Case Study: Reviewing an Assessment Reporting Template

1. **Does this template meet the NCSC stated requirement of preparing a baseline to use as a reference point for pen tests? If not what changes/amendments would you make?**

The template helps to prepare a baseline that may be used as a point of reference for pen tests, which partially satisfies the NCSC baseline requirements. The assessment findings are thoroughly summarised in the template, with information on each vulnerability's potential impact, degree of severity, and recommended repair actions, as NCSC (2021) suggests. It is challenging to determine whether or not the vulnerabilities have been fixed because the template does not set a baseline for each one.

Although the assessment presents the risk assessment, it does not show the comparison against a security standard. Hence, to ensure compliance with the NCSC's baseline requirement, I would add a column on the table of risk assessments that explicitly outlines the acceptable severity levels for each vulnerability, as Swanagan (2022) suggests. This will assist the company in determining if vulnerabilities have been resolved to a good standard.

I would create two new sections, Remediation History and Incident Response Plan. These sections will track the progress of vulnerabilities over time, helping the company assess the effectiveness of its remediation efforts. This will also enable the company to identify any vulnerabilities that still pose a threat to its security, as pointed out by Basu (2022). In case of such exposures, the company can immediately follow its Incident Response Plan, as NCSC (2020) suggested.

2. **What are the two best lessons/examples presented in the report?**

The report offers two important lessons related to vulnerability assessment and repair:

1. The importance of classifying vulnerabilities: The report emphasises the significance of categorising vulnerabilities according to their severity level. As Tenable (2020) points out, organisations can prioritise remediation efforts using this classification and concentrate on the most severe vulnerabilities first.

2. The requirement for prompt correction: The report emphasises in the Executive Summary how critical it is to address vulnerabilities as soon as possible to reduce their potential impact. Delaying remediation can lead to cyber-attacks and data breaches, causing damage to reputation, as Robinson (2020) highlights.

3. **What two things do you think are unnecessary or could be done more effectively?**

Two things in the report could be replaced with more effective alternatives, for example:

1. While scan results may be helpful for some organisations, most may find them overwhelming and challenging to interpret (Malik, 2023). Hence, this point could be integrated as a summary of the key findings.

2. The inclusion of a list of every identified vulnerability is unnecessary. A table summarising the most critical vulnerabilities would be more valuable than listing all identified vulnerabilities. This would allow organisations to focus on the most essential risks first, as pointed out by Tenable (2020).

Reflection

While I reflect on this activity, I can tell that it was not as challenging as previous ones, but it was not easy either. I had prepared for the upcoming final assessment by conducting extensive research on different vulnerability assessment reports. This exercise helped me develop the necessary skills to answer the questions effectively. By analysing various pieces, I gained a deeper understanding of the subject matter, enabling me to approach the questions confidently. I am grateful for this opportunity and confident that my acquired skills will serve me well.

I wanted to mention that this activity was informative and insightful. The knowledge and experience gained through this activity will significantly impact my final report assessment. This newfound understanding gives me a clearer idea of what should be integrated into my last report. I am confident that the quality of my information will be enhanced as a result.

References:

- National Cyber Security Centre (2021). *Device Security Guidance*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/collection/device-security-guidance.
- Swanagan, M. (2022). *Why Vulnerability Management Reports Fail (& How To Fix It)*. [online] Available at: https://purplesec.us/learn/vulnerability-management-reporting/ [Accessed 8 Dec. 2023].
- Basu, S. (2022). *Vulnerability Assessment Report: A Beginners' Guide*. [online] www.getastra.com. Available at: https://www.getastra.com/blog/security-audit/vulnerability-assessment-report/.
- NCSC (2020). *Cyber Security Response and Recovery*. Available at: https://ncsc.gov.ie/pdfs/Cyber_Security_Baseline_Standards_Rev_1_2022_Final.pdf
- Tenable (2020). *What Is VPR and How Is It Different from CVSS?* [online] Available at: https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss.
- Robinson, A (2020). *Vulnerability management lifecycle explained!* [online] Available at: https://blog.6clicks.com/vulnerability-management-lifecycle-explained [Accessed 8 Dec. 2023].
- Malik, K. (2023). *What is Continuous Vulnerability Scanning?* [online] Available at: https://www.getastra.com/blog/security-audit/continuous-vulnerability-scanning/.