



ThreatCluster

Platform Overview

For MSSPs



hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ

Our Mission

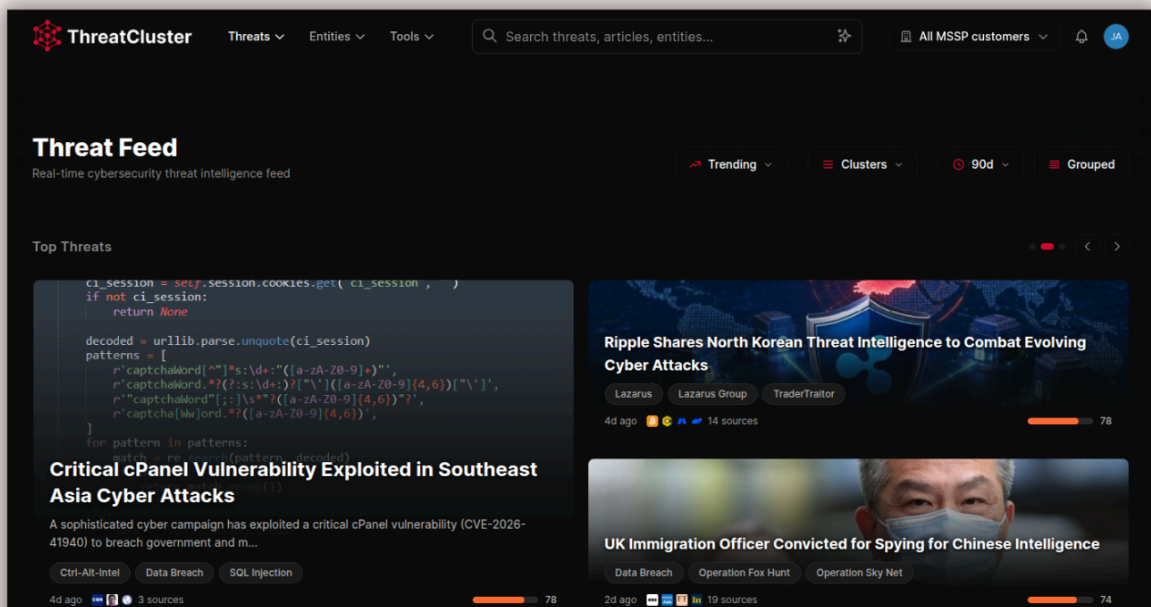
Threat intelligence should tell you what to do, not give you more to read. ThreatCluster turns 12,000+ curated sources into clustered, scored, actionable intelligence, and maps it against the environments you're protecting.

Overview

ThreatCluster aggregates open-source threat reporting in real time, clusters related incidents using semantic analysis, and enriches every cluster with threat actors, CVEs, MITRE ATT&CK techniques, malware, industries, IOCs and more. Each cluster is scored for severity, actionability and urgency so analysts spend time on what matters.

The platform is multi-tenant by design. MSSP analysts manage multiple clients from a single console, with each client getting a scoped view of their own threat landscape. Clients connect their asset inventories - Tenable, Defender, CrowdStrike, or custom via API, and ThreatCluster cross-references vulnerabilities against their actual tech stack, ranked using CISA's SSVC framework. Attack flows, public exploit tracking, MITRE D3FEND countermeasures, and AI-assisted investigation are built in.

One platform. Per-client intelligence. No stitching together five tools to deliver what your clients expect.



ThreatCluster Threat Feed

hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

Platform Features



Real-time clustering

12,000+ sources aggregated continuously. Related articles are grouped automatically using density-based semantic clustering, so one incident reported across thirty outlets becomes one cluster, not thirty alerts.



Enrichment

Every cluster is enriched with threat actors, malware families, CVEs, CWEs, MITRE ATT&CK techniques, targeted industries, countries, and IOCs. Scored for severity, actionability and urgency.



Attack Flows

AI-generated kill chains mapped to MITRE ATT&CK and structured to CTID Attack Flow v3.



D3FEND

Defensive techniques mapped from the attack flow, so analysts know what to deploy against the TTPs in play.



Exploit tracking

PoC and weaponised exploit code tracked via Sonar across GitHub, Exploit-DB and other sources. Linked directly to CVEs and clusters.



ThreatCluster AI

Investigation assistant grounded in cluster content with inline source citations. Distinguishes between facts drawn from the data and general knowledge.



Exposure Monitor

Connect Tenable, Microsoft Defender, CrowdStrike, or push assets via API. ThreatCluster cross-references your inventory against the live threat feed and ranks every asset by CISA SSVC.



CVE intelligence

CVSS, EPSS, KEV status, exploit availability, vendor references, related clusters, and X mentions in one view per CVE.

hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

Platform Features



Custom Alerts

Keyword, entity, CVE, or threat score triggers delivered via email or webhook.



Exports

Clusters, entities, IOCs, and attack flows exportable as JSON, CSV, STIX 2.1, SVG, and PNG.



Workflows

Trigger on new clusters, CVE thresholds, or tagged entities. Actions include webhooks, Slack posts, AI summaries, tickets, and email digests. Visual drag-and-drop editor.



Tags

Mark the entities, vendors, products, and actors that matter. Tags drive personalised feeds, digest rules, exposure scoring, and AI summaries across the platform.



Collections

Save clusters, articles, and entities into named folders. Pin to an incident, client, or research thread. Shareable via link.



Dark Web

Ransomware leak-site tracking, credential market monitoring, and breach drop alerts. Spot when a client's domain or supplier hits a victim list.



CLI

Single binary, one `tc login`. Query clusters, fetch CVEs, push assets, trigger workflows. Same data as the web UI, built for scripts, cron jobs, and analysts who'd rather not click.



Threat Hunting

Pre-built hunts mapped to MITRE ATT&CK. Copy straight into Splunk or Sentinel. Cluster context confirms whether the technique is active in the wild right now.

hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

Built for MSSPs

Multi-customer scoping

Switch the active customer from the navbar and everything re-scopes: feeds, alerts, webhooks, workflows, reports, dashboards, exposures. Data isolation is enforced server-side at the database layer, not just the UI. A customer-A rule cannot fire to customer-B's webhook.

Per-customer exposure management

Pair each client's asset inventory with the live threat feed. CISA SSVC stage per host. Pull inventory via Tenable, Defender, CrowdStrike, bulk upload, or API. Tag assets as internet-facing, crown-jewel, or isolated and the SSVC tree adapts. One-line patch-priority answer your analyst hands to the client.

White-label reports

Threat reports branded with the customer's name and logo, not yours. Schedule weekly, monthly, or one-off delivery direct to their stakeholders. Content is scoped to their estate.

Customer-scoped alert routing

Webhooks, Slack, Teams, and email destinations are scoped per customer. Cross-customer routing is blocked at the API. One place to manage alert rules across your book. Each customer gets a clean notification stream as if you only worked for them.

Aggregate dashboard

Single roll-up across every customer. Total assets under management, KEV exposures by client, CVEs affecting multiple clients, and which customers are most at risk this week. Prioritise your team's day without spreadsheet gymnastics.

One platform, every client

No per-client instances. No duplicated configuration. Scale by adding clients, not infrastructure.

Real-Time Clustering

ThreatCluster ingests from over 12,000 curated sources continuously, security vendors, government advisories, researcher blogs, news outlets, dark web forums, social platforms, and vulnerability databases. Every article is processed through a multi-layer NLP pipeline that extracts entities, generates semantic embeddings, and groups related reporting using density-based clustering (DBSCAN). Thirty articles about the same incident become one cluster, scored and enriched, not thirty separate alerts.

Each cluster is automatically enriched with extracted entities: threat actors, malware families, CVEs, CWEs, MITRE ATT&CK techniques, targeted industries, countries, platforms, tools, companies, and IOCs. This entity layer is what makes custom feeds possible.

The screenshot displays the ThreatCluster web interface. At the top, there is a navigation bar with 'Threats', 'Entities', and 'Tools' menus, a search bar, and a user profile 'JA'. The main content area features a large image of the 'stryker' logo. Below the image, the article title is 'Iran-Linked Handala Group Launches Cyberattack on Stryker Medical Technology', dated 11/03/2026, with a similarity score of 83% and a score of 75.0. The article content is displayed in a scrollable view, showing a summary of the attack on Stryker. To the right, an 'Extracted Entities' sidebar lists various categories: APT Groups (4), Attack Types (5), Campaigns (3), and Companies (14), each with expandable items.

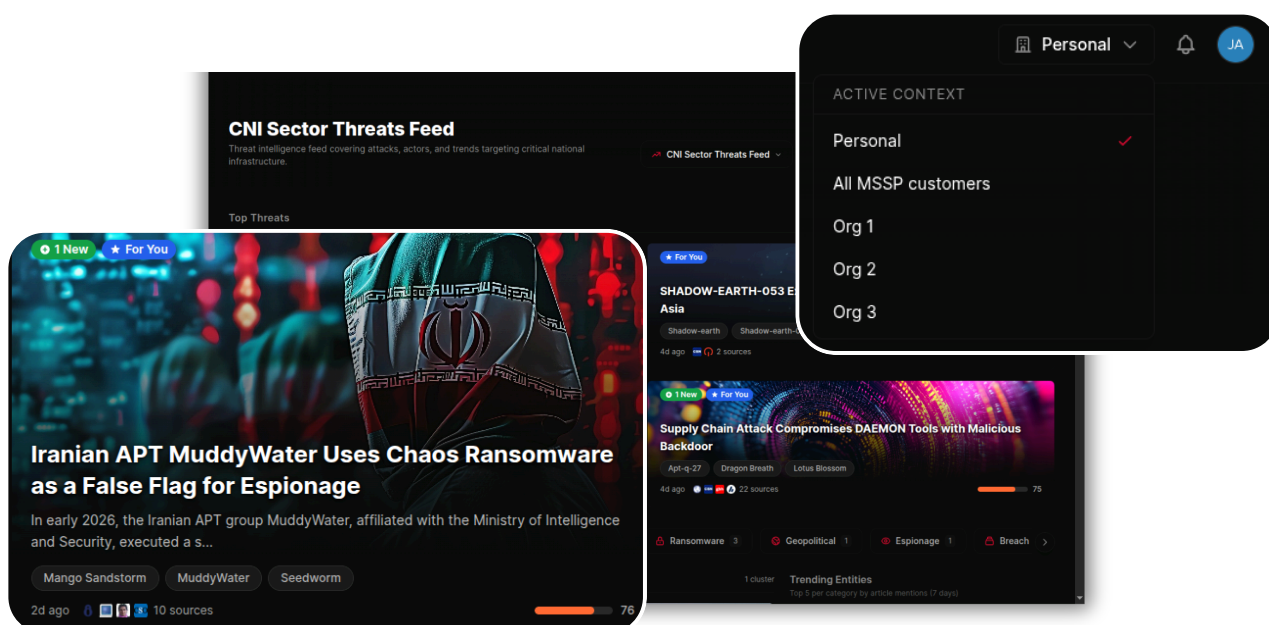
Cluster Detail Page

hello@threatcluster.io
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



Custom feeds per client

For each MSSP client, you define a feed profile built from entity filters, their tech stack (vendors, products, platforms), countries of operation, industries, supply chain companies, specific threat actors or campaigns they care about, and any CVEs or tools they want to track. The feed surfaces only the clusters that match, scored and ranked.



Feeds can be consumed however the client or analyst prefers:

- **Web app:** filtered dashboard scoped to the client's feed profile.
- **CLI:** `tc` command-line tool for scripting and automation.
- **API:** RESTful endpoints returning clusters, entities, IOCs, and enrichment in JSON.
- **RSS:** standard feed for integration with existing readers and SIEM ingestion.
- **Email digests:** scheduled delivery at defined cadence and thresholds.
- **Webhooks:** real-time push to Slack, Teams, SOAR platforms, or custom tooling.

One client might want a daily email covering anything above threat score 70 that affects their industry. Another might want a webhook firing the moment a CVE hits their declared tech stack. Both run from the same platform, configured in minutes.

hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



Cluster Enrichment

Every cluster is automatically enriched with structured entities extracted from the source reporting: threat actors, malware families, CVEs, CWEs, campaigns, targeted industries, countries, companies, platforms, tools, domains, file hashes, and MITRE ATT&CK techniques, and more. These aren't static tags, each entity builds a living profile over time.

employed. Indicators include specific C2 infrastructure overlaps and used by **MuddyWater**.

Recommended Response
Prioritize monitoring for unusual **Microsoft Teams** activity, especially social anomalies. Deploy detections for **DWAgent**, **AnyDesk**, and the custom associated C2 infrastructure and code-signing certificates linked to **MuddyWater** configurations and restrict remote access tools to trusted sources. Investigate leak site activity for signs of compromise, focusing on persistence mechanisms and **ransomware** indicators.

➔ Enhanced Analysis

Enhanced analysis

AI-generated summary, impact assessment, technical details, and recommended response. Enhanced analysis updates as new reporting lands.

Timeline

Sourced timeline reconstructing the sequence of events with linked references. See how the incident unfolded in the order it was reported.

Timeline

- 2026-05-06**
Rapid7 report reveals MuddyWater's tactics
Rapid7 published findings on MuddyWater's use of Chaos ransomware attack methods and persistence mechanisms used.
Infosecurity-Magazine
- 2026-05-06**
MuddyWater's intrusion begins
The attack commenced with social engineering through Microsoft Teams.
Bleepingcomputer

Article Content Include sub-articles < 3 / 12

MuddyWater hackers use Chaos ransomware as a key tactic in attacks

Bleepingcomputer • May 6, 2026 at 02:02 PM • 84% match

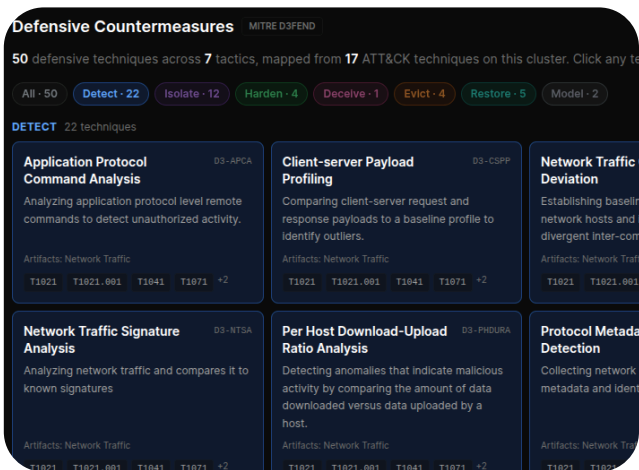
MuddyWater Iranian hackers disguised their operations as a **Chaos ransomware** attack, relying on **Microsoft Teams** social engineering to gain access and establish persistence.

Clustered Articles

Cycle through every source article and sub-article without leaving the page. Sub-articles follow outbound links from the original reporting one level deep.

hello@threatcluster.io
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



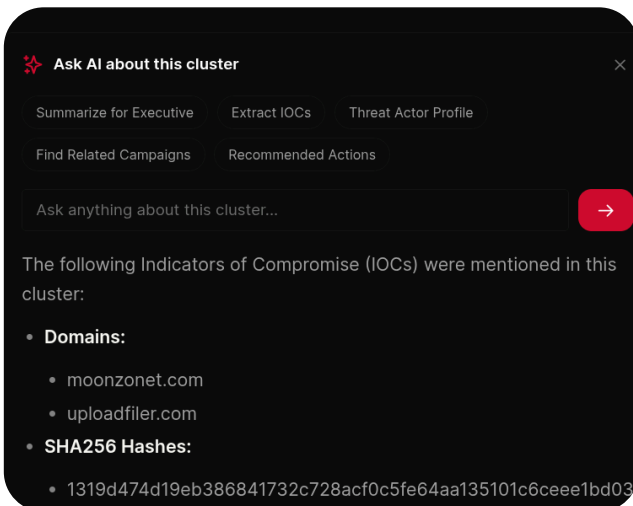
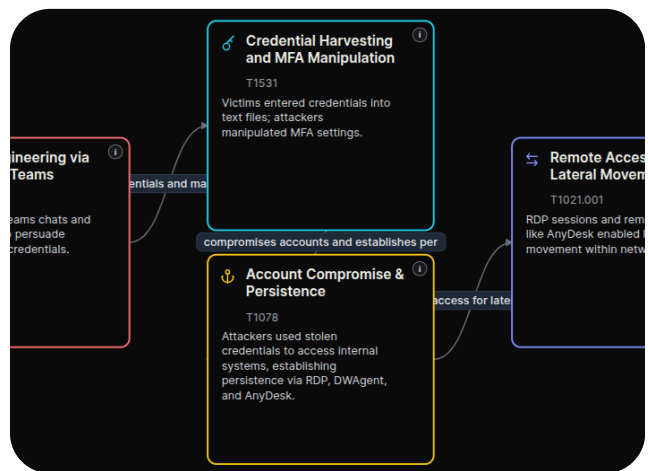


D3FEND countermeasures

Defensive techniques mapped directly from the attack flow. Each step in the kill chain gets a corresponding countermeasure so analysts know what to deploy, not just what to look for.

Attack flows

AI-generated kill chains per cluster, mapped to MITRE ATT&CK and structured to CTID Attack Flow v3. Each node cites the source material. Flows regenerate as new reporting lands. Export as SVG, PNG, JSON, or STIX 2.1.



Ask AI

Investigation assistant grounded in the cluster's content with inline source citations. Distinguishes between facts drawn from the data and general knowledge.

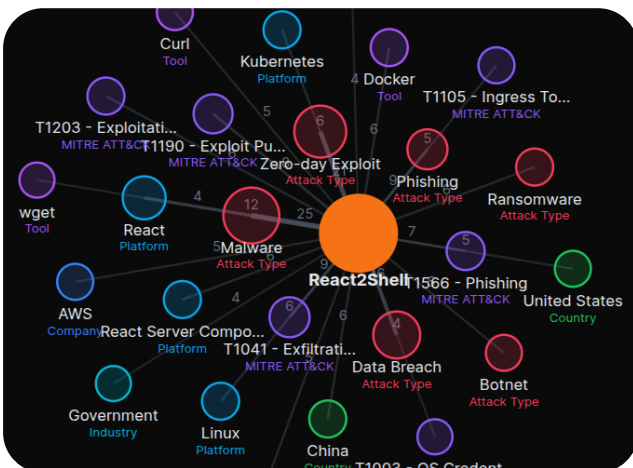
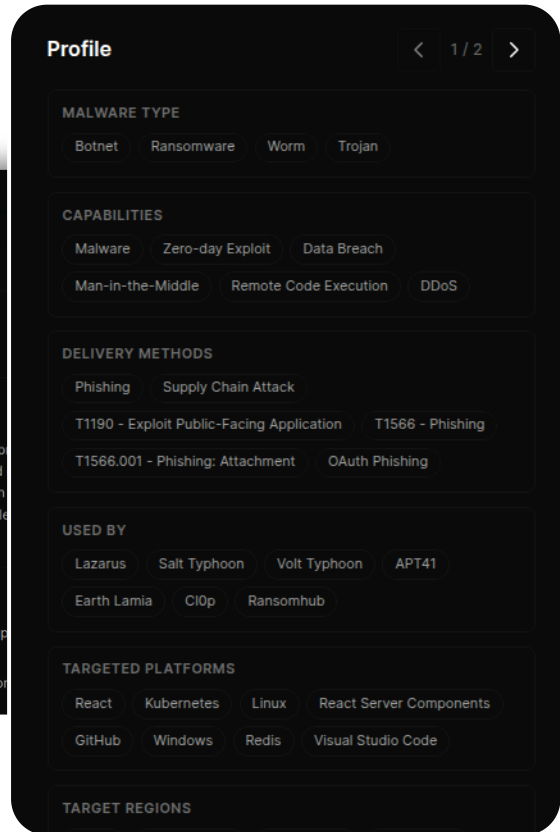
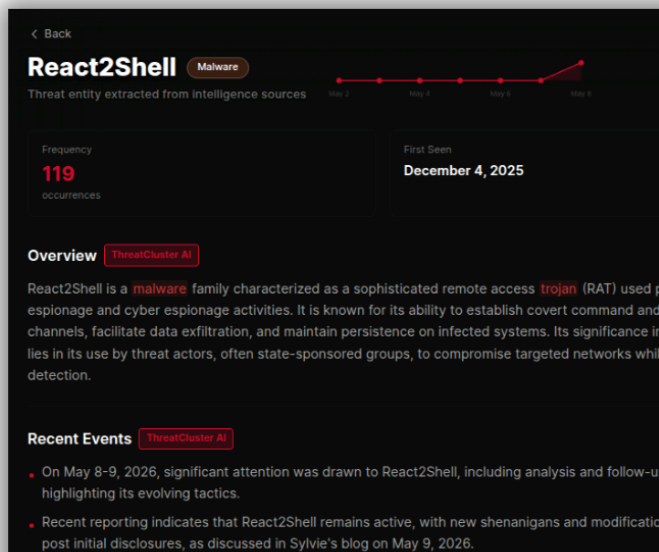
hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



Entity Intelligence

Click any extracted entity and get a full intelligence page. AI-generated overview, recent events, threat profile (capabilities, delivery methods, targeted platforms, target regions, target sectors, common TTPs, associated campaigns and CVEs), and frequency tracking from first seen to last seen. All drawn from the intelligence the platform has collected, not a static database.



Relationship graph

Every entity page maps its connections to other entities visually. See which threat actors use which malware, which malware targets which platforms, which CVEs are associated with which campaigns. Explore laterally across the graph to find connections that aren't obvious from reading individual clusters.

hello@threatcluster.io
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



Exposure Management

Threat intelligence becomes useful when it points at your boxes. Exposures joins the live threat feed with each client's asset inventory and tells you what to patch first.

Every active CVE and threat actor that touches the client's stack. Two streams: direct exposures (CVEs against their installed software) and related threats (actors and malware targeting their tech). Filter by KEV-only, CVSS ≥ 9 , or has-exploit. Sort by severity, latest activity, asset reach, or cluster volume.

The screenshot shows a dashboard titled "Exposures" with the subtitle "CVEs and threat actors targeting your inventory". It features a summary section with four metrics: ASSETS (15, 18 products tracked), CPE MATCHED (17, Searchable software), IN KEV (8, Actively exploited), and DIRECT EXPOSURES (376, 18 related threats). Below this is a search bar and filter options (All, Direct only, Related only, KEV only). A list of CVEs is shown, with a callout box for CVE-2026-24858. The callout box displays: "Critical 9.8 EPSS 6.2%", "In your stack", "1 asset · 1 install", "Fortinet FortiOS 7.4.2", "2 clusters", and "10/02/2026".

Connectors

Pull asset inventory via Tenable, Microsoft Defender, CrowdStrike, bulk CSV/JSON upload, or the public REST API. All per-client. Soft-deletion and re-syncs are non-destructive. Assets you stop reporting fall out gracefully without losing history.



hello@threatcluster.io

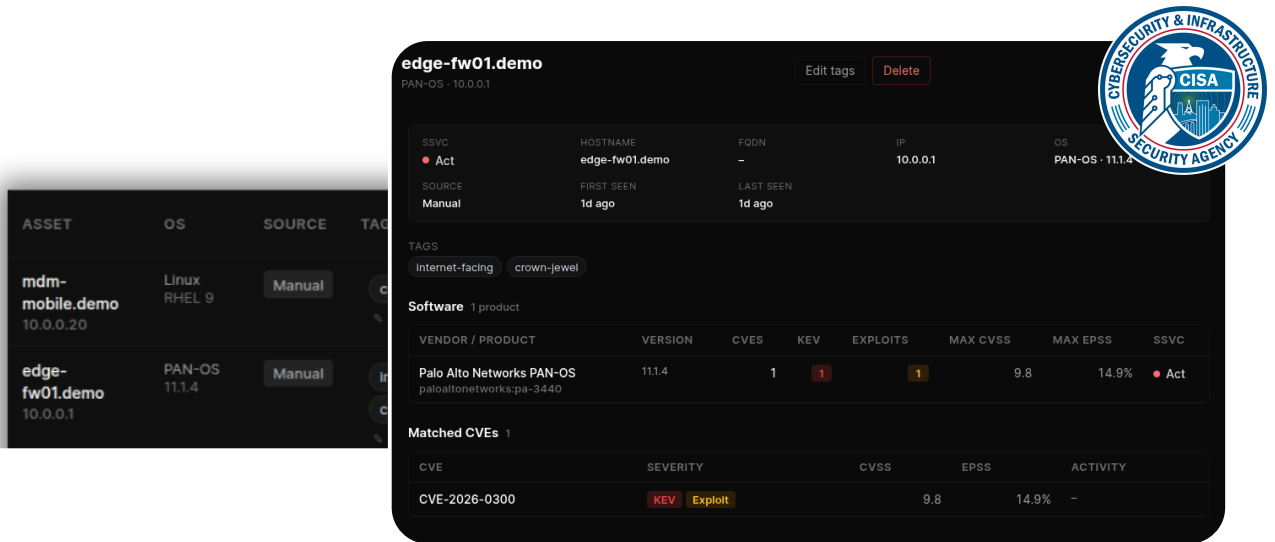
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

Assets View

Every host ranked by CISA SSSC: Act, Attend, Track*, Track, Clear. Things to patch first sit at the top. Hover any pill for the reasoning. Tag assets as internet-facing, crown-jewel, or isolated and the SSSC tree adapts. Bulk columns surface CVE count, KEV count, exploit count, max CVSS, and max EPSS at a glance.

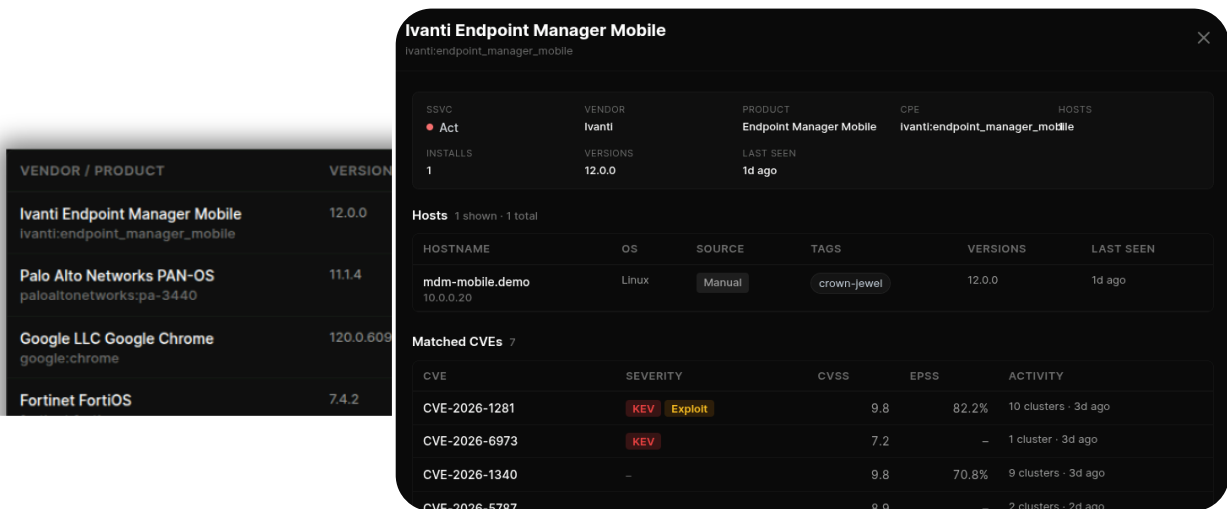


The Assets View interface displays a list of assets on the left and a detailed view for a selected asset on the right. The detailed view for 'edge-fw01.demo' includes the following information:

- Asset Details:**
 - SSVC: Act
 - HOSTNAME: edge-fw01.demo
 - FQDN: -
 - IP: 10.0.0.1
 - OS: PAN-OS 11.1.4
 - SOURCE: Manual
 - FIRST SEEN: 1d ago
 - LAST SEEN: 1d ago
- TAGS:** internet-facing, crown-jewel
- Software:** 1 product
 - VENDOR / PRODUCT: Palo Alto Networks PAN-OS (paloaltonetworks:pa-3440)
 - VERSION: 11.1.4
 - CVES: 1
 - KEV: 1
 - EXPLOITS: 1
 - MAX CVSS: 9.8
 - MAX EPSS: 14.9%
 - SSVC: Act
- Matched CVEs:** 1
 - CVE: CVE-2026-0300
 - SEVERITY: KEV, Exploit
 - CVSS: 9.8
 - EPSS: 14.9%
 - ACTIVITY: -

Software View

Pivoted by vendor and product so patch decisions land at product level. Same SSSC ranking aggregated across every host running that product. Shows the blast radius before you start the rollout.



The Software View interface displays a list of software products on the left and a detailed view for a selected product on the right. The detailed view for 'Ivanti Endpoint Manager Mobile' includes the following information:

- Product Details:**
 - SSVC: Act
 - VENDOR: Ivanti
 - PRODUCT: Endpoint Manager Mobile
 - CPE: Ivanti:endpoint_manager_mobile
 - HOSTS: 1
 - INSTALLS: 1
 - VERSIONS: 12.0.0
 - LAST SEEN: 1d ago
- Hosts:** 1 shown - 1 total
 - HOSTNAME: mdm-mobile.demo (10.0.0.20)
 - OS: Linux
 - SOURCE: Manual
 - TAGS: crown-jewel
 - VERSIONS: 12.0.0
 - LAST SEEN: 1d ago
- Matched CVEs:** 7
 - CVE: CVE-2026-1281
 - SEVERITY: KEV, Exploit
 - CVSS: 9.8
 - EPSS: 82.2%
 - ACTIVITY: 10 clusters - 3d ago
 - CVE: CVE-2026-6973
 - SEVERITY: KEV
 - CVSS: 7.2
 - EPSS: -
 - ACTIVITY: 1 cluster - 3d ago
 - CVE: CVE-2026-1340
 - SEVERITY: -
 - CVSS: 9.8
 - EPSS: 70.8%
 - ACTIVITY: 9 clusters - 3d ago
 - CVE: CVE-2026-5787
 - SEVERITY: -
 - CVSS: 8.9
 - EPSS: -
 - ACTIVITY: 2 clusters - 2d ago

hello@threatcluster.io

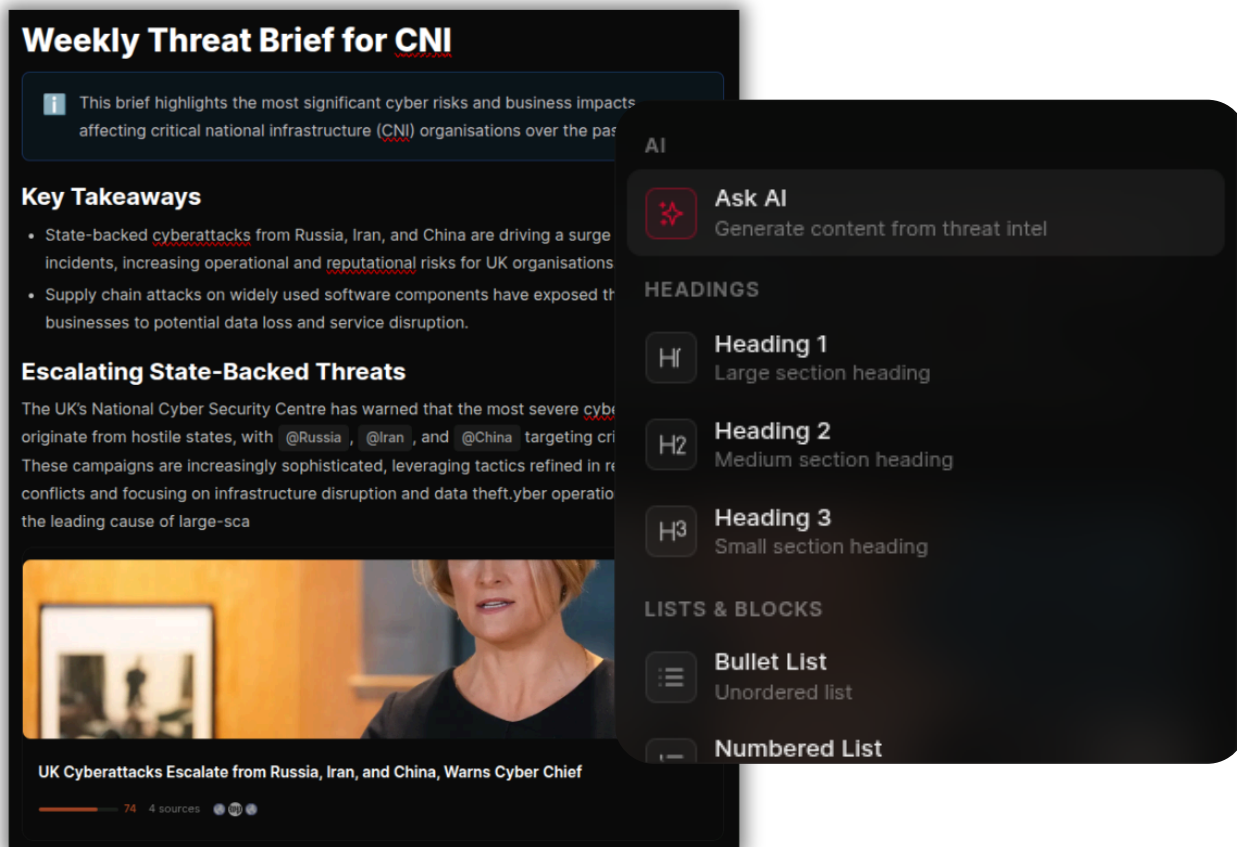
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

Reports

Turn what you've found into something you can hand to a stakeholder. Reports are live, editable documents in a Notion-style editor that pull live threat data on every render. Set one up once and it stays current every time it's opened.



The image shows a dark-themed report titled "Weekly Threat Brief for CNI". The report content includes:

- Key Takeaways**
 - State-backed cyberattacks from Russia, Iran, and China are driving a surge in incidents, increasing operational and reputational risks for UK organisations.
 - Supply chain attacks on widely used software components have exposed businesses to potential data loss and service disruption.
- Escalating State-Backed Threats**

The UK's National Cyber Security Centre has warned that the most severe cyber incidents originate from hostile states, with @Russia, @Iran, and @China targeting critical infrastructure. These campaigns are increasingly sophisticated, leveraging tactics refined in recent conflicts and focusing on infrastructure disruption and data theft. Cyber operations are becoming the leading cause of large-scale incidents.

Below the text is a video thumbnail showing a woman speaking, with the caption "UK Cyberattacks Escalate from Russia, Iran, and China, Warns Cyber Chief". At the bottom of the report, it shows "74 4 sources" with social media icons.

Overlaid on the right is an "AI" menu with the following options:

- Ask AI**: Generate content from threat intel
- HEADINGS**
 - H1**: Heading 1 (Large section heading)
 - H2**: Heading 2 (Medium section heading)
 - H3**: Heading 3 (Small section heading)
- LISTS & BLOCKS**
 - Bullet List**: Unordered list
 - Numbered List**

Dynamic content blocks

Drop in blocks that stay in sync with your live data: threat feed, dark web activity, CVE watch, trending entities, key stats, trend charts, breakdowns by region or sector, and AI-generated narrative sections. Every block re-fetches at render time. A weekly brief you built six months ago reports on this week's activity.

hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



Threat Report

SHADOW-EARTH-053 Exploits Microsoft...

The China-aligned threat group SHADOW-EARTH-053 has been exploiting unpatched Microsoft Exchange and IIS server vulnerab...

2 sources

Critical Vulnerabilities In Yarbo Robot Firmware...

AHA! disclosed three critical vulnerabilities in Yarbo robot firmware v2.3.9, identified as CVE-2026-7413, CVE-2026-7414...

3 sources

CISA Launches CI Fortify to Enhance Critical...

The Cybersecurity and Infrastructure Security Agency (CISA) has initiated the CI Fortify program to bolster the resilienc...

20 sources

Ukrainian Magura V3 Drone Found Off Lefkada with...

A Ukrainian-designed Magura

Last 7 days Vulnerabilities

- XSS**
+700% 8 mentions
- Dirty Pipe**
+300% 12 mentions
- Dirty Frag**
NEW 39 mentions
- Pack2TheRoot**
+100% 2 mentions
- HTTP Request S... Header Preceden...**
NEW 2 mentions

Last 7 days

- CVE-2026-1340**
+200% 3 mentions (prev 1)
- CVE-2026-22679**
+200% 3 mentions (prev 1)
- CVE-2026-1281**
+200% 3 mentions (prev 1)

DYNAMIC DATA

- Threat Feed**
Live top threats — regenerates on every open
- Dark Web Activity**
Ransomware victims + breaches
- CVE Watch**
Trending CVEs for the period
- Trending Entities**
Top APTs, ransomware, malware, CVEs by velocity
- Key Statistics**
Big-number tiles for the period
- Breakdown Chart**
Industry / country / sector distribution
- Trend Over Time**
Line chart of threats / victims / CVEs

Report Types

Executive briefings (business-framed, KPI-led, low jargon), technical deep-dives (IOC tables, CVSS/EPSS, MITRE mappings, detection guidance in Sigma/KQL/SPL), incident reports (timeline-driven, evidence-anchored), and MSSP customer briefings (white-labelled, scoped to the client's estate). Save your own templates and reuse them.

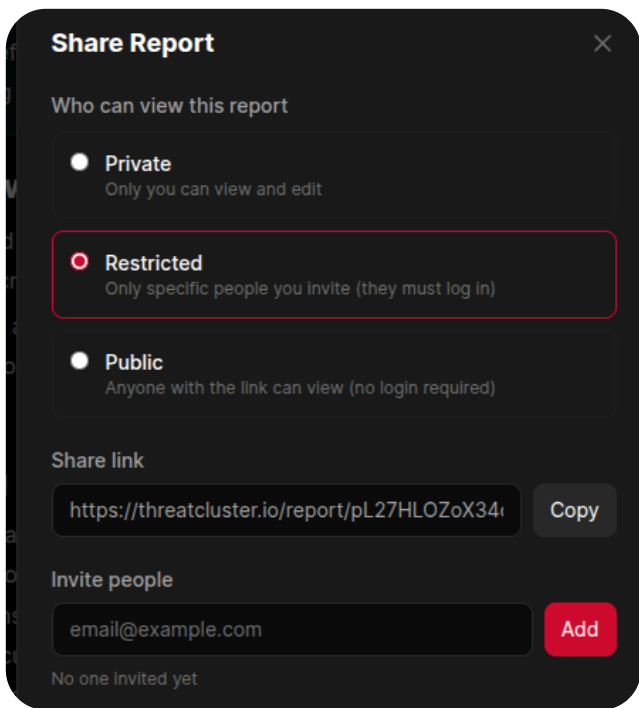
Pick a layout 1/10 saved

Start from a blank page, a built-in layout, or one of your saved templates.

- Blank report**
Start with an empty page.
- Incident Report** BUILT-IN
Detection → containment → remediation, with IOC table and...
- Vulnerability Advisory** BUILT-IN
CVE-led structure: summary, technical details, detection, mitigation.
- Weekly Threat Brief** BUILT-IN
Recap of the week: featured stories, CVEs, actor activity.
- Executive Briefing** BUILT-IN
Business-framed: bottom line up front, key takeaways, recommended actions.
- Executive Briefing - 2** SAVED

hello@threatcluster.io
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ





Share Report [Close]

Who can view this report

- Private
Only you can view and edit
- Restricted**
Only specific people you invite (they must log in)
- Public
Anyone with the link can view (no login required)

Share link

Invite people

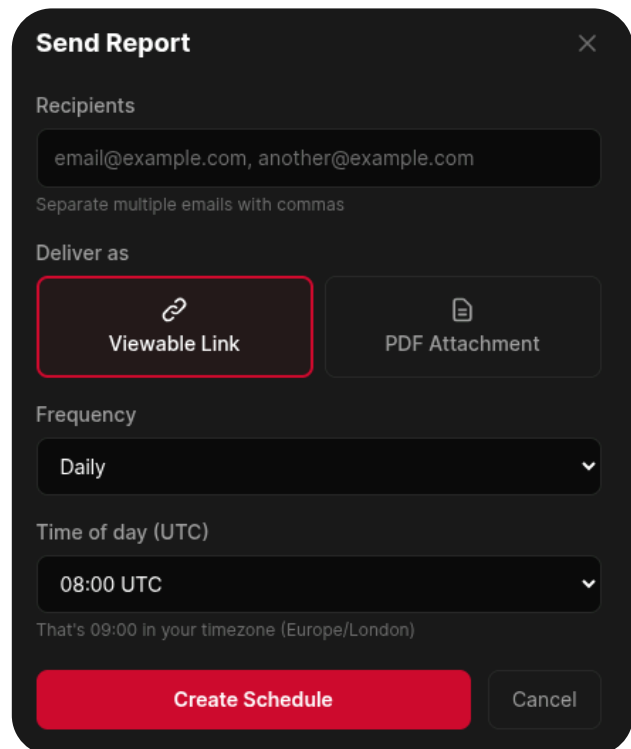
No one invited yet

Sharing

Private drafts, restricted access by email, public web URL with no login required, PDF export, Markdown/HTML export, or direct email send. Customer-scoped reports prompt for confirmation before going public.

Scheduled delivery

Private drafts, restricted access by email, public web URL with no login required, PDF export, Markdown/HTML export, or direct email send. Customer-scoped reports prompt for confirmation before going public.



Send Report [Close]

Recipients

Separate multiple emails with commas

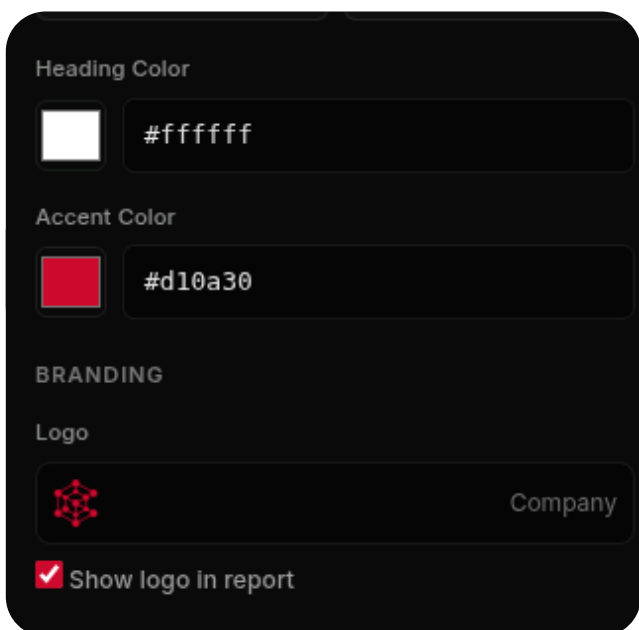
Deliver as

-
-

Frequency

Time of day (UTC)

That's 09:00 in your timezone (Europe/London)



Heading Color

Accent Color

BRANDING

Logo

Show logo in report

White-label

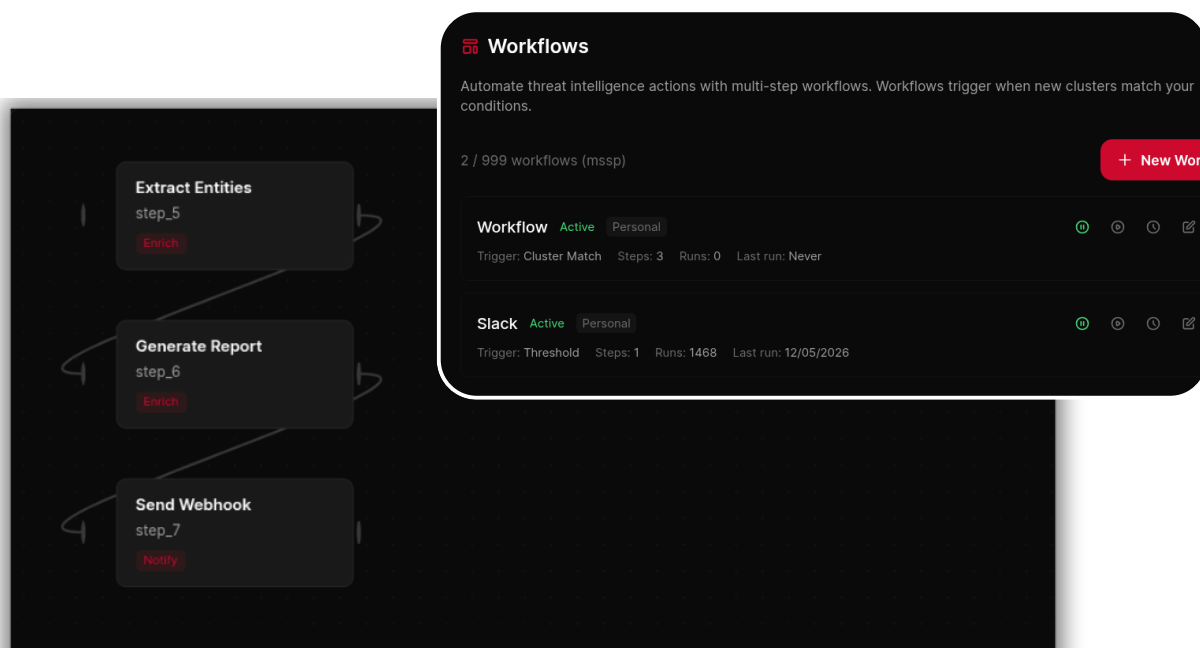
Tag a report with a managed customer and their name, logo, brand colours, and contact details replace ThreatCluster's everywhere. Rendered HTML, PDF headers, email from-line. One analyst, ten branded briefings on a Monday Morning.

hello@threatcluster.io
 71-75 Shelton Street, Covent Garden,
 London, WC2H 9JQ



Workflows

Automate the routine triage so analysts spend time on decisions, not button-clicks.



Triggers

A new cluster matches your interests, a CVE crosses an EPSS threshold, a tagged entity appears in the feed. Triggers fire per-client in MSSP environments.

Actions

Notify a webhook, post to Slack or Teams, generate an AI summary, open a ticket, send an email digest, add to a collection. Chain multiple actions into a single workflow.

Visual Editor

Build workflows with drag-and-drop. No code. Set conditions, branch logic, and action sequences visually.

Per-client Scoping

workflows created under one client can only fire to that client's destinations. One place to manage workflows across your entire book.

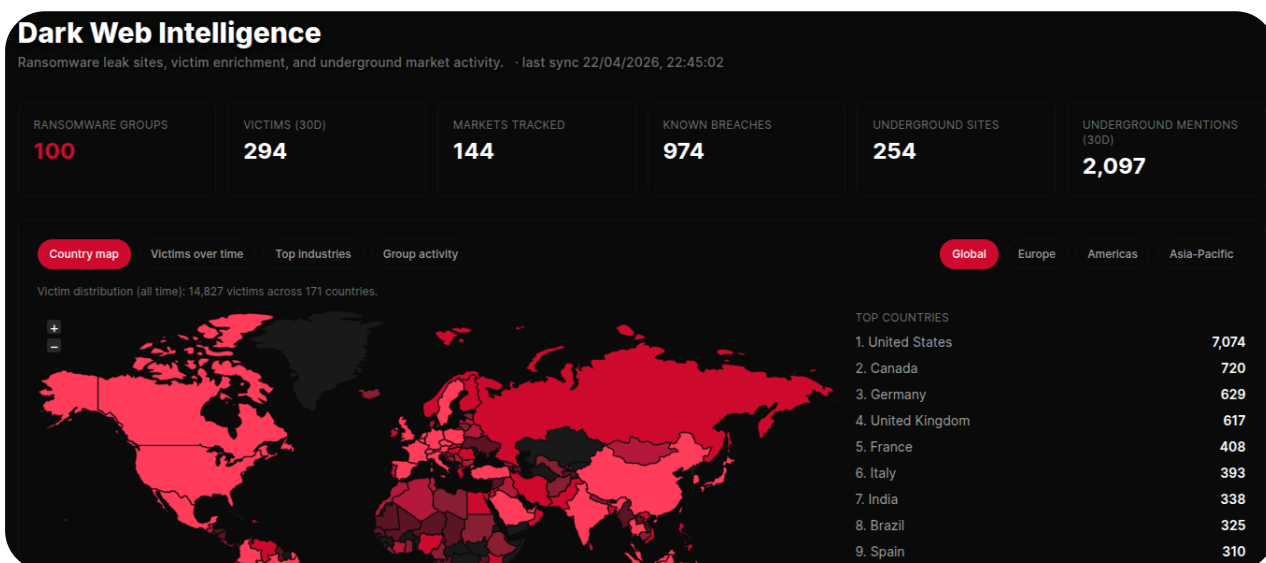
hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



Dark Web Monitoring

In-house collection stack, not a reseller integration. ThreatCluster discovers, scrapes, enriches, and surfaces dark web content directly.



Collection

Three independent scrapers cover ransomware and data-leak group sites, underground forums (paste sites, initial-access broker boards, combolists, defacement archives), and Tor/clearnet marketplaces.



Discovery

Four sources find new sites in parallel: curated CTI repositories, Tor search engines, GitHub-published onion lists, and Telegram channels. New candidates go through liveness probing, a depth-1 link harvest, then automated classification. Most competitors buy a list. We find our own.



Enrichment

Every captured page goes through two stages. Deterministic regex extraction pulls crypto addresses, emails, Tox IDs, XMPP handles, Telegram handles, PGP blocks, and CVE references. LLM-based extraction then confirms and extends with victim names, tools, threat actor attribution, language, and summary. Extracted entities cross-reference into the main entity graph, so a victim domain or tool name surfaces on its entity page alongside news clusters.

hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster



Surfacing

Group profile pages with victims and active campaigns. Per-victim detail with enrichment. Markets with category and entity tags. Underground hosts with screenshots, captions, and metadata. Breach indexes. Filter by country, sector, group, status, or freshness.

Primius Law Firm

Ransomware Victim DRAGONFORCE PUBLICATION: 5 DAYS 09:41:32 .GR

Ransomware leak-site victim intelligence · EL

| | | | |
|------------------------------|------------------------------|--------------------------|--------------------------------------|
| Data size 71.93 GB | Posted 22 Apr 2026 | Country Greece | Industry Business Services |
|------------------------------|------------------------------|--------------------------|--------------------------------------|

Victim profile

HEADQUARTERS
Αγ. Μηνά 4, (2ος & 3ος Όροφος) 54625 Θεσσαλονίκη
Thessaloniki, Greece

DOMAINS
www.primiuslawfirm.gr primiuslawfirm.gr

What was taken

A modern and effective legal firm providing holistic solutions across branches of law in Greece.

DATA CATEGORIES
Contracts Emails PII Databases

LEAK SITE TAGS
Publication Primius Law Firm

Leak-site images (3)

Images from the victim's leak listing. Thumbnails scraped from the onion page are blurred by default — click a thumbnail to view.

Source

GROUP
dragonforce

POSTED
22 Apr 2026

LAST SCRAPED
22 Apr 2026

VICTIM WEBSITE
primiuslawfirm.gr

LEAK PAGE (ONION)
http://z3wqggtxtft71d31br7sr1vv5gjof5fwg76slewnzwwakjuf3nlh
ukdid.onion/blog/?post_uid=e27d9dd4-78f5-4355-a624-a1357e
dd9b69

Copy onion URL

Recent dragonforce victims

INCYTE
22 Apr 2026 · US

The Gallilher Law Firm
22 Apr 2026 · US



Alerts

Three independent scrapers cover ransomware and data-leak group sites, underground forums (paste sites, initial-access broker boards, combolists, defacement archives), and Tor/clearnet marketplaces.



Safety

Four sources find new sites in parallel: curated CTI repositories, Tor search engines, GitHub-published onion lists, and Telegram channels. New candidates go through liveness probing, a depth-1 link harvest, then automated classification. Most competitors buy a list. We find our own.

hello@threatcluster.io

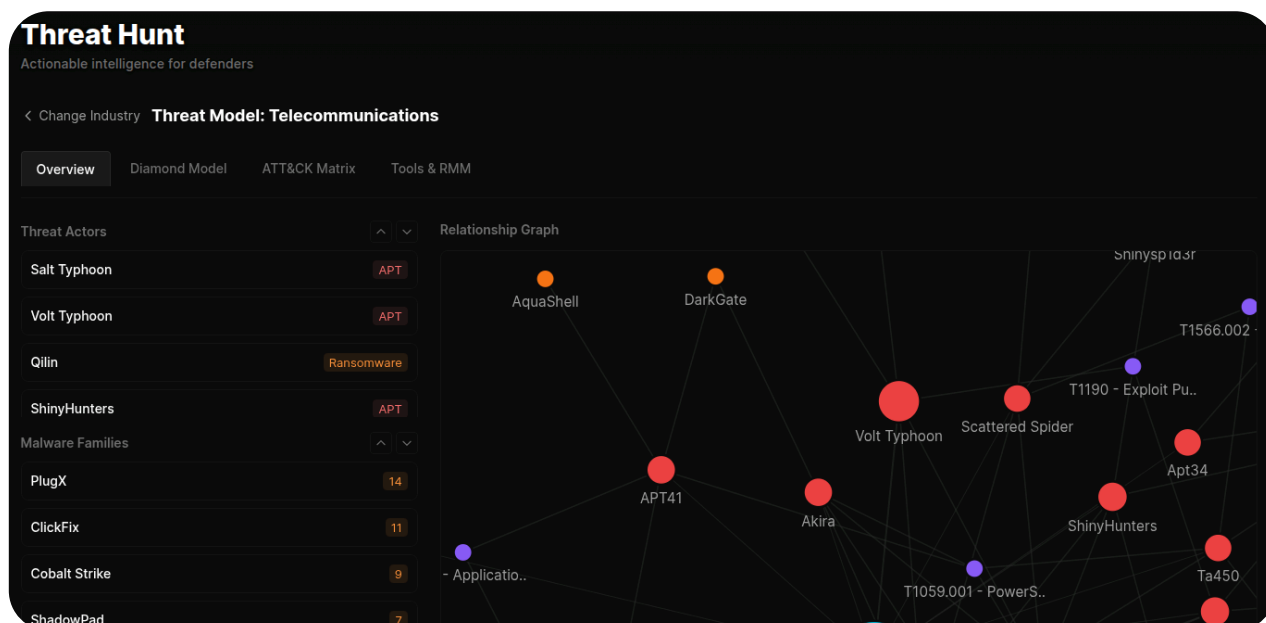
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

Threat Hunting

Go from "this sector is being targeted" to "here are the queries to run in your SIEM" in one page.



Industry threat models

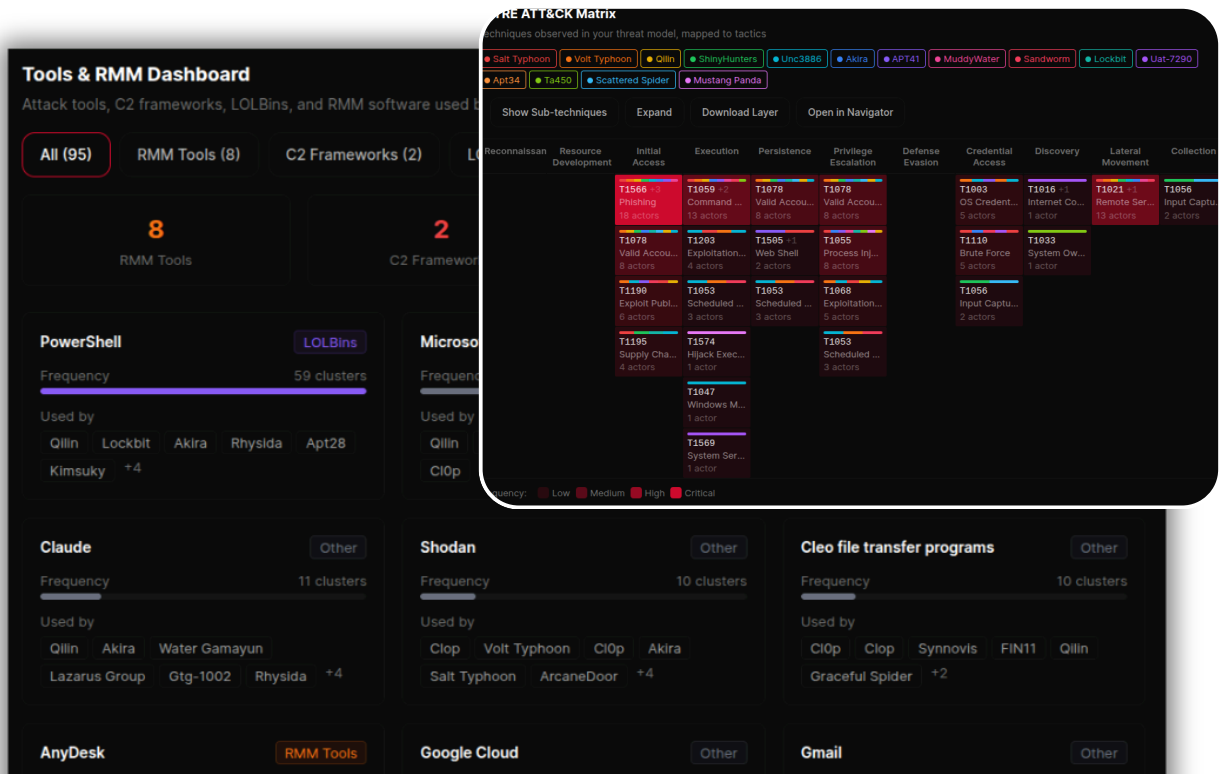
Pick a sector (17 covered today) and ThreatCluster builds a live threat model from the knowledge graph: every actor, malware family, campaign, tool, and MITRE ATT&CK technique that co-occurs with that industry in the cluster data. No manual curation. When a new group starts targeting healthcare, it surfaces in the healthcare model on the next refresh.

Four views

Overview (actors, malware, campaigns, relationship graph, consolidated IOC watchlist), Diamond Model, ATT&CK matrix colour-graded by frequency with toggleable sub-techniques, and a Tools & RMM dashboard covering C2 frameworks, LOLBins, and remote access software.

hello@threatcluster.io
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ





SIEM-ready hunting queries

Export in KQL (Sentinel/Defender XDR), SPL (Splunk), or Lucene (Elastic/OpenSearch). Two kinds: deterministic IOC queries built from the live entity graph without an LLM in the loop, and curated TTP queries sourced from SigmaHQ and Microsoft Sentinel rule libraries, mapped to every technique in the model.

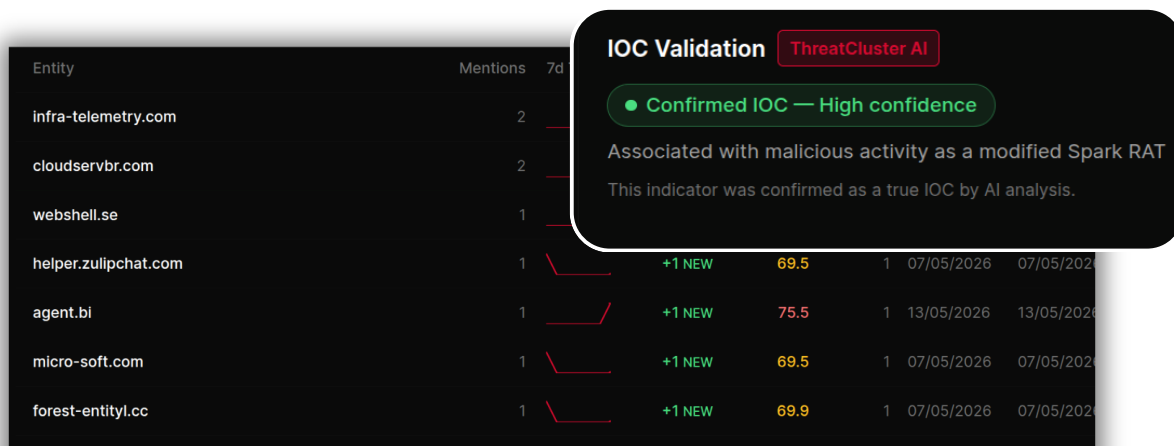


hello@threatcluster.io
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



Indicators of Compromise

Every article that enters the pipeline is extracted for IOCs, validated for confidence, and made available wherever your analysts and tooling need them.



| Entity | Mentions | 7d | | | | | |
|----------------------|----------|----|--------|------|---|------------|------------|
| infra-telemetry.com | 2 | | | | | | |
| cloudservbr.com | 2 | | | | | | |
| webshell.se | 1 | | | | | | |
| helper.zulipchat.com | 1 | | +1 NEW | 69.5 | 1 | 07/05/2026 | 07/05/2026 |
| agent.bi | 1 | | +1 NEW | 75.5 | 1 | 13/05/2026 | 13/05/2026 |
| micro-soft.com | 1 | | +1 NEW | 69.5 | 1 | 07/05/2026 | 07/05/2026 |
| forest-entityl.cc | 1 | | +1 NEW | 69.9 | 1 | 07/05/2026 | 07/05/2026 |

Extraction

Two extractors run on every article. Deterministic regex captures IPv4, IPv6, domains, URLs, MD5/SHA1/SHA256 hashes, CVE IDs, and crypto wallet addresses. LLM-based extraction handles contextual entities: threat actors, malware families, MITRE techniques, tools, industries, and targets. Benign domains, invalid hashes, and known false positives are filtered at extraction time.

Validation

Every IOC is assigned a confidence level (high, medium, low, or false positive) with a written justification. Confidence feeds every downstream filter so analysts only see what's been verified.

Formats

Per-cluster or in bulk: TXT, CSV, JSON, STIX 2.1 bundles (with TLP marking), and ATT&CK Navigator layers. Filter by type (IP, domain, hash, URL), confidence, and time range.

hello@threatcluster.io
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



IOC Integrations

ThreatCluster plugs into your existing stack. No rip-and-replace.



MISP feed

Native MISP-compatible feed with manifest, hashes, and event JSON. Stable UUIDs across regenerations so MISP correlation works cleanly.



STIX 2.1

Full bundles per cluster including Report, ThreatActor, Malware, AttackPattern, Vulnerability, Tool, Campaign, Indicator, and Relationships. TLP-marked at export. Compatible with the CTID Attack Flow Builder and any tooling that speaks the standard.



SIEM ingestion

IOC feeds available via REST API, RSS, or direct webhook push into Splunk, Microsoft Sentinel, Elastic, and OpenSearch. Filter by confidence, type, and freshness. Hunting queries export natively in KQL, SPL, and Lucene.



CLI

``tc iocs feed`, `tc iocs export`, `tc threats iocs`, `tc threats stix``. Same data as the web UI, built for scripts, cron jobs, and CI/CD pipelines.

hello@threatcluster.io

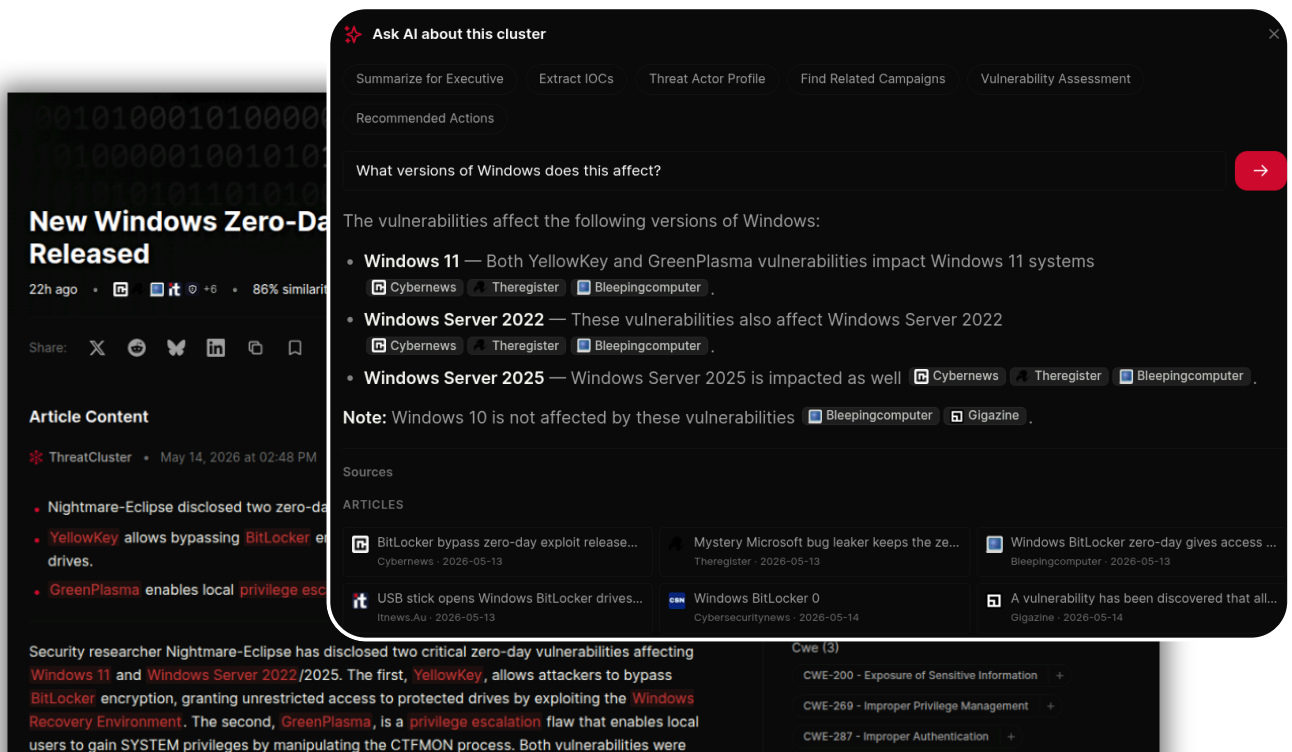
71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

ThreatCluster AI

The analyst layer on top of the threat graph. Ask questions, get answers grounded in the data, with citations to every source.



Ask AI on a cluster

Six pre-built actions: Executive Summary, Extract IOCs, Threat Actor Profile, Related Campaigns, Vulnerability Assessment, and Recommended Actions. Plus a free-form question box for whatever else you need.



Across the platform

The global search bar handles cross-cluster questions. "Which Russian APTs targeted healthcare in the last 30 days?" gets an answer drawn from the full corpus.



Grounded, not general

The model works from the cluster's own context: article bodies, sub-articles, vendor advisories, CVE enrichment, threat actor profiles, IOCs, and related clusters. Not the open web.

hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

CLI and API

ThreatCluster without the browser. Every capability the platform has is reachable as a REST API, a `tc` command, or a tool any agent runtime can call.



Easy Install

``pipx install threatcluster-cli``. One line. Mint an agent key in Settings with scoped permissions (threats:read, iocs:read, darkweb:read, etc.), paste it into ``tc auth login``, and credentials live in your OS keyring. Never on disk.

JSON First

Every command outputs structured JSON. ``tc <cmd> | jq`` for everything. Shell pipelines, cron jobs, and CI/CD steps are first-class.

Live Streaming

``tc threats list --watch`` streams the cluster feed as NDJSON. Pull STIX bundles (``tc threats stix <id>``), grep IOCs by type (``tc iocs feed --type hash``), export in bulk with full filter controls.

Agent Ready

Drop-in tool surface for any agent runtime: Claude Code, custom GPTs, or your own agents. Same endpoints the website uses, same auth, same scopes.

Rest API

Full documentation at `/docs/cli`. Everything available in the web UI is available programmatically.



hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



Pricing and tiers

MSSP pricing is per managed customer. You pay for the clients you have, not the clients you might have. No minimum commitment, no maximum cap. Add a customer when you win the contract, remove them when you don't. The platform grows with your book.

| Category | Feature | MSSP |
|--------------|------------------------------------|----------------|
| Intelligence | Cluster Views | Unlimited |
| | Entity Views | Unlimited |
| | Enhanced Analysis | Yes |
| | Attack Flows (CTID Attack Flow v3) | Yes |
| | D3FEND Countermeasures | Yes |
| | CWE Extraction | Yes |
| | Public Exploit Tracking (Sonar) | Yes |
| | Sub-Article Link Enrichment | Yes |
| | X/Twitter Intelligence | Yes |
| | Rising Threats (Explore) | Yes |
| Dark Web | Ransomware Leak-Site Tracking | Yes |
| | Credential Market Monitoring | Yes |
| | Underground Forum Monitoring | Yes |
| | Breach Matching | Yes |
| | Company Domain Monitoring | Multi-customer |

| Category | Feature | MSSP |
|---------------------|--|------|
| Exposure Management | Per-Customer Asset Inventory | Yes |
| | Asset Connectors (Tenable, Defender, CrowdStrike) | Yes |
| | Bulk Upload (CSV/JSON) | Yes |
| | API Asset Push | Yes |
| | CISA SSVC Ranking | Yes |
| | Asset Tagging (internet-facing, crown-jewel, isolated) | Yes |
| Threat Hunting | Industry Threat Models (17 sectors) | Yes |
| | Hunting Queries (KQL, SPL, Lucene) | Yes |
| | Hunt Playbooks | Yes |
| | ATT&CK Navigator Export | Yes |
| | Diamond Model View | Yes |
| | IOC Watchlist Export | Yes |

| Category | Feature | MSSP |
|------------------|--|-----------|
| Feeds and Alerts | Personalised Threat Digest | Yes |
| | Custom Feeds | Custom |
| | Tracked Interests | Unlimited |
| | Alert Rules | Custom |
| | Webhooks | Custom |
| | RSS Feed | Yes |
| | MISP Feed | 50 events |
| | Scheduled Reports | Yes |
| | Triggers (cluster, CVE threshold, entity, KEV) | Yes |
| | Actions (webhook, Slack, Teams, email, ticket, AI summary) | Yes |
| | Dry-Run Against Historical Data | Yes |
| | Per-Workflow Audit Log | Yes |
| Reporting | Report Generation | Custom |
| | Notion-Style Editor | Yes |
| | Dynamic Content Blocks | Yes |
| | White-Labelled Reporting | Yes |
| | Scheduled Delivery (daily/weekly/monthly/quarterly) | Yes |
| | PDF / HTML / Markdown Export | Yes |
| | Public Shareable URL | Yes |
| | Theming (dark/light, colours, fonts, logo) | Yes |

| Category | Feature | MSSP |
|----------------------|--|------------------|
| MSSP | Multi-Customer Scoping | Yes |
| | Customer Portal (read-only client view) | Yes |
| | Aggregate MSSP Dashboard | Yes |
| | Customer-Scoped Alert Routing | Yes |
| | Per-Customer Exposure Management | Yes |
| | Custom Feature Development | Yes |
| AI | Ask AI (per-cluster) | 99/day |
| | Cluster AI (global search) | 999/day |
| | Report AI (editor) | Yes |
| | Inline Source Citations | Yes |
| Collections and Tags | Collections | Custom |
| | Tags | Unlimited |
| | Team Sharing | Yes (with roles) |
| IOC Exports | TXT / CSV / JSON | Yes |
| | STIX 2.1 Bundles (TLP-marked) | Yes |
| | Bulk IOC Export (confidence/type/time filters) | Yes |
| Integrations | REST API | Higher limits |
| | CLI (tc) | Yes |
| | Agent Tool Surface | Yes |
| | SIEM Ingestion (Splunk, Sentinel, Elastic, OpenSearch) | Yes |
| | SOAR / Ticketing (webhook routing) | Yes |

Behind ThreatCluster



James Mockford

Co-Founder & Managing Director

Security engineering background spanning defence consultancy, managed security, telecoms infrastructure, and critical national infrastructure including OT/ICS in the water sector. Petty Officer in the Royal Naval Reserve Maritime Cyber Unit.



Reyben T. Cortes

Co-Founder & Director of Threat Research

Network Security Engineer, Cyber Threat Intelligence Analyst, and OSINT practitioner. Former Cyber Threat Analyst for the U.S. Department of Homeland Security, delivering briefings to SLTT, CISA, and FBI InfraGard leaders on ransomware, APTs, and election infrastructure threats.

Advisory Partnerships

ThreatCluster co-publishes joint threat advisories with Defused (cyber deception and early warning), Ransom-ISAC (ransomware analysis and collective defence), and detections.ai (community-driven detection rules). These partnerships bring complementary data sources into the platform where open-source scraping alone doesn't reach.



RANSOM-ISAC



detections.ai

hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster

Get Started

Create a free account at threatcluster.io and explore the platform, no sales call required. Everything in this document is built on top of what's already there.

When you're ready to talk, book a demo and we'll scope it to your environment. From first call to delivering intelligence to your first client in under a week.

hello@threatcluster.io

threatcluster.io

**ThreatCluster Ltd. Registered in England and Wales.
Company No. 17124226.**

**Registered Office: 71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ.**



hello@threatcluster.io

71-75 Shelton Street, Covent Garden,
London, WC2H 9JQ



ThreatCluster