Telecom Vulnerability Intelligence

Vendor-Risk Advisory - Service Overview

Prepared by: James Kay	Location: Little Neston, United Kingdom
Email: jameskaydevuser@gmail.com	LinkedIn: linkedin.com/in/jameskaydev
Website: [insert your website URL]	Document: Service Overview

1. Who I Am

I am a UK-based senior fullstack developer and freelance consultant with over 12 years of commercial experience building web applications, mobile products, backend systems, REST APIs, admin panels, and cloud-supported platforms for international clients.

My technical background includes Laravel, PHP, Flutter, WordPress, AWS, Docker, Redis, Elasticsearch, RabbitMQ, MySQL, PostgreSQL, API design, scalable backend architecture, and client-facing software delivery.

I am now formalising a specialist advisory service focused on telecom vulnerability intelligence and vendor-risk reporting for telecom-adjacent organizations.

2. Service Summary

Telecom Vulnerability Intelligence & Vendor-Risk Advisory helps telecom-adjacent businesses understand known vulnerabilities, affected vendors, affected protocols, business impact, and remediation priorities.

The service is designed for organizations that work with or depend on telecom/mobile technologies but may not have a dedicated telecom security intelligence function.

- MVNOs	- eSIM providers
- Mobile-data providers	- VoIP/SIP providers
- Private LTE/5G businesses	- Telecom-adjacent startups
- Cybersecurity firms serving telecom clients	- Software companies integrating telecom or mobile-network services

3. What the Service Provides

The service provides defensive advisory outputs such as:

- Telecom vulnerability-intelligence reports
- Vendor and product risk summaries
- Telecom CVE and advisory analysis
- Remediation-planning notes
- Executive risk summaries
- Vendor questions checklists
- Exposure-triage support

The goal is to turn complex telecom vulnerability information into clear, practical, business-ready guidance.

VKB-only use case	The request is for VKB as an internal intelligence source. It is not a request for live monitoring, active telecom testing, exploit capability, or managed incident response.

4. Why VKB Is Needed

Public CVEs and vendor advisories are useful, but they often lack telecom-specific context. For telecom-adjacent clients, the important questions are often:

- Which telecom layer is affected?
- Which protocol or interface is involved?
- Which vendor or product may be relevant?
- Could the issue affect service availability, subscriber privacy, roaming, fraud risk, or operations?
- What mitigation or vendor action should be considered?

VKB is valuable because it can support mapping vulnerability information to protocols, vendors, network domains, network elements, impact, and remediation guidance.

5. Intended Use of VKB

The intended use is VKB-only at this stage. VKB would be used internally as a professional intelligence source to support:

- Vendor-risk reporting
- Telecom CVE/advisory analysis
- Exposure triage
- Remediation-planning guidance
- Client-facing advisory summaries
- Executive risk briefings

Clients would not receive direct VKB access, and raw VKB entries would not be redistributed.

6. What This Is Not

- Live telecom traffic monitoring	- Active telecom vulnerability testing
- Penetration testing	- Exploit development
- SS7 hacking or SIM interception	- Unauthorized telecom probing
- Managed SOC or 24/7 incident response	

If a client later requires live monitoring, testing, or managed response, that should be discussed separately through the correct tools, providers, authorization, and scope.

7. Responsible-Use Commitments

I understand that telecom vulnerability intelligence can be sensitive. I am willing to comply with NDA, acceptable-use, non-distribution, and responsible-disclosure requirements.

- No unauthorized testing	- No exploit development
- No redistribution of raw VKB content	- No publication of sensitive vulnerability details
- Defensive reporting only	- Clear scope for every engagement
- Responsible disclosure where appropriate	

8. Commercial Model

The commercial model is based on recurring advisory services, not one-off access to a database. VKB would support monthly telecom vulnerability-intelligence briefs, vendor/product risk tracking, urgent advisory notes, remediation-planning reports, executive summaries, and supplier-risk questions.

The goal is to build a recurring telecom vulnerability-intelligence advisory service for multiple telecom-adjacent clients.

9. Requested Discussion

I would like to understand whether full VKB-only access can be licensed to an independent consultant or small consultancy for this type of defensive vulnerability-intelligence and vendor-risk advisory use case.

- Licensing model
- Acceptable-use requirements
- NDA and non-distribution terms
- Whether partner status is required
- Whether one named-user access is possible
- Restrictions for client-facing summaries

[redacted]

A short call to discuss commercial fit, licensing route, responsible-use boundaries, and whether VKB-only access is appropriate for this consultancy model.