ITU-T X.1060

CDC FOR AFRICA

SG17 Q3

ITU-T SG17 Question 3 Rapporteur
X.1060 Editors
Our Journey Today
A very simplified story – Few words about me just for context + I am colorblind

What is ITU-T X.1060 and Cyber Defence Center (CDC)?
Where does it come from?
Why and why now?
What is it?

How will African nations/countries implement?
The ”German” way!

Key outcomes from SG17?
A VERY good meeting!

Arnaud Taddei – Broadcom Software Group – Symantec Enterprise Division
- Global Security Strategist
- Techno-Diplomat on the UK Delegation
- Leadership positions in Standard Organizations
  - SG17 Vice Chairman, TSAG associate Rapporteur RG-IEM for Emerging tech
  - Standardization Maturity level: “teenager”

I am not here for that today

<table>
<thead>
<tr>
<th>baby</th>
<th>kid</th>
<th>teenager</th>
<th>adult</th>
<th>senior</th>
<th>red</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td>30</td>
<td>40</td>
</tr>
</tbody>
</table>

Nb Years in Standardization
WHY USING X.1060?
Common language

- Widely common language for cybersecurity and available to everyone.
- Codifying the services and listing whole security services as best practices.
CDC = Broader concept that embraces the existing organizations

- CDC implies new concept
- But it does not mean a new organization - it may be performed by the existing functions
- A CDC is existing, if the services in X.1060 are provided and the related organizations works together
- CDC is rather broader concept than CSIRTs or SOCs - CDC includes them as a part of the services
- The concept of CDC become so important as an organization to counter broader impacts that are not limited to information systems, caused by cyber incidents
Process to the CDC

1. Risk management process (include cybersecurity)

2. Prioritize those risks (include cybersecurity)

3. CISO decide to organize the CDC

4. Reference the X.1060 as a framework
CDC provides security services which counter business risks.

- Cybersecurity is considered as a one of the important business risk.
- In order to deal with the risk of cybersecurity, it is necessary to provide not only the existing SOC and CSIRT/CERT/CIRT services but also a wide range of security services.
Teams assigned security services are sometimes called “SOC” or “CSIRT”.

- If the organization already has a ”SOC” or “CSIRT” and implements CDC services, we can think of it as implementing part of CDC.
ITU-T X.1060 OVERVIEW
WHAT IS CDC?
X.1060

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

■ Scope
  - *X.1060 provides a framework for organizations to build and manage a Cyber Defence Centre (CDC), and to evaluate its effectiveness. The framework indicates how the CDC should define and implement security services to enable an organization’s security.*

  - *This Recommendation is intended for those who is responsible for security at the top management level of an organization, such as Chief Security Officer (CSO) and/or Chief Information Security Officer (CISO), and security supervisors who assist the CSO and/or CISO.*
What is “Cyber Defence Centre (CDC)”?

■ Definition

- **CDC is an entity within an organization that offers security services to manage the cybersecurity risks of its business activities**

*Figure 1 – Stakeholders and their roles for CDC operation*
CDC in the organization

CxOs commit their business objectives.

CISO defines and controls security policies to manage cyber risks.

CDC is empowered by CISO to define and implement CDC services for enabling security policies.

CDC assigns resources to activate security functions which compose CDC services.
CDC is an entity, and the structures and names of organizations vary.

- It is not the purpose to build a division or unit with the name “CDC”. It is up to each organization to name the entity.
- Depending on how security services have been implemented, the form and name of the CDC is vary among organizations.
X.1060 provides only a framework.

- X.1060 is only framework for the creation and operation of the CDC.
- It is necessary to utilize various existing documents in order to implement CDC services which is actually implemented in the organization.
Out of scope of X.1060

- Using any guidelines and documents for complement and specify X.1060.

CxOs to do: for business risk, for cybersecurity risk

CISO to do: for security policies, for strategies

Specific design: for design specific CDC organization

How to implement in teams: for procedures for techniques for controls
FRAMEWORK FOR THE CREATION AND OPERATION OF A CYBER DEFENCE CENTRE
The framework

- Three processes to maintain security activities
- Build – Management - Evaluation

![Diagram showing the framework with processes and phases]

*Figure 2 - Framework for the creation and operation of CDC*
Build Process

**Process**

- CDC service list
- Organization specific CDC service catalogue
- Organization specific CDC service profile

**Output**

<table>
<thead>
<tr>
<th>Service</th>
<th>Recommendation level</th>
<th>Service assignment</th>
<th>Service score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service ex.1</td>
<td>Basic</td>
<td>Insourcing (AB dept.)</td>
<td>3</td>
</tr>
<tr>
<td>Service ex.2</td>
<td>Standard</td>
<td>Outsourcing (Z-MSSP)</td>
<td>2</td>
</tr>
<tr>
<td>Service ex.3</td>
<td>Advanced</td>
<td>Unassignable</td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 3 - Phases to build services for CDC**
## CDC service category

<table>
<thead>
<tr>
<th>Service category</th>
<th>Number of services</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Strategic management of CDC</td>
<td>13</td>
</tr>
<tr>
<td>B Real-time analysis</td>
<td>4</td>
</tr>
<tr>
<td>C Deep analysis</td>
<td>4</td>
</tr>
<tr>
<td>D Incident response</td>
<td>7</td>
</tr>
<tr>
<td>E Check and evaluate</td>
<td>9</td>
</tr>
<tr>
<td>F Collection, analyzing and evaluating threat intelligence</td>
<td>5</td>
</tr>
<tr>
<td>G Development and maintenance of CDC platforms</td>
<td>13</td>
</tr>
<tr>
<td>H Supporting internal fraud response</td>
<td>2</td>
</tr>
<tr>
<td>I Active relationship with external parties</td>
<td>7</td>
</tr>
</tbody>
</table>
### CDC service list

<table>
<thead>
<tr>
<th>A</th>
<th>Strategic management of CDC</th>
<th>F</th>
<th>Collecting, analyzing and evaluating threat intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>A-1</td>
<td>Risk management</td>
<td>F-1</td>
<td>Post mortem analysis</td>
</tr>
<tr>
<td>A-2</td>
<td>Risk assessment</td>
<td>F-2</td>
<td>Internal threat intelligence collection and analysis</td>
</tr>
<tr>
<td>A-3</td>
<td>Policy planning</td>
<td>F-3</td>
<td>External threat intelligence collection and evaluation</td>
</tr>
<tr>
<td>A-4</td>
<td>Policy management</td>
<td>F-4</td>
<td>Threat intelligence report</td>
</tr>
<tr>
<td>A-5</td>
<td>Business continuity</td>
<td>F-5</td>
<td>Threat intelligence utilization</td>
</tr>
<tr>
<td>A-6</td>
<td>Business impact analysis</td>
<td>G-1</td>
<td>Security architecture implementation</td>
</tr>
<tr>
<td>A-7</td>
<td>Resource management</td>
<td>G-2</td>
<td>Basic operation for network security asset</td>
</tr>
<tr>
<td>A-8</td>
<td>Security architecture design</td>
<td>G-3</td>
<td>Advanced operation for network security asset</td>
</tr>
<tr>
<td>A-9</td>
<td>Triage criteria management</td>
<td>G-4</td>
<td>Basic operation for endpoint security asset</td>
</tr>
<tr>
<td>A-10</td>
<td>Counter measures selection</td>
<td>G-5</td>
<td>Advanced operation for endpoint security asset</td>
</tr>
<tr>
<td>A-11</td>
<td>Quality management</td>
<td>G-6</td>
<td>Basic operation for cloud security products</td>
</tr>
<tr>
<td>A-12</td>
<td>Security audit</td>
<td>G-7</td>
<td>Advanced operation for cloud security products</td>
</tr>
<tr>
<td>A-13</td>
<td>Certification</td>
<td>G-8</td>
<td>Deep analysis tool operation</td>
</tr>
<tr>
<td>B</td>
<td>Real-time analysis</td>
<td>G-9</td>
<td>Basic operation for analysis platform</td>
</tr>
<tr>
<td>B-1</td>
<td>Real-time asset monitoring</td>
<td>G-10</td>
<td>Advanced operation for analysis platform</td>
</tr>
<tr>
<td>B-2</td>
<td>Event data retention</td>
<td>G-11</td>
<td>Operates CDC systems</td>
</tr>
<tr>
<td>B-3</td>
<td>Alerting &amp; warning</td>
<td>G-12</td>
<td>Existing security tools evaluation</td>
</tr>
<tr>
<td>B-4</td>
<td>Handling inquiry on report</td>
<td>G-13</td>
<td>New security tools evaluation</td>
</tr>
<tr>
<td>C</td>
<td>Deep analysis</td>
<td>H-1</td>
<td>Internal fraud response and analysis support</td>
</tr>
<tr>
<td>C-1</td>
<td>Forensic analysis</td>
<td>H-2</td>
<td>Internal fraud detection and reoccurrence prevention support</td>
</tr>
<tr>
<td>C-2</td>
<td>Malware sample analysis</td>
<td>I-1</td>
<td>Awareness</td>
</tr>
<tr>
<td>C-3</td>
<td>Tracking &amp; tracing</td>
<td>I-2</td>
<td>Education &amp; training</td>
</tr>
<tr>
<td>C-4</td>
<td>Forensic evidence collection</td>
<td>I-3</td>
<td>Security consulting</td>
</tr>
<tr>
<td>D</td>
<td>Incident response</td>
<td>I-4</td>
<td>Security vendor collaboration</td>
</tr>
<tr>
<td>D-1</td>
<td>Incident report acceptance</td>
<td>I-5</td>
<td>Collaboration service with external security communities</td>
</tr>
<tr>
<td>D-2</td>
<td>Incident handling</td>
<td>I-6</td>
<td>Technical reporting</td>
</tr>
<tr>
<td>D-3</td>
<td>Incident classification</td>
<td>I-7</td>
<td>Executive security reporting</td>
</tr>
<tr>
<td>D-4</td>
<td>Incident response &amp; containment</td>
<td>I-8</td>
<td></td>
</tr>
<tr>
<td>D-5</td>
<td>Incident recovery</td>
<td>I-9</td>
<td></td>
</tr>
<tr>
<td>D-6</td>
<td>Incident notification</td>
<td>I-10</td>
<td></td>
</tr>
<tr>
<td>D-7</td>
<td>Incident response report</td>
<td>I-11</td>
<td></td>
</tr>
<tr>
<td>E</td>
<td>Check and evaluate</td>
<td>I-12</td>
<td></td>
</tr>
<tr>
<td>E-1</td>
<td>Network information collection</td>
<td>I-13</td>
<td></td>
</tr>
<tr>
<td>E-2</td>
<td>Asset inventory</td>
<td>I-14</td>
<td></td>
</tr>
<tr>
<td>E-3</td>
<td>Vulnerability assessment</td>
<td>I-15</td>
<td></td>
</tr>
<tr>
<td>E-4</td>
<td>Patch management</td>
<td>I-16</td>
<td></td>
</tr>
<tr>
<td>E-5</td>
<td>Penetration test</td>
<td>I-17</td>
<td></td>
</tr>
<tr>
<td>E-6</td>
<td>Defence capability against APT attack evaluation</td>
<td>I-18</td>
<td></td>
</tr>
<tr>
<td>E-7</td>
<td>Handling capability on cyber attack evaluation</td>
<td>I-19</td>
<td></td>
</tr>
<tr>
<td>E-8</td>
<td>Policy compliance</td>
<td>I-20</td>
<td></td>
</tr>
<tr>
<td>E-9</td>
<td>Hardening</td>
<td>I-21</td>
<td></td>
</tr>
</tbody>
</table>

### 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

### Supporting internal fraud response

- **H-1**: Internal fraud response and analysis support
- **H-2**: Internal fraud detection and reoccurrence prevention support

### 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
HOW CAN AFRICAN NATIONS IMPLEMENT CDC
Before anything!
“Leadership The German Way”

- You build the story for the decision makers!
- And it doesn’t start by the word assessment!
- This is a LEADERSHIP ACT
- And it starts with the Story
- STORY =

  NARRATIVE
  +

  BACK TO BACK AGREEMENTS WITH THE CONSTITUENCIES THAT CAN CONTRIBUTE TO THE NARRATIVE!
What is at stake at organizations level?

- Organizations = not only government! Think your private sector!
- The intention of the CDC framework is to provide a common language to elevate the bar of the security services organization
- This is an answer to several issues
  - Lack of a formal normative common language
  - Lack of executive understanding and engagement
  - SOC and others are too operational and not enough business level
  - Fractalization of organizations

The Narrative is a TRANSFORMATION Narrative
“CDC is about elevating and harmonizing our security services portfolio to better answer our business needs”

The ‘astuce’ is that X.1060 is ‘external’ to the organization so it blocks internal politicking
What is at stake at regional level: AFRICA

- If tomorrow a new Wannacry explodes
  - *and the world got VERY LUCKY with Wannacry it could have been MUCH worse*
- Today what are the chances that all African countries are able to engage ALL the services capabilities of ALL their constituencies across the continent?
  - *National entities, private sector, foreign private sector, service providers, etc.*
  - *
- Like in any place in the world probably very complicated
- CDC for Africa is a common language to give a minimal first condition to allow one aspect of a truly joint regional answer

The narrative is a REGIONAL HARMONISATION narrative
“CDC sets a common foundation and language at the right level of all our organization to improve collaboration, cooperation and the continent resiliency”
How to create? Build Process

Making the catalogue

Making the profiles

Making the portfolio
How to manage? Management Process

3 Phases
- Strategic management
- Operations
- Response

2 Cycles
- Short
- Long
Mapping service categories and “Management process”.

I. Active relationship with external parties

A. Strategic management of CDC

B. Real-time analysis

C. Deep analysis

D. Incident response

H. Support of internal fraud response

E. Collection, analysis and evaluation of threat intelligence

F. Checking and evaluation

G. Development and maintenance of CDC platforms
OUTCOME FROM SG17 MEETING
What happened

- Q3/17 met and reviewed 2 contributions for X.sup-cdc from editors
  - One concentrating on the base text and the tutorial
  - One concentrating on next steps
- A joint Q3/SG17AFR meeting
- Participation to SG17AFR meeting
- A great informal lunch with SG17AFR delegates (learnt a lot and fun)
- A very valuable CDC work-day on X.sup-cdc
Main outcomes

■ Key progress on the layout of X.sup-cdc + content
■ Great input from SG17AFR for the next questionnaire
■ A lot of enthusiasm
  – Need for a governance model
  – Need for an assessment model
  – Need for a certification approach
  – Need for detailed implementation (service templates, etc.)
■ But the bar of entry to go the next steps is contradicted by some other gaps elsewhere
The problem

- Provoking Statement
  - “There is no international agreed consensus of a security architecture since X.800 (1991)”
- We miss a context!
- SG17 worked hard since 5 years (CG-XSS, CG-SECAD, CG-WTSA-PREP, etc.)
  - This already changed the national cybersecurity of some countries
    - (incredible? But true!)
- Big important first success at WTSA20 in March 2022 on Resolution 50

---

Resolution 50 – Cybersecurity

5 to define a general/common set of security capabilities for each phase of information system/network/application lifecycles, so that consequently security by design (security capabilities and features available by design) could be achieved for systems/networks/applications from day one;

6 to design one or more security architecture reference frameworks with security functional components which could be considered as the basis of security architecture design for various systems/networks/applications in order to improve the quality of Recommendations on security,
The Quest for a new Context!
Current Candidate \(\rightarrow\) An OSI model for Security!

We are here on the map
If you layer the candidate model (looks more and more like an OSI model)

<table>
<thead>
<tr>
<th>People and Processes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td></td>
</tr>
<tr>
<td>Endogen Stack</td>
<td>Exogen Stack</td>
</tr>
<tr>
<td>Universal Capabilities</td>
<td></td>
</tr>
</tbody>
</table>
# Mapping CDC

<table>
<thead>
<tr>
<th>People and Processes</th>
<th>SG17: X.1060</th>
<th>SG17: X.sup-cdc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>OASIS: CACAO</td>
<td></td>
</tr>
<tr>
<td>Endogen Stack</td>
<td>SG17: TR.smpl</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SG17: X.security</td>
<td>OASIS: OpenC2</td>
</tr>
<tr>
<td>Universal Capabilities</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terms, Definitions, Design</td>
<td>SG17: X.arch-design</td>
<td></td>
</tr>
<tr>
<td>Principles, Architecture</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Methodology, etc.</td>
<td>SG17: X.800</td>
<td></td>
</tr>
</tbody>
</table>
A service template shows a LOT of dependencies to the context
And a lot of gaps
My asks

- Give feedback – Nothing is perfect!
- Join the effort
- Bring contributions to the next SG17 meeting end of August
- Need contributions on the detailed description of some or all of your services
  - *do not share data you cannot share of course*
  - *Do not even try to map to CDC, just describe in your words what you have*
    - Title, Description, SLA
    - Input to the service (tools, data, etc.)
    - Output to the service (playbooks, policy suggestions, remediation, responses, etc.)
    - Dependencies (service X depends on service Y, service A inputs to service B)
    - List of security capabilities needed
    - Etc.
Thank you

X.1060 Editors
Mr. Arnaud TADDEI
Mr. Shigenori TAKEI
Mr. Shinji ABE

Q3/17 Rapporteur
Ms. Miho NAGANUMA

Broadcom Inc.
NTT Corporation
NEC Corporation