CTI-Informed Exposure Assessment
Case study: The Medina of Fez, Morocco

Hybrid Cyber Exposure in Emerging Markets

robpinna.com

Executive Summary

This strategic assessment identifies a "Hybrid Exposure Model" within the Medina of Fes, where informal, trust-based digital networks intersect with legacy internet-facing surveillance infrastructure.

Historic high-density urban environments across the MENA region are often supported by informal digital infrastructure shaped by social trust and family-based cooperation. The sharing of connectivity resources — Wi-Fi passwords, router access, surveillance footage — is normalised, creating a laterally permeable network environment that standard perimeter-based security models fail to address.

Passive OSINT analysis identified 3,890 unique surveillance-related endpoints across Fes, with an estimated 900–1,700 concentrated in the Medina. A ground-level Wi-Fi proximity survey conducted in March 2026 detected 3,210 unique access points across the Medina and adjacent areas.
OSINT metadata indicates continued presence of legacy camera and NVR platforms with well-documented vulnerabilities including authentication bypasses and hardcoded credentials. Exploitation can enable persistent, low-footprint access to surveillance streams and connected networks.

This risk profile aligns with tradecraft of criminal-intelligence hybrids, access brokers, and APT-adjacent groups prioritising persistent access and data monetisation over disruption.
As Morocco attracts international investment, these dynamics introduce non-obvious risks for foreign market entrants. This assessment identifies feasible risk pathways consistent with known tradecraft, without implying confirmed incidents.

Surveillance-related endpoints found by remote OSINT enumeration only. APs found by local passive wardriving.

Key numbers

3,890 total Fes endpoints	≈900–1,700 medina endpoints	3,210 APs
Unique surveillance-related endpoints identified across Fes. Deduplicated by IP + port.	Estimated endpoints plausibly concentrated in the Medina (scenario-based).	Shared local Wi-Fi — 3,210 APs, 69.6% WPS-enabled.

Methodology & Data Sources

Scope: This assessment focuses on civilian surveillance-related infrastructure and associated network exposure. It excludes active probing, authentication attempts, exploitation, credential testing, or interception of any kind.

Data Sources: Passive OSINT enumeration (RTSP exposure, IP camera identification); open demographic and urban density references; secondary OSINT on tourism density and urban structure. Data sourced from public OSINT platforms including Shodan and Censys.

Collection Period: Single observation window (snapshot analysis).

Analytical Approach : Multiple OSINT queries were executed and merged into a single dataset, deduplicated using IP + port as a composite key. Internet-facing assets are treated as a proxy for broader, partially observable exposure.

Limitations: City-level geolocation limits neighbourhood precision; NAT-based shared networks are underrepresented; findings represent structural feasibility, not incident confirmation.

OSINT Findings — Scale & Distribution

Passive OSINT enumeration identified 3,890 unique surveillance-related endpoints across Fes. These include RTSP-exposed streams and internet-reachable IP cameras associated with civilian environments.

Legacy Firmware Indicators (Aggregated OSINT Sample)
While not all observable endpoints expose versioning metadata, a representative subset provided sufficient information to derive firmware age indicators.

Firmware Generation	Observed Count	Share of Sample
2014–2017	51	1.189%
2018–2020	244	5.688%
2021–Present	134	3.124%

These figures do not imply active exploitation. However, they indicate that a non-trivial portion of observable surveillance endpoints operates on older firmware generations, historically associated with unpatched CVEs.

The persistence of older firmware generations should not be interpreted as neglect or lack of technical awareness. In many contexts, extended device lifecycles reflect cost-efficiency, repairability, and the practical realities of resource-constrained micro-business operations.

Local Network Intelligence — Wi-Fi Proximity Survey

A passive Wi-Fi proximity survey was conducted across the Medina of Fes and adjacent areas using WiGLE wardriving methodology (March 3–6, 2026). The survey detected 3,210 unique Wi-Fi access points and provides direct empirical validation of the Hybrid Exposure Model's local layer.

Hardware Composition & Consumer Infrastructure:
OUI-based vendor identification reveals strong concentration of Arcadyan Technology equipment (1,081 networks, 33.7% of total), the manufacturer of the standard ISP-provided routers distributed by Maroc Telecom. This indicates a homogeneous, ISP-managed hardware baseline across the surveyed area.

69.6% of surveyed access points are WPS-enabled — substantially elevating network compromise feasibility across the Medina.

WPS PIN brute-force (Reaver, Bully) is a well-documented, low-skill attack vector available in commodity toolkits.

Network Security Profile

Security Indicator	Count	Share
WPS enabled (all access points)	2,234	696%
Mixed WPA/WPA2 mode (legacy compatibility)	830	259%
Open/unencrypted networks	73	23%
2.4 GHz band only (legacy hardware indicator)	2,313	721%
Wi-Fi 6E / 6 GHz band (modern deployment indicator)	0	0%

Note: Survey data was collected in March 2026 across the Medina of Fes and immediate surroundings. No network names, MAC addresses, or precise geolocation data are retained or reported. Vendor attribution is based solely on OUI prefix analysis.

The WPS figure is the most operationally significant finding. WPS PIN-based authentication remains subject to well-documented brute-force vulnerabilities (Reaver, Bully), and its presence on 69.6% of surveyed access points substantially elevates network compromise feasibility.

Validation of the Hybrid Exposure Model — Local Layer:
These findings directly corroborate the Layer 2 (Local Shared Network) component of the Hybrid Exposure Model. The survey confirms that the wireless infrastructure supporting guest and residential traffic across the Medina is overwhelmingly consumer-grade, WPS-enabled, and operating on legacy 2.4 GHz hardware.

Estimation Model — Medina Focus

Due to geolocation constraints, a scenario-based estimation was applied to infer plausible exposure within the Medina.

Assumptions
— Medina population represents approximately 16–17% of Fes.
— Tourism-facing micro-business density exceeds the city average.
— Surveillance infrastructure density scales with foot traffic and access control needs.

Scenario Range
— Conservative: ≈900 endpoints.
— Realistic: ≈1,200–1,400 endpoints.
— Stress: ≈1,700 endpoints.

Threat Model — Hybrid Exposure

Observed exposure patterns converge toward a repeatable hybrid access condition.

The dominant risk dynamic arises from the interaction of two layers: the Internet-Facing Layer (remote access potential) and the Local Shared Layer (proximity-based access within trust networks). Together, these layers create compounded exposure that is greater than either layer in isolation.

Threat behaviours identified in this assessment are mapped to the MITRE ATT&CK framework to ensure alignment with international technical standards and support downstream defensive operations.

Layer 1 — Internet-Facing (Remote Access)
— Legacy CCTV/NVR (RTSP ports 554, 8000–8999)
— Admin panels (HTTP/HTTPS 80, 443, 8080)
— Cloud relay services (P2P protocols)

Layer 2 — Local Shared Network (Proximity Access)
— Guest Wi-Fi (flat topology, weak/no segmentation — empirically confirmed: 3,210 APs surveyed, 0% enterprise-grade)
— Surveillance infrastructure on same subnet
— POS terminals, smartphones, IoT devices

Key Judgements

Confidence levels: High = strong evidential basis. Medium = structural plausibility.

Judgement	Confidence
Trust-based shared infrastructure is structurally embedded in dense urban environments; proximity survey confirms scale and consumer-grade hardware profile.	**High**
Observable OSINT exposure is a lower bound of total risk surface; ground-level Wi-Fi survey confirms extensive local layer invisible to remote enumeration.	**High**
Concentration of surveillance endpoints in historic cores is plausible under density-adjusted scenarios.	Medium
Hybrid exposure amplifies feasibility of passive exploitation.	**High**
Identity aggregation is feasible without overt intrusion.	Medium
Risk aligns with non-disruptive tradecraft focused on persistence and monetization.	Medium
Long-term abuse is unlikely to be locally detected.	**High**

Threat Actor Profiles

Analytical note: The most relevant risk in this case is not disruptive intrusion, but durable low-noise access supporting observation, identity enrichment, and downstream monetisation.

Actor type	Likely objective	Likely access path	Representative behaviours
Criminal access brokers	Acquire and resell footholds tied to commercially useful environments	RTSP/NVR exposure, weakly segmented guest Wi-Fi, WPS-enabled local access	External remote services, valid accounts, network discovery, access resale
Financially motivated fraud operators	Build high-credibility fraud using contextual identity fragments	Surveillance visibility, business identity reuse, local social engineering	Phishing for information, data aggregation, impersonation, account abuse
Intelligence-adjacent collectors	Maintain low-noise visibility on people, patterns, and places of interest	Persistent observation through exposed cameras and proximity-based shared networks	Video capture, pattern-of-life observation, internal network discovery, low-footprint persistence

Operational Scenarios

Scenario 1 — Identity Harvesting for High-Credibility Fraud
Hybrid access enables aggregation of identity fragments supporting tourism and real-estate fraud.

Scenario 2 — Informal Surveillance and Economic Pressure
Persistent pattern-of-life awareness enables selective coercion or competitive pressure.

Scenario 3 — Contextualised Access Brokerage
Footholds tied to dense civilian clusters are resold to downstream actors.

Risk is likely to increase alongside economic growth, driven by digitalisation of micro-businesses, persistence of legacy infrastructure, and increased value of contextual identity.

Key Risk Indicators & Early Warning Signals

Indicators are selected for observability and trend sensitivity rather than precision attribution.

Key Risk Indicators (KRIs)

— Growth in RTSP-exposed endpoints
— Persistence of legacy surveillance stacks
— Vendor concentration
— Expansion of shared Wi-Fi usage (baseline: 3,210 APs, March 2026)
— Rising tourism-linked identity reuse

Early Warning Signals (EWS)

— Surge in fake tourism listings
— Recycled business identities
— Social engineering with local context
— Increased access resale chatter

Collection Priorities for Defenders

This assessment identifies a structurally plausible exposure model. The next analytical priority is to determine where observed exposure translates into durable access, repeated abuse, or commercially relevant compromise.

Priority collection questions

Are exposed surveillance assets concentrated around tourism-facing and investor-relevant properties?

Do guest Wi-Fi networks and surveillance devices share flat local network topology in representative properties?

Are reused business identifiers, phone numbers, or branding assets appearing across fake listings or impersonation workflows?

Is there evidence of access resale or fraud activity referencing hospitality, property rental, or local business infrastructure?

What defenders should monitor

— Growth or persistence of RTSP/NVR exposure over time
— Repeated reuse of business names, phone numbers, or imagery across tourism listings
— Signs of local-context social engineering targeting visitors, investors, or hosts
— Exposure of default or legacy remote administration interfaces Shared credentials or unmanaged consumer routers in commercial settings

What would increase confidence

— Property-level confirmation of flat network segmentation
— Repeated exposure of the same device clusters across multiple observation windows
— Fraud cases showing overlap with locally observable identity fragments
— Reporting or telemetry indicating resale of footholds tied to hospitality infrastructure

What would reduce confidence

— Widespread adoption of segmented networks across surveyed properties
— Rapid decline in WPS-enabled access points and legacy remote exposure
— Lack of repeatability across future collection windows
— No observable link between exposed infrastructure and fraud-enabling identity misuse

Decision Implications

Hospitality Brands, Tech Investors, Real Estate & Services:
Risk here is primarily inherited, not actively introduced.

For investors and market entrants, the risk is asymmetry rather than instability. Hospitality brands may inherit latent identity and reputational risk; tech investors may face hybrid environments where standard security assumptions do not hold; real estate and services sectors may encounter friction in due diligence processes not yet calibrated to informal digital infrastructure.

Local Residents:
While this assessment is framed to inform investors and decision-makers, it is important to recognise that the long-term impact of unchecked exposure would primarily affect local residents. Privacy, autonomy, and economic agency are at stake in ways that aggregate risk metrics do not fully capture.

These measures address structural exposure without requiring wholesale infrastructure replacement.

Mitigation Considerations

While comprehensive security transformation is beyond the scope of this assessment, basic mitigations exist.

For Micro-Business Operators (Riads, Guesthouses)
— Implement network segmentation: separate VLANs for surveillance, guest Wi-Fi, and management traffic
— Firmware inventory and update cycle for internet-facing devices
— Disable UPnP and unnecessary port forwarding on routers

For Foreign Investors Conducting Due Diligence
— Red flags: shared ISP credentials across properties, absence of device inventory, flat network topology, reliance on consumer-grade equipment for commercial operations
— Assessment scope: Include network architecture review, not just IT/application security

For Technology Vendors Targeting MENA Hospitality
— Design for zero-trust: assume flat networks and shared credentials
— Prefer local processing over cloud relay to reduce attack surface
— Provide simplified segmentation tools (wizard-based VLAN configuration)

Generalisation & Transferability

The Medina of Fes illustrates a repeatable model applicable to high-density urban areas where informal or semi-formal digital infrastructure supports mixed residential, commercial, and transient populations. Similar dynamics are observable in comparable environments across the MENA region and beyond.

Risk Trajectory (12–36 Months)

Risk is likely to increase alongside economic growth, driven by digitalisation of micro-businesses, persistence of legacy infrastructure, and increased value of contextual identity.

> As digital infrastructure mirrors social structure, cyber risk shifts from centralised systems to informal networks — where trust replaces governance and persistence replaces disruption.

Strategic Outlook

As digital infrastructure mirrors social structure, cyber risk shifts from centralised systems to informal networks, where trust replaces governance and persistence replaces disruption. Future CTI must incorporate cultural and sociological frameworks alongside technical indicators to remain analytically valid.

Bottom Line

The Medina of Fes should be treated as a hybrid exposure environment where remotely observable surveillance assets and trust-based local connectivity create feasible low-noise access conditions for financially motivated and intelligence-adjacent actors. Confidence is high on structural exposure, moderate on concentration estimates, and low on attribution absent victim-side telemetry.

Personal takeaway

Effective cyber intelligence in emerging markets requires not only technical insight, but cultural literacy and an understanding of how security, trust, and sovereignty are locally defined. For market entrants, risk literacy must extend beyond firewalls.

Index