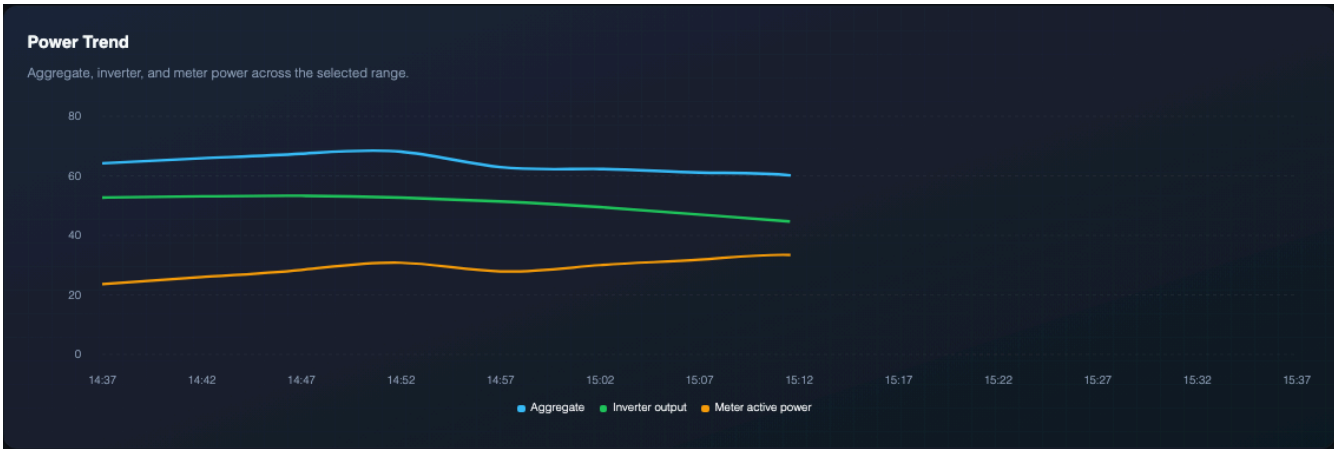
zcrOT · Brochure

Turn OT blind spots into a reviewable picture.

Understand which devices communicate, which events deserve attention and how energy telemetry relates to operations — with zcrOT.



Power Trend — compare the displayed telemetry series over time. Illustrative demo data, not customer results or performance evidence; English UI. The chart does not label its vertical-axis unit. Open full-size capture ↗

Three questions. One operational context.

What is connected?	Observe copied OT traffic passively from a network TAP, SPAN/mirror port or sensor feed, outside the control path. Map observed assets and communication relationships; distinguish known and unknown devices.
What changed?	Review Modbus-aware signals, behavior baselines and risk context using real/near-real-time sensor analysis and stored current/historical telemetry.
What should we share?	Use energy telemetry and weekly/monthly OT reports to support plant, security and management reviews.

> For operational technology (OT), industrial control system (ICS), plant, network and security teams — and their managed security service partners.

Fit the platform to your environment

zcrOT is available as SaaS, a VM or a Hardware Appliance. Select the deployment and data boundaries with an approved partner before specifying infrastructure.

Deployment	Planning considerations
Cloud / SaaS	Bundle: 1 Security Collector, zcrLog SaaS for 1 year and 1 OT Software Stack. Confirm data location and connectivity with your approved partner.
Virtual machine (VM)	Available on customer-managed infrastructure; the approved partner quotes compute, storage, interfaces and collection scope for your site.
Hardware Appliance	One-time bundle including year 1: 1 Collector, 1 zcrLog Server and 1 OT Software Stack. MA starts in year 2; the partner confirms the scoped proposal.

Current bundle prices, VAT and maintenance terms: see the pricing page. Collector quantities are physical units, not licensed network segments or capacity guarantees. View current package pricing ↗

Define the integration boundary

Besides passive traffic capture, zcrOT receives syslog on dedicated per-source ports. Use the API/integration framework for security operations, SIEM, monitoring and analytics workflows. Confirm fields, authentication and data direction; outbound syslog and named connectors are not promised.

zcrOT is a visibility and detection platform, not an inline control system. Scope collection, operational changes and response ownership with the plant team. Integration, coverage and isolated operation need site-specific validation.

Plan your evaluation with an approved partner

Bring a network sketch, segment/sensor estimates, required data sources and deployment constraints. An approved distributor, reseller/SI or MSP/MSSP handles commercial proposals, contracting and customer delivery. zcr.ai can help connect you with a partner.

Find a partner / discuss scope ↗ Explore zcrOT ↗ Try the public demo ↗

zcr.ai/en/contact/ · zcr.ai/en/product/zcrot/ · demo.ot.zcr.ai/

Illustrations and demo data explain workflows. They do not promise complete asset discovery, guaranteed prevention, customer outcomes or certification.