DevOps Bootcamp

18 PMI PDUs | 18 IIBA CDUs

Format: Live Instructor-Led Online through Zoom
Duration: Four 5 hour sessions

Technology and Attendance Requirements: Computer with a browser, Zoom, a microphone and speaker. For this workshop, camera should be on if possible and you must be actively participating.

Any project professional wanting an introduction into DevOps value stream mindset, workflows and requirements.

This course will cover DevOps Fundamentals and DevOps Security. In solving one problem, agile has created a new bottleneck at the interface between development and operations teams (and others such as security teams), each having very different goals. DevOps has evolved as a way to bring these teams together and accelerate the delivery of value to the users and customers.

Taking a holistic view, the course looks at what is needed from the perspectives of the people and culture, the processes followed, and the technology used. The experiences of organizations successfully applying DevOps is used to drive an evidence-based approach to change. Emphasis is placed on using value stream mapping to understand the big picture and identify any improvements to make.

DevSecOps is taking DevOps and integrating IT teams and security experts, from the beginning, to plan and develop in stages and looking at security in those stages instead of just looking at security at the end of the project. To understand what you need to be "concerned" about you will learn vulnerabilities and security risks so that you can prevent them and build a secure DevOps operation and move your DevOps to DevSecOps.

Learning Outcomes:

- Identify practices to support the desired culture
- Evaluate how effectively the current technical practices support the delivery of value
- Use value stream mapping to understand the needs and constraints
- dentify what changes to make as part of continuous improvement
- Identify cyber security risks and stay up to date with the latest threat tactics as they emerge and change
- Assess the impact of security threats on different phases of the software development lifecycle (SDLC)
- Use good practices for building a secure DevOps pipeline.

Content:

- History and challenges that led to DevOps
- Cultural challenges and effective leadership
- Changing the culture and processes
- Value stream mapping
- Effective use of the supporting technical practices (e.g. continuous integration, infrastructure as code)
- Getting useful telemetry to understand where any problems are
- Architecture and its impact on delivering value
- Incorporating security / DevSecOps
- Building a pipeline for CI (Continuous Integration) / CD (Continuous Delivery)
- Continuity planning, SRE (Site Reliability Engineering), and ITIL (IT Infrastructure Library)
- Understand Security risks and threats
- Securing DevOps Pipeline