CONTINUOUS THREAT EXPOSURE MANAGEMENT

zcrCTEM

See your exposure.
Prioritize the next action.

CTEM platform: EASM maps your attack surface, CAASM finds security-tool coverage gaps and DRP tracks dark web findings, while analysts approve AI proposals.

EASM · CAASM · DRP · Threat Intel · Takedown · AI proposes, analysts decide

Deployment options

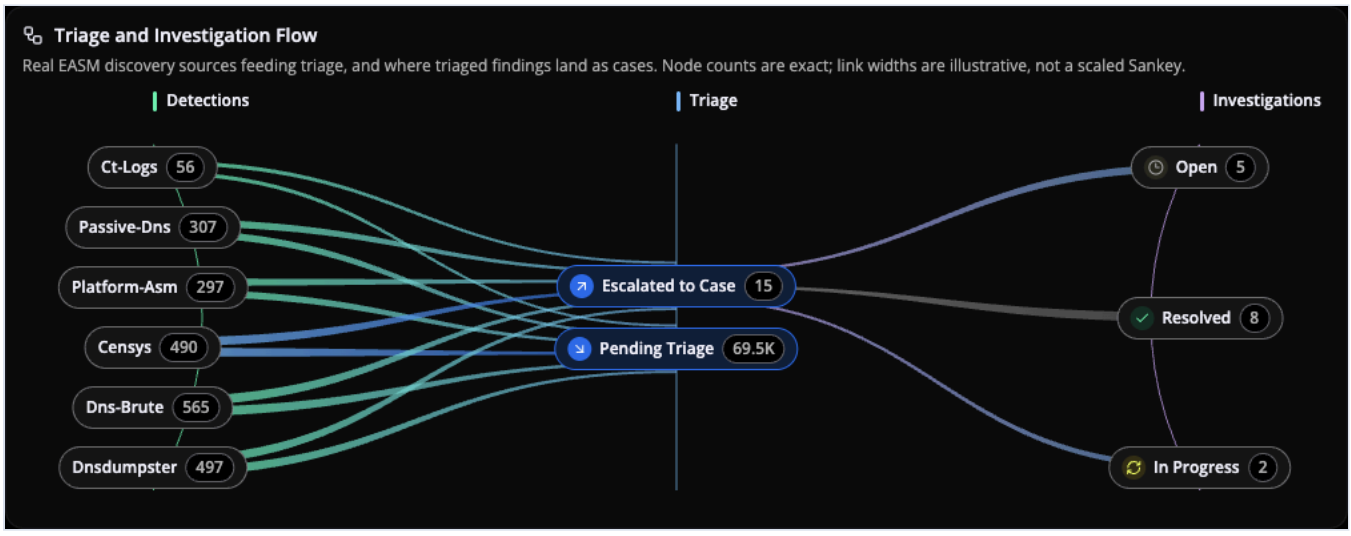
Cloud / SaaS

On-premises software

01	02	03	04
Discover	**Prioritize**	**Investigate**	**Act with approval**

Conceptual operating workflow, not a physical deployment architecture.

Agentic SOC dashboard



Trace sample-tenant discovery sources through pending triage or escalation to cases, then see investigation states. Flow widths are illustrative, not a performance measure. Real screen from the public demo. Values on screen are sample data.

Actual public-demo capture. Tenant values and flow widths are illustrative, not measured performance.

Evaluate scope and modules with a partner

Explore the demo ↗ Find a partner ↗

PRODUCT DETAIL

Operating workflow

02

Built for

Security operations teams, vulnerability management teams, risk and third-party risk teams, MSSPs managing multiple tenants, and CISOs

The operating gap

External scans, EDR and vulnerability consoles, dark web feeds and vendor questionnaires each hold part of the picture. When a connector quietly stops syncing, nobody notices, and the team keeps prioritizing from a view that is already out of date.

Deployment

Cloud / SaaS or on-premises software, confirmed in solution design.

How it works

Discovery, prioritization and investigation end in an action a person signs off.

01 / DISCOVER
Set seed domains and scope rules. EASM keeps discovering, CAASM pulls assets from connected tools, and Sync Health warns when a source goes quiet.

02 / PRIORITIZE
Rank findings by risk score, EPSS and the business tier you assign, so crown-jewel assets come first.

03 / INVESTIGATE
Open a finding or dark web signal to see the evidence, confidence, MITRE ATT&CK mapping and matching assets.

04 / ACT WITH APPROVAL
Agents and the AI assistant draft tickets and takedown requests. An analyst approves or rejects each one, and the audit trail keeps the record.

PRODUCT DETAIL

Core capabilities

03

Core capabilities

Agentic SOC dashboard that traces discovery sources through triage or escalation to cases, then to investigation states
EASM discovery from seed domains, with include/exclude scope rules by subdomain, CIDR or ASN
Findings for vulnerabilities, certificates and open ports, with risk score, EPSS for CVEs and redacted evidence
Priority tiers such as crown jewels, set by the business and kept separate from technical severity
CAASM inventory showing EDR, vulnerability-scan and cloud-posture coverage per asset, with Sync Health alerts when a source goes quiet
Threat Intelligence for dark web findings, with confidence scoring, MITRE ATT&CK mapping and asset correlation
DRP takedown policies, incident case tracking and third-party security questionnaires
Agentic workflows and an AI assistant that draft work for review, logged in an audit trail, with analyst approval before an AI-drafted ticket or takedown moves
Risk scenarios plotted by likelihood and loss magnitude, with annualized loss and evidence links
AI & Compliance module: PDPA/CII readiness, breach-notification drafts and AI-assisted compliance reporting

Finding detail

Open a finding to see its risk score, EPSS where a CVE applies, detected ports, redacted evidence and investigation path before you mobilize a ticket. Real screen from the public demo. Values on screen are sample data.

Open original capture ↗

PRODUCT DETAIL

EASM and CAASM

04

EASM

Map what you expose to the internet, starting from your own root domains

- Discovery from seed domains, with bulk import and include/exclude rules by subdomain, CIDR or ASN
- Findings for vulnerabilities, certificates and open ports, with a risk score and EPSS for CVEs
- Priority tiers such as crown jewels, kept separate from technical severity, with auto-assign by severity
- A change log of who enabled or edited seed domains and scope rules

CAASM

Know which assets your security tools actually cover

- One canonical inventory of hosts, devices and cloud resources merged from connected sources
- Per-asset coverage for EDR, vulnerability scanning and cloud posture: present, missing or unknown
- A risk score and an internet-safety status for each asset
- Sync Health warns of a blind spot when a source disconnects, degrades or stops reporting

Scope & Discovery

Set the seed domains, include/exclude rules and discovery sources that the next EASM sync runs against. Real screen from the public demo. Values on screen are sample data.

Open original capture ↗

Asset inventory

Review every asset's EDR, vulnerability-scan and cloud-posture coverage, risk score and priority tier in one CAASM inventory. Real screen from the public demo. Values on screen are sample data.

Open original capture ↗

PRODUCT DETAIL

DRP, Threat Intelligence

05

DRP

Act on impersonation and third-party risk, with takedowns under policy

- Detects look-alike domains, fake mobile apps and messaging channels exposing your organization
- Protected-asset policies set whether takedown is allowed, how many approvals it needs and whether rollback is required
- Incident cases that group correlated findings, with severity, status, SLA and assignee
- A third-party vendor registry with security questionnaires and reusable templates

Threat Intelligence

Decide whether a dark web finding is really about you

- Dark web findings for leaked credentials, stealer logs, ransomware leak-site posts and exposed source code
- A confidence score that shows which evidence was checked and what is still missing
- MITRE ATT&CK mapping, correlation to EASM inventory and cited public incidents with similar signals
- Separate Darkweb, Email Security and Briefs views, with triage and ticket creation on dark web findings

Threat assessment

Weigh a dark web finding by its confidence, the evidence still missing, MITRE ATT&CK techniques and matching assets, then triage it or create a ticket. Real screen from the public demo. Values on screen are sample data.

Open original capture ↗

PRODUCT DETAIL

AI & Compliance

06

01

Readiness

PDPA / CII

02

Notification drafts

Breach notification

03

Reporting support

AI-assisted reporting

A separately priced module for compliance preparation and reporting

- PDPA/CII readiness and breach-notification drafts
- AI-assisted compliance reporting
- Confirm the applicable framework, evidence requirements and workflow with an approved partner; this document does not establish certification or legal compliance.

Public demo

The public demo runs on sample data and covers EASM, CAASM, DRP, threat intelligence, agentic workflows and the audit trail. The compliance module is not in the demo; request a partner-led walkthrough.

> Threat Intelligence is quoted separately; it is not automatically included in the four modules priced in this datasheet or their four-module bundle discount.

Evaluate scope and modules with a partner

Confirm asset scope, modules, integrations and operating responsibilities with your partner.

Find a partner ↗

PRODUCT DETAIL

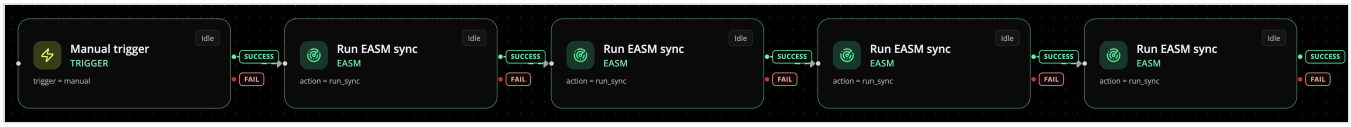
Agentic workflow

07

Agent workflow canvas

Build an agent as a chain of trigger and action steps with success and failure branches, then activate it or run it on demand. Real screen from the public demo. Values on screen are sample data.

Open original capture ↗



Complete fitted view: manual trigger → four EASM sync actions. Success/failure outputs and both ends are visible; the nodes are Idle. This screen does not show an executed ticket or takedown. Open original capture ↗

Real public-demo screen · Sample tenant and values · English UI retained



Enlarged start of the same chain. Configure trigger/action steps and success/failure branches; activate the workflow or run it on demand. In this read-only sample, failure outputs are visible but unconnected. Open original capture ↗

Real public-demo screen · Sample tenant and values · English UI retained

The workflow and audit screens show separate sample views, not a verified end-to-end execution of the same case.

PRODUCT DETAIL

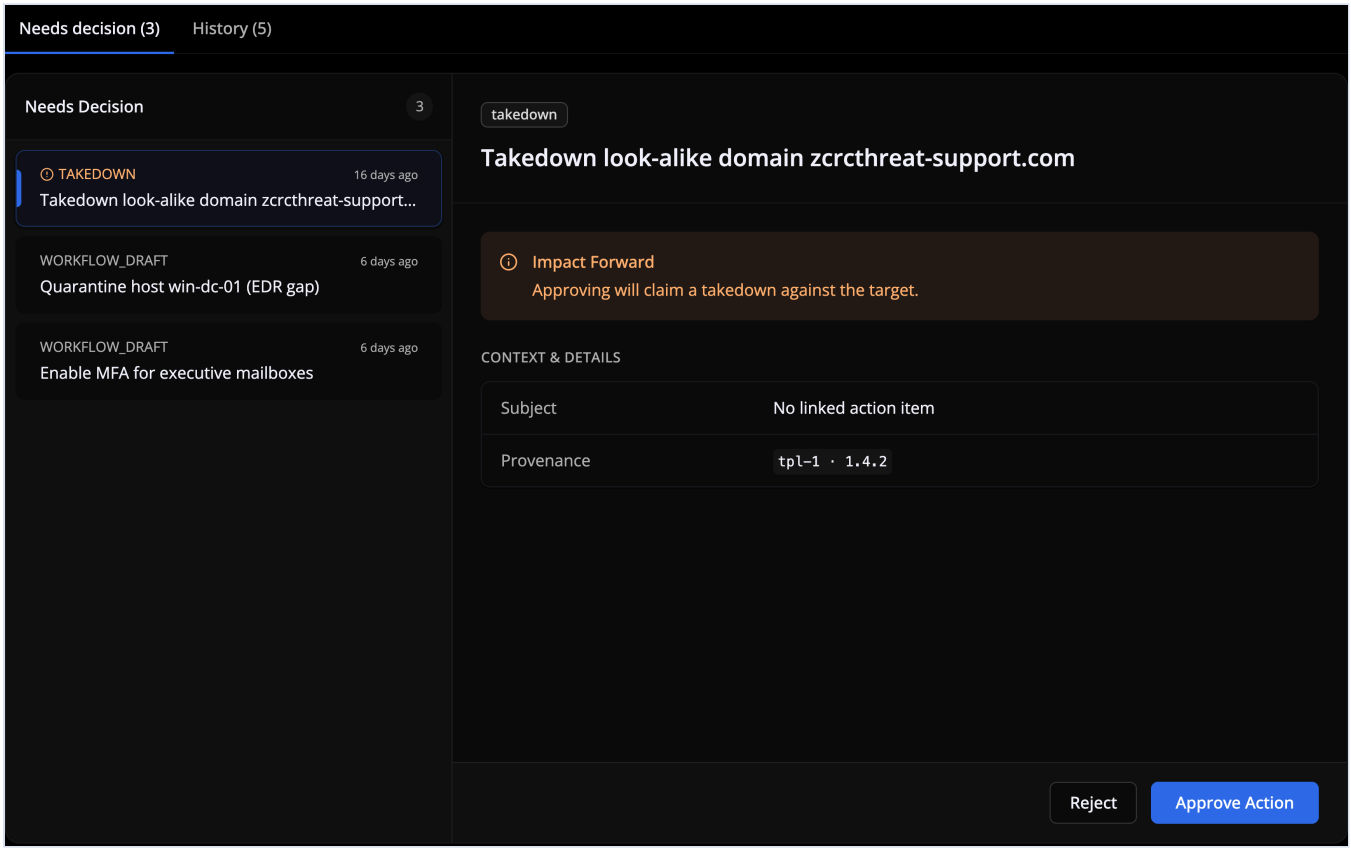
Evidence and approval

08

Audit trail

Approve or reject AI-drafted ticket and takedown proposals, with each draft traced to the template and version that produced it. Real screen from the public demo. Values on screen are sample data.

Open original capture ↗



A complete visible takedown proposal with template tpl-1, version 1.4.2, and Approve / Reject controls. It is awaiting a decision; no approval or takedown was performed for this datasheet. Open original capture ↗

Real public-demo screen · Sample tenant and values · English UI retained

The workflow and audit screens show separate sample views, not a verified end-to-end execution of the same case.

PRODUCT DETAIL

Packages and billing units

09

Packages

EASM — from ฿10,600/mo	External attack surface discovery, 5 tiers CTEM1-5 up to 2,000 assets (฿10,600-85,500/mo), +฿21/asset/mo beyond. Priced on countable assets — domains, subdomains, public IPs, SSL/TLS certs. Billed monthly on a 12-month term, VAT included.
CAASM — from ฿10,600/mo	Cloud + internal asset inventory (AWS/Azure/GCP/M365/OT), 5 tiers up to 20,000 assets (฿10,600-85,500/mo, priced identically to EASM), +฿2.35/asset/mo beyond. Billed monthly on a 12-month term, VAT included.
DRP + Dark Web — from ฿21,300/mo	Digital risk protection and dark web monitoring with takedowns, 5 tiers up to 100 monitored keywords (฿21,300-160,400/mo), +฿856/keyword/mo beyond. Includes 3-60 takedown requests/year by tier. Billed monthly on a 12-month term, VAT included.
AI & Compliance — from ฿10,600/mo	PDPA/CII readiness, breach notification, AI compliance reporting, 5 tiers up to 10,000 employees (฿10,600-96,200/mo), +฿5.35/employee/mo beyond. Billed monthly on a 12-month term, VAT included.

Each module is priced on its own unit. Billed monthly on a 12-month term, VAT included. Full tiers and the 4-module bundle discount: zcr.ai/pricing/

Reference prices are in Thai baht (THB), VAT included, billed monthly on a 12-month term. Your partner confirms proposal and scope before ordering.

> Threat Intelligence is quoted separately; it is not automatically included in the four modules priced in this datasheet or their four-module bundle discount.

Delivery boundary

Takedown success is not guaranteed — it depends on cooperation from the hosting provider or registrar involved.

PRODUCT DETAIL

Partner-led evaluation

10

FAQ

What does zcrCTEM cover?

zcrCTEM covers the external attack surface (EASM), internal and cloud asset coverage (CAASM), digital risk protection (DRP) and threat intelligence in one console. Compliance reporting for PDPA and CII is available as the separately priced AI & Compliance module.

Does the AI take action on its own?

Only for routine steps you configure, such as running a sync. A ticket or takedown drafted by AI stays a proposal until an analyst approves or rejects it, and every AI answer and draft is recorded in the audit trail with the template and version that produced it.

Is compliance reporting shown in the public demo?

No. The public demo covers the exposure workspace: EASM, CAASM, DRP, threat intelligence and agentic workflows. PDPA/CII readiness, breach notification drafts and AI compliance reporting belong to the AI & Compliance module; request a walkthrough through an approved zcr partner.

Scope check

Asset scope, modules, onboarding, implementation, integrations, support, SLA and pricing are confirmed in the solution design and quotation.

Request a partner-led evaluation through an approved zcr partner

Try the zcrCTEM demo, no login needed

Partner-led evaluation ↗ Current packages ↗ Explore the demo ↗

zcr.ai/contact/?lng=en · zcr.ai/pricing/?lng=en · demo.zcrctem.zcr.ai/dashboards