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



Continuous Hardening_J

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

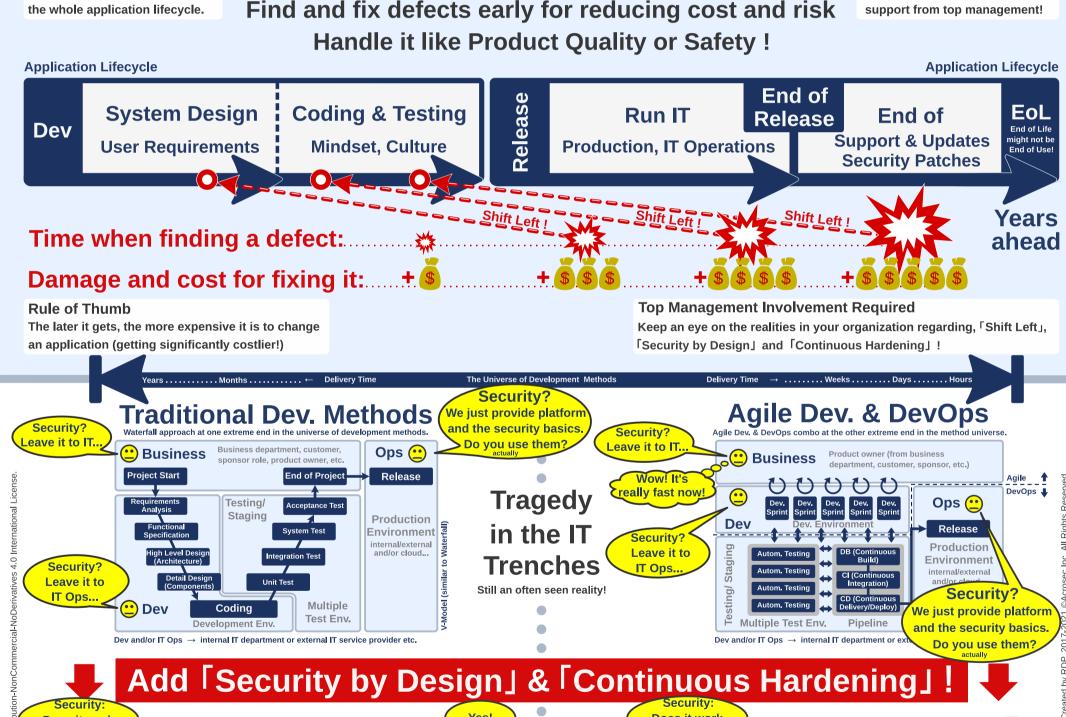
Shift Left

Mindset for increasing efficiency and controlling cost during

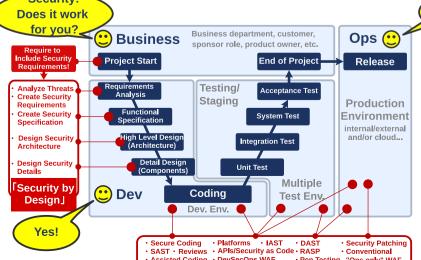
「Shift Left!」

Find and fix defects early for reducing cost and risk

Top-Down Support Efficient Application Security is not feasible without strong



Yes! Does it work for you? for you? Business department, customer Product owner (from business **Business** Ops 😬 **Business** sponsor role, product owner, etc department, customer, sponsor, etc.) **End of Project** Release



Support for 「Continuous Hardening」

Better Approach

- 1. Business requires a proactive approach and provides budget.
- 2. Development project creates a security design. Suggested starting point: Zero Trust.
- 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.

Agile 000Ops 🙂 Analyze Threat Create Security Requirements Dev Release Production **Environment** internal/external and/or cloud... Security by **Design**J Multiple Test Env. Security Patchi 「DevSecOps」 support for 「Continuous Hardening」