INTRODUCTION TO S-SDLC

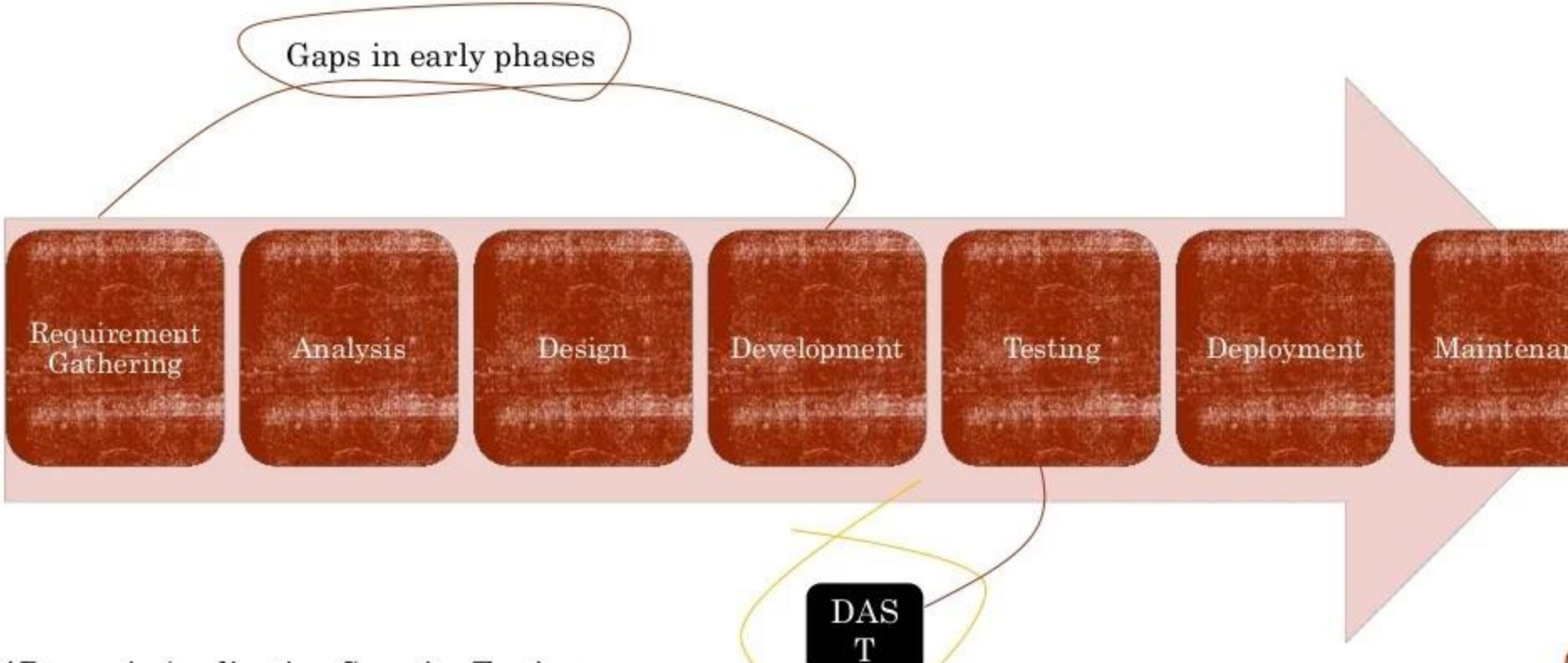
Rishi Kant

AGENDA

- ❑ About me
- ❑ DAST Process in typical organizations
- ❑ Classical Integration of DAST in SDLC
- ❑ Gaps of an AppSec Program
- ❑ Gaps aren’t covered by SAST & DAST tools
- ❑ Statistics analysis of remediation cost/stages
- ❑ AppSec. quality improvement approach
- ❑ S-SDLC | Type 1 | Waterfall
- ❑ S-SDLC | Type 2 | Agile
- ❑ Comparison of all 2 approach

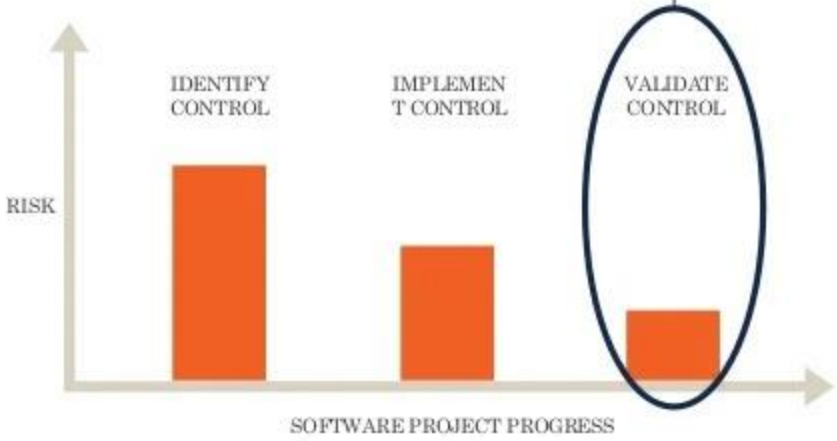
DAST PROCESS IN TYPICAL ORGANIZATIONS

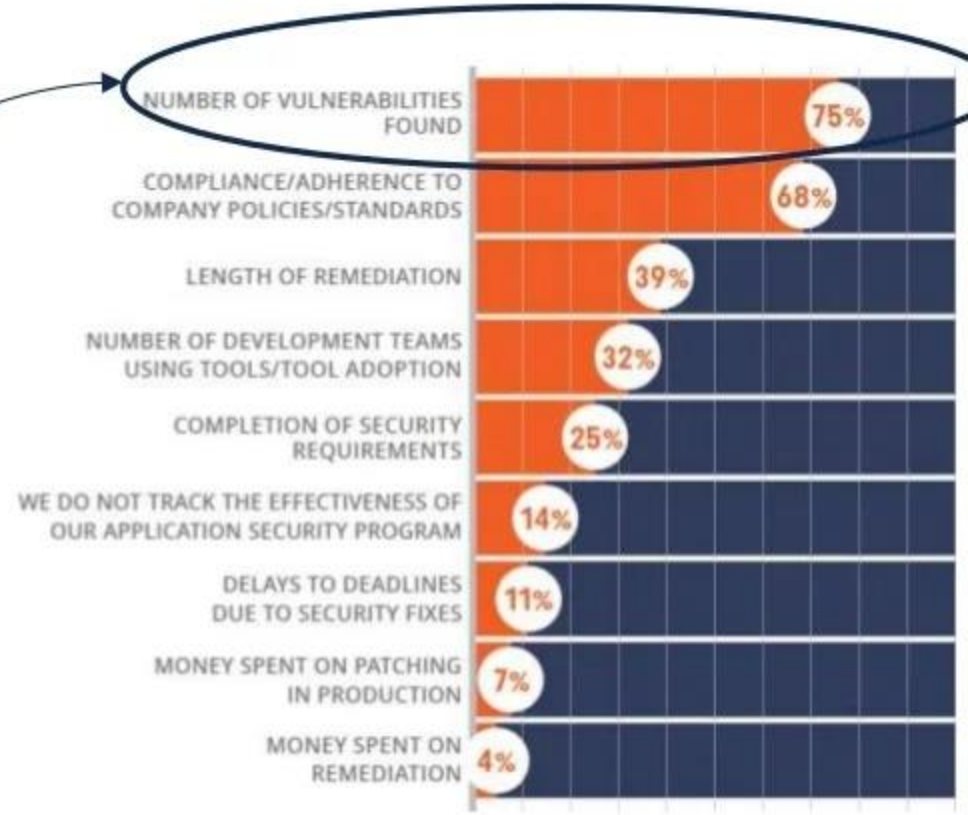
CLASSICAL INTEGRATION OF DAST IN SDLC



GAPS OF AN APPLICATION SECURITY PROGRAM

We have jumped straight to validation without identifying the root cause and implementing the appropriate controls to reduce application security risk.





GAPS ARE NOT COVERED BY SAST & DAST TOOLS

70% of risks **unaddressed**

*Adapted from:
National Institute of Standards and Technology. "Report on the Static Analysis Tool Exposition IV".
Gartner for Technical Professionals. "Application Security Think Big and Start with What Matters".

GAPS ARE NOT COVERED BY SAST & DAST TOOLS

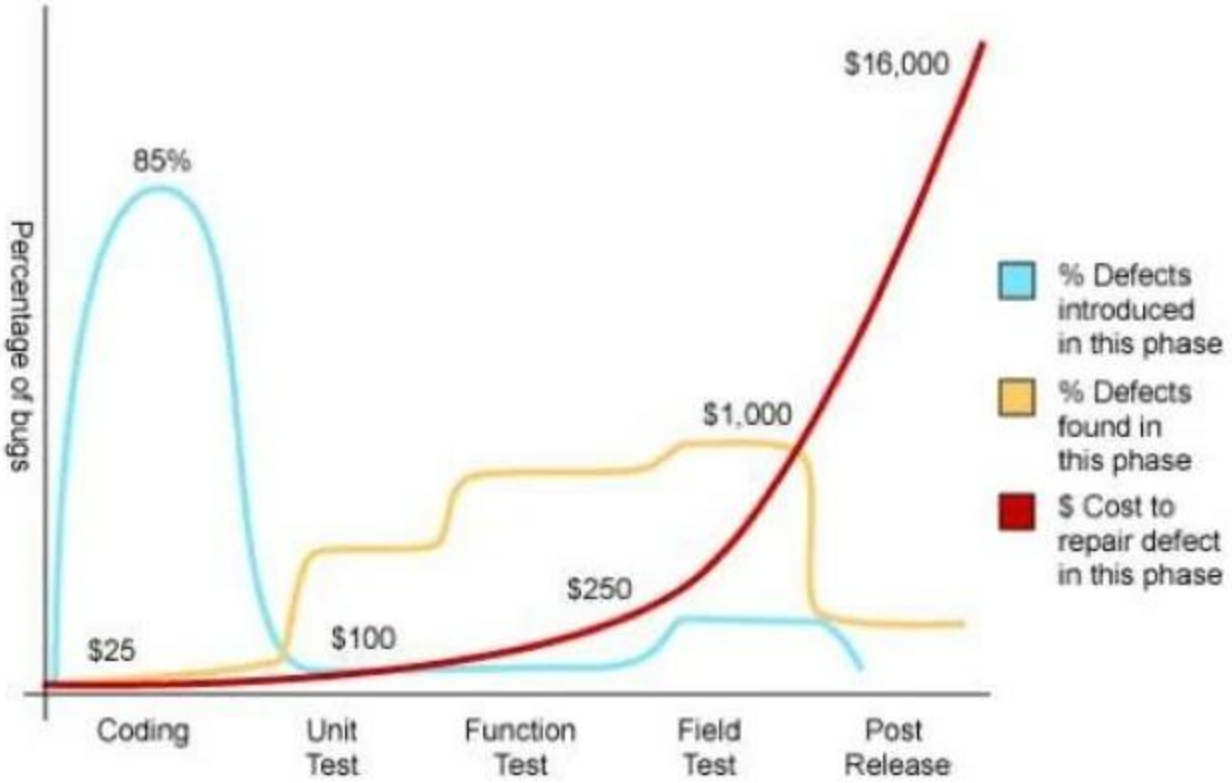
70% of risks **unaddressed**

*Adapted from:
National Institute of Standards and Technology. "Report on the Static Analysis Tool Exposition IV".
Gartner for Technical Professionals. "Application Security Think Big and Start with What Matters".

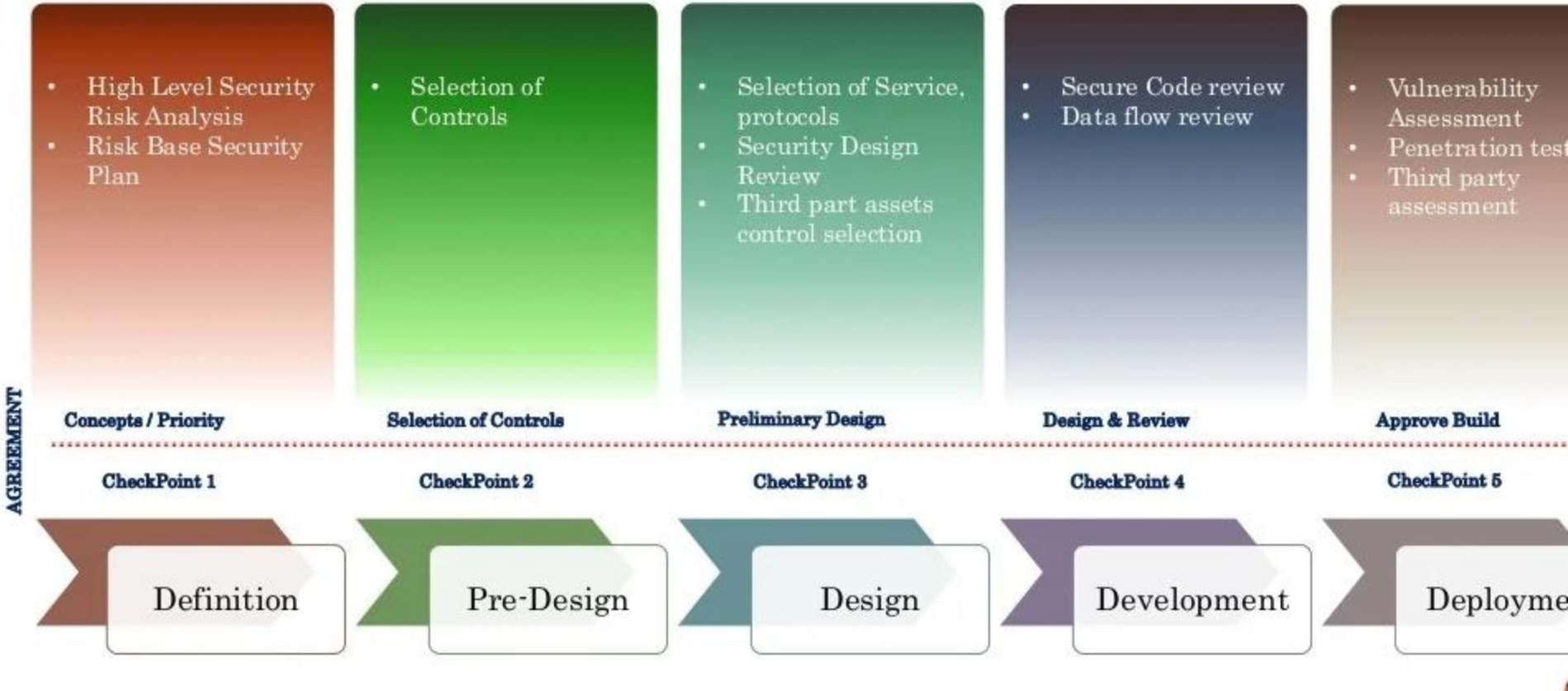
STATISTICS ANALYSIS OF REMEDIATION COST/STAGES

- Cost of remediation is always lesser in coding phases irrespective to number of bugs found.
- Impact on services, risk delta is always increases as the SDLC phases increases.
- Increase in effectiveness of controls help to decrease the number of bugs found and remediation costs.
- Decrease the impact on reputation, brand, business, reliability.

"The cost of removing an application security vulnerability during the design phase ranges from 30-60 times less than if removed during production."



APPLICATION SEC. QUALITY IMPROVEMENT APPROACH

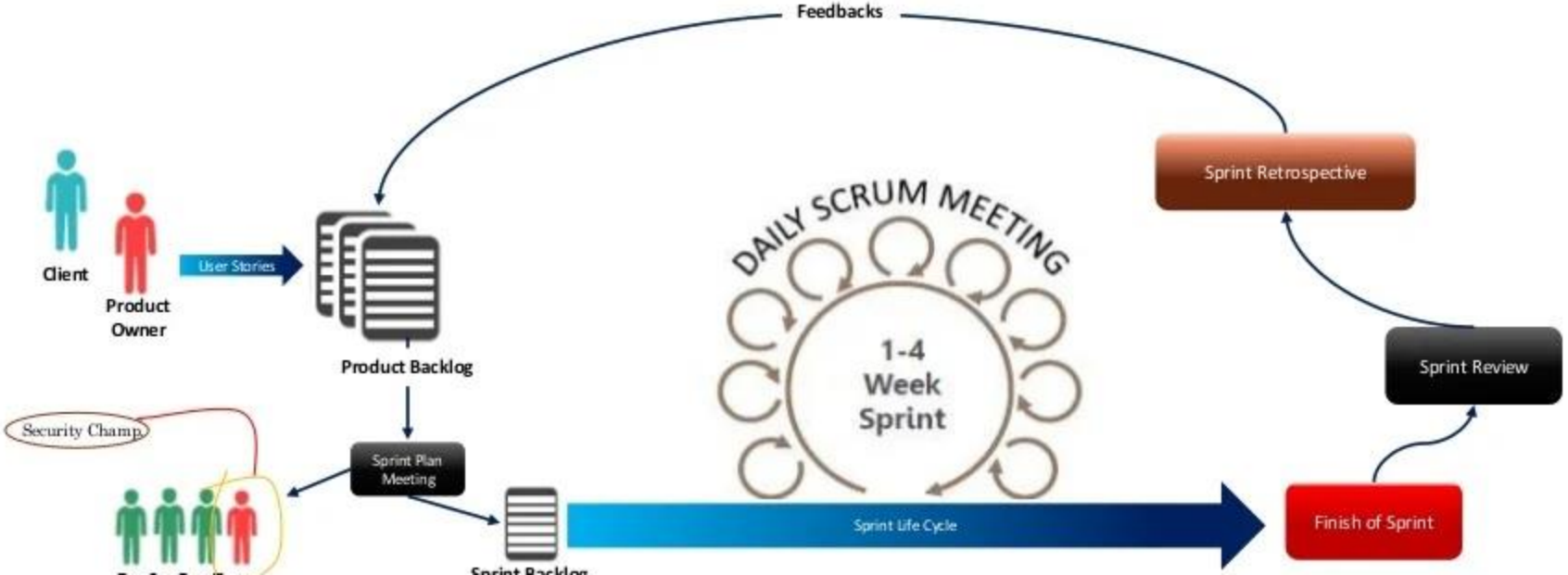


WATERFALL APPROACH FOR S-SDLC

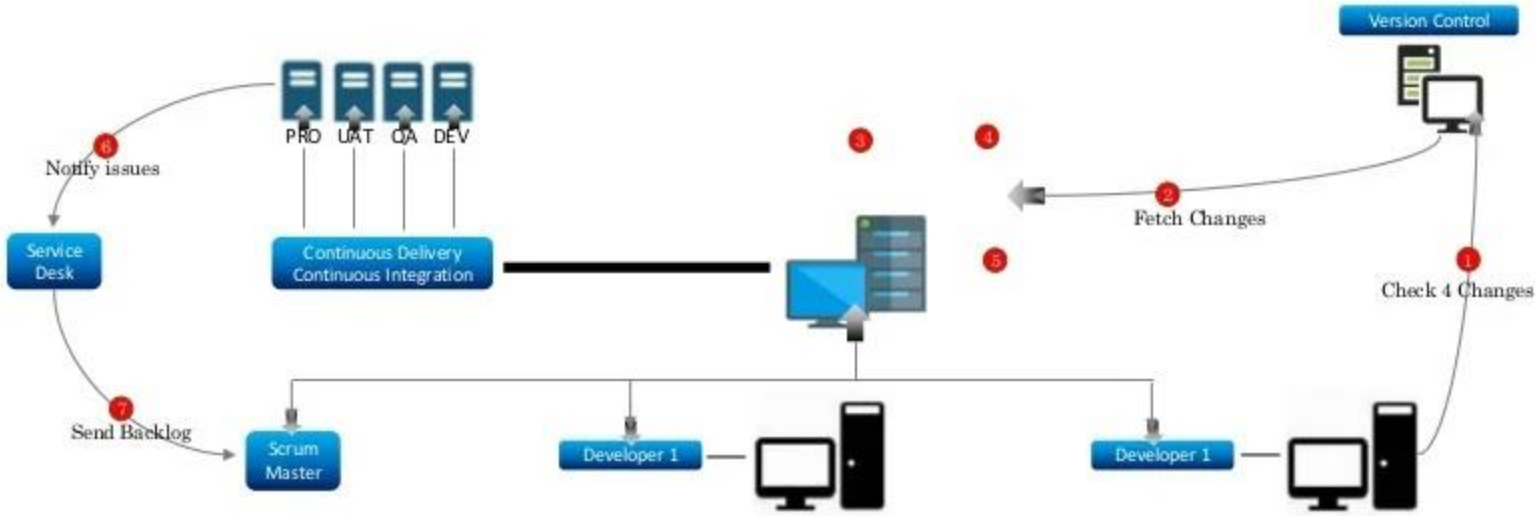
AGILE APPROACH FOR S-SDLC

GENERAL AGILE SDLC

- Product owner accept the inputs from the Client to conclude the user stories for product backlog.
- Every product backlog further divided into sprint backlog as per the group of same type of functionalities.
- Every Sprint backlog have the cycle of Coding and testing aligned with daily follow-up scrum meeting with scrum master, product owner, developers.
- Scrum meeting is on daily basis for better analysis the growth of the project.
- On the finish of Sprint, we need to review followed by Sprint retrospective for feedback to product owner likely for gaps evaluation.



CI/CD APPROACH S-SDLC



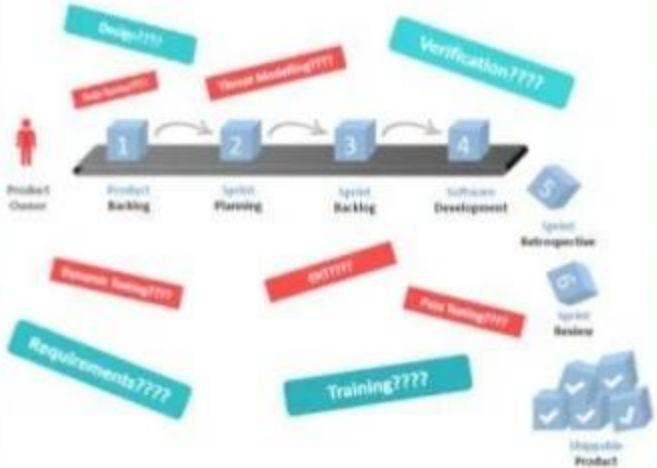
WATERFALL | AGILE | CI/CD IN S-SDLC

- Waterfall SDLC easy to alignment with Secure SDLC irrespective to Agile & CI/CD methodologies.
- Waterfall model follow the consecutive process irrespective to Agile & CI/CD methodologies.
- Implementation of Security in waterfall is easier then Agile & CICD but we can use some enhanced criteria for better & secure agile/CI/CD SDLCs

Secure SDLC in Waterfall

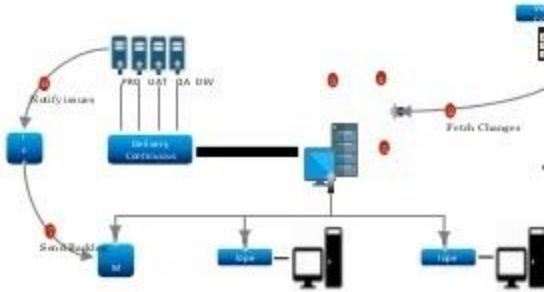
** Perfectly aligned with security blocks*

Secure SDLC in Agile



** Hard to fit as per the security blocks*

Secure SDLC in CI/CD



** Hard to fit as per the security blocks*