African Mining Sector
Cyber Threat Intelligence Report

Q1 2026

Cybershield Security Intelligence Platform

Report Generated: January 09, 2026

Executive Summary

This quarterly report analyzes the cybersecurity posture of 3 mining companies operating across Africa. Our assessment reveals significant exposure to data breach and ransomware attack vectors, with 0.0% of companies classified as CRITICAL risk.

Metric	Value	Risk Level
Companies Scanned	3	
Critical Risk Companies	0	HIGH
Avg Risk Score	0.0/100	
Exposed Databases	0	CRITICAL
Exposed Remote Access	0	HIGH

IMPACT AREA 1: Data Breach Vectors

Exposed database services represent the primary vector for data breaches in the African mining sector. Directly internet-facing databases enable attackers to exfiltrate sensitive operational data, financial records, and employee information.

Most Common Exposed Databases:

No exposed databases detected in this quarter.

IMPACT AREA 2: Ransomware Entry Points

Exposed remote access services (RDP, SSH, VNC) are the primary initial access vectors for ransomware attacks. Mining companies with multiple exposed entry points face significantly elevated risk of ransomware incidents.

Most Common Ransomware Entry Points:

No exposed remote access services detected.