Continuous Threat Exposure Management (CTEM)

zcrCTEM

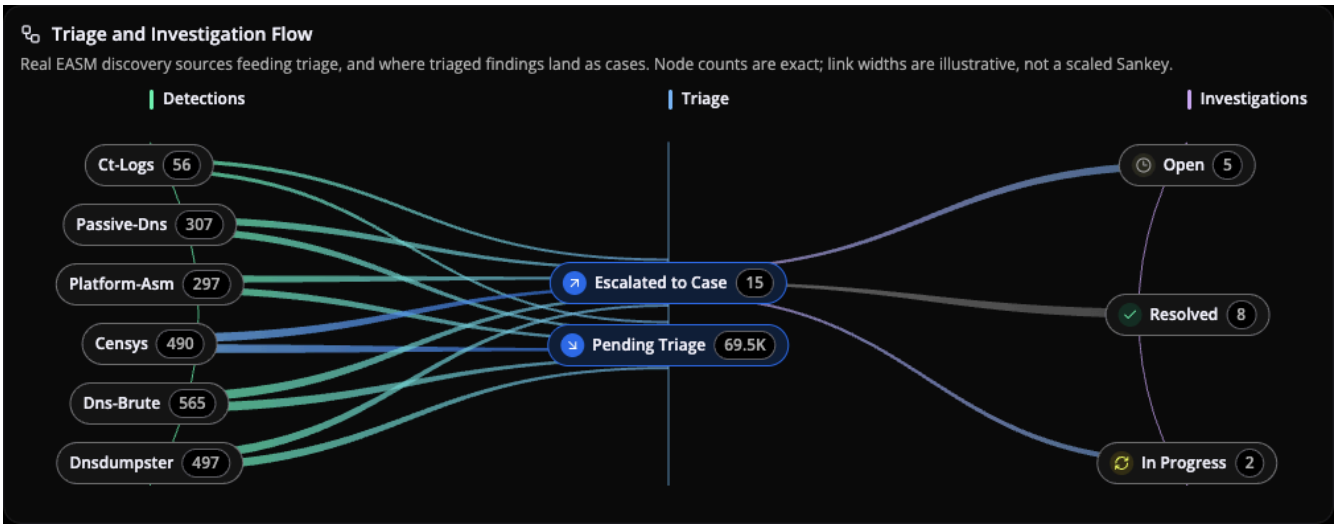
From signal to approved action

Bring external exposure, security-tool coverage gaps and dark web findings into one console. Artificial intelligence (AI) proposes work; an analyst decides whether it proceeds.

EASM	Discover externally exposed assets. External Attack Surface Management
CAASM	Find gaps in security-tool coverage. Cyber Asset Attack Surface Management
DRP	Track exposure on the dark web. Digital Risk Protection

Deployment · Cloud / Software as a Service (SaaS) or on-premises software; confirmed in solution design.

Follow exposure into investigation



Agentic Security Operations Center (SOC) dashboard: discovery sources → pending triage or escalation to cases → investigation states. Flow widths are illustrative, not performance measures. Open source view ↗

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

Built for · Security operations and vulnerability teams; risk and third-party risk teams; managed security service providers (MSSPs) running multiple tenants; chief information security officers (CISOs).

One operating sequence, one approval gate

External scans, endpoint detection and response (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 When a connector quietly stops syncing, nobody notices, and the team keeps prioritizing from a view that is already out of date.

Conceptual editorial sequence; not an integration topology.

01 **Discover**

Set seed domains and include/exclude rules by subdomain, network range (CIDR) or autonomous system number (ASN). EASM discovers continuously. CAASM pulls assets from connected tools and shows EDR, vulnerability-scan and cloud-posture coverage per asset. Sync Health flags silent sources.

Output: a scoped asset inventory and coverage gaps.

02 **Prioritize**

Rank findings by risk score, Exploit Prediction Scoring System (EPSS) and the business tier your team assigns, so the most important assets come first.

Output: findings ordered for review.

03 **Investigate**

Inspect a finding or dark web signal: evidence, confidence scoring, correlation with the EASM asset inventory and mapping to MITRE ATT&CK, a knowledge base of adversary tactics and techniques. Threat Intelligence is sold separately.

Output: evidence connected to the affected assets.

04 **Act with approval**

Agents and the AI assistant draft tickets and takedown requests. An analyst approves or rejects each proposal before it proceeds. Every AI answer, draft and decision is recorded in the audit trail.

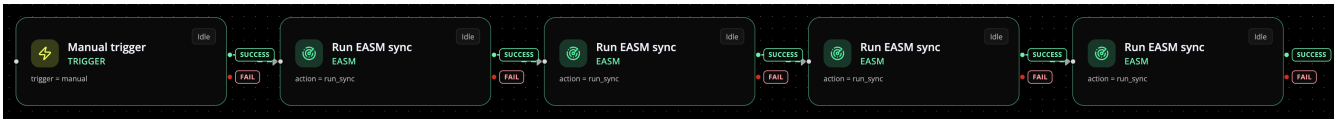
Human gate: approve or reject → traceable action record.

FIRST's EPSS estimates the probability that a published vulnerability will be exploited in the next 30 days; it is not proof of exploitation.

FIRST · EPSS ↗
CIDR = Classless Inter-Domain Routing (network ranges); ASN = Autonomous System Number.

Inspect the proposal before it moves

01 / Agent workflow canvas



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 demo view ↗

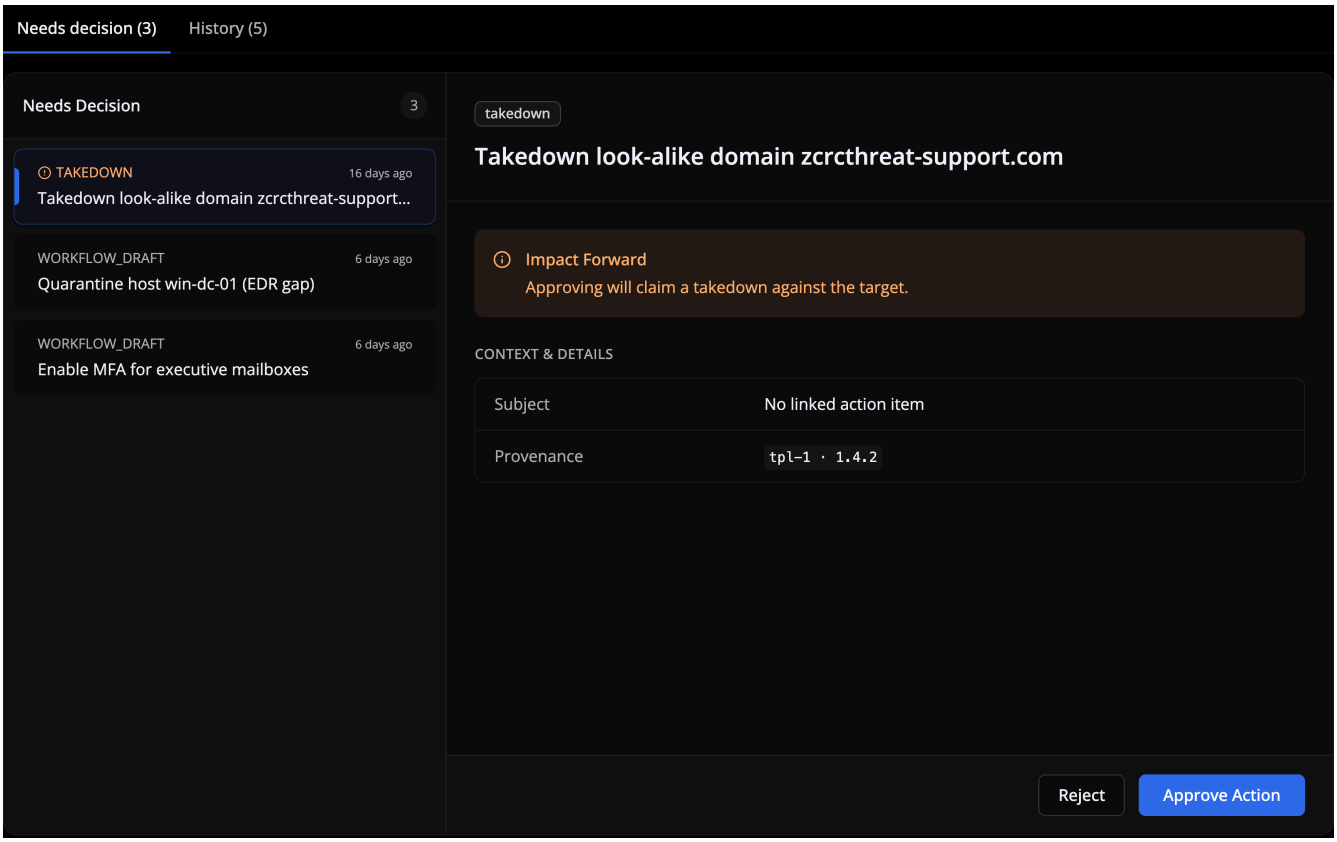
Real public-demo screen · Sample tenant and values · English UI retained



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 demo view ↗

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

02 / Pending proposal and provenance



Pending takedown proposal for zcrcthreat-support.com; provenance tpl-1 / 1.4.2; Subject: No linked action item. Impact Forward warns that approval will claim a takedown against the target. Reject / Approve Action remain untouched; no approval or takedown was performed for this brochure. Open demo view ↗

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.

Choose the scope with your partner

Modules and commercial boundaries

EASM · CAASM · DRP	Select the asset scope and modules with the approved partner; demo visibility does not establish purchased entitlements.
Threat Intelligence	Sold separately and quoted by an approved zcr partner. Not included in the four priced modules or their bundle discount.
AI & Compliance	Separately priced: readiness for Thailand's Personal Data Protection Act (PDPA) and Critical Information Infrastructure (CII), breach-notification drafts and AI-assisted compliance reporting.

Compliance boundary · Confirm the applicable framework, evidence requirements and workflow with an approved partner; this document does not establish certification or legal compliance.

What the public demo covers · 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.

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

Request a partner-led evaluation through an approved zcr partner

Bring seed domains, target asset scope and business tiers; current security tools and connectors; preferred SaaS or on-premises model; approval owners and evidence needs.

The approved partner uses these inputs to confirm modules, onboarding, implementation, integrations, support, the service-level agreement (SLA) and pricing in the solution design and quotation.

Try the zcrCTEM demo, no login needed

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

The channel partner is your first line of support; zcr backs the partner.