ZEWNĘTRZNE ZAPLECZE TECHNICZNE BEZPIECZEŃSTWA

Wy odpowiadacie za prawną stronę NIS2. Ja — za techniczną. Bez budowania działu.

Dla kancelarii i firm doradczych, których klienci pytają o NIS2/KSC. Wy prowadzicie analizę prawną i odpowiedzialność zarządu; potem pada pytanie wykonawcze — „i jak to technicznie zrobić?". To już moja część. Klient i relacja zostają u Was.

- ✓ Prelegent Black Hat USA 2025
- ✓ 20 lat w cyberbezpieczeństwie
- ✓ Red team lead · SaaS · ISO 27001 / SOC 2

WERYFIKOWALNE — PROFIL BLACK HAT USA 2025

SYTUACJA

Opinia prawna to połowa. Potem pada: „i jak to technicznie zrobić?"

Ustalacie klientowi obowiązki z NIS2/KSC, odpowiedzialność zarządu (osobistą, poza polisą D&O), kwestie umów i łańcucha dostaw. Potem pada pytanie wykonawcze — jak wdrożyć SZBI, co zrobić po incydencie, jak udowodnić należytą staranność. To już nie jest praca prawnika. „To nie nasza działka" zostawia klienta w połowie drogi, a Waszą radę bez pokrycia.

KIM DLA WAS JESTEM

Waszym zapleczem technicznym — nie konkurentem o klienta.

Wchodzę tam, gdzie kończy się doradztwo prawne: projekt SZBI, procedury i playbooki reagowania, architektura bezpieczeństwa, techniczna obsługa incydentu oraz dowody należytej staranności, które obronią się przed regulatorem. Pracuję **pod Waszą marką** albo **obok niej** jako wskazany wykonawca. Klienta i relację trzymacie Wy.

CO DOSTARCZAM

01 · NIS2 / KSC

Techniczne wdrożenie zgodności

Wy robicie analizę prawną, ja stronę techniczną: od analizy luk po projekt SZBI, procedury, playbooki i nadzór nad wdrożeniem, które realizują sprawdzone firmy pod moją kontrolą.

`ocena luk — od ~6 000 zł · wdrożenie wg zakresu`

02 · INCYDENT

Reagowanie i dowody

Gdy się pali: techniczne ustalenie faktów, timeline, priorytety 24–72 h i raport, który obroni się w postępowaniu i przed regulatorem. Wy prowadzicie stronę prawną i notyfikacje — ja techniczną.

`na wezwanie lub retainer`

03 · ARCHITEKTURA

Pokrycie dla Waszej rady

Realne środki, które stoją za opinią o zgodności: zero-trust, segmentacja, tożsamość, monitoring. Należyta staranność, którą da się udowodnić — ochrona zarządu, nie tylko papier.

`doradztwo / nadzór — wg zakresu`

NA START — ZERO PRACY PO WASZEJ STRONIE

Dostajecie **gotowe materiały**: checklistę kwalifikacji do KSC, FAQ na pytania klientów i przykładowe opracowania. Na pytanie o konkretnego klienta **odpowiadam do 2 dni roboczych** — bez pracy po Waszej stronie.

JAK TO DZIAŁA

01

Wy doradzacie

Prowadzicie analizę prawną, odpowiedzialność zarządu i relację z klientem.

02

Ja projektuję i nadzoruję

Projektuję całość — technologię, procedury i playbooki. Wdrożenie realizują sprawdzone firmy pod moim nadzorem, a cały proces prowadzę i za niego odpowiadam.

03

Klient obsłużony w całości

Prawo i technika w jednym miejscu — u Was. Relacja i zaufanie zostają po Waszej stronie.

→ **15 minut rozmowy — sprawdzimy, którzy z Waszych klientów podlegają KSC.**

Bartek Binder — FatDot

Cyberbezpieczeństwo, zgodność (NIS2 / KSC), reagowanie na incydenty. Dwie dekady praktyki ofensywnej i inżynierii bezpieczeństwa.

bartek@fatdot.pl

+48 609 737 000

fatdot.pl