SkillOps
Real-World Approaches to Skilling and building World-Class Security and Technology Teams
Abhay Bhargav

- Founder @ we45 and AppSecEngineer
- Chief Architect - Orchestron
- Avid Pythonista and AppSec Automation Junkie
- Trainer/Speaker at DEF CON, BlackHat, OWASP Events, etc world-wide
- Lead Trainer - we45 Training and Workshops
- Co-author of Secure Java For Web Application Development
- Author of PCI Compliance: A Definitive Guide
Community Initiatives

YouTube Channel: https://bit.ly/3hmAleC

Blog: abhaybhargav.com

Talks/Workshops at several OWASP Events
Agenda

• The Changing nature of IT and IT Security jobs

• SkillOps - A Perspective on Training a new generation of professionals

• Conclusions
2020 and 2021

CORONA LISA

BECAUSE...

IT'S IN THE CLOUD

SOLARWINDS

Password: solarwinds

SOLARWINDS

Password: solarwinds123
Some numbers

3.12 MILLION Jobs going unfilled (ISC2)

99% Cloud Security Failures Will be attributed to customers (Gartner)

32% IT Budgets will be On the cloud (Forbes)

52% Hands-on skills required For cyber-security education (ISSA)

70% Organizations impacted by Talent shortages (ISSA)
And of course...

100:10:1

Dev    DevOps    InfoSec
Before

• Security Consulting

• Vulnerability Assessment & Penetration Testing

• Threat Modeling

• Vulnerability Management

LOTS AND LOTS AND LOTS OF WORK!
Now...

• Security Consulting
• Bug Bounty

• Vulnerability Assessment & Penetration Testing
• Threat Hunting

• Threat Modeling
• Red-Teaming

• Vulnerability Management
• Cloud Security

• DevSecOps
• Kubernetes Security
The best teams...

- Decentralize
- Treat Engineering as a Customer
- Security Defaults
How “SkillOps” can help

Continuous, Micro Training

Hands-on + Cyber-Ranges

Purple-Team Training Approach
Continuous, Micro Training

- Works well with a Distributed Workforce
- Encourages small-wins. Builds on the compounding effect
- 45 mins to 1 hour courses with hands-on content
- Focused Content with Hands-on Labs and Cyber-Ranges
For example

- Authentication and Authorization with Kubernetes vs Kubernetes Security
- AWS Network Security vs AWS Security
- Implementing Security Workflows with Jenkins vs DevSecOps with Jenkins
Hands-on + Cyber-Ranges

- Hands-on Labs are essential for building skills in InfoSec

- Easy to run, easy to setup

- Element of Challenge is always something that can go a long way

- Capture and Defend-the-Flag events
The problem with Security Training

- Security industry has had an obsession with red-team or exploit-focused education.
- However, the needs from security folks have changed to include defence implementations as well.
- Added to that, Cloud-Native technologies require a greater understanding of defensive configurations and parameters.
Purple–Teaming Security Training

• Technical Security Training works when you demonstrate offensive concepts contrasted with defensive concepts

• Works across team constituents - developers, security engineers, architects, DevOps

• Mix in Security Defaults to make secure patterns more effective
Existing Resources

• AppSecEngineer - AppSec, Cloud Security, Kubernetes, Threat Modeling and other Micro-Training offerings

• Web Security Academy from Portswigger

• HacktheBox

• TryHackMe
Conclusions

• Training is essential when you want to build successful Security (and Technology teams)

• Leverage continuous, Micro-training that is remote-friendly

• Hands-on Labs and Cyber-Ranges are essential

• Offensive and Defensive Security education are necessary
Thank you!

abhaybargav

we45

AppSecEngineer

AppSecEngineer.com

abhaybhargav