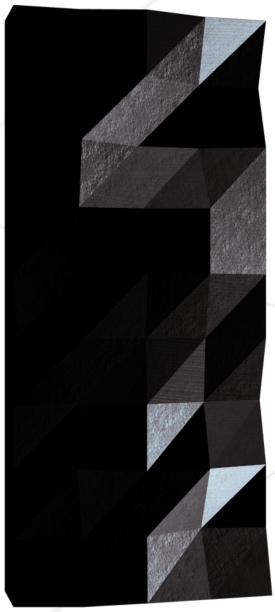

Administrative Directory

Introduction to GPO and SIEM.

Summary: This subject introduces you to Active Directory's GPO and SIEM for analyzing your event log.

Version: 1.00

Contents

Chapter I

Preamble

This subject is the production of a partnership between 42 and Microsoft Corporation.

Microsoft Corporation is an American multinational technology corporation headquartered in Redmond, Washington.Microsoft's best-known software products are the Windows line of operating systems, the Microsoft Office suite, and the Internet Explorer and Edge web browsers.

Through this partnership, we aim to provide you with a unique opportunity to simplify your journey towards obtaining certifications offered by Microsoft. These certifications hold significant value and recognition in the industry, enabling you to enhance your professional profile and unlock exciting career prospects in the field of security.

To access the Microsoft certification programs and explore the wide range of certificates available, you can visit the following link: Microsoft Security Certification. This comprehensive platform offers extensive training resources and examinations covering various security-related topics.

By successfully completing the projects and earning Microsoft certifications, you will demonstrate your proficiency and expertise in security practices. These certifications serve as a testament to your skills and can open doors to exciting career opportunities.

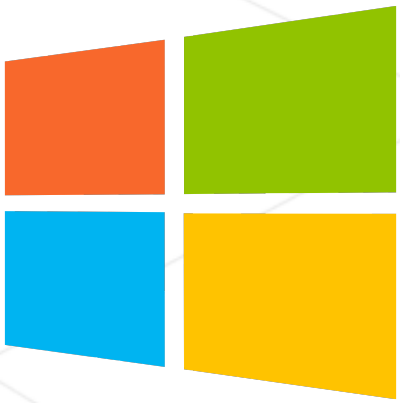

Figure I.1: https://www.microsoft.com/

Chapter II

Info

In partnership with Microsoft

Domolia is highly satisfied with the deployment you have completed for them. They now have a desire to enhance the security measures regarding user access and monitor network activities. To achieve this, they would like you to utilize two built-in features of Active Directory: GPO and SIEM.

GPOs serve as "rules" that are enforced on the network and users, while SIEM functions as a logging system that records all network activities.

You're provided with a helper pdf, foundable inside the attachments of the subject.
It will show you how to access the VMs created for you to complete this subject, how to lock your VMs, etc.

Chapter III

Mandatory part

III.1 Preparation

In this subject, you are required to carry out specific preparations and creations :

- Organisation Unit "Workspace"
- Organisation Unit "Administration"
- Group "Worker"
- Group "Direction"
- Group "Secretary"
- Group "Administrator"
- Disk "D:"
- Disk "E:"
- Folder "D:/WorkPlan"
- Folder "D:/Management"
- Folder "E:/HumanResources"
- Folder "E:/Estimate"
- Folder "E:/Client"

III.2 GPOs creation

Now that the preparations have been completed, here is the list of GPOs they would like you to create.

- Define screen desktop
- Define OpenOffice program deployement if required by each user
- Define Slack non-optionnal installation for each new user
- Allow groups to access certain disk, and automaticaly connect to them
  Every groups should access the two mandatory disks
- Allow groups to access certain folders, with example as :
  Worker : Access to folders :
  - D:/WorkPlan
  - D:/Management
  - E:/HumanResources

  Direction : Access to folders :
  - D:/WorkPlan
  - E:/HumanResources
  - E:/Estimate
  - E:/Client

  Secretary : Access to folders :
  - D:/Management
  - E:/HumanResources
  - E:/Estimate
  - E:/Client

  Administrator : Access to every folder
- Allow groups to edit certain folders/files
  Worker : Edit folder :
  - D:/WorkPlan

  Direction : Edit folders :
  - D:/WorkPlan
  - D:/Management
  - E:/HumanResources
  - E:/Estimate
  - E:/Client

  Secretary : Edit folders :
  - D:/Management
  - E:/HumanResources
  - E:/Estimate
  - E:/Client

  Administrator : Can edit every folders
- Allow groups to create certain folders/files
  Worker : Create files in :
  - D:/WorkPlan

  Direction : Create files in :

- D:/WorkPlan
- D:/Management
- E:/HumanResources
- E:/Estimate
- E:/Client

Secretary : Create files in :
- D:/Management
- E:/HumanResources
- E:/Estimate
- E:/Client

Administrator : Can create files in every folders

- Allow groups to delete certain folders/files
  Worker : Nothing
  Direction : Delete files in
  - D:/WorkPlan,
  - D:/Management,
  - E:/HumanResources,
  - E:/Estimate
  - E:/Client

  Secretary : Delete files in
  - D:/Management,
  - E:/HumanResources
  - E:/Estimate
  - E:/Client Administrator : Can delete files in every folders

III.3 Network event logging

In addition to your GPO and installation work, Domolia has requested that you implement a method for them to receive notifications regarding network activities.

They are interested in obtaining information about the following activities:

- Computer Account Management Activity
- Distribution Group Management Activity
- Security Group Management Activity
- User Account Management Activity
- Directory Service Access Activity
- Logoff Activity
- Logon Activity

`The Domolia manager has heard the term SIEM used without necessarily understanding why.`

III.4 Logging scripts

In addition to monitoring, you have been tasked with creating any necessary scripts to facilitate log reading. Domolia has specifically requested the ability to perform the following operations through a script:

- A script that list who's connected between 2 time tag
- A script to show event concerning one user between 2 time tag
- A script to isolate access and modification one certain folder
- A script to list of IPs used by users
- A script listing security incidents

Chapter IV

Bonuses

Below are some suggested bonus ideas that you can create. Some of them may prove to be useful. Feel free to come up with your own ideas as well, which will be evaluated by your evaluator based on their individual preferences.

- Some GPO
- Some SIEM necessary log
- Some script to activate/deactivate SIEM log type
- Some script to automatize actions over SIEM log

The bonus part will only be assessed if the mandatory part is PERFECT. Perfect means the mandatory part has been integrally done and works without malfunctioning. If you have not passed ALL the mandatory requirements, your bonus part will not be evaluated at all.

Chapter V

Submission and peer-evaluation

You're provided with a helper pdf, foundable inside the attachments of the subject.
It will show you how to access the VMs created for you to complete this subject, how to lock your VMs, etc.

Once you've finish your assignment, you may lock your virtual machine, following the "Submission" section of the helper PDF. Note that, once locked, you will not be able to edit your virtual machines anymore, and a snapshot will be taken of your virtual machines at this moment, and will be reset to said snapshot before each evaluation.

So, be sure to have completly finished your work, as no modification non-requested by the scale will be acceptable during the evaluation !