RSAConference2022
San Francisco & Digital | June 6 – 9

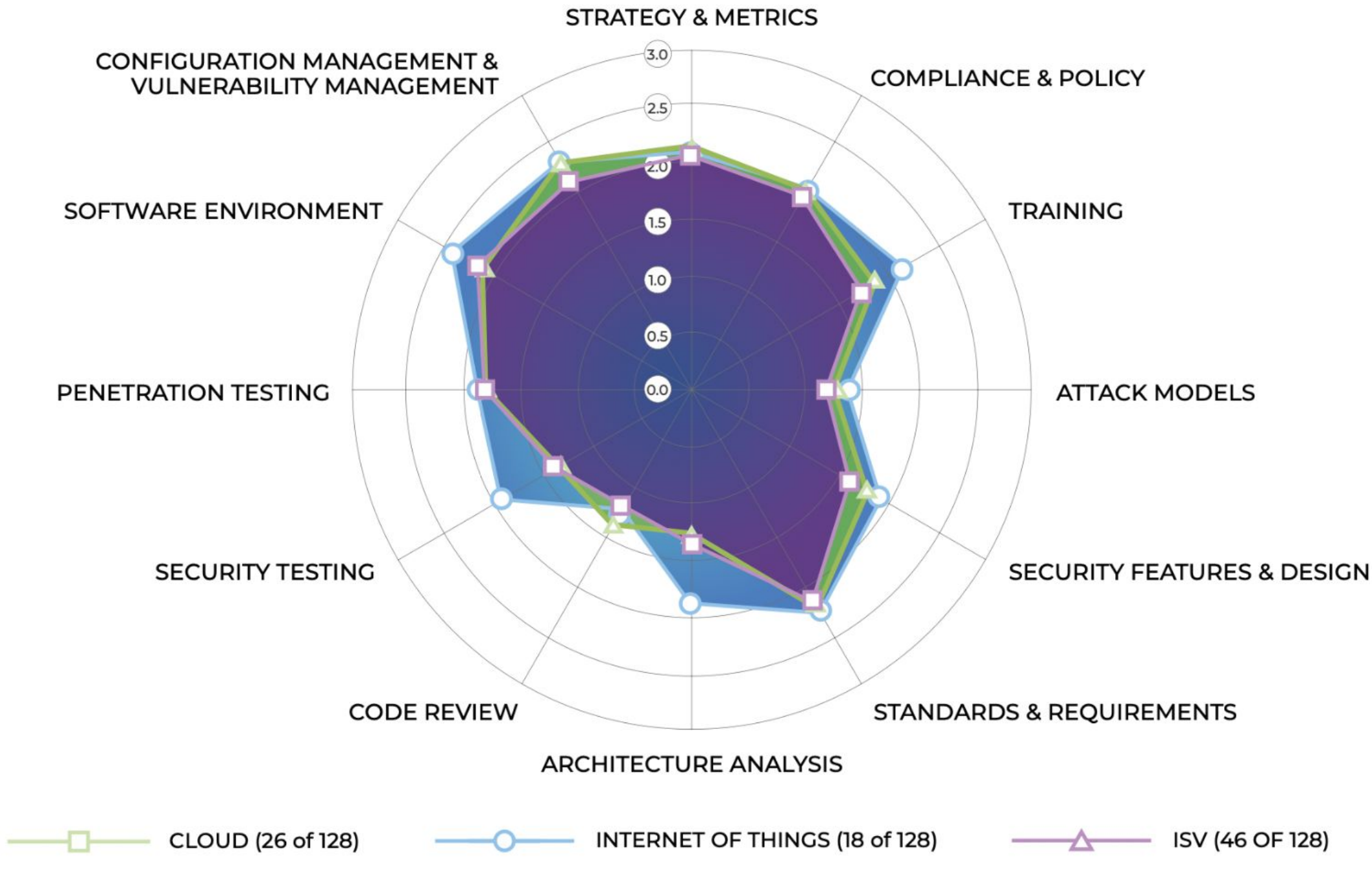
TRANSFORM

SESSION ID: **DSO-M01**

The Practicalities of Pentesting at Scale

Caroline Wong

Chief Strategy Officer at Cobalt


STRATEGY & METRICS
COMPLIANCE & POLICY
TRAINING
ATTACK MODELS
SECURITY FEATURES & DESIGN
STANDARDS & REQUIREMENTS
ARCHITECTURE ANALYSIS
CODE REVIEW
SECURITY TESTING
PENETRATION TESTING
SOFTWARE ENVIRONMENT
CONFIGURATION MANAGEMENT & VULNERABILITY MANAGEMENT
3.0
2.5
2.0
1.5
1.0
0.5
0.0
CLOUD (26 of 128)
INTERNET OF THINGS (18 of 128)
ISV (46 OF 128)

From Terrifying to …

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	32	33	34	35	36	37	38	39	40
41	42							49	50
51	52							59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2013 - 2016

From Terrifying to … Good Enough?

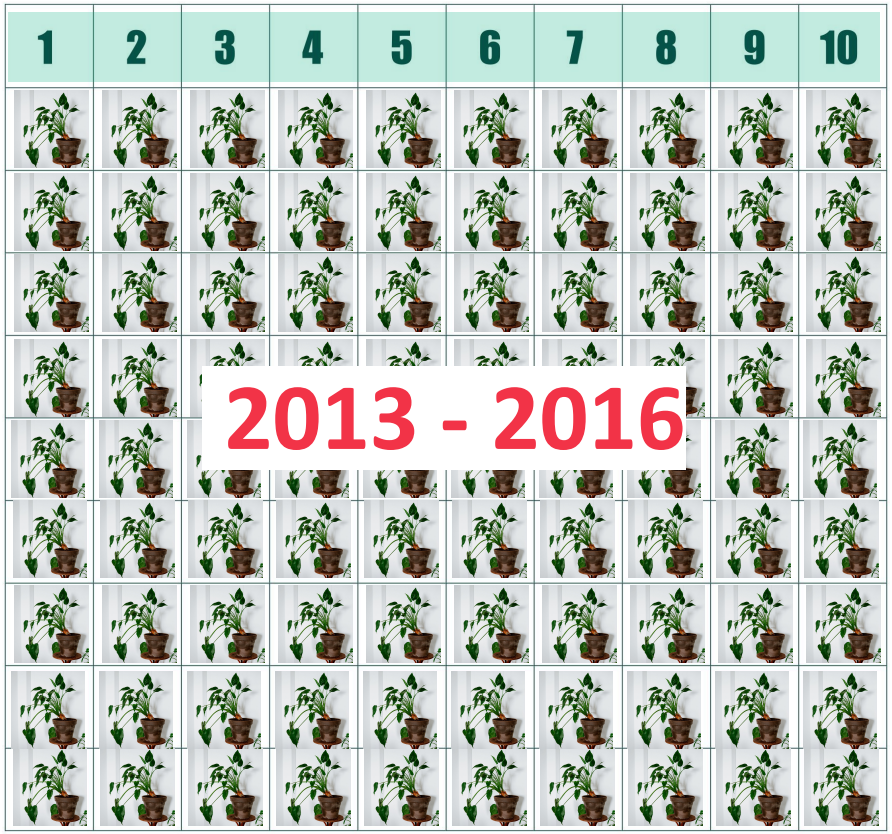
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42							49	50
51	52							59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

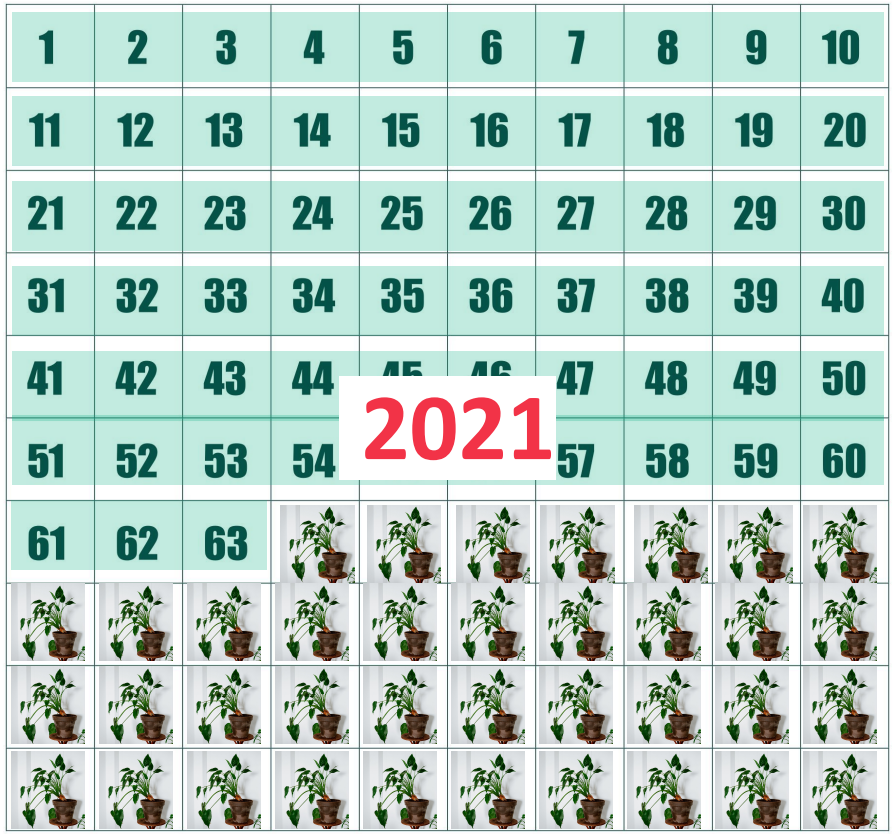
2013 - 2016

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	32	33	34	35	36	37	38	39	40
41	42	43	44			47	48	49	50
51	52	53	54			57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2021

House Plants





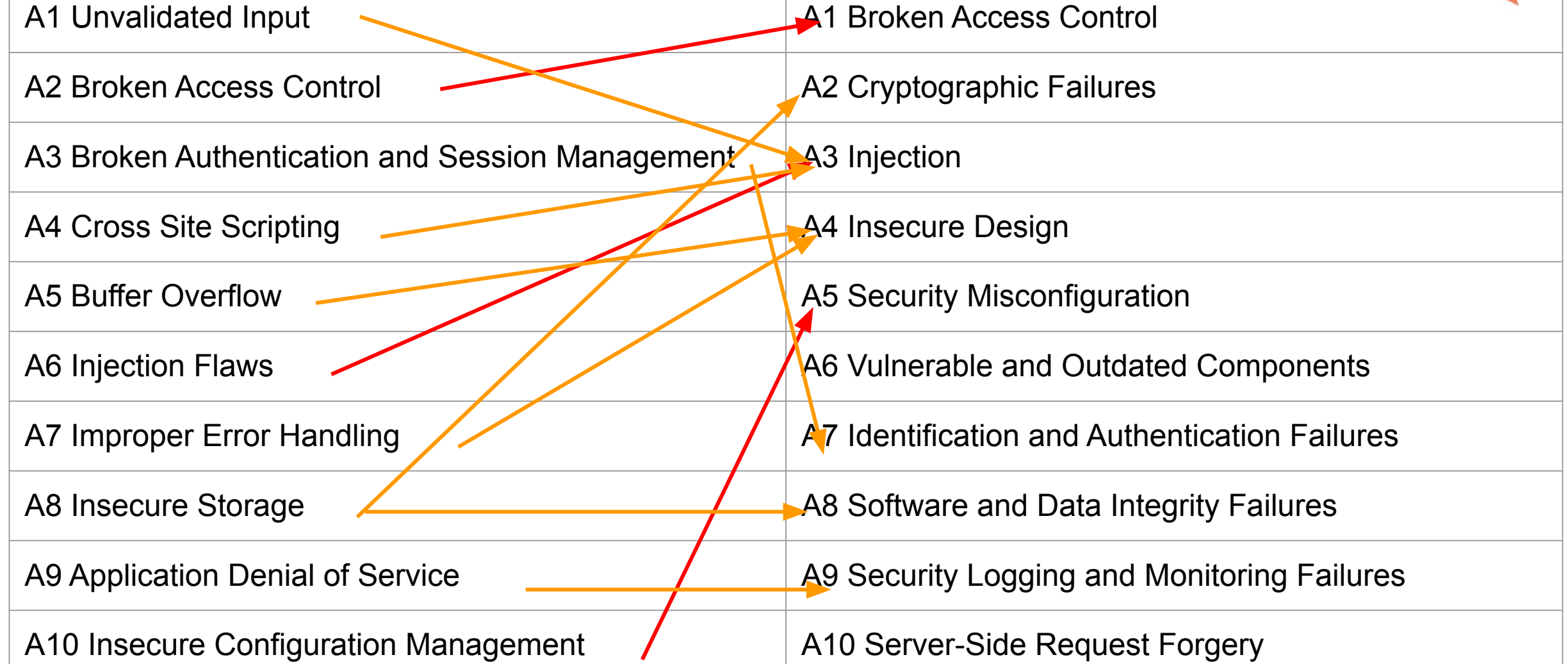
Cats


1 2 3 4 5 6 7 8 9 10
2013 - 2016


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 32 33 34 35 36 37 38 39 40
41 42 43 44 47 48 49 50
51 52 53 54 57 58 59 60
61 62 63
2021

OWASP Top 10: 2003 vs. 2021

A1 Unvalidated Input	A1 Broken Access Control
A2 Broken Access Control	A2 Cryptographic Failures
A3 Broken Authentication and Session Management	A3 Injection
A4 Cross Site Scripting	A4 Insecure Design
A5 Buffer Overflow	A5 Security Misconfiguration
A6 Injection Flaws	A6 Vulnerable and Outdated Components
A7 Improper Error Handling	A7 Identification and Authentication Failures
A8 Insecure Storage	A8 Software and Data Integrity Failures
A9 Application Denial of Service	A9 Security Logging and Monitoring Failures
A10 Insecure Configuration Management	A10 Server-Side Request Forgery



Matthew McConaughey in 2003

Matthew McConaughey in 2021

Let’s discuss.

- A history lesson: cybersecurity and software development
- A maturity model for pentesting
- *2022 State of Pentesting* research findings
- How to scale pentesting

But… why?

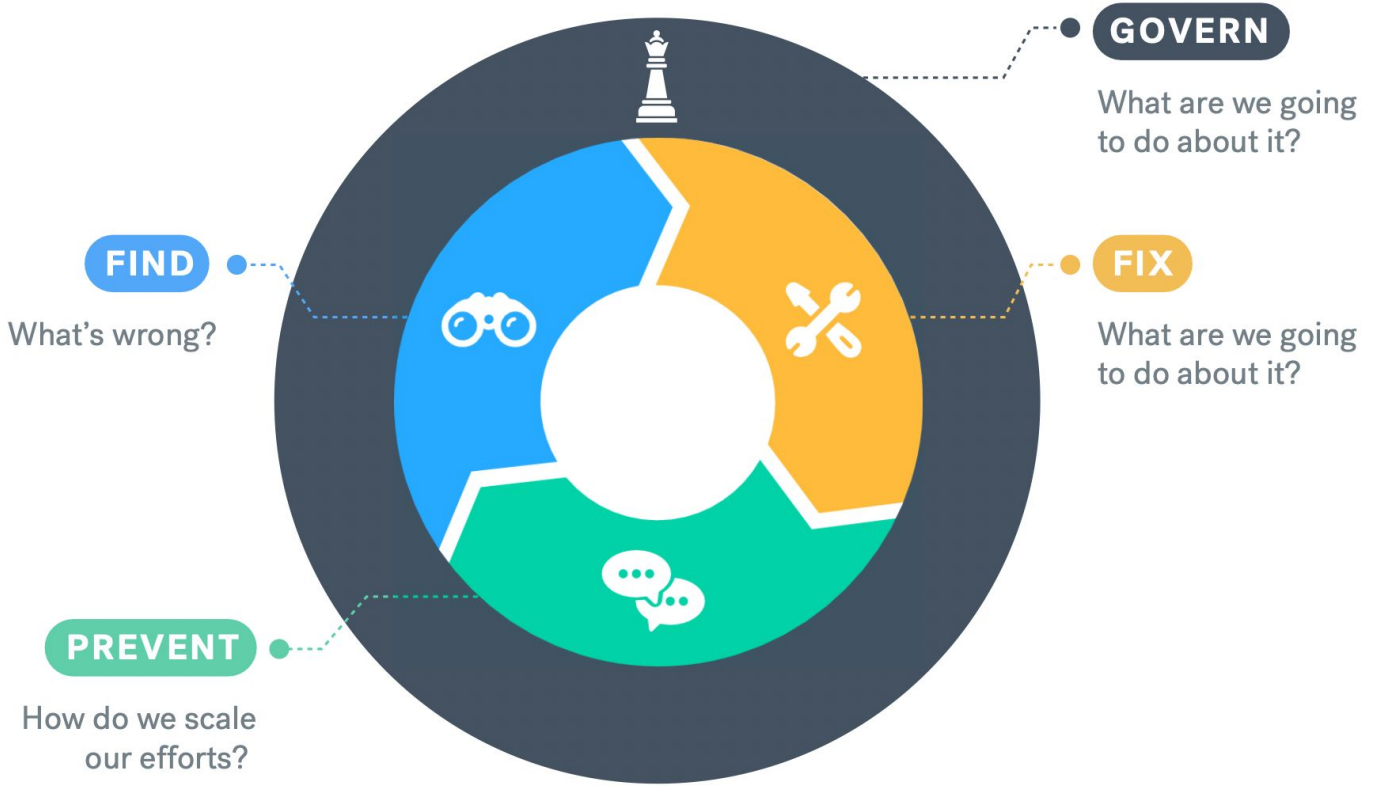

1 2 3 4 5 6 7 8 9 10
2013 - 2016


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 32 33 34 35 36 37 38 39 40
41 42 43 44 47 48 49 50
51 52 53 54 57 58 59 60
61 62 63
2021

Doing Controls vs. Managing Risk

Table of Contents

The Modern AppSec Framework



Cobalt

RSAConference2022

Risk Management Objectives: Externally Driven

1. Use cybersecurity as a competitive differentiator.
2. Comply with a regulatory requirement, contractual obligation, or industry standard.
3. Achieve a defensible level of “due care.”
4. Achieve a comparable level of cybersecurity to peers and/or competition.

Risk Management Objectives: Internally Driven

1. Prevent the same cybersecurity problems from happening over and over again.
2. Reduce the probability that malicious attackers can stop critical systems and applications from functioning.
3. Require fixes for security bugs for which well known attacks exist.

“Prioritizing compliance or features over a comprehensive process that increases resistance to attack (and also gives us compliance and better security features) is not the risk management we need.”

- Sammy Migues

Cobalt

Cybersecurity: a decade in review

Cobalt

Cybersecurity:
2 decades in review

Cobalt

PowerPost • Analysis

The Cybersecurity 202: These hackers warned Congress the internet was not secure. 20 years later, their message is the same.

By Derek Hawkins
Reporter

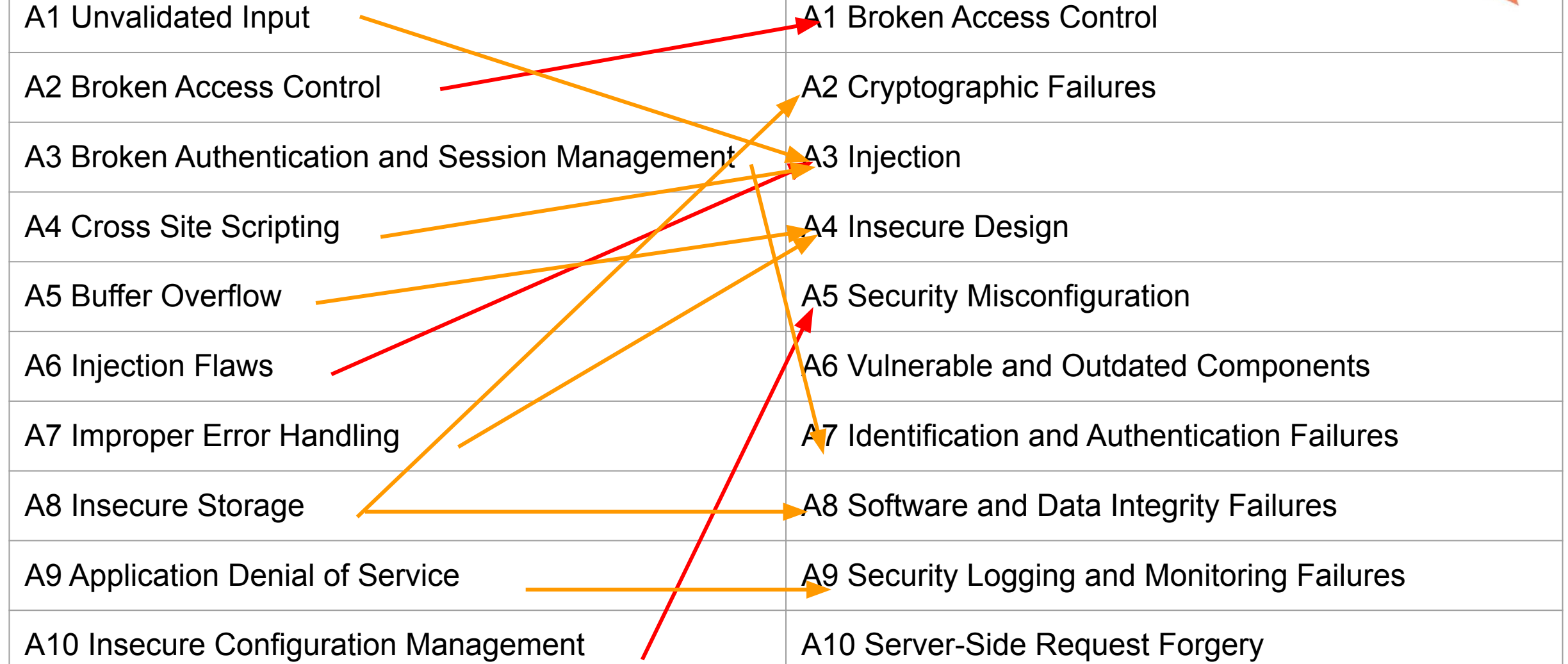
May 23, 2018

with Bastien Inzaurralde

THE KEY

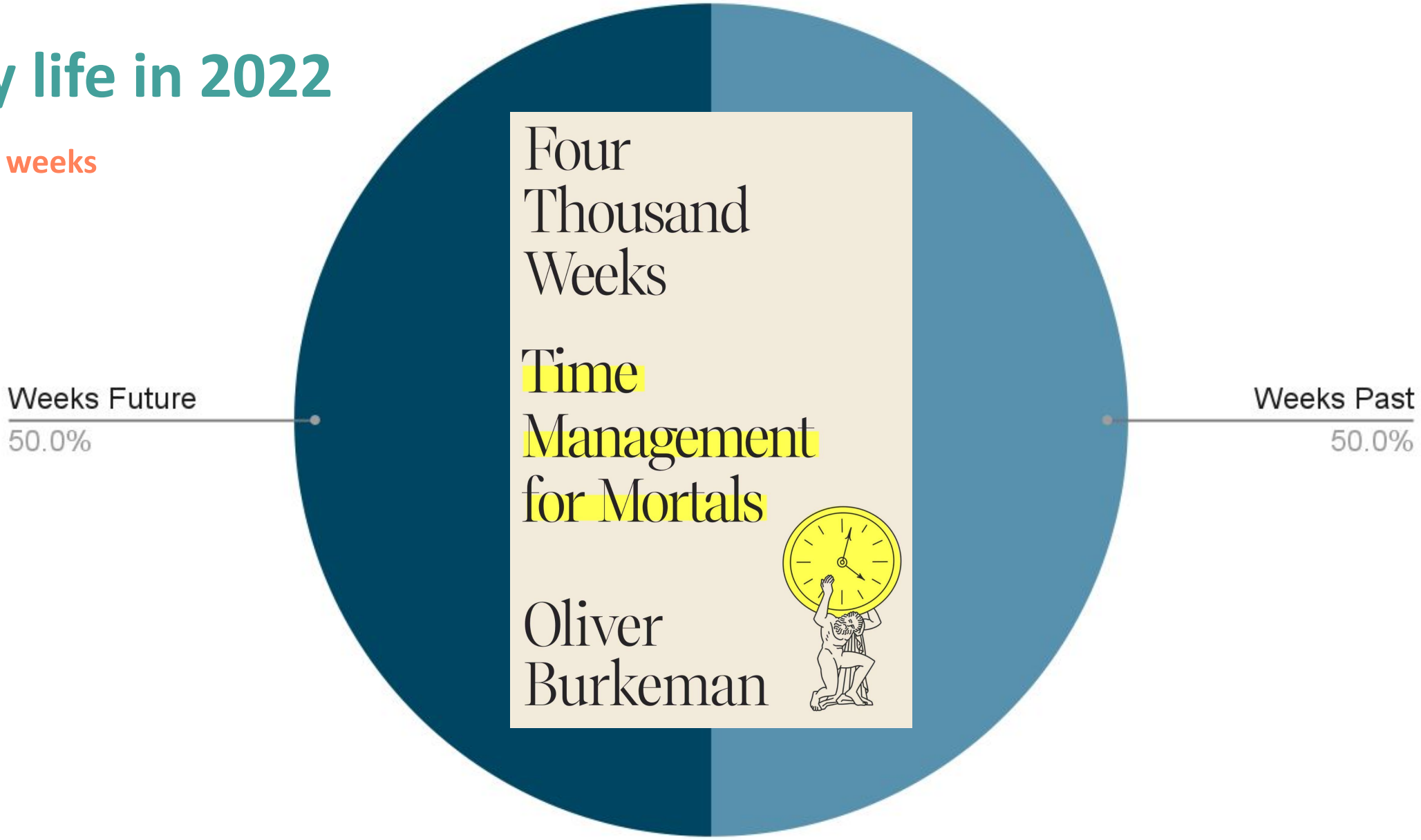
OWASP Top 10: 2003 vs. 2021

A1 Unvalidated Input	A1 Broken Access Control
A2 Broken Access Control	A2 Cryptographic Failures
A3 Broken Authentication and Session Management	A3 Injection
A4 Cross Site Scripting	A4 Insecure Design
A5 Buffer Overflow	A5 Security Misconfiguration
A6 Injection Flaws	A6 Vulnerable and Outdated Components
A7 Improper Error Handling	A7 Identification and Authentication Failures
A8 Insecure Storage	A8 Software and Data Integrity Failures
A9 Application Denial of Service	A9 Security Logging and Monitoring Failures
A10 Insecure Configuration Management	A10 Server-Side Request Forgery



My life in 2022

2000 weeks



Software development: a decade in review

Cobalt

The case for DevOps remains clear

Highly evolved organizations have consistently demonstrated higher performance across four key software performance metrics.

	Low	Mid	High
Deployment frequency	Monthly or less often	Between daily and weekly	On demand (whenever we want)
Lead time for changes	Between a week and 6 months	Less than a week	Less than an hour
MTTR	Less than a week	Less than a day	Less than an hour
Change failure rate	Less than 15%	Less than 15%	Less than 5%

LILY HAY NEWMAN SECURITY 12.08.2021 06:23 PM

A Year After the SolarWinds Hack, Supply Chain Threats Still Loom

The Russia-led campaign was a wake-up call to the industry, but there's no one solution to the threat.

Security Practice

Test for security	58%
Integrate security reviews into every phase	54%
Security reviews	60%
Build pre-approved code	49%
Invite InfoSec early and often	63%

Then and Now: SaaS Benefits

On Prem		Cloud
High	Cost	Low
Low	Flexibility	High
No	On-demand	Yes
Little	Redundancy	A lot
Few	Workloads	Many

Then and Now: Pentesting → PtaaS

Pentesting		PtaaS
High	Cost	Low
Low	Flexibility	High
No	On-demand	Yes
Little	Redundancy	A lot
Few	Workloads	Many

Pentesting Maturity Model

	Ad-hoc	Structured	Strategic
Planning	Delays Last-minute	We have a plan	Our plan is great
Collaboration	Owners unknown	We found some friends	We work together
Information Sharing	Scattered Silos	We have data	Data is where it needs to be

Pentesting Maturity Model

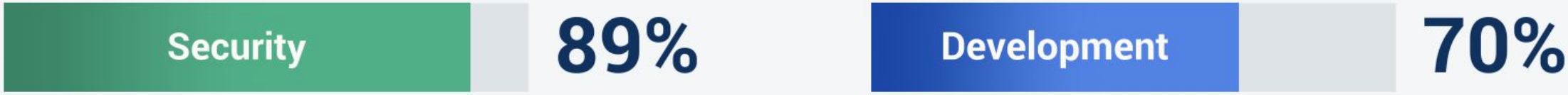
	Ad-hoc	Structured	Strategic
Planning	Delays Last-minute	We have a plan	Our plan is great
Collaboration	Owners unknown	We found some friends	We work together
Information Sharing	Scattered Silos	We have data	Data is where it needs to be

2022 State of Pentesting: research findings

Cobalt

How we used to think about cybersecurity

How it really is



Percentage of respondents struggling to collaborate

of security teams see a slower response to patching critical vulnerabilities

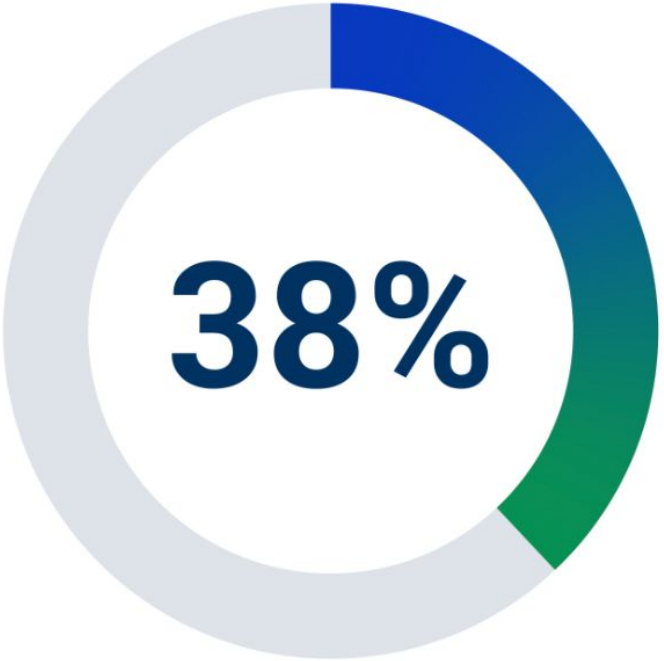
of developers struggle to meet critical launch deadlines

of developers said collaboration challenges with the security team compromise the quality of their code

Top 5 Vulnerability Categories

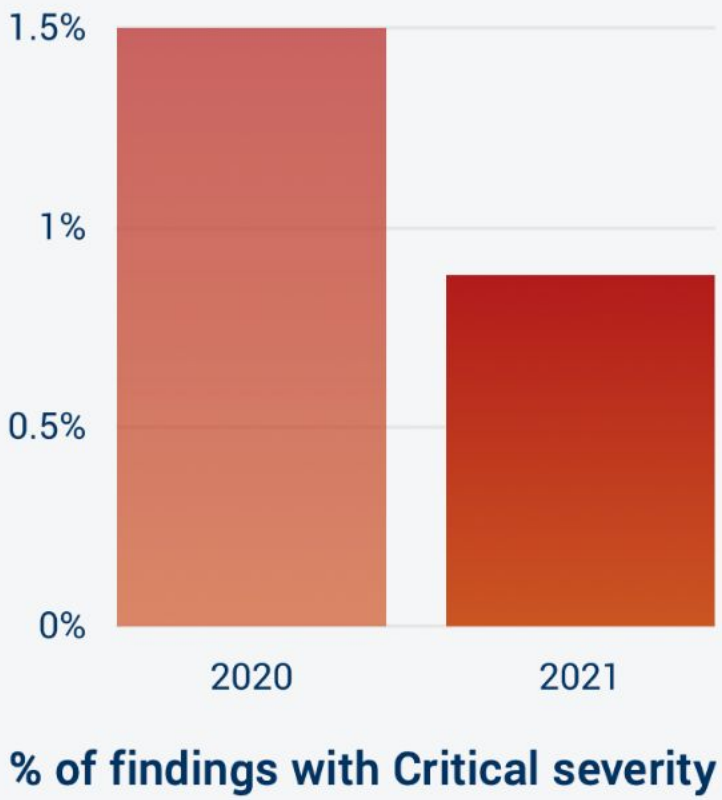
Following the same hierarchy, we started our analysis with the 5 most frequently discovered vulnerability categories in 2021:

1. Server Security Misconfigurations: 38%
2. Cross-Site Scripting (XSS): 13%
3. Broken Access Control: 11%
4. Sensitive Data Exposure: 10%
5. Authentication and Sessions: 8%

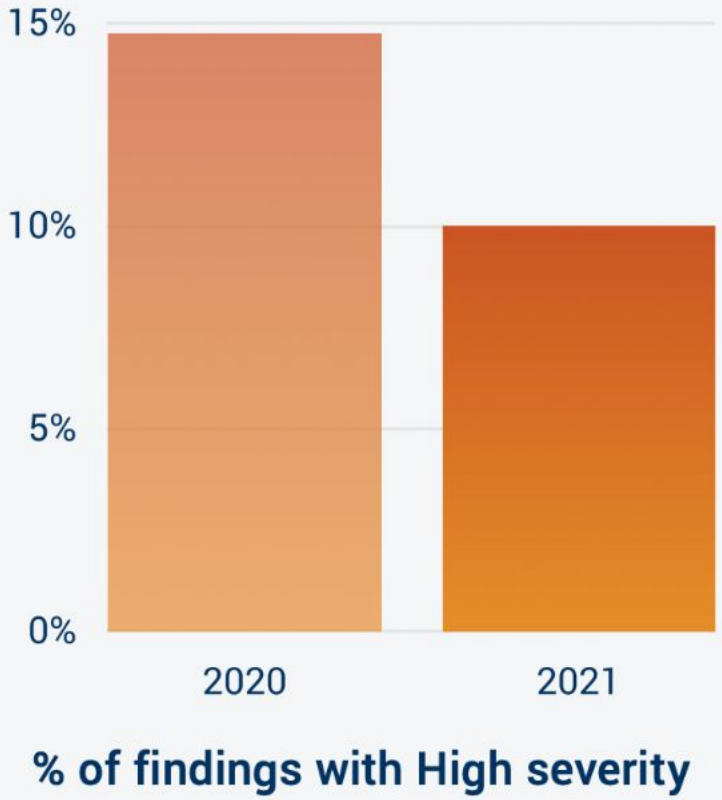


of our 2021 findings are connected to Server Security Misconfigurations

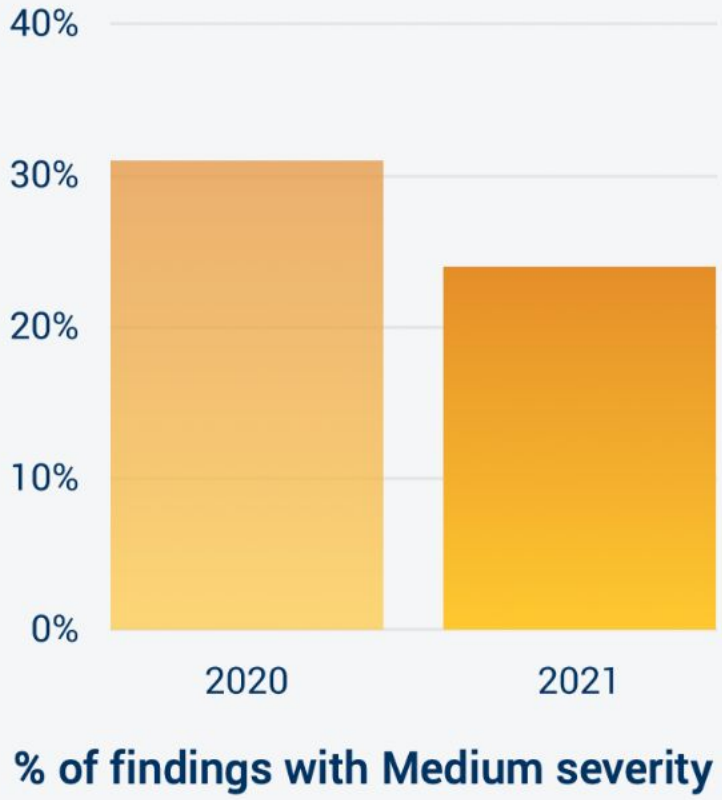
Findings with Critical, High, Medium Severity



% of findings with Critical severity

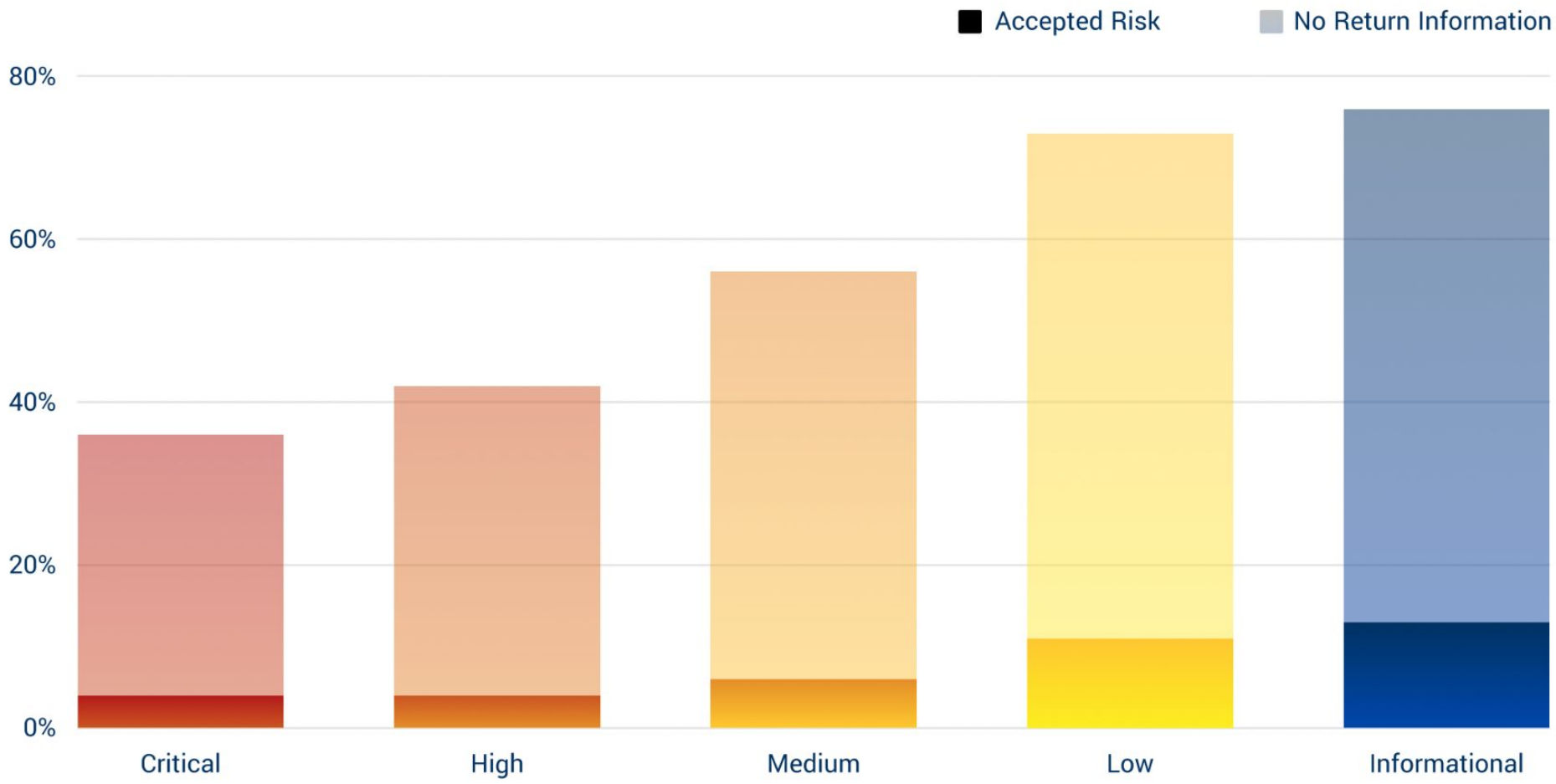


% of findings with High severity

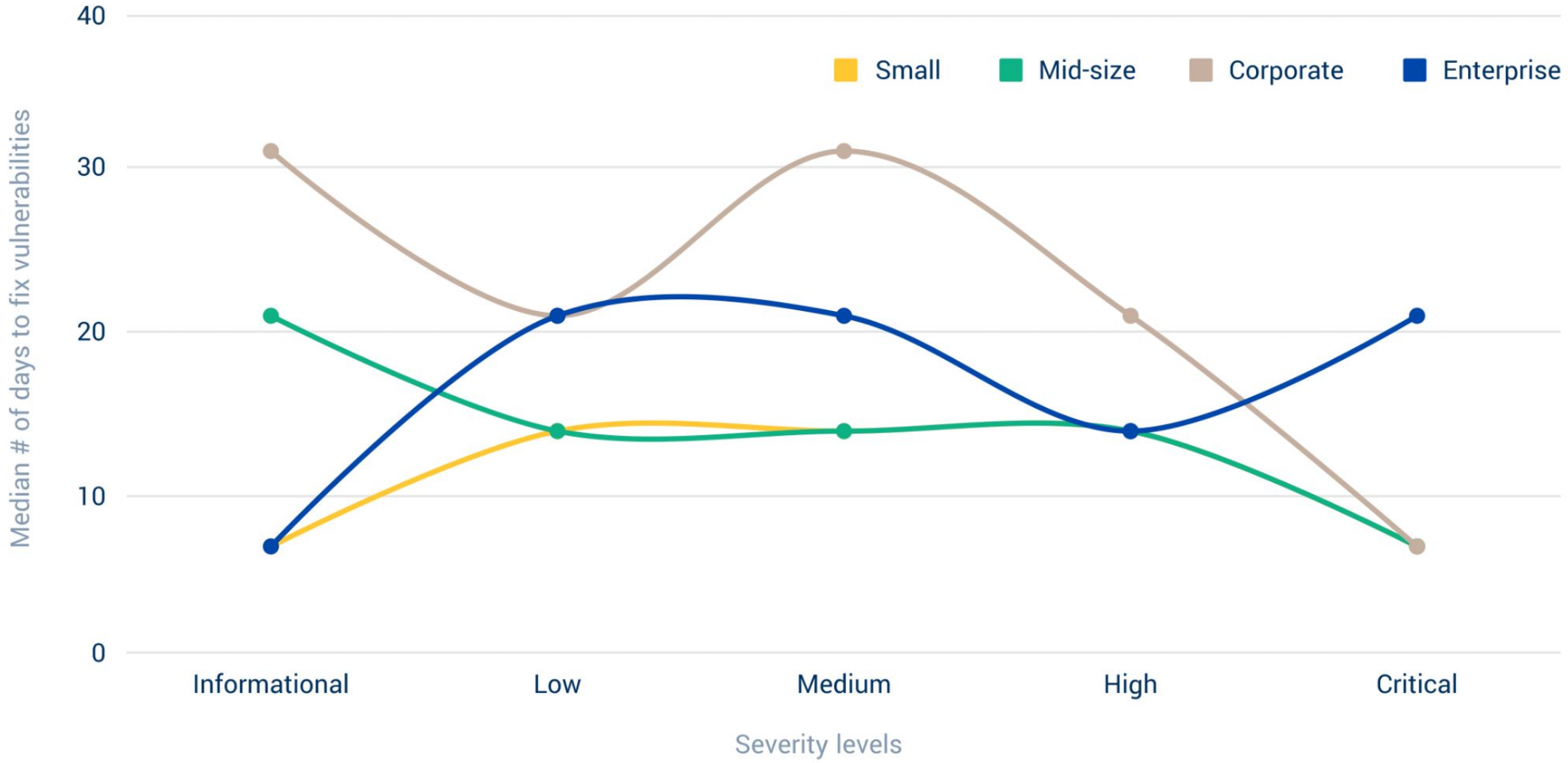


% of findings with Medium severity

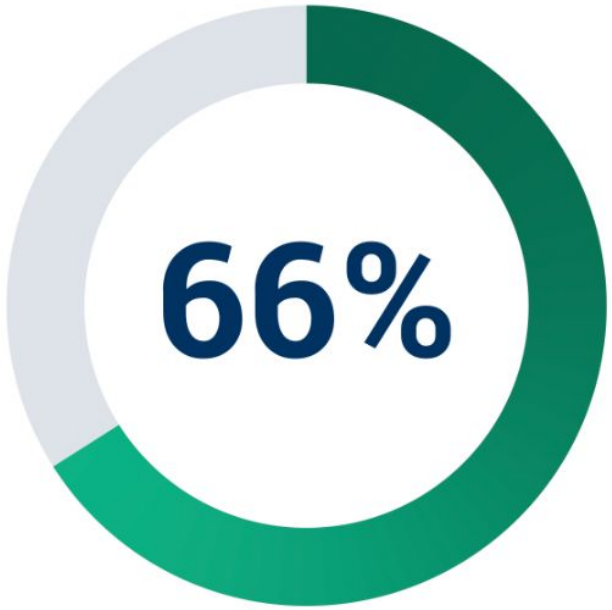
Findings marked “Accepted Risk” or “No Info”



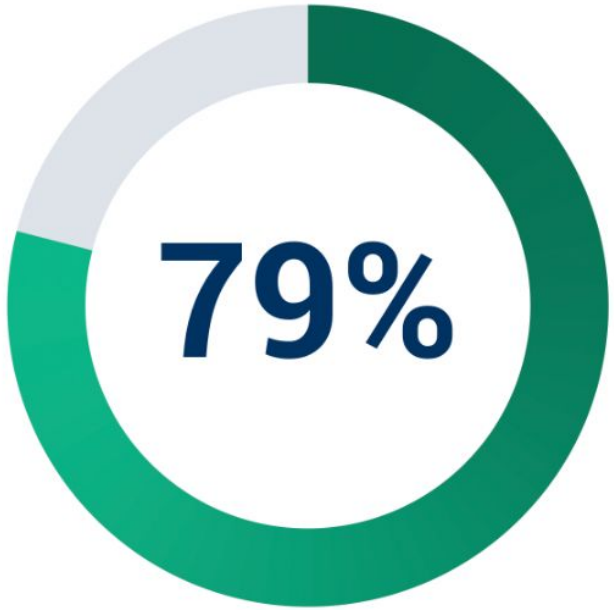
Number of Days to Fix Findings



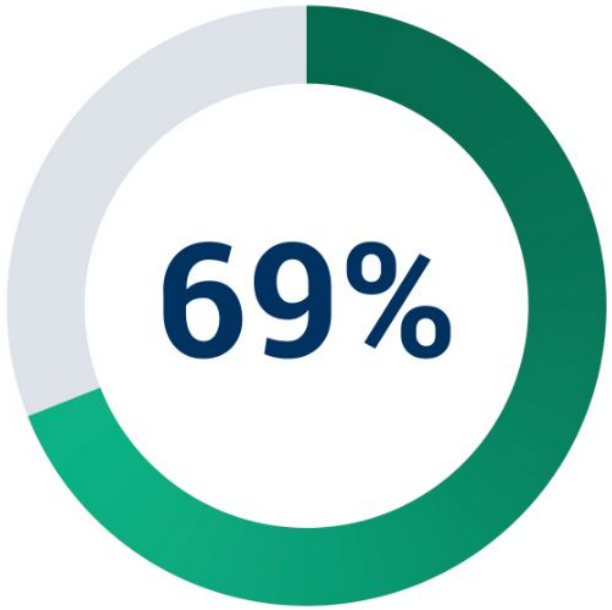
We still have a talent shortage



struggle to maintain high quality security standards

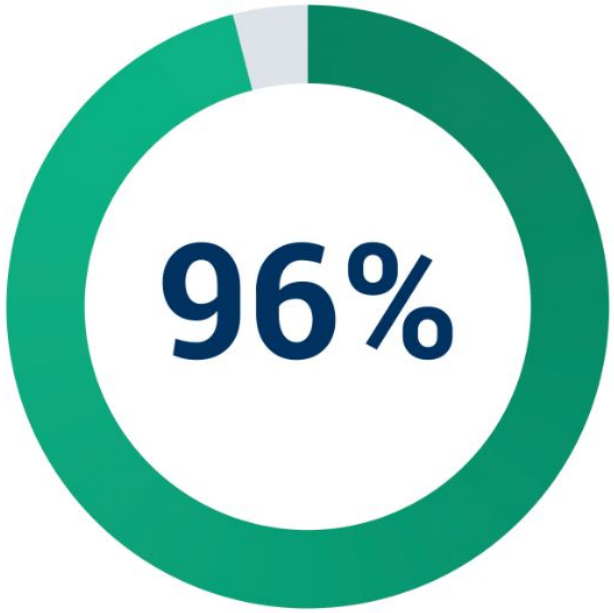


struggle to consistently monitor for vulnerabilities

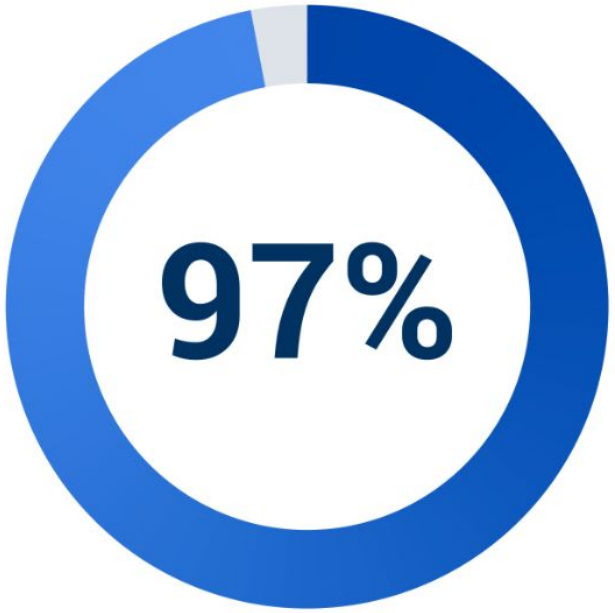


struggle to monitor for and respond to security incidents

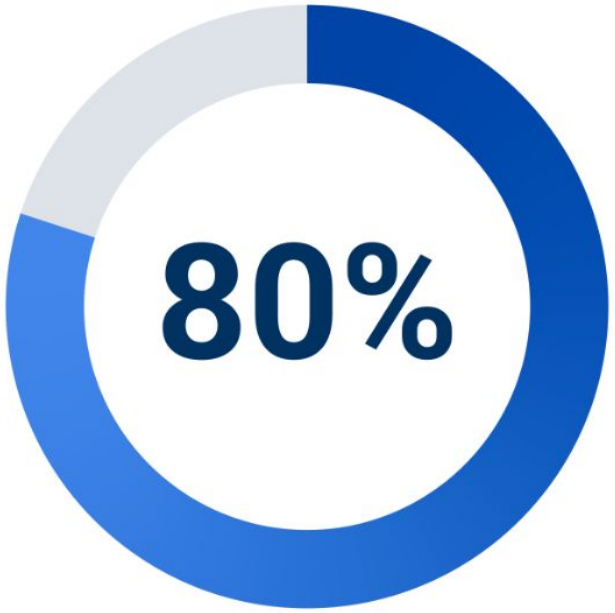
The talent shortage affects collaboration



of security respondents struggling to collaborate see a slower response to patching critical vulnerabilities



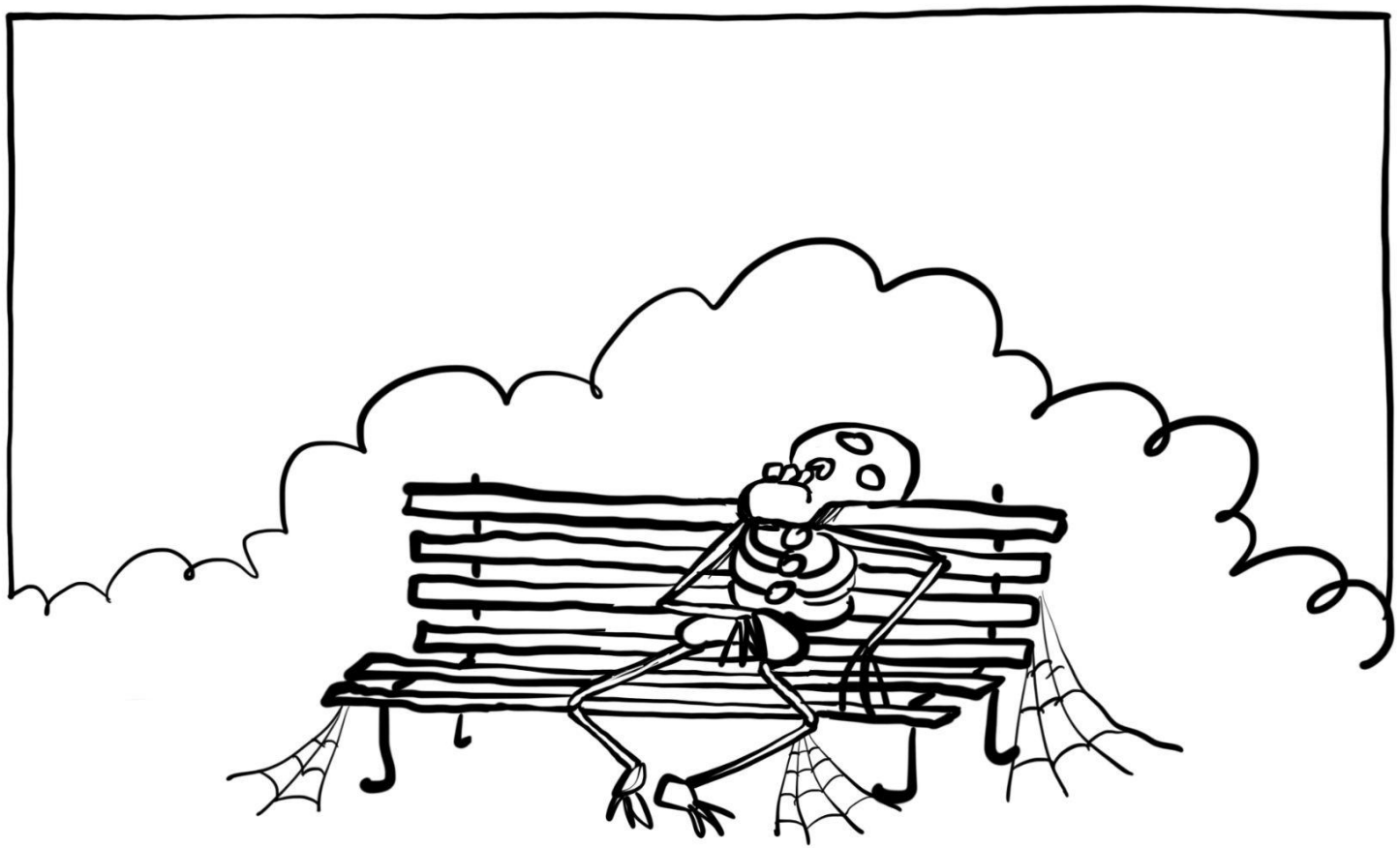
of developers said collaboration challenges make it harder to meet critical launch deadlines

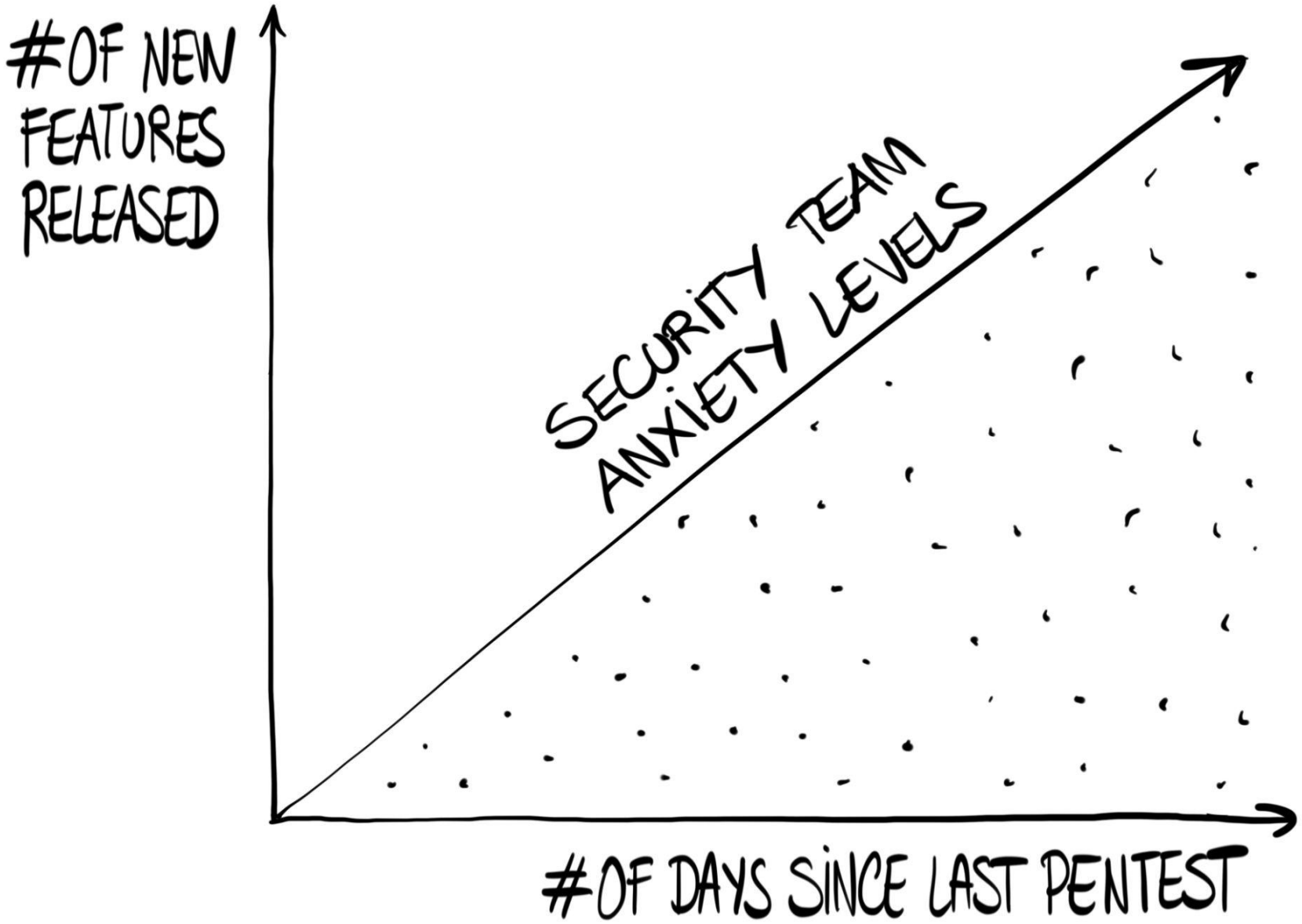


of developers agreed collaboration challenges compromise the quality and security of their code

How to scale pentesting: do it faster and more often

Cobalt

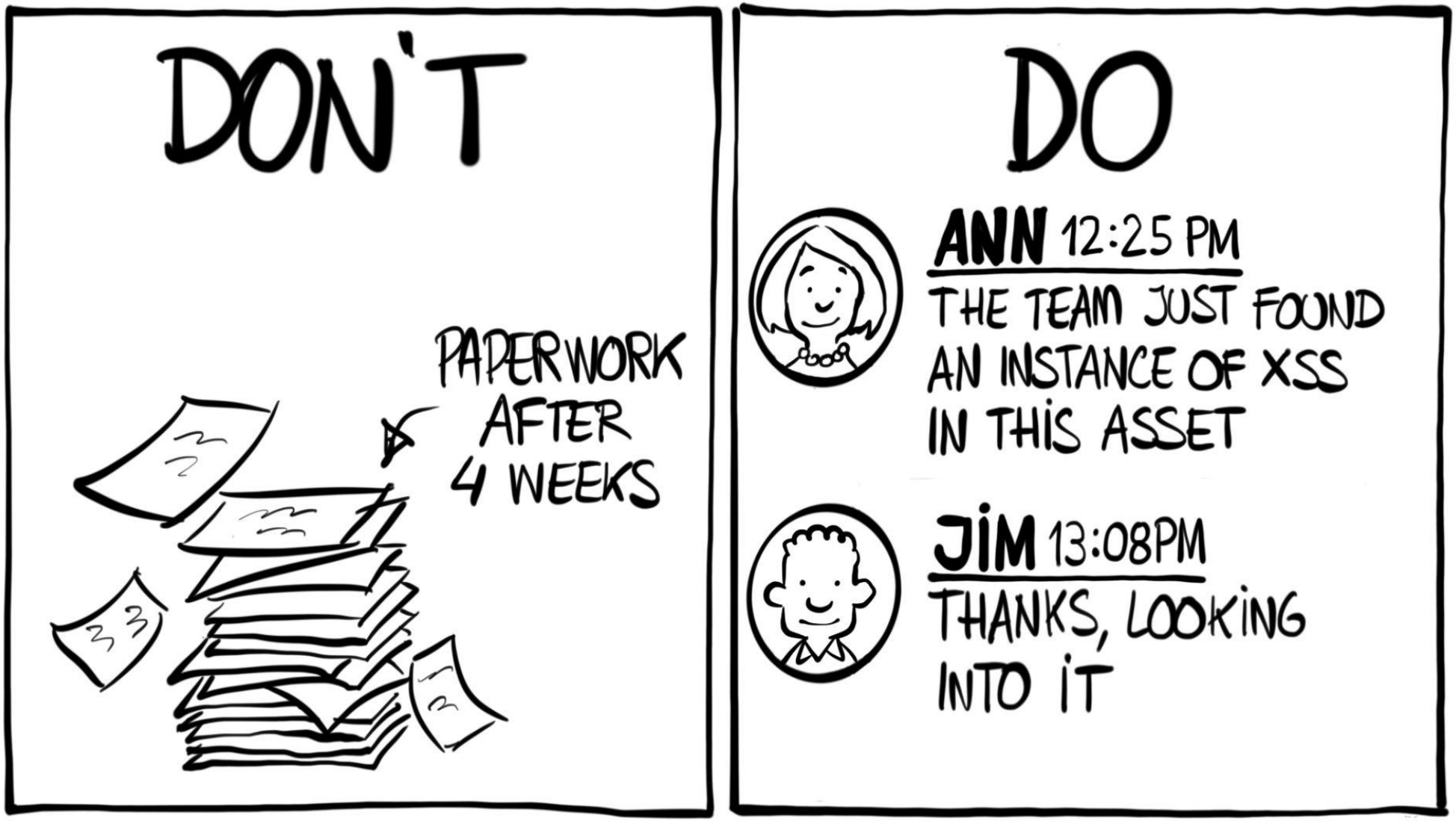

WAITING FOR MY PENTEST TO START.


#OF NEW FEATURES RELEASED
SECURITY TEAM ANXIETY LEVELS
#OF DAYS SINCE LAST PENTEST

Cobal

How to scale pentesting: remediate risk collaboratively

Cobalt

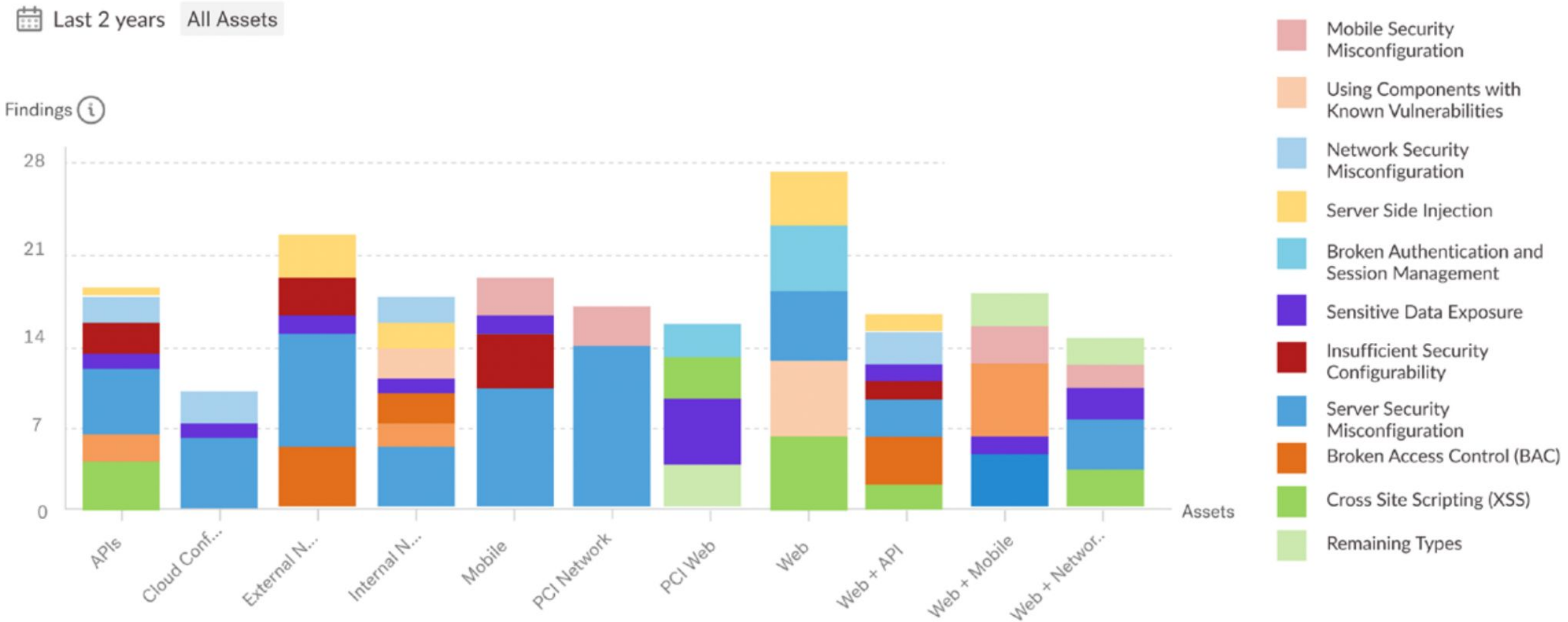


TIMELY SHARING OF FINDINGS

How to scale pentesting: use data

Cobalt

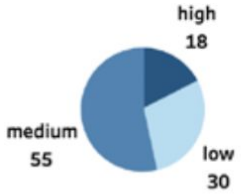
All Findings by Type



Open Findings Per Asset By State

Asset	State				
	carried_o..	check_fix	need_fix	new	triaging
Saxophone External Netw..		1	3		
Payment API		3	2		
Azure External Network		1	4	1	
Saxophone Mobile		8	7		
Saxophone US Web App	9	2	8	2	
Cloud Config		9	24	4	1

Severity Distribution of Open Findings



Open High Severity Findings Per Asset

Asset	
Payment API	2
Saxophone US Web App	2
Saxophone Mobile	5

Open Medium Severity Findings Per Asset

Asset	
Saxophone External Netw..	1
Azure External Network	3
Saxophone Mobile	8
Saxophone US Web App	9
Cloud Config	28

Open Low Severity Findings Per Asset

Asset	
Saxophone Mobile	2
Azure External Network	2
Saxophone External Netw..	3
Payment API	3
Cloud Config	5
Saxophone US Web App	8

Open Findings Per Asset

Asset	
Saxophone External Netw..	5
Saxophone Internal Netw..	6
Payment API	6
Azure External Network	12
Saxophone Mobile	21
Saxophone US Web App	24
Cloud Config	43

Closed Findings Per Asset

Asset	
Saxophone External Netw..	1
Payment API	1
Saxophone US Web App	3
Cloud Config	5
Saxophone Internal Netw..	6
Saxophone Mobile	6
Azure External Network	6

Total Findings By State

State	
out_of_scope	1
triaging	1
invalid	2
duplicate	3
new	7
valid_fix	7
carried_over	9
wont_fix	15
check_fix	24
need_fix	48

THE FIVE IDEALS

The First Ideal: Locality and Simplicity

The Second Ideal: Focus, Flow, and Joy

The Third Ideal: Improvement of Daily Work

The Fourth Ideal: Psychological Safety

The Fifth Ideal: Customer Focus

How to Scale Pentesting

- Start faster
- Remediate risk smarter
- Use data

RSAConference2022

Thank you - let's keep in touch.

caroline@cobalt.io
https://www.linkedin.com/in/carolinewmwong/