SAMM Benchmark
Top 10 Lessons Learned

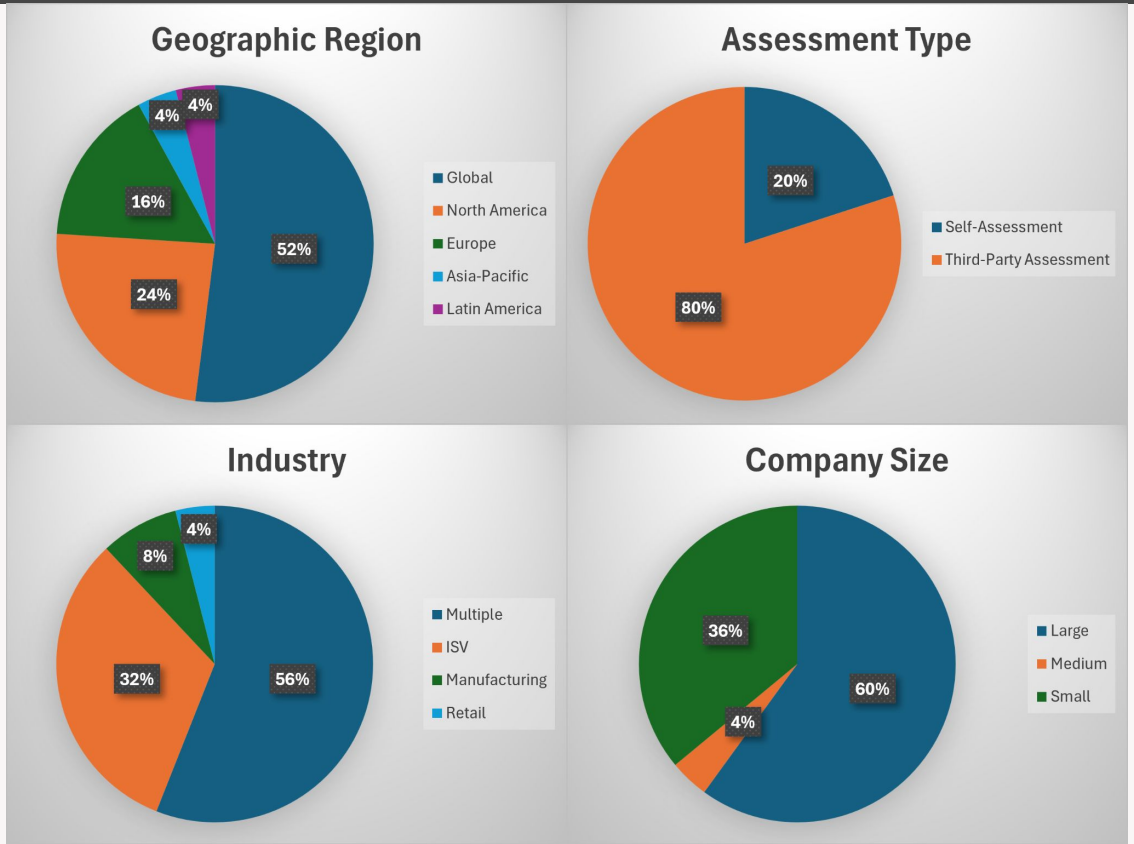
SAMM User Day
June 26, 2024

SAMM Benchmark

Benchmark tab in Excel Toolbox and SAMMY tool

https://bit.ly/sammbenchmarksubmission

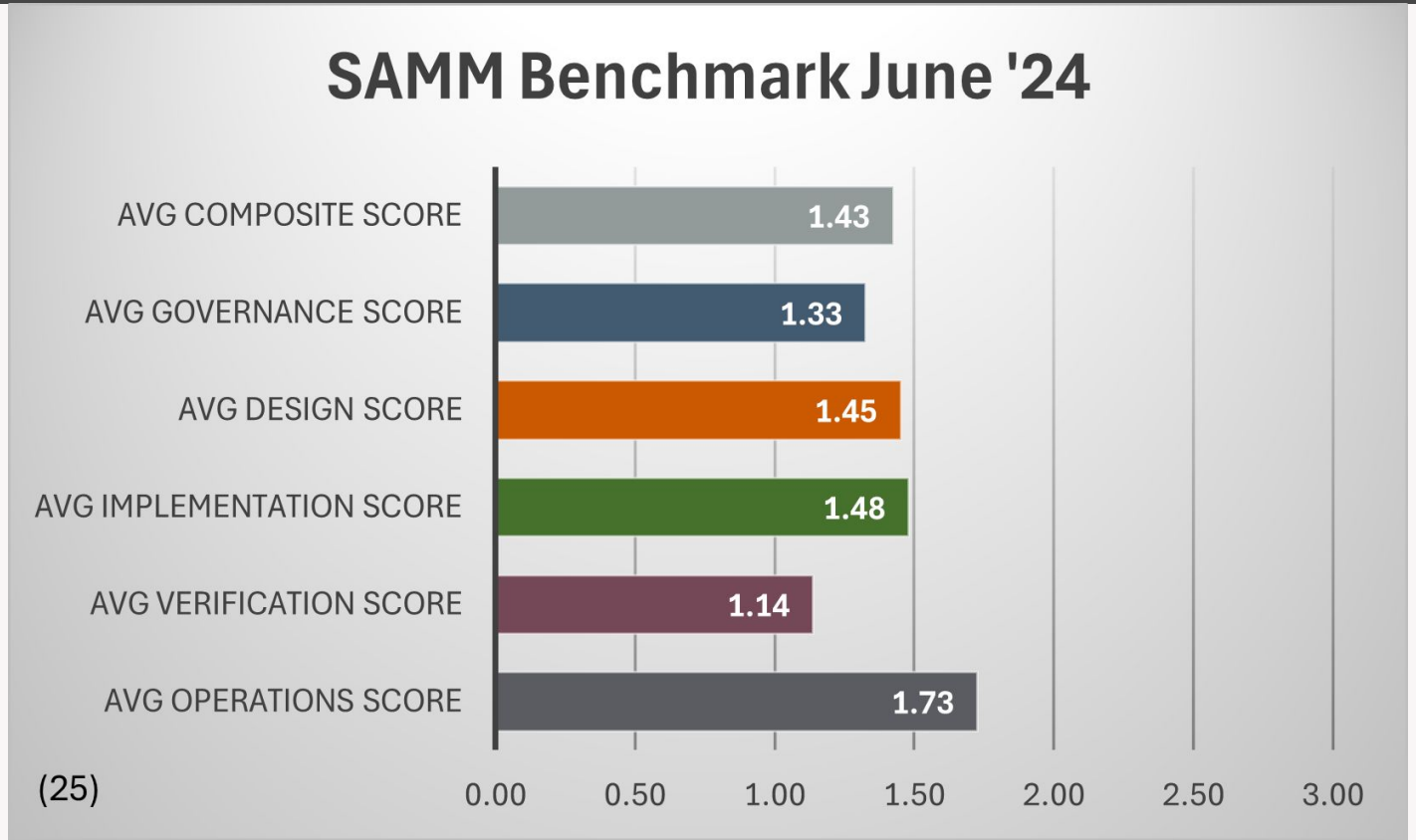
Demographics



Demographics Highlights

- 25 datasets
  - Too few to provide more granular results
- Most assessments are done by a reputable third party
  - High quality data
- The majority of the companies are large multinationals
  - Mid-sized companies are underrepresented
- Results averaging problems
  - Governance and Operations in multinationals vs small

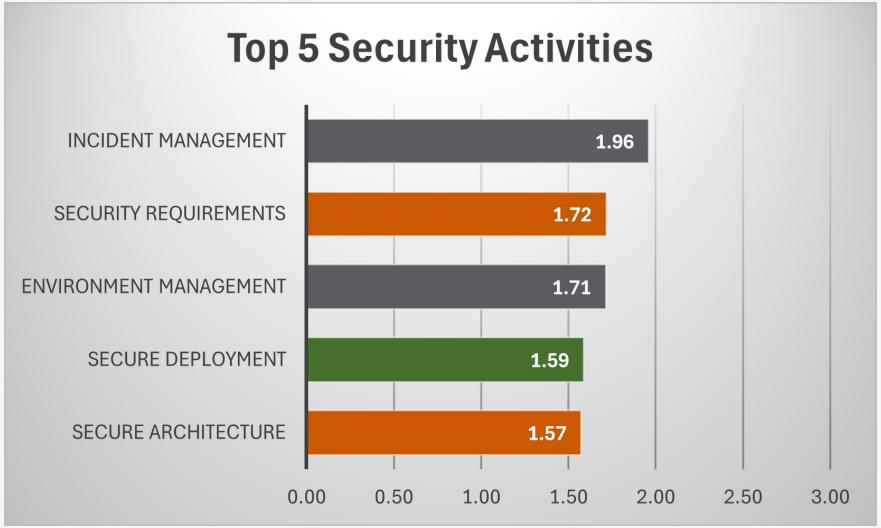
Overall Results

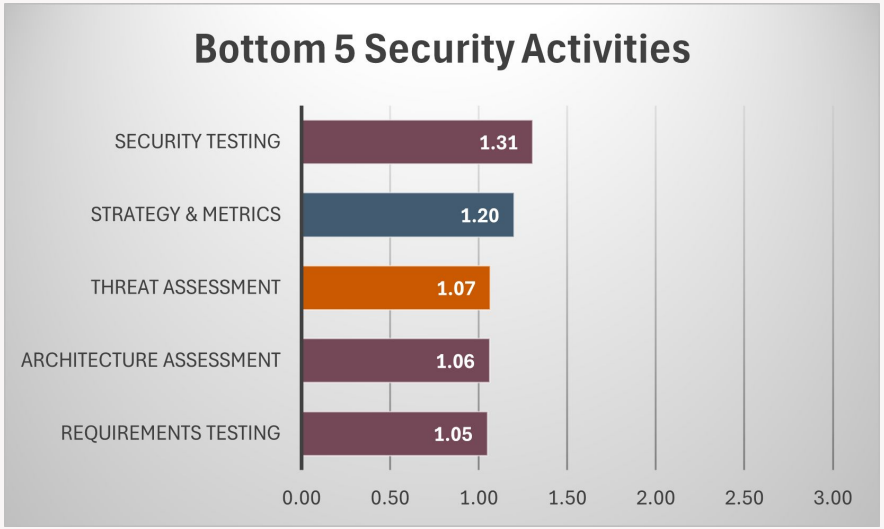


Overall Results

- Higher score on Operations
  - Expected especially for large multinationals
- Higher score for Implementation
  - The success of the Dev(Sec)Ops paradigm
- Lower Governance score is surprising
  - Arguably due averaging skewing
- Higher score on Design
  - “Shift left”

Top vs Bottom Scoring Activities





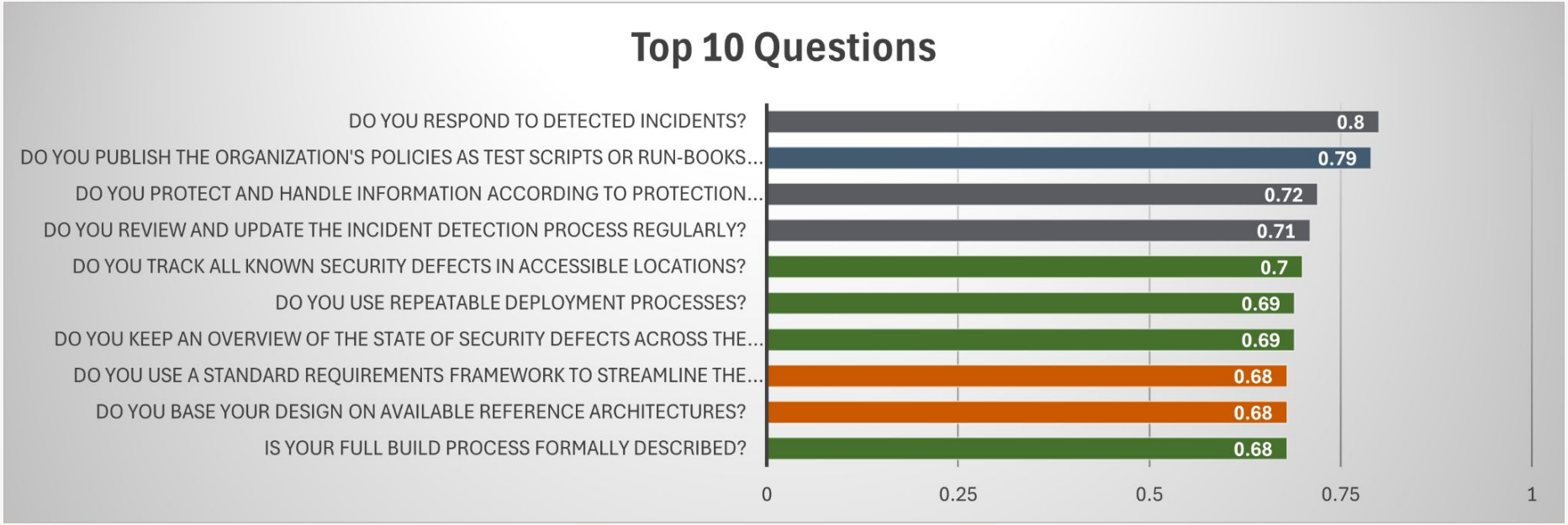
Top vs Bottom Scoring Activities

- Incident & Environment Management are historically handled well at large multinationals
- Deployment is thanks to Dev(Sec)Ops successes
- Security Requirements and Secure Architecture are probably thanks to the “Shift Left” paradigm

Top vs Bottom Scoring Activities

- Low scores on Requirements Testing and Architecture Assessment are surprising in combination with “Shift Left”
  - Did we do the right thing?
- Threat Assessment is historically a low scoring activity
- Low scores on Security Testing is surprising
  - Best practices for SAST/DAST usage
  - Pen testing lessons learned (L3)
- Low scores on Strategy & Metrics is very surprising
  - Perhaps averaging issues

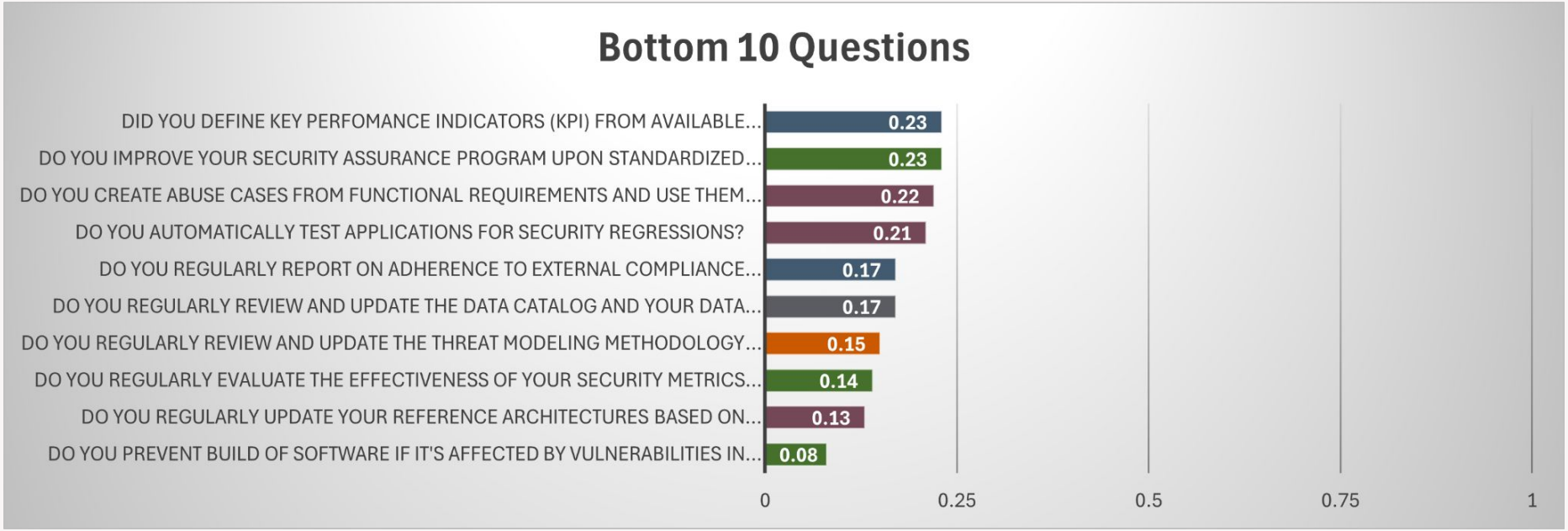
Top Scoring Questions



Top Scoring Questions

- Top scorers that are inline with expectations
  - Incident management
  - Defect management
  - Deployment process
  - Data protection
- Top scorers that are surprising
  - Security requirements framework
  - Publishing policies and standards as runbooks

Bottom Scoring Questions



Bottom Scoring Questions

- Bottom scores inline with expectations
  - Creating abuse cases from requirements
  - Regular review and update of the threat modeling methodology
  - Compliance-related questions
    - Report on compliance adherence
    - Data catalog review and update

Bottom Scoring Questions

- Bottom scores that are surprising
  - Testing applications for the correct functioning of standard security controls
  - KPI and effectiveness of security metrics
  - Preventing build of software if it’s affected by vulnerabilities

Thank you!

owaspsamm.org