SECURITY IN CI/CD PIPELINE

Integrating new activity to a delivery pipeline is always hard due to multiple contradictory requirements. PMs pushing for more features, dev teams want to slow down and refactor, operation teams, looking for better response time and less complicated landscape. Business owners just want to have the feature released before the end of the quarter. It is hard to add security to this when nobody sees a value. It's good we know to do it and bring value to everyone in the value chain.

OBJECTIVE

After kick-off meeting we defined these objectives:

- Less bugs and iterations between DevOps and security;
- More features delivered and more equalized delivery pipeline;
- Less findings during security tests (more findings eliminated during development);
- Compliant with regulation – corporate security handles big picture, DevOps eliminates security issues where possible.

ABOUT THE CLIENT

A multinational company with internal development and operations team in the finance industry. Internal technological landscape consists of over 50 internally developed and used applications and 20 client facing applications.

CHALLENGE

To achieve a positive return on investment and ease of management we had to integrate security to delivery chain, technology stack, culture, and processes.

RESULT

1. Time to close vulnerability **improved by 79%;**
2. **60%** application teams performing **security testing before release** (increase from 12%);
3. **Decrease** of usage of **critically vulnerable** open source components (CVE 7+) **from 31% to 7%;**
4. Automated code quality scanning showed **overall security code scores** has **increased** by **13%;**
5. **68%** of older **technical debt** and **security defects** have been **eliminated**, addressed via managed sundown of assets or have remediation plan in place.

HOW WE DID IT?

INTEGRATING CULTURE

1. By training development teams to develop secure code using SSDL, brown bag sessions, capture the flag (CTF) and on demand training;
2. By empowering DevOps and engaging business partners;
3. Verification of “CleanScans“, periodic application static and dynamic security testing.

MAKING SECURITY EASY

1. Focusing on value, not on tools (utilizing the same systems and applications DevOps using);
2. Integrating preventive security controls and tests in the development phase;
3. Providing AppSec testers and following build lifecycle.

AUTOMATING

1. Helping DevOps automate as many security tests as possible to run alongside regular tests;
2. Integrating static and dynamic analysis tools into the CI/CD pipeline;
3. Automatically detecting when application relies on libraries with known vulnerabilities.

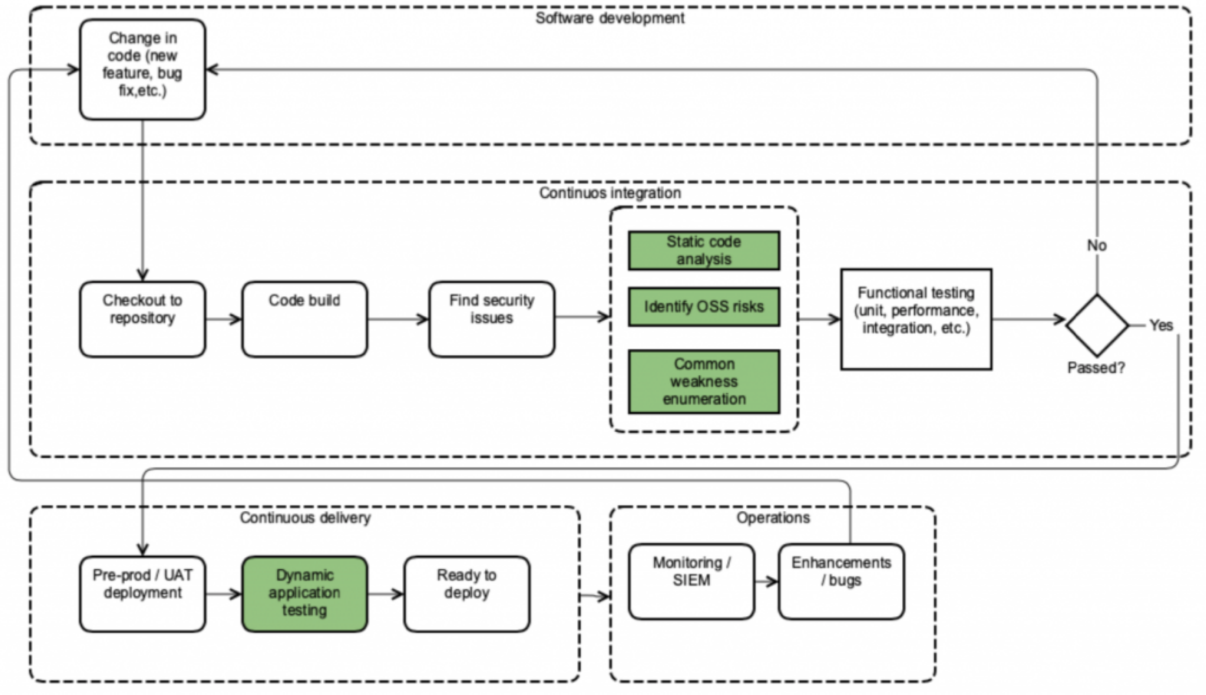
EQUALIZING DELIVERY PIPELINE

1. Less drama;
2. Predictable product lifecycle;
3. No surprises for DevOps and Security dept.;
4. Happier business owners.

STEPS TO DYNAMIC SECURITY TESTING

1. Kick-off and onboarding;
2. Planning, the definition of targets and testing strategy;
3. Access to build;
4. Dynamic application security testing;
5. Results delivered to DevOps team;
6. Retrospective and automation.

END TO END VALUE STREAM



HAVE ANY QUESTIONS? INTERESTED? GET IN TOUCH!

CALL US +420 228 224 645, DROP US EMAIL ON HELLO@ROLKEN.CZ