TimeSheet Threat Model

REVIEW | HISTORY

Meets Specifications

Dear Student,

Congratulation🔥

You have successfully completed ✅ all of the tasks to secure the TimeSheets application from existing issues and future attacks.

This includes concerns that the IT and other responsible teams need to address. You have also mentioned detailed recommendations to give the concerned team proper directions to mitigation the concerns and issues. Issues related to encryption have been identified correctly and proper recommendations have been given to resolve these issues. Recommendations to secure infrastructure not limiting to only encryption are also given which will help access the current security issues and make the infrastructure more secure.

Keep up the good work!!👏🏽

Further Reading

- Vulnerability Scanning and Vulnerability Management
- Malware Detection Techniques

Vulnerability Analysis

✓ **Explain why the four identified encryption issues are considered vulnerabilities and the potential result of each exploited vulnerability.**

Great Job! 👍🏽

- You have correctly identified the different scenarios in which keeping unencrypted data at rest could be exploited
- In your explanation, you have given a practical example for each of the scenario.

Extra Resources

- Encryption Policy
- Vulnerability Assessment

✓ **There are several issues with the architecture. Provide one or more recommendations. What would you recommend to make this a secure architecture?**

Please explain your recommendation.

Great Job! 👍🏽

- You have correctly identified that firewall, redundancy, encryption are not present in the architecture.
- The recommendations have proper justification for how the use of firewalls could help secure the infrastructure.

Notes

There are other security measures that could also help to secure the architecture.

- Using firewalls both internal and external.
- Make use of redundancy to ensure high availability and use of backup sites in case if one site is down.

Extra Resources

- How to make infrastructure more secure

Risk Analysis

✓ **You must rank each of the four identified encryption issues and explain your ranking.**

Your explanations must be based on content from this course as well as observations from the initial report.

Great Job! 👍🏽

- You have correctly ranked each of the encryption issues with Data in transit encryption as most critical issue.
- Also you have provided good explanation to justify your risk score.

Notes

- Along with the risk description, mention of risk scoring scheme, will add more value to your justification of the risk.
- Risk scoring scheme refers to the parameters you considered while computing risk, Example, **risk = threat x vulnerability or likelihood x impact**

Extra Resources

- IT Security Risk Assessment Methodology

Mitigation Plan

✓ **You must create a mitigation plan with justification for your recommendations.**

The audience is engineering teams who may or may not have an understanding of why these are issues. Additionally, they may need assistance in implementing your recommendations. You must provide guidance on how to implement your recommendations.

Great work! You have created four mitigation plans for the four identified issues, with your recommendation justifications. All the justifications adhere to the feasible mitigation. I'd further like to recommend you to have a look at this resource for the implementation and progress monitoring of risk mitigation.

✓ **You must suggest steps that the audit team can take to ensure that the systemic encryption issues are solved going forward.**

Great Job! 👍🏽

You have recommended a good strategy to help audit team take necessary actions to mitigate the encryption issues.

Notes

Below is a list that audit team can take to ensure their encryption issue are resolved and patched.

Concerns that security team needs to address :

Insecure movement of keys, Insecure use of keys, Secure Re-use of keys, Non-rotation of keys, Inappropriate storage of keys, Inadequate protection of keys, Insecure movement of keys, Non-destruction of keys, etc.

Recommendation that security team could take :

Audit logging of key cycle, Use dual control, Split Knowledge of clear text encryption keys, Restrict access to encryption keys, Data assets must be classified, Full lifecycle management of keys, Generation of strong keys, Protection of keys using tamper-resistant HSM, Strict policy-based controls to prevent reuse/misuse of keys.

Extra Resources

- Cryptographic Key Management - Risks and Mitigation
- Guide to encryption key management

✓ **Using the diagram in section one, make changes and additions to address identified issues as well as other architectural problems. What changes would you make to existing systems? What additional systems would you add to increase security?**

Provide justifications for why you made those changes/additions.

✓ **Take your understanding of security issues a step further by looking beyond the identified encryption issues. What changes can you make (system or process) to avoid issues like this going forward?**

DOWNLOAD PROJECT

RETURN TO PATH