AFRICA CERT (AF-CERT) TRAINING MATERIAL

IMPORTANCE AND ROLE OF A CSIRT

Outline

- Definitions
- Roles and Responsibilities
- CSIRT Framework
- CSIRT Types and Environments
- CSIRT Services

Definitions..

- **Security Event**

  A security event is an occurrence in a system that is relevant to the security of the system. Such an occurrence is intended to impact on the the confidentiality, integrity or availability of an ICT system through an act that contravenes prescribed security policy.

- **Incident**

  A security incident is an event that impacts on the confidentiality, integrity or availability of an ICT system through an act that contravenes prescribed security policy.

- **Incident handling**

  This refers to the process of receiving incidents reports, evaluating these incident reports (analysis) and responding to incidents through support and coordination.

..Definitions..

- **Computer Security Incident Response Team (CSIRT)**
  - A team of IT security experts whose main business is to respond to computer security incidents affecting its constituents.
  - At a minimum, a CSIRT should provide incident response services to a defined constituency.

- Various abbreviations used for the same sort of teams include:

CERT	Computer Emergency Response Team - *as distinct from CERT, a registered trademark owned by Carnegie Mellon University*
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
CSIRC	Computer Security Incident Response Capability
CSRC	Computer Security Response Capability
IHT	Incident Handling Team
IRC	Incident Response Center/Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

..Definitions

- **Constituency**
  - Refers to the customer base of a CSIRT, the specific group of people and/or organizations that the CSIRT was established to serve
  - A CSIRTs constituency has access to services offered by the CSIRT.

- **Stakeholders**
  - Refers to those responsible for the strategy and direction of a CSIRT and/or have a responsibility for Information Security.
  - Have an interest in the success of the CSIRT and its mission.
  - Can be those who will report to the CSIRT, receive help from the CSIRT, provide funding and sponsorship to the CSIRT, or interface with the CSIRT through information sharing or the coordination of incident and vulnerability handling activities.

Roles & Responsibilities

- Having a dedicated IT security team helps an organisation to mitigate and prevent major incidents and helps to protect its valuable assets.

- The fundamental role of a CSIRT includes:
  - Centralizing coordination of IT security issues within the organisation (Point of Contact, PoC);
  - Providing for centralized and specialized handling of and response to IT incidents;
  - Providing the expertise at hand to support and assist the users to quickly recover from security incidents;
  - Dealing with legal issues and preserving evidence in the event of a lawsuit;
  - Keeping track of developments in the security field;
  - Stimulating cooperation within the constituency on IT security (awareness building).

CSIRT Framework..

- **Mission Statement**
  - The purpose of a mission statement is to communicate the purpose of the CSIRT
  - Should therefore be clearly and concisely defined, documented, adhered to and announced widely to the CSIRT constituency as well as to other CSIRTs.

- A CSIRT's mission statement should include references to the following:
  - Protecting and maintain the security
  - Coordinating incident response activities
  - Mitigating damage
  - Educating the constituency

..CSIRT Framework..

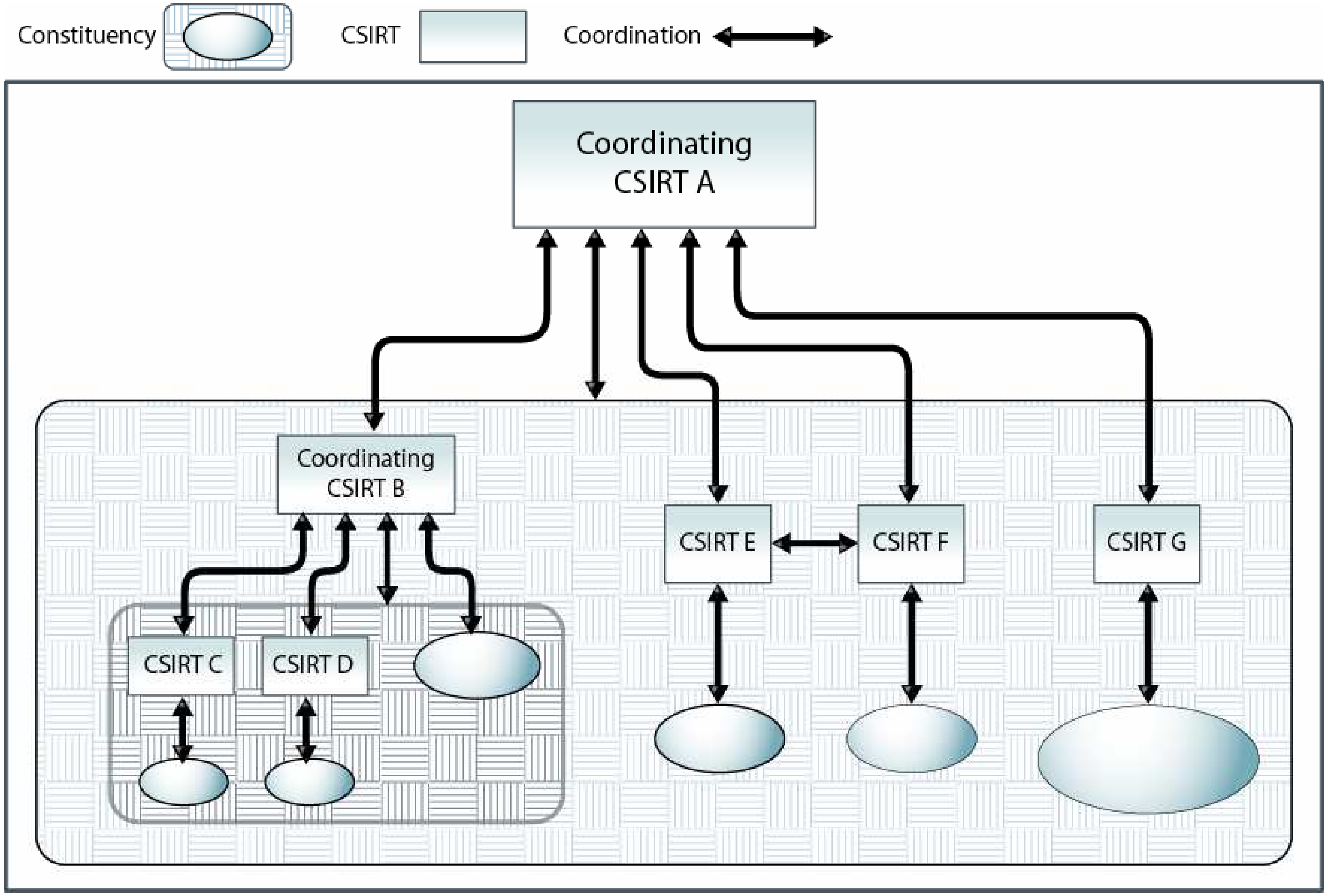
- **Constituency**
  - Refers to a specific group of people and/or organizations that the CSIRT was established to serve.
  - A CSIRTs constituency has access to services offered by the CSIRT.

- CSIRT Jurisdiction: A CSIRT can be:
  - *Unbounded* - the CSIRT will provide service to anyone requesting it
  - *Bound* by some constraints. Most commonly, CSIRTs have bounded constituencies that tend to be a reflection of the CSIRT funding source. The most common constraints that are used to bound a constituency include national, geographical, political (e.g., government departments), technical (e.g., use of a specific operating system), organizational (e.g., within a given corporation or company), network service provider (e.g., connection to a specific network), or contractual (e.g., the customers of a fee-for-service team).

..CSIRT Framework..

- **Place in organization**
  - Determined by the role the CSIRT plays in overall risk management in the context of its organizational environment and constituency.
  - In a commercial organizational setting, different groups in the same organization may have the responsibility for different aspects of risk management. Examples:
    - The network operations team responsible for network security issues;
    - The system administrators responsible for host security issues;
    - Corporate security responsible for setting company-wide policies and procedures including all other security-related teams and personnel;
    - The physical security team responsible for access to buildings and facilities;
    - The CSIRT responsible for coordination of response to any computer security incident reports.
  - It is imperative that the CSIRTs role is supported by management and understood by all parties involved.

..CSIRT Framework



Relation to other CSIRTs

CSIRT Types & Environments..

- CSIRT serve a particular constituency.
- Examples of constituencies that a CSIRT may serve include:
  - *Academic Sector CSIRT* - provides CSIRT services to academic and educational institutions
  - *Commercial CSIRT* - provides CSIRT services commercially to their constituents.
  - *CIP/CIIP Sector CSIRT* - mainly focus on Critical Information Protection (CIP) and / or Critical Information and Infrastructure Protection (CIIP). Such CSIRTs usually cooperate closely with a Governmental CIIP department.
  - *Governmental Sector CSIRT* - provides services to government agencies and in some cases to the citizens.
  - *Internal CSIRT* - provides services to its hosting organisation only. Constituents include internal staff and IT department of the hosting organisation.

..CSIRT Types & Environments

- *Military Sector CSIRT* - provides services to the military.

- *Small & Medium Enterprises (SME) Sector CSIRT* - provides its services to its own business branch or similar user group, e.g. the Association of Manufacturers of a country.

- *Vendor CSIRT* - focuses on the support of the vendor-specific products. Its aim usually is to develop and provide solutions in order to remove vulnerabilities and to mitigate potential negative effects of flaws. Constituents are product owners.

- *National CSIRT* – This refers to a CSIRT with a national focus and is considered as a security Point of Contact (PoC) for a country. In some cases the governmental CISRT also acts as national PoC. This type of CSIRT usually does not have direct constituents, as the national CSIRT only plays an intermediary role for the whole country.

CSIRT Services..

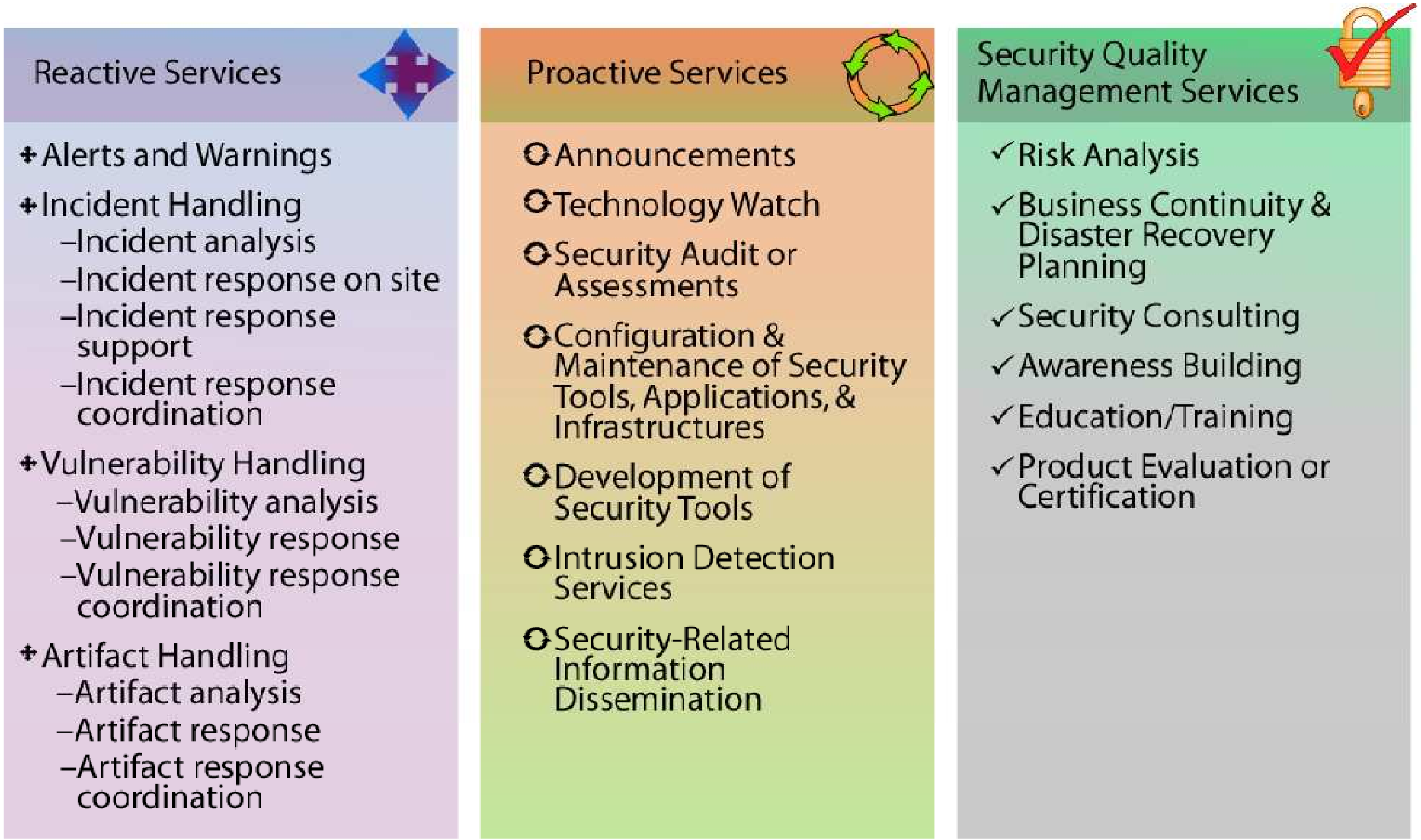
- The services that a CSIRT provides should be based on the *mission*, *purpose*, and *constituency* of the team.

- CSIRT services can be grouped into 3 categories:
  - *Reactive Services:* These services are triggered by an event or request and are the core component of CSIRT work.

  - *Proactive Services:* Proactive services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events.

  - *Security Quality Management Services:* These are generally proactive services that contribute indirectly to reducing the number of incidents.

..CSIRT Services



Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

List of Common CSIRT Services

CHAPTER 5: CSIRT SERVICES