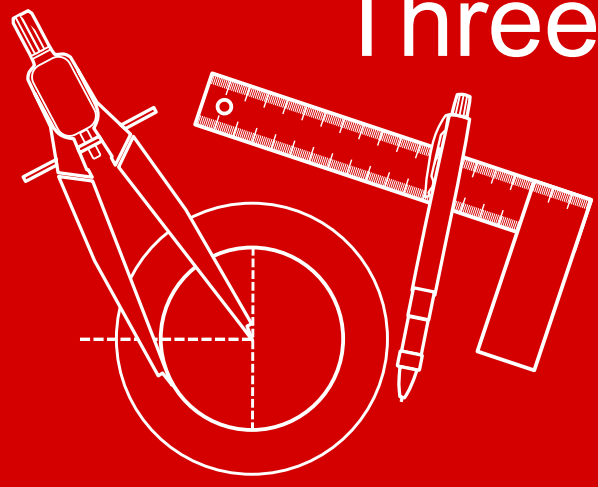
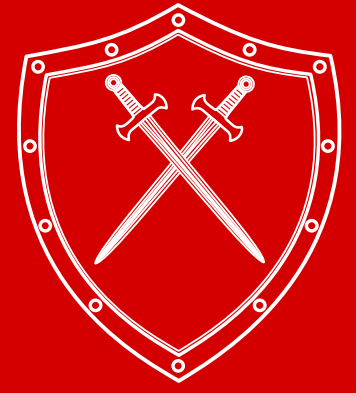


Most attacks happen on the application layer where infrastructure security solutions are not effective. Application Security is important, however, still rare in application development. Let's change that!

## Three important elements of Application Security:



# 「Shift Left」



## 「Security by Design」

## 「DevSecOps」 Continuous Hardening

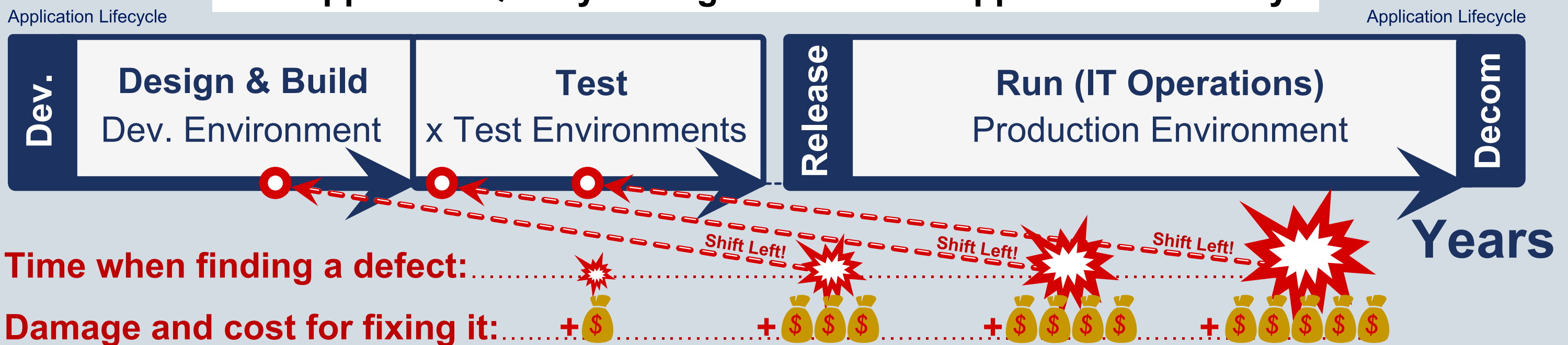
A security story so that 「bottom-up」 meets 「top-down」

**Shift Left:**  
Mindset for increasing efficiency and controlling cost during the whole application lifecycle

### 「Shift Left」!

**Top-down support:**  
Efficient Application Security is not possible without strong support from top management!

**Find and fix application defects early for reducing cost and risk!  
This applies to Quality Management and to Application Security!**

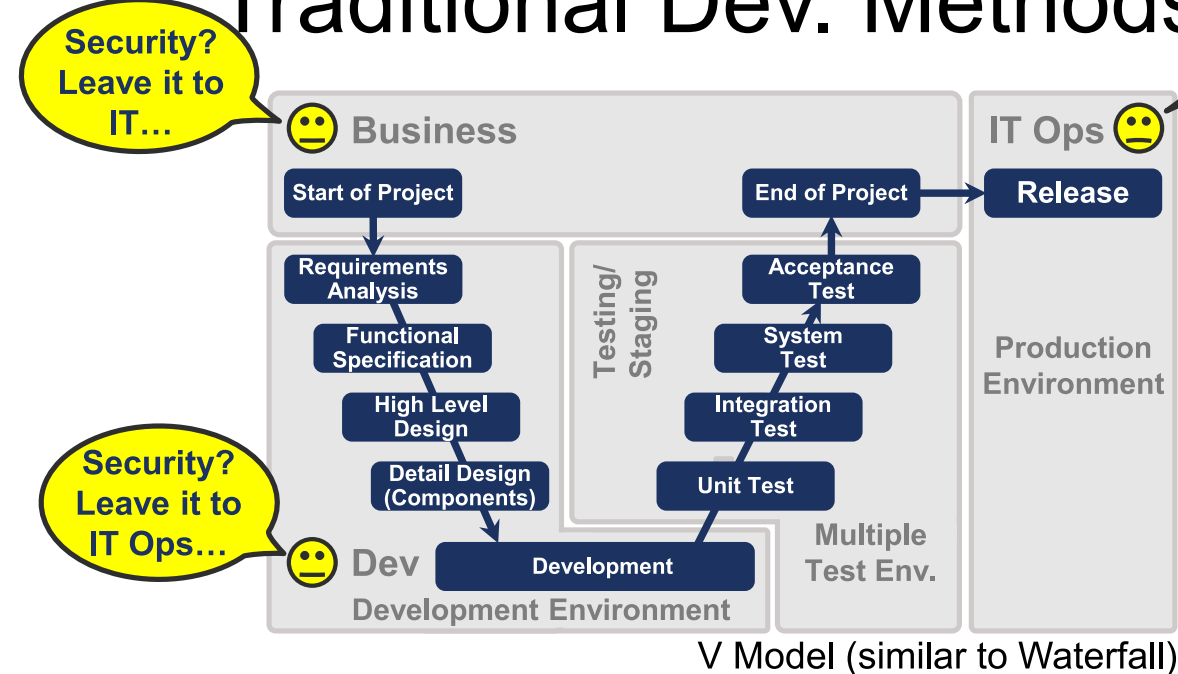


**Rule of thumb:**  
The later it gets, the more expensive it is to change an application (significantly costlier!)

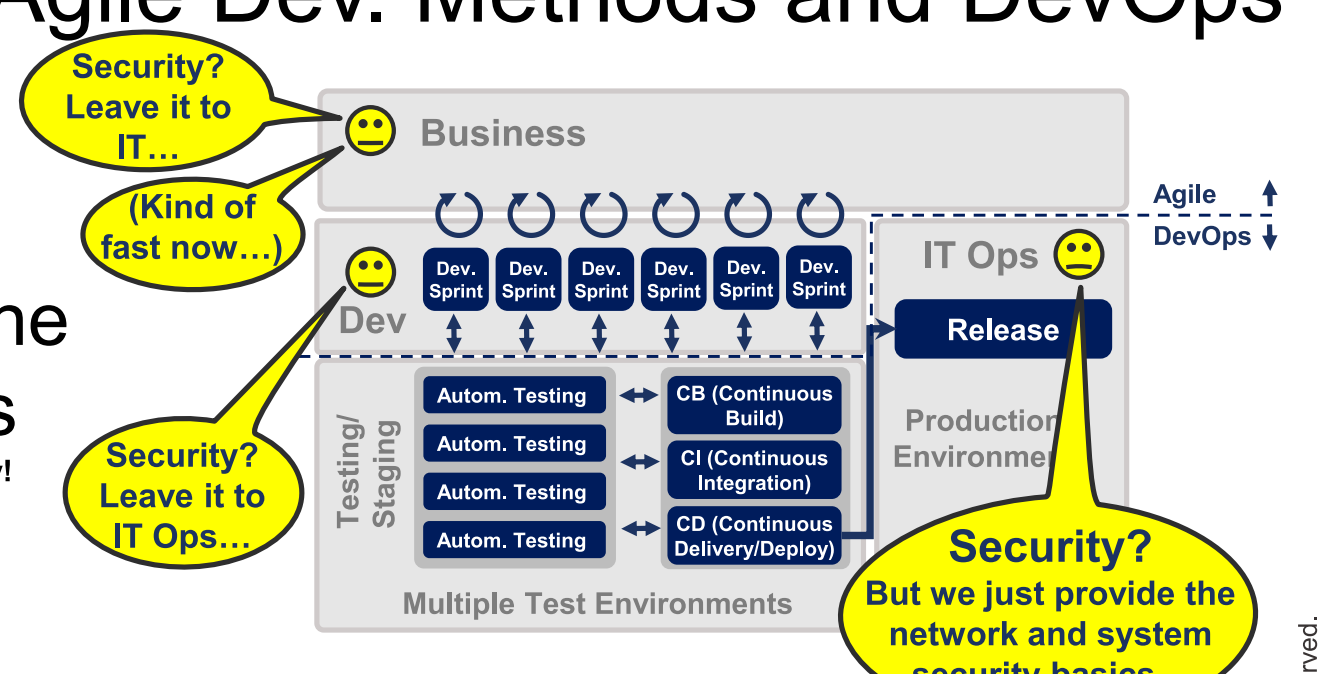
**Top management involvement required:**  
Keep an eye on the realities in the organization regarding 「Shift Left」, 「Security by Design」 and 「DevSecOps」!

### Traditional Dev. Methods

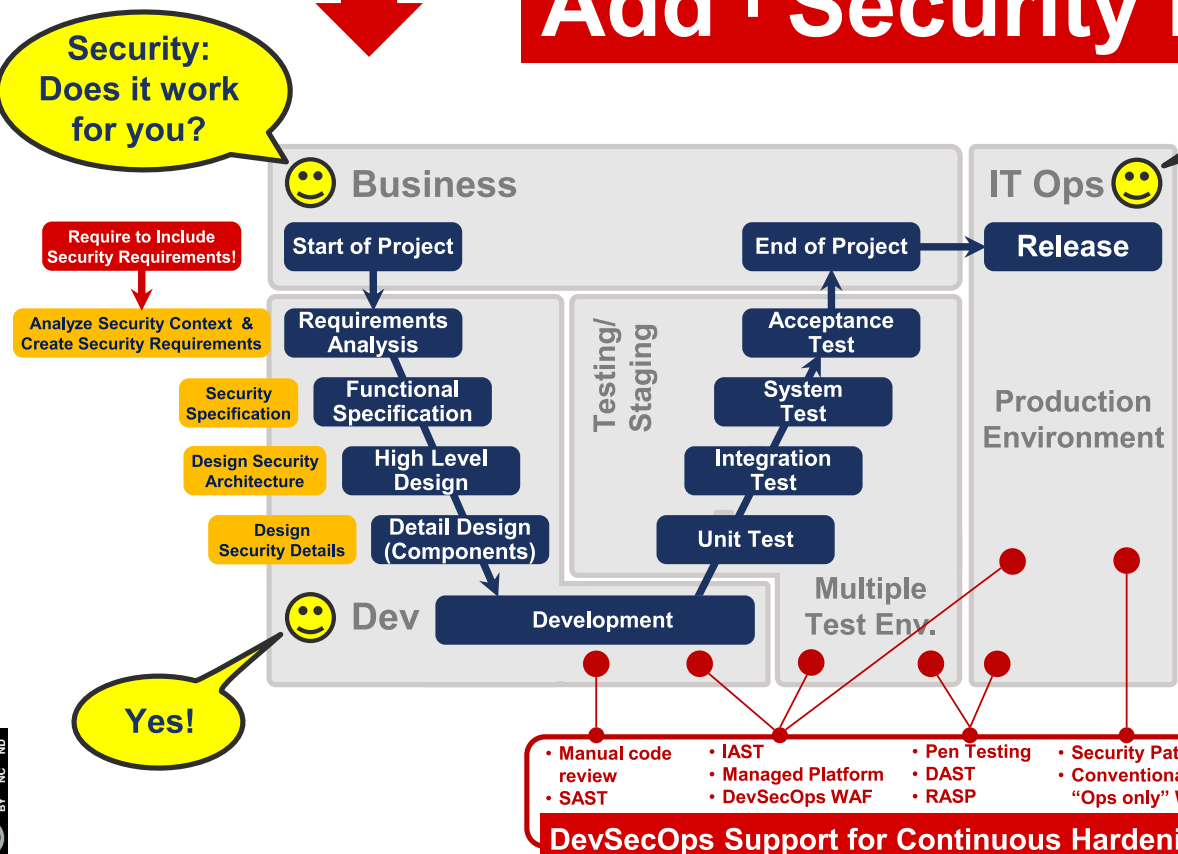
### Agile Dev. Methods and DevOps



**Tragedy in the IT trenches**  
Still an often seen reality!



## Add 「Security by Design」 & 「DevSecOps」!



### Better approach

1. Business explicitly requires a preventive approach for Application Security (incl. appropriate budget).
2. Dev. team creates a security design for the application.
3. Ops. and Dev. teams work together in order to implement security hardening a) efficiently and b) continuously in order to maintain the intended security quality over time.

