

Applications are as risky as ever



of all applications used some kind of hard-coded password



of all applications use broken or risky cryptographic algorithms



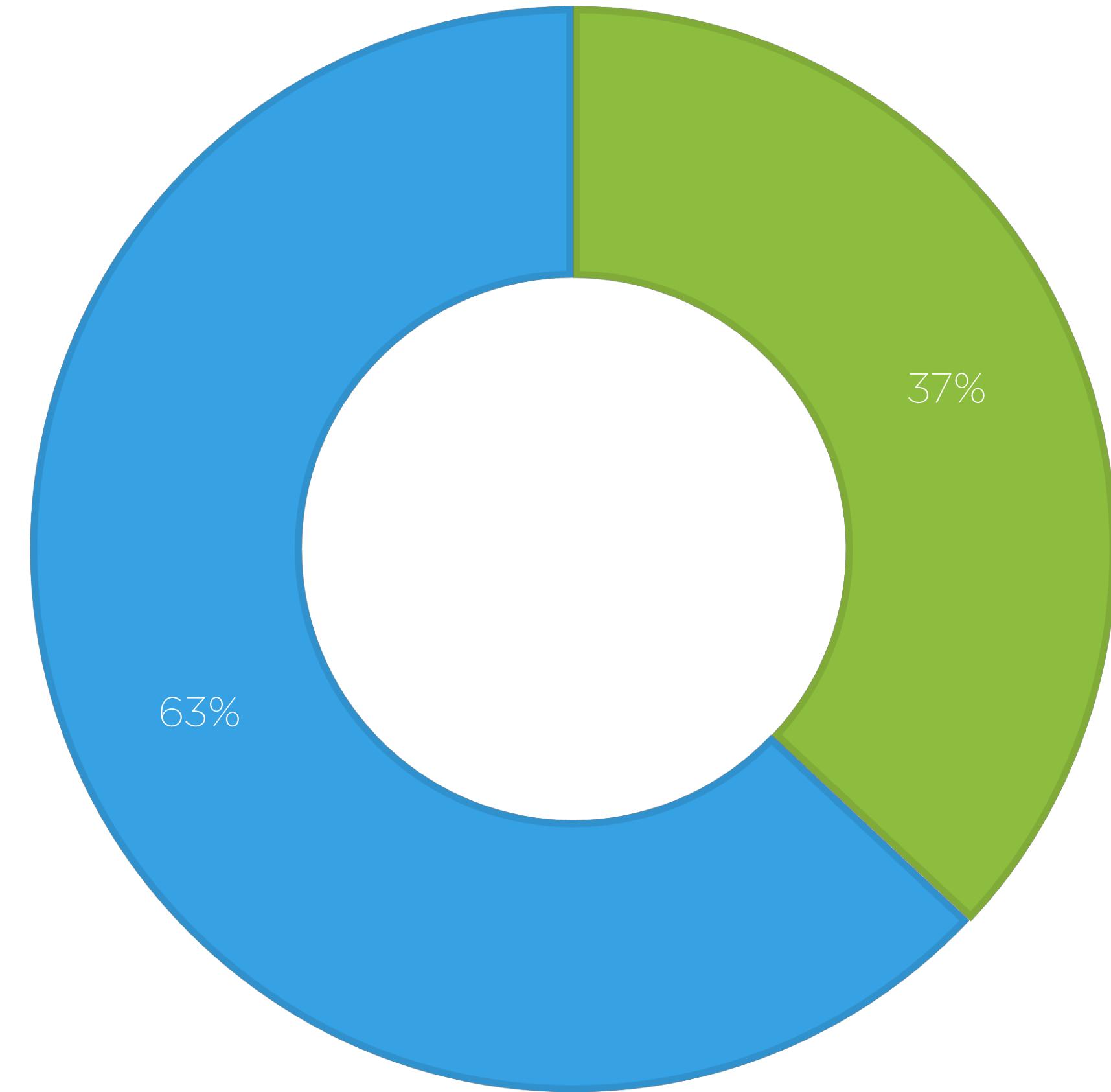
of all applications were vulnerable to open redirect attacks



of all applications mix trusted and untrusted data in the same data structure or message

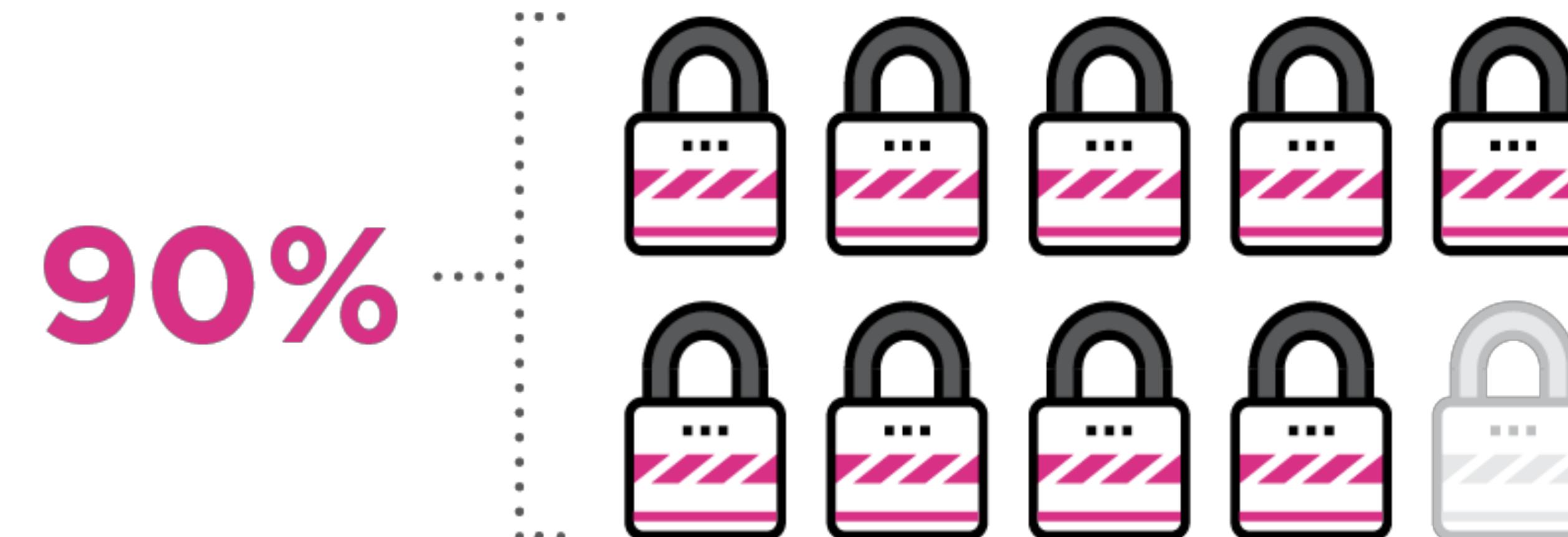
Majority of internally developed applications fail OWASP

01



Lack of App Security is Damaging Companies

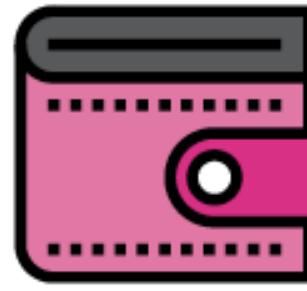
U.S. Department of Homeland Security (DHS) research found that **90 percent** of security incidents result from exploits against defects in software.



High Profile Breaches

All attacked through the app layer

01



TARGET

HOW: Sophisticated kill chain including exploitation of a vulnerable web application

RESULT: Hackers stole names, mailing addresses, phone numbers and email addresses from over 70 million shoppers



JPMORGAN CHASE

HOW: Vulnerability on website built and maintained by a third-party vendor in support of a charity

RESULT: Usernames and passwords for 76 million households and 7 million businesses accounts were stolen

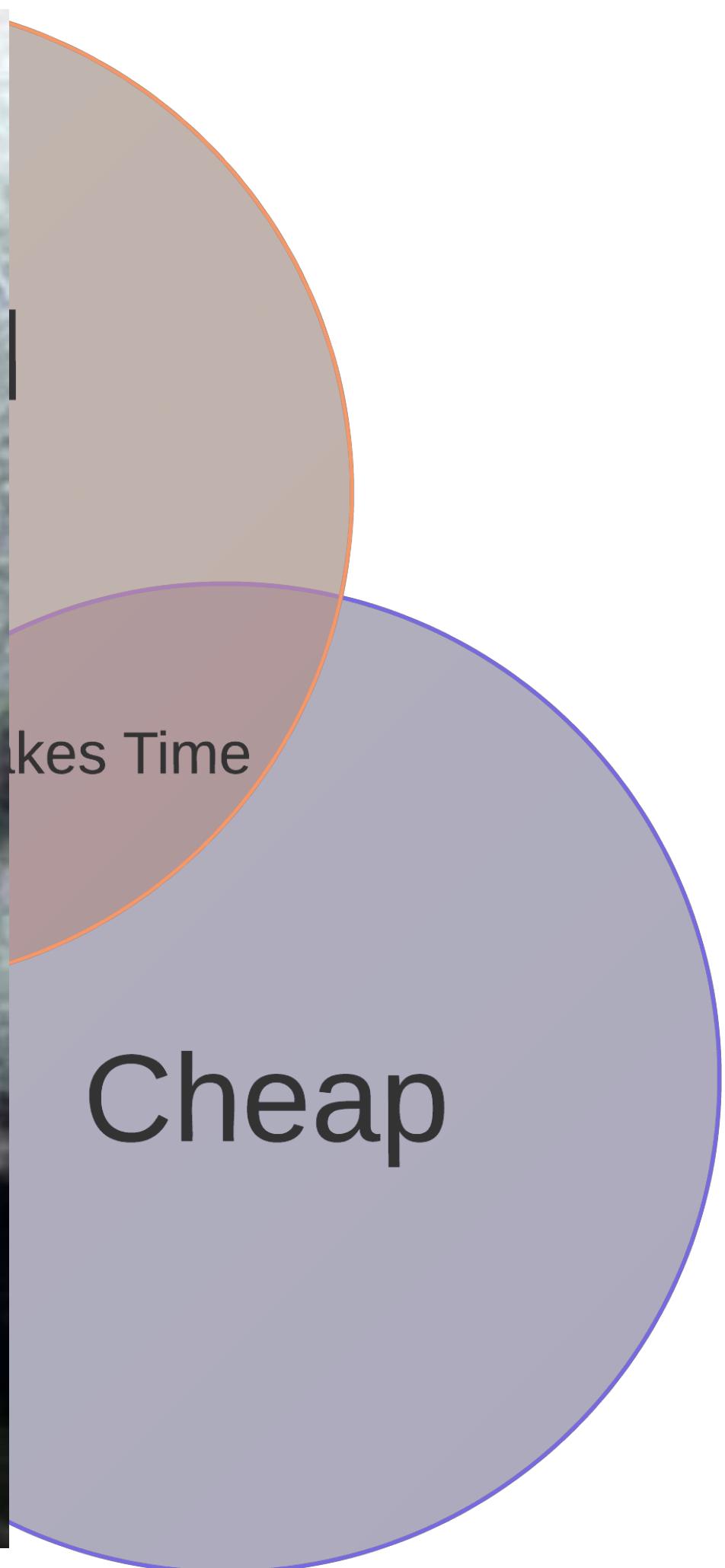
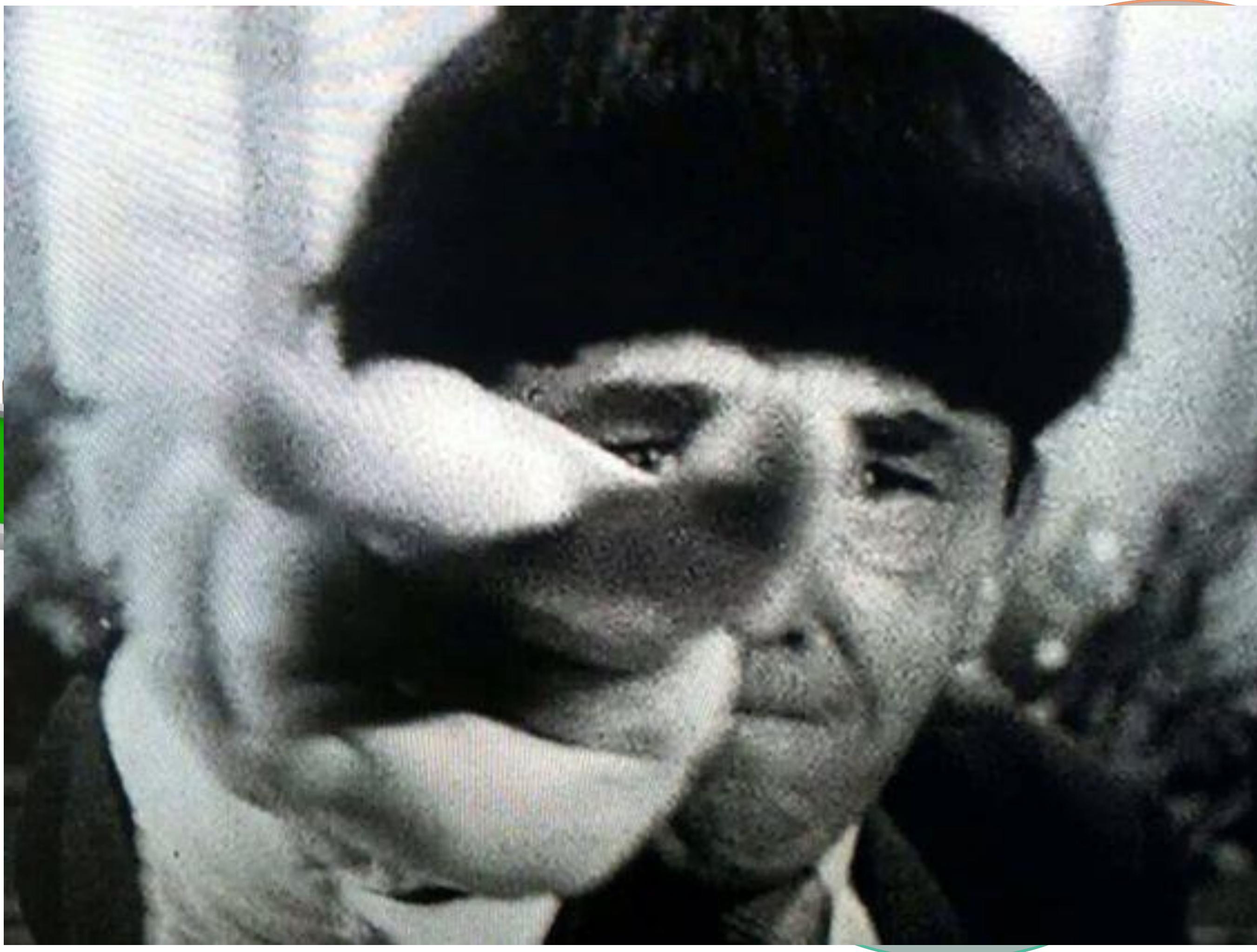


COMMUNITY HEALTH

HOW: Targeted a flaw in OpenSSL, CVE-2014-0160, better known as Heartbleed

RESULT: The theft of Social Security numbers and other personal data belonging to 4.5 million patients

Business Mandate



Compressed Timelines

01

Waterfall

January							February							March						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S
4	5	6	7	8	9	10	8	9	10	11	12	13	14	8	9	10	11	12	13	14
11	12	13	14	15	16	17	15	16	17	18	19	20	21	15	16	17	18	19	20	21
18	19	20	21	22	23	24	22	23	24	25	26	27	28	22	23	24	25	26	27	28
25	26	27	28	29	30	31	29	30	31					29	30	31				
0:4 0:13 0:20 0:26							0:3 0:11 0:18 0:25							0:5 0:13 0:20 0:27						
April							May							June						
5	6	7	8	9	10	11	3	4	5	6	7	8	9	7	8	9	10	11	12	13
12	13	14	15	16	17	18	10	11	12	13	14	15	16	14	15	16	17	18	19	20
19	20	21	22	23	24	25	17	18	19	20	21	22	23	21	22	23	24	25	26	27
26	27	28	29	30			24	25	26	27	28	29	30	21	22	23	24	25	26	27
0:4 0:11 0:18 0:25							0:3 0:11 0:18 0:25							0:2 0:9 0:16 0:24						
July							August							September						
5	6	7	8	9	10	11	2	3	4	5	6	7	8	9	10	11	12	13	14	
12	13	14	15	16	17	18	9	10	11	12	13	14	15	13	14	15	16	17	18	19
19	20	21	22	23	24	25	16	17	18	19	20	21	22	20	21	22	23	24	25	26
26	27	28	29	30	31		23	24	25	26	27	28	29	27	28	29	30	31		
0:1 0:8 0:15 0:24 0:31							0:6 0:14 0:22 0:29							0:5 0:13 0:21 0:27						
October							November							December						
4	5	6	7	8	9	10	8	9	10	11	12	13	14	6	7	8	9	10	11	12
11	12	13	14	15	16	17	15	16	17	18	19	20	21	13	14	15	16	17	18	19
18	19	20	21	22	23	24	22	23	24	25	26	27	28	20	21	22	23	24	25	26
25	26	27	28	29	30	31	29	30						27	28	29	30	31		
0:4 0:12 0:20 0:27							0:3 0:11 0:19 0:25							0:3 0:11 0:18 0:25						

1-4 Releases
Per Year

Agile

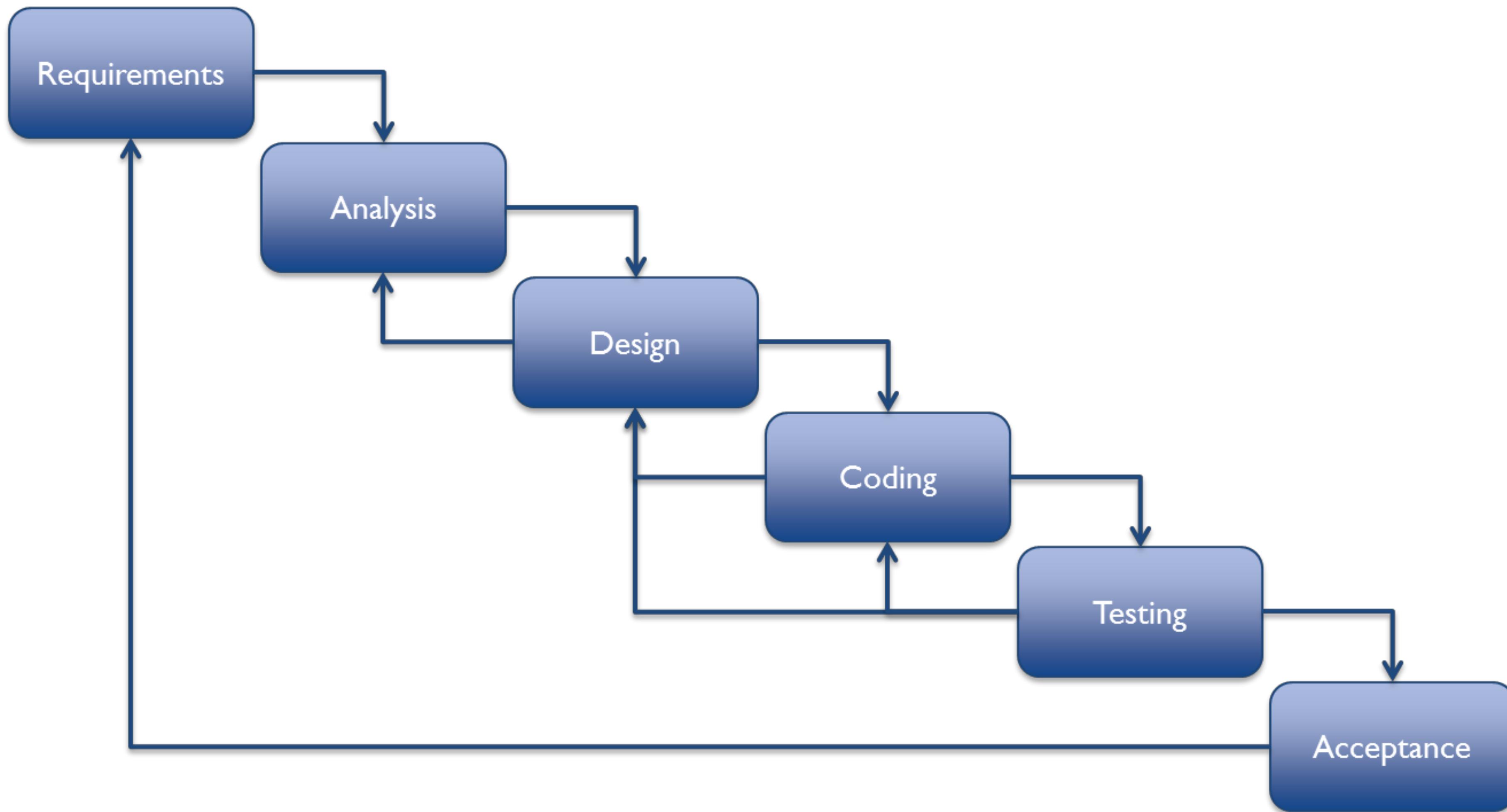
January							February							March						
S	M	T	W	T	F	S	S	M	T	W	T	F	S	S	M	T	W	T	F	S
4	5	6	7	8	9	10	8	9	10	11	12	13	14	8	9	10	11	12	13	14
11	12	13	14	15	16	17	15	16	17	18	19	20	21	15	16	17	18	19	20	21
18	19	20	21	22	23	24	22	23	24	25	26	27	28	22	23	24	25	26	27	28
25	26	27	28	29	30		29	30						27	28	29	30	31		
0:4 0:13 0:20 0:26							0:3 0:11 0:18 0:25							0:5 0:13 0:20 0:27						
April							May							June						
5	6	7	8	9	10	11	3	4	5	6	7	8	9	7	8	9	10	11	12	13
12	13	14	15	16	17	18	10	11	12	13	14	15	16	14	15	16	17	18	19	20
19	20	21	22	23	24	25	17	18	19	20	21	22	23	21	22	23	24	25	26	27
26	27	28	29	30			24	25	26	27	28	29	30	21	22	23	24	25	26	27
0:4 0:11 0:18 0:25							0:3 0:11 0:18 0:25							0:2 0:9 0:16 0:24						
July							August							September						
5	6	7	8	9	10	11	2	3	4	5	6	7	8	9	10	11	12	13	14	
12	13	14	15	16	17	18	9	10	11	12	13	14	15	13	14	15	16	17	18	19
1																				

Definition of DevOps

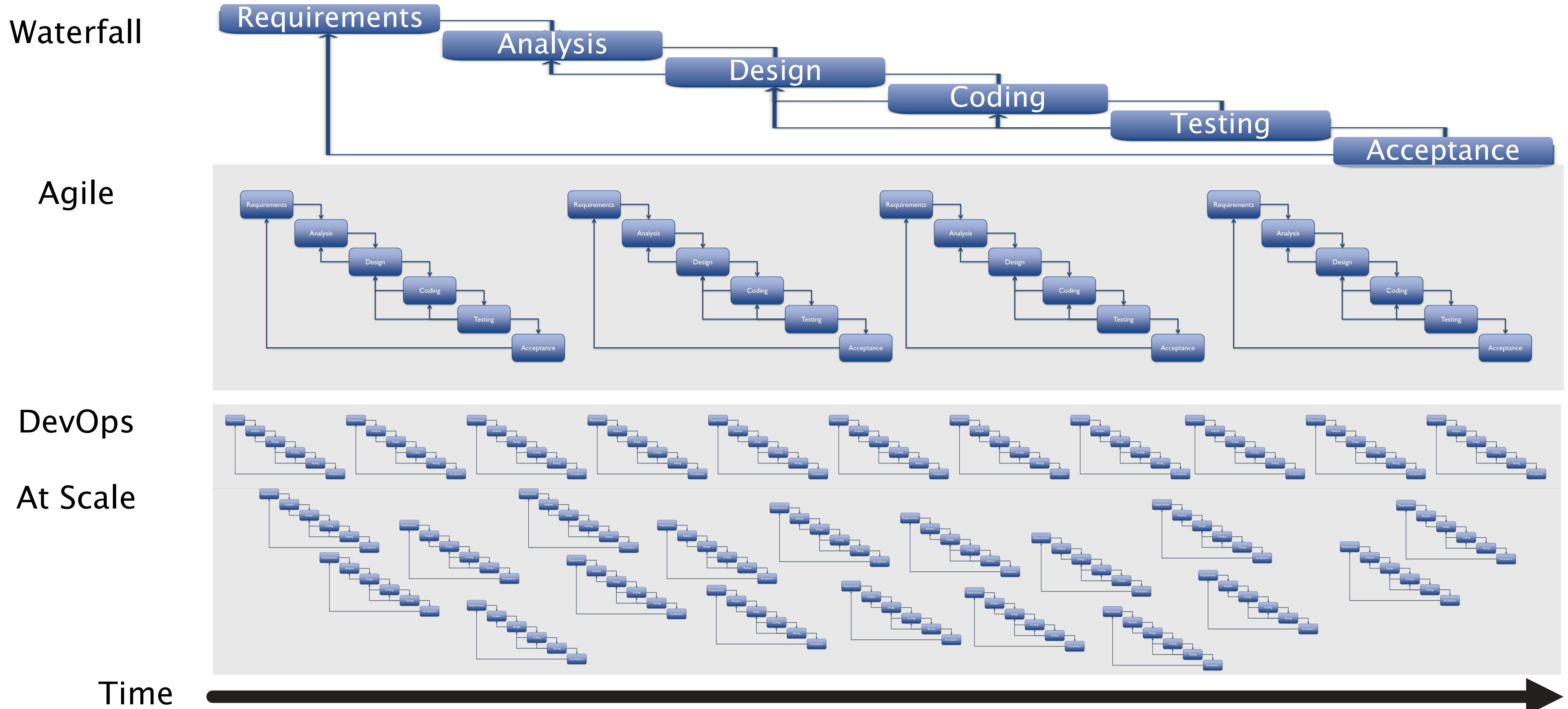
“DevOps is a cultural and professional movement, focused on how we build and operate high velocity organizations, born from the experiences of its practitioners.”

- Nathan Harvey (Chef)

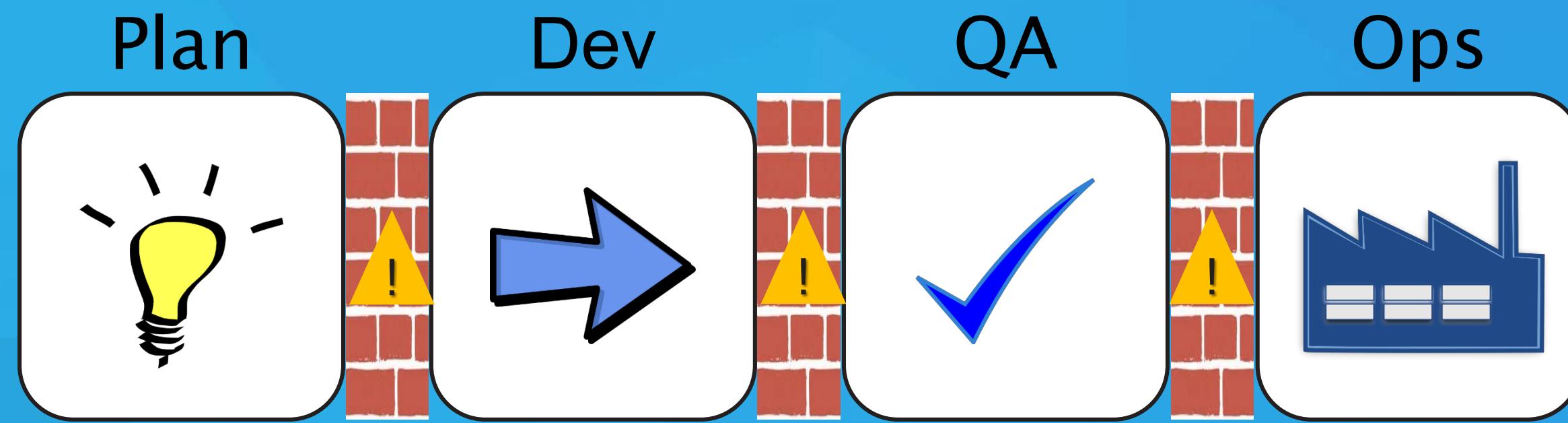
Basic development cycle



Not so different after all



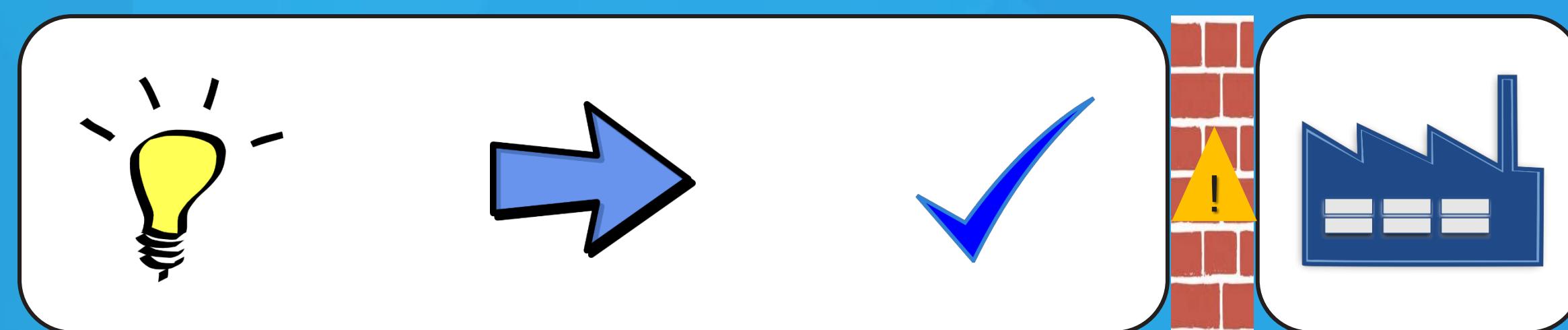
Waterfall



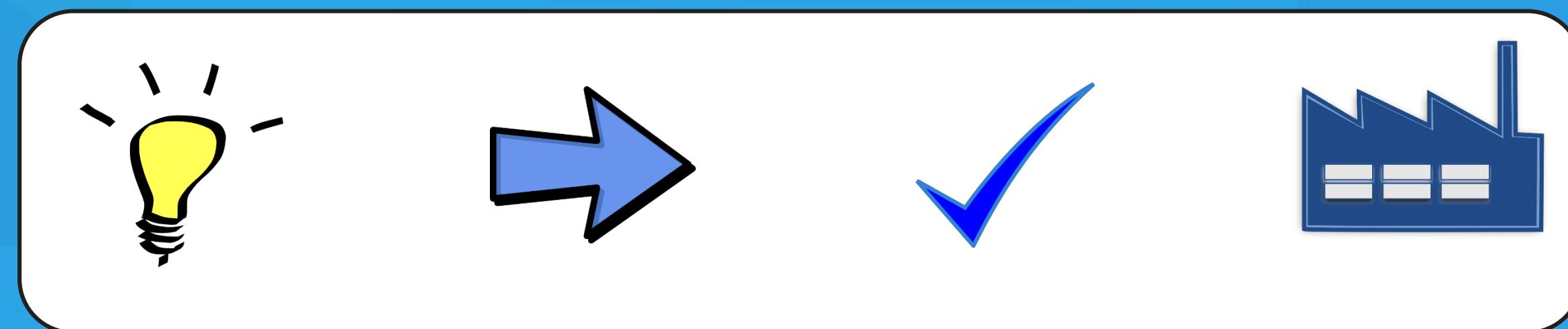
Business Intent
App Knowledge
Ops Knowledge

Business Intent
App Knowledge
Ops Knowledge

Agile



DevOps



Continuity

Agile - Process



Transformation - Technology

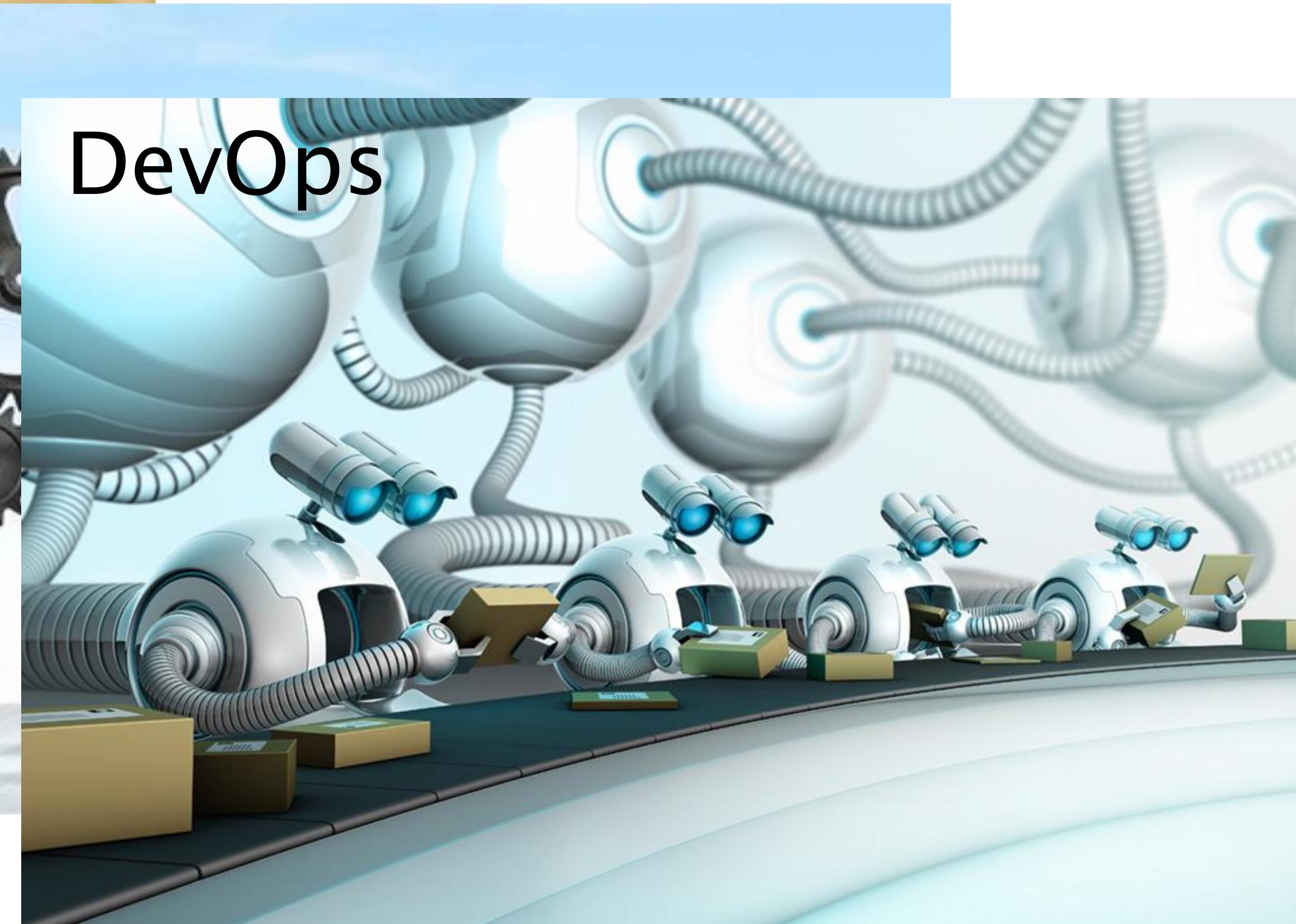
Waterfall



Agile



DevOps



Is this your current AppSec program?



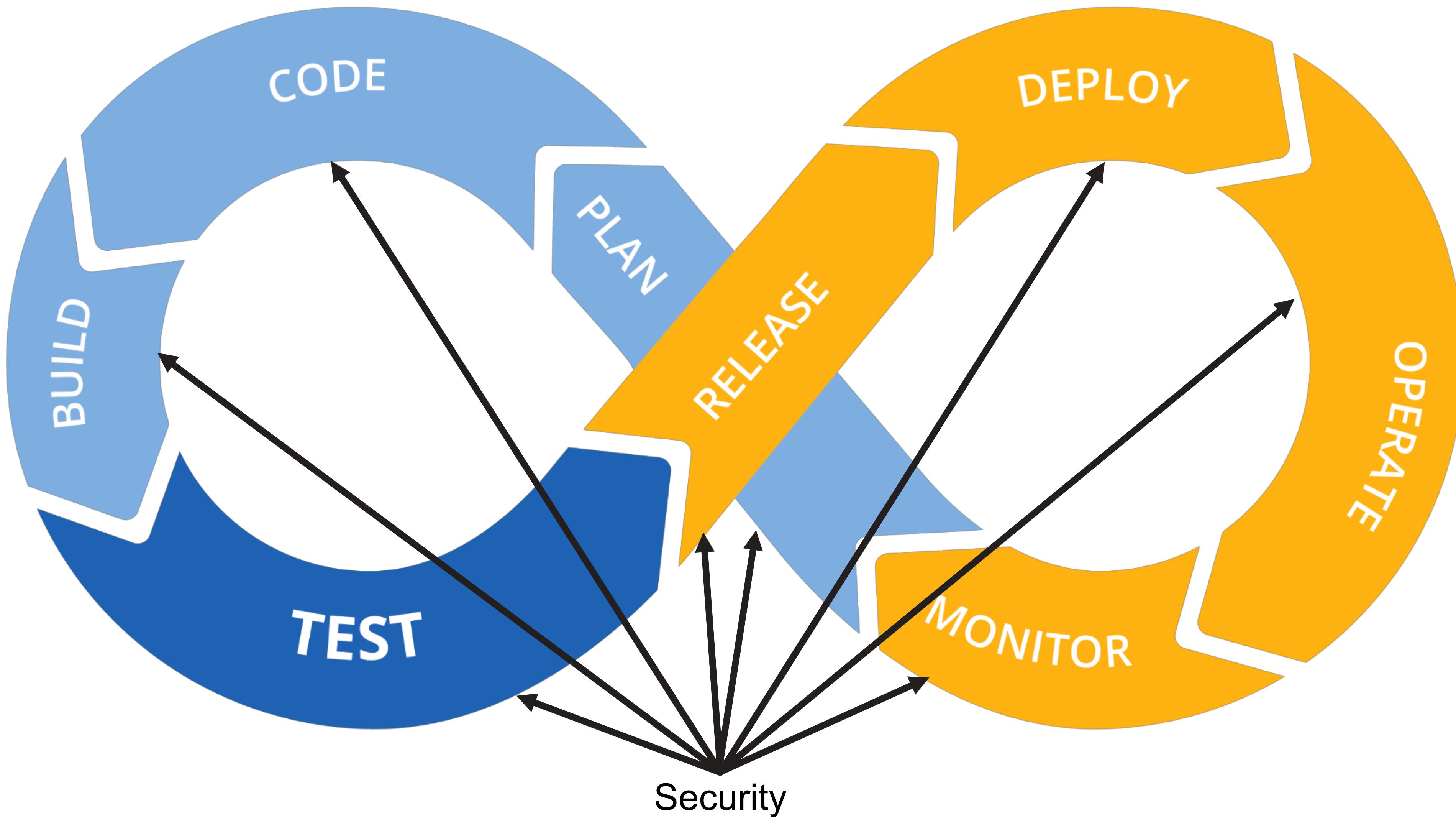
They/We know it's coming...



Which outcome do you see?



DevOps – Process: Where is security?



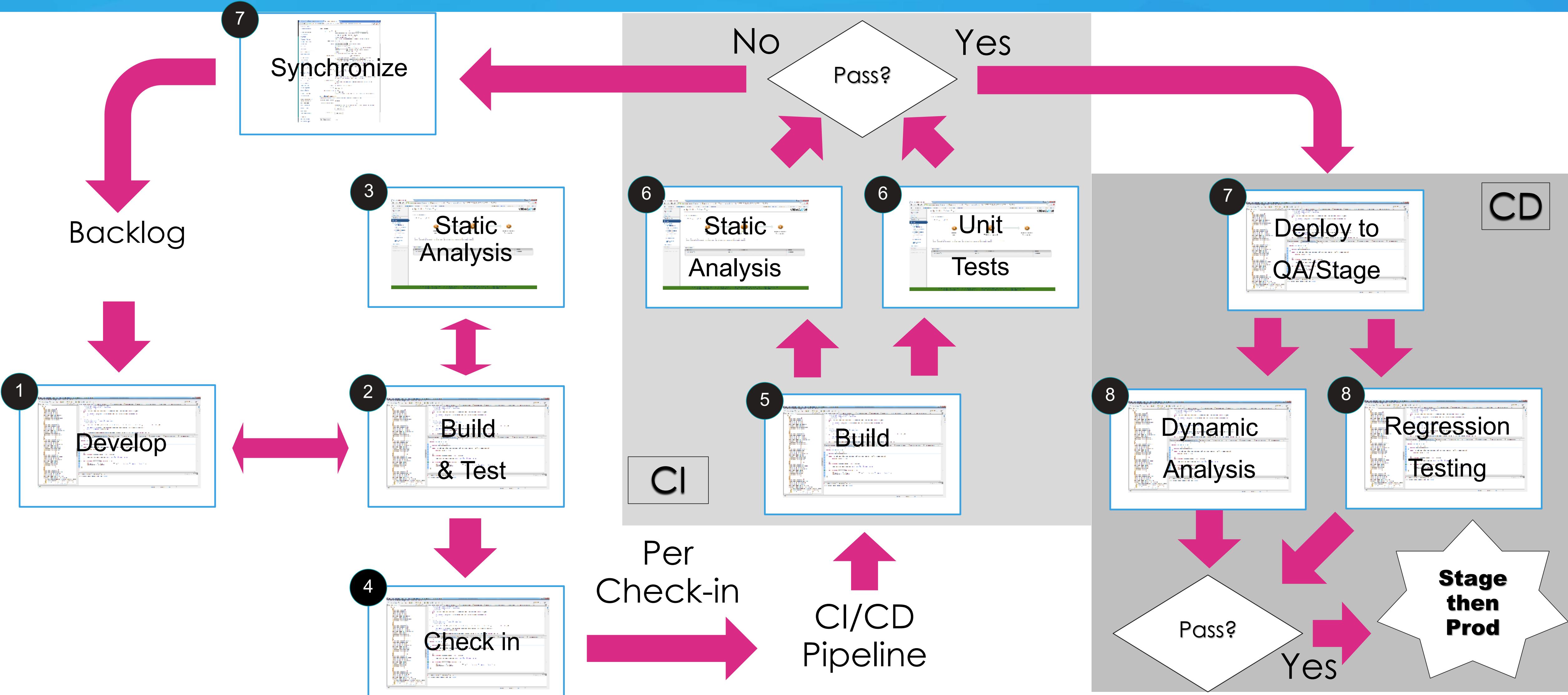
Strategy

- Integration & Automation
- 3-legged barstool:
 - Training
 - Remediation Coaching
 - Scan early & often



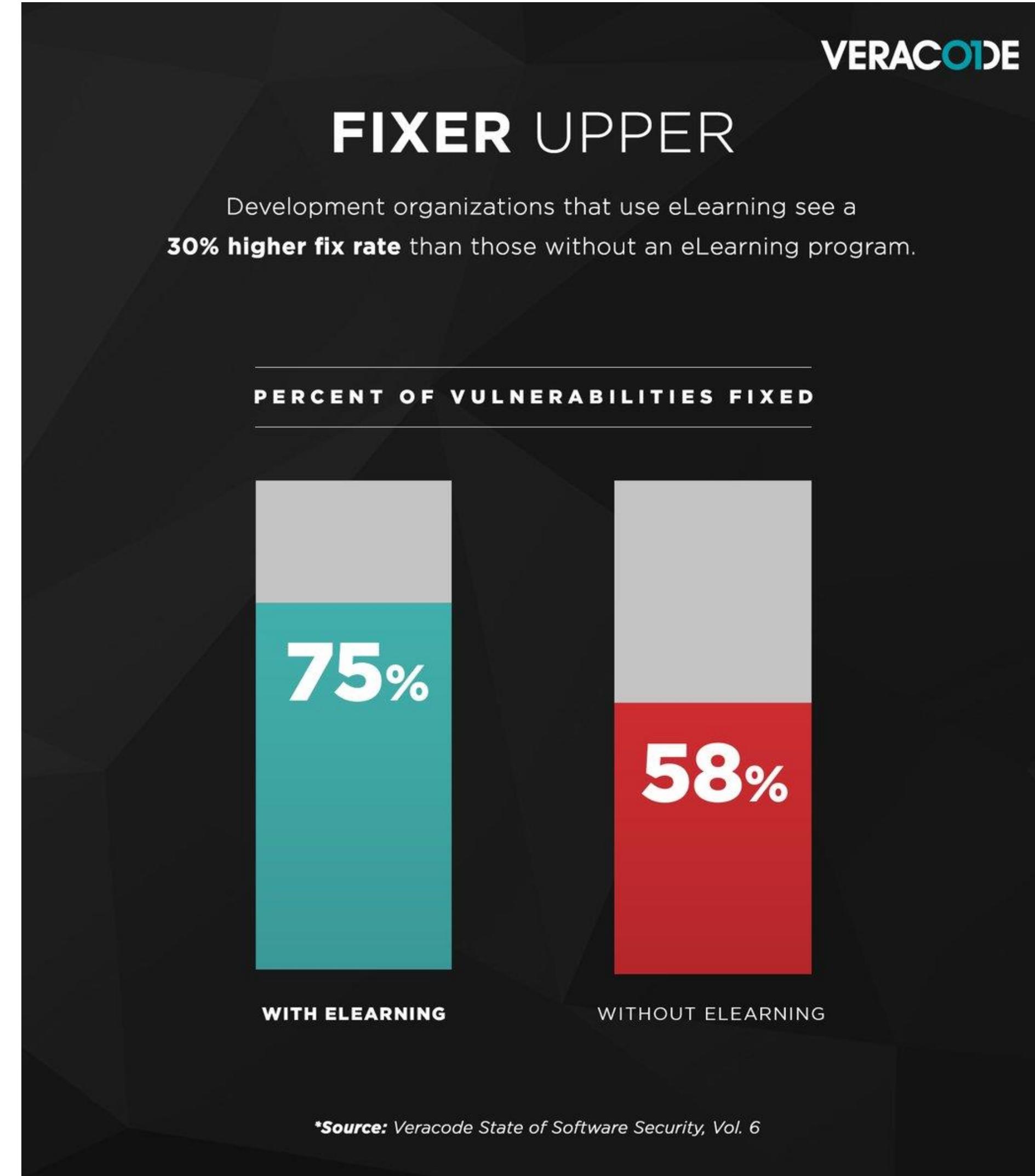
Strategy – Integration & Automation

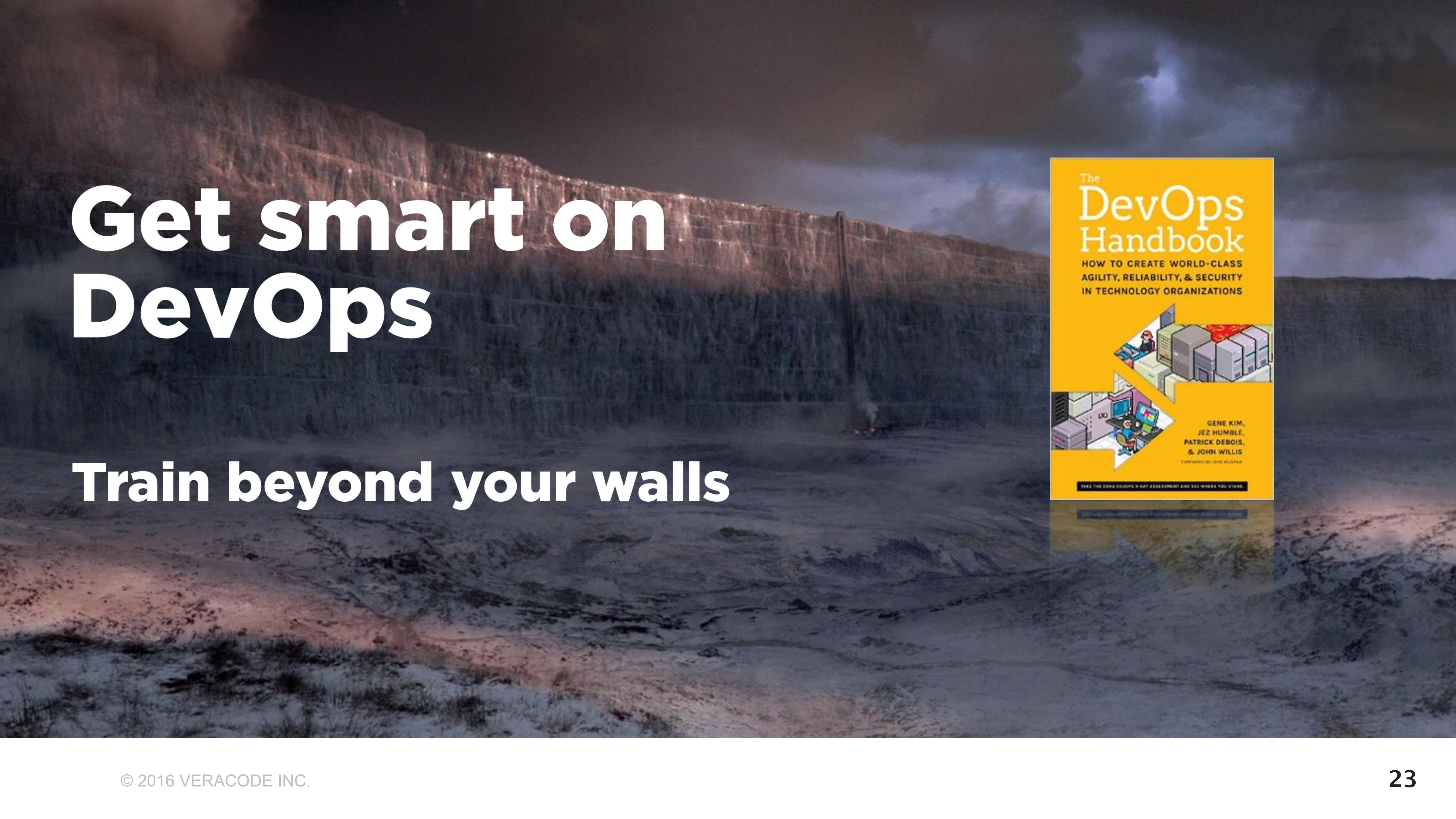
01



Strategy - Training

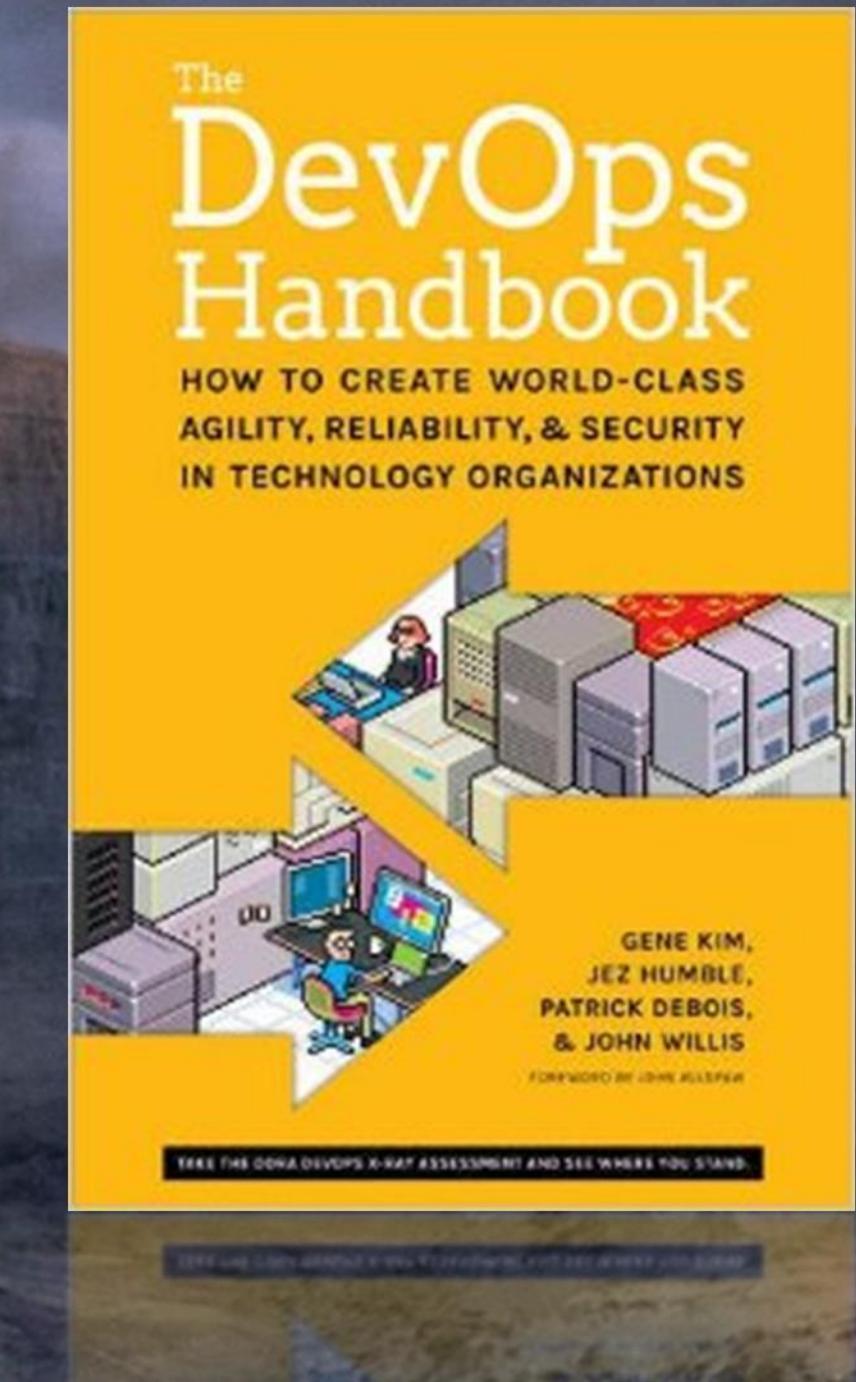
- Security teams can help developers by providing training, either through eLearning or in-person Instructor Led Training
- Think about targeted training based on policy violations





Get smart on DevOps

Train beyond your walls



Strategy - Remediation Coaching

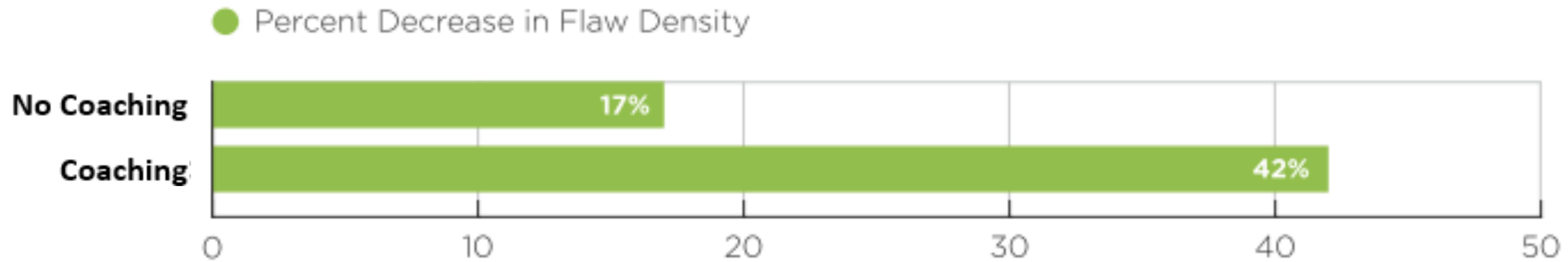
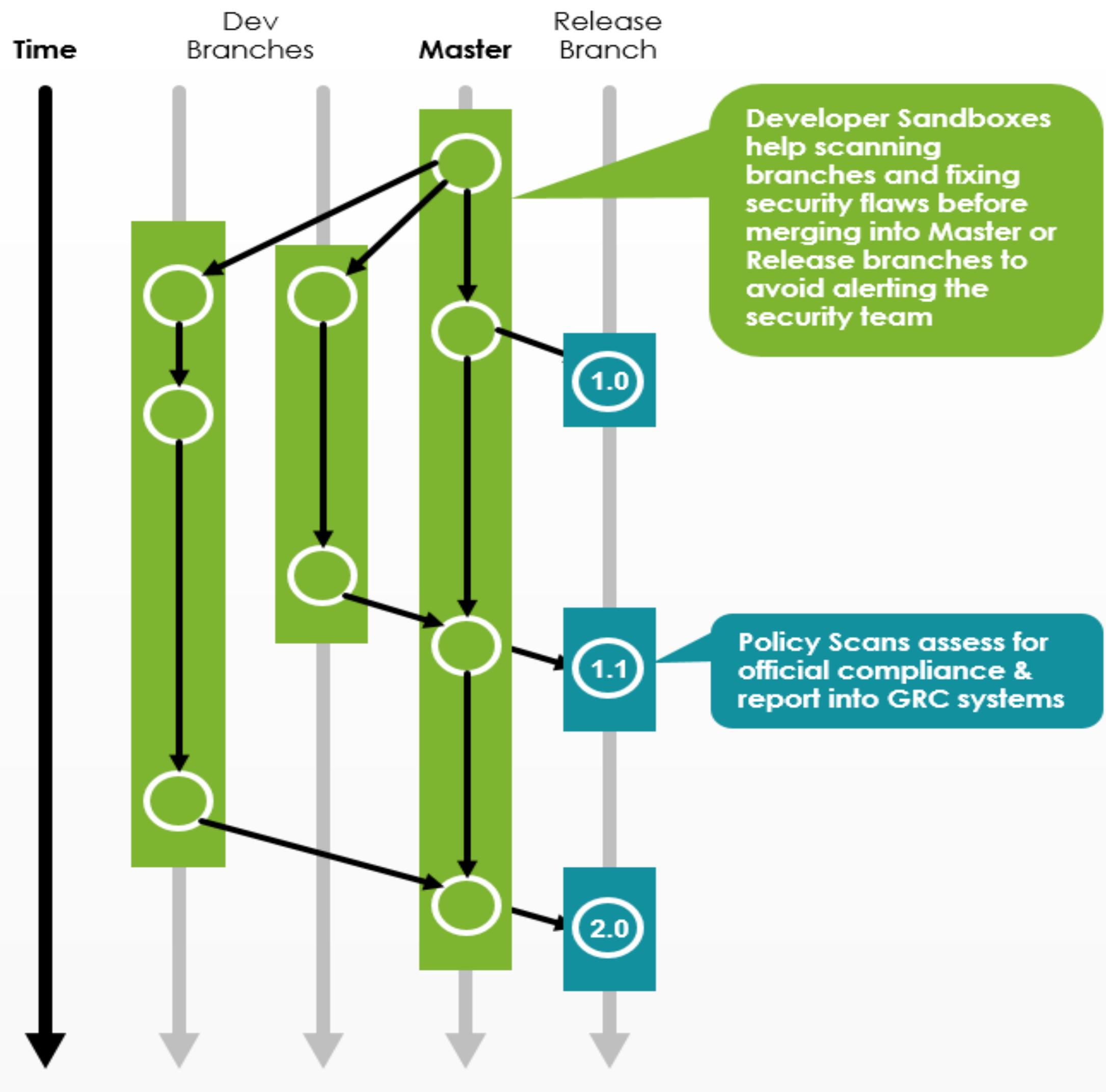


Figure 10: Relative Improvement in Flaw Density via Remediation Coaching (Readout)

**For applications that used remediation coaching,
development teams fixed more than 2.5x the
average # of flaws per megabyte**

Strategy – Measurement (Scan early, scan often)



Applications that used sandbox had an average fix rate of 59%, or a 2x improvement in fix rate

DevOps – Pervasive Security



Training
(eLearning, instructor led, metadata driven)



Static Application Security Testing + 3rd Party Risk Analysis

Dynamic Application Security Testing

**Runtime Application
Self Protection**



**Threat Modeling
Security Grooming
Secure Design**

**Remediation and Mitigation Guidance
Secure Code Reviews**

**Manual Penetration Testing
Red Team Activities**