SAMPLE · ANONYMISED COMPOSITE · NO REAL CLIENT DATA

Identity and Access Ledger

Evidence file · engagement OP-03 · sample extract

CLIENT	Mid-size manufacturer, Netherlands (fictional composite)
PERIOD	2 – 20 March 2026
OPERATOR	Block The Chain · KvK 84616458
CLASSIFICATION	Sample. Every name, host, account and hash on these pages is synthetic.
FULL FILE	38 pages, 61 evidence items, 5 retest cycles. This extract shows the structure.

What the full file contains

This document is a fictional, anonymised composite built to show the structure of a Block The Chain evidence file. It contains no real client data.

1. Scope, method, rules

In scope

- Identity provider (cloud tenant) and its directory sync
- Two ERP environments and the CI system that deploys them
- VPN and remote-access accounts of eleven vendors
- Mail domain policies and legacy protocols

Out of scope

- OT and plant networks (separate engagement)
- Any destructive testing, any social engineering

Method

Read-only configuration and log review, authenticated as a named audit account. Every claim below is tied to an evidence item that was hashed (SHA-256) and time-stamped at capture and kept under chain of custody until hand-over. Nothing was changed on client systems during the review.

2. Findings summary

ID	FINDING	SEVERITY	STATUS AT HAND-OVER	EVIDENCE
F-01	Dormant domain admin from 2019 still authenticates	CRITICAL	Fixed · retested 18 Mar	E-04 E-05 E-09
F-02	One CI secret reused across three production systems	HIGH	Fixed · retested 19 Mar	E-12 E-13
F-03	Legacy mail protocol bypasses MFA for 14 mailboxes	HIGH	Mitigated · retest planned	E-21 E-22
F-04	Vendor VPN account without an owner	MEDIUM	Fixed · retested 18 Mar	E-31
F-05	DMARC policy set to none	LOW	Open · owner assigned	E-40

3. Finding F-01 in full

F-01 · CRITICAL

Dormant domain admin from 2019 still authenticates

AFFECTED	Directory account ADM-SVC-BACKUP02 (domain admin), last password change 2019-11-04, last successful logon 2026-03-09 02:14 UTC from an internal address.
WHAT WAS PROVEN	The account is enabled, holds domain-admin membership, is excluded from the MFA policy by a 2019 exception, and was used nine times in the review window. No owner is recorded.
HOW IT WAS REPRODUCED	Directory export (E-04) shows membership and last-set date. Sign-in log extract (E-05) shows nine interactive logons. Policy export (E-09) shows the MFA exclusion. Steps and queries are listed in appendix A.3.
IMPACT	Full directory control with a five-year-old credential outside MFA. Any prior leak of that password is a current domain compromise.
CONTROL MAPPING	ISO 27001 A.5.16, A.5.18, A.8.2 · NIST CSF 2.0 PR.AA-01, PR.AA-05 · CIS v8 5.3, 6.5
REMEDIATION	Account disabled 11 Mar, membership removed, exception deleted, password reset and vaulted. Quarterly review of privileged accounts added to the ledger with a named owner.
RETEST	18 Mar: logon attempt with the old credential fails (E-09b); membership export shows no dormant privileged accounts older than 90 days (E-09c).

4. Evidence register (extract)

ID	TYPE	SOURCE	CAPTURED (UTC)	SHA-256	CUSTODY
E-04	Directory export	Identity provider	2026-03-10 09:12	e862af725bcfa8dd…	operator → client vault
E-05	Sign-in log extract	Identity provider logs	2026-03-10 09:40	bfa9d6d8d2e7fb86…	operator → client vault
E-09	Policy export	Conditional access	2026-03-10 10:05	e78342c7ee0fd7cd…	operator → client vault
E-09b	Retest screenshot	Logon attempt	2026-03-18 14:21	4b42e098f436e4af…	operator → client vault
E-12	Pipeline variable dump	CI system	2026-03-11 15:30	09c5ad78abd48464…	operator → client vault

5. Retest and attestation

Every fixed finding was retested by the operator against the original evidence. Retest evidence carries a suffix (E-09b) and its own hash. The attestation on the last page of the full file states, per finding, what was verified, when, and by which method, and is signed by the operator. Evidence was deleted from operator systems on 27 March 2026; deletion confirmed in writing (E-61).

Next steps

- Close F-03 after the mail migration; retest scheduled.
- Assign an owner and a date to F-05; a one-line DNS change.
- Quarterly privileged-account review now runs from the ledger.

This document is a fictional, anonymised composite built to show the structure of a Block The Chain evidence file. It contains no real client data.