

AI-POWERED SIEM

zcrSIEM

AI-powered security information and event management

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

BUILT FOR	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

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
- 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

Data sources and integrations

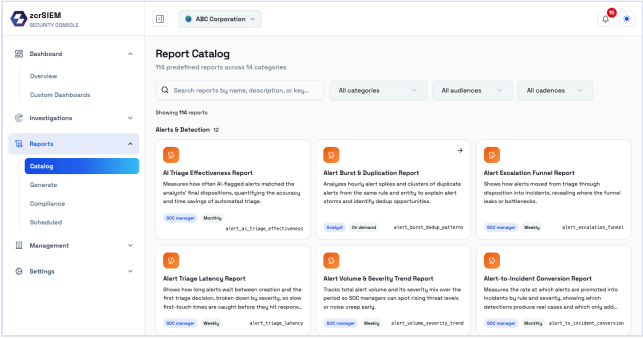
SOURCE FAMILIES	Network devices · Firewalls · IDS/IPS · Windows and Linux · Identity systems · Endpoint security · Email security · Cloud platforms · Containers and Kubernetes · EDR, NDR, and network sensors
CLOUD PLATFORMS	AWS · Azure · Google Cloud · Huawei Cloud · GDCC Cloud · GDCC OpenData, connected 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.

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.



Security operations dashboard — Illustrative demo data, not live figures



Report catalog — Illustrative demo data, not live figures

In the console

The screenshot shows the 'Threat Hunting' section of the zcrSIEM Security Console. The left sidebar contains navigation links: Dashboard, Overview, Custom Dashboards, Investigations (selected), Incidents, Alerts, Log Search, Threat Hunting (highlighted), Detection Rules, Asset Inventory, Threat Intel, Reports, and Management. The main content area is titled 'Threat Hunting' and includes a description: 'Search normalized telemetry, investigate patterns, and save repeatable hunts.' Below this are two tabs: 'Query Workspace' (selected) and 'Hunt Library'. The 'Query Workspace' tab contains a text input field with the query 'powershell downloading a file from the internet'. Below the input field are two rows of tags: 'powershell downloading a file from the internet', 'rdp logins by an administrator account', 'dns lookups to a suspicious top-level domain', and 'processes spawned by microsoft word'. A 'Translate' button is located to the right of the tags. Below the tags is a text input field with the example query 'e.g. process_name:powershell* AND event_action:blocked'. To the right of this field is a 'Last 24 hours' dropdown menu and a 'Run' button. At the bottom of the main content area, there is a note: 'field:value · combine with AND OR NOT · wildcard * · numeric > < >= <= · quote values with spaces'.

AI-assisted threat hunting — Illustrative demo data, not live figures

The screenshot shows the 'Detection Coverage' section of the zcrSIEM Security Console. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Detection Coverage' and includes a description: 'Measure source and MITRE ATT&CK coverage to expose detection blind spots.' Below this are three tabs: 'Rule Catalog' (selected), 'Coverage', and 'Engine Health'. The 'Rule Catalog' tab contains a table with the following data:

Source	Status	Count
FortiGate network	Ingested	16
Palo Alto network	Ingested	11
Cisco ASA network	Ingested	8
Sangfor NGAF network	Ingested	6
Sangfor Proxy proxy	Ingested	7
CrowdStrike Falcon endpoint	Ingested	12

To the right of the table is a 'MITRE ATT&CK coverage by tactic' section. It contains a horizontal bar chart showing the coverage of various MITRE ATT&CK techniques. The techniques and their coverage are:

Tactic	Coverage
Reconnaissance	100%
Initial Access	100%
Execution	100%
Persistence	100%
Privilege Escalation	100%
Defense Evasion	100%
Credential Access	100%
Discovery	100%

MITRE ATT&CK coverage — Illustrative demo data, not live figures

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.

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

Talk to a zcr channel partner for a technical demo and solution-fit discussion.

Your partner runs the technical demo, sizes the deployment with your team, and prepares the solution design and quotation.

Partner-led evaluation ↗

zcr.ai/contact/?lng=en