CyberSec Hub

Connecting People. Delivering Security.

cybersechub.com.au | platform.cybersechub.com.au

Information Security – Keeping Up With DevOps

Stas Filshtinkskiy

- Applied Mathematics degree
- 20 years in Information Security
- 10 years of that in software development
- Co-founder of Cyber Security Hub
- stas.filshtinskiy@cybersechub.com.au

Cyber Security Hub

Innovation-driven cyber security organisation. HQ in Melbourne, offices in ME and Singapore

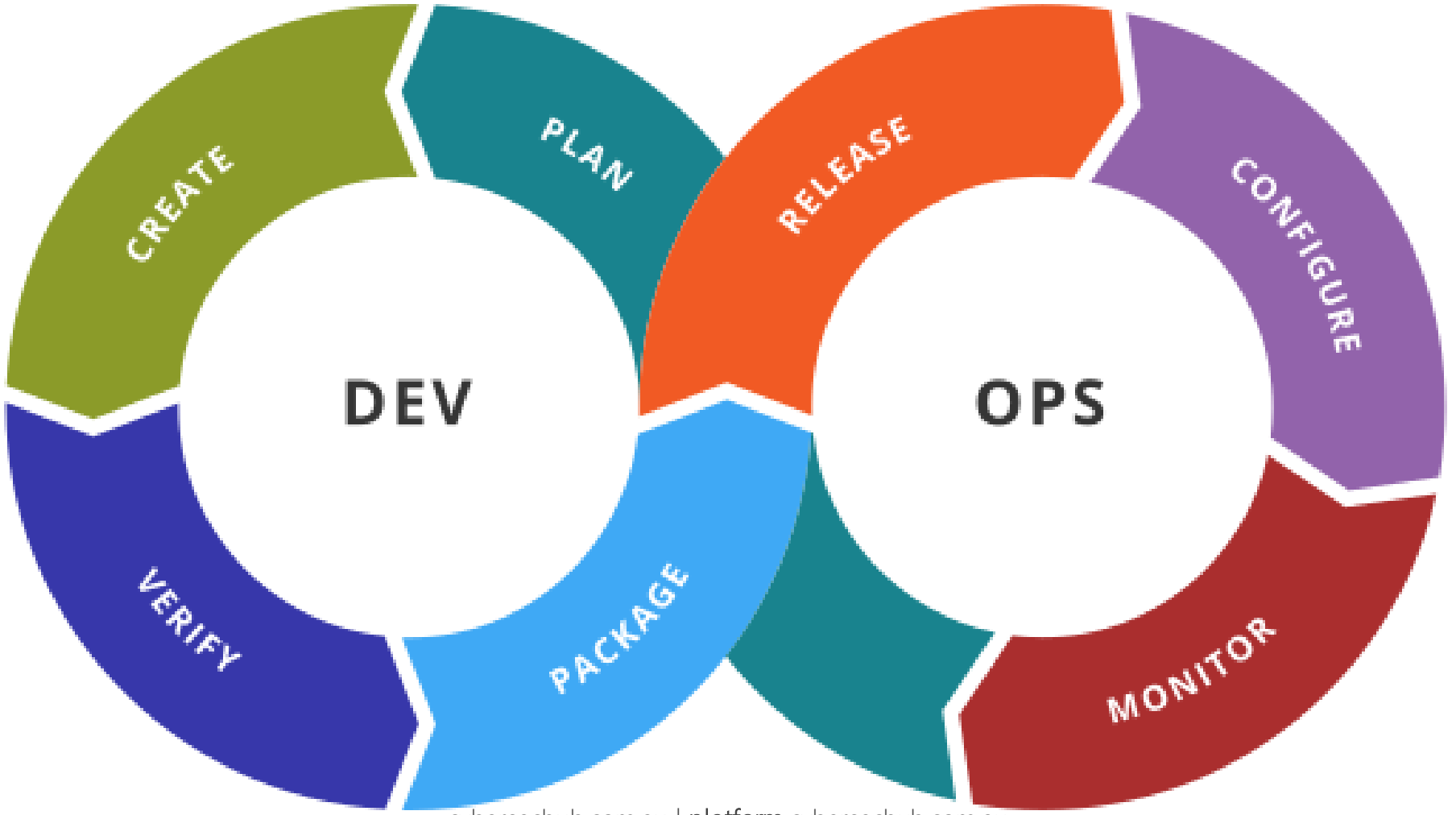
Operating 'Uber-like' security consulting. Wholesaler security services

Currently provide information security services within Asia-Pacific and Middle-East alongside major banks, telecommunications, energy & utilities, integrators and retail companies, as well as federal and state governments

Deliver a large portfolio of information security services with a strong focus on security testing and governance, risk & compliancy services

Transforming way security professionals are engaged on projects and how services are delivered

DevOps - Benefits



Is this you?

- Engage with Business continuously?
- Accept new requirements?
- Quality control and (scripted) Testing?
- Automate everything?
- Promote in to production fast?

You are amazing!

Security Challenges

- Security slow things down
- Security requirements are always changing
- Testing for Security Requirements is one big Unknown

Security Challenges: For All

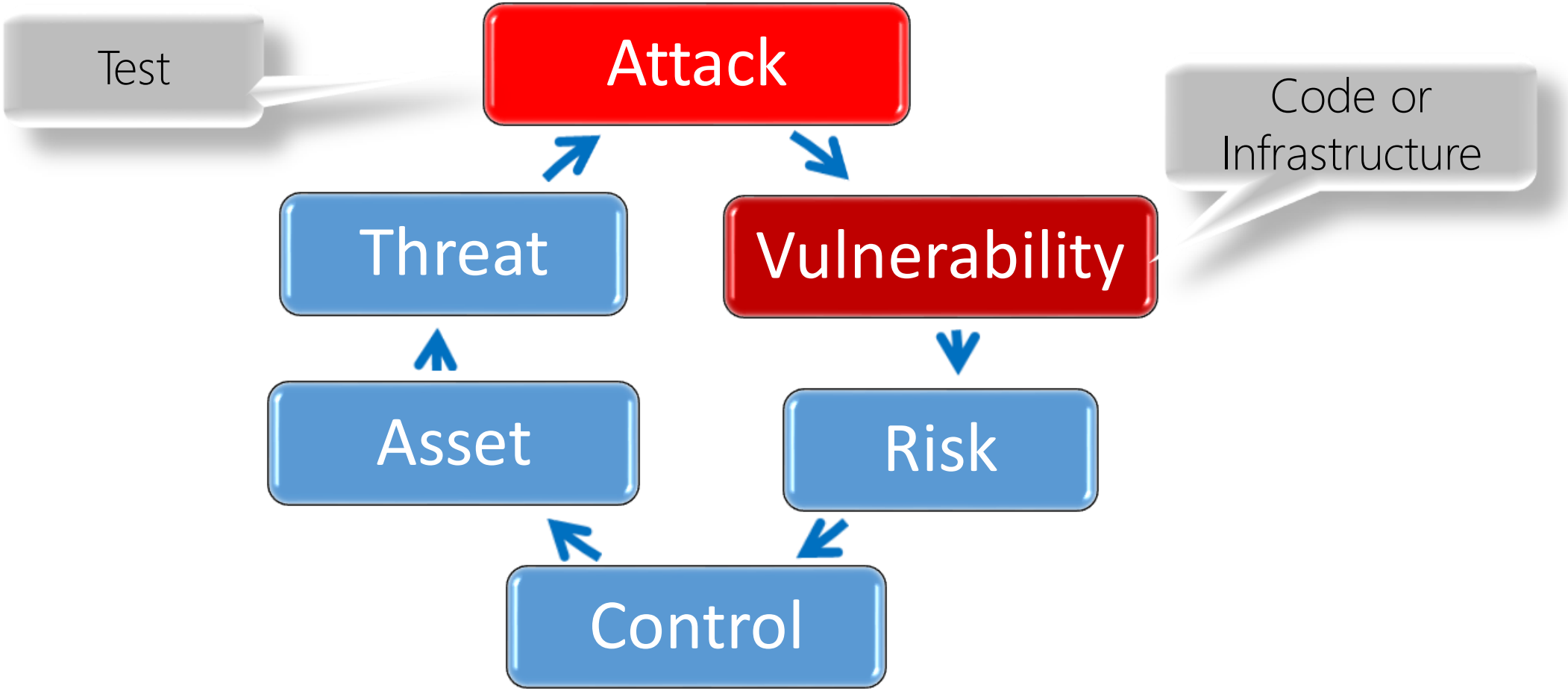
- Systems are more complex
- Attackers get better at what they do
- People make mistakes

You are the only people who can get us (more) secure!

Engaging Security (as part of Business)

- Get Security to be part of DevOps Team
- Ask for training

Cycle of Risk



Treat Security the same

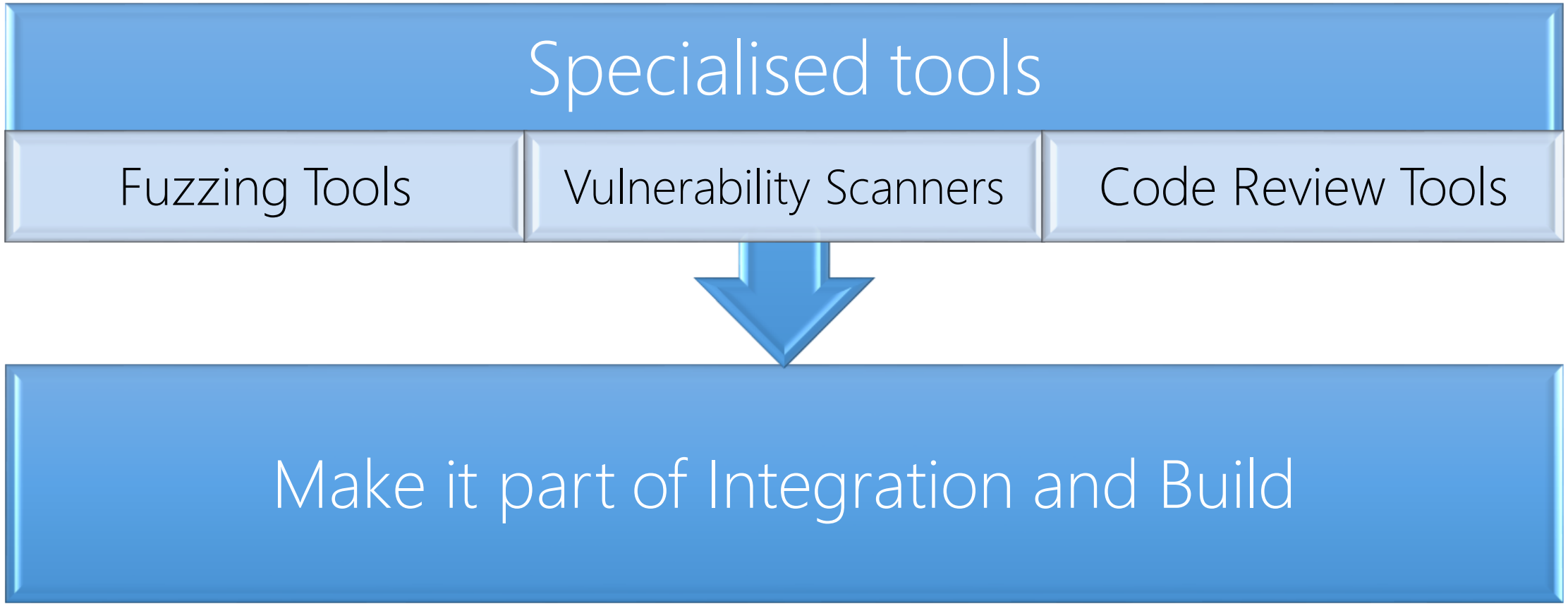
Security Activities

Static Code Review & Vuln. Scanning

Make it part of build process

Fail build if security is below agreed threshold

Security tools



Security tools

Fuzzing Tools

- Against all interfaces

Vulnerability Scanners

- Against all components

Security Tools

- Nessus
- SoapUI
- Burp suite
- OWASP Zed Attack Proxy
- Metasploit
- Different fuzzing tools for different applications
- FindBugs (Java)
- CheckStyle (Java)
- FxCop (.Net)
- PMD (XML/Java/JS/C/C++/PHP/Python/GO/Swift/Ruby/Groovy)
- Etc…

Penetration Testing

It is a process and an Art

It has to be done on something closely resembling the Production Environment

Requires specialised expertise

Findings are buried in PDF report somewhere

Penetration Testing: Process & Art

Automate what is possible to automate: do it every time

Leave the Art to the Artists: on major releases

Maintain access to experts

Penetration Testing: Environment

Automate tests as much as possible

Run those tests in the relevant environment: Dev, Test, or Stage

Penetration Testing: Report

Demand near real time access to findings

Demand test cases to test your fixes

Summary

Integrate security people and expertise in your team and process

Every time security finds anything – ask how to test for it

Integrate security test cases alongside your other test cases

Questions