PRESS RELEASE: FOURTH AFRICA CYBER DRILL: LEVEL UP YOUR READINESS

The Forum of Africa Computer Emergency Response Teams, known as AfricaCERT, successfully completed its Fourth Annual Cyber Drill, titled **"Leveling Up Your Readiness,"** at Avani Victoria Falls Resort in **Livingstone, Zambia**, **on November 29-30, 2024**.

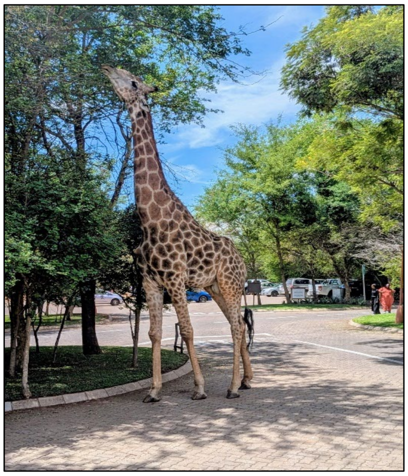
This drill builds upon the successes of the previous three drills conducted in 2021, 2022, and 2023, reinforcing our commitment to advancing cybersecurity readiness across the continent. The themes of our past drills - **"Fill The Gaps," "Stay On Alert," and "Testing The Waters"** - have established a robust foundation that we will continue to expand upon.

A Welcome Return to Zambia

AfricaCERT extends its gratitude to the Government of Zambia and the Zambia Information and Communications Technology Authority (ZICTA) for once again graciously hosting this community, following the **AfricaCERT IV event, "What Solutions for the African Continent," held from June 10-15, 2013, in Lusaka.**

About the Fourth Africa Cyber Drill

The Fourth Africa Cyber Drill was strategically conducted during the Africa Regional Cybersecurity Symposium 2024, highlighting powerful collaboration between the Southern African Development Community (SADC) Secretariat and the FIRST AfricaCERT Symposium 2024. AfricaCERT, with unwavering backing from the SADC Secretariat, ZICTA, and key partners, including the Computer Emergency Response Team of Mauritius (CERT-MU), Forum of Incident Response and Security Teams (FIRST), Benin Incident Response Team (bjCSIRT), and Iservices Systems, successfully hosted this hybrid cyber drill during the symposium. Cyber Ranges by Silensec provided its cyber range platform to facilitate the scenarios.



Why We Conduct an Annual Cyber Drill

Since 2013, AfricaCERT has implemented structured and customizable exercises and training sessions designed to significantly enhance stakeholders' response capabilities and cyber competencies, with the Africa Asia Forum on Network Research and Engineering (AAF) and numerous partners such as the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), the Asia Pacific Computer Emergency Response Team (APCERT), the Organization of The Islamic Cooperation (OIC) CERT, the International Telecommunication Union (ITU), the Tunisian Computer Emergency Response Team (TunCERT), the Egyptian National Computer Emergency Readiness Team (EG-CERT)FIRST, the Software Engineering Institute (SEI), CERT-FR, SURFcert, GEANT, The Task Force on Computer Security Incident Response Teams (TF-CSIRT. The trainings happened at the African Network Operators Group (AfNOG) and African Network Information Center (AfriNIC) meetings. The exercises encompass capture the flags and tabletop exercises held throughout the year.

The COVID-19 pandemic introduced unique challenges requiring a comprehensive approach to bolster cyber resilience within participating organizations. Teams including bjCSIRT (Benin), CERT-MU (Mauritius), EGCERT (Egypt), KE-CIRT (Kenya), KEYSTONE (Tunisia), tunCERT (Tunisia), and Iservices Systems (US) played a pivotal role in designing the foundational structure of the Africa Cyber Drill, employing new formats for exercises and scenarios. These exercises provide clear insights into participants' preparedness and drive necessary behavioral changes.

Objectives

The drill scenarios include a wide array of threat simulations, such as ransomware attacks, malware reverse engineering, and tabletop scenarios tailored to current cyber risks. These scenarios simulate real-world cyber incidents in a controlled environment, enabling participating organizations to effectively practice responses to everyday challenges, rigorously evaluate their incident response capabilities, and enhance their technical and operational readiness. Furthermore, they foster collaboration with other teams across sectorial, continental, and international levels to tackle complex cyber scenarios head-on.

A typical scenario can gather executives, policymakers, and stakeholders involved in managing and responding to cybersecurity incidents, alongside technical staff, all participating in simulation-based exercises that reinforce collaboration and communication during crises. The goal is to rigorously test and enhance existing communication mechanisms while strengthening cooperation between Security Incident Response teams and their stakeholders, thereby significantly advancing the region's cybersecurity readiness and incident response capabilities through agile, hands-on exercises.

Structure of the Fourth Africa Cyber Drill

The structure of this year's drill included remarks, presentations, and immersive exercises.

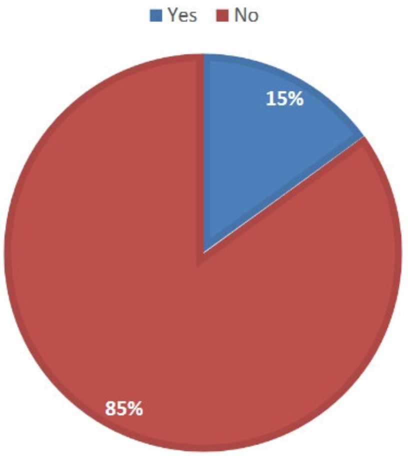
*Remarks**

The annual cyber drill commenced and concluded with remarks from representatives from Zimbabwe and Angola, serving as the Chair and Vice Chair of SADC, as well as representatives from AfricaCERT and the host country, Zambia.

*Presentations**

- **JPCERT CVD Process**:

The Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), a trusted ally of AfricaCERT and the African security community since 2010, delivered a crucial presentation on Coordinated Vulnerability Disclosure (CVD). One key finding from the AfricaCERT annual survey highlighted that only fifteen percent of surveyed countries have a national vulnerability coordination process in place, underscoring the urgent need for improvement.



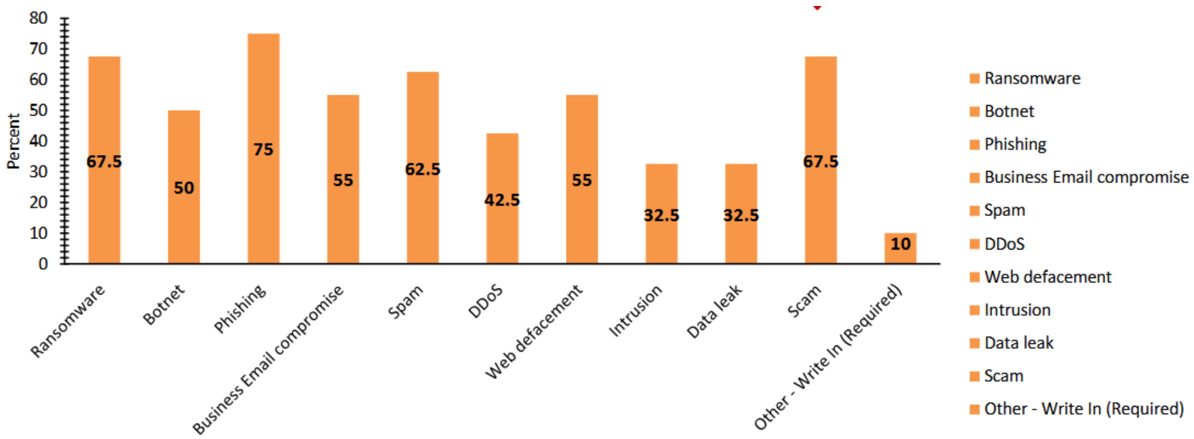
(1). AfricaCERT Report. African Countries with National Vulnerability Disclosure Policies in Place in Africa

- **Detecting Active Directory Post-Exploitation with ELK SIEM**:

A representative from the Benin Republic Incident Response Team showcased advanced methods for detecting post-exploitation activities in Active Directory environments, concentrating on credential dumping and persistence techniques.

Exercises

The exercises simulated the most pressing incidents reported in the last twelve months, as documented in the annual AfricaCERT Cybersecurity report. These cases included ransomware, malware reverse engineering, and financial fraud scenarios.



(2). AfricaCERT Report: The main observed incidents in the last 12 months.

****Participants****

The drill saw participation from **45 African countries**, including Somalia, Nigeria, Morocco, Benin, Ghana, Chad, Zambia, Botswana, South Africa, Eswatini, Mauritius, Rwanda, Mali, Mozambique, Malawi, Djibouti, Togo, Burkina Faso, Angola, The Gambia, Tunisia, Kenya, Zimbabwe, the Democratic Republic of Congo, Sierra Leone, South Sudan, Liberia, Burundi, Uganda, Lesotho, Egypt, Tanzania, Ivory Coast, Namibia, Ethiopia, Comoros, Madagascar, and Seychelles.

Colleagues from OIC-CERT and APCERT (including representatives from Pakistan, Bahrain, Malaysia, Bangladesh, Japan, India, China, and Afghanistan) joined their African counterparts.

The organizing team wishes to thank the speakers and sponsors, including Cyber Ranges, Mopani, UK International Development, Veritas, The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), and Iservices Systems.

We look forward to seeing everyone in fall 2025, for the next event themed "**REDUCE, INCREASE, DECREASE."**