REFLECTION PAPER 2

Diego Izquierdo

01269416

CYSE 368

March 8, 2025

Reflection paper 2

Reporting Period: February 10, 2025, to February 28, 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

Fairly busy period, I made some significant headway in some projects and also started new ad-hoc projects. Also, I have been promoted to Enterprise Systems Architect, so I will be slowly moving away from operational duties and doing a lot more design. Very excited about the new role and looking forward to the challenge.

What went well?

- Continue working on implementing SSO for different LoB applications. We have identified a couple more applications that will need SSO integration, so we added them to the backlog. Now we have a rhythm going with the SSO rollout, I am finalizing the documentation for SSO implementation and will be cross training somebody from my team to take over the SSO rollout. Also, I am noticing a shift with more companies preferring OIDC over SAML for SSO, we discussed this during our architectural review board and we will be sticking with SAML as our primary SSO protocol.
- Started developing standards and policies for Azure service principals and managed identities.
- Started doing a proof of concept of Azure/s Cloud infrastructure entitlement management (CIEM) to discover, remediate and monitor permissions entitlement across our cloud infrastructure. The end goal is to use the principle of least privilege to grant cloud administrators just the permissions they need to do their jobs https://learn.microsoft.com/en-us/entra/permissions-management/
- Rotated the password for several service accounts without any disruptions. We still have over 100 service accounts that need to be rotated so I will continue planning and coordinating these changes for the next few months. I think once we are done with this project, I will see if we can streamline this process, it is a time-consuming effort, and we will be doing it every year.
- Troubleshot an issue with a critical server, it appears the windows firewall was mistakenly blocking inbound traffic to the VM and causing issues with an application.

What needs improvement?

Prioritizing work. We laid out the goals for this year, so we will need to prioritize our workloads better,

What's next?

- Developing a plan to mitigate the critical, medium and low findings from the Penetration test.