

LepideAuditor

Sample Data Risk Assessment Report


Welcome to the Lepide Risk Assessment

The Lepide Risk Assessment Report is a detailed summary of the potential security threats in your organisation right now. It is based on data collected over 15 days from a sample of your live environment and is designed to highlight security vulnerabilities and recommend remediation.

DISCLAIMER

The information contained in these documents is confidential, privileged and intended only for the recipient. It may not be published or redistributed without the prior written consent of both Lepide and the recipient.

Contents Summary



- 1 Permissions and Privileges
- 2 User and Entity Behavior Analytics
- 3 Environment States and Changes
- 4 Risk Summaries
- 5 Recommendations

Permissions & Privileges



Risk Level - Moderate

Knowing who has access to your data and when these permissions change is critical to ensuring you are operating on a policy of least privilege and reducing the risk of privilege abuse.

Risk Summary:

We detected 33 changes to File Server permissions and 29 changes to Exchange Server permissions which may both require further investigation.

High levels of permission changes could indicate data potentially becoming over exposed; which could lead to vulnerabilities and a higher risk of a data breach occurring.

Recommended Actions:

Your organization should be operating on a policy of least privilege where users only have access to the files and folders they need to do their job, nothing more.

We recommend that you regularly review, and create proactive alerts for permission changes.

Whenever permission changes occur to your most sensitive data, they need to be analyzed to determine whether they are necessary or should be reversed.

29

Exchange Server Permission Changes

779

Mailbox Modifications

33

File Server Permission Changes

35

AD Group Modifications

Lepide Auditor 18.6

Permissions by Object

Object Name	Object Type	Owner	Content Type	Risk Level	Last Scan
Admin Team	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Apprentice and Graduate	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Autocad	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Business Improvement	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
CAE	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Electrical	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Human Resources	FOLDER	apvblr\Administrators	N/A	N/A	19/11/2018 15:00:06
IED	FOLDER	apvblr\Administrators	N/A	N/A	19/11/2018 15:00:06

Access Type	Permission	Permission Method	Inherited From	Applies To
Full Control	Direct Applied	Not inherited	This folder, subfolders...	
Read permissions, Cha...	Through Ownership	Not inherited	This Object only	

Effective Permissions: (Full Control)

Effective Permission: list folder / read data, create files / write data, create folders / append data, read extended attributes, write extended attributes, traverse folder / execute file, delete subfolders and files, read attributes, write attributes, delete

User & Entity Behavior



Risk Level - High

Knowing how your users and entities are interacting with your data is critical to ensuring that data breaches and attacks do not go unnoticed.

Risk Summary:

A high number of failed logons could be indicative of a brute force attack.

Over 10,000 files copied over the analysis period could potentially be an indication of a data breach and drastically increases the threat surface area.

A large number of files being moved and modified could result in data being stored in unsecure locations or being hidden.

Over 24,800 failed file reads coupled with over 5,000 files renamed could signify a potential ransomware attack in motion, immediate investigation is recommended.

Recommended Actions:

The sheer volume of failed logons, file/folder modifications and file copy events per day makes proactive monitoring essential.

A longer learning period is required to better determine whether these figures are normal for the organization or indicative of ongoing attacks/threats.

A longer learning period will also ensure that our anomaly spotting technology will become more accurate.

5,073

Failed Logons

10,535

Files Copied

24,867

Failed File Reads

5,220

Files Renamed

583

Files Moved

38,552

Files Created

LepideAuditor 18.6

Object Name	Object Type	Owner	Content Type	Risk Level	Last Scan
Admin Team	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Apprentice and Graduate	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Autocad	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Business Improvement	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
CAE	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Electrical	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Human Resources	FOLDER	apvblr\Administrators	N/A	N/A	19/11/2018 15:00:06
IED	FOLDER	apvblr\Administrators	N/A	N/A	19/11/2018 15:00:06

Access Type	Permission	Permission Method	Inherited From	Applies To	Read	Write	Execute	Full Control	Read Attributes	Write Attributes	Read Extended Attributes	Write Extended Attributes
Full Control	Full Control	Direct Applied	Not inherited	This folder, subfolders...	✓	✓	✓	✓	✓	✓	✓	✓
Read permissions, Cha...	Read permissions, Cha...	Through Ownership	Not inherited	This Object only	✓	✓	✓	✓	✓	✓	✓	✓

States & Changes



Risk Level - High

An important part of data security is understanding whether the infrastructure surrounding the data is secure. If you spot any environment states or changes that pose a risk to data security, action needs to be taken.

Risk Summary:

A large number of inactive / stale users creates a larger attack surface for external threats.

It is recommended that passwords should be rotated on a regular basis to reduce the risk of a user or service account being compromised. It is not recommended to have any accounts where the password is set to never expire.

OU and Sec Group Modifications can potentially lead to unnecessary access being granted to systems and resources that could put your data at risk.

Open shares increase the risk of privilege abuse resulting in data breaches.

Recommended Actions:

Make sure you're operating on a policy of least privilege by reducing the number of open shares to zero. Open shares may leave data vulnerable to exposure.

Create stricter password policies that require all users to change their passwords regularly (every 30 days, for example) and not to share passwords.

Implement adequate security controls and monitor any modifications to your environment to ensure they don't result in over-privileged users.

425

Inactive Users

214

Users with Passwords That Never Expire

80

Password Change Attempts

32

OU Modifications

32

Security Group Modifications

3

Open Shares

Lepide Auditor 18.6

Permissions by Object

Object Name	Object Type	Owner	Content Type	Risk Level	Last Scan
Admin Team	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Apprentice and Graduate	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Autocad	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Business Improvement	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
CAE	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Electrical	FOLDER	apvblr\Administrators	N/A	N/A	26/11/2018 15:00:07
Human Resources	FOLDER	apvblr\Administrators	N/A	N/A	19/11/2018 15:00:06
IED	FOLDER	apvblr\Administrators	N/A	N/A	19/11/2018 15:00:06

Access Type	Permission	Permission Method	Inherited From	Applies To	Read	Write	Execute	Full Control	Read Attributes	Write Attributes	Read Extended Attributes	Write Extended Attributes
Full Control	Full Control	Direct Applied	Not inherited	This folder, subfolders...	✓	✓	✓	✓	✓	✓	✓	✓
Read permissions, Cha...	Read permissions, Cha...	Through Ownership	Not inherited	This Object only	✓	✓	✓	✓	✓	✓	✓	✓

Risk Summaries

LOW RISK

0 AD Permission Modifications
0 Mailbox Database Modifications
0 Policy Modifications
0 Admin Template Policy Modifications
0 Startup Script Modifications
0 Security Options Policy Modifications
0 Trust Modifications
0 Schema Modifications
0 DNS Zone Modifications

Recommendation

Continuous and proactive scanning of your IT environment is required to ensure that no states or changes pose risk to your data. Continually monitor activity to spot any anomalous user and entity behavior.

MEDIUM RISK

29 Exchange Server Permission Changes
779 Mailbox Modifications
33 File Server Permission Changes
35 AD Group Modifications
425 Inactive Users
44,355 Files Created/Moved/Modified

Recommendation

There is a large attack surface that needs to be addressed. Clean up inactive users and audit file creations/modifications to address this problem. Determine which users are trying to access files they don't have permission to and monitor them closely.

HIGH RISK

5,073 Failed Logons
3 Open Shares
10,535 Files Copied
24,867 Failed File Reads

Recommendation

You need to determine why you are seeing so many failed logons. Is there a brute force attack underway? Ensure that you remove all open shares to reduce your potential attack surface and the chance of privilege abuse. Audit file copy events and failed file reads to determine whether sensitive data is at risk.

Recommendations and Summary

Based on our 15 day analysis of your environment, we have determined the following next steps we believe that you should take to immediately increase your data security.

STEP 1

You need to determine why you are seeing so many failed logons. Is there a brute force attack underway? Ensure that you remove all open shares to reduce your potential attack surface and the chance of privilege abuse. Audit file copy events and failed file reads to determine whether sensitive data is at risk.

STEP 2

Upon identifying sensitive data and potential risks and threats that could lead to a security or data breach, ensure there are adequate and efficient security controls in place to effectively mitigate the risk. This could include alerting, monitoring, auditing and a periodic review process which should not be limited to a single team. Encourage effective data owners, department managers and all other personnel responsible for sensitive data to manage these security controls implemented by the DCAP solutions.

STEP 3

Categorize, in order of importance, the highest areas of risk surrounding the silos that require adequate protection starting with the data at most risk first. Also, identify if applicable where there could be a crossover between solution specific functionality based upon storage type but also upon the different security controls required such as DCAP and DLP as an example.

STEP 4

Where applicable, look for native security controls and log sources that can be leveraged and integrated with DCAP specific security solutions. Understand the shortcomings between the different types of security solutions available and through continuously monitoring and reviewing any existing security controls, perform a gap analysis in the existing security strategy and plan for appropriate measure to fill those gaps.

STEP 5

Identify how data is being transferred between data silos and the user interactions surrounding the data. Understand the permissions and privileges being granted to both users and applications/systems and where appropriate, revoke any unnecessary permissions to adopt a least privilege model surround the data.

ABOUT LEPIDE

Lepide are the fastest growing provider of data-centric audit and protection solutions to enterprises all over the world. The award-winning LepideAuditor enables you to put data at the heart of your security strategy; mitigating the risks of data breaches and helping to meet compliance requirements.



Discovery &
Classification



Permissions &
Privileges



User & Entity
Behavior



Environment
States & Changes

