Organization/Industry: Mid-sized in the financial services sector

Actors: Who and what and where will be accessing the system. Who initiates and who reacts to each use case

Use cases:

IDS (Use case diagram)

Firewall (activity diagram)

Authentication System(Sequence

Actors: employees, managers,

System: organizational cybersecurity system

* Access control, incident detection/response
* Using data analysis, security compliance, and secure DevOps
* IDS/IPS
  + (Network) Intrusion Detection System: Analyzes network traffic to detect anomalies in the traffic that may indicate unusual activity in the network.
  + Firewall
    - Check user login
  + Network-wide monitoring program
  + Tracking network traffic
    - Analyze network packets
  + Workflows that automatically send alerts when triggered
    - Ex. Accessing the malicious website
    - Kill Switch
    - Dropping malicious packets
* DevOps pipeline
  + Source Code Management (using Github)
  + Continuous Integration (set up automatic tests)
  + Build (compile source code into executable format)
  + Continuous Deployment
  + Deployment (testing)
  + Monitoring and Logging
  + Feedback loops
* Data Analysis Report (access log, security change logs)
  + Using data analysis to analyze IDS logs and access control logs
  + Summary of data
  + Implement logging capability into business operations to gather data
  + Methodology for data collection
  + Findings and analysis (incidents if necessary)
  + Threat and vulnerability assessment
  + Discussion, conclusion, and recommendations
* Access Control
  + Security process that limits access to resources like data, apps, and physical spaces.
  + First, one must verify the users they claim to be (Authentication) using passwords or multi-factor authentication (MFA).
  + Then, one must grant the user appropriate access to the resource (Authorization) using Access Control Lists
  + Also, one must enforce policies to keep access control, such as password policies (min char. Requirement of 12 with different characters: 2 upper, 2 lower, 2 numbers, 2 special char.)

Challenges:

Data breach and unauthorized access to internal systems

Use CaseSystems/System boundary: IDS [Link](https://lucid.app/lucidchart/1bb4faa9-76a2-4f4f-9e92-be6a694a19f4/edit?viewport_loc=-109%2C-30%2C1304%2C586%2C0_0&invitationId=inv_b288620f-a74d-416b-a117-495d2a032043)

Sequence: Firewall [Link](https://lucid.app/lucidchart/d269b336-2017-4004-9cea-d1e6e6debd32/edit?view_items=XS5jqnQsODTo%2CXS5j7lz1CdoN%2CXS5jKKwQYVbe%2CXS5jHVw4l~aS%2CXS5j8lB2ZHP_%2CXS5jD.rkf.US%2CXS5jsurTPxcB%2CXS5jHymPj4WB%2CXS5jphTXfaZV%2CXS5j06oC2oxJ%2CXS5j0pC_lPRb%2CXS5jppn-CQVs%2CXS5jQzIyWizb%2CXS5jpVXK0kKc%2CXS5jCl7CBdBO%2CXS5jVEBZ0Y2-%2CXS5jvR7439x.%2CXS5j38PnA2~z%2CXS5jjjd2jquv%2CXS5jq97-xl.3%2CXS5jRTrI-7ha%2CXS5jfcgSy6TZ&invitationId=inv_eebaf479-c9c9-45c8-ab5f-b02119cc4ef1)

Activity: Authentication [Link](https://lucid.app/lucidchart/9aee4a5e-6a3b-4bf2-8e1f-6adb6653e9c2/edit?viewport_loc=-2397%2C-1234%2C4080%2C2064%2C0_0&invitationId=inv_aeb68ecb-075d-4a15-b712-e6328d800789)