OreKeep
CYBER

ONE-PAGER · 2026 · CONFIDENTIAL

OT / ICS | SCADA | PLC | IT | CLOUD | IDENTITY | AI SYSTEMS | OSINT

CYBERSECURITY FOR INDUSTRIAL OPERATIONS

From unknown exposure to a defended operation.

OreKeep Cyber secures industrial operators and the vendors holding standing access to their systems. One team across **IT, OT and AI** — assessment, hardening, monitoring, threat intelligence, incident response and authorised offensive testing — planned with the engineers who run the plant, so security does not become the outage.

ASSESS · PROTECT · MONITOR · HUNT · RESPOND

PRIVATE INDUSTRY · PUBLIC PURPOSE

THE TARGET
Weeks, not guesswork.

A first engagement returns a mapped estate, a risk picture ranked by production impact, and a costed plan.

OreKeep engagement model

DWELL TIME
42 days

average time ransomware sits inside an OT environment — against 5 days with full visibility.

Dragos OT/ICS Report, 2026

THREAT GROWTH
+49%

year-on-year rise in ransomware attacks on industrial organisations; 3,300 organisations hit in 2025.

Dragos OT/ICS Report, 2026

WHY IT IS STRATEGIC
86%

of key mineral processing sits with the top three refining nations — which is why these sites are national assets.

IEA Global Critical Minerals Outlook, 2026

THE CHALLENGE

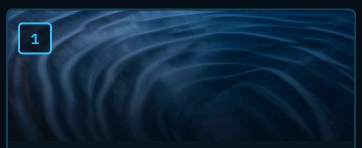
- Water and mineral operations run on connected plants, remote vendors and industrial control systems. In July 2026 CISA issued a sector-wide alert on **active targeting of internet-exposed PLCs** at water utilities in at least 12 US states, including one that shut a pump station and dropped system pressure.
- Most operators cannot answer the basic questions: what is connected, who can reach it, and what stops if it fails. And **IT security methods copied into an OT network** can cause the outage they were bought to prevent.

THE OreKeep ANSWER

- **One team across IT, OT and AI.** Twenty services in five families, from governance and vCISO leadership to OT hardening, monitoring, threat intelligence and incident response — scoped per site, against the systems actually installed.
- **Safety and uptime outrank test coverage.** Work is planned with operations and engineering. Production systems are tested only under separate written scope and approval — with an owner, a window and a rollback.

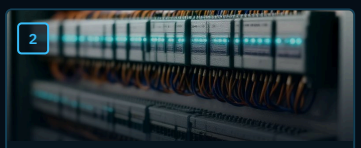
WHAT AN OreKeep ENGAGEMENT LOOKS LIKE

FOUR STAGES · ONE CHAIN OF EVIDENCE



1 Assess
Asset and exposure mapping across IT and OT, dependency and crown-jewel analysis, and a risk register ranked by production impact.

ASSETS · EXPOSURE · IMPACT



2 Protect
Network segmentation, controlled vendor remote access, identity and privilege, and hardening of engineering stations and SCADA.

SEGMENT · HARDEN · CONTROL

3 Monitor & hunt
Log sources and detection rules built for the site, proactive threat hunting, and targeted intelligence and OSINT on the site's assets and vendors.

DETECT · HUNT · INTELLIGENCE

4 Respond
Response plans and named roles, tabletop exercises, forensics and containment, and recovery proven by tested restores — not by a backup policy.

CONTAIN · RECOVER · LEARN

HUMAN-LED · PLANNED WITH OPERATIONS · AUTHORISED SCOPE · EVIDENCE AT EVERY STAGE

WHAT OreKeep DELIVERS

FIVE FAMILIES · TWENTY SERVICES

01 Governance, risk & privacy
- Cyber risk survey and defence plan
- Security leadership and vCISO
- Governance and audit readiness
- Privacy, data protection and DPO support

02 Systems, operations & data
- IT, cloud and endpoint hardening
- OT / ICS / SCADA defence
- Identity, privilege, remote access
- Data protection and leak prevention

03 Testing, monitoring & intelligence
- Penetration testing and red team
- Exposure and vulnerability management
- SOC / MDR build and uplift
- Threat intelligence and OSINT

04 Response, continuity & fraud
- Incident response and forensics
- Continuity and ransomware recovery
- Payment-fraud and BEC controls
- Training and executive exercises

05 Supply chain, secure build & AI
- Vendor and supply-chain security
- Secure architecture for new projects
- AI and autonomous-agent security
- AI automation for defence teams

WHO IT IS FOR

MINING · CRITICAL MINERALS · WATER · INDUSTRY · GOVERNMENT

Mining operations
Pit, plant, tailings and haulage systems, and the data behind them.

Critical minerals
Processing and recovery sites carrying strategic supply risk.

Water & wastewater
Treatment, desalination and distribution, where safety is the outcome.

Industrial supply chain
Vendors and integrators holding standing access to client systems.

Government
Public-sector and critical-infrastructure bodies and their assurance needs.

Human-led. AI-enabled. Operation-aware.

ASSESS · PROTECT · MONITOR · RESPOND

Dr. Ronny Banker CEO

PhD chemistry, MBA; 25+ years in water, cleantech, mining and environmental technology; registered US patents. Brings the operating-environment knowledge OT security depends on.

ronny@bankergroup.co · +972 55-504-5770

Idor Ovitz CTO

Cybersecurity leader and technology entrepreneur with extensive experience in cybersecurity consulting, cyber defence centre management, and Security Operations Centre (SOC) leadership. A certified Data Protection Officer (DPO), he combines operational security expertise with a background in cyber intelligence, investigations, risk management, and data protection. His work bridges cybersecurity and advanced AI, bringing together strategic advisory, operational leadership, and the design and implementation of intelligent systems for complex, data-sensitive environments.

+972 54-817-6921

Engagements HOW WE START

Engagements start with a scoped assessment of one site, or a focused review of a single question — remote access, segmentation, backups or vendor risk — and expand from the findings.

Remote and on-site · international engagements