Što radimo nakon audita

KleoSEC provodi tehničke mjere koje ISO 27001 ili NIS2 audit propiše i isporučuje dokaz da su provedene, pod vašim imenom ili kao vaš partner. Vi vodite savjetovanje i dokumentaciju, mi tehničku provedbu.

Tri koraka

01

Provjera

Pentest (vanjski, interni, web aplikacije), vulnerability assessment, pregled IT/OT mrežne arhitekture.

Dobivate: Izvještaj s prioritiziranim nalazima, mapiran na ISO 27001 Annex A i NIS2 čl. 21.

02

Sanacija

Hardening po CIS benchmarku, segmentacija mreže i OT zone, MFA i pregled privilegiranih računa, zatvaranje nalaza iz gap analize.

Dobivate: Provedene mjere, konfiguracije prije i poslije.

03

Dokaz

Retest, izvješće o provedbi mjera i uvođenje alata koji sami bilježe dokaz za auditora: centralno logiranje (SIEM), EDR i backup s testom obnove.

Dobivate: Dokumentacija koju auditor prihvaća bez prepravljanja.

Kako surađujemo

Vi birate model koji vam odgovara za svakog klijenta:

Model	Ugovor s klijentom	Fakturira klijentu	Što dobivate
Pod vašim imenom	Vi, mi smo vaš podizvođač	Vi, s vlastitom maržom	Izvještaji na vašem predlošku, klijent ostaje vaš
Preporuka	Mi, nakon vašeg predstavljanja	Mi	Dogovorena provizija, bez vlastitog angažmana
Zajednička ponuda	Oboje, jedna ponuda	Svatko svoj dio	Jedan sugovornik za klijenta, širi opseg usluge

Što audit propiše, a mi isporučimo

Svaki tipičan nalaz iz gap analize vežemo uz kontrolu koju auditor provjerava, uz ono što provedemo i uz dokaz koji ostaje u dokumentaciji klijenta.

Nalaz iz audita	ISO 27001:2022 Annex A	NIS2 čl. 21(2)	Naša isporuka	Dokaz za auditora
Nema provjerenih ranjivosti / pentesta	A.8.8, A.8.29	(e), (f)	Pentest + retest nakon sanacije	Izvještaj i potvrda retesta
Slaba kontrola pristupa, nema MFA	A.5.15, A.5.18, A.8.2, A.8.5	(i), (j)	Uvođenje MFA, pregled privilegiranih računa	Konfiguracija i popis računa prije/poslije
Ravna mreža, OT i IT zajedno	A.8.20–A.8.22	(e)	Segmentacija, pravila firewalla, OT zone po IEC 62443	Mrežna shema i test prolaza između zona
Nema logiranja ni detekcije	A.8.15, A.8.16, A.8.7	(b)	Centralno logiranje / SIEM, EDR na krajnjim točkama	Pokrivenost izvora logova, testni alarm
Backup bez testa obnove	A.8.13	(c)	Postavljanje backupa i test obnove	Zapisnik testa obnove
Nestandardne konfiguracije	A.8.9	(e)	Hardening po CIS benchmarku	Izvještaj usklađenosti prije/poslije

Što ne radimo

ISMS dokumentaciju, politike i procedure, vođenje audita, SOC i dežurstva. Ne nudimo savjetovanje vašim klijentima. To stoji u partnerskom ugovoru, uz NDA i klauzulu o nenagovaranju.

Način rada

Remote, uz dolazak na lokaciju za OT i mrežne radove. Tipičan opseg traje 5 do 15 radnih dana. Plan provedbe s procjenom vraćamo u 48 sati od primitka nalaza gap analize.

TKO SMO

KleoSEC je security integrator iz Hrvatske. Certifikati: OSCP+, PNPT, CNPen, eWPT, eJPT, a ISA/IEC 62443 je u pripremi. Iskustvo s IT/OT mrežnom arhitekturom solarnih elektrana: energetika je NIS2 obveznik, a OT segmentacija je nalaz koji se u tom sektoru najteže zatvara.

KONTAKT

Mislav Kovač

mislav.kovac@kleosec.com

+385 99 367 7737

kleosec.com

KleoSEC d.o.o. · Kralja Zvonimira 8, 40000 Čakovec, Hrvatska