A Multivocal Literature Review of Current Tools for Increasing the Degree of Automation in the Development of Secure and Privacy Compliant Applications

John Nguyen, 23. November 2020, Final Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de
Outline

Motivation and background

Research goal and methodology

- Methodology
- Research questions
- Search strategy

Results

- Key drivers for security automation tools
- Tool classification
- Mapping of tools with security activities

Summary

- Conclusion
- Limitations

Bibliography
Motivation and background (cont’d)

Average cost of a data breach by security automation level in organizations worldwide from 2018 to 2020 (in million U.S. dollars)

Note: Worldwide; August 2019 to April 2020; 524 organizations
Further information regarding this statistic can be found on page 8.
Source(s): IBM; Ponemon Institute; ID 1176688

John Nguyen (TUM)
Motivation and background (cont’d)

Need for security and privacy automation tools

Challenges in agile software development

- Neglection of non-functional requirements
- Rapid pace of development and deployment
- Knowledge boundaries (e.g., documentation) [3-4]

Benefits

- Improving scalability
- Reducing human error [1]
- Checking continuously instead of an interval basis [2]
- Avoid cost explosion due to fixing at implementation stage [9]
- Lack of security experts [10]
- Parallel testing [13]

→ Challenges of finding relevant security automation tools

- Lack of an overview of current security automation tools
- State-of-the-practice overview lack level of abstraction [5-6]
Outline

Motivation and background

Research goal and methodology
- Methodology
- Research questions
- Search strategy

Results
- Key drivers for security automation tools
- Tool classification
- Mapping of tools with security activities

Summary
- Conclusion
- Limitations

Bibliography
Multivocal literature review

- Form of systematic literature review
- Covers both the state-of-the-art and practice
- Inclusion of a large body of grey literature

Benefits

- Certain evidence is often based on experience and opinion
- Inclusion of real-world needs in industrial settings
- May avoid publication bias

Challenges

- Quality assessment
- Large volumes of data → need for a termination criteria
- Bias and lack of quality [14]
Research questions

Research questions 1 (RQ1): What challenges can automation tools address when developing security and privacy compliant applications?

Research questions 2 (RQ2): How can the identified tools and technologies be classified?

Research questions 3 (RQ3): How can the identified tools be mapped to the activities of the BSIMM10 framework to assess the current automation level?
BSIMM10

- Building Security In Maturity Model (BSIMM)
- Four domains with 12 practices including 119 activities

**Domains**

**Governance**
- Strategy & Metrics (SM)
- Compliance & Policy (CP)
- Training (T)

**Intelligence**
- Attack Models (AM)
- Security Features & Design (SFD)
- Standards & Requirements (SR)

**SSDL Touchpoints**
- Architecture Analysis (AA)
- Code Review (CR)
- Security Testing (ST)

**Deployment**
- Penetration Testing (PT)
- Software Environment (SE)
- Configuration Management & Vulnerability Management (CMVM) [15]

**TEN CORE ACTIVITIES “EVERYBODY” DOES**

<table>
<thead>
<tr>
<th>ACTIVITY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>[SM.1]</td>
<td>Identify gate locations and gather necessary artifacts.</td>
</tr>
<tr>
<td>[CP.1]</td>
<td>Identify PII obligations.</td>
</tr>
<tr>
<td>[T.1]</td>
<td>Provide awareness training.</td>
</tr>
<tr>
<td>[AM.1]</td>
<td>Create a data classification scheme and inventory.</td>
</tr>
<tr>
<td>[SFD1.1]</td>
<td>Build and publish security features.</td>
</tr>
<tr>
<td>[SR.1]</td>
<td>Translate compliance constraints to requirements.</td>
</tr>
<tr>
<td>[AA.1]</td>
<td>Perform security feature review.</td>
</tr>
<tr>
<td>[CR.1]</td>
<td>Have SSG perform ad hoc review.</td>
</tr>
<tr>
<td>[ST.1]</td>
<td>Ensure QA supports edge/boundary value condition testing.</td>
</tr>
<tr>
<td>[PT.1]</td>
<td>Use external penetration testers to find problems.</td>
</tr>
<tr>
<td>[SE.1]</td>
<td>Ensure host and network security basics are in place.</td>
</tr>
<tr>
<td>[CMVM1.2]</td>
<td>Identify software bugs found in operations monitoring and feed them back to development.</td>
</tr>
</tbody>
</table>

[Image: https://www.hack2secure.com/images/blog/BSIMM%20Skeleton%2002.png (13.06.2020)]
### Academic literature

**Inclusion criteria**
- Written in English and full text accessible
- Accessible with TUM rights or freely accessible
- Online available
- The paper must discuss security or privacy compliance automation
- The paper must include any kind of tool, framework demonstration/implementation, prototype, or similar to the support software development lifecycle
- Within the Software Engineering domain
- The paper must be published in a journal or conference paper
- Published between 2015-2020 (initial search)

**Exclusion criteria**
- Duplicates or repeated studies
- Lack of relevance for RQs
- Algorithms and concepts
- Workshops and tutorials are excluded

### Grey literature

**Inclusion criteria**
- Written in English and full text accessible
- Accessible with TUM rights or freely accessible
- Online available
- The artifact must discuss security or privacy compliance automation
- The artifact must include any kind of tool, framework demonstration/implementation, prototype, or similar to the support software development lifecycle
- Within the Software Engineering domain
- Published between 2015-2020 (initial search)

**Exclusion criteria**
- Duplicates or repeated studies
- Lack of relevance for RQs
- Algorithms and concepts
- Thesis, Workshops, and tutorials are excluded
Search strategy (cont’d)

Academic Literature

- ACM DL: 1155
- IEEE: 26
- Springer Link: 606
- Web of Science: 27
- Total of 1810

Initial Search

Filter

Stage 1: Filter by title
- n = 381

Stage 2: Filter by abstract (and conclusion) & removing duplicates
- n = 120

Stage 4: Quality assessment & Obtain primary publications
- n = 30

Grey Literature

- Google Scholar
  - Additional Search
    - n = 100
    - Filter
      - n = 2
      - Snowballing
        - n = 3
        - n = 93

- Google
  - Initial Search
    - n = 213
    - Filter
      - n = 30
      - Snowballing
        - n = 31

        - n = 53 (+ 6 GL)
Search string (cont’d)

- **SLR:** (secur* OR priva* OR protect*) AND ("software development" OR "software engineering") AND (tool* OR control*) AND (automat* OR "continuous") AND ("DevOps" OR "agile")
- **GLR:** (security OR privacy) tool automation (DevOps OR Agile)

<table>
<thead>
<tr>
<th>Database</th>
<th>Search pool</th>
<th>Title</th>
<th>Abs.</th>
<th>TR</th>
<th>QA</th>
<th>PL</th>
<th>Snowballing</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACM DL</td>
<td>1155</td>
<td>247</td>
<td>63</td>
<td>12</td>
<td>12</td>
<td>-1</td>
<td>+13 (+0)</td>
<td>24</td>
</tr>
<tr>
<td>IEEE</td>
<td>26</td>
<td>17</td>
<td>12</td>
<td>6</td>
<td>6</td>
<td>-2</td>
<td>+2 (+5)</td>
<td>11</td>
</tr>
<tr>
<td>Springer</td>
<td>606</td>
<td>112</td>
<td>43</td>
<td>12</td>
<td>12</td>
<td>-2</td>
<td>+13 (+1)</td>
<td>24</td>
</tr>
<tr>
<td>Web of Science</td>
<td>23</td>
<td>5</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Google.com</td>
<td>213</td>
<td>150</td>
<td>104</td>
<td>71</td>
<td>30</td>
<td>-0</td>
<td>+1</td>
<td>31</td>
</tr>
<tr>
<td>Google Scholar</td>
<td>100</td>
<td>19</td>
<td>7</td>
<td>2</td>
<td>2</td>
<td>-0</td>
<td>+1</td>
<td>3</td>
</tr>
</tbody>
</table>

Abs.: Abstract  
TR: Text review  
QA: Quality assurance  
PL: Primary literature  
(n): Shows the additional number (n) of GL artifacts
Outline

Motivation and background

Research goal and methodology

- Methodology
- Research questions
- Search strategy

Results

- Key drivers for security automation tools
- Tool classification
- Mapping of tools with security activities

Summary

- Conclusion
- Limitations

Bibliography
Key drivers for automation tools

- Autonomy
- Competitiveness
- Collaboration
- Non-Expert Testing
- Reviewing Security Properties
- Issue Response
- Preventive Analysis
- Code Maintenance
- Scalability and Efficiency
- Keeping Security Up-To-Date
- Security Awareness and Mindset
- Reduction of Manual Errors
- Traceability
- Policy Enforcement

Number of hits

Academic literature
Grey literature
Tool classification (cont’d)

Distribution of the classification per category

- Configuration Management
- Infrastructure Analysis
- Infrastructure Hardening
- Alert
- Issue Tracking
- Code Tracking
- Dynamic Attack Protection
- Automated Attack
- Monitoring & Logging
- Assistive Tools
- Code Hardening
- Architecture Hardening
- Test Management
- Code & Build Review
- Vulnerability Management
- Security Awareness
- Threat Modeling

Number of hits
<table>
<thead>
<tr>
<th>Category</th>
<th>Tool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Modeling</td>
<td>IrinRisk, no name (attack graph generation), OWASP Threat Dragon, Scorpio, ThreatModeler</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>HackerOne, no name (commit message analysis), no name (semantic wiki), QL, SD Elements</td>
</tr>
<tr>
<td>Test Management</td>
<td>Bamboo, Chef InSpec, Cabernet, Codacy, Code Climate, Code Dx, coveralls, DetectDojo, DrTest, Faraday, GitLab, Istanbul, JackHammer, Jenkins, Jest, JSCover, Klaros, LogCoGo, OWASP Code Pulse, Phantom (Splunk Phantom), Rational Quality, Manager (IBM Engineering Test Management), Seccubus, Selenium, SeleniumBase, ThreadFix, WhiteHat Sentinel Application Security Platform</td>
</tr>
<tr>
<td>Architecture Hardening</td>
<td>Chef Vault, creditstash, CyberArk Conjur, GOBLIN, HashiCorp Vault, Jisat, KeyWhiz, no name (clone detection), no name (identify insecure dataflows), Pitravirs, Red October, Scorpio, sneaker, Speaker KeyWhiz project, Trouseau, Venafi Trust Protection Platform</td>
</tr>
<tr>
<td>Code Hardening</td>
<td>PHP Aspis</td>
</tr>
<tr>
<td>Assistive Tools</td>
<td>ActiveState Platform, ffuu</td>
</tr>
<tr>
<td>Monitoring &amp; Logging</td>
<td>Alert Logic, AlienVault OSSIM, AppDynamics, AppScan, Artifactory (JFROG), AuthMatrix, Cacti, CloudMonix, CloudPassage Halo, CloudWatch, Dagda, DataDog, digital.ai, Dome9 SecOps, Dynatrace, Elasticsearch, Falco, FileBeat, Ganglia, God, Grafana, Graphite, GrayLog, Icinga, Infobyte HUNT, Kibana, LogRhythm, Logstash, Logz.io, Monit, MUSA Security Assurance Platform (MSAP), Nagios, New Relic, Nexpose (Rapid7), OSSEC, PagerDuty, Phantom (Splunk Phantom), Pingdom, PortVis, Prometheus, Qualys (cloud platform), Redlock (Evidence.io), ReGrade, Rsyslog, runit, Sensu, Snort, Splunk (enterprise), SumoLogic, Supervisor, Suricata, Syslog-NG, systemd, Threat Stack, VictorOps, Zabbix</td>
</tr>
<tr>
<td>Dynamic Attack Protection</td>
<td>CANDID, Contrast Protect, Contrast Security, Fortify Application Defender, Illiumo, Immunio, NeuVector, OpenRASP, Preyoty, Signal Science, iCell, Waratek</td>
</tr>
<tr>
<td>Code Tracking</td>
<td>Atlassian Crucible, Gerrit, loggly, PaperTrails, Phabricator</td>
</tr>
<tr>
<td>Issue Tracking</td>
<td>Bugzilla, JIRA, Redmine</td>
</tr>
<tr>
<td>Alert</td>
<td>Alerta, AppDynamics, DataDog, Dynatrace, ElastAlert, HipChat, Logz.io, Nagios, New Relic, PagerDuty, Phantom (Splunk Phantom), Pingdom, Prometheus, Stack, Splunk (enterprise), VictorOps</td>
</tr>
<tr>
<td>Infrastructure Hardening</td>
<td>GPG</td>
</tr>
<tr>
<td>Infrastructure Analysis</td>
<td>Amazon AWS Inspector, ChefSpec, CIS Benchmarks, CVEChecker, Dagda, Dome9 Arc, Iftu, GRaVITY, Hping, Jmeter, LMD (linux malware detection), Lynis Security Auditing, masscan, Nessus, NMAP, OpenVAS, SECUBAT, Serverspec, SSLyze, Stethoscope, Test Kitchen, Tripwire, VirusTotal, WhatWeb, Wireshark</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Anible, Charles Proxy, Chef, Cloudbees, digital.ai, Istio, LGTM, NeuVector, Palerra LORIC, Puppet, Rational Team Concert (IBM Engineering Workflow Management), SaltStack, StackStorm, topoS</td>
</tr>
</tbody>
</table>

John Nguyen (TUM) © sebis 17
<table>
<thead>
<tr>
<th>Activity</th>
<th>Summary</th>
<th>A</th>
<th>Translation</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>SM1.1</td>
<td>Make the security plan public to all relevant entities</td>
<td>N</td>
<td>The process and decision to issue a security plan is a decision-making activity</td>
<td>-</td>
</tr>
<tr>
<td>T1.1</td>
<td>Improve awareness regarding security and privacy concepts of individuals</td>
<td>Y</td>
<td>Here, we look at tools that facilitate the security and privacy awareness of an individual. Tools like DdSG can improve security perception by training, e.g., attack patterns through playing a tower-defense game. This approach can be made through any kind of e-learning tool. We want to note that the respective organizations can execute this approach without additional manual effort. In contrast, the learning process for individuals is not automatable.</td>
<td>DdSG</td>
</tr>
<tr>
<td>T1.7</td>
<td>Provide customized teaching of security and privacy concepts</td>
<td>Y</td>
<td>Any kind of tool that can give customized teaching of security and privacy concepts belong to this activity. In particular, all SAST, IAST, and DAST tools are matched to this activity. For example, the SAST tool Findbugs can give developers real-time feedback on common security vulnerabilities, depending on their respective code. It is noteworthy that T1.7 is directly connected to T1.1 because tools can be individually adjusted to the participant's experience.</td>
<td>Findbugs</td>
</tr>
<tr>
<td>SE1.1</td>
<td>Implement monitoring for input data</td>
<td>Y</td>
<td>For this activity, we look into two major approaches: logging and monitoring. Tools capable of monitoring either infrastructure or software, such as Grafana and infrastructure logging tools like SumoLogic, match this activity. Furthermore, we also assign hybrid-tools that require monitoring to work correctly, such as RASP tools.</td>
<td>Grafana, SumoLogic</td>
</tr>
<tr>
<td>CMVM.3.3</td>
<td>Mimic attacks on software security</td>
<td>Y</td>
<td>For this matter, we identified several tools that can automatically mimic an attack, such as DOS-attacks or unplug randomly severs like Chaos Monkey.</td>
<td>Chaos Monkey</td>
</tr>
</tbody>
</table>
Tool-support of BSIMM10-activities (cont’d)

Distribution per BSIMM-dimension, separated between artifact types

Relative number of tool-matches

GOVERNANCE | INTELLIGENCE | SSDL TOUCHPOINTS | DEPLOYMENT

0% | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100%

Grey literature
Academic literature
All artifacts
Tool-support of BSIMM10-activities (cont’d)

Distribution per BSIMM-practice without non-tool-supported activities
## Tool-support of BSIMM10-activities (cont’d)

### Examples

<table>
<thead>
<tr>
<th>Tool</th>
<th>Matched BSIMM-activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aqua Security</td>
<td>SFD3.2, SR2.4, SR3.1, CR1.2, CR1.4, CR1.5, CR2.7, CR3.4</td>
</tr>
<tr>
<td>Chef Vault</td>
<td>SE3.2</td>
</tr>
<tr>
<td>ConPan</td>
<td>SFD3.2, SR2.4, SR3.1, CR1.2, CR1.4, CR1.5, CR2.7, CR3.4</td>
</tr>
<tr>
<td>Gauntlt</td>
<td>AM3.2, ST2.1</td>
</tr>
<tr>
<td>NMAP</td>
<td>SE1.2</td>
</tr>
<tr>
<td>OWASP ZAP</td>
<td>ST1.1, ST2.1, ST2.6, PT1.3</td>
</tr>
<tr>
<td>Snort</td>
<td>SE1.1, SE1.2, SE3.3</td>
</tr>
<tr>
<td>Wireshark</td>
<td>SE1.2</td>
</tr>
</tbody>
</table>
Tool-support of BSIMM10-activities (cont’d)

Average highest watermark by BSIMM-firms

Highest watermark by all identified tools

Outline

Motivation and background

Research goal and methodology

- Methodology
- Research questions
- Search strategy

Results

- Key drivers for security automation tools
- Tool classification
- Mapping of tools with security activities

Summary

- Conclusion
- Limitations

Bibliography
Conclusion

Key points
- Scalability and efficiency key driver for implementing security automation
- Majority of tools concerns with code and build review
- Governance related activities are neglected by identified tools

Challenges of tools
- Emphasis on culture
- Management of tools

Future research
- Tool-study
- In-depth analysis of cross-tool-integration
- Tools within the IT governance area of different sized firms
- Change of perspective on tools
Limitations

- Non-peer-reviewed artifacts
- Google Search Engine results might be biased
- Dependency between artifacts
- Sample size
- No practical implementation of all tools
Limitations (cont’d)
Security and privacy automation is not a silver bullet

Utilization of security tools assume an established security-aware culture and knowledge

- Wide range of skills required
- Integration of new tools
  - Conflict with legacy systems
  - Conflict with an established mindset [7]
- Faded boundaries between the security team and developers [8]
- Additional cost
  - Need for additional education and improved culture
  - Acquiring new tools and technologies
- Cross-team cooperation necessary [1]
- Isolated tools to solve specific problems [11]
  \(\Rightarrow\) We also look into centralized solutions

Outline

Motivation and background

Research goal and methodology

- Methodology
- Research questions
- Search strategy

Results

- Key drivers for security automation tools
- Tool classification
- Mapping of tools with security activities

Summary

- Conclusion
- Limitations

Bibliography
Backup Slides
Schedule

- **Thesis Kickoff**: 15 Jun
- **Submission**: 29 Oct
- **Thesis completion**: 15 Nov

2020

- **Jun**: Today, Preparation Phase, Research Phase, Writing Phase, Correction Phase
- **Jul**: 15 days
- **Aug**: 5 days, 62 days
- **Sep**: 50 days
- **Oct**: 12 days
- **Nov**: 13 days, Buffer from 28 Oct to 15 Nov
Motivation and background

Challenge: More and more data is being stored and processed → Volume of stolen data increases

Issues:

- **Violation of security principles**
  - Least privilege
  - Defense in depth
  - Minimum exposure
- **Lack of security training**
  - Security awareness [8]
- **Old technologies** [9]
- **Conflict of interests between stakeholders**
  - Focus on functional requirements
  - Developers ↔ Architects ↔ Management

Note: Worldwide; April 2020; based on number of records lost
Further information regarding this statistic can be found on page 8.
Source(s): Information is Beautiful; Various sources (VizSweet), Thomson Reuters; ID 290525
Not so different after all

Waterfall

Agile

DevOps

DevOps At Scale

Time
### Questions to determine the need for an MLR

<table>
<thead>
<tr>
<th>#</th>
<th>Question</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Is the subject “complex” and not solvable by considering only the formal literature?</td>
<td>Yes. The formal literature cannot represent all relevant security and privacy tools due to the rapid change and complexity of security and privacy concerns.</td>
</tr>
<tr>
<td>2</td>
<td>Is there a lack of volume or quality of evidence, or a lack of consensus of outcome measurement in the formal literature?</td>
<td>Yes. The industrial setting is required to give an overview of all relevant tools.</td>
</tr>
<tr>
<td>3</td>
<td>Is the contextual information important to the subject under study?</td>
<td>Yes. We focus on security and privacy tools within a particular context (DevOps and agile).</td>
</tr>
<tr>
<td>4</td>
<td>Is it the goal to validate or corroborate scientific outcomes with practical experiences?</td>
<td>Yes. Focus on practical views on tools regarding privacy and security concerns.</td>
</tr>
<tr>
<td>5</td>
<td>Is it the goal to challenge assumptions or falsify results from practice using academic research or vice versa?</td>
<td>Yes. There is a research gap in-between tool interaction and how non-automatable activities can be considered in the automation process.</td>
</tr>
<tr>
<td>6</td>
<td>Would a synthesis of insights and evidence from the industrial and academic community be useful to one or even both communities?</td>
<td>Yes. Finding gaps within the toolchain can support the development of more centralized tools and identify potential weaknesses. This also supports the overall flexibility of the software development process.</td>
</tr>
<tr>
<td>7</td>
<td>Is there a large volume of practitioner sources indicating high practitioner interest in a topic?</td>
<td>Yes. Security and privacy automation tools are getting more and more relevant due to digitalization.</td>
</tr>
</tbody>
</table>

Knowledge of developers (2018)

100 employees of a selected industrial company

"Which tools do you know and/or use?"

Response options:

▪ (DevOps tools) Jenkins; Kubernetes; TeamCity; Spinnaker; Travis; GoCD; Concourse CI; JFrog Artifactory;
▪ (static analysis tools) PMD; Checkstyle; FindBugs; FindBugs Security;
▪ (security tools) OWASP ZAP; BDD Security; JFrog Xray; Security Monkey; Black Duck; Snyk” [1]
“What application security standards or models do you follow? Select all that apply.” [5]
435 respondents
OWASP Top 10 leading standard

Shackleford, D. (2016). A DevSecOps Playbook. SANS Institute InfoSec Reading Room. A DevSecOps Playbook Figure 2 p. 11 [5]
OWASP

- International non-profit organization
- Focus on web application security
- Goal: Improve web application security
- OWASP Top 10: represents top 10 risks (critical) [3]

<table>
<thead>
<tr>
<th>OWASP Top 10 - 2013</th>
<th>OWASP Top 10 - 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>A2 – Broken Authentication and Session Management</td>
<td>A2:2017-Broken Authentication</td>
</tr>
<tr>
<td>A3 – Cross-Site Scripting (XSS)</td>
<td>A3:2017-Sensitive Data Exposure</td>
</tr>
<tr>
<td>A6 – Sensitive Data Exposure</td>
<td>A6:2017-Security Misconfiguration</td>
</tr>
<tr>
<td>A8 – Cross-Site Request Forgery (CSRF)</td>
<td>A8:2017-Insecure Deserialization [NEW, Community]</td>
</tr>
<tr>
<td>A9 – Using Components with Known Vulnerabilities</td>
<td>A9:2017-Using Components with Known Vulnerabilities</td>
</tr>
</tbody>
</table>

https://www.heise.de/developer/imgs/06/2/3/6/0/4/7/9/2013-2017-50ed36036974520.png [Date: 04.06.2020]
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Questions</th>
</tr>
</thead>
</table>
| Authority of the producer      | • Is the publishing organization reputable? E.g., the Software Engineering Institute (SEI)  
• Is an individual author associated with a reputable organization?  
• Has the author published other work in the field?  
• Does the author have expertise in the area? (e.g. job title principal software engineer) |                                                                                                                                                                                                                                                                             |
| Methodology                    | • Does the source have a clearly stated aim?  
• Does the source have a stated methodology?  
• Is the source supported by authoritative, contemporary references?  
• Are any limits clearly stated?  
• Does the work cover a specific question?  
• Does the work refer to a particular population or case? |                                                                                                                                                                                                                                                                             |
| Objectivity                    | • Does the work seem to be balanced in presentation?  
• Is the statement in the sources as objective as possible? Or, is the statement a subjective opinion?  
• Is there vested interest? E.g., a tool comparison by authors that are working for particular tool vendor  
• Are the conclusions supported by the data? |                                                                                                                                                                                                                                                                             |
| Date                           | • Does the item have a clearly stated date? |                                                                                                                                                                                                                                                                             |
| Position w.r.t. related sources| • Have key related GL or formal sources been linked to / discussed? |                                                                                                                                                                                                                                                                             |
| Novelty                        | • Does it enrich or add something unique to the research?  
• Does it strengthen or refute a current position? |                                                                                                                                                                                                                                                                             |
| Impact                         | • Normalize all the following impact metrics into a single aggregated impact metric (when data are available): Number of citations, Number of backlinks, Number of social media shares (the so-called “alt-metrics”), Number of comments posted for a specific online entries like a blog post or a video, Number of page or paper views |                                                                                                                                                                                                                                                                             |
| Outlet type                    | • 1<sup>st</sup> tier GL (measure=1): High outlet control/ High credibility: Books, magazines, theses, government reports, white papers  
• 2<sup>nd</sup> tier GL (measure=0.5): Moderate outlet control/ Moderate credibility: Annual reports, news articles, presentations, videos, Q/A sites (such as StackOverflow), Wiki articles  
• 3<sup>rd</sup> tier GL (measure=0): Low outlet control/ Low credibility: Blogs, emails, tweets |                                                                                                                                                                                                                                                                             |

## Quality assessment in MLRs (cont’d)

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>is the publishing organization reputable?</td>
</tr>
<tr>
<td></td>
<td>is the author published or associated with a reputable organization?</td>
</tr>
<tr>
<td></td>
<td>Does the author have expertise in the area?</td>
</tr>
<tr>
<td>Methodology</td>
<td>Does the source have a clearly stated aim?</td>
</tr>
<tr>
<td></td>
<td>Does the source have a stated methodology?</td>
</tr>
<tr>
<td></td>
<td>is the source supported by authoritative, documented references?</td>
</tr>
<tr>
<td></td>
<td>Are any limits clearly stated?</td>
</tr>
<tr>
<td></td>
<td>Does the work cover a specific question?</td>
</tr>
<tr>
<td></td>
<td>Does the work refer to a particular population?</td>
</tr>
<tr>
<td>Objectivity</td>
<td>Does the work seem to be balanced in presentation?</td>
</tr>
<tr>
<td></td>
<td>is the statement in the sources as objective as possible?</td>
</tr>
<tr>
<td></td>
<td>Are the conclusions supported by the data?</td>
</tr>
<tr>
<td>Date</td>
<td>Does the item have a clearly stated date?</td>
</tr>
<tr>
<td>Position</td>
<td>Have key related GL.</td>
</tr>
<tr>
<td></td>
<td>sources been linked to / discussed?</td>
</tr>
<tr>
<td>Noveltvity</td>
<td>Does it enrich or add something unique to the review?</td>
</tr>
<tr>
<td></td>
<td>Does it strengthen or refute a current position?</td>
</tr>
<tr>
<td>Outlet type</td>
<td>Outlet Tier</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>is the publishing organization reputable?</td>
</tr>
<tr>
<td></td>
<td>is the author published or associated with a reputable organization?</td>
</tr>
<tr>
<td></td>
<td>Does the author have expertise in the area?</td>
</tr>
<tr>
<td>Methodology</td>
<td>Does the source have a clearly stated aim?</td>
</tr>
<tr>
<td></td>
<td>Does the source have a stated methodology?</td>
</tr>
<tr>
<td></td>
<td>is the source supported by authoritative, documented references?</td>
</tr>
<tr>
<td></td>
<td>Are any limits clearly stated?</td>
</tr>
<tr>
<td></td>
<td>Does the work cover a specific question?</td>
</tr>
<tr>
<td></td>
<td>Does the work refer to a particular population?</td>
</tr>
<tr>
<td>Objectivity</td>
<td>Does the work seem to be balanced in presentation?</td>
</tr>
<tr>
<td></td>
<td>is the statement in the sources as objective as possible?</td>
</tr>
<tr>
<td></td>
<td>Are the conclusions supported by the data?</td>
</tr>
<tr>
<td>Date</td>
<td>Does the item have a clearly stated date?</td>
</tr>
<tr>
<td>Position</td>
<td>Have key related GL.</td>
</tr>
<tr>
<td></td>
<td>sources been linked to / discussed?</td>
</tr>
<tr>
<td>Noveltvity</td>
<td>Does it enrich or add something unique to the review?</td>
</tr>
<tr>
<td></td>
<td>Does it strengthen or refute a current position?</td>
</tr>
<tr>
<td>Outlet type</td>
<td>Outlet Tier</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>is the publishing organization reputable?</td>
</tr>
<tr>
<td></td>
<td>is the author published or associated with a reputable organization?</td>
</tr>
<tr>
<td></td>
<td>Does the author have expertise in the area?</td>
</tr>
<tr>
<td>Methodology</td>
<td>Does the source have a clearly stated aim?</td>
</tr>
<tr>
<td></td>
<td>Does the source have a stated methodology?</td>
</tr>
<tr>
<td></td>
<td>is the source supported by authoritative, documented references?</td>
</tr>
<tr>
<td></td>
<td>Are any limits clearly stated?</td>
</tr>
<tr>
<td></td>
<td>Does the work cover a specific question?</td>
</tr>
<tr>
<td></td>
<td>Does the work refer to a particular population?</td>
</tr>
<tr>
<td>Objectivity</td>
<td>Does the work seem to be balanced in presentation?</td>
</tr>
<tr>
<td></td>
<td>is the statement in the sources as objective as possible?</td>
</tr>
<tr>
<td></td>
<td>Are the conclusions supported by the data?</td>
</tr>
<tr>
<td>Date</td>
<td>Does the item have a clearly stated date?</td>
</tr>
<tr>
<td>Position</td>
<td>Have key related GL.</td>
</tr>
<tr>
<td></td>
<td>sources been linked to / discussed?</td>
</tr>
<tr>
<td>Noveltvity</td>
<td>Does it enrich or add something unique to the review?</td>
</tr>
<tr>
<td></td>
<td>Does it strengthen or refute a current position?</td>
</tr>
<tr>
<td>Outlet type</td>
<td>Outlet Tier</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>is the publishing organization reputable?</td>
</tr>
<tr>
<td></td>
<td>is the author published or associated with a reputable organization?</td>
</tr>
<tr>
<td></td>
<td>Does the author have expertise in the area?</td>
</tr>
<tr>
<td>Methodology</td>
<td>Does the source have a clearly stated aim?</td>
</tr>
<tr>
<td></td>
<td>Does the source have a stated methodology?</td>
</tr>
<tr>
<td></td>
<td>is the source supported by authoritative, documented references?</td>
</tr>
<tr>
<td></td>
<td>Are any limits clearly stated?</td>
</tr>
<tr>
<td></td>
<td>Does the work cover a specific question?</td>
</tr>
<tr>
<td></td>
<td>Does the work refer to a particular population?</td>
</tr>
<tr>
<td>Objectivity</td>
<td>Does the work seem to be balanced in presentation?</td>
</tr>
<tr>
<td></td>
<td>is the statement in the sources as objective as possible?</td>
</tr>
<tr>
<td></td>
<td>Are the conclusions supported by the data?</td>
</tr>
<tr>
<td>Date</td>
<td>Does the item have a clearly stated date?</td>
</tr>
<tr>
<td>Position</td>
<td>Have key related GL.</td>
</tr>
<tr>
<td></td>
<td>sources been linked to / discussed?</td>
</tr>
<tr>
<td>Noveltvity</td>
<td>Does it enrich or add something unique to the review?</td>
</tr>
<tr>
<td></td>
<td>Does it strengthen or refute a current position?</td>
</tr>
<tr>
<td>Outlet type</td>
<td>Outlet Tier</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority</td>
<td>is the publishing organization reputable?</td>
</tr>
<tr>
<td></td>
<td>is the author published or associated with a reputable organization?</td>
</tr>
<tr>
<td></td>
<td>Does the author have expertise in the area?</td>
</tr>
<tr>
<td>Methodology</td>
<td>Does the source have a clearly stated aim?</td>
</tr>
<tr>
<td></td>
<td>Does the source have a stated methodology?</td>
</tr>
<tr>
<td></td>
<td>is the source supported by authoritative, documented references?</td>
</tr>
<tr>
<td></td>
<td>Are any limits clearly stated?</td>
</tr>
<tr>
<td></td>
<td>Does the work cover a specific question?</td>
</tr>
<tr>
<td></td>
<td>Does the work refer to a particular population?</td>
</tr>
<tr>
<td>Objectivity</td>
<td>Does the work seem to be balanced in presentation?</td>
</tr>
<tr>
<td></td>
<td>is the statement in the sources as objective as possible?</td>
</tr>
<tr>
<td></td>
<td>Are the conclusions supported by the data?</td>
</tr>
<tr>
<td>Date</td>
<td>Does the item have a clearly stated date?</td>
</tr>
<tr>
<td>Position</td>
<td>Have key related GL.</td>
</tr>
<tr>
<td></td>
<td>sources been linked to / discussed?</td>
</tr>
<tr>
<td>Noveltvity</td>
<td>Does it enrich or add something unique to the review?</td>
</tr>
<tr>
<td></td>
<td>Does it strengthen or refute a current position?</td>
</tr>
<tr>
<td>Outlet type</td>
<td>Outlet Tier</td>
</tr>
</tbody>
</table>
Search strategy
Concept distribution between artifacts

Academic literature

Grey literature

- Framework
- Case study
- Prototype
- Survey
- Tool evaluation
- Tool overview

- Book
- Blog post / Web article
- Presentation
- Whitepaper
- Youtube video
- Thesis
- Report
GOVERNANCE

STRATEGY & METRICS (SM)
• SM1.1 Publish process and evolve as necessary.
• SM1.2 Create evangelism role and perform internal marketing.
• SM1.3 Educate executives.
• SM1.4 Identify gate locations, gather necessary artifacts.
• SM2.1 Publish data about software security internally.
• SM2.2 Enforce gates with measurements and track exceptions.
• SM2.3 Create or grow a satellite.
• SM2.6 Require security sign-off.
• SM3.1 Use an internal tracking application with portfolio view.
• SM3.2 Run an external marketing program.
• SM3.3 Identify metrics and use them to drive budgets.
• SM3.4 Integrate software-defined lifecycle governance.

COMPLIANCE & POLICY (CP)
• CP1.1 Unify regulatory pressures.
• CP1.2 Identify PII obligations.
• CP1.3 Create policy.
• CP2.1 Identify PII inventory.
• CP2.2 Require security sign-off for compliance-related risk.
• CP2.3 Implement and track controls for compliance.
• CP2.4 Include software security SLAs in all vendor contracts.
• CP2.5 Ensure executive awareness of compliance and privacy obligations.
• CP3.1 Create a regulator compliance story.
• CP3.2 Impose policy on vendors.
• CP3.3 Drive feedback from software lifecycle data back to policy.

TRAINING (T)
• T1.1 Conduct awareness training.
• T1.6 Deliver role-specific advanced curriculum.
• T1.7 Deliver on-demand individual training.
• T2.5 Enhance satellite through training and events.
• T2.6 Include security resources in onboarding.
• T2.8 Create and use material specific to company history.
• T3.1 Reward progression through curriculum.
• T3.2 Provide training for vendors or outsourced workers.
• T3.3 Host software security events.
• T3.4 Require an annual refresher.
• T3.5 Establish SSG office hours.
• T3.6 Identify new satellite members through training.

INTELLIGENCE

ATTACK MODELS (AM)
• AM1.2 Create a data classification scheme and inventory.
• AM1.3 Identify potential attackers.
• AM1.5 Gather and use attack intelligence.
• AM2.1 Build attack patterns and abuse cases tied to potential attackers.
• AM2.2 Create technology-specific attack patterns.
• AM2.5 Build and maintain a top N possible attacks list.
• AM2.6 Collect and publish attack stories.
• AM2.7 Build an internal forum to discuss attacks.
• AM3.1 Have a science team that develops new attack methods.
• AM3.2 Create and use automation to mimic attackers.
• AM3.3 Monitor automated asset creation.

SECURITY FEATURES & DESIGN (SFD)
• SFD1.1 Build and publish security features.
• SFD1.2 Engage the SSG with architecture teams.
• SFD2.1 Leverage secure-by-design middleware frameworks and common libraries.
• SFD2.2 Create an SSG capability to solve difficult design problems.
• SFD3.1 Form a review board or central committee to approve and maintain secure design patterns.
• SFD3.2 Require use of approved security features and frameworks.
• SFD3.3 Find and publish mature design patterns from the organization.

STANDARDS & REQUIREMENTS (SR)
• SR1.1 Create security standards.
• SR1.2 Create a security portal.
• SR1.3 Translate compliance constraints to requirements.
• SR2.1 Create a standards review board.
• SR2.4 Identify open source.
• SR2.5 Create SLA boilerplate.
• SR3.1 Control open source risk.
• SR3.2 Communicate standards to vendors.
• SR3.3 Use secure coding standards.
• SR3.4 Create standards for technology stacks.
SSDL TOUCHPOINTS

ARCHITECTURE ANALYSIS (AA)
- AA1.1 Perform security feature review.
- AA1.2 Perform design review for high-risk applications.
- AA1.3 Have SSG lead design review efforts.
- AA1.4 Use a risk questionnaire to rank applications.
- AA2.1 Define and use AA process.
- AA2.2 Standardize architectural descriptions.
- AA3.1 Have engineering teams lead AA process.
- AA3.2 Drive analysis results into standard architecture patterns.
- AA3.3 Make the SSG available.

CODE REVIEW (CR)
- CR1.2 Have the SSG perform ad hoc review.
- CR1.4 Use automated tools along with manual review.
- CR1.5 Make code review mandatory for all projects.
- CR1.6 Use centralized reporting to close the knowledge loop and drive training.
- CR2.5 Assign tool mentors.
- CR2.6 Use automated tools with tailored rules.
- CR2.7 Use a top N bugs list (real data preferred).
- CR3.2 Build a capability to combine assessment results.
- CR3.3 Eradicate specific bugs from the entire codebase.
- CR3.4 Automate malicious code detection.
- CR3.5 Enforce coding standards. ST1.1 Ensure QA supports edge/boundary value condition testing.

SECURITY TESTING (ST)
- ST1.3 Drive tests with security requirements and security features.
- ST2.1 Integrate black-box security tools into the QA process.
- ST2.4 Share security results with QA.
- ST2.5 Include security tests in QA automation.
- ST2.6 Perform fuzz testing customized to application APIs.
- ST3.3 Drive tests with risk analysis results.
- ST3.4 Leverage coverage analysis.
- ST3.5 Begin to build and apply adversarial security tests (abuse cases).

DEPLOYMENT

PENETRATION TESTING (PT)
- PT1.1 Use external penetration testers to find problems.
- PT1.2 Feed results to the defect management and mitigation system.
- PT1.3 Use penetration testing tools internally.
- PT2.2 Penetration testers use all available information.
- PT2.3 Schedule periodic penetration tests for application coverage.
- PT3.1 Use external penetration testers to perform deep-dive analysis.
- PT3.2 Have the SSG customize penetration testing tools and scripts.

SOFTWARE ENVIRONMENT (SE)
- SE1.1 Use application input monitoring.
- SE1.2 Ensure host and network security basics are in place.
- SE2.2 Publish installation guides.
- SE2.4 Use code signing.
- SE3.2 Use code protection.
- SE3.3 Use application behavior monitoring and diagnostics.
- SE3.4 Use application containers.
- SE3.5 Use orchestration for containers and virtualized environments.
- SE3.6 Enhance application inventory with operations bill of materials.
- SE3.7 Ensure cloud security basics.

CONFIGURATION MANAGEMENT & VULNERABILITY MANAGEMENT (CMVM)
- CMVM1.1 Create or interface with incident response.
- CMVM1.2 Identify software defects found in operations monitoring and feed them back to development.
- CMVM2.1 Have emergency codebase response.
- CMVM2.2 Track software bugs found in operations monitoring and feed them back to development.
- CMVM2.3 Develop an operations inventory of applications.
- CMVM3.1 Fix all occurrences of software bugs found in operations.
- CMVM3.2 Enhance the SSDL to prevent software bugs found in operations.
- CMVM3.3 Simulate software crises.
- CMVM3.4 Operate a bug bounty program.
- CMVM3.5 Automate verification of operational infrastructure security [10]
Demographic distribution of grey and academic literature

Number of artifacts by year for grey and academic literature.
Tool-support of BSIMM10-activities

Distribution per BSIMM-dimension

© sebis
John Nguyen (TUM)
Distribution between free and commercial tools

Number of tools

Free

Commercial
Tool-support of BSIMM10-activities

Distribution per BSIMM-practice
Cross-tool-integration

- Developers often use several tools to improve the estimation and validity of the analysis [6, Sec. Secure code scanning tools]
- One tool alone is often insufficient for an in-depth analysis [7]
- Platform tools are facilitated to combine different results of tools
  - CloudPassage Halo (https://www.cloudpassage.com/)
  - digital.ai (https://digital.ai/)
  - GitLab (https://about.gitlab.com/)
  - Splunk Phantom (https://www.splunk.com/)


