CYSE 130

Group 5

Week 5 Assignment

**System Requirements:**

For our system requirements, we will be making a lot of changes to the current security architecture of this wealth management firm. The firm currently has virtually no real security practices in place. There is no activity logging, free access to the entire company for any employee, and no indication of any intrusion detection system or monitoring.

In terms of access control, we will be moving to a system with the principle of least privilege, as the company currently uses badges that allow any employee access to anywhere in their building. There were no listed permissions or privileges for employees reported to us, so we will be shifting the company’s security towards less physical access, as well as creating groups for the employees to determine what they can access in regard to company data.

We need to implement incident detection that allows us to detect a breach almost immediately since packets were reportedly leaking from the company for months with no knowledge or suspicion. We will be implementing activity logs as well as monitoring to detect any sort of unusual activity, such as a suspicious amount of packets coming from overseas or strange times of access. Company policy should state employees must report any suspicious activity or leaks they think might have happened immediately or anything else in regard to company data being extorted.

We will be creating a script that automatically scans through logs for any suspicious activity, such as accessing information outside of regular hours, repeated attempts to access restricted data, or any downloading or other activity regarding sensitive information. The script will compile all the suspicious activity along with timestamps and log it for the company to investigate.

Once we finish creating the system, we will be setting up a schedule for security audits, including penetration testing and vulnerability assessments to determine any still present risks. Updates will be made to the system when vulnerabilities are identified, to help with risk management for the organization.

**UML Activity Diagram:**

**A diagram of a process

Description automatically generated**

**Use Case Diagram:**

A diagram of a person's account

Description automatically generated

**Project Timeline:**

* Initial planning and design: 10/21 – 10/25
* Automation and scripting: 10/25 – 11/04
* Advanced data analytics and machine learning implementation: 11/04 – 11/11
* Risk management planning: 11/11 – 11/18
* Finalization and presentation: 11/18 – 12/02

**Role Assignment**

* Project Manager
  + Dillon Furey
* Systems Modelers
  + Saif Khan
  + Zain Salim
* Python Developers
  + Zachary Ho
  + Nguyen Phuc Be
* Data Analyst
  + Anthony Jaldin