📖 SCOPE: Supply Chain OSINT & Prediction Engine

Executive Summary

SCOPE (Supply Chain OSINT & Prediction Engine) is a modern Third Party Risk Management (TPRM) platform focused entirely on cybersecurity. It enables organizations to continuously monitor, assess, and mitigate the cybersecurity risks of third-party vendors. The platform combines OSINT-driven intelligence, breach history tracking, threat surface analysis, and automated risk scoring into a unified dashboard for security stakeholders, procurement leaders, and compliance teams.

This whitepaper provides a one-stop, comprehensive view of SCOPE — including how vendors are onboarded, how risks are calculated, what each module does, and how it all integrates to create a cyber-aware supply chain.

🚀 Project Objectives

- Deliver continuous visibility into vendor cybersecurity postures
- Simulate adversarial intelligence using open-source reconnaissance
- Enable rapid and contextual onboarding of third parties
- Score vendor risk with category-specific intelligence
- Empower stakeholders with automated analytics and alerts
- Ensure all outputs are audit-ready and actionable

🏗️ Vendor Onboarding & Intake Flow

The vendor onboarding module collects structured data critical for evaluating cyber risk. It is a multi-step form that captures:

1. Basic Information

- Vendor Name
- Country of Operation
- Industry / Sector
- Website / Domain

2. Business & Operational Context

- Size of company (Employee count)
- Annual Revenue (optional)
- Geographical footprint (HQ, DCs, cloud regions)

3. Asset Impact & Dependency

- Criticality of service (Low / Medium / High / Critical)
- Services consumed (infra, software, data handling)
- Number of internal systems dependent on this vendor

4. Security Declarations (Optional Self-attested)

- Certifications (ISO 27001, SOC 2, etc.)
- Compliance coverage (GDPR, HIPAA, NIST, etc.)
- Presence of security teams, IR plans, MDM, etc.

5. External Observables (Derived via OSINT)

- Domain enumeration (subdomains, endpoints)
- DNS, TLS, CDN info

- GitHub/org leak checks

All of this is used to create a vendor profile that is continuously re-evaluated every 3 hours by the platform.

📊 Risk Scoring & Classification (Overview)

The scoring system breaks risk into **four main pillars**, each with measurable subcategories. These are:

1. **Cybersecurity Posture**: External attack surface, email/code/web security
2. **Compliance & Legal**: Standards, fines, contracts, data privacy laws
3. **Geopolitical Context**: Sector risk, country instability, infra jurisdiction
4. **Reputation & Exposure**: Breach history, leaked data, brand spoofing

Each pillar is scored individually (0–100) and classified as Low / Medium / High / Critical.
For a full breakdown, refer to the **SCOPE Risk Scoring Whitepaper**.

🎯 Why It Matters to Stakeholders

🛡️ For Security Teams:

- Identify high-risk vendors before onboarding
- Automatically prioritize vendors tied to critical systems
- Monitor third-party posture continuously, not once a year

📋 For Compliance Teams:

- Track framework alignment (e.g., ISO, NIST, GDPR)
- Get audit-ready reports per vendor

- Generate risk-adjusted compliance maps

🧾 For Procurement / Business:

- Choose vendors with lowest cyber risk
- Reduce exposure from suppliers in unstable regions or industries
- Justify switching vendors with historical scoring logs

📉 For Executives:

- Reduce the chance of third-party-originated cyber incidents
- Quantify supply chain cyber exposure at any time
- Ensure enterprise-wide cyber resilience is maintained

🧰 Feature Breakdown

1. Risk Intelligence Dashboard

- Real-time scoring across all vendors
- Filter by sector, country, exposure level
- Per-category score cards

2. Threat Intelligence Feed

- IOC tracking (IPs, hashes, domains)
- Reputation analysis via threat feeds
- Auto-link vendor infra to threat actor infra (via C2/IP abuse databases)

3. Breach History Tracker

- Publicly reported breaches by vendor
- Credential leaks from HIBP, Pastebin, Telegram
- Signal-level exposure across deep/dark web

4. Compliance Matrix View

- Tracks declared and verified certifications
- Highlights gaps based on industry standards
- Maps coverage across global compliance frameworks

5. Asset Risk Matrix

- Correlates vendor score with asset criticality
- Color-coded matrix: Critical assets with high vendor risk trigger alerts
- Enables prioritization of vendor reviews

6. Export & Audit Support

- Export vendor data as PDF, CSV, JSON
- All score history retained for audit trail
- Customizable compliance summaries

🧱 Technical Foundation

Frontend

- **Next.js 14 + TypeScript**
- TailwindCSS for UI

- App Router + Context API for multi-tenant view switching

Backend

- **Flask (Python)**
- PostgreSQL via SQLAlchemy
- Marshmallow for request validation
- CORS & secure headers middleware

Risk Engine

- Rule-based scoring logic (see attached whitepaper)
- OSINT-driven enrichment modules (e.g., Shodan, DNSRecon)
- Modular scoring logic for extension (AI/ML ready)

🔄 System Workflow

1. **Vendor is onboarded via form**
2. **System triggers data collection** (passive recon, DNS, certs, leaks)
3. **Risk engine calculates per-category scores**
4. **Dashboard displays score and alert badge**
5. **Every 3 hours, re-scan is triggered**
6. **Changes are logged, alerts are raised if thresholds breached**

⚠️ Known Limitations (v1 MVP)

- OSINT feeds are mocked; live data integrations planned
- No role-based access yet (authentication in v2)
- ML features (e.g., breach prediction) are roadmap items
- Third-party scoring API (RiskRecon/Bitsight) not integrated yet

---

🔜 What's Coming Next

- Real-time feed ingestion (Shodan, Censys, VT, HIBP)
- User login, RBAC and organization separation
- Alert management module + notification engine
- Score trend graphs and time-series risk analysis
- Playbook system for automated action suggestions

📎 Supporting Documentation

- **SCOPE Risk Scoring Whitepaper** (attached): detailed scoring framework
- **Vendor Intake Form Reference Sheet** (optional future doc)

🏁 Final Thought

SCOPE is designed to deliver **clarity, continuity, and confidence** in cyber supply chain security. It enables every stakeholder — from analysts to executives — to measure, monitor, and minimize the hidden risks of third-party relationships. Its modular foundation, explainable scoring model, and actionable dashboards make it a next-gen approach to cybersecurity-focused TPRM. **No more spreadsheets. No more one-time audits. Just continuous, transparent vendor risk intelligence.**