

CASE FILE · LB / 2026 · SEC · ARC

Lars Blomgaard.

IT-Security Arkitekt · AI Governance · Digital
Efterforsker

21+ års erfaring med at beskytte, undersøge og formidle kompleks informationssikkerhed — fra Rigspolitiets NC3 til offentlige enterprise-miljøer og nu governance af AI i staten.

— DOSSIER

STATUS

Aktiv

BASE

Vurderingsstyrelsen

FRA

Marts 2026

DOMENE

DFIR · AI Gov

KLAR

Offentlig

blomgaard@gmail.com

lablo.dk

linkedin.com/in/leb56751gvgr

§ 01 — AKTUEL POSITION

Hvor jeg er nu.

• MARTS 2026 — I DAG

Vurderingsstyrelsen

IT-Security Arkitekt · AI Governance

Arbejder med sikker arkitektur og governance af AI-systemer i en af statens centrale myndigheder. Fokus på risikovurdering, compliance (EU AI Act, NIS2) og brobygning mellem teknisk sikkerhed og forretningsmæssig beslutningskraft.

§ 02 — KERNEKOMPETENCER

Det jeg kan.

21+ år

Informationssikkerhed

Strategisk formidling af beskyttelse, risici og trusselslandskab på tværs af organisatoriske niveauer.

600+ sager

Incident Response & DFIR

Chain of custody, malware-analyse, RAM-dumps, log- og netværkstrafik, triage i pressede situationer.

7+ år

Digital Efterforskning

Bevissikring, bekæmpelse af IT-kriminalitet og triangulering af data — trænet hos Politiets NC3.

∞ formidling

Undervisning & Storytelling

Gør kompleks IT-sikkerhed forståelig — fra C-suite briefings til tekniske deep-dives.

▲ FOKUSOMRÅDE · 2026

Governance af AI, ikke bare sikkerhed *mod* den.

AI ændrer angrebsfladen — men også organisationens ansvar. Mit arbejde forener klassisk cybersikkerhed med de nye krav til gennemsigtighed, dokumentation og risikostyring, der

følger med intelligente systemer.

<p>01</p> <h3>EU AI Act & NIS2 Compliance</h3> <p>Oversættelse af regulatoriske krav til konkrete kontroller og tekniske design-beslutninger.</p>	<p>02</p> <h3>Risikovurdering af AI-systemer</h3> <p>Klassificering, data-governance, model-monitoring og shadow-AI i offentlige miljøer.</p>
<p>03</p> <h3>Sikker Implementering</h3> <p>Prompt injection, data-leakage, adgangskontrol og audit trails for AI-assisterede workflows.</p>	<p>04</p> <h3>Kulturforandring & Awareness</h3> <p>Briefinger der ruster medarbejdere til at bruge AI klogt, ansvarligt og uden at blotte forretningen.</p>

§ 03 — NØGLETAL

I tal.

+600

SAGER

Efterforskninger hvor beviset blev fundet i komplekse datamængder.

40%

KOMMUNIKATION

Brobygning mellem teknisk sikkerhed og forretningsforståelse.

7 år

SPEAKER

CPH B-Sides: dataindsamling, analyse og netværks-triage.

30%

UNDERVISNING

Governance, angrebshåndtering og forensic metode.

§ 04 — KARRIERE

Tidslinje.

• AKTUEL

Marts 2026 →

Vurderingsstyrelsen

◦ ARKIV

2024 — 2026

DUBEX A/S

◦ ARKIV

2022 — 2024

DSV A/S

IT-Security Arkitekt · AI Governance

- Sikker arkitektur og governance af AI-systemer i den offentlige sektor.
- Risikovurdering, compliance med EU AI Act og NIS2, samt operationel modenhed.
- Brobygning mellem teknisk sikkerhed og forretningsmæssig beslutningskraft.

Senior IT-Security Consultant · IR & Forensics

- Undervisning i Dubex Academy og onboarding af nye og eksisterende kunder.
- Implementering af nye services og opbygning af testmiljøer.
- Deltagelse i Incident Response-vagten. Chain of custody og forensic indsamling.

Senior IT-Security Architect

- Sikrede at alle systemer overholdt politikker og standarder.
- Deltog i udvikling af strategier og retningslinjer for IT-arkitektur.
- Bidrog til udarbejdelse af forensics-politik og vedligeholdt incident response.
- Ansvarlig for undervisning og formidling af informationssikkerhed.

◦ ARKIV

2014 — 2022

Rigspolitiet · NC3

Digital Efterforsker · IT-konsulent

- Digital efterforskning af cyberkriminalitet (hacking, misbrug, afpresning mv.).
- Forensic datasikring og analyse. Triangulering af data og identifikation af gerningspersoner.
- Undervisning af IT-koordinatorer og borgere. Oplægsholder for NC3.
- Første responder og guide ved anmeldelser til politiet. Forebyggelsesmateriale.

◦ ARKIV

2010 — 2014

NNIT

Security Operations Specialist

- Drift og vedligeholdelse af antivirusprodukter, proxy-servere og log management.
- Udarbejdelse af procedurer og handlingsplaner for AV-produkter.
- Styring og koordinering af incidents / security incidents.
- Medvirkede til opstart af Security Operations Center og SIEM-system.

◦ ARKIV

2006 — 2010

NNIT

Surveillance Specialist

- Overvågning af servere, databaser og webhoteller.
- Håndtering af „major incidents” og monitorering for sikkerhedshændelser.
- Betjening af eksterne kunder.

— PARALLELT SPOR

· BIBESKÆFTIGELSE

◦ ARKIV

2020 — 2025KEA · Københavns
Erhvervsakademi

Underviser · Diplom i IT-sikkerhed

- Undervisning i standarder, frameworks, sikkerhedsarbejde og dokumentation.
- Awareness-træning, incident response, CIS-kontroller og ISO 2700x.

§ 05 — UDDANNELSE

Fundament & værktøj.

— UDDANNELSE

2017 — 2019

Diplom i IT-sikkerhed

KEA · Københavns Erhvervsakademi

2003 — 2005

Datamatiker

Erhvervsakademi

— SPROG

Dansk modersmål**Engelsk** flydende i skrift og tale**Svensk / Norsk** kommunikationsniveau

— TEKNISK VÆRKTØJSKASSE

AI	AI Governance & Formidling
Auto	Automation & Scripting
Net	Netværk & Endpoint Security
Lab	Malware Analyse (REMnux, FLARE)
OSINT	Open Source Intelligence
Std	ISO 2700x, CIS, NIS2, AI Act

„God sikkerhed og god formidling har samme DNA: **gentagelse, teknik og evnen til at forklare hvorfor det er vigtigt.**”

— END OF FILE · EOF ■

Kontakt · blomgaard@gmail.com · lablo.dk · linkedin.com/in/leb56751gvgr