

Webinar on “DevSec Ops” In Association with Oracle Volunteering on 23rd June 2021

Centre of Excellence- Big Data Analytics organized a webinar entitled "DevSecOps Security" on 23rd June 2021 for the students of MCA. The webinar series was conducted in association with ORACLE Volunteering.

The speaker Mr. Deepak Agarwal started the session with Introduction of DevSecops and the need of it along with the difference between DevOps and DevSecops and how it involves injecting security practices into an organization’s DevOps pipeline. He continued the session with the main goal of DevSecops and how to incorporate security into all stages of the software development workflow. The speaker concluded the session with latest DevSecops tools in which security is adapted into all stages of software.



The image is a promotional flyer for a webinar. At the top, it reads "Center Of Excellence - Bigdata Analytics". Below this, the title "Session 3: DevSec Ops" is displayed in yellow and red. The date "Date: 23rd June 2021" and time "Time: 11 a.m to 12:30 p.m" are listed. A central diagram shows two interlocking gears: a blue gear for "Dev" with stages "code", "plan", "test", and "build"; and a purple gear for "Ops" with stages "deploy", "operate", and "monitor". A red arrow labeled "release" connects the two gears. On the bottom left, a grey box identifies the speaker as "Expert Deepak Agarwal, Principal member of Tech Staff". On the bottom right, a white and yellow graphic states "Organizes WEBINAR SERIES In Association With ORACLE Volunteering".

Center Of Excellence - Bigdata Analytics

**Session 3:
DevSec Ops**

Date: 23rd June 2021
Time: 11 a.m to 12:30 p.m

Expert
Deepak Agarwal,
Principal
member of Tech Staff

Organizes
WEBINAR SERIES
In Association With
ORACLE
Volunteering

Photo 1 : Broacher

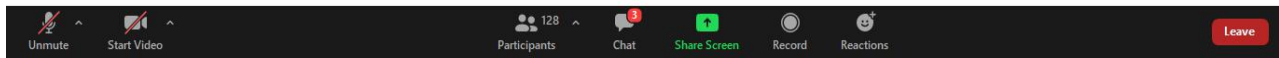


How Does DevSecOps Work?

Nowadays the greatest obstacle to DevSecOps is culture, not technology. Traditionally, security teams work separately. To successfully move to a DevSecOps methodology, follow the DevOps methodology for both Sec. and Dev. Teams must make application security an integrated strategy and continue to educate on security awareness.

Effective ways to adopt it:

- Automate the process as much as possible.
- Follow the DevOps methodology.
- Train to code securely.
- Evaluation of current security measures and concluding what to do to overcome problems.
- Integrate the security to DevSecOps.
- By adopting the right DevSecOps tools.
- Monitoring Continuous Integration and Continuous Delivery.
- Analyze code and do a vulnerability assessment.
- Mandatory security at every stage.



1. Working of DevSecops

The screenshot shows a Zoom meeting interface. The main content is a slide titled "DevSecOps Pipeline" which features a circular diagram with the following components: Code Review, Static Analysis, Threat Model, Log, Audit, Deploy, Threat Intelligence, Monitor, Detect, Response, Recover, Compliance Validation, Release, Plan, Policies, Build, Test, Penetration Testing, and Operate. The diagram is divided into two main paths: a blue path on the left (Code Review, Build, Test, Penetration Testing) and an orange path on the right (Audit, Deploy, Operate, Recover). The center of the diagram includes Threat Model, Log, Policies, Release, and Compliance Validation. The Zoom interface also shows a list of 130 participants on the right side.

2. Pipeline of DevSecops



3. Difference between DevOps and DevSecOps

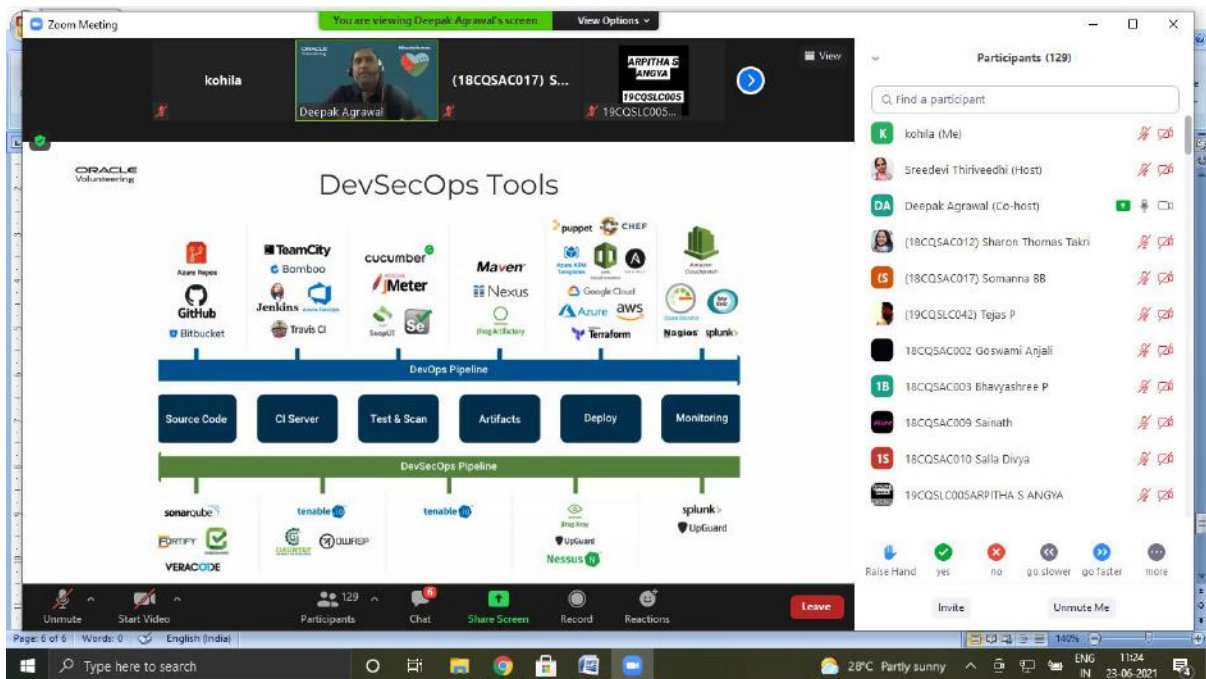


Photo 5: DevSecops Tools