LE CERT BANCAIRE

MANNAI FATHI - APTBEF/FINANCIAL CERT

SOMMAIRE

- Présentation du CERT Bancaire
  - CERT Bancaire: Services et Missions
    - CERT Bancaire: Activités et Actions
      - CERT Bancaire: Collaboration et Coordination

PRÉSENTATION DU CERT BANCAIRE

Le CERT bancaire est une entité de collaboration en matière de cybersécurité:

- Le premier CERT sectoriel dans L'Afrique du Nord créée dans le cadre d'une convention entre **l'APTBEF** et **l'ANSI**
- Fournir un cadre au sein du secteur financier tunisien de lutte contre les cyber-attaques
- Permettre aux différentes parties prenantes de renforcer leur niveau de sécurité
- Appuyer les efforts assurés par les différents régulateurs notamment la BCT et l'ANSI.
- Fournir des bases favorables pour le partage d'informations dans Le secteur financier
- Partager l'expérience ,l'expertise technique et les bonnes pratiques entre les différents acteurs

CERT BANCAIRE: SERVICES ET MISSIONS

LES MISSIONS

1. Assurer une activité de veille pour identifier les menaces potentielles et alerter les parties concernées
2. Partager les données relatives aux incidents, menaces, vulnérabilités, bonnes pratiques, etc
3. Agir comme étant un hub de communication pour tout le secteur et surtout durant les périodes de crises.
4. Collaborer avec tous les intervenants (ANSI, BCT, Justice, Police, media, etc.).
5. Organiser des actions de sensibilisation et de formation, pour le secteur et pour le grand public
6. Coordination avec d'autres CERT sectorielles, privée

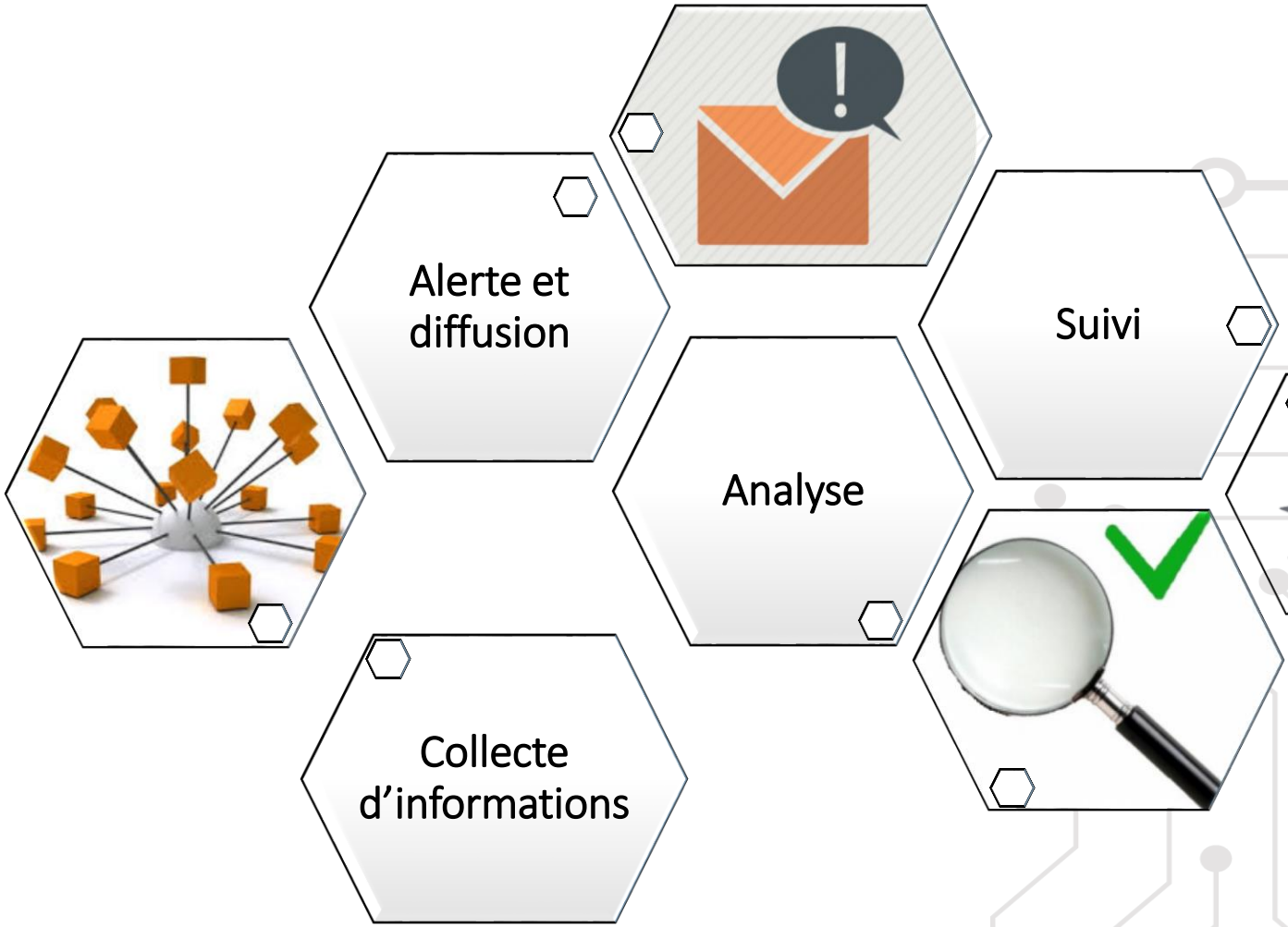
CERT BANCAIRE: SERVICES ET MISSIONS

LES SERVICES

1. Alertes et Avertissements
2. Analyse et Appui à la réponse aux incidents
3. Coordination de la réponse aux incidents
4. Sensibilisation et formation
5. Veille technologique
6. Etc

CERT BANCAIRE: ACTIVITÉS ET ACTIONS

LES ACTIVITES



1 Cyber Threat Intelligence

Le CERT Assure une activité de veille continue et de monitoring sur les vulnérabilités , les malwares et les tentatives d'attaques ciblant le secteur bancaire et financier en Tunisie.

CERT BANCAIRE: ACTIVITÉS ET ACTIONS

LES ACTIVITES

- Catégoriser les attaques pour mieux les analyser et se préparer à y répondre
- Analyser les données et identifier les méthodes utilisées par les criminels
- Identifier des risques
- Développer les capacités de prévention, de détection et de protection.

2 Traitement (1/2)

Face à des attaques de plus en plus compliquées et sophistiquées, le CERT Bancaire se charge de mener des investigations lors des tentatives d'attaques.

Diffusion + Confidentialité

CERT BANCAIRE: ACTIVITÉS ET ACTIONS

LES ACTIVITES

❸ Traitement (2/2)

Traitement d'attaque Web Defacement

Traitement d'attaque par phishing

Traitement en collaboration avec l'ANSI

CERT BANCAIRE: ACTIVITÉS ET ACTIONS

LES ACTIVITES

4 Sensibilisation

Le CERT Bancaire organise éventuellement des sessions de sensibilisation sur les menaces informatiques afin d'évaluer le niveau de maturité en cybersécurité dans le secteur bancaire.

- Découvrir et assimiler la sécurité informatique
- Appréhender et comprendre les attaques informatiques
- Identifier les menaces informatiques
- Adopter les bonnes pratiques pour se protéger

CERT BANCAIRE: ACTIVITÉS ET ACTIONS

LES ACTIONS

1 Cyber Drill –Cyber Exercice

3 Cyber Exercices depuis la fin de l'année 2017 avec
Une Première édition en collaboration avec l'ANSI

CERT BANCAIRE: ACTIVITÉS ET ACTIONS

LES ACTIONS

❷ Organisation des Workshops

- **21/03/2017 Workshop sur la cyber sécurité**
- **16/03/2017 Journée de sensibilisation à la cyber sécurité avec les experts de citigroup**
- **25/05/2017 Workshop de sécurité sur le thème « Retour sur l'attaque WannaCry »**

CERT BANCAIRE: ACTIVITÉS ET ACTIONS

LES ACTIONS

3 Organisation des événements de sensibilisation

Des sessions de sensibilisation sur des thèmes d'actualité:

- **Phishing**
- **Attaque des DABs**
- **Les ransomwares**
- **Le CSP SWIFT**
- **ETC**

CERT BANCAIRE: ACTIVITÉS ET ACTIONS

LES ACTIONS

3 Organisation des événements de sensibilisation

Mois de la cybersécurité - Octobre 2018

CERT BANCAIRE: COLLABORATION ET COORDINATION

COLLABORATION

Dans ses activités, le CERT Bancaire collabore avec

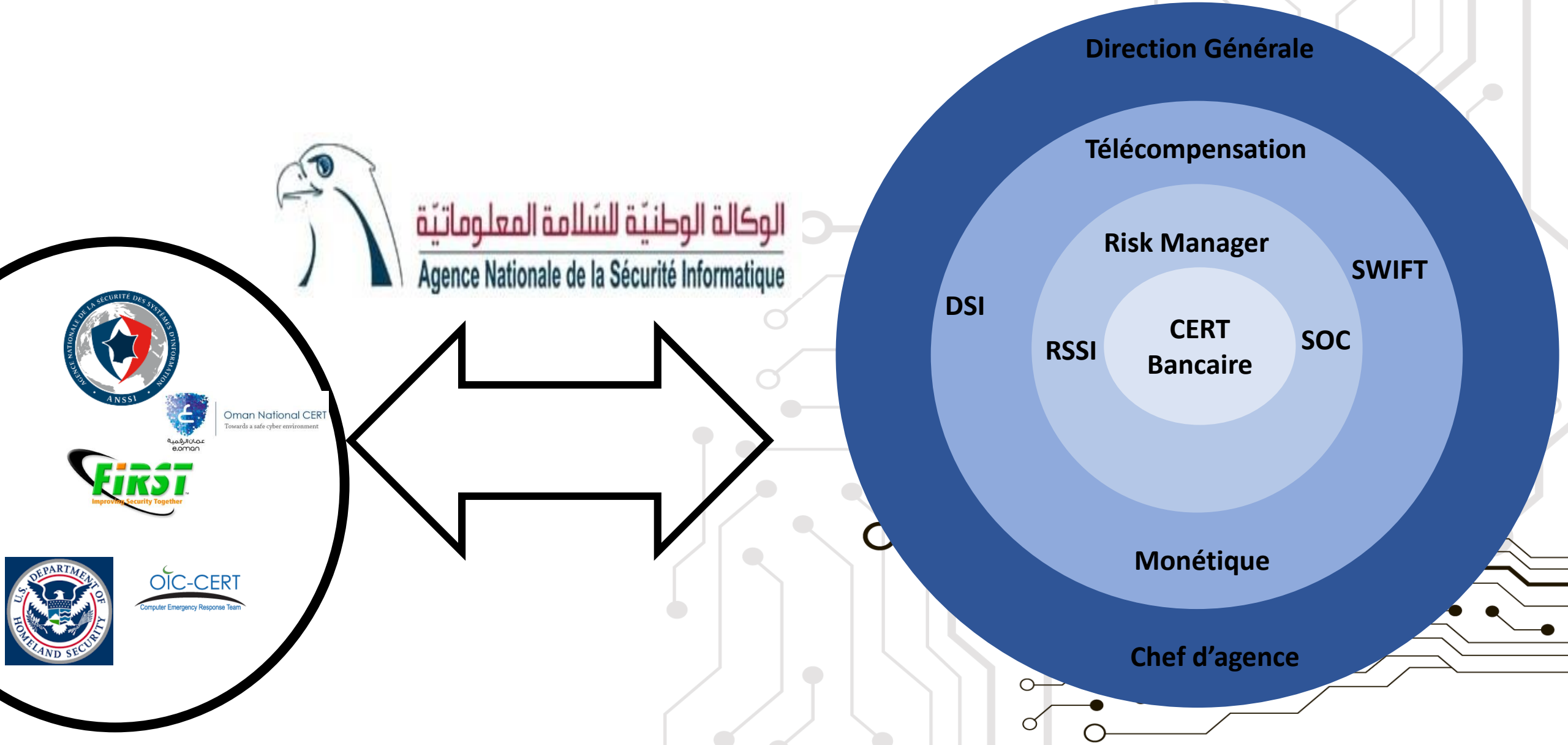
- Les principaux vis-à-vis des banques et Etablissement Financiers
  - RSSI
  - SOC
- Les responsables métiers
  - Risk manager
  - DSI
  - SWIFT
  - Monétique
- Les chefs d'agences et Les directions régionaux

COORDINATION

Le CERT bancaire jouera le rôle de coordinateur au sein du secteur financier et jouera le rôle d'interlocuteur avec :

- L'ANSI/TunCert
- D'autres entités comme :
  - Les services judiciaires,
  - La police,
  - Les fournisseurs,
  - Les médias,
  - Le secteur privé, Etc.

CERT BANCAIRE: COLLABORATION ET COORDINATION



BESOIN DE COLLABORATION ENTRE LES PARTIES PRENANTES

Toutes les parties prenantes sont confrontées aux problèmes similaires et elles auront besoin de partager des informations et de collaborer ensemble pour mener une réponse efficace aux cyber-menaces. La collaboration devra permettre de:

- Prévenir et détecter les attaques: recueillir, centraliser et partager des informations sur les cyber-menaces et sur les tendances,
- Assurer une intervention collective en cas d'urgence,
- Conduire des exercices de sécurité (opérations blanches),
- Développer une communication efficace,
- Partager des informations sur les meilleures pratiques et sur les procédures,
- Consolider les efforts de lutte contre la cybercriminalité .

BESOIN DE COLLABORATION ENTRE LES PARTIES PRENANTES

Cette collaboration sera développée par:

- **La mise en place d'un réseau de coordination pour lutter contre les cyber-attaques: Prévenir, détecter et répondre,**
- **La mise en place d'un cercle de confiance pour partager les informations relatives aux incidents et pour le partage d'expérience,**
- **La mise en place d'un cadre règlementaire : décret, convention, charte de collaboration,**
- **Le développement d'expertise technique en relation avec les moyens de détection et de réponse aux cyber-attaques,**
- **Le développement d'un processus de communication efficace avec les parties prenantes locales et étrangères,**
- **La mise en place d'une cellule de crise pour gérer des incidents majeurs,**

MERCI POUR VOTRE ATTENTION