



VOORBEELD • GEANONIMISEERDE SAMENSTELLING • GEEN ECHTE KLANTDATA

Identity and Access Ledger

Evidence file • opdracht OP-03 • voorbeelduittreksel

OPDRACHTGEVER	Middelgrote maakindustrie, Nederland (fictieve samenstelling)
PERIODE	2 – 20 maart 2026
OPERATOR	Block The Chain • KvK 84616458
CLASSIFICATIE	Voorbeeld. Elke naam, host, account en hash op deze pagina's is verzonnen.
VOLLEDIG DOSSIER	38 pagina's, 61 bewijsstukken, 5 retestrondes. Dit uittreksel toont de structuur.

Wat het volledige dossier bevat

- 1. Scope, methode en rules of engagement
- 2. Samenvatting van bevindingen en ernst
- 3. Bevindingen volledig uitgewerkt (hier één: F-01)
- 4. Bewijsregister met hashes en chain of custody
- 5. Retest en attestatie
- 6. Control mapping (ISO 27001 • NIST CSF 2.0 • CIS v8)
- Bijlagen: ruwe exports, screenshots, logfragmenten

Dit document is een fictieve, geanonimiseerde samenstelling die de structuur van een Block The Chain evidence file laat zien. Het bevat geen echte klantgegevens.

1. Scope, methode, regels

In scope

- Identity provider (cloud-tenant) en de directory-sync
- Twee ERP-omgevingen en het CI-systeem dat ze uitrolt
- VPN- en remote-access-accounts van elf leveranciers
- Mail-domeinbeleid en legacy-protocollen

Buiten scope

- OT- en fabrieksnetwerken (aparte opdracht)
- Elke vorm van destructief testen, elke vorm van social engineering

Methode

Read-only review van configuratie en logs, aangemeld als een benoemd auditaccount. Elke bewering hieronder hangt aan een bewijsstuk dat bij vastlegging is gehasht (SHA-256) en van een tijdstempel voorzien, en tot de oplevering onder chain of custody is gebleven. Er is niets gewijzigd op systemen van de opdrachtgever.

2. Samenvatting bevindingen

ID	BEVINDING	ERNST	STATUS BIJ OPLEVERING	BEWIJS
F-01	Slapende domain admin uit 2019 kan nog inloggen	KRITIEK	Gefixt · geretest 18 mrt	E-04 E-05 E-09
F-02	Eén CI-secret hergebruikt in drie productiesystemen	HOOG	Gefixt · geretest 19 mrt	E-12 E-13
F-03	Legacy mailprotocol omzeilt MFA voor 14 mailboxen	HOOG	Gemitigeerd · retest gepland	E-21 E-22
F-04	Leveranciers-VPN-account zonder eigenaar	MIDDEL	Gefixt · geretest 18 mrt	E-31
F-05	DMARC-policy staat op none	LAAG	Open · eigenaar toegewezen	E-40

3. Bevinding F-01 volledig

F-01 ·

KRITIEK

Slapende domain admin uit 2019 kan nog inloggen

BETREFT	Directory-account ADM-SVC-BACKUP02 (domain admin), laatste wachtwoordwijziging 2019-11-04, laatste geslaagde logon 2026-03-09 02:14 UTC vanaf een intern adres.
WAT IS BEWEZEN	Het account is actief, is lid van domain admins, is via een uitzondering uit 2019 uitgesloten van het MFA-beleid en is in de reviewperiode negen keer gebruikt. Er is geen eigenaar vastgelegd.
HOE HET IS GEREPRODUCEERD	De directory-export (E-04) toont lidmaatschap en wijzigingsdatum. Het sign-in-logfragment (E-05) toont negen interactieve logons. De policy-export (E-09) toont de MFA-uitzondering. Stappen en queries staan in bijlage A.3.
IMPACT	Volledige controle over de directory met een vijf jaar oud credential buiten MFA. Elk eerder lek van dat wachtwoord is nu een domeincompromittering.
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
HERSTEL	Account uitgeschakeld op 11 maart, lidmaatschap verwijderd, uitzondering verwijderd, wachtwoord gereset en in de vault gezet. Kwartaalreview van bevoorrechte accounts toegevoegd aan de ledger, met een benoemde eigenaar.
RETEST	18 maart: logonpoging met het oude credential mislukt (E-09b); de lidmaatschapsexport toont geen slapende bevoorrechte accounts ouder dan 90 dagen (E-09c).

4. Bewijsregister (uittreksel)

ID	TYPE	BRON	FASTGELEGD (UTC)	SHA-256	CUSTODY
E-04	Directory-export	Identity provider	2026-03-10 09:12	e862af725bcfa8dd...	operator → vault opdrachtgever
E-05	Sign-in- logfragment	Logs identity provider	2026-03-10 09:40	bfa9d6d8d2e7fb86...	operator → vault opdrachtgever
E-09	Policy-export	Conditional access	2026-03-10 10:05	e78342c7ee0fd7cd...	operator → vault opdrachtgever
E-09b	Retest-screenshot	Logonpoging	2026-03-18 14:21	4b42e098f436e4af...	operator → vault opdrachtgever
E-12	Dump pipeline- variabelen	CI-systeem	2026-03-11 15:30	09c5ad78abd48464...	operator → vault opdrachtgever

5. Retest en attestatie

Elke gefixte bevinding is door de operator opnieuw getest tegen het oorspronkelijke bewijs. Retestbewijs krijgt een achtervoegsel (E-09b) en een eigen hash. De attestatie op de laatste pagina van het volledige dossier stelt per bevinding vast wat is geverifieerd, wanneer en met welke methode, en is door de operator ondertekend. Het bewijs is op 27 maart 2026 van de systemen van de operator verwijderd; verwijdering schriftelijk bevestigd (E-61).

Vervolgstappen

- F-03 sluiten na de mailmigratie; retest ingepland.
- Eigenaar en datum voor F-05; een DNS-wijziging van één regel.
- De kwartaalreview van bevoorrechte accounts draait nu vanuit de ledger.

Dit document is een fictieve, geanonimiseerde samenstelling die de structuur van een Block The Chain evidence file laat zien. Het bevat geen echte klantgegevens.