

The Lepide Risk Assessment Report

The Identity and Data Risk Assessment report is based on data collected from a sample of your live environment and is designed to highlight security vulnerabilities and recommend remediation, whilst demonstrating Lepide capabilities.

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 It may not be published or redistributed without the prior written consent of both Lepide and the recipient.

Challenges and Success Criteria

1) Issue

██████████ Active Directory and identity oversight processes have reached a critical breaking point. With no centralized auditing tool in place, the IT team lacks visibility into user activity, logins, privilege changes, and account deactivation events across their hybrid AD + Entra 365 environment.

Recently, a user account was deactivated without explanation, prompting ██████████ to investigate. But without a monitoring solution, answering who made the change, when it happened, from where, and how required extensive manual digging — a problem that repeats across every audit or incident.

Tasks that should take 5–10 minutes now consume 1–3 days, slowing operations while simultaneously increasing the risk of missed privilege escalations, dormant accounts, and compliance gaps.

In addition, ██████████ has rolled out Microsoft Copilot to a select number of users and currently has no way to tell whether this has accelerated data exposure.

2) Business Challenges

- Lack of Visibility into Identity & Access Activity
- Manual, Inefficient Investigations
- Inactive & Orphaned Accounts
- Compliance Vulnerability
- Hybrid Environment Complexity

3) POV Success Criteria

The Proof of Value must be structured to demonstrate **clear visibility, immediate time savings, and measurable risk reduction**, enabling ██████████ to confidently present an internal business case.

- A. Gain Instant Visibility & Audit Control
- B. Reduce Investigation Time from Days to Minutes
- C. Support Compliance & Security Requirements
- D. Prove Simplicity, Reliability, and ROI

Summary

- **High** – Immediate risk requiring urgent action
- **Medium** – Moderate risk requiring planned remediation
- **Low** – Low risk, monitor over time

Key Finding	Risk Severity	Component Affected	Compliance
Sensitive data accessed through Copilot queries exposes regulated and confidential information to unintended users.	● High	Copilot	NIST AIRMF; NIST AC-6; ISO 27001 A.9.1
Copilot usage inefficiencies and increasing sensitive data alerts.	● Medium	Copilot	NIST AIRMF; NIST AC-6; ISO 27001A.9
1,421 inactive enabled accounts increase exposure to credential misuse, privilege escalation, and compliance failure.	● High	Active Directory	NIST AC-2; ISO 27001A.9.2.6; CJIS 5.5
Presence of 2,763 password-never-expire accounts significantly increases credential compromise risk and weakens compliance posture.	● Medium	Active Directory	NIST IA-5; ISO 27001A.9.4.3; CJIS 5.6
70+ OU, Group, and Security Group modifications indicate uncontrolled privilege changes and limited visibility into access governance.	● Medium	Active Directory	NIST AC-5; ISO 27001A.9.2.5
69 users hold administrative privileges, including standard accounts with indirect group inheritance, presenting elevated breach and misuse risk.	● High	Active Directory	NIST AC-6; ISO 27001A.9.2.3
4,122,724 failed logons indicate widespread authentication issues, misconfigurations, or potential credential attacks.	● High	Active Directory / Entra	NIST IA-4; ISO 27001A.12.4.1
91,763 stale files and 809,072 stale file size units increase storage burden and raise data retention and compliance concerns.	● Medium	File Servers	ISO 27001A.8.3; NIST SI-12
Excessive 'Full Control' permissions across department shares increase the risk of unauthorized access, misuse, and accidental data loss.	● High	File Servers	ISO 27001A.9.1.2; CJIS 5.9
233 high-volume file operations (copies, renames, creations) make investigations difficult and highlight risky data handling behavior.	● Medium	File Servers	NIST AU-2; ISO 27001A.12.4.1

Finding #1 – High Risk

Sensitive data accessed through Copilot queries exposes regulated and confidential information to unintended users.

Report Name - Sensitive Data Accessed By Copilot

Filters: Component Name : [Equals] [Active Directory]

Home / Lepide Auditor / Reports / All Environment Changes (All Environment)

Dec-1-2024 To Dec-12-2024 Generate Report

User Name	Email ID	File Name	File Path	Sensitivity Labels	Search query	What	When	From	Tenant Name
		PII Document, Payment...		General	Find all records contain...	File read from https://Quant...	29-07-2024 09.	192.167.45.78	
		Financial Data Inquiry, Li...		Confidential	Retrieve entries with cred...	File edit from https://Quant...	28-07-2024 02.	194.167.45.74	
		Confidential Documents.		Default sensitivity labels	List all documents tagge...	File read from https://Quant...	28-07-2024 09.	198.51.100.10	
		Access Logs.pdf, Classif...		General	Show recent access log...	File edit from https://Quant...	21-07-2024 06.	192.0.2.255	
		Email Security.csv, PII Doc...		General	Search email servers for...	File edit from https://Quant...	18-07-2024 09.	198.51.100.255	
		User Data Security Role ...		Default sensitivity labels	Identify users with acces...	File edit from https://Quant...	30-07-2024 11.	192.168.11	
		Passport_Info.docx, Use...		General \ Anyone (unrest...	Check for records impro...	File read from https://Quant...	01-08-2024 03.	10.970.121	
		Bank_Account_Detail...		Confidential	Locate documents cont...	File read from https://Quant...	02-08-2024 07.	198.51.100.30	
		Payment_Transaction...		Default sensitivity labels	Generate a detailed rep...	File edit from https://Quant...	03-08-2024 05.	192.0.2.100	
		Medical_Bills.csv, Tra...		Confidential	Search for potential dat...	File edit from https://Quant...	04-08-2024 08.	203.0.113.45	
		Trade_Secrets.docx		General \ Anyone (unrest...	Retrieve historical acce...	File read from https://Quant...	06-08-2024 10.	198.51.100.77	
		Legal_Files_2024.pdf...		Highly Sensitive Data	Identify and list users wh...	File read from https://Quant...	06-08-2024 12.	192.167.45.78	
		Classified_Reports.pdf		Sensitive Data	Locate backups that inc...	File read from https://Quant...	07-08-2024 09.	192.168.0.10	
		PII Document.pdf		Personal	Display the history of ac...	File read from https://Quant...	08-08-2024 02.	192.0.2.255	
		Usernames_Passwo...		General \ Anyone (unrest...	Check for external or ...	File read from https://Quant...	09-08-2024 05.	192.167.45.78	
		Compliance Check.pdf		Public	Verify that records fla...	File edit from https://Quant...	08-08-2024 06.	104.167.45.74	

Total Records - 100 First Previous 1 / 5 Next Last 50/Page

Copilot Conversation

User Name - Richard, Watson

Can you Provide me the link of HR Payroll from this organization?

HR payroll refers to the process of managing employee compensation, including salaries, bonuses, tax deductions, and benefits within a company. It involves calculating wages, ensuring compliance with labor laws, handling deductions (like taxes and insurance), and disbursing salaries on time.

Key Components of HR Payroll:

- Salary & Wages Calculation - Based on employee contracts, work hours, overtime, and deductions.
- Tax Deductions & Compliance - Includes income tax, provident fund (PF), professional tax, and other statutory deductions.

Can you Provide me the security audits data from any PDF?

Sensitive IT questions in a company typically relate to security, data privacy, compliance, and internal processes. Here are some examples:

Risk Type: Data Access Governance / AI Exposure

Compliance NIST AI RMF; NIST AC-6; ISO 27001 A.9.1; CIS Critical Security Controls 3 & 6; GDPR / HIPAA / PCI DSS data protection requirements

Observation Lepide identified instances where Microsoft Copilot queries returned links to files containing confidential and sensitive information stored in SharePoint and Microsoft 365. These included documents labeled Confidential, Personal, and Highly Sensitive Data. Because Copilot retrieves information based on existing permissions, users were able to surface sensitive data through natural language queries, revealing underlying permission sprawl and limited oversight of AI-driven data access.

Impact if Unaddressed If Copilot can surface sensitive documents through simple queries, the risk of unintended exposure increases. Employees may discover financial records, personal information, or internal documents they would not normally access. In regulated environments, this increases the likelihood of insider data leakage, accidental disclosure, and compliance violations as AI adoption expands.

Recommended Actions The organization should review permissions across SharePoint, OneDrive, and Microsoft 365 repositories to identify sensitive data accessible to broad user groups. Implementing least-privilege access controls, strengthening data classification, and auditing AI-driven access patterns will reduce exposure. Governance policies for Copilot usage should also be established.

How Lepide Helps Lepide provides visibility into how Microsoft Copilot interacts with organizational data, showing which users accessed sensitive files, what queries were used, and which repositories were involved. Security teams can quickly detect over-permissioned data sources and remediate risky access before sensitive information becomes widely discoverable.

Finding #2 – Medium Risk

Copilot Usage Inefficiencies and Increasing Sensitive Data Alerts



Risk Type: AI Governance / License Optimization / Sensitive Data Exposure

Compliance NIST AI RMF; NIST AC-6; ISO 27001 A.9; CIS Controls 3 & 6; GDPR / HIPAA / PCI DSS data protection requirements.

Observation Lepide identified a growing number of inactive Copilot users, indicating licenses assigned to accounts that are not actively using the service. The dashboard also shows increasing Copilot alerts, suggesting sensitive data is being accessed more frequently through AI queries.

Impact if Unaddressed Unused Copilot licenses create unnecessary cost while rising alert activity indicates sensitive data may be surfaced more frequently through AI interactions. Without monitoring and governance, organizations risk both wasted AI investment and increased data exposure.

Recommended Actions Review Copilot license usage to identify inactive users and reassign or remove unnecessary licenses. Monitor Copilot alerts and review permissions on sensitive data to ensure AI tools cannot surface confidential information to overly broad user groups.

How Lepide Helps Lepide dashboards provide visibility into Copilot usage, inactive licensed users, and alerts triggered by sensitive data access. Security and IT teams can optimize licensing costs while monitoring and controlling AI-driven data exposure.

Finding #3 – High Risk

1,090 inactive enabled accounts significantly increase exposure to credential misuse, privilege escalation, and compliance failure.

Total Records : 1090

SAM Account Name	Object Path	Email Address	Last Logon Time	When Created	Inactivity Time(In days)	Account Age(In days)
VMware_Con...	Never	7/6/2023 12:30:38 PM	N/A	868 Day(s), 21 Hour(s)
4precinct	1/2/2023 2:30:02 PM	4/19/2012 10:51:14 AM	1053 Day(s), 19 Hour(s)	4963 Day(s), 22 Hour(s)
adams	7/17/2025 10:12:20 AM	6/21/2019 12:27:58 PM	126 Day(s), 23 Hour(s)	2344 Day(s), 21 Hour(s)
addison	1/30/2025 10:07:20 AM	8/26/2020 2:17:08 PM	294 Day(s), 23 Hour(s)	1912 Day(s), 19 Hour(s)
adelana	6/9/2025 8:40:53 AM	6/9/2025 7:37:34 AM	165 Day(s), 00 Hour(s)	165 Day(s), 02 Hour(s)
abanks	7/15/2025 8:18:34 AM	7/3/2013 9:09:04 AM	129 Day(s), 01 Hour(s)	4524 Day(s), 00 Hour(s)
abooker	8/1/2025 3:52:42 PM	4/24/2023 10:22:03 AM	111 Day(s), 17 Hour(s)	941 Day(s), 23 Hour(s)
ABS	Never	7/3/2024 10:04:01 AM	N/A	505 Day(s), 23 Hour(s)
acaldwell	2/6/2024 2:48:44 PM	6/20/2023 12:55:18 PM	653 Day(s), 18 Hour(s)	884 Day(s), 20 Hour(s)
acampbell	9/9/2025 5:53:19 PM	8/27/2020 10:09:35 AM	72 Day(s), 15 Hour(s)	1911 Day(s), 23 Hour(s)
achamberlain	8/11/2025 10:37:22 AM	5/19/2024 5:13:28 PM	101 Day(s), 23 Hour(s)	550 Day(s), 16 Hour(s)
aclemmons	10/16/2025 7:55:24 AM	6/24/2019 9:11:28 AM	36 Day(s), 01 Hour(s)	2342 Day(s), 00 Hour(s)
acooper	11/20/2023 1:20:21 AM	8/24/2006 8:21:13 AM	732 Day(s), 08 Hour(s)	7029 Day(s), 01 Hour(s)
across	8/10/2025 2:58:21 PM	1/7/2021 10:39:37 AM	71 Day(s), 18 Hour(s)	1778 Day(s), 22 Hour(s)
adale	2/3/2025 4:44:48 PM	12/12/2019 3:08:01 PM	290 Day(s), 16 Hour(s)	2170 Day(s), 18 Hour(s)
adiah	9/25/2025 5:25:22 PM	8/28/2020 10:08:32 AM	56 Day(s), 16 Hour(s)	1910 Day(s), 23 Hour(s)
adrianh	3/18/2025 7:08:05 PM	8/28/2020 8:42:31 AM	247 Day(s), 14 Hour(s)	1911 Day(s), 00 Hour(s)
adur	8/14/2025 12:16:33 AM	3/14/2018 3:02:42 PM	99 Day(s), 09 Hour(s)	2808 Day(s), 18 Hour(s)
aeverett	10/11/2025 3:37:14 AM	7/10/2017 4:39:32 PM	41 Day(s), 06 Hour(s)	3055 Day(s), 16 Hour(s)
afair	7/9/2025 10:41:52 AM	7/28/2021 11:43:28 AM	134 Day(s), 22 Hour(s)	1576 Day(s), 21 Hour(s)
agay	12/17/2021 2:35:16 PM	12/1/2021 10:35:31 AM	1434 Day(s), 19 Hour(s)	1450 Day(s), 23 Hour(s)
agray	6/5/2025 6:06:01 AM	8/28/2020 7:44:45 AM	169 Day(s), 03 Hour(s)	1911 Day(s), 01 Hour(s)
aharalson	4/12/2025 9:26:12 PM	1/6/2021 9:20:00 AM	222 Day(s), 12 Hour(s)	1780 Day(s), 00 Hour(s)
aharvey	1/31/2025 8:46:16 AM	8/30/2006 10:43:05 AM	294 Day(s), 00 Hour(s)	7022 Day(s), 22 Hour(s)
ahenderson	2/19/2025 5:49:33 PM	8/28/2020 9:14:42 AM	274 Day(s), 15 Hour(s)	1911 Day(s), 00 Hour(s)
ahicks	6/6/2025 9:05:30 AM	2/8/2022 4:58:32 PM	168 Day(s), 00 Hour(s)	1381 Day(s), 16 Hour(s)
ahubbert	8/28/2025 5:10:21 AM	11/26/2019 1:35:03 PM	85 Day(s), 04 Hour(s)	2186 Day(s), 20 Hour(s)
ahutchins	8/8/2025 11:14:36 AM	11/8/2022 1:30:23 PM	104 Day(s), 22 Hour(s)	1108 Day(s), 20 Hour(s)
alacy	10/20/2025 9:07:46 PM	9/23/2025 7:41:25 PM	31 Day(s), 12 Hour(s)	58 Day(s), 13 Hour(s)

Risk Type:	Account Hygiene
Compliance	NISTAC-2; ISO 27001 A.9.2.6; CJIS 5.5; State/Local Government Audit Requirements
Observation	Lepide identified hundreds of enabled accounts with no recent logon activity. Several accounts appear to have never logged in at all since creation. With no automated auditing in place, the city cannot maintain a consistent identity lifecycle process or validate activity across AD and Entra. This results in blind spots that slow investigations and increase operational workload.
Impact if Unaddressed	Dormant accounts remain one of the most common footholds for attackers. In a government environment managing sensitive employee and citizen data, leaving inactive accounts enabled creates multiple risks: increased likelihood of credential theft, undetected privilege escalation, lateral movement opportunities, and failing audit requirements. Additionally, investigations that should take minutes can extend into days due to the absence of centralized visibility.
Recommended Actions	██████████ should review and disable inactive accounts regularly, establish inactivity thresholds, implement automated deactivation workflows, and ensure alignment with HR onboarding/offboarding processes. Consistent lifecycle enforcement reduces risk and supports compliance mandates.
How Lepide Helps	Lepide delivers continuous visibility into account activity, automatically highlights inactive identities, triggers alerts as thresholds are crossed, and supports automated disablement actions. This enables the ██████████ ██████████ to quickly identify and remediate dormant accounts, reduce manual investigation time, and maintain ongoing security and compliance readiness across both AD and Entra environments.

Finding #4 – Medium Risk

2,763 accounts with “Password Never Expires” significantly increase the risk of credential compromise.

Drag a column header here to group by that column.

User Name	User Path	OU Container	Object Path
__VMware_Conv_SA__	\us\ms\y	Users	\us\ms\y
2ndfloorcopier	\us\ms\y	Shared Accounts	\us\ms\y
311temp	\us\ms\y	Constituent Services	\us\ms\y
4precinct	\us\ms\y	Investigative Operation	\us\ms\y
aadams	\us\ms\y	Patrol Operations	\us\ms\y
aadelana	\us\ms\y	Summer Workers	\us\ms\y
aalipoe	\us\ms\y	Server Administration	\us\ms\y
aanderson	\us\ms\y	City Clerk	\us\ms\y
aatkinson	\us\ms\y	Community Affairs	\us\ms\y
aballard	\us\ms\y	Patrol Operations	\us\ms\y
abanks	\us\ms\y	Executive Staff	\us\ms\y
abennett	\us\ms\y	Community Improvement	\us\ms\y
abolden	\us\ms\y	Patrol Operations	\us\ms\y
abooker	\us\ms\y	Recreation Services	\us\ms\y
aboone	\us\ms\y	Action Line	\us\ms\y
ABS	\us\ms\y	Service Accounts	\us\ms\y
abuck	\us\ms\y	Recreation Services	\us\ms\y
abums	\us\ms\y	Auditorium	\us\ms\y
acaldwell	\us\ms\y	Patrol Operations	\us\ms\y
acampbell	\us\ms\y	Users	\us\ms\y

Risk Type:	Account Hygiene
Compliance	NIST IA-5; ISO 27001 A.9.4.3; CJIS 5.6; State/Local Government Audit Requirements
Observation	Lepide identified 2,763 user accounts where the Password Never Expires setting is enabled. Many belong to standard human users across departments such as Police, Parks & Recreation, Human Resources, Server Administration, and Community Affairs. With no centralized auditing solution in place, the city cannot easily assess password age or rotation, creating long-term exposure if any of these credentials are compromised.
Impact if Unaddressed	Never-expiring passwords significantly increase the likelihood of credential theft, brute-force success, and unauthorized access. Combined with other identity hygiene issues, these static credentials expand the city’s attack surface and heighten the risk of undetected lateral movement. This directly affects compliance with NIST, CJIS, and state audit requirements, where lack of password rotation and oversight is a serious deficiency.
Recommended Actions	The City of Jackson should remove Password Never Expires from all non-service accounts, enforce password aging policies aligned with NIST/CJIS requirements, and apply strict controls for any exceptional accounts. Regular password hygiene reviews and automated reporting should be implemented to reduce manual effort and maintain accountability.
How Lepide Helps	Lepide continuously monitors password settings, highlights non-expiring passwords, and alerts when high-risk configurations appear. Automated reporting and ongoing visibility allow the City of Jackson to quickly identify and remediate these accounts, strengthen credential hygiene, and maintain compliance without relying on manual checks.

Finding #6 – High Risk

4,122,724 failed logon attempts in one month obscure real threats and increase the likelihood of undetected attacks.

Who	When	Where	Reason
Administrador	11/21/2025 9:50:24 AM	WIN-OF79NV11JJA	user name does not exist
curvbackup	11/21/2025 9:50:24 AM	GANGA	user name does not exist
fellis	11/21/2025 9:50:24 AM	172.31.229.48	Bad password
fellis	11/21/2025 9:50:24 AM	130.10.10.138	Bad password
administrator	11/21/2025 9:50:23 AM	GANGA	user name is correct but the password i...
ADMINISTRATOR	11/21/2025 9:50:22 AM		user name is correct but the password i...
NOHEMIL	11/21/2025 9:50:22 AM		user name does not exist
Administrador	11/21/2025 9:50:22 AM	WIN-OF79NV11JJA	user name does not exist
ptibackup	11/21/2025 9:50:22 AM	GANGA	user name does not exist
administrator	11/21/2025 9:50:21 AM	GANGA	user name is correct but the passw...
SEAN	11/21/2025 9:50:20 AM		user name does not exist
account-raj.sheetal	11/21/2025 9:50:20 AM	WIN-MULNJJTVHO	user name does not exist
qgsbackup	11/21/2025 9:50:20 AM	GANGA	user name does not exist
Administrador	11/21/2025 9:50:20 AM	WIN-OF79NV11JJA	user name does not exist
administrator	11/21/2025 9:50:19 AM	GANGA	user name is correct but the passw...
acorey	11/21/2025 9:50:19 AM	WIN-55M50ISVAOC	user name does not exist
MPC	11/21/2025 9:50:18 AM		user name does not exist
pyhbackup	11/21/2025 9:50:18 AM	GANGA	user name does not exist
ADMINISTRATOR	11/21/2025 9:50:18 AM		user name is correct but the passw...
MSSQLSERVER	11/21/2025 9:50:17 AM		user name does not exist
NOAHPNLL	11/21/2025 9:50:17 AM		user name does not exist
Administrador	11/21/2025 9:50:16 AM	WIN-OF79NV11JJA	user name does not exist
curvbackup	11/21/2025 9:50:16 AM	GANGA	user name does not exist



Risk Type: Identity & Authentication Security

Compliance: NISTIA-5; ISO 27001A.12.4.1; CJIS 5.5; State/Local Government Audit Requirements

Observation: Lepide recorded 4,122,724 failed logon events within the current month. These attempts come from a wide range of accounts — including Administrator, MSSQLSERVER, backup accounts, service accounts, and misspelled or non-existent usernames. Many failures originate from systems such as GANGA, WIN-OF79NV11JJA, WIN-MULNJJTVHO, and public IPs. Without a centralized auditing solution, the City lacks the ability to distinguish normal account lockouts from automated attacks, brute-force attempts, or misconfigurations.

Impact if Unaddressed: This volume of failures creates overwhelming noise, making it nearly impossible to identify real threats. Potential brute-force attacks, compromised service accounts, password spraying attempts, or lateral movement could occur unnoticed. Excessive authentication failures also introduce operational issues, increase helpdesk workload, and pose compliance risks, as auditors require clear explanations and patterns behind authentication anomalies.

Recommended Actions: The City should monitor failed logons in real time, investigate repeated failures from the same accounts or hosts, and review service accounts for incorrect configurations. Threshold-based alerting and automated correlation should be implemented to highlight suspicious behavior and reduce noise.

How Lepide Helps: Lepide automatically aggregates failed logon activity, highlights abnormal patterns, and provides real-time alerts for high-risk events such as repeated failures, non-existent accounts, or attempts from unexpected hosts. This allows the City to quickly identify attack activity, reduce noise, and support compliance by maintaining clear and searchable authentication audit trails.

Finding #7 – High Risk

69 users with admin privileges increase the risk of unauthorized escalation and excessive access.

User Name	User Path	Object GUID	Display Name	Permission Method
Group Name: CITY.JACKSON.MS.USAdministrators				
cchampion		{1DCE0EB0-90C6-43BC-96B4-A62ADD47EEFA}	Christopher Champion	Direct and Indirect via group(s) [Domain Admins , Local Admin , System Group]
iproctor		{248BF246-83D9-4B07-A1CE-057FDD0E01CFD}	Jetaun Proctor	Indirect via group(s) [CrimeLabUsers]
wharper		{CA953D8E-B285-42D4-9265-9E698812A3F3}	Wille Harper	Direct and Indirect via group(s) [Domain Admins , System Group]
riddell		{128FC3FF-E769-4C92-B201-CBEF397A5D8D}	Rosalind Liddell	Indirect via group(s) [CrimeLabUsers]
lthomas		{54A5071D-56E6-4702-9E6C-E47C68A21685}	LaTanya Thomas-Bennett	Indirect via group(s) [CrimeLabUsers]
aalpoe		{AA73B3C8-BD5B-4A98-8F98-C13E3E1B005E}	Adote Alpoe	Direct and Indirect via group(s) [Domain Admins , Local Admin , System Group]
krobbins		{60C05363-070B-4CDA-B4FC-3B5B1CF425AD}	Katrina Robbins	Indirect via group(s) [CrimeLabUsers]
bmitchell		{70EE533A-D2B5-4383-8149-39535ABA2CF3}	Byart Mitchell	Direct and Indirect via group(s) [Domain Admins , System Group]
emccoy		{250D7124-DEE9-4A02-83EA-C5F9397B61C4}	Evelyn McCoy	Indirect via group(s) [CrimeLabUsers]
lgardner		{42814E1A-87CE-4854-84C2-44DCF4D35305}	Jacquelyn Gardner	Indirect via group(s) [CrimeLabUsers]
rhushellm		{450F3184-69E5-4D95-AFAA-4344C95E740E}	Rhushell Moore	Direct and Indirect via group(s) [Domain Admins , Local Admin]
kstevenson		{81D8BD42-7E02-446F-BEE5-C1959049A09A}	Katherlene Stevenson	Indirect via group(s) [CrimeLabUsers]
jilcaldwell		{949B1747-098E-4A40-836E-4A7F78CDBA6E}	Jillian Caldwell	Direct and Indirect via group(s) [Domain Admins]
O365_Hybrid		{6C3CD508-2BC9-4CC3-A778-6D0D2F82AB68}	O365 Hybrid	Indirect via group(s) [Domain Admins]
hpatton		{55A75954-6214-4144-8514-738676F74432}	Harold Patton	Direct
tbroome		{639C8BF1-15E1-46D4-831B-7AD38D8E26B1}	Taherah Broome	Direct and Indirect via group(s) [Domain Admins]
pbarnes		{6EB89D74-C470-4368-8F10-DD2D1CBA8146}	Patricia Barnes	Indirect via group(s) [CrimeLabUsers]
crimelab		{FD2C564C-E568-4E76-B748-0DBF89330C84}	crimelab	Indirect via group(s) [CrimeLabUsers]
lepide		{33C7811C-0729-40A3-8CD2-CBA801FD85BF}	Lepide	Indirect via group(s) [Domain Admins]
bmallock		{2D86D145-2358-4C37-B6A1-63AE4F709B31}	Bryan C. Mallock	Indirect via group(s) [Domain Admins]
camstrong		{5565A84D-060B-4145-984F-5A2F6C7355AF}	Corey Armstrong	Indirect via group(s) [Domain Admins , Local Admin]
tmonson		{7D5D4581-68F5-433B-A066-0AF9030E71BA}	Thomas Monson	Indirect via group(s) [CrimeLabUsers , Enterprise Admins]
lgoodloe		{74C18142-7569-4237-8224-174F0F0FC26}	Lloyd Goodloe	Direct and Indirect via group(s) [Domain Admins]
pdq		{3EADFCB-D481-4E6C-8926-653DEA850C6B}	PDQ	Indirect via group(s) [Domain Admins]
anichard		{634403A6-D1D6-4041-A583-C5FCE9521F7}	Andrew Richard	Direct and Indirect via group(s) [Domain Admins]
rmatory		{17A4616F-E22C-4019-B3C9-5D36C984D6A7}	Maurice Matory	Indirect via group(s) [Domain Admins]
kerryw		{3CDB6856-29DC-4468-8BDA-96B707FA35F2}	Kerry West	Direct and Indirect via group(s) [Domain Admins]

Risk Type:	Privilege & Access Management
Compliance	NIST AC-2 & AC-6; ISO 27001 A.9.2.3; CJIS 5.3
Observation	Lepide identified 69 users with administrative privileges, many assigned through indirect nested groups such as Domain Admins, Local Admin, Enterprise Admins, and departmental groups like CrimeLabUsers. These include standard staff and service accounts. Without centralized auditing, the City cannot easily confirm why these users hold elevated access or whether privileges remain appropriate.
Impact if Unaddressed	Excessive administrative access increases the likelihood of misuse, escalation, and unauthorized control over critical systems. Indirect group nesting can unintentionally grant broad privileges, undermining least-privilege controls. If any privileged account is compromised, attackers could access sensitive systems and data. Lack of visibility also complicates compliance efforts and delays investigations requiring privilege verification.
Recommended Actions	Review all privileged users, remove unnecessary admin rights, eliminate risky nested groups, implement approval workflows for elevated access, and perform routine recertification to ensure privileges align with job roles and operational requirements.
How Lepide Helps	Lepide provides full visibility into privileged accounts, showing whether rights are assigned directly or inherited through nested groups. Real-time alerts, automated reporting, and detailed privilege mapping help identify unnecessary access, enforce least-privilege, and streamline compliance reviews. This ensures the City maintains accurate oversight of all administrative permissions.

Finding #9 – High Risk

Full Control permissions across departmental shares increase the risk of unauthorized access and accidental data modification.

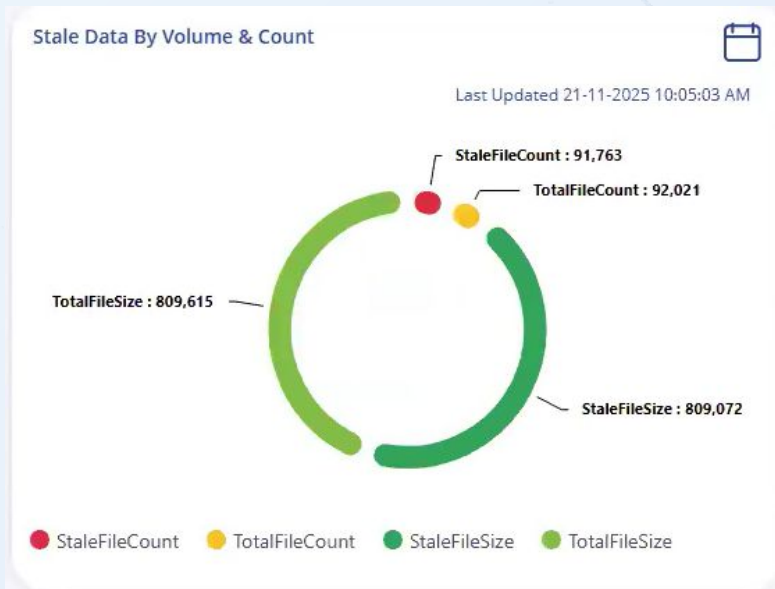
Object Name	Object Type	Owner	Content Type	Compliance	Monetary Value	Risk Level	Last Scan
2025 Fleet Inspections	FOLDER	DEPTSHARES\Adm...	N/A	N/A	N/A	N/A	2025-11-18 10:09:27
426-430 5-14-24	FOLDER	DEPTSHARES\Adm...	N/A	N/A	N/A	N/A	2025-11-18 10:09:27
Accident & Incidents	FOLDER	DEPTSHARES\Adm...	N/A	N/A	N/A	N/A	2025-11-18 10:09:27
ADA Coordinator	FOLDER	DEPTSHARES\Adm...	N/A	N/A	N/A	N/A	2025-11-18 10:09:27
Alexis Jones	FOLDER	Jackson\alexisjones	N/A	N/A	N/A	N/A	2025-11-18 10:09:27
Bus Sign Inventory Photos	FOLDER	DEPTSHARES\Adm...	N/A	N/A	N/A	N/A	2025-11-18 10:09:27
Call Recordings	FOLDER	DEPTSHARES\Adm...	N/A	N/A	N/A	N/A	2025-11-18 10:09:27
Cameras	FOLDER	DEPTSHARES\Adm...	N/A	N/A	N/A	N/A	2025-11-18 10:09:27

Account (Principal)	Effective Permission	Full Control	Read & Execute	Read	Write	Execute	Change	Control
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓
[Redacted]	Full Control	✓	✓	✓	✓	✓	✓	✓

Risk Type:	Permissions Management & Data Access Governance
Compliance	NIST AC-3; ISO 27001 A.9.1.2; CJIS 5.9; State/Local Government Data Access Requirements
Observation	Lepide found numerous users with Full Control permissions across the deptshares\jatron directory, including standard departmental accounts such as alexisjones, cweems, cwelch, ngrissle, ngjuice, and others. These broad permissions allow unrestricted access to create, modify, delete, or move files, significantly exceeding typical least-privilege requirements for operational file shares.
Impact if Unaddressed	Full Control permissions increase the likelihood of accidental deletion, unauthorized data alteration, and hidden data movement. If any account with broad access is compromised, attackers gain the ability to manipulate sensitive transportation documents without detection. Excessive access complicates audits, reduces accountability, and undermines the City's ability to maintain secure and compliant data handling practices.
Recommended Actions	Review all Full Control permissions, restrict access to necessary roles, enforce least-privilege, and implement approval workflows for high-risk permissions. Conduct periodic access reviews to validate ongoing business need.
How Lepide Helps	Lepide provides a clear view of effective permissions across every folder, highlighting excessive rights and showing who has Full Control, how it was granted, and when it changes. Automated alerts, detailed access reports, and visual permission mapping help the City reduce unnecessary access, prevent accidental data misuse, and maintain strong governance across departmental file shares.

Finding #10 – Moderate Risk

Over 91,000 stale files create unnecessary storage use and increase compliance and data lifecycle management risks.



Risk Type:	Data Hygiene & Storage Governance
Compliance	NIST SI-12; ISO 27001 A.8.3; State/Local Government Records Retention Requirements
Observation	Lepide identified 91,763 stale files out of 92,021 total files, representing nearly all stored content. These files account for 809,072 units of stale file size compared to 809,615 total, indicating that most data on departmental shares has not been accessed or modified for extended periods. This suggests outdated, unused, or forgotten content consuming valuable storage.
Impact if Unaddressed	Large volumes of stale files increase storage costs, complicate data searches, and make it harder to locate current, accurate information. Retaining outdated data also creates compliance challenges for regulated record-keeping and may expose sensitive information longer than necessary. Stale content increases risk during incidents, as irrelevant or legacy files complicate investigations and recovery workflows.
Recommended Actions	Review stale data regularly, classify files based on retention requirements, archive or delete unused content, and enforce data lifecycle policies to reduce clutter and maintain accurate, compliant storage environments.
How Lepide Helps	Lepide automatically identifies stale files, visualizes storage usage, and highlights content no longer accessed or required. Administrators can quickly evaluate what should be archived, deleted, or retained. Automated reporting streamlines cleanup efforts, reduces storage overhead, and supports compliance with data retention mandates across departmental file shares.

The cost of inaction.

If the [REDACTED] were to take no action, the operational, financial, and compliance impact of these findings would be significant. The assessment uncovered 1,421 inactive enabled accounts, 91,763 stale files, 4,122,724 failed logons, 69 administrative -privilege users, and unmonitored activity across OU, Group, and file systems. Combined with excessive Full Control permissions, high-volume file activity, and widespread password-never-expire configurations, these weaknesses create multiple attack paths and elevate both insider-risk and external-threat exposure.

Routine investigation tasks — tracking privilege changes, validating file activity, locating the source of failed logons, or determining who copied sensitive documents — currently depend on manual searches, event log review, and scripting. This creates substantial operational drag, consuming valuable time across IT, security, and departmental teams. Without reliable auditing across AD, Entra, and file shares, legal and compliance inquiries risk taking days rather than minutes, increasing the likelihood of missed deadlines,

incomplete evidence, and non-compliance.

Regulatory exposure under ISO 27001, NIST, CJIS, and state retention laws could result in fines or legal consequences. A single incident — such as misuse of a privileged account, unauthorized changes to security groups, or undetected high-volume file copying — could cost \$250,000–\$500,000 in investigation, remediation, and business disruption. According to IBM's Cost of a Data Breach Report 2025, the average breach now exceeds \$4.88 million, rising to \$5.72 million when compromised credentials or sensitive data are involved — both of which are present in [REDACTED] environment today.

Lepide helps prevent these costs through continuous monitoring, automated investigation workflows, and real-time alerting on abnormal identity or file activity. With Lepide, [REDACTED] reduces manual investigation workload, closes dangerous visibility gaps, and significantly lowers the risk that a privileged or externally shared account could be exploited without detection.

Next steps – reducing your risk for good.

The assessment shows that while the [REDACTED] has strong foundational controls, the absence of reliable auditing, continuous monitoring, and automated privilege governance leaves significant blind spots across Active Directory, Entra, and departmental file shares. Manual reviews and reactive checks cannot keep pace with the scale of changes and activity observed — including 1,421 inactive users, 4.1M failed logons, 69 admin-privileged accounts, 91,763 stale files, and widespread Full Control permissions across critical folders. With no consistent audit trail in place, [REDACTED] remains exposed to credential misuse, insider-risk, and compliance challenges. By enabling Lepide's continuous monitoring, threat models, and automated workflows, the [REDACTED] can shift from reactive investigations to proactive protection — reducing the likelihood of a breach, strengthening compliance posture, and reclaiming valuable operational time across IT and security teams.



Become a Lepide Customer Partner: Move beyond assessment mode with full deployment, dedicated success support, and tailored reporting to continually demonstrate risk reduction and ROI across your organization.



Activate Lepide's Threat Models and Automated Workflows: Use pre-built intelligence to spot risky behaviors — from privilege escalation to insider threats — and trigger automated responses that prevent escalation.



Implement Continuous Monitoring with Lepide: Gain real-time visibility into permission changes, failed logons, and data movement across AD and Microsoft 365 to detect threats as they happen.