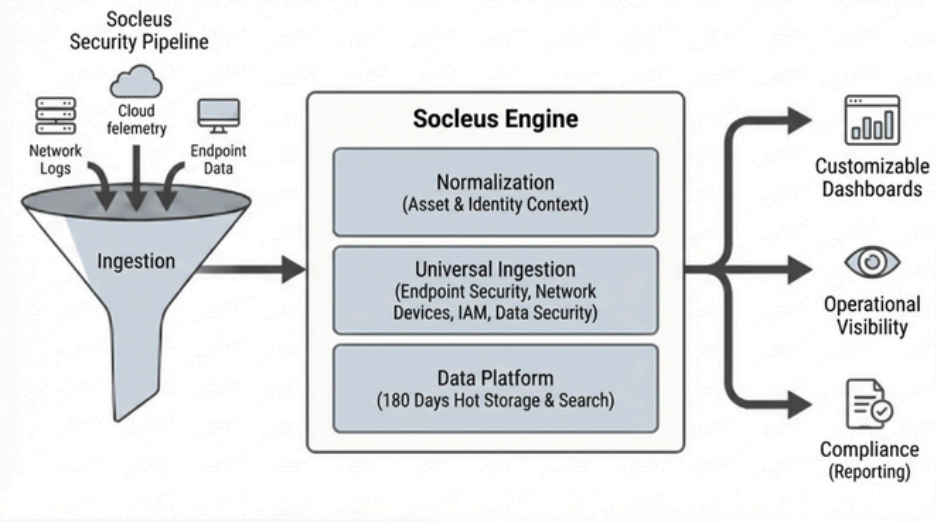
CYBER EVOLVE | SOCLEUS

Socleus LogStream: A High-Performance Logging and Visualization Foundation for the Enterprise

Modern enterprises are characterized by explosive data growth and relentless regulatory pressure, requiring a robust foundation for security telemetry. Socleus LogStream is an enterprise-grade SIEM Logger designed to prioritize visibility, performance, and operational efficiency. By focusing on high-throughput ingestion, normalization, and rapid search, LogStream provides the essential data layer required for compliance readiness and accelerated investigations.

Whitepaper



High-Performance Data Platform and Search

Socleus LogStream is engineered for speed, providing the infrastructure necessary for rapid access to historical security data.

- Indexing and Storage: The platform delivers 180 days of hot storage, enabling full-text search capabilities across all ingested telemetry. This eliminates the complexity of tiered storage while ensuring data is immediately available for query.
- Search Performance: The system is optimized for "SOC speed," allowing for fast triage and investigation of historical records to expose the scope of activity within the environment.

High-Throughput Log Ingestion and Normalization

The core of the Socleus pipeline is built to handle high-volume security and non-security telemetry from diverse sources, including network logs, cloud telemetry, and endpoint data.

- Universal Ingestion: The platform utilizes a centralized hub to collect data from on-premise servers, firewalls, cloud platforms, network devices, and applications.
- Universal Ingestion: The platform utilizes a centralized hub to collect data from on-premise servers, firewalls, cloud platforms, network devices, and applications.

This architecture ensures that diverse multi-tenant or multi-departmental telemetry is normalized across all environments without the need for custom engineering per source.

Visual Dashboards and Compliance Reporting

Beyond data storage, LogStream provides the tools necessary to transform raw logs into actionable insights through visual reporting.

- **Customizable Dashboards**: The platform includes an analytics interface for real-time monitoring of security telemetry through intuitive visualizations.
- **Audit-Ready Reporting**: To meet regulatory requirements, the system supports automated compliance reporting, providing a clear audit trail of all indexed activities.
- **Operational Visibility**: Decision-makers gain a unified view of ingestion health and system performance, aligning security operations with business risk and resilience objectives.

Architecture and Deployment Flexibility

Flexible, Scalable, and Cost-Predictable Deployment

- Supports flexible deployment models, including on-premises and cloud environments
- Meets enterprise data residency and compliance requirements
- Built on a scalable architecture to handle growing data volumes
- Ensures predictable and controlled costs as log ingestion scales

Conclusion

Socleus LogStream delivers a strategic logging foundation designed to meet the scale and operational demands of the modern enterprise.

- Provides a high-performance environment for log collection, normalization, and visualization
- Empowers CISOs and SOC Managers with clarity and control for audit readiness
- Enables rapid and effective investigations
- Ensures predictable costs through a focused operational approach
- Supports a scalable path for long-term 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