The Making Of The OWASP Top Ten 2025

OWASP 2025 GLOBAL AppSec | USA

Brian Glas

The OWASP Top Ten 2025

A01:2025 Broken Access Control

A02:2025 Security Misconfiguration

A03:2025 Software Supply Chain Failures

A04:2025 Cryptographic Failures

A05:2025 Injection

A06:2025 Insecure Design

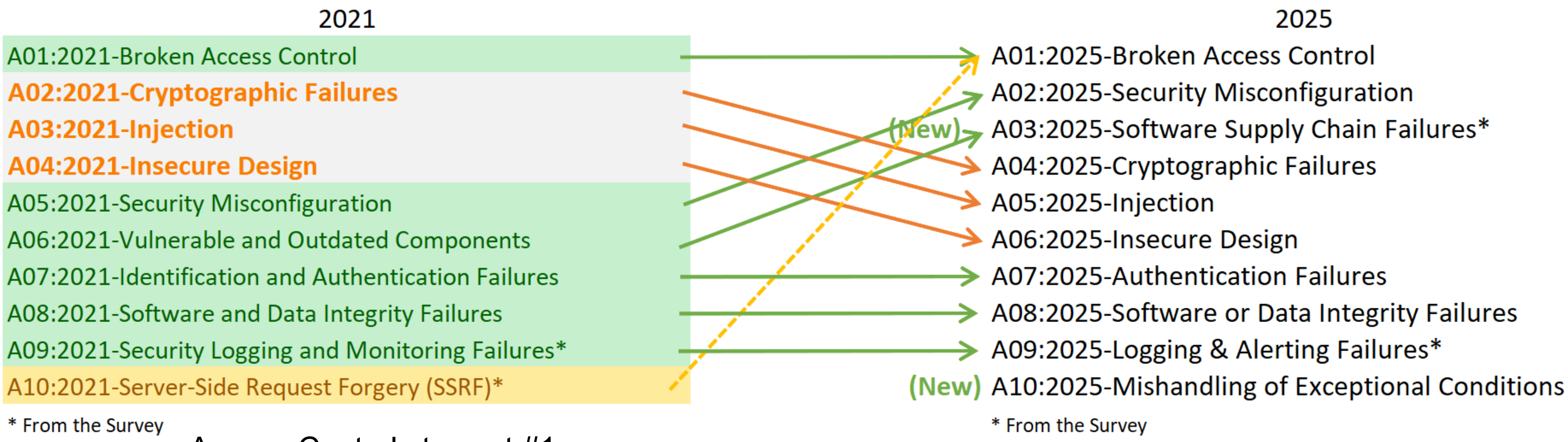
A07:2025 Authentication Failures

A08:2025 Software or Data Integrity Failures

A09:2025 Logging & Alerting Failures

A10:2025 Mishandling of Exceptional Conditions

The Changes



2021

A01:2021-Broken Access Control

A02:2021-Cryptographic Failures

A03:2021-Injection

A04:2021-Insecure Design

A05:2021-Security Misconfiguration

A06:2021-Vulnerable and Outdated Components

A07:2021-Identification and Authentication Failures

A08:2021-Software and Data Integrity Failures

A09:2021-Security Logging and Monitoring Failures*

A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

2025

A01:2025-Broken Access Control

A02:2025-Security Misconfiguration

(New) A03:2025-Software Supply Chain Failures*

A04:2025-Cryptographic Failures

A05:2025-Injection

A06:2025-Insecure Design

A07:2025-Authentication Failures

A08:2025-Software or Data Integrity Failures

A09:2025-Logging & Alerting Failures*

(New) A10:2025-Mishandling of Exceptional Conditions

* From the Survey

- Access Control stays at #1
- Security Misconfiguration goes from 5 -> 2 (data score)
- Software Supply Chain goes from 6 -> 3 (data was 10th, but survey was 1st)
- Cryptographic Failures goes from 2 -> 4 (data score is 3)
- Injection goes from 3 -> 5 (data was 4th)
- Insecure Design goes from 4 -> 6 (data was 6th)
- Authentication stays at 7th (data was 5th)
- Software and Data Integrity Failures stays at 8th (data was 9th, survey was 2nd)
- Logging & Alerting Failures stays at 9th (data was 11th, survey was 3rd)
- Mishandling of Exceptional Conditions is added at 10th (data was 7th, but survey was 5th)

The History

2003

A1-Unvalidated Parameters
A2-Broken Access Control
A3-Broken Account and Session Management
A4-Cross Site Scripting (XSS) Flaws
A5-Buffer Overflows
A6-Command Injection Flaws
A7-Error Handling Problems
A8-Insecure Use of Cryptography
A9-Remote Administration Flaws
A10-Web and Application Server Misconfiguration

2004

A1-Unvalidated Input
A2-Broken Access Control
A3-Broken Authentication and Session Management
A4-Cross Site Scripting (XSS) Flaws
A5-Buffer Overflows
A6-Injection Flaws
A7-Improper Error Handling
A8-Insecure Storage
A9-Denial of Service
A10-Insecure Configuration Management

2007

A1-Cross Site Scripting (XSS)
A2-Injection Flaws
A3-Malicious File Execution
A4-Insecure Direct Object Reference
A5-Cross Site Request Forgery (CSRF)
A6-Information Leakage and Improper Error Handling
A7-Broken Authentication and Session Management
A8-Insecure Cryptographic Storage
A9-Insecure Communications
A10-Failure to Restrict URL Access

2010

A1-Injection
A2-Cross-Site Scripting (XSS)
A3-Broken Authentication and Session Management
A4-Insecure Direct Object References
A5-Cross-Site Request Forgery (CSRF)
A6-Security Misconfiguration
A7-Insecure Cryptographic Storage
A8-Failure to Restrict URL Access
A9-Insufficient Transport Layer Protection
A10-Unvalidated Redirects and Forwards

2013

A1-Injection
A2-Broken Authentication and Session Management
A3-Cross-Site Scripting (XSS)
A4-Insecure Direct Object References
A5-Security Misconfiguration
A6-Sensitive Data Exposure
A7-Missing Function Level Access Control
A8-Cross-Site Request Forgery (CSRF)
A9-Using Components with Known Vulnerabilities
A10-Unvalidated Redirects and Forwards

2017

A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilitie
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

2025

A01:2025-Broken Access Control
A02:2025-Security Misconfiguration
A03:2025-Software Supply Chain Failures*
A04:2025-Cryptographic Failures
A05:2025-Injection
A06:2025-Insecure Design
A07:2025-Authentication Failures
A08:2025-Software or Data Integrity Failures
A09:2025-Logging & Alerting Failures*
A10:2025-Mishandling of Exceptional Conditions

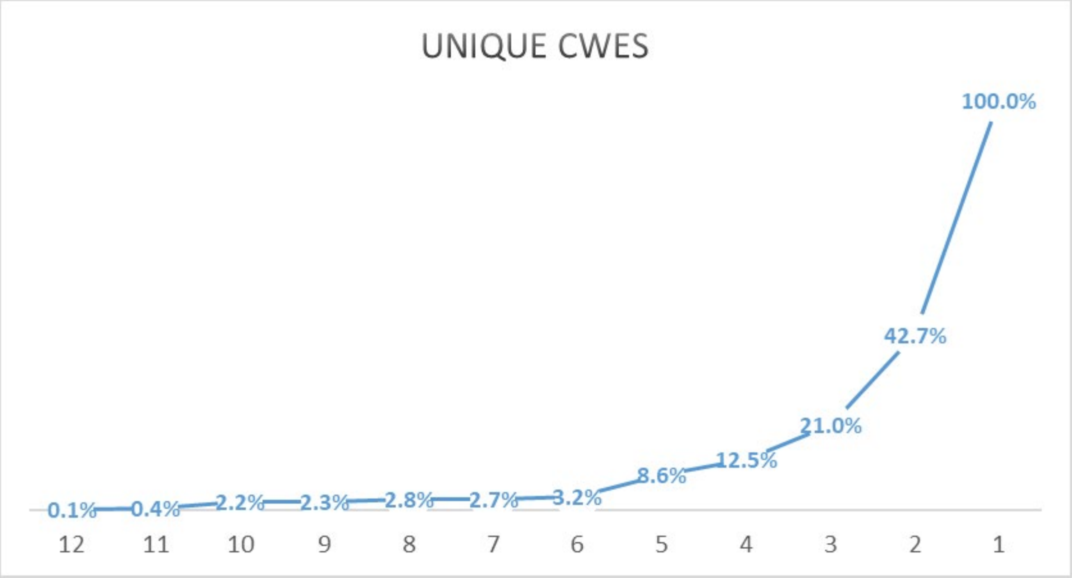
High Level Process

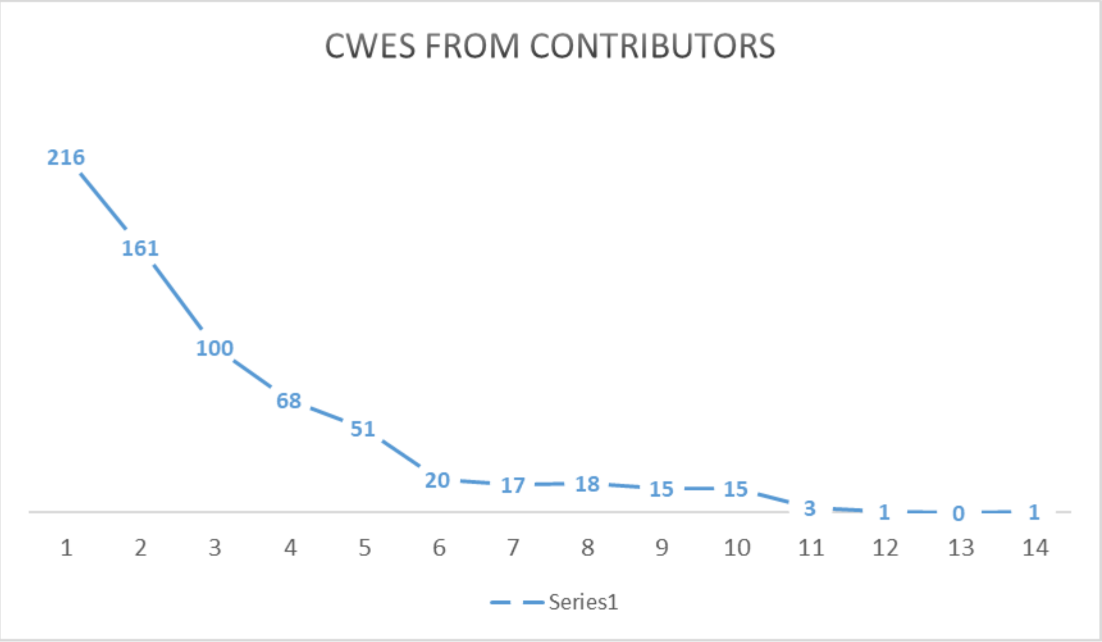
- We ask for data... **It takes 14-16 months**
- Normalize the data
- Pull National Vulnerability Database for CVE -> CWE
- Normalize Exploit and Impact from CVSS
- Pull the CWE dictionary and group CWEs into logical categories
- Determine the formula weighting
- Build a data Top Ten
- Run Community Survey
- Weigh the survey with the data
- Determine the new Top Ten
- Write a lot, discuss, write more, review, feedback, discuss, release

Data Collection

CWEs (968ish)

- 2017 = 30 CWEs
- 2021 = 390 CWEs
- 2025 = 686 CWEs





- •Accenture (Prague)
- •Anonymous (multiple)
- •Bugcrowd
- •Contrast Security
- •CryptoNet Labs
- •Intuitor SoftTech Services
- •Orca Security
- •Probley
- •Semgrep
- •Sonar
- •usd AG
- •Veracode
- •Wallarm

Data Collection

Contributions

- 2.8 million applications (conservatively)
- Min Data Request
  - Year
  - CWE
  - Population tested
  - Apps found with at least one instance of the CWE

Example: 2021, CWE-89, 1000, 200

Risk

Likelihood x Impact = Risk

Likelihood

Frequency vs Incidence Rate

- Frequency is not our friend in this case
- Tool-assisted Human (TaH) vs Human-assisted Tool (TaH)

How to normalize?

- Epidemiology
- Incidence Rate to determine impact in a population

What percentage of the population of tested apps has the vulnerability?

Likelihood

Incidence Rate: Incidence rate is the percentage of applications vulnerable to that CWE from the population tested by that org for that time period.

(Testing) Coverage: The percentage of applications tested by all organizations for a given CWE.

Total Occurrences: Total number of applications found to have the CWEs mapped to a category.

Impact

Impact

- Can vary wildly
- We use the NVD for Exploit and Impact

NVD Stats

- 219,291 CVEs
  - 159,544 have CVSSv2 scores
  - 156,407 have CVSSv3 scores
  - 6,299 have CVSSv4 scores

Impact

Top 10 CWEs by count of CVE mappings

CWE-79 - Improper Neutralization of Input During

NVD-CWE-Other

NVD-CWE-noinfo

CWE-89 - Improper Neutralization of Special Elem

CWE-119 - Improper Restriction of Operations wi

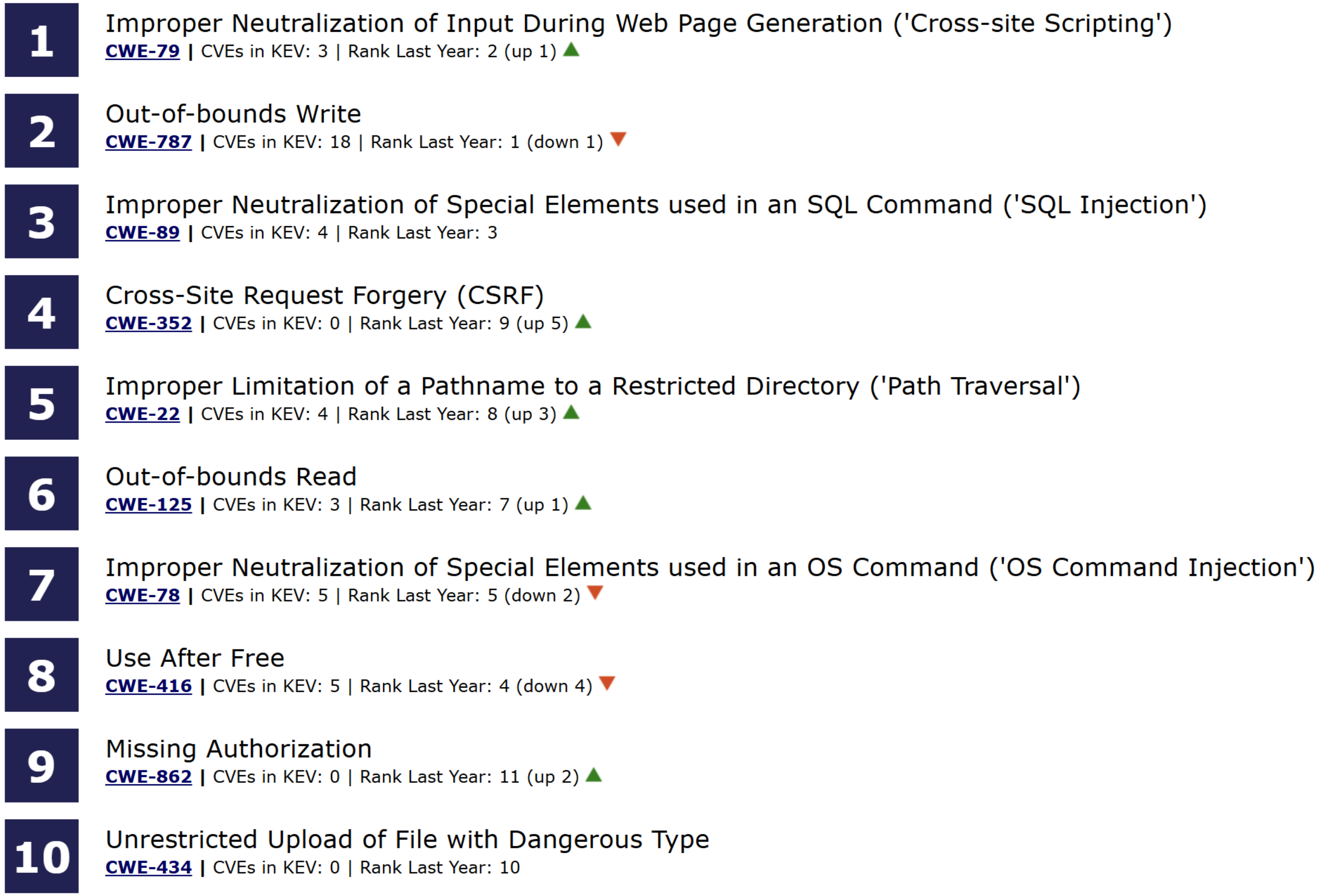
CWE-20 - Improper Input Validation

CWE-787 - Out-of-bounds Write

CWE-200 - Exposure of Sensitive Information to a

CWE-22 - Improper Limitation of a Pathname to a

CWE-352 - Cross-Site Request Forgery (CSRF)



1 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-79 | CVEs in KEV: 3 | Rank Last Year: 2 (up 1) ▲

2 Out-of-bounds Write
CWE-787 | CVEs in KEV: 18 | Rank Last Year: 1 (down 1) ▼

3 Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-89 | CVEs in KEV: 4 | Rank Last Year: 3

4 Cross-Site Request Forgery (CSRF)
CWE-352 | CVEs in KEV: 0 | Rank Last Year: 9 (up 5) ▲

5 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-22 | CVEs in KEV: 4 | Rank Last Year: 8 (up 3) ▲

6 Out-of-bounds Read
CWE-125 | CVEs in KEV: 3 | Rank Last Year: 7 (up 1) ▲

7 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-78 | CVEs in KEV: 5 | Rank Last Year: 5 (down 2) ▼

8 Use After Free
CWE-416 | CVEs in KEV: 5 | Rank Last Year: 4 (down 4) ▼

9 Missing Authorization
CWE-862 | CVEs in KEV: 0 | Rank Last Year: 11 (up 2) ▲

10 Unrestricted Upload of File with Dangerous Type
CWE-434 | CVEs in KEV: 0 | Rank Last Year: 10

Impact

Top 10 CWEs by count of CVE mappings

CWE-125 - Out-of-bounds Read

CWE-264 - **Permissions, Privileges, and Access Con**

CWE-94 - Improper Control of Generation of Code ('Code

CWE-416 - Use After Free

CWE-434 - Unrestricted Upload of File with Dangerous T

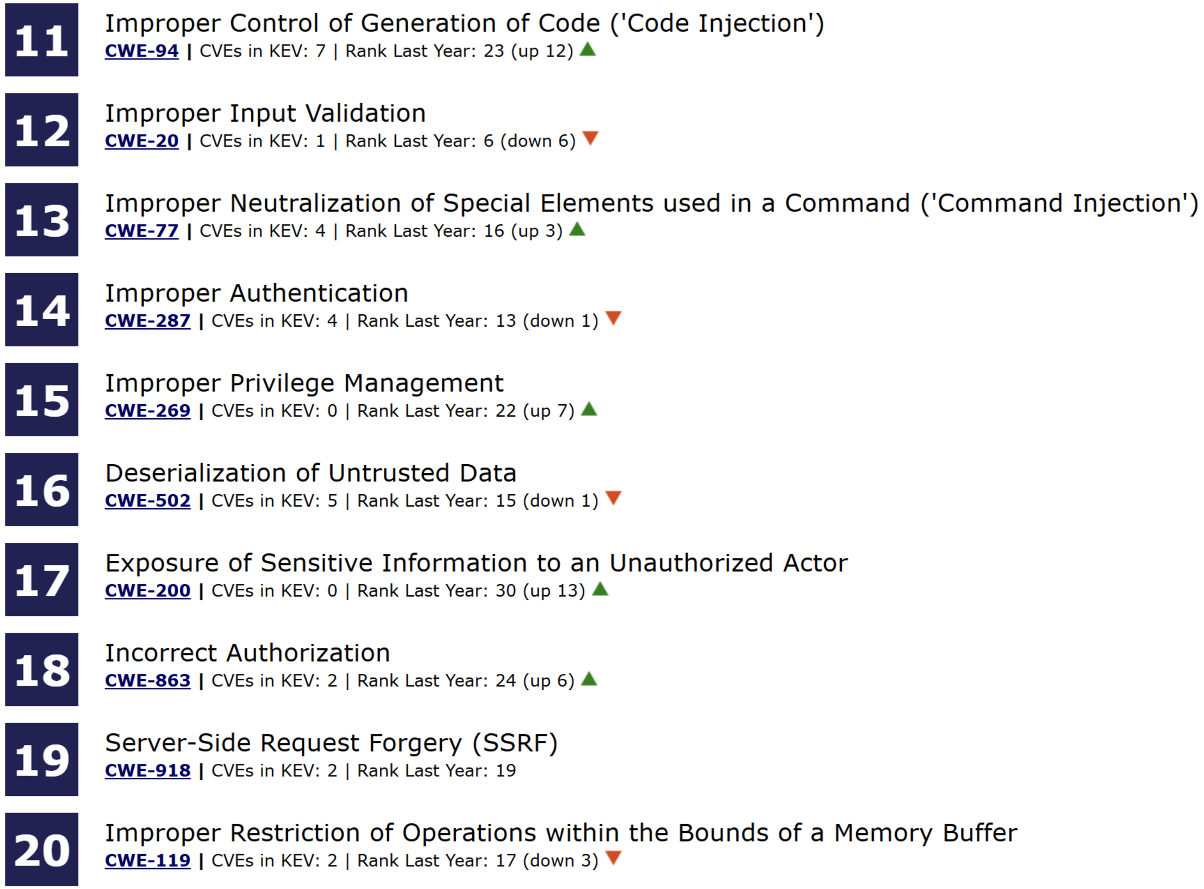
CWE-287 - Improper Authentication

CWE-862 - Premature Release of Resource During Expect

CWE-284 - Improper Access Control

CWE-310 - **Cryptographic Issues (Prohibited)**

CWE-78 - Improper Neutralization of Special Elements us



11 Improper Control of Generation of Code ('Code Injection')
CWE-94 | CVEs in KEV: 7 | Rank Last Year: 23 (up 12) ▲

12 Improper Input Validation
CWE-20 | CVEs in KEV: 1 | Rank Last Year: 6 (down 6) ▼

13 Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-77 | CVEs in KEV: 4 | Rank Last Year: 16 (up 3) ▲

14 Improper Authentication
CWE-287 | CVEs in KEV: 4 | Rank Last Year: 13 (down 1) ▼

15 Improper Privilege Management
CWE-269 | CVEs in KEV: 0 | Rank Last Year: 22 (up 7) ▲

16 Deserialization of Untrusted Data
CWE-502 | CVEs in KEV: 5 | Rank Last Year: 15 (down 1) ▼

17 Exposure of Sensitive Information to an Unauthorized Actor
CWE-200 | CVEs in KEV: 0 | Rank Last Year: 30 (up 13) ▲

18 Incorrect Authorization
CWE-863 | CVEs in KEV: 2 | Rank Last Year: 24 (up 6) ▲

19 Server-Side Request Forgery (SSRF)
CWE-918 | CVEs in KEV: 2 | Rank Last Year: 19

20 Improper Restriction of Operations within the Bounds of a Memory Buffer
CWE-119 | CVEs in KEV: 2 | Rank Last Year: 17 (down 3) ▼

Impact

Weighted Exploit: The Exploit sub-score from CVSSv2 and CVSSv3 scores assigned to CVEs mapped to CWEs, normalized, and placed on a 10-point scale.

Weighted Impact: The Impact sub-score from CVSSv2 and CVSSv3 scores assigned to CVEs mapped to CWEs, normalized, and placed on a 10-point scale.

Total CVEs: Total number of CVEs in the NVD DB that were mapped to the CWEs mapped to a category.

Data Factors

CWEs Mapped: The number of CWEs mapped to a category by the Top Ten team.

Incidence Rate: Incidence rate is the percentage of applications vulnerable to that CWE from the population tested by that org for that time period.

Weighted Exploit: The Exploit sub-score from CVSSv2 and CVSSv3 scores assigned to CVEs mapped to CWEs, normalized, and placed on a 10pt scale.

Weighted Impact: The Impact sub-score from CVSSv2 and CVSSv3 scores assigned to CVEs mapped to CWEs, normalized, and placed on a 10pt scale.

(Testing) Coverage: The percentage of applications tested by all organizations for a given CWE.

Total Occurrences: Total number of applications found to have the CWEs mapped to a category.

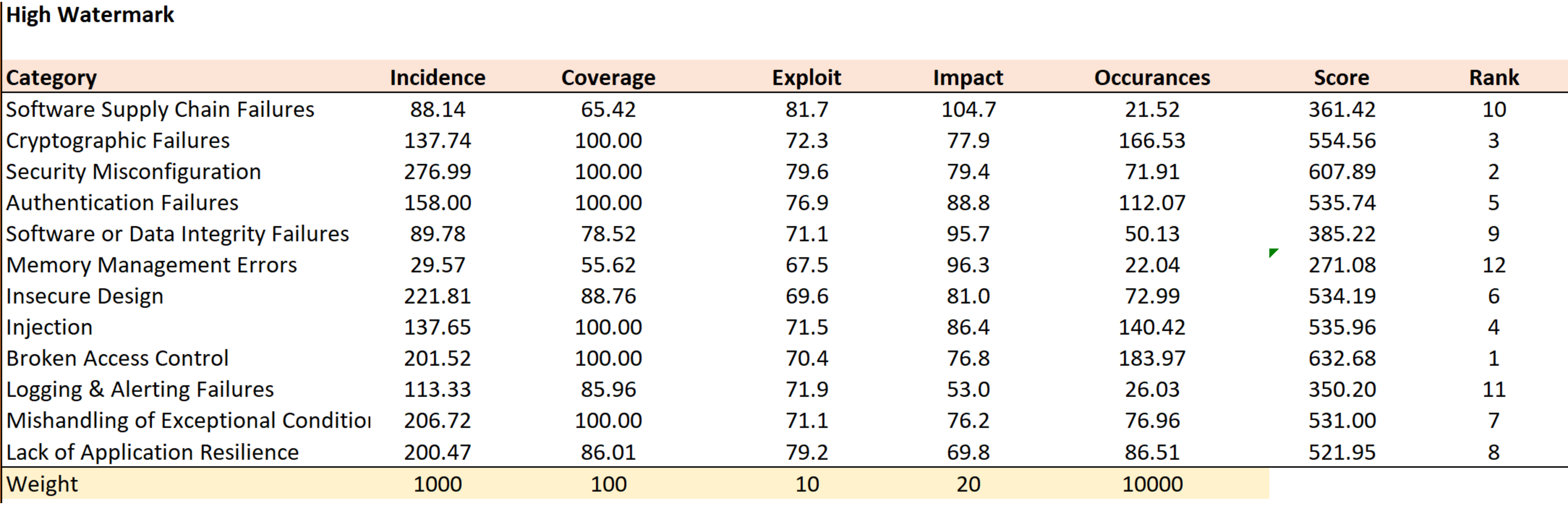
Total CVEs: Total number of CVEs in the NVD DB that were mapped to the CWEs mapped to a category.

Formula: (Max Incidence Rate % * 1000) + (Max Coverage % * 100) + (Avg Exploit * 10) + (Avg Impact * 20) + (Sum Occurrences / 10000) = Risk Score

OWASP 2025 GLOBAL AppSec | USA

TOP 10

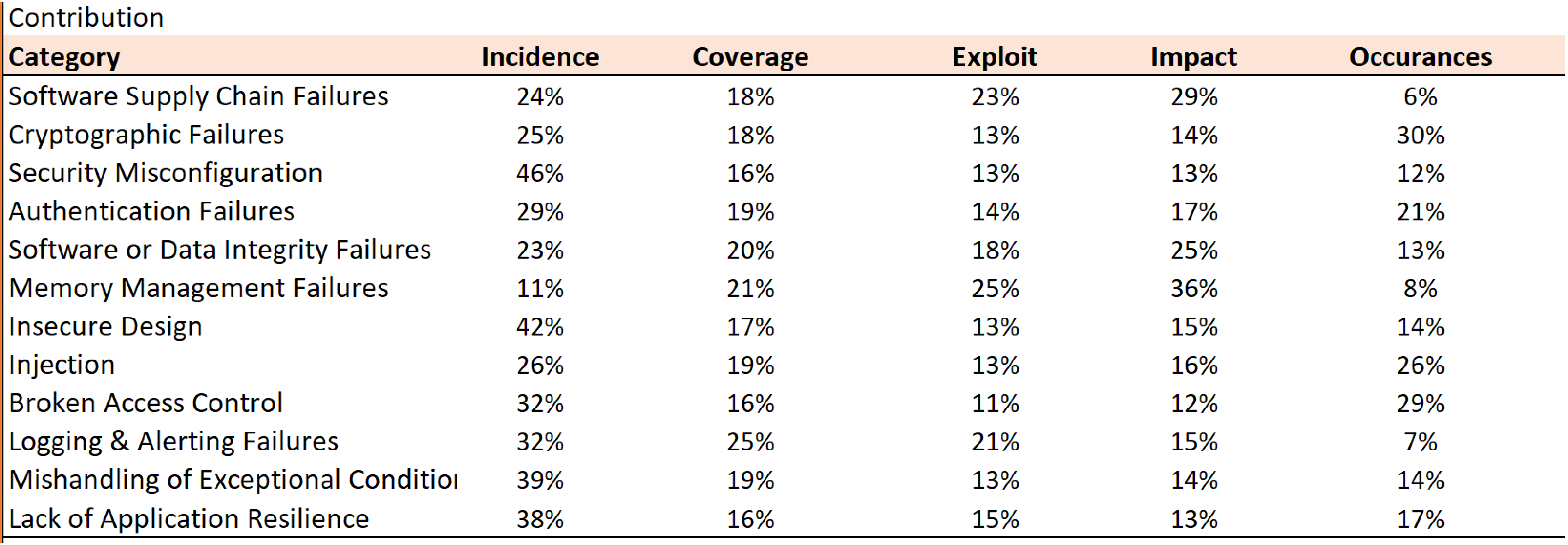
Data Factors



High Watermark

Category	Incidence	Coverage	Exploit	Impact	Occurances	Score	Rank
Software Supply Chain Failures	88.14	65.42	81.7	104.7	21.52	361.42	10
Cryptographic Failures	137.74	100.00	72.3	77.9	166.53	554.56	3
Security Misconfiguration	276.99	100.00	79.6	79.4	71.91	607.89	2
Authentication Failures	158.00	100.00	76.9	88.8	112.07	535.74	5
Software or Data Integrity Failures	89.78	78.52	71.1	95.7	50.13	385.22	9
Memory Management Errors	29.57	55.62	67.5	96.3	22.04	271.08	12
Insecure Design	221.81	88.76	69.6	81.0	72.99	534.19	6
Injection	137.65	100.00	71.5	86.4	140.42	535.96	4
Broken Access Control	201.52	100.00	70.4	76.8	183.97	632.68	1
Logging & Alerting Failures	113.33	85.96	71.9	53.0	26.03	350.20	11
Mishandling of Exceptional Conditioi	206.72	100.00	71.1	76.2	76.96	531.00	7
Lack of Application Resilience	200.47	86.01	79.2	69.8	86.51	521.95	8
Weight	1000	100	10	20	10000		

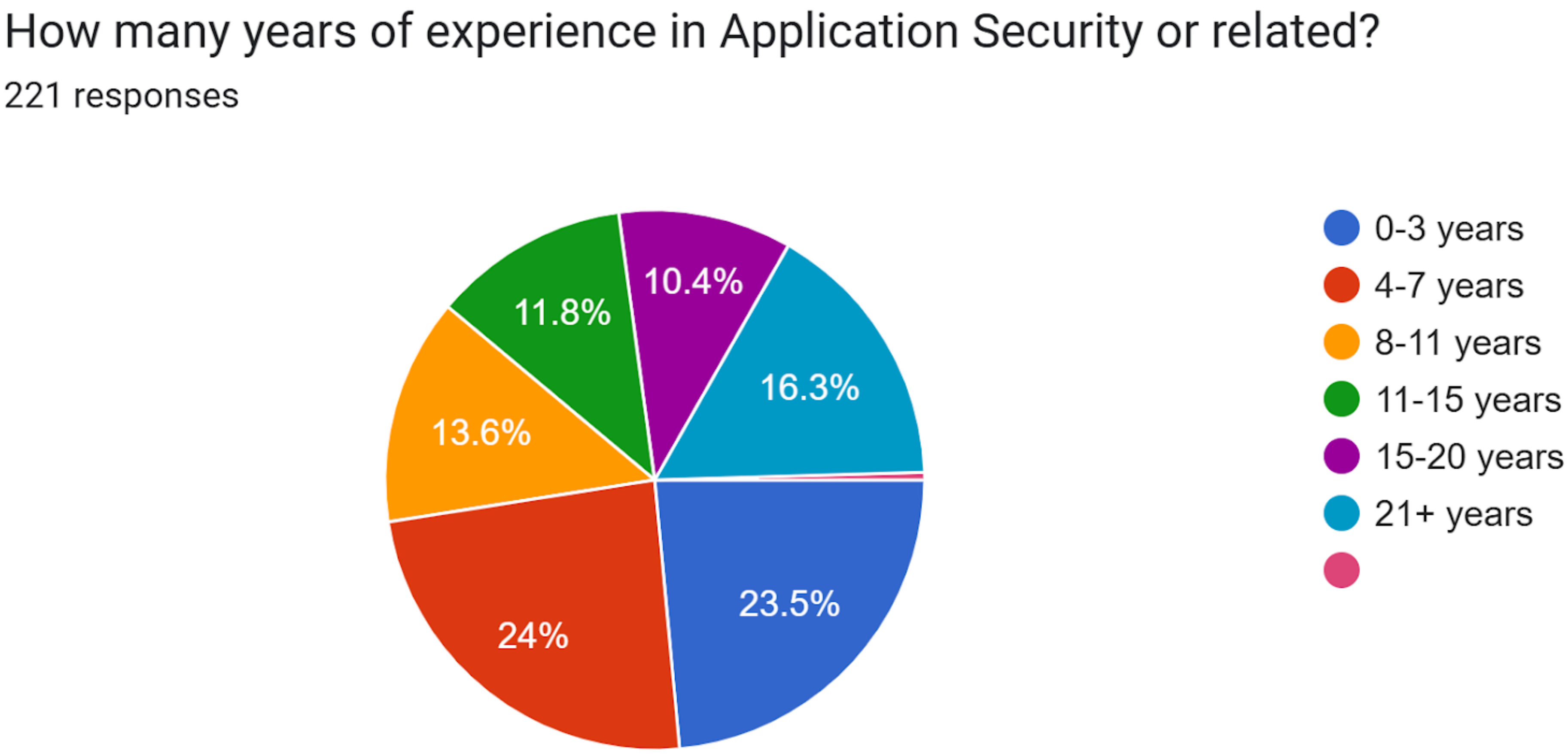
Data Factors



Contribution

Category	Incidence	Coverage	Exploit	Impact	Occurances
Software Supply Chain Failures	24%	18%	23%	29%	6%
Cryptographic Failures	25%	18%	13%	14%	30%
Security Misconfiguration	46%	16%	13%	13%	12%
Authentication Failures	29%	19%	14%	17%	21%
Software or Data Integrity Failures	23%	20%	18%	25%	13%
Memory Management Failures	11%	21%	25%	36%	8%
Insecure Design	42%	17%	13%	15%	14%
Injection	26%	19%	13%	16%	26%
Broken Access Control	32%	16%	11%	12%	29%
Logging & Alerting Failures	32%	25%	21%	15%	7%
Mishandling of Exceptional Conditio	39%	19%	13%	14%	14%
Lack of Application Resilience	38%	16%	15%	13%	17%

Survey Data



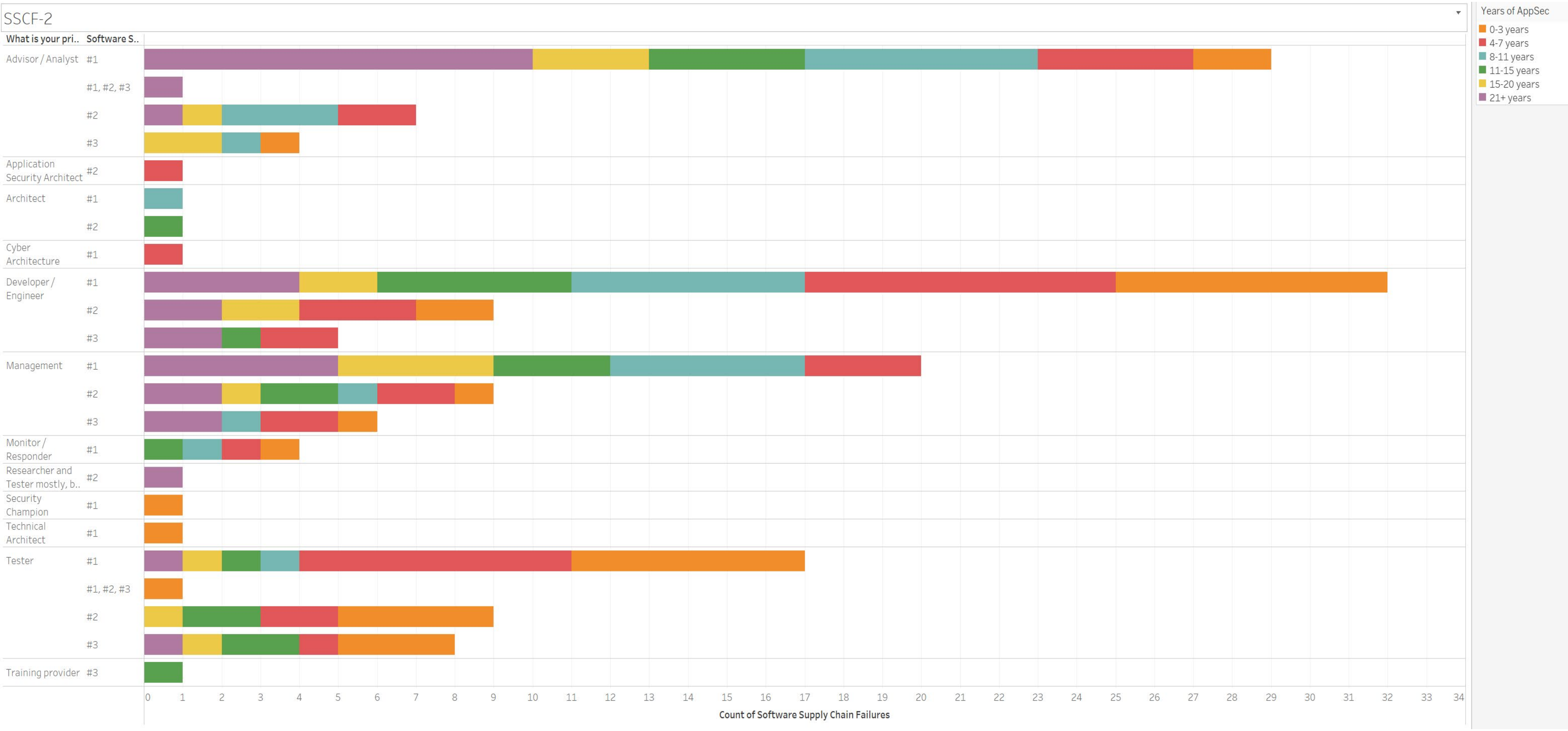
How many years of experience in Application Security or related?

221 responses

Survey Data

Count	Purpose
145	It helps provides structure for standards, requirements, security tests, test results, etc
129	Mostly for education of developers
85	We have to adhere to compliance that references the Top Ten
79	We build processes around it
46	We build tools to test for it
19	It doesn’t, but I think it’s important
1	Awareness and examples
1	Helps me discuss with clients finding and how best to harden systems in order to provide Cyber insurance
1	in immature companies/orgs its a starting point. mature orgs mature into org specific top 5 for each 6 month release cycle
1	None of the above
1	we have a SAST tool and our users are interested in how our categories map to the OWASP Top 10
1	We use it to focus people on the important issues in appsec and make sure they're not confused about what area of cybersecurity we are talking about.

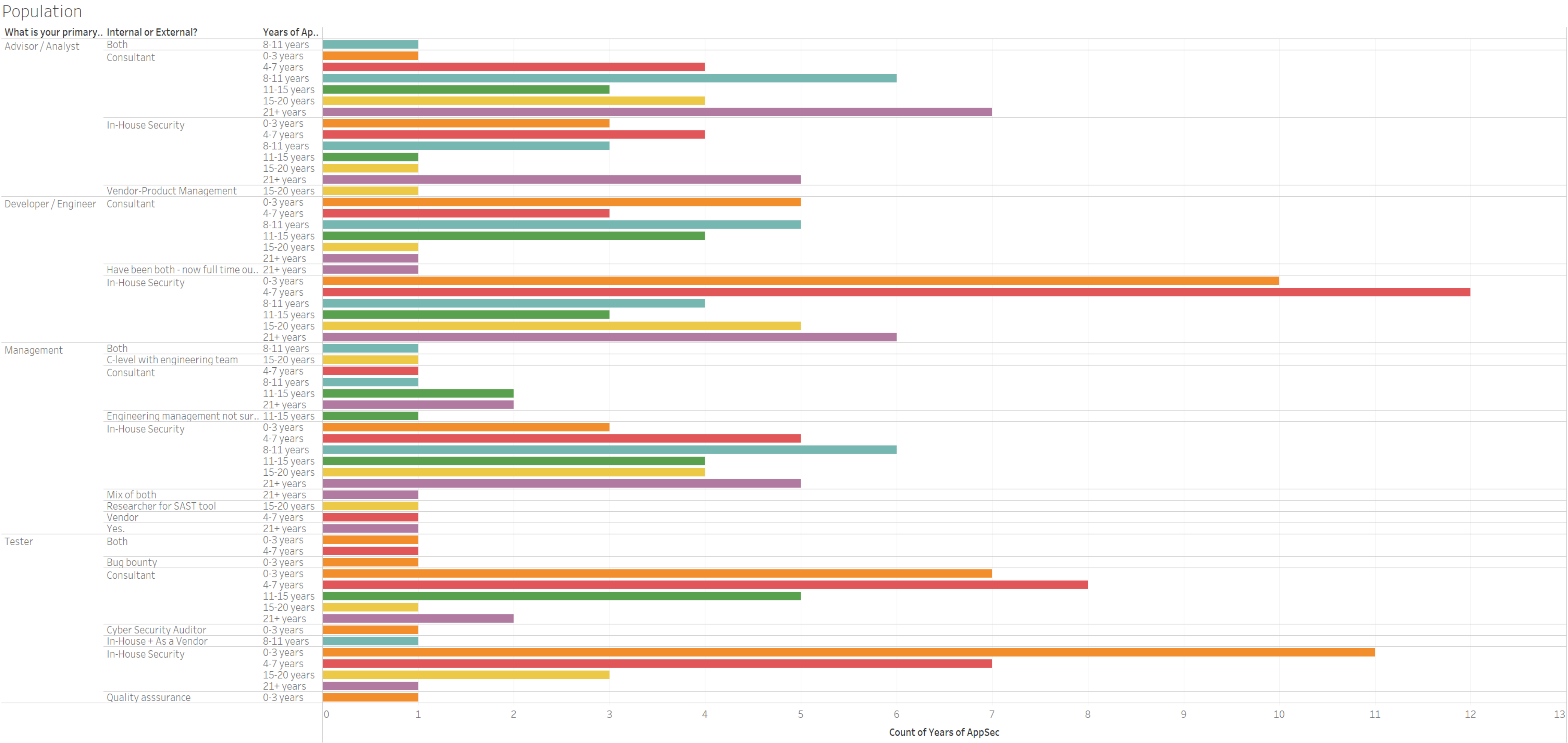
Survey Data


SSCF-2
What is your pri..
Software S..
Advisor / Analyst
#1
#1, #2, #3
#2
#3
Application Security Architect
#2
Architect
#1
#2
Cyber Architecture
#1
Developer / Engineer
#1
#2
#3
Management
#1
#2
#3
Monitor / Responder
#1
Researcher and Tester mostly, b..
#2
Security Champion
#1
Technical Architect
#1
Tester
#1
#1, #2, #3
#2
#3
Training provider
#3
0
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
Count of Software Supply Chain Failures
Years of AppSec
0-3 years
4-7 years
8-11 years
11-15 years
15-20 years
21+ years

OWASP 2025 GLOBAL AppSec | USA

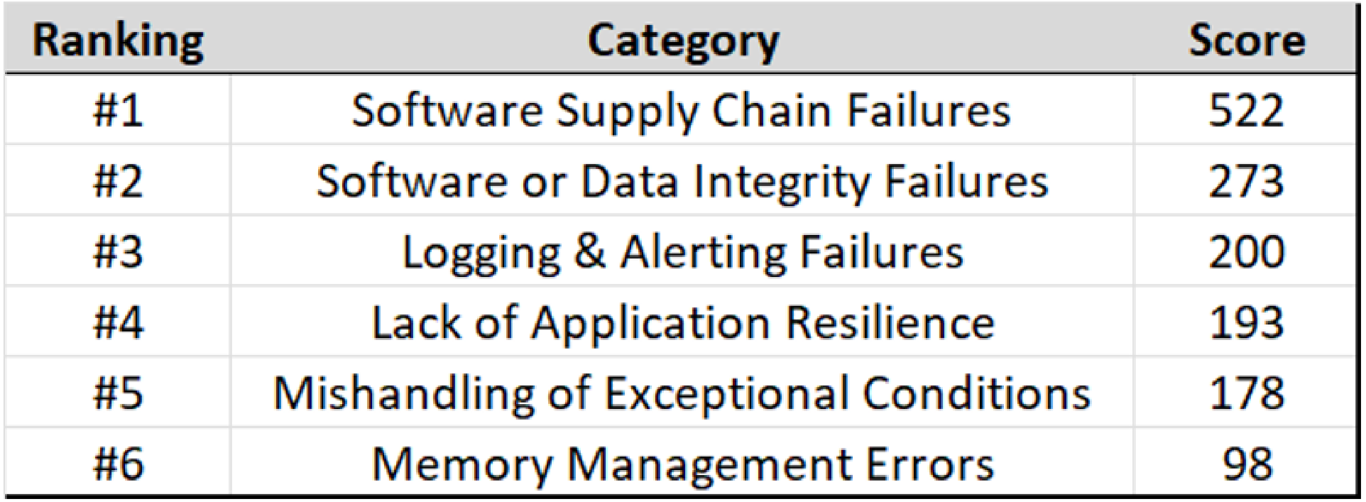
Survey Data

TOP 10

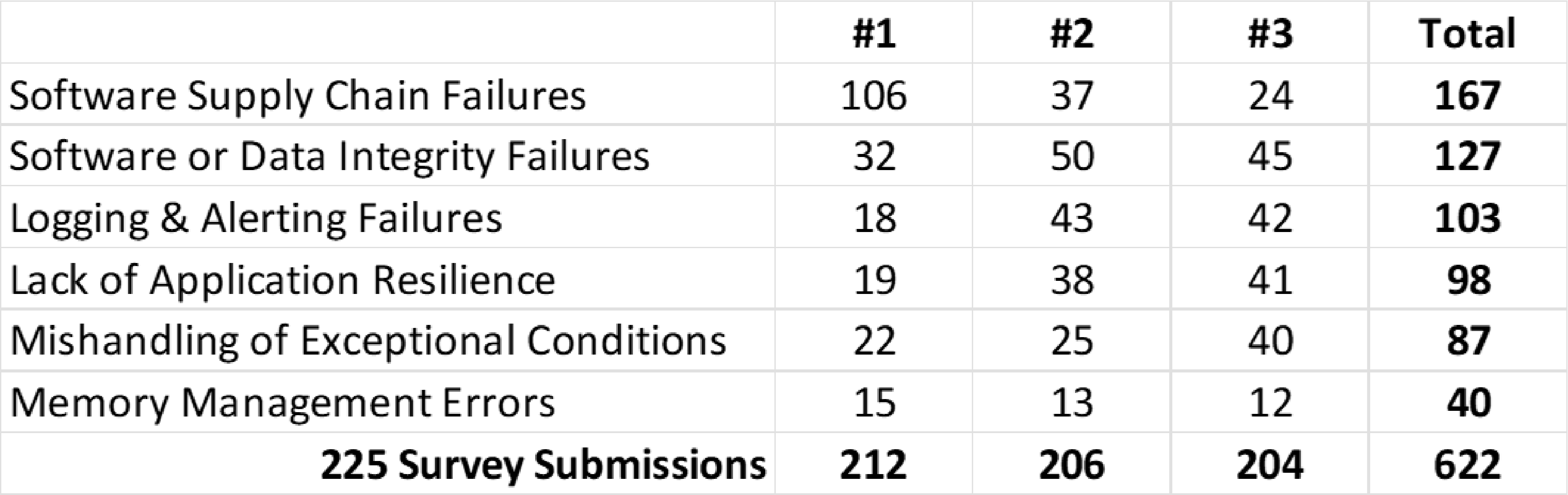


Population

The Survey Results



Ranking	Category	Score
#1	Software Supply Chain Failures	522
#2	Software or Data Integrity Failures	273
#3	Logging & Alerting Failures	200
#4	Lack of Application Resilience	193
#5	Mishandling of Exceptional Conditions	178
#6	Memory Management Errors	98



	#1	#2	#3	Total
Software Supply Chain Failures	106	37	24	**167**
Software or Data Integrity Failures	32	50	45	**127**
Logging & Alerting Failures	18	43	42	**103**
Lack of Application Resilience	19	38	41	**98**
Mishandling of Exceptional Conditions	22	25	40	**87**
Memory Management Errors	15	13	12	**40**
225 Survey Submissions	**212**	**206**	**204**	**622**

What can you do?

- Map findings to CWEs
- Map findings to good CWEs (stop using prohibited)
- Map findings to root cause CWEs
- There is so much more than the Top Ten
- OWASP SAMM (https://owaspsamm.org)
- Many other OWASP projects

QR Code here for slides

That's All Folks

OWASP 2025 GLOBAL AppSec | USA

THANK YOU!