LunarChain

SECURITY

RED TEAM

Red Team Report

Complete illustrative redacted sample

CUSTOMER-SAFE SAMPLE

Lunarchain Security LTD
Registered in England and Wales · Company no. 17419798

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	Objective-Based Red Team Operation
REPORT REFERENCE	RT-2026-REDACTED-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 objective outcomes.
- Rules of engagement, scope and methodology.
- Findings summary and detailed technical write-ups.
- Complete write-ups for 9 findings: RT-01, RT-02, RT-03, RT-04, RT-05, RT-06, RT-07, RT-08, RT-09.
- Redacted attack timeline and detection matrix.
- Risk grading, tools used, purple-team 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.

OVERALL ASSESSMENT

CRITICAL BUSINESS RISK

The sample operation achieved its objectives because identity, segmentation and response controls did not contain a realistic attacker path.

LunarChain Security performed a redacted objective-based adversary simulation to test prevention, detection and response across people, process and technology.

The sample operation achieved the agreed objectives in a controlled manner. The decisive weaknesses were not a single exploit, but gaps in phishing-resistant authentication, identity blast radius, environment segmentation and alert response.

This report is structured like a complete red team deliverable: objectives, rules of engagement, narrative timeline, control-performance assessment, root-cause findings and remediation plan.

CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
4	4	1	0	0	9

IMMEDIATE PRIORITIES

- Operationalise detection: critical identity, data and endpoint alerts need ownership, triage SLA and containment playbooks.
- Deploy phishing-resistant MFA for privileged, finance and sensitive application users.
- Separate corporate and sensitive environments through identity tiering, hardened administration paths and network controls.
- Reduce service account privilege and remove shared secrets from user-accessible storage.
- Run a purple team replay using the report timeline to verify improvements.

SCOPE AND METHODOLOGY

ENGAGEMENT TYPE	Objective-based red team operation
OBJECTIVES	Gain corporate access, reach sensitive data and simulate business impact under controlled conditions
CONTROL GROUP	Small redacted control group, SOC and wider IT not informed during the live phase
TESTING WINDOW	Sample period, three weeks
HARD EXCLUSIONS	No destructive action, no production payment execution, no real customer data access outside agreed proof points

METHODOLOGY

- Developed a realistic threat scenario, rules of engagement and deconfliction process.
- Performed open-source reconnaissance, social engineering, initial access attempts and controlled post-exploitation.
- Mapped actions to MITRE ATT&CK and recorded timestamps for defender replay.
- Evaluated whether controls prevented, detected or responded to each material action.
- Converted attack-path observations into root-cause findings and prioritised remediation.

ASSESSMENT CONSTRAINTS

All activity was authorised, controlled and deconflicted. This sample removes exact target names, operator infrastructure, payloads, screenshots and customer-specific timeline entries.

FINDINGS SUMMARY

REF	FINDING	RISK	STATUS	CATEGORY
RT-01	Sensitive data exposed through over-permissive shares and unmanaged secrets	CRITICAL	Open	T1552 / TA0010
RT-02	Over-privileged service accounts expand identity blast radius	CRITICAL	Open	T1078 / T1558
RT-03	Sensitive environment reachable from corporate trust tier	CRITICAL	Open	T1021
RT-04	Alerts were generated but not triaged within useful windows	CRITICAL	Open	SOC process
RT-05	Phishing-resistant MFA not enforced for high-risk users	HIGH	Open	T1566 / T1621
RT-06	Initial access and social engineering controls can be bypassed with credible pretexts	HIGH	Open	T1566
RT-07	Command and control egress and persistence were not reliably detected	HIGH	Open	T1071 / TA0003
RT-08	Segregation of duties weakness allows simulated business-process abuse	HIGH	Open	Process
RT-09	Incident response playbooks do not cover identity-led intrusion end to end	MEDIUM	Open	IR process

DISTRIBUTION BY THEME

THEME	FINDINGS
Initial access and social engineering	2
Identity and privilege	2
Segmentation and business impact	2
Detection, response and resilience	3

4.1 SENSITIVE DATA EXPOSED THROUGH OVER-PERMISSIVE SHARES AND UNMANAGED SECRETS

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
CRITICAL	RT-01	9.4	Open	Low

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
CATEGORY	MITRE T1552 / TA0010 - Unsecured Credentials and Exfiltration

IMPACTED SYSTEMS

ASSET	NOTES
File shares	Sensitive operational and user data readable by broad groups.
Shared documents	Credentials and reset material present in redacted files.
Backup locations	Bulk data available without proportional monitoring.

DESCRIPTION

The red team identified sensitive data and credential material in locations accessible to users beyond the documented business requirement.

This finding materially contributed to the achievement of red team objectives by accelerating discovery, credential access and business impact demonstration.

DETAIL

After gaining an initial foothold, LunarChain Security enumerated accessible shares and collaboration locations. Several contained information that should be restricted, including operational notes, exported data and redacted credential material.

The volume and sensitivity of accessible data meant the attack path did not require exploitation of a complex vulnerability to achieve meaningful business impact.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-01-E01	Low-privileged account accessed redacted sensitive share.
RT-01-E02	Document search located credential-like material in user-accessible location.
RT-01-E03	Bulk access did not trigger timely response during the simulation.

ILLUSTRATIVE DIAGRAM

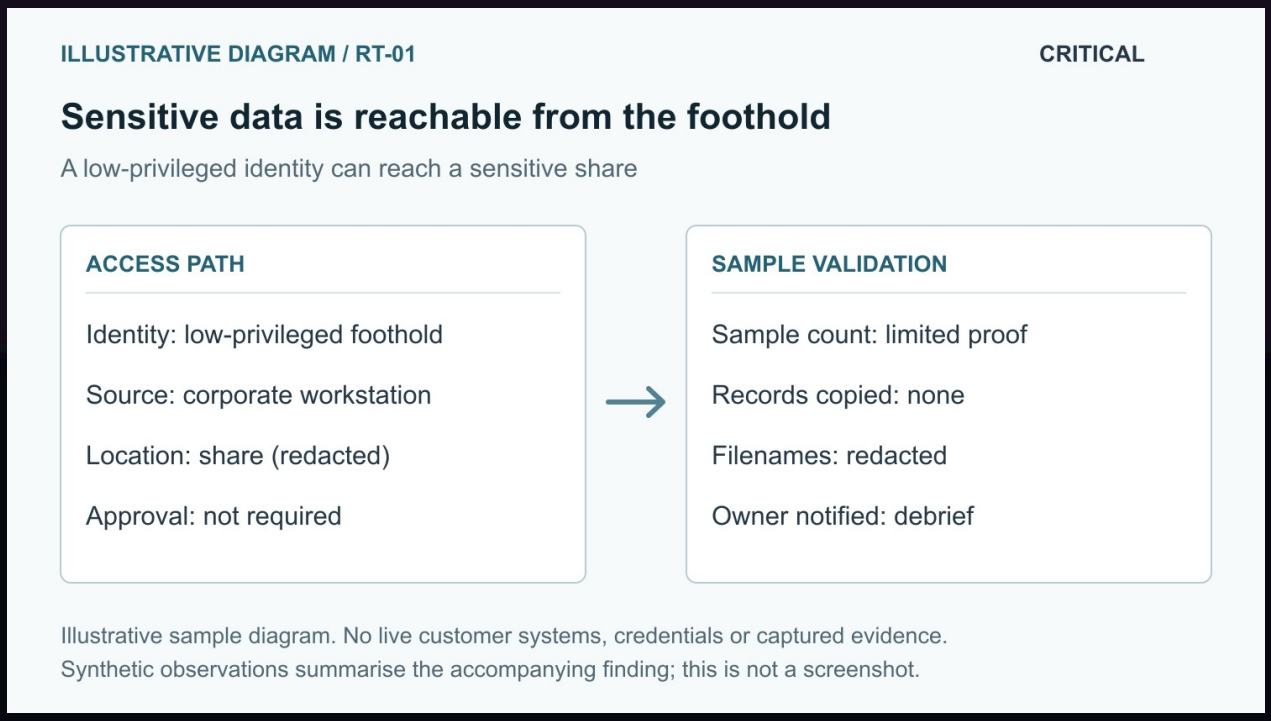


Figure RT-01-1: Illustrative diagram of sensitive data reachability without customer names or records.

RISK

A motivated attacker can use accessible internal data to escalate privileges, improve social engineering, identify high-value systems and exfiltrate sensitive records.

Unmanaged secrets also undermine password rotation and access control, because credentials may remain available in historic files and backups.

RECOMMENDATION

- Perform a permission review of all file shares, collaboration spaces and backup locations.
- Remove broad read access to sensitive data and enforce least privilege.
- Deploy data discovery for credentials, keys, passwords and regulated data in shared storage.
- Move secrets into an approved secrets management platform and rotate any exposed values.
- Alert on bulk access, unusual access time and sensitive keyword hits in shared storage.

RETEST GUIDANCE

- Use a standard user account to confirm sensitive shares are not accessible.
- Run approved secret scanning across collaboration and file storage.
- Perform controlled bulk-access simulation and confirm monitoring response.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1552 - Unsecured Credentials.
- MITRE ATT&CK TA0010 - Exfiltration.

4.2 OVER-PRIVILEGED SERVICE ACCOUNTS EXPAND IDENTITY BLAST RADIUS

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
CRITICAL	RT-02	9.1	Open	Low

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L
CATEGORY	MITRE T1078 / T1558.003 - Valid Accounts and Kerberoasting

IMPACTED SYSTEMS

ACCOUNT CLASS	NOTES
Service accounts	Held local or domain privileges beyond documented need.
Application administration	Shared credentials and long-lived passwords observed.
Privileged groups	Membership review showed excessive effective access.

DESCRIPTION

Service and application accounts had broader access than required for their documented functions. Some accounts also used long-lived password material.

Compromise of one such account allowed the red team to move quickly from initial access toward higher privileges.

DETAIL

LunarChain Security reviewed effective privileges, group memberships and observed account usage during the simulation. Several accounts could administer multiple systems or access sensitive data without a clear operational requirement.

Over-privileged service accounts are especially dangerous because they are often excluded from MFA, used non-interactively and monitored less closely than human administrators.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-02-E01	Redacted service account held broad local administrator rights.
RT-02-E02	Credential age and usage indicated long-lived manually managed account.
RT-02-E03	Privilege path analysis showed route from service account to sensitive objective.

RISK

A single credential exposure can grant access across many systems, bypassing the intended separation between business functions.

Attackers favour service accounts because they are stable, trusted and often noisy to rotate during incident response.

RECOMMENDATION

- Inventory service accounts, owners, systems, privileges and authentication methods.
- Reduce each service account to the minimum required access and remove interactive login where not needed.
- Move eligible workloads to gMSA or managed identities.
- Apply enhanced password standards, rotation and monitoring for any remaining manually managed service accounts.
- Alert on service account use outside expected hosts, hours and protocols.

RETEST GUIDANCE

- Re-run privilege path analysis and confirm no unnecessary paths remain.
- Confirm service accounts cannot perform interactive logon unless explicitly required.
- Review monitoring for service account use from unusual source hosts.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1078 - Valid Accounts.
- MITRE ATT&CK T1558.003 - Kerberoasting.

4.3 SENSITIVE ENVIRONMENT REACHABLE FROM CORPORATE TRUST TIER

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
CRITICAL	RT-03	9.0	Open	Medium

CVSS VECTOR	AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:L
CATEGORY	MITRE T1021 - Remote Services

IMPACTED SYSTEMS

BOUNDARY	NOTES
Corporate network	Compromised corporate access could reach sensitive administration paths.
Sensitive environment	Segmentation relied on shared administration and reused identity trust.
Jump hosts	Access path did not enforce sufficient tier separation.

DESCRIPTION

The red team was able to move from the corporate environment toward a more sensitive business environment because network and identity trust boundaries were not sufficiently separated.

The issue allowed a corporate compromise to become a route to sensitive data and business-process impact.

DETAIL

LunarChain Security identified shared administration paths and reused identity trust between the corporate and sensitive environments. Access was demonstrated in a controlled manner against non-production or approved proof targets.

The sensitive environment did not require a clean-room administrative identity or phishing-resistant step-up from a dedicated privileged workstation.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-03-E01	Redacted corporate host could reach sensitive administration path.
RT-03-E02	Identity review showed shared trust between tiers.
RT-03-E03	Controlled objective access was achieved without production impact.

RISK

Flat trust turns an ordinary corporate compromise into a path toward the organisation's most important systems.

Attackers who reach sensitive environments may be able to access regulated data, alter business workflows or cause operational disruption.

RECOMMENDATION

- Define and enforce administration tiers for corporate, server and sensitive business environments.
- Remove dual-homed systems and shared administration paths that bridge tiers.
- Require separate privileged identities and phishing-resistant MFA for sensitive environment access.
- Route administration through hardened, monitored privileged access workstations or bastions.
- Monitor and block unauthorised cross-segment authentication and management protocols.

RETEST GUIDANCE

- Attempt controlled access from corporate test hosts to sensitive administration paths and confirm it is blocked.
- Review identity trust and confirm no shared administrative groups bridge tiers unnecessarily.
- Confirm privileged access requires approved workstation, identity and MFA controls.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1021 - Remote Services.
- Microsoft enterprise access model guidance.

4.4 ALERTS WERE GENERATED BUT NOT TRIAGED WITHIN USEFUL WINDOWS

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
CRITICAL	RT-04	9.3	Open	Low

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L
CATEGORY	Detection and response process failure

IMPACTED SYSTEMS

AREA	NOTES
SIEM	High-value alerts existed but were not consistently escalated.
DLP	Data movement signal was suppressed or deprioritised.
EDR	Blocked event did not trigger broader investigation.

DESCRIPTION

The simulation showed that the organisation was not blind. Telemetry existed for several important actions, but alerts were not triaged quickly enough to change the outcome.

This is the core red team finding: detection without response does not reduce attacker impact.

DETAIL

LunarChain Security mapped red team actions to available customer telemetry during the debrief. Several actions produced logs or alerts, but the process did not consistently create an analyst-owned investigation.

The first meaningful response occurred after deliberate high-signal activity, rather than during earlier objective-enabling actions.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-04-E01	Redacted high-risk identity alert was present but not escalated within the engagement window.
RT-04-E02	Redacted data movement alert was suppressed or auto-closed.
RT-04-E03	EDR prevention event did not trigger threat-hunting follow-up.

ILLUSTRATIVE DIAGRAM

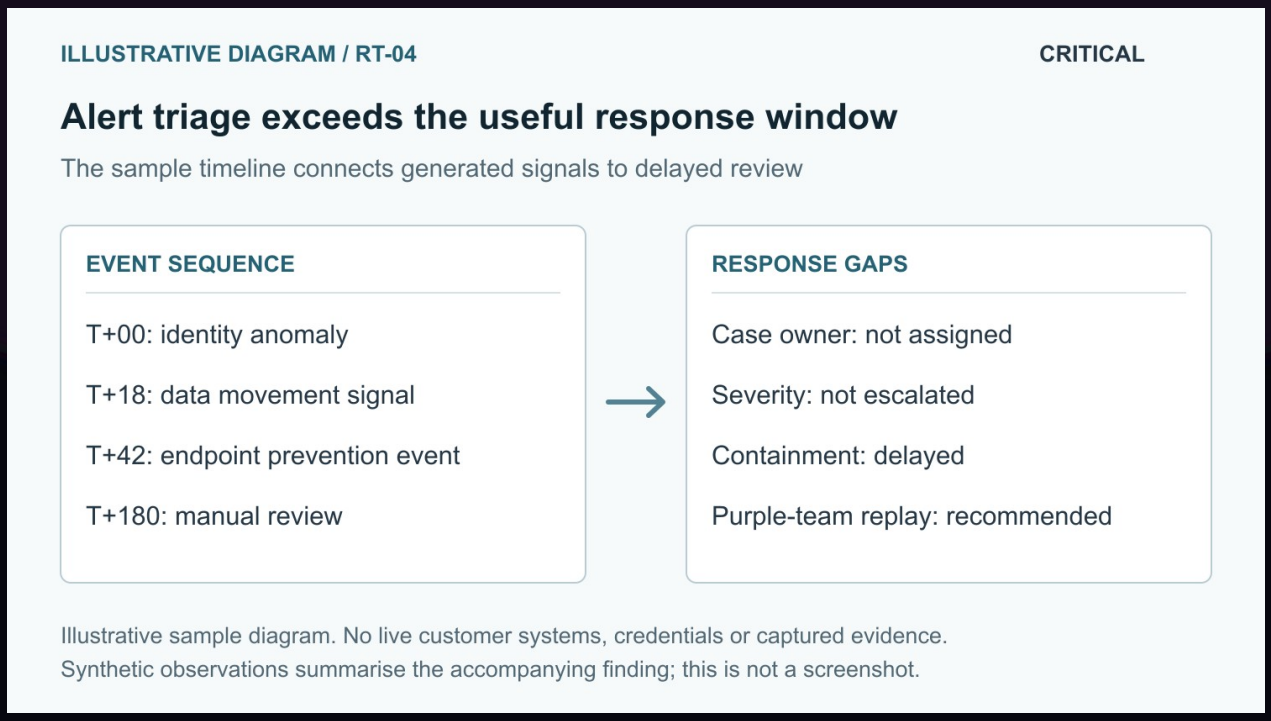


Figure RT-04-1: Illustrative diagram of alert generation and delayed triage in the sample timeline.

RISK

An attacker can complete objectives if security tools generate alerts that nobody investigates in time.

Operational response gaps also waste existing security investment, because telemetry fails to become containment.

RECOMMENDATION

- Define severity-based triage SLAs and make ownership explicit for critical identity, endpoint and data events.
- Remove broad auto-suppression rules for high-value alerts and require documented exceptions.
- Build use-case runbooks for phishing session theft, DCSync, bulk data access, C2 and persistence.
- Measure mean time to triage and mean time to contain during regular exercises.
- Run a purple team replay of this sample operation using the redacted timeline.

RETEST GUIDANCE

- Replay agreed red team indicators and confirm each creates a case with owner, severity and SLA.
- Review closed and suppressed alerts for the previous 90 days to identify unsafe patterns.
- Run a tabletop using this report's attack path and confirm response decisions are documented.

ADDITIONAL INFORMATION

- MITRE ATT&CK detection engineering guidance.
- NIST SP 800-61 incident handling guidance.

4.5 PHISHING-RESISTANT MFA NOT ENFORCED FOR HIGH-RISK USERS

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
HIGH	RT-05	8.1	Open	Medium

CVSS VECTOR	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
CATEGORY	MITRE T1566 / T1621 - Phishing and MFA Request Generation

IMPACTED SYSTEMS

CONTROL	NOTES
Identity provider	Push and OTP factors accepted for high-risk users.
Privileged and finance roles	Phishing-resistant factors not consistently required.

DESCRIPTION

The organisation relied on MFA methods that are susceptible to real-time phishing and social engineering for some high-risk users.

During the simulation, a controlled user interaction demonstrated that an attacker could obtain a session without knowing the user's password long term.

DETAIL

LunarChain Security used a controlled red team scenario to test whether current MFA controls resisted a realistic adversary-in-the-middle sign-in flow. The test confirmed that some factors could be proxied or socially approved.

This does not mean MFA has no value. It means the highest-risk roles need phishing-resistant methods that cryptographically bind authentication to the legitimate origin.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-05-E01	Controlled sign-in flow showed non-phishing-resistant factor accepted.
RT-05-E02	High-risk group review showed inconsistent FIDO2/WebAuthn enforcement.
RT-05-E03	Anomalous sign-in did not trigger timely containment during the sample scenario.

RISK

A realistic external attacker can use convincing pretexts to bypass push or OTP-based MFA and obtain an authenticated session.

If the compromised user has access to sensitive systems or can reach internal applications, the attacker can continue without needing malware on the endpoint.

RECOMMENDATION

- Require phishing-resistant MFA such as FIDO2/WebAuthn for administrators, finance users and sensitive application users.
- Block legacy authentication and enforce conditional access for unmanaged devices and unusual locations.
- Train users to report MFA prompts they did not initiate, but do not rely on training as the primary control.
- Create detections for impossible travel, new device sign-ins and session token anomalies.

RETEST GUIDANCE

- Repeat the controlled sign-in scenario against a test account in each high-risk group.
- Confirm non-phishing-resistant factors cannot satisfy high-risk access policies.
- Confirm anomalous sign-ins produce security cases with clear owner and SLA.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1566 - Phishing.
- CISA guidance on phishing-resistant MFA.

4.6 INITIAL ACCESS AND SOCIAL ENGINEERING CONTROLS CAN BE BYPASSED WITH CREDIBLE PRETEXTS

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
HIGH	RT-06	7.8	Open	Medium

CVSS VECTOR	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:L/A:N
CATEGORY	MITRE T1566 - Phishing

IMPACTED SYSTEMS

AREA	NOTES
Email security	Some redacted pretexts were delivered to target inboxes.
User reporting	Reporting occurred but was not consistently escalated to response.
Collaboration tools	External invitation controls require tightening.

DESCRIPTION

The red team achieved user interaction through credible business pretexts and collaboration flows. Some preventative controls worked, but enough messages reached users to create an initial access opportunity.

The purpose of this finding is not to blame users. It highlights where process and technical controls should absorb realistic human error.

DETAIL

LunarChain Security prepared several low-volume pretexts based on open-source business context. The campaign avoided mass sending and used approved safe landing pages.

User interaction and reporting varied by channel. Some reports did not create a security response quickly enough to remove the attack infrastructure or warn further targets.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-06-E01	Redacted phishing email delivered to user mailbox.
RT-06-E02	External collaboration invitation accepted by a test target.
RT-06-E03	User report did not consistently trigger containment workflow.

ILLUSTRATIVE DIAGRAM

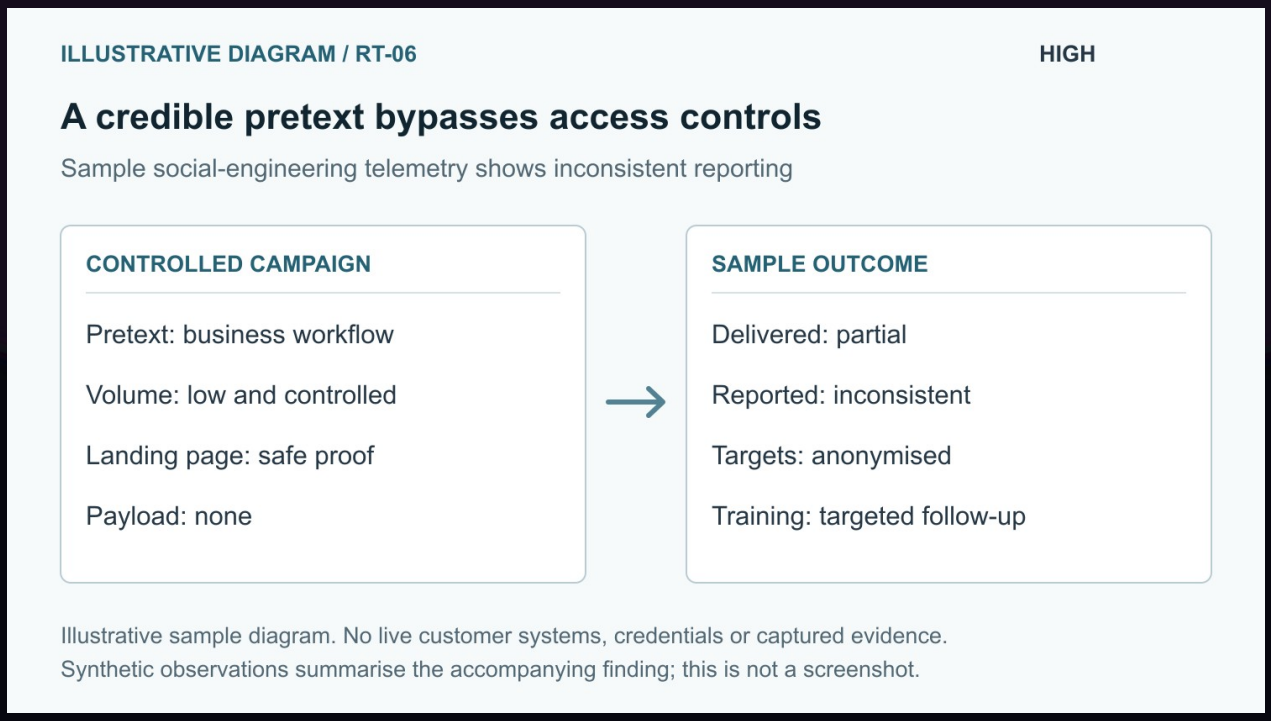


Figure RT-06-1: Illustrative diagram of social-engineering delivery and reporting behaviour.

RISK

Credible social engineering remains a practical route into the organisation. Once a session is obtained, attackers can bypass many perimeter controls.

Delayed escalation of user reports gives attackers more time to reuse infrastructure and target additional users.

RECOMMENDATION

- Tune email security controls for lookalike domains, QR-code lures, attachment detonation and recently registered domains.
- Restrict external collaboration invites and require stronger warnings or approvals for unknown tenants.
- Make user reporting one-click and route reports into a defined security triage process.
- Run targeted awareness training based on observed pretexts and reinforce positive reporting behaviour.

RETEST GUIDANCE

- Run a controlled phishing simulation and measure delivery, interaction, reporting and response time.
- Confirm reported phish creates a security case and triggers infrastructure blocking.
- Review collaboration tool external access policy against business need.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1566 - Phishing.
- NCSC guidance on phishing attacks.

4.7 COMMAND AND CONTROL EGRESS AND PERSISTENCE WERE NOT RELIABLY DETECTED

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
HIGH	RT-07	8.0	Open	Medium

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
CATEGORY	MITRE T1071 / TA0003 - Application Layer Protocol and Persistence

IMPACTED SYSTEMS

CONTROL	NOTES
Egress filtering	Outbound HTTPS to untrusted infrastructure was permitted.
Endpoint monitoring	Persistence-like actions did not trigger timely response.
DNS monitoring	Domain age and category controls did not block redacted infrastructure.

DESCRIPTION

The red team maintained controlled command-and-control style communications and established benign persistence indicators without reliable detection or response.

Payloads used in this sample were controlled and removed at the end of the engagement.

DETAIL

LunarChain Security used low-volume communications over allowed protocols to test whether the environment identified unusual outbound behaviour. Selected persistence-like actions were also performed under the rules of engagement.

Some telemetry existed, but it was not correlated into a response that would have contained the operation.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-07-E01	Controlled outbound communication to redacted infrastructure was permitted.
RT-07-E02	Persistence-like event did not generate a timely analyst response.
RT-07-E03	DNS and proxy logs contained indicators but were not correlated into a case.

RISK

Attackers often use normal web protocols to blend into business traffic. If egress and endpoint signals are not correlated, they can maintain long dwell time.

Undetected persistence increases the chance that a compromise survives password resets and initial containment.

RECOMMENDATION

- Restrict outbound traffic to required destinations through a monitored proxy.
- Alert on new or uncategorised domains, unusual JA3/TLS profiles and rare destination patterns.
- Deploy endpoint detections for common persistence locations and unusual scheduled tasks or services.
- Correlate DNS, proxy, EDR and identity telemetry into investigation cases.
- Create containment playbooks for suspected C2 or persistence events.

RETEST GUIDANCE

- Run controlled benign C2-like indicators and confirm proxy, DNS and EDR alerts fire.
- Create a test persistence artefact under change control and confirm detection and response.
- Review case workflow from alert creation through containment decision.

ADDITIONAL INFORMATION

- MITRE ATT&CK T1071 - Application Layer Protocol.
- MITRE ATT&CK TA0003 - Persistence.

4.8 SEGREGATION OF DUTIES WEAKNESS ALLOWS SIMULATED BUSINESS-PROCESS ABUSE

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
HIGH	RT-08	7.9	Open	Medium

CVSS VECTOR	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
CATEGORY	Business process control weakness

IMPACTED SYSTEMS

WORKFLOW	NOTES
Approval workflow	Same identity could satisfy incompatible roles in a non-production proof.
Sensitive action	Compensating alerting did not trigger during the simulation.

DESCRIPTION

A sensitive workflow did not enforce sufficient separation between initiation and approval roles in the tested path.

The red team used a non-production or approved test workflow only. No real transactions or customer records were modified.

DETAIL

After achieving privileged access, LunarChain Security reviewed whether a sensitive business action required independent approval. The tested path allowed a single compromised identity or privilege set to progress further than expected.

This kind of weakness is often overlooked in technical testing because it is a business-control failure rather than a software exploit.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-08-E01	Redacted workflow allowed maker and checker control to collapse in test path.
RT-08-E02	No high-severity alert generated for unusual approval sequence.
RT-08-E03	Business-process owner confirmed the proof action was representative.

RISK

If a real attacker reaches the relevant privilege level, they may be able to bypass intended four-eyes controls and perform financially or operationally sensitive actions.

Weak process controls can turn technical compromise into direct business impact.

RECOMMENDATION

- Enforce separation of duties at the application and identity layers for all sensitive workflows.
- Prevent the same user, group or session from acting as both maker and checker.
- Alert on emergency access, role changes and unusual approval sequences.
- Review non-production environments if they mirror production controls or contain real data.
- Document business-control owners and include them in security testing.

RETEST GUIDANCE

- Attempt the workflow with a controlled test account and confirm independent approval is required.
- Confirm role changes and sensitive approvals create auditable events.
- Review exception processes and break-glass controls for abuse potential.

ADDITIONAL INFORMATION

- NIST SP 800-53 AC-5 Separation of Duties.
- CIS Control 6 - Access Control Management.

4.9 INCIDENT RESPONSE PLAYBOOKS DO NOT COVER IDENTITY-LED INTRUSION END TO END

SEVERITY	REF	CVSS	STATUS	DIFFICULTY
MEDIUM	RT-09	6.4	Open	Medium

CVSS VECTOR	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N
CATEGORY	Incident response process weakness

IMPACTED SYSTEMS

AREA	NOTES
Runbooks	Identity compromise, token theft and data access response steps incomplete.
Deconfliction	Escalation path existed but operational handoffs were slow.
Evidence capture	Required logs were not always retained or easy to retrieve.

DESCRIPTION

The organisation had incident response processes, but the red team scenario showed gaps in end-to-end handling of identity-led compromise.

The main weakness was coordination: linking identity alerts, endpoint signals, data access, containment and executive decision-making.

DETAIL

During debrief, responders could identify some individual signals but lacked a single rehearsed workflow for this specific scenario.

Identity-led intrusions often progress without obvious malware. Response playbooks therefore need to focus on session revocation, credential rotation, privilege review, log preservation and data-impact assessment.

EVIDENCE SUMMARY

EVIDENCE ID	CUSTOMER-SAFE DESCRIPTION
RT-09-E01	Runbook review showed incomplete steps for session theft and token revocation.
RT-09-E02	Data access assessment required manual log retrieval from multiple owners.
RT-09-E03	Escalation path did not define decision points for containment versus business continuity.

RISK

Without rehearsed identity-led intrusion response, attackers can retain access through sessions, tokens and service accounts even after visible indicators are contained.

Unclear evidence ownership also slows breach assessment and regulatory decision-making.

RECOMMENDATION

- Create incident runbooks for phishing-resistant MFA bypass, session theft, privileged account compromise and data exfiltration.
- Include session revocation, token invalidation, password rotation and service account review steps.
- Define log owners, retention expectations and evidence export steps before an incident.
- Run tabletop and technical exercises using this sample attack path.
- Record executive decision points for containment actions that may disrupt business operations.

RETEST GUIDANCE

- Run a tabletop exercise and confirm owners can execute the identity compromise runbook.
- Perform a technical drill for revoking sessions and rotating affected credentials.
- Confirm logs required for data-impact assessment can be retrieved within agreed timeframes.

ADDITIONAL INFORMATION

- NIST SP 800-61 incident handling guidance.
- Microsoft incident response playbooks for identity compromise.

OPERATION TIMELINE

This condensed timeline shows the redacted operational path. A live report would include exact timestamps, source IPs, payload hashes, infrastructure and defender telemetry.

PHASE	ACTIVITY	CUSTOMER-SAFE EVIDENCE
Days 1-3	Open-source reconnaissance identified staff, technology, identity portals and business pretexts.	RT-NAR-E01
Day 4	Controlled social engineering obtained a session from a redacted test target.	RT-05-E01
Day 5	Foothold discovery identified sensitive shares and over-privileged service accounts.	RT-01-E01 / RT-02-E01
Day 6	Privilege escalation path reached domain-level control in the approved proof environment.	RT-NAR-E04
Days 8-11	Corporate compromise crossed into a sensitive environment through shared administration paths.	RT-03-E01
Days 12-14	Business-process impact was simulated in a non-production workflow.	RT-08-E01
Days 15-17	Deliberately loud indicators were used to test detection and response.	RT-04-E01

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.

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
OSINT tooling	Public information discovery and external attack-surface mapping.
Approved phishing platform	Controlled social engineering delivery and reporting measurement.
C2 simulation tooling	Benign command-and-control style telemetry generation.
BloodHound	Active Directory relationship and attack-path analysis.
SIEM / EDR exports	Detection mapping, timeline replay and blue team correlation.

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.