ITU- INTERPOL regional Cyber Drill twelfth edition for Africa Region, at Kofi Annan International Peacekeeping Training Centre, Accra, Ghana
02-06 September 2024

DRAFT AGENDA

DAY 1: TRAININGS

Monday 2nd September 2024

09:00 – 09:30	Registration
09:30 – 10:30	**External Attack Surface Management,** Mirza Asrar Baig, CTM360
10:30 – 10:45	Networking Break
10:45 – 12:30	**Threat Intelligence,** MirzaAsrar Baig, CTM360
12:30 – 13:30	Lunch Break
13:30 – 16:00	**Hunting for Winter Vivern,** Gibson Michira, Cyberranges
16:00 – 16:30	Networking Coffee

DAY 2: TRAININGS

Tuesday 3rd September 2024

09:00 – 09:30	**Registration**	
09:30 – 10:30	Training Track I: **Building Malware Analysis Capability for CERTs,** Mr. Paweł Pawliński, FIRST	Training Track II: **Cyber crisis management** Mr. Samir Aliyev, Swiss Cyber Institute
10:30 – 10:45	**Networking Break**	
10:45 – 12:30	Training Track I: **Building Malware Analysis Capability for CERTs,** Mr. Paweł Pawliński, FIRST	Training Track II: **Cyber crisis management** Mr. Samir Aliyev, Swiss Cyber Institute
12:30 – 13:30	**Lunch Break**	
13:30 – 16:00	Training Track I: **Building Malware Analysis Capability for CERTs,** **Mr. Paweł Pawliński, FIRST**	Training Track II: **Cyber crisis management** **Mr. Samir Aliyev,** **Swiss Cyber Institute**
16:00 – 16:30	**Networking Coffee**	

DAY 3: ITU-INTERPOL Regional Forum: Bridging the Gap, Building the Future

Wednesday 4th September 2024

08:00 – 09:00 Registration

09:00 – 09:40 **Opening Ceremony**

- Welcome Remarks by Host Country: **Albert Antwi-Boasiako** Director-General, CSA
- Welcome Statements by ITU: **Ali Drissa BADIEL**, Area Representative of ITU Area Office for West Africa
- Opening Statements by INTERPOL: **Enrique Hernandez Gonzalez,** Assistant Director Cybercrime Operations, INTERPOL Cybercrime Directorate
- Opening remarks by UN: **Charles Abani**, UN resident coordinator office (Tbc)
- Keynote: **Ursula Owusu-Ekuful**, Minister for Communications and Digitalisation for the Republic of Ghana

---

09:40 – 10:00 Networking Break and Group Photo

10:00 - 10:20 **Presentation on Ghana's Cybersecurity Architecture, CSA**

10:20 – 10:40 **GCI 2024 Insights – Key Discoveries, Lessons, and Challenges in Africa**

This presentation will explore the key findings from the Global Cybersecurity Index (GCI) 2024 report, with a specific focus on Africa region. The speaker will highlight significant trends, developments, and challenges identified in the cybersecurity landscape of these areas. The discussion will cover various aspects, including legal measures, technical capabilities, organizational structures, capacity development initiatives, and regional cooperation efforts.

S.V. Zongo, Program Officer, ITU regional Office for Africa

10:40 – 11:50 **Panel Discussion: Strengthening Africa's Cybersecurity Posture**

Provide a comprehensive understanding of the current state of cybersecurity and cybercrime in the African region, highlighting key trends, challenges, and opportunities.

Moderator: **Ali Drissa BADIEL**, Area Representative of ITU Area Office for West Africa

Panellists: **J. R. Hountomey** CEO, AFRICACERT, **Mirza Asrar Baig** CEO, CTM360, Member state, CSA

11:50 – 12:10 **AfricaCERT UPDATE**

Jean-Robert Hountomey, CEO AfricaCERT

12:10 – 12:30 **Technical Presentation**

CSA Partner

12:30 – 14:00 Lunch Break

14:00 – 14:20 **INTERPOL African Cyberthreat Assessment Report 2024**

Peter STANIER, Cybercrime Intelligence Officer, Cybercrime Directorate, INTERPOL

14:20 – 15:35 **Panel Discussion: Building Effective Partnerships Between CIRTs and Law Enforcement**

This session explores how National CIRTs, and Law Enforcement can join forces, leveraging unique expertise and resources to build a more effective response. Explore best practices, overcome collaboration challenges, and discover real-world examples of how partnerships deliver stronger cyber defense capabilities.
Moderator: Jackson CHEBOI, Regional Specialized Officer, project AFJOC, INTERPOL Cybercrime Directorate.
Panellists: Felix AFEDI, Officer, Law Enforcement Unit, Cyber Security Authority, Ghana,
Jacob MUWAJA, Deputy Head, Cybercrimes Unit, Tanzania Police Force,
Mohammed ISAH, Head of the Africa Desk, INTERPOL Cybercrime Directorate,
Ilya ROZHNOV, CERT Executive Engineer, Group IB

15:35 – 16:00 Coffee Break

16:00 – 16:10 **Law Enforcement capacity building through the Global Action on Cybercrime.**
Cybercrime is complicated and needs a broader solution, overarching harmonized legislation, national policies, judicial training, and international police cooperation. In his presentation, Specialized Officer Dong Uk KIM will show how INTERPOL and the Council of Europe have been cooperating through the Global Action on Cybercrime (GLACY) project and invite the security community represented by members of the CSIRTs to join forces with INTERPOL.
Dong Uk KIM, Specialized Officer, Project GLACY-e. Cybercrime Directorate, INTERPOL

16:10 – 16:20 **Capacitating African Member Countries in combatting Cybercrime.**
An outline of the cybercrime training program that empowers African Member Countries with tools and training to enhance the quality of investigations and operations across the continent
Preshan KISSOONDOYAL, Cyber Specialized Officer, Project ISPA-AFRIPOL INTERPOL

16:20 – 16:30 **AFRIPOL Cybercrime Strategy**
The presentation describes the main areas of action of Afripol's anti-cybercrime strategy. This strategy aims to help its member states fight Cybercrime more effectively through coordination and establishment of specialized police capacities for the period 2020-2024
Rivel Marius NGUIE, Senior Cybercrime Analyst, AFRIPOL

16:30 – 16:40 **Combatting Cybercrime in the Africa region – AFJOC Project**
An overview of the AFJOC II Project, which aims to further enhance the capabilities of national law enforcement agencies in Africa by focusing on preventing, detecting, investigating, and disrupting cybercrime activities, thereby strengthening regional capacity and collaboration

	Lauren MISSLER, Regional Cybercrime Specialized Officer, Cybercrime Directorate, Project AFJOC
16:40 – 16:50	**The importance of a Pan African approach in strengthening cyber security and tackling cyber crime** **Tim GALVIN,** Africa Cyber Programme Manager, UK FCDO
16:50 – 17:20	**Closing Remarks**

DAY 3 and 4: CYBER EXERCISES

Thursday 5th September 2024

Target Audience:	National CSIRTs/CIRTs team members and Law Enforcement officers specializing in cybercrime within the African region.
Team configuration:	Participating countries will form teams combining their National CSIRT/CIRT experts and law enforcement cybercrime specialists. This collaborative approach enhances communication and cooperation within each nation, facilitating swift responses to threats and strengthening national cybersecurity defenses through collective action and knowledge sharing

09:30 – 10:00	Team creation, registering team accounts to Cyber Range
10:00 – 12:30	**Scenario 1:** FIRST Scenario-based exercise
12:30 – 13:30	Lunch Break
13:30 – 16:00	**Scenario 2 :** Swiss Cyber Institute Scenario-based exercise

Friday 5th September 2024

09:30 – 11:00	**Scenario 3 :** INTERPOL Scenario-based exercise
11:00 – 13:00	**Scenario 4:** ITU Scenario-based exercise
13:00 – 14:00	Lunch Break
13:30 – 16:00	**Scenario 5:** Cyberranges- Scenario-based exercise
16:00 – 16:30	**Closing remarks**

TRAININGS

Training Track I: External Attack Surface Management (09:30 -10:30)

Description:	Consolidating your External Attack Surface Managing cyber risk across your third parties
Audience:	National cybersecurity professionals in the Africa region: From CSIRTs/CERTs, National Cyber Security Agencies, and Critical Infrastructure operators
Course level:	Intermediate
Pre-requisites	None

Training Track I: Threat Intelligence (11:00 -12:00)

Description:	Managing cyber–Threat Intelligence challenges Leveraging from cyber kill-chain concept
Audience:	National cybersecurity professionals in the Africa region: From CSIRTs/CERTs, National Cyber Security Agencies, and Critical Infrastructure operators
Course level:	Intermediate
Pre-requisites	None

Training Track II: Hunting for Winter Vivern

Description:	This session will involve practical simulation exercises where participants, guided by the instructor, will engage in a hands-on threat hunting/incident response activity, specifically aimed at observing and identifying TTPs from the known threat actor Winter Vivern.
Audience:	National cybersecurity professionals in the Africa region: From CSIRTs/CERTs, National Cyber Security Agencies, and Critical Infrastructure operators
Course level:	Intermediate
Pre-requisites	Each participant gets access to a VM with a Linux environment, accessible via SSH and RDP/VNC. Submitting answers to tasks in the hands-on part of the training and challenges during the exercise in a dedicated on-line platform. The course is hands-on, and a laptop is required to be able to work through all the practical hands-on Workshops. The minimum laptop requirements are: x86-compatible 1.5 GHz minimum or higher, 4GB RAM minimum or higher, 20GB available hard drive space, capable of installing virtualization software

Training Track III: Building Malware Analysis Capability for CERTs

Description:	The goal of this training is to kickstart malware analysis capability, especially for smaller and less mature teams. This is a technical training, which provides an overview of multiple aspects of malware analysis for CSIRTs, including introduction into malware ecosystem, triage, different approaches to investigation, remediation and hunting. It covers creation of appropriate internal workflows, leveraging online services and using open-source tools. This one-day training covers multiple topics related to malware analysis on an introductory level in order to provide a broad overview of the subject, so the participants will be able to decide on a development path suitable for their requirements and, possibly, move on to more in-depth courses. Nevertheless, many hands-on exercises are included, so participants will gain practical skills in using free tools and services to investigate malware threats.
Audience:	National cybersecurity professionals in the Africa region: From CSIRTs/CERTs, National Cyber Security Agencies, and Critical Infrastructure operators
Course level:	Intermediate
Pre-requisites	Each participant gets access to a VM with a Linux environment, accessible via SSH and RDP/VNC. Submitting answers to tasks in the hands-on part of the training and challenges during the exercise in a dedicated on-line platform. The course is hands-on, and a laptop is required to be able to work through all the practical hands-on Workshops. The minimum laptop requirements are: x86-compatible 1.5 GHz minimum or higher, 4GB RAM minimum or higher, 20GB available hard drive space, capable of installing virtualization software

Training Track IV Cyber crisis management

Description:	This Cyber Crisis Management Training is an intensive, hands-on program designed for professionals from National CSIRTs, Cyber Security Authorities, Cyber Security Agencies, and law enforcement officers specializing in cybercrime. Over the course of six hours, participants will engage in practical exercises, including real-world simulations, to develop and refine their skills in managing cyber crises. The training emphasizes effective incident response planning, crisis communication, inter-agency coordination, and post-crisis recovery. By the end of the program, attendees will be equipped with the essential tools and knowledge to respond swiftly and efficiently to cyber crises, ensuring national cybersecurity resilience.
Audience:	National cybersecurity professionals in the Africa region and managers
Course level:	Intermediate
Pre-requisites	The course is hands-on, and a laptop is required to be able to work through all the practical hands-on Workshops. The minimum laptop requirements are: x86-compatible 1.5 GHz minimum or higher, 4GB RAM minimum or higher, 20GB available hard drive space, capable of installing virtualization software