SECURITY ARCHITECT & ADVISOR

Remco Vaal

Principal Security Consultant — Enterprise & Solution Security Architecture · Security Officer / CISO Advisory

CISSP · CCSP · AAISM · CCZT · CCSK · ISO 27001 LI · SABSA SCF · ArchiMate · 25+ jaar in IT & security

Hellevoetsluis, Nederland · +31 6 11 85 81 03 · remco@vaal-consulting.nl · vaal-consulting.nl · Portfolio · LinkedIn

PROFIELSCHETS

Principal Security Consultant met 25+ jaar ervaring in IT en information security, waarvan ruim 4 jaar als zelfstandig consultant. Actief binnen enterprise security architecture, solution security architecture, security governance en Security Officer / CISO advisory, veelal voor organisaties in gereguleerde, kritieke of complexe omgevingen.

Een natuurlijke verbinder die regelgeving, privacybeginselen, industriestandaarden en bedrijfsdoelen samenbrengt tot samenhangende, volledige en operationeel effectieve securityprogramma's — of het nu gaat om één project of een organisatiebreed InfoSec-programma. Heeft oprechte passie voor het vakgebied en legt complexe security-onderwerpen toegankelijk uit aan zowel engineers als bestuurders, met de focus op het mogelijk maken van de business in plaats van het blokkeren ervan.

Volgt actief opkomende technologische ontwikkelingen, waaronder AI, en vertaalt deze naar effectieve, verantwoorde en toekomstgerichte security-aanpakken. Vendor-agnostisch by design — werkt vloeiend met meerdere vendor-stacks per security- en netwerkcategorie.

KERNVAARDIGHEDEN

#	DOMEIN	SCOPE	ROLLEN
1	**Governance, Policy & Frameworks**	Controlraamwerken (ISO, NIST, CIS, ISF), policy-lifecycle, control mapping & validatie, governance-structuren	CISO, (T)ISO
2	**AI Security & Governance**	AI-risicoraamwerken, aansluiting op de EU AI Act, beveiligen van AI-systemen en pipelines, AI threat modeling, verantwoorde AI-governance	ESA, CISO, Advisor
3	**Privacy & Data Protection**	GDPR-complianceprogramma's, privacy-by-design, DPIA, internationale datagovernance, integratie met security-architectuur en regelgeving	(T)ISO, CISO, ESA
4	**Regulatory & Compliance**	DORA, NIS2/CBW, PCI DSS, GDPR: verplichtingen in kaart brengen en vertalen naar doelarchitectuur, roadmaps en control-ontwerp	CISO, (T)ISO
5	**Zero Trust & Identity**	Zero Trust-strategie, ZTA, IAM/PAM, CASB/MCAS, Conditional Access, identity-first patronen	ESA, SSA
6	**Supplier / Third-Party Assurance**	TPRM, leveranciersclausules, beoordeling van SOC/ISAE/ISO-bewijs, beheer van assurance-bevindingen	(T)ISO, CISO
7	**DevSecOps & Secure SDLC**	Secure SDLC, CI/CD-controls (SAST/DAST/SCA), governance rond code review, pipeline hardening	SSA, (T)ISO
8	**Security Architecture & Design**	Target-state architecturen, referentiepatronen, security-by-design, architectural decision records, design reviews	ESA, SSA
9	**Risk & Decision Support**	Besluitvormingsdocumenten, opties-analyse, risicoafwegingen, advisering richting directie, governance rond risk acceptance	CISO, ESA
10	**Network Security & SASE**	SASE-adoptie, SD-WAN-migratie, segmentatie, NDR, ontwerp van secure connectivity	ESA, SSA, Advisor
11	**SOC / SIEM / Detection**	Opbouw van SIEM/SOAR, loggingstandaarden, use-case lifecycle, MSSP-onboarding, Blue Team-strategie	SSA, ESA
12	**Vulnerability Mgmt / CTEM**	CTEM-roadmaps, prioriteringsmodellen, remediation-workflows, operating models & dashboarding	(T)ISO, ESA, SSA

#	DOMEIN	SCOPE	ROLLEN
13	**Applied AI & Security Tooling**	Effectieve en verantwoorde inzet van AI in security-werk; AI-ondersteunde analyse, threat modeling, documentatie en oplossingsontwerp; beoordelen van AI-toolrisico's	ESA, Advisor, CISO
14	**Security Process Design & Optimisation**	In kaart brengen en verbeteren van security-processen; oplossen van complexe security-vraagstukken; ontwerpen van pragmatische, efficiënte operating models over security-domeinen heen	All roles

BELANGRIJKSTE RESULTATEN

- DORA- en NIS2/CBW-verplichtingen vertaald naar architectuur en roadmaps bij vijf gereguleerde klanten in betaalinfrastructuur, verzekeringen, telecom, spoor en vastgoedbeleggingen — waaronder dienstverleners die de verplichtingen van een onder toezicht staande eindklant dragen.
- Rusland IT-isolatie ontworpen onder acute geopolitieke druk, met behoud van de continuïteit van de wereldwijde voedselvoorzieningsketen (Viterra).
- Enterprise DevSecOps capability model gedefinieerd en organisatiebreed secure code review gestandaardiseerd over alle developmentteams (Ahold Delhaize).
- CTEM-roadmap ontworpen en organisatie-specifiek operating concept uitgewerkt (Fédèrale Insurance — onder toezicht van de Nationale Bank van België).
- Strategische security architectuur vormgegeven via het 9-laags model van Rik Maes (business / information / technology); roadmap, governance en stakeholder-besluitvorming uitgelijnd over initiatieven heen (KPN).

WERKERVARING — ZELFSTANDIG CONSULTANT, VAAL CONSULTING B.V. (MRT 2022 – HEDEN)

ANWB — Security Consultant / Content Lead

jul 2026 – heden

Nederlandse mobiliteits- en wegenwachtorganisatie; driejarig programma voor securityvolwassenheid, momenteel in uitvoering.

- De meerjarige volwassenheidsroadmap vormgegeven over acht securitythema's (netwerk, vulnerability, malware, logging & monitoring, digital trust services, IAM, dataprotectie & recovery, penetratietesten), gericht op herinrichting van capabilities in plaats van incrementeel procesherstel.
- Compliance-by-design als expliciet programmadoel geïntroduceerd, gericht op het terugbrengen van de handmatige inspanning om compliance aan te tonen.
- De versnellingstrack bedacht en inhoudelijk geleid: een cyberhygiënecheck vanuit goedhuisvaderschap, afgeleid van de NCSC-basismaatregelen en CIS Controls IG1, met parallel het op orde brengen van de CMDB.
- Inhoudelijke coördinatie over de expertiseteams en validatie van de opgeleverde resultaten; opgetreden als onafhankelijke architectuurtoets bij technologie- en productkeuzes waar volledige vervanging op tafel lag.

KPN — Enterprise Security Architect

aug 2024 – heden

Gereguleerde Nederlandse telecomoperator.

- Strategische security architectuur vormgegeven via het 9-laags model van Rik Maes (business / information / technology) om besluitvorming bij stakeholders te ondersteunen en initiatieven uit te lijnen op domeinen en governance.
- HLD governance-standaard gedefinieerd (template, security review checklist, ARB-integratie) waarmee design-kwaliteit en consistentie over projecten heen verbeterden.
- DORA regulatory advisory geleid op contracten, SLAs, supply chain en documentatie; SIAM-propositie opgeleverd in lijn met DORA Chapter V (third-party ICT risk).
- VM-naar-CTEM strategisch richtingdocument opgeleverd, NDR-as-a-Service viability assessment, supplier assurance evidence review-guidance en GDPR privacy-by-design consultancy.

Geldmaat — Enterprise Security Advisor
aug 2024 – mei 2026

Operator van kritieke ATM-infrastructuur voor de Nederlandse banksector.

- DORA + NIS2 (Cyberbeveiligingswet) compliance-programma opgeleverd: executive framing, obligation mapping, governance-structuur, gefaseerde roadmap en evidence-aanpak.
- Zero Trust target state en gefaseerde roadmap gedefinieerd (identity-first, device posture, micro-segmentation, conditional access); bijgedragen aan de GAPA-architectuurboard.
- CTEM operating model gebouwd (RACI, prioritering op criticality × exploitability × exposure, KPI/KRI dashboarding) ter vervanging van een gefragmenteerd VM-proces.
- Penetration testing-strategie en -governance opgeleverd, uitgelijnd op DORA TLPT en NIS2/CBW; tevens lifecycle-management framework dat invulling geeft aan DORA Art. 8 en NIS2 asset/patch verplichtingen.
- Continuïteitsscenario's voor 72-uurs stroomuitval beoordeeld voor het nationale ATM-netwerk (LEO-satelliet / dark-fibre fallback, dieselafhankelijkheid, prioritering).

NS — Dutch Railways — Solution Security Architect
jul 2025 – jan 2026

Nationale spoorwegmaatschappij, SDI-domein (Software-Defined Infrastructure) — OT/IT-grensvlak.

- VM/CTEM operating model ontworpen voor het SDI-domein (RACI, SLA's, risk-based prioritering, rapportage en uitzonderingsbehandeling).
- NFR-bibliotheek en security requirements engineering-standaard opgebouwd, met traceability naar het control framework en supplier intake-vragenlijst.
- Intern + leveranciers-framework gemapt op CIS Controls v8.2 voor uniforme rapportage; modular vs. siloed architectuur-decision paper opgeleverd.
- Regulatory compliance-advies geleverd over NIS2/CBW, DORA, PCI DSS en GDPR met control-to-obligation traceability; pen test governance-standaard uitgelijnd op TIBER-EU / DORA TLPT.

(Confidential) — Dutch Army — Enterprise Security Architect / Advisor
dec 2024 – jul 2025

Defensie-omgeving; missiekritieke OT/IT in een geclassificeerde operationele context.

- Geadviseerd over NIST RMF alignment: SP 800-53r5 control-validatie en SP 800-37r2 RMF-implementatie (SSP-structuur, ATO-proces, FIPS 199 categorisatie).
- Zero Trust target architecture en gefaseerde implementatie-roadmap gedefinieerd (identity-first, device posture, segmentation, conditional access, ZTNA/PAM/Entra tooling-guidance).
- Battle Management System security reference architecture opgeleverd op basis van defence-in-depth, IEC 62443 en Purdue-model segmentation.

Fédèrale Insurance (BE) — Enterprise Security Architect / CISO Advisor
jul 2023 – jul 2024

Belgische onderlinge verzekeraar, onder toezicht van de Nationale Bank van België (BNB).

- ISO 27001-aligned InfoSec-programma verbeterd om aan te sluiten op de toezichtverwachtingen van de BNB (current-state assessment, gap-analyse, remediation plan).
- DORA-verplichtingen geïntegreerd in InfoSec-strategie, roadmap en governance charter — ICT risk, third-party risk, incident reporting en TLPT resilience testing.
- MSSP / SIEM RFP en PoC-supervisie aangestuurd; SIEM/SOC target operating model gebouwd, log onboarding-standaarden, initiële use-case backlog en MSSP-integration design.
- CTEM roadmap (phase 1 implementatie), PAM roadmap met requirements + vendor-selectie, en BAS-programma uitgelijnd op MITRE ATT&CK gedefinieerd.
- Obsolescence & EOL/EOS risk-programma geleid (policy, classificatie, risk register, acceptatie-framework, remediation-roadmap), geïntegreerd met VM en lifecycle management.

Ahold Delhaize (global) — Enterprise / Solution Security Architect / CISO Advisor
aug 2022 – jun 2023

Wereldwijde food retail group; enterprise-scale security architectuur en DevSecOps.

- Enterprise DevSecOps capability model ontworpen: target operating model, secure SDLC baseline, CI/CD control set (SAST / DAST / SCA / secret scanning) en metrics/quality gates.
- Organisatiebreed code review gestandaardiseerd (segregation of duties, branch protections, required checks) met enablement-pakket voor alle developmentteams.
- Zscaler vs. Microsoft E5 tooling-consolidation decision paper opgeleverd; CASB baseline voor Microsoft Defender for Cloud Apps (policies, Conditional Access, SIEM-routing).
- Risk-based vulnerability management operating model gebouwd (RACI, prioritering, reporting/dashboarding) en geconsolideerde control-framework-strategie met ISO/NIST/CIS crosswalk naar één baseline.

Viterra — Enterprise / Solution Security Architect / CISO Advisor mrt 2022 – sep 2022

Wereldwijde landbouwgrondstoffen-trader; mondiale netwerksecurity-transformatie.

- SASE / SSE target architecture opgeleverd, security guardrails voor mondiaal netwerk en vendor decision paper met gefaseerde roadmap.
- Russia IT isolation & segmentation ontworpen als reactie op geopolitiek risico (NAC, air-gapping, operationeel runbook), met behoud van minimale operationele continuïteit voor de mondiale voedselvoorzieningsketen.
- Enterprise security architecture principles catalogue en NFR framework opgebouwd (SABSA / TOGAF + ISO 25010 alignment); OneMessaging security architecture en secure data-exchange portal voor juridische partijen.
- Control-framework optimalisatie naar ISF SoGP afgerond en MITRE ATT&CK / Cyber Kill Chain control heatmap opgeleverd ter ondersteuning van de blue-team strategie.

Aanvullende opdrachten (details op aanvraag): Sequoia (jul 2023 – okt 2025) — Enterprise Security Architect · 10x (mrt 2026 – jul 2026) — Security Consultant · Gerson Lehrman Group (jul 2024 – heden) — IT Security Advisor · Gemeente Purmerend (okt – nov 2023) — Security Consultant · Partners IN Finance (jul 2023 – jul 2024) — Security / IT Consultant · De Voornse Hoeve (mei 2025 – jul 2026) — Security / IT Consultant · Uitmuntent B.V. (mrt 2022 – heden) — IT Advisor & Engineer · Valid Managed Services (sep 2026 – heden) — Solutions Architect (Security), eindklant Vesteda.

LOOPBAAN IN DIENSTVERBAND

nov 2021 – mrt 2022	**KPMG Netherlands** — Senior IT Security Advisor
mrt 2021 – okt 2021	**SimplifyNow** — Security Architect
jul 2020 – feb 2021	**Damen Schelde Naval Shipbuilding** — Cyber Security Lead
okt 2019 – jun 2020	**citizenM** — Information Security Manager
dec 2018 – sep 2019	**Quality** — Security Architect
dec 2012 – nov 2018	**HMSHost International** — Manager Network & Security
mei 2008 – nov 2012	**Icento (Peopleware ICT Solutions)** — Network & Security Consultant
feb 2007 – apr 2008	**Novisource** — Network & Security Specialist
feb 1999 – jan 2007	**Quality & Results (DataBalk)** — Network & Security Specialist → Senior Engineer

BIJ- EN NASCHOLING — CERTIFICERINGEN

Certified Information Systems Security Professional (CISSP) — ISC²	Nr. 77541 · 2005 · geldig tot jul 2029
Certified Cloud Security Professional (CCSP) — ISC²	Nr. 77541 · 2023 · geldig tot okt 2029
Advanced in AI Security Management (AAISM) — ISACA	Gecertificeerd 2026
Certified in Risk and Information Systems Control (CRISC) — ISACA	Gepland
CSA Certificate of Competence in Zero Trust (CCZT)	Gecertificeerd 2026
CSA Certificate of Cloud Security Knowledge (CCSK)	Gecertificeerd 2026
Zero Trust Strategy Certificate — ISC²	Loopt
ISO 27001 Lead Implementer	november 2024
SABSA Chartered Foundation (SCF)	June 2019
ArchiMate Practitioner — The Open Group	december 2022
DevSecOps Professional — CI/CD Security	2023
PCI DSS Internal Security Assessor (ISA)	Nr. 802-090 · 2013 (historical)

Legacy technical foundations spanning many network & security components and services (Cisco CCNP Security, Juniper, Symantec, VASCO, ITIL, PCIP, eCPPT, Prince II, NIST CSF) — full list with certification numbers available on request.

TECHNOLOGIEËN & TOOLS — vendor-agnostisch; praktijkervaring met meerdere stacks per categorie

IDENTITY & ACCESS / ZERO TRUST

Microsoft Entra ID (Conditional Access, PIM, B2B), CyberArk, BeyondTrust, Delinea, HashiCorp Vault, Zscaler ZPA/ZIA/ZDX, Palo Alto Prisma Access, CATO Networks, Aryaka.

DETECTION & RESPONSE / SOC

Microsoft Sentinel, Splunk ES, IBM QRadar, Elastic SIEM, Palo Alto Cortex XSIAM/XSOAR, CrowdStrike Falcon, SentinelOne, Microsoft Defender XDR, Vectra AI, Darktrace, ExtraHop, SecureWorks Taegis.

VULNERABILITY & EXPOSURE MANAGEMENT

Tenable One / Nessus, Qualys VMDR / TruRisk, XM Cyber, Cortex Expanse (EASM), Wiz, Ivanti, Heimdall, Pentera / AttackIQ / SafeBreach (BAS), ServiceNow CMDB, Flexera One.

CLOUD & APPLICATION SECURITY

Microsoft Defender for Cloud Apps, Microsoft Purview, Azure, Microsoft 365 / Exchange Online / SharePoint, CheckMarx, CodeQL / GitHub Advanced Security, Proofpoint / Mimecast, Docker / Kubernetes / AKS, DataDog.

NETWORK SECURITY

Palo Alto NGFW / Panorama, Check Point NGFW, Fortinet FortiGate / Secure SD-WAN, Cisco Firepower / ISE / Meraki, Cloudflare One, Netskope, Azure WAN / DNS, LEO satellite (Starlink / OneWeb).

FRAMEWORKS & METHODOLOGIES

ISO 27001/27002, NIST CSF 2.0, CIS v8, DORA, NIS2 / CBW, GDPR, NIST SP 800-53r5 / 800-37r2, SABSA, TOGAF, ArchiMate, MITRE ATT&CK / D3FEND, TIBER-EU / DORA TLPT, IEC 62443, OWASP, ISF SoGP, SCF.

OPLEIDING, TALEN & LIDMAATSCHAPPEN

OPLEIDING

1999	**HBO — Hogere Informatica (cum laude)** Telematica · Hogeschool 's-Hertogenbosch (HTS)
1995	**MTS — Procesautomatisering** Crabeth College, Gouda
1991	**MAVO** Malsna-MAVO, Geldermalsen

TALEN

Nederlands — moedertaal · Engels — C1, vloeiend in spreken en schrijven (getraind bij Regina Coeli, 2015).

LIDMAATSCHAPPEN

- ISC² — internationale groep & Nederlandse chapter
- ISACA — internationale groep & Nederlandse chapter
- The Open Group — vendor-neutrale technologiestandaarden
- SABSA Institute — Enterprise Security Architecture
- IAPP — International Association of Privacy Professionals (privacy)
- CSA — Cloud Security Alliance (werkgroepen: Zero Trust, Cloud Controls Matrix, IAM, Security Control Catalog)
- Aryaka Technical Advisory Board — SD-WAN & SASE