Powering Zambia's National Cybersecurity Backbone: The SMART Zambia Institute PSOC



AI-Driven Threat Detection and Response delivered through Africa's first government-owned, centrally operated national Public Security Operation Centre.

Executive Summary

Seceon's deployment at the SMART Zambia Institute (SZI) Public Security Operation Centre (PSOC) in Lusaka has delivered AI-powered, automation-first cybersecurity across every Government Ministry of the Republic of Zambia, positioning SZI as the sovereign owner and operator of one of Africa's most advanced national-scale SOCs. Ministries are onboarded to the unified Seceon aiSIEM & aiXDR platform within hours, with coverage progressively scaling to all government entities.

National Context

Zambia's government institutions face an escalating threat landscape spanning citizen data, financial systems, health records, and critical digital infrastructure. As custodian of the country's digital estate, SMART Zambia Institute recognised the need for a unified, centrally managed, sovereign cybersecurity framework, making Zambia a proving ground for AI-driven, government-owned national SOC operations.

Customer Challenge

SMART Zambia Institute required a centralized cybersecurity platform capable of protecting government ministries through a single sovereign Security Operations Centre. The solution needed to provide rapid onboarding, centralized visibility, AI-driven threat detection, and the scalability to support nationwide digital transformation.

Key Outcome at a Glance
Platform Deployed: Seceon aiSIEM & aiXDR (Unified Platform)
Client: SMART Zambia Institute (SZI) – e-Government Division, Office of the President
Scope: All Government Ministries across the Republic of Zambia
SOC Location: Lusaka, Zambia
Model: Government-Owned, Centrally-Operated Public Security Operation Centre
Status: Operational – Actively Monitoring & Protecting National Digital Infrastructure

Real Outcomes Across the SZI PSOC

Since going operational, the PSOC has onboarded key ministries onto a single unified platform, with the remaining government entities progressively joining toward full national coverage. The engagement has surfaced consistent, measurable outcomes:

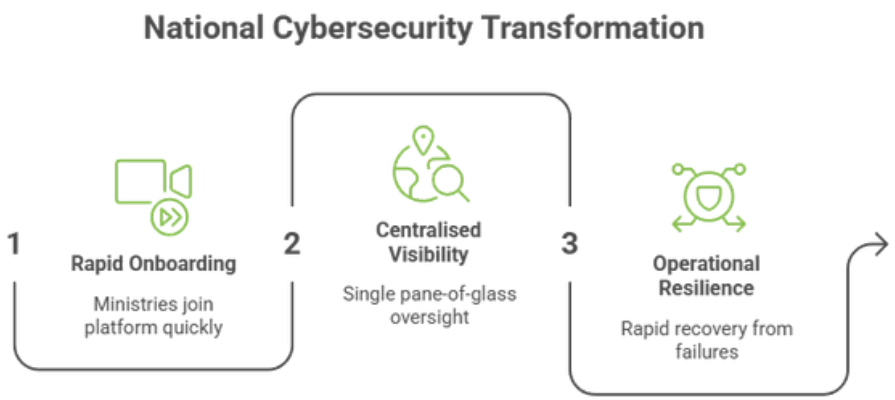
- **Ministries active:** Finance, Education, Statehouse (Office of the President), Justice, Health, and Agriculture are fully onboarded.
- **Coverage target:** 100% of all Government Ministries across Zambia, under progressive onboarding.
- **Operational status:** Live, 24×7 real-time monitoring and protection of national digital infrastructure.

Key Growth Drivers

- **1. Rapid ministry onboarding –** New ministries are brought onto the platform in hours per entity, replacing what typically takes weeks or months with traditional SIEM deployments.
- **2. Centralised visibility at scale –** A single pane-of-glass from Lusaka gives the PSOC team oversight of the entire national digital estate.
- **3. Operational resilience –** Seceon's container-based architecture enables rapid recovery from failures, minimising disruption to multi-tenant government SOC operations.
- **4. Regional benchmark –** The programme positions Zambia as a proven, replicable blueprint for national cybersecurity transformation across African governments.

Seceon deployed its unified aiSIEM and aiXDR platform at the SMART Zambia Institute Public Security Operation Centre in Lusaka. Government ministries are progressively onboarded through a standardized deployment model, enabling centralized monitoring and AI-driven threat detection from a single national SOC.

Zambia's Vision
SMART Zambia Institute has a strategic plan to continuously expand the PSOC's human capital programme training the next generation of cybersecurity professionals from across all government entities to sustain long-term national cybersecurity resilience.



Why SMART Zambia Selected Seceon

Seceon's AI- and ML-powered Open Threat Management platform unifies aiSIEM, aiXDR, UEBA, threat intelligence, and automated response into a single licence – the primary reason SZI selected Seceon to power a national-scale SOC.

- **Single Unified Platform –** SIEM, XDR, UEBA, threat intelligence, and automated response included under one licence, eliminating vendor sprawl.
- **AI/ML at Core –** Machine learning-driven detection reduces false positives and surfaces sophisticated, previously unknown attacks.
- **No Per-EPS Pricing Penalty –** Government can ingest logs from unlimited sources across all Ministries without escalating per-event costs.
- **Built for MSSPs & National SOCs –** Architected for multi-tenant, large-scale deployments – ideal for a national public SOC model.
- **Automated Remediation –** Threats are automatically contained and resolved, reducing dependence on large analyst teams.
- **Rapid Deployment –** Operational within days, with ministry onboarding achievable in hours per entity.

About Seceon

Seceon enables MSPs, MSSPs, and Enterprises to reduce cyber threat risks and their security stack complexity while greatly improving their ability to detect and block threats, and breaches at scale. Seceon's Open Threat Management (OTM) platform augments and automates MSP and MSSP security services with our AI and ML-powered aiSIEM, and aiXDR platforms. The platform delivers gapless coverage by collecting telemetry from logs, identity management, network logs and flows, endpoints, clouds, and applications. It's all enriched and analyzed in real-time by applying threat intelligence, AI and ML models built on behavioral analysis, and correlation engines to create reliable, transparent detections and alerts. Over 850 partners are reselling and/or running the industry's lowest TCO, efficient security services with automated cyber threat remediation and continuous compliance for over 9,800 clients.

Learn more about Seceon

Schedule a Demo www.seceon.com/contact-us/



© 2026 Seceon Inc. All rights reserved. aiSIEM, aiXDR, are trademarks and registered trademarks of Seceon Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners.