



BRUSSELS · 8 OCTOBER 2026

DEFENDING THE GRID

Running a Security Operations Centre
through a full-scale war — and how AI
changed it



OLEKSII SHAMRO

Head of the Information Security Events and
Incidents Management Department

WHO WE ARE

The backbone of Ukraine's power system

NPC Ukrenergo is Ukraine's transmission system operator and dispatches the national power system.

21.8K

km of high-voltage lines, 220-750 kV

2022

Synchronised with Continental Europe
on 16 March 2022

Full ENTSO-E member since 2024

**ISO
27001**

ISO/IEC 27001:2022
certified, audited annually

Under constant pressure since February 2022: our threat model is written by the adversary.

THE TEAM

A SOC built for IT and OT

15

analysts and engineers

Information Security Events and
Incidents Management
Department

SIEM & SOAR

Platform administration, detection engineering,
automated response playbooks

Monitoring & IR

incident response, threat hunting, forensics

Vulnerabilities & PAM

Scanning, remediation tracking, privileged access for
contractors

OT & Threat Intel

Substation network monitoring, sandboxing and MISP

FEBRUARY 2022 ONWARDS

What the war took from us

Infrastructure

Substations and facilities shelled repeatedly. Equipment, links and monitoring coverage lost overnight — and rebuilt under fire.

Places to work

Offices damaged or unusable. Blackouts and air raids forced us to distribute the SOC across people, communication links and work locations.

People

Colleagues mobilised to the Armed Forces and intelligence services. Half of the shift roster gone in months.

Vendor support

Manufacturers suspended support and deliveries. We had to keep systems running without the vendor on the line.

None of this was a reason to lower monitoring coverage. The grid does not get a maintenance window.

THE HARDEST GAP

Rebuilding a team you cannot hire



THE PROBLEM: experienced analysts mobilised, the cyber job market emptied out, and no time for a 12-month ramp-up.



AI-screened juniors

Filtered by our in-house AI built service, trained in live operations



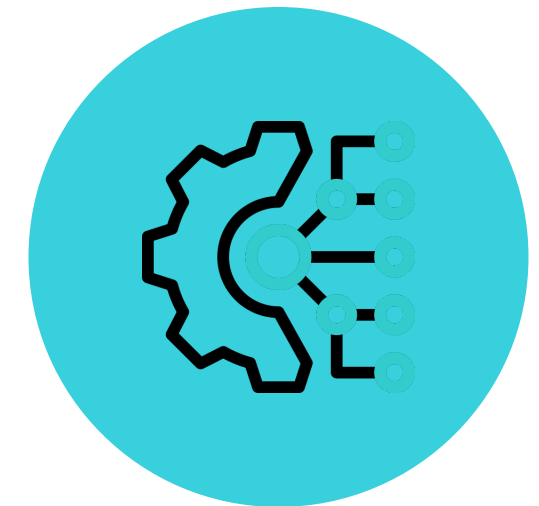
Playbooks

Runbooks and decision trees for every alert type



AI mentor for every junior

Explains alerts, logs, queries and malware behaviour



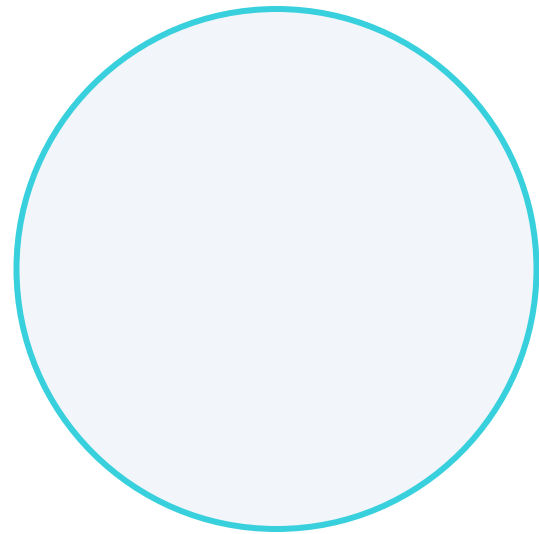
Tier-1 automation

Repetitive work moved to SOAR, so a small team holds the line

Knowledge that lived in people's heads now lives in documents and tools.

Where AI actually earns its place

AI-driven attacks move faster — so analyst reaction has to as well.



Faster reaction

Enrichment, log and script explanation, draft triage — minutes, not hours



Onboarding & support

Juniors ask AI first, a senior second



Finding our own gaps

Review of configs, code, scan output and detection coverage



Reporting

Incident write-ups and management summaries in two languages

AI proposes — a human decides. No autonomous action on production or OT.

The adversary got the same tools

AI-DRIVEN THREAT

Phishing without mistakes

Flawless Ukrainian and English lures, tailored to our roles and current events



Faster malware

Variants and exploit chains mutate quicker than signatures follow



Deepfakes & pretexting

Voice and video impersonation of staff, contractors and partners



OUR COUNTERMEASURE

Awareness rewritten

Training built for AI-quality phishing, not typos

Behaviour over signatures

Sandboxing, automated enrichment of every suspicious artefact and speeding up analyst decision with AI.

Out-of-band verification

Any voice or video request is confirmed through a second channel

WHAT WE TAKE TO EUROPE

Resilience is a people problem first.

01 People are the fragile part

Technology survived the shelling. Plan for losing half of the team.

02 AI closes an experience gap, not a judgement gap

Juniors work at a level we could not have trained them to in time — the decision stays human.

NEXT

From principles to practice: how AI already works in our daily processes

