# **Socleus:** A Next-Generation SIEM for Enterprise Security Operations

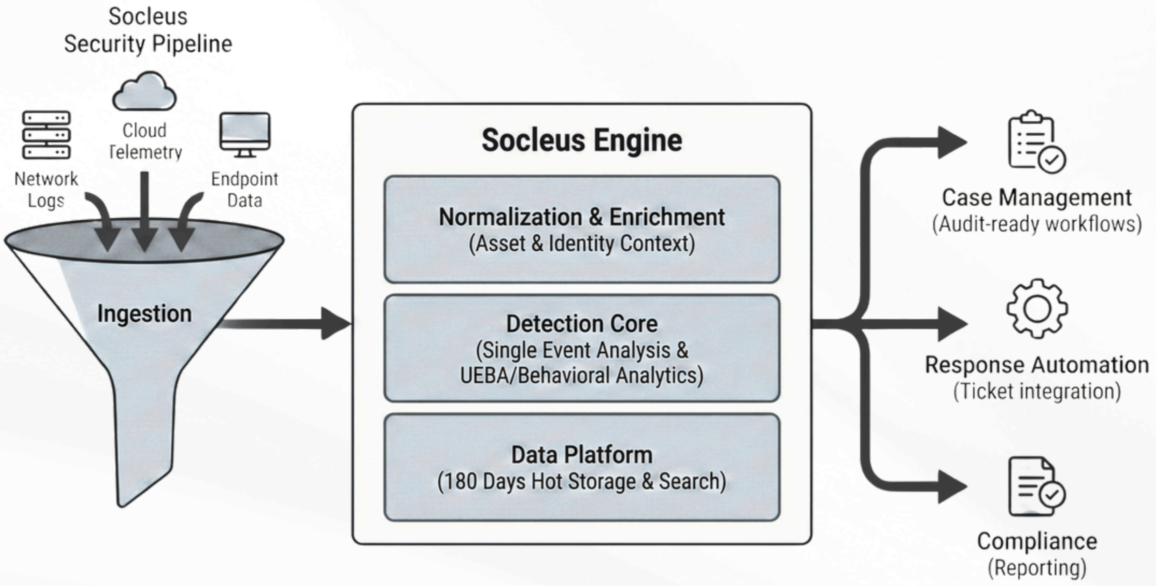
Modern enterprises face escalating threat complexity, explosive data growth, and relentless regulatory pressure. Traditional SIEM platforms struggle to scale, correlate, and deliver actionable intelligence at SOC speed. Socleus is designed as a next-generation, AI-ready SIEM foundation that prioritizes visibility, performance, and operational efficiency for enterprise SOCs.

Whitepaper

## Log Collection, Translation, and Enrichment

### Consistent data fidelity, improved detection accuracy, and reduced analyst preparation effort

Socleus ingests high-volume security and non-security telemetry, normalizes diverse formats, and enriches events with asset, identity, and threat intelligence context.



Socleus Security Pipeline
Network Logs
Cloud Telemetry
Endpoint Data
Ingestion
Socleus Engine
Normalization & Enrichment (Asset & Identity Context)
Detection Core (Single Event Analysis & UEBA/Behavioral Analytics)
Data Platform (180 Days Hot Storage & Search)
Case Management (Audit-ready workflows)
Response Automation (Ticket integration)
Compliance (Reporting)

## Single and Aggregate Event Analysis

### Faster triage, higher signal-to-noise ratio, and earlier threat containment

Socleus enables deep single-event inspection while correlating events across time, users, and assets to expose multi-stage and low-signal attacks.

## Behavioral Analytics

### Improved insider threat visibility

Built-in UEBA models baseline normal behavior and detect anomalies indicating compromised credentials, insider risk, or lateral movement.

### Case Management and Workflow

Consistent response execution improved operational resilience.

Socleus provides centralized case management with evidence tracking, collaboration, and audit-ready investigation workflows.

### Data Platform and Search Performance

Compliance readiness, accelerated investigations, and predictable operational costs.

Socleus delivers 180 days of hot storage and full-text search for rapid access to historical security data.

### Response Automation and Integrations

Reduced manual effort, improved response consistency, and controlled risk exposure.

Limited automation integrates with ticketing systems and external intelligence sources to streamline enrichment and governed response actions.

### Deployment Models

Architectural flexibility and long-term platform control.

Socleus supports on-premises and hosted cloud deployments, ensuring consistent capabilities while meeting enterprise data residency and compliance requirements.

# Conclusion

## A Strategic SIEM Foundation for the Enterprise CISO

Socleus delivers a modern SIEM platform designed to meet enterprise-scale security, compliance, and operational demands.

- Provides a scalable, high-performance SIEM foundation for modern SOCs
- Unifies ingestion, analytics, UEBA, and workflows to reduce tool sprawl
- Enables faster investigations and governed response with full visibility
- Supports on-premises and cloud deployments to meet regulatory requirements
- Delivers predictable costs, operational efficiency, and audit readiness
- Aligns security operations with business risk, resilience, and growth objectives

Socleus empowers CISOs with clarity, control, and confidence—today and as threat landscapes evolve.

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