Security analytics software · partner-led evaluation

zcrSIEM

Validate the sources, workflow and package that fit your team.

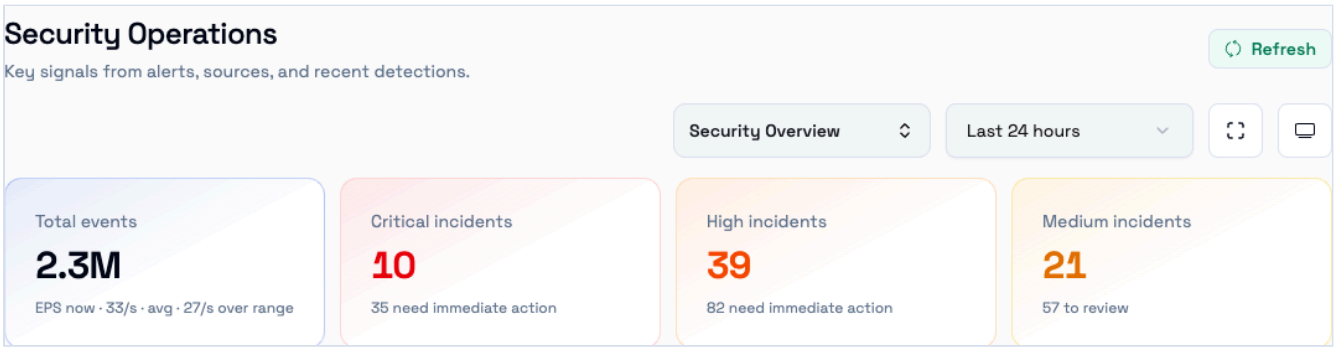
Detect, investigate, and connect security events in one analyst workflow.

SOC, MDR, MSSP, CISO, and enterprise security teams

> zcrSIEM collects its own sources. zcrLog is not required. Managed monitoring and incident-response services are contracted separately; automated playbooks are a separate zcrSOAR product.

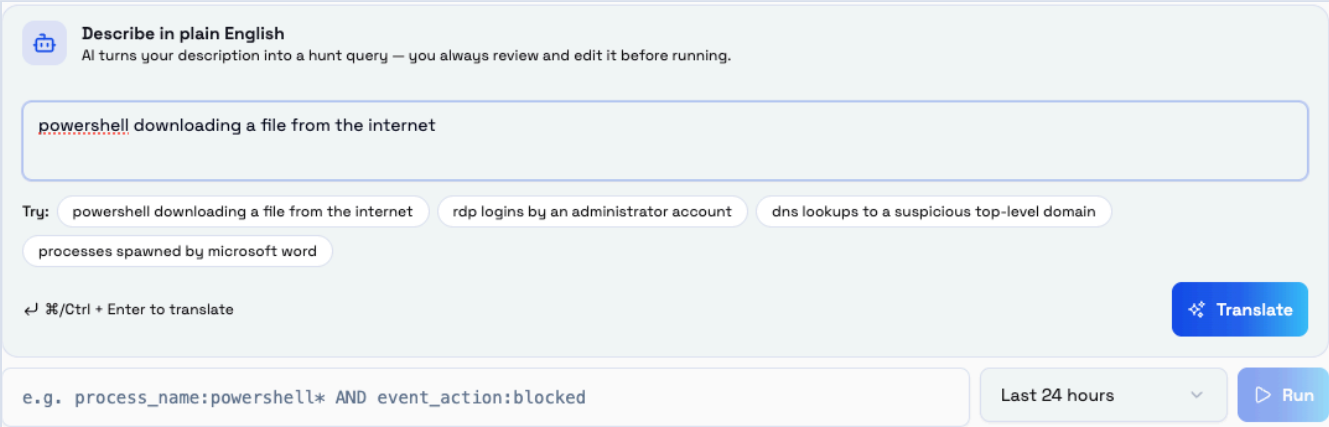
Data sources and integrations

SOURCE FAMILIES	Network devices · Firewalls · IDS/IPS · Windows and Linux · Identity systems · Endpoint security · Email security · Cloud platforms · Containers and Kubernetes · EDR, NDR, and network sensors
CLOUD PLATFORMS	AWS · Azure · Google Cloud · Huawei Cloud · GDCC Cloud · GDCC OpenData, connected through API, Webhook, Syslog, or native connector
ENDPOINT, EMAIL, NETWORK	Windows, Linux, and macOS endpoint signals · Microsoft Defender for Office 365 · NDR, network sensors, and IDS/IPS
THREAT INTELLIGENCE	Open-source and commercial threat intelligence through API, feeds, and STIX/TAXII
COLLECTION	zcrSIEM ingests its own sources directly, with its own daily ingest capacity on every package. zcrLog is not required.

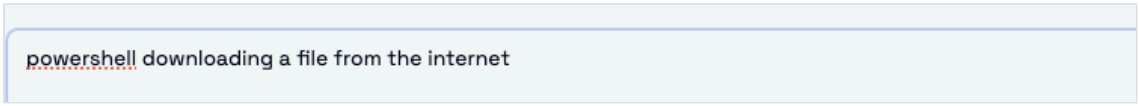


Security Operations — the overview groups sample events and incidents by severity. Illustrative demo data, not customer volume, capacity or performance evidence; English UI. Open original capture ↗

Ask a question. Review the query. Choose when to run it.



Threat Hunting — the question and query controls in the example console, before translation or execution. Illustrative demo data; English UI, not a customer investigation or detection result. Open original capture ↗



Detail of the typed example question. The original field continues beyond this crop; the question text is retained in full. Open original capture ↗

01

Describe

State the investigation question.

02

Review

Inspect and edit the generated query before running it.

03

Run

The analyst chooses to execute the reviewed query.

The example console requests English input. Confirm your required input languages in the partner technical demo.

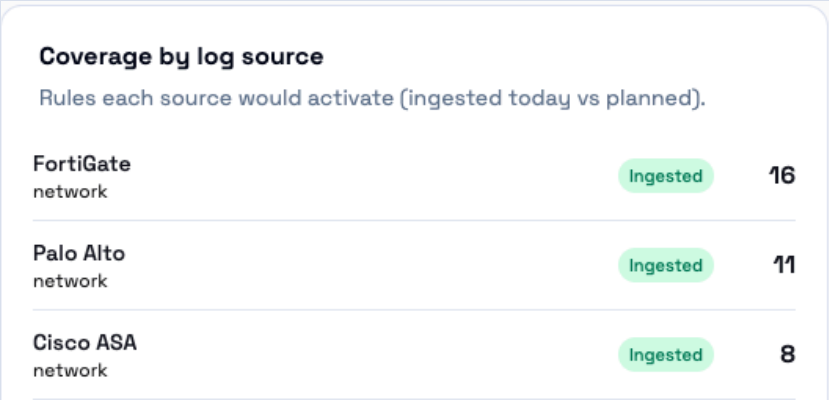
Core capabilities

- AI-assisted threat detection and event correlation
- Describe a threat in plain language and review the generated query before running it
- Investigate with MITRE ATT&CK context and detection coverage tracking

Capacity, retention, onboarding, implementation, integrations, support, and SLA are confirmed in the applicable solution design and quotation.

Use the zcrSIEM Brochure for the concise investigation story. This overview supports technical and package evaluation.

See which sources activate your detection rules.



Detection Coverage — three complete example log-source rows and their rule counts. Selected rows, not the full source catalog. Illustrative demo data, not detection effectiveness or a coverage guarantee; English UI. Open original capture ↗

- Sync Sigma and Elastic rules and see coverage by tactic and log source
- Real-time dashboards, alerts, and response visibility
- Move from alert to incident workflow, MDR reporting, and executive communication
- Multi-tenant operation with isolated data and policies, the same on cloud and on-premises, and unlimited tenants and users on every package

From signal to accountable response

01 / DETECT
Correlate events and surface suspicious activity.

02 / INVESTIGATE
Pivot through related events with reviewable hunting queries.

03 / RESPOND
Track incidents, ownership, and response progress.

04 / REPORT
Turn operational evidence into MDR and executive reports.

zcrSIEM is software. Incidents, dashboards, and MDR or executive reports in the console do not mean analyst monitoring or incident-response services are included; those are separate services.

Packages and pricing

Package	Daily ingest	Retention	Price per month (VAT incl.)
SaaS (Cloud)			
zcrSIEM-1	1 GB	90 days	฿6,000
zcrSIEM-3	3 GB	90 days	฿18,000
zcrSIEM-5	5 GB	90 days	฿30,000
zcrSIEM-10	10 GB	90 days	฿45,000
On-premises (Software)			
SITE-10	10 GB	Per customer-provided storage	฿31,500
SITE-20	20 GB	Per customer-provided storage	฿52,500
SITE-50	50 GB	Per customer-provided storage	฿92,400
SITE-100	100 GB	Per customer-provided storage	฿158,900

Every package is billed monthly on a 12-month term, VAT included, with unlimited tenants and users. On-premises packages are software only and run on your own hardware or VMs.

> On-premises installation and configuration are quoted separately from the monthly subscription, according to the actual scope, through the approved partner commercial path.

Your approved channel partner provides first-line support; zcr provides product support to that partner. Support commitments are set in the applicable agreement.

Plan a technical evaluation with an approved partner.

Bring source inventory, estimated daily ingest, retention needs and your deployment preference. Your partner confirms the scope, solution design and quotation.

Discuss the evaluation with a partner ↗ Product resources ↗