Many 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 useful notions for proactive Application Security!



「Shift Left」



「Security by Design

Staging

Design Security Details

Security by

DesignJ

🙂 Dev

System Test

· IAST

DevSecOps | support for Continuous Hardening

Multiple

Test Env.

Unit Test



TDevSecOpsJ **Continuous Hardening**

A security story so that \(^{\text{bottom-up}}\) meets \(^{\text{top-down}}\)

Shift Left

Mindset for increasing efficiency and controlling cost during the whole application lifecycle.

「Shift Left!」

Find and fix defects early for reducing cost and risk

Top-Down Support Efficient Application Security is not feasible without strong support from top management!

Release

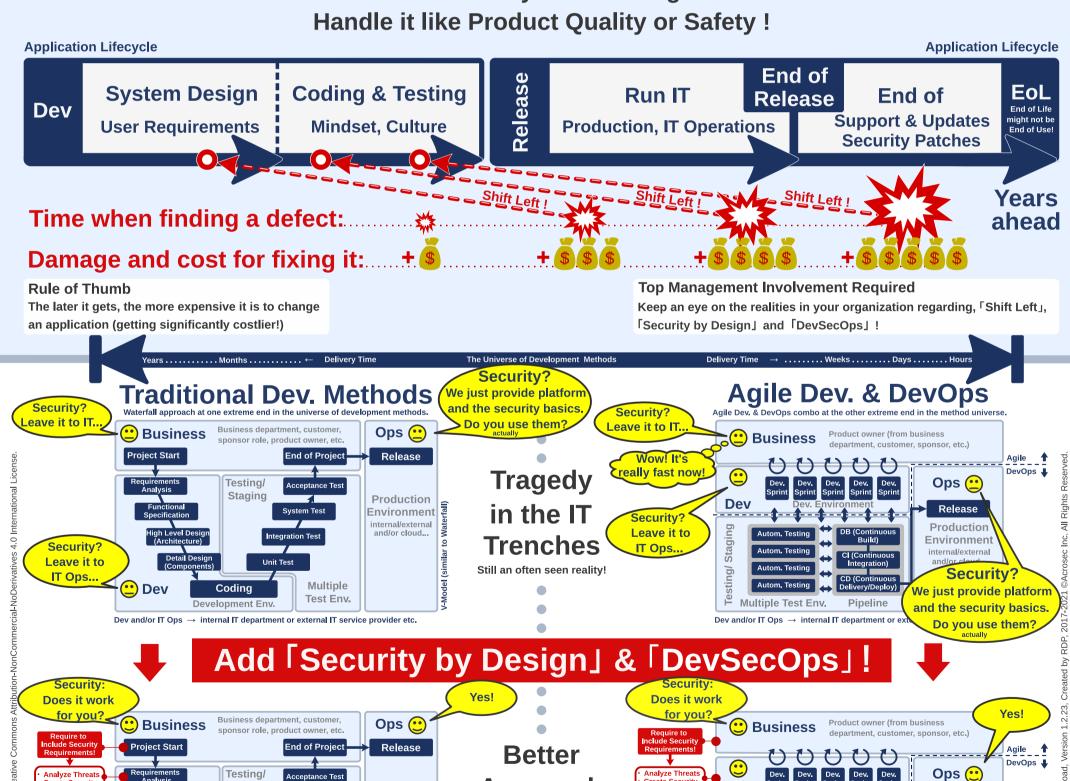
Production

Environment

internal/external

and/or cloud...

· Security Patchi



Approach

1. Business requires a proactive

2. Development project creates a

security design. Suggested

3. Development and other teams

work together for efficiently

a) implementing Continuous Hardening.

b) maintaining the intended security level

afterwards in order to stay consistent over time.

starting point: Zero Trust.

approach and provides budget.

Requirements

Security by

DesignJ

Dev

Multiple Test Env.

「DevSecOps」 support for 「Continuous Hardening」

Production

Environment internal/external

and/or cloud..

Security Patchin