

AppSec in a DevOps World

Peter Chestna, Director of Developer Engagement

Who am I?

- 25 Years Software Development Experience
- 10+ Years Application Security Experience
- Certified Agile Product Owner and Scrum Master
- At Veracode since 2006
 - From Waterfall to Agile to DevOps
 - From Monolith to MicroService
 - Consultant on DevSecOps best practices
- Fun Fact: I love whiskey!





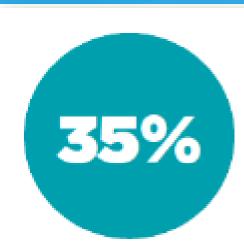
Goals



- Why is AppSec important?
- · How is DevOps changing application development?
- · How is AppSec traditionally done?
- · What needs to change?
 - What to build
 - What to measure
 - How to help

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



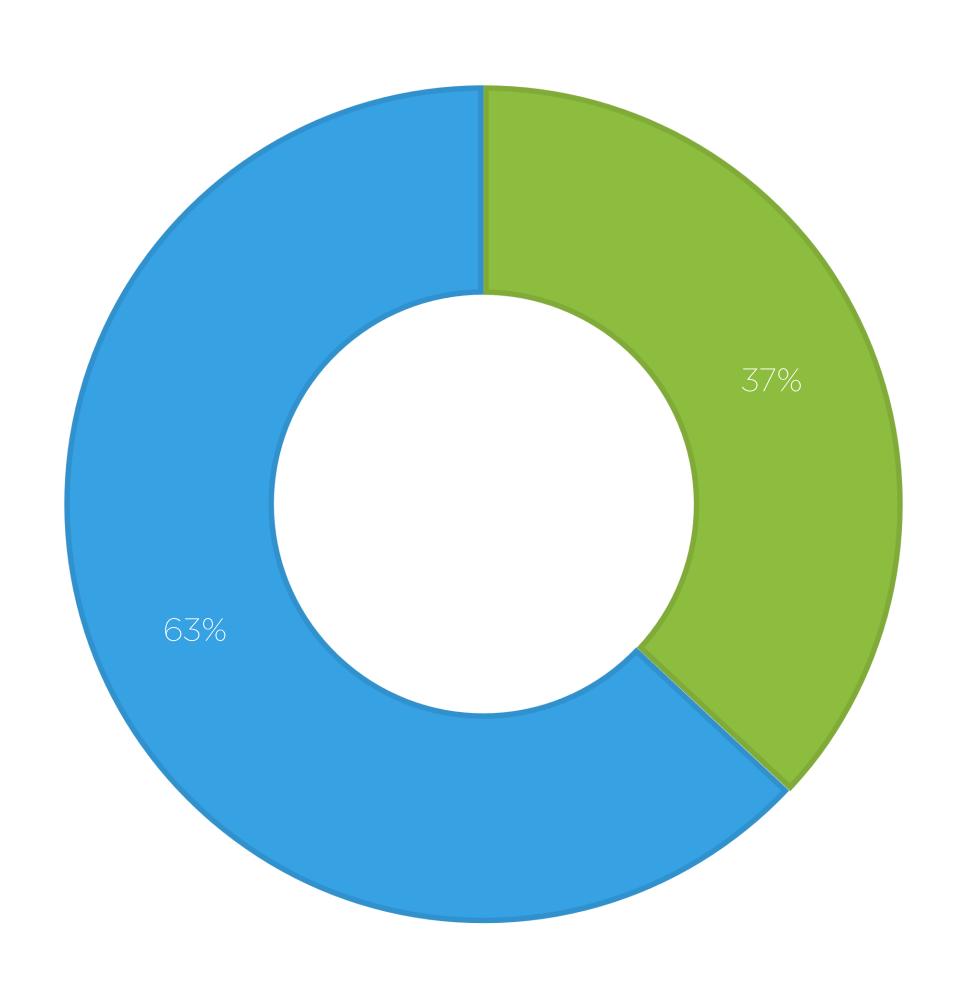
of all applications were vulnerable to open redirect attacks



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

Majority of internally developed applications fail OWASP

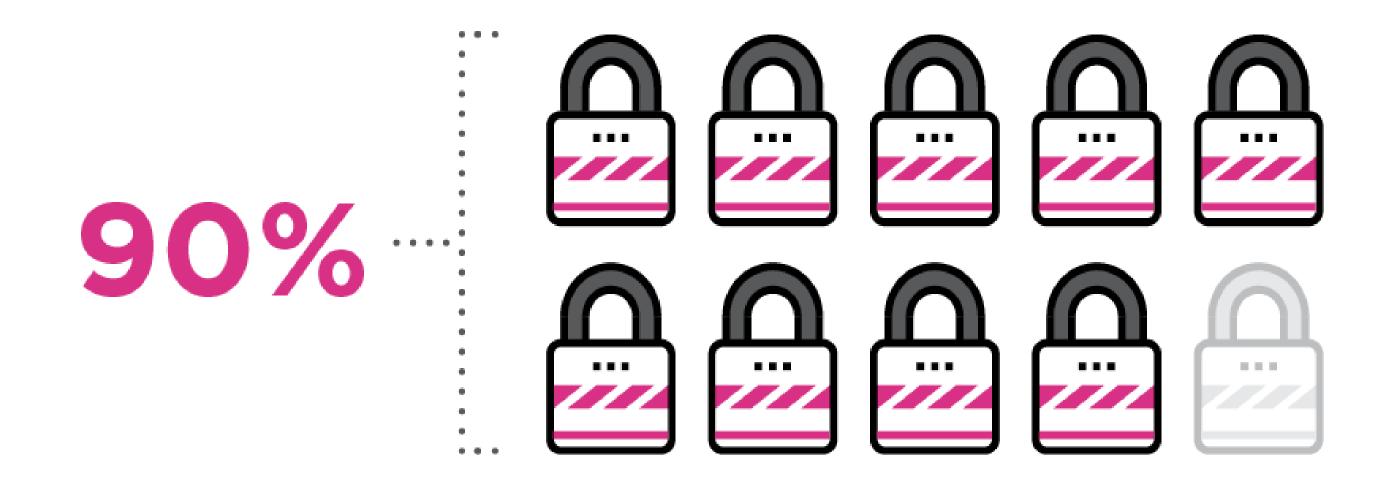




Lack of App Security is Damaging Companies



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





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



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

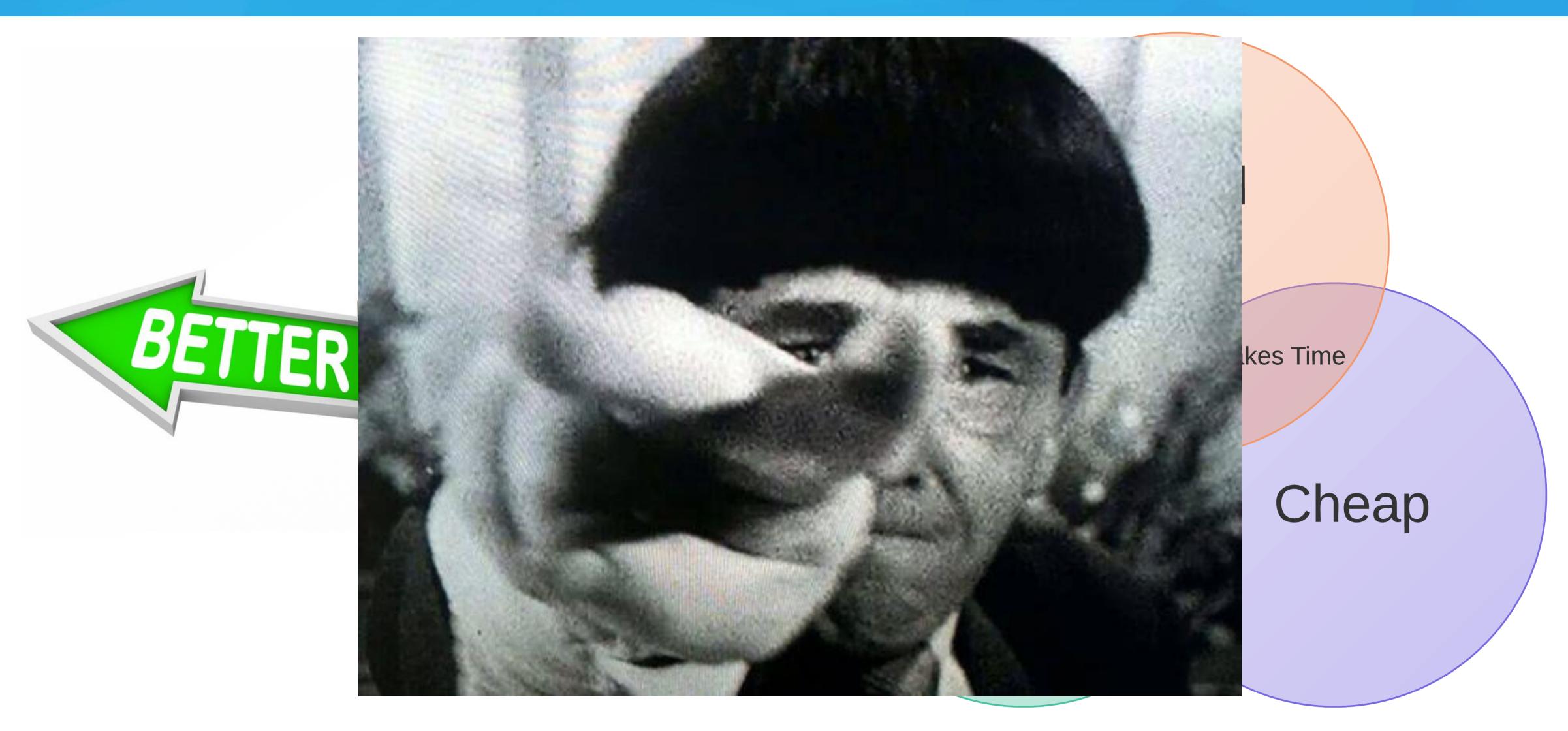


HOW: Targeted a flaw in OpenSSL, CVE-2014-0160, better known as Heartbleed

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

Business Mandate





Compressed Timelines



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						
1 2 3	1 2 3 4 5 6 7	1 2 3 4 5 6 7						
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						
O:4 @:13 @:20 @:26	O:3 Q:11 ●:18 €:25	O:5 @:13 @:20 €:27						
April	May	June						
S M T W T F S	S M T W T F S	S M T W T F S						
1 2 3 4	1 2	1 2 3 4 5 6						
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	4 Keleas	\mathbf{P} \mathbf{C} 30						
O:4 Q:11 @:18 D:25	O:3 Q:11 @:18 O:25	O:2 @:9 @:16 @:24						
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:4 0:13 •:20 •:26 April S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18		September						
July	August	September						
S M T W T F S	TO M T TO S C	S M T W T F S						
s M T W T F S 1 2 3 4	TO M T TO S C	s M T W T F S 1 2 3 4 5						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11	Per Year	s M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18	Per Year	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	Per Year 9 10 11 12 13 14 15 16 17 18 19 20 21 22	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25	Per Year 9 10 11 12 13 14 15 16 17 18 19 20 21 22	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 O:1 Q:8 •:15 C:24 O:31	Per 4 5 6 ear 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 0:14 0:22 0:29	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 0:5 •:13 •:21 0:27						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 October	Per 4 5 6 ear 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 •:14 •:22 0:29 November	s M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 0:5 •:13 •:21 0:27 December						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 October S M T W T F S	Per 4 5 6 ear 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 •:14 •:22 0:29 November S M T W T F S	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 0:5 •:13 •:21 0:27 December S M T W T F S						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 October S M T W T F S 1 2 3	Per 4 5 6 ear 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 •:14 •:22 0:29 November S M T W T F S 1 2 3 4 5 6 7	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 December S M T W T F S 1 2 3 4 5						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 October S M T W T F S	Per 4 5 6 ear 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 •:14 •:22 0:29 November S M T W T F S	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 December S M T W T F S 1 2 3 4 5						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 October S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	Per 4 5 6 ear 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 •:14 •:22 0:29 November S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 December S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 October S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17	Per 4 5 6 ear 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 •:14 •:22 0:29 November S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 December S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 October S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31	Per 4 5 6 Car 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 0:14 0:22 0:29 November S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 0:5 •:13 •:21 0:27 December S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31						
S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 October S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24	Per 4 5 6 Car 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 0:6 0:14 0:22 0:29 November S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28	S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 0:5 •:13 •:21 0:27 December S M T W T F S 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26						

Agile



DevOps

		Ja	anua	ry						Fe	bru	ary						Λ	/larc	h		
S	M	T	W	T	F	S		S	М	T	W	T	F	S		S	M	T	W	T	F	S
			_	1	2	3		1	2	3	4	5	6	7		1	2	3	4	5	6	7
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 31	25	26	27	28
25	26	27	28	29	30	31										29	30	31				
	0:4	g: 1	3 :	20 O	: 26				0:3	g: 1	1 :	18 €	: 25				0:5	g:1	3 :	20 €	: 27	
			Apri								Мау	/							June	Э		
S	M	T	W	T	F	S		S	М	T	W	T	F	S		S	М	T	W	T	F	S
			1	2	3	4							1	2			1	2	3	4	5	6
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				24	1	0	17	18	19	20	21	22	23		21	22	23	24		26	27
26	27			30				24	25					25	419	G ^o		5				
		0:1	1 0:	18 0	: 25		J	31	0:3	0:1		18 0			~ •				9 :	16 e	24	
			linky							Δ	11011	ct						Sor	atom	hor		
c	м		July								ugu		-				1.1	Sep	otem			c
S	М	Т	July w	7 2	F 3	s 4		D	M				F	S	r		М	Sep T	otem w	ber 3	F 4	s 5
s 5	м			T		s 4 11		2	e				9	å	r	s 6	м 7	Sep 1 8		T		
	м 6 13		W 1	2	3	4		2 9	e				2	a 15	r	6 13	M 7 14	1		3	4	5
5	6 13 20		1 8	7 2 9	3 10	11	ı	_	M 10 17						r	6 13 20	7	1 8		3	4	5 12
5	6	7 14	1 8 15	7 2 9 16	3 10 17	4 11 18	ı	9	10	r	5 12	Y ₆	14	15	r	6	7 14	T 1 8 15	w 2 9 16	3 10 17	4 11 18	5 12 19
5 12 19	6 13 20	7 14 21	w 1 8 15 22	7 2 9 16 23	3 10 17 24	4 11 18	ı	9	10	11	5 12 19	6 13 20	14 21	15 22	r	6 13 20	7 14 21	1 8 15 22	w 2 9 16 23	3 10 17	4 11 18	5 12 19
5 12 19 26	6 13 20	7 14 21 28	w 1 8 15 22 29	9 16 23 30	3 10 17 24 31	4 11 18 25		9 16 23	10 17 24 31	11 18 25	5 12 19 26	6 13 20	14 21 28	15 22	r	6 13 20	7 14 21 28	1 8 15 22 29	w 2 9 16 23	3 10 17 24	4 11 18 25	5 12 19
5 12 19 26	6 13 20 27	7 14 21 28	w 1 8 15 22 29	7 2 9 16 23 30	3 10 17 24 31	4 11 18 25	ı	9 16 23	10 17 24 31	11 18 25	5 12 19 26	13 20 27	14 21 28	15 22	r	6 13 20	7 14 21 28	1 8 15 22 29	2 9 16 23 30	1 3 10 17 24	4 11 18 25	5 12 19
5 12 19 26	6 13 20 27	7 14 21 28	w 1 8 15 22 29	1 2 9 16 23 30 •: 24 er	3 10 17 24 31 0:31	4 11 18 25		9 16 23 30	10 17 24 31 o:6	11 18 25 •:1	5 12 19 26 14 ©:	6 13 20 27 22 0	14 21 28 229	15 22 29 s	r	6 13 20	7 14 21 28	1 8 15 22 29 •:1	2 9 16 23 30	1 3 10 17 24 21 0	4 11 18 25 :27	5 12 19 26
5 12 19 26	6 13 20 27 0:1	7 14 21 28 0:8 0	w 1 8 15 22 29 •: 15 ctob	7 9 16 23 30 •: 24 er 1	3 10 17 24 31 0:31	4 11 18 25 s		9 16 23 30 s	10 17 24 31 o:6	11 18 25 Nor T	5 12 19 26 14 0: vem w	6 13 20 27 22 0 ber 5	14 21 28 229 F	15 22 29 s 7	r	6 13 20 27	7 14 21 28 •:5	1 8 15 22 29 De	w 2 9 16 23 30 13 ©:	1 3 10 17 24 21 0 ber	4 11 18 25 :27	5 12 19 26 s
5 12 19 26	6 13 20 27 0:1 M	7 14 21 28 0:8 0	w 1 8 15 22 29 •: 15 ctob	1 2 9 16 23 30 • c: 24 er 1 8	3 10 17 24 31 0:31 F 2 9	4 11 18 25 s 3 10		9 16 23 30 s 1 8	10 17 24 31 o::6 M 2 9	11 18 25 •:1 Nor T 3 10	5 12 19 26 14 ©: vem w 4 11	6 13 20 27 22 0 ber 1 5 12	14 21 28 29 F 6 13	15 22 29 s 7 14	r	6 13 20 27 s	7 14 21 28 •:5	1 8 15 22 29 •:1 De	2 9 16 23 30 13 ©: cem w 2 9	1 3 10 17 24 21 0 ber 1 3 10	4 11 18 25 :27	5 12 19 26 s 5 12
5 12 19 26 s	6 13 20 27 0:1 M	7 14 21 28 0:8 0 T	w 1 8 15 22 29 •: 15 ctob w	7 9 16 23 30 •: 24 er 1 8 15	3 10 17 24 31 0:31 F 2 9 16	4 11 18 25 s 3 10 17		9 16 23 30 s 1 8 15	10 17 24 31 0:6 M 2 9 16	11 18 25 Nor 1 3 10 17	5 12 19 26 14 0: vem w 4 11	6 13 20 27 22 0 ber 1 5 12	14 21 28 29 F 6 13 20	15 22 29 s 7 14 21	r	6 13 20 27 s	7 14 21 28 •:5 M	1 8 15 22 29 De 1 1 8 15	w 2 9 16 23 30 cem w 2 9 16	10 17 24 21 0 ber 1 3 10 17	4 11 18 25 :27 F 4 11 18	5 12 19 26 s 5 12 19
5 12 19 26 s	6 13 20 27 0:1 M 5 12	7 14 21 28 0:8 0 7 6 13 20	w 1 8 15 22 29 •:15 ctob w 7 14 21	1 2 9 16 23 30 0:24 er 1 8 15 22	3 10 17 24 31 0:31 F 2 9 16 23	4 11 18 25 s 3 10 17 24		9 16 23 30 s 1 8 15 22	10 17 24 31 0:6 M 2 9 16 23	11 18 25 •:1 Nor T 3 10	5 12 19 26 14 ©: vem w 4 11	6 13 20 27 22 0 ber 1 5 12	14 21 28 29 F 6 13	15 22 29 s 7 14	r	6 13 20 27 s 6 13 20	7 14 21 28 •:5 M 7 14 21	1 8 15 22 29 •:1 De 1 8 15 22	2 9 16 23 30 13 ©: cem w 2 9 16 23	10 17 24 21 0 ber 1 3 10 17 24	4 11 18 25 :27	5 12 19 26 s 5 12
5 12 19 26 s	6 13 20 27 0:1 M	7 14 21 28 0:8 0 T	w 1 8 15 22 29 •: 15 ctob w	7 9 16 23 30 •: 24 er 1 8 15	3 10 17 24 31 0:31 F 2 9 16	4 11 18 25 s 3 10 17		9 16 23 30 s 1 8 15	10 17 24 31 0:6 M 2 9 16 23	11 18 25 Nor 1 3 10 17	5 12 19 26 14 0: vem w 4 11	6 13 20 27 22 0 ber 1 5 12	14 21 28 29 F 6 13 20	15 22 29 s 7 14 21	r	6 13 20 27 s	7 14 21 28 •:5 M	1 8 15 22 29 De 1 1 8 15	w 2 9 16 23 30 cem w 2 9 16	10 17 24 21 0 ber 1 3 10 17	4 11 18 25 :27 F 4 11 18	5 12 19 26 s 5 12 19
5 12 19 26 s	6 13 20 27 0:1 M 5 12 19 26	7 14 21 28 0:8 0 7 6 13 20 27	w 1 8 15 22 29 •:15 ctob w 7 14 21	1 2 9 16 23 30 0:24 er 1 8 15 22 29	3 10 17 24 31 0:31 F 2 9 16 23 30	4 11 18 25 8 3 10 17 24 31		9 16 23 30 s 1 8 15 22 29	10 17 24 31 0:6 M 2 9 16 23 30	11 18 25 Nor 1 3 10 17 24	5 12 19 26 14 ©: vem w 4 11 18 25	6 13 20 27 22 0 ber 1 5 12	14 21 28 29 F 6 13 20 27	15 22 29 s 7 14 21 28		6 13 20 27 s 6 13 20 27	7 14 21 28 •:5 M 7 14 21 28	1 8 15 22 29 •:1 1 8 15 22 29	2 9 16 23 30 13 ©: cem w 2 9 16 23	10 17 24 21 0 ber 10 17 24 31	4 11 18 25 25 11 18 25	5 12 19 26 s 5 12 19

Definition of DevOps

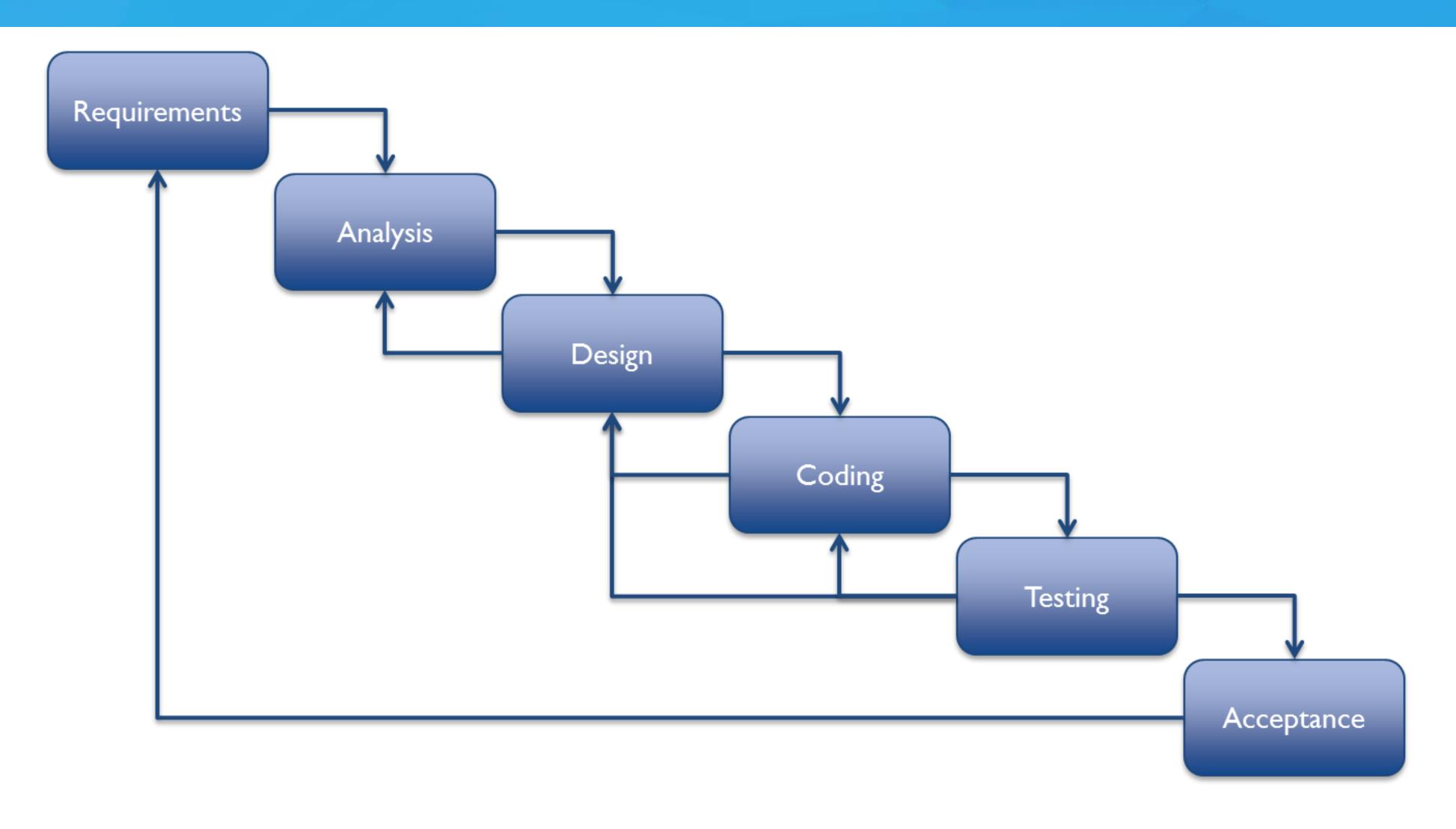


"DevOps is a cultural and professional movement, focused on how we build and operate high velocity organizations, born from the experiences of its practitioners."

- Nathan Harvey (Chef)

Basic development cycle





Not so different after all



Acceptance

Waterfall

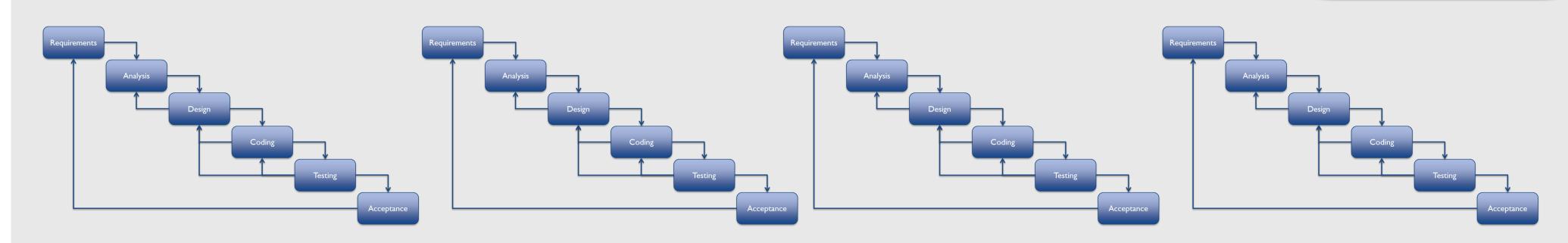
Analysis

Design

Coding

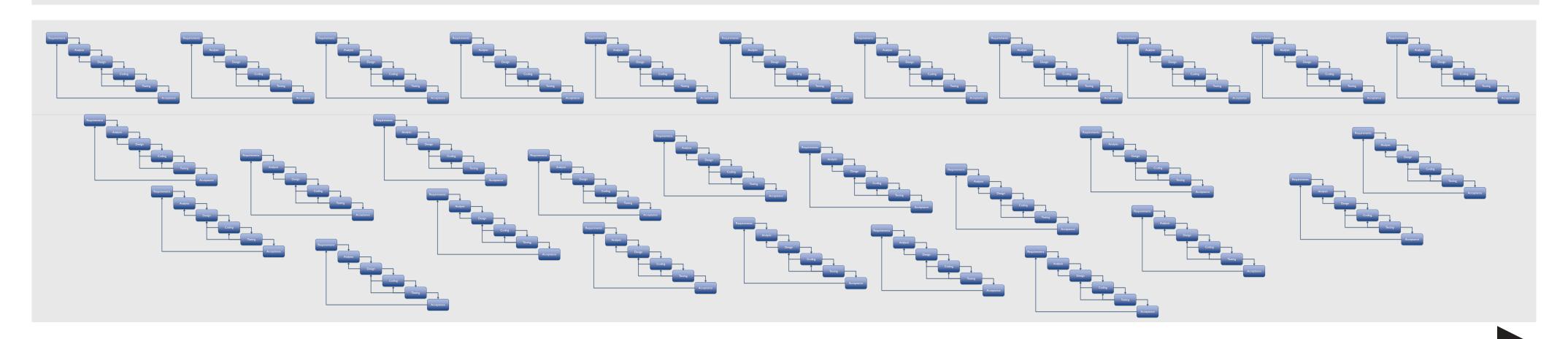
Testing

Agile

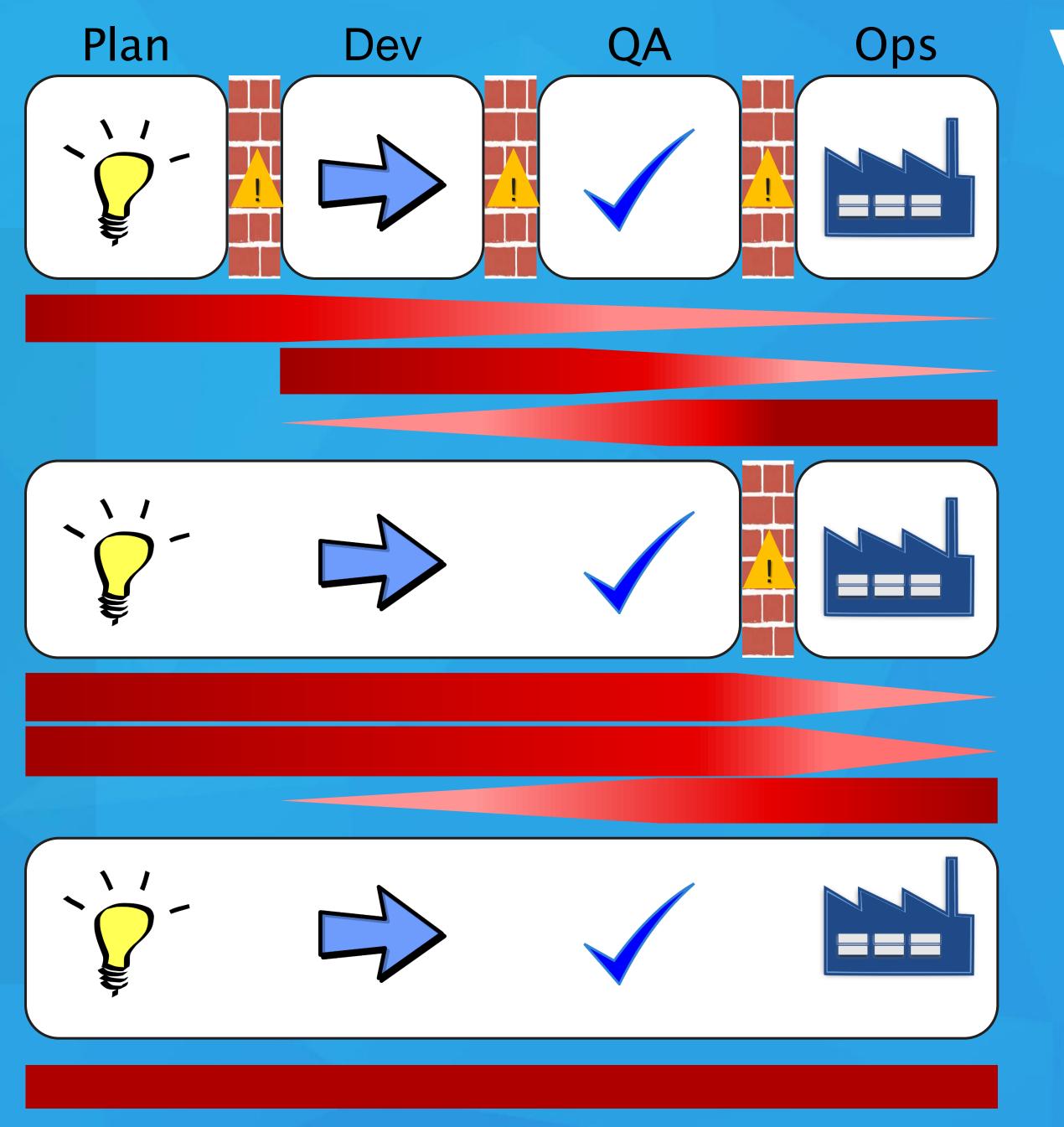


DevOps

At Scale



Time



VERACODE

= Handoff

Business Intent App Knowledge Ops Knowledge

Business Intent App Knowledge Ops Knowledge

Continuity

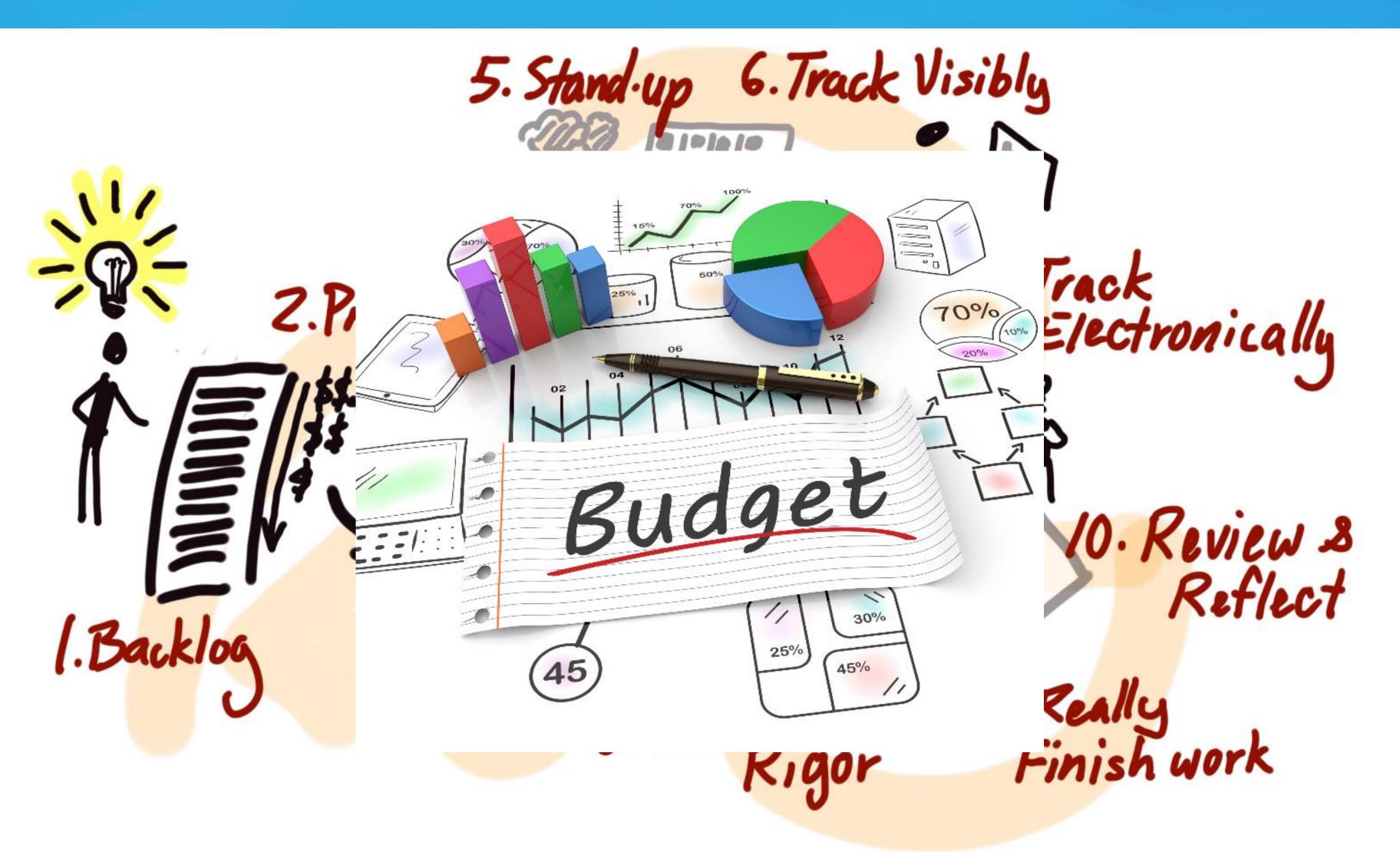
DevOps

Waterfall

Agile

Agile - Process

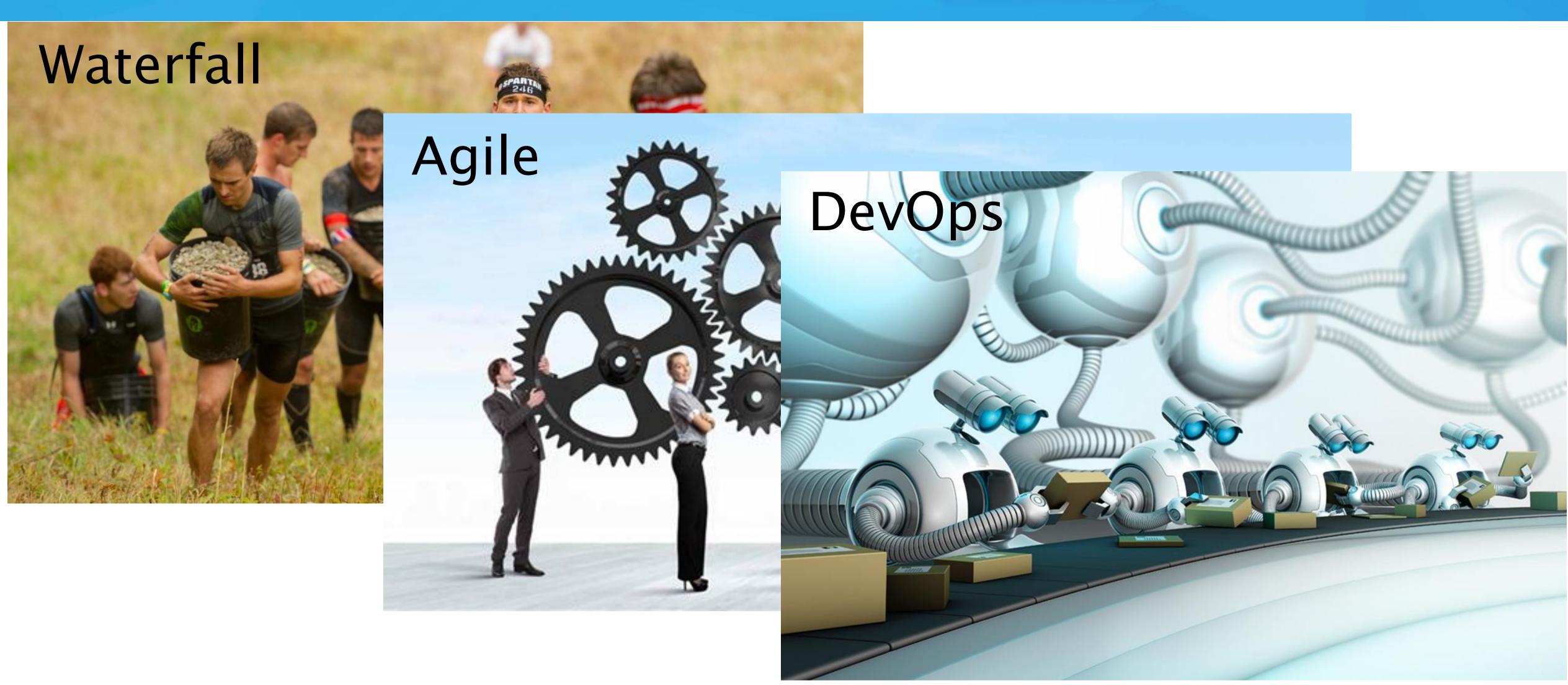






Transformation - Technology





Is this your current AppSec program?





They/We know it's coming...





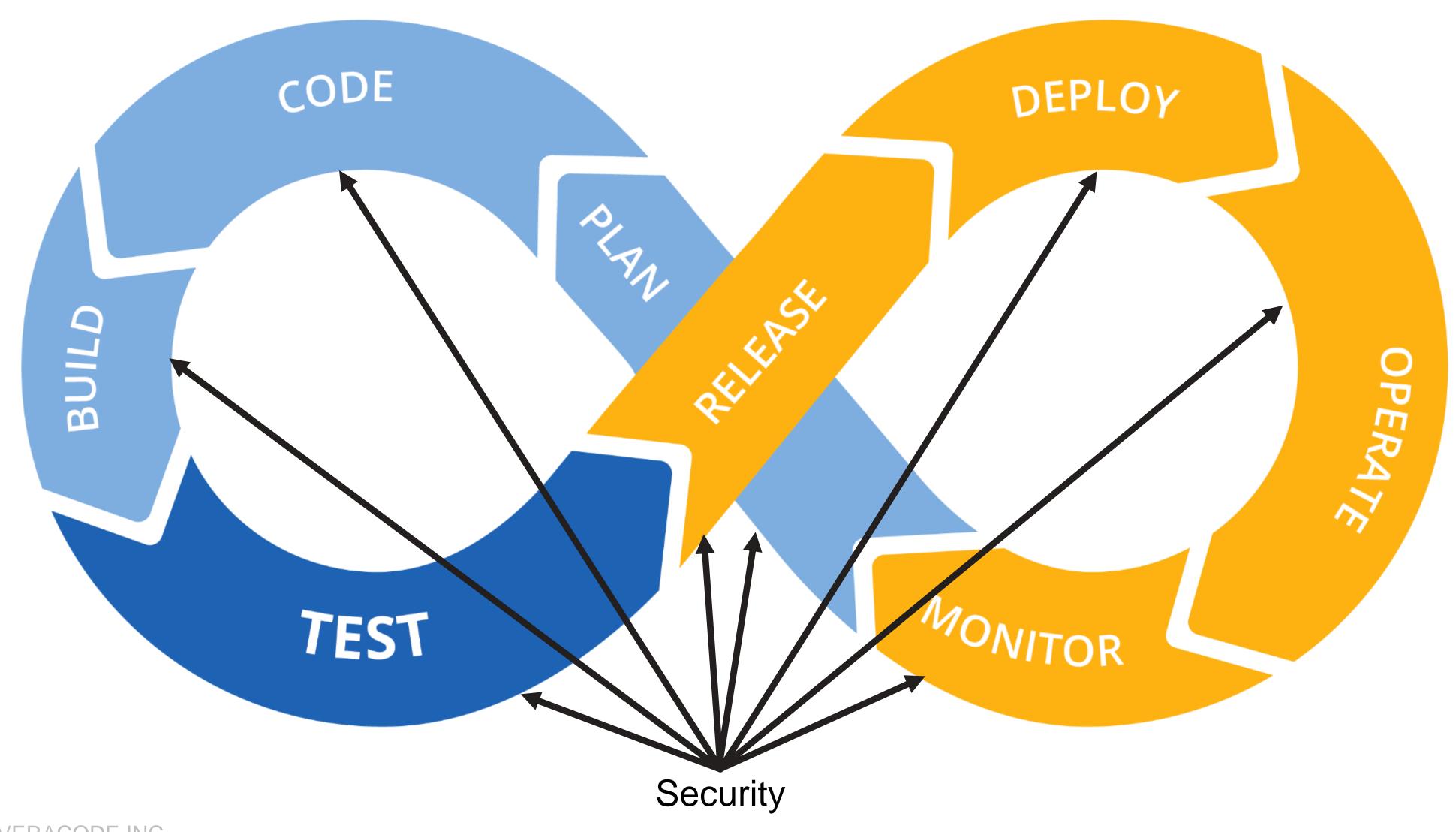
Which outcome do you see?





DevOps - Process: Where is security?





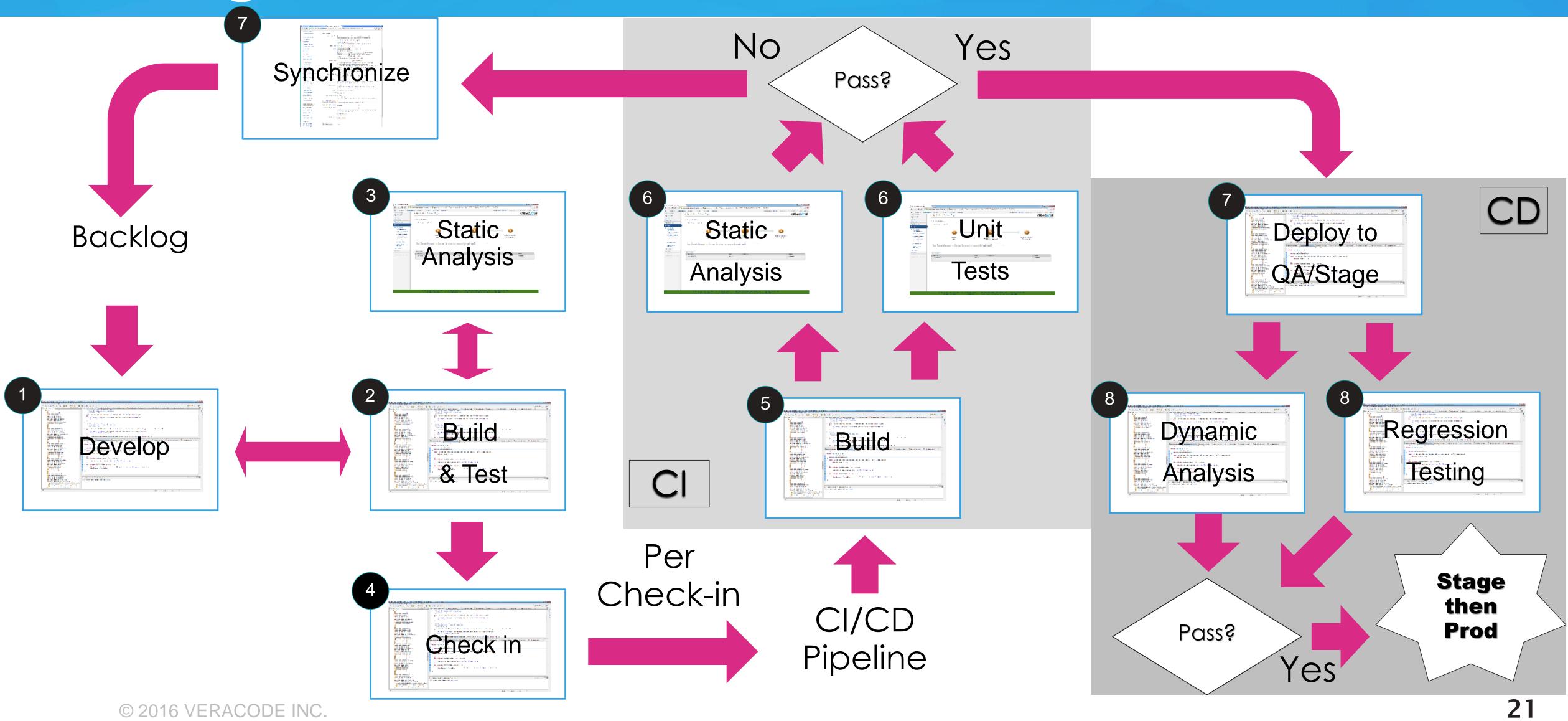
Strategy

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



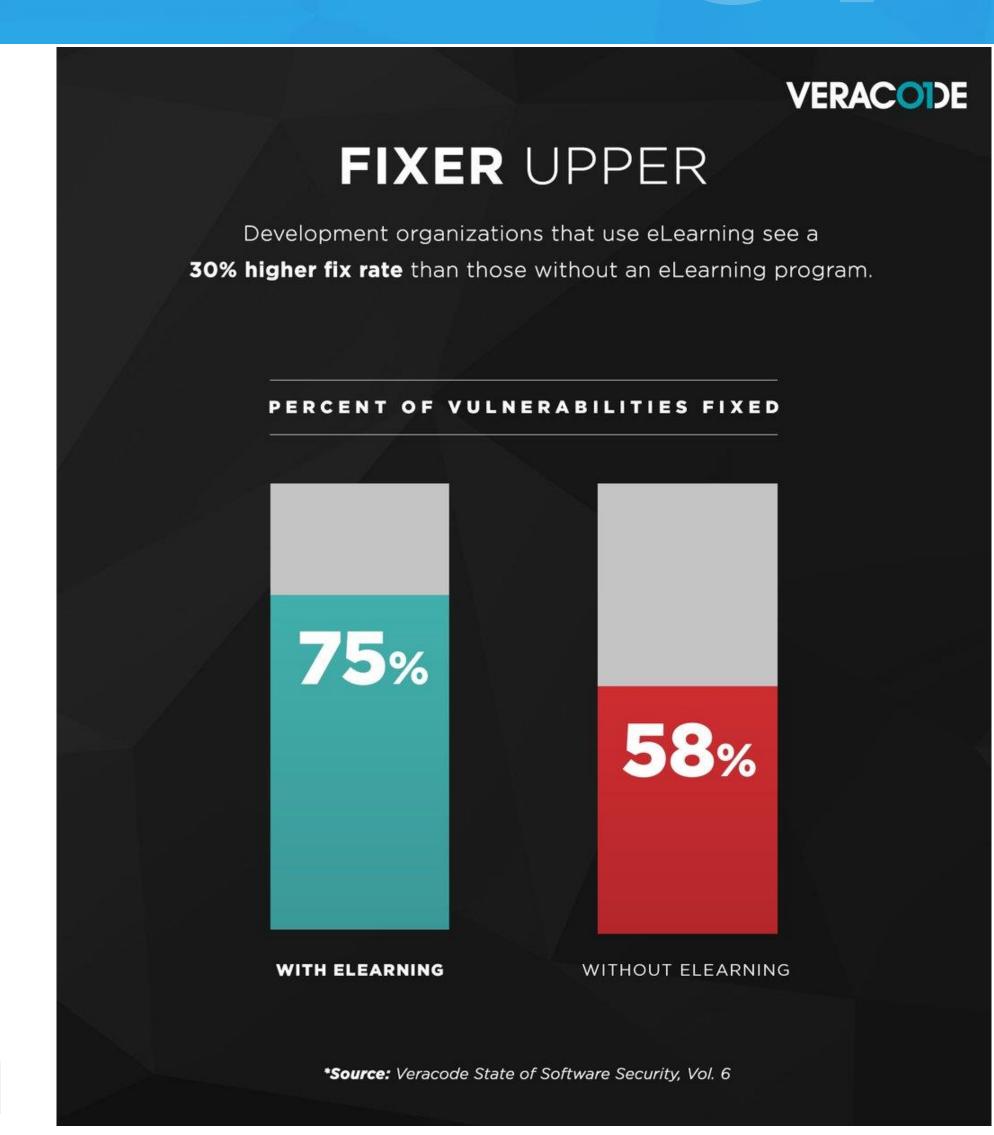
Strategy – Integration & Automation



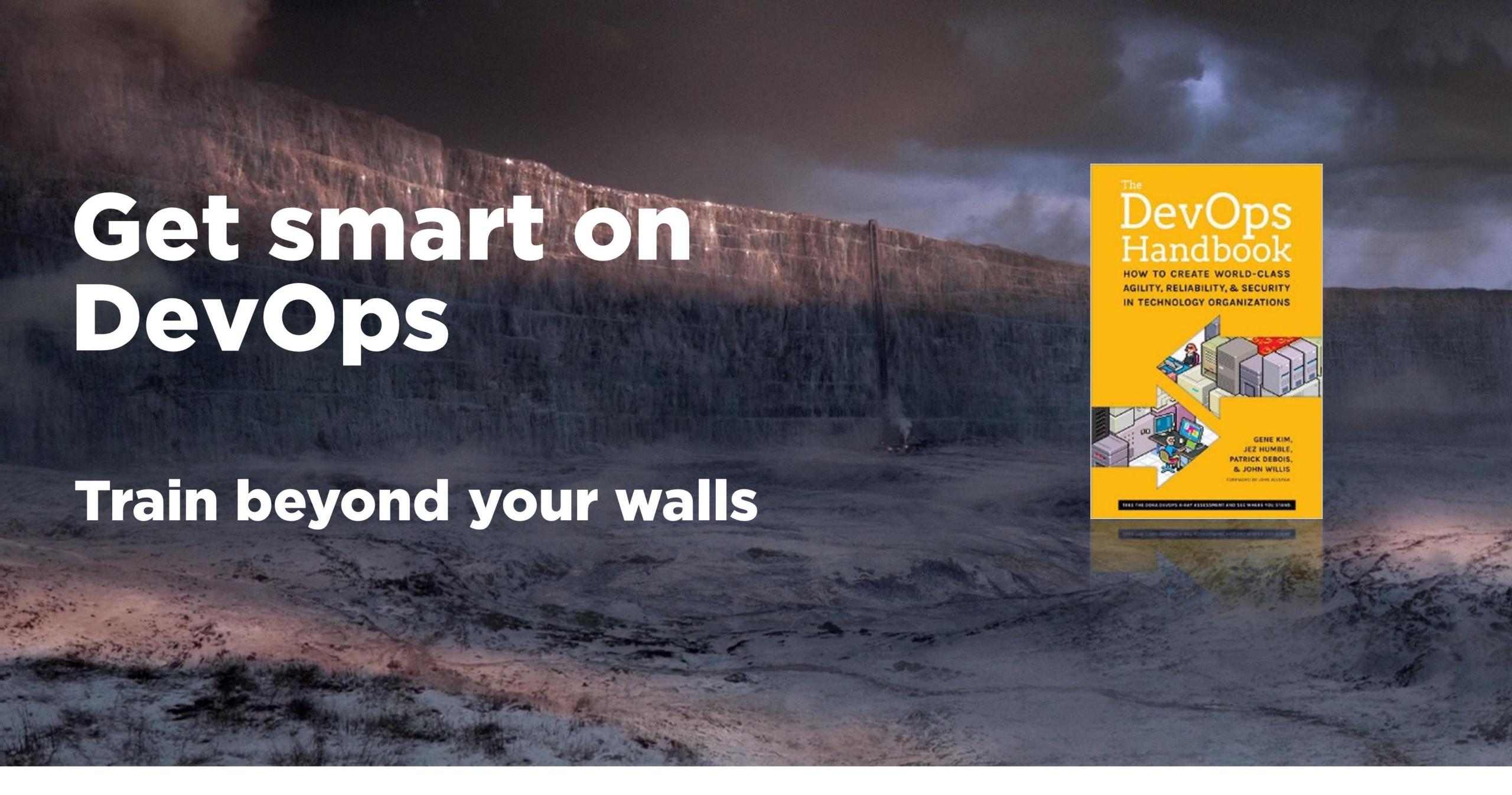


Strategy - Training

- 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



State of Software Security Report: Focus on Industry Verticals, Volume 6, Veracode



Strategy - Remediation Coaching



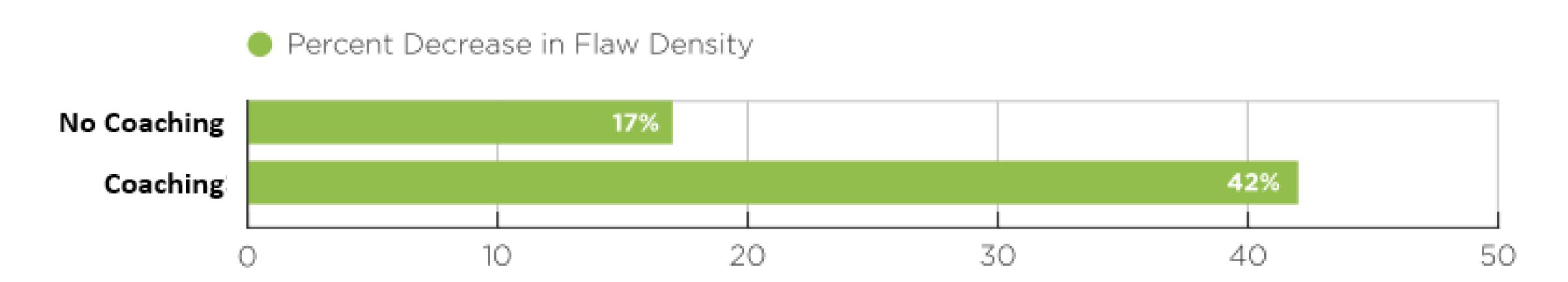
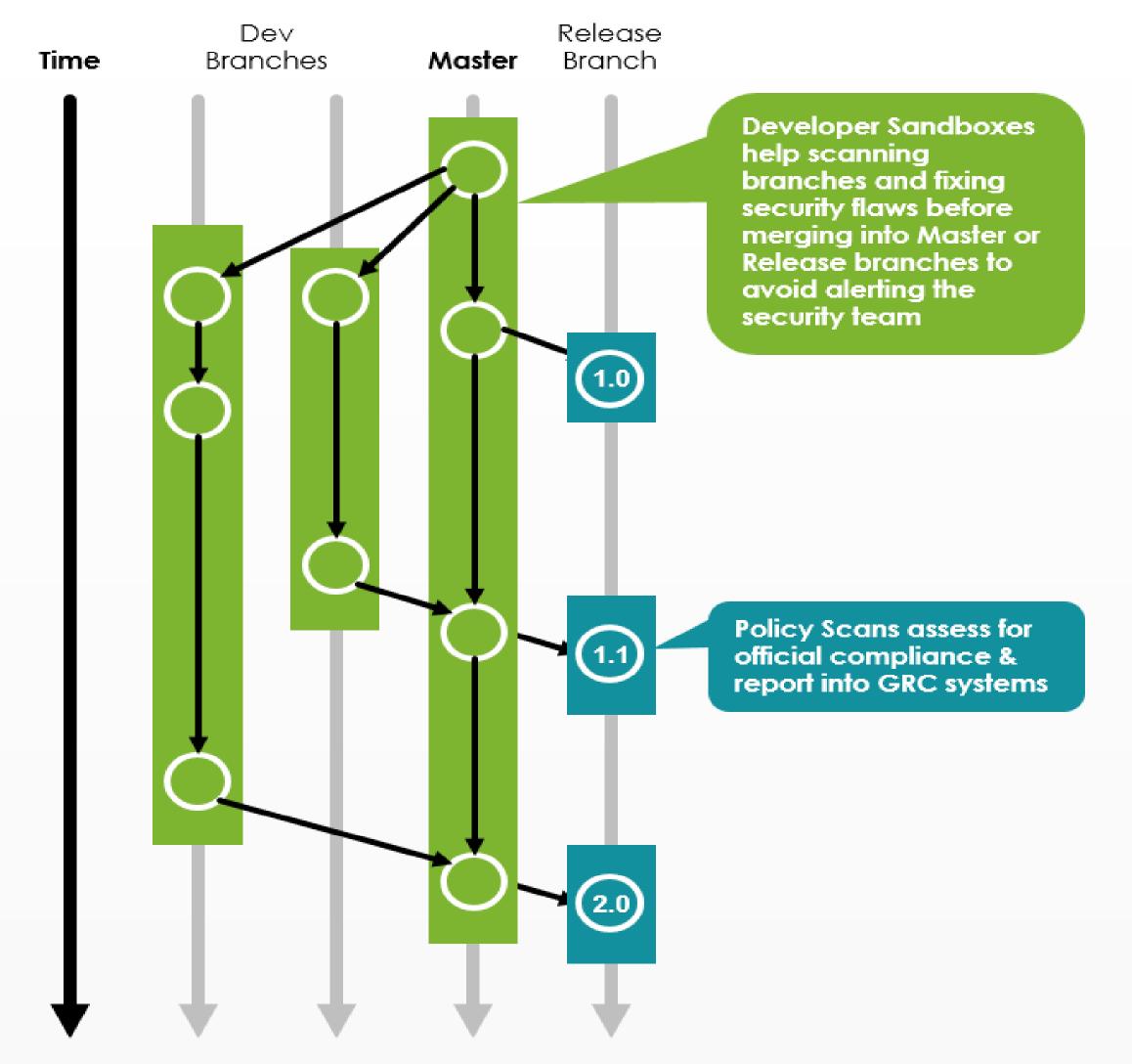


Figure 10: Relative Improvement in Flaw Density via Remediation Coaching (Readout)

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



Thank You!