oqio NEXUS · INTELLIGENCE

CYBER THREAT REPORT

Nexus Global Threat Landscape 2026

Attack-surface telemetry, emerging exposure classes, and remediation trends observed across the Oqio Nexus network.

Executive summary

This sample report illustrates the format Oqio Nexus uses to publish threat intelligence to platform subscribers. It summarizes exposure trends observed across anonymized, aggregated telemetry.

Replace this text with your production analysis. Keep the focus on cybersecurity, cloud, AI/ML, and geospatial telemetry topics.

Key findings

1. Time-to-exploit for newly disclosed exposures continued to compress, raising the value of automated, human-validated remediation.

2. Unmanaged and unknown assets remained the leading source of initial access across observed environments.

3. Geospatial correlation of telemetry improved detection of coordinated, multi-region activity.

Methodology

Findings are derived from opt-in, encrypted telemetry contributed by Nexus deployments. Data is aggregated and de-identified prior to analysis.