Solution Guide: Threat Modeling Step 6: Mitigating Risk

In this activity, you devised a risk mitigation plan based on analysis obtained in the previous activity.

1. Refer to the risk analysis you performed previously, and identify all of the risks you should monitor, manage, or mitigate.

    - XSS injection used to hook web app users' browsers.
    - SQL injection used to dump database.
    - Employee downloads backdoor into corporate intranet.
    - Engineer steals trading algorithms from technology database.

2. Suggest a security control for each risk.

    XSS injection used to hook web app users' browsers.

    - **Recommendation**: Use a framework to handle user input.
    - **Type**: Technical.
    - **Intent**: Preventive.
    - **Time to Implementation**: One quarter.
    - **Cost of Implementation**: Low (<$10k). Engineers must simply refactor existing code.

    SQL injection used to dump database. - **Recommendation**: Use a framework to handle user input. - **Type**: Technical. - **Intent**: Preventive. - **Time to Implementation**: One quarter. - **Cost of Implementation**: Low (<$10k). Engineers must simply refactor existing code.

    Employee downloads backdoor into corporate intranet.

    - **Recommendation**: Install antivirus over whole Enterprise domain.
    - **Type**: Technical,
    - **Intent**: Preventive.
    - **Time to Implementation**: Very fast.
    - **Cost of Implementation**: Very low (<$10). Cost is mostly due to licensing the software.

Engineer steals trading algorithms from technology database. - **Recommendation**: Restrict access to databases containing confidential information. - **Type**: Technical. - **Intent**: Preventive. - **Time to Implementation**: Very fast. - **Cost of Implementation**: Very low (<$10). Cost is mostly due to licensing the software.

3. Finally, rank these issues from least to most important, taking into consideration how much each solution costs.

    1. Employee downloads backdoor into corporate intranet.
    2. XSS injection used to hook web app users' browsers.
    3. Engineer steals trading algorithms from technology database.
    4. SQL injection used to dump database.

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.