SKOPION INTELLIGENCE

SERVICE PARTNER FOR AGENCIES & IT PROVIDERS

As of: November 2026 · Reference: SKP-PARTNER-2026-11

# Engineering & IT security capacity in a white-label model

SKOPION Intelligence delivers clearly scoped technical work packages for software houses, digital agencies, IT service providers (Systemhäuser), advisers, and prime contractors: full-stack engineering, German e-invoicing (E-Rechnung), cloud & DevSecOps, independent security verification, and compliance readiness. Strictly remote across Germany, DACH, and the EU.

## PARTNERSHIP PRINCIPLE Two roles, strictly separated

**Either implementation or independent verification: never both roles in the same client project.** Client ownership, commercial relationship, and follow-on business stay with the partner. Where no personal data is processed, full white-label delivery applies; otherwise we act transparently as a sub-processor (Art. 28(2) GDPR) under non-circumvention and NDA.

### Role A · Delivery capacity (white-label)

We execute well-defined work packages within the partner project: software development, integrations, infrastructure, or DevSecOps. Direct coordination with your team and clean handover with documentation.

### Role B · Independent verification (four-eyes principle)

We verify applications, APIs, and infrastructure built by the partner team or third parties. Findings and remediation guidance go to your team, followed by a retest after fixes.

## WHO WE SUPPORT Typical partners

### Software houses & digital agencies

Engineering capacity, integrations, WCAG/BFSG delivery, and pre-launch security checks.

### IT service providers (Systemhäuser)

Infrastructure hardening, independent verification for cyber insurers, and audit evidence.

### NIS2, ISO & DPO advisers

Technical evidence, SBOM/CSAF artefacts, and testing without competing for DPO mandates or advisory contracts.

### Prime contractors & consortia

Clearly scoped work packages in delivery and EU R&D projects (PIC 861665939).

## SERVICES · ROLE A Engineering & implementation

MODULE 01

### Full-stack apps, portals & desktop

- Client portals, internal tools, custom line-of-business systems, and desktop apps.
- Rust, Python/FastAPI, TypeScript/Next.js, React, PHP/Laravel, Python/Qt; PostgreSQL, Redis.
- Accessible interfaces aligned with WCAG/BFSG and clearly documented APIs.

skopion.de/en/secure-softwareentwicklung

MODULE 02

### APIs, integrations, e-commerce & E-Rechnung

- REST/GraphQL APIs, webhooks, system integrations, and role/access models (OAuth2/OIDC).
- WordPress/WooCommerce, Shopware, plus payment and supply-chain integrations.
- German E-Rechnung: XRechnung, ZUGFeRD (EN 16931), KoSIT validation, and technical GoBD support.

skopion.de/en/services

MODULE 03

### Modernisation, refactoring & migration

- Incremental stabilisation and migration of existing applications without downtime.
- Legacy systems (Delphi, VB6, COM, .NET), FoxPro/Paradox/Btrieve databases, and DATEV formats (1:1 migration).
- Technical reconstruction and migration blueprints even without available source code.

skopion.de/en/legacy-system-analysis

MODULE 04

### Infrastructure, cloud & hardening

- Linux and Windows Server, Active Directory/Entra ID, network segmentation, and access control.
- Firewalls, VPNs, encrypted backups, and isolated mail services.
- AWS, Google Cloud, Azure, Kubernetes/Helm, Terraform, Cloudflare Workers/R2.

skopion.de/en/services

MODULE 05

### DevSecOps, CI/CD gates & handover

- Security, quality, and WCAG/BFSG checks enforced as automated CI/CD gates.
- Code and dependency analysis, build-time SBOM/CSAF/VEX generation, and CVE backport verification.
- Repeatable zero-downtime deployments, monitoring, and technical handover documentation.

skopion.de/en/services

MODULE 06

### AI workflows, MCP & data architectures

- RAG pipelines and multi-agent workflows with controlled data and permission boundaries.
- Multi-model routing and runtime guardrails preventing unintended data leakage.
- Custom MCP servers and tool bridges (ChatGPT/Codex, Claude, Gemini); sovereign EU LLM gateways.

skopion.de/en/services

## SELECTED TECHNOLOGIES & STANDARDS

Rust · Python / FastAPI · Python / Qt · TypeScript / Next.js · React · Node.js · PHP / Laravel · PostgreSQL / MySQL / SQLite · Redis · Qdrant · MinIO · Docker · Kubernetes / Helm · Terraform · AWS / Google Cloud / Azure · Cloudflare Workers / R2 · Linux · Windows Server · Active Directory / Entra ID · WireGuard / OpenVPN · GitHub Actions · Gitea CI/CD · n8n · OWASP ZAP · Trivy · DefectDojo · CycloneDX / SPDX / OpenVEX · CSAF 2.0 · XRechnung / ZUGFeRD · OAuth2 / OIDC · HashiCorp Vault · LiteLLM · MCP · RAG · PyTorch · XRPL · Solana · Monero · EVM / Solidity

## SERVICES · ROLE B Security verification & compliance

MODULE 07

### Penetration testing & application security

- Manually verified testing across web apps, APIs, Active Directory, and AI workflows per OWASP ASVS.
- Authentication, authorisation, and business-logic flaws (IDOR/BOLA, tenant isolation, session fixation).
- Executive summary, evidence-backed technical report, and one retest after remediation.

skopion.de/en/penetration-testing

MODULE 08

### Security review & attack surface

- Structured review of M365/Entra ID, mail security, backups, and external attack surface.
- Review of mail, domain and DNS hardening (SPF/DKIM/DMARC/DNSSEC/CAA) and phishing resilience.
- Technical evidence for ISO 27001, BSI IT-Grundschutz, and cyber insurance questionnaires; CVE backport checks.

skopion.de/en/it-security-check
skopion.de/en/check

MODULE 09

### OSINT, brand abuse & dark-web exposure

- Early detection of lookalike domains, counterfeit storefronts, and brand impersonation.
- Passive leak and exposure indicators without storing plaintext credentials.
- Technical investigations with evidence packages, IOC reports, and takedown requests.

skopion.de/en/brand-abuse-phishing

MODULE 10

### NIS2, DORA readiness & incident playbooks

- Technical risk assessment and evidence for NIS2 (Art. 21 / § 30 BSIG DE), DORA ICT resilience, and supply chains.
- Reporting workflows (24 h / 72 h) and practical business continuity playbooks.
- Versioned gap analyses and evidence registers via the NIS2Steps portal.

skopion.de/en/nis2-readiness · nis2steps.eu

MODULE 11

### EU CRA, SBOM, CSAF & zero-source

- Technical pre-assessment of scope and product classes, Art. 14 CRA reporting support, and CSAF 2.0.
- Review of SBOM and VEX (CycloneDX, SPDX, OpenVEX) and their integration into CI/CD pipelines.
- Binary SBOM for legacy systems without source code; CRASteps compliance portal.

skopion.de/en/cra-readiness · crasteps.eu

MODULE 12

### EU AI Act & AI security review

- Technical support on system classification, transparency, and technical documentation (non-legal scope).
- Testing of chatbots, assistants, and AI agents: prompt injection, model artefact scanning, tool controls.
- AIActSteps portal for evidence tracking and remediation roadmaps.

skopion.de/en/ai-security-check
aiactsteps.eu

*Role B strictly covers independent technical verification and evidence preparation; it excludes legal advice (German RDG) and formal ISO/BSI certification.*

## COMPLEMENTARY Prevention & triage support

**Awareness & GDPR readiness**
Phishing recognition training and technical data-protection fundamentals for partner and client teams.

**Secure communications**
Rollout of end-to-end encryption, PGP correspondence workflows, and post-quantum cryptography (PQC).

**Initial incident triage**
Structured first-line assessment of suspicious emails, headers, domains, IP indicators, and log excerpts.

**Blockchain transaction tracing**
Assessment of public on-chain trails, flow analysis, and technical documentation of next steps.

## COLLABORATION Contract models & delivery process

### Subcontracting & white-label

B2B subcontracting agreement with the partner as prime contractor: NDA, non-circumvention, and DPA/AVV (Art. 28 GDPR). Processing in DE/EU, personal delivery by a senior engineer (no junior delegation) in scoped packages (no 24/7 ops); fixed price, time & materials, or retainer.

### Direct end-client mandate

The end client contracts SKOPION directly (self-performed without subcontractors or freelancers), while the partner handles implementation and operations separately. Only this model qualifies for NRW MID-Digitale Sicherheit for NRW SMEs (§ 4.3 excludes subcontracts and freelancers; min. €8,000 net threshold, monthly NRW.BANK lottery, 28-day filing window, approval required before project start, no grant guarantee).

STEP 01

**Short scoping call**
15 minutes covering objectives, work package or private pilot (1 to 3 days), and role separation (A or B).

STEP 02

**Scope, NDA & DPA/AVV**
Bounded work scope, contract model, DPA/AVV (Art. 28 GDPR), non-circumvention, and confidentiality terms.

STEP 03

**Delivery / verification**
Strictly remote, inside partner repositories and CI/CD, EU processing, zero disruption to live production.

STEP 04

**Handover & retest**
Complete source handover without vendor lock-in, documentation or evidence-backed report, plus retest.

## PLATFORM ENGINEERING — Engineering depth proven across in-house systems

### EASM & OSINT platforms

External attack-surface assets, DNS/TLS/CT telemetry, and vulnerability feeds correlated into structured dossiers.

### German E-Rechnung, GoBD & desktop

XRechnung, ZUGFeRD (EN 16931), KoSIT validation, append-only SHA-256 audit logs, and Python/Qt desktop apps.

### SaaS billing & multi-tenant

Recurring billing, HMAC-signed webhooks with retry handling, PostgreSQL RLS isolation, and scoped API keys.

### Multilingual AI assistants & RAG

Qdrant vector stores, multi-provider LLM routing, strict tenant isolation, and enforced security guardrails.

### Transactional Rust backends

Axum, SQLx, Redis: event sourcing, strict idempotency, dead-letter queues, and fault-resilience testing.

### Reverse engineering & recovery

Native binaries, .NET/JVM, Android/iOS, Web/JS, and firmware; clean reconstruction with Z3 equivalence proofs.

### OT, legacy systems & migration

PROFINET, EtherCAT, S7comm, OPC-UA, PLCs; FoxPro, Paradox, Btrieve databases, and DATEV exports with PII anonymisation.

### PHP, Laravel & WordPress plugins

Laravel/Filament admin panels with secrets vaults; WP plugins covering WAF, scanners, 2FA, content protection, TDM rules, and signed updates.

### Multi-agent AI & LLM gateways

Sandboxed agent orchestration, prompt-injection filters, model artefact scanning, and EU-hosted LiteLLM routing.

### Fuzzing & evidence-based checks

libFuzzer, AFL++, cargo-fuzz, Jazzer; CVE backport verification, OOB canary tokens, and differential HTTP analysis.

### Zero-Knowledge vaults & WebCrypto

Client-side AES-256-GCM encryption, SCRAM-SHA-256 auth, threshold signatures, and air-gapped HTML recovery.

### Cloudflare fleets, Edge R2 & mail

Multi-domain WAF/DNS fleets, Workers, EU R2 zero-copy failover, Origin CA, and isolated Postfix, Dovecot, OpenDKIM, Sieve stacks.

### Low-level software & edge

System services and device drivers in Rust (USB HID, hardware telemetry); Android apps with media pipelines (ExoPlayer, FFmpeg) and SQLite FTS.

### MCP bridges, Voice AI & federation

Custom MCP servers (IMAP/OAuth mail with send guard, file gateways, DACH registries), Voice AI, and self-hosted nodes (AT Protocol, ActivityPub).

### Data pipelines, FinTech & registries

Open-data and IoT collectors (OGC SensorThings), TCO and energy engines (ECB, Eurostat), and EU registries including Safety Gate.

### Self-hosted Kubernetes & CI/CD

Helm and Terraform with mTLS, NetworkPolicy, KMS signing, trust rotation, and WCAG/BFSG plus CSAF/SBOM gates in SARIF.

## CRYPTOGRAPHY & BLOCKCHAIN — Cryptographic engineering & blockchain settlement

### XRP Ledger & settlement

Client platform engineering: token escrow, batch DvP, checks, payment channels, RWA; 2-of-3 multisig vaults, API connectors for OFAC/Travel Rule screening, and ISO 20022 formats.

### Non-custodial payment flows

Zero-custody architecture (including RPC integrations for Monero and UTXO chains): unique subaddress per invoice, view-key detection, confirmations, and reorg buffer.

### Multi-chain verification

EVM network integrations and state reads (Ethereum, Base, Arbitrum, USDC) plus Solana via JSON-RPC; smart-contract reviews (Solidity, Foundry).

### Cryptography, signatures & forensics

Multi-chain transaction flow analysis, privacy-exposure assessment, Ed25519 signatures, and post-quantum schemes (ML-DSA).

## CONTACT & EXPERIENCE — Lead engineer & project track record

### Bartosz Joachimiak

**PRINCIPAL & LEAD ENGINEER**

Over 20 years of hands-on practice across IT and electronics (from marine systems and infrastructure to platforms and secure code); personal execution from backend to hardening. English, German, Polish.

- Authorised web/API testing (CVD, BSI CERT-Bund); ISSA International member; IHK/DIHK contribution (healthcare cyber resilience).
- OSS contribution to OWASP DSOMM; EU Funding & Tenders candidate (EX2026D1528552, no EC contract); ORCID 0009-0002-1713-9490 · DOI 10.5281/zenodo.24295340.
- Non-commercial R&D: RWTH (WestAI), Jülich (JUPITER), GWDG (KISSKI); Fraunhofer FKIE (Malpedia) & CESNET (NERD).

Contact: bj@skopion.de · skopion.de/en/legal-notice · Signal/PGP
Mönchengladbach (NRW, DE) · Sole proprietorship · VAT ID DE297106209

**PROJECT TRACK RECORD (ANONYMISED)**

- **Rail sector supplier (KRITIS supply chain, DE)**, 2026: network segmentation, gateway and access hardening, encrypted backups.
- **FTTH fibre infrastructure contractor (DE)**, 2025: FTTH data engineering, Python automation, Linux hardening.
- **Global pharmaceutical group (Switzerland)**, 2024 to 2025: remote infrastructure engineering.
- **European OEM integrators: workstations, high-performance & mobile IPC systems (DACH)**, 2008 to 2025: firmware and driver engineering (hardware-software integration), multi-tenant hosting, e-commerce, and payment integrations.

## CREDENTIALS — Industry certifications & completed training tracks

**CERTIFICATIONS**

### Security & networking

- **Qualys Certified Specialist**: TotalAppSec, VMDR, CSAM.
- **Fortinet NSE 3** (Cybersecurity) plus FortiGate 7.6 Operator training.
- **Cisco NetAcad**: Ethical Hacker track (pentesting & assessment).
- **Red Team & DFIR**: Hack Smarter, HTB Academy, CyberDefenders.

**INDUSTRIAL & EU**

### OT/ICS & EU agencies

- **CISA / INL ICS**: complete industrial track (100W, 210W, 300, 401).
- **ENISA**: Zero Trust, Cyber Threat Management, ITSRM.
- **AttackIQ**: Purple Teaming, Threat-Informed Architecture.

**SUPPLY CHAIN**

### CRA, OpenSSF & cloud AI

- **Linux Foundation / OpenSSF**: EU CRA, SBOM, Sigstore, Scorecard, Secure Software, AI/ML, OSS licensing.
- **Google Cloud, Anthropic, OpenAI**: Model Armor, ADK & MCP, SCC, Codex & API.
- **Digital Product Passports (DPP)**: PFR track (ESPR/EU alignment).

**FORENSICS**

### OSINT & financial analysis

- **Basel Institute on Governance**: OSINT plus Visualise Cases & Flows of Money.
- **IFC / World Bank**: Trade-Based Money Laundering (TBML).
- **World Bank Group Institute**: metadata documentation standards.

## PRODUCTS & RESEARCH — In-house products, portals & R&D initiatives

**PRODUCT**

### Zero-LLM Website Assistant

Deterministic assistant with zero runtime LLM: answers strictly from verified sources; deployable as container, REST bridge, or air-gapped image.

skopion.de/en/zero-llm-assistant

**SERVICE**

### Legacy & zero-source CRA

Reconstruction of legacy systems and firmware, OT protocol audits, and binary SBOMs with cryptographic compliance proofs.

skopion.de/en/legacy-system-analysis

**PORTALS**

### NIS2Steps, CRASteps & AIActSteps

Versioned gap-analysis reports, encrypted evidence registers, and remediation plans for NIS2, EU CRA, and EU AI Act.

nis2steps.eu · crasteps.eu · aiactsteps.eu

**RISK MONITORING**

### Kommunal-Radar & Standort-Atlas

Continuously updated public overviews of external attack surfaces across municipalities, regions, and enterprises.

skopion.de/en/regional-cyber-atlas

**OPEN SOURCE**

### VersionSec

Python CLI inspecting Gitea/Forgejo instances for version hygiene, known CVEs, and hardening, with SARIF output for CI pipelines.

versionsec.com · PyPI

**SUPPLY CHAIN**

### zkBOM

Zero-Knowledge proofs (STARK, WASM verifier) for SBOM, CBOM, and AI-BOM; ML-DSA and Ed25519 signatures, RFC 3161 timestamps, and product passport.

zkbom.com

**RESEARCH**

### Power-SCADA resilience

Formal safety verification of switching operations under coupled power-grid and SCADA contingencies.

skopion.de/en/research-innovation

**RESEARCH**

### Defensive AI & evidence

Neuro-symbolic scoring of passive risk indicators, CEGIS loop, conformal calibration; BSFZ R&D certificate (2026) for in-house research; non-commercial compute on RWTH / JSC / GWDG.

skopion.de/en/trust · Zenodo DOI

**KNOWLEDGE & SAMPLES**

### Case studies & templates

Analyses of real-world fraud and phishing cases, CRA/NIS2 guides, and open KoSIT-validated XRechnung/ZUGFeRD templates.

skopion.de/en/case-studies · GitHub

**Fast-track partnership onboarding (reply within 24 business hours)**

Brief 15-minute scoping call on role (A or B), scoped work package, or private pilot (1 to 3 days). Domestic German invoicing or intra-EU B2B reverse charge.

**Direct contact**
bj@skopion.de
skopion.de/en/services
Signal / PGP key on request



**PARTNER NOTICE & LEGAL DISCLAIMER:** Non-binding partner capability brief (forwarding to prospective end clients permitted; mutual NDA and non-circumvention executed prior to project data exchange on request). The BSFZ Seal certifies R&D activity of companies holding at least one positive certificate from Bescheinigungsstelle Forschungszulage (BSFZ); it applies solely to SKOPION in-house research (passive SME cyber-risk analysis, certificate dated 05.11.2026) and does **not** constitute an audit, approval, or quality certification of client services (such as pentesting, CRA/SBOM readiness, or software engineering). No legal advice (German RDG); no guarantee of lottery selection or grant approval.