■ **Project Title:**

Home Office Asset Classification and Sensitivity Assessment

Summary for GitHub Portfolio

This project focused on applying foundational asset management principles to a home office network environment — demonstrating the ability to identify, categorize, and classify devices based on their sensitivity to risk. Asset management plays a critical role in cybersecurity because it establishes visibility into all devices that interact with sensitive information or business systems. In this activity, I acted as a security analyst managing a small business network operated from a home office. The objective was to create a structured asset inventory listing devices connected to the network and assess each device's confidentiality, integrity, and availability (CIA) risk profile.

Three primary assets were selected:

Personal Laptop – Contains business data, documents, and login credentials.
Smartphone – Used for communication and business account access, often connecting to public Wi-Fi. External Hard Drive – Used for data backup and file storage.

Asset Inventory Table

Asset	Network Access	Owner	Location	Notes	Sensitivity
Laptop	Always connected	Business Owner	Office Desk	Contains sensitive business and client data	Confidential
Smartphone	Frequent	Business Owner	Variable (home/public)	Used for MFA business accounts	Private
External Hard Drive	Intermittent	Business Owner	Secured Drawer	Secured Drawer Backup of client info and critical documents	Highly Confidential

Sensitivity Classification

The classification process applied four sensitivity levels — Public, Private, Confidential, and Highly Confidential — to determine the priority for protection. Devices containing personally identifiable information (PII), client data, or credentials were classified at higher sensitivity levels to guide stronger protection measures such as encryption, secure storage, and access control.

Threats and Vulnerabilities

Unauthorized network access via unsecured Wi-Fi, physical theft of portable devices, malware infection through removable media, and weak password management were identified as major risks.

Mitigation Measures

- Implement network segmentation for guest and work devices.
- Enable encryption and multi-factor authentication (MFA).
- Maintain updated firmware and antivirus protection.
- Conduct regular audits of connected network devices.

Key Takeaways

Developed a structured asset inventory aligned with industry frameworks. Classified assets by sensitivity and risk impact, simulating a real-world organizational risk evaluation process. Strengthened understanding of how device management directly supports data protection, confidentiality, and business continuity. Reinforced the connection between asset visibility and effective incident prevention.