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+ years in IT & security

Hellevoetsluis, Netherlands · +31 6 11 85 81 03 · info@vaal-consulting.nl · www.vaal-consulting.nl · linkedin.com/in/remcovaal

PROFILE

Principal Security Consultant with 25+ years in IT and information security, including 4 years as an independent consultant — working across enterprise security architecture, solution security architecture, security governance and Security Officer / CISO advisory roles, often for organisations in regulated, critical or complex environments.

A natural integrator who connects regulatory obligations, privacy principles, industry standards and business objectives into coherent, complete and operationally effective security programmes — whether shaping a single project or building an organisation-wide InfoSec programme. Brings genuine passion to the field and explains complex security topics clearly to both engineers and executives, with a focus on enabling the business rather than blocking it.

Actively follows emerging technologies, including AI, and translates them into effective, responsible and future-oriented security approaches. Vendor-agnostic by design — works fluently across multiple vendor stacks per security and network category.

CORE SKILLS

#	CORE SKILL	SCOPE	PRIMARY ROLE(S)
1	**Governance, Policy & Frameworks**	Control frameworks (ISO, NIST, CIS, ISF), policy lifecycle, control mapping & validation, governance structures	CISO, (T)ISO
2	**AI Security & Governance**	AI risk frameworks, EU AI Act alignment, securing AI systems & pipelines, AI threat modeling, responsible AI governance	ESA, CISO, Advisor
3	**Privacy & Data Protection**	GDPR compliance programs, privacy-by-design, DPIA, international data governance, integration with security architecture	(T)ISO, CISO, ESA
4	**Regulatory & Compliance**	DORA, NIS2, PCI DSS, GDPR: gap analysis, obligation mapping, remediation roadmaps	CISO, (T)ISO
5	**Zero Trust & Identity**	Zero Trust strategy, ZTA, IAM/PAM, CASB/MCAS, Conditional Access, identity-first patterns	ESA, SSA
6	**Supplier / Third-Party Assurance**	TPRM, supplier clauses, SOC/ISAE/ISO evidence review, assurance findings management	(T)ISO, CISO
7	**DevSecOps & Secure SDLC**	Secure SDLC, CI/CD controls (SAST/DAST/SCA), code review governance, pipeline hardening	SSA, (T)ISO
8	**Security Architecture & Design**	Target-state architectures, reference patterns, security-by-design, ADRs, design reviews	ESA, SSA
9	**Risk & Decision Support**	Decision papers, options analysis, risk trade-offs, executive advisory, risk acceptance governance	CISO, ESA
10	**Network Security & SASE**	SASE adoption, SD-WAN migration, segmentation, NDR, secure connectivity design	ESA, SSA, Advisor
11	**SOC / SIEM / Detection**	SIEM/SOAR build-out, logging standards, use-case lifecycle, MSSP onboarding, Blue Team strategy	SSA, ESA
12	**Vulnerability Mgmt / CTEM**	CTEM roadmaps, prioritisation models, remediation workflows, operating models & dashboarding	(T)ISO, ESA, SSA
13	**Applied AI & Security Tooling**	Effective and responsible use of AI in security work; AI-assisted analysis, threat modeling, documentation & design; evaluating AI tool risk	ESA, Advisor, CISO

#	CORE SKILL	SCOPE	PRIMARY ROLE(S)
14	**Security Process Design & Optimisation**	Mapping and improving security processes; troubleshooting complex security issues; designing pragmatic, efficient operating models	All roles

SELECTED ACHIEVEMENTS

- Led substantive DORA + NIS2 (Cyberbeveiligingswet) compliance discussions and shaped applicability strategy in relation to the major Dutch banks (Geldmaat — critical national ATM infrastructure).
- Designed Russia IT isolation under acute geopolitical pressure, preserving global food-supply continuity (Viterra).
- Defined an enterprise DevSecOps capability model and standardised organisation-wide secure code review across all development teams (Ahold Delhaize).
- Designed a CTEM / Vulnerability Management roadmap and operating concept (Fédérale Insurance — BNB-supervised Belgian mutual insurer).
- Shaped strategic security architecture using the 9-layer model of Rik Maes, aligning roadmap, governance and stakeholder decisions for a regulated Dutch telecom operator (KPN).

PROFESSIONAL EXPERIENCE — INDEPENDENT CONSULTANT, VAAL CONSULTING B.V. (MAR 2022 – PRESENT)

KPN — Enterprise Security Architect

Aug 2024 – May 2026

Regulated Dutch telecommunications operator.

- Shaped strategic security architecture using the 9-layer model of Rik Maes to drive stakeholder decisions and align initiatives to domains and governance.
- Defined the HLD governance standard (template, security review checklist, ARB integration), improving design quality and consistency across projects.
- Led DORA regulatory advisory across contracts, SLAs, supply chain and documentation; delivered SIAM proposition aligned to DORA Chapter V (third-party ICT risk).
- Produced VM-to-CTEM strategic direction, NDR-as-a-Service viability assessment, supplier assurance evidence-review guidance and GDPR privacy-by-design consultancy.

Geldmaat — Enterprise Security Advisor

Aug 2024 – May 2026

Critical ATM infrastructure operator for the Dutch banking sector.

- Delivered the DORA + NIS2 (Cyberbeveiligingswet) compliance programme: executive framing, obligation mapping, governance structure, phased roadmap and evidence approach.
- Defined a Zero Trust target state and phased roadmap (identity-first, device posture, micro-segmentation, conditional access); contributed to the GAPA architecture board.
- Built a CTEM operating model (RACI, prioritisation by criticality × exploitability × exposure, KPI/KRI dashboarding) replacing a fragmented VM process.
- Produced penetration-testing strategy aligned to DORA TLPT and NIS2/CBW, plus a lifecycle-management framework addressing DORA Art. 8 and NIS2 asset/patch obligations.
- Assessed 72-hour power-outage continuity scenarios for the national ATM network (LEO satellite / dark-fibre fallback, diesel dependency, prioritisation).

NS — Dutch Railways — Solution Security Architect

Jul 2025 – Jan 2026

National rail operator, SDI (Software-Defined Infrastructure) domain — OT / IT boundary.

- Designed the VM / CTEM operating model for the SDI domain (RACI, SLAs, risk-based prioritisation, reporting and exception handling).
- Built an NFR library and security requirements-engineering standard with traceability to the control framework and supplier intake questionnaire.
- Mapped internal + supplier framework to CIS Controls v8.2 for unified reporting; produced a modular vs. siloed architecture decision paper.
- Delivered regulatory advisory across NIS2/CBW, DORA, PCI DSS and GDPR with control-to-obligation traceability, plus pen-test governance aligned to TIBER-EU / DORA TLPT.

(Confidential) — Dutch Army — Enterprise Security Architect / Advisor

Dec 2024 – Jul 2025

Defence environment; mission-critical OT / IT in a classified operational context.

- Advised on NIST RMF alignment: SP 800-53r5 control validation and SP 800-37r2 RMF implementation (SSP structure, ATO process, FIPS 199 categorisation).
- Defined a Zero Trust target architecture and phased roadmap (identity-first, device posture, segmentation, conditional access, ZTNA/PAM/Entra tooling guidance).
- Produced the Battle Management System security reference architecture applying defence-in-depth, IEC 62443 and Purdue-model segmentation.

Fédèrale Insurance (BE) — Enterprise Security Architect / CISO Advisor

Jul 2023 – Jul 2024

Belgian mutual insurer, supervised by the National Bank of Belgium (BNB).

- Drove ISO 27001-aligned InfoSec programme improvement to meet BNB supervisory expectations (current-state assessment, gap analysis, remediation plan).
- Integrated DORA obligations into InfoSec strategy, roadmap and governance charter — ICT risk, third-party risk, incident reporting and TLPT resilience testing.
- Managed MSSP / SIEM RFP and PoC oversight; built the SIEM / SOC target operating model, log-onboarding standards, use-case backlog and MSSP integration design.
- Defined a CTEM roadmap (phase 1), a PAM roadmap with requirements + vendor selection, and a BAS programme aligned to MITRE ATT&CK; led the obsolescence & EOL/EOS risk programme.

Ahold Delhaize (global) — Enterprise / Solution Security Architect / CISO Advisor

Aug 2022 – Jun 2023

Global food-retail group; enterprise-scale security architecture and DevSecOps.

- Designed an enterprise DevSecOps capability model: target operating model, secure SDLC baseline, CI/CD control set (SAST / DAST / SCA / secret scanning), metrics and quality gates.
- Standardised organisation-wide code review (segregation of duties, branch protections, required checks) with an enablement package for all development teams.
- Produced a Zscaler vs. Microsoft E5 tooling-consolidation decision paper and a CASB baseline for Microsoft Defender for Cloud Apps.
- Built a risk-based VM operating model and a consolidated control-framework strategy with an ISO/NIST/CIS crosswalk to a single baseline.

Viterra — Enterprise / Solution Security Architect / CISO Advisor

Mar 2022 – Sep 2022

Global agricultural-commodities trader; global network-security transformation.

- Delivered a SASE / SSE target architecture, security guardrails for global networking and a vendor decision paper with phased roadmap.
- Designed Russia IT isolation & segmentation in response to geopolitical risk (NAC, air-gapping, operational runbook) while preserving minimum operational continuity.
- Built an enterprise security-architecture principles catalogue and NFR framework (SABSA / TOGAF + ISO 25010); produced a MITRE ATT&CK / Cyber Kill Chain control heatmap driving blue-team strategy.

Additional engagements (details on request): 10x (Mar 2026 – present, Security Consultant) · Gerson Lehrman Group (Jul 2024 – present, IT Security Advisor) · Sequoia (Jul 2023 – Oct 2025, Enterprise Security Architect) · De Voornse Hoeve (May 2025 – present, Security / IT Consultant) · Partners IN Finance (Jul 2023 – Jul 2024, Security / IT Consultant) · Gemeente Purmerend (Oct – Nov 2023, Security Consultant) · Uitmuntent B.V. (Mar 2022 – present, IT Advisor & Engineer).

EMPLOYMENT HISTORY

Nov 2021 – Mar 2022	**KPMG Netherlands** — Senior IT Security Advisor
Mar 2021 – Oct 2021	**SimplifyNow** — Security Architect
Jul 2020 – Feb 2021	**Damen Schelde Naval Shipbuilding** — Cyber Security Lead
Oct 2019 – Jun 2020	**citizenM** — Information Security Manager
Dec 2018 – Sep 2019	**Quality** — Security Architect
Dec 2012 – Nov 2018	**HMSHost International** — Manager Network & Security
May 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

PROFESSIONAL DEVELOPMENT — CERTIFICATIONS

Certified Information Systems Security Professional (CISSP) — ISC²	No. 77541 · 2005 · valid till Jul 2029
Certified Cloud Security Professional (CCSP) — ISC²	No. 77541 · 2023 · valid till Oct 2029
Advanced in AI Security Management (AAISM) — ISACA	Certified 2026
Certified in Risk and Information Systems Control (CRISC) — ISACA	Planned
CSA Certificate of Competence in Zero Trust (CCZT)	Certified 2026
CSA Certificate of Cloud Security Knowledge (CCSK)	Certified 2026
Zero Trust Strategy Certificate — ISC²	In progress
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)	No. 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.

TECHNOLOGIES & TOOLS — vendor-agnostic; real project exposure across multiple stacks per category

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.

EDUCATION, LANGUAGES & MEMBERSHIPS

EDUCATION

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

LANGUAGES

Dutch — mother tongue · English — C1, fluent spoken & written (trained at Regina Coeli, 2015).

PROFESSIONAL MEMBERSHIPS

- ISC² — international group & Dutch chapter
- ISACA — international group & Dutch chapter
- The Open Group — vendor-neutral technology standards
- SABSA Institute — Enterprise Security Architecture
- IAPP — International Association of Privacy Professionals
- CSA — Cloud Security Alliance (working groups: Zero Trust, Cloud Controls Matrix, IAM, Security Control Catalog)
- Aryaka Technical Advisory Board — SD-WAN & SASE