■ **Project Title:**

Access Control Incident Investigation and Mitigation Report

Summary for GitHub Portfolio

This project involved conducting an incident investigation for a financial transaction anomaly within a small business network. As the first cybersecurity professional at the organization, I was tasked with reviewing system event logs, identifying access control issues, and recommending mitigations to prevent future incidents. The project reinforced critical principles of access management, log analysis, and cybersecurity governance.

Scenario Overview

A payroll deposit was mistakenly sent to an unauthorized bank account. Upon review, it was determined that an internal user may have abused or accidentally triggered an access control flaw in the company's shared cloud drive. The goal of this investigation was to analyze log activity, identify weaknesses in access control, and propose actionable security mitigations.

Investigation Notes

I reviewed the event logs to identify patterns of user behavior, IP addresses, and timestamps associated with the suspicious transaction. The analysis revealed login attempts from multiple IP addresses inconsistent with the user's normal behavior. Furthermore, shared credentials were being used across employees, which introduced accountability issues and increased the likelihood of unauthorized access.

Access Control Issues Identified

1. Employees were using shared accounts for cloud storage access, resulting in poor accountability and traceability.
2. Access privileges were not revoked for former employees, leaving sensitive data exposed.

Recommendations for Mitigation

1. Implement Role-Based Access Control (RBAC) to ensure employees have access only to the resources required for their job duties.
2. Require multi-factor authentication (MFA) and unique user credentials to eliminate shared account risks.
3. Establish an offboarding process that automatically revokes access when an employee leaves the company.
4. Conduct regular access reviews and monitor login anomalies using SIEM tools for proactive detection.

Key Takeaways

This investigation enhanced my skills in access control evaluation, log interpretation, and cybersecurity risk management. By mapping the event findings to NIST SP 800-53 AC-2 and AC-3 access control guidelines, I demonstrated an ability to identify gaps and propose industry-aligned solutions. The project reinforced how strong identity management and access control frameworks serve as foundational components of information security and fraud prevention.