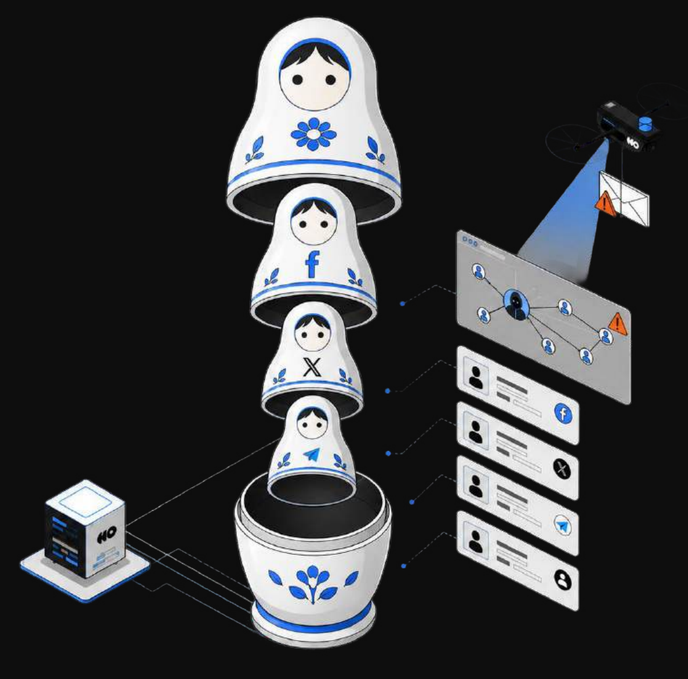
outtake Actor Tracing

The threat is the person.
Not the post.

Actor Tracing models the real-world threat actor behind digital threats, linking accounts across platforms with audit-logged human confirmation, scoring risk across three signal layers, and writing the daily Threat Report your security team needs.



88%
of social engineering attacks rely on impersonation

67%
of security leaders say AI expanded their attack surface

~2 hrs
manual analyst time to link one actor across platforms

15 min
Outtake detection cadence from signal to alert

THE PROBLEM

You're finding the accounts. Intake is finding the people.

01 Watchlist Firehose

All the noise. None of the threat.

Legacy watchlists pull in every mention of every name. Fan posts. Neutral coverage. Passing references. The actual threats to your protected assets sit unread in the same queue.

02 Alert noise

Posts without people.

A first-time troll and a five-month fixation case look identical at the content layer. Most tools score the post. They cannot score the person behind it.

03 No continuity

Physical exposure without digital visibility.

When the same actor surfaces against a new principal, the fixation history, linked accounts, and prior escalation pattern do not carry over. Intelligence dies at the case boundary.

THE ACTOR INVESTIGATION JOURNEY

From signal to actor to action, autonomously.

Step 01 →

Detect Signals

Workflow Agent classifies content across social, fringe forums, dark web, and the open web against the protected principal.

Step 02 →

Model the Actor

Profile Agent creates a Threat Actor record only when threat signals warrant. Threat-initiated by design.

Step 03 →

Alias Across Platforms

Graph expansion proposes linked accounts. Every confirmation logged: who, when, why.

Step 04 →

Score & Tier

Continuous risk scoring across content, account, and threat actor signal layers. Critical, Medium, Low.

Step 05 →

Deliver the Digest

Daily Threat Report Digest writes itself for the GSOC, the CISO, or outside counsel.

TRUSTED BY THE BEST

ANTHROP\C · NVIDIA · DUNKIN' DONUTS · OpenAI · Pershing Square Holdings · APPLOVIN

THE DIGITAL TRUST PLATFORM

GLOBAL SIGNAL NETWORK

DARK WEB · DOMAINS · ADS

DIGITAL TRUST RESERVOIR™

The more it sees, the more it knows.

THREAT GRAPHING

One signal. Their whole operation exposed.

REMEDIATION

Brand
Impersonation · Fraud

Executive
VIPs · PII · Extortion

Product
SaaS abuse · Token fraud

Threats removed in hours, not weeks

SOLUTIONS

Built for every team that investigates people or groups.

Executive Protection

Principal security teams, family offices, and GSOCs protecting named individuals.

- **POI Daily Triage**
  Risk-ranked actor workflow per principal. Replaces flat content queues.
- **Cross-Platform Identity Linking**
  Aliasing with audit-logged human confirmation. Survives the takedown.

Coordinated Group Threats

Security and brand risk teams facing activist campaigns, boycotts, and protest movements targeting the brand.

- **Group-Level Actor Tracing**
  Map every operator inside a coordinated movement. The channels they organize in, the instigators driving escalation.
- **Pre-Action Coordination Tracking**
  Watch organizing activity intensify across platforms before a campaign reaches the brand or agency.

FinServ & Insider Risk

Asset managers, hedge funds, insurers, and corporate insider-risk teams.

- **Fixation & Escalation Tracking**
  Pattern recognition across time. Dormant actors return to triage when behavior changes.
- **Auditable Aliasing**
  Court-ready dossiers. Every identity decision logged with full audit trail.

PROVEN OUTCOMES

Results that compound with every actor.

3
Signal layers per actor: content, account, threat actor.

2hrs
Manual cross-platform identity linking, replaced by a confirmation click.

34+
Connected nodes per investigation (SAMPLE)

Ready to see the threat before it arrives?

outtake.ai hello@outtake.ai

REQUEST A DEMO →