OT SECURITY / TECHNICAL DATASHEET

zcrOT

See OT communications. Investigate with context.

zcrOT brings passive network visibility, Modbus-aware detection and energy telemetry into one operational view for industrial and energy teams.

Delivery forms

- Cloud / SaaS
- Virtual machine
- Hardware appliance

1 **Observe** — TAP / SPAN and telemetry

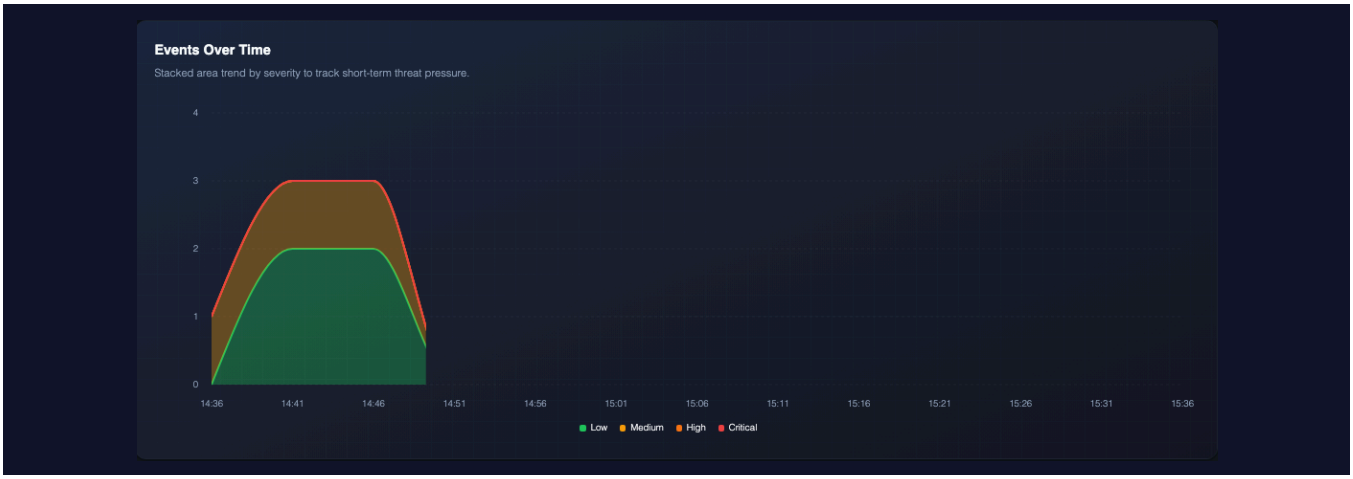
2 **Context** — Assets, paths, baselines

3 **Investigate** — Risk and event triage

4 **Report** — Weekly / monthly review

Conceptual operational workflow, not a physical deployment diagram. No control or blocking action is implied.

Observe the event trend



Security Exposure → Events Over Time: event count by severity across the selected window. Illustrative demo data; counts are not customer results, capacity limits or detection-accuracy measurements. The product UI shown is English. Open full-size capture

In this datasheet

2 Technical capabilities
3 Commercial terms and deployment
4 Deployment boundaries
5 Validate the evidence before rollout
6 Assets and protocol metadata
7 Detection and control reliability
8 Packet evidence and export
9 Correlation, operations and reports

TECHNICAL SCOPE

Technical capabilities

02

Use the observed network, protocol and telemetry context to decide which asset or event needs investigation.

Capability	Technical scope
Passive discovery	Observe OT traffic and the IT/OT boundary through a network TAP, SPAN / mirrored port or sensor feed. Coverage is limited by the capture scope.
Communication mapping	Show source, destination, protocol, port and direction; relate OT gateways and logical units to observed communication paths.
Modbus-aware detection	Classify read, write, error and malformed commands. Validate the required protocol versions and site-specific traffic during evaluation.
Identity and risk context	Tag known and unknown devices; use identity context, risk scores and attack-likelihood verdicts to prioritize review, not as proof of compromise.
Behavior baselines	Analyze sensor traffic in real or near real time; compare behavior with its baseline and examine changes. This is not a specified end-to-end latency guarantee.
Energy telemetry	Store and analyze current/historical telemetry, including solar output, electric vehicle (EV) charger status and factory power where data is available.
Source ingestion	Dedicated per-source syslog ingestion ports and live traffic counters help operators check whether expected inputs are arriving.
Triage and reporting	Review security events in an incident-triage workflow and generate weekly or monthly OT visibility and security reports. Reports support internal review; they do not establish certification.
API integration	An application programming interface (API) and integration framework support external security operations centers (SOC), security information and event management (SIEM), monitoring and analytics workflows. Confirm the exact interfaces and fields.

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

TECHNICAL SCOPE

Commercial terms and deployment

03

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	Package and commercial terms
zcrOT-Appliance	฿3,200,000 one-time, including the first year, excluding VAT. Includes 1 security collector unit, 1 zcrLog server unit and 1 zcrOT software stack. From year 2: annual maintenance (MA) at 30% of the net package price, ฿960,000/year plus VAT.
Cloud / SaaS	฿1,500,000/year, excluding VAT. Includes 1 security collector unit, zcrLog SaaS for 1 year and 1 zcrOT software stack.
Virtual machine (VM)	Customer-managed, on-premises VM remains available. An approved partner quotes the configuration, infrastructure and commercial scope; this bundle source sets no standalone VM price.

Included in both bundles

Integration and commissioning; AI detection models; threat intelligence and updates; Cloud API monitoring; support. Agree hardware specifications, implementation acceptance, renewal scope, support hours and SLA with the approved partner.

> As of 31 October 2026. All stated prices exclude VAT; VAT is added to the appliance, SaaS and annual MA charges. Appliance MA starts in year 2 at 30% of the net package price. The partner confirms the actual quotation and its validity.

Agree sizing, not demo numbers

Size by segments, collectors, observed traffic, telemetry sources, retention and report cadence. Included unit counts do not specify licensed segments or capacity. CPU, RAM, storage, throughput, sensor limits, additional collection points, VM pricing, hardware BOM and SLA require the scoped partner proposal. No default capacity is stated.

TECHNICAL SCOPE

Deployment boundaries

04

Passive, out-of-band visibility

The passive network workflow uses copied traffic rather than sitting inline with control traffic. It does not require endpoint agents for that workflow or directly control OT devices. Agree capture changes and change windows with the plant owner; “passive” is not a guarantee of zero deployment risk.

Isolated and offline environments

For proposed offline appliance monitoring, validate licensing, updates, support access, time synchronization and export procedures in the isolated environment. Not every integration can be assumed to work offline.

Define the integration boundary

Document source → collector → platform → downstream system. Confirm syslog/API formats, authentication, data direction and ownership. No named third-party connector or automatic response action is promised by this document.

> The channel partner provides first-line support; zcr supports the partner. Support hours, escalation, SLA, implementation scope and maintenance responsibilities are agreed in the proposal.

What is happening across your OT network?

Map observed assets and communication paths, distinguish known from unknown devices, and use protocol context to review unusual activity. Visibility depends on the traffic and telemetry made available to the platform.

TECHNICAL SCOPE

Validate the evidence before rollout

05

A focused evaluation should produce an agreed visibility boundary and an operational handover, not just a dashboard screenshot.

Evaluation area	What to verify
Capture scope	Identify segments, capture points, interfaces and the traffic that cannot be observed.
Protocols and devices	Check representative Modbus read/write/error traffic, gateways and known/unknown device labeling.
Telemetry and events	Confirm source counters, timestamp alignment, energy units and event context using the site's approved test data.
Operations	Agree retention, report cadence, access ownership, support and maintenance responsibilities.

Agree sizing, not demo numbers

Size by segments, collectors, observed traffic, telemetry sources, retention and report cadence. Included unit counts do not specify licensed segments or capacity. CPU, RAM, storage, throughput, sensor limits, additional collection points, VM pricing, hardware BOM and SLA require the scoped partner proposal. No default capacity is stated.

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

TECHNICAL SCOPE · AGREED DEPLOYMENT

Assets and protocol metadata

06

Validate the exact fields, protocol coverage and filters against representative site traffic.

Technical scope · agreed deployment

These capabilities are available for the agreed deployment. Agree acceptance criteria with your partner for sources, protocol versions, interfaces, access and retention. Validate required interoperability and isolated operation before rollout. No capacity, performance, certification or SLA guarantee is implied.

Capability	Technical scope
Asset detail	IP and MAC addresses, protocol, port, device type, logical unit, communication direction and mapping status. Naming, descriptions and grouping distinguish known/unknown devices, engineering workstations, network infrastructure, industrial gateways and other OT assets.
Paths and filters	Internal, external, top and previously unseen communication paths; communication volume. Filter by time, device, protocol, risk level and direction. Compare baselines to investigate unknown devices, external destinations, changed paths and possible lateral movement or command and control.
Gateway context	Distinguish directly observed Ethernet/IP assets from logical OT units identified through gateway telemetry; an IP address alone may not identify each unit.
Metadata fields	Timestamp, source IP/MAC, destination IP/MAC, protocol, port, direction, session context, classification and related anomaly status. Query and relate metadata without opening raw packets for every investigation.
Protocol list	HTTP, DNS, SMB, HTTPS, TLS, TCP, UDP, ICMP, SNMP, Modbus TCP and EtherNet/IP. Exact parser versions and field coverage require validation; the list is not an interoperability certification.
Application fields	HTTP: method, host, URI, status code, user agent and direction. DNS: query, response, record type, resolved IP and anomalous behavior. SMB: session, user, share, file operation and activity relevant to lateral movement.

TECHNICAL SCOPE · AGREED DEPLOYMENT

Detection and control reliability

07

Validate rule behavior and operational signals without interpreting them as guaranteed prevention or detection accuracy.

Technical scope · agreed deployment

These capabilities are available for the agreed deployment. Agree acceptance criteria with your partner for sources, protocol versions, interfaces, access and retention. Validate required interoperability and isolated operation before rollout. No capacity, performance, certification or SLA guarantee is implied.

Capability	Technical scope
Modbus reliability	Unit/operation-level request volume, error count, response time, slow poll, success rate and logical-unit status. Compare historical behavior to investigate operational degradation and potential production impact; no throughput or latency value is specified.
Operational anomalies	Unusual requests or previously unseen functions, unauthorized unit access, increased errors, abnormal response times and activity outside operating hours.
Rule inputs	Default and custom rules using traffic, protocol metadata, asset context and operational telemetry. Conditions: source, destination, protocol, port, direction, asset, time window, baseline, severity and event classification.
Detection examples	Unknown client, new path, external communication, activity outside business hours, unauthorized protocol, suspicious port, Modbus disruption, abnormal request volume, repeated error, slow poll and baseline deviations.
Prioritization and tuning	Severity, risk score, verdict and classification; allowlists for approved activity and rule tuning. Validate the effect on false positives rather than assuming a guaranteed reduction.
Exposure and lifecycle	Security events, high/critical events, unknown clients, likely-attack verdicts, trends, verdict distribution and top-risk sources; event-detail/evidence drill-down. Related incidents include asset, alert, protocol, source/destination, severity, timeline and evidence from initial detection through closure.

TECHNICAL SCOPE · AGREED DEPLOYMENT

Packet evidence and export

08

Validate capture, retention, access and export behavior before relying on packet evidence.

Technical scope · agreed deployment

These capabilities are available for the agreed deployment. Agree acceptance criteria with your partner for sources, protocol versions, interfaces, access and retention. Validate required interoperability and isolated operation before rollout. No capacity, performance, certification or SLA guarantee is implied.

Capability	Technical scope
Capture format	Full packet capture through an on-site network sensor, with PCAP or PCAPNG evidence for network and OT investigation. Confirm actual capture interfaces, capacity, storage and retention; none is specified here.
Capture policy	Sensor, network segment, protocol, asset, time window, detection rule and severity control packet scope and volume, with priority for critical systems and assets.
Triggered evidence	An IDS signature match triggers automatic related PCAP recording before, during and after detection and links the file to the alert or incident. Validate buffering, trigger timing and behavior in the proposed deployment.
Incident references	Sensor, capture time, source IP, destination IP, protocol, file size, file hash and incident reference in the incident workspace. A displayed hash alone does not certify chain of custody.
Authorized export	Authorized users copy, download or export incident-related PCAP through a secure channel for Wireshark or external network-forensics analysis.
Export continuity	Retain timestamps, capture metadata, incident reference and required audit references so SOC, incident-response and digital-forensics teams can analyze evidence outside the platform. Confirm permissions, transfer method and preserved fields.

TECHNICAL SCOPE · AGREED DEPLOYMENT

Correlation, operations and reports

09

Validate cross-system relationships, administration and report contents in the proposed edition.

Technical scope · agreed deployment

These capabilities are available for the agreed deployment. Agree acceptance criteria with your partner for sources, protocol versions, interfaces, access and retention. Validate required interoperability and isolated operation before rollout. No capacity, performance, certification or SLA guarantee is implied.

Capability	Technical scope
Cross-system correlation	Automatic grouping of network, endpoint, identity/user, cloud and other security-control events into one case/incident. Confirm matching logic, available inputs and edition; automatic response is not implied.
Relations and root cause	Alert, entity, host, user, IP, asset, process, file and network session relationships with timeline/kill-chain views. Trace initial activity, lateral movement, command and control, data access and impact using network/endpoint/identity/cloud/control events, metadata, detections and PCAP.
EDR and external inputs	API, Webhook, Syslog and integration framework; endpoint alert, process, command line, file, hash, user, network connection and mitigation-action context. Validate connections to EDR, SIEM, identity, cloud, firewall, IDS/IPS, ticketing and monitoring systems. No named connector or mitigation execution is established.
Administration	Central views of assets, paths, exposure, incidents, power, ports, user access and input health. Map device names/types/details by IP, MAC or Modbus Unit ID. Manage dedicated syslog ports, sensor inputs and telemetry sources; last activity/counters and add/disable/edit actions require confirmation.
Reporting	Executive Summary and OT Visibility & Security Report: observed assets, known/unknown devices, paths, events, high/critical events, incidents, top-risk sources, control reliability and overall risk posture. Validate chosen periods, trends, key-event summaries and export for management, OT, security and internal review.
Isolated operation	Plan on-premises VM/appliance for the agreed offline or isolated environment. Confirm data-residency, licensing, updates, time synchronization, support and export. Do not assume all integrations work offline.