White Paper · Pre-Seed & Pilot Launch

CyberSecurity AD

Veilige AI-analyse van digitale strafdossiers

voor de strafrechtadvocatuur

Amsterdam · februari 2026

Vertrouwelijk · Reproduceerbaar · Juridisch toetsbaar

Dit document is bestemd voor strafrechtadvocaten en investeerders.

Inhoud

Samenvatting (Executive Summary)

Digitale opsporing is grotendeels geautomatiseerd. Digitale dossiers zijn omvangrijk, technisch complex en vaak samengesteld via geavanceerde analysetools. De verdediging wordt in toenemende mate geconfronteerd met technisch bewijs dat praktisch oncontroleerbaar is zonder gespecialiseerde infrastructuur.

CyberSecurity AD (CSAD) ontwikkelt en beheert afgeschermde technische infrastructuur voor de gecontroleerde analyse van digitale strafdossiers, met inzet van AI onder volledige controle van de verdediging.

De infrastructuur:

- creëert geen bewijs;
- verricht geen juridische beoordeling;
- verricht geen opsporing;
- en heeft geen inzage in dossierdata.

CSAD levert uitsluitend technische analyse-infrastructuur die forensisch reproduceerbaar, juridisch toetsbaar en vertrouwelijk is ingericht, conform geldende wetgeving, NOvA-uitgangspunten en de aankomende Cyberbeveiligingswet (NIS2).

1.

Het probleem

1.1 Digitale ongelijkheid in de strafrechtsketen

In strafzaken is digitale bewijsvoering structureel verschoven van menselijke analyse naar geautomatiseerde verwerking:

- telecomdata
- device-extracties
- serverlogs
- chatdatasets (o.a. EncroChat, Sky ECC)
- metadata-analyses

Deze datasets worden vaak gegenereerd, gefilterd en samengevat door opsporingssoftware die voor de verdediging niet inzichtelijk of reproduceerbaar is.

De verdediging moet deze uitkomsten juridisch bestrijden, maar beschikt zelden over:

- vergelijkbare technische analysecapaciteit;
- controleerbare verwerkingsketens;
- reproduceerbare analyse-omgevingen.

1.2 Het ontbreken van juridisch veilige AI-infrastructuur

Publieke AI-modellen en cloudoplossingen zijn onverenigbaar met:

- beroepsgeheim;
- vertrouwelijkheid;
- herleidbaarheid;
- en juridische toetsing.

> **Wat ontbreekt is neutrale technische infrastructuur, expliciet ontworpen voor gebruik door de strafrechtadvocatuur.**

2.

Wat CyberSecurity AD is (en niet is)

2.1 Wat CSAD wel is

CyberSecurity AD ontwikkelt en beheert:

- afgeschermde technische infrastructuur;
- voor gecontroleerde analyse van digitale strafdossiers;
- met inzet van gespecialiseerde AI-modellen;
- in een vaste, reproduceerbare analyseketen.

2.2 Wat CSAD niet is

CSAD:

- beoordeelt geen dossiers;
- interpreteert geen bewijs;
- trekt geen conclusies;
- verricht geen opsporing;
- en heeft geen toegang tot aangeleverde data.

> **Alle juridische interpretatie en strategische inzet blijft uitsluitend bij de verdediging.**

3.

Juridische positionering: technische toetsbaarheid

3.1 Juridisch toetsbaar ≠ juridisch oordeel

Binnen CSAD betekent "juridisch toetsbaar": technisch controleerbaar door verdediging en rechter, zonder bewijswaardering of juridische kwalificatie.

De infrastructuur is ontworpen om:

- aannames zichtbaar te maken;
- methodiek te controleren;
- herleidbaarheid te borgen;
- reproduceerbaarheid mogelijk te maken.

> **Niet om waarheid te claimen.**

4.

Architectuur: gescheiden, afgeschermd, controleerbaar

De CSAD-infrastructuur bestaat uit twee strikt gescheiden componenten:

4.1 CSAD-applicatie (gebruikerszijde)

- lokaal geïnstalleerd (desktop of mobiel);
- per zaak een geïsoleerde werkomgeving;
- gebruiker selecteert dataset en analysekaders;
- geen automatische koppelingen;
- geen verborgen verwerking.

4.2 CSAD-serveromgeving (verwerkingszijde)

- volledig afgeschermd;
- geen cloud;
- geen publiek internet;
- geen data-inzage;
- vaste AI-keten per analyse.

5.

Beveiligde gegevensoverdracht

Gegevensoverdracht vindt uitsluitend plaats via:

- end-to-end encryptie;
- cryptografische verificatie (SHA-512);
- geauthenticeerde verbindingen;
- tijdelijke sessies.

CyberSecurity AD kan technisch geen kennis nemen van dossierinhoud.

6.

De AI-analyseketen (server-side)

De verwerking bestaat uit een vaste, sequentiële keten van vier gespecialiseerde AI-modellen.

AI-Model 1 — Forensische data-extractie

Technische extractie van digitale bronbestanden volgens forensische standaarden. Focus op structuur, consistentie en volledigheid.

AI-Model 2 — Technische verificatie

Onafhankelijke controle van aannames, methodiek en interne logica. Gericht op het voorkomen van interpretatie- en bevestigingsbias.

AI-Model 3 — Reproduceerbaarheidstoets

Cross-validatie tegen originele brondata. Toetsing van herleidbaarheid en reproduceerbaarheid van bevindingen.

AI-Model 4 — Juridische rapportagestructuur

Structurering van gevalideerde technische bevindingen in een objectief, juridisch bruikbaar format. Zonder normatieve conclusies.

7.

Terugkoppeling & rapportage

De gebruiker ontvangt:

- een technisch rapport;
- volledige traceerbaarheid van analysestappen;
- verificatiegegevens voor reproduceerbaarheid.

Het rapport blijft lokaal bij de gebruiker.

8.

Vertrouwelijkheid & compliance

CSAD waarborgt:

- geen datadeling;
- geïsoleerde verwerking per zaak;
- geen hergebruik;
- volledige verwijderbaarheid.

De infrastructuur sluit aan bij:

- geldende wetgeving;
- cybersecurity-best-practices;
- NIS2 (Cyberbeveiligingswet 2026);
- NOvA-uitgangspunten.

9.

Waarom CyberSecurity AD bestaat

CyberSecurity AD is niet ontstaan vanuit marktpositionering, maar vanuit een technische noodzaak:

> **Digitale bewijsvoering vereist technische controleerbaarheid om juridische toetsing mogelijk te maken.**

10.

Oprichter & technische basis

P.W. Oldenburger

Cum laude afgestudeerd CyberSecurity-specialist (GPA 8.02), met focus op:

- digitale forensiek;
- reproduceerbaarheid;
- juridisch toetsbare systemen.

De rol van de oprichter beperkt zich tot:

- ontwerp;
- technische architectuur;
- infrastructuurbeheer.

Geen inhoudelijke rol in individuele analyses.

11.

Launchstrategie: pre-seed & pilot

11.1 Fase 1 — Pilot customers (advocatuur)

- beperkt aantal strafrechtkantoren;
- gecontroleerde inzet;
- feedback op bruikbaarheid en juridische inpassing;
- geen schaalambitie in deze fase.

11.2 Fase 2 — Pre-seed funding

Doel:

- verdere hardening van infrastructuur;
- certificering en compliance-documentatie;
- beperkte teamuitbreiding (infra / security).

11.3 Fase 3 — Gecontroleerde opschaling

- uitbreiding binnen Nederlandse strafrechtpraktijk;
- behoud van gesloten, defensieve positionering;
- geen publieke AI-modellen.

12.

Slotverklaring

CyberSecurity AD levert infrastructuur, geen oordeel.

De technologie is ontworpen om:

- controle mogelijk te maken;
- transparantie af te dwingen;
- juridische gelijkwaardigheid te herstellen.

Niet om waarheid te produceren, maar om haar toetsbaar te maken.

CyberSecurity AD

Sint Olofssteeg 4 C, 1012 AK Amsterdam

info@cybersecurityad.com · www.cybersecurityad.com

Amsterdam · februari 2026