Authorization Policy (Least Privilege)

Introduction

In this assignment, I'm explaining how three SOC roles should get access on a new file server. I used the Principle of Least Privilege, which means giving people only the exact amount of access they need and nothing extra.

Tier 1 Analyst – Read Only

A Tier 1 Analyst just checks alerts and looks at logs. They don't need to edit or create anything. So **reading-only** is enough for them. This also helps avoid any mistakes.

Threat Hunter – Read and Write

A Threat Hunter goes deeper into investigations. They create detection files, update things, and sometimes write scripts. Because of this, they need **read and write access**. They don't need full control, just enough to do their job.

SOC Manager – Full Access

The SOC Manager is the one in charge. They need to see everything, change things when needed, and manage permissions. So they should get **full access**.

Summary Table

Role	Access Level	Why
Tier 1 Analyst	Read	Only needs to view alerts/logs.
Threat Hunter	Read + Write	Needs to edit/create files for investigations.
SOC Manager	Full Access	Oversees everything and manages permissions.

Conclusion

Each person gets only what they need to work. This follows the Least Privilege principle and helps keep the system safer.