Engineering- und IT-Sicherheitskapazität im White-Label-Modell

SKOPION Intelligence liefert klar abgegrenzte Arbeitspakete für Softwarehäuser, Digitalagenturen, IT-Systemhäuser, Berater und Generalunternehmer: Full-Stack-Entwicklung, E-Rechnung DE, Cloud & DevSecOps, unabhängige Sicherheitsprüfung und Compliance-Readiness. Ausschließlich remote, in Deutschland, der DACH-Region und der gesamten EU.

PARTNERSCHAFTSPRINZIP Zwei Rollen, sauber getrennt

Entweder Umsetzung oder unabhängige Prüfung: niemals beide Rollen im selben Kundenprojekt. Kundenbeziehung, Angebotshoheit und Folgegeschäft verbleiben beim Partner. Ohne Personenbezug im vollen White-Label-Modell; bei personenbezogenen Daten offen als Unterauftragsverarbeiter (Art. 28 Abs. 2 DSGVO) mit Kundenschutz und NDA.

Rolle A · Umsetzungskapazität (White-Label)

Wir übernehmen definierte Arbeitspakete im Partnerprojekt: Entwicklung, Integrationen, Infrastruktur oder DevSecOps. Direkte Abstimmung mit dem Partnerteam und saubere Übergabe inklusive Dokumentation.

Rolle B · Unabhängige Prüfung (Vier-Augen-Prinzip)

Wir prüfen Anwendungen, Schnittstellen und Infrastruktur, die vom Partnerteam oder Dritten entwickelt wurden. Befunde und Empfehlungen gehen an das Partnerteam; nach Behebung folgt ein Retest.

ZIELGRUPPE Typische Partner

Softwarehäuser & Digitalagenturen
Entwicklungskapazität, Integrationen, WCAG/BFSG-Umsetzung und Sicherheitsprüfung vor Go-Live.

IT-Systemhäuser
Infrastruktur-Hardening, unabhängige Verifikation für Versicherer und Audit-Nachweise.

NIS2-, ISO- & DSB-Berater
Technische Nachweise, SBOM/CSAF und Tests ohne Wettbewerb um DSB-Mandate oder Beratungsverträge.

Generalunternehmer & Konsortien
Abgegrenzte Arbeitspakete in Projekten, inklusive EU-FuE-Konsortien (PIC 861665939).

LEISTUNGEN · ROLLE A Engineering & Umsetzung

MODUL 01

Full-Stack-Apps, Portale & Desktop

- Kundenportale, interne Werkzeuge, Fachanwendungen und Desktop-Software.
- Rust, Python/FastAPI, TypeScript/Next.js, React, PHP/Laravel, Python/Qt; PostgreSQL, Redis.
- Barrierearme Oberflächen (WCAG/BFSG) und sauber dokumentierte APIs.

skopion.de/de/secure-softwareentwicklung

MODUL 02

APIs, Integrationen, E-Commerce & E-Rechnung

- REST-/GraphQL-APIs, Webhooks, Systemintegrationen sowie Rollen- und Rechtemodelle (OAuth2/OIDC).
- WordPress/WooCommerce, Shopware, Zahlungs- und Lieferketten-Anbindungen.
- E-Rechnung DE: XRechnung, ZUGFeRD (EN 16931), KoSIT-Validierung und technische GoBD-Unterstützung.

skopion.de/de/leistungen

MODUL 03

Modernisierung, Refactoring & Migration

- Schrittweise Stabilisierung und Migration bestehender Anwendungen ohne Betriebsunterbrechung.
- Legacy-Systeme (Delphi, VB6, COM, .NET), FoxPro/Paradox/Btrieve-Datenbanken und DATEV-Formate (1:1-Migration).
- Technische Rekonstruktion und Migrationspläne auch ohne verfügbaren Quellcode.

skopion.de/de/legacy-system-analyse

MODUL 04

Infrastruktur, Cloud & Hardening

- Linux- und Windows-Server, Active Directory/Entra ID, Netzwerksegmentierung und Zugriffskontrolle.
- Firewalls, VPN, verschlüsselte Backups sowie isolierte E-Mail-Infrastruktur.
- AWS, Google Cloud, Azure, Kubernetes/Helm, Terraform, Cloudflare Workers/R2.

skopion.de/de/leistungen

MODUL 05

DevSecOps, CI/CD-Gates & Übergabe

- Sicherheits-, Qualitäts- und WCAG/BFSG-Prüfungen als feste Quality Gates in der CI/CD-Pipeline.
- Code- und Abhängigkeitsanalyse, SBOM/CSAF/VEX im Build-Prozess sowie CVE-Backport-Prüfung.
- Reproduzierbare Deployments ohne Ausfallzeit, Monitoring und technische Dokumentation.

skopion.de/de/leistungen

MODUL 06

KI-Workflows, MCP & Datenarchitekturen

- RAG-Systeme und Multi-Agent-Workflows mit kontrolliertem Daten- und Berechtigungsfluss.
- Multi-Modell-Routing und Laufzeit-Schutzmechanismen gegen Datenabfluss.
- Eigene MCP-Server und Tool-Bridges (ChatGPT/Codex, Claude, Gemini); souveräne LLM-Gateways in der EU.

skopion.de/de/leistungen

AUSGEWÄHLTE TECHNOLOGIEN UND 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

LEISTUNGEN · ROLLE B Sicherheitsprüfung & Compliance

MODUL 07

Penetrationstests & AppSec-Prüfung

- Manuell verifizierte Tests für Web, API, Active Directory und KI-Workflows nach OWASP ASVS.
- Fehler in Authentifizierung, Autorisierung und Geschäftslogik (IDOR/BOLA, Mandantentrennung, Session-Fixation).
- Executive Summary, Bericht mit Nachweisen und ein Retest nach Fehlerbehebung.

skopion.de/de/penetrationstest

MODUL 08

Sicherheitsprüfung & Angriffsfläche

- Strukturierte Prüfung: M365/Entra ID, E-Mail, Backups und externe Angriffsfläche.
- Prüfung der Mail-, Domain- und DNS-Härtung (SPF/DKIM/DMARC/DNSSEC/CAA) sowie der Phishing-Resistenz.
- Technische Nachweise für ISO 27001, BSI IT-Grundschutz und Versicherer-Fragebögen; CVE-Backport-Prüfung.

skopion.de/de/it-sicherheitscheck
skopion.de/de/check

MODUL 09

OSINT, Markenschutz & Darknet-Exposition

- Früherkennung von Lookalike-Domains, Fake-Shops und Markenmissbrauch.
- Passive Leak- und Expositionsindikatoren ohne Klartext-Passwort-Vorhaltung.
- Technische Ermittlung mit Beweispaket, IOC-Meldungen und Takedown-Anträgen.

skopion.de/de/markenmissbrauch-phishing

MODUL 10

NIS2-, DORA-Readiness & Notfallplan

- Technische Risikoanalyse und Nachweise für NIS2 (Art. 21 / § 30 BSIG), DORA (IKT-Resilienz) und Lieferkette.
- Meldewege (24 h / 72 h) sowie praxistaugliche Notfall- und Wiederanlaufpläne.
- Versionierte Gap-Analysen und Nachweisregister im Portal NIS2Steps.

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

MODUL 11

EU CRA, SBOM, CSAF & Zero-Source

- Technische Vorbewertung von Scope und Produktklassen, Unterstützung bei Meldeprozessen (Art. 14 CRA) und CSAF 2.0.
- Prüfung von SBOM und VEX (CycloneDX, SPDX, OpenVEX) sowie ihrer Einbindung in CI/CD-Pipelines.
- Binär-SBOM für Legacy-Systeme ohne Quellcode; Nachweisportal CRASteps.

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

MODUL 12

EU AI Act & KI-Sicherheitscheck

- Technische Unterstützung bei Klassifizierung, Transparenz und Dokumentationspflichten (ohne Rechtsberatung).
- Prüfung von Chatbots, Assistenten und KI-Agenten: Prompt Injection, Modell-Artefakt-Scan, Tool-Kontrolle.
- AIActSteps-Portal für Nachweisdokumentation und Maßnahmenpläne.

skopion.de/de/ki-sicherheitscheck
aiactsteps.eu

Rolle B umfasst ausschließlich unabhängige technische Prüfung und Nachweisvorbereitung, ohne Rechtsberatung (RDG) und ohne formale ISO-/BSI-Zertifizierung.

ERGÄNZEND Prävention & Unterstützung

Awareness & DSGVO-Grundlagen

Phishing-Schulungen sowie technische Datenschutz-Grundlagen für Partnerteams und Endkunden.

Sichere Kommunikation

Einführung von Ende-zu-Ende-Verschlüsselung, PGP-Korrespondenz und Post-Quanten-Kryptografie (PQC).

Ersteinschätzung bei Vorfällen

Strukturierte Erst-Triage verdächtiger E-Mails, Header, Domains, IP-Adressen und Log-Auszüge.

Blockchain-Transaktionsanalyse

Auswertung öffentlicher Blockchain-Spuren (Tracing), Mittelfluss-Analyse und Dokumentation weiterer Schritte.

ZUSAMMENARBEIT Vertragsmodelle & Projektablauf

Subunternehmer & White-Label

B2B-Subunternehmervertrag mit dem Partner als Generalunternehmer: NDA, Kundenschutz und AVV / Unterauftragsverarbeitung (Art. 28 DSGVO). Verarbeitung in DE/EU, persönliche Umsetzung durch einen erfahrenen Lead Engineer (ohne Delegation an Junior-Entwickler) in definierten Paketen (kein 24/7-Betrieb); Festpreis, Time & Material oder Retainer.

Direktauftrag durch Endkunden

Der Endkunde beauftragt SKOPION direkt (Eigenleistung ohne Subunternehmer oder Freelancer), der Partner übernimmt Umsetzung und Betrieb separat. Nur dieses Modell erfüllt die Vorgaben von MID-Digitale Sicherheit für KMU in NRW (§ 4.3 schließt Unteraufträge und Freelancer aus; ab 8.000 EUR netto, monatliche Auslosung über NRW.BANK, 28 Tage Antragsfrist, Bewilligung vor Projektstart, ohne Rechtsanspruch auf Förderung).

SCHRITT 01

Kurzes Abstimmungsgespräch

15 Minuten zu Zielbild, Paketumfang oder privatem Pilotprojekt (1 bis 3 Tage) und Rollentrennung (A oder B).

SCHRITT 02

Scoping, NDA & AVV

Abgegrenzter Leistungsumfang, Vertragsmodell, AVV (Art. 28 DSGVO), Kundenschutz und Vertraulichkeit.

SCHRITT 03

Umsetzung / Prüfung

Ausschließlich remote, im Repository und CI/CD des Partners, Verarbeitung in der EU, ohne Produktionsstörung.

SCHRITT 04

Übergabe & Retest

Vollständige Code-Übergabe ohne Vendor Lock-in, Dokumentation oder Prüfbericht mit Nachweisen sowie Retest.

PLATTFORM-KOMPETENZEN Technologische Tiefe aus eigener Produktentwicklung

EASM- & OSINT-Plattformen

Externe Assets, DNS/TLS/CT und Schwachstellen-Feeds korreliert in konsistente Vorfalls-Dossiers.

E-Rechnung DE, GoBD & Desktop

XRechnung, ZUGFeRD (EN 16931), KoSIT-Validierung, unveränderliches SHA-256-Audit-Log (append-only) und Python/Qt-Apps.

SaaS-Billing & Multi-Tenant

Wiederkehrende Abrechnung, HMAC-signierte Webhooks mit Retry, PostgreSQL-RLS-Trennung und API-Schlüssel.

Mehrsprachige KI-Assistenten & RAG

Qdrant-Vektordatenbanken, Multi-Provider-LLM-Routing, Mandanten-Isolation und durchgesetzte Sicherheits-Guardrails.

Transaktionale Rust-Backends

Axum, SQLx, Redis: Event Sourcing, strikte Idempotenz, Dead-Letter-Queues und Ausfallsicherheits-Tests.

Reverse Engineering & Rekonstruktion

Native Binaries, .NET/JVM, Android/iOS, Web/JS und Firmware; Rekonstruktion mit Z3-Äquivalenznachweis.

OT, Legacy-Systeme & Migration

PROFINET, EtherCAT, S7comm, OPC-UA, SPS; FoxPro-, Paradox- und Btrieve-Datenbanken sowie DATEV mit PII-Anonymisierung.

PHP, Laravel & WordPress-Plugins

Laravel/Filament-Panels mit Secrets Vault; WP-Plugins: WAF, Scanner, 2FA, Content-Schutz, TDM-Regeln und signierte Updates.

Multi-Agent-KI & LLM-Gateways

Agenten-Orchestrierung in isolierten Umgebungen, Schutzfilter gegen Prompt Injection, Modell-Scan und EU-LiteLLM-Routing.

Fuzzing & evidenzbasierte Prüfung

libFuzzer, AFL++, cargo-fuzz, Jazzer; CVE-Backport-Verifikation, OOB-Canary-Tokens und differenzielle HTTP-Analyse.

Zero-Knowledge-Vaults & WebCrypto

Clientseitige AES-256-GCM-Verschlüsselung, SCRAM-SHA-256-Auth, Schwellenwert-Signaturen und Air-Gap-HTML-Wiederherstellung.

Cloudflare-Flotten, Edge R2 & Mail

Betrieb großer WAF/DNS-Flotten, Workers, EU R2 Zero-Copy Failover, Origin CA und isolierte Mail-Systeme mit Postfix, Dovecot, OpenDKIM, Sieve.

Systemnahe Software & Edge

Systemdienste und Gerätetreiber in Rust (USB-HID, Hardware-Telemetrie); Android-Apps mit Medienverarbeitung (ExoPlayer, FFmpeg) und SQLite FTS.

MCP-Bridges, Voice AI & Föderation

Eigene MCP-Server (IMAP/OAuth-Mail mit Versandkontrolle, Dateizugriff, DACH-Daten), Voice AI und eigene Nodes (AT Protocol, ActivityPub).

Datenpipelines, FinTech & Open Data

Open-Data- und IoT-Kollektoren (OGC SensorThings), TCO- und Energiepreis-Engines (EZB, Eurostat) sowie EU-Register (u. a. Safety Gate).

Self-Hosted Kubernetes & CI/CD

Helm und Terraform mit mTLS, NetworkPolicy, KMS-Signierung, Trust-Rotation sowie WCAG/BFSG- und CSAF/SBOM-Gates im SARIF-Format.

KRYPTOGRAFIE & BLOCKCHAIN Kryptografisches Engineering & Blockchain-Settlement

XRP Ledger & Settlement

Technische Umsetzung für Kundenplattformen: Token-Escrow, Batch-DvP, Checks, Payment Channels, RWA; Multisig-Vaults (2-aus-3), API-Konnektoren für OFAC-/Travel-Rule-Screening und ISO 20022.

Nicht-verwahrendes Payment (Non-Custodial)

Architektur ohne Fremdmittelverwahrung (u. a. RPC-Integrationen für Monero und UTXO-Netze): eigene Subadresse je Rechnung, View-Key-Erkennung, Bestätigungen und Reorg-Puffer.

Multi-Chain-Verifikation

Integration und Auslesung von EVM-Netzen (Ethereum, Base, Arbitrum, USDC) sowie Solana per JSON-RPC; Smart-Contract-Prüfung (Solidity, Foundry).

Kryptografie, Signaturen & Forensik

Multi-Chain-Flussanalyse, Privacy-Exposure-Bewertung, Ed25519-Signaturen sowie Post-Quanten-Algorithmen (ML-DSA).

KONTAKT & ERFAHRUNG Lead Engineer & Projektreferenzen

Bartosz Joachimiak

INHABER & LEAD ENGINEER

Über 20 Jahre Praxis in IT und Elektronik (von maritimen Systemen und Infrastruktur bis hin zu Plattformen und sicherem Code); persönliche Umsetzung vom Backend bis zum Hardening. Deutsch, Polnisch, Englisch.

- Autorisierte Web-/API-Tests (CVD, BSI CERT-Bund); Mitglied bei ISSA International; IHK/DIHK-Beitrag (Cyberresilienz Gesundheit).
- OSS-Beitrag zu OWASP DSOMM; Kandidat EU Funding & Tenders (EX2026D1528552, ohne EU-Vertrag); ORCID 0009-0002-1713-9490 · DOI 10.5281/zenodo.24295340.
- Nicht-kommerzielle FuE: RWTH (WestAI), Jülich (JUPITER), GWDG (KISSKI); Fraunhofer FKIE (Malpedia) & CESNET (NERD).

Kontakt: bj@skopion.de · skopion.de/de/impressum · Signal/PGP
Mönchengladbach (NRW, DE) · Einzelunternehmen · USt-IdNr. DE297106209

PROJEKTREFERENZEN (ANONYMISIERT)

- **Zulieferer des Bahnsektors (KRITIS-Lieferkette, DE)**, 2026: Netzwerksegmentierung, Gateway- und Zugriffshardening, verschlüsselte Backups.
- **Ausbauunternehmen Glasfaserinfrastruktur FTTH (DE)**, 2025: FTTH-Datenengineering, Python-Automatisierung, Linux-Hardening.
- **Globaler Pharmakonzern (Schweiz)**, 2024 bis 2025: Remote-Infrastruktur-Engineering.
- **Europäische OEM-Integratoren: Workstations, Hochleistungs- und mobile IPC-Systeme (DACH)**, 2008 bis 2025: Firmware- und Treiberarbeiten (Hardware-Software-Integration), Multi-Tenant-Hosting, E-Commerce und Zahlungsintegrationen.

QUALIFIKATIONEN Branchenzertifikate & abgeschlossene Trainingspfade

ZERTIFIKATE

Sicherheit & Netzwerke

- **Qualys Certified Specialist**: TotalAppSec, VMDR, CSAM.
- **Fortinet NSE 3** (Cybersecurity) sowie Kurs FortiGate 7.6 Operator.
- **Cisco NetAcad**: Pfad Ethical Hacker (Pentests & Schwachstellen).
- **Red Team & DFIR**: Hack Smarter, HTB Academy, CyberDefenders.

INDUSTRIE & EU

OT/ICS & EU-Agenturen

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

LIEFERKETTE

CRA, OpenSSF & Cloud-KI

- **Linux Foundation / OpenSSF**: EU CRA, SBOM, Sigstore, Scorecard, Secure Software, AI/ML, OSS-Lizenzen.
- **Google Cloud, Anthropic, OpenAI**: Model Armor, ADK & MCP, SCC, Codex & API.
- **Digitale Produktpässe (DPP)**: PFR-Pfad (ESPR/EU-Konformität).

FORENSIK

OSINT & Finanzanalyse

- **Basel Institute on Governance**: OSINT sowie Visualise Cases & Flows of Money.
- **IFC / Weltbank**: Trade-Based Money Laundering (TBML).
- **World Bank Group Institute**: Standards für Metadaten-Dokumentation.

PRODUKTE & FORSCHUNG Eigene Produkte, Portale & FuE-Vorhaben

PRODUKT

Zero-LLM Website Assistant

Deterministischer Assistent ohne LLM zur Laufzeit: antwortet ausschließlich auf Basis geprüfter Quellen; als Container, REST-Bridge oder Air-Gap-Image.

skopion.de/de/zero-llm-assistent

LEISTUNG

Legacy & Zero-Source CRA

Rekonstruktion von Legacy-Systemen und Firmware, OT-Protokoll-Audits, Binär-SBOM mit kryptografischen Konformitätsnachweisen.

skopion.de/de/legacy-system-analyse

PORTALE

NIS2Steps, CRASteps & AIActSteps

Versionierte Gap-Analysen, verschlüsselte Nachweisregister und Maßnahmenpläne für NIS2, EU CRA und EU AI Act.

nis2steps.eu · crasteps.eu · aiactsteps.eu

RISIKO-MONITORING

Kommunal-Radar & Standort-Atlas

Laufend aktualisierte öffentliche Lagebilder externer Angriffsflächen für Kommunen, Regionen und Unternehmen.

skopion.de/de/standort-atlas

OPEN SOURCE

VersionSec

Python-CLI zur Prüfung von Gitea/Forgejo-Instanzen auf aktuelle Versionen, bekannte CVEs und Hardening mit SARIF-Ausgabe für CI.

versionsec.com · PyPI

LIEFERKETTE

zkBOM

Zero-Knowledge-Nachweise (STARK, WASM-Verifier) für SBOM, CBOM und AI-BOM; ML-DSA- und Ed25519-Signaturen, RFC-3161-Zeitstempel und Produktpass.

zkbom.com

FORSCHUNG

Power-SCADA-Resilienz

Formale Sicherheitsverifikation von Schalthandlungen bei gekoppelten Störungen zwischen Stromnetz und SCADA.

skopion.de/de/forschung-innovation

FORSCHUNG

Defensive KI & Nachweise

Neurosymbolische Bewertung passiver Risikoindikatoren, CEGIS-Umgebung, konforme Kalibrierung; BSFZ-FuE-Bescheinigung (2026) für Eigenforschung; nicht-kommerzielle Rechenzeit RWTH / JSC / GWDG.

skopion.de/de/vertrauen · Zenodo DOI

WISSEN & PRAXIS

Fallstudien & Vorlagen

Analysen realer Betrugs- und Phishing-Fälle, CRA-/NIS2-Leitfäden sowie offene, KoSIT-geprüfte XRechnung-/ZUGFeRD-Vorlagen.

skopion.de/de/fallstudien · GitHub

Schneller Start der Partnerschaft (Rückmeldung innerhalb von 24 Stunden werktags)

Kurzes Scoping-Gespräch (15 Min.) zu Rolle (A oder B), Paket oder privatem Pilotprojekt (1 bis 3 Tage). Abrechnung in Deutschland oder innergemeinschaftlich in der EU (B2B-Reverse-Charge).

Direktkontakt
bj@skopion.de
skopion.de/de/leistungen
Signal / PGP-Schlüssel auf Anfrage

SKOPION INTELLIGENCE

Sitz: Mönchengladbach (gesetzliche Pflichtmitgliedschaft: **IHK Mittlerer Niederrhein**) • **WFMG #startupMG** • **BSFZ-Siegel 2026**
(eigenbetriebliche FuE: passive KMU-Cyberrisikoanalyse, Bescheinigung vom 05.11.2026, § 6 FZulG)
Teilnehmer: **Allianz für Cyber-Sicherheit** • Netzwerk: **EC AI Pact**, **Apply AI Alliance** • **UN IGF 2026** (Online-Aussteller) • **EU-PIC 861665939**

PARTNERHINWEIS & RECHTSHINWEISE: Unverbindliche Fachinformation für Partner (Weitergabe an interessierte Endkunden gestattet; auf Wunsch gegenseitiges NDA und Kundenschutz vor Projektdatenaustausch). Das BSFZ-Siegel bescheinigt FuE-Tätigkeit von Unternehmen mit mindestens einer positiven Bescheinigung der Bescheinigungsstelle Forschungszulage (BSFZ); es bezieht sich ausschließlich auf SKOPION-Eigenforschung (passive KMU-Cyberrisikoanalyse, Bescheinigung vom 05.11.2026) und stellt **keine** Prüfung, Zulassung oder Qualitätszertifizierung angebotener Leistungen (z. B. Penetrationstests, CRA-/SBOM-Readiness oder Engineering-Leistungen) dar. Keine Rechtsberatung (RDG); keine Garantie auf Auslosung oder Bewilligung von Fördermitteln.