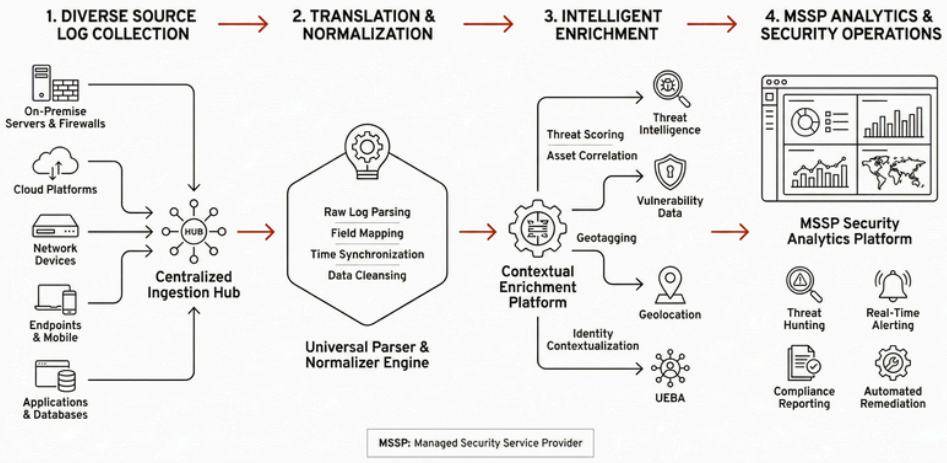
CYBER EVOLVE | SOCLEUS

Socleus: A Next-Generation SIEM Built for MSSP Scale, Efficiency, and Profitability

Managed Security Service Providers (MSSPs) operate under constant pressure to deliver high-quality security outcomes while maintaining strict cost controls and predictable margins. Traditional SIEM platforms, designed primarily for single-enterprise environments, often introduce operational overhead, licensing complexity, and scalability challenges that directly impact MSSP profitability. Socleus is purpose-built as a next-generation SIEM platform that enables MSSPs to operate efficiently, scale services seamlessly, and deliver differentiated security value to customers.

Whitepaper



Log Collection, Translation, and Enrichment at MSSP Scale

Value: Reduced onboarding time, lower integration costs, and faster time-to-revenue for new customers

Socleus ingests and normalizes high-volume, multi-tenant telemetry across diverse customer environments, security tools, and cloud platforms. Enrichment adds asset, identity, and threat intelligence context without custom engineering per tenant.

Single and Aggregate Event Analysis for Multi-Tenant SOCs

Higher analyst productivity reduced false positives, and consistent detection quality across all customers.

Socleus supports deep single-event analysis while correlating events across users, assets, and timelines within each tenant. Correlation logic is reusable across customers, minimizing rule duplication.

Behavioral Analytics (UEBA)

Improved alert prioritization and differentiated premium detection services.

Built-in UEBA establishes behavioral baselines per tenant and detects anomalies indicative of compromised accounts, insider threats, or lateral movement. Risk scoring prioritizes investigations across customers.

Response Automation and Ecosystem Integrations

Reduced manual effort, and scalable response operations without added risk.

Native integrations with ticketing systems and third-party threat intelligence tools streamline enrichment and response workflows while keeping analysts in control.

High-Performance Data Platform and Search

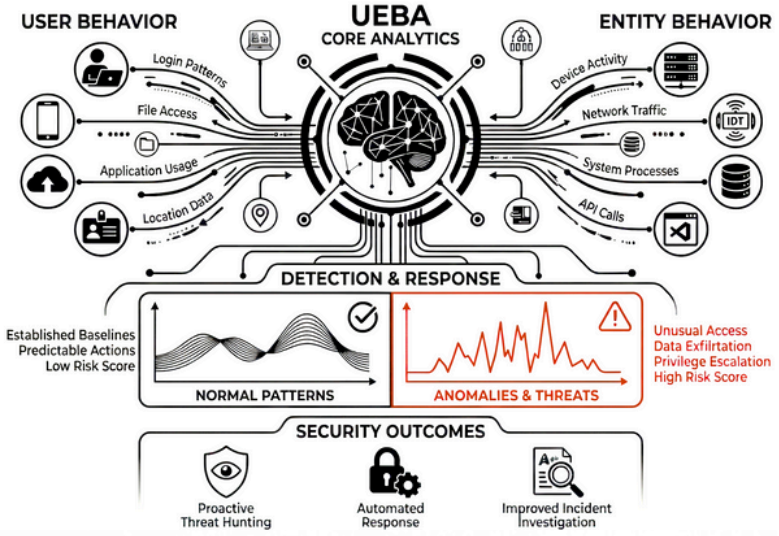
Value: Predictable infrastructure costs, faster investigations, and simplified compliance support for customers.

Socleus offers 180 days of hot storage and full-text search across all customer telemetry, enabling rapid investigations without tiered storage complexity.

Flexible Deployment Models for MSSP Operations

Value: Deployment flexibility and reduced infrastructure lock-in.

Socleus supports both on-premise and hosted cloud deployments, enabling MSSPs to align with customer data residency, regulatory, and commercial requirements.



Conclusion

Driving MSSP Efficiency and Margin Expansion

Socleus is designed to help MSSPs scale security operations profitably while delivering consistent, high-value outcomes to customers.

- Reduces operational overhead and analyst workload
- Enables multi-tenant scale without complexity
- Lowers onboarding, integration, and infrastructure costs
- Supports flexible pricing and differentiated service tiers
- Improves margin predictability and long-term growth

For MSSP CISOs and business owners, Socleus is not just a SIEM it is a strategic platform for operational efficiency, cost optimization, and sustainable revenue growth.

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