

AI-POWERED SIEM

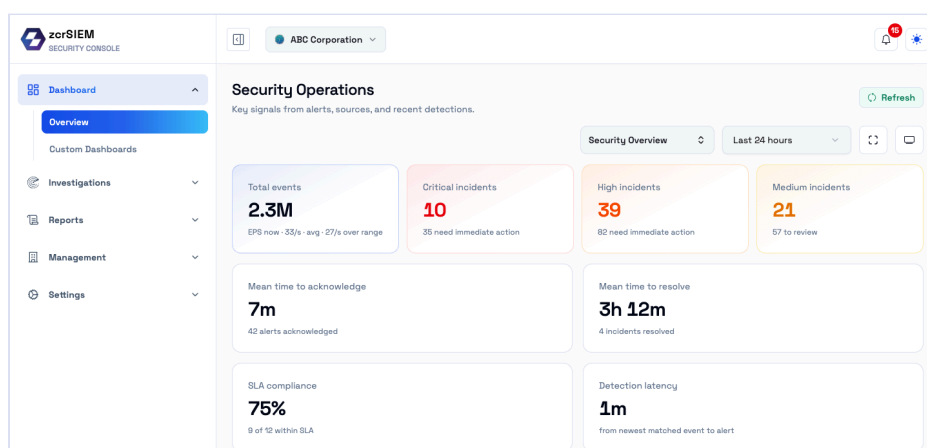
zcrSIEM**AI-powered security information and event management**

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.

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



Security operations dashboard — Illustrative demo data, not live figures

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.

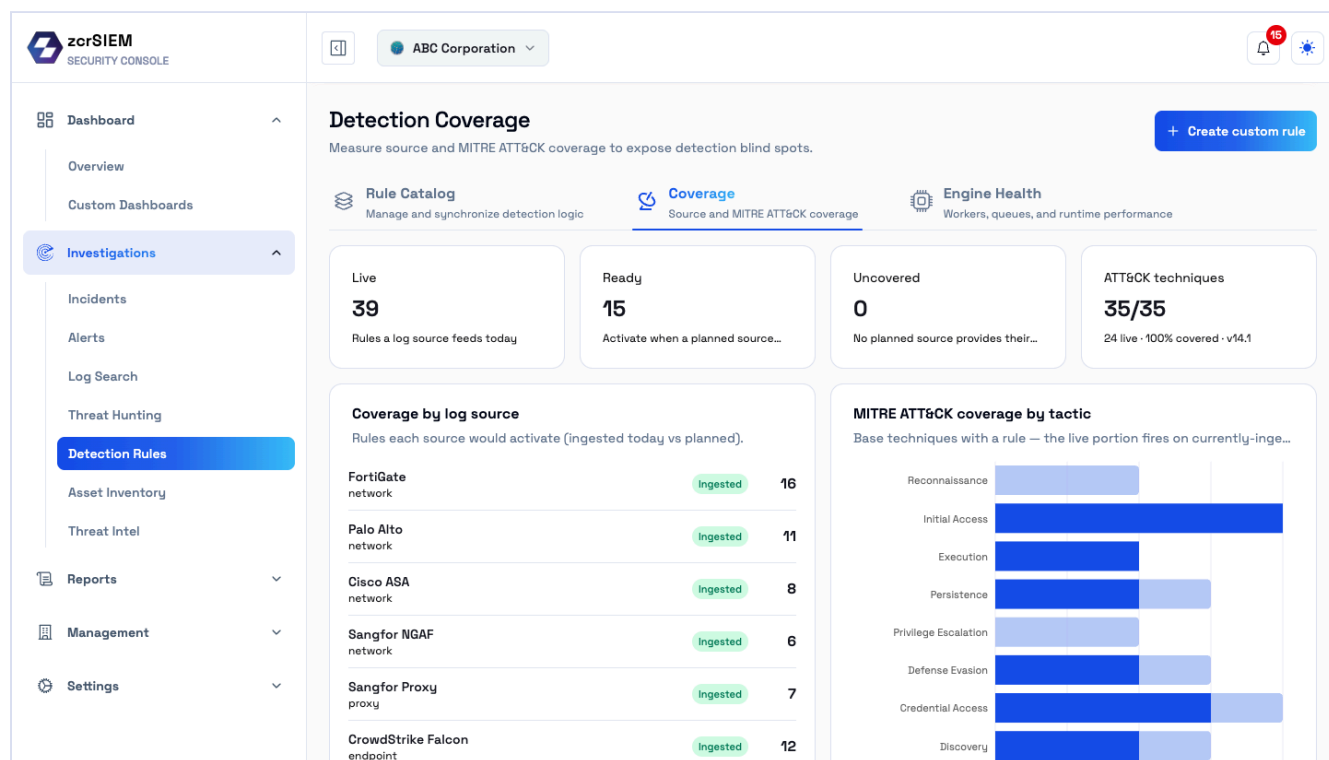
The screenshot displays the zcrSIEM Security Console interface. On the left is a sidebar with navigation links: Dashboard, Overview, Custom Dashboards, Investigations (selected), Incidents, Alerts, Log Search, Threat Hunting, Detection Rules, Asset Inventory, Threat Intel, Reports, and Management. The 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' (active) and 'Hunt Library'. The 'Query Workspace' tab contains a text input field with the query 'powershell downloading a file from the internet'. Above the input is a 'Describe in plain English' button. Below the input is a 'Try:' section with several suggested queries: '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 input field. At the bottom, there is a 'Run' button and a 'Last 24 hours' dropdown menu. A footer note states: 'field:value · combine with AND OR NOT · wildcard * · numeric > < >= <= · quote values with spaces'.

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

Data sources and deployment

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.

In the console



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

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