CYBER EVOLVE

Whitepaper

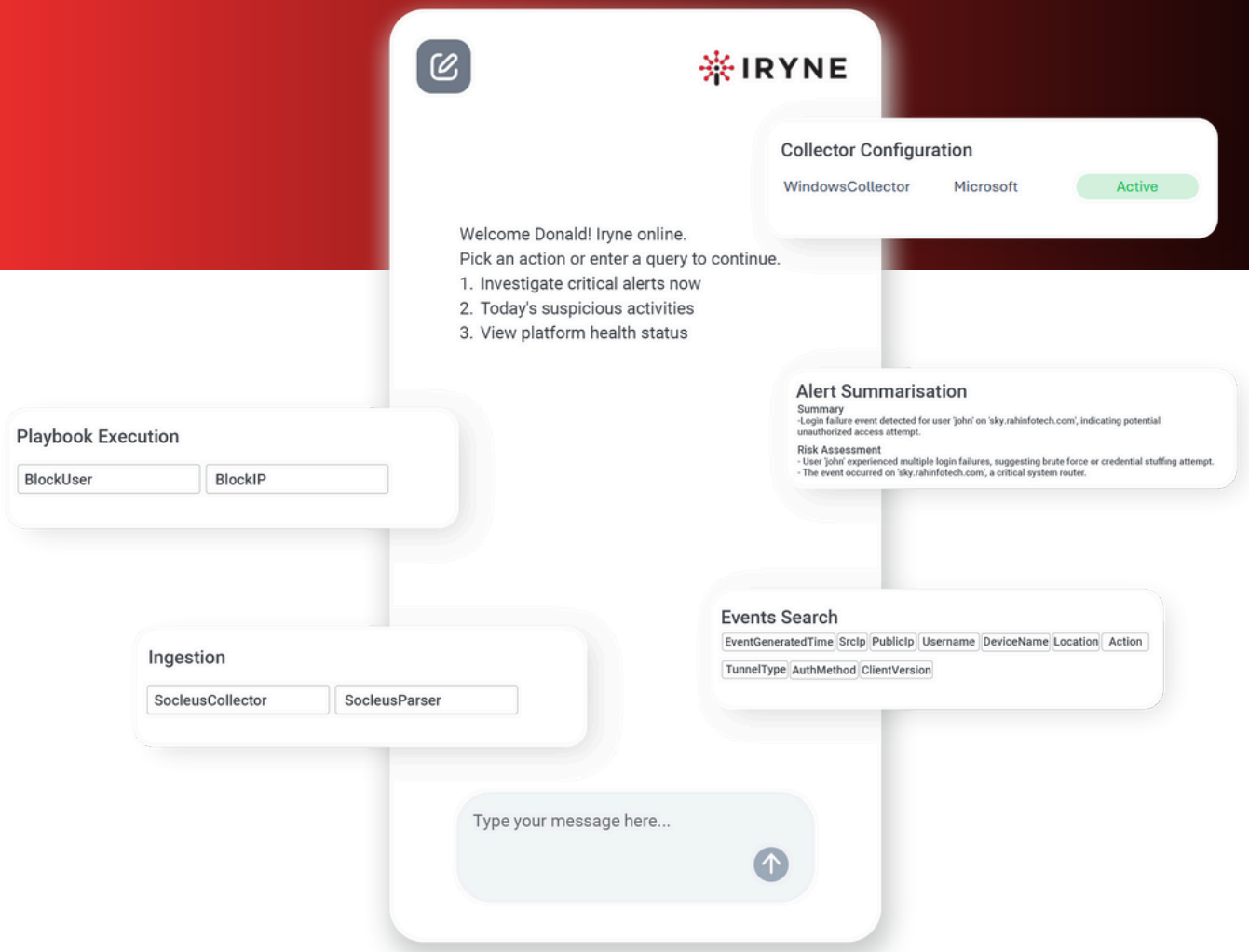
IRYNE

Agentic AI for Autonomous Security Operations

Executive Overview

Security Operations Centers (SOCs) are overwhelmed by alert volumes, fragmented tooling, and analyst burnout. While SIEM platforms have evolved in scale and analytics, response operations remain largely manual, rule-driven, and dependent on scarce human expertise. IRYNE addresses this gap by introducing **Agentic AI** into security operations transforming detection into decisive, outcome-driven action.

IRYNE is an Agentic AI execution layer, designed to operate **natively within Cyber Evolves Socleus and as a bolt-on capability for third-party SIEM platforms**. It enables intelligent investigation, reasoning, and response while preserving governance, transparency, and human control.



The Role of IRYNE in Modern SOC Architecture

Value: Accelerated time-to-value without SIEM replacement risk.

- IRYNE functions as the decision and execution plane of the SOC, sitting downstream of detection and analytics.
- With Cyber Evolves Socleus, IRYNE is deeply embedded, sharing data models, context, and workflows.
- With external SIEMs, IRYNE integrates through standardized ingestion, APIs, and connectors without disrupting existing investments.

Built-In with Socleus: Native Agentic Intelligence

Value: Faster investigations, lower MTTR, and reduced analyst fatigue.
When deployed with Socleus, IRYNE operates as a first-class, built-in capability.

- Direct access to enriched events, alerts, threats, cases, and historical context
- Native orchestration across investigation, enrichment, and response steps
- Unified analyst experience with AI-driven insights and recommendations
- This tight coupling enables IRYNE agents to reason holistically across alerts, behaviours, assets, and timelines.

Bolted-On for Any SIEM: Vendor-Agnostic Autonomy

Value: AI-driven efficiency layered on top of existing SIEM investments.

IRYNE is architected to function independently of the underlying SIEM.

- Integrates with leading SIEM platforms via APIs and alert pipelines
- Normalizes incoming alerts into IRYNE's reasoning framework
- Executes investigations and actions while respecting existing workflows

This allows organizations and MSSPs to introduce agentic AI without re-platforming.

Agentic AI Capabilities

Value: Consistent, explainable decisions at SOC scale.

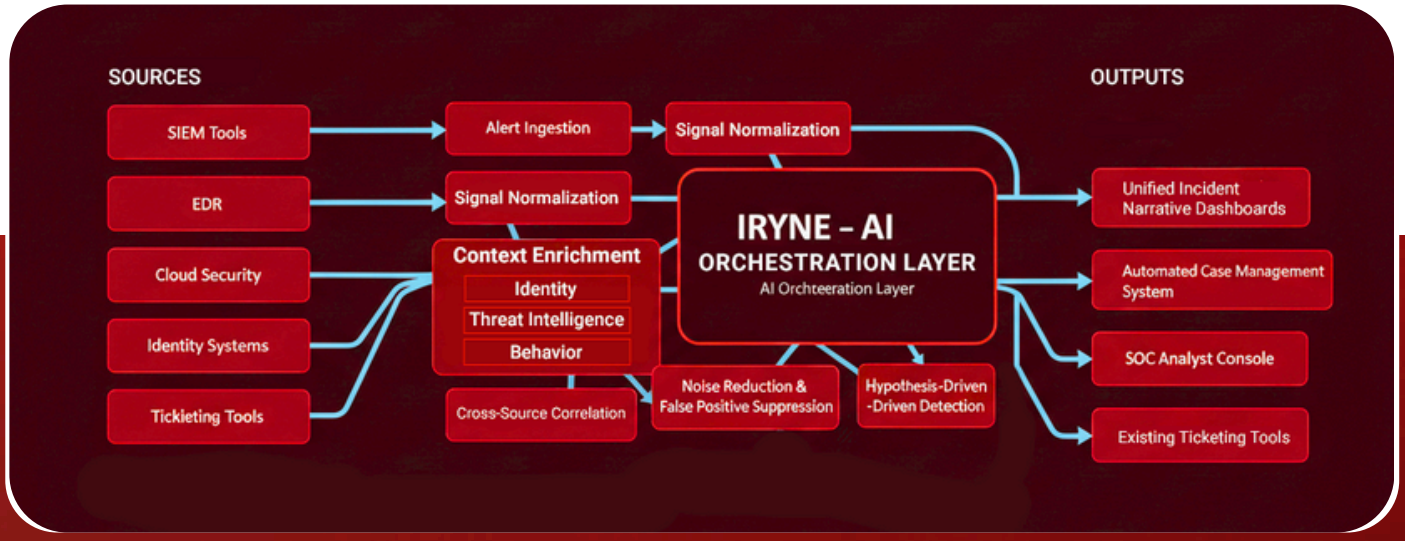
- IRYNE goes beyond traditional SOAR by introducing reasoning agents:
- Autonomous alert triage and prioritization
- Multi-step investigation and evidence gathering
- Threat intelligence correlation and hypothesis testing
- Analyst-in-the-loop or policy-driven execution

Governance, Control, and Trust

Value: Autonomy without loss of control or accountability.

IRYNE is designed with enterprise-grade controls:

- Human approval gates and confidence scoring
- Full audit trails of AI decisions and actions
- Policy-based autonomy levels by customer or tenant



Conclusion

From Automation to Autonomy

IRYNE represents the evolution from scripted automation to intelligent, agent-driven security operations.

- Built-in for Socleus to unlock full AI-native SOC transformation
- Bolted-on for all other SIEMs to extend their operational lifespan
- Designed for enterprises and MSSPs seeking efficiency, scale, and differentiation

IRYNE transforms security operations from reactive execution to autonomous defence with human confidence.

CYBER EVOLVE

About Cyber Evolve

Cyber Evolve delivers an AI-native cybersecurity platform designed for modern threats. By combining Responsible Agentic AI, real-time intelligence, and automated investigation, we help security teams move faster, reduce noise, and respond with confidence—built for the future of cyber defense.

www.cyberevolve.com