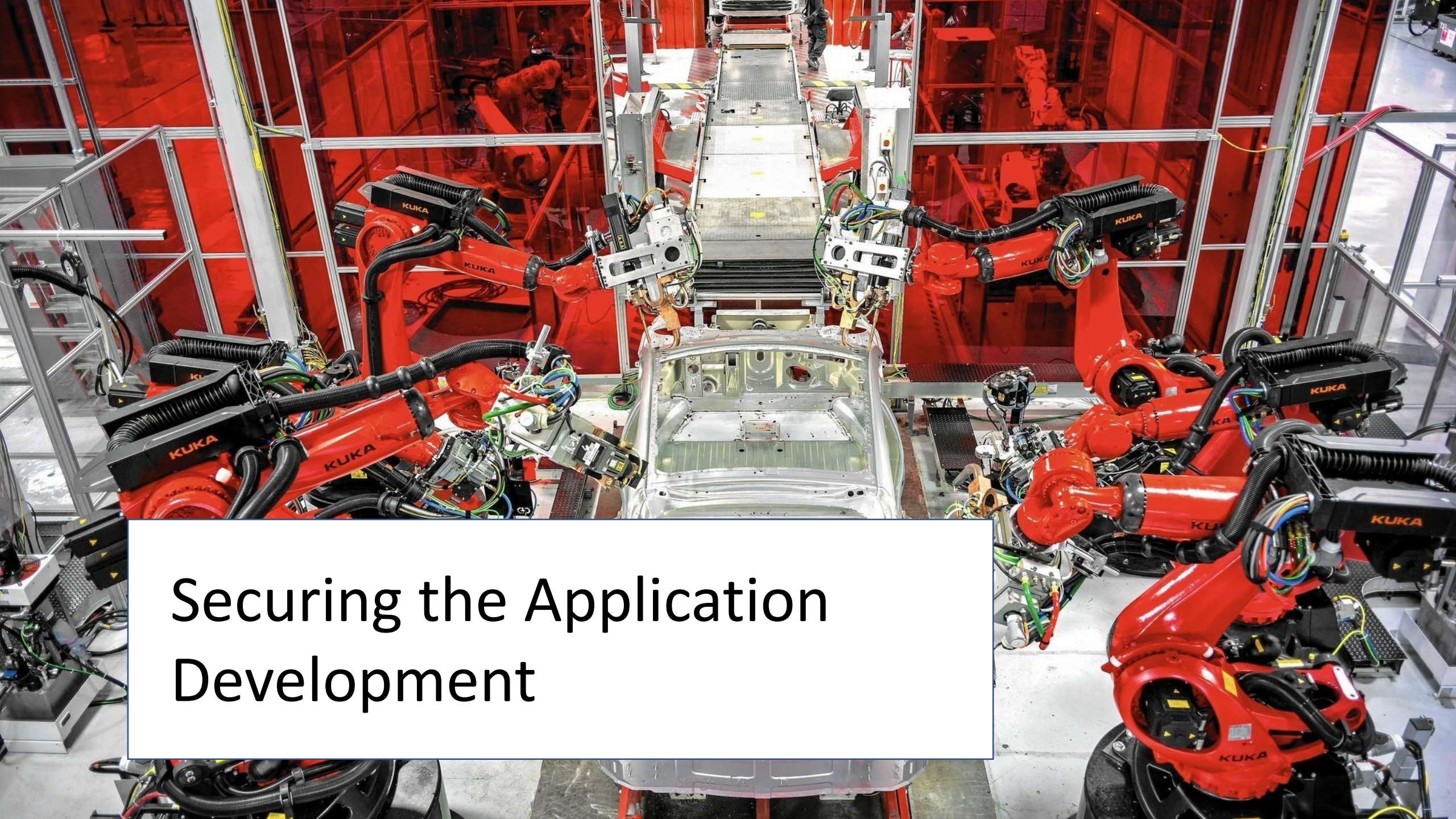
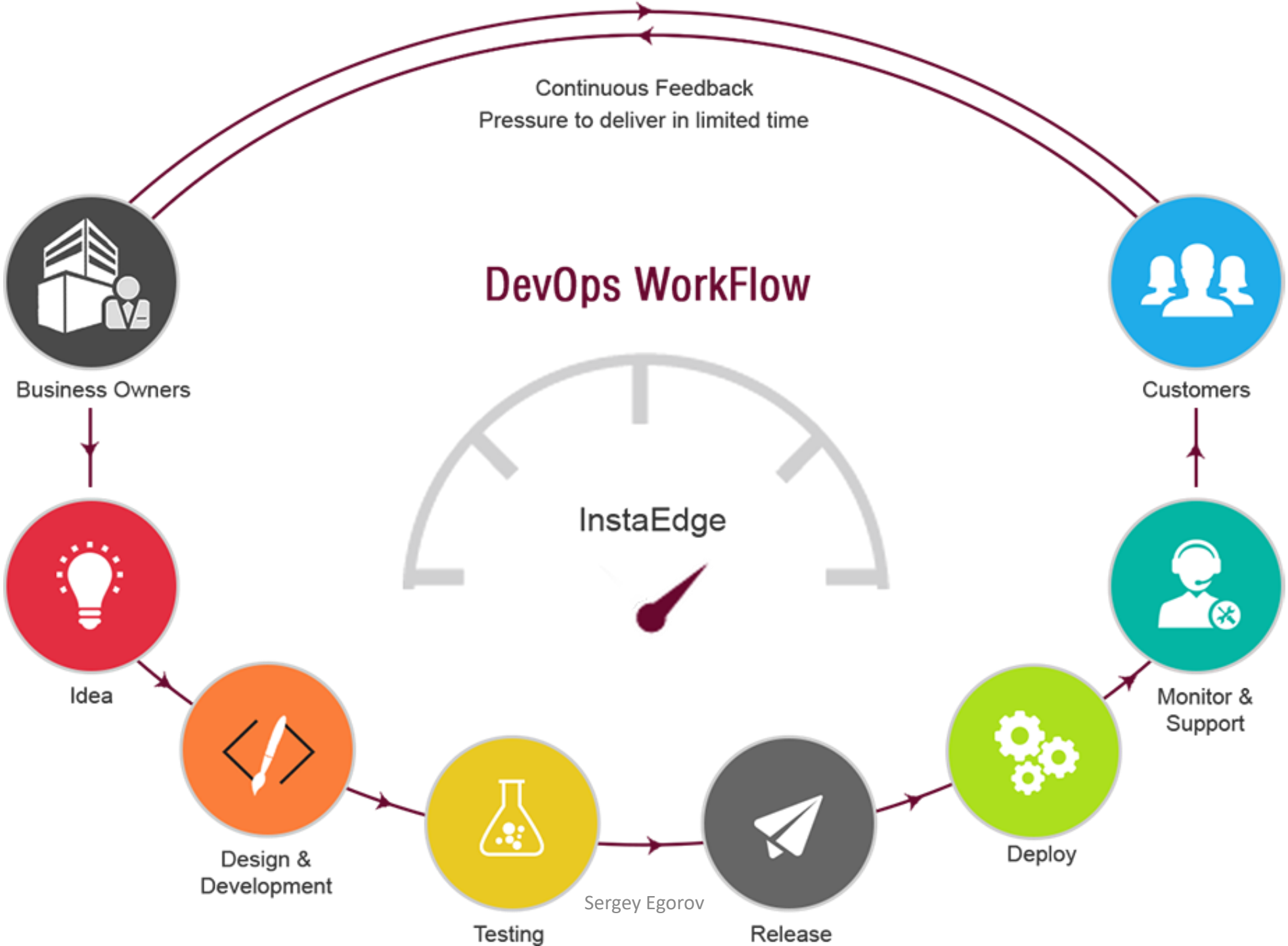
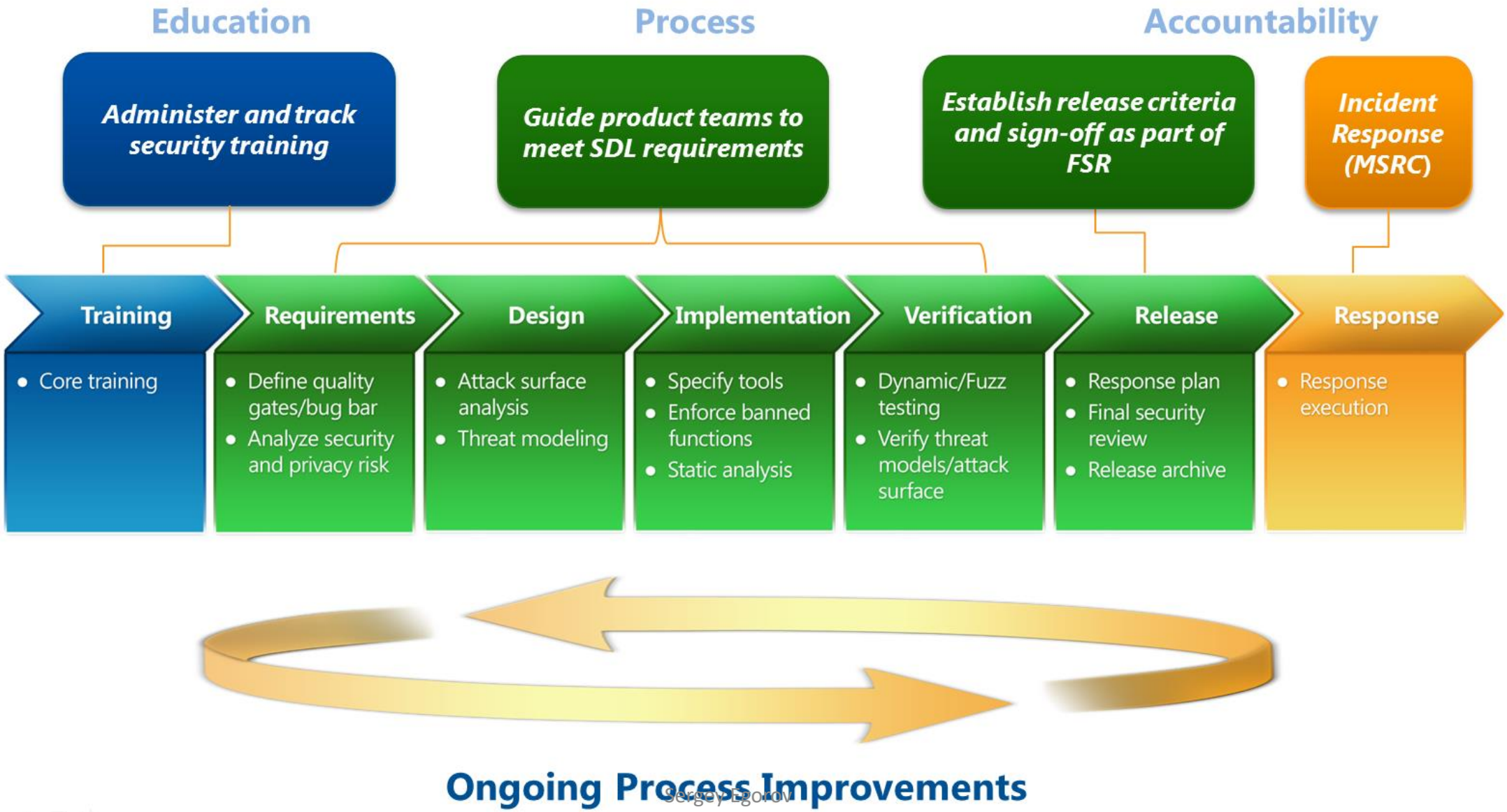


Securing the Application Development

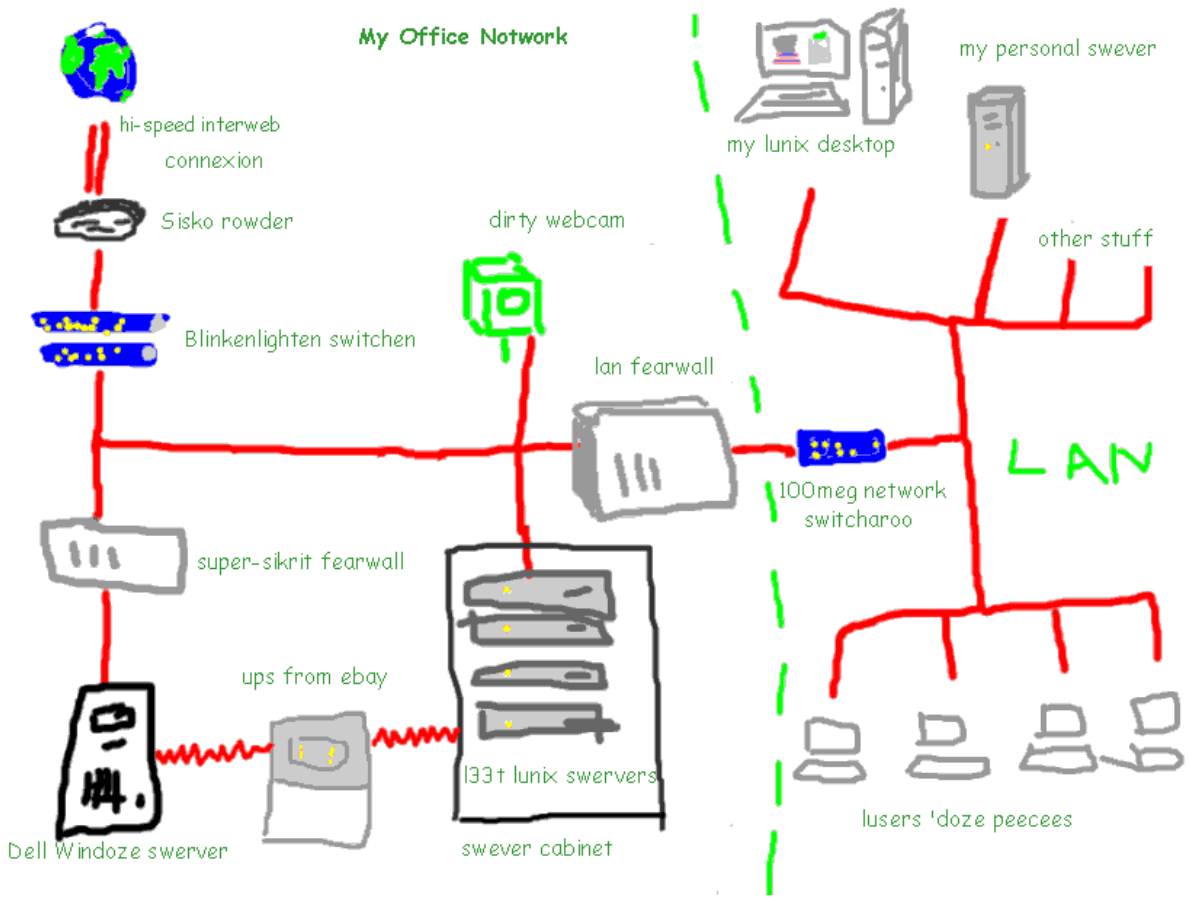

Continuous Feedback
Pressure to deliver in limited time
DevOps WorkFlow
InstaEdge
Business Owners
Customers
Idea
Design & Development
Testing
Release
Deploy
Monitor & Support
Sergey Egorov

Microsoft SDL



Threat modelling

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege



SAST
Static AppSec Testing

DAST
Dynamic AppSec Testing

Constraints & Limitations

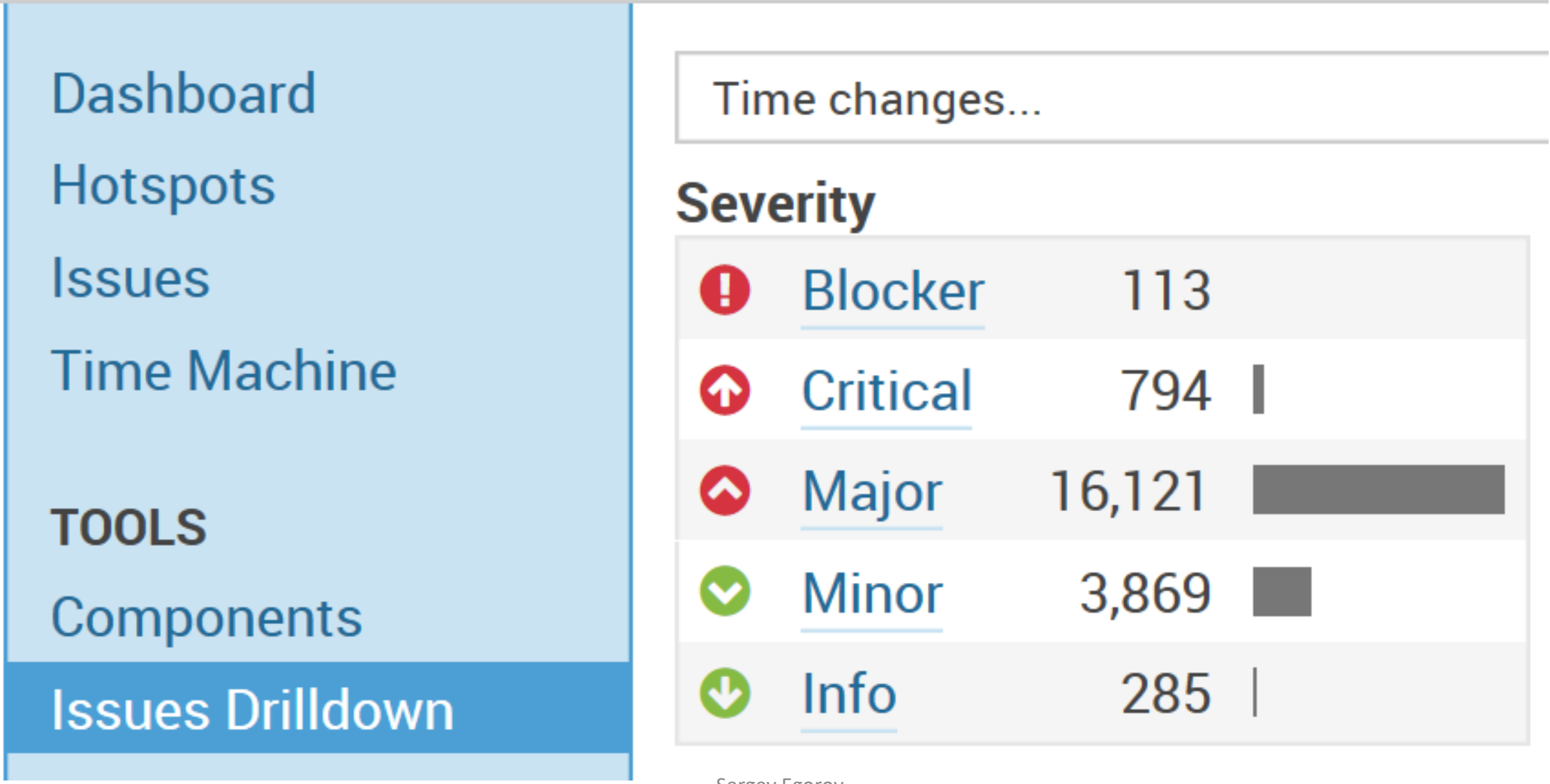
- False positives
- Time to scan
- Adjusting

- App crawlers
- Intrusive or not comprehensive
- Business logic vulnerabilities

IAST
Interactive AppSec Testing

- Time to discover vs time to fix
- Instrumentation of production code
- Limitations of DAST

Static code analysis (SAST) results:



WAF

Web Application Firewall

- Signature based (False Negatives, Bypass)
- Manage rules (Configure – QA - Deploy)
- False positives (App functions change)
- Business logic vulnerabilities

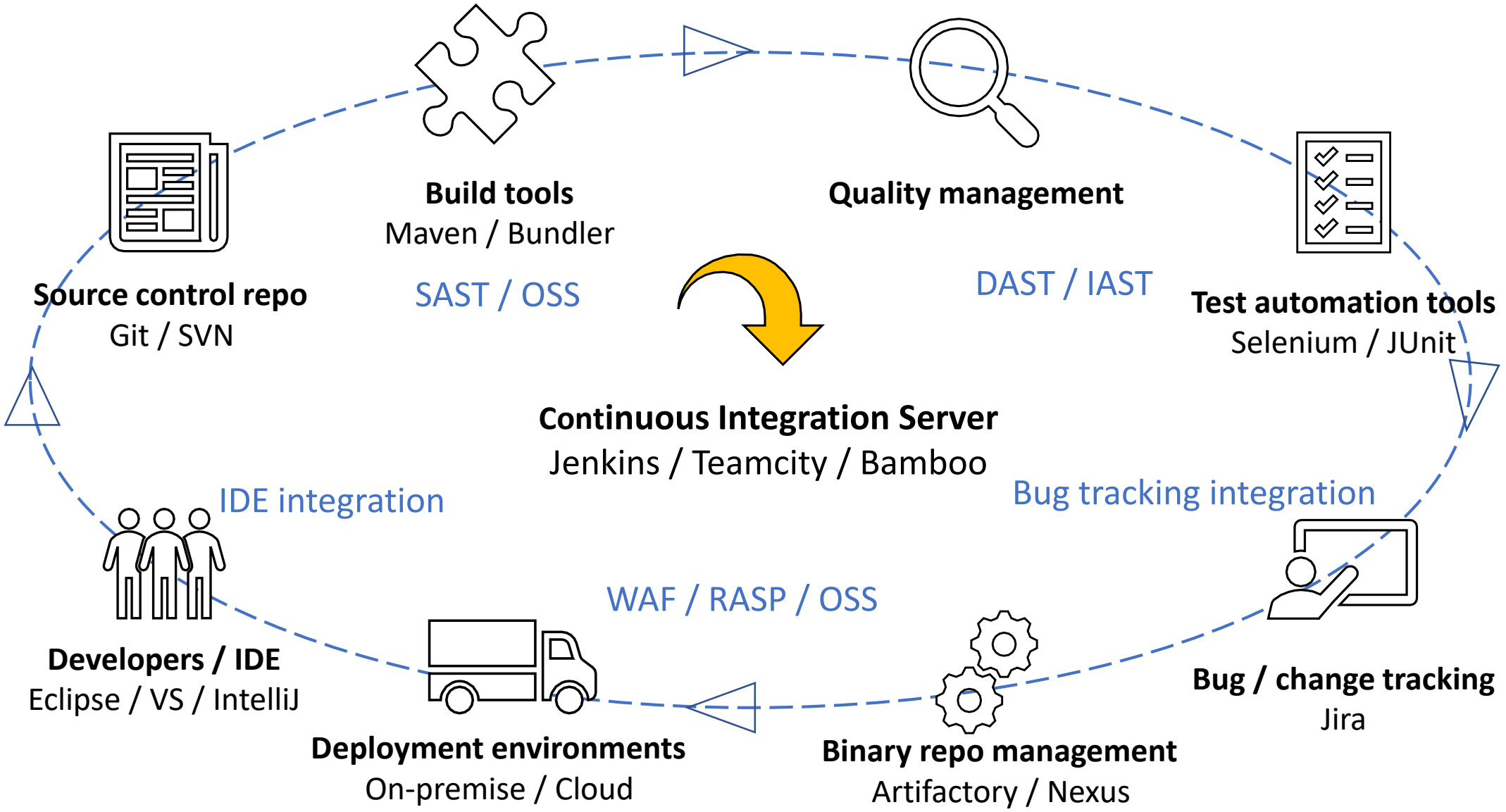
RASP

Runtime Application Self-Protection

- Performance overhead
- Taint Analysis (False Positives / Negatives)
- Business logic vulnerabilities
- Requires runtime env. (JVM, .NET)

Application stack

- ✓ Apps and APIs
- ✓ 3rd Party Libraries
- ✓ 3rd Party Frameworks
- ✓ Application Platform
- ✓ Container Runtime
- ✓ OS Runtime
- ✓ Physical Host or VM


Build tools
Maven / Bundler
Quality management
Source control repo
Git / SVN
SAST / OSS
DAST / IAST
Test automation tools
Selenium / JUnit
Continuous Integration Server
Jenkins / Teamcity / Bamboo
IDE integration
Bug tracking integration
WAF / RASP / OSS
Developers / IDE
Eclipse / VS / IntelliJ
Deployment environments
On-premise / Cloud
Binary repo management
Artifactory / Nexus
Bug / change tracking
Jira

Penetration Testing

Pros:

- Contract, Scope, NDA
- Whitebox, internal, more services
- Results are confidential

Cons:

- Time and scope limits
- Pay for time, not findings
- Expertise is limited by few consultants

Bug Bounty

Pros:

- Lots of skilled security researchers
- Flexible, Pay for results
- Constant motivation to improve security

Cons:

- Half of the world is trying to hack you
- Confidentiality issues
- Only public facing apps

the unofficial HackerOne disclosure timeline.

text to filter reports

HackerOne disclosed a bug submitted by **hackerone2017** 01 Nov 2017
Adding or removing a new non-preferred payout method does not trigger an e-mail or account notification

AlienVault disclosed a bug submitted by **ramsexy** 01 Nov 2017
[www.threatcrowd.org] - reflected XSS in report.php

AlienVault disclosed a bug submitted by **ramsexy** 01 Nov 2017
[www.threatcrowd.org] - reflected XSS in graphViewMap.php

AlienVault disclosed a bug submitted by **ramsexy** 01 Nov 2017
[www.threatcrowd.org] - reflected XSS

Infogram disclosed a bug submitted by **jarmouz** 01 Nov 2017
XSS on infogram.com

Infogram disclosed a bug submitted by **jarmouz** 01 Nov 2017
Multiple xss on infogram templates

Infogram disclosed a bug submitted by **haystack_needle** 01 Nov 2017
XSS when Shared

arxius disclosed a bug submitted by **kunal_bahl** 31 Oct 2017
API leaking infinite amount of valid Tokens.

Inflection disclosed a bug submitted by **thalaivarsubu** 31 Oct 2017
Host Header Injection or cache poisoning in multiple domains

Inflection disclosed a bug submitted by **thalaivarsubu** 31 Oct 2017
XST(Cross Site Tracing)