BSIMM QUESTIONS FOR TEAMS

Welcome, and thanks for taking the time to fill answer the questions below. The objective is to map the existing application security practices to the BSIMM (Building Security In Maturity Model).

Please try to answer the questions bellow quickly, and make a note if you don't understand the question.

PII - Personal Identifiable Information
SLA - Service Level Agreements
WAF - Web Application Firewall
DAST - Dynamic Application Security Testing (BlackBox)
SAST - Static Application Security Testing (WhitBox)

Your name: _____ , You role: _____ , Team: _____ , Today's date: _____

Type of Application : _____ , Technology Stack: _____

Version: 0.5 (26/April/2016)

BSIMM Activity	Question	Yes	No	N/A	If Yes, 'where is info about it?' / If No, 'why not?'
SM1.1	Is there a formal SDL (Software Development Lifecycle) used?	☐	☐	☐	
CP1.1	Are there any regulatory or compliance drivers? (to do Security)	☐	☐	☐	
CP2.1	Does the application holds PII data?	☐	☐	☐	
CP3.2	Are 3rd parties involved in development?	☐	☐	☐	
CP3.2	Are there security SLAs for 3rd party development teams?	☐	☐	☐	
T1.1	Have all developers received Application Security Awareness training?	☐	☐	☐	
T1.2	Have all developers received role-specific Application Security training?	☐	☐	☐	
T2.5	Do new hires receive Application Security Training?	☐	☐	☐	
T3.2	Do 3rd party or outsourced developers receive Application Security Training?	☐	☐	☐	
T3.4	Is there an annual refresh of Application Security Training?	☐	☐	☐	
AM1.2	Is there an data classification scheme?	☐	☐	☐	
AM1.2	Is there an inventory of how classified data maps to existing applications?	☐	☐	☐	
AM1.3	Is there a mapping of the attackers to be worried about?	☐	☐	☐	
AM1.4	Is there information on past attacks (successful or not)?	☐	☐	☐	
SFD1.1	Are there standard security features? (i.e. Secure Controls)	☐	☐	☐	
SDF1.2	Are Security Champions (SCs) involved Architecture and Design?	☐	☐	☐	
SDF1.2	Are Security Champions doing Threat Models for existing/new Apps or features?	☐	☐	☐	
SR1.1	Are there Security Standards for development?	☐	☐	☐	
SR1.2	Is there an Software Security Portal?	☐	☐	☐	
SR1.3	Are there Software requirements based on Compliance constraints?	☐	☐	☐	
SR2.4	For in-housed developed apps, is Open Source components usage tracked?	☐	☐	☐	
SR2.4	For 3rd party dependencies or apps, is Open Source components usage tracked?	☐	☐	☐	
SR2.6	Are there Secure Coding Guidelines?	☐	☐	☐	
SR2.5	Is there a standard SLA boilerplate for vendor contracts & outsourcing providers? (mapping required Software Security efforts)	☐	☐	☐	
AA1.1	Have apps been Threat Modelled?	☐	☐	☐	
AA1.4	Is there a risk questionnaire to rank Applications and Features?	☐	☐	☐	
CR1.1	Is there a list of the most dangerous bugs/vulnerabilities that developers should be aware of?	☐	☐	☐	
CR1.2	Have Security Reviews been done to the released applications?	☐	☐	☐	
CR1.5	Have security-focused code reviews been done on released applications?	☐	☐	☐	
CR2.2	Are secure coding standards enforced?	☐	☐	☐	
ST1.1	Does QA perform basic Security or Adversarial tests?	☐	☐	☐	
ST2.1	Are there BlackBox (DAST) tools executed by QA?	☐	☐	☐	
ST2.5	Are there automated security tests executed by QA?	☐	☐	☐	
ST2.6	Are there Fuzz tests executed by QA?	☐	☐	☐	
ST3.4	Is Code Coverage measured for Security tools/tests execution?	☐	☐	☐	
PT1.1	Have applications been penetration tested?	☐	☐	☐	
PT1.2	Are penetration tests results added to JIRA?	☐	☐	☐	
PT2.2	Do penetration testers have access to all available information? (for example source-code, JIRA tickets, test accounts)	☐	☐	☐	
PT2.3	Is there an periodic penetration testing sheadule?	☐	☐	☐	
SE1.1	Is application live input captured and monitored?	☐	☐	☐	
SE1.1	Is live data sent to InfoSec monitoring systems? (Splunk based)	☐	☐	☐	
SE1.1	Is there an WAF protecting the applications?	☐	☐	☐	
SE1.4	Are hosts and networks configured securely?	☐	☐	☐	
SE2.2	Are there secure installation and deployment guidelines?	☐	☐	☐	
SE2.4	Is code developed signed?	☐	☐	☐	
SE3.2	Are applications executed with code protection? (DEP, ASLR, VM Sandboxes)	☐	☐	☐	
SE3.3	Are live applications monitored for misbehaviours or signs of attacks?	☐	☐	☐	

CMVM1.1	Is there an incident response plan?	☐	☐	☐	
CMVM1.2	Are bugs and security issues being identified via live monitoring?	☐	☐	☐	
CMVM2.1	Is there an emergency codebase response plan? (i.e. quickly push code fixes to production)	☐	☐	☐	
CMVM2.3	Is there an operation inventory of deployed applications?	☐	☐	☐	
Feedback:	Please use this space to enter comments, problems or recommendations (for example missing questions)				

BSIMM QUESTIONS FOR TEAMS (NOT ASKED)

BSIMM Activity	Question	Yes	No	N/A	If Yes, 'where is info about it?' / If No, 'why not?'
SM1.4	Are there security hooks into the SDL that gather artefacts (new code deployments, test execution results, binaries)	☐	☐	☐	
SM2.3	Is there an Security Champion?	☐	☐	☐	
CP1,2	Have PII obligations been identified?	☐	☐	☐	
CP2.2	Are compliance-related risks signed off?	☐	☐	☐	
CP2.4	Do 3rd Party vendor contracts have software security SLAs?	☐	☐	☐	
CP2.5	Are executives aware of compliance and privacy obligations?	☐	☐	☐	
CP3.2	Are Security policies imposed on 3rd party vendors?	☐	☐	☐	
T1.6	Is training material specific to current tech stack and company history?	☐	☐	☐	
T1.7	Is there on-demand individual security training?	☐	☐	☐	
T2.6	Do new developers received relevant Security training?	☐	☐	☐	
ST1.3	Are security requirements are insecurity features used to drive tests?	☐	☐	☐	
ST1.3	Are there security focused tests?	☐	☐	☐	
ST2.3	Is risk analysis used to drive tests?	☐	☐	☐	
ST3.4	Are there adversarial security tests?	☐	☐	☐	
CMVM2.2	Are reported security issues found tracked thought-out its fix process? (reported by code-review, QA, pentest or externally)	☐	☐	☐	
CMVM3.1	Are all reported security issues fixed?	☐	☐	☐	
CMVM3.2	Is Security SDL changed in order to prevent creating of reported security issues?	☐	☐	☐	

BSIMM QUESTIONS FOR SGS (SOFTWARE SECURITY GROUP)

BSIMM Activity	Question	Yes	No	N/A	If Yes, 'where is info about it?' / If No, 'why not?'
SM1.2	Is there an active SSG (Software Security Group)?	☐	☐	☐	
SM1.3	Have executives even educated on InfoSec and AppSec?	☐	☐	☐	
SM2.1	Is data about software security published internally?	☐	☐	☐	
SM2.2	Are there at least two deployment pipelines (with one having the ability to block the release)?	☐	☐	☐	
SM2.5	Do security metrics exist and published in security portal?	☐	☐	☐	
SM2.5	Is Security budget based on real-world metrics and data?	☐	☐	☐	
SM2.6	Are Security risk explicitly signed off by business owners and management?	☐	☐	☐	
CP1.3	Is there an Software Security Policty?	☐	☐	☐	
CP2.3	Are compliance controls tracked?	☐	☐	☐	
CP3.1	Is management security reports and operational data used by compliance assessments?	☐	☐	☐	
CP3.3	Does feedback from Secure SDL influence policies?	☐	☐	☐	
T2.5	Are there regular Security Champions meetings? (weekly or monthly)	☐	☐	☐	
T2.7	Is there a process to identify and onboard Security Champions?	☐	☐	☐	
T3.1	Are there rewards (or corporate perks) for Security Champions?	☐	☐	☐	
T3.3	Are there Software Security events hosted internally, but allowing external participation? (for ex: OWASP chapter meeting)	☐	☐	☐	
T3.5	Are there scheduled office hours when Software Security support is provided?	☐	☐	☐	
AM1.1	Is there a list of top N possible attacks?	☐	☐	☐	
AM1.5	Are new types of attacks and vulnerabilities researched?	☐	☐	☐	
AM1.6	Are there collaboration forums for Security Champions? (Slack or mailing lists)	☐	☐	☐	
AM2.1	Are attack patterns and abuse cases mapped to attackers?	☐	☐	☐	
AM2.2	Are technologic specific attack patterns created by internal research teams?	☐	☐	☐	
	Is there a an internal research team that develops new attack methods?	☐	☐	☐	
AM3.2	Is QA able to automate and replicate new types of attacks and exploits?	☐	☐	☐	
SFD2.1	Are there secure-by-design frameworks or common libraries?	☐	☐	☐	
SDF2.2	Is there capability to support the solution of difficult secure design problems?	☐	☐	☐	
SDF3.1	Is there a central group that maintains secure design patterns?	☐	☐	☐	
SDF3.2	Is use of approved security features and frameworks required?	☐	☐	☐	
SDF3.3	Are mature design patterns documented and published?	☐	☐	☐	
SR2.2	Is there a standards review board?	☐	☐	☐	
SR2.3	Are there standards for used technology stacks?	☐	☐	☐	
SR3.1	Is expose to Open Source vulnerabilities managed?	☐	☐	☐	
SR3.2	Are 3rd party vendors aware of existing security standards and policies?	☐	☐	☐	
AA1.2	Are security design reviews performed on high risk applications?	☐	☐	☐	
AA2.2	Are architecture descriptions and data flows standardised?	☐	☐	☐	
AA2.3	Is Architecture Analysis available as an resource or mentoring?	☐	☐	☐	
AA3.1	Does InfoSec or AppSec have software architects that can lead design review efforts?	☐	☐	☐	
AA3.2	Do analysis results feed into standard architecture patterns?	☐	☐	☐	
CR1.4	Are static analysis tools (SAST) used to help security code review activities?	☐	☐	☐	
CR1.6	Is centralised reporting used to close the knowledge loop and drive training?	☐	☐	☐	
CR2.5	Are security tools (when used by developers) supported by mentors?	☐	☐	☐	
CR2.6	Are security tools (SAST, DAST) executed with targeted and customised rules?	☐	☐	☐	
CR3.2	Are multiple analysis techniques and tools combined into consolidated reports?	☐	☐	☐	
CR3.3	Is there the capability to eradicating specific bugs/vulnerabilities from existing codebase?	☐	☐	☐	
CR3.4	Is malicious code written by in-house our outsource developers automatically identified?	☐	☐	☐	
ST2.4	Are security results shared with QA?	☐	☐	☐	
PT1.3	Are penetration testing tools used internally?	☐	☐	☐	
PT3.1	Do external penetration testers perform deep-dive analysis?	☐	☐	☐	
PT3.2	Are penetration testing testing tools and scripts customised?	☐	☐	☐	
CMVM3.3	Are software crisis and attacks simulated?	☐	☐	☐	
CMVM3.4	Is there an bug bounty program?	☐	☐	☐	