COMP90073 - Security Analytics

Week 2 Tutorial

University of Melbourne, S2 2020

Case Study 1

You are just hired by Mars University as the security expert to help them secure their IT system, in particular:

- Payroll

- Learning Management System (LMS), and

- Subject handbook hosting site

Assignment Project Exam Help

https://tutorcs.com

WeChat: cstutorcs

Case Study 1 – Q1

Q1. How do you measure the confidentiality of information you need to protect?

By Data Classification.

- **Payroll Information**: Confidential

- **LMS Information**: Internal Use Only

- **Handbook Information**: Public

Case Study 1 – Q2

Q2. What are the controls you can implement to ensure the CIA triad are supported?

- Security Control for Confidentiality: Information Encryption

- Security Control for Integrity: Segregation of Duties, Approval Checkpoints

- Security Control for Availability: Up-to Date Systems, Tested Incident Management, and Disaster Recovery Planning

University of Melbourne, S2 2020

Case Study 1 – Q3

Q3. What are the access control principles you can apply, and how?

- **Access control policy:** specify the requirement for 2 factor authentication for payroll system, and only staff in finance can have access to payroll information;

- **Separation of duties:** user access to payroll system needs to be approved by both the people leader of the requester and the head of finance;

- **Least privilege:** student has read only access to the content related to their enrolled subjects

University of Melbourne, S2 2020

Splunk & App Installation

Setup your own Splunk instance.

- Splunk Enterprise version 7.3.0 is recommended for this Project. The latest version 8.0.x may experience compatibility issue with some apps due to the Python version upgrade.

- Apply the 10G Enterprise license (download link to be updated)

Install "PCAP Analyzer for Splunk" app version 4.1.x

Recommend free Splunk course to watch

- "**Free Splunk Fundamentals 1**"