PRACTICAL DEVSECOPS 2023

Tools & Techniques to Embed Security as part of the DevOps Pipeline

20-22 February 2023 I Sheraton Imperial Hotel KL

We all have heard about DevSecOps, Shifting Left, Rugged DevOps but there are no clear examples or frameworks available for security professionals to implement in their organization. This hands-on course will teach you exactly that, tools and techniques to embed security as part of the DevOps pipeline. Delegates will learn how unicorns like Google, Facebook, Amazon, Etsy handle security at scale and what we can learn from them to mature our security programs.

In this course, you will learn how to handle security at scale using DevSecOps practices. We will start off with the basics of the DevOps, DevSecOps and move towards advanced concepts such as Threat Modelling as Code, RASP/IAST, Container Security, Secrets management, etc

COURSE TRAINER

Mohammed A. "Secfigo" Imran is the Founder of Hysn/Practical DevSecOps and seasoned security professional with over a decade of experience in helping organizations in their Information Security Programs. He is the author of the DevSecOps Studio and Awesome Fuzzing and also listed as top #50 Influential #DevSecOps experts in the world. He has a diverse background in R&D, consulting, and product-based companies with a passion for solving complex security programs. Imran is the founder of Null Singapore. He was also nominated as a community star for being the go-to person in the community whose contributions and knowledge sharing has helped many professionals in the security industry. He is a regular speaker at Blackhat, DevSecCon, AppSec, All Day DevOps, Nullcon,and many other international conference in USA, UK, Europe, Australia and Asia.

BENEFITS OF ATTENDING:

- Create a culture of sharing and collaboration among the stakeholders.
- Start or mature your application security program using DevOps practices
- Scale security team's effort to reduce the attack surface.
- Embed security as part of DevOps and CI/CD Start or mature your application security program using modern Secure SDLC practices.
- Harden infrastructure using Infrastructure as Code and maintain compliance using Compliance as Code tools and techniques.
- Consolidate and co-relate vulnerabilities to scale false-positive analysis using automated tools.

DELEGATES WILL RECEIVE

Course manuals & lab guide	Course videos, checklists & tools	Access to a dedicated slack channel	30 days Online Lab Access worth USD200.00	One exam attempt for Certified DevSecOps Professional (CDP), worth USD100.00

Exclusively by: THOMVELL international

Supported by: Practical DevSecOps

TRAINER

Mohammed A. “secfigo” Imran is the Founder and CEO of Hysn/Practical DevSecOps and seasoned security professional with over a decade of experience in helping organizations in their Information Security Programs. He is the author of the DevSecOps Studio and Awesome Fuzzing and also listed as top #50 Influential #DevSecOps experts in the world. He has a diverse background in R&D, consulting, and product-based companies with a passion for solving complex security programs. Imran is the founder of Null Singapore, the most significant information security community in Singapore, where he has organized more than 60 events & workshops to spread security awareness.

He was also nominated as a community star for being the go-to person in the community whose contributions and knowledge sharing has helped many professionals in the security industry. He is usually seen speaking and giving training in conferences like Blackhat, DevSecCon, AppSec, All Day DevOps, Nullcon, and many other international conference in USA, UK, Europe, Australia and Asia.
Practical DevSecOps is the world's first dedicated DevSecOps certification program. The certification are achieved after rigorous tests of skill and are considered the most valuable in the information security field with @secfigo highly rated workshops conducted worldwide.

TESTIMONIAL

“Thumbs Up! If you have an interest in #ShiftingLeft, #AppSec or #DevSecOps, highly recommend Imran’s workshop”. Software Engineer, **CODESTACK**

“Well-structured & above expectation. One of the best training platform, easy to use plus being the first certified in Malaysia, it help promotes the DevSecOps practice in the local cyber security community”. Head Cyber Defense, **CELCOM (M)**

“Excellent Course, learned how to mature DevSecOps process in an organization from scratch with hands-on experiences”. Snr Penetration Tester, **FIDELITY INVESTMENTS (UK)**

“Highly recommended & great support from technical team!”. DevOps Lead, **LEMVIGH-MULLER A/S (M)**

“Good course, well-structured with practical insights”. Security Professional, **ING (Europe)**

“Good program, covered lots of topics In Secure SDLC. Highly recommend this practical training”. Technologist, **Dow Jones, USA**

Certified DevSecOps Professional (CDP)

Issued by Practical DevSecOps

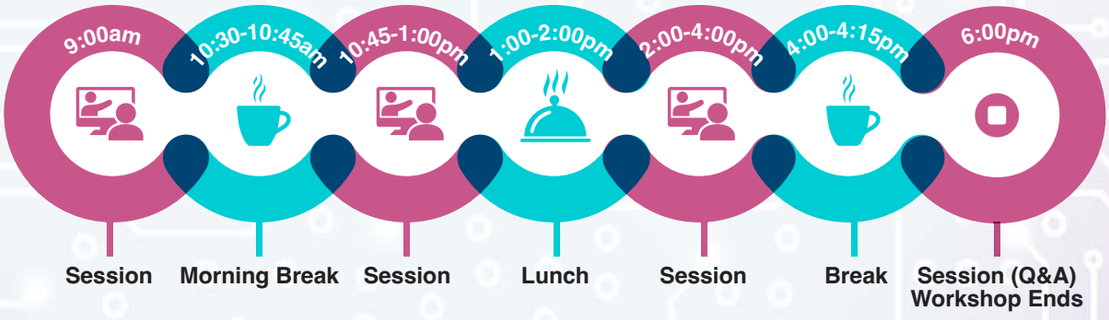
The CDP credential validates the practical expertise to understand, implement and manage the DevSecOps program in an organization. A CDP can assess the current state of DevSecOps, embed security as part of DevOps, manage vulnerabilities and improve the overall Maturity Level. CDP holders can also identify gaps in secure SDLC implementation, Implement security as part of DevOps using Software Component Analysis, Static Analysis, Dynamic Analysis tools, Infrastructure as Code & Compliance as code.

WHO SHOULD ATTEND

This course is aimed at anyone who is looking to embed security as part of agile/cloud/DevOps environments:

- Security Professionals
- Penetration Testers
- IT managers
- Developers
- Red Teamers
- DevOps Engineers

WORKSHOP TIMING



DELEGATES REQUIREMENTS

- There are no pre-requisites to attend this course however delegates will benefit from having some basic knowledge about linux commands like ls, cd, mkdir etc.,
- Delegates should have some basic understanding of application Security practices like OWASP Top 10 though not a necessity.

SOFTWARE AND HARDWARE REQUIREMENTS

Our state of the lab is deployed on AWS so you would need the following to connect to the lab environment:

1) Laptop with decent specs at least 4GB of RAM and a modern CPU to login into our lab VPN.
2) Administrator access to install software like VirtualBox, VPN client and change BIOS settings to enable virtualization