National Communications Authority (NCA)

Somalia Computer Emergency Response Team (SomCERT)

SomCERT GUIDELINES

2021

1. SomCERT Guidelines

1.1. Guidelines on SomCERT Services

a) **Incident Response** – Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats; uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security.

b) **Actionable Security Intelligence** - is the real-time collection, normalization, and analysis of the data generated by users, applications and infrastructure that impacts the IT security and risk posture of an enterprise. The goal of Security Intelligence is to provide actionable and comprehensive insight that reduces risk and operational effort for any size organization.

c) **Signal Intelligence** – Intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems.

d) **Early Warning System** – Cyber-attack warning system can be a powerful tool as an early warning system for related attacks, both physical and virtual. A common technique now being used by attackers is to use a denial of service attack as a distraction while another more sinister attack actually takes place.

e) **ICT Equipment Testing Lab** – A local test laboratory contributes to the development of the national industry by providing inputs that enable projects validation and improvement. In addition, a test laboratory promotes the growth of knowledge and supports the regulatory agencies in the certification process.

f) **Web Intelligence (WEBINT)** - exploits Artificial Intelligence (AI) and advanced information technology on the Web and Internet. It is the key and the most urgent research field of IT for business intelligence. WEBINT is a means to efficiently identify the intelligence available in open source (OSINT). Structuring and visualizing web- based information allows an analyst to surface tactical information like technical indicators, and strategic understandings like the swaying sentiment of a troubled region.

1.2. Orientation and Preparation of SOMCERT Personnel Guideline

This section establishes the guidelines that shall prepare the personnel tasked and assigned to manage and handle responses on information security incident or event. It will provide ample preparation for each person with specific roles to play and provide direction for other members of the team for implementing the SOMCERT.

a) Personnel assigned as the initial POC shall include:

1. Familiarity with the forms that are used for first and second assessment.
2. Familiarity with the different classification and taxonomy used for incident response.
3. Familiarity with the key processes of incident response.
4. Familiarity with the flowchart of handling the incident response.
5. Familiarity with the protocols when communicating and endorsing information collected and compiled for second assessment to members of the SOMCERT.
6. Importance of proper logging and recording of the event, e.g. accuracy of time stamping, source of event, person reporting, etc.
7. Importance of updating and recording of events into the database system for information security including recording of data on “false alarms” for future references.
8. Importance of the time to take to log the report for first assessment will also affect the ability of the SOMCERT to respond effectively.

b) Orientation for personnel assigned to the SOMCERT and tasked to respond to incidents or events detected or reported after the initial POC shall include:

1. Familiarity with the forms that are used for first and second assessment;
2. Familiarity with the different classification and taxonomy used for incident response;
3. Familiarity with the key processes of SOMCERT.
4. Familiarity with the flowchart of handling incident response.
5. Familiarity with the communication protocols after event evaluation and early impact assessment has been conducted and endorsed to the SOMCERT for escalation for further assessment and/or decisions that are required.

6. Importance of correct and appropriate logging of record and data for later analysis.
7. Importance of updating the information security event or incident database.

c) Orientation of personnel assigned with the responsibility of managing the SOMCERT shall include:

1. Implementation of a regular monitoring system to track and monitor all reported incidents and events.
2. Review procedure for evaluating applicability of the SOMCERT.
3. Treatment and handling procedures for internal security breach protocols.
4. Training program requirement for continuous development and capability building for personnel.
5. Communication plans with other stakeholders.
6. Escalation processes and procedures.
7. Activation procedures for crisis management.

4.1. Reporting and Submitting Incident Reports Guideline

As we know, Time is an important factor that will determine the ability of the SOMCERT to respond to any reported event. Providing initial information about an information security event and determining the information security incident will prompt the appropriate people to respond according to the situation and urgency of the response requirement.

1. If the person suspects an information security event is in progress or may have occurred with particular emphasis on events which may cause substantial loss or damage to the organization, report should be completed and submitted immediately.
2. The information provided shall be used to initiate appropriate assessment which will determine whether the event is to be categorized as an information security incident or not and if remedial measures are necessary to prevent or limit any loss or damage.
3. If the person reviewing the already completed or partly completed form is assigned to analyze the reports, the event needs to be categorized whether it is an information security incident or a false alarm.
4. If the person reviewing the information security event and incident forms is a member of the SOMCERT, then the incident form should be updated as the investigation progresses

and related updates made to the information security event/incident database.

5. As much as possible, the form should be completed and submitted electronically, including when it is thought possible that the system is under attack and reporting forms can be read by unauthorized people only, then alternative means of reporting should be used:
    - ❖ Alternative means or forms of reporting include in person, by telephone, by text messaging or by facsimile.
    - ❖ Provide information that are only factual and avoid speculating in order to complete the fields within a specified time period, where it is appropriate to provide information that cannot be confirmed, state clearly the information that is unconfirmed and annotation of information that may lead to what may be true.
    - ❖ Always provide full contact details when submitting the completed form. There may be a necessity to contact the person who filed the report either very soon or at a later date to obtain further information concerning the report.
    - ❖ Information that were provided during the report discovered to be inaccurate, incomplete or misleading at a later date are amended and resubmitted to update the record and log the correct information into the database.
    - ❖ Closure of report will update the database or if the event has not been fully resolved and tagged as open, the record are still updated.

1.3. Handling Incident Response Guidelines

This section will cover the guidelines for handling responses on information security incident or event. It provides direction in determining whether the information security events become information security incidents. When an occurrence of an information security event is detected and reported by (human or automatic means), the event will initiate series of phases and stages prompting the SOMCERT to respond accordingly.

a) Detection Reporting

1. Incident events detected and reported either by human or automated feed shall be immediately logged into the information security incident monitoring and tracking system.
2. Reported incident or detected event shall be communicated immediately to the SOMCERT.

3. Communicated reports shall be logged immediately to update records.
4. Always update the system with changes or responses made associated with the incident report ticket number.

b) Assessment Decision

1. Information gathered and collected are submitted to the SOMCERT.
2. False positive results from initial assessment shall also be logged into the system to track all reported events and incidents.
3. Team Leaders assigning caseloads to SOMCERT Analyst shall log and record incident report ticket number to update database.
4. Initial assessment that contains relevant information shall be assigned to SOMCERT Analyst for further analysis and evaluation.
5. Results from second assessment shall be recorded and logged into the system.
6. Communicate results for immediate response to SOMCERT members, technical support team, and other external support groups.
7. Terminate or close incident report ticket number by updating the system when cases are concluded as resolved.

c) Response

1. List of personnel tasked and assigned with specific role in SOMCERT shall be regularly updated and posted to message boards.
2. Immediate objectives for responding to incidents or events is to lower the level of vulnerability and impact.
    a. Adverse impact, risk levels and associated threats and vulnerabilities shall be immediately evaluated and assessed to initiate various controls and appropriate level of responses.
    b. Immediate response shall be documented accordingly.
    c. Reports shall be completed and filed immediately to update the system.
    d. First responders to the reported incident or event on breach of information security shall conduct appropriate turnover procedure.
    e. Log appropriate tagging of incident report, e.g. closed/open, resolved/unresolved.

f. Immediate responses to reported events and detected incidents shall be evaluated regularly to determine the effectiveness of these responses and improve the system of responding to any information security breach.

1.4. Collecting and Gathering Data Guidelines

This section establishes the guidelines for collecting and gathering data as to be initial and second assessment on reported and detected incidents and events and information for analysis that will direct the SOMCERT to respond accordingly.

1.4.1. Guidelines on Collecting and Gathering Data and Information for Analysis

1. Events or incidents that are detected and reported either by human or automated means shall be logged immediately and recorded appropriately into the system.
2. Information, after it has been collected, shall be classified according to information categories.
3. Reported incidents or events shall be classified according to its potential impact to the organization: limited adverse effect, serious adverse effect, or severe/catastrophic adverse effect.
4. These information shall be classified and rated based from its security objectives: Confidentiality, Integrity and Availability of Information.
5. Data or information shall also be evaluated according to the sources of threats which can occur on three levels: the organizational level, the mission or business process level, and the information level.
6. Information that has been collected shall be classified according to its type. This can be adversarial, accidental, structural or environmental in nature.
7. Once data or information is collected, it shall also tagged according to its characteristics and the range of its effect.
    I. Information collection and data gathering shall be complete and substantial to provide analyst ample /detail data to perform analysis which will initiate immediate response or prompt series of incident response activities;

II. Time stamping and recording of event is crucial. It is therefore very important for the person collecting data to determine the time the event or incident occurred or initially detected and reported.

III. Information that is classified as "false" positive shall be logged and recorded into the database as input for future analysis.

1.5. Guidelines on Acquiring New Information

The modern world thrives on information and it is the driving force that now fuels the society. It is crucial to many aspects of business and life of individuals and organizations and therefore should be managed well. This has also led to the evolution of using technology to store, process or transmit information through electronic means. This section will provide general guidelines when acquiring information to conduct forensic analysis done by the SOMCERT.

1.5.1. Guidelines for handling e-discovery

I. Adopt a process for reporting information relating to a probable threat of litigation to a responsible decision maker to assist in demonstrating reasonableness and good faith.

II. To determine scope of information that should be preserved, it should be factored into the process of decision making, the amount of information that should be preserved, the nature of the issues raised in the matter of information preservation, the accessibility of information, the probative value of information and the relative burdens and costs of preservation efforts.

III. Compliance with a legal hold should be regularly monitored.

IV. Any legal hold policy, procedure or practice should include provisions for releasing the hold upon the termination of the matter at issue so that the organization can adhere to polices for managing information through its useful lifecycle in the absence of legal a hold.