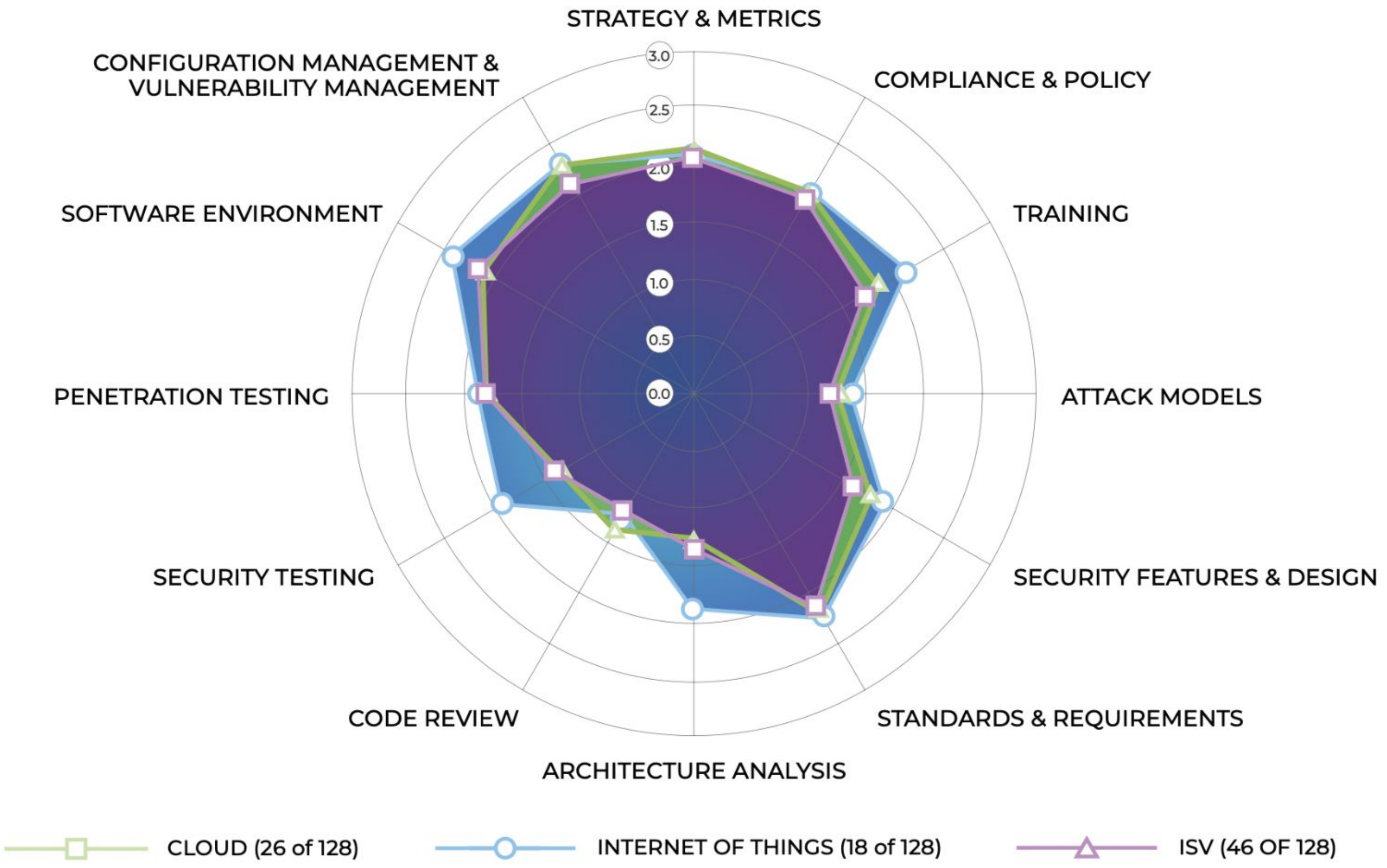
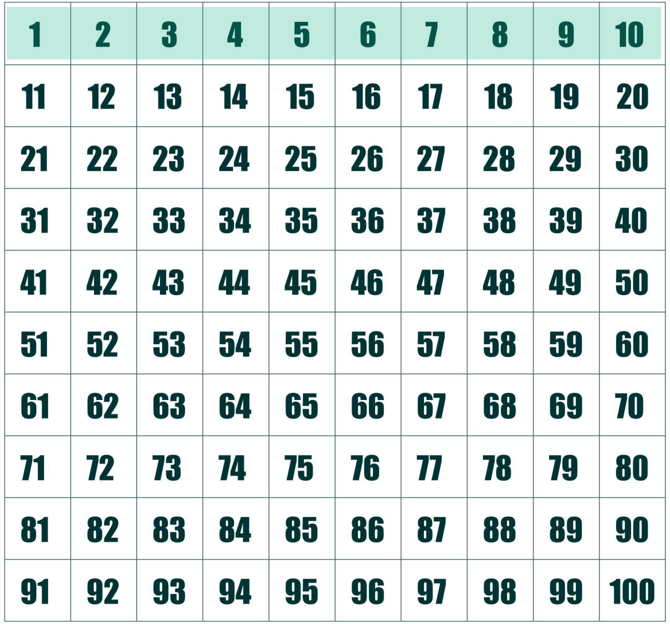
Cobalt

Pentesting at Scale

OWASP NZ Day 2022

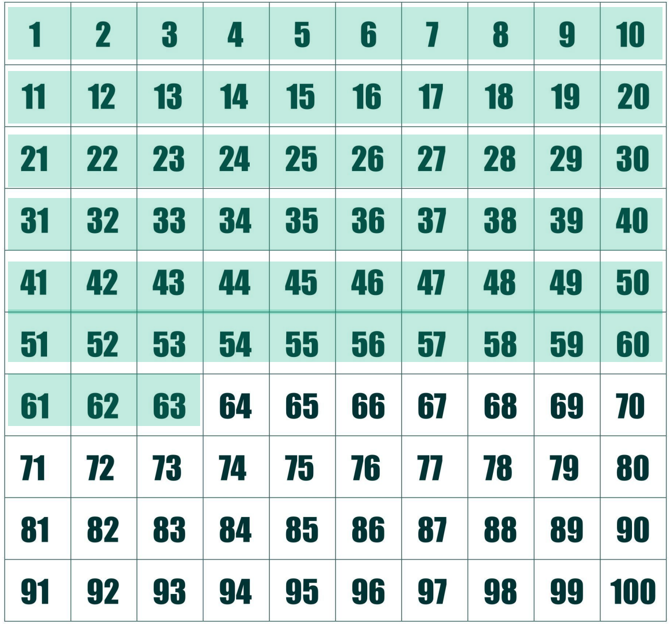

STRATEGY & METRICS
COMPLIANCE & POLICY
TRAINING
ATTACK MODELS
SECURITY FEATURES & DESIGN
STANDARDS & REQUIREMENTS
ARCHITECTURE ANALYSIS
CODE REVIEW
SECURITY TESTING
PENETRATION TESTING
SOFTWARE ENVIRONMENT
CONFIGURATION MANAGEMENT & VULNERABILITY MANAGEMENT
3.0
2.5
2.0
1.5
1.0
0.5
0.0
CLOUD (26 of 128)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

From Terrifying to … 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	43	44	45	46	47	48	49	50
51	52	53	54	55	56	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

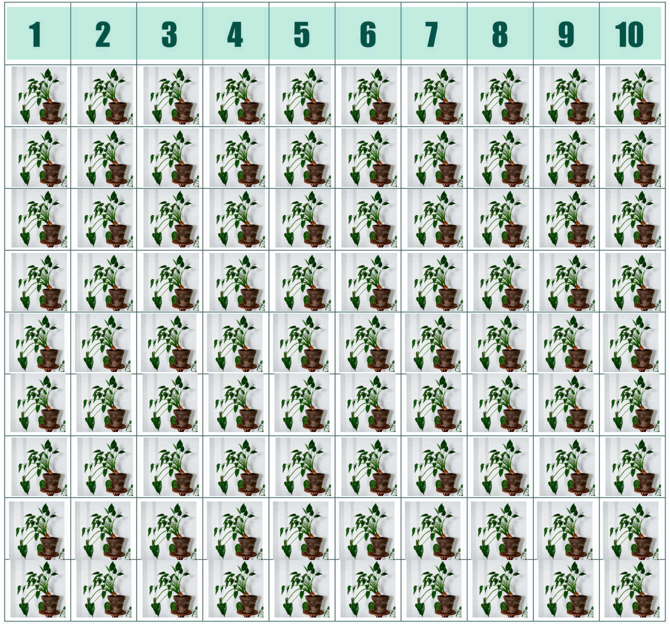
2013 - 2016



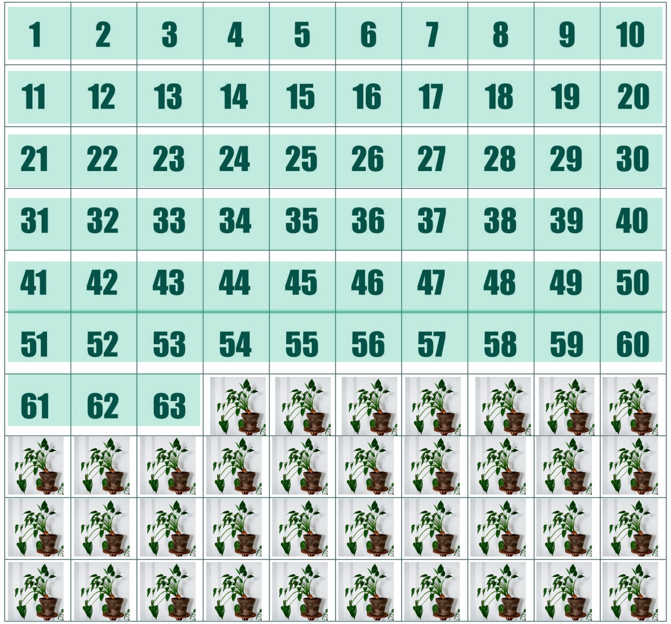
1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2021

House Plants

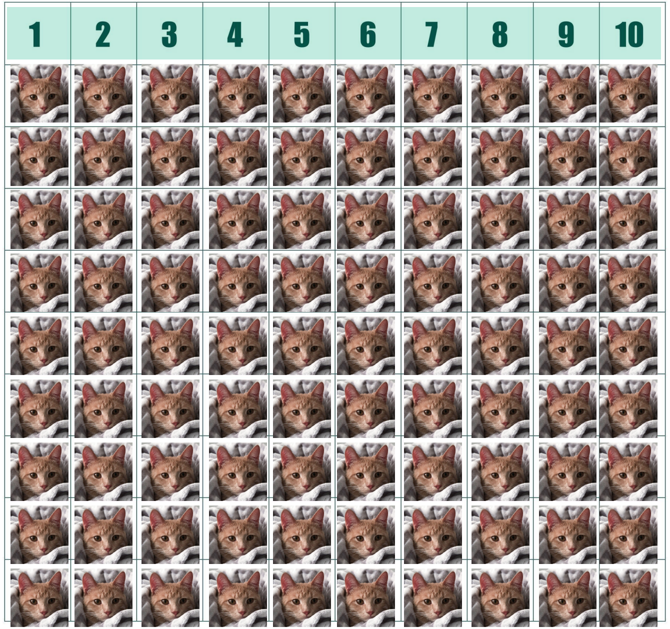


2013 - 2016



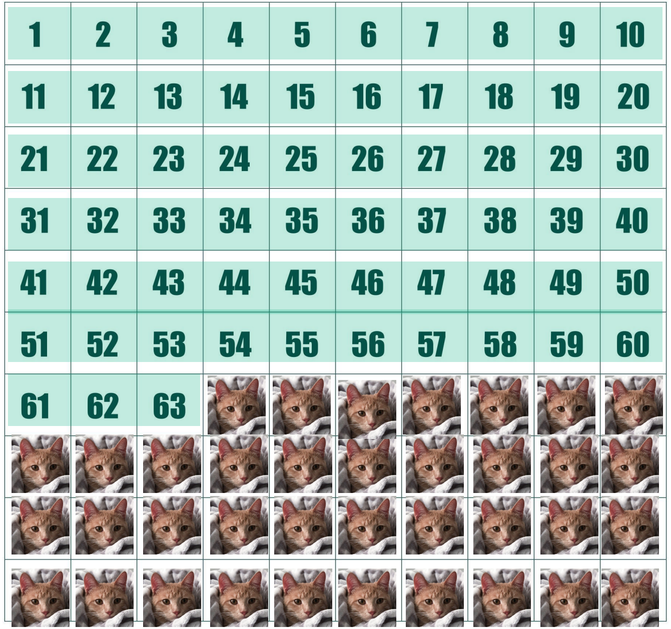
2021

Cats



1	2	3	4	5	6	7	8	9	10

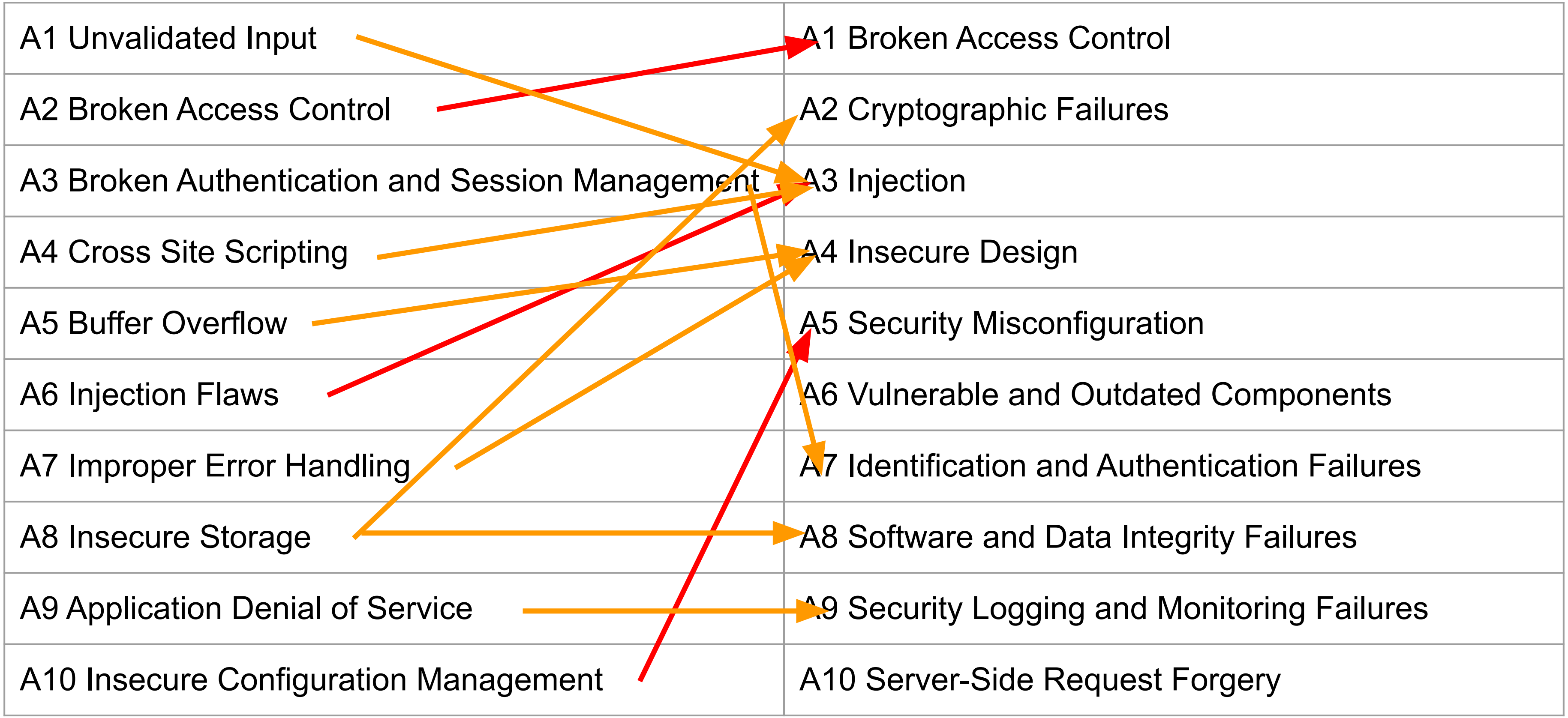
2013 - 2016



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	45	46	47	48	49	50
51	52	53	54	55	56	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

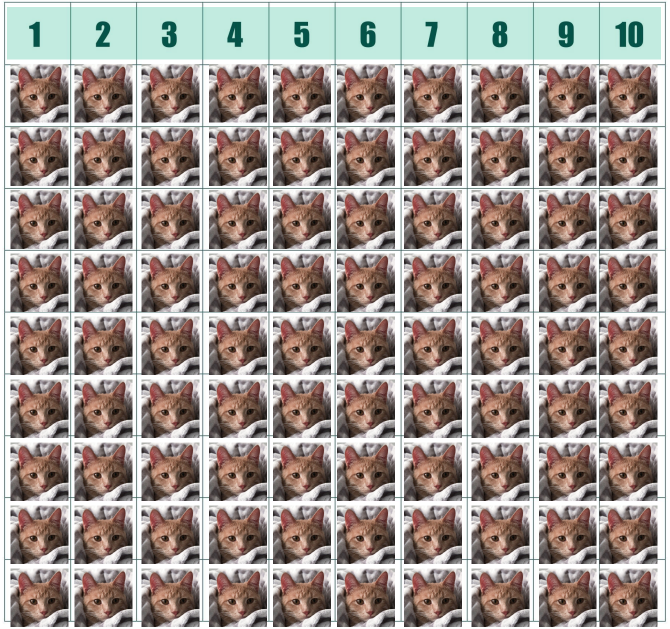
Topics

1 History Lesson: Cybersecurity and Software Development

2 A Maturity Model for Pentesting

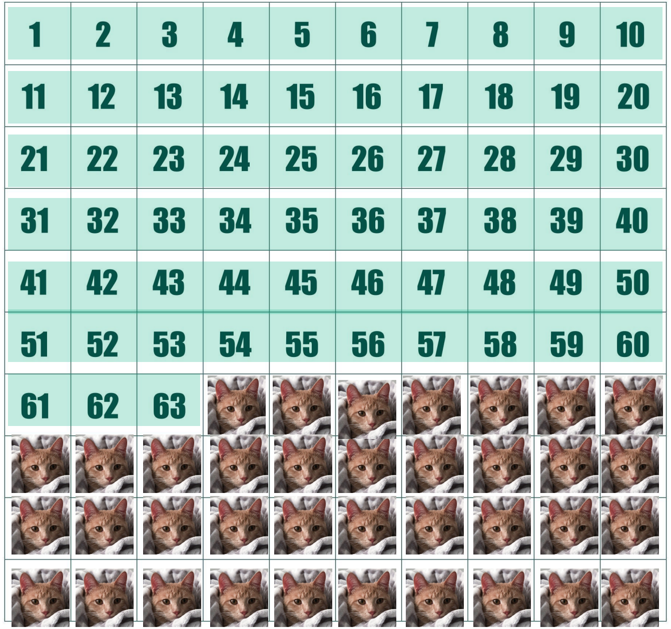
3 How to Scale Pentesting (and achieve the 5 Ideals)

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	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63							

2021

hilo

Doing Controls vs. Managing Risk

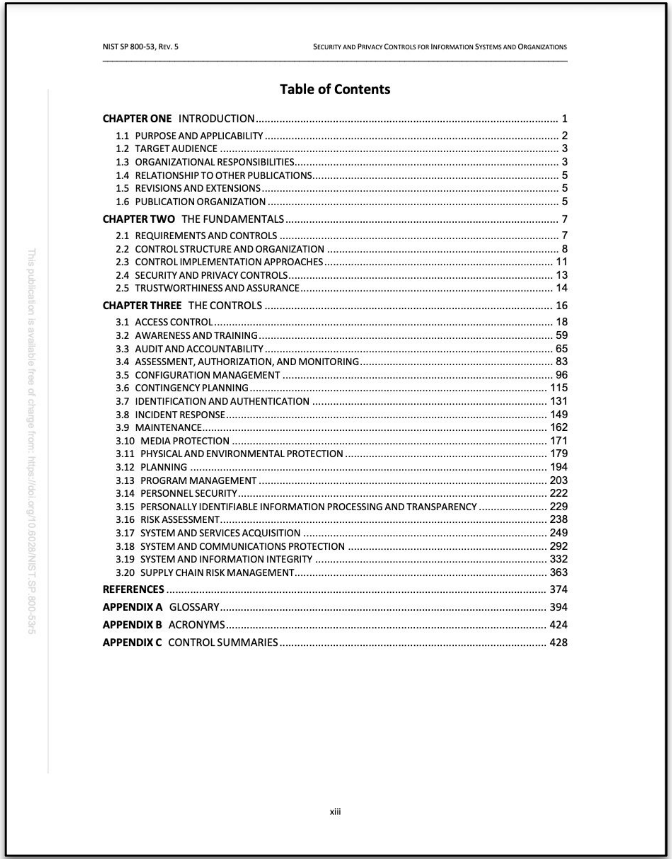
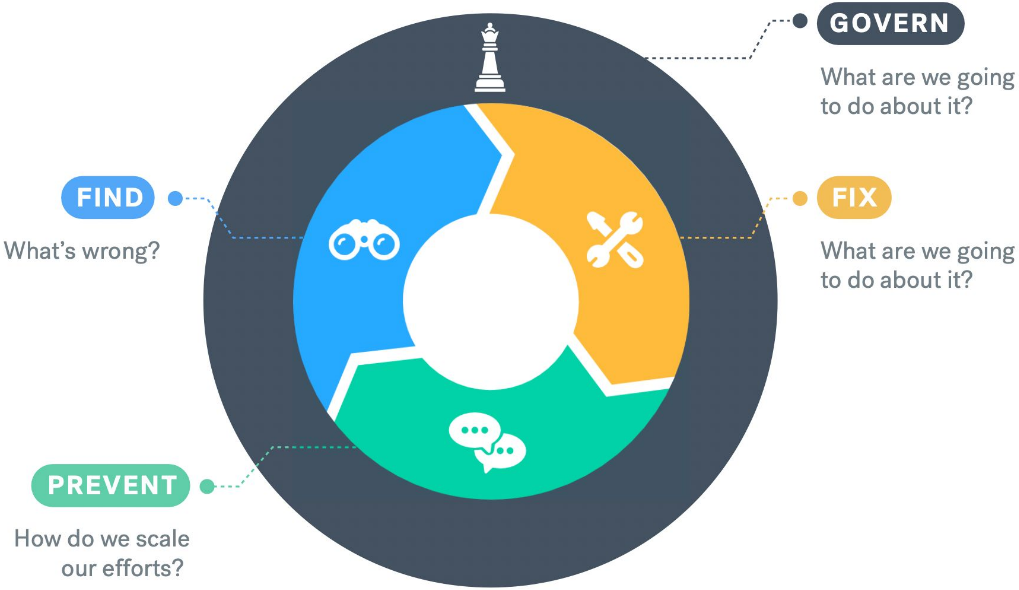


Table of Contents

The Modern AppSec Framework



GOVERN
What are we going to do about it?
FIND
What's wrong?
FIX
What are we going to do about it?
PREVENT
How do we scale our efforts?

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.

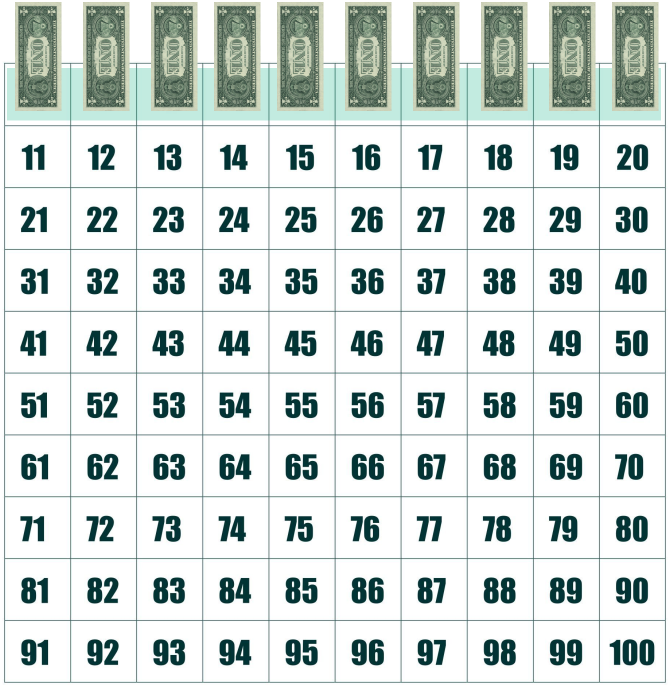
Risk Management Objectives: Internally Driven

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

Budget-driven “risk management”



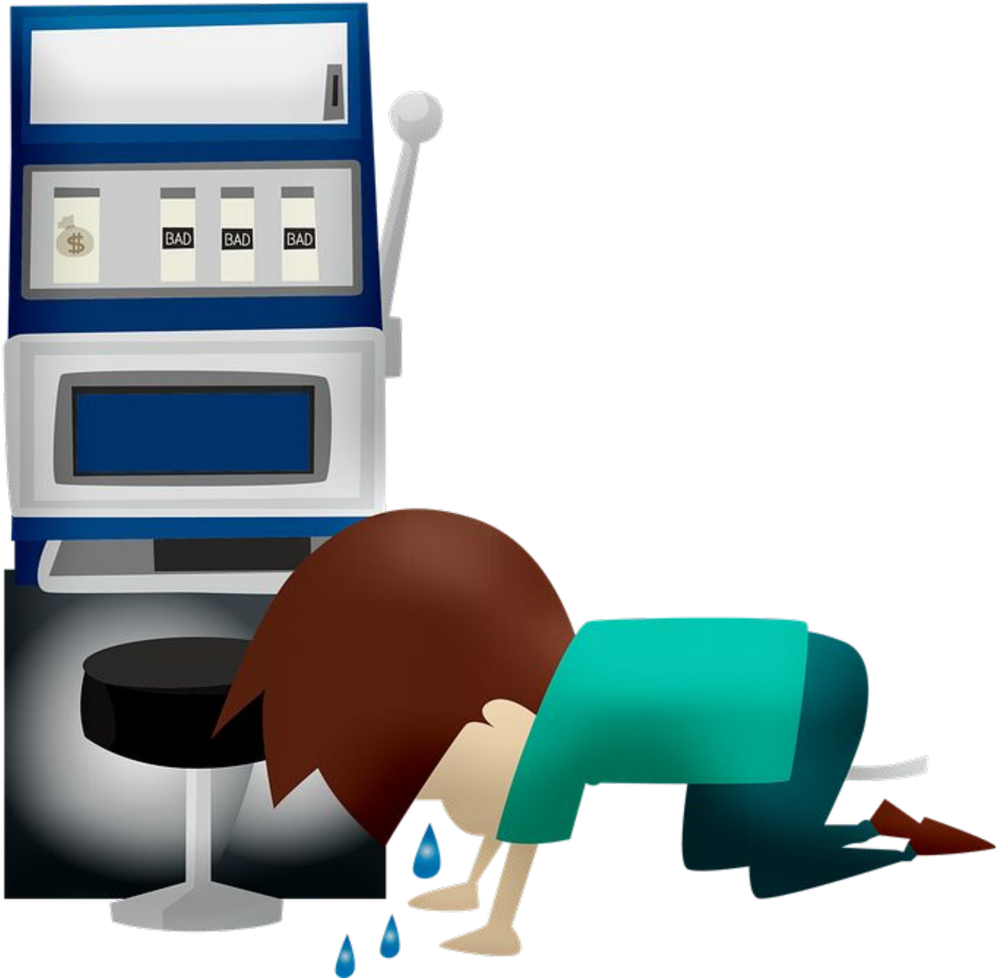
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2013 - 2016

Sorry, you’re out of luck.

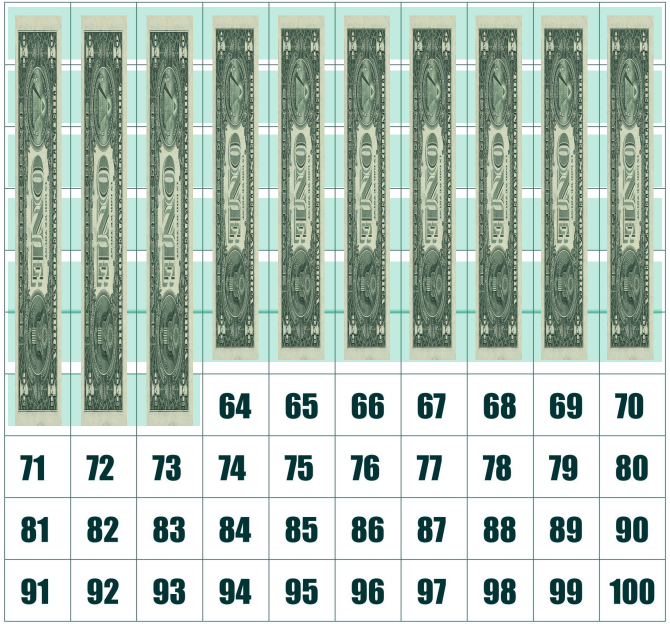
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL
SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL	SOL

2013 - 2016



BAD
BAD
BAD
$

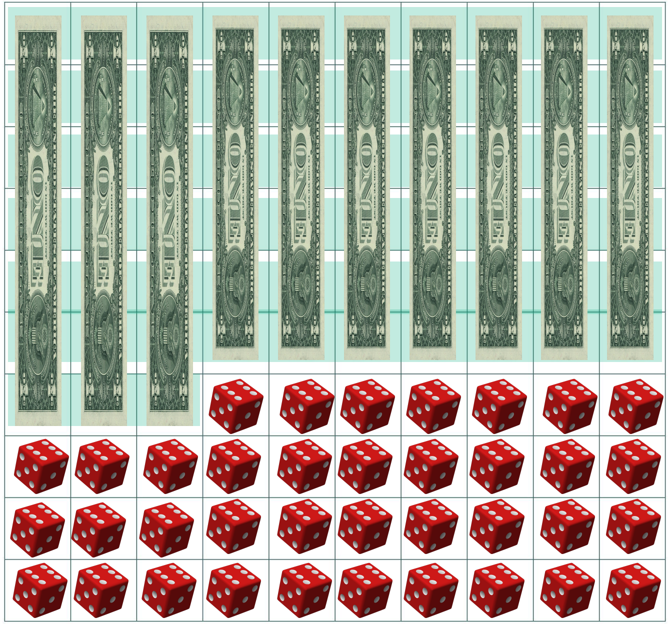
Our odds might be slightly better



			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

But we’re still rolling the dice



2021

Cybersecurity: a decade in review

Cybersecurity: ~~a~~ 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.

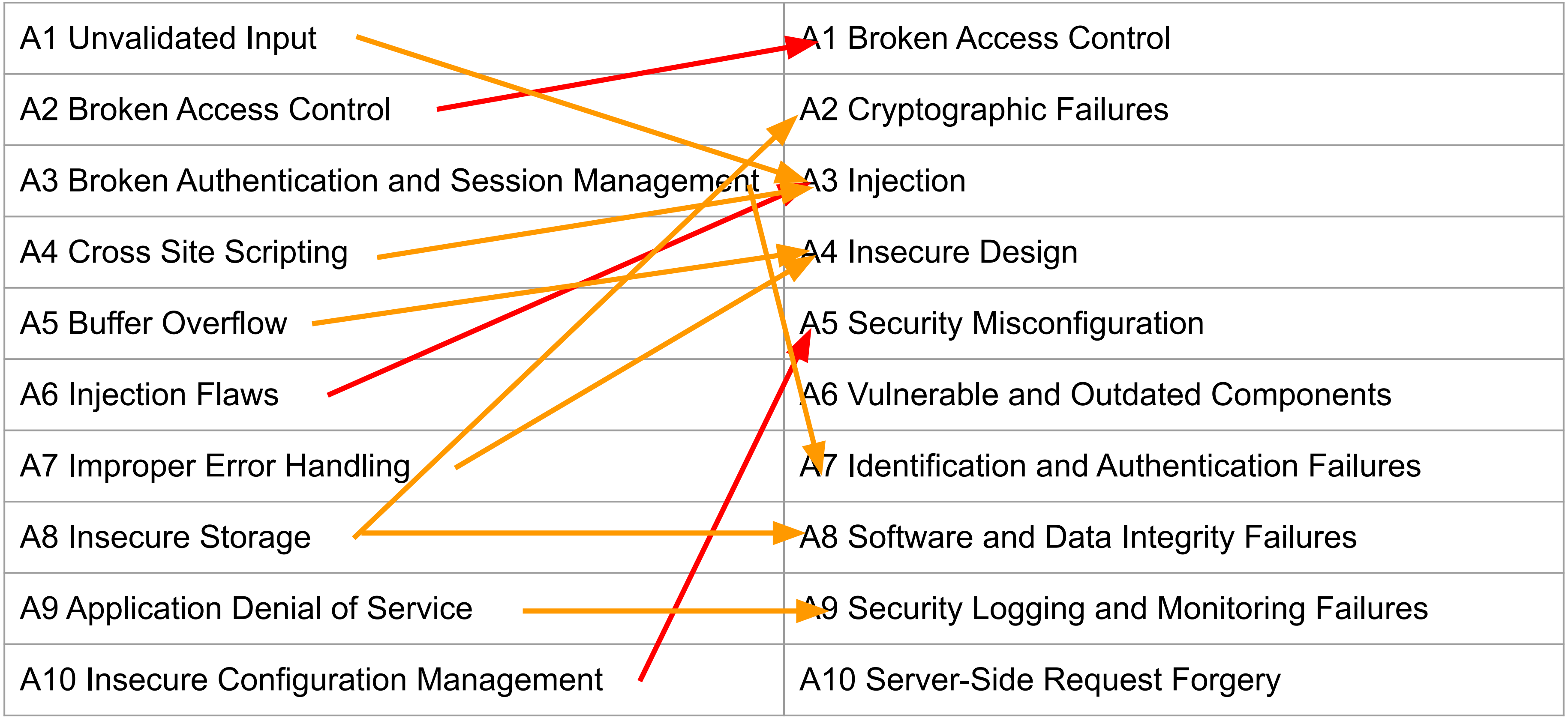
By Derek Hawkins
Reporter

May 23, 2018

with Bastien Inzaurralde

THE KEY

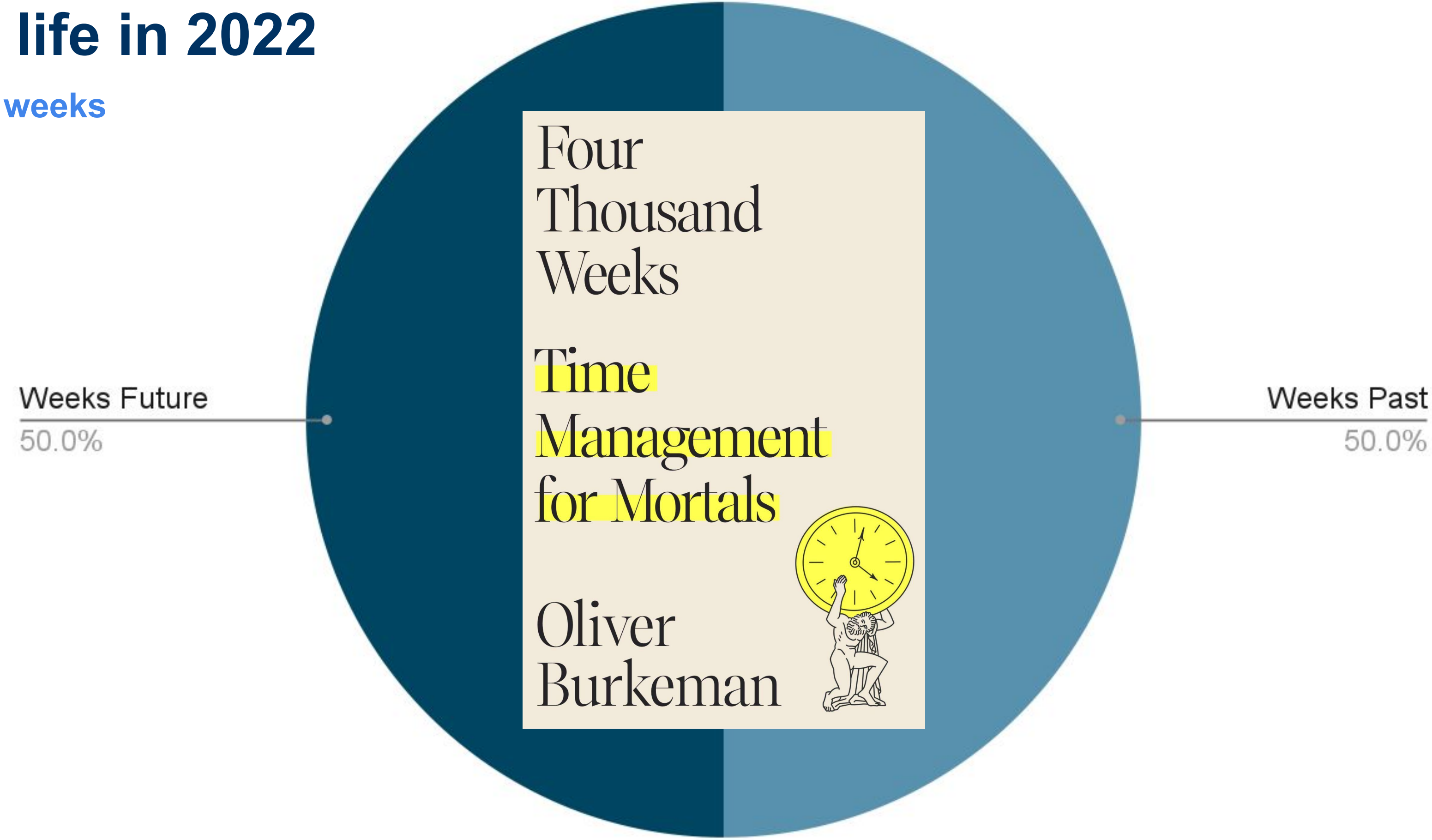
OWASP Top 10: 2003 vs. 2021



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

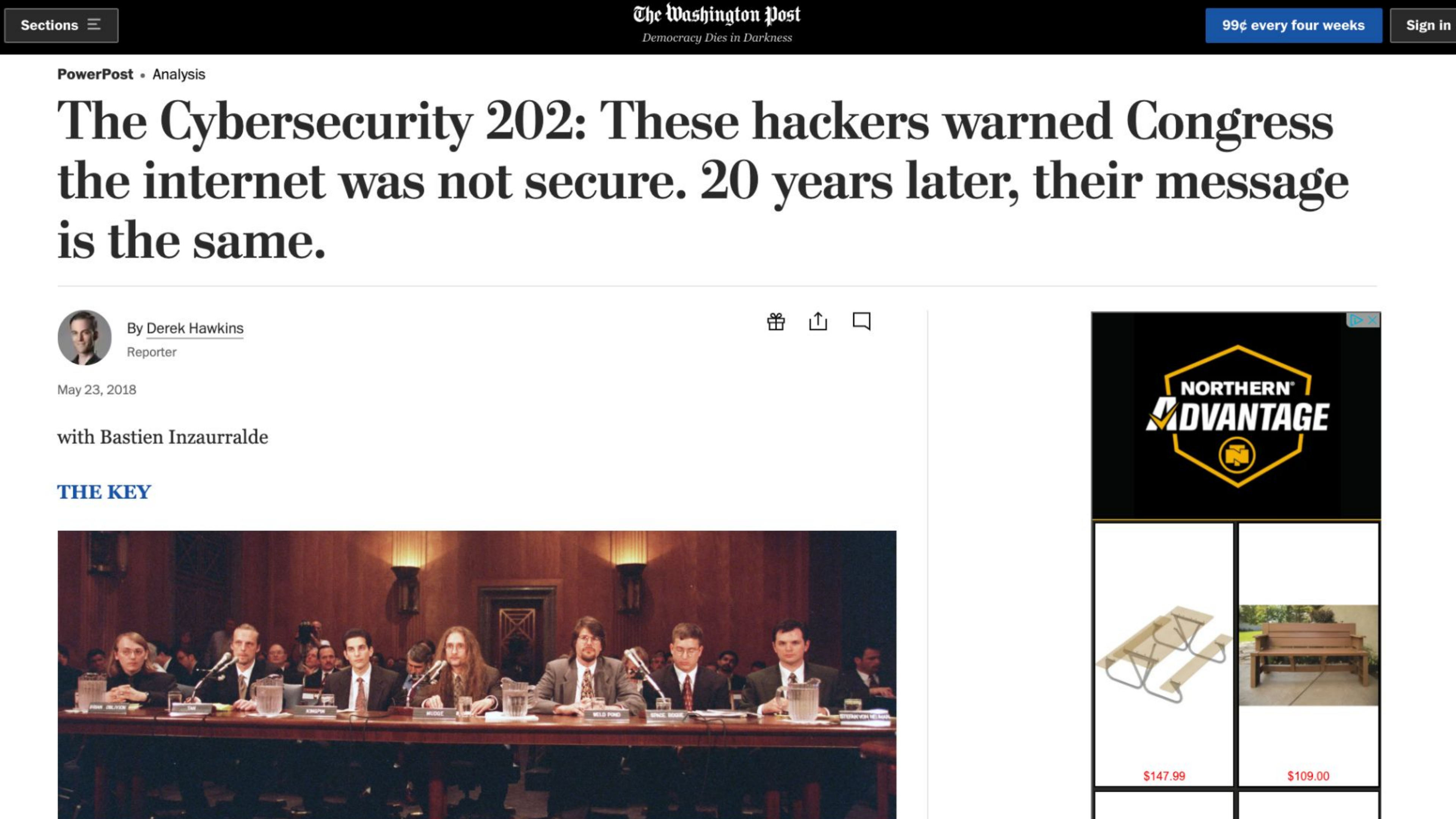
My life in 2022

2000 weeks



Cybersecurity: a decade in review

Cybersecurity: ~~a~~
2 decades in review



The Washington Post
Democracy Dies in Darkness

PowerPost • Analysis

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

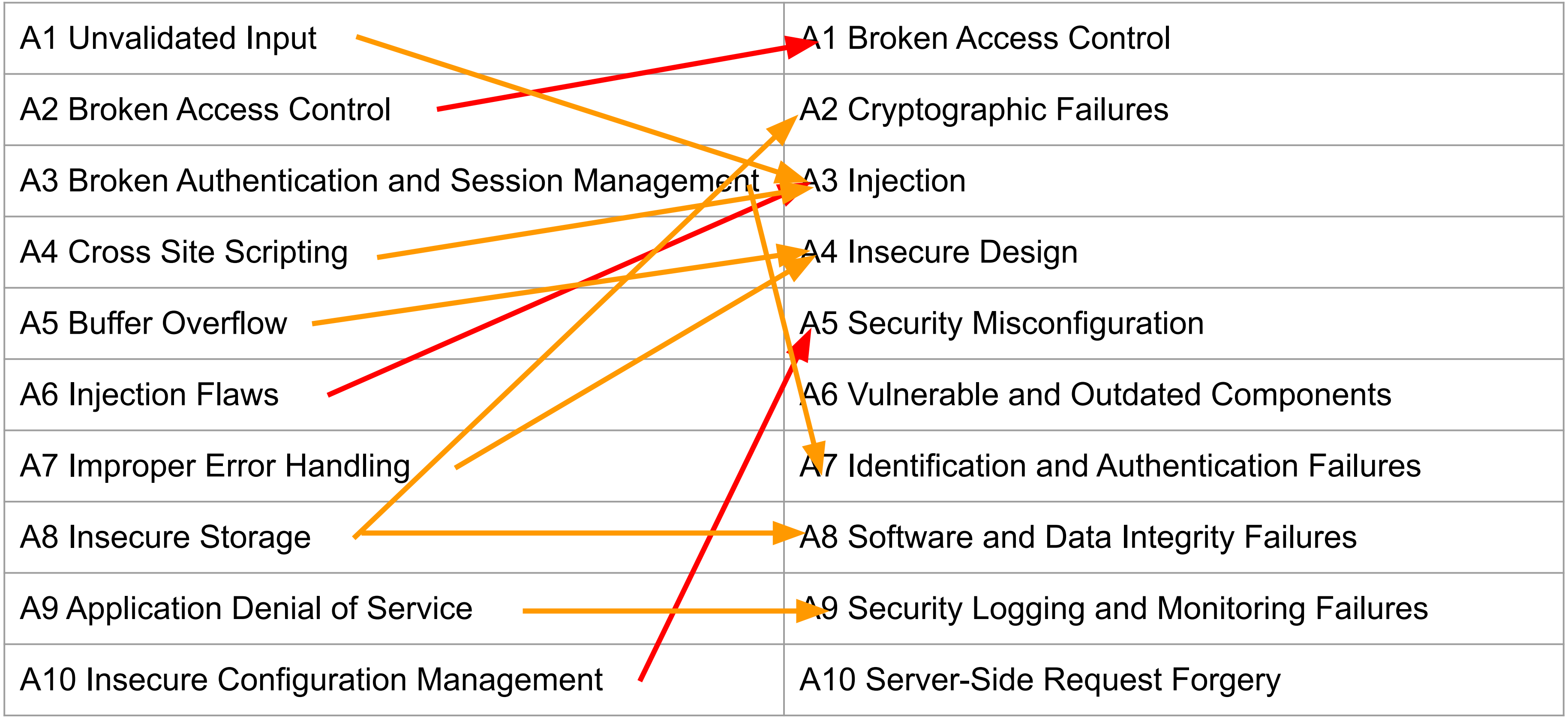
By Derek Hawkins
Reporter

May 23, 2018

with Bastien Inzaurralde

THE KEY

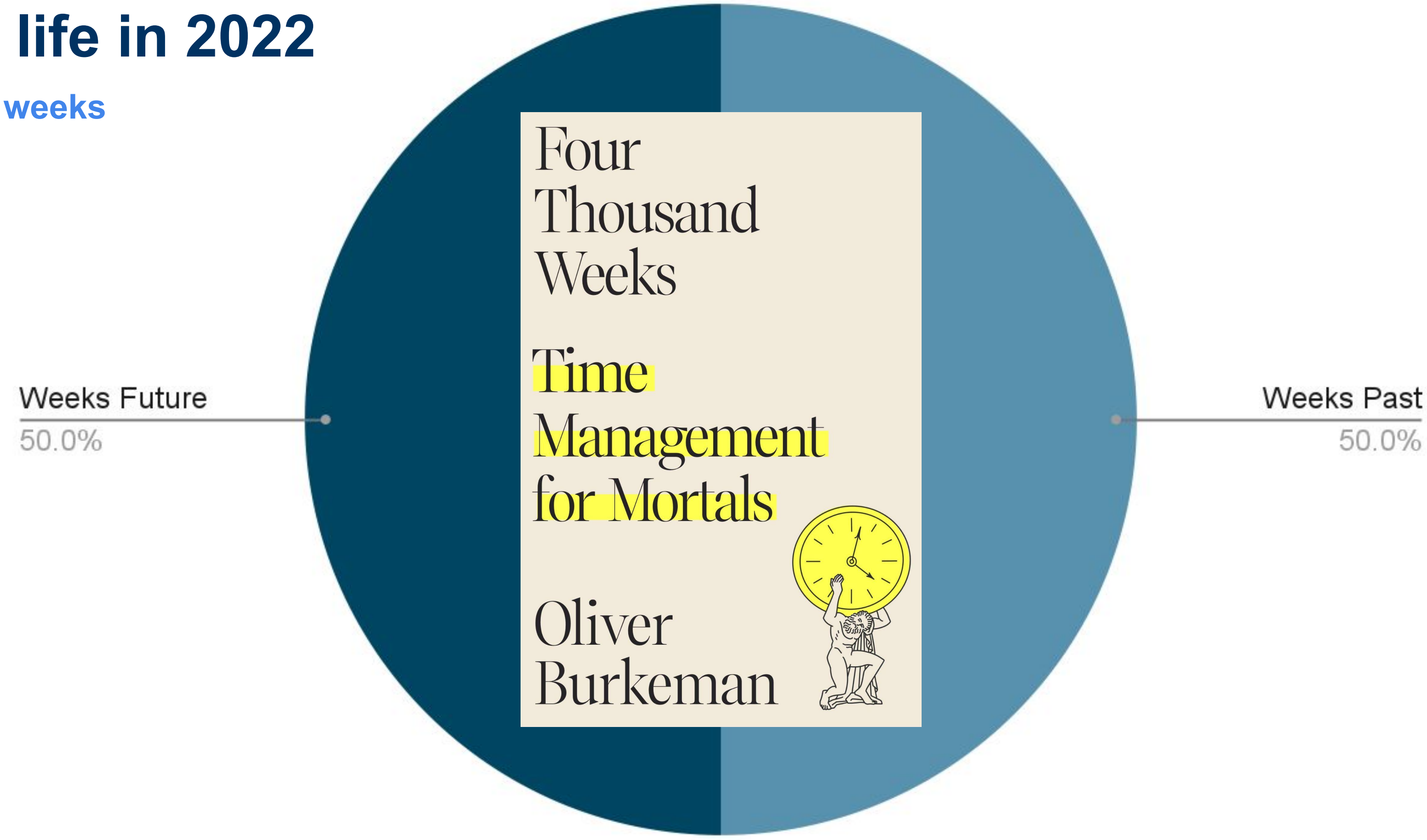
OWASP Top 10: 2003 vs. 2021



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

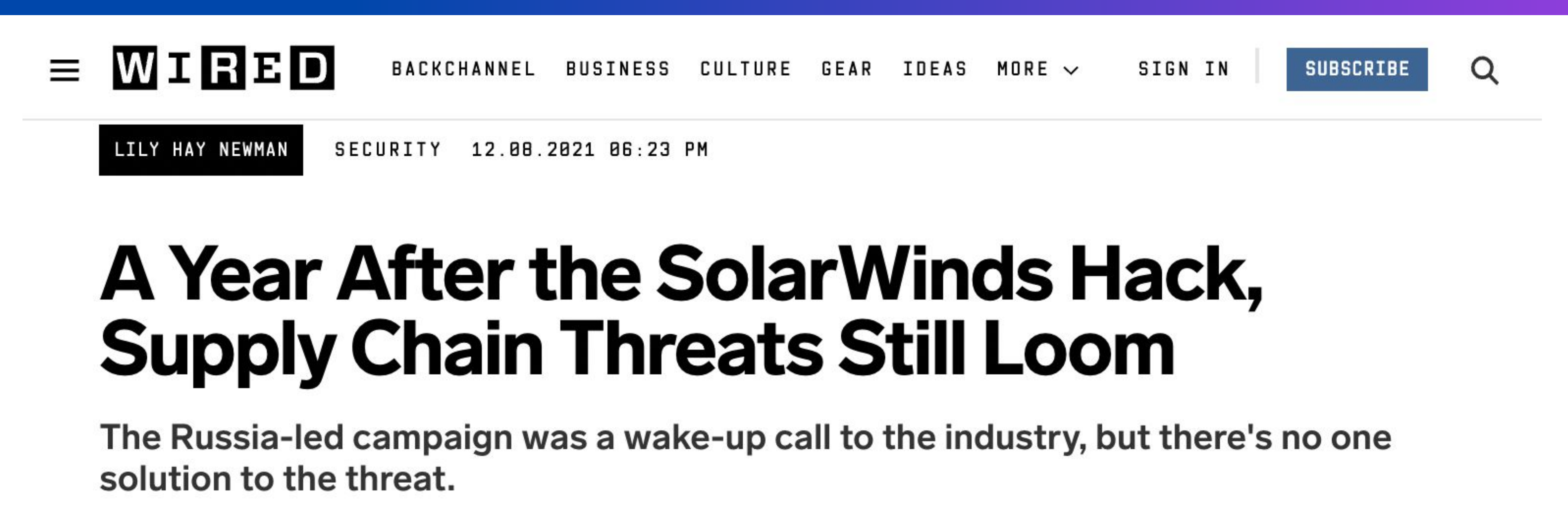


Software development: a decade in review

The case for DevOps remains clear

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

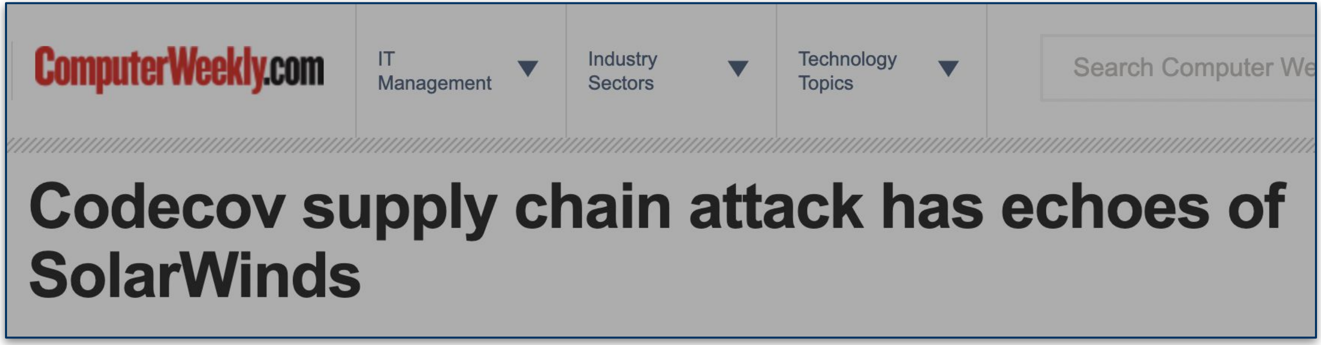
	Low	Mid	High
Deployment frequency	Monthly or less often	Between daily and weekly	On demand (whenever we want)
Lead time for changes	Between a week and 6 months	Less than a week	Less than an hour
MTTR	Less than a week	Less than a day	Less than an hour
Change failure rate	Less than 15%	Less than 15%	Less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



LILY HAY NEWMAN SECURITY 12.08.2021 06:23 PM

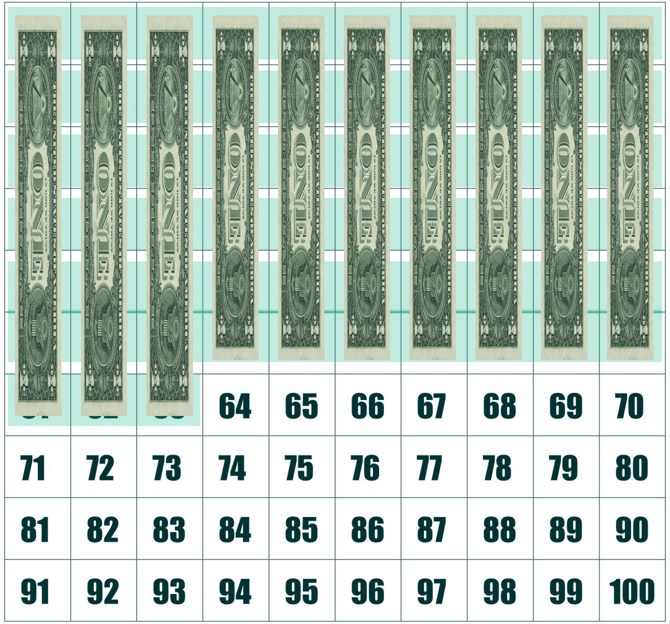
A Year After the SolarWinds Hack, Supply Chain Threats Still Loom

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



Codecov supply chain attack has echoes of SolarWinds

State of DevOps 2021



2021

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

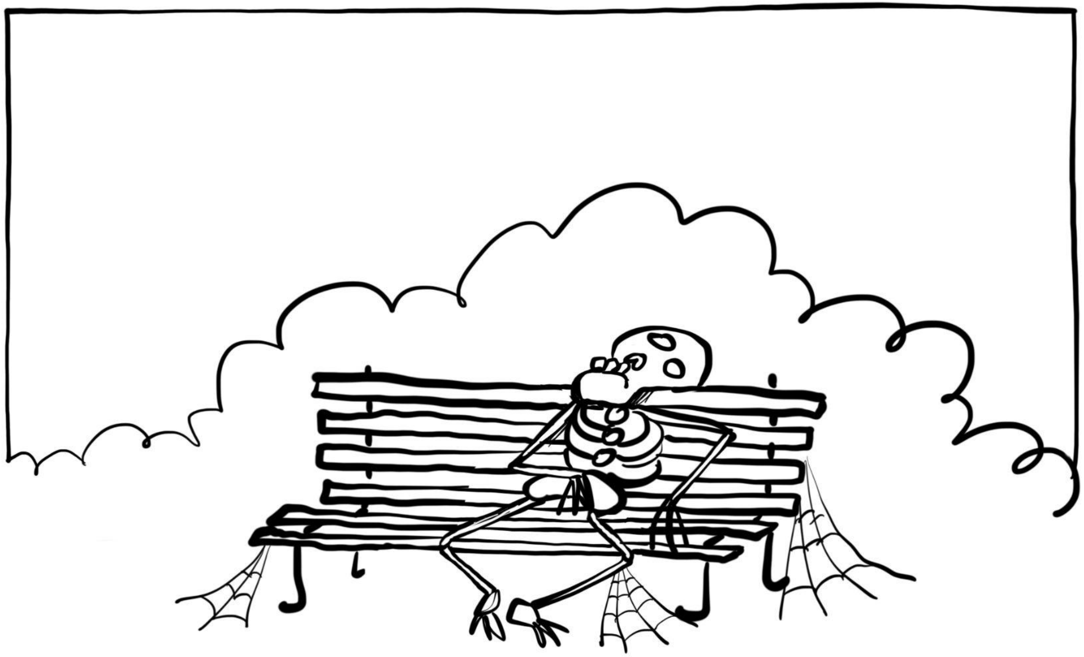
Pentesting Maturity Model

	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

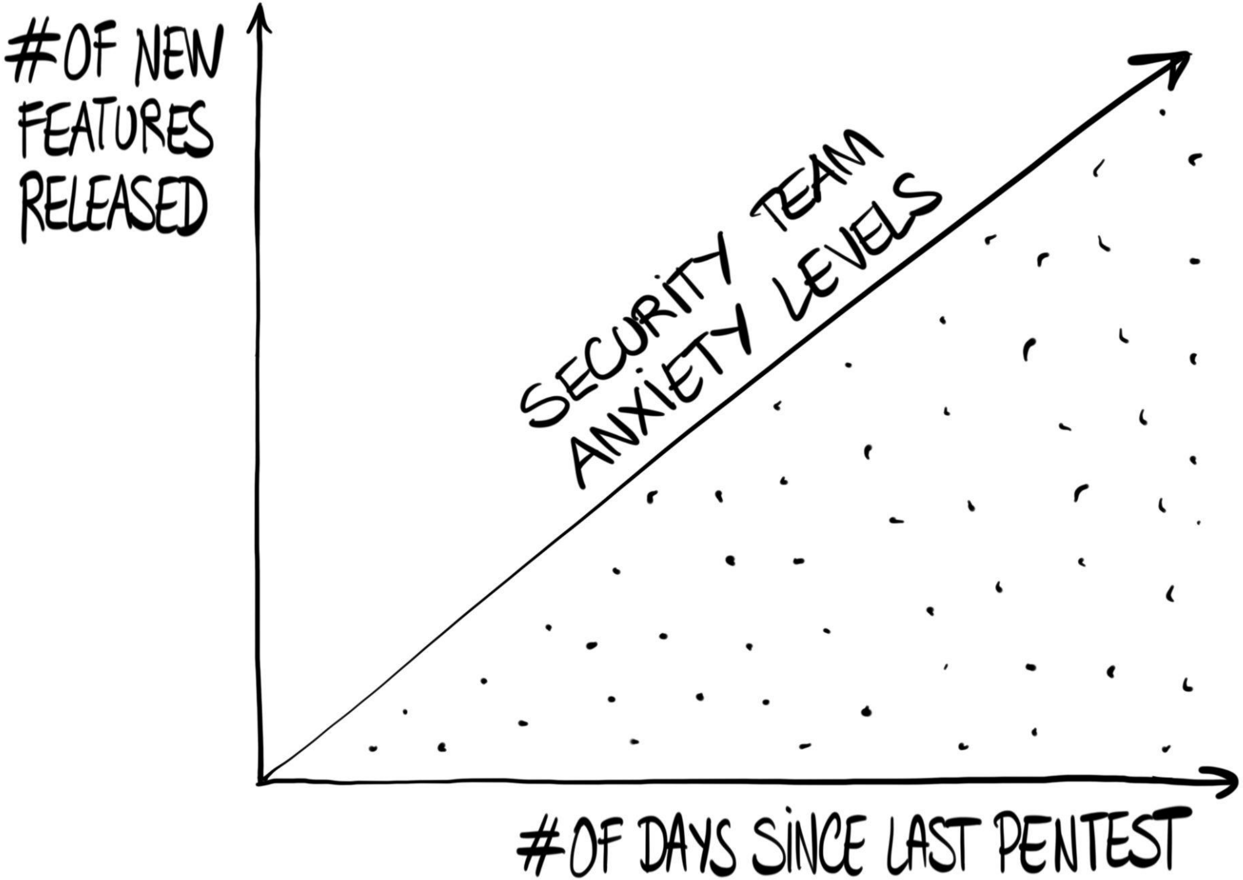
Pentesting Maturity Model

	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

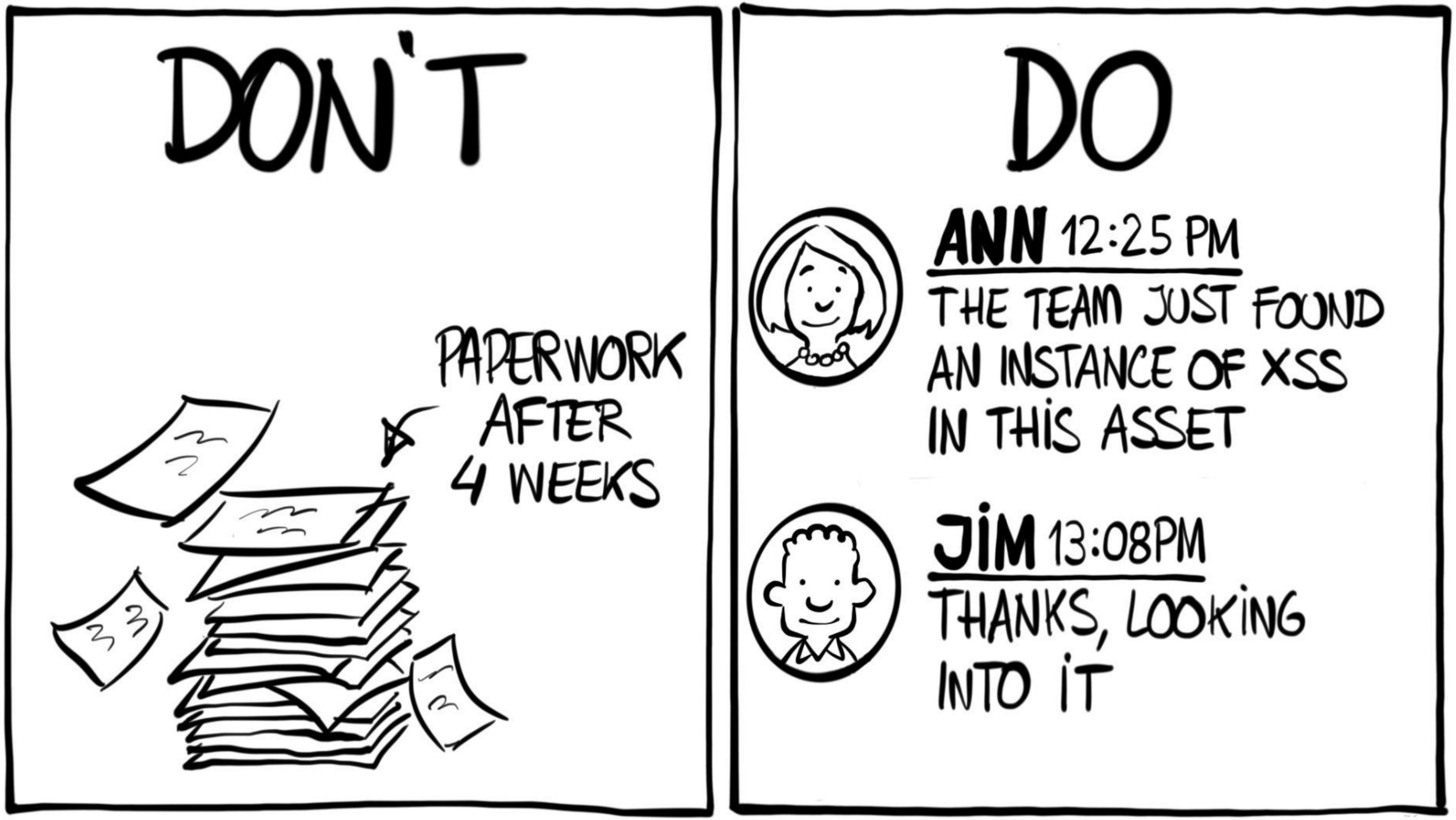
How to Scale Pentesting:
Do It Faster and More Often



WAITING FOR MY PENTEST TO START.


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

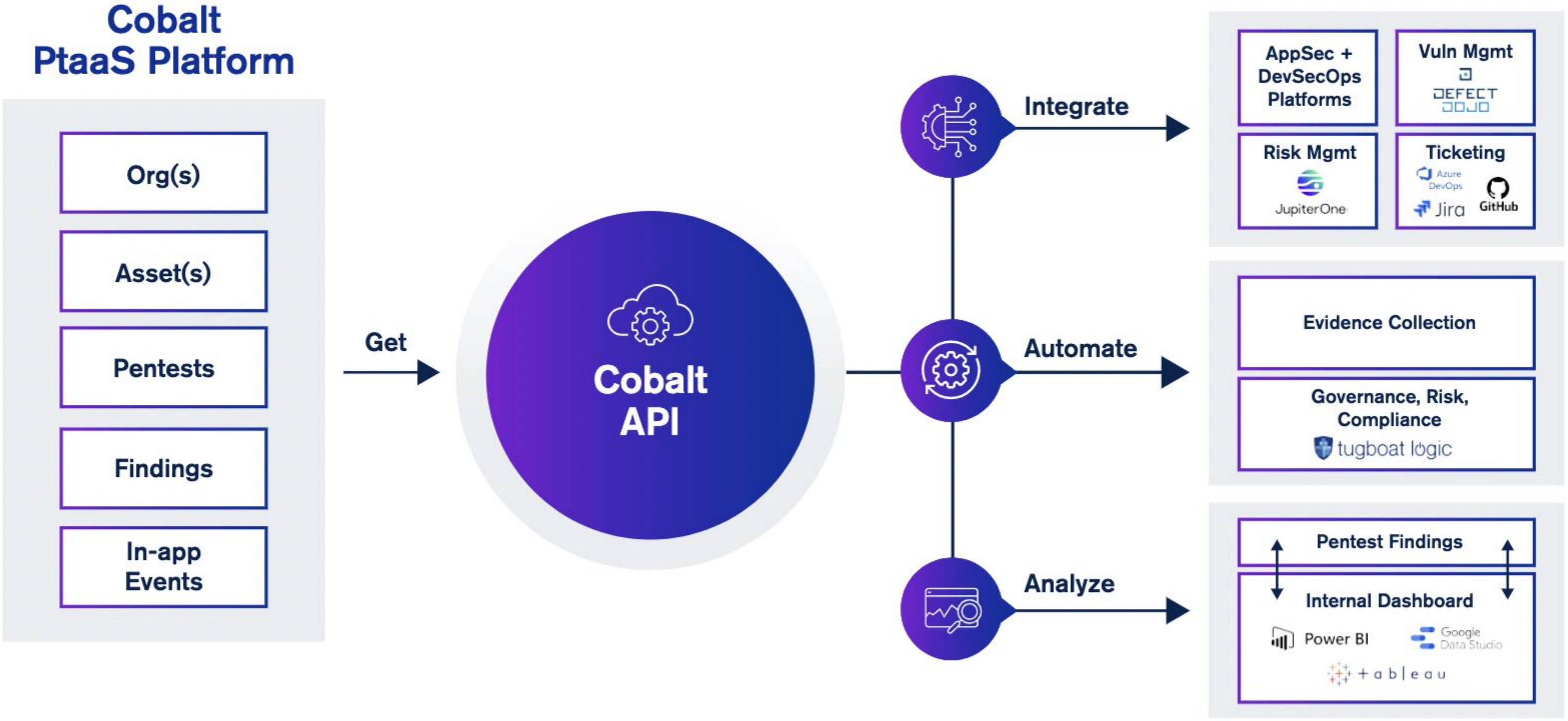
How to Scale Pentesting: **Remediate Risk Smarter**



TIMELY SHARING OF FINDINGS

How to Scale Pentesting: **Use Data to Make Security Stronger**

API + Integrations: A Data Driven Approach



Cobalt PtaaS Platform

- Org(s)
- Asset(s)
- Pentests
- Findings
- In-app Events

Get

Cobalt API

Integrate

- AppSec + DevSecOps Platforms
- Vuln Mgmt: DEFECT DOJO
- Risk Mgmt: JupiterOne
- Ticketing: Azure DevOps, Jira, GitHub

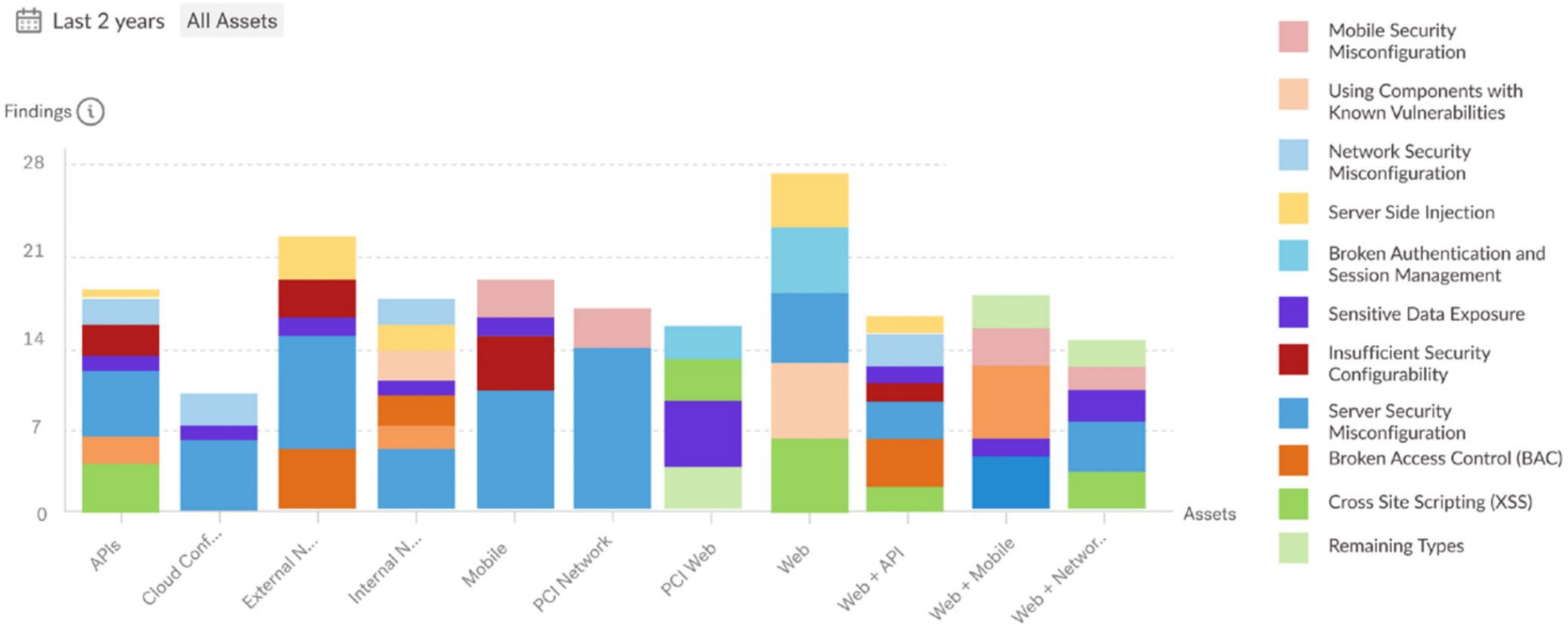
Automate

- Evidence Collection
- Governance, Risk, Compliance: tugboat logic

Analyze

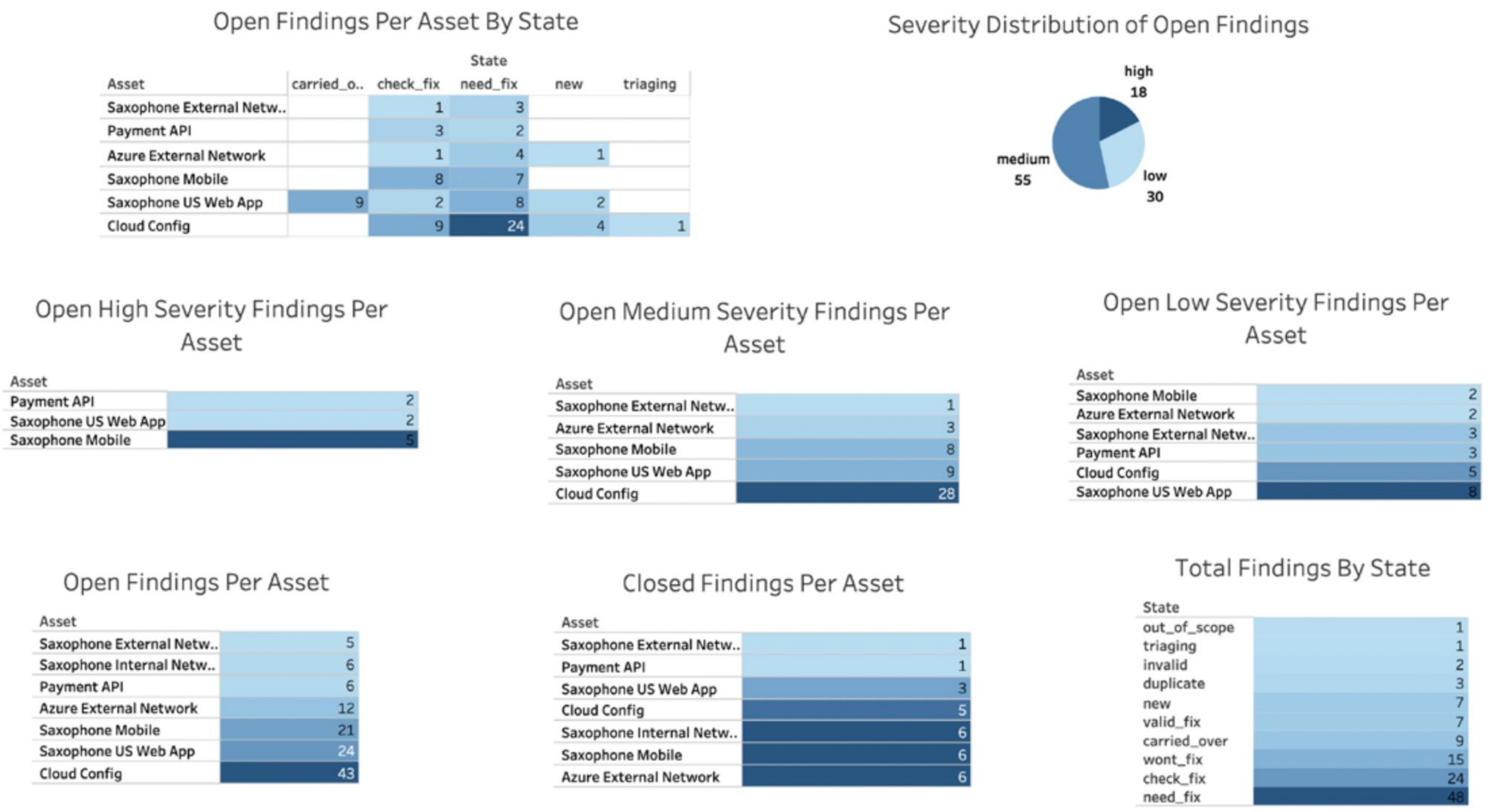
- Pentest Findings
- Internal Dashboard: Power BI, Google Data Studio, tableau

All Findings by Type



Last 2 years All Assets

Findings Overview



Open Findings Per Asset By State

	State				
Asset	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

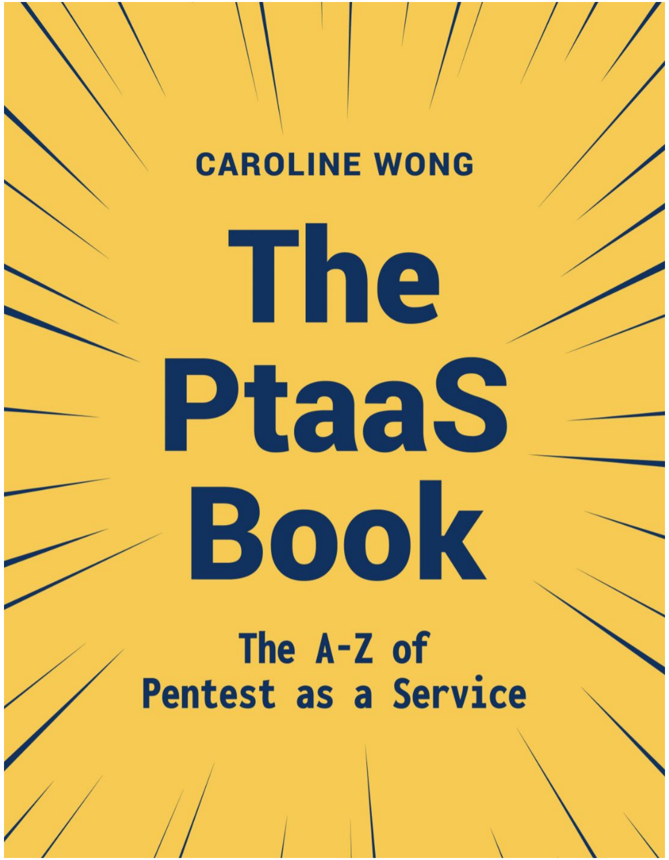
The First Ideal: Locality and Simplicity

The Second Ideal: Focus, Flow, and Joy

The Third Ideal: Improvement of Daily Work

The Fourth Ideal: Psychological Safety

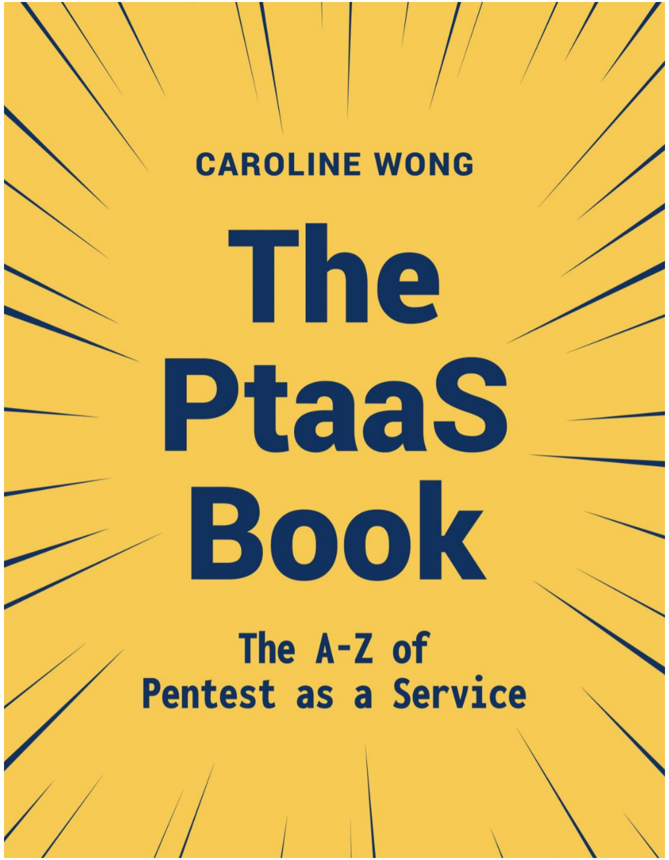
The Fifth Ideal: Customer Focus



CAROLINE WONG

The PtaaS Book

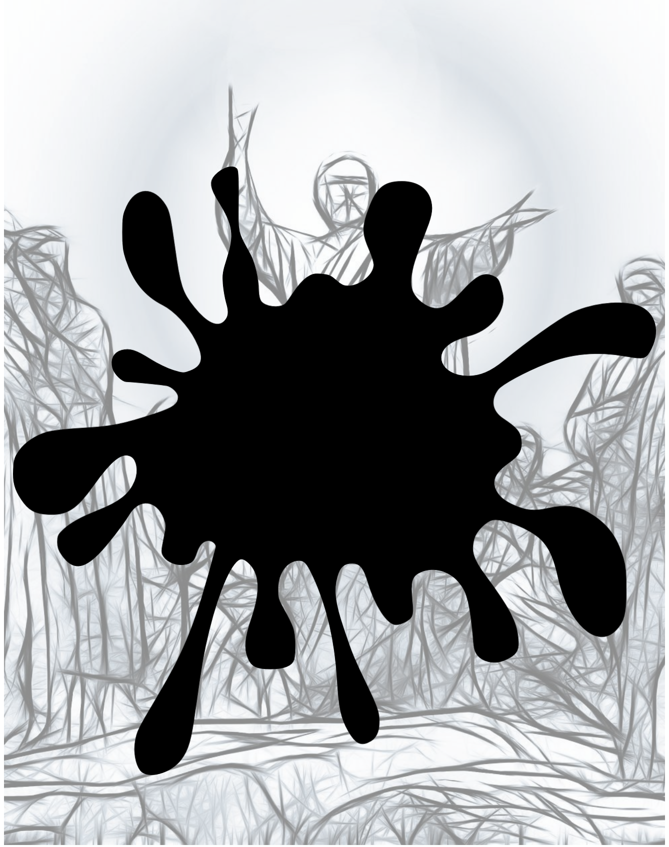
The A-Z of Pentest as a Service

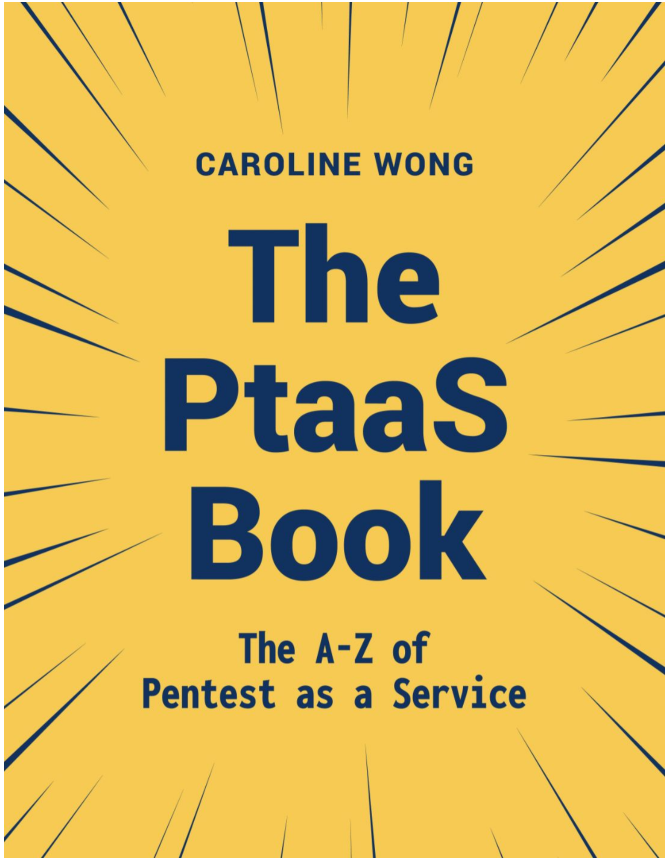


CAROLINE WONG

The PtaaS Book

The A-Z of Pentest as a Service





CAROLINE WONG

The PtaaS Book

The A-Z of Pentest as a Service

Ransomware payment in 1989

$189

Ransomware payment in 2021

$500,000

DOT

Let’s talk some more.

Caroline Wong

caroline@cobalt.io

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