Making Incident Response and Security Teams Effective within Africa

Contact: secretariat@africacert.org

who we are

AfricaCERT
United Teams promoting Cybersecurity in Africa

Provides a trusted forum for African Computer Security Incident Response Teams and alike organizations to more effectively respond to security incidents.

Members: government, commercials, academic sectors / Structured and unstructured

Capacity Building **International Cooperation** **Maturity Enhancement**

- Technical Assistance
- Education and Capacity Building (Events, Trainings, Annual or Local Cyber drills …)
- Access to Tools, Technology, standards and Resources including fellowships and funding
- Participating in public policies and debates related to CSIRT operations and Cybersecurity
- Coordination with the Incident Response and Security Community at Large
- Facilitation of critical incident resolution through the support of international incident response community
- Incident Response Team of last resort.

Technical Assistance

Takes various forms through a pool of experts

- Support to stand teams capability
- Deploy tools
- Coaching
- Engagement with another team or other stakeholders
- Maturity Assessments and Support for Memberships (Since 2015, support for FIRST Membership, OIC-CERT Membership, etc…)
- Standards implementation advise

Technical Assistance

- **Engagement with certification providers as <u>Membership Perks</u>**
  - Africa League of Trainers
  - Training at discounted prices
  - Members or Though a National Team that is a member
    - Global Partnership with **ISC2**
    - **COMPTIA**
    - **SANS (15%)**
- **Partnerships**

Important project can happen by seeking out partners, and diverse collaborators, who are willing to share ideas and share works.

  - **ATU**
  - **GFCE**
  - **FIRST**
  - **ITU-T (SG17)**
  - **SMART AFRICA**
  - **Home of Africa Anti Abuse Working Group (M3AAWG)**
  - **OIC-CERT**
  - **APCERT**

- **Capacity building and events**

  - Webinars / Meetings
    - SolarWinds supply chain attack with **Microsoft (AfAAWG/M3AAWG)**
    - Log4J Coordination
    - UN Norms
    - ICANN on DNS Abuse
    - Passive DNS **(Threat Intel Project)**
    - Ransomware Incident Response – **Palo Alto Networks**.
    - Abuse Desk training **(M3AAWG)**

Third SADC Cyberdrill (co-Organizer).
20th to 21st October 2022

Annual Africa Cyber Drill: 2nd Africa CYBER DRILL "Stay on Alert"
September 8-9, 2022 –

Offcial CISSP Bootcamp
- Nov 21 – 25, 2022
- July 11 – 15, 2022

- **Exercises**
  - **1st Africa Cyberdrill 30 June – 01 July 2021.** “Testing The Waters”. The Drill aimed to test the response capability of participating teams facing the following scenarios: Phishing, Defacement, REM, Ransomware investigation.
  - ❑ The African countries participating in the Drill are **Benin, Botswana, Cote d’Ivoire, Djibouti, Egypt, Gambia, Kenya, Lesotho, Mozambique, Nigeria, The Seychelles, Tanzania, Tunisia, and Zambia**, in addition to the team from the SADC secretariat. Colleagues from OIC-CERT and APCERT (**Brunei, India, Indonesia, Malaysia, Japan, Pakistan, Philippines, Sri-Lanka, Uzbekistan, Turkey, and Syria**) joined African Teams. 32 Computer Security Incident Response Teams from 25 countries have participated in the Drill, including the organizing teams.

  - **2nd Africa CYBER DRILL “Stay On Alert”. September 8 to 9 2022.** The Drill aimed to test the response capability of participating teams facing the following scenarios: Business Email Compromise, SQL injection, and Supply chain vulnerabilities.50 Computer Security Incident Response Teams from 39 countries.
  - ❑ The African countries participating in the Drill are Benin, **Botswana, Burkina Faso, Cameroon, the Republic of Chad, Cote d’Ivoire, Comoros, Djibouti, Egypt, Gabon, Gambia, Ghana, Kenya, Libya, Madagascar, Malawi, Morocco, Mozambique, Niger, Nigeria, Rwanda, Sierra Leone, Seychelles, South Sudan, Sudan, Tanzania, Togolese Republic, Tunisia, Uganda, and Zambia**. Colleagues from OIC-CERT and APCERT (**Bangladesh, Brunei, India, Indonesia, Malaysia, Philippines, Uzbekistan, and Turkey**) as well as from Latin America joined African Teams.

“Cyber Incident Management in Low-Income Countries” project, funded by Global Affairs Canada. The project aims to create a tailorable guide for low-income countries to develop or improve their CSIRT capabilities in an affordable way to respond to the evolving cyber threat environment effectively.

https://cybilportal.org/publications/cyber-incident-management-in-low-income-countries-part-1-a-holistic-view-on-csirt-development/

Publications

UPCOMING

- Second Publication about Standards Implementation in Africa
- Member Service Platform
- New Website
- CVE / CNA / Project

Upcoming Working Groups

- Training and Capacity building working Group
- ICS security Working Group
- Working Group on UN Cyber norms and CBM for the CSIRT Community

- Webinars (1 - 4 h event) shared through emails
- Crisis Management TTXs (one day event)
- AfricaCERT, CISSP 5 Day, 8hrs per Day Bootcamp May 2023
- AfricaCERT Member Meeting Tentatively End of April 2023
- Jointly meeting with AfriNIC, AfNOG July (TBD)
- Participation in the upcoming cyberdrill in Malawi Beg May 2023
- (Offensive Security Training – Aug /Sep 2023 (TBA)

Membership Drive

- Operational Member CSIRT
- Supporting Member JPCERT
- Individual Member
- Honorary Members (people who have contributed)

UPCOMING – in the pipeline

- Full Operational Member (Full Member)
- Associate Members
- Individual Members
- Honorary Members
- AfricaCERT Partners

❖ Supporting Members
❖ Organizational Partners

Thank you.

Contact: secretariat@africacert.org