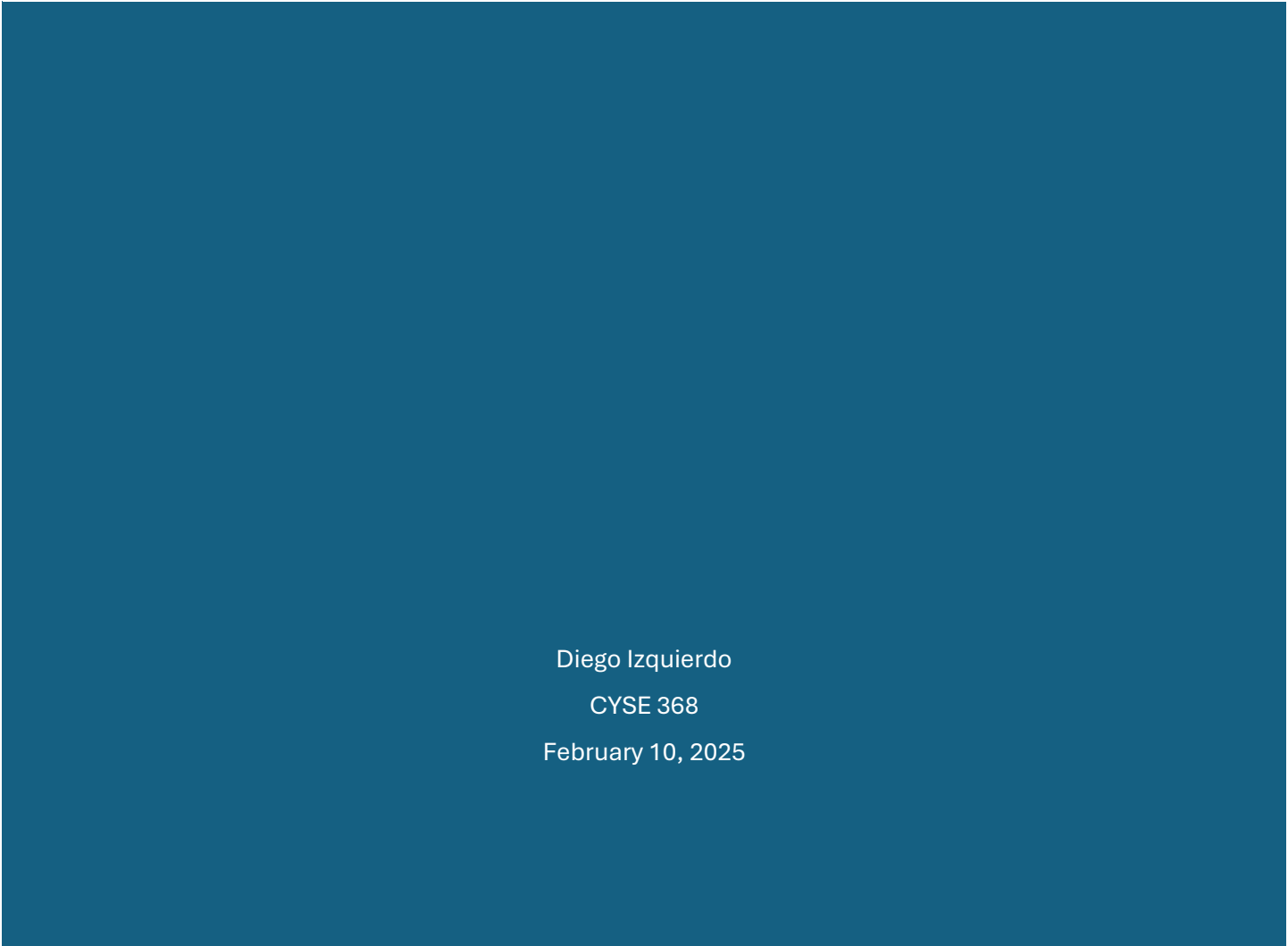# REFLECTION PAPER 1

Diego Izquierdo

CYSE 368

February 10, 2025

Reflection paper 1

Reporting Period: January 21st, 2025, to February 7th, 2025

Primary Objectives

1. Enhance security posture for private and public cloud environments
2. Develop policies and procedures for securing Azure storage accounts and Key Vaults
3. Implement IAM solution for Azure Cloud
4. Learn procedures and best practices for managing Cisco Firewalls

Overview

Completed the first 50 hours of my internship at TowneBank, while I had some major milestones, I still feel like I didn't accomplish everything I wanted to accomplish.

What went well?

- Made some significant headway on migrating critical line of business applications from legacy authentication to Single Sign-On using SAML. During this period, we migrated two LOBs to SSO using Entra ID. One of the SSO implementations required that the SAML token needed to be encryption, this is a fairly new feature, and I am expecting it will become a mainstream requirement in the near future.
- Started to develop standards and procedures to lock down Azure Storage accounts by implementing Azure private endpoints. This will allow traffic from our on-premises network to route through the private Azure Express route rather routing through the public internet. Successfully converted the first Storage account from public facing to private facing by deploying a private endpoint.
- Had a meeting with a Microsoft specialist to review the findings of a recent security assessment of the Azure environment. There were quite a bit of items that need to be remediated so I will be developing an action plan to address those findings

What needs improvement?

Time management. I am splitting my week between the cybersecurity internship tasks and operational duties, so I need to try improving my time management and minimizing the time I spend on ad-hoc requests. I need to watch this video about the "Big Rocks, Little Rocks" time management concept

https://www.youtube.com/watch?v=pHR4RpxD6m0

What's next?

- We had a third party conduct a pen test of our cloud and on-prem environments back in December and we just got the final report. There were only a handful of critical findings that will need to be addressed as soon as possible, but don't think it will be a major headache. Overall, the pen test went great for us.
- We got tasked with coordinating and implementing the rotation of passwords for service accounts. We will need to identify the stakeholders, affected applications and coordinate with our change management board to rotate these passwords. Not looking forward to this project