INFO8120 – Emerging Trends

Assignment 1

Security in a Pre- and Post-Quantum Age

DUE BEFORE 6PM OCT 23

1. Submission Guidelines

All assignments must be submitted via the econestoga course website before the due date in to the assignment folder.

You may make multiple submissions, but only the most current submission will be graded.

Assignments submitted after the due date will receive a 20% penalty.

Assignments submitted after 8am the day following the due date will receive a mark of 0.

Submissions should include be in MS WORD format. This will allow me to make comments directly on your assignment if needed.

2. Grading

This assignment will be worth 10% of your total grade in the course.

Assignments submitted after the due date will receive a 20% penalty.

Assignments submitted after 8am the day following the due date will receive a mark of 0.

3. Background

Frequently, your employer will hear about a new technology or product at a conference, online, for from a sale representative and will ask you to research and discover more about it. This assignment is designed to replicate that experience and to give you the opportunity to develop the following skills:

a. Research an emerging technology or product efficiently.
b. Summarizing the technology for a general audience.
c. Identifying the most relevant details and applications to your particular context.

This assignment covers and expands on the two presentations given in the course: Presentation 1 – Cryptography and Presentation 2 – Big Data Security.

To this end, all questions will be based on the graphic presented in Presentation 2 and reproduced in the Appendix.

4. Assignment Tasks

a. Question 1 – 16 marks

Quantum computing brings with it many security concerns. Describe how quantum computing may influence each of the eight attack vectors. Note that QC may not directly influence every vector equally, so be aware of indirect influences as well. For example, if predictive analytics for internal fraud detection run on quantum computers could be done in real time, it would indirectly address Attack Vector 4 (Internal Threats).

Answers should be ~ 50 words per vector.

b. Question 2 – 20 marks

For each of the technologies/processes listed below, please give a brief summary of the technology, describe which attack vectors the technology might address and the manner is which they may address it.

NOTE – Research on each technology should take

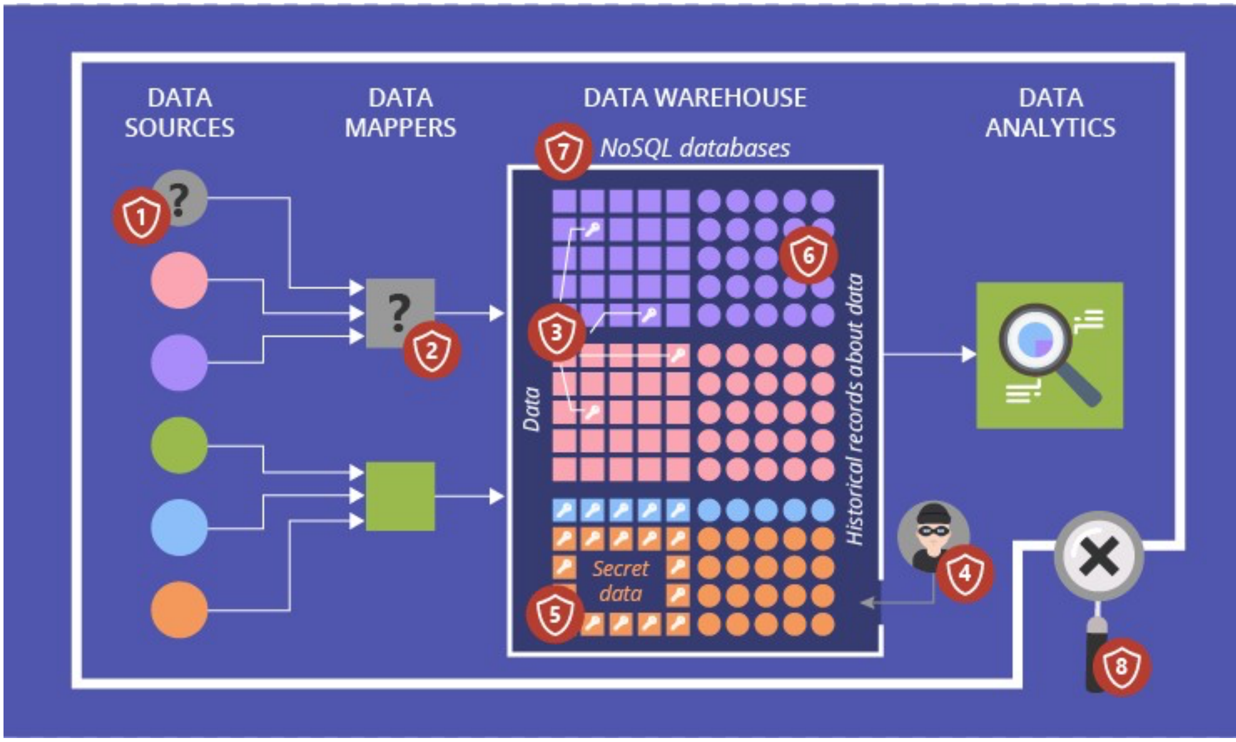
Answers should be ~ 100 words per technology.

a. Tokenization
b. Hypervisors (High Assurance and otherwise)
c. Master Data Management
d. IaaS Container Encryption
e. Hardware Authentication

c. Professionalism and Quality of References – 4 marks

As described in many classes, all references and sources should be identified using the Conestoga College citation guidelines and standards (https://apa.conestogac.on.ca/). Remember, all reference works and quotations must be identified: I am interested in *your* work and *your* insights.

APPENDIX



Alex Bekker, *ScienceSoft,* April 4, 2018

1. Counterfeit Data Creation
2. Untrustworthy Mappers
3. Inadequate Encryption Measures
4. Internal Threat to Sensitive Data
5. Granular Data Controls
6. Data Source Record Keeping
7. Speed of Development and Security Considerations
8. Lack of Proper Audit Functionality