Whitehat.NG
2023 Annual Report

Nigeria Cyberspace ISAC + PEOPLE CERT

Whitehat.NG 2023 Annual Report

cert@projectwhitehat.ng

Report Outline

whitehat.ng

Introduction

Whitehat.NG

whitehat.ng

Introduction

Whitehat.NG is a comprehensive community project with a primary focus on enhancing cybersecurity in Nigeria. Through its multifaceted approach, the project aims to address various aspects of cybersecurity. It offers a responsible disclosure program to discover and report security vulnerabilities in Nigerian digital applications and systems, contributing to the overall security of the country's digital infrastructure.

Additionally, Whitehat.NG provides a repository of events and reports, enabling stakeholders to stay updated on the latest cybersecurity incidents in Nigeria. This feature allows for in-depth analysis and understanding of cybersecurity trends and patterns within the country.

Furthermore, the project actively encourages collaboration with private and public organizations on cybersecurity initiatives and projects, fostering innovation and effective strategies to secure Nigeria's cyberspace. Lastly, Whitehat.NG offers access to webinars, and podcasts covering various cybersecurity topics and skills, empowering individuals with the knowledge and expertise needed to contribute to the improvement of cybersecurity in Nigeria.

Introduction

By reporting and disclosing these security vulnerabilities, the project will contribute to the safety of cyberspace in Nigeria by fostering a culture of responsible disclosure and proactive vulnerability management. This approach aligns with the project's focus on "**Report and Fix**," as it encourages the discovery and reporting of security vulnerabilities in Nigerian digital applications and systems. By doing so, organizations can promptly address these vulnerabilities, leading to improved cybersecurity posture and reduced risk of exploitation.

Furthermore, the project's emphasis on "**Track and Analyze**" will benefit from these reports, as they will serve as valuable additions to the repository of cybersecurity incidents in Nigeria.

This repository will provide insights into emerging threats and trends, enabling stakeholders to stay updated on the latest cybersecurity incidents and take proactive measures to protect digital assets.

In line with "**Collaborate and Innovate**," the responsible disclosure of these vulnerabilities will facilitate partnerships with private and public organizations on cybersecurity initiatives. By working together to address these vulnerabilities, stakeholders can collaboratively innovate and develop best practices for securing Nigeria's cyberspace.

Lastly, by sharing information about these vulnerabilities and their impact, the project can contribute to "**Learn and Grow**" by providing real-world case studies for educational resources.

Responsible Disclosure

Whitehat.NG

whitehat.ng

Rsponsible Disclosure

Multiple critical vulnerabilities have been discovered across various systems, exposing sensitive data and posing severe risks to the privacy, security, and integrity of organizations and individuals. These vulnerabilities include exposed credentials, API calls revealing PII, IDOR vulnerabilities, and proxy-chain attacks targeting Microsoft Exchange/OWA. The potential consequences encompass financial loss, reputational damage, regulatory non-compliance, and the compromise of millions of citizens' data.

Reporting these findings and notifying the affected parties is crucial to ensure transparency, prompt mitigation, and compliance with legal and ethical responsibilities.

By promptly informing the relevant stakeholders, including the organization's leadership, IT security teams, and affected individuals, proactive measures can be taken to address the vulnerabilities, mitigate potential damages, and prevent further exploitation.

Additionally, timely disclosure fosters trust and accountability, demonstrating the organization's commitment to addressing security concerns and protecting the interests of its stakeholders. This approach aligns with best practices in cybersecurity incident response and serves to uphold the organization's reputation and integrity in the face of these critical vulnerabilities.

Responsible Disclosure

Throughout the year, responsible disclosure efforts have resulted in the identification and reporting of security vulnerabilities across various sectors. These include 10 disclosures within the banking and finance sector, 9 within government entities, 7 within the education sector, 3 within both the information technology, 6 within telecommunication sectors, and 1 each within the construction industry, new media sector, and transportation (airline).

This comprehensive approach to responsible disclosure underscores the commitment to enhancing cybersecurity across diverse industries.

By engaging with stakeholders in these sectors, proactive steps have been taken to address vulnerabilities, mitigate potential risks, and contribute to the overall security of digital systems and data.

The collaborative nature of these disclosures reflects a concerted effort to promote transparency, accountability, and continuous improvement in cybersecurity practices across multiple sectors.

By the Numbers

10
BANKING & FINANCE

9
GOVERNMENT

7
EDUCATION

6
TELECOMMUNICATION

3
INFORMATION TECH.

1
NEW MEDIA

1
CONSTRUCTION

1
TRANSPORTATION

The vast majority of disclosure activities are centered on identifying and addressing vulnerabilities that ultimately lead to unauthorized access to Personally Identifiable Information (PII)

Note **–** Addressing ongoing findings, some affected parties have been unresponsive.

Nigeria's Cyberspace
ISAC + PEOPLE CERT

1

Uncovering valid Personally Identifiable Information (PII) of employees, gaining complete access to the company's payroll, attendance, and inventory through the misconfigured Enterprise Resource Planning (ERP) system.

This poses a critical risk to the company's operations, privacy, and security.

Industry - Construction

2

Valid Personally Identifiable Information (PII) of users, including Bank Verification Numbers (BVN) and other identifiers such as NIN data and voter cards, found in old servers used to store scanned copies of customer registration forms and other documents.

This presents a severe risk to the security and privacy of the individuals affected and the company's compliance with data protection regulations.

Industry - Banking and Finance

3

Valid Personally Identifiable Information (PII) of users has been identified in the test environment of an application under development. Additionally, credentials to access dashboards and other sensitive areas have also been compromised.

This poses critical risk to the security and confidentiality of user data, and integrity of app

Industry - Information Technology

Nigeria's Cyberspace
ISAC + PEOPLE CERT

4

A directory traversal vulnerability was discovered, leading to the leakage of source codes to e-portals designed for staff, students, and other users. This resulted in the exposure of Personally Identifiable Information (PII) and other application access credentials.

This represents a critical risk to the security and confidentiality of sensitive data

Industry - Education

5

Data belonging to over 1,000 enrollees was exposed, along with the discovery of admin credentials. Additionally, the website has been compromised with a cross-site scripting (XSS) vulnerability.

This presents a severe risk to the privacy and security of the affected individuals, as well as the integrity of the system and its data.

Industry - Education

6

Credentials have been inadvertently exposed within the application settings and configuration files on GitHub, potentially compromising sensitive access information.

This poses a severe risk to the security and integrity of the application, as well as the confidentiality of any data accessible through these credentials.

Industry - Banking and Finance

Nigeria's Cyberspace
ISAC + PEOPLE CERT

7

Live data used for analysis by a third-party analytic team has led to the exposure of transaction details and users' Personally Identifiable Information (PII) such as Bank Verification Numbers (BVN) and phone numbers.

This presents a critical risk to the privacy and security of the individuals affected, as well as potential regulatory non-compliance.

Industry - Banking and Finance

8

The discovery of admin and super-admin credentials in a configuration file has resulted in the exposure of state Bureau of Public Procurement (BPP) data belonging to a state government.

This poses a critical risk to the security and confidentiality of sensitive government data

Industry - Government

9

Credentials have been inadvertently exposed within the application settings and configuration files on GitHub, allowing unauthorized access to the mail system of a state Ministry of Education.

This presents a severe risk to the security and confidentiality of the ministry's communication and potentially compromises sensitive information.

Industry - Government

Nigeria's Cyberspace
ISAC + PEOPLE CERT

10

The API server has been exposed, and the configuration allows for potential unauthorized access, enabling the enumeration and potential exploitation of the API.

This poses a critical risk to the security and integrity of the API, potentially leading to unauthorized access and misuse of sensitive data or system resources.

Industry - Banking and Finance

11

Credentials granting access to the technical ERP notification email inbox have been inadvertently exposed.

This poses a moderate risk to the security and integrity of the ERP notification system.

Industry - Banking and Finance

12

Credentials granting access to the admin email account have been found exposed, and the email is currently being exploited as a test bed for phishing activities.

This presents a severe risk to the security and integrity of the email system, as well as the potential impersonation of the affected entity domain used in phishing activities.

Industry - Information Technology

Nigeria's Cyberspace
ISAC + PEOPLE CERT

13

A development environment designed for BVN validation has been identified, with an account created and tested for validation purposes, resulting in the confirmation of the return of users' Personally Identifiable Information (PII).

This poses a critical risk to the privacy and security of individuals, as well as the potential for regulatory non-compliance and legal implications.

Industry - Information Technology

14

Credentials granting access to the blogs and backend of the platform have been discovered, potentially exposing the platform to vandalism and the posting of potentially inciting content.

This presents a severe risk to the integrity and reputation of the platform, as well as potential legal and regulatory repercussions

Industry - New Media

15

The backend credentials for the e-portal were exposed in the source code, leading to the discovery of this flaw. The exposed credentials have put sensitive student and staff data at risk, with the timeframe indicating that this data may have fallen into the hands of threat actors.

This presents a critical risk to the privacy and security of the students and staff, as well as potential legal and regulatory implications.

Industry - Education

Nigeria's Cyberspace
ISAC + PEOPLE CERT

16

The credentials for a technical support email were found exposed, and the inbox was discovered to be used as a testbed for sharing phishing emails.

This poses a severe risk to the security and integrity of the email system. Additionally, it could damage the trust and reputation of the organization

Industry - Government

17

Due to misconfigurations, access to the main website backend has been left vulnerable, providing administrative privileges that could potentially allow the overwrite of all web content.

This presents a critical risk to the integrity and security of the website, as unauthorized access and content.

Industry - Telecommunication

18

An exposed API identified on the CRP platform, which, upon providing a simple digit as input, can potentially reveal the PII of millions of citizens. Additionally, other critical vuln were discovered on the portal, potentially leading to the leakage of activity data of registered users, possibly due to IDOR.

This poses a critical risk to the privacy and security of millions of citizens, as well as the potential for severe legal and regulatory implications

Industry - Government

Nigeria's Cyberspace
ISAC + PEOPLE CERT

19

A critical Insecure Direct Object References (IDOR) vulnerability has been identified, allowing unauthorized access to user-linked National Identification Number (NIN) information.

This poses a severe risk to the privacy and security of users, as well as potential legal and regulatory implications.

Industry - Telecommunication

20

A new product in development has led to the exposure of source codes and Personally Identifiable Information (PII) of over 3,000 users, including sensitive financial data.

This presents a critical risk to the privacy and security of the affected users, as well as the potential for financial fraud and regulatory non-compliance

Industry - Banking and Finance

21

A new platform in development has resulted in the exposure of sensitive business information, including financial, HR, and other critical data.

This poses a critical risk to the confidentiality and integrity of the organization's operations, potentially leading to financial loss, reputational damage, and legal implications.

Industry - Telecommunication

22

The Microsoft Exchange/OWA system has been targeted by proxy-chain attacks exploiting vulnerabilities such as ProxyShell, ProxyLogon, and ProxyOracle, resulting in the reporting of over 13 Outlook Web Access (OWA) vulnerable instances to ngCERT and the community.

This presents a critical risk to the security and confidentiality of the affected systems, potentially leading to unauthorized access, data breaches, and further exploitation of the compromised infrastructure

Industry - Government & Private

Nigeria's Cyberspace
ISAC + PEOPLE CERT

whitehat.ng

Disclose a vulnerability today !

You can use the QR code below to disclose a vulnerability today. The second QR code also contains What You Should Know - Researchers and Organizations on Responsible Disclosure

Disclose Vulnerability (ies)

What you should know

Some of the findings are still being addressed, and there has been limited responsiveness from certain affected parties. We strongly encourage the organization to utilize our Vulnerability Disclosure Policy (VPD) template as a comprehensive guide for establishing a structured process that enables researchers to effectively communicate their findings. This will facilitate a smoother and more efficient engagement between the organization and external researchers, ensuring that vulnerabilities are addressed in a timely and coordinated manner.

Cybersecurity Incidents Tracking

Whitehat.NG

whitehat.ng

Cyber Incidents Tracking

Throughout the year 2023, various **major** cyber incidents were tracked, with the most prevalent being ransomware, accounting for 53.8% of the incidents. These incidents were attributed to various ransomware groups, including Black Cat (ALPHV), Mallox, Meow, Elbei, and OXXX, which topped the list of reported incidents. Other notable incidents include defacement, breach, and stolen funds, and Ponzi scheme crashes, each accounting for 15.4% of the total incidents. Phishing/data collection, insider threat & stolen funds, controversial disclosure, DDoS, and info & credential stealer campaign each accounted for 7.7% of the tracked cyber incidents. It's evident that ransomware posed a significant threat, while a variety of other cyber incidents also made an impact throughout the year.

We acknowledge that there may be more incidents in these categories that have not been reported for various reasons. We urge the stakeholders to maintain the practice of reporting to enable access to more quality data that can assist in making informed decisions to tackle national cybersecurity challenges.

By the Numbers

7
RANSOMWARE

2
DEFACEMENT

2
PONZI SCHEME CRASHES OFF

2
BREACH & STOLEN FUND

2
PHISHING / DATA COLLECTION

1
DDOS

1
INSIDER THREAT

1
INFO STEALER MALWARE CAMPAIGN

It's evident that ransomware posed a significant threat, while a variety of other cyber incidents also made an impact throughout the year.

January 2023

Phishing / Data Collection

A malicious actor created a fake portal for the 2023 General Election in Nigeria, using a domain with a spelling error (Recriutment) and phishing for users' personal information. The same domain has been hosting similar fake platforms since 2022, targeting users in Nigeria, Ghana, and Kenya with fake youth empowerment, jobs, visa sponsorship, and grants from presidential aspirants. The malicious actor uses a URL shortener (Lyupz) to hide the main domain and distributes the links through WhatsApp Groups, relying on unsuspecting users to share them with others

https://blog.cyberplural.com/beyond-fake-inec-portal-threat-actor-targeting-users-in-3-african-countries/

January 2023

Ransomware

A Federal agency experienced a ransomware incident on one of its internet-facing servers where all files in the shared folder got encrypted. The ransom note read the files have been encrypted by **OXXX Virus** and victims can buy decryption for $ 300 USD in bitcoin by sending the unique ID to sergev_petrov1983@mail.ru

March 2023

Breach and Stolen Fund

Hackers transferred over ₦2.9 billion from Flutterwave accounts in early February 2023. Flutterwave reported the case to the police and filed a suit to freeze accounts in 27 financial institutions in Nigeria where some of the money was moved. Flutterwave denied the hack and claimed that no user lost any funds. It also said it invests heavily in security measures such as audits, certifications, and licenses. Some Twitter users confirmed that their accounts were frozen or locked as a result of the hack. Some also questioned Flutterwave's security and transparency

March 2023

Defacement

Babcock University's Information Management System (UIMS) Account was hacked and the website was defaced with pornographic content

https://techcabal.com/2023/03/10/hundreds-of-accounts-frozen-during-flutterwave-hack-allegation/

https://www.premiumtimesng.com/news/top-news/589716-management-apologises-as-hackers-upload-porn-videos-on-babcock-university-website.html

April 2023

Ransomware

The Leadway Assurance hack was an attempted cyberattack on the Leadway Assurance Company Ltd., a leading Nigerian insurance company, in April 2023. The attack was allegedly carried out by the **ALPHV** ransomware group, a cybercriminal gang that encrypts and steals data from its victims. Sample data released to the dark web

https://twitter.com/FalconFeedsio/status/1647449976207818753?s=20

https://independent.ng/how-i-hacked-stole-billions-from-afriq-arbitrage-system-staff-abayomi-segun-confesses-video/

https://punchng.com/leadway-stops-hackers-attempts-to-breach-network/

May 2023

Insider Threat & Stolen Funds

The hackers of Afriq Arbitrage System (AAS), a global crypto space, were led by one of its staffers, Abayomi Segun Oluwasesan, who betrayed his boss, Jesam Micheal, while he was undergoing a liver transplant. Abayomi and his cohorts hacked the platform and withdrew several millions of dollars from over 100,000 investors from over 75 countries. They spent the money on exotic cars, properties, citizenships, and travel. The hacking incident crashed the platform and left many investors in suicidal, traumatic, and helpless situations. Some of them lost their retirement savings, family members, and lifelines. They demand justice for Abayomi's crimes.

May 2023

Controversial Disclosure

A controversial LinkedIn post by David Sennaike about Nigeria's Financial Institutions and the plethora of vulnerabilities on which they operate generated a lot of comments and received mixed reactions from Cybersecurity leadership across the Financial Space.

https://www.linkedin.com/pulse/how-i-hacked-group-hackers-operating-nigerian-banks-tale-sennaike/

https://techcabal.com/2023/05/27/patricia-loses-2m-to-hack/

https://punchng.com/hacker-takes-over-ogun-govt-website/

May 2023

Breach & Stolen Funds

Patricia's recent announcement of a breach on its retail trading app, which froze withdrawals for users. It reveals that the breach happened in January 2022 and cost the company $2 million.

July 2023

Defacement

The Ogun State Government website was defaced with a message hinting the technical team to update their security.

July 2023

Ransomware

Globacom Nigeria's recent ransomware attack was a cyberattack on Globacom Nigeria Ltd., a leading Nigerian telecommunications company, in July 2023. The attack was allegedly carried out by a known ransomware group **(ALPHV**), a cybercriminal gang that encrypts and steals data from its victims. The hacker, who is demanding $2.5m, claims to have been in control of the network for 12 days undetected

https://twitter.com/rbiakpara/status/1680546604443488256

https://blog.cyberplural.com/anonymous-sudan-launches-cyberattacks-on-nigerias-vital-information-systems/

https://www.ccinfo.nl/actuele-aanvallen/cyberaanvallen-weekoverzichten/1415274_overzicht-van-slachtoffers-cyberaanvallen-week-30-2023

August 2023

Distributed Denial of Service

On August 1, 2023, Anonymous Sudan declared on their Telegram channel that it would launch cyberattacks on Nigeria's vital information systems. This was in response to Nigeria's participation in ECOWAS's recent instructions to the Nigerien military to hand over power to the democratically elected government of the Niger Republic. This planned attack began on the 2nd of August, with MTN Nigeria leading the victim list and a partial service outage was observed by customers and users of various services

August 2023

Info & Credential Stealer Malware Campaign

Several MSSPs and private SOCs were reporting cases of information and credential stealer malware in their various constituents. One reported some markets and forums on the dark web have started listing credentials stolen from different Nigerian platforms for sale for as low as $10 per credential. RedLine, Racoon, Lumba, and other samples have been reported so far

https://www.binance.com/en/feed/post/972773

August 2023

Ponzi Scheme Crashed Off

In a harrowing turn of events, Nigeria has been rocked by what is now known as the MTFE Ponzi scheme, an audacious crypto fraud that duped unsuspecting investors out of a staggering $1 billion. Most tragically, the majority of victims hail from the northern regions of the country, serving as a grim reminder of the critical role that knowledge plays in safeguarding oneself against Ponzi schemes and fraudulent crypto projects.

October 2023

Ransomware

A notable construction company in Nigeria was recently attacked by the **Mallox** Ransomware Group. The attack resulted in the encryption of critical servers, and the group demanded a ransom which the company refused to pay. This incident is part of a recent trend of increased activity by the Mallox ransomware group over the past few months.

Whitehat.NG Telegram Group

November 2023

Ransomware

An internet-facing server of a federal agency was recently involved in a ransomware incident. During the incident response, it was discovered that the server was running an older version of the operating system, Windows Vista. The ransom note demanded that the victim write their ID as the message title and send it to back2up@swismail[.]com. All encrypted files had the .**Elbie** extension.

November 2023

Ponzi Scheme Crashes Off

A purported e-commerce earning app called SRA, which gained popularity in some states in North Central Nigeria, has recently crashed. The app was known to offer investment opportunities and allowed users to earn money by fulfilling orders. Unfortunately, it has now been revealed that the app was a scam, and thousands of unsuspecting users in the affected states have lost all of their investments.

Whitehat.NG Telegram Group

https://twitter.com/FalconFeedsio/status/1727989516789801267

November 2023

Ransomware

The **Meow** ransomware group has announced that they successfully breached Wema Bank. A post on the leak site included the bank's machine accounts from its domain controllers, with a threat to release additional data if the bank doesn't negotiate. The breach is believed to have occurred a month earlier, before the listing in November.

December 2023

Ransomware

In a developing story, the **Mallox** ransomware group has seized control of the server of a federal commission responsible for regulating an industry where one of the top players had previously experienced an incident caused by the **ALPHV** group earlier this year. The ransomware group is demanding payment, and all data on the affected server is currently encrypted.

Whitehat.NG Telegram Group

Cybersecurity Incidents Tracking - Whitehat.NG

You can continue to follow the cybersecurity incidents tracking for previous and upcoming years and on our GitHub page by using this link https://github.com/ngwhitehat/Nigeria-Cyber-Incidents or scan the QR code below

Track Incident(s)

Report Incident(s)

Collaborative Initiatives

Whitehat.NG

whitehat.ng

The Whitehat.NG team took the chance to highlight the significance of collaboration and how the community project has been enhancing organizational security across industry vertical.

Speaking at the ISACA Abuja Chapter Annual Conference themed "Digital Trust: The Balance of Governance Innovation and Sustainability" on August 28th, 2023. Presentation focus was "Building Trust for a Cyber-Resilient Nigeria"

The event was organized in collaboration with the US Embassy in Nigeria and other key stakeholders in the sector, and targeted officers of the Ministry of Justice and selected high schoolers from some public and private schools within the FCT

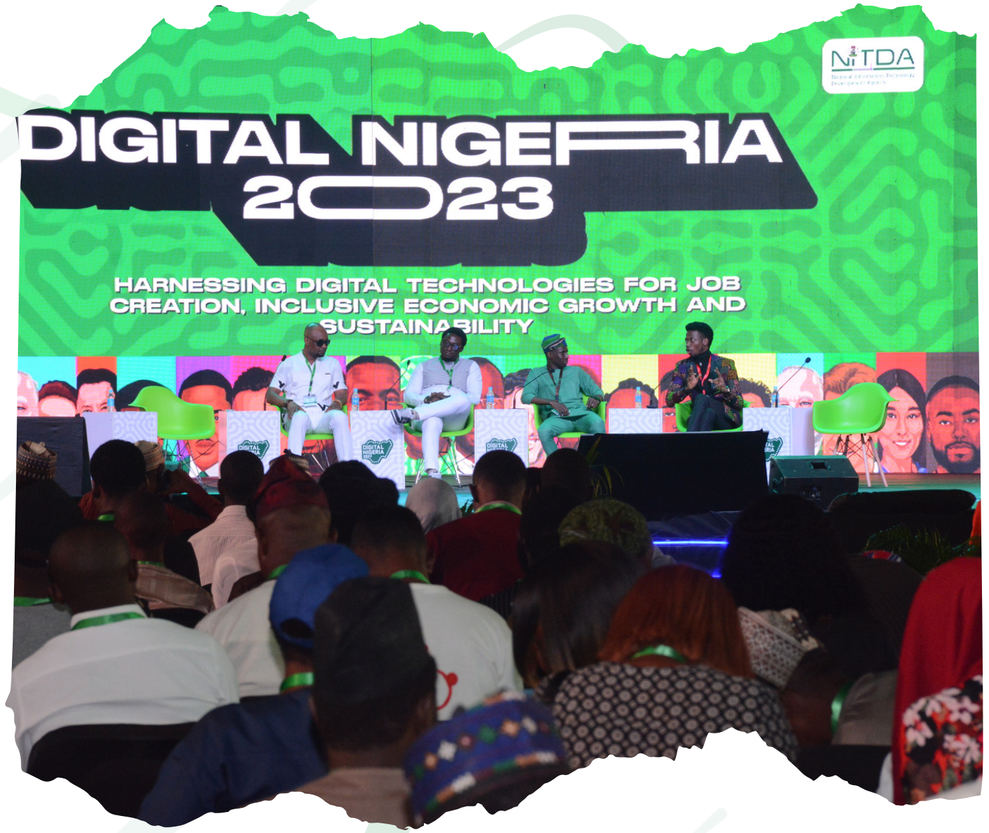
The FMOJ organized a 3-day awareness program on cybercrimes tagged "Don't Fall victim, Don't Perpetrate". The program, which was the first of its kind, focused on conducts criminalized under the existing legal framework on cybercrimes in commemoration of the cybersecurity awareness month - October.

Photo courtesy of CYSED via LinkedIn

The event witnessed the presence of numerous stakeholders from various government agencies, including ONSA, EFCC, ID4D, Nigerian Communications Commission, FMoJ, the Nigeria Army - DSA, NAVY, CDI, as well as NGOs, journalists, and professional bodies such as Cyber Security Experts Association of Nigeria (CSEAN), CPN, ISACA, and ISPON, Banks and Managed Security Service Providers.

On November 22, 2023, a significant event took place as the Senate Joint Committees on ICT & Cybersecurity and National Security & Intelligence conducted a one-day public hearing. The focus of the hearing was to discuss a bill aimed at amending Cybercrime (Prevention, Prohibition, etc.) Act of 2015, along with other related matters.

Cybersecurity Education Initiative (CYSED)- organized technical workshop for Nigerian Federal Government Ministries, Departments, and Agencies (MDAs)



Digital Nigeria Conference 2023. The session revolved around the crucial topic of 'Cybersecurity and Government: Safeguarding Public Services in the Digital Era.'

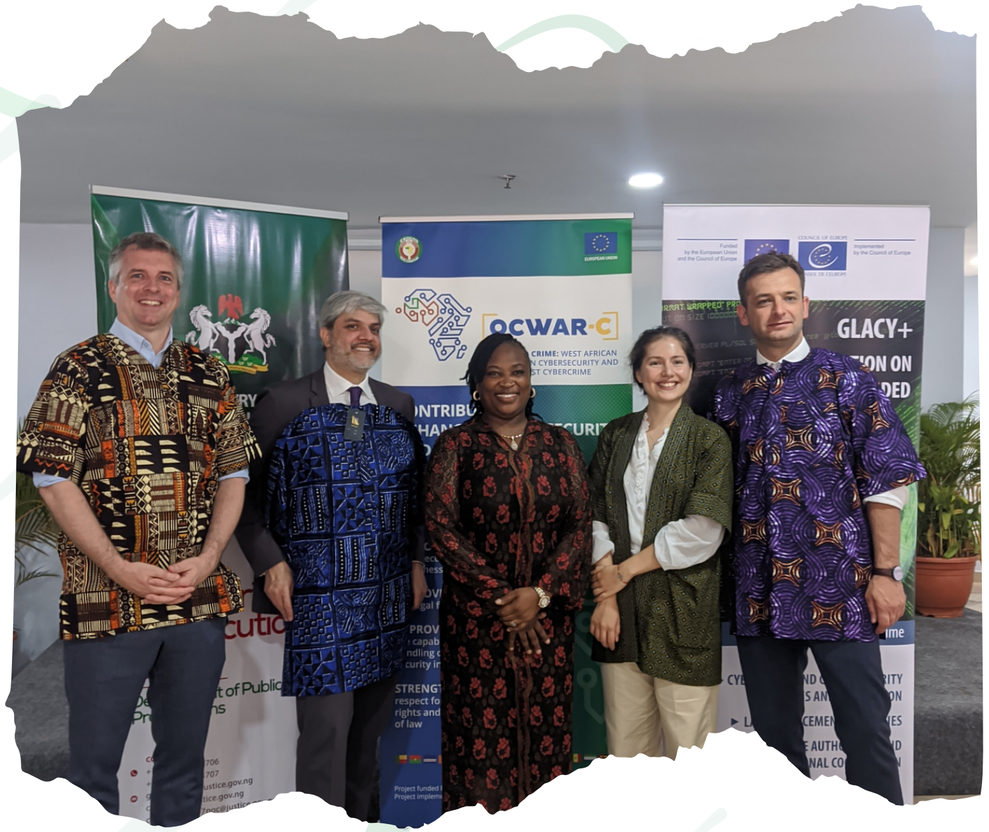
International Security In Cyberspace: Regional Workshop With African Partners On Countering The Threat Of Ransomware. FMoJ ably represented Nigeria.

Photo courtesy of Nne Akpia via LinkedIn

Nigeria Data Protection Strategic Roadmap and Action Plan (NDP-SRAP) 2023-2027 - The National Commissioner and The Drafting Team

Photo courtesy of Hassan.O via LinkedIn

Two days of workshops on Cybersecurity capacity building workshop organized by the Federal Ministry of Communications, Nigeria, and The World Bank Group



Consultation on the national legal framework on cybercrime that the Federal Ministry of Justice, Nigeria organized in partnership with GLACY+ and OCWAR-C projects of the Council of Europe. Stakeholders like ONSA, NFIU, EFCC, NPC-CCC, NCC, MFA, CSEAN, Judges, and more witnessed this consultation.

Inaugural Africa Summit on Countering Online Child Sexual Exploitation and Abuse at Addis Ababa, Ethiopia,

The FMoJ Team, Nne Akpan Ikoiwak, and Leyii Mekko ably represented Nigeria.

Photo courtesy of Nne Akpian Ikoiwak via LinkedIn

Nigeria and the AUCSEG participated in the global fight against cybercrime at the Octopus Conference hosted by the Council of Europe in Romania.

Photo courtesy of Abdul-Hakeem Ajijola via LinkedIn

The GC3B event was the first-ever Global Conference on Cyber Capacity Building, which took place in Accra, Ghana. Nigeria was ably represented in this landmark event for the international community, as it fostered collaboration and coordination among different stakeholders and sectors to ensure a free, open, and secure digital world for all.

Educational Offerings

Whitehat.NG

whitehat.ng

Educational Offerings

Throughout 2023, several non-profit organizations and NGOs dedicated themselves to providing cybersecurity training across various learning paths, including Devsecops, GRC, Security Operations, and VAPT. Notable leaders in this field include the Cybersafe Foundation, Secopstalents, Cyblack, and the Cybersecurity Education Initiative (CYSED). Their efforts have resulted in capacity building for participants from diverse cohorts, contributing significantly to capacity building within Nigerian cyberspace.

https://cysed.org/
https://cybersafefoundation.org/
https://secopstalents.com/

In addition, during the cybersecurity awareness month, we witnessed awareness sessions taking place at various levels, conducted by both public and private sector entities, as well as at the organizational, marketplace, and religious center levels. This widespread effort reflects a growing commitment to raising awareness about cybersecurity across different sectors of society.

Professional bodies and associations like the Cyber Security Expert Association of Nigeria (CSEAN), Nigeria Computer Society (NCS), ISACA, and others organized conferences and workshops that brought stakeholders, professionals, members, and the public together to discuss and address key cybersecurity issues relevant to Nigeria.

Conclusion

Whitehat.NG

Conclusion

We extend our gratitude to our team, researchers, and MSSPs whose contributions have been instrumental in the success of the Whitehat.NG project.

As we look ahead to 2024, we remain open to collaborating with additional researchers and receiving support from MSSPs and in-house SOCs across the country. You can express your willingness to contribute by using our email, and we eagerly anticipate the opportunity to work with you.

The 2023 Annual Report reflects the unwavering commitment of Whitehat.NG to fortifying Nigeria's cybersecurity landscape. The responsible disclosure of security vulnerabilities, tracking of cyber incidents, and collaborative initiatives underscore our dedication to safeguarding Nigeria's digital infrastructure.

As we move forward, we remain steadfast in our pursuit of fostering partnerships, innovation, and education in cybersecurity. The report serves as a testament to our collective efforts in enhancing cybersecurity resilience.

Together, we continue to build a safer and more secure digital environment for Nigeria

whitehat.ng

Nigeria's Cyberspace ISAC + PEOPLE CERT

YOU SEE SOMETHING,
SAY SOMETHING
BUT RESPONSIBLY.

Follow and Contact Us

https://whitehat.ng

ngwhitehat

https://linkedin.com/company/whitehat-ng

cert@projectwhitehat.ng

ngwhitehat

Partnering

ngCERT Nigeria Computer Emergency Response Team

NITDA CERRT. NG

NCC CSIRT