BSIMM Framework Domains and Practices

Megan Leonard

ISEC 475

6/18/2023

BSIMM, building security in maturity model, is made up of 4 domains that house the 12 practices of the framework. Each domain covers its own area within the model, and each has 3 of the 12 practices inside. The areas are governance, intelligence, SSDL Touchpoints, and deployment.

The governance domain looks over the management of the software security such as the workers and the rules to follow. The first of its practices is strategy and metrics which looks at creating a plan, roles, and responsibilities that are needed to reach their security goals such as creating roles like log manager or network manager, and they need to track the traffic of the application. The second is compliance and policy which goes over the rules associated with the created roles and how to comply with the software security policies, this could be like how the network manager is to only access the network side and the inside connections. Then we have training which is teaching the employees how their roles work, what to expect, and awareness of threats. They look at the human side and work to make sure people have the knowledge that they need to complete their responsibilities and take on their roles. An example would be how the network manager can access the network and what they need to do inside and what they should record.

Intelligence starts with creating the models and security that will be able to follow the standards and adhere to the policies. The first of the practices is the attack model which is creating threat models, data patterns, and attack patterns. This is to gather information on the threats that you may face in the future such as malware or shoulder surfing. Then there is security features and design which takes the gathered information and organizes it so we can see patterns and start building frameworks for the major security controls and security design. This could be like using the NIST security framework or CISCO. Then we have the standards and requirements where you are creating the security standards that best fit your security controls and design, this could be the implementation of firewalls or setting up role-based access control. This leads to the creation of the standards review board who make sure that the standards are being followed.

SSDL Touchpoints look at quality control to make sure that everything is going as planned and nothing is being forgotten or not given enough attention. The first requirement in this domain is the architecture analysis where they will look at the software architecture and run it against the risks and threats from the attack models like how it can hold against brute force attacks or malware. This will be reviewed and planned to fix it should the structure not hold against the threats. Then we have the code review where we look over the code to check it in different areas like performance and if any parts of the code are redundant or repeating. These can have custom rules to follow based on the organization and their needs. Finally, we have the security testing where you run the different security tests to see how it runs against threats and attacks like black box testing to find any vulnerabilities that could be exploited such as open unprotected ports.

The final domain is deployment which expands on the threat response, patches, and updates. The first of its practices is the penetration testing with is the vulnerability testing that is done for the final version. This is the time to make sure known vulnerabilities are covered and threats are mitigated. After this is the software environment which looks at the digital side such as firewalls, the operating system, patching, and installation documentation. This is looking at the software set up that is needed for the final configuration to work. Finally, we have the configuration and vulnerability management which is the patches and updates for the application after it’s been released to handle incidents and up the protection as new threats arise.

Citation:

CyLab, C. M. (n.d.). *Evolving rapidly, BSIMM2 offers key elements of successful software security initiatives shared by 30 major corporations*. CyBlog.

<http://www.cyblog.cylab.cmu.edu/2010/05/evolving-rapidly-bsimm2-offers-key.html>

McGraw, G. (2009). *Owasp Foundation*. Building Security In Maturity Model. <https://owasp.org/www-pdf-archive//Bsimm09.pdf>

McGraw, G., Migues, S., & West, J. (2015). *School of Informatics | The University of Edinburgh*. BSIMM. <https://www.inf.ed.ac.uk/teaching/courses/sp/2015/lecs/BSIMM6.pdf>

Mead, N. R., & Woody, C. C. (2017). *Cyber Security Engineering: A practical approach for systems and software assurance*. Addison-Wesley.

*What is the BSIMM and how does it work?*. Synopsys. (n.d.). <https://www.synopsys.com/glossary/what-is-bsimm.html>