Doing More With Less - DevSecOps With Limited Budget

Pramod Rana (@IAmVarchashva)

Sr. Manager, Application Security Assurance

Thank You to Our Sponsors and Hosts!

AppSec NZ
appsec.org.nz

OWASP NEW ZEALAND
owasp.org.nz

AUT UNIVERSITY
TE WĀNANGA ARONUI O TAMAKI MAKAU RAU

BASTION
SECURITY GROUP

DATACOM

aws

84.

PentesterLab

plexure

VERACODE

Without them, this Conference couldn't happen.

About Me

- Sr. Manager - Application Security Assurance @Netskope
- Responsible for Security Testing & DevSecOps functions
- Author of three open source products:

  Omniscient - LetsMapYourNetwork: a graph-based asset management framework

  vPrioritizer - Art of Risk Prioritization: a risk prioritization framework

  CICDGuard - SecurityOFCICD: Orchestrating visibility and security of CICD ecosystem
- Speaker @BlackHat | Defcon | OWASPGlobalAppSec | Insomnihack | HackInParis | nullcon | HackMiami
- OWASP Pune Chapter Leader | OSCP

Agenda

- DevSecOps - What, Why, How
- Cost Challenge
- Cost Analysis
- Optimization Tips and Techniques
- Use Cases

DevSecOps - What, Why, How

WHAT

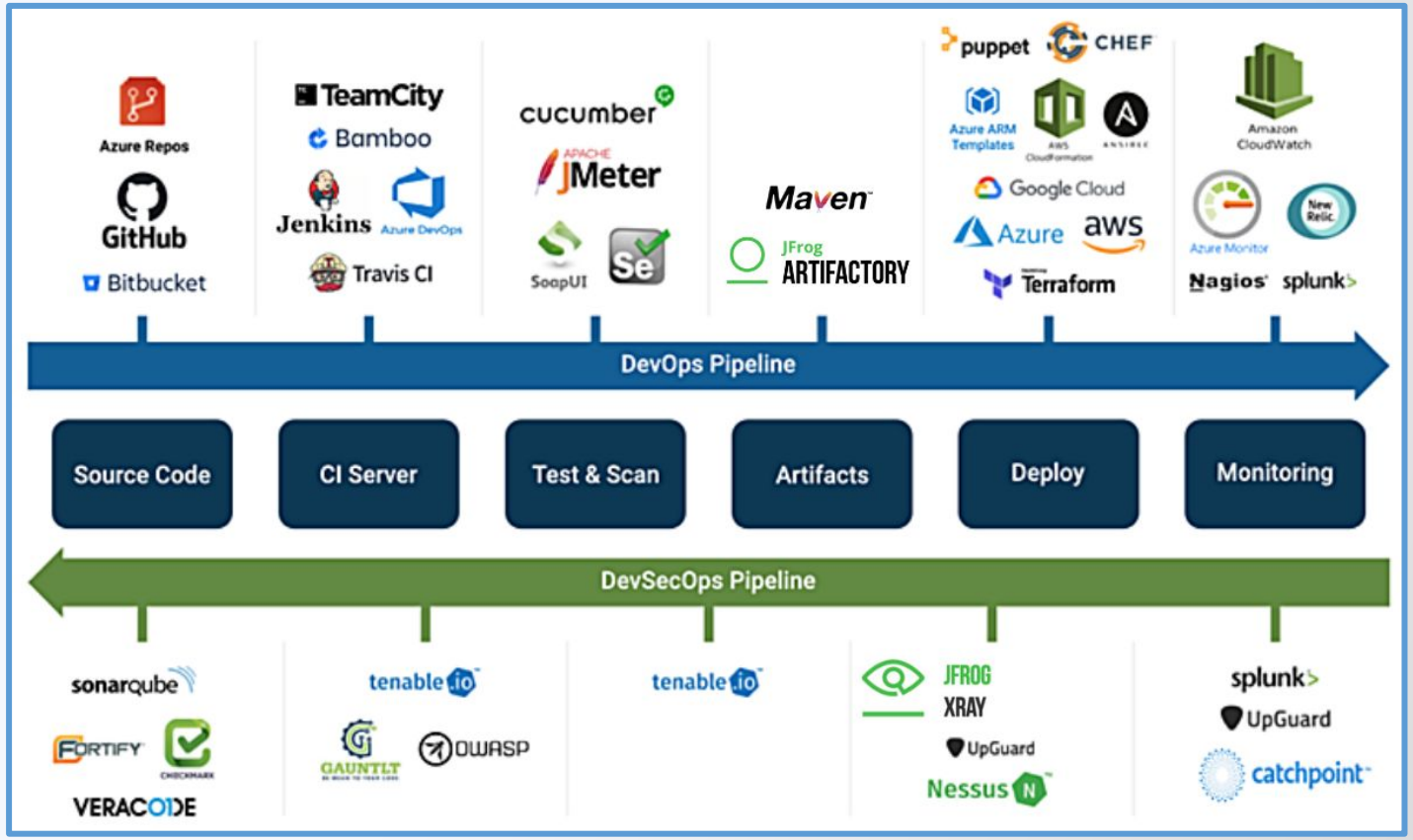
DevSecOps - Development, Security, and Operations - All integrated together

WHY

It's imperative to adopt DevSecOps to build software faster and secure

HOW

DevSecOps works on each layer of People, Process and Technology



Cost Challenge

I Have Unlimited Security Budget

said **NO CISO** ever…

Cost Challenge

In today's time everyone will agree and we have enough data to prove that

- Business demands software fast and frequent and secure
- Technologies are growing at unprecedented rate
- Organizations are operationally complex
- Software security skill gap is real
- Software security is tough
- Budget is limited

Cost Analysis

Cost to security teams (IDENTIFYING the security

- Building and maintaining a security team is a challenging and expensive process
- Technology space is growing faster than ever -> ChatGPT 1M users within 5 days. Ref
- Security skill gap is very real - both in depth and breadth
- Contextual understanding is limited

Cost to product teams (FIXING the security gaps)

- Prioritizing fix of security gaps, by definition, means giving resources from feature development
- Lack of contextual understanding means product teams work on not-applicable and/or non-severe vulnerabilities

Security is a

Cost Center

or

Profit Center

Optimization Tips and Techniques

- ~~Automation~~ Effective Automation
- Shift Left != Pushing security to developer
- Shift Left = Developer and security team working together
  - Security team understanding the business and SDLC and providing security capabilities accordingly
  - Development teams need to be proactive in adopting the capabilities and providing suggestions
  - Every organization need “security warrior” - an extension of security team
- Contextual analysis is key. Severity != Risk.
  - Every organization has different risk and thus different approach for each vulnerabilities

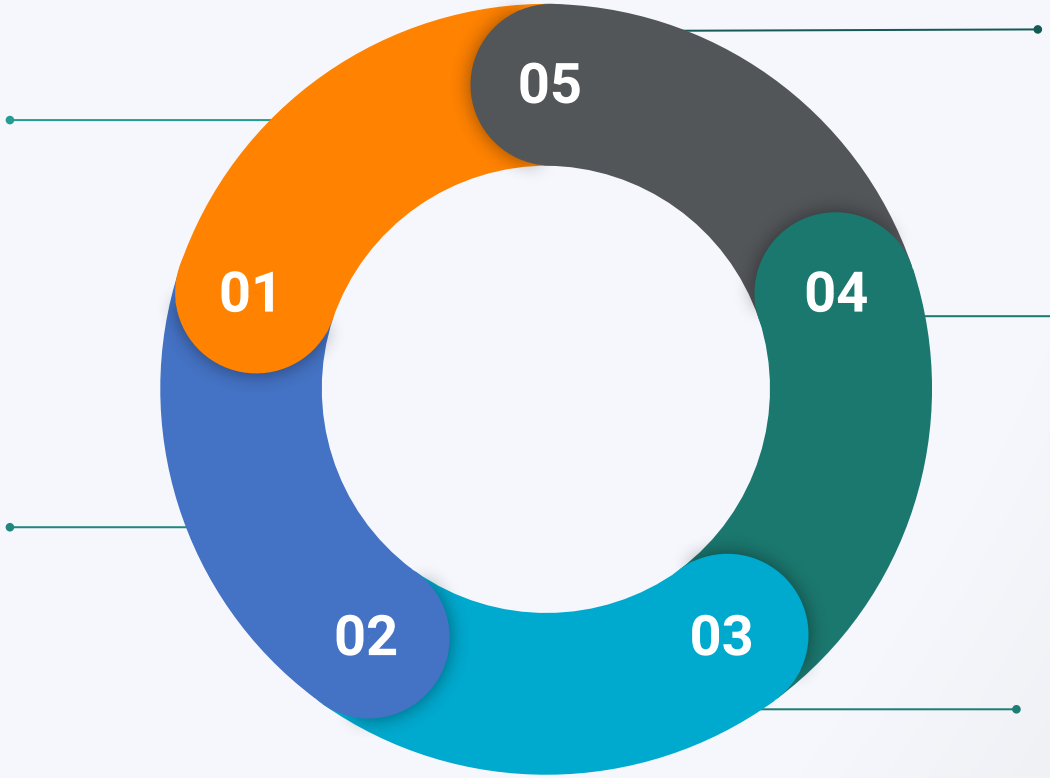
Use Case - Secret Validator

Scanning Engine

Scanner with defined regexes periodically scans entire codebase for hard coded secrets

Validation

Validator validate the identified secret against universal endpoints such as GitHub PAT



(Re)Prioritization

Secrets get (re)prioritized depending on analysis done by automation. Validation > Context Analysis > Endpoint Analysis

Endpoint Analysis

Endpoint analysis engine identifies the endpoint to validate the secrets and assign confidence to it

Context Analysis

Context analysis engine identifies the additional context of secrets -> complimentary secrets like AWS_SECRET_ID and AWS_Secret_Key

Use Case - Security Warriors

- Security warrior is a liaison between the security teams and their engineering groups - developers, QA, DevOps, SRE
- Different trainings and guidance to onboard the security warriors
- Periodic awareness sessions and knowledge sharing with security warriors, combination of in-person and virtual
- Dedicated communication channel for any ad-hoc queries, questions, feedback
- Practically working as an extension of security teams and making sure that security is followed right from the start

Thank you!

@IAmVarchashva