LUNARCHAIN
SECURITY

INTERNAL NETWORK

Penetration Test Report

Complete illustrative redacted sample

CUSTOMER-SAFE SAMPLE

Lunarchain Security LTD

01 / DOCUMENT CONTROL

REDACTED REPORT PACK

CUSTOMER-SAFE SAMPLE

This is a complete illustrative report. Customer names, domains, IP addresses, people, credentials, screenshots, payloads and command output have been removed or generalised.

REPORT TYPE	Internal Network and Active Directory Assessment
REPORT REFERENCE	PT-2026-REDACTED-INT-COMPLETE
REPORT DATE	17 July 2026
VERSION	2.0 - illustrative diagrams
CLASSIFICATION	Customer-safe redacted sample
PREPARED BY	LunarChain Security
CUSTOMER	[REDACTED CUSTOMER]
DISTRIBUTION	Approved for prospective customer review

CONTENTS

- Executive summary and critical attack path.
- Scope, methodology and assumptions.
- Findings summary and detailed technical write-ups.
- Complete write-ups for 8 findings: INT-01, INT-02, INT-03, INT-04, INT-05, INT-06, INT-07, INT-08.
- Internal compromise narrative and customer-safe evidence timeline.
- Risk grading, tools used, retest guidance and redaction appendix.

REDACTION APPROACH

The report preserves the level of analysis and remediation guidance expected in a live engagement while removing information that could identify a customer or provide reusable exploitation artefacts.

Evidence entries use redacted IDs so a reader can see how evidence would be referenced. A live report would include screenshots, request captures, timestamps, affected assets and consultant notes.

02 / EXECUTIVE SUMMARY

OVERALL ASSESSMENT

CRITICAL RISK

The sample internal environment contained multiple independent paths from a standard internal position to domain-level compromise.

LunarChain Security performed an assumed-breach internal network and Active Directory assessment from a redacted internal network position. Testing measured how far an attacker could progress from initial internal access.

The most severe issues were identity and privilege weaknesses: vulnerable ADCS configuration, kerberoastable privileged service accounts, overly permissive shares and lateral movement controls.

The findings show how common enterprise misconfigurations combine into a full compromise path without requiring a novel software vulnerability.

CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
3	3	2	0	0	8

IMMEDIATE PRIORITIES

- Remediate ADCS template exposure and revoke any certificates issued through vulnerable templates.
- Rotate and reduce service account privileges, moving services to gMSA where possible.
- Restrict sensitive shares and encrypt backup data.
- Disable legacy relay paths and deploy unique local administrator passwords.
- Build detections for the specific identity attack paths described in the report.

03 / SCOPE

SCOPE AND METHODOLOGY

ENGAGEMENT TYPE	Assumed-breach internal network and Active Directory assessment
TARGETS	[REDACTED] corporate networks, Windows estate, Active Directory and supporting services
STARTING POSITION	Internal network access with no privileged credentials
TESTING WINDOW	Sample period, five business days
OUT OF SCOPE	Denial of service, OT modification, destructive action and production data alteration

METHODOLOGY

- Performed passive discovery, host enumeration and service validation.
- Assessed Active Directory relationships, privilege paths, certificate services, delegation and service accounts.
- Tested relay exposure, local administrator controls and credential handling using controlled methods.
- Reviewed sensitive shares and backup locations for excessive access.
- Mapped findings to realistic attack paths and produced retest guidance for each control.

ASSESSMENT CONSTRAINTS

Testing avoided destructive actions and limited data access to redacted proof points. Credential material and screenshots are not included in this customer-safe sample.

04 / ASSESSMENT RESULTS

FINDINGS SUMMARY

REF	FINDING	RISK	STATUS	CATEGORY
INT-01	Active Directory Certificate Services template permits user impersonation	CRITICAL	Open	T1649
INT-02	Kerberoastable privileged service account uses weak password material	CRITICAL	Open	T1558.003
INT-03	Overly permissive file shares expose sensitive data and credentials	CRITICAL	Open	T1135 / T1552
INT-04	Legacy name resolution and SMB signing gaps enable NTLM relay	HIGH	Open	T1557.001
INT-05	Local administrator password reuse enables broad lateral movement	HIGH	Open	T1078
INT-06	Delegation and tiering weaknesses expose privileged authentication material	HIGH	Open	T1550 / T1187
INT-07	Password policy and credential handling weaknesses increase account compromise risk	MEDIUM	Open	T1110 / T1552
INT-08	Logging and monitoring gaps delay detection of compromise activity	MEDIUM	Open	TA0007 / TA0010

DISTRIBUTION BY THEME

THEME	FINDINGS
Identity and privilege escalation	4
Data exposure and file share controls	1
Lateral movement controls	2
Logging and monitoring	1

04 / ASSESSMENT RESULTS / TECHNICAL FINDING

4.1 ACTIVE DIRECTORY CERTIFICATE SERVICES TEMPLATE PERMITS USER IMPERSONATION

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
CRITICAL	INT-01	9.8	Open	Low

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CATEGORY	MITRE T1649 - Steal or Forge Authentication Certificates

IMPACTED SYSTEMS

SYSTEM	NOTES
[REDACTED]-CA01	Enterprise CA publishing vulnerable client authentication template.
[REDACTED]User	Template allowed low-privileged enrolment and requester-supplied identity attributes.

DESCRIPTION

A certificate template was configured in a way that allowed low-privileged domain users to request authentication certificates for other principals.

This class of issue can provide a direct path to privileged Kerberos authentication without knowing the target user's password.

DETAIL

LunarChain Security reviewed the certificate authority and template configuration from a standard domain account. The affected template allowed enrolment by a broad group and permitted requester-controlled identity information.

A controlled proof of impact was performed against a redacted test principal only. The certificate was revoked and no persistence was left in place.

EVIDENCE SUMMARY

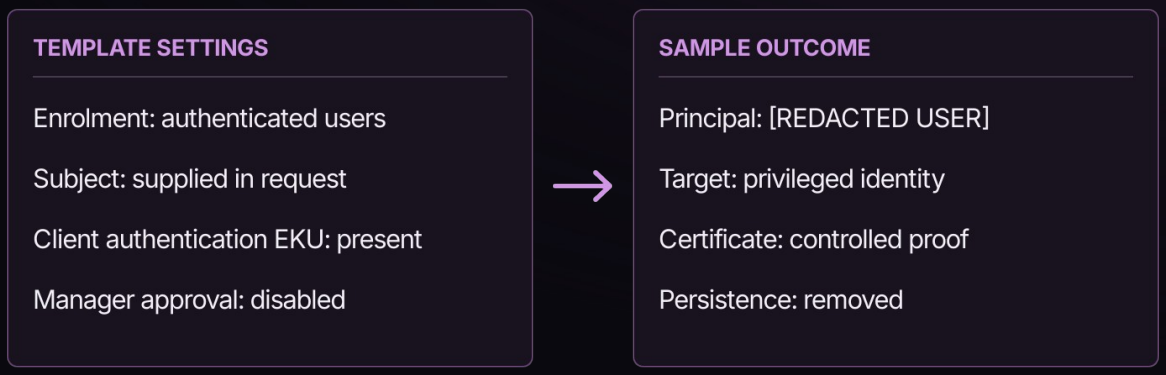
EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
INT-01-E01	Template permissions showed broad enrolment rights. Template name redacted.
INT-01-E02	Template settings permitted requester-controlled subject information.
INT-01-E03	Controlled authentication proof completed against redacted test principal.

ILLUSTRATIVE DIAGRAM

ILLUSTRATIVE DIAGRAM / INT-01 CRITICAL

Certificate template permits impersonation

The combined ADCS settings enable a privileged identity request



Illustrative sample diagram. No live customer systems, credentials or captured evidence.
Synthetic observations summarise the accompanying finding; this is not a screenshot.

Figure INT-01-1: Illustrative diagram of the certificate-template controls enabling impersonation.

RISK

Any attacker who obtains a standard domain account could potentially authenticate as a privileged user, bypassing password rotation and many conventional login controls.

Certificate-based compromise can be difficult to detect and may persist beyond password resets if certificates are not revoked and template controls are not corrected.

RECOMMENDATION

- Remove requester-supplied subject controls from templates that allow client authentication.
- Restrict enrolment permissions to the minimum required groups and remove broad domain user access.
- Require manager approval for sensitive templates or remove templates that are no longer required.
- Audit all ADCS templates for known escalation patterns and monitor certificate issuance events.
- Revoke certificates issued through vulnerable templates after remediation.

RETEST GUIDANCE

- Attempt enrolment as a standard test user and confirm impersonation is no longer possible.
- Review CA logs for suspicious certificate requests before the fix date.
- Confirm certificate issuance events are forwarded to the monitoring platform.

ADDITIONAL INFORMATION

- SpecterOps Certified Pre-Owned ADCS research.
- MITRE ATT&CK T1649 - Steal or Forge Authentication Certificates.

04 / ASSESSMENT RESULTS / TECHNICAL FINDING

4.2 KERBEROASTABLE PRIVILEGED SERVICE ACCOUNT USES WEAK PASSWORD MATERIAL

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
CRITICAL	INT-02	9.0	Open	Low

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L
CATEGORY	MITRE T1558.003 - Kerberoasting

IMPACTED SYSTEMS

ACCOUNT	NOTES
[REDACTED]\svc_app_admin	Service Principal Name present; account held excessive privilege.
[REDACTED] servers	Account granted local administrator rights beyond documented requirement.

DESCRIPTION

A service account with an associated Service Principal Name was over-privileged and used weak password material. Kerberos service tickets for this account could be requested by any authenticated domain user and attacked offline.

LunarChain Security confirmed recoverability of the password in a controlled manner and did not disclose the plaintext credential in this sample.

DETAIL

The account was identified during domain enumeration as both kerberoastable and privileged. The recovered credential provided local administrative access on multiple systems.

This issue is common where long-lived service accounts are manually managed, excluded from normal password rotation and granted broad access for convenience.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
INT-02-E01	Domain enumeration identified redacted SPN-bearing service account.
INT-02-E02	Offline password recovery succeeded within the engagement window.
INT-02-E03	Group membership and local access review showed excessive privilege.

RISK

A low-privileged attacker can request service tickets without interacting with the target host, making the attack low-noise and practical.

Compromise of a privileged service account can enable lateral movement, credential dumping, data access and persistence.

RECOMMENDATION

- Rotate the affected account password immediately using a long, unique 25+ character value.
- Move eligible services to group Managed Service Accounts.
- Remove interactive login rights and unnecessary local administrator privileges from service accounts.
- Disable RC4 where feasible and require modern Kerberos encryption types.
- Monitor for abnormal service ticket requests and high-volume Kerberos activity.

RETEST GUIDANCE

- Repeat Kerberoast assessment and confirm no privileged accounts are recoverable.
- Confirm service account privileges map to documented service requirements.
- Verify monitoring alerts on abnormal service ticket activity.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1558.003 - Kerberoasting.
- Microsoft guidance for group Managed Service Accounts.

04 / ASSESSMENT RESULTS / TECHNICAL FINDING

4.3 OVERLY PERMISSIVE FILE SHARES EXPOSE SENSITIVE DATA AND CREDENTIALS

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
CRITICAL	INT-03	9.4	Open	Low

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
CATEGORY	MITRE T1135 / T1552 - Network Share Discovery and Unsecured Credentials

IMPACTED SYSTEMS

SHARE	NOTES
\\[REDACTED]\UserBackups$	Contained mailbox and profile backups readable by broad user groups.
\\[REDACTED]\SqlBackups$	Contained database backups with sensitive records.
\\[REDACTED]\IT$	Contained operational notes and reset material.

DESCRIPTION

Several network shares were readable by low-privileged users and contained sensitive operational, mailbox or database backup data.

The data available through these shares materially accelerated the compromise path and would support both data theft and privilege escalation.

DETAIL

LunarChain Security enumerated shares using a standard domain account. The account could list and read data beyond its expected business need.

Redacted samples of mailbox exports, database backups and operational documents were reviewed to confirm sensitivity. Bulk extraction was limited and controlled under the rules of engagement.

EVIDENCE SUMMARY

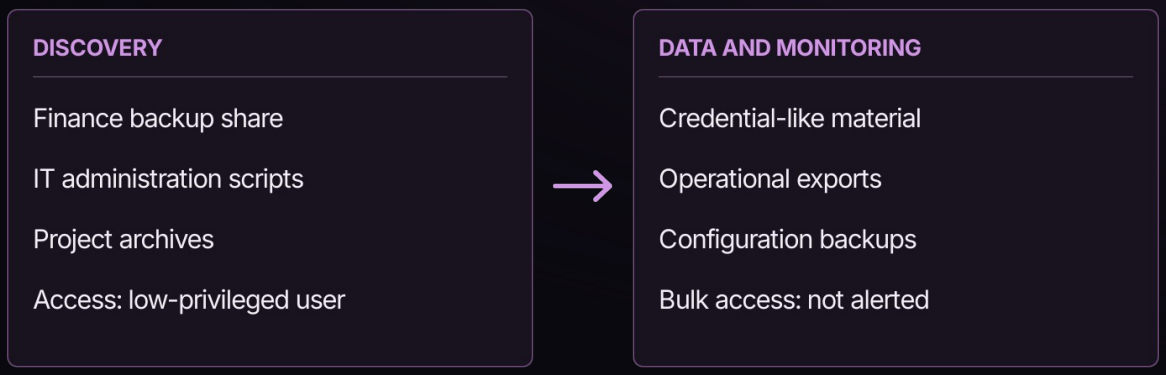
EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
INT-03-E01	Broad group permissions allowed a low-privileged user to read backup directories.
INT-03-E02	Redacted mailbox backup contained support conversations and reset material.
INT-03-E03	Database backup names and metadata indicated sensitive customer records.

ILLUSTRATIVE DIAGRAM

ILLUSTRATIVE DIAGRAM / INT-03 CRITICAL

Low privilege share access exposes sensitive data

Sample share categories illustrate the effect of permissive access



Illustrative sample diagram. No live customer systems, credentials or captured evidence.
Synthetic observations summarise the accompanying finding; this is not a screenshot.

Figure INT-03-1: Illustrative diagram of sensitive file-share categories accessible to a low-privileged user.

RISK

A single compromised account could access large volumes of sensitive data without exploiting a software vulnerability.

Backups often contain credentials, historic data and records excluded from normal application access controls, making them high-value targets.

RECOMMENDATION

- Review all shares for broad groups such as Domain Users, Authenticated Users and Everyone.
- Restrict backups to service accounts and administrators with a documented need.
- Encrypt sensitive backups and separate backup read rights from restore administration rights.
- Move mailbox and profile backups into access-controlled storage with per-user permissions.
- Monitor access to backup locations and alert on bulk read behaviour.

RETEST GUIDANCE

- Use a standard test account to enumerate shares and confirm sensitive locations are not readable.
- Confirm backup data is encrypted and access is audited.
- Review monitoring alerts by performing a controlled bulk-read simulation.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1078 - Valid Accounts.
- MITRE ATT&CK T1552 - Unsecured Credentials.
- MITRE ATT&CK TA0010 - Exfiltration.

04 / ASSESSMENT RESULTS / TECHNICAL FINDING

4.4 LEGACY NAME RESOLUTION AND SMB SIGNING GAPS ENABLE NTLM RELAY

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
HIGH	INT-04	8.8	Open	Low

CVSS VECTOR	AV:A/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L
CATEGORY	MITRE T1557.001 - LLMNR/NBT-NS Poisoning and SMB Relay

IMPACTED SYSTEMS

CONTROL	NOTES
LLMNR / NBT-NS	Legacy name resolution remained enabled on client networks.
SMB services	Signing not enforced consistently across servers.
LDAP services	Channel binding and signing require review.

DESCRIPTION

Legacy broadcast name-resolution protocols remained enabled, and several services did not enforce signing. This allowed captured authentication attempts to be relayed rather than only collected.

The test was conducted carefully to avoid disruption and used controlled relay targets.

DETAIL

When hosts attempted to resolve mistyped or unavailable names, their authentication attempts could be coerced to a tester-controlled listener. Because signing was not enforced on selected services, authentication could be relayed to gain access as the victim user.

This provides a route from physical or network-adjacent access to an authenticated foothold without knowing a password.

EVIDENCE SUMMARY

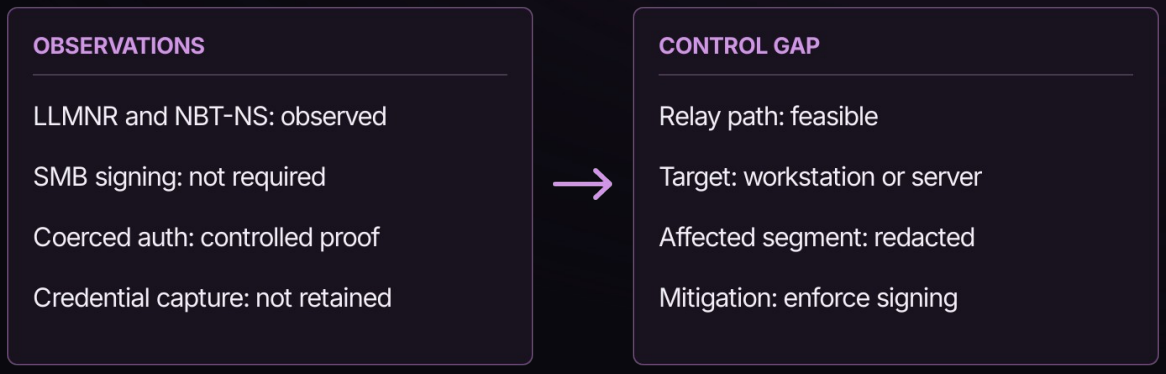
EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
INT-04-E01	Client network generated LLMNR/NBT-NS traffic during passive observation.
INT-04-E02	Selected SMB services accepted unsigned sessions.
INT-04-E03	Controlled relay attempt produced authenticated access to a redacted target.

ILLUSTRATIVE DIAGRAM

ILLUSTRATIVE DIAGRAM / INT-04 HIGH

Name resolution and signing gaps allow relay

Legacy protocols and missing SMB signing form a relay path



Illustrative sample diagram. No live customer systems, credentials or captured evidence.
Synthetic observations summarise the accompanying finding; this is not a screenshot.

Figure INT-04-1: Illustrative diagram of legacy name-resolution and SMB signing conditions enabling relay.

RISK

An attacker on the internal network or a compromised host can use this weakness to obtain access as legitimate users and move laterally.

Relay attacks are especially dangerous where users hold local administrator rights or where LDAP protections are not enforced.

RECOMMENDATION

- Disable LLMNR and NBT-NS through Group Policy.
- Enforce SMB signing across servers and workstations where supported.
- Enable LDAP signing and channel binding, testing compatibility first.
- Reduce local administrator rights and remove broad administrative access from standard users.
- Monitor for name-resolution poisoning, relay indicators and unusual authentication patterns.

RETEST GUIDANCE

- Repeat passive observation and confirm LLMNR/NBT-NS traffic is absent.
- Validate SMB signing enforcement across representative server groups.
- Attempt controlled relay tests and confirm they fail.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1557.001 - LLMNR/NBT-NS Poisoning and SMB Relay.
- Microsoft guidance for SMB signing and LDAP channel binding.

04 / ASSESSMENT RESULTS / TECHNICAL FINDING

4.5 LOCAL ADMINISTRATOR PASSWORD REUSE ENABLES BROAD LATERAL MOVEMENT

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
HIGH	INT-05	8.4	Open	Low

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L
CATEGORY	MITRE T1078 - Valid Accounts

IMPACTED SYSTEMS

ASSET GROUP	NOTES
Workstations	Local administrator password not uniquely managed.
Member servers	Recovered local credential worked on multiple hosts.

DESCRIPTION

Local administrator credentials were reused across multiple systems or were not managed by a solution that guarantees uniqueness and rotation.

A credential recovered from one host could therefore be reused to access additional hosts.

DETAIL

LunarChain Security obtained local credential material from a redacted host where administrative access was already authorised for testing. The credential was then tested against a limited set of agreed hosts and succeeded more broadly than expected.

This weakness is a common reason small compromises turn into rapid estate-wide lateral movement.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
INT-05-E01	Recovered local administrator credential succeeded on multiple redacted hosts.
INT-05-E02	No evidence of centralised unique local password management on sampled systems.

RISK

An attacker who compromises one endpoint can reuse the credential across many systems, expanding access and increasing opportunities to recover domain credentials.

Password reuse also makes containment harder because responders must assume many hosts are compromised.

RECOMMENDATION

- Deploy Windows LAPS or Microsoft Entra LAPS across all supported Windows systems.
- Ensure local administrator passwords are unique, random and automatically rotated.
- Disable or remove unnecessary local administrator accounts.
- Restrict remote local administrator logins where not required.
- Monitor authentication using local administrator accounts across the estate.

RETEST GUIDANCE

- Confirm sampled hosts have unique LAPS-managed local administrator passwords.
- Attempt credential reuse with an approved test account and confirm it fails.
- Confirm password retrieval is limited to authorised administrators and audited.

ADDITIONAL INFORMATION

- Microsoft Windows LAPS documentation.
- MITRE ATT&CK T1078 - Valid Accounts.

04 / ASSESSMENT RESULTS / TECHNICAL FINDING

4.6 DELEGATION AND TIERING WEAKNESSES EXPOSE PRIVILEGED AUTHENTICATION MATERIAL

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
HIGH	INT-06	8.1	Open	Medium

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N
CATEGORY	MITRE T1550 / T1187 - Use Alternate Authentication Material and Forced Authentication

IMPACTED SYSTEMS

AREA	NOTES
Delegation configuration	Selected systems trusted for delegation beyond documented need.
Administrative tiering	Privileged accounts had exposure to lower-trust systems.

DESCRIPTION

Delegation settings and administrative tiering allowed privileged authentication material to be exposed to systems outside the intended trust boundary.

The issue creates a path for attackers to capture or reuse privileged Kerberos material after compromising an intermediate host.

DETAIL

LunarChain Security identified systems configured with delegation settings that were not aligned to documented business requirements. In addition, privileged users had interactive exposure to lower-tier hosts.

A controlled proof demonstrated that a compromised intermediate system could become a stepping stone toward higher privilege.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
INT-06-E01	Delegation settings showed redacted server trusted beyond documented requirement.
INT-06-E02	Privileged logon exposure observed on lower-trust system.
INT-06-E03	Controlled path analysis showed route to privileged material.

RISK

Delegation and tiering weaknesses can allow compromise of a server or workstation to become compromise of an administrator or domain service.

This undermines the separation expected between standard user, server administration and domain administration tiers.

RECOMMENDATION

- Remove unconstrained delegation and replace it with constrained or resource-based delegation only where required.
- Implement administrative tiering so domain administrators never authenticate to lower-trust systems.
- Use Privileged Access Workstations for high-privilege administration.
- Place privileged users in Protected Users where compatible.
- Monitor for sensitive privilege use on non-admin systems.

RETEST GUIDANCE

- Review delegation settings and confirm only documented, constrained use remains.
- Confirm privileged users do not have interactive logon events on lower-tier hosts.
- Run path analysis and confirm no practical route from low-tier systems to domain administration remains.

ADDITIONAL INFORMATION

- Microsoft enterprise access model guidance.
- MITRE ATT&CK T1550 - Use Alternate Authentication Material.

04 / ASSESSMENT RESULTS / TECHNICAL FINDING

4.7 PASSWORD POLICY AND CREDENTIAL HANDLING WEAKNESSES INCREASE ACCOUNT COMPROMISE RISK

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
MEDIUM	INT-07	6.8	Open	Low

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
CATEGORY	MITRE T1110 - Brute Force and T1552 - Unsecured Credentials

IMPACTED SYSTEMS

CONTROL	NOTES
Domain password policy	Minimum length and lockout controls require strengthening.
Support process	Temporary credentials observed in redacted support artefacts.
Privileged users	Enhanced password and protection requirements not consistently applied.

DESCRIPTION

Password and credential handling controls were not consistently strong enough for the environment. LunarChain Security observed weak password policy settings and support processes that increased credential exposure.

The finding is rated medium as a standalone control issue, but it becomes high impact when chained with exposed shares or service account weaknesses.

DETAIL

Configuration review showed that standard account password requirements did not align with current best practice. Redacted support artefacts also showed temporary credential handling that could expose accounts if mailbox or file share access is compromised.

Privileged accounts did not consistently enforce a materially stronger standard than normal user accounts.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
INT-07-E01	Domain policy review showed redacted weak password settings.
INT-07-E02	Support artefact contained redacted temporary credential material.
INT-07-E03	Privileged group review showed inconsistent enhanced controls.

RISK

Weak or exposed credentials remain one of the fastest ways for attackers to move from initial access to broad compromise.

Temporary credentials sent through normal communication channels are frequently captured from mailboxes, backups and ticket systems.

RECOMMENDATION

- Set a minimum standard user password length of at least 14 characters and block common, breached and organisation-specific passwords.
- Require 25+ character unique passwords or gMSA for service and privileged accounts.
- Stop sending temporary passwords in cleartext through email or chat.
- Force password change on first use for any reset flow and expire temporary credentials quickly.
- Apply phishing-resistant MFA and Protected Users membership for privileged accounts where compatible.

RETEST GUIDANCE

- Review effective domain password policy and password filter controls.
- Sample support reset workflows and confirm temporary credentials are not exposed in cleartext.
- Confirm privileged accounts meet the enhanced standard.

ADDITIONAL INFORMATION

- NCSC password administration guidance.
- MITRE ATT&CK T1110 - Brute Force.

04 / ASSESSMENT RESULTS / TECHNICAL FINDING

4.8 LOGGING AND MONITORING GAPS DELAY DETECTION OF COMPROMISE ACTIVITY

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
MEDIUM	INT-08	6.5	Open	Medium

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
CATEGORY	MITRE TA0007 / TA0010 - Discovery and Exfiltration

IMPACTED SYSTEMS

AREA	NOTES
Domain controllers	High-risk identity events not consistently alerting.
File servers	Bulk read and backup access telemetry incomplete.
SQL servers	Privileged database actions not centrally monitored.

DESCRIPTION

Several high-risk actions performed during the assessment did not generate timely security alerts or were not visible in the central monitoring process.

Detection does not prevent every compromise, but it should reduce dwell time and provide responders with an opportunity to contain the attack before material impact.

DETAIL

LunarChain Security performed controlled discovery, share access, privileged authentication and database enumeration. In the evidence made available during the engagement, these actions were not consistently triaged or correlated.

The highest-value gaps were identity events, bulk access to sensitive shares and privileged database configuration changes.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
INT-08-E01	Controlled sensitive share access did not produce a timely alert.
INT-08-E02	Privileged database action was not correlated with user context.
INT-08-E03	Identity event coverage did not support full attack-path reconstruction.

RISK

Without timely detection, attackers can perform discovery, collect data and escalate privileges long before responders have a clear picture.

Monitoring gaps also make post-incident investigation slower and less reliable.

RECOMMENDATION

- Forward domain controller, file server, endpoint and SQL audit logs to a central monitoring platform.
- Create detections for DCSync, certificate abuse, Kerberoasting spikes, sensitive share access and privileged group changes.
- Alert on abnormal bulk reads from backup shares and unusual database administrative actions.
- Define triage SLAs and ensure critical alerts are investigated by trained responders.
- Run regular purple team validation to prove the detections work end to end.

RETEST GUIDANCE

- Replay agreed benign indicators for each critical attack path and confirm alerts fire.
- Review SIEM cases to confirm alerts are triaged within agreed SLA.
- Confirm logs contain enough context to reconstruct user, host, process and target.

ADDITIONAL INFORMATION

- MITRE ATT&CK data source guidance.
- Microsoft Sentinel and Windows event auditing best practice.

05 / NARRATIVE

FOOTHOLD TO DOMAIN COMPROMISE

The following redacted narrative shows how a realistic attacker could chain common internal weaknesses into domain compromise. Exact credentials, hosts and commands are removed.

PHASE	ACTIVITY	CUSTOMER-SAFE EVIDENCE
Network position	Testing began from a standard internal network position with no privileged account.	INT-NAR-E01
Initial credential	Legacy name resolution and relay exposure produced an authenticated foothold in a controlled test.	INT-04-E03
Data discovery	Broadly readable shares exposed operational data and credential material.	INT-03-E02
Privilege path	Service account and certificate-service weaknesses provided independent escalation routes.	INT-01-E03 / INT-02-E02
Domain impact	Path analysis showed that domain-level compromise was achievable from the tested position.	INT-NAR-E05

EVIDENCE NOTE

In the live report each phase would link to timestamps, screenshots and log references. This sample keeps only the narrative structure and redaction markers.

06 / APPENDICES

RISK GRADING AND RETEST

Findings are prioritised using impact, difficulty, exposure, business context and the likelihood that a realistic attacker would discover and exploit the issue.

RISK	DESCRIPTION
CRITICAL	Likely to enable domain compromise, major data exposure, fraudulent action, full tenant compromise or material business disruption.
HIGH	Likely to enable unauthorised access, privilege escalation, significant data exposure or a material step in a compromise chain.
MEDIUM	Requires chaining, a specific precondition or has limited direct impact, but still weakens the environment materially.
LOW	Hardening or defence-in-depth issue with limited standalone exploitability.
INFO	Informational observation, contextual note or best-practice improvement with no direct standalone security impact.

STATUS DEFINITIONS

STATUS	DEFINITION
Open	The issue has not been remediated or has not yet been retested.
Partially remediated	Some affected assets or paths are fixed, but at least one remains exposed.
Closed	The issue was remediated across the agreed scope and retest evidence supports closure.
Risk accepted	The customer has formally accepted the residual risk.

TOOLS USED

TOOL	PURPOSE
Nmap	Host and service discovery within agreed ranges.
BloodHound / SharpHound	Active Directory path analysis.
Certipy / PSPKIAudit	Certificate services configuration review.
Responder-style validation	Controlled name-resolution and relay exposure testing.
Windows event logs	Identity, file share and privilege activity review.

REDACTION INVENTORY

CATEGORY	TREATMENT
Customer identifiers	Replaced with [REDACTED CUSTOMER] and generic organisation labels.
Assets	Hostnames, IP addresses, URLs, domains and cloud resources removed or generalised.
Identity data	Usernames, emails, account IDs, tokens, cookies, hashes and credentials removed.
Evidence	Screenshots, request bodies, response bodies, payloads and exact commands removed.
Operational detail	Operator infrastructure, exact source IPs and deconfliction notes reduced.

CUSTOMER HANDOUT STATEMENT

This complete sample demonstrates report depth, structure and tone. It should not be treated as evidence of testing for any named organisation.