# **Enterprise Security and Automated Compliance Platform**

My project focuses on establishing a robust, secure, and highly observable enterprise environment. It emphasizes DevSecOps principles, rigorous policy enforcement via Active Directory, and advanced data visualization to maintain system integrity and compliance.

### **Table of Contents**

1. [DevSecOps and Vulnerability Integration](#_1n1qpju32us6)
2. [Rigorous Group Policy Enforcement](#_h2z8ab5xpkij)
3. [Advanced Monitoring and Visualization Platform](#_8c8ag8j5fb5a)
4. [Automated Security Response and Compliance](#_pzk5k9mvdo9h)
5. [Cloud Identity Security](#_dfv1pgguf0gx)

## **1. DevSecOps and Vulnerability Integration**

This section defines how the project incorporates modern enterprise security tools to proactively maintain compliance, drawing on concepts of **DevSecOps** and **Advanced Security**.

| Task | Detail |
| --- | --- |
| **DevSecOps Integration** | Focus on integrating security practices throughout the operational lifecycle. This aligns with modern IT use cases like **App Modernization** and **DevOps** |
| **Vulnerability Management** | Utilize platforms such as **GitHub Advanced Security** to identify and implement measures to **find and fix vulnerabilities** within the deployed systems and scripts |
| **Enterprise Security Features** | Demonstration of proficiency with **Enterprise-grade security features** and **security tools** applicable to both on-premises and cloud resources |
| **Core Systems** | The core platform remains the **Windows Server 2022** environment acting as the hub for policy and identity. |

****

## **2. Rigorous Group Policy Enforcement**

This section details the implementation of **Group Policy Objects (GPOs)** to lock down system configurations and enforce mandatory security settings across the domain, ensuring **consistency and control**.

### **Policy Implementation Steps**

1. **GPO Creation and Linking**: Policies must be created in the **Group Policy Management Console (GPMC)** and linked to the **Domain** or specific **Organizational Units (OUs)**.
2. **Password Policy Enforcement**: A mandatory GPO applied at the Domain level under **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy**. The policy must specify a minimum password length of **8 characters**.
3. **Client Restriction Policy**: Implement the policy to **Prohibit access to the Control Panel and Settings**, located under **User Configuration**. This prevents unauthorized system changes.
4. **Removable Storage Security**: Implement a GPO to **Deny read and write access to removable storage devices** to mitigate **data loss and malware introduction**.

## **3. Advanced Monitoring and Visualization Platform**

This section details the dedicated setup of the Linux VM (**MON01**) for **Proactive Issue Detection** and **Performance Optimization**, critical for maintaining a secure and compliant platform.

### **Monitoring Infrastructure (MON01)**

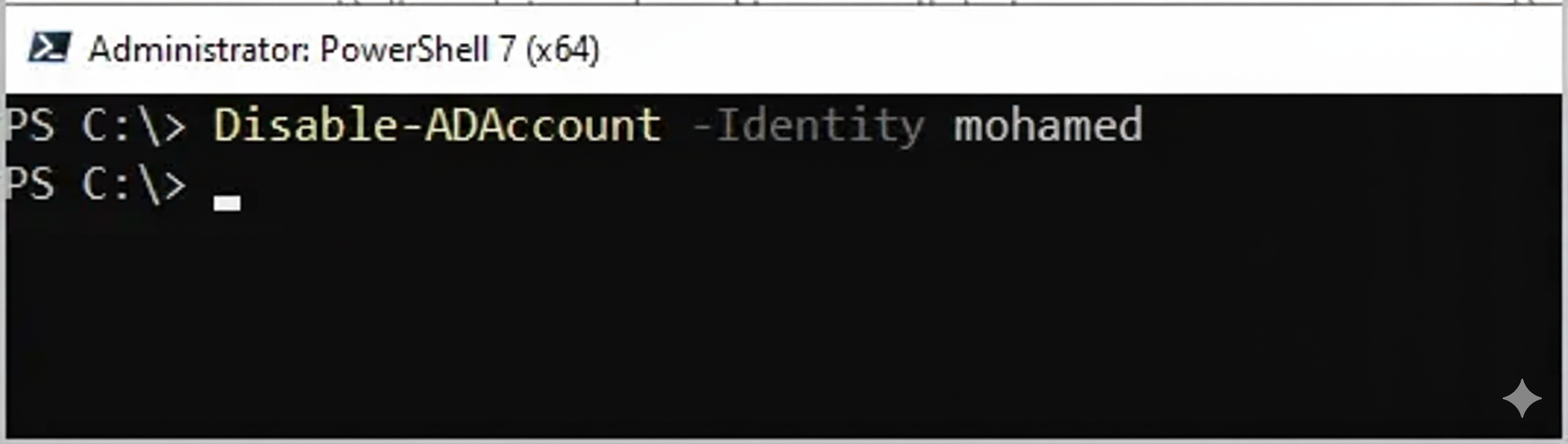
| **Step** | **Detail** |
| --- | --- |
| **OS Selection** | Deployment of the Linux server (named **MON01**) using the **Debian 12.5 distro** with **3GB (3072MB) of RAM** allocated |
| **Zabbix Server Setup** | Installation of the **Zabbix Server, Frontend, and Agent**. Configuration uses **MariaDB** (a MySQL fork) for the database and **Apache** as the web server |
| **Agent Deployment** | The Zabbix agent is manually installed on Windows hosts (like **DC01** and **SV02**) or deployed via **PDQ Deploy**. The agent points to the Zabbix server’s IP address |
| **Grafana Integration** | **Grafana** is installed using the **apt package manager** and integrated as a data source using the Zabbix API |
| **Visualization Goal** | Creation of visualization dashboards using the **Time Series** graph type to analyze metrics like **CPU Utilization** and **Disk Write Rate** for security and performance tracking. |

### 

## **4. Automated Security Response and Compliance**

This section demonstrates the use of **PowerShell** for enforcing security and managing compliance consistently.

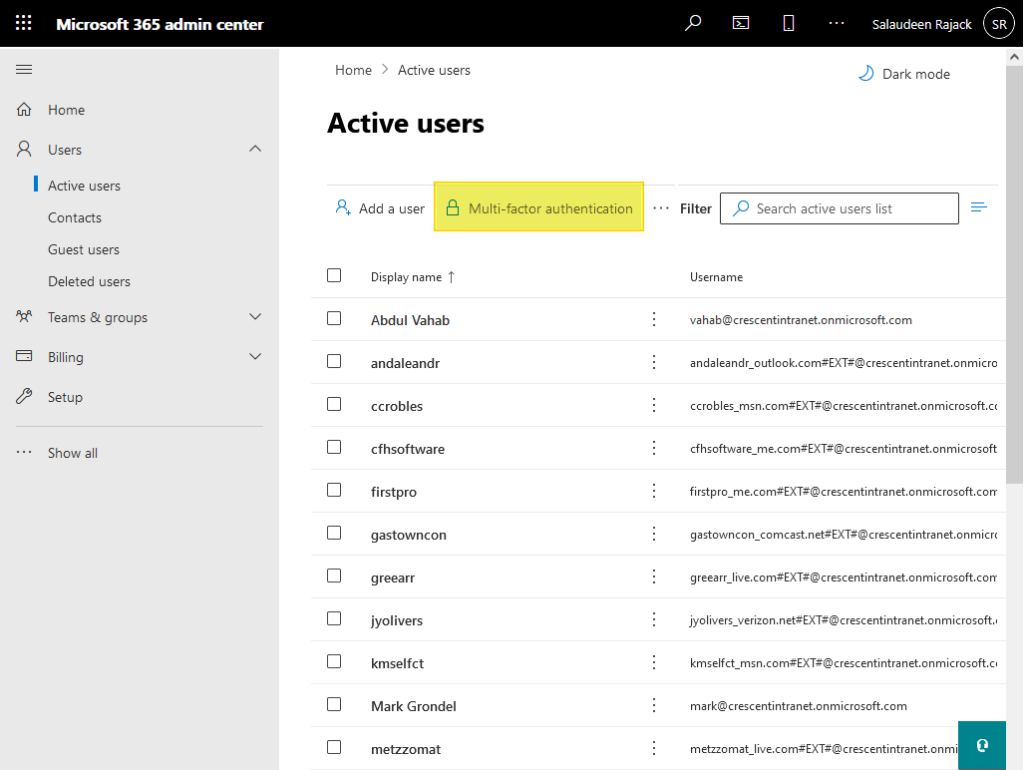
| Task | Detail |
| --- | --- |
| **Bulk User Management** | PowerShell scripts are used to perform tasks that affect multiple users quickly, ensuring **efficiency and consistency** |
| **Automated Security Action** | Use the **Disable-ADAccount** command to rapidly suspend user access, such as disabling all users belonging to the 'IT' department. This is critical for security incidents or compliance breaches. |
| **Configuration Consistency** | Scripts ensure the **same accurate result every time**, reducing human error when managing large numbers of objects or settings in Active Directory |
| **Centralized Software Control** | **PDQ Deploy** (installed on SV02) is used to silently distribute software (e.g., **7zip** using the /S parameter) to maintain a uniform and secure software baseline across client machines (JMFSOFT-PC01/02) |

****

## **5. Cloud Identity Security**

This final section focuses on securing the cloud identity perimeter, leveraging **Microsoft 365** and **Azure Active Directory (Microsoft Entra ID)**.

| Feature | Implementation Detail |
| --- | --- |
| **Multi-Factor Authentication (MFA)** | MFA is enabled via the **Azure portal** by navigating to Users and selecting **"MFA per user"**. This **significantly enhances security** against phishing and theft |
| **Azure AD Management** | Creation and management of users/groups within **Microsoft Entra ID** via the **Azure portal** or through bulk creation using a **.csv file**. |
| **Security Groups** | Management involves creating **Security Groups** to control access to resources via roles and permissions, distinct from Distribution Lists |
| **User Recovery** | Demonstrated ability to handle standard IT support tasks, such as **password reset** in Azure AD, which automatically generates a temporary password |

****