Inside the Risk Intelligence Process

How Alpha Recon Turns Threat Signals into Decision-Grade Risk Intelligence

THE PROBLEM: SIGNALS WITHOUT INTELLIGENCE

Security teams are drowning in **alerts, fragmented data, and changing conditions.** Teams lack the time and tools to continuously reassess risk. 90% of targeted incidents had prior warning signals that were never operationalized. The gap is not information. It is the intelligence infrastructure to act on it.

$405B	90%	$44M
Global Private Security Market	Of targeted incidents had prior warning signals	Median nuclear verdict when negligence is proven

WHAT IS RISK INTELLIGENCE?

Risk intelligence is the probability of threats to create negative impacts on assets. If there is no probability of impact on your security operations and assets, it's noise. Good intelligence helps to make better decisions without requiring more work.

It is the structured process of:

- Identifying indicators of risk across physical, digital, behavioral, and geopolitical domains
- Filtering noise, relevance and source validity against your specific assets and operations
- Assessing exposure, vulnerability, and impact potential with weighted, repeatable scoring
- Producing clear, contributes to defensible recommendations tied to operational decision-making
- Applying risk assessment to security management and strategy

Alpha Recon delivers decision-grade intelligence. Not speculation, not aggregated data, not generic alerts. Every assessment follows structured analytic methods, so it is accurate, repeatable, and usable in real operations, client conversations, and insurance discussions.

HOW IT WORKS: THE RECONOPS HUB

ReconOps Hub is a central risk workflow and management environment. Risk signals are collected, triaged, verified, linked to assets, turned into finished outputs, and documented. The result is a **complete audit trail** for every risk decision.

01
Collect
Monitor open, deep, and dark web sources; social platforms; gov and law enforcement reporting; operational telemetry and crowd-sourced signals.

02
Triage
Rexx AI accelerates signal identification and noise reduction across thousands of data points, isolating developments relevant to your assets.

03
Verify
Human analysts with FBI, DIA, military, and protective intelligence backgrounds validate credibility and assess operational relevance.

04
Link & Score
Each signal is linked to specific assets, locations, routes, or principals. Weighted scoring: Threat Activity (40%), Exposure/Vulnerability (35%), Impact Potential (25%).

05
Analyze
Cross-domain context is applied across physical, political, reputational, behavioral, and digital risk domains. Confidence levels assigned.

06
Summarize
Structured narrative outputs aligned to AR25-50 standards. Sourced, brief-ready, and calibrated to the operational need.

07
Recommend
Clear, defensible recommendations tied to posture, planning, and decision thresholds. No open-ended summaries.

08
Deliver + Audit
Outputs delivered via the SecuRecon platform. Every decision and action is logged in a complete audit trail for defensibility.

THE TECHNOLOGY: REXX AI + SECURECON PLATFORM

SecuRecon is powered by **Rexx**, our security risk management chat bot and manages the AI agents and responds to user commands and ties it to intelligence outputs. Rexx is not a generic LLM wrapper. It is built on real operational security data and trained on proprietary non-public datasets across physical security, travel risk, executive protection, and geo-threat. **Rexx** handles the volume. Our **analysts** handle the judgment. You get outputs that are fast, verified, and operationally relevant.

Domain-Specific
Trained on proprietary, non-public security datasets. Understands the language and logic of protective operations.

Human-in-the-Loop
Machine speed with expert analyst oversight. All outputs are validated before delivery. AI accelerates; analysts decide.

Modular Architecture
Deploys inside GSOCs, field ops, and partner environments. Integrates into existing workflows without disruption.

The **SecuRecon platform** delivers the full **ReconOps workflow** in a single interface: monitoring, scoring, visualization, briefing tools, and report delivery. Unlimited users. Access from Core to Elite tiers.

WHAT WE DELIVER

Monitoring. Reports. Briefings. For new security companies to Fortune 10 companies.

Recon Bytes	Recon Reports	SecuReports
Short, time-sensitive updates delivered through the platform as conditions shift. Continuous monitoring tied to your assets, locations, routes, and principals.	On-demand, structured, operator-ready intelligence reports. TVAs, INTSUMs, SITREPs, Route Recons, City Assessments, Entity Risk Scans, Human Risk Assessments, and more. Sourced, briefable, and defensible.	Monthly intelligence briefs covering emerging risks, incidents, and relevant developments. Keeps teams informed between advances and operations. Includes discounted Recon Report access.

WHAT MAKES ALPHA RECON DIFFERENT

Feature	Why Alpha Recon Stands Out
Methodology	IC-grade tradecraft, robust data sourcing and noise control adapted to protective operations and corporate security. Not academic analysis or generic threat intel.
Rexx AI Engine	Proprietary AI trained on non-public security datasets. Not a generic LLM. Accelerates triage and synthesis while analysts validate every output.
Precision Scoring	Weighted scoring across Threat Activity (40%), Exposure/Vulnerability (35%), and Impact Potential (25%). Every assessment is structured and repeatable.
Defensible Outputs	Every report includes source types, relevance notes, and confidence levels. Designed to hold up in insurance conversations, client briefings, and legal reviews.
Real-World Application	Built for EP teams, GSOCs, HNW environments, corporate leaders, and venue operations. Not generic threat intel platforms.
Analyst Team	Former FBI, DIA, special ops, and protective intelligence professionals. Analysts who have operated in various threat environments in the world.

Better security decisions. Less liability. More contracts. High-end intelligence capability without building your own intel team.