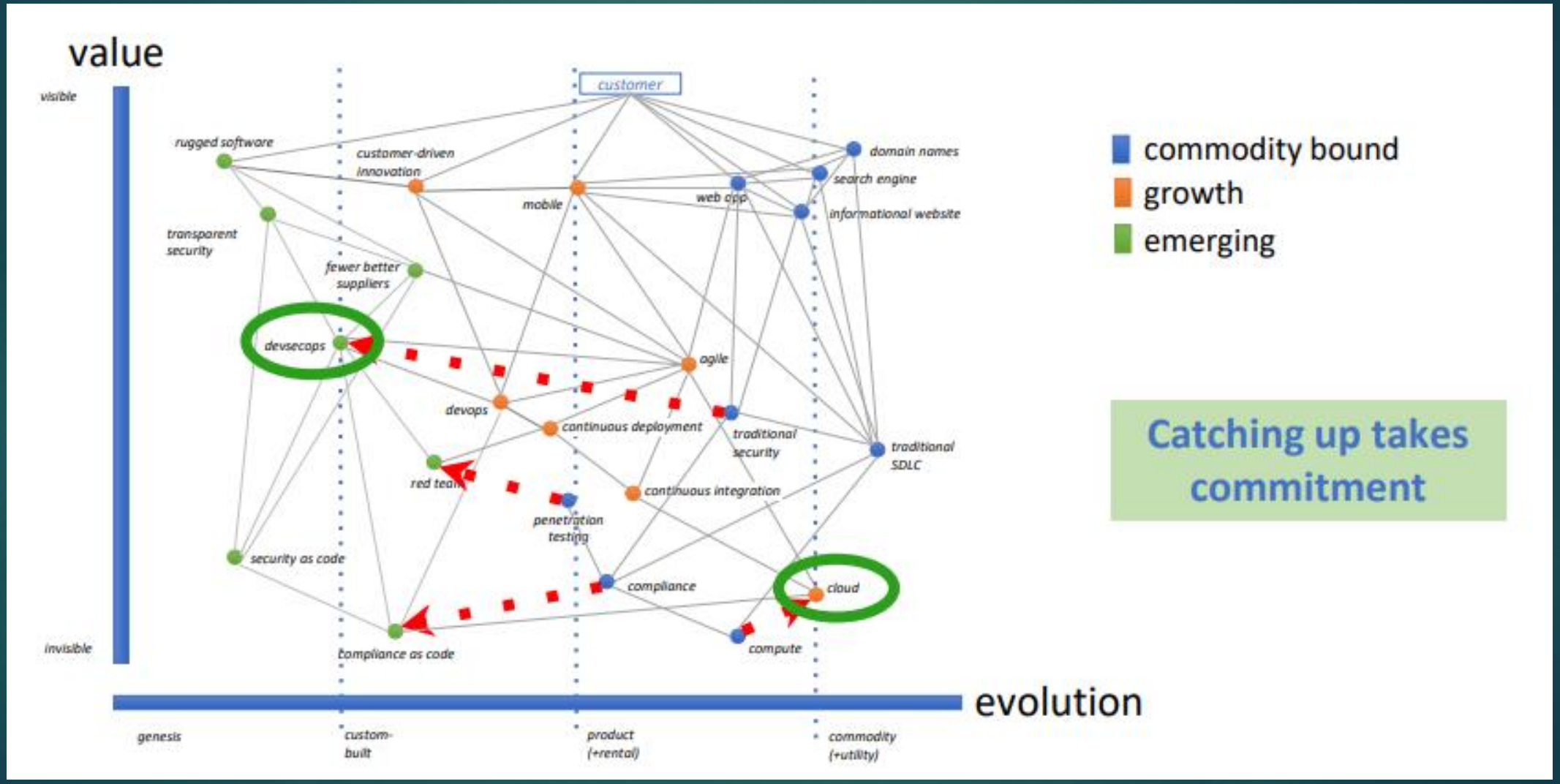


DEVSECOPS
-- FOUNDER -
-

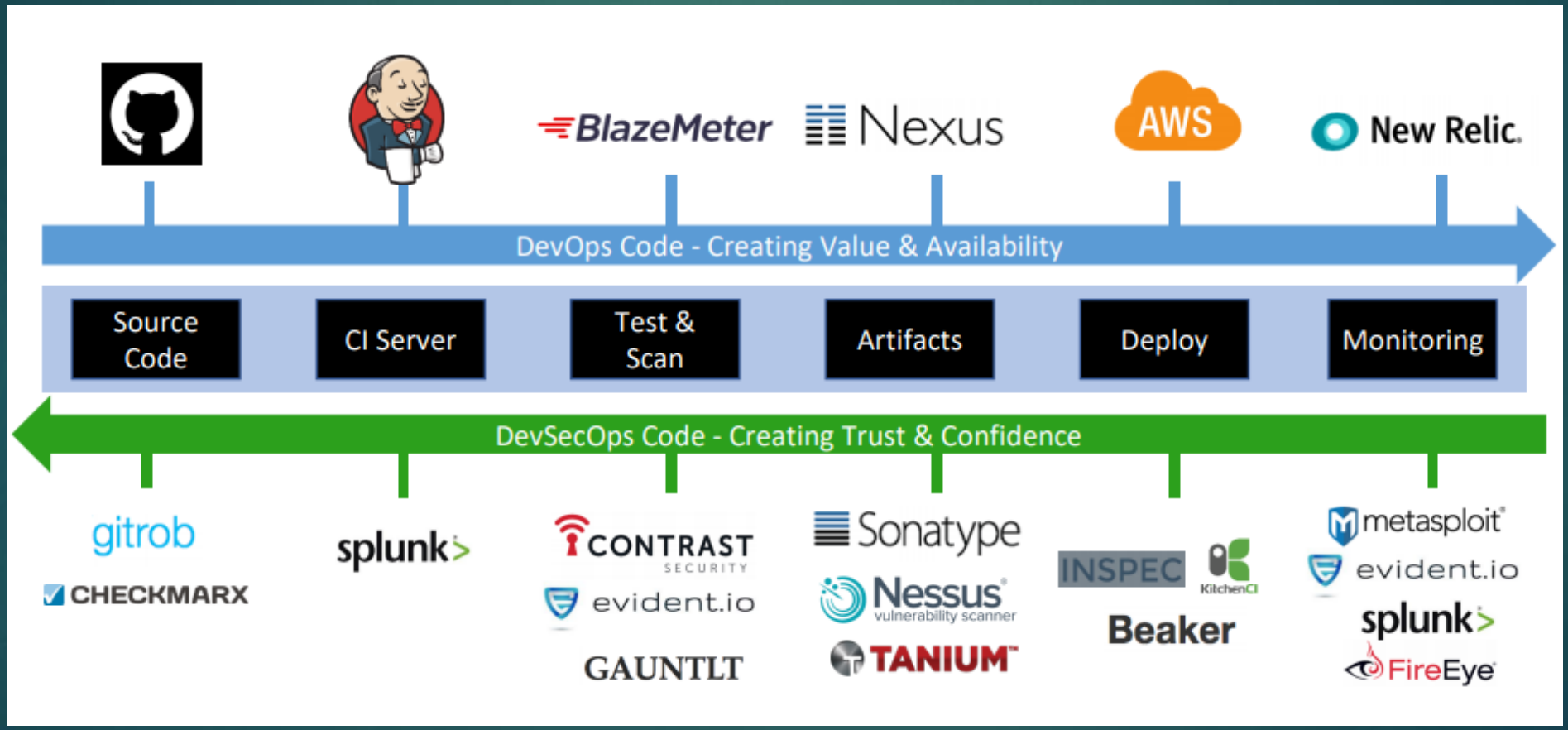
HACKERGIRL

All Day DevOps

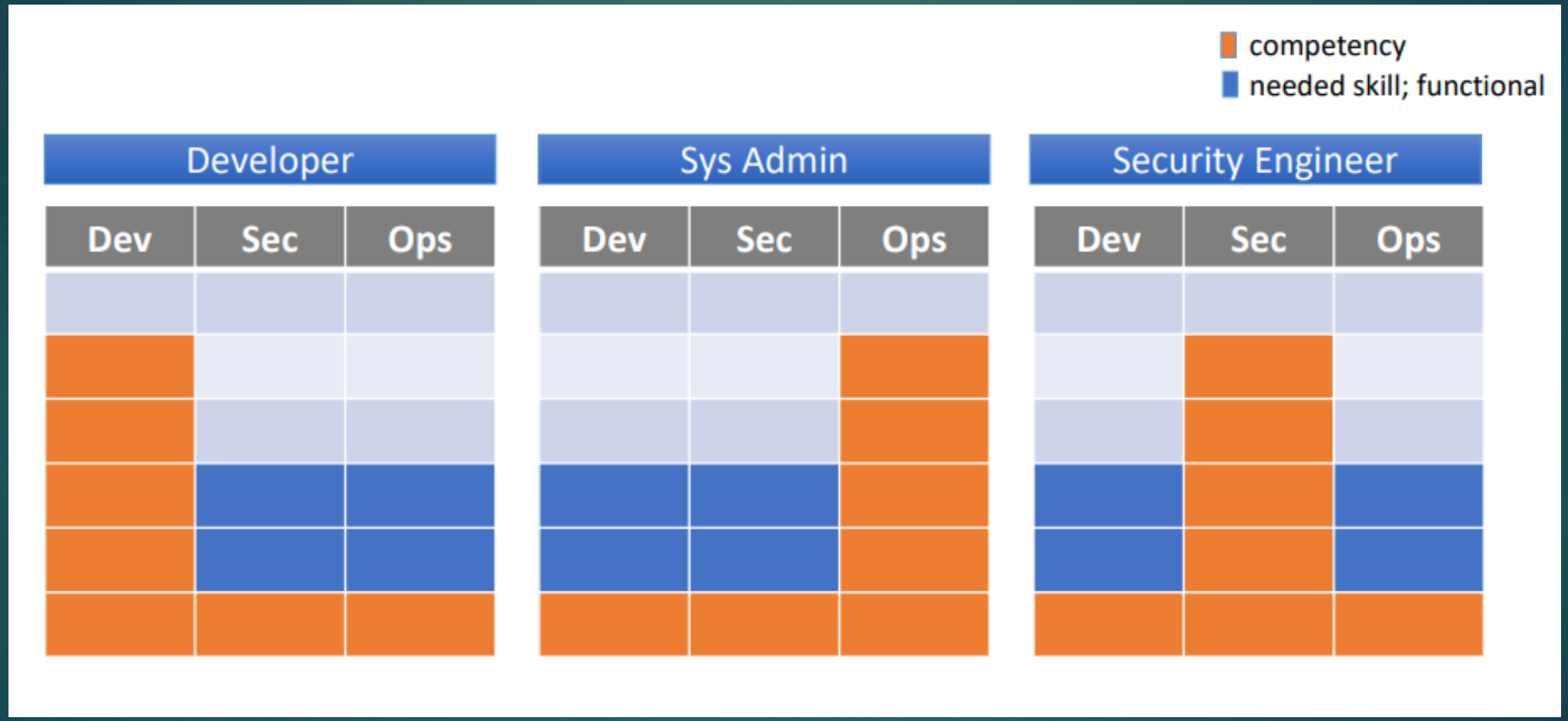
Why Change


value
visible
invisible
customer
rugged software
customer-driven innovation
mobile
web app
domain names
search engine
informational website
transparent security
fewer better suppliers
devsecops
agile
devops
continuous deployment
traditional security
traditional SDLC
red team
continuous integration
penetration testing
security as code
compliance
cloud
compute
compliance as code
evolution
genesis
custom-built
product (+rental)
commodity (+utility)
commodity bound
growth
emerging
Catching up takes commitment

How Hard



What Skills are needed?



THANK YOU