VOORBEELD · GEANONIMISEERDE SAMENSTELLING · GEEN ECHTE KLANTDATA

Identity and Access Ledger

Evidence file · opdracht OP-03 · voorbeeld (uitsnede)

OPDRACHTGEVER	PERIODE	OPERATOR	CLASSIFICATIE
Middelgroot productiebedrijf, Nederland (fictieve samenstelling)	2 – 20 maart 2026	BlockTheChain · KvK 84616458	Voorbeeld. Elke naam, host, account en hash op deze pagina's is fictief.

WAT HET VOLLEDIGE DOSSIER BEVAT

1. Scope, methode, regels

In scope

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

Buiten scope

- OT- en fabrieksnetwerken (aparte opdracht)
- Destructief testen en social engineering, in welke vorm dan ook

Methode

Read-only review van configuratie en logs, via een op naam gesteld auditaccount. Elke bewering hieronder rust op een bewijsstuk dat bij vastlegging is gehasht (SHA-256) en van een tijdstempel voorzien, en dat tot de oplevering onder chain of custody is gebleven. Tijdens de review is niets gewijzigd op systemen van de opdrachtgever.

OPDRACHTGEVER	Middelgroot productiebedrijf, Nederland (fictieve samenstelling)
PERIODE	2 – 20 maart 2026
OPERATOR	BlockTheChain · KvK 84616458
CLASSIFICATIE	Voorbeeld. Elke naam, host, account en hash op deze pagina's is fictief.
VOLLEDIG DOSSIER	38 pagina's, 61 bewijsstukken, 5 retestrondes. Deze uitsnede toont de structuur.

2. SAMENVATTING BEVINDINGEN

Vijf bevindingen. Eén kritiek, drie opgelost vóór de oplevering.

05	01	03	05
BEVINDINGEN	KRITIEK	OPGELOST EN HERTEST	BEWIJSSTUKKEN

ID	BEVINDING	ERNST	STATUS BIJ OPLEVERING	BEWIJS
F-01	**Slapende domain admin uit 2019 kan nog inloggen**	KRITIEK	Opgelost · retest 18 mrt	E-04 E-05 E-09
F-02	**Eén CI-secret hergebruikt in drie productiesystemen**	HOOG	Opgelost · retest 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	**VPN-account van leverancier zonder eigenaar**	MIDDEN	Opgelost · retest 18 mrt	E-31
F-05	**DMARC-policy staat op none**	LAAG	Open · eigenaar toegewezen	E-40

De ernst is gebaseerd op de impact op de organisatie, niet op scanneroutput. De status is de stand bij oplevering; elke opgeloste bevinding is opnieuw getest tegen het oorspronkelijke bewijs.

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 aanmelding 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 het lidmaatschap en de laatste wachtwoordwijziging. Het fragment uit het aanmeldlog (E-05) toont negen interactieve aanmeldingen. De policy-export (E-09) toont de MFA-uitzondering. Stappen en queries staan in bijlage A.3.
IMPACT	Volledige controle over de directory met vijf jaar oude inloggegevens zonder MFA. Is dat wachtwoord ooit gelekt, dan is het domein nu gecompromitteerd.
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 op 11 maart uitgeschakeld, lidmaatschap ingetrokken, uitzondering verwijderd, wachtwoord gereset en in de vault opgeslagen. Kwartaalreview van bevoorrechte accounts opgenomen in de ledger, met een benoemde eigenaar.
RETEST	18 maart: aanmeldpoging met de oude inloggegevens mislukt (E-09b); de export van lidmaatschappen toont geen slapende bevoorrechte accounts ouder dan 90 dagen (E-09c).

Hier staat één bevinding volledig uitgewerkt. Het complete dossier bevat alle vijf in deze vorm, elk met eigen bewijsverwijzingen, eigenaar en datum.

4. BEWIJSREGISTER (UITSNEDE)

Elke bewering rust op een gehasht bewijsstuk met tijdstempel

ID	TYPE	BRON	VASTGELEGD (UTC)	SHA-256	BEWARING
E-04	Directory-export	Identity provider	2026-03-10 09:12	e862af725bcfa8dd…	operator → vault opdrachtgever
E-05	Fragment aanmeldlog	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	Aanmeldpoging	2026-03-18 14:21	4b42e098f436e4af…	operator → vault opdrachtgever
E-12	Dump van pipelinevariabelen	CI-systeem	2026-03-11 15:30	09c5ad78abd48464…	operator → vault opdrachtgever

De hashes zijn SHA-256 en hier ingekort vanwege de kolombreedte. Het volledige dossier bevat de complete hashes en per bewijsstuk de chain of custody.

5. RETEST EN VERKLARING

Retest en verklaring

Elke opgeloste bevinding is door de operator opnieuw getest tegen het oorspronkelijke bewijs. Retestbewijs krijgt een achtervoegsel (E-09b) en een eigen hash. De verklaring op de laatste pagina van het volledige dossier legt 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; de verwijdering is schriftelijk bevestigd (E-61).

VERVOLGSTAPPEN

F-03 sluiten na de mailmigratie; retest ingepland.

Eigenaar en datum toewijzen aan 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 laat zien hoe een evidence file van BlockTheChain is opgebouwd. Het bevat geen echte klantgegevens.