SKOPION INTELLIGENCE

PARTNER SERWISOWY DLA AGENCJI I FIRM IT

Stan: listopad 2026 · Referencja: SKP-PARTNER-2026-11

Wsparcie inżynieryjne i bezpieczeństwo IT w modelu white-label

SKOPION Intelligence realizuje jasno wydzielone pakiety prac technicznych dla software house'ów, agencji cyfrowych, firm IT (Systemhäuser), doradców i generalnych wykonawców: tworzenie aplikacji full-stack, e-fakturowanie DE (E-Rechnung), chmura i DevSecOps, niezależna weryfikacja bezpieczeństwa oraz gotowość compliance. Wyłącznie zdalnie, w Niemczech, krajach DACH i całej UE.

ZASADA PARTNERSTWA Dwie role, ściśle rozdzielone

Albo realizacja, albo niezależna weryfikacja: nigdy obie role w jednym projekcie klienta. Relacja z klientem, oferta i kolejne zlecenia zostają po stronie partnera. Bez dostępu do danych osobowych możliwy jest pełny model white-label; przy danych osobowych działamy jawnie jako podprocesor (art. 28 ust. 2 RODO) z klauzulą ochrony klienta (non-circumvention) i NDA.

Rola A · Zaplecze wykonawcze (white-label)

Dostarczamy zdefiniowane pakiety prac w projekcie partnera: tworzenie oprogramowania, integracje, infrastrukturę lub DevSecOps. Bezpośrednia koordynacja z zespołem partnera i przekazanie z pełną dokumentacją.

Rola B · Niezależna weryfikacja (zasada czterech oczu)

Weryfikujemy aplikacje, interfejsy i infrastrukturę zbudowane przez zespół partnera lub podmioty trzecie. Wykryte podatności i rekomendacje przekazujemy do wdrożenia zespołowi partnera, a po poprawkach wykonujemy retest.

DLA KOGO Typowi partnerzy

Software house'y i agencje cyfrowe

Wsparcie programistyczne, integracje, WCAG/BFSG oraz audyt bezpieczeństwa przed wdrożeniem (Go-Live).

Firmy IT (Systemhäuser)

Hardening infrastruktury, niezależna weryfikacja dla ubezpieczycieli i audytów.

Doradcy NIS2, ISO i IOD

Dowody techniczne, SBOM/CSAF i testy bez konkurowania o funkcję IOD ani kontrakty doradcze.

Generalni wykonawcy i konsorcja

Wydzielone pakiety prac w projektach, także B+R UE (PIC 861665939).

USŁUGI · ROLA A Inżynieria i realizacja

MODUŁ 01

Aplikacje full-stack, portale i desktop

- Portale klienta, narzędzia wewnętrzne, systemy na zamówienie i aplikacje desktopowe.
- Rust, Python/FastAPI, TypeScript/Next.js, React, PHP/Laravel, Python/Qt; PostgreSQL, Redis.
- Interfejsy zgodne z wymogami dostępności (WCAG/BFSG) i udokumentowane API.

skopion.de/pl/secure-softwareentwicklung

MODUŁ 02

API, integracje, e-commerce i E-Rechnung

- API REST/GraphQL, webhooki, integracje systemów oraz role i dostępy (OAuth2/OIDC).
- WordPress/WooCommerce, Shopware, integracje płatności i łańcucha dostaw.
- E-Rechnung DE: XRechnung, ZUGFeRD (EN 16931), walidacja KoSIT i wsparcie techniczne wymogów GoBD.

skopion.de/pl/uslugi

MODUŁ 03

Modernizacja, refaktoryzacja i migracja

- Stopniowa stabilizacja i migracja istniejących aplikacji bez przestoju.
- Systemy legacy (Delphi, VB6, COM, .NET), bazy FoxPro/Paradox/Btrieve oraz formaty danych DATEV (migracja 1:1).
- Rekonstrukcja techniczna i plany migracji także bez kodu źródłowego.

skopion.de/pl/analiza-systemow-legacy

MODUŁ 04

Infrastruktura, chmura i hardening

- Linux i Windows Server, Active Directory/Entra ID, segmentacja sieci i kontrola dostępu.
- Firewalle, VPN, szyfrowane kopie zapasowe oraz izolowane usługi poczty.
- AWS, Google Cloud, Azure, Kubernetes/Helm, Terraform, Cloudflare Workers/R2.

skopion.de/pl/uslugi

MODUŁ 05

DevSecOps, bramki CI/CD i przekazanie

- Kontrole bezpieczeństwa, jakości i WCAG/BFSG jako stałe bramki (security gates) w CI/CD.
- Analiza kodu i zależności, SBOM/CSAF/VEX na etapie budowania (CI) i weryfikacja backportów CVE.
- Powtarzalne wdrożenia bez przestojów, monitoring i dokumentacja techniczna.

skopion.de/pl/uslugi

MODUŁ 06

Przepływy AI, MCP i architektury danych

- Systemy RAG i przepływy wieloagentowe z kontrolowanym przepływem danych i uprawnień.
- Routing wielu modeli i zabezpieczenia w czasie wykonania (runtime) przed wyciekiem danych.
- Własne serwery MCP i mosty narzędziowe (ChatGPT/Codex, Claude, Gemini); suwerenne bramy LLM w UE.

skopion.de/pl/uslugi

WYBRANE TECHNOLOGIE I STANDARDY

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

USŁUGI · ROLA B Weryfikacja bezpieczeństwa i compliance

MODUŁ 07

Testy penetracyjne i bezpieczeństwo aplikacji

- Ręcznie weryfikowane testy web, API, Active Directory i przepływów AI wg OWASP ASVS.
- Błędy uwierzytelniania, autoryzacji i logiki biznesowej (IDOR/BOLA, izolacja klientów, narzucanie identyfikatora sesji / session fixation).
- Podsumowanie dla zarządu (Executive Summary), raport z dowodami oraz jeden retest po poprawkach.

skopion.de/pl/testy-penetracyjne

MODUŁ 08

Przegląd bezpieczeństwa i powierzchnia ataku

- Ustrukturyzowana ocena: M365/Entra ID, poczta, kopie zapasowe i powierzchnia zewnętrzna.
- Ocena hardeningu poczty, domen i DNS (SPF/DKIM/DMARC/DNSSEC/CAA) oraz odporności na phishing.
- Dowody techniczne pod ISO 27001, BSI IT-Grundschutz i ankiety ubezpieczycieli; weryfikacja backportów CVE.

skopion.de/pl/audyt-bezpieczenstwa-it
skopion.de/pl/check

MODUŁ 09

OSINT, marka i ekspozycja w dark webie

- Wczesne wykrywanie domen podszywających się pod markę (lookalike), fałszywych sklepów i nadużyć.
- Pasywne sygnały wycieków i ekspozycji bez przechowywania haseł w jawnej postaci.
- Śledztwa techniczne z pakietem dowodów, zgłoszeniami IOC i wnioskami o usunięcie zasobów (takedown).

skopion.de/pl/naduzycie-marki-phishing

MODUŁ 10

Gotowość NIS2, DORA i plan awaryjny

- Techniczna analiza ryzyka i dowody pod wymogi NIS2 (art. 21 / § 30 BSIG DE), DORA (odporność ICT) i łańcuch dostaw.
- Ścieżki zgłoszeń incydentów (24 h / 72 h) oraz praktyczny plan ciągłości działania.
- Wersjonowane raporty analizy luk zgodności (gap analysis) i rejestr dowodów w portalu NIS2Steps.

skopion.de/pl/gotowosc-nis2 · nis2steps.eu

MODUŁ 11

EU CRA, SBOM, CSAF, zero-source

- Techniczna ocena wstępna zakresu i klas produktów, wsparcie procesów zgłaszania (art. 14 CRA) oraz CSAF 2.0.
- Weryfikacja SBOM i VEX (CycloneDX, SPDX, OpenVEX) oraz ich integracji z potokami CI/CD.
- Binarny SBOM dla systemów legacy bez kodu źródłowego; portal CRASteps.

skopion.de/pl/gotowosc-cra · crasteps.eu

MODUŁ 12

EU AI Act i przegląd bezpieczeństwa AI

- Techniczne wsparcie klasyfikacji systemów, wymogów przejrzystości i dokumentacji technicznej (bez doradztwa prawnego).
- Testy chatbotów, asystentów i agentów AI: prompt injection, skan artefaktów modeli, kontrola narzędzi.
- Portal AIActSteps do zarządzania dowodami i planami działań naprawczych.

skopion.de/pl/audyt-bezpieczenstwa-ai
aiactsteps.eu

Zakres Roli B obejmuje wyłącznie niezależną weryfikację techniczną i przygotowanie dowodów, bez doradztwa prawnego (niem. RDG) ani formalnej certyfikacji ISO/BSI.

UZUPEŁNIAJĄCO Prewencja i wsparcie

Awareness i gotowość RODO

Szkolenia z rozpoznawania phishingu i techniczne podstawy ochrony danych dla zespołów partnera oraz klientów końcowych.

Bezpieczna komunikacja

Wdrażanie szyfrowania end-to-end, kluczy PGP dla korespondencji oraz algorytmów kryptografii postkwantowej (PQC).

Wstępna kwalifikacja incydentów

Ustrukturyzowana pierwsza ocena (triaż) podejrzanych e-maili, nagłówków, domen, adresów IP i wyciągów z logów.

Analiza transakcji blockchain

Ocena publicznych śladów w sieciach blockchain (tracing), analiza przepływów oraz dokumentacja kolejnych kroków.

WSPÓŁPRACA Modele umów i przebieg współpracy

Podwykonawstwo i white-label

Umowa podwykonawcza B2B z partnerem jako generalnym wykonawcą: NDA, klauzula ochrony klienta oraz umowa powierzenia lub podpowierzenia danych (DPA / niem. AVV, art. 28 RODO). Przetwarzanie w DE/UE, osobista realizacja przez doświadczonego inżyniera (bez delegowania prac juniorom) w zamkniętych pakietach (bez utrzymania 24/7); ryczałt, rozliczenie wg czasu pracy (T&M) lub abonament (retainer).

Bezpośrednie zlecenie od klienta końcowego

Klient końcowy zleca prace bezpośrednio SKOPION (realizacja własna bez podwykonawców i freelancerów), a partner odpowiada oddzielnie za wdrożenie i utrzymanie. Wyłącznie ten model spełnia wymogi NRW MID-Digitale Sicherheit dla MŚP z NRW (§ 4.3 wyklucza podwykonawstwo i freelancerów; próg min. 8 000 euro netto, miesięczne losowanie NRW.BANK, 28 dni na wniosek, pozytywna decyzja przed startem prac, bez gwarancji przyznania).

KROK 01

Krótka rozmowa

15 minut o celu, zakresie pakietu lub prywatnego pilotażu (od 1 do 3 dni) oraz podziale ról (A lub B).

KROK 02

Scoping, NDA i DPA/AVV

Wydzielony zakres prac, model umowy, umowa powierzenia (art. 28 RODO), ochrona klienta i poufność.

KROK 03

Realizacja / weryfikacja

Wyłącznie zdalnie, w repozytorium i CI/CD partnera, przetwarzanie w UE, bez zakłócania ciągłości produkcji.

KROK 04

Przekazanie i retest

Pełne przekazanie kodu bez vendor lock-in, dokumentacja lub raport z dowodami oraz retest.

KOMPETENCJE PLATFORMOWE — Kompetencje technologiczne potwierdzone we własnych systemach

Platformy EASM i OSINT

Zasoby zewnętrzne, DNS/TLS/CT oraz feedy podatności korelowane w spójne dossier incydentów.

E-Rechnung DE, GoBD i desktop

XRechnung, ZUGFeRD (EN 16931), walidacja KoSIT, dziennik audytowy SHA-256 (append-only) i aplikacje Python/Qt.

Billing SaaS i multi-tenant

Rozliczenia cykliczne, webhooki podpisywane HMAC z mechanizmem ponawiania (retry), separacja PostgreSQL RLS i klucze API.

Wielojęzyczni asystenci AI i RAG

Bazy wektorowe Qdrant, routing wielu dostawców LLM, izolacja klientów oraz wymuszanie polityk bezpieczeństwa (guardrails).

Transakcyjne backendy w Rust

Axum, SQLx, Redis: event sourcing, pełna idempotencja, kolejki DLQ oraz testy odporności na błędy.

Reverse engineering i rekonstrukcja

Binaria natywne, .NET/JVM, Android/iOS, Web/JS, firmware; rekonstrukcja z weryfikacją równoważności (Z3).

OT, systemy legacy i migracja

PROFINET, EtherCAT, S7comm, OPC-UA, PLC; bazy FoxPro, Paradox, Btrieve oraz formaty danych DATEV z anonimizacją PII.

PHP, Laravel i wtyczki WordPress

Panel Laravel/Filament z sejfem sekretów; wtyczki WP: WAF, skaner, 2FA, ochrona treści, reguły TDM i podpisane aktualizacje.

Wieloagentowe systemy AI i bramy LLM

Orkiestracja agentów AI w izolowanych środowiskach, filtry ochrony przed prompt injection, skan artefaktów modeli oraz routing LiteLLM w infrastrukturze UE.

Fuzzing i weryfikacja oparta na dowodach

libFuzzer, AFL++, cargo-fuzz, Jazzer; weryfikacja backportów CVE, tokeny detekcyjne OOB (canary tokens) i analiza różnicowa HTTP.

Skarbce Zero-Knowledge i WebCrypto

Szyfrowanie klienckie AES-256-GCM, uwierzytelnianie SCRAM-SHA-256, podpisy progowe i odzyskiwanie air-gap HTML.

Floty Cloudflare, Edge R2 i poczta

Zarządzanie rozbudowanymi flotami WAF/DNS, Workers i EU R2 zero-copy failover, Origin CA oraz izolowana poczta Postfix, Dovecot, OpenDKIM, Sieve.

Oprogramowanie niskopoziomowe i edge

Usługi systemowe i sterowniki urządzeń w Rust (USB HID, telemetria sprzętowa); aplikacje Android z przetwarzaniem mediów (ExoPlayer, FFmpeg) i SQLite FTS.

Mosty MCP, Voice AI i węzły federacyjne

Własne serwery MCP (poczta IMAP/OAuth z kontrolą wysyłki, dostęp plikowy, dane DACH), Voice AI oraz własne węzły komunikacji (AT Protocol, ActivityPub).

Potoki danych, FinTech i otwarte rejestry

Kolektory open data i IoT (OGC SensorThings), silniki wyceny TCO i energii (EBC, Eurostat) oraz integracje rejestrów europejskich (m.in. Safety Gate).

Self-hosted Kubernetes i bramki CI/CD

Helm i Terraform z mTLS, NetworkPolicy, podpisywaniem KMS i rotacją zaufania oraz bramkami WCAG/BFSG i CSAF/SBOM w SARIF.

KRYPTOGRAFIA I BLOCKCHAIN — Inżynieria kryptograficzna i rozliczenia blockchain

XRP Ledger i rozliczenia

Implementacja techniczna dla platform klientów: token escrow, batch DvP, czeki, kanały płatności, RWA; skarbiec wielopodpisowy (multisig 2-z-3), konektory API do screeningu OFAC/Travel Rule i formaty ISO 20022.

Płatności bezpowiernicze (non-custodial)

Architektura bez przechowywania środków klienta (m.in. integracje RPC dla Monero i sieci UTXO): osobny subadres na fakturę, wykrywanie kluczem podglądu (view key), potwierdzenia i bufor reorganizacji łańcucha.

Weryfikacja multi-chain

Integracje i odczyt sieci EVM (Ethereum, Base, Arbitrum, USDC) oraz Solana przez JSON-RPC; przeglądy smart kontraktów (Solidity, Foundry).

Kryptografia, podpisy i analiza śledcza

Analiza przepływów multi-chain, ocena ekspozycji prywatności, podpisy Ed25519 oraz algorytmy postkwantowe (ML-DSA).

KONTAKT I DOŚWIADCZENIE Lead engineer i referencje projektowe

Bartosz Joachimiak

WŁAŚCICIEL I LEAD ENGINEER

Ponad 20 lat praktyki w IT i elektronice (od systemów morskich i infrastruktury po platformy i bezpieczny kod); osobista realizacja, od backendu po hardening. Polski, niemiecki, angielski.

- Autoryzowane testy web/API (CVD, BSI CERT-Bund); członek ISSA International; wkład IHK/DIHK (cyberodporność ochrony zdrowia).
- Wkład OSS w OWASP DSOMM; kandydat EU Funding & Tenders (EX2026D1528552, bez kontraktu KE); ORCID 0009-0002-1713-9490 · DOI 10.5281/zenodo.24295340.
- Niekomercyjne B+R: RWTH (WestAI), Jülich (JUPITER), GWDG (KISSKI); Fraunhofer FKIE (Malpedia) i CESNET (NERD).

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

REFERENCJE PROJEKTOWE (ZANONIMIZOWANE)

- **Dostawca sektora kolejowego (łańcuch dostaw KRITIS, DE)**, 2026 r.: segmentacja sieci, hardening bramy i dostępu, szyfrowane kopie zapasowe.
- **Wykonawca infrastruktury światłowodowej FTTH (DE)**, 2025 r.: inżynieria danych FTTH, automatyzacja w Pythonie, hardening Linuksa.
- **Globalny koncern farmaceutyczny (Szwajcaria)**, od 2024 do 2025 r.: zdalna inżynieria infrastruktury.
- **Europejscy integratorzy OEM: stacje robocze, systemy wysokowydajne i mobilne IPC (DACH)**, od 2008 do 2025 r.: prace nad firmware i sterownikami (integracja sprzętowo-programowa), hosting multi-tenant, e-commerce i integracje płatności.

KWALIFIKACJE Certyfikaty branżowe i ukończone ścieżki szkoleniowe

CERTYFIKATY

Bezpieczeństwo i sieci

- **Qualys Certified Specialist**: TotalAppSec, VMDR, CSAM.
- **Fortinet NSE 3** (Cybersecurity) oraz kurs FortiGate 7.6 Operator.
- **Cisco NetAcad**: ścieżka Ethical Hacker (pentesty i ocena podatności).
- **Red Team i DFIR**: Hack Smarter, HTB Academy, CyberDefenders.

PRZEMYSŁ I UE

OT/ICS i agencje UE

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

ŁAŃCUCH DOSTAW

CRA, OpenSSF i chmura AI

- **Linux Foundation / OpenSSF**: EU CRA, SBOM, Sigstore, Scorecard, Secure Software, AI/ML, licencje OSS.
- **Google Cloud, Anthropic, OpenAI**: Model Armor, ADK & MCP, SCC, Codex & API.
- **Cyfrowe paszporty produktów (DPP)**: ścieżka PFR (zgodność z ESPR/UE).

ANALIZA ŚLEDCZA

OSINT i analiza finansowa

- **Basel Institute on Governance**: OSINT oraz Visualise Cases & Flows of Money.
- **IFC / Bank Światowy**: przeciwdziałanie praniu pieniędzy w handlu (TBML).
- **World Bank Group Institute**: standardy dokumentowania metadanych.

PRODUKTY I BADANIA Własne produkty, portale i badania B+R

PRODUKT

Zero-LLM Website Assistant

Deterministyczny asystent bez LLM w runtime: odpowiada wyłącznie na podstawie potwierdzonych źródeł; jako kontener, most REST lub obraz air-gap.

skopion.de/pl/asystent-zero-llm

USŁUGA

Legacy i zero-source CRA

Rekonstrukcja systemów legacy i firmware, audyty protokołów OT, binarny SBOM z kryptograficznymi dowodami zgodności.

skopion.de/pl/analiza-systemow-legacy

PORTALE

NIS2Steps, CRASteps i AIActSteps

Wersjonowane raporty analizy luk zgodności (gap analysis), szyfrowane rejestry dowodów i plany naprawcze dla NIS2, EU CRA i EU AI Act.

nis2steps.eu · crasteps.eu · aiactsteps.eu

MONITORING RYZYKA

Kommunal-Radar i Standort-Atlas

Stale aktualizowane publiczne obrazy zewnętrznych powierzchni ataku dla gmin, regionów i firm.

skopion.de/pl/atlas-ryzyka

OPEN SOURCE

VersionSec

CLI w Pythonie sprawdzające Gitea/Forgejo pod kątem aktualności wersji, znanych CVE i hardeningu, z raportowaniem SARIF dla CI.

versionsec.com · PyPI

ŁAŃCUCH DOSTAW

zkBOM

Dowody zero-knowledge (STARK, weryfikator WASM) dla SBOM, CBOM i AI-BOM; podpisy ML-DSA i Ed25519, znaczniki czasu RFC 3161 i paszport produktu.

zkbom.com

BADANIA

Odporność Power-SCADA

Formalna weryfikacja bezpieczeństwa działań łączeniowych przy sprzężonych awariach sieci energetycznej i SCADA.

skopion.de/pl/badania-innowacje

BADANIA

Defensywne AI i dowody

Neurosymboliczna ocena pasywnych wskaźników ryzyka, środowisko CEGIS, kalibracja konformalna; zaświadczenie B+R BSFZ (2026) dla badań własnych; niekomercyjne obliczenia na RWTH / JSC / GWDG.

skopion.de/pl/zaufanie · Zenodo DOI

WIEDZA I MATERIAŁY

Studia przypadków i wzorce

Analizy realnych oszustw i phishingu, poradniki CRA/NIS2 oraz otwarte wzorce XRechnung/ZUGFeRD sprawdzone narzędziem KoSIT.

skopion.de/pl/studia-przypadku · GitHub

Szybki start współpracy partnerskiej (odpowiedź w 24 h robocze)

Krótka rozmowa scopingowa (15 min) o roli (A lub B), pakiecie lub prywatnym pilotażu (od 1 do 3 dni). Rozliczenie w Niemczech lub wewnątrzwspólnotowo w UE (Reverse Charge B2B).

Kontakt bezpośredni
bj@skopion.de
skopion.de/pl/uslugi
Signal / klucz PGP na życzenie

INFORMACJA O WSPÓŁPRACY I NOTA PRAWNA: Niewiążąca informacja handlowa dla partnerów (dozwolone przekazanie klientom końcowym; na życzenie wzajemne NDA i ochrona klienta przed wymianą danych projektowych). Znak BSFZ poświadcza działalność B+R firm, które otrzymały co najmniej jedno pozytywne zaświadczenie Bescheinigungsstelle Forschungszulage (BSFZ); dotyczy wyłącznie własnych badań SKOPION (pasywna analiza ryzyka cybernetycznego MŚP, zaświadczenie z 05.11.2026 r.) i **nie** stanowi weryfikacji, dopuszczenia ani certyfikacji jakości oferowanych usług (np. testów penetracyjnych, gotowości CRA/SBOM czy prac inżynierskich). Bez doradztwa prawnego (niem. RDG); brak gwarancji wylosowania lub dofinansowania.