AfricaCERT
United in promoting cyber security in Africa

FIRST

REGIONAL SYMPOSIUM
FEB 28 - MAR 3, 2023 | KIGALI, RWANDA

# SOC, CSIRT and then "Cyber Defense Centre"

## Workshop On How to Defend African Nations/Businesses with ITU-T X.1060

CO-HOST

National Cyber Security Authority

# Agenda

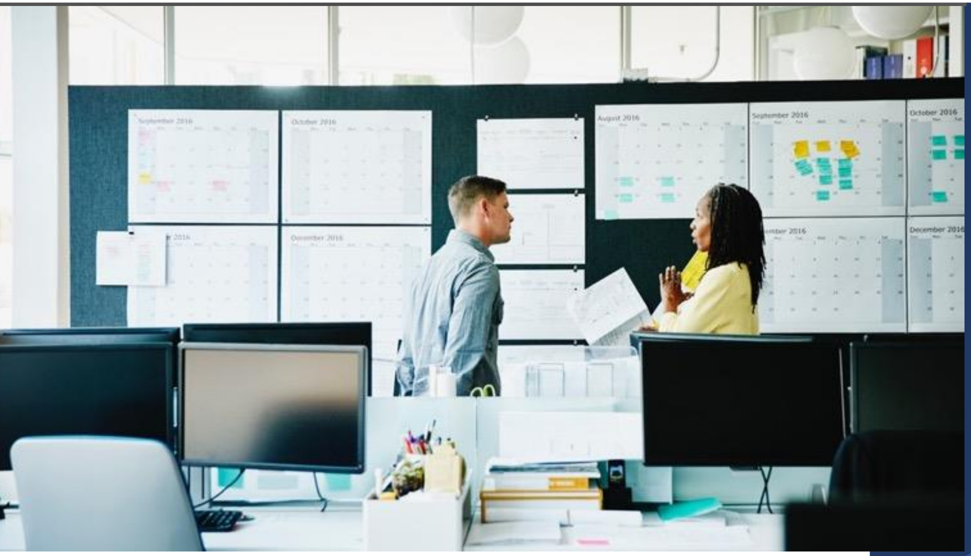
X.1060
Cyber
Defence
Centre

9:00 Opening/Intro(Koichiro)
9:10 remarks by Arnaud
9:40 remarks by Jema
10:00 remarks by Koichiro
10:25 Q&A session (Jema will lead the Q&A. )
10:55 Close

# How frameworks guide you to have better SOC/CSIRT/Cyber Defence Center

Dr. Koichiro Sparky Komiyama (CISSP)
JPCERT/CC
Director, Global Coordination Division

# Cyber Security is a team sports.

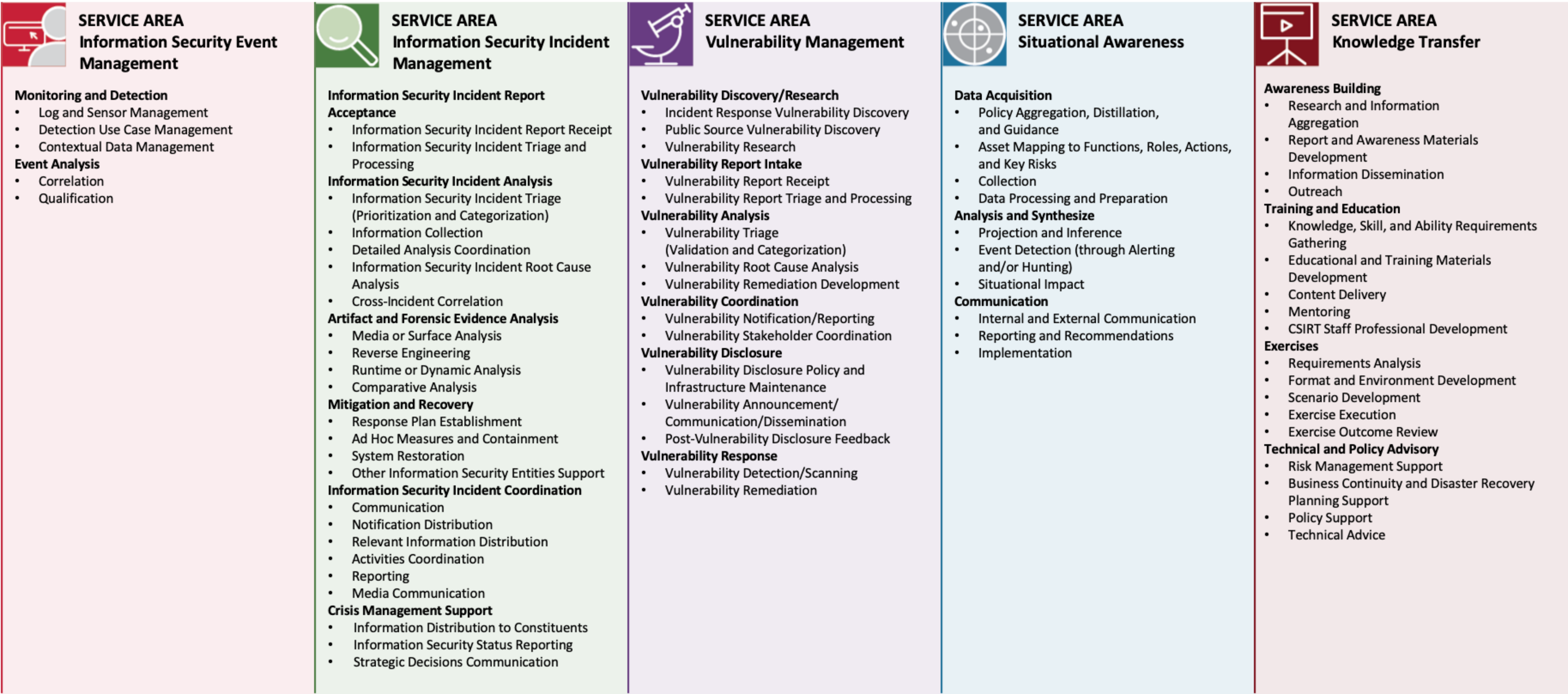


# Framework enables you to do:

1. A jump start
2. More comprehensive approach

# FIRST CSIRT Services Framework v2.1

- Available in seven languages(Fr, Arabic, Es, Chinese, Ru, Jp)



SERVICE AREA
**Information Security Event Management**

**Monitoring and Detection**
- Log and Sensor Management
- Detection Use Case Management
- Contextual Data Management

**Event Analysis**
- Correlation
- Qualification

SERVICE AREA
**Information Security Incident Management**

**Information Security Incident Report Acceptance**
- Information Security Incident Report Receipt
- Information Security Incident Triage and Processing

**Information Security Incident Analysis**
- Information Security Incident Triage (Prioritization and Categorization)
- Information Collection
- Detailed Analysis Coordination
- Information Security Incident Root Cause Analysis
- Cross-Incident Correlation

**Artifact and Forensic Evidence Analysis**
- Media or Surface Analysis
- Reverse Engineering
- Runtime or Dynamic Analysis
- Comparative Analysis

**Mitigation and Recovery**
- Response Plan Establishment
- Ad Hoc Measures and Containment
- System Restoration
- Other Information Security Entities Support

**Information Security Incident Coordination**
- Communication
- Notification Distribution
- Relevant Information Distribution
- Activities Coordination
- Reporting
- Media Communication

**Crisis Management Support**
- Information Distribution to Constituents
- Information Security Status Reporting
- Strategic Decisions Communication

SERVICE AREA
**Vulnerability Management**

**Vulnerability Discovery/Research**
- Incident Response Vulnerability Discovery
- Public Source Vulnerability Discovery
- Vulnerability Research

**Vulnerability Report Intake**
- Vulnerability Report Receipt
- Vulnerability Report Triage and Processing

**Vulnerability Analysis**
- Vulnerability Triage (Validation and Categorization)
- Vulnerability Root Cause Analysis
- Vulnerability Remediation Development

**Vulnerability Coordination**
- Vulnerability Notification/Reporting
- Vulnerability Stakeholder Coordination

**Vulnerability Disclosure**
- Vulnerability Disclosure Policy and Infrastructure Maintenance
- Vulnerability Announcement/ Communication/Dissemination
- Post-Vulnerability Disclosure Feedback

**Vulnerability Response**
- Vulnerability Detection/Scanning
- Vulnerability Remediation

SERVICE AREA
**Situational Awareness**

**Data Acquisition**
- Policy Aggregation, Distillation, and Guidance
- Asset Mapping to Functions, Roles, Actions, and Key Risks
- Collection
- Data Processing and Preparation

**Analysis and Synthesize**
- Projection and Inference
- Event Detection (through Alerting and/or Hunting)
- Situational Impact

**Communication**
- Internal and External Communication
- Reporting and Recommendations
- Implementation

SERVICE AREA
**Knowledge Transfer**

**Awareness Building**
- Research and Information Aggregation
- Report and Awareness Materials Development
- Information Dissemination
- Outreach

**Training and Education**
- Knowledge, Skill, and Ability Requirements Gathering
- Educational and Training Materials Development
- Content Delivery
- Mentoring
- CSIRT Staff Professional Development

**Exercises**
- Requirements Analysis
- Format and Environment Development
- Scenario Development
- Exercise Execution
- Exercise Outcome Review

**Technical and Policy Advisory**
- Risk Management Support
- Business Continuity and Disaster Recovery Planning Support
- Policy Support
- Technical Advice

# NIST SP800-61 Rev2

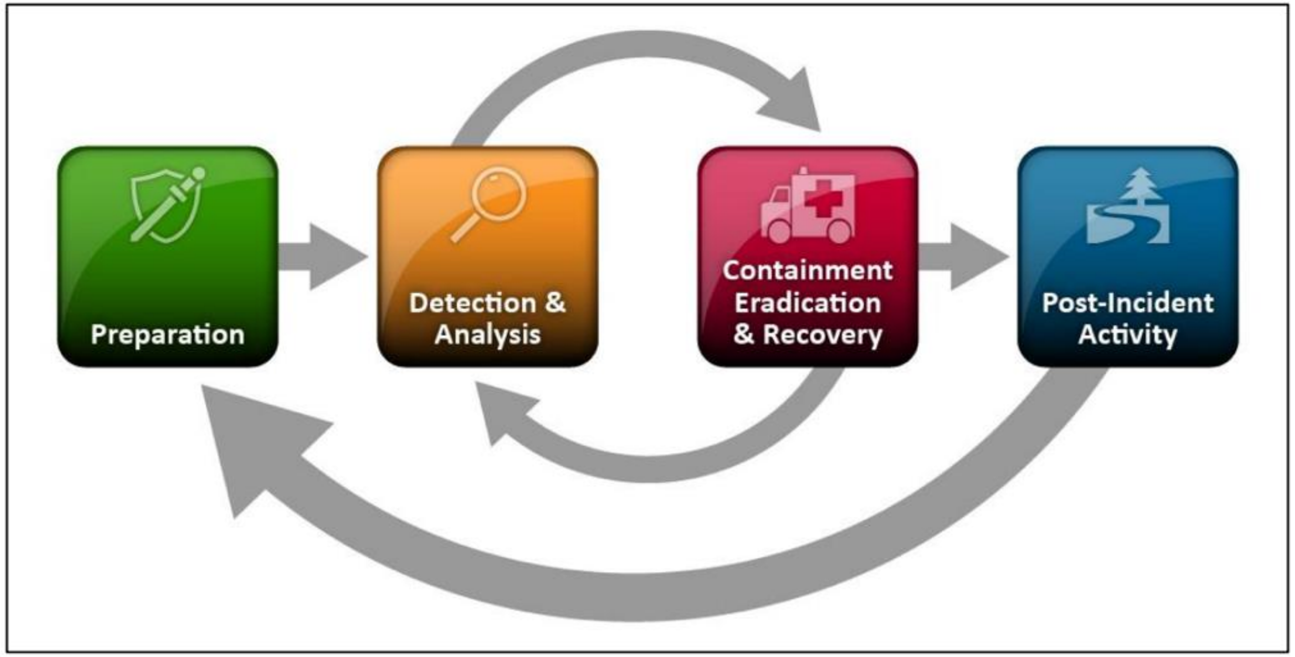
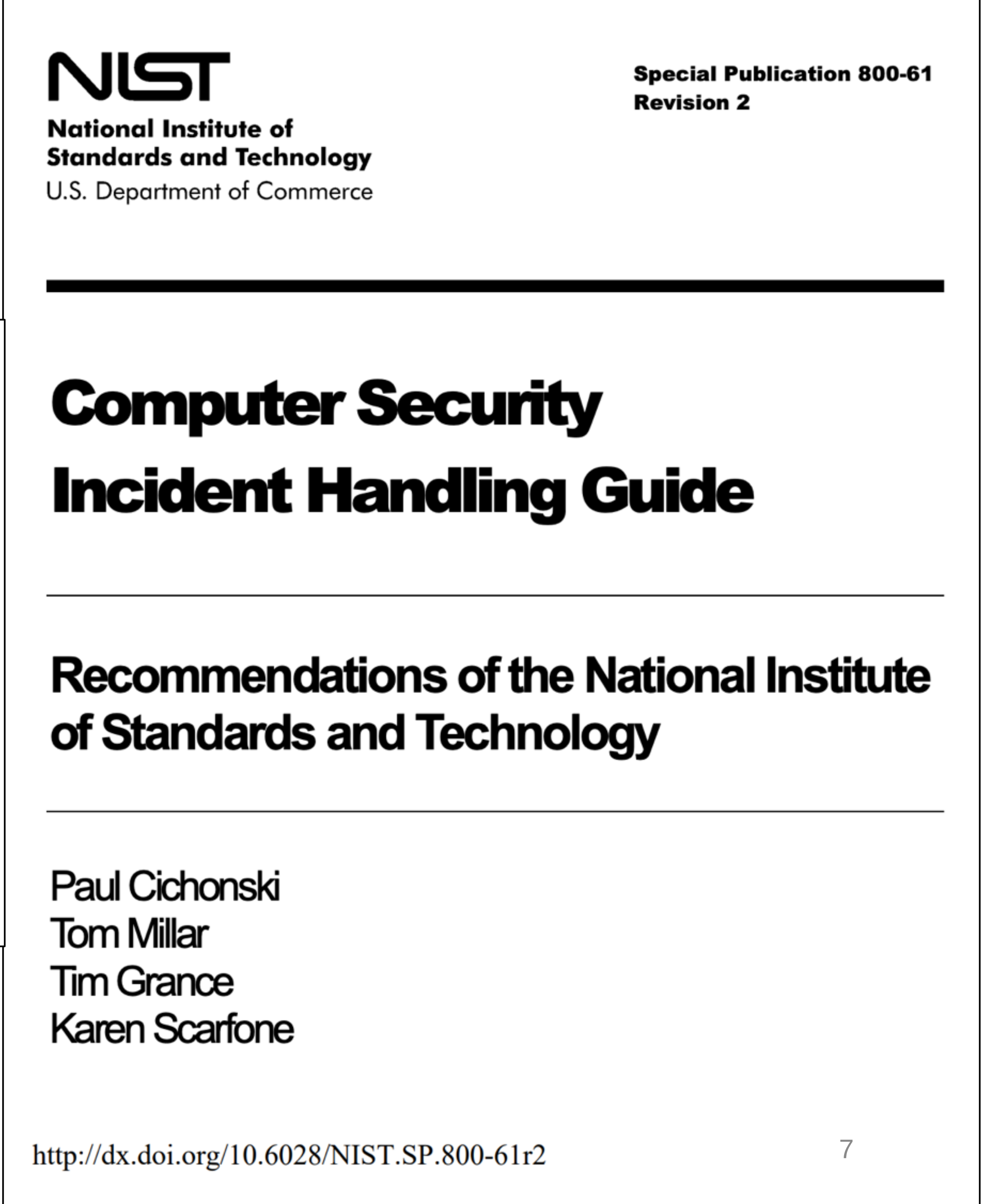


Figure 3-1. Incident Response Life Cycle


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

## Computer Security Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

X.1060 Cyber Defence Centre

# ITU-T X.1060 Cyber Defence Centre

# “Cyber Defence Centre“ in a Nutshell

- **CSIRT + SOC + Strategy = Cyber Defence Centre**
  - As cybersecurity threats evolves, you need a SOC to monitor, a CERT/CSIRT to protect your nation or business. On the top of that, you need an entity for  strategic planning, policy shaping and risk management. What we call “Cyber Defense Centre(CDC)”
- ITU-T standardize this concept as X.1060 in 2021.

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1060

(06/2021)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Information and network security – Security management

**Framework for the creation and operation of a cyber defence centre**

Recommendation ITU-T X.1060

# X.1060 and CDC help you by

- For Policy maker
  - Over the years of investment, many developed countries have, in effect, CDC functions inside government. Time to review your case.
  - Private sector needs policy assistance.
- For any CISO, CSO, CTO
  - X.1060 helps sketch a comprehensive vision of measures. As it lists services a CDC entity can offer. There are 64 different services in 9 different categories, as in the right.
- For CSIRT/SOC Manager
  - Make no mistake that CSIRTs/SOCs are the integral part of a CDC.
  - Compare your current situation with industry best practices to learn what needs to be improved.

- You can establish CDC entity by expanding capabilities and responsibilities of existing organization.

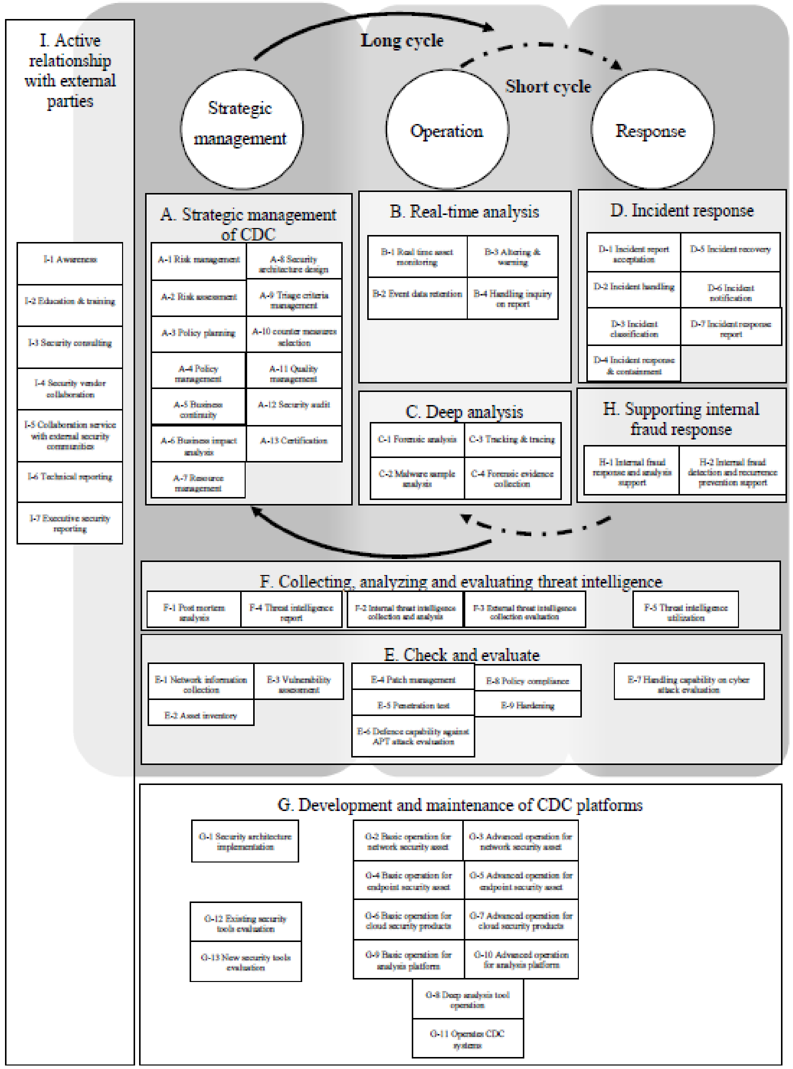

I. Active relationship with external parties
I-1 Awareness
I-2 Education & training
I-3 Security consulting
I-4 Security vendor collaboration
I-5 Collaboration service with external security communities
I-6 Technical reporting
I-7 Executive security reporting
Long cycle
Short cycle
Strategic management
Operation
Response
A. Strategic management of CDC
A-1 Risk management
A-2 Risk assessment
A-3 Policy planning
A-4 Policy management
A-5 Business continuity
A-6 Business impact analysis
A-7 Resource management
A-8 Security architecture design
A-9 Triage criteria management
A-10 counter measures selection
A-11 Quality management
A-12 Security audit
A-13 Certification
B. Real-time analysis
B-1 Real time asset monitoring
B-2 Event data retention
B-3 Alerting & warning
B-4 Handling inquiry on report
D. Incident response
D-1 Incident report acceptation
D-2 Incident handling
D-3 Incident classification
D-4 Incident response & containment
D-5 Incident recovery
D-6 Incident notification
D-7 Incident response report
C. Deep analysis
C-1 Forensic analysis
C-2 Malware sample analysis
C-3 Tracking & tracing
C-4 Forensic evidence collection
H. Supporting internal fraud response
H-1 Internal fraud response and analysis support
H-2 Internal fraud detection and recurrence prevention support
F. Collecting, analyzing and evaluating threat intelligence
F-1 Post mortem analysis
F-4 Threat intelligence report
F-2 Internal threat intelligence collection and analysis
F-3 External threat intelligence collection evaluation
F-5 Threat intelligence utilization
E. Check and evaluate
E-1 Network information collection
E-2 Asset inventory
E-3 Vulnerability assessment
E-4 Patch management
E-5 Penetration test
E-6 Defence capability against APT attack evaluation
E-8 Policy compliance
E-9 Hardening
E-7 Handling capability on cyber attack evaluation
G. Development and maintenance of CDC platforms
G-1 Security architecture implementation
G-12 Existing security tools evaluation
G-13 New security tools evaluation
G-2 Basic operation for network security asset
G-3 Advanced operation for network security asset
G-4 Basic operation for endpoint security asset
G-5 Advanced operation for endpoint security asset
G-6 Basic operation for cloud security products
G-7 Advanced operation for cloud security products
G-9 Basic operation for analysis platform
G-10 Advanced operation for analysis platform
G-8 Deep analysis tool operation
G-11 Operate CDC systems

*Figure 8 - CDC service categories*

# CDC service list

| | |
|---|---|
| **A** | **Strategic management of CDC** |
| A-1 | Risk management |
| A-2 | Risk assessment |
| A-3 | Policy planning |
| A-4 | Policy management |
| A-5 | Business continuity |
| A-6 | Business impact analysis |
| A-7 | Resource management |
| A-8 | Security architecture design |
| A-9 | Triage criteria management |
| A-10 | Counter measures selection |
| A-11 | Quality management |
| A-12 | Security audit |
| A-13 | Certification |
| **B** | **Real-time analysis** |
| B-1 | Real-time asset monitoring |
| B-2 | Event data retention |
| B-3 | Alerting & warning |
| B-4 | Handling inquiry on report |
| **C** | **Deep analysis** |
| C-1 | Forensic analysis |
| C-2 | Malware sample analysis |
| C-3 | Tracking & tracing |
| C-4 | Forensic evidence collection |
| **D** | **Incident response** |
| D-1 | Incident report acceptation |
| D-2 | Incident handling |
| D-3 | Incident classification |
| D-4 | Incident response & containment |
| D-5 | Incident recovery |
| D-6 | Incident notification |
| D-7 | Incident response report |
| **E** | **Check and evaluate** |
| E-1 | Network information collection |
| E-2 | Asset inventory |
| E-3 | Vulnerability assessment |
| E-4 | Patch management |
| E-5 | Penetration test |
| E-6 | Defence capability against APT attack evaluation |
| E-7 | Handling capability on cyber attack evaluation |
| E-8 | Policy compliance |
| E-9 | Hardening |
| **F** | **Collecting, analyzing and evaluating threat intelligence** |
| F-1 | Post mortem analysis |
| F-2 | Internal threat intelligence collection and analysis |
| F-3 | External threat intelligence collection and evaluation |
| F-4 | Threat intelligence report |
| F-5 | Threat intelligence utilization |
| **G** | **Development and maintenance of CDC platforms** |
| G-1 | Security architecture implementation |
| G-2 | Basic operation for network security asset |
| G-3 | Advanced operation for network security asset |
| G-4 | Basic operation for endpoint security asset |
| G-5 | Advanced operation for endpoint security asset |
| G-6 | Basic operation for cloud security products |
| G-7 | Advanced operation for cloud security products |
| G-8 | Deep analysis tool operation |
| G-9 | Basic operation for analysis platform |
| G-10 | Advanced operation for analysis platform |
| G-11 | Operates CDC systems |
| G-12 | Existing security tools evaluation |
| G-13 | New security tools evaluation |
| **H** | **Supporting internal fraud response** |
| H-1 | Internal fraud response and analysis support |
| H-2 | Internal fraud detection and reoccurrence prevention support |
| **I** | **Active relationship with external parties** |
| I-1 | Awareness |
| I-2 | Education & training |
| I-3 | Security consulting |
| I-4 | Security vendor collaboration |
| I-5 | Collaboration service with external security communities |
| I-6 | Technical reporting |
| I-7 | Executive security reporting |

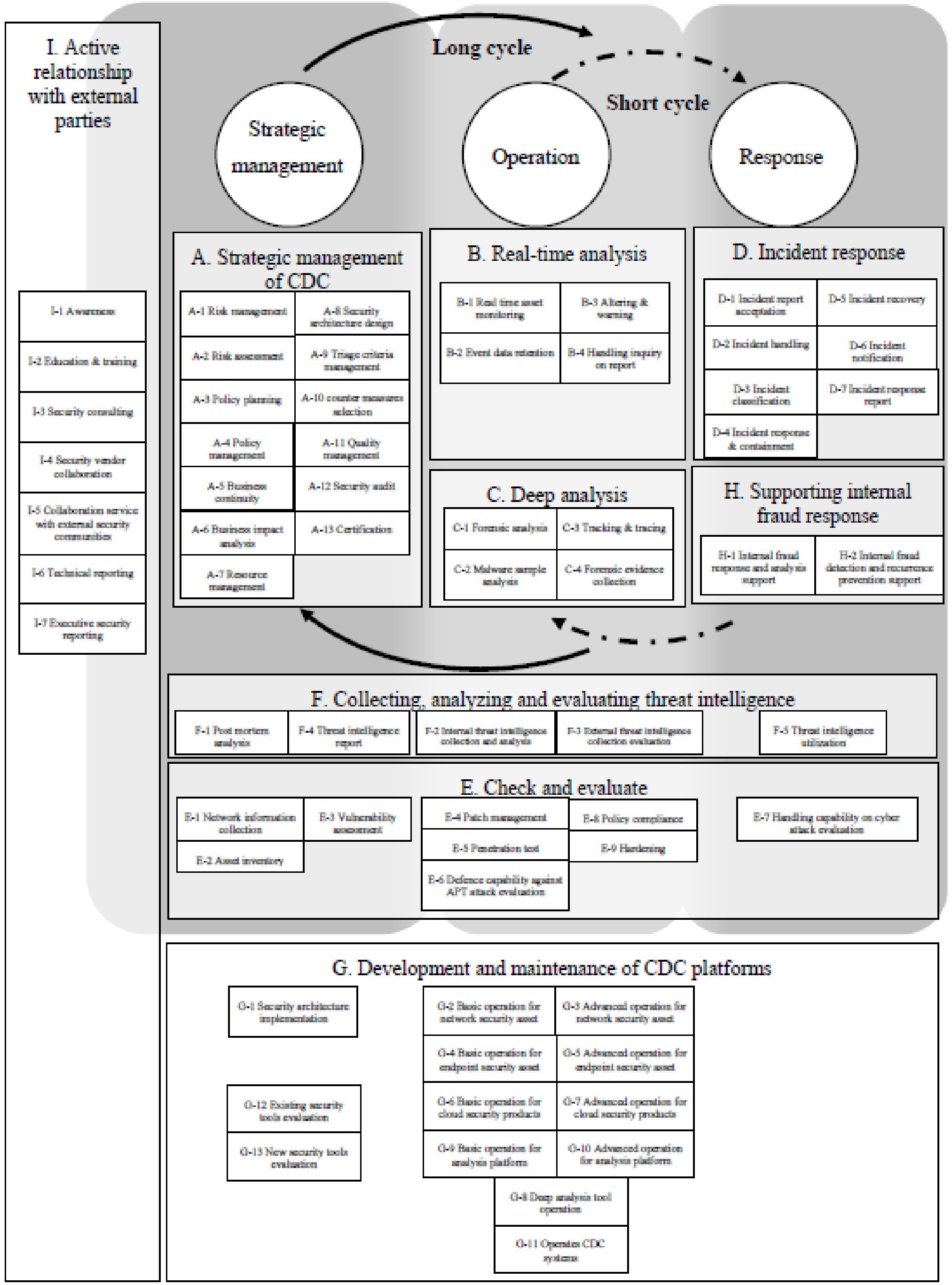

I. Active relationship with external parties
I-1 Awareness
I-2 Education & training
I-3 Security consulting
I-4 Security vendor collaboration
I-5 Collaboration service with external security communities
I-6 Technical reporting
I-7 Executive security reporting
Long cycle
Short cycle
Strategic management
Operation
Response
A. Strategic management of CDC
A-1 Risk management
A-8 Security architecture design
A-2 Risk assessment
A-9 Triage criteria management
A-3 Policy planning
A-10 counter measures selection
A-4 Policy management
A-11 Quality management
A-5 Business continuity
A-12 Security audit
A-6 Business impact analysis
A-13 Certification
A-7 Resource management
B. Real-time analysis
B-1 Real time asset monitoring
B-3 Alerting & warning
B-2 Event data retention
B-4 Handling inquiry on report
D. Incident response
D-1 Incident report acceptation
D-5 Incident recovery
D-2 Incident handling
D-6 Incident notification
D-3 Incident classification
D-7 Incident response report
D-4 Incident response & containment
C. Deep analysis
C-1 Forensic analysis
C-3 Tracking & tracing
C-2 Malware sample analysis
C-4 Forensic evidence collection
H. Supporting internal fraud response
H-1 Internal fraud response and analysis support
H-2 Internal fraud detection and recurrence prevention support
F. Collecting, analyzing and evaluating threat intelligence
F-1 Post mortem analysis
F-4 Threat intelligence report
F-2 Internal threat intelligence collection and analysis
F-3 External threat intelligence collection evaluation
F-5 Threat intelligence utilization
E. Check and evaluate
E-1 Network information collection
E-3 Vulnerability assessment
E-2 Asset inventory
E-4 Patch management
E-5 Penetration test
E-6 Defence capability against APT attack evaluation
E-8 Policy compliance
E-9 Hardening
E-7 Handling capability on cyber attack evaluation
G. Development and maintenance of CDC platforms
G-1 Security architecture implementation
G-2 Basic operation for network security asset
G-3 Advanced operation for network security asset
G-4 Basic operation for endpoint security asset
G-5 Advanced operation for endpoint security asset
G-6 Basic operation for cloud security products
G-7 Advanced operation for cloud security products
G-9 Basic operation for analysis platform
G-10 Advanced operation for analysis platform
G-12 Existing security tools evaluation
G-13 New security tools evaluation
G-8 Deep analysis tool operation
G-11 Operates CDC systems

*Figure 8 - CDC service categories*

## Frameworks

ITU-T X.1060 Cyber Defence Center

- https://www.itu.int/rec/T-REC-X.1060-202106-I

SP800-61 rev2

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

FIRST CSIRT Service Framework

- https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

FIRST PSIRT Framework

- https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

SIM3 by Open CSIRT Foundation

- https://opencsirt.org/csirt-maturity/sim3-and-references/

## Training Materials

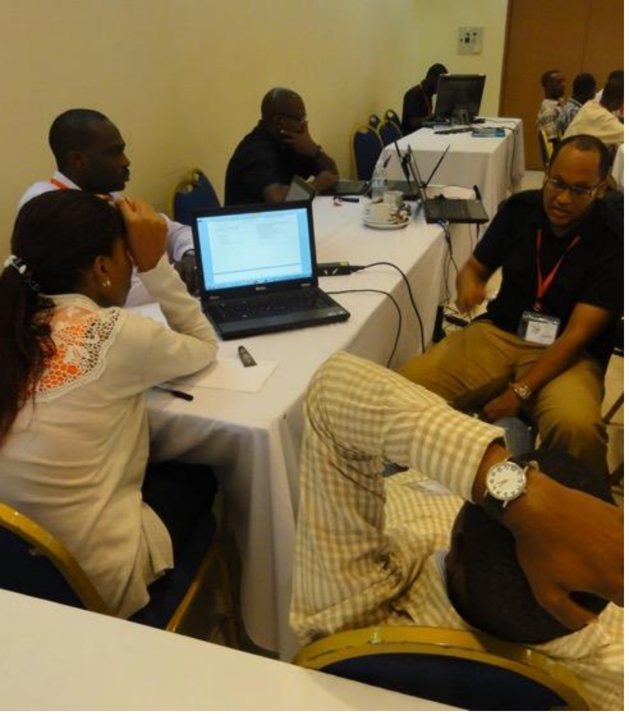
FIRST Materials

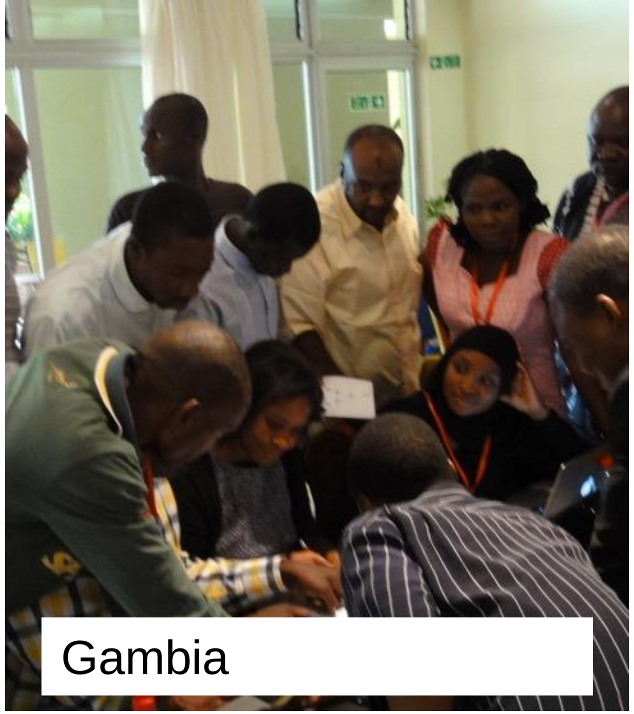
- https://www.first.org/education/trainings

Introduction to Cyber Security by APNIC Academy

- https://academy.apnic.net/en/course/introduction-to-cybersecurity

# Your resources





Gambia

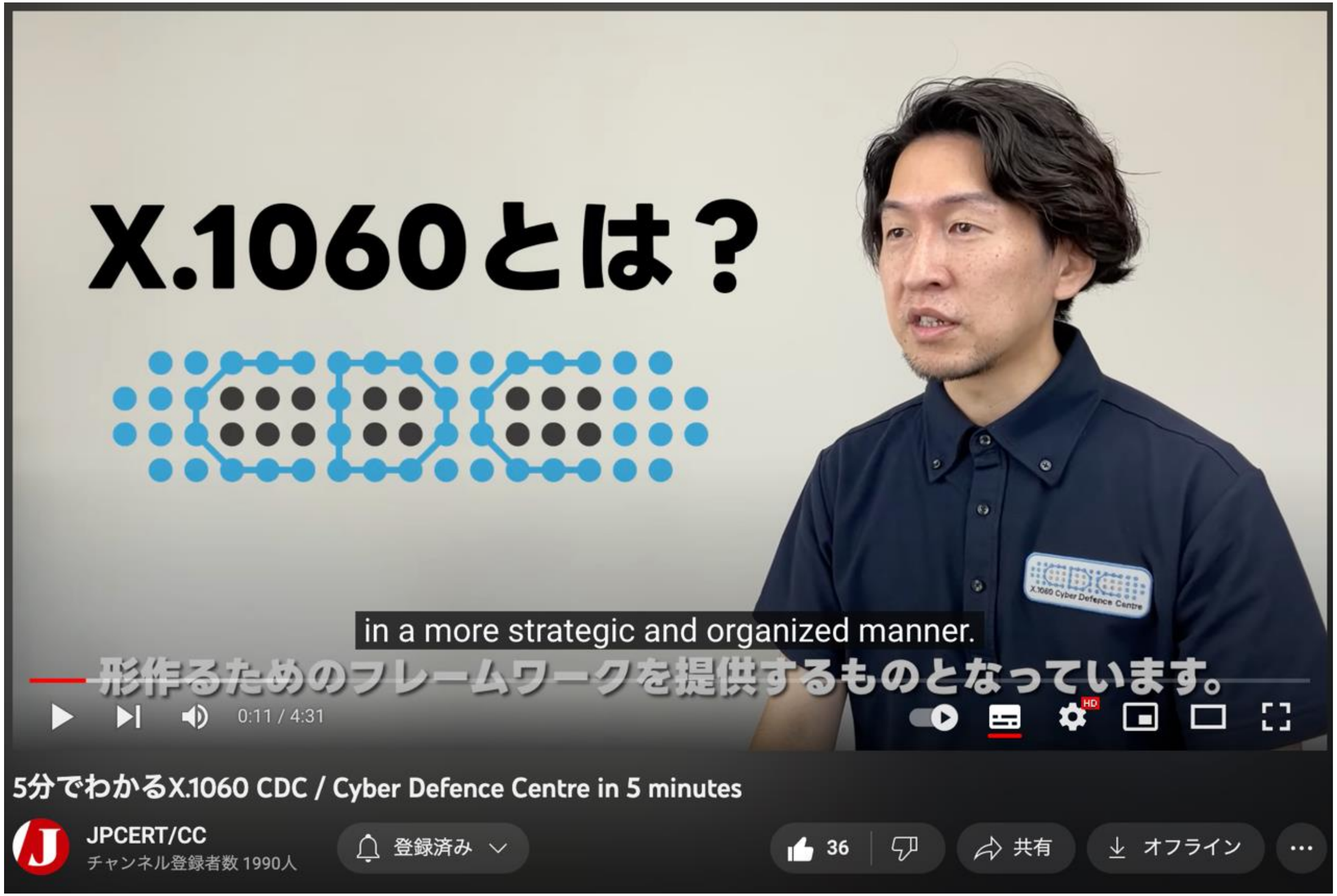
Lusaka, Zambia

Johannesburg, 2010

Yaunde, Cameroon

Framework is a map

# Another co-editor explain the value of X.1060 on YouTube



in a more strategic and organized manner.

形作るためのフレームワークを提供するものとなっています。

5分でわかるX.1060 CDC / Cyber Defence Centre in 5 minutes

AfricaCERT
United in promoting cyber security in Africa

FIRST

REGIONAL SYMPOSIUM
FEB 28 - MAR 3, 2023 | KIGALI, RWANDA

# Thank you!
# Appreciate your feedback to this workshop on Google form.

CO-HOST

National Cyber
Security Authority