Sub-national composite risk - darker = higher. Source: GeoBit.

Mauritius dataset (CSV) - events, per-region risk, cyber & sources

1 Day - $5

1 Week - $15

1 Month - $39 - best value

function gbBuyCsv(s,dt,range){var u='/api/data-checkout?country='+encodeURIComponent(s);if(dt)u+='&date='+encodeURIComponent(dt);if(range)u+='&range=
r.json();}).then(function(d){if(d&&d.url){location.href=d.url;}else{alert((d&&d.error)||'Dataset download is not available yet.');}}).catch(function(){alert('Could not start checkout.');});}

Threat Trajectory

Threat Breakdown

Each category 0-100, scored from live conflict, insurgency, crime, protest & Cloudflare Radar cyber feeds. See the full threat matrix

Cyber & Internet Disruption

Layer-7 DDoS attack intensity (0-100, normalized) & internet outages over the last 28 days - Source: Cloudflare Radar.

Situation Summary

Mauritius remains a low-threat destination globally (rank #186, composite score 2) but faces elevated internal volatility driven by post-election political tension, widespread cyber-attack exposure, and concentrated street crime in urban and tourist zones. Port Louis dominates the risk profile (92/100), with secondary urban and resort areas presenting material petty-crime and opportunistic-theft hazards. While no active armed conflict or terrorism incidents are recorded, the combination of political contestation, cyber vulnerability in critical infrastructure, and crime concentration in high-footfall areas creates compounded duty-of-care exposure for corporate operations and visiting personnel.

Key Developments

- Port Louis & national capitals - post-election political tension elevated. General elections concluded amid allegations of state surveillance and wiretapping; opposition parties continue to contest fairness, sustaining high political temperature nationwide and increasing risk of civil unrest or public gatherings that may require avoidance.

- Port Louis, Flic en Flac, Grand Baie - crime hotspots for visitors. U.S. State Department maintains Level 2 advisory (exercise increased caution) citing pickpocketing, purse-snatching, harassment of women, and occasional violent crime concentrated in these three zones; Canadian travel advice confirms higher frequency of theft targeting tourists in these locations.

- Nationwide - thousands of weekly cyber-attacks on key sectors. Financial services, telecoms,

government, and data-driven enterprises face sustained attack volume; exposure to ransomware, data exfiltration, and service disruption remains pervasive and unabated across the country.

- Sands Suites Resort & Spa - LockBit 5.0 ransomware with data-theft threat. High-profile hospitality sector hit with extortion-class ransomware; threat group threatening public data release; illustrates active risk to hotel infrastructure and guest data security across the tourism industry.

- Mauritius Telecom infrastructure - data-exposure and resilience gaps. Publicly accessible My.T customer database combined with history of DDoS attacks against Telecom DNS underscores continuing vulnerabilities in critical telecom infrastructure; poses risk to service continuity and misuse of exposed customer data.

- Cross-border banking operations - persistent SWIFT and fraud exposure. Historic loss linked to State Bank of Mauritius India operations via suspected fraudulent SWIFT transactions indicates ongoing sophistication of financial cybercrime targeting cross-border payments.

Highest-Risk Areas

Port Louis (92) drives the majority of recorded risk, driven by street crime, political density, and urban crime concentration in tourist and business districts. Secondary risk clusters in Plaines Wilhems (68), Black River (65), and Flacq (62) reflect broader petty-crime and opportunistic-theft patterns in populated commercial and resort zones. Outlying districts (Rodrigues, Saint Brandon, Agalega) and northern rural areas present minimal risk. Risk is predominantly street-crime and cyber-operational rather than political violence or instability.

How GeoBit Would Assist

Security teams operating in Mauritius would deploy AOI Monitoring & Early Warning on Port Louis, Flic en Flac, and Grand Baie to track crime incident clustering and protest activity in real time; OSINT fusion (social media, local news, Telegram) to monitor post-election political sentiment and civil-unrest signals; and cyber threat intelligence (network & actor analysis, dark-web monitoring) to track active ransomware and financial-crime actors targeting Mauritian banking and telecom infrastructure. Routing & Network Analysis would support alternative journey planning for personnel in high-crime zones.

7-Day Outlook

Political temperature is expected to remain elevated as opposition contestation persists; no major civil unrest is anticipated but public gatherings and traffic disruption around political events remain possible. Cyber-attack volume and sophistication are forecast to remain constant, with hospitality and financial services continuing as primary targets. Street-crime risk in Port Louis and coastal resorts will remain stable and seasonal (high during tourist season).

Highest-Risk Areas - Ranked

#State / RegionRisk1Port Louis922Plaines Wilhems683Black River654Flacq625Grand Port586Moka527Savanne488Pamplemousses459Riviere du Rempart District3810Rodrigues2211Saint Brandon812Agalega5

Sources

- engine.com
- cybergl.com

- youtube.com
- travel.state.gov
- mu.usembassy.gov
- youtube.com
- travel.gc.ca

Download PDF

Email me the PDF

Subscribe to Mauritius daily

See Mauritius live.GeoBit maps Mauritius - every region, event, and risk layer - on demand.Request a live demo

Automated by GeoBit AI from publicly reported events and open-source research. Context only; not a risk advisory. Recognized by Deloitte - NVIDIA Inception - Geospatial World Forum.

REPORTED EVENTS (MOST-CITED)

No high-confidence events in the current window.