Active Directory Project

Author: M1KEgithub

Purpose of the project

The purpose of this project was to implement a **secure, resilient, and well-organized Active Directory (AD) infrastructure** tailored to meet modern security requirements and organizational needs. This included designing a structured **Organizational Unit (OU)** hierarchy with **role-based access controls (RBAC)** to enforce the principle of least privilege.

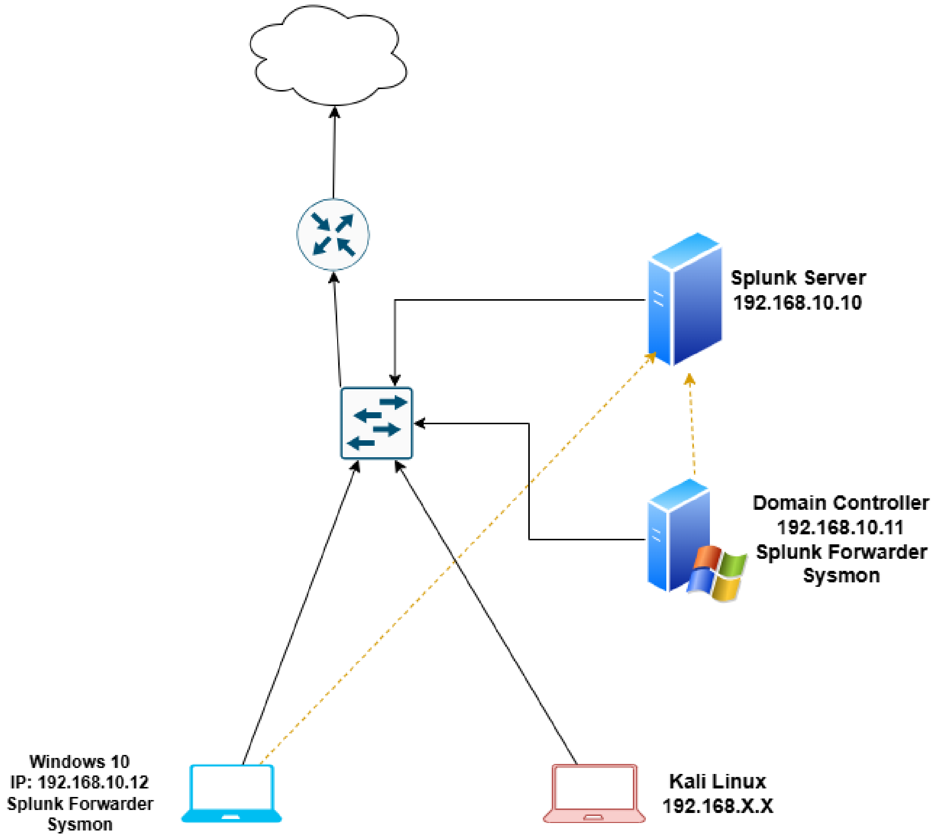
Comprehensive **Group Policy Object (GPO)** configurations were applied to **harden workstations and domain controllers**, focusing on critical areas such as password management policies, NTLM restrictions, and securing local administrator accounts. Additionally, the **Local Administrator Password Solution (LAPS)** was deployed to ensure secure and automated management of local administrator passwords across domain-joined machines, mitigating risks associated with credential misuse.

To enhance monitoring and incident detection capabilities, **Splunk** was integrated as a centralized logging and security analytics platform. Custom dashboards and alerts were configured to monitor critical events such as **logon activity, privilege escalations, unauthorized access attempts**, and potential Kerberos-based attacks, including **Golden Ticket** and **Silver Ticket** threats. This proactive monitoring ensures rapid detection and response to security incidents, strengthening the overall defense posture of the AD environment.

The effectiveness of the implemented hardening measures was validated using **PingCastle**, an Active Directory security assessment tool. PingCastle provided comprehensive health check reports, helping identify potential vulnerabilities and ensuring that the security posture adhered to industry standards. By leveraging PingCastle, the AD environment was further refined and validated to achieve a robust and secure configuration.

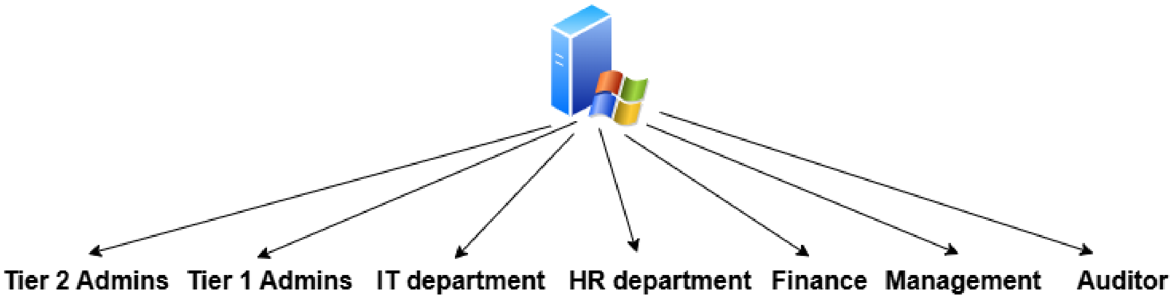
This project demonstrates a holistic approach to **Active Directory hardening** by integrating secure configurations, automated tools, proactive monitoring, and thorough testing. The result is a scalable, resilient, and security-focused AD environment that aligns with industry best practices for identity and access management.

Active Directory Network schema



- **Domain Controller** – Windows Server 2022 instance with implemented sysmon service. Works also as Splunk Forwarder to send events to Splunk Server.
- **Windows 10** – Instance that should imitate computer connected to company's network used by employee. This VM also provides sysmon service installed and sending logs to Splunk Server via Splunk Forwarder.
- **Splunk Server** – Instance with installed Ubuntu Server. Its purpose is to aggregate and store logs from above endpoints.
- **Kali Linux** – Instance to perform red team operations against AD network.

Active Directory OUs Company Structure



- **Tier 2 Admins** – Admins with basic access to regular employes. They should perform all day Admin tasks – resetting password, updating employe's information etc.
  - **Permissions:**
    - Managing regular employees accounts (resetting password, contact information updating)
    - Restricted access to employee's personal data, excluding financial information.

- **Tier 1 Admins** – Admins with higher privileges, managing Tier 1 Admins and Management accounts, excluding their confidential data (eg. comapany's finance data).
  - **Permissions:**
    - Managing all Tier 2 Admins with grant/revoke access privilege
    - Restricted access to managing accounts in OU Management
    - Viewing and editing technical logs (eg. system errors) from audits

- **IT department** – regular employees, performing all day tasks. (eg. Software devs)
  - **Permissions:**
    - Access to systems and applications within their department.

- **HR department** – regular employees, but with access to personal data of employees and their salaries.
  - **Permissions:**
    - Full access to employees personal data and salaries.
    - Privilege of creating regular employee accounts – IT, Tier 2 Admin

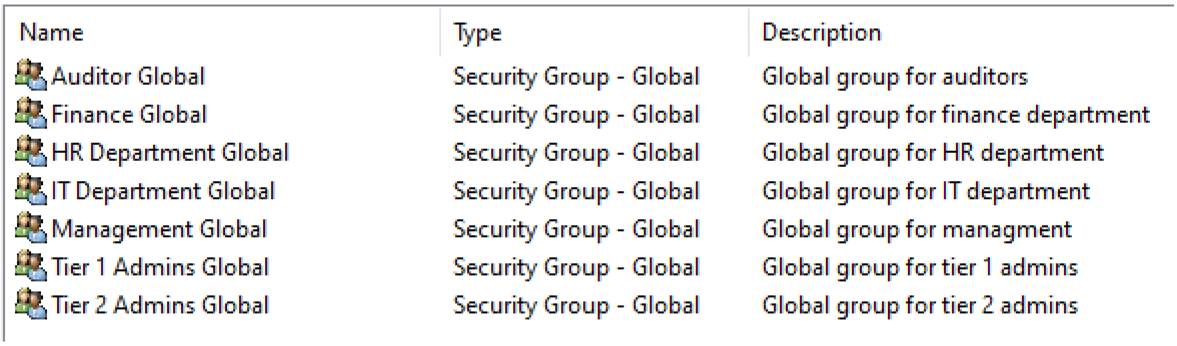
- **Finance** – regular employees, with access to employee’s salaries.
  - **Permissions:**
    - Read-only access to employee’s salaries and basic personal data.

- **Management** – high-profile managers, with access to classified company’s information.
  - **Permissions:**
    - Full access to company’s financial data.
    - Minimum necessary access to employee’s personal data, excluding salaries.

- **Auditor** – Security Auditor within the organization. His role is only to monitor security policy inside the domain.
  - Permissions:
    - Read only access to not confidential management data.
    - Read only access to logs and security audits inside organization.
    - Read only access to GPOs
    - No access to company’s financial data

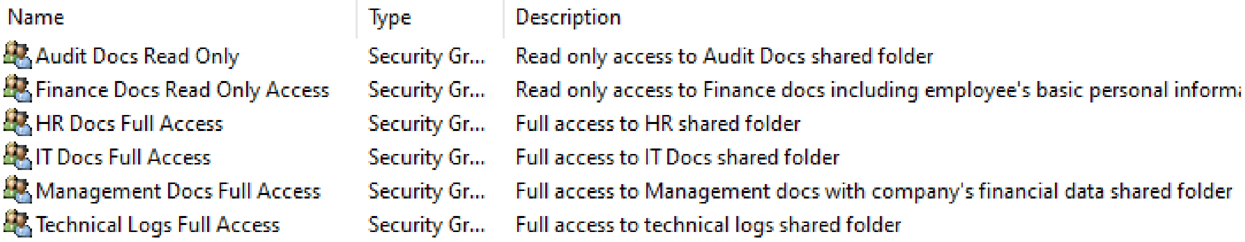
AGLDP implementation

As a first step to achieve AGLDP access-control policy is to create Global group for every department from domain.



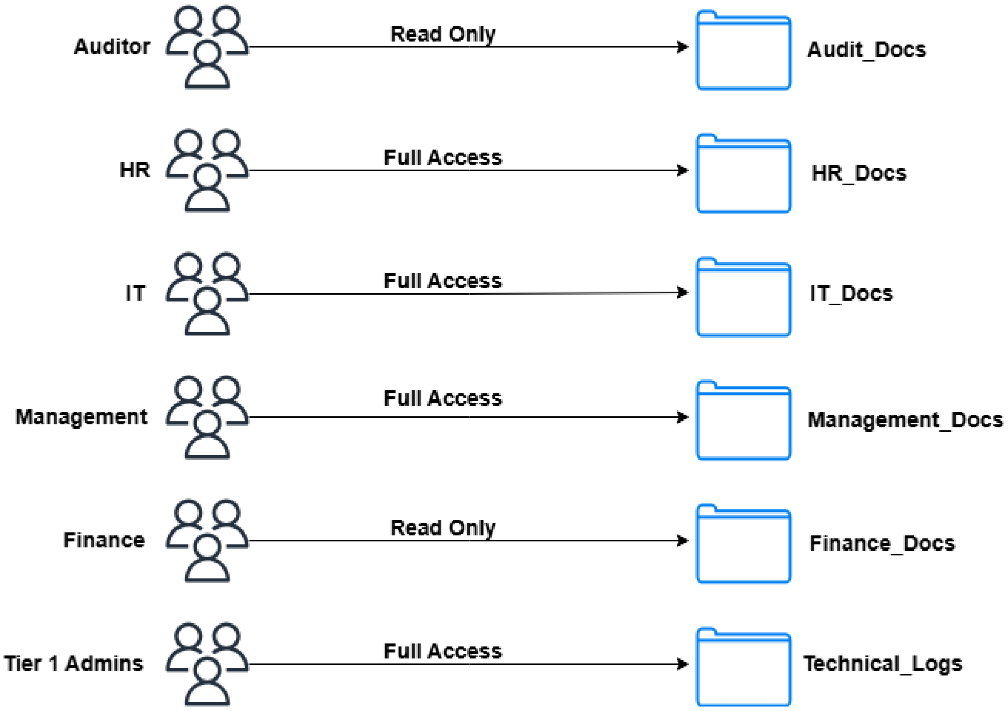
Name	Type	Description
Auditor Global	Security Group - Global	Global group for auditors
Finance Global	Security Group - Global	Global group for finance department
HR Department Global	Security Group - Global	Global group for HR department
IT Department Global	Security Group - Global	Global group for IT department
Management Global	Security Group - Global	Global group for managment
Tier 1 Admins Global	Security Group - Global	Global group for tier 1 admins
Tier 2 Admins Global	Security Group - Global	Global group for tier 2 admins

In the next step the Domain Local groups has been created to define access policy to certain shared folders and files:



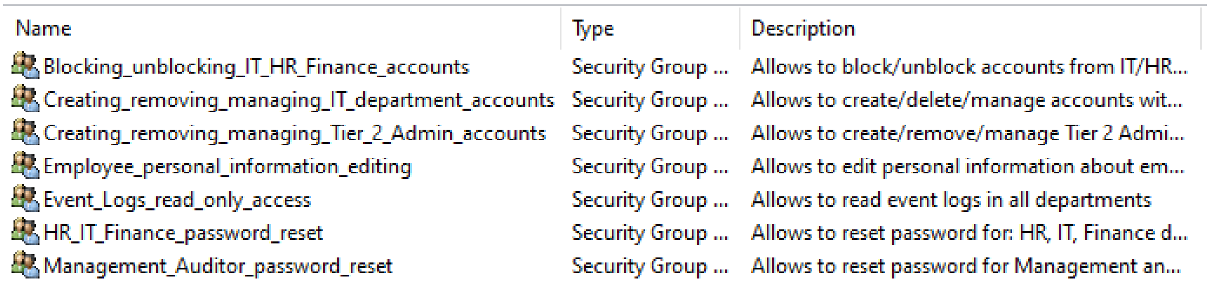
Name	Type	Description
Audit Docs Read Only	Security Gr...	Read only access to Audit Docs shared folder
Finance Docs Read Only Access	Security Gr...	Read only access to Finance docs including employee's basic personal informa
HR Docs Full Access	Security Gr...	Full access to HR shared folder
IT Docs Full Access	Security Gr...	Full access to IT Docs shared folder
Management Docs Full Access	Security Gr...	Full access to Management docs with company's financial data shared folder
Technical Logs Full Access	Security Gr...	Full access to technical logs shared folder

Below is presented the chart that shows final access of certain account group to specific shared folders:



Security privilege delegation

To ensure that every employee has minimal required access to perform his work, certain privilege delegations have been done:



Name	Type	Description
Blocking_unblocking_IT_HR_Finance_accounts	Security Group ...	Allows to block/unblock accounts from IT/HR...
Creating_removing_managing_IT_department_accounts	Security Group ...	Allows to create/delete/manage accounts wit...
Creating_removing_managing_Tier_2_Admin_accounts	Security Group ...	Allows to create/remove/manage Tier 2 Admi...
Employee_personal_information_editing	Security Group ...	Allows to edit personal information about em...
Event_Logs_read_only_access	Security Group ...	Allows to read event logs in all departments
HR_IT_Finance_password_reset	Security Group ...	Allows to reset password for: HR, IT, Finance d...
Management_Auditor_password_reset	Security Group ...	Allows to reset password for Management an...

1. Blocking_unblocking_IT_HR_Finance_accounts - Tier 1 Admins

- **Purpose:** Tier 1 Admins are allowed to block or unblock accounts within the IT, HR, and Finance departments. This is typically needed to enforce security protocols, such as quickly locking accounts in case of suspicious activities.
- **Real-world relevance:** In real environments, this control enables the helpdesk or first-level admins to maintain security standards without needing higher-level intervention. It ensures quick response to incidents within non-critical departments.

2. Creating_removing_managing_IT_department_accounts - HR Department

- **Purpose**: The HR department can create, delete, and manage user accounts specifically within the IT department. This delegation supports onboarding and offboarding of employees under HR's responsibility.
- **Real-world relevance:** HR teams are often responsible for managing employee lifecycles, and having control over IT accounts allows them to keep employee information updated while following HR processes.

3. Creating_removing_managing_Tier_2_admin_accounts – Tier 1 Admins

- **Purpose:** Tier 1 Admins have control over Tier 2 Admin accounts, allowing them to manage creation, deletion, and basic account settings.
- **Real-world relevance:** This is helpful in environments where higher level admin oversees administrative changes for specific administrative roles, such as Tier 2 Admins, allowing Tier 1 Admin to handle staffing updates while keeping high-level admin accounts restricted.

4. Employee_personal_information_editing - HR Department

- **Purpose:** HR can edit personal information for employees across all departments. This includes basic details like address, phone number, and position, but excludes access to sensitive information.
- **Real-world relevance:** HR teams need the ability to manage and update personal details for all employees, which is critical for record-keeping, payroll, and contact purposes.

5. Event_logs_read_only_access - Auditor Global and Tier 1 Admins

- **Purpose:** This grants Auditor Global and Tier 1 Admins read-only access to event logs across all departments, excluding the Domain Controller.
- **Real-world relevance:** Read-only access to logs enables Tier 1 Admins to monitor events for troubleshooting and allows auditors to review activity for compliance and security monitoring without the risk of modifying log data.

6. HR_IT_Finance_password_reset - Tier 1 and Tier 2 Admins

- **Purpose:** Both Tier 1 and Tier 2 Admins can reset passwords for users within the HR, IT, and Finance departments, facilitating user support for these areas.
- **Real-world relevance:** Password resets are a common task, and delegating it to both Tier 1 and Tier 2 Admins ensures quicker resolution of login issues, reducing downtime for employees.

7. Management_Auditor_password_reset - Tier 1 Admins

- **Purpose:** Tier 1 Admins are allowed to reset passwords for Management and Auditor accounts. This ensures support for critical accounts without involving higher-level administrators.
- **Real-world relevance:** Limiting password reset permissions for high-level accounts like Management and Auditors to Tier 1 Admins prevents misuse and maintains security for sensitive roles.

GPO implementation

Enhanced Default Domain Policy

1. Setting Account lockout for 15 minutes after 5 failed login attempts. Account lockout counter will reset after 15 minutes.
2. Setting Machine inactivity limit to 15 minutes (900 seconds) to ensure that unused machines will be automatically locked.
3. Password policy:
    a. Minimum password age: 1 day
    b. Maximum password age: 180 days
    c. Minimum password length: 8 characters (only for project purposes, in real environments password policy should enforce more complexed password proposals)
4. Preventing machine from storing hashes locally by LAN Manager.
5. Disabling all authentication via NTLM
6. Enabling option to encrypt or sign secure channel data (always).
7. Setting Machine inactivity limit to 15 minutes (900 seconds) to ensure that, not used DC will be automatically locked.

Enhanced Default Domain Controllers Configuration policy

1. Disabling Guest accounts.
2. Limiting Local Account to user blank password in console only.
3. Disabling anonymous SID/Name translation.
4. Disabling “Let everyone permissions apply to anonymous users”.
5. Kerberos Settings:
    a. Type of allowed encryptions: AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types
    b. Enforcing user logon restrictions
    c. Maximum lifetime for service ticket – 600 minutes
    d. Maximum lifetime for user ticket – 10 hours
    e. Maximum lifetime for user ticket renewal – 7 days
    f. Maximum tolerance for computer clock synchronization – 5 minutes

Enhanced Advanced Audit Policy Configuration

In this project, implementing the Advanced Audit Policy Configuration is critical for enhancing the monitoring and security of the Active Directory environment. These settings ensure detailed logging of key events, such as changes to user accounts, failed logon attempts, or modifications to security policies. By applying these configurations:

1. **Improved Accountability:** We can trace specific actions to individual users or processes, ensuring proper tracking of activities like account management and privilege usage.
2. **Enhanced Security Monitoring:** Policies such as Kerberos authentication tracking and sensitive privilege use auditing help detect unauthorized access attempts or misuse of administrative permissions.
3. **Operational Transparency:** Changes to Active Directory objects, such as security groups or directory services, are logged to maintain a clear audit trail.
4. **Compliance Support:** These settings align with industry best practices and demonstrate a commitment to maintaining secure and transparent operations within the organization.

This addition to the project demonstrates a proactive approach to security and ensures that the Active Directory infrastructure is prepared to meet real-world audit and compliance requirements.

Category	Policy Name	Policy Setting	Description
Account Logon	Audit Credential Validation	Success and Failure	Monitors failed credential validation tests during user logon attempts.
	Audit Kerberos Authentication Services	Failure	Logs failed Kerberos authentication requests.

	Audit Kerberos Service Ticket Operations	Success and Failure	Monitors Kerberos service ticket operations for user accounts.
Account Management	Audit Computer Account Management	Success	Logs changes to computer accounts (creation, modification, deletion).
	Audit Other Account Management Events	Success and Failure	Monitors and logs additional account management operations that are not covered by other specific policies.
	Audit Security Group Management	Success and Failure	Logs changes to security group memberships.
	Audit User Account Management	Success and Failure	Monitors modifications to user accounts (creation, password changes, etc.).
Detailed Tracking	Audit PNP Activity	Success	Logs Plug and Play activities, such as the installation or removal of devices, helping to monitor unauthorized hardware changes.
	Audit Process Creation	Success	Logs the creation of new processes and identifies the application or user responsible.
DS Access	Audit Directory Service Access	Success and Failure	Monitors access attempts to Active Directory objects.
	Audit Directory Service Changes	Success and Failure	Logs changes to AD objects, including creation, deletion, or modification.

Logon/Logoff	Audit Account Lockout	Success and Failure	Tracks account lockout events, helping to identify potential brute-force attacks or user lockout issues.
	Audit Group Membership	Success	Logs changes in group memberships, ensuring visibility into privilege escalations or role modifications.
	Audit Logoff	Success	Monitors user logoff events, providing insights into session activities and user behavior.
	Audit Logon	Success and Failure	Monitors successful and failed logon attempts.
	Audit Other Logon/Logoff Events	Success and Failure	Captures additional events related to session activities, such as remote disconnections or reconnects.
	Audit Special Logon	Success	Tracks logons with elevated privileges.
Object Access	Audit Detailed Share	Failure	Logs detailed information about shared folder access events.
	Audit File Share	Success and Failure	Monitors access to shared files and folders.
	Audit Other Object Access Event	Success and Failure	Tracks events generated by the management of task scheduler jobs or COM+ objects.
	Audit Removable Storage	Success and Failure	Tracks access attempts to removable storage devices.

Policy Change	Audit Audit Policy Change	Success	Logs changes to security audit policy settings.
	Audit Authentication Policy Change	Success	Logs changes to authentication policies, such as domain trusts or Kerberos settings.
	Audit Authorization Policy Change	Success	Tracks modifications to authorization policies ex. – assigning/removing user rights.
	Audit MPSSVC Rule-Level Policy Change	Success and Failure	Monitors changes to Windows Defender Firewall rules.
	Audit Other Policy Change Events	Failure	Logs changes to other policy settings not covered by specific audit policies.
Privilege Use	Audit Sensitive Privilege Use	Success and Failure	Monitors the use of sensitive privileges (e.g., Take Ownership).
System	Audit IPsec Driver	Success and Failure	Logs events related to IPsec driver activity, including initialization and termination.
	Audit Other System Events	Success and Failure	Tracks miscellaneous system events not covered by other policies, such as service failures.
	Audit Security State Change	Success	Monitors changes in the system's security state, such as startup or shutdown of security services.
	Audit Security System Extension	Success	Logs events related to the loading or unloading of security system components, such as antivirus or intrusion detection systems.
	Audit System Integrity	Success and Failure	Logs events that could compromise the integrity of the security subsystem.

AD Workstations Security Policy

1. Disallowing plugging-in all USB devices except of keyboards and mouses:
    a. Allowed Mouse GID: 4D36E96F-E325-11CE-BFC1-08002BE10318
    b. Allowed Keyboard GID: 4D36E96B-E325-11CE-BFC1-08002BE10318
    c. Enabling: “Removable Disks Deny: read, write, execution”
2. Windows Defender on Workstations
    a. Disabling option to turn off Windows Defender on Workstations
    b. Real-time protection
        i. Turn off real-time protection – disabled
        ii. Monitor file and program activity on your computer – enabled
        iii. Scan all downloaded files and attachments – enabled
        iv. Turn on behavior monitoring – enabled
    c. Security Intelligence Updates
        i. Specify the day of the week to check for security intelligence updates – disabled (it will update it every day because that is the default setting)
3. Disabling Guest accounts.
4. Preventing machine from storing hashes locally by LAN Manager.
5. Limiting Local Account to user blank password in console only.
6. Disabling anonymous SID/Name translation.
7. Disabling “Let everyone permissions apply to anonymous users”.
8. Enabling option to audit all attempts of authentication via NTLM
9. Enable User Account Control (UAC):
    a. Behavior of the elevation prompt for administrators in Admin Approval Mode – Prompt for consent on secure desktop
    b. Run all administrators in Admin Approval Mode
    c. Behavior of the elevation prompt for standard users – Prompt for credentials
    d. Only elevate executables that are signed and valid - Enabled
    e. Virtualize file and registry write failures to per-user locations – Enabled
    f. Admin Approval Mode for the Built-in Administrator account – Enabled
    g. Switch to the secure desktop when prompting for elevation – Enabled
    h. Detect application installations and prompt for elevation – Enabled
    i. : Behavior of the elevation prompt for administrators in Admin Approval Mode – elevate without prompting

AD Workstations – Local Admin Group Members

Adding GPO linked to AD Workstations OU to enforce Local Admin Group Membership only for users/groups:

1. PROJECT\Domain Admins
2. PROJECT\Tier 1 Admins Global
3. Administrator

AD Workstations – Firewall baseline policy

1. Windows Defender Firewall startup mode is set to automatic
2. Protect all network connections – enabled
3. Enabling Firewall on all types of connections: Domain, Public, Private
4. Allowing connections to port 445/TCP (SMB) only from inside the domain

GPO for standard users

Policy that will be inherited by all users inside Departments OU, so in practice all Users expect Enterprise admin.

1. Limited access to Control Panel.
2. Enabling "Prohibit User Installs".
3. Prevent access to registry editing tools

GPO with exceptions for Tier 1 Admins

Policy that will overwrite "GPO for standard users" to ensure that Admins will have necessary tools and options available for them.

1. Disabling limited access to Control Panel inherited from "GPO for standard users".
2. Disabling "Prohibit User Installs" inherited from above GPO.

AD Hardening

LAPS

LAPS has been implemented to enhance the security of local administrator accounts by ensuring that each machine has a unique, automatically managed local administrator password. These passwords are securely stored in Active Directory and can only be accessed by authorized users, mitigating the risk of lateral movement during potential attacks and aligning with best practices for Active Directory hardening.

LAN Manager authentication level

The LAN Manager authentication level has been configured in the Enhanced Default Domain Policy to enforce the use of NTLMv2 and disable the use of weaker authentication protocols. This ensures enhanced security by preventing the use of outdated and vulnerable LAN Manager authentication methods, reducing the risk of credential theft and unauthorized access.

Non-admin users can’t add computers to a domain

The "Add workstations to a domain" option has been configured in the Enhanced Default Policy to restrict this privilege exclusively to the Domain Admins and Tier 1 Admins Global groups. This ensures that only authorized administrative groups can join devices to the domain, reducing the risk of unauthorized or rogue machines being added and enhancing overall domain security.

Disabling Admin Account delegation

The "Account is sensitive and cannot be delegated" setting has been enabled for the Domain Administrator account. This ensures that the account cannot be used in delegation scenarios, protecting it from being misused in unauthorized service or task delegations. This configuration strengthens the security of the most privileged account in the domain, minimizing potential attack vectors.

Deleting every user from group „Schema Admins”

All users have been removed from the Schema Admins group to minimize potential risks associated with accidental or malicious schema modifications. This group now remains empty by default, adhering to best practices for Active Directory security by restricting access to highly privileged operations only when absolutely necessary.

Enabling Recycle Bin

The "Enable Recycle Bin" feature has been activated in the Active Directory environment. This provides the ability to recover deleted objects, such as users or groups, with their attributes intact, improving resiliency and minimizing the impact of accidental deletions. This setting is part of strengthening Active Directory management and ensuring data recoverability.

Creating Backup

Creating regular backups of Active Directory is a critical practice to ensure the safety and recoverability of the environment in case of data corruption, accidental deletions, or cyberattacks. Backups allow restoration of objects, configurations, and the directory structure to a previous state, minimizing downtime and data loss. This is an essential part of maintaining a robust disaster recovery plan.

Disabling spooler service

Disabling the Spooler service has been implemented to mitigate the risk of Print Spooler vulnerabilities being exploited, which are commonly used for privilege escalation or remote code execution attacks. By turning off this service on Domain Controllers, I ensure that unnecessary attack surfaces are minimized, aligning with best practices for securing critical infrastructure.

Reducing the number of computers a regular user can add

Reducing the number of computers a regular user can add to a domain has been implemented to limit unauthorized additions of devices to the network. By setting this value to 0, only authorized administrators, such as Domain Admins, tier 0 admins can add computers to the domain, thereby enhancing security and reducing potential attack vectors.

Adding subnet to Active Directory Sites and Services

Adding subnets to Active Directory Sites and Services has been implemented to ensure accurate site-to-subnet mapping. This allows clients to efficiently locate the nearest Domain Controller, optimizing authentication and replication traffic while reducing latency. It also enhances security by restricting authentication and replication to specific network boundaries.

Enhancing audit policy

The following audit policies were identified as missing on the domain controllers:

1. **Detailed Tracking / DPAPI Activity**

   Missing this policy means that sensitive operations related to the Data Protection API (DPAPI), such as the generation or retrieval of protected secrets, are not being tracked. This can result in a lack of visibility into potential misuse or attacks on encrypted data within the environment. **Setting was set to success/failure.**

2. **Account Logon / Kerberos Authentication Service**

   The absence of this policy impacts the auditing of Kerberos authentication requests, including ticket-granting ticket (TGT) requests and other Kerberos-related activity. This could lead to a loss of insight into authentication attempts, potentially obscuring suspicious or unauthorized activity. **Setting was changed from failure to success/failure.**

Hardening UNC Paths (SYSVOL, NETLOGON)

UNC Hardening for SYSVOL and NETLOGON is a security enhancement applied to Universal Naming Convention (UNC) paths, specifically those used by SYSVOL and NETLOGON shares in an Active Directory environment. This configuration enforces stronger authentication and integrity requirements when accessing these critical network paths.

Splunk

Splunk has been seamlessly integrated into the Active Directory (AD) environment to enhance monitoring, security, and reporting capabilities. This integration allows for advanced detection of security events, proactive alerting, and robust infrastructure health assessments, ensuring the AD environment remains secure and well-maintained.

AD basic security dashboard

A comprehensive **Active Directory Basic Security Dashboard** has been developed on the Splunk platform to monitor critical AD activities in real-time. The dashboard includes visibility into the following events:

- **User Logon Events** – Successful authentication to the AD network.
- **User Logoff Events** – Monitoring of user session terminations.
- **Privilege Escalation Events** – Alerts for privilege modifications or escalations.
- **Account Lockouts** – Tracking and alerting for user accounts locked due to failed login attempts.
- **Security Alerts** – Proactive identification of potential security incidents.

Security alerts

Several critical alerts have been configured within Splunk to detect unauthorized activities and potential threats against the AD environment. These alerts include:

1. **Unauthorized Access Detection**
    a. **Trigger:** 5 failed login attempts within a 10-minute threshold.
    b. **Purpose:** Detect and mitigate unauthorized access attempts.
2. **Group Policy Modification Alert**
    a. **Trigger:** When a Group Policy Object (GPO) has been modified.
    b. **Frequency:** Checker runs every hour.
    c. **Purpose:** Ensures visibility and control over critical policy changes.
3. **Golden Ticket Attack Detection**
    a. **Trigger:** Potential attack on a Golden Ticket.
    b. **Frequency:** Checker runs every 5 minutes.
    c. **Purpose:** Detects forged Kerberos tickets used for lateral movement and privilege escalation.

4. **Silver Ticket Attack Detection**
    a. **Trigger:** Suspicious activity indicative of a Silver Ticket attack.
    b. **Frequency:** Checker runs every 5 minutes.
    c. **Purpose:** Identifies attempts to exploit Kerberos service tickets for unauthorized access.
5. **Brute Force Attack Against Kerberos Alert**
    a. **Trigger:** More than 10 failed authentication attempts detected in a short period.
    b. **Frequency:** Checker runs every 5 minutes.
    c. **Purpose:** Detects and mitigates brute force attacks targeting Kerberos authentication.

Active Directory infrastructure health report

To ensure the health and security of the AD infrastructure, automated reporting has been implemented. A **weekly AD Health Report** is generated to assess the following:

1. **Account Creation and Deletion**
    a. Monitors changes in user and computer accounts, ensuring all modifications are authorized and documented.
2. **Accounts without Password Expiration**
    a. Identifies any accounts configured with passwords that do not expire, which can pose a security risk.
3. **High Privilege Group Changes**
    a. Tracks all changes made to high-privilege groups (e.g., Domain Admins, Enterprise Admins), ensuring visibility into potential misuse or privilege escalation.