CLOUD SECURITY

ON DATA LOSS PREVENTION (DLP) WITH MICROSOFT PURVIEW

BY

JIMOH TOHEEB

(GROUP 7)

1. Introduction

This is a firsthand account of carrying out the Data Loss Prevention (DLP) part of a global group project focused on enhancing cloud security. The general goal for our team was to implement good security controls in a cloud system to protect sensitive organizational data. My specific goal was to develop, deploy, and validate DLP policies in Microsoft Purview to prevent unauthorized exfiltration of significant data. To illustrate, we utilized the identification of Canadian Credit Card data as one of our key examples. Microsoft Purview served as the main platform for managing data and data governance, bringing together features like Information Protection and Data Loss Prevention.

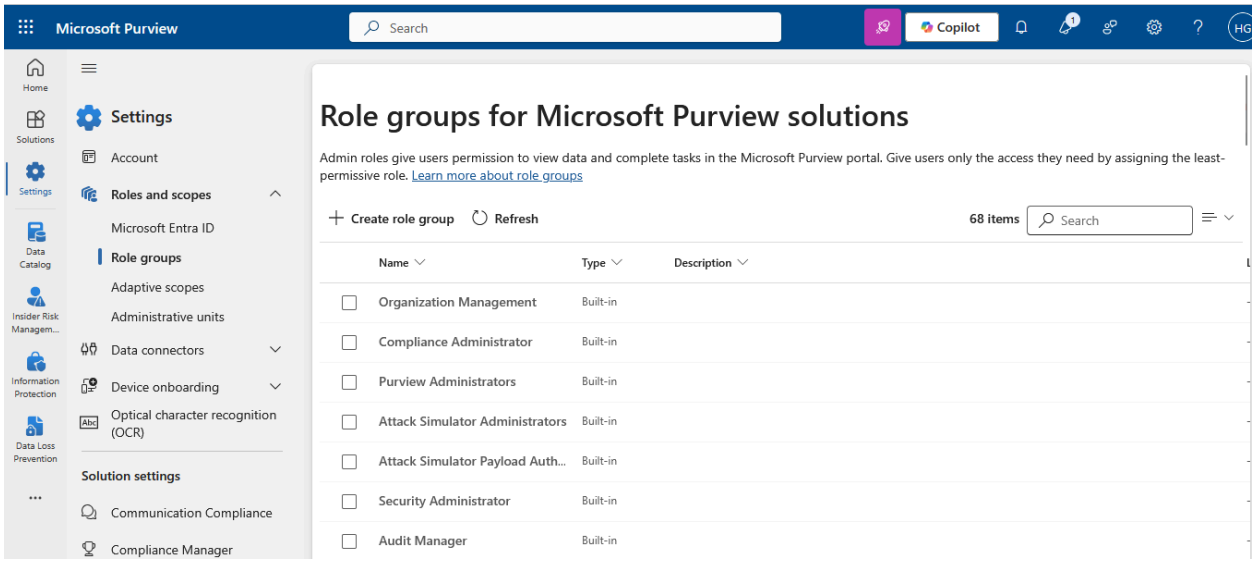
2. My Contribution and Role

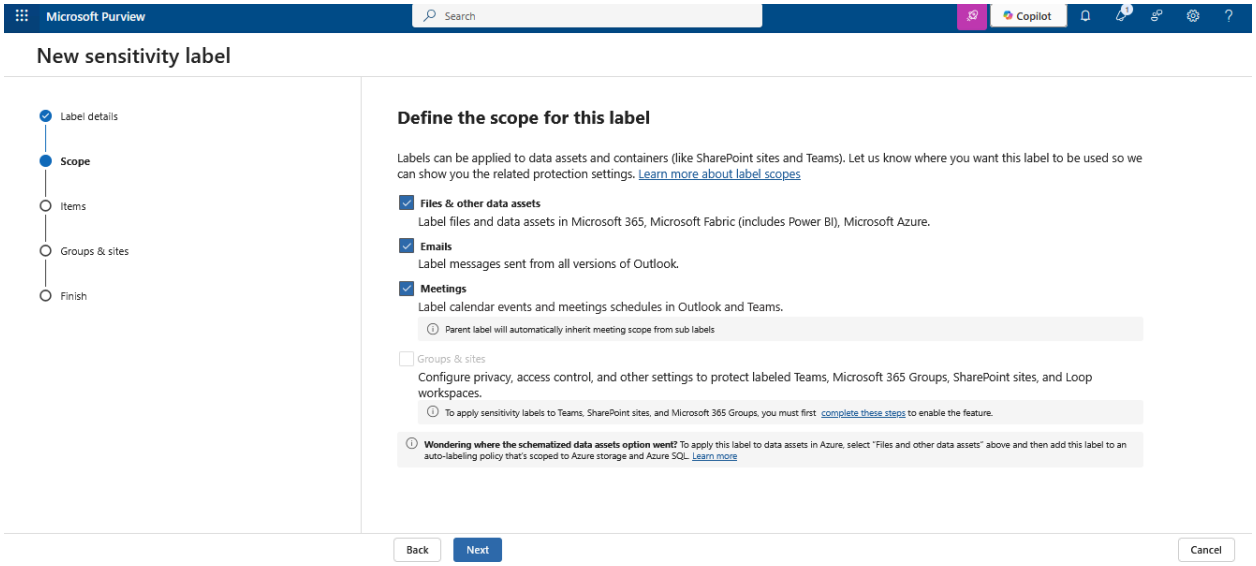
My primary responsibility for this project was to manage the roll-out of Data Loss Prevention within Microsoft Purview. This entailed a series of deliberate actions intended to keep sensitive information under organizational control, either from inadvertent or intentional egress.

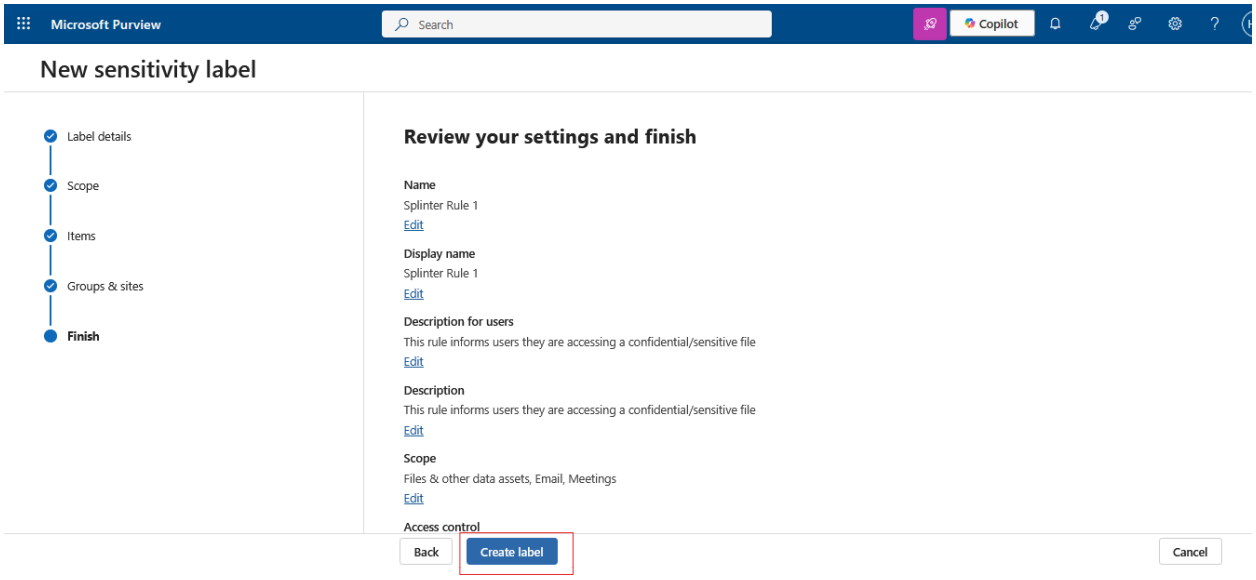
My specific responsibilities included:

Configuring RBAC Permissions: I was part of the team also responsible for configuring Role-Based Access Control (RBAC) in Microsoft Purview to grant the concerned team members the necessary permissions for data governance and compliance tasks. It involved creating roles such as "Compliance Administrator" for system administrators (Habib, Isaiah) and "Data Loss Prevention Analyst" for cybersecurity engineers (Jimoh), including myself, to manage DLP

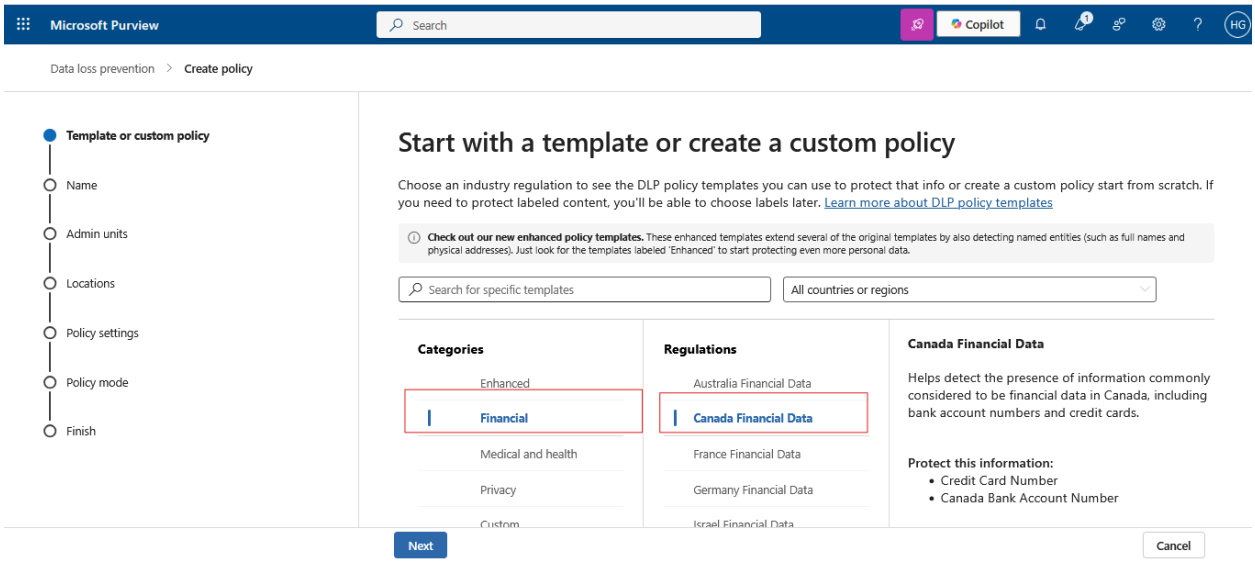
policies and view alerts. I accessed the Microsoft Purview compliance portal directly to see settings (under "Solutions"), role groups for management, and assigning members to their respective groups as per the above-discussed steps.
Rollout of Sensitivity Labels: To display visual notifications and label sensitive data, I set up Sensitivity Labels directly within Microsoft Purview Information Protection. My action was to design a new label, scope it out, and choose protection settings, such as watermarking as the option to visibly identify confidential information. I also made these labels auto-apply to content, and subsequently published the policy developed. This helped in making users realize that the information they were working on was sensitive.
Configuring DLP Policies: My initial task was to create and implement a robust DLP policy. I started off by navigating to the Data Loss Prevention section in Purview and then creating a new policy. The policy was specifically designed to search for Canadian Credit Card information, which was our proof of concept. I titled the policy, outlined it, and applied it to all the users within our directory, prescribing its scope of application. I then specified cautiously what content to secure, assigning protection actions, and specifying override and access settings. Finally, I activated the policy to ensure that it started to work the instant it was submitted.
In this way, my DLP installation helped the team's general cloud security goals by being a foundation for protecting confidential information against improper disclosure, a critical component of a secure cloud.







Policy to detect Sensitive information



3. Challenges and Issues Faced

While the overall process was structured, I encountered several tangible challenges in implementing DLP:

RBAC Understanding: As a preliminary step, understanding finer nuances of Microsoft Purview's Role-Based Access Control and granting correct permissions for managing DLP demanded meticulous focus. Correct segregation between compliance access roles and DLP policy management-specific roles was a must.
Sensitivity Label Deployment: To verify whether sensitivity labels had been correctly configured to automatically apply and display warnings, for example, watermarks, to sensitive information proved difficult in regards to setup. I needed to ensure that I set conditions for automatic labeling with utmost care to avoid misclassifications.
DLP Alerting Discrepancy: One of the biggest challenges I encountered was that although the DLP policy was set to alert on detection of Canadian Credit Card data and actually trigger an email notification to users to avoid sending sensitive data, the associated alerts were not consistently dropping within my Microsoft Purview console. This discrepancy between the user-imperative warning and lack of the alert in the Purview console required a closer examination of policy reporting and potential backend configuration.
Policy Rule Definition and Testing: DLP policy rule definition, particularly to identify specific sensitive information like Canadian Credit Card numbers, was all about precise definition of content types and conditions. Obtaining the policy right for testing to avoid false positives while ensuring complete coverage was a continuous process of optimization. I had to ensure that the policy was robust enough to pick up real credit card numbers without flagging nonsensical data.
Policy Mode Effect Knowledge: Enabling the policy with the "turn on as soon as possible" setting needed to be interpreted in light of its immediate effect on user experience and data handling, hence needing immediate close examination prior to submission.

I overcome these difficulties through careful study of Microsoft documentation, testing various policy settings in a test environment, and conducting iterative testing to confirm effectiveness and accuracy of the DLP policies and sensitivity labels. For the alerting problem, this translated to more in-depth research in Purview's alert functions and reporting features. This drill-down troubleshooting helped me get my concept right and implement it successfully in spite of the particular alerting obstacle but still i was not able to still get the alert even after thinking i already did.

4. **Skills and Knowledge Obtained**

This project greatly enhanced my technical and analysis skills in cyber security, particularly Data Loss Prevention and cloud compliance.

Technical Skills: I gained hands-on experience in deploying and configuring Microsoft Purview as a compliance-grade solution for the business. This involved hands-on experience with Role-Based Access Control (RBAC) within Purview, the creation and management of Sensitivity Labels, and the explicit configuration of DLP policies based on specific sensitive data types. My skills at configuring policy scopes, content types, actions, and access overrides were significantly enhanced.
Analytical Frameworks: Identifying what is "sensitive data" and how to best avoid it from being lost to begin with sharpened my analytical mind. I was educated to break down intricate data protection requirements down into actionable policy rules and have the ability to forecast likely data exfiltration vectors. The issue of alerts not dropping in Purview specifically honed my debugging and analytical skills in determining policy effectiveness regardless of user-visible alerts.
Compliance Knowledge: While it was more about execution, this project enhanced the comprehension of DLP importance for regulatory compliance such as GDPR, HIPAA, and ISO 27001 through ensuring the safe handling of Personally Identifiable Information (PII), Payment Card Information (PCI), and other sensitive information. My proficiency in translating compliance needs into technical solutions was augmented further.

5. **Teamwork and Workflow**

Although my specific DLP implementation was my own task and also one of my other colleague, it was a component of our broader team's cloud security initiative. I collaborated with my team by ensuring that the DLP policies were integrated into the overall security framework and other cloud security mechanisms being put in place. I informed the team about my work and any policy considerations so that we could have a unified understanding of our cloud security stance.

6. **Personal Development and Self-Reflection**

I believe I successfully demonstrated an operational and properly configured DLP solution with Microsoft Purview by successfully demonstrating the blocking of sensitive data exfiltration through warning users and applying policy. My extremely detailed effort in defining and testing policy was a showstopper.

Improvement areas that I identified for future projects are:

Advanced Alerting and Reporting: Getting deeper into the reasons for alerts not dropping off in Purview and becoming proficient in advanced reporting and analysis capabilities for DLP incidents to identify trends and refine policies ahead of time.
Automated Policy Testing: Finding methods for automated DLP policy testing to analyze various data exfiltration vectors faster and more thoroughly.
User Training Integration: Providing a special element to educate users on DLP policies and sensitivity labels to make the users more compliant and prevent unintentional data loss.

7. Conclusion

This project provided me with hands-on experience in implementing Data Loss Prevention in a cloud platform with Microsoft Purview that was well-timed and rewarding. It compelled me out of the world of hypothetical knowledge and to translate real-world data protection use scenarios into organized configurations. I think that I am now sufficiently qualified to execute data loss prevention work in real-world environments and more at ease with industry-standard tool and framework utilization for cloud compliance and data governance.