

Insider Threat & Human Intelligence

The most dangerous vulnerabilities are not in your code — they are in your people.

Insider threats originate from within the perimeter of trust — from people who already have access, already know your systems, and understand exactly where the sensitive data lives. Our HUMINT methodology combines behavioral intelligence with structured assessment to identify risk patterns before they escalate into incidents, and to build the layer of human defense that technology alone is structurally unable to provide.

60%**OF INCIDENTS**

involve an insider with fully legitimate system access at time of the event

197**DAYS DETECT**

average days to detect an insider threat without behavioral monitoring active

\$15.4M**ANNUAL COST**

average annual cost of insider threat incidents per organization worldwide

82%**PREVENTABLE**

show prior observable behavioral indicators that simply went unaddressed

Our HUMINT Services

1

Behavioral Risk Profiling

We assess employee behavior patterns, loyalty indicators, and organizational stress factors using HUMINT methodologies developed for genuinely high-stakes environments.

3

GDPR Conduct Auditing

We audit how employees actually handle personal data in day-to-day practice — identifying gaps between stated policy and real behavior that create regulatory exposure.

5

Security Awareness Training

Scenario-based training that builds genuine security instinct rather than checkbox compliance. Social engineering simulations included in every program by default.

2

Stress Scenario Testing

Simulated high-pressure professional situations to evaluate individual responses under conditions that statistically precede integrity failures and security incidents.

4

Internal Fraud Detection

Early indicators of financial fraud, asset misappropriation, and unauthorized data access — identified through combined behavioral and technical signal analysis.

6

Management Risk Assessment

Evaluation of executive-level risks — expense pattern analysis, fleet monitoring, conflict of interest mapping, and loyalty assessment across the leadership layer.

Why Human Risk Cannot Be Ignored

Technology Has Blind Spots

No DLP or SIEM can detect an employee who decides to walk out with sensitive data. Behavioral intelligence fills the critical gap that technical controls cannot reach.

Indicators Are Always There

Insider threats rarely happen without warning signs. Financial stress, access anomalies, and behavioral shifts are observable — if you have the methodology to look.

Training Changes Behavior

Generic compliance training is forgotten in weeks. Role-specific, scenario-based awareness programs create durable security instinct that protects the organization long-term.

What You Gain

A

Human Risk Mapped

A complete map of your human attack surface — ranked by risk level with proportionate, specific mitigation recommendations for every identified exposure area.

B

Incidents Prevented

Early identification of behavioral risk indicators allows targeted intervention before any incident occurs — protecting data, reputation, and operational continuity.

C

Resilient Culture

An organization whose people understand threats, recognize social engineering, and report anomalies proactively is fundamentally harder to attack from any direction.

"

The behavioral assessment identified three employees displaying active indicators of data exfiltration intent. We acted before a single file left the organization. The avoided loss estimate exceeded €800K.
— CISO, manufacturing group — HUMINT Assessment client

Understand your human risk before it becomes your most costly breach. secureintel.ro