graylog

How ScaryByte Secures Critical Institutions with Graylog, AWS & AI-Powered Detection

COMPANY SNAPSHOT

Industry:

Information Technology & Services

Headquarters:

Johannesburg, Gauteng, South Africa

Company Size: 50 employees

Founded: 2020

Core Capabilities:

Penetration Testing, Red Teaming, SIEM, IPS/IDS, Digital Forensics, Incident Response, Behavioral Monitoring, Cyber Intelligence

Products Used:

Graylog Security, AWS, Obala AI Platform, Consumer Profile Bureau, HornetStrike

SCARYBYTE

OVERVIEW

ScaryByte, founded in 2020, is a South Africa-based cybersecurity firm built to tackle complex security challenges that others avoid. With deep expertise in red teaming, SIEM, behavioral threat detection, and digital forensics, ScaryByte helps organizations across industries transform data chaos into actionable security outcomes.

Their proprietary platform, Obala (Zulu for "in the open"), reflects their mission to deliver transparency where none exists, detect threats others miss, and protect institutions where trust is critical. Whether safeguarding educational institutions from academic fraud, helping banks mitigate insider threats, supporting credit bureaus in data integrity, or assisting public sector agencies with fraud detection, ScaryByte tailors its approach to meet each client's unique security challenges.

"We don't just detect anomalies; we are rebuilding integrity where it matters most."

— Karim Jabar, CEO, ScaryByte

THE PROBLEM: DATA EVERYWHERE, NO VISIBILITY

From universities and credit bureaus to financial institutions and public sector entities, organizations face an overwhelming flood of logs from fragmented systems but lack the unified visibility to connect the dots. Without centralized observability, security teams struggle to detect:

- Shared credentials and location anomalies
- Suspicious behaviors across transactions, exams, or access attempts
- Patterns of misconduct or fraud
- Data leaks and integrity violations

Manual investigations across siloed systems consume valuable time while threats continue unchecked.

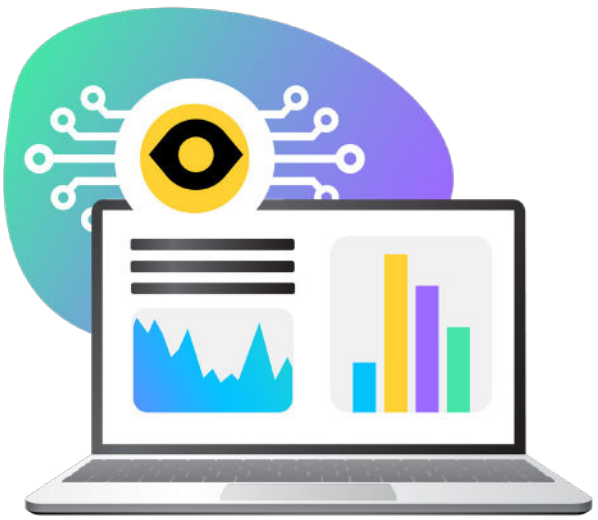
THE SOLUTION: OBALA, GRAYLOG SECURITY, AND AWS

ScaryByte's integrated security platform combines **Graylog Security**, **AWS**, and **Obala AI** to unify observability, streamline detection, and accelerate response across industries. Whether deployed in a university, bank, or government agency, the platform adapts to provide comprehensive visibility and control.

Obala's Key Modules Include:

- **Obala Core:** Ingestion, correlation, and decision-making engine
- **Obala Signal:** Telemetry collection from networks, endpoints, and APIs
- **Obala Insight:** Mapping of data flows for leadership-level visibility
- **Obala Guard:** Real-time threat mitigation with automated response orchestration

Clients gain a scalable security framework capable of ingesting logs seamlessly, detecting advanced threats in real time, and accelerating response cycles.



Outcomes That Matter

UNIFIED OBSERVABILITY

- Centralizes logs from fragmented platforms across sectors such as education, banking, and public service
- Surfaces anomalies through Obala's flow maps and Graylog dashboards

REAL-TIME THREAT DETECTION

- Behavioral scoring flags high-risk activities in both academic and enterprise environments
- Automated workflows reduce response times and eliminate manual bottlenecks

FASTER FORENSICS AND COMPLIANCE

- Investigations that once took hours are resolved in minutes
- Comprehensive audit trails improve transparency and regulatory alignment

EXPERT-LED DEPLOYMENTS, SCALABLE ON AWS

- Each deployment is customized by ScaryByte experts to address industry-specific use cases
- AWS scalability ensures performance for institutions of all sizes

OPEN SOURCE: THE FOOT IN THE DOOR

In South Africa's public sector, lengthy procurement processes often stall security initiatives. For ScaryByte, open source Graylog provided a powerful enabler to circumvent these delays.

Emergency deployments of Graylog Open allowed ScaryByte to deliver immediate value in environments like banks battling internal fraud or public sector agencies facing data integrity threats. This hands-on proof of value streamlined the transition to Graylog Security, accelerating adoption across multiple industries.

A PARTNER THAT DELIVERS OUTCOMES, NOT JUST ALERTS

ScaryByte's model is built around partnership-driven security services. They don't just deploy software—they align detection strategies with each client's operational mission, ensuring outcomes that matter.

Leveraging Graylog's intuitive platform, Obala's AI-driven insights, and ScaryByte's SOC expertise, clients across sectors gain the ability to:

- Detect fraud and misconduct early, whether in education or financial services
- Investigate incidents rapidly with full context
- Prove system integrity through clear, auditable evidence

> **The open source deployment has given us that sort of footing in the door to allow us to present Graylog as a solution. Public sector groups are skeptical and want to see proof before allocating budgets. Open source allows us to demonstrate Graylog's capabilities firsthand, allowing us to demonstrate to clients the value of having Graylog within their network before any CapEx commitments.**
>
> **— Rayhaan Younuss, Partner & Channel Director, ScaryByte**

CYBERSECURITY THAT BUILDS CONFIDENCE

ScaryByte's work with Graylog and AWS goes beyond technical deployments. It's about restoring trust across critical industries. Whether protecting educational institutions from exam fraud, ensuring banks maintain transactional integrity, or helping public sector agencies improve transparency, ScaryByte delivers clarity, control, and confidence.

Because real security does not just alert; it protects what matters. Ready to elevate your detection strategy?

Explore Graylog Security >