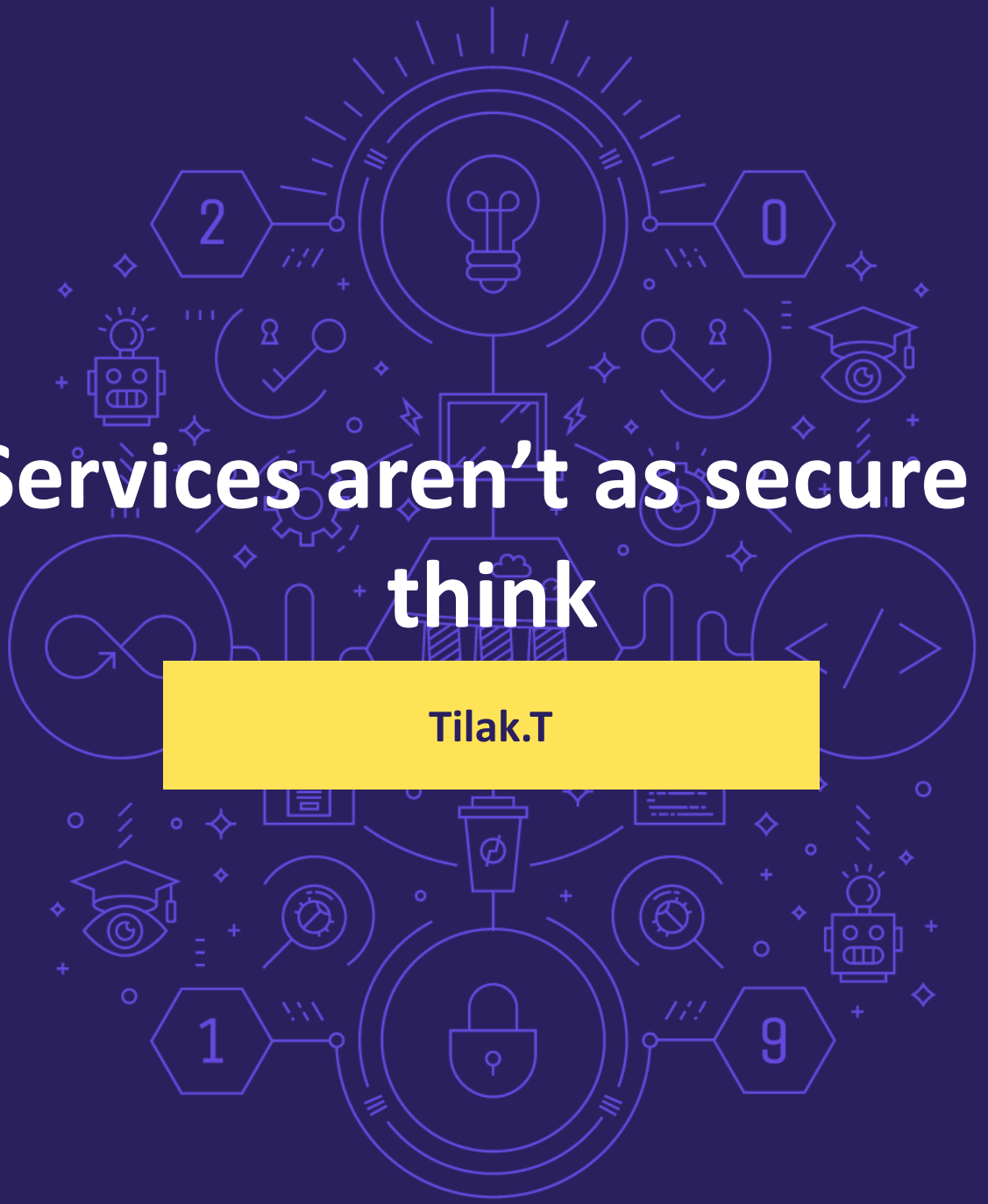
DevSecCon



Web Services aren’t as secure as we think

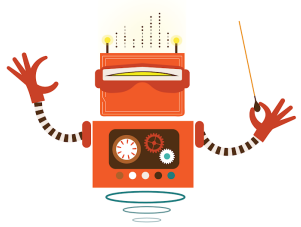
Tilak.T

we45

Singapore | 28 Feb - 01 Mar 2019

Yours truly

- Senior Solutions Engineer at we45
- Full Stack Developer
- Developer of Open-Source
- Trainer and Speaker
- PSF Member
- Part of multiple CTF



ORCHESTRON

@ti1akt

Outline

- Why security is important
- Unique Vulnerabilities
- Demo !
- DevSecOps Pipeline

Why web services aren't secure

API (Application Programming Interface) vulnerabilities are becoming more widespread as time goes by. Figure 4 shows the number of API vulnerabilities between 2015-2018. New API vulnerabilities in 2018 (264) increased by 23% over 2017 (214), by 56% compared to 2016 (169), and by 154% compared to 2015 (104).

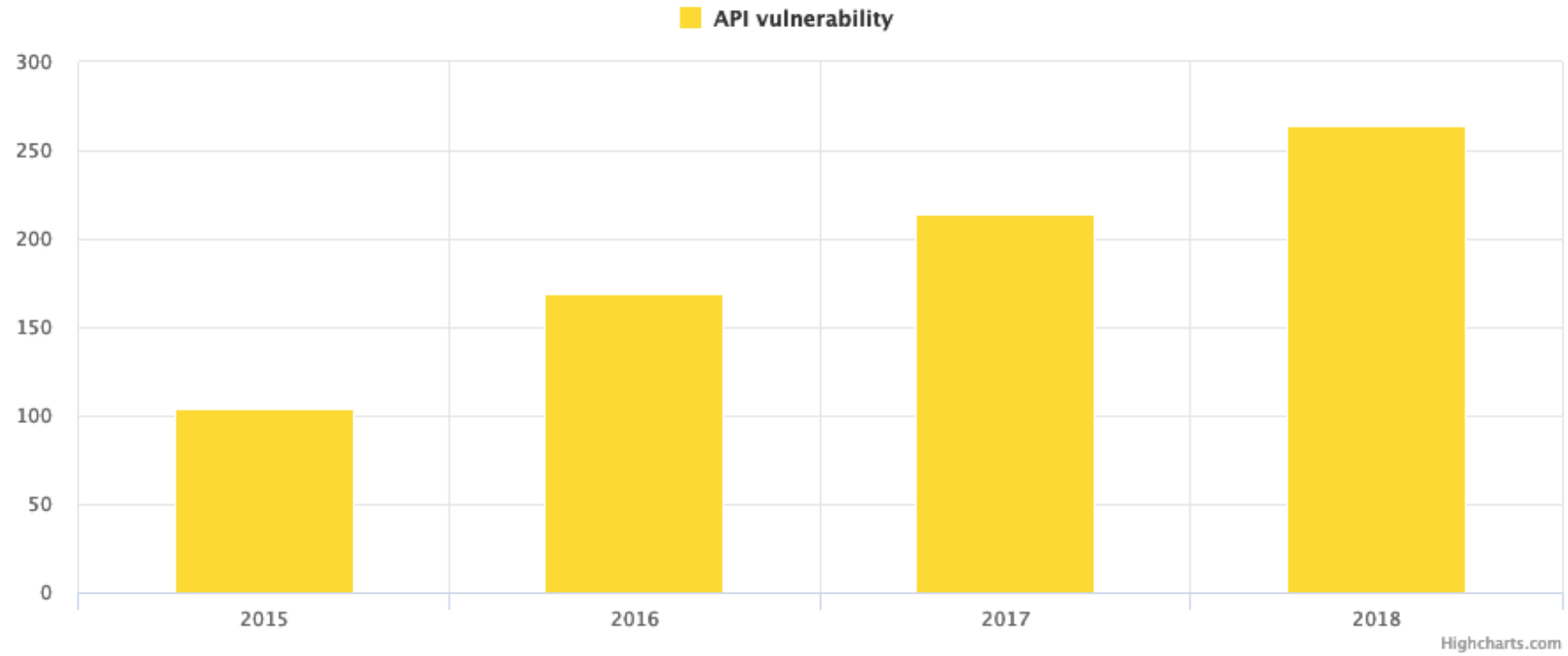


Figure 4: API vulnerabilities 2015-2018

Ref: https://www.imperva.com/blog/the-state-of-web-application-vulnerabilities-in-2018/

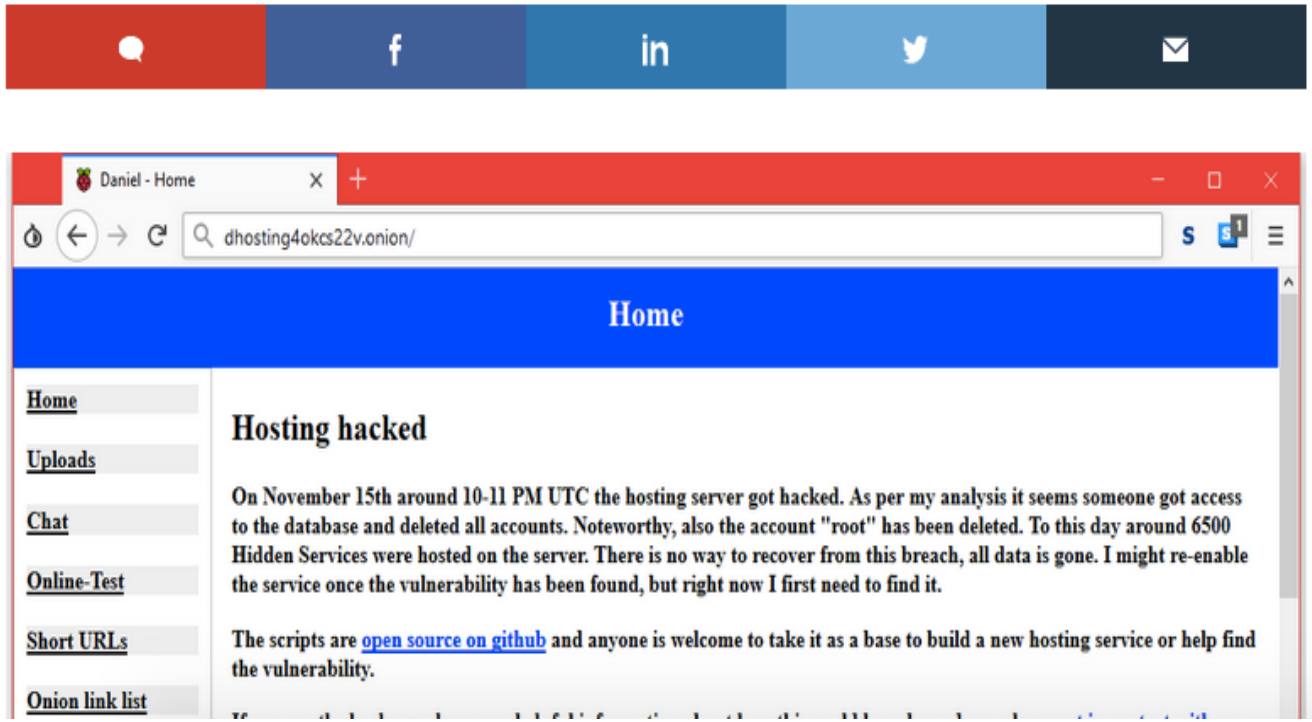
Unique Vulnerabilities

- JWT Manipulation
- Insecure Deserialization
- Insecure Direct Object Reference
- Etc …

Popular Dark Web hosting provider got hacked, 6,500 sites down

Hosting provider is still looking for the hacker's point of entry.

By Catalin Cimpanu for Zero Day | November 17, 2018 -- 21:39 GMT (03:09 IST) | Topic: Security



MORE FROM CATALIN CIMPANU

Security
Malware that hunts for account credentials on adult websites tripled in 2018

Security
A third of all Chrome extensions request access to user data on any site

Security
Microsoft publishes security alert on IIS bug that causes 100% CPU usage spikes

Security

@ti1akt

JWT Manipulation

OWASP-2017 A5 Broken Access Control

@ti1akt

Why JWT

- Stateless Application
- Authorization Mechanism
- Transfers information between server and client
- Scalable and decoupled

@ti1akt

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ
zdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4
gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJ
SMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
```

@ti1akt

Lots of ways to get JWT wrong

- Modify the algorithm to `none`
- Leakage of sensitive information
- Algorithm Confusion
- Cracking Secret Keys

@ti1akt

CVE-2018-15801: Authorization Bypass During JWT Issuer Validation with spring-security

Severity

Low

Vendor

Spring by Pivotal

Description

Spring Security versions 5.1.x prior to 5.1.2 contain an authorization bypass vulnerability during JWT issuer validation. In order to be impacted, the same private key for an honest issuer and a malicious user must be used when signing JWTs. In that case, a malicious user could fashion signed JWTs with the malicious issuer URL that may be granted for the honest issuer.

Affected Pivotal Products and Versions

Severity is low unless otherwise noted.

@ti1akt

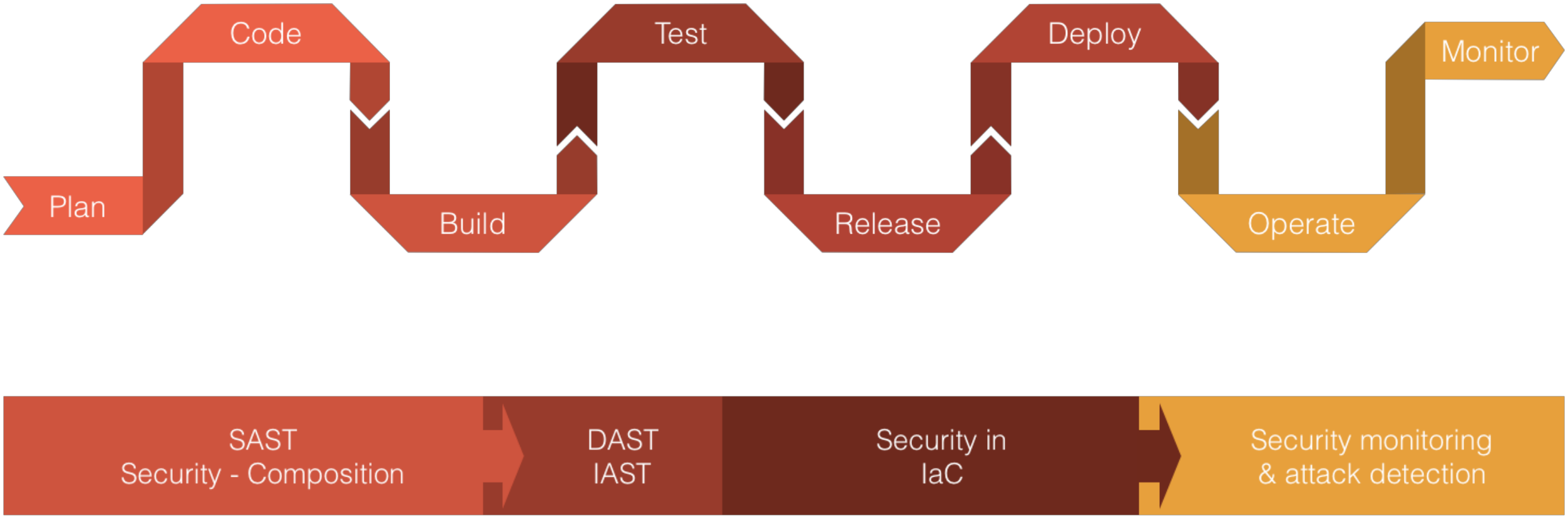
Insecure Deserialization

OWASP-2017 A5 Broken Access Control

@ti1akt


TIME FOR SOME
ACTION
imgflip.com

@ti1akt

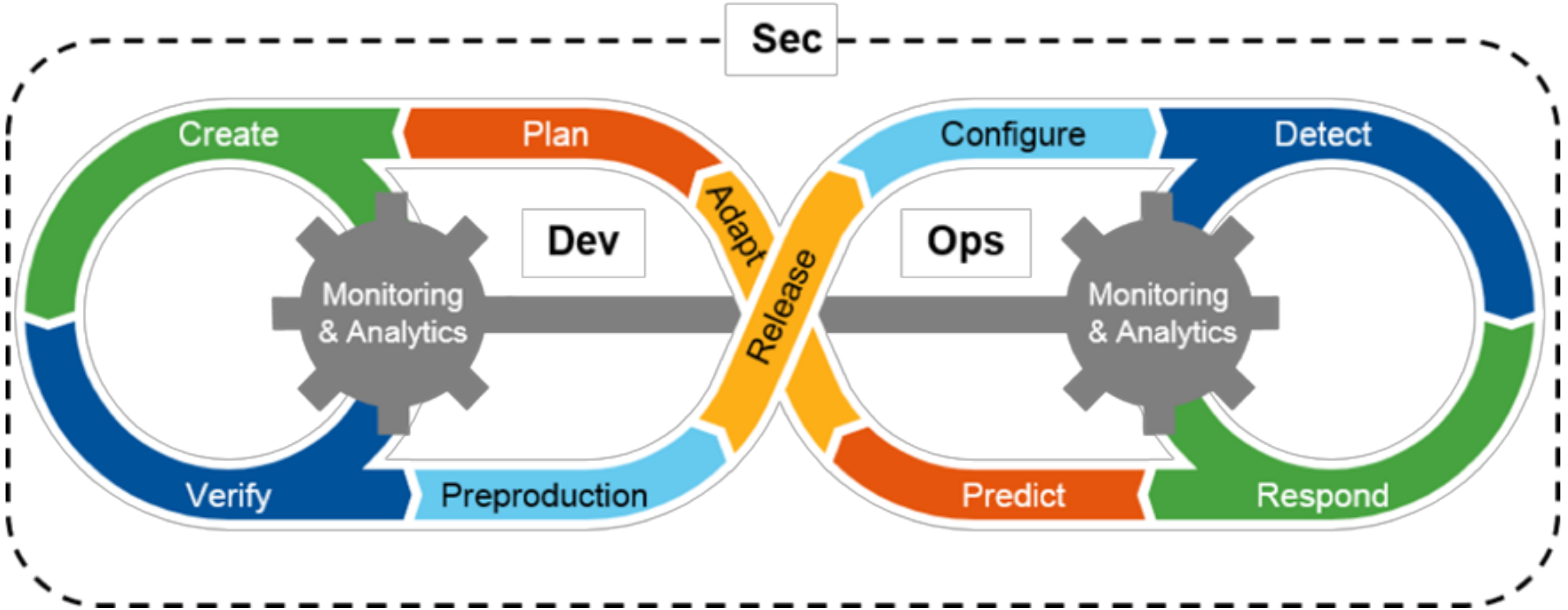

Plan
Code
Build
Test
Release
Deploy
Operate
Monitor
SAST
Security - Composition
DAST
IAST
Security in
IaC
Security monitoring
& attack detection

@ti1akt

"Our average customer takes 174 days to fix a vulnerability found when using dynamic analysis in production. However, our customers that have implemented DevSecOps do it in just 92 days. If we look at vulnerabilities found in development using static analysis, an average company takes 113 days, while the DevSecOps companies take just 51 days. [It's] a pretty drastic improvement," says O'Leary. "In addition, vulnerabilities that were found and fixed in just 10 days for an average customer were just 15 percent of the total number of vulnerabilities ultimately fixed. For DevSecOps companies, 53 percent of vulnerabilities found were fixed in just 10 days."

Basic Pipeline Demo

SecDevOps Jenkins pipeline


Sec
Create
Plan
Configure
Detect
Dev
Adapt
Release
Ops
Monitoring & Analytics
Monitoring & Analytics
Verify
Preproduction
Predict
Respond

@ti1akt

DevSecCon

Abhay Bhargav
Rahul Raghavan
Sandeep Patil
Sharath Kumar
Nithin Jois

Singapore | 28 Feb - 01 Mar 2019

DevSecCon

Thank You

https://github.com/we45/DevSecCon2019

@ti1akt