Security analytics software · partner-led evaluation

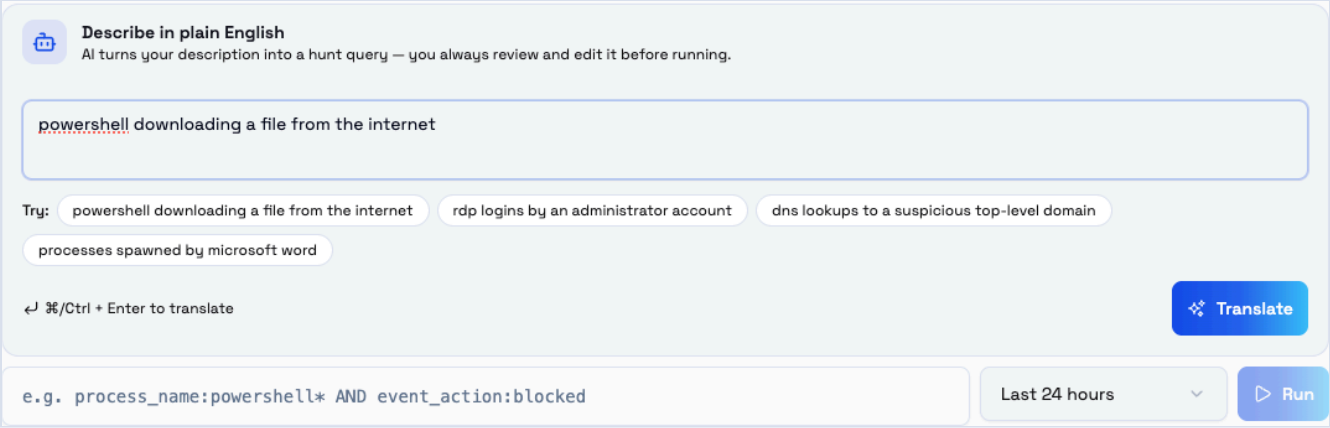
zcrSIEM

Turn security signals into a reviewable investigation.

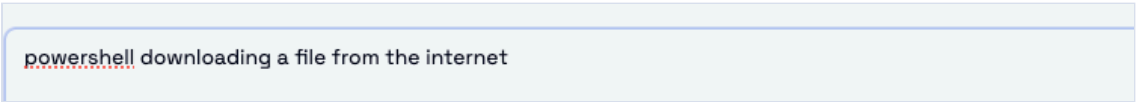
Detect, investigate, and connect security events in one analyst workflow.

> 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.

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.

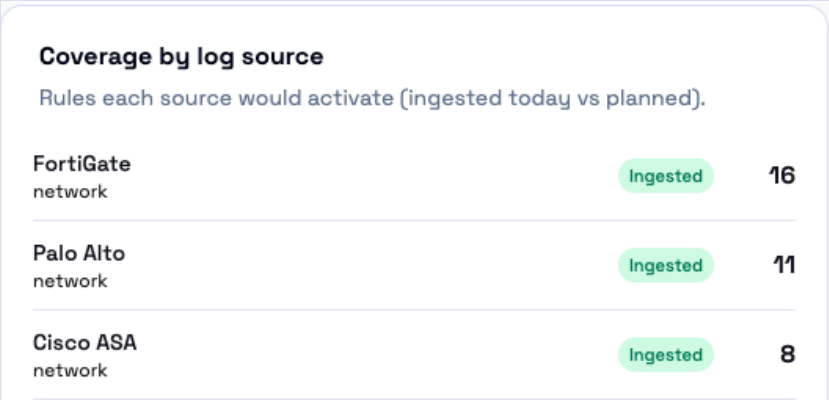
03

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.

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 ↗

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
- Sync Sigma and Elastic rules and see coverage by tactic and log source

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.

Match the software to your operating model.

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

THE OPERATING GAP	Security data, disconnected tools, and alert volume make it difficult to decide what happened and what to do next.
SECURITY DATA SOURCES	Firewall · Active Directory · Endpoint · Network · Microsoft 365 · Cloud services
OPERATING MODEL	Cloud / SaaS or on-premises software, confirmed in solution design
COLLECTION	zcrSIEM ingests its own sources directly, with its own daily ingest capacity on every package. zcrLog is not required.

- 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

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.

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

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

Continue with the zcrSIEM Product Overview for source families, deployment, packages and evaluation scope.

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 ↗