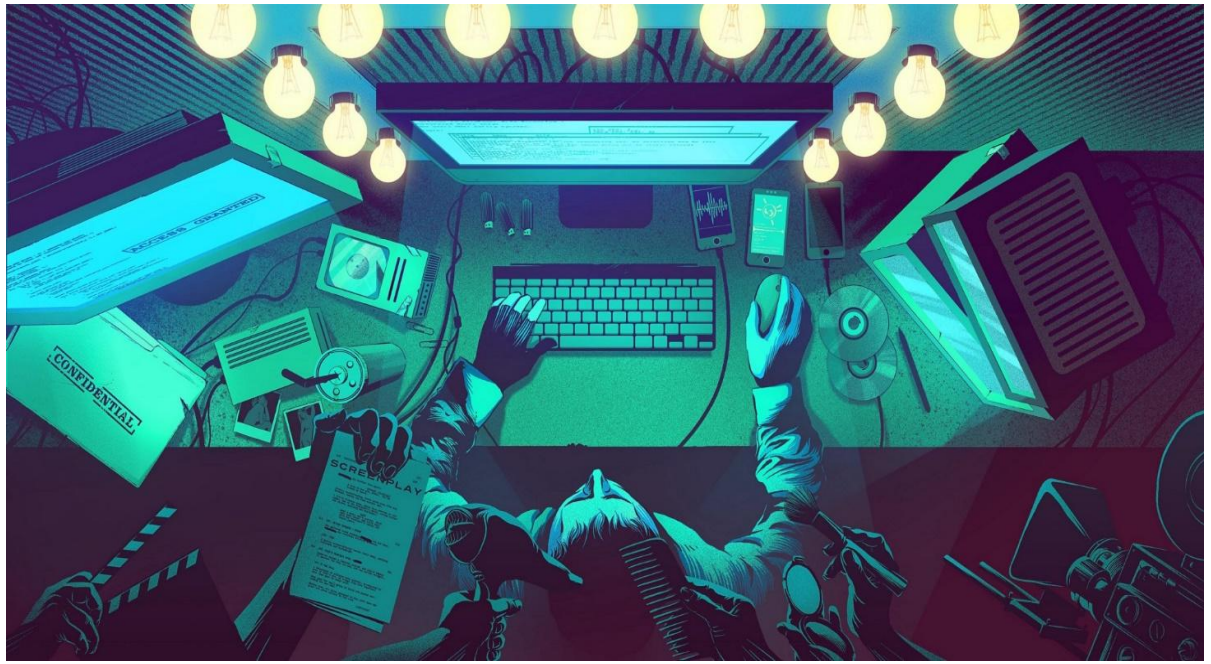
# Les défis de sécurité pour le secteur bancaire

**Haythem EL MIR, CISSP**

**Consultant en Cybersécurité**

SITIC AFRICA 2017
18 - 20 Avril 2017
Parc des expositions du Kram
LE HUB DES EXPERTS AFRICAINS EN TIC

# Attaquer une banque: hold-up ou cyber-attaque

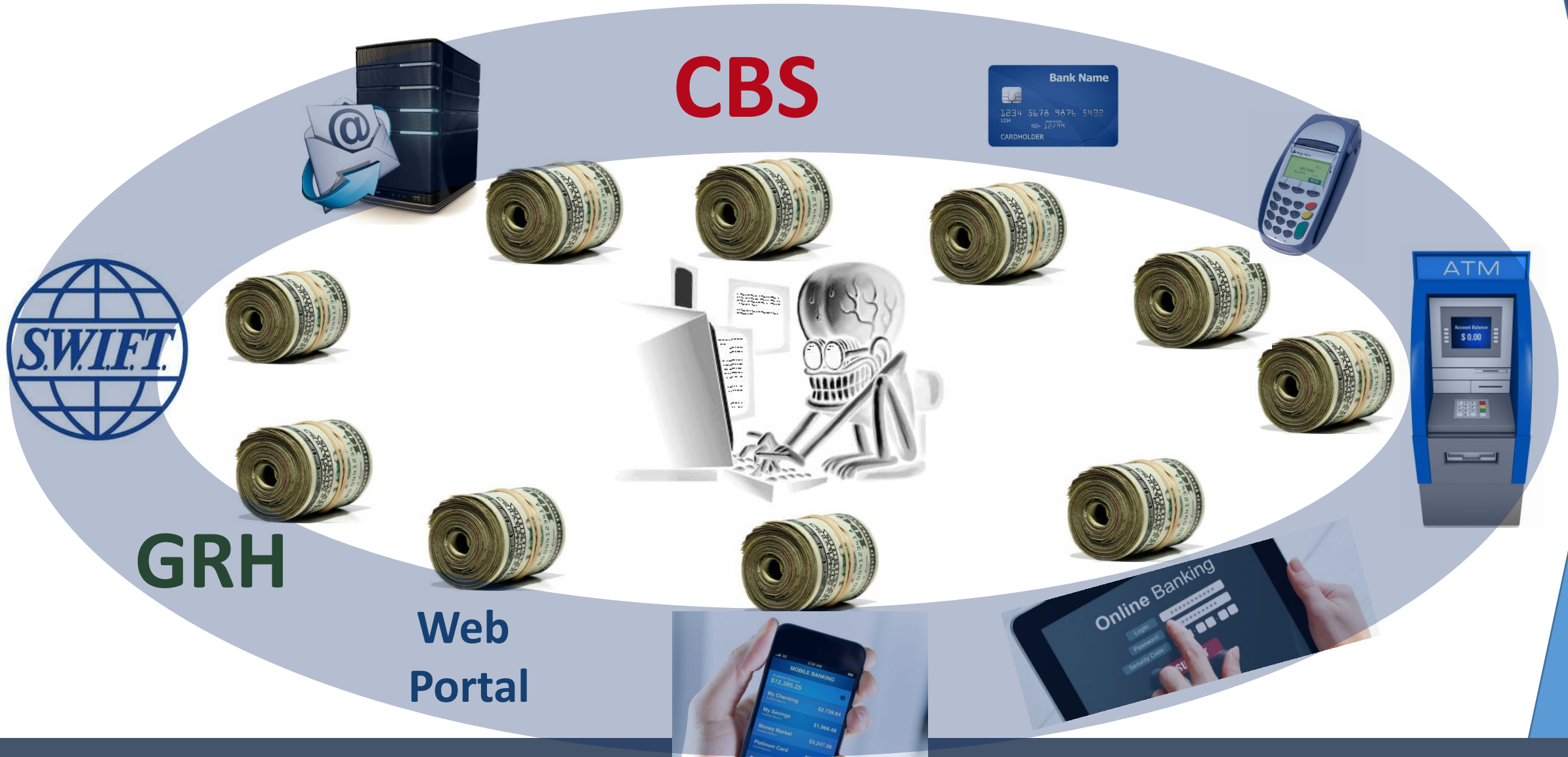



Les attaques informatiques sont moins risquées et peuvent assurer l’anonymat.

# Comment les pirates voient les banques?

# Comment les banques voient les pirates?

# Qu’est ce qu’une banque pour un pirate?



# Des conséquences graves

**Perte directe d'argent**
**Pénalités**


**Perte de clients/Part de marché**

**Perte de recette**

**Atteinte à la réputation**

**Poursuites légales**

# Situation actuelle

- Ouverture,
- Digitalisation,
- Diversification des moyens de paiement,
- Superposition de multitude de périmètres avec des technologies hétérogènes,
- Difficultés à maitriser les périmètres,
- Présence d’un grand nombre systèmes vulnérables,
- **Résultats: des systèmes exposés face à des menaces très sophistiquées = Attaques = Fraudes.**

# Que faire?
# Mettre en œuvre une stratégie de défense.

# Quelle sécurité?

- Audit – Plan(s) d'action,
- Politique de sécurité – SMSI,
- PCA/PRA,
- Risk management,
- Monitoring,
- PCI/DSS,
- ISO27001,
- Gestion des identités
- Authentification forte,
- Technologies.

**Face au menaces d'aujourd'hui, l'approche classique risque de ne pas être assez efficace.**

# Quelle sécurité?

Développer une stratégie et définir une vision de développement de la sécurité faisant partie intégrante de la vision de développement globale et surtout du développement numérique.


Partir d'une étude des menaces internes et surtout externes: identifier qui sont réellement ces pirates et s'ils sont vraiment présents.

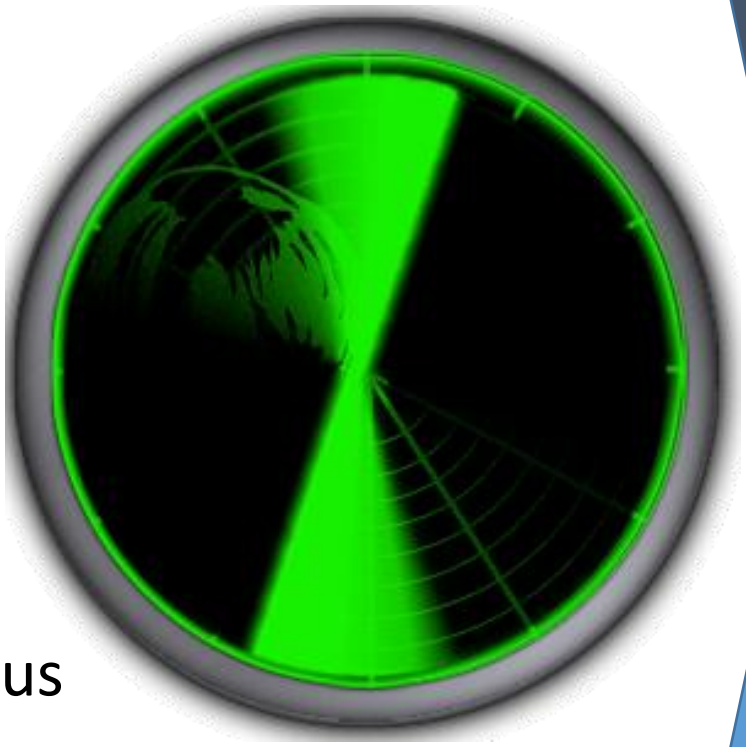
Stratégie adoptée par le top management et inclusive en incluant tous les périmètres et toutes les parties prenantes (internes et externes).

# Quelle sécurité?

- Une défense en profondeur,
- Une approche proactive,
- Une intelligence basée sur une collecte et une analyse de données en continue,
- Une réactivité rapide,
- Une communication efficace,
- Une collaboration interne et externe en impliquant tous les acteurs,
- Une défense qui se base sur un comportement prudent.

# Quelle sécurité?

- Etudier l'ecosystème :
  - Qui sont les pirates,
  - Quelles sont leurs motivations,
  - Quel est leur niveau d'expertise,
  - Quels sont leurs outils,
  - Comment ils coordonnent et planifient,
- Voler les données de cartes ne motive pas les pirates dans les pays à monnaie non-convertible,
- Dans certain pays les hacktivistes posent un risque plus important que les criminels,
- Parfois, la falsification d'ordre de virement est une menaces plus importante que les attaques contre l'e-banking.



# Approche collaborative

- Etre informé: La collecte et le partage d'information peut aider à:
  - Anticiper les attaques,
  - Maitriser les menaces,
  - Répondre efficacement aux attaques/fraudes,
- Une approche de protection sectorielle impliquant tous les intervenants et assurant une meilleure coordination avec les entités externes.
- Exemple Tunisien: Le Financial CERT:
  - Veille,
  - Coordination à la réponse eux incident,
  - Collecte et partage de données.

# Approche collaborative

Le concept du Financial CERT se base sur l'objectif suivant:

*coordonner et consolider les efforts de tous les intervenants du secteur financier… le partage d'information et la coordination assureront plus d'efficacité pour lutter contre les attaques et les fraudes.*

Mission:

Renforcer les capacités du secteur financier Tunisien pour lutter contre les cyber-attaques en  assurant la coordination et le partage d'informations relatives aux nouvelles menaces et aux incidents.

# Merci pour votre attention

**Haythem EL MIR**

**Haythem.elmir@keystone.tn**