kleosec CYBERSECURITY SERVICES

For ISO 27001 and NIS2 consultants and auditors

What we do after the audit

KleoSEC implements the technical measures an ISO 27001 or NIS2 audit prescribes and delivers the evidence that they are in place, under your name or as your partner. You lead the advisory and documentation, we do the technical implementation.

Three steps

01

Verify

Penetration testing (external, internal, web applications), vulnerability assessment, IT/OT network architecture review.

You get: Report with prioritised findings, mapped to ISO 27001 Annex A and NIS2 Art. 21.

02

Remediate

Hardening to CIS benchmarks, network segmentation and OT zones, MFA and privileged-account review, closing gap-analysis findings.

You get: Implemented measures, before/after configurations.

03

Prove

Retest, implementation report and deployment of tools that record the evidence for the auditor: central logging (SIEM), EDR and backup with restore test.

You get: Documentation the auditor accepts without rework.

How we work together

You choose the model that fits each client:

Model	Contract with the client	Invoices the client	What you get
Under your name	You, we are your subcontractor	You, with your own margin	Reports on your template, the client stays yours
Referral	Us, after your introduction	Us	An agreed commission, no delivery effort on your side
Joint proposal	Both, one proposal	Each side its own part	One point of contact for the client, a wider service scope

What the audit prescribes, what we deliver

Each typical gap-analysis finding is tied to the control the auditor checks, to what we implement, and to the evidence that stays in the client's documentation.

Audit finding	ISO 27001:2022 Annex A	NIS2 Art. 21(2)	Our delivery	Evidence for the auditor
No verified vulnerabilities / no pentest	A.8.8, A.8.29	(e), (f)	Pentest + retest after remediation	Report and retest confirmation
Weak access control, no MFA	A.5.15, A.5.18, A.8.2, A.8.5	(i), (j)	MFA rollout, privileged-account review	Configuration and account list before/after
Flat network, OT and IT together	A.8.20–A.8.22	(e)	Segmentation, firewall rules, OT zones per IEC 62443	Network diagram and zone-crossing test
No logging or detection	A.8.15, A.8.16, A.8.7	(b)	Central logging / SIEM, EDR on endpoints	Log-source coverage, test alert
Backup never restore-tested	A.8.13	(c)	Backup setup and restore test	Restore test record
Non-standard configurations	A.8.9	(e)	Hardening to CIS benchmarks	Compliance report before/after

What we do not do

ISMS documentation, policies and procedures, running the audit, SOC or on-call. We do not offer advisory to your clients. This is written into the partner agreement, together with an NDA and a non-solicitation clause.

Way of working

Remote, with on-site work for OT and network tasks. A typical scope takes 5 to 15 working days. We return an implementation plan with an estimate within 48 hours of receiving the gap-analysis findings.

WHO WE ARE

KleoSEC is a security integrator based in Croatia. Certifications: OSCP+, PNPT, CNPen, eWPT, eJPT, with ISA/IEC 62443 in preparation. Experience with the IT/OT network architecture of solar power plants: energy is a NIS2 sector, and OT segmentation is the finding that is hardest to close there.

CONTACT

Mislav Kovač

mislav.kovac@kleosec.com

+385 99 367 7737

kleosec.com

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