Activity Exemplar: Analysis of network hardening

Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity.

Completed Exemplar

To review the exemplar for this course item, click the link below and select *Use Template*.

Security risk assessment report exemplar

OR

If you don't have a Google account, you can download the exemplar directly from the attachment below.

Security risk assessment report exemplar
DOCX File

Assessment of Exemplar

Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.

Note: *The exemplar represents one possible explanation for the issues that the social media organization is facing. There are multiple correct security hardening tools and methods to use. What's important is that you identified the network hardening measures that are most effective for managing the vulnerabilities selected. In your role as a security analyst, you and your team would then explain your decisions and make a case for why those measures will be effective at securing the network.*

The exemplar focuses on the vulnerability of an outdated software for an on-premises database. One potential solution to the vulnerability is identified and included in the report for the direct supervisors. The report explains how the company might be compromised in the future if the database is not patched and if employees continue to share passwords.

In the section about the organization's information security policy, the report includes information about adding general security hardening practices, a recommendation for how often the hardening practices should be performed, and an explanation of what the potential

consequences are if the policy is not followed. This is one example of how a security risk assessment report can be analyzed and how an information security policy might be written.

Key Takeaways

As a security analyst, you may be responsible for initiating network security practices. Making executive decisions about which tools to use based on what you know about certain vulnerabilities will be a starting point for helping the organization improve its network security. Explaining and documenting your decisions as a cybersecurity analyst will help in the future if the network ever needs to be troubleshooted. It will also help give non-technical employees buy-in and help them follow security practices, such as multifactor authentication.