Module 4 Topic 3

Worksheet

Group (or Individual) Activities

(Task 1) Consider the NCSC Security Architecture Anti-Patterns Whitepaper
https://www.ncsc.gov.uk/whitepaper/security-architecture-anti-patterns

a. What is NCSC?

…..

b. What are Security Architecture Anti-Patterns?

….

c. What is a whitepaper?

….

d. What are bastion hosts?

….

e) For each anti-pattern presented, assign it to the most relevant CIS control(s):
https://www.cisecurity.org/controls/cis-controls-list

Anti-pattern 1: ‘Browse-up’ for administration
The relevant CIS controls are .....

Anti-pattern 2: Management bypass

The relevant CIS controls are
.....

Anti-pattern 3: Back-to-back firewalls

The relevant CIS controls are .....

Anti-pattern 4: Building an 'on-prem' solution in the cloud

The relevant CIS controls are .....

Anti-pattern 5. Uncontrolled and unobserved third party access

The relevant CIS controls are .....

Anti-pattern 6: The un-patchable system

The relevant CIS controls are .....

TASK 2 – Cyber Security Discussion

You can use the following sources, or any other reputable sources, to select a data breach that you find interesting, and discuss what could be done to prevent it from happening:

a. https://www.codecademy.com/article/case-studies-notable-breaches
b. https://www.techtarget.com/searchsecurity/feature/10-biggest-data-breaches-in-history-and-how-to-prevent-them
c. https://www.british-assessment.co.uk/the-worst-data-breaches-in-history/

Write your findings below

- …
- …
- …
- …
- …

Task 3 – Using scholarly papers to inform your discussion

Utilising scholarly papers as your primary source of information ensures credibility and depth in your research. Unlike blogs and casual online articles, academic papers undergo rigorous peer review processes, ensuring that the content is true, reliable, and contributes to the field. By referencing such sources, you not only elevate the quality of your presentation but also demonstrate a commitment to academic rigor and integrity, making your arguments more persuasive and your stance more authoritative. Choose academic sources to give your audience the best, most trustworthy information available. For Level 5, you are expected to gain familiarity with scholarly sources.

Consider the following two papers:

"The Challenges of Leveraging Threat Intelligence to Stop Data Breaches"

https://www.frontiersin.org/articles/10.3389/fcomp.2020.00036/full

and

"Enterprise data breach: causes, challenges, prevention, and future directions"

https://wires.onlinelibrary.wiley.com/doi/full/10.1002/widm.1211

Split the work between group members and then discuss your results at the end:

- In your group, ask one person to list out the major benefits and limitations of using threat intelligence in stopping data breaches.

- Ask the second person to write a 200-word summary of each paper highlighting the future directions of the research.

- Ask the third person to design an infographic that illustrates the main causes AND preventative measures associated with enterprise data breaches.