OWASP

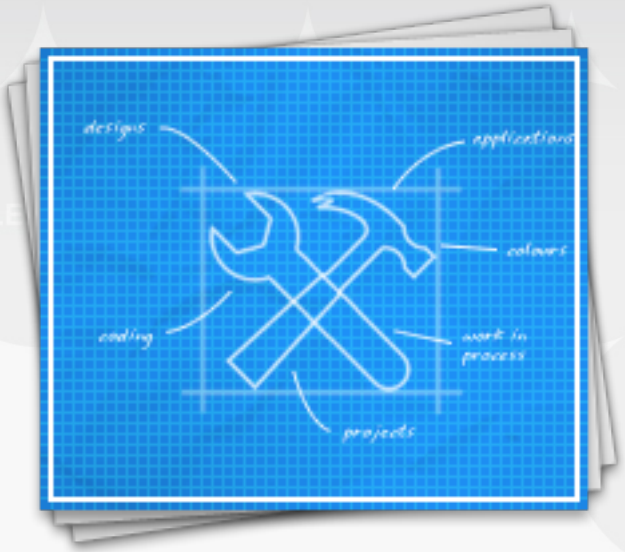
Open Web Application Security Project

OWASP Mobile Top Ten 2015 Data Synthesis and Key Trends

Part of the
OWASP Mobile Security Group
Umbrella Project

Agenda

1. Strategy of the Project for 2015
2. Marketplace Data – Synthesis Results
3. 2014 Call for Data – Synthesis Results
4. “Safe bets” for 2015



STRATEGIC ROADMAP
PAST AND PRESENT

Previous 2014 Plan

1. Guide technical audiences around mobile appsec risks
2. Publish a list that prioritizes what organizations should address for mobile app risks
3. Establish the group as an authoritative source for mobile technical guidance that is trustworthy to technical communities
   - Follow an evidence-based (rather than purely prescriptive) approach to recommendations
     - Generate / gather vulnerability data by January 2014
     - Gather feedback from OWASP community over 90 days

Successes of 2014 Plan

Objective Outcomes for 2014:

- Data was successfully gathered by January 2014;
- Data was successfully grouped and presented AppSec Cali 2014
- List was finalized in August 2014

Strategic Outcomes for 2014:

- Publication of list was achieved;
- An evidence-based approach to data collection was executed

Goal Outcomes for 2014:

- Guiding technical audiences around mobile risk achieved

Lessons Learned From 2014 Plan

1. Goal of providing clear guidance was a partial success
   - Grouping vulnerabilities and attaining consensus is difficult
   - Difficulty in understanding who exactly are the primary audiences
2. Goal of establishing legitimacy was a partial success
   - Not enough data sources / transparency in data analysis
   - Not enough inclusion of other OWASP projects

2015 Strategic / Objective Plan

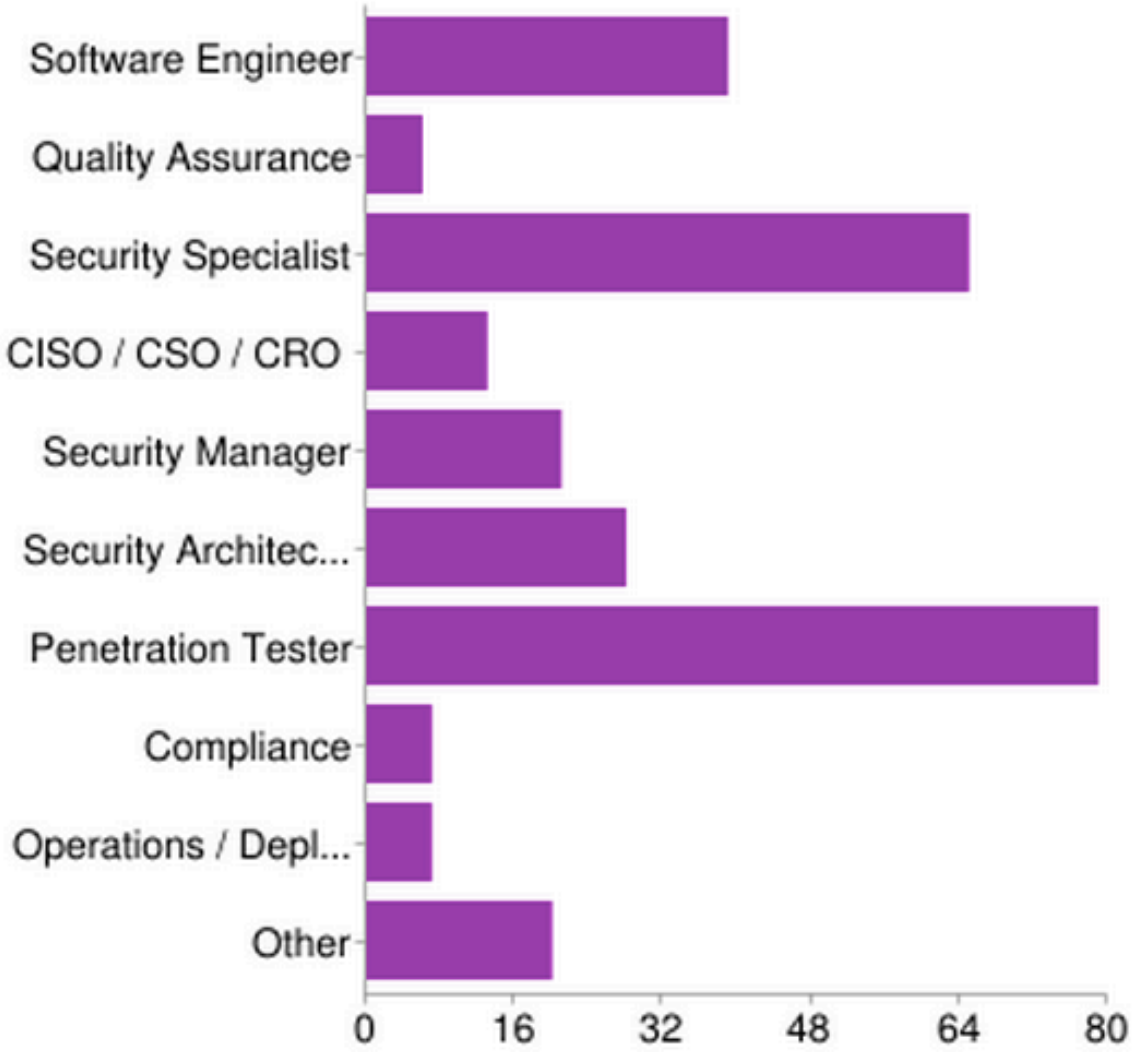
1. Clarify who is using the list and why:
   - Formally analyze the users to help clarify the way the list should be organized and presented
2. Improve transparency of data / existing processes in group:
   - Increase number of data contributors and their diversity
   - Provide greater transparency of data / data analysis
3. Increase outreach:
   - Engage / promote other OWASP projects within list
   - Promote more feedback opportunities

MARKET ANALYSIS

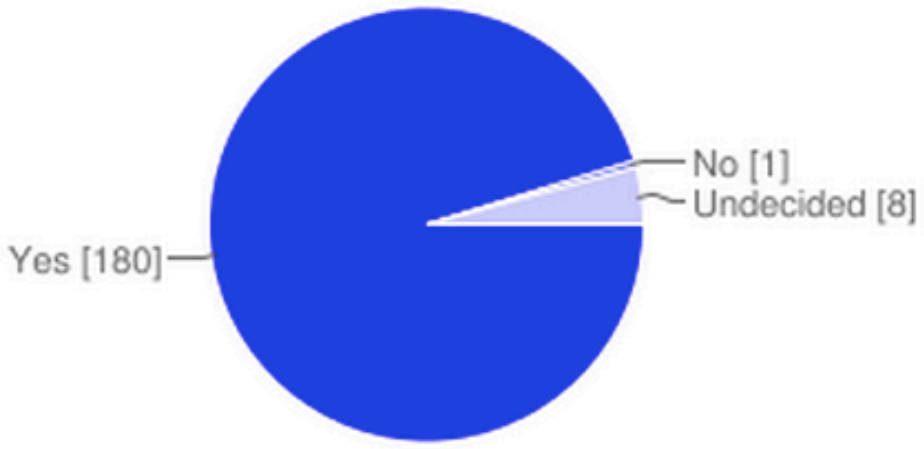
Q: Who is using the list and why?

Answering this question helps clarify how to group things and present solutions.

What is your current role?

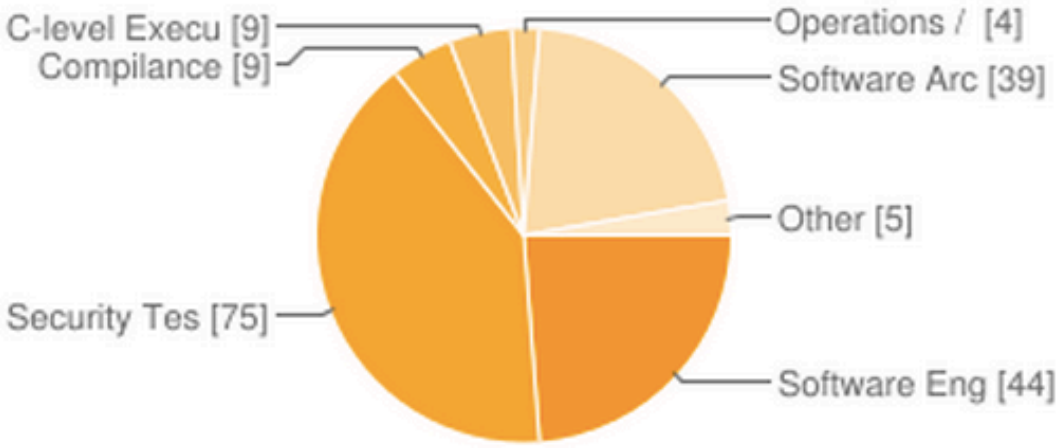


Do you see value in having an OWASP Mobile Top 10 list?

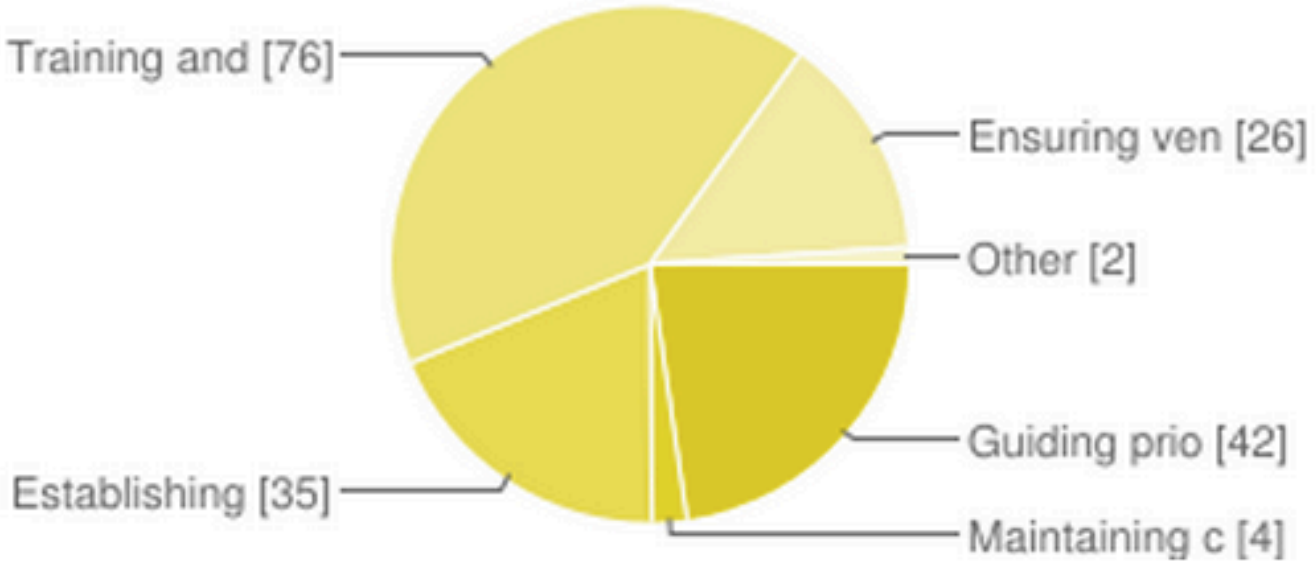


Yes	**180**	95.2%
No	**1**	0.5%
Undecided	**8**	4.2%

Who do you think would benefit the most from utilizing it within your organization?



If you believe it is of value, what is its greatest value?



Guiding prioritization of vulnerability remediation	**42**	22.7%
Maintaining compliance	**4**	2.2%
Establishing testing methodologies	**35**	18.9%
Training and security awareness	**76**	41.1%
Ensuring vendors think about security	**26**	14.1%
Other	**2**	1.1%

DATA ANALYSIS

Q: What does the latest vulnerability data suggest?

Answering this question helps clarify what the list can afford to drop or introduce.

Participants

cigital

bugcrowd

HackLabs

MetaIntelli™
Identify Risks - Avoid Threats

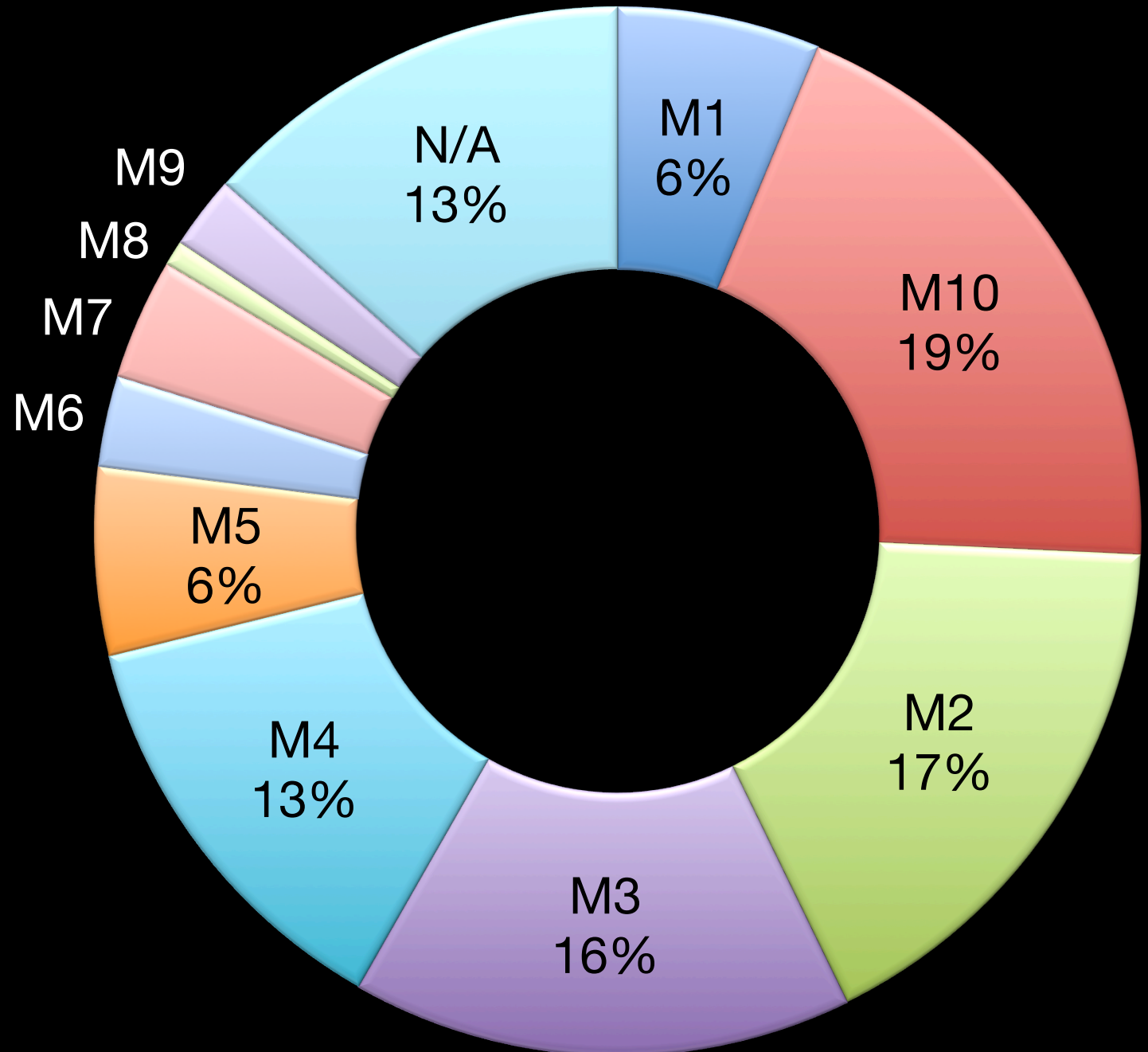
securenetwork

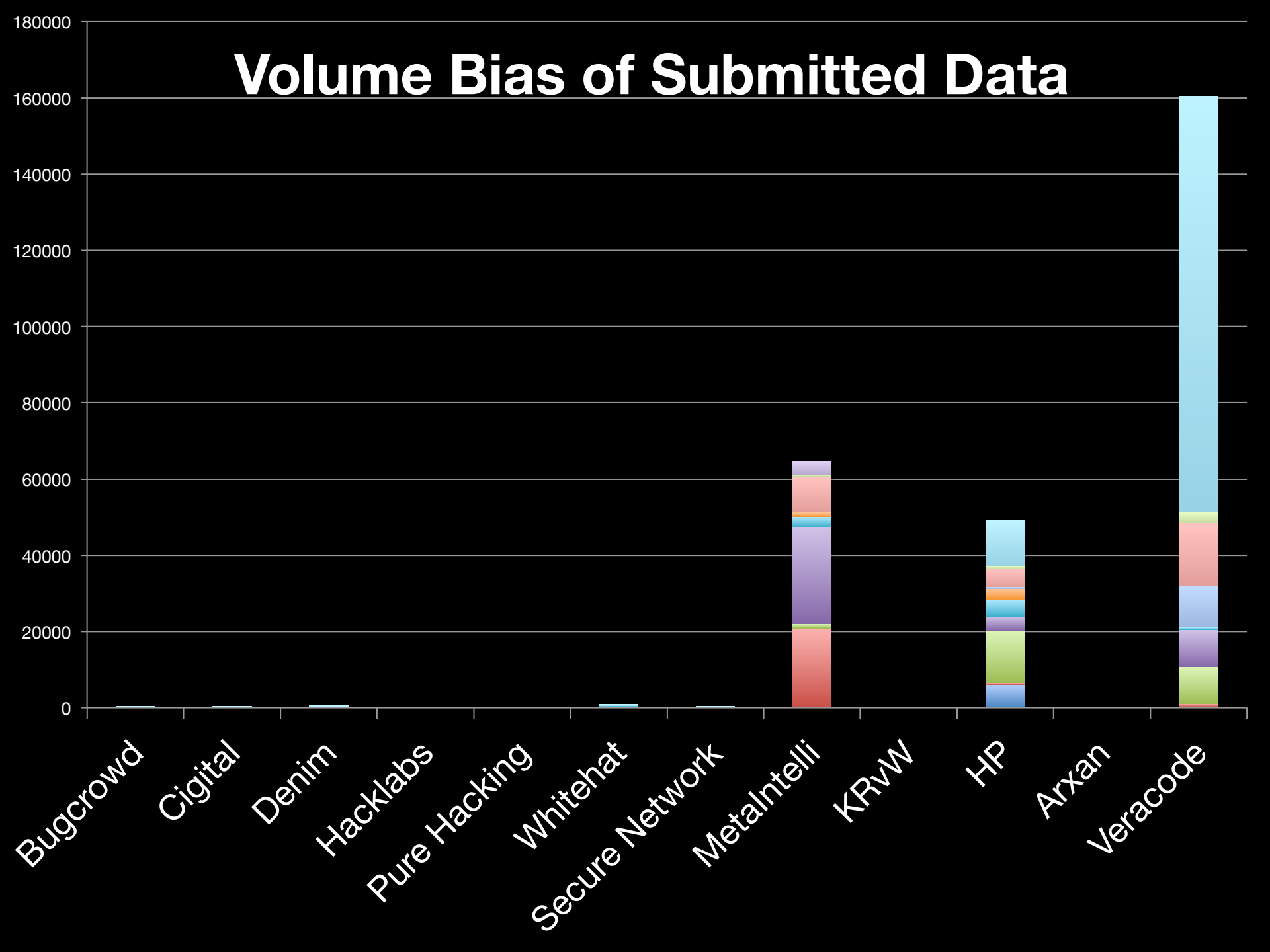
KRvW Associates, LLC
Information Security -- Consulting and Training Services

PURE HACKING

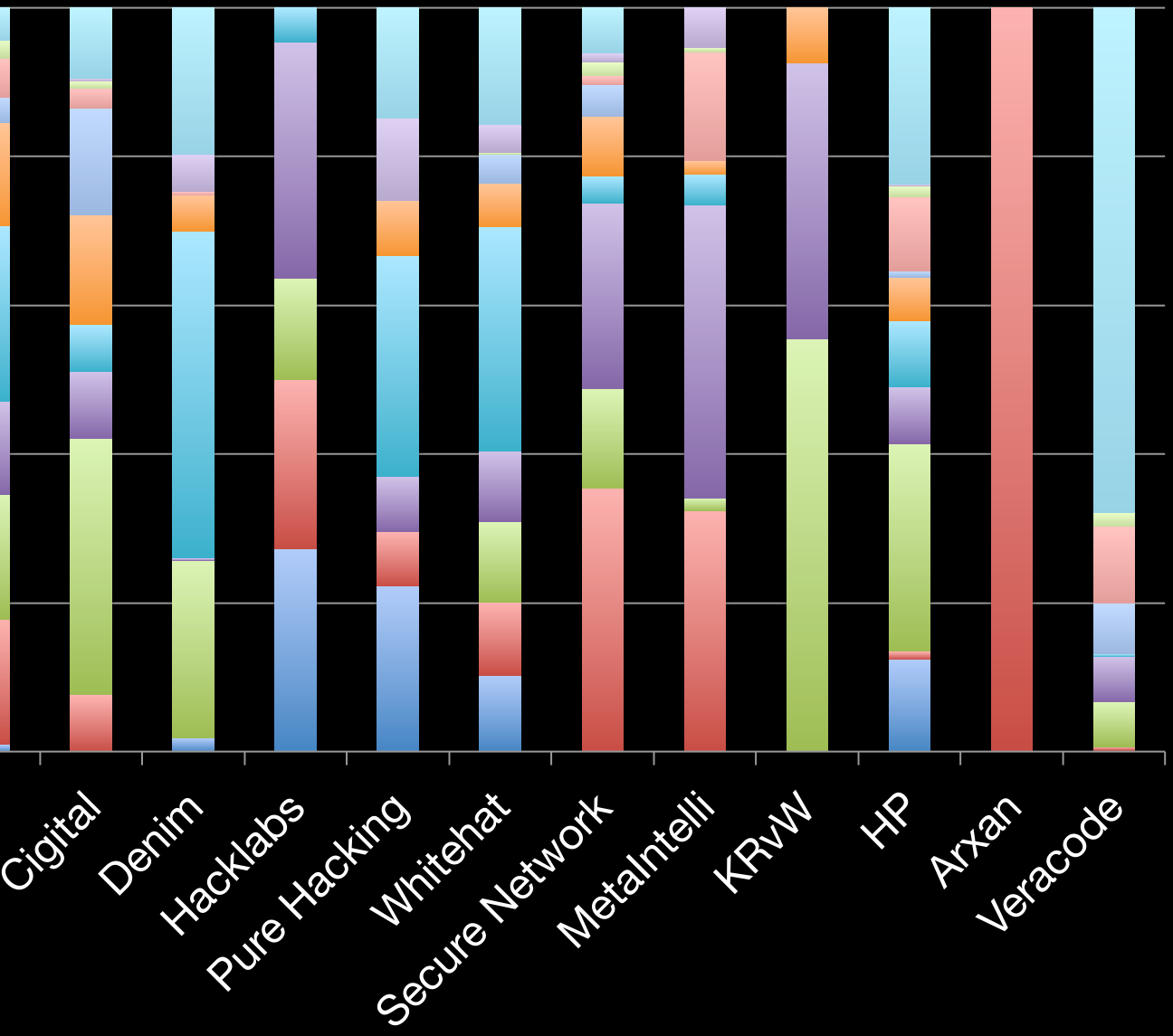
VERACODE

OWASP
Open Web Application Security Project

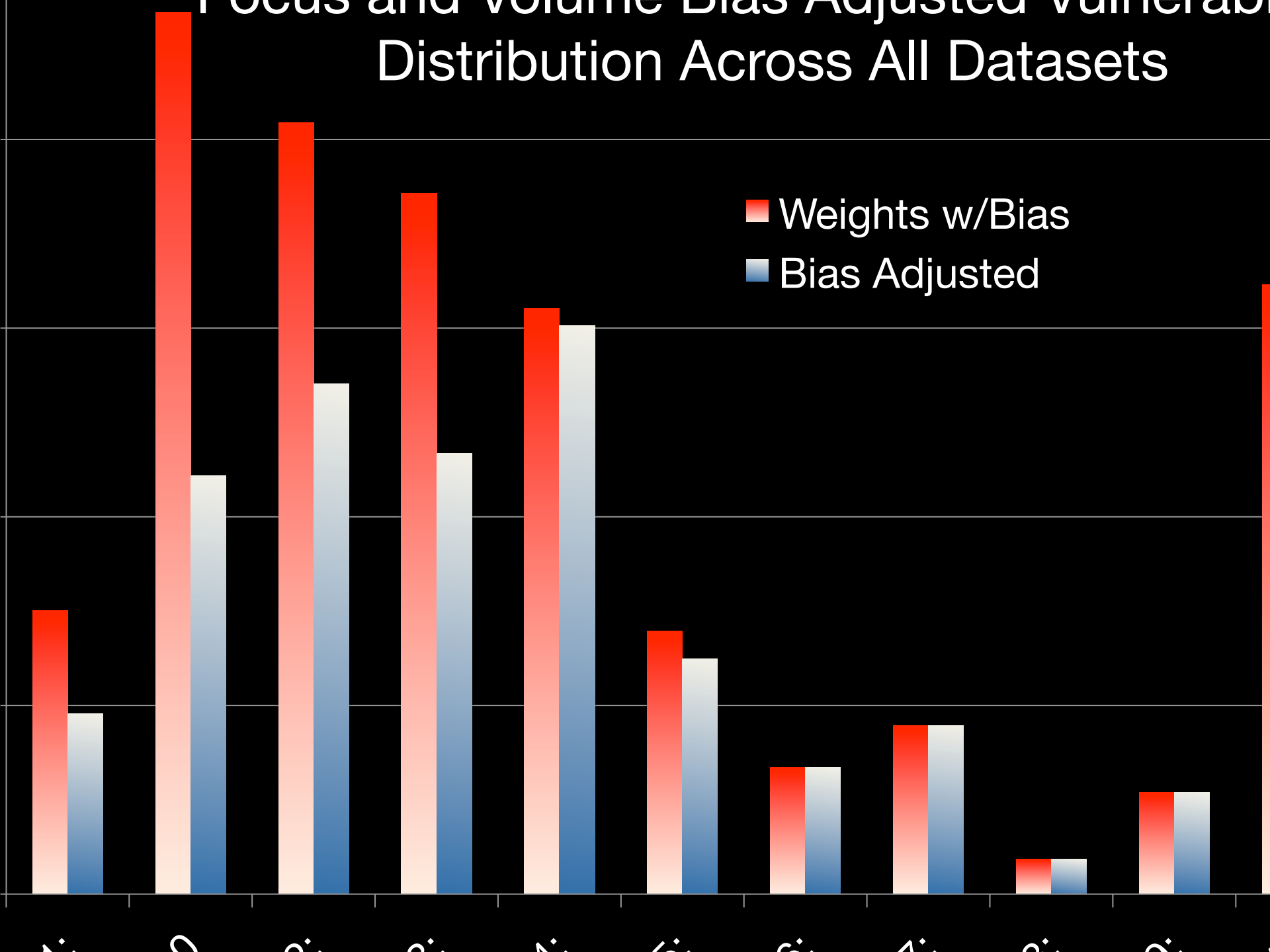

M1
6%
M10
19%
M2
17%
M3
16%
M4
13%
M5
6%
M6
M7
M8
M9
N/A
13%


Volume Bias of Submitted Data
180000
160000
140000
120000
100000
80000
60000
40000
20000
0
Bugcrowd
Cigital
Denim
Hacklabs
Pure Hacking
Whitehat
Secure Network
MetaIntelli
KRvW
HP
Arxan
Veracode

Focus Bias

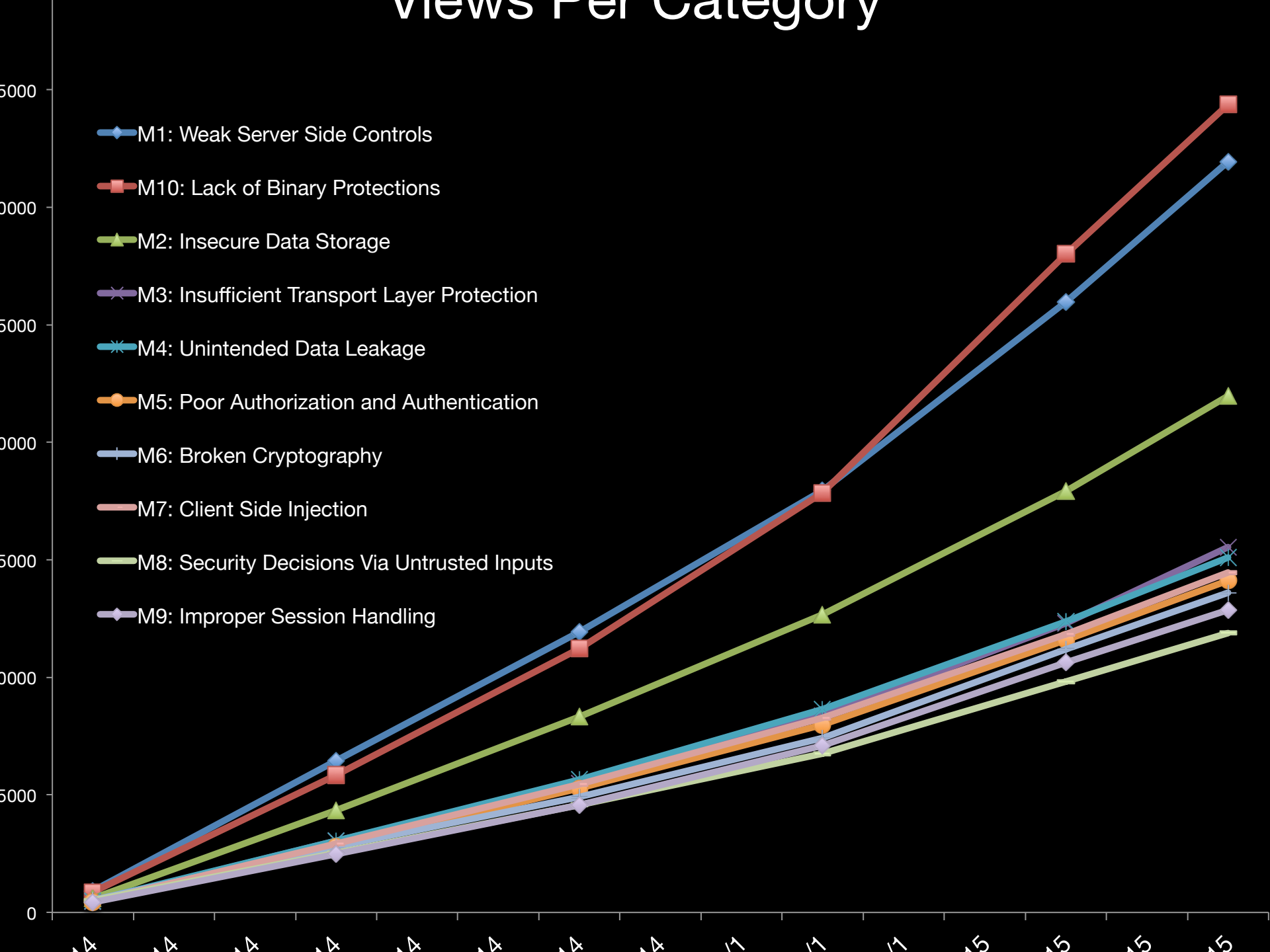


- N/A: No Appropriate Categor
- M9: Improper Session Handl
- M8: Security Decisions Via U Inputs
- M7: Client Side Injection
- M6: Broken Cryptography
- M5: Poor Authorization and Authentication
- M4: Unintended Data Leakag
- M3: Insufficient Transport La Protection
- M2: Insecure Data Storage
- M10: Lack of Binary Protecti


Focus and Volume Bias Adjusted Vulnerab
Distribution Across All Datasets
Weights w/Bias
Bias Adjusted

Potential Data Bias from Products

- Products used to automate analysis results can also skew results:
  - Static code analysis rules (ease with which to report on things found in source code)
  - Dynamic analysis rules (ease with which to report on runtime behaviors)


Views Per Category
M1: Weak Server Side Controls
M10: Lack of Binary Protections
M2: Insecure Data Storage
M3: Insufficient Transport Layer Protection
M4: Unintended Data Leakage
M5: Poor Authorization and Authentication
M6: Broken Cryptography
M7: Client Side Injection
M8: Security Decisions Via Untrusted Inputs
M9: Improper Session Handling
5000
0000
5000
0000
5000
0000
5000
0

INSIGHTS FROM THE ANALYSIS

Key Observations

1. People believe the MTT is valuable and will serve Software Engineers and Pen Testers the most
   - Security awareness / training primarily
   - Remediation prioritization secondarily

2. Substantial number of findings that don't currently have a home:
   - code-quality / stability issues

3. Some categories are
   - M1 <-> M7; M2 <-> M4; M8

4. There are many categories that aren't being reported very often:
   - M1; M6; M7; M8; M9

Safe Bets...

1. Categories least often used will get axed
2. M2, M3, and M4 are definitely working and will stay but probably tweaked further
3. M10 will be included but overhauled based on lots of feedback
4. New category will be added to take into account code-quality / stability issues
5. Categories will become less ambiguous
6. Categories will be presented differently for each audience (pen tester; engineer; consumer; etc.)

Next Steps

- Analysis is now complete
- Group is currently meeting to debate new groupings / tweaks to existing content
- After release candidate is formulated, conduct 90-day review cycle with formal market analysis

Would you like to join the debate?
Join the OWASP Mobile Top Ten mailing list!

Subscribe:
owasp-mobile-top-10-risks@owasp.org