NIGERIA COMPUTER SOCIETY | CYBERSECURITY WORKSHOP

Building Cybersecurity Capacity Through Open Threat Intelligence

Harnessing Artificial Intelligence for National Cyber Resilience

Dr. Robinson Tombari Sibe

CEO & Lead Forensic Examiner | Digital Footprints Nig. Ltd.

Fellow, Nigerian Society of Engineers | Professor of Practice (Cybersecurity), MIVA Open University

Cybersecurity Personality of the Year — Nigeria 2025

THE THREAT LANDSCAPE: NIGERIA IN THE CROSSHAIRS

$500M+

Annual cybercrime losses to Nigeria's economy (NCC, 2022)

#3

Africa's most targeted nation for cyberattacks

600%

Rise in ransomware attacks (2020–2024)

70%+

Over 70% of African SMEs lack formal cybersecurity policies" — UNECA, 2023

KEY INSIGHT: Nigeria's financial sector, government infrastructure, and telecommunications networks face coordinated, persistent attacks from state-affiliated APT groups, organised criminal syndicates, and opportunistic threat actors — many leveraging publicly known vulnerabilities and TTPs that **open threat intelligence can expose and neutralise.**

THE THREAT LANDSCAPE: NIGERIA IN THE CROSSHAIRS

Ransomware

Double-extortion campaigns targeting government agencies, hospitals, and service operators — data encrypted and threatened for release.

BEC

High-yield fraud against finance and procurement teams — often the initial access vector for deeper network intrusion.

SCM Attacks

Compromise of trusted vendors to reach upstream targets. SMEs are frequent vectors into larger organisations and government contractors.

State-Sponsored Attacks

Persistent access operations against government networks, telecoms, and energy infrastructure for espionage and disruption.

KEY INSIGHT: SMEs are increasingly targeted as perceived soft entry points into larger supply chains and contractor ecosystems.

// 01 — SETTING THE STAGE

The Capacity Gap

Government Agencies

Siloed incident response — information rarely crosses agency boundaries

Bureaucratic procurement cycles slow adoption of defensive tooling

Limited intelligence sharing culture; threat data held within departments

CERT and SOC capacity under-resourced relative to threat volume

Small and Medium Enterprises

No dedicated security staff — IT generalists absorb all security risk

Minimal budgets preclude commercial threat intelligence subscriptions

Largely unaware that structured CTI is practically accessible at zero cost

Commodity malware exposure not treated as an intelligence problem

> Open CTI addresses both sets of constraints from a single approach — **at zero cost.**

WHAT IS OPEN THREAT INTELLIGENCE?

DEFINITION

Open Threat Intelligence (OTI) is the collection, analysis, and sharing of cybersecurity threat data from publicly available and community-shared sources — enabling organisations to anticipate, detect, and respond to cyber threats proactively.

- **Indicators of Compromise (IOCs) —**
  IPs, domains, file hashes, URLs
- **Tactics, Techniques & Procedures (TTPs) —**
  MITRE ATT&CK framework mappings
- **Vulnerability Intelligence —**
  CVE feeds, exploit databases, PoCs
- **Threat Actor Profiles —**
  APT groups, attribution, campaigns

THE INTELLIGENCE LIFECYCLE

1. **DIRECTION**
   Define what intelligence is needed and why
2. **COLLECTION**
   Gather data from OTI feeds, ISACs, OSINT
3. **PROCESSING**
   Normalise, deduplicate, enrich data
4. **ANALYSIS**
   Identify patterns, TTP mapping, attribution
5. **DISSEMINATION**
   Share with stakeholders in actionable formats
6. **FEEDBACK**
   Refine collection based on outcomes

WHAT IS OPEN THREAT INTELLIGENCE?

Strategic	Long-term threat trends and adversary intent; input for senior leadership and policy decisions	Nation-state capability assessment · Annual threat landscape report for government leadership
Operational	Intelligence about specific active campaigns and threat actors currently in motion	Active phishing wave targeting federal MDAs · Identified threat actor TTPs & infrastructure
Tactical	Attack patterns and adversary techniques mapped to MITRE ATT&CK	Spear-phishing via ISO attachments · Living-off-the-land execution chains
Technical	Machine-readable indicators of compromise for direct integration into security tooling	Malicious IPs, hashes, domains · YARA rules · Suricata signatures

// 02 — UNDERSTANDING OPEN THREAT INTELLIGENCE

Open vs. Proprietary Intelligence

Open ≠ Low Quality

Proprietary / Commercial

- Curated vendor feeds with commercial SLA: Recorded Future, CrowdStrike TI, Mandiant
- High fidelity, enriched context, dedicated research teams
- Annual cost: typically $50,000 – $500,000+
- Access barrier: prohibitive for most public-sector units and virtually all SMEs

Open / Community

- MISP communities, Abuse.ch, Shadowserver Foundation, AlienVault OTX, Spamhaus
- Comparable operational value, community-validated, continuously updated
- Cost: zero. Accessible with any internet connection and basic technical literacy
- Integration-ready via STIX/TAXII and REST APIs. They plug into existing tooling

> For resource-constrained government units and SMEs, open CTI **is the realistic option.**

// 02 — UNDERSTANDING OPEN THREAT INTELLIGENCE

Public and Community-Driven Intelligence Feeds

Community-Driven

- MISP Communities
- AlienVault OTX
- Abuse.ch / URLhaus
- MalwareBazaar
- ThreatFox
- FeodoTracker
- Spamhaus Project

Public-Interest & Non-Profit

- Shadowserver Foundation
- Daily: scanning, sinkholes, botnet victim alerts
- Free to national CERTs
- ngCERT partnership eligible
- Direct SME IP-range access

Government & Intergovernmental

- CISA AIS
- ENISA Threat Landscape
- FIRST.org / national CERTs
- Interpol cybercrime initiatives
- AU Cybersecurity Expert Group

Passive DNS & Scanning

- Shodan
- Censys
- CIRCL Passive DNS
- Know your exposure before attackers do

KEY OTI PLATFORMS & COMMUNITY SOURCES

FREE & OPEN SOURCE

MISP

Malware Information Sharing Platform

EU-backed open-source threat sharing. Used by 6,000+ organisations globally. Automates IOC exchange via structured formats (STIX/TAXII).

FREE COMMUNITY

AlienVault OTX

Open Threat Exchange

One of world's largest open threat intel community — reportedly 200,000+ participants. "Pulses" deliver real-time IOC collections with MITRE ATT&CK mappings.

FREE / PREMIUM

VirusTotal

Google's Threat Analysis Platform

Scans files, URLs, IPs against 70+ antivirus engines. The gold standard for rapid malware triage. Free tier available for analysts.

FREE & OPEN

MITRE ATT&CK

Adversarial Tactics, Techniques & Common Knowledge

Globally-accessible knowledge base of adversary behaviour. Maps attack patterns to defensive controls. Foundation of modern threat modelling.

FREE / PREMIUM

Shodan

Internet-Connected Device Intelligence

Search engine for internet-facing devices. Reveals exposed Nigerian infrastructure — ICS, cameras, routers — before attackers do.

FREE

CIRCL CVE Search

Vulnerability & CVE Intelligence

Real-time access to National Vulnerability Database (NVD) and CVE feeds. Enables proactive patch prioritisation for Nigerian organisations.

STIX/TAXII: The universal language of threat intelligence sharing — Structured Threat Information Expression (STIX) + Trusted Automated eXchange (TAXII) protocol.

Sinkholes »

Scans »

Honeypots »

DDoS »

ICS/OT »

Web CVEs »

Compromised devices »

Post-exploitation frameworks/C2 »

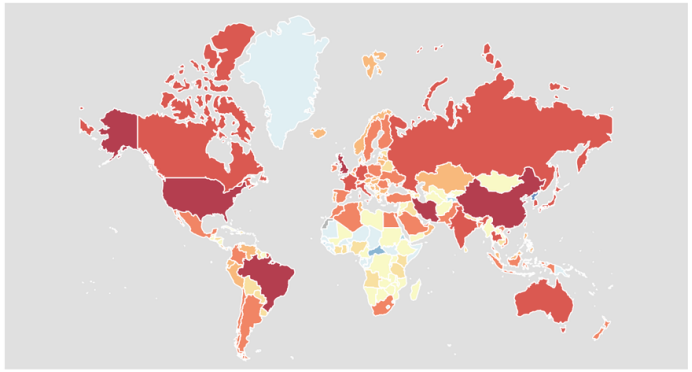
About this data

Shadowserver scans the entire IPv4 Internet for over 100 different network protocols every day, and also performs IPv6 scans based on IPv6 hitlists for selected protocols. These are “hello” type port scans that do not exploit any vulnerability. They enable identification of misconfigured, vulnerable or abusable devices, unnecessarily exposed attack surfaces, or simply just population enumeration. Population enumeration results can be found under the “population” source type.

Trending queries | **Attention! cPanel/WHM CVE-2026-41940 attacks ongoing - at least 44K instances compromised »** More details

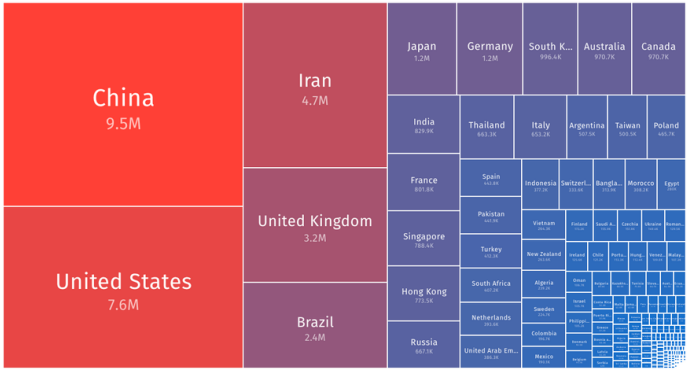
Unique IP addresses per country

2026-06-14



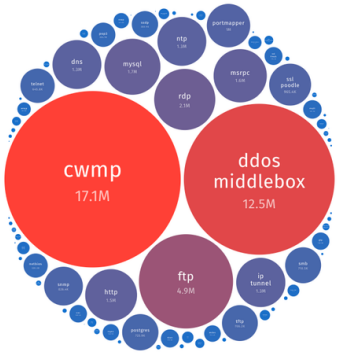
Unique IP addresses per country

2026-06-14



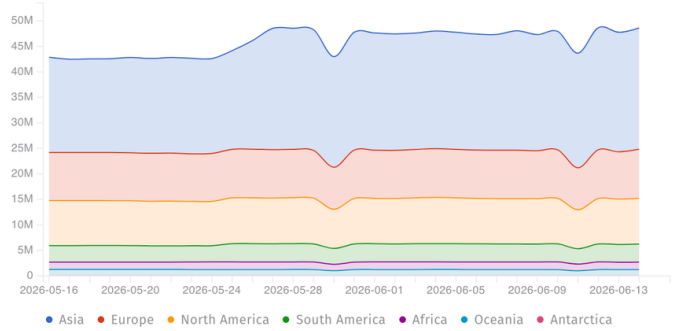
Unique IP addresses per tag

2026-06-14



Unique IP addresses over time

2026-05-16 to 2026-06-14



// 02 — INTEROPERABILITY STANDARDS

STIX / TAXII

STIX — Structured Threat Information eXpression

A machine-readable format for expressing CTI objects and their relationships

TAXII — Trusted Automated eXchange of Indicator Information

The transport protocol for sharing STIX content between organisations and platforms. no manual translation required.

Intelligence consumed from one tool feeds directly into another without conversion

// STIX 2.1 OBJECT RELATIONSHIPS

Threat Actor	— uses →	Malware
Malware	— targets →	Victim
Malware	— uses →	Infrastructure
Indicator	— indicates →	Malware
Campaign	— attributed-to →	Threat Actor
Campaign	— uses →	Attack Pattern

AI + OTI: AMPLIFYING INTELLIGENCE AT SCALE

AI ENGINE

Automated IOC Correlation
Cross-reference millions of indicators in seconds

Predictive Threat Scoring
Prioritise which vulnerabilities will be exploited next

Anomaly Detection
ML models flag deviations from baseline behaviour

Automated Playbook Triggers
SOAR integration auto-blocks IOCs in real-time

Threat Actor Attribution
NLP & graph analysis links campaigns to known APTs

Dark Web Monitoring
AI scrapes underground forums for Nigeria-specific threats

IBM Security (2023): AI-augmented threat intel reduces mean-time-to-detect (MTTD) from **197 days to under 30 days** — a 85% improvement in detection speed.

// 03 — BUILDING CAPACITY THROUGH OPEN CTI

The Intelligence Cycle: Government Applications

1. **Direction**
   Define intelligence requirements and gaps from leadership priorities
2. **Collection**
   Ingest open feeds, sensor data, Shadowserver reports, partner intelligence
3. **Processing**
   Normalise, deduplicate, and enrich indicators with context in MISP
4. **Analysis**
   Contextualise, attribute, assess confidence level and operational impact
5. **Dissemination**
   Share finished intelligence with decision-makers and ngCERT constituents
6. **Feedback**
   Refine collection requirements based on decisions and observed outcomes

// Scenario — Ransomware Targeting Public Sector

MITRE ATT&CK IN ACTION: A NIGERIAN USE CASE

SCENARIO: APT Group Targets a Nigerian Commercial Bank — Using OTI + ATT&CK to Detect & Respond

ATTACK PHASE	ADVERSARY TACTIC	OTI-DERIVED INTEL	DEFENSIVE ACTION
INITIAL ACCESS	ADVERSARY TTP: Spear-phishing via BEC email	OTI SOURCE: OTX Pulse: TA505 campaign IOCs	DEFENSIVE ACTION: Block sender domain, alert HR
EXECUTION	ADVERSARY TTP: Office document lure exploiting CVE-2022-30190 (MSDT/Follina) (CVE-2022-30190)	OTI SOURCE: NVD feed: CVE patched, PoC circulating	DEFENSIVE ACTION: Force-patch Office fleet, disable macros
LATERAL MOVEMENT	ADVERSARY TTP: Pass-the-Hash via compromised AD	OTI SOURCE: MISP: similar TTP from recent EMEA incident	DEFENSIVE ACTION: Enforce Credential Guard; enforce least-privilege AD segmentation
EXFILTRATION	ADVERSARY TTP: Data staging to Dropbox C2 channel	OTI SOURCE: Shodan/AlienVault: C2 IP flagged 3 days prior	DEFENSIVE ACTION: Block egress to flagged IP, forensic imaging

// 03 — BUILDING CAPACITY THROUGH OPEN CTI

The Intelligence Cycle: SME Applications

1

Subscribe

Register for open feeds relevant to your sector and internet-facing infrastructure. Email delivery requires no technical configuration.

2

Integrate

Push indicators into firewalls, endpoint tools, and email filters. Abuse.ch and Spamhaus integrate directly into common open-source tooling.

3

Report

Share observations with ngCERT and sector peers. Your data improves collective defence for the entire ecosystem.

Capacity-building does not require a dedicated threat intelligence team. It requires **the right habits and the right tools.**

// 03 — BUILDING CAPACITY THROUGH OPEN CTI

Deploying an Open CTI Platform

Full Deployment — SOC / CERT

Deploy MISP or OpenCTI on-premises or cloud infrastructure

Integrate with Wazuh / ELK Stack SIEM for correlated alerting

Ingest Shadowserver daily reports, Abuse.ch feeds, and OTX pulses automatically via TAXII

Role-based access controls, sharing groups, and SLA-backed response workflows

```
// Minimum Infrastructure
```

4–8 vCPU · 16 GB RAM · 500 GB storage · Stable outbound for feed ingestion

Lightweight Entry — SMEs

Browser-accessible OTX and MISP dashboards — no local installation required

Email-based feed subscriptions from Shadowserver and Spamhaus

Direct integration into pfSense, Suricata, or CrowdSec

Simple daily hygiene: check, block, and log — no analyst required

```
// Entry Point — Start Here
```

Shadowserver free network reports + Abuse.ch FeodoTracker. Both deliver immediate value with no technical configuration.

// 03 — BUILDING CAPACITY THROUGH OPEN CTI

Threat Intelligence Sharing Frameworks and Policy

National

ngCERT — national coordination hub under ONSA; the primary point of contact for threat sharing

Nigeria National Cybersecurity Policy and Strategy 2021

Sector ISACs for fintech, telecoms, and oil and gas services supply chains

Regional

African Union Cybersecurity Expert Group — continental policy coordination

ECOWAS regional cyber coordination frameworks for West African member states

Shadowserver partnerships with African national CERTs — daily free reports

Cross-border notification protocols for shared infrastructure incidents

International & SME Participation

FIRST.org — global CERT network, incident coordination, and training resources

Interpol cybercrime intelligence cooperation and notices

SMEs as ISAC participants: both consumers and active contributors of threat data

Evidence Act 2011 — provenance standards for open-source intelligence

// 03 — BUILDING CAPACITY THROUGH OPEN CTI

CTI in Investigations and Legal Proceedings

Law Enforcement and Regulatory

- CTI products as evidence: digital artefacts require documented chain-of-custody from acquisition to court
- Provenance must be established for all open-source intelligence before it enters an evidentiary record — source, acquisition method, timestamp, and analyst notes
- Admissibility standards under the Evidence Act 2011
- Prosecution pathway under Cybercrimes Act 2015 as amended 2024

SME Obligations and Protections

- Understand reporting obligations following a confirmed incident — timelines and relevant regulatory contacts vary by sector
- An internal CTI log documents the full IOC lifecycle: source, date added, action taken, and outcome
- Contemporaneous records strengthen legal position and support subsequent law enforcement investigations
- Proactive intelligence sharing with ngCERT may constitute a mitigating factor in regulatory proceedings

// 04 — THE ROAD AHEAD

Policy Recommendations

Regulators & Government Leadership

- Mandate threat intelligence sharing between MDAs via ngCERT as coordination hub
- Formalise a Shadowserver partnership at national CERT level — free, immediately available, high value
- Establish sector-specific ISACs for critical infrastructure: energy, finance, and telecoms
- Allocate dedicated budget lines for open CTI infrastructure within agency security programmes

Regulators with SME Oversight

- Create incentive structures and formal recognition for voluntary incident reporting
- Establish safe harbour provisions that encourage threat data sharing without punitive consequences
- Recognise open CTI programme participation within compliance and licensing frameworks
- Fund sector-level ISAC development in fintech, telecoms, and oil and gas services

SMEs — Starting Today

- Subscribe to Shadowserver network reports for your IP space
- Integrate at least 2 open/free TI feeds into your firewall
- Treat intelligence sharing as collective defence, not a competitive or reputational risk

BUILDING OTI CAPACITY IN NIGERIA: A STRATEGIC ROADMAP

01

TECHNICAL INFRASTRUCTURE

- Deploy MISP instance as national/sectoral threat sharing hub
- Integrate free OTI feeds: OTX, Abuse.ch, Feodo Tracker, URLhaus
- Implement SIEM (e.g. Wazuh — open source) with OTI feed ingestion
- Configure automated STIX/TAXII feed subscriptions
- Establish threat hunting capability using Sigma rules

02

HUMAN CAPITAL & SKILLS

- Train analysts in CTI frameworks: MITRE ATT&CK, Diamond Model
- Certify practitioners: GCTI, CTIA, OpenCTI Analyst credentials
- Embed CTI modules in university cybersecurity curricula
- Establish mentorship pipelines via NCS, ISACA Nigeria, ISC2 Nigeria
- Build specialised SOC analyst cadre with OTI competencies

03

POLICY & COLLABORATION

- Mandate OTI sharing in NITDA & CBN cybersecurity frameworks
- Establish sector-specific ISACs: FinTech, Energy, Telecoms, Gov
- Formalise data-sharing MOUs between CERTs, NCC, DSS, NPF
- Join FIRST (Forum of Incident Response & Security Teams)
- Contribute to INTERPOL's Africa Cybercrime Operations (AFRIPOL)

PRACTICAL IMPLEMENTATION: YOUR 90-DAY OTI QUICKSTART

DAYS 1–30
FOUNDATIONS

- Register on AlienVault OTX — subscribe to Nigeria-relevant pulses
- Create accounts on VirusTotal, MITRE ATT&CK Navigator
- Map your crown-jewel assets and define intelligence requirements
- Conduct Shodan scan on your organisation's external attack surface
- Identify 2 internal threat intel champions for upskilling

DAYS 31–60
INTEGRATION

- Deploy Wazuh SIEM (open source) and ingest your first OTI feed
- Configure automated alerts for IOCs from Abuse.ch & Feodo Tracker
- Run first tabletop exercise using an ATT&CK-mapped scenario
- Establish threat sharing relationship with a peer organisation
- Enrol analysts in MITRE ATT&CK Defender (MAD) training

DAYS 61–90
OPERATIONALISATION

- Stand up a basic MISP instance for internal IOC management
- Produce your first Weekly Threat Intelligence Digest for leadership
- Formally join a sector peer-sharing group (banking, telecoms, etc.)
- Develop your first 5 ATT&CK-based detection use cases in SIEM
- Brief board/executive team on OTI ROI and programme KPIs

THE BUSINESS CASE FOR OTI: COST VS. VALUE

WHAT OTI COSTS

MISP (open source deployment) Server hosting: ~₦50,000/month	₦0
AlienVault OTX community tier Full community feed access	₦0
Wazuh SIEM (open source) Optional cloud: ~₦80,000/month	₦0
Abuse.ch / Feodo / URLhaus feeds Hourly updated C2/malware feeds	₦0
MITRE ATT&CK Navigator Hosted free by MITRE	₦0
CTI Analyst Training (entry level) One-time per analyst	~₦250,000
Annual OTI Programme (SME) Staffing + infrastructure	~₦2–5M

WHAT A BREACH COSTS

Average cost of a data breach globally (IBM 2024)	$4.88M
Average cost in Africa (rising trend, IBM Security)	$2.78M
Average CBN enforcement fine (data breach)	₦150M–500M
Reputational damage multiplier	3–5× cost
Business downtime (avg. ransomware)	22 days
Customer trust recovery timeline	18–36 months

OTI ROI: A ₦5M annual OTI programme that prevents one breach saves an estimated **~~₦500M~~–₦2B in breach response, fines, and reputational costs.** That is a 100× return on investment.

CHALLENGES — AND HOW NIGERIA OVERCOMES THEM

Analyst Skills Gap	Shortage of trained CTI practitioners across Nigerian organisations	NCS-led CTI certification pathway; university curriculum integration; mentorship programmes through professional bodies
Intelligence Overload	Raw OTI feeds generate thousands of IOCs daily — signal vs. noise problem	Deploy AI-based threat scoring (MISP's built-in taxonomies + ML filtering); context-specific feed curation aligned to sector
Trust Deficit in Sharing	Organisations reluctant to share threat data — reputational and competitive concerns	Enforce TLP protocols; enable anonymised sharing via NG-ISAC; legislate safe-harbour provisions for good-faith sharing
Regulatory Fragmentation	Disparate cybersecurity mandates across CBN, NCC, NITDA, NDPC, DSS	National Cybersecurity Policy 2021 as unifying framework; ONSA coordination mandate; sector ISAC MOUs with regulatory backing
Infrastructure Limitations	Inconsistent bandwidth, power reliability, and cloud access in some regions	On-premise MISP deployment; offline IOC feed caching; lightweight agents (Wazuh is resource-efficient); mobile-first dissemination

A CALL TO COLLECTIVE ACTION

GOVERNMENT

- Enact safe-harbour legislation for good-faith threat sharing
- Fund a National Threat Intelligence Centre under ONSA
- Mandate OTI programme reporting in NCC & CBN frameworks

PRIVATE SECTOR

- Allocate dedicated CTI budget — a minimum of 10% of cybersecurity spend
- Participate in sector ISACs and contribute IOCs bi-weekly
- Require OTI programme evidence in third-party vendor assessments

ACADEMIA & NCS

- Integrate CTI methodology into all cybersecurity degree programmes
- Launch NCS-accredited Open Threat Intelligence Certification
- Publish Nigeria-specific threat research to enrich global OTI ecosystems

"Intelligence shared is an attack prevented. Intelligence hoarded is a breach waiting to happen."

KEY TAKEAWAYS

1. Open Threat Intelligence is not optional — it is the foundation of proactive cyber defence in 2026 and beyond.
2. The tools are free. MISP, OTX, Wazuh, ATT&CK Navigator. The barrier is not cost — it is will and skills.
3. AI amplifies OTI — reducing detection time from months to days and enabling predictive defence at scale.
4. Sharing intelligence is a force multiplier. Nigeria's cybersecurity is only as strong as its weakest link — and that link is currently isolation.
5. Start today: register on AlienVault OTX, scan your perimeter on Shodan, and map your assets to the ATT&CK framework.

Questions & Discussion | Dr. R.T. Sibe | Digital Footprints Nig. Ltd.