EXIGEN services

Return on Intelligence company

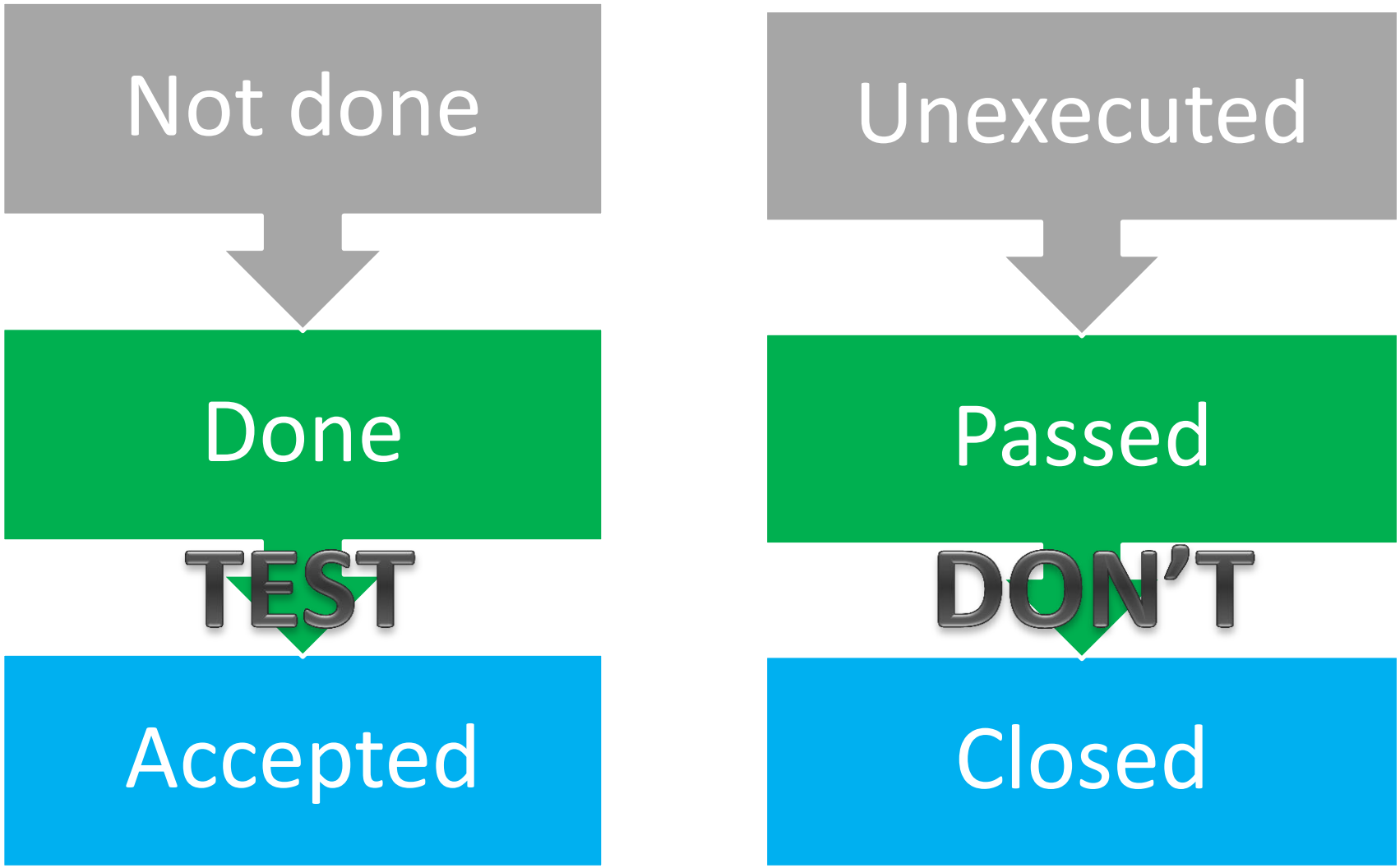
Who Tests the Test?

Security tester's story by

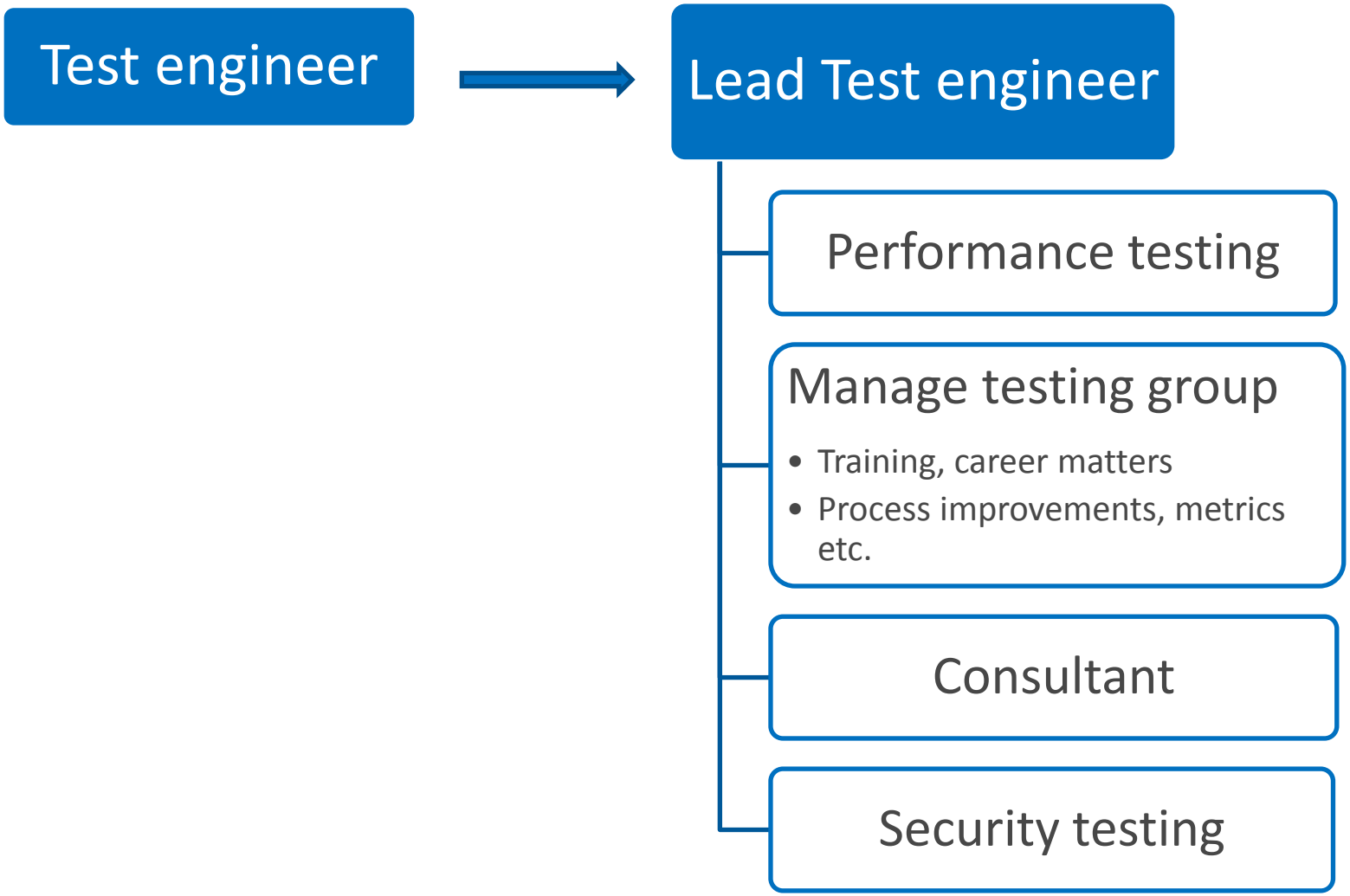
Ainārs Galvāns

Exigen Services Latvia

Dev. Task versus Test Case



About myself



Ideas behind the Story

- Compare functional and security testing
- Values I was surprised about
  - Techniques over procedures
  - Skills over methodology
  - Results over visibility
  - Repeatability is not a value
- Questioning functional testing maturity
- Old ideas revisited

Security “test case”

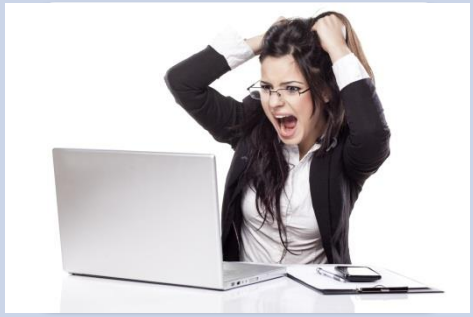
- Enter <script>alert(-1)</script> into each field
  - If don’t accept try alternatives
  - If accept check all outputs

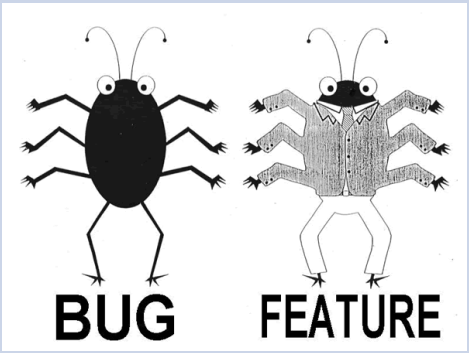
Functional testing VS Security testing

	Functional	Security
Prepare	Analyze docs, play with software	
Test	Expected result	Expected fault
Tools	“Replace tester”	Help tester
Result	Test Docs, defects	Defects, “sign-off”
Evaluate	Defect rates	Defect count

Lear about Missed bugs

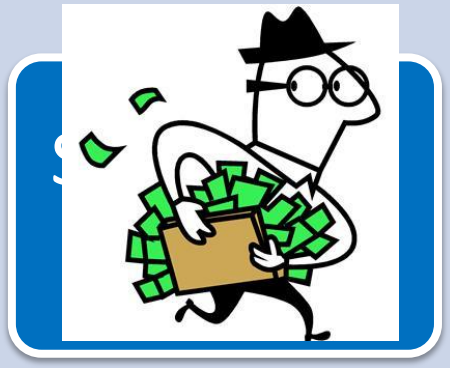
Functional





Performance

Security



Documents referenced by customers

- Security testing
  - OWASP code review guide (best practices)
  - OWASP test guide (test techniques)
  - OWASP testing standard (minimal tests to be done)
  - ISO 2700*(suggested security controls to support organization's security policy)
- Functional testing
  - IEEE Std 829, Standard for test documentation
  - "Equivalence partitioning and boundary cases"

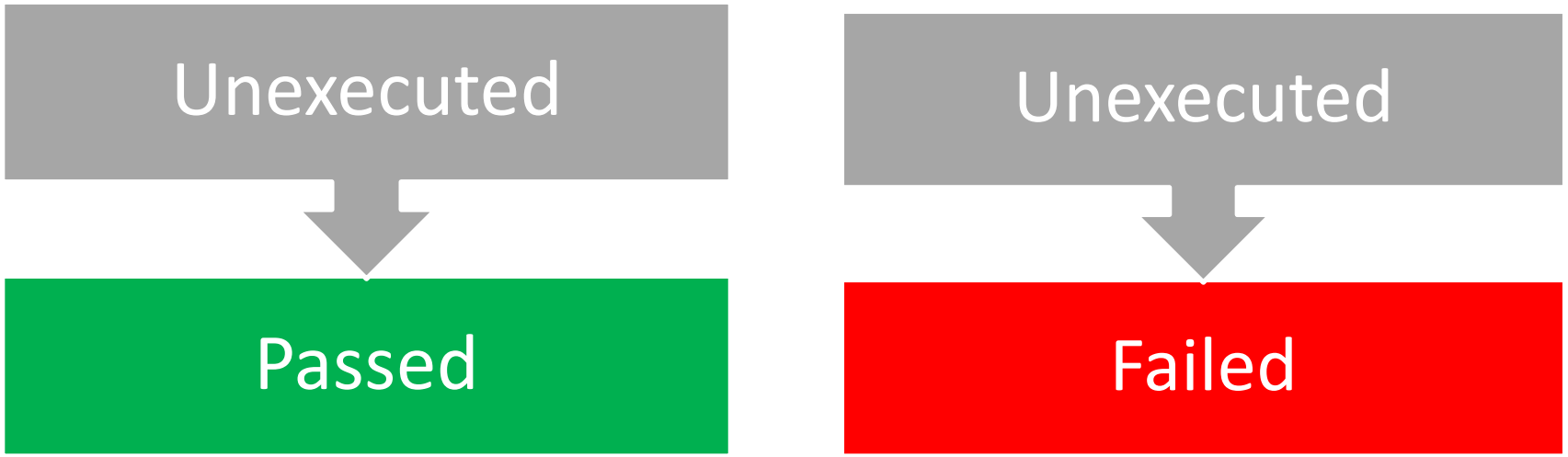
Certification – about

- ISTQB: functional testing
  - Body of Knowledge
  - best practices
- CEH: (ethical) hacker
  - security threats, Hacking Techniques, tools, tricks, and security measures,…
- CPTE: penetration testing
  - testing techniques
  - identify and repair vulnerabilities

Conclusions a grandpa would make

- Functional testing care about
  - Test documentation
  - Formal process followed
  - [Controlling those who test]
- Security testing care about
  - Security testing
  - Security
  - [Empowering those who tests]

Test case pass/fail ratio



WIKIPEDIA:

…passing security testing is not an indication that no flaws exist or that the system adequately satisfies the security requirements

Test Case don’t just pas or fail

Gate keeper	Agile: feedback
 Pass	 OK (safe) to use
 Fail	 Use at your own risk **Not tested enough**
 Not Yet Tested	 Don’t use: hazardous
	? **Implemented** Not Yet ~~Tested~~

QUESTIONS?

Contact:

Ainārs Galvāns

Security Tester, Exigen Services Latvia

ainars.galvans@exigenservices.com

J.Dalina iela| Riga, LV-1013, Latvia

phone +371 6707 2976 | mobile +371 2943 2698

www.exigenservices.lv