Coaching a Team Through Secure Development Lifecycle:

How effective is it?

Tandon School of Engineering, New York University, Brooklyn, NY 11201

Hypotyposis/Abstract— It is hypothesized that coaching a development team to build security into the products and services they develop can reduce the frequency of security vulnerabilities and/or security incidents overtime.

1. Introduction

“There is always a trade-off between usability and security. And between cost and risk”. [1]. This thinking has led to the rise of DevSecOps, or also known as secure development lifecycle (SDL). “DevSecOps is a transformational shift that incorporates secure culture, practices, and tools into each phase of the DevOps process.” [2]. That were SDL coaching comes in. An SDL coach will meet with a development team and coach them through DevSecOps principles including security testing, codes reviews, configuration, and vulnerability management [2].

In this extended abstract, I would like to see if SDL coaching can reduce a development teams cybersecurity risk. To do this, I will use vulnerability data from application development teams to see if the average vulnerability severity, based on the CVSS v3.1 [3] score, decreases once the team is onboarded to an SDL coaching program.

1. Related Works

Kokinen in their thesis *DevSecOps: Building Security into the core of DevOps* takes the approach of “a Systematic Literature Review to discover how security actives can be added into the core of the DevOps development process…”. [1]. This approach is effective in outlining a DevSecOps workflow but does little to demonstrate if that workflow can reduce cyber risk. In this extended abstract, I compare vulnerability data from various security resources to see if coaching a team to build security into their development process can reduce the severity of a security vulnerability.

Sohel and authors in their abstract *OWASP Top 10 – Do Startups Care?* “Performed penetration testing on applications made by five startup companies” to see if those startups were building applications that limited the number of OWASP vulnerabilities. [2] This approach is effective to determine if statups know and are aware of the OWASP Top 10 vulnerabilities, however it does not provided insight into = if consistent Secure Development coaching can successfully reduce the severity of security vulnerabilities. A secure development coaching program is built on the foundation that an organization is aware of the OWASP Top 10, however I would like to see how effective the coaching is in reducing high risk vulnerabilities.

1. Metrics (in-progress)

For the related data, I will compare average severity of security vulnerabilities from DAST/ SAST code vulnerability tolls, before onboarding to the coaching program vs. after onboarding to the coaching program to see if the severity of the security vulnerabilities decreased after the team onboarded to the coaching program.

From here on is not in use. It is saved for the format.

Page Layout

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it or use the paste function.

1. Page Layout

The paper can be maximum ten pages in length.

Your paper must use a page size corresponding to the US Letter paper size, which is 216mm (8.5") wide and 279mm (11 ") long. The margins must be set as follows:

* Top = 18mm (0.7")
* Bottom = 18mm (0.7")
* Left = Right = 16.5mm (0.65")

Your paper must be in two column format with a column width of 90mm (3.55") and a space of 5mm (0.2") between columns.

Do not edit the header or footer of the document. Page numbers will be inserted later.

1. Page Style

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

1. Text Font of Entire Document

The entire document should be in Times New Roman or Times font. Type 3 fonts must not be used. Other font types may be used if needed for special purposes.

Recommended font sizes are shown in Table 1.

1. Title and Author Details

Title must be in 24 pt Regular font. Author name must be in 11 pt Regular font. Author affiliation must be in 10 pt Italic. Contact email address must be in 9 pt Courier Regular font.

TABLE I  
Font Sizes for Papers

|  |  |  |  |
| --- | --- | --- | --- |
| Font Size | Appearance (in Time New Roman or Times) | | |
| Regular | Bold | Italic |
| 8 | table caption (in Small Caps),  figure caption,  reference item |  | reference item (partial) |
| 9 | Contact author email address (in Courier), cell in a table | abstract body | abstract heading (also in Bold) |
| 10 | level-1 heading (in Small Caps),  paragraph |  | level-2 heading,  level-3 heading,  author affiliation |
| 11 | author name |  |  |
| 24 | title |  |  |

All title and author details must be in single-column format and must be centered.

To avoid confusion, the family name must be written as the last part of each author name (e.g. John A.K. Smith).

Each affiliation must include, at the very least, the name of the institute/university and the name of the country where the author is based (e.g. University of Tokyo, Japan).

Email address is compulsory for the corresponding author.

1. Figures and Tables

Figures and tables must be centered in the column. Large figures and tables may span across both columns. Any table or figure that takes up more than 1 column width must be positioned either at the top or at the bottom of the page.

Graphics may be full color. All colors will be retained in the online proceedings but will be gray scale in the printed proceedings. Graphics must not use stipple fill patterns because they may not be reproduced properly. Please use only *SOLID FILL* colors which contrast well both on screen and on a black-and-white hardcopy, as shown in Fig. 1.



Fig. 1 A sample line graph using colors which contrast well both on screen and on a black-and-white hardcopy

Fig. 2 shows an example of a low-resolution image which would not be acceptable, whereas Fig. 3 shows an example of an image with adequate resolution. Check that the resolution is adequate to reveal the important detail in the figure.

Please check all figures in your paper both on screen and on a black-and-white hardcopy. When you check your paper on a black-and-white hardcopy, please ensure that:

* the colors used in each figure contrast well,
* the image used in each figure is clear,
* all text labels in each figure are legible.
* That each figure is centred.

1. Figure Captions

Figures must be numbered using Arabic numerals. Figure captions must be in 8 pt Regular font. Captions of a single line (e.g. Fig. 2) must be centered whereas multi-line captions must be justified (e.g. Fig. 1). Captions with figure numbers must be placed after their associated figures, as shown in Fig. 1.



Fig. 2 Example of an unacceptable low-resolution image



Fig. 3 Example of an image with acceptable resolution

1. Table Captions

Tables must be numbered using uppercase Roman numerals. Table captions must be centred and in 8 pt Regular font with Small Caps. Every word in a table caption must be capitalized except for short minor words as listed in Section III-B. Captions with table numbers must be placed before their associated tables, as shown in Table 1.

1. Page Numbers, Headers and Footers

Page numbers and footers must not be used. Please leave the header unchanged.

1. Links and Bookmarks

All hypertext links and section bookmarks will be removed from papers during the processing of papers for publication. If you need to refer to an Internet email address or URL in your paper, you must type out the address or URL fully in Regular font.

1. References

The heading of the References section must not be numbered. All reference items must be in 8 pt font. Please use Regular and Italic styles to distinguish different fields as shown in the References section. Number the reference items consecutively in square brackets (e.g. [1]).

When referring to a reference item, please simply use the reference number, as in [2]. Do not use “Ref. [3]” or “Reference [3]” except at the beginning of a sentence, e.g. “Reference [3] shows …”. Multiple references are each numbered with separate brackets (e.g. [2], [3], [4]–[6]).

1. Conclusions

This template is partly based on the IEEE extended abstract template.

Acknowledgment

The heading of the Acknowledgment section and the References section must not be numbered.

References

|  |  |
| --- | --- |
| *[1]* | *H. Sϕhoel, M. G. Jaatun and C. Boyd, “OWASP Top 10 - Do Startups Care?,” in 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), Glasgow, 2018.* |
| *[2]* | *A. Koskinen, DevSecOps: Building Security Into the Core of DevOps, Jyväskylä: M.S. Thesis, University of Jyväskylä's Faculty of Information Technology, 2020.* |
| *[3]* | *FIRST.Org, Inc, “Common Vulnerability Scoring System v3.1: User Guide,” [Online]. Available: https://www.first.org/cvss/v3.1/user-guide.* |