

# RSA® Conference 2022

San Francisco & Digital | June 6 – 9

SESSION ID: DSO-M01

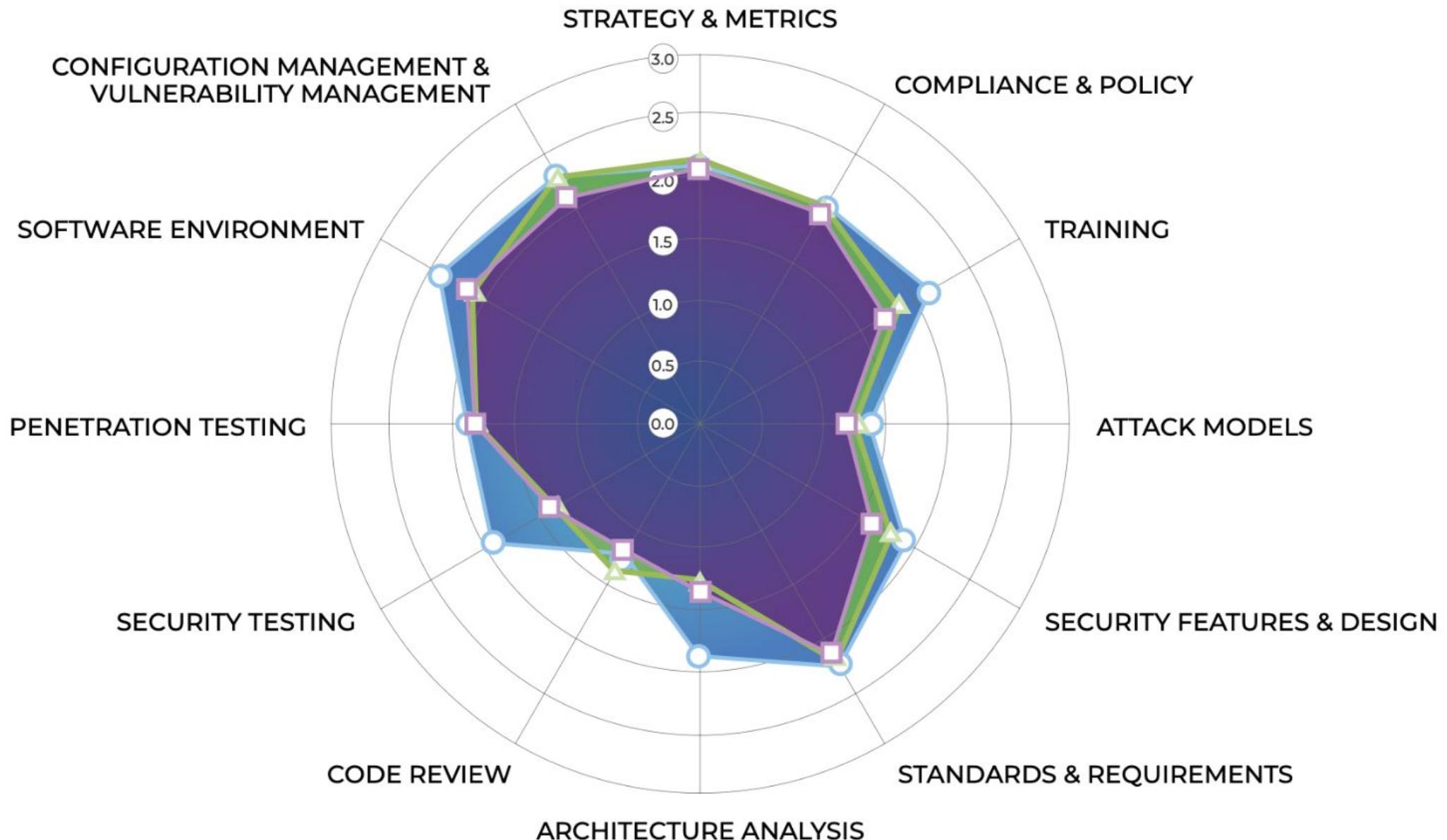
## The Practicalities of Pentesting at Scale

**Caroline Wong**

Chief Strategy Officer at Cobalt

# TRANSFORM





—□— 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

# From Terrifying to ... Good Enough?

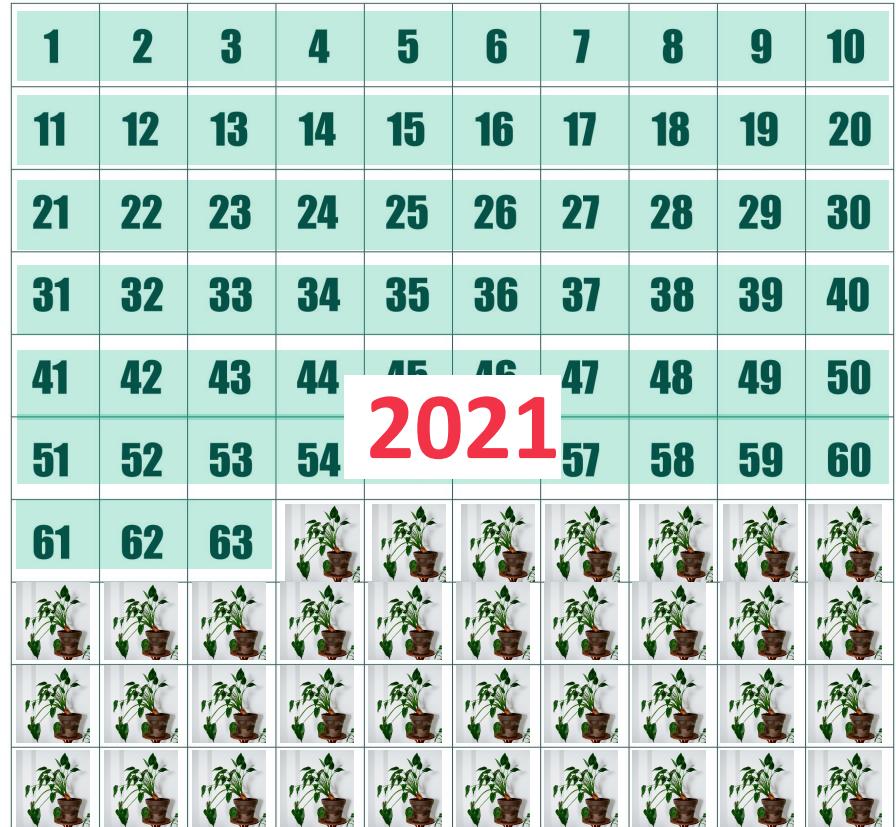
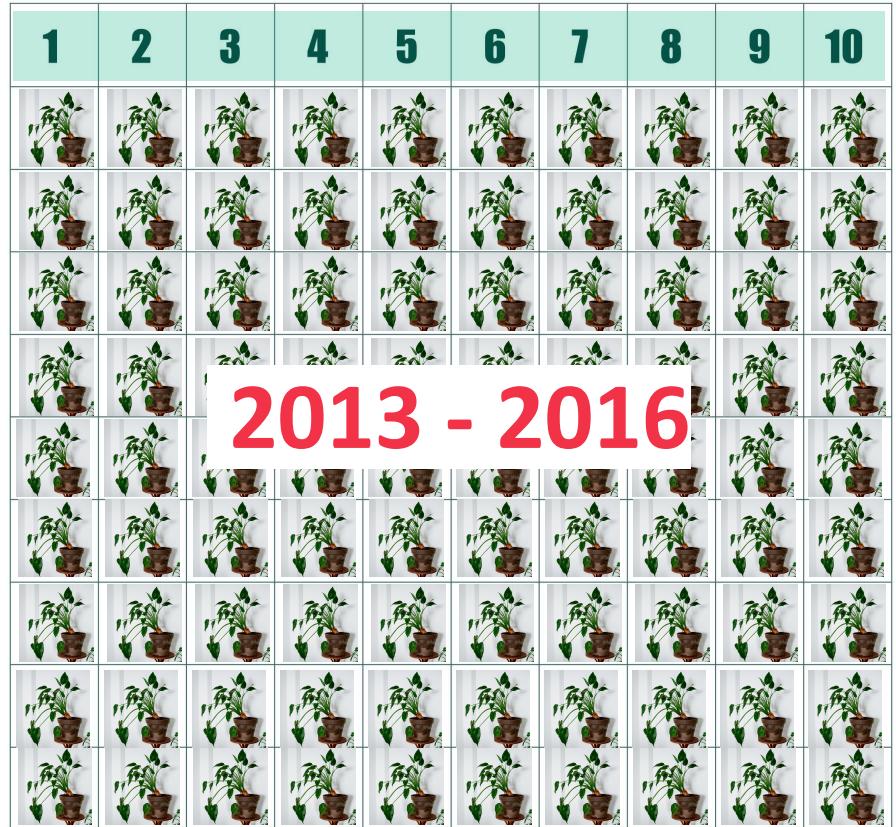
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	--	--	--	--	--	--	49	50
51	52	--	--	--	--	--	--	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

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	45	46	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

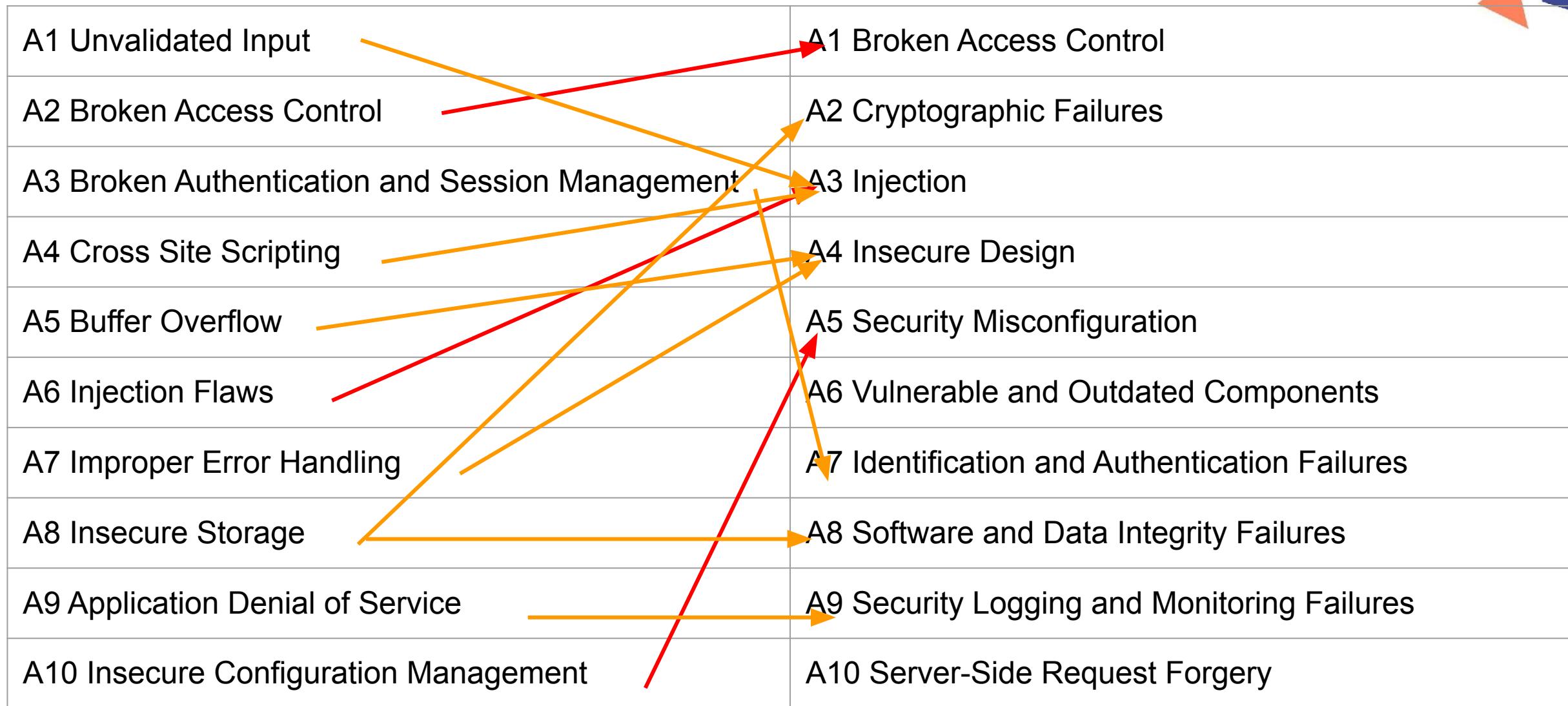
# House Plants



# Cats



# OWASP Top 10: 2003 vs. 2021



Matthew McConaughey in 2003

301



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?





# Doing Controls vs. Managing Risk

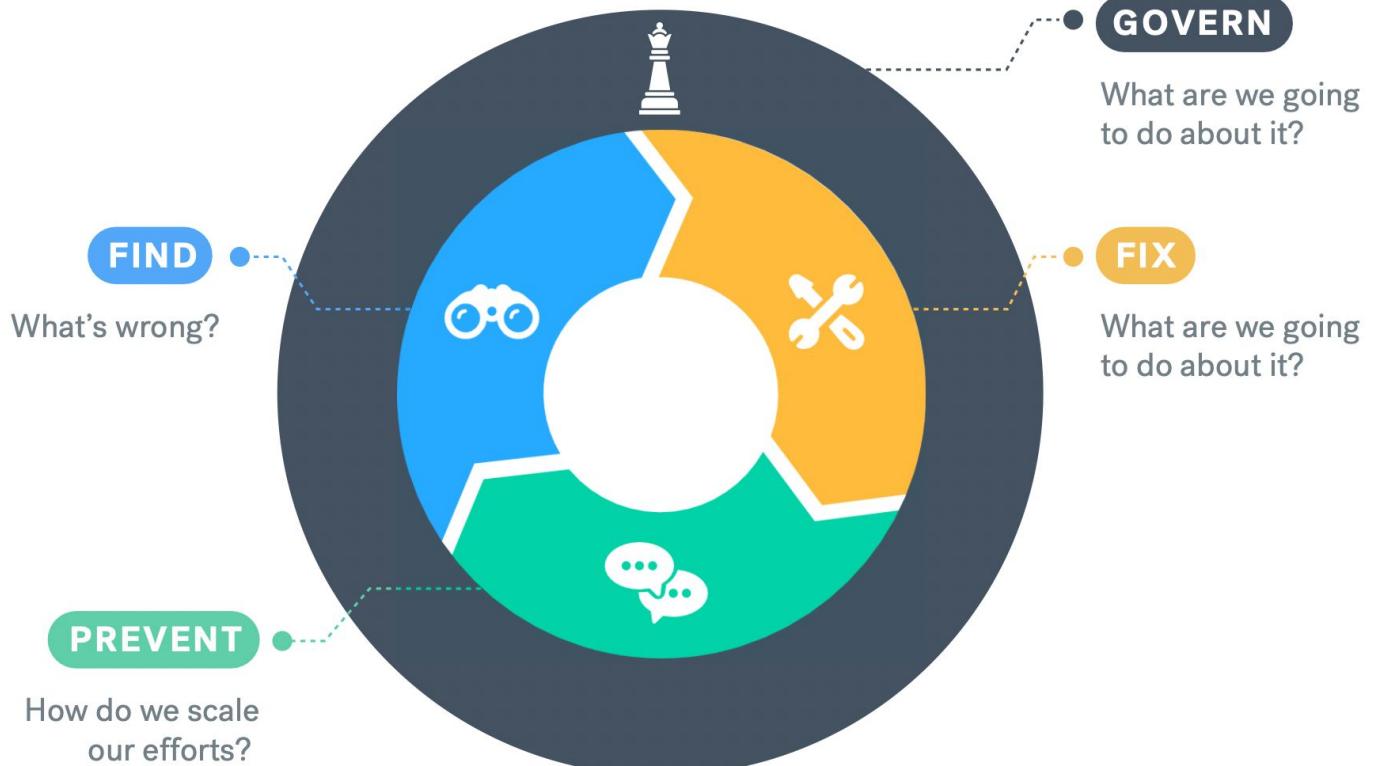
NIST SP 800-53, Rev. 5  
SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

**Table of Contents**

<b>CHAPTER ONE</b>	<b>INTRODUCTION.....</b>	<b>1</b>
1.1	PURPOSE AND APPLICABILITY.....	2
1.2	TARGET AUDIENCE .....	3
1.3	ORGANIZATIONAL RESPONSIBILITIES.....	3
1.4	RELATIONSHIP TO OTHER PUBLICATIONS.....	5
1.5	REVISONS AND EXTENSIONS.....	5
1.6	PUBLICATION ORGANIZATION.....	5
<b>CHAPTER TWO</b>	<b>THE FUNDAMENTALS.....</b>	<b>7</b>
2.1	REQUIREMENTS AND CONTROLS.....	7
2.2	CONTROL STRUCTURE AND ORGANIZATION.....	8
2.3	CONTROL IMPLEMENTATION APPROACHES.....	11
2.4	SECURITY AND PRIVACY CONTROLS.....	13
2.5	TRUSTWORTHINESS AND ASSURANCE.....	14
<b>CHAPTER THREE</b>	<b>THE CONTROLS.....</b>	<b>16</b>
3.1	ACCESS CONTROL.....	18
3.2	AWARENESS AND TRAINING.....	59
3.3	AUDIT AND ACCOUNTABILITY.....	65
3.4	ASSESSMENT, AUTHORIZATION, AND MONITORING.....	83
3.5	CONFIGURATION MANAGEMENT.....	96
3.6	CONTINGENCY PLANNING.....	115
3.7	IDENTIFICATION AND AUTHENTICATION.....	131
3.8	INCIDENT RESPONSE.....	149
3.9	Maintenance.....	162
3.10	MEDIA PROTECTION.....	171
3.11	PHYSICAL AND ENVIRONMENTAL PROTECTION.....	179
3.12	PLANNING.....	194
3.13	PROGRAM MANAGEMENT.....	203
3.14	PERSONNEL SECURITY.....	222
3.15	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING AND TRANSPARENCY.....	229
3.16	RISK ASSESSMENT.....	238
3.17	SYSTEM AND SERVICES ACQUISITION.....	249
3.18	SYSTEM AND COMMUNICATIONS PROTECTION.....	292
3.19	SYSTEM AND INFORMATION INTEGRITY.....	332
3.20	SUPPLY CHAIN RISK MANAGEMENT.....	363
<b>REFERENCES.....</b>	<b>374</b>	
<b>APPENDIX A</b>	<b>GLOSSARY.....</b>	<b>394</b>
<b>APPENDIX B</b>	<b>ACRONYMS.....</b>	<b>424</b>
<b>APPENDIX C</b>	<b>CONTROL SUMMARIES.....</b>	<b>428</b>

APPENDIX C	CONTROLS.....	384
APPENDIX B	ACRONYMS.....	454
APPENDIX A	GLOSSARY.....	466
REFERENCES	31	471
REFERENCES	303	471
REFERENCES	326	471
REFERENCES	335	471
REFERENCES	345	471
REFERENCES	348	471
REFERENCES	358	471
REFERENCES	359	471
REFERENCES	363	471
REFERENCES	373	471
REFERENCES	375	471
REFERENCES	376	471
REFERENCES	377	471
REFERENCES	378	471
REFERENCES	379	471
REFERENCES	380	471
REFERENCES	381	471
REFERENCES	382	471
REFERENCES	383	471
REFERENCES	384	471
REFERENCES	385	471
REFERENCES	386	471
REFERENCES	387	471
REFERENCES	388	471
REFERENCES	389	471
REFERENCES	390	471
REFERENCES	391	471
REFERENCES	392	471
REFERENCES	393	471
REFERENCES	394	471
REFERENCES	395	471
REFERENCES	396	471
REFERENCES	397	471
REFERENCES	398	471
REFERENCES	399	471
REFERENCES	400	471
REFERENCES	401	471
REFERENCES	402	471
REFERENCES	403	471
REFERENCES	404	471
REFERENCES	405	471
REFERENCES	406	471
REFERENCES	407	471
REFERENCES	408	471
REFERENCES	409	471
REFERENCES	410	471
REFERENCES	411	471
REFERENCES	412	471
REFERENCES	413	471
REFERENCES	414	471
REFERENCES	415	471
REFERENCES	416	471
REFERENCES	417	471
REFERENCES	418	471
REFERENCES	419	471
REFERENCES	420	471
REFERENCES	421	471
REFERENCES	422	471
REFERENCES	423	471
REFERENCES	424	471
REFERENCES	425	471
REFERENCES	426	471
REFERENCES	427	471
REFERENCES	428	471
REFERENCES	429	471
REFERENCES	430	471
REFERENCES	431	471
REFERENCES	432	471
REFERENCES	433	471
REFERENCES	434	471
REFERENCES	435	471
REFERENCES	436	471
REFERENCES	437	471
REFERENCES	438	471
REFERENCES	439	471
REFERENCES	440	471
REFERENCES	441	471
REFERENCES	442	471
REFERENCES	443	471
REFERENCES	444	471
REFERENCES	445	471
REFERENCES	446	471
REFERENCES	447	471
REFERENCES	448	471
REFERENCES	449	471
REFERENCES	450	471
REFERENCES	451	471
REFERENCES	452	471
REFERENCES	453	471
REFERENCES	454	471
REFERENCES	455	471
REFERENCES	456	471
REFERENCES	457	471
REFERENCES	458	471
REFERENCES	459	471
REFERENCES	460	471
REFERENCES	461	471
REFERENCES	462	471
REFERENCES	463	471
REFERENCES	464	471
REFERENCES	465	471
REFERENCES	466	471
REFERENCES	467	471
REFERENCES	468	471
REFERENCES	469	471
REFERENCES	470	471
REFERENCES	471	471

## The Modern AppSec Framework



# 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

# Cybersecurity: a decade in review

# Cybersecurity: 2 decades in review

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

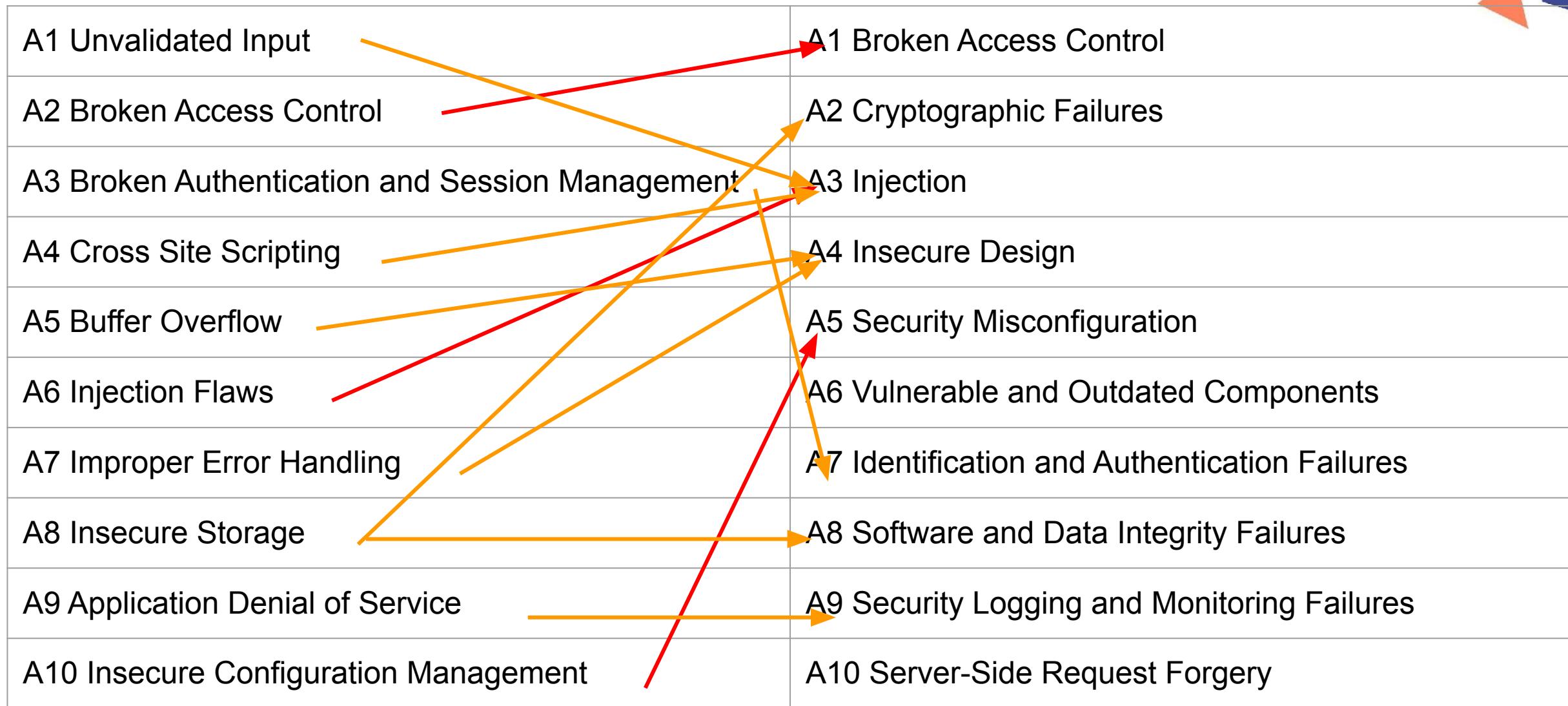
with Bastien Inzaurrealde

## THE KEY



	\$147.99
	\$109.00

# OWASP Top 10: 2003 vs. 2021



# My life in 2022

2000 weeks

Weeks Future  
50.0%

Weeks Past  
50.0%

Four  
Thousand  
Weeks

Time  
Management  
for Mortals

Oliver  
Burkeman



# Software development: a decade in review

## The case for DevOps remains clear

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

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

ComputerWeekly.com

IT Management ▾

Industry Sectors ▾

Technology Topics ▾

Search Computer We

## Codecov supply chain attack has echoes of SolarWinds

# Security Practice



# 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	✗	<b>Cost</b> Low
Low	✗	<b>Flexibility</b> High
No	✗	<b>On-demand</b> Yes
Little	✗	<b>Redundancy</b> A lot
Few	✗	<b>Workloads</b> Many

# Pentesting Maturity Model

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

# Pentesting Maturity Model

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

# 2022 State of Pentesting: research findings

# How we used to think about cybersecurity



# How it really is



Security

89%

Development

70%

Percentage of respondents struggling to collaborate



96%

of security teams see a slower response to patching critical vulnerabilities



97%

of developers struggle to meet critical launch deadlines



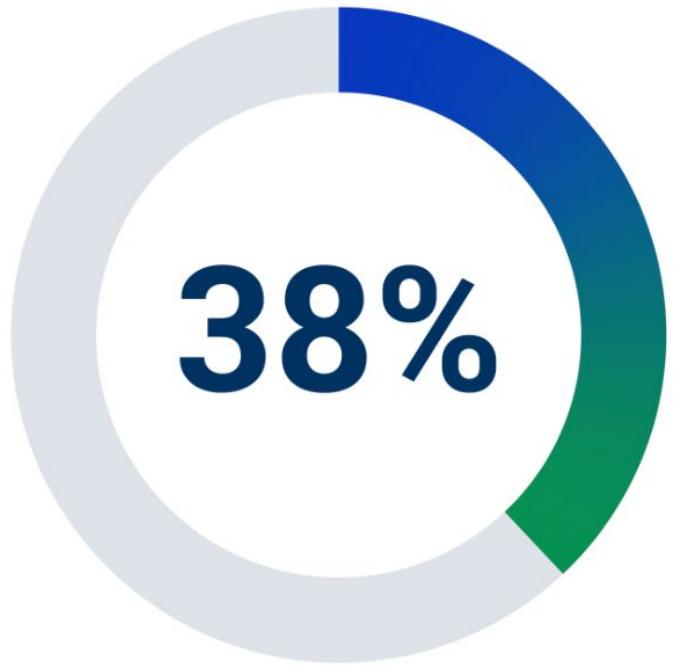
80%

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

# Top 5 Vulnerability Categories

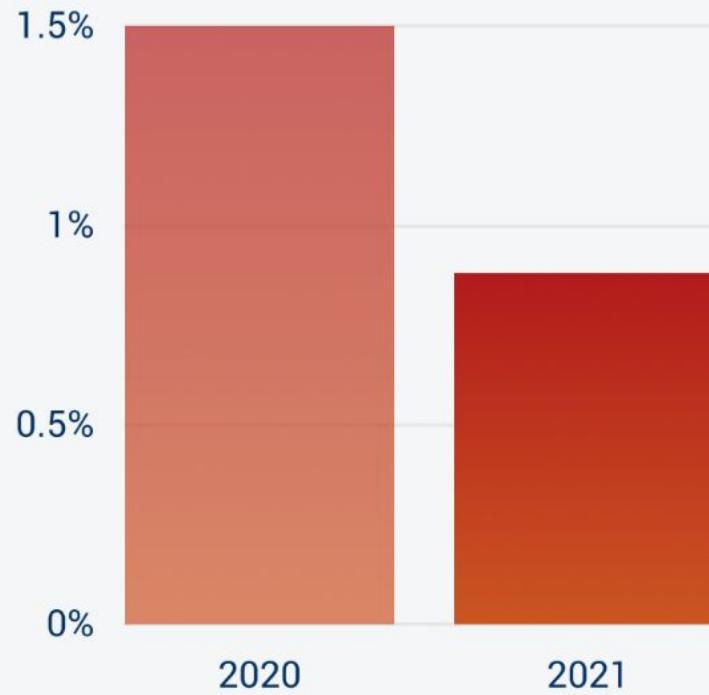
Following the same hierarchy, we started our analysis with the 5 most frequently discovered vulnerability categories in 2021:

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%

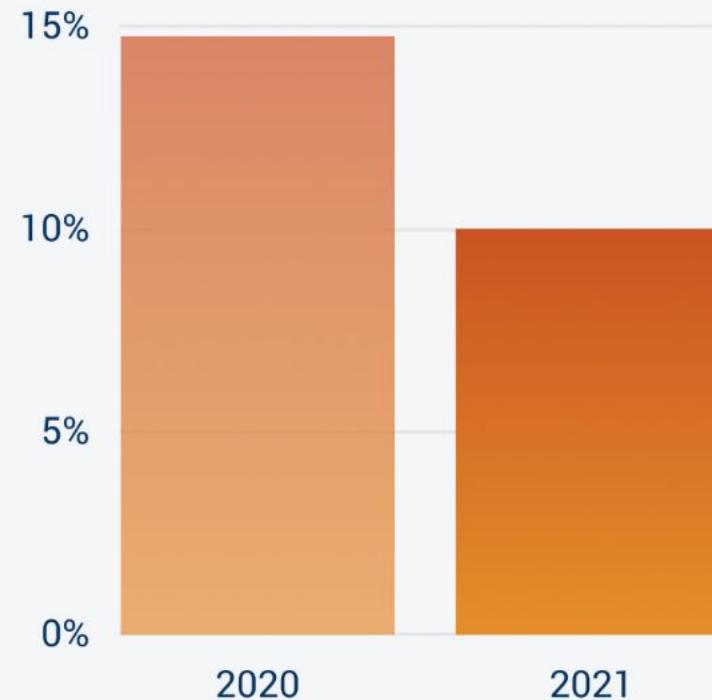


of our 2021 findings are  
connected to Server Security  
Misconfigurations

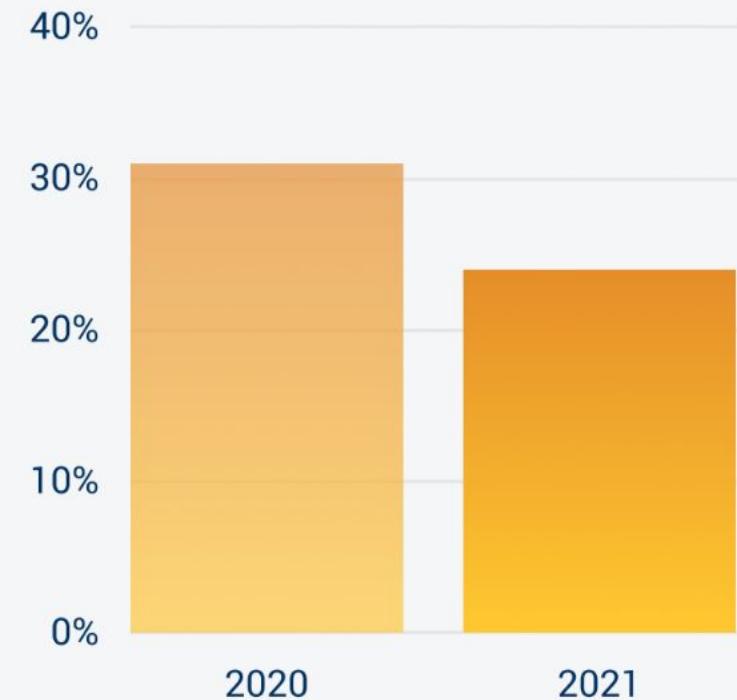
# Findings with Critical, High, Medium Severity



% of findings with Critical severity

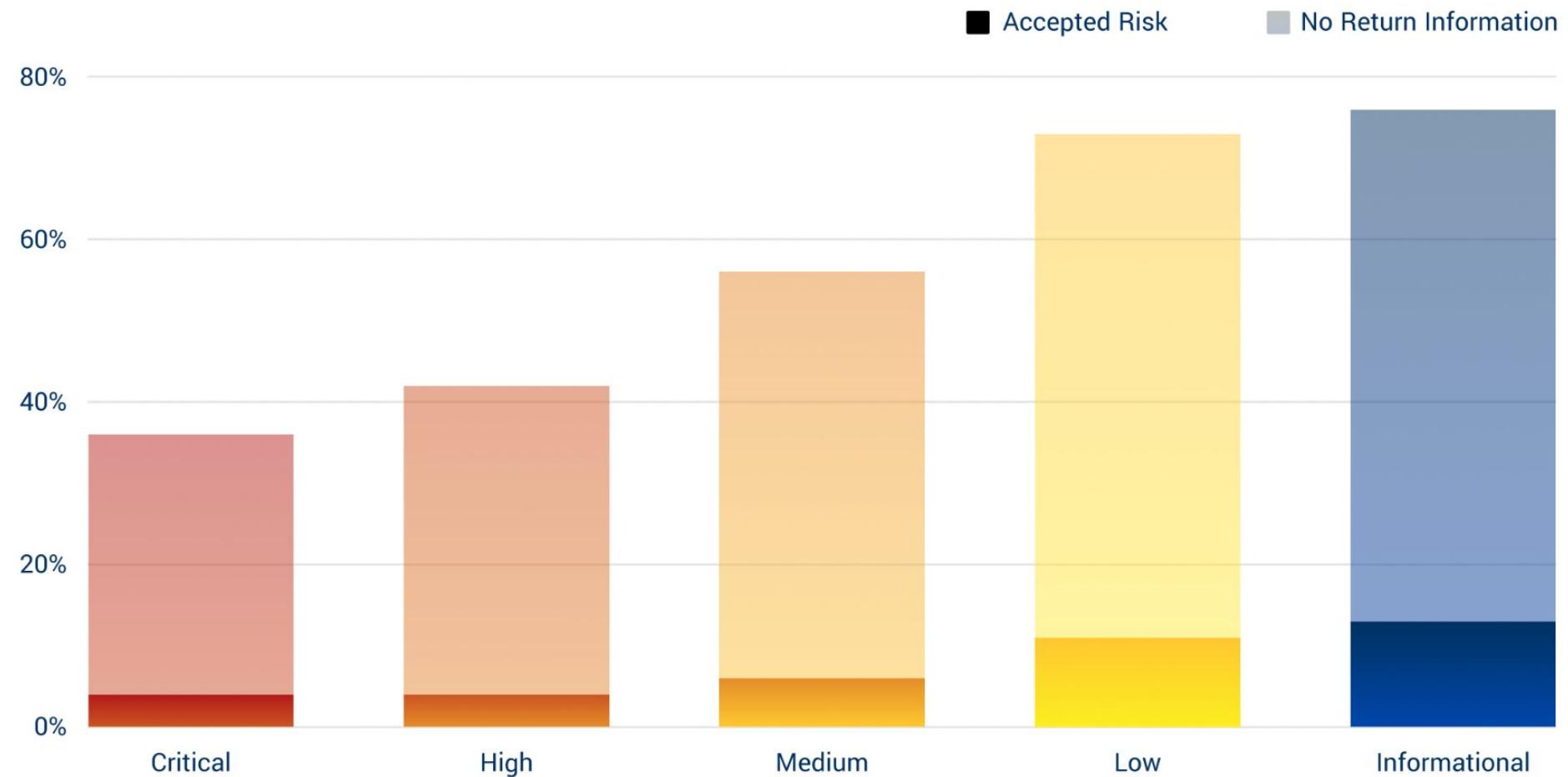


% of findings with High severity

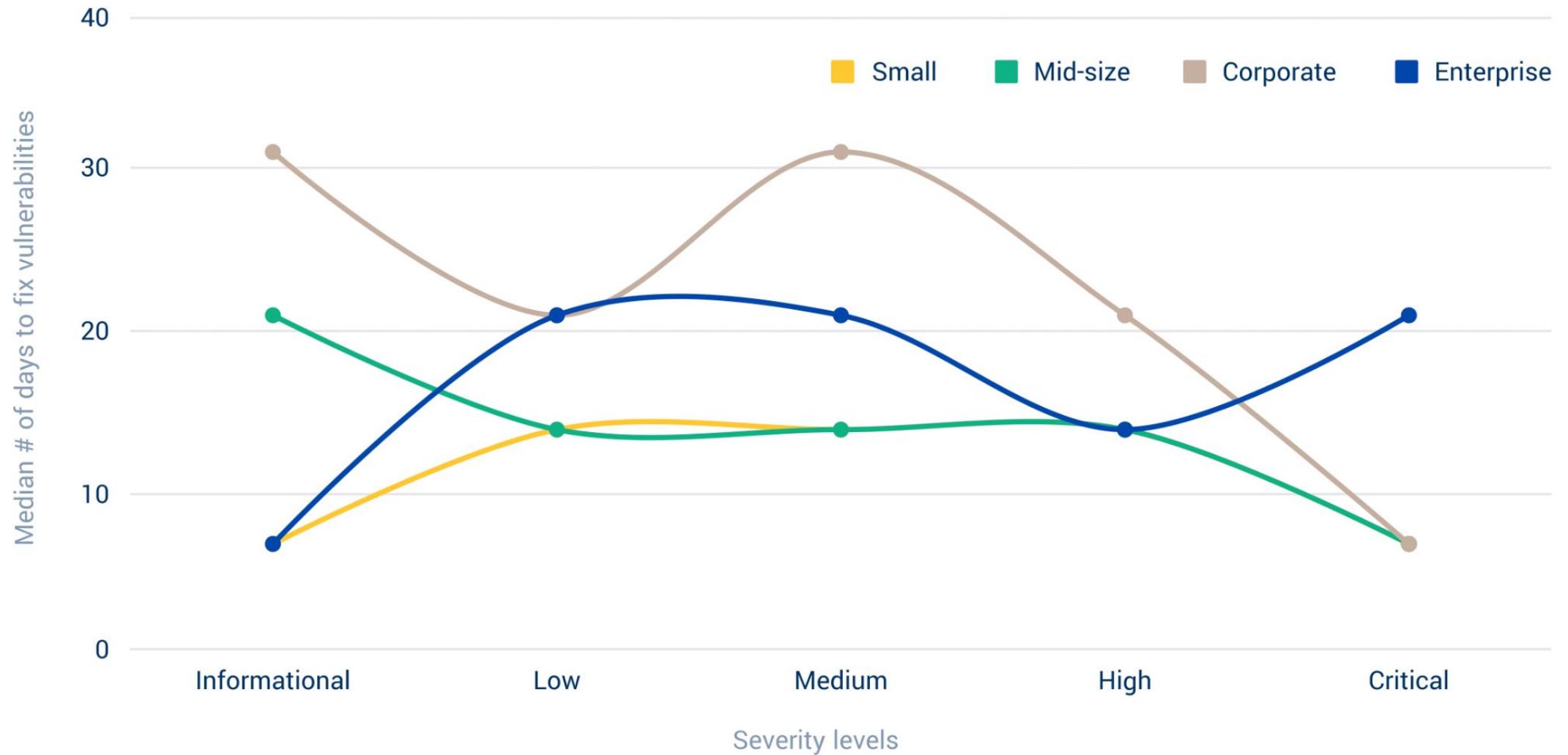


% of findings with Medium severity

# Findings marked “Accepted Risk” or “No Info”



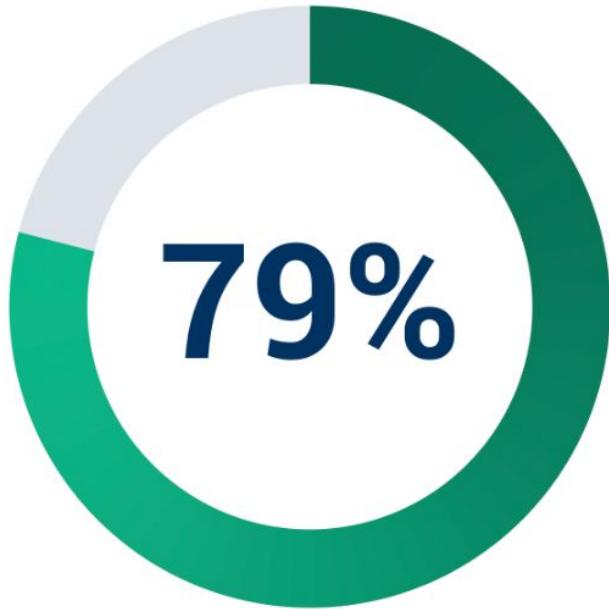
# Number of Days to Fix Findings



# We still have a talent shortage



struggle to maintain high  
quality security standards

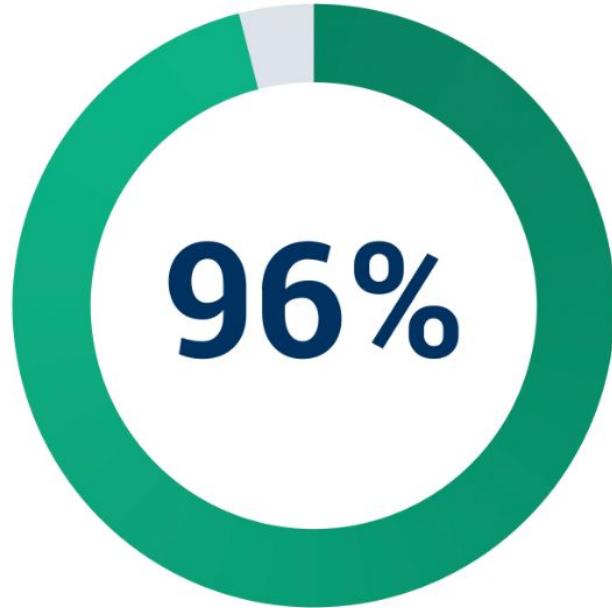


struggle to consistently  
monitor for vulnerabilities

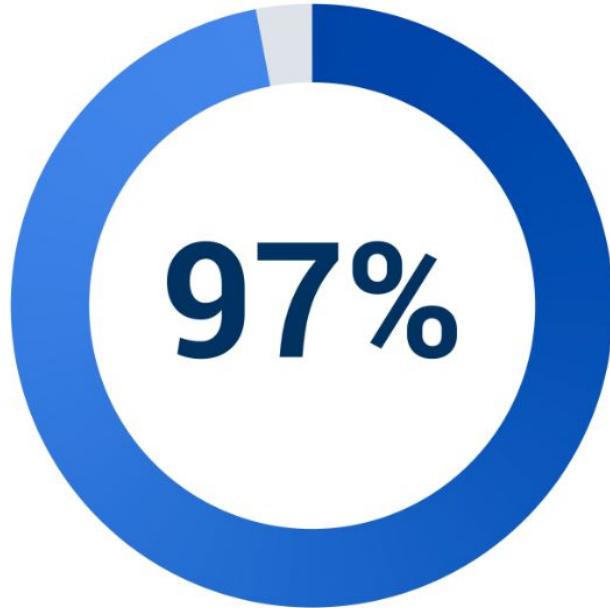


struggle to monitor for and  
respond to security incidents

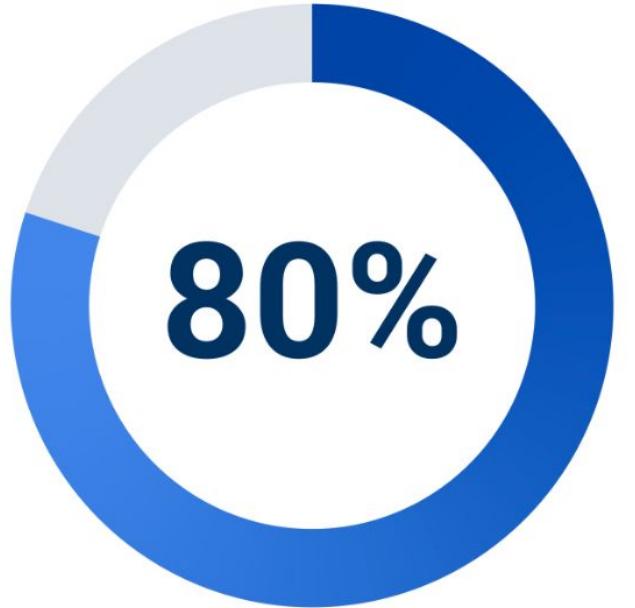
# The talent shortage affects collaboration



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

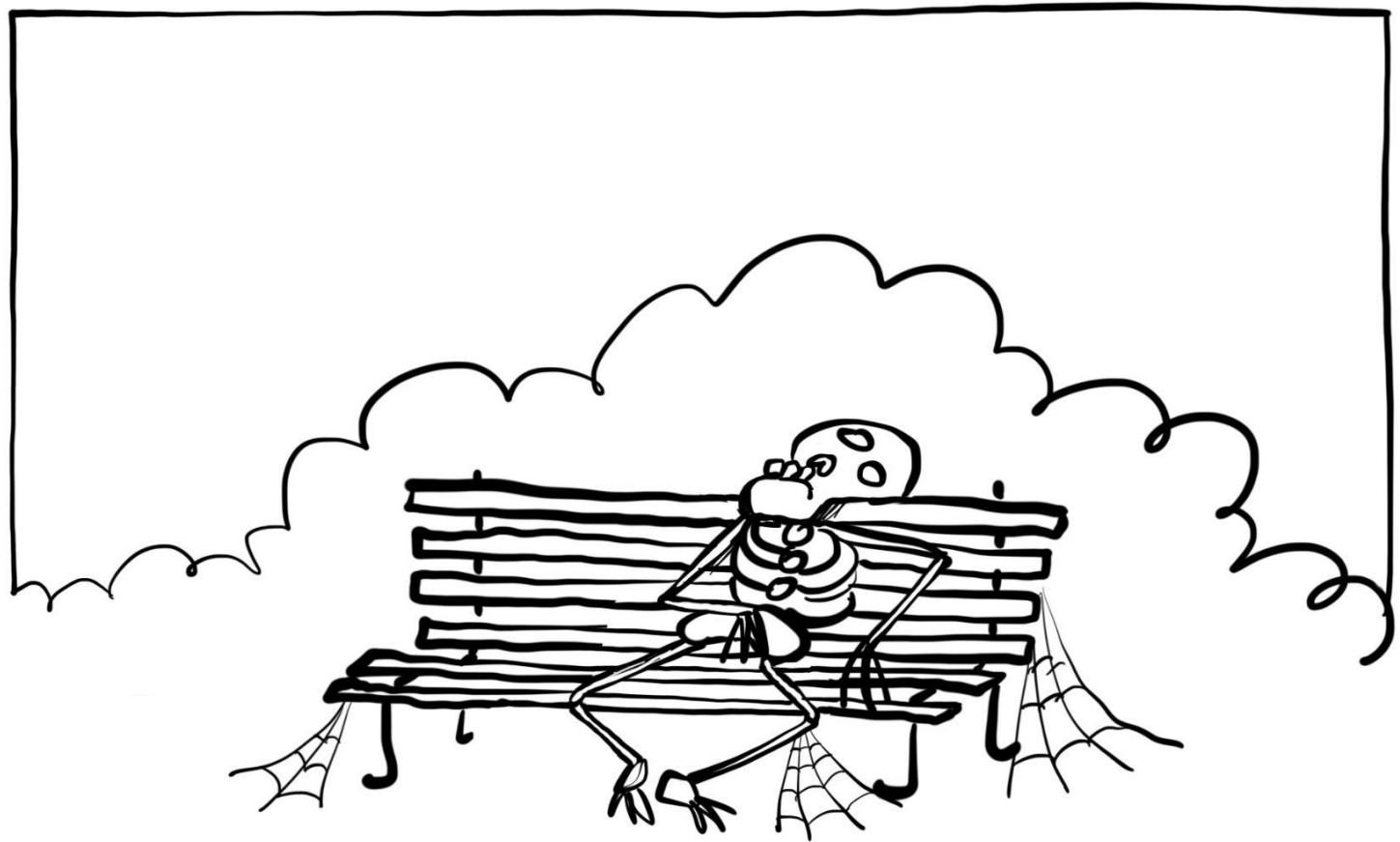


of developers said collaboration  
challenges make it harder to  
meet critical launch deadlines

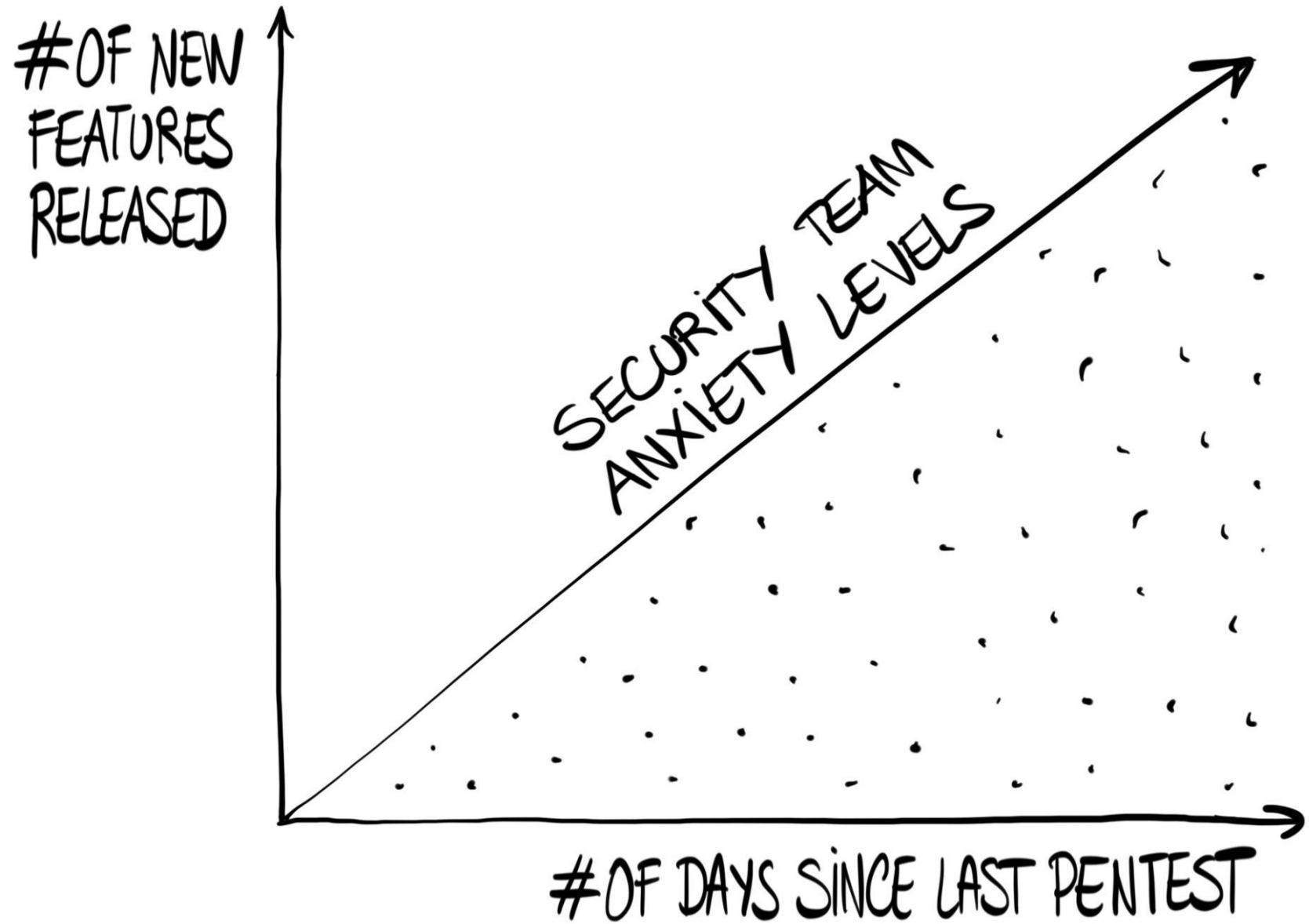


of developers agreed  
collaboration challenges  
compromise the quality and  
security of their code

# How to scale pentesting: do it faster and more often

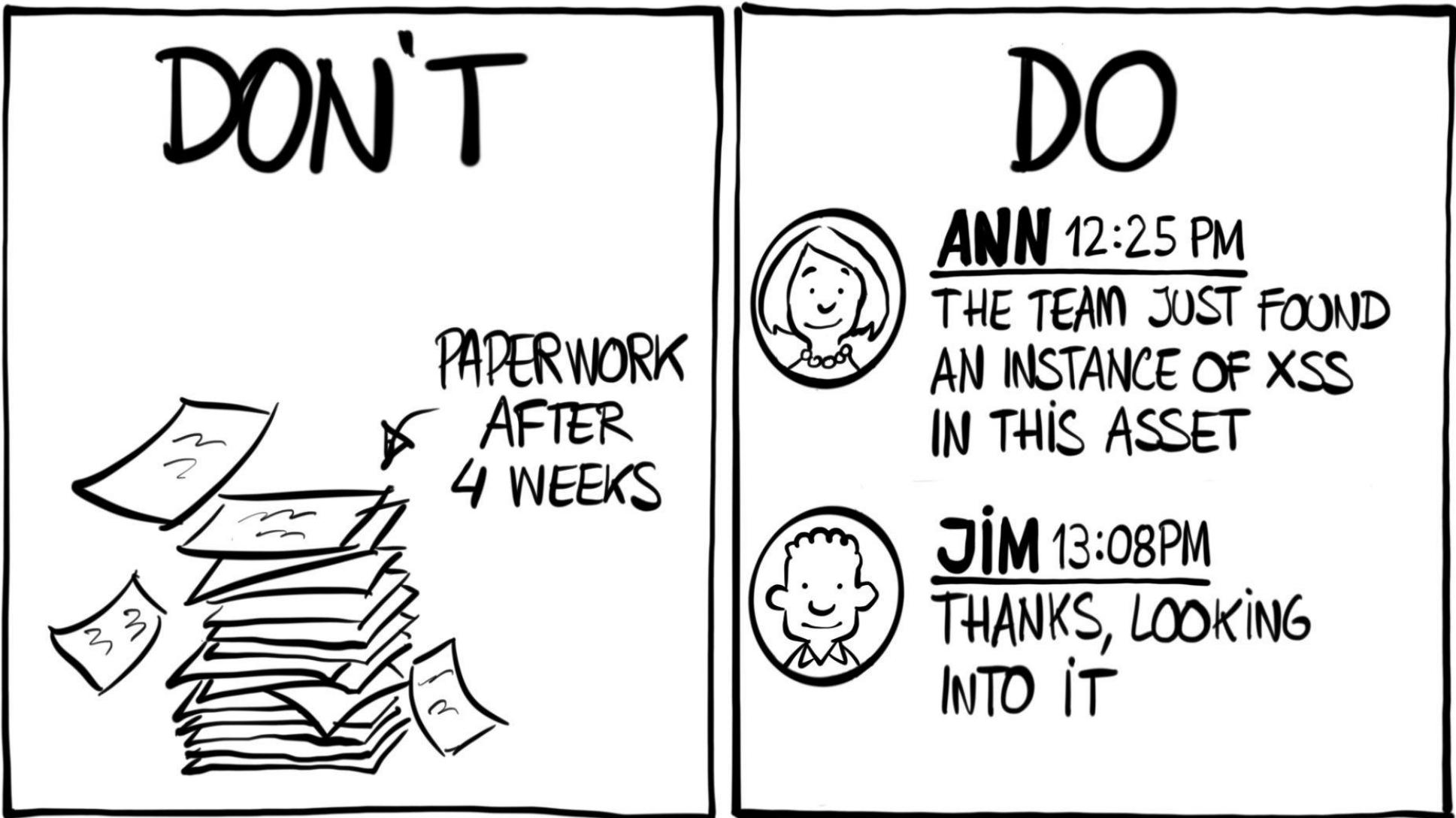


WAITING FOR MY PENTEST TO START.



# How to scale pentesting: remediate risk collaboratively





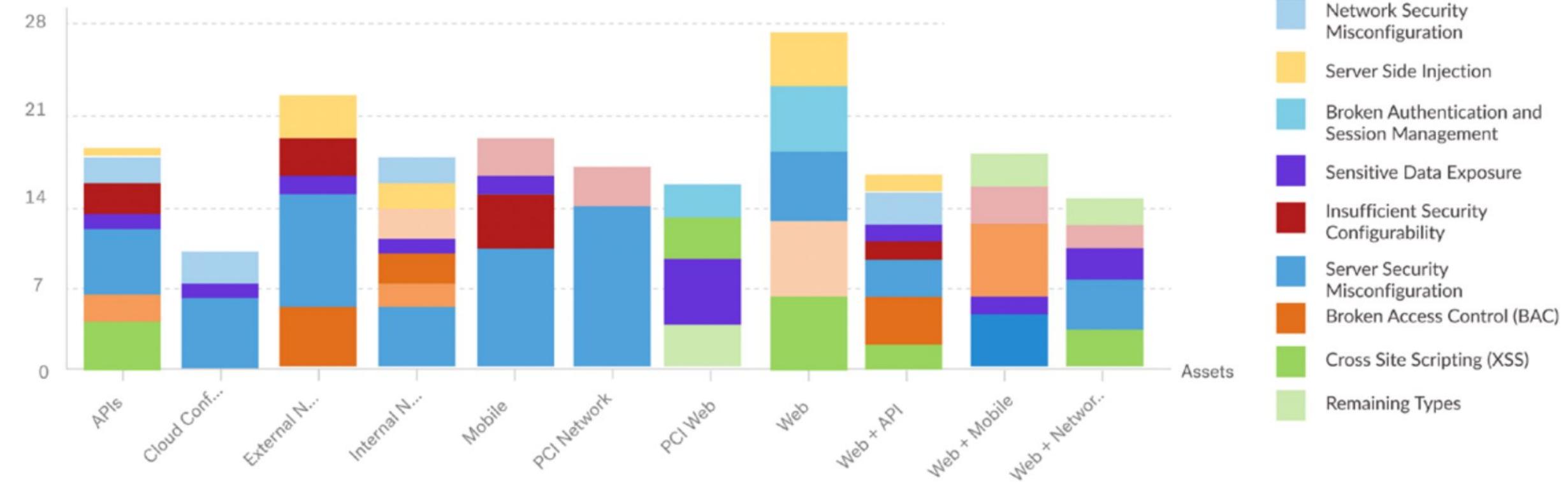
TIMELY SHARING OF FINDINGS

# How to scale pentesting: use data

# All Findings by Type

Last 2 years All Assets

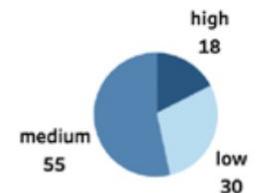
Findings ⓘ



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

Open Medium Severity Findings Per Asset

Asset	Value
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	Value
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	Value
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	Value
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	Value
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	49

# 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

# RSA® Conference 2022

Thank you - let's keep in touch.

[caroline@cobalt.io](mailto:caroline@cobalt.io)

<https://www.linkedin.com/in/carolinewmwong/>

