



SEMINAIRE DE PRESENTATION DES ACTIVITES DU CIRT-BF

Ouagadougou, le 03 mai 2013

Hôtel Palm Beach

PRESENTATION DU CIRT-BF

Georges P. LALLOGO,
Manager/CIRT-BF
[glallogo\(at\)cirt.bf](mailto:glallogo(at)cirt.bf)

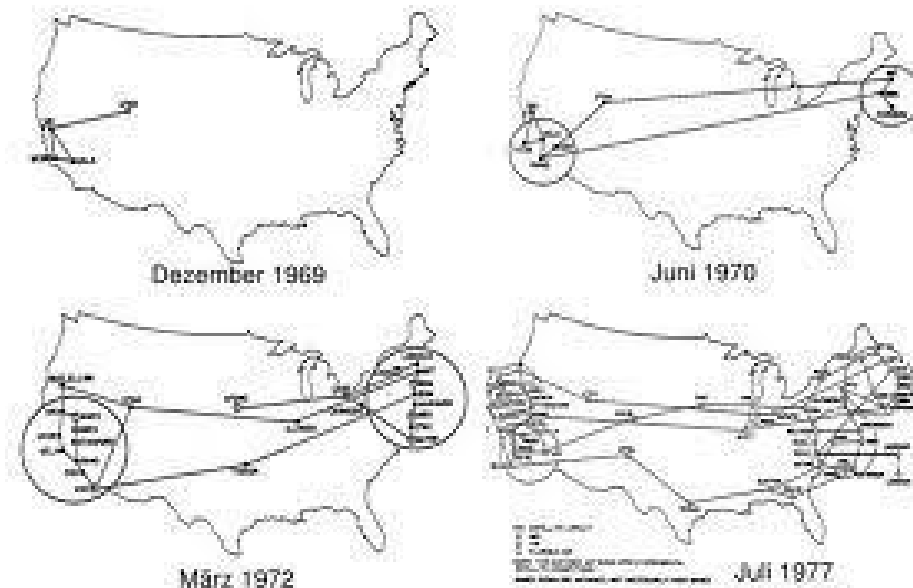
INTRODUCTION

- I. CONCEPT D'UNE EQUIPE DE REPONSE AUX INCIDENTS INFORMATIQUES
- II. CONTEXTE DE LA CREATION DU CIRT-BF
- III. MISSIONS, ORGANISATION ET FONCTIONNEMENT DU CIRT-BF
- IV. PERSPECTIVES DU CIRT-BF

CONCLUSION

INTRODUCTION

- ” L’histoire d’Internet commence en 1969
- Le projet ARPANET financé par *The Advanced Research Projects Agency (ARPA)* commence à tisser sa toile

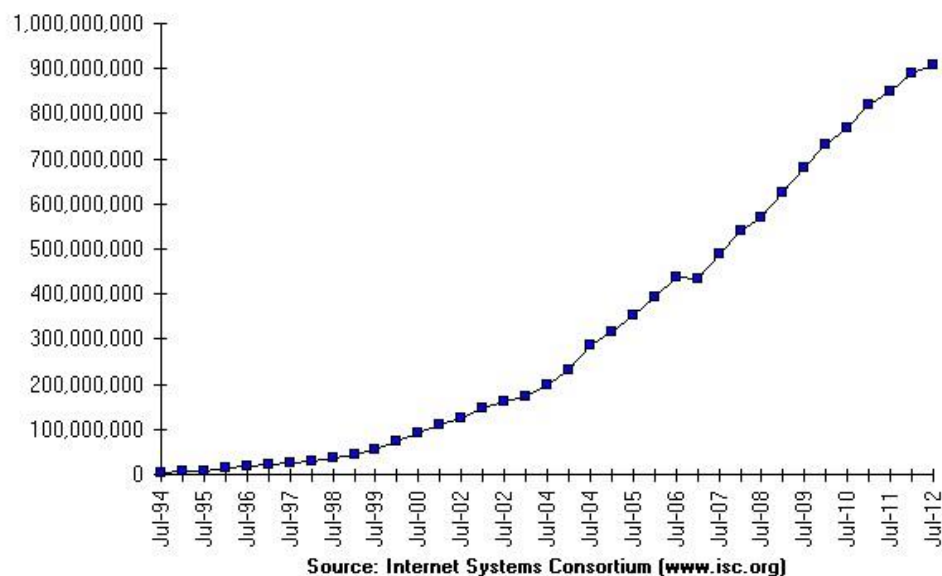


INTRODUCTION

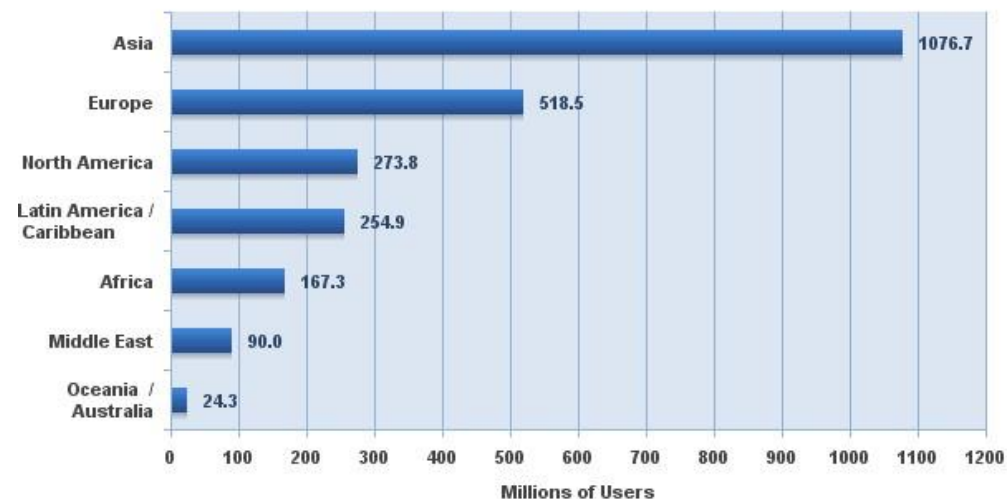
Internet c'est aujourd'hui près de 908,585,739 hôtes recensés (Juil. 2012) répartis sur 234 nations ou territoires.

INTERNET c'est 2,405,518,376 d'utilisateurs : 1 terrien sur 3 soit environ 35% de la population humaine.

Internet Domain Survey Host Count



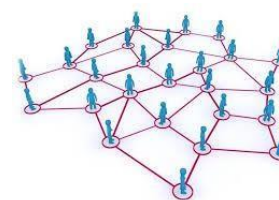
Internet Users in the World
by Geographic Regions - 2012 Q2



Source: Internet World Stats - www.internetworldstats.com/stats.htm
2,405,518,376 Internet users estimated for June 30, 2012
Copyright © 2012, Miniwatts Marketing Group

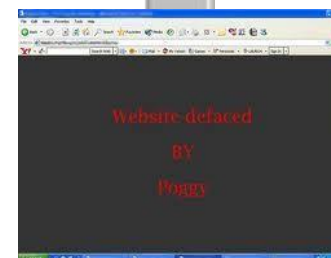
INTRODUCTION

“ Internet attire tout le monde pour toutes sortes d’activités :



INTRODUCTION

“ Les actes malveillants se multiplient ...



“ Le nombre de victimes se comptent par centaines de milliers ...

“ **L'impact des incidents se chiffre annuellement à des centaines voire des milliers de milliards de dollars...**

INTRODUCTION

Vous êtes menacés ou victimes d'un incident informatique

Que faire ?



Réponse : Contacter une équipe de réponse aux incidents informatiques

I. LE CONCEPT d'une équipe de réponse aux incidents informatiques

” SELON LE CERT

<http://www.cert.org>



Software Engineering Institute
Carnegie Mellon

une équipe de réponse aux incidents informatiques (...) est un organisme de service qui est chargé de recevoir, d'examiner et de répondre aux signalements des **incidents informatiques**. Leurs **services** sont généralement effectués dans une circonscription définie qui pourrait être une entité mère comme une personne morale, gouvernementale ou organisation pédagogique, une région ou un pays, un réseau de recherche, ou un client payé.

Une **équipe de réponse aux incidents informatiques** peut être une équipe formalisée ou une équipe ad hoc. Une équipe formalisée effectue un travail de **réponse aux incidents** dans la majeure partie de son activité. Une équipe ad hoc est convoquée lors d'un **incident informatique** ou pour répondre à un incident lorsque le besoin s'en fait sentir.

I. LE CONCEPT d'une équipe de réponse aux incidents informatiques

” SELON l'ENISA

<http://www.enisa.europa.eu>



une **équipe de réponse aux incidents informatiques** est une équipe d'experts en sécurité informatique ayant pour mission principale de répondre aux incidents en proposant les services nécessaires au traitement des attaques et en aidant leurs parties prenantes à restaurer les systèmes qui en ont fait l'objet.

La plupart des **équipes de réponse aux incidents informatiques** offrent également à leurs parties prenantes, dans le but d'atténuer les risques et de minimiser le nombre d'interventions requises, des services à caractère préventif et éducatif. Elles publient des bulletins et avis de vulnérabilités concernant les logiciels et matériels en usage, et informent les utilisateurs des exploits et virus tirant parti des failles constatées. Les parties prenantes sont dès lors en mesure de procéder rapidement à l'application de correctifs et à la mise à jour de leurs systèmes.

I. LE CONCEPT d'une équipe de réponse aux incidents informatiques

” Dans le jargon des équipes de réponse aux incidents informatiques, les expressions suivantes sont couramment rencontrées :

- ☐ Incidents
- ☐ Vulnérabilité
- ☐ Services
- ☐ Réponses aux incidents
- ☐ Alertes de vulnérabilité
- ☐ Partie prenante
- ☐ ...

I. LE CONCEPT d'une équipe de réponse aux incidents informatiques

- “ Les équipes de réponse aux incidents informatiques possèdent différentes appellations mais réalisent plus moins les mêmes activités.
- “ Appellations courantes :
 - . **CERT** ou **CERT/CC** (*Computer Emergency Response Team / Coordination Center*)
 - . **CSIRT** (*Computer Security Incident Response Team*)
 - . **IRT** (*Incident Response Team*)
 - . **CIRT** (*Computer Incident Response Team*)
 - . **SERT** (*Security Emergency Response Team*)
 -
- “ Désormais, on utilisera le terme générique **CSIRT** pour désigner dans cette présentation une équipe *quelconque* de réponse aux incidents informatiques.

I. LE CONCEPT d'une équipe de réponse aux incidents informatiques

“ Les *CSIRT* offrent des services à leurs clients ou parties prenantes

<u>Reactive Services</u>	<u>Proactive Services</u>	<u>Artifact Handling</u>
<u>Alerts and Warnings</u> <u>Incident Handling</u> <u>Incident analysis</u> <u>Incident response on site</u> <u>Incident response support</u> <u>Incident response coordination</u> <u>Vulnerability Handling</u> <u>Vulnerability analysis</u> <u>Vulnerability response</u> <u>Vulnerability response coordination</u>	<u>Announcements</u> <u>Technology Watch</u> <u>Security Audits or Assessments</u> <u>Configuration and Maintenance of Security</u> <u>Development of Security Tools</u> <u>Intrusion Detection Services</u> <u>Security-Related Information</u> <u>Dissemination</u>	<u>Artifact analysis</u> <u>Artifact response</u> <u>Artifact response coordination</u>
		<u>Security Quality Management</u>
		<u>Risk Analysis</u> <u>Business Continuity and Disaster Recovery</u> <u>Security Consulting</u> <u>Awareness Building</u> <u>Education/Training</u> <u>Product Evaluation or Certification</u>

I. LE CONCEPT d'une équipe de réponse aux incidents informatiques

Les services réactifs

Les services réactifs sont des services conçus et offerts par un CSIRT à ses parties prenantes en vue de répondre aux demandes d'assistance et aux signalements d'incidents venant de leur part ainsi que toute menace ou attaque dirigée vers lui [le CSIRT]. Certains services peuvent être initiés par la notification d'une tierce partie ou à travers le monitoring des logs ou des alertes provenant de sondes.

Les services proactifs

Les services proactifs sont ceux conçus en vue de renforcer l'infrastructure et la sécurité des processus des parties prenantes avant qu'un incident ne survienne ou ne soit détecté. Les buts recherchés sont la réduction de l'impact et l'étendue lorsque que des incidents se produisent.

Les services de management de la qualité

Les services de cette catégorie sont ceux qui ne sont pas spécifiques à la gestion des incidents ou caractéristiques aux CSIRT. Ce sont des services classiques conçus pour améliorer la sécurité globale d'une entreprise. En valorisant l'expérience tirée dans la fourniture des services proactifs et réactifs, un CSIRT peut apporter des perspectives uniques dans la qualité des processus de management ... Ces services sont conçus pour intégrer les feedbacks et les leçons apprises à travers les réponses aux incidents, les vulnérabilités et les attaques...

II. CONTEXTE DE CREATION DU CIRT-BF

Le BURKINA FASO, a décidé de la mise en place d'un CSIRT **dénommé CIRT-BF.**

PLUSIEURS RAISONS MAJEURES

1 Sur le plan international

- le lancement par l'UIT du programme GCA en 2007 pour traiter la question de la cybersécurité



- L'adoption par L'ASSEMBLÉE MONDIALE DE NORMALISATION DES TÉLÉCOMMUNICATIONS de la Résolution 58 *Encourageant la création d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement*

II. CONTEXTE DE CREATION DU CIRT-BF

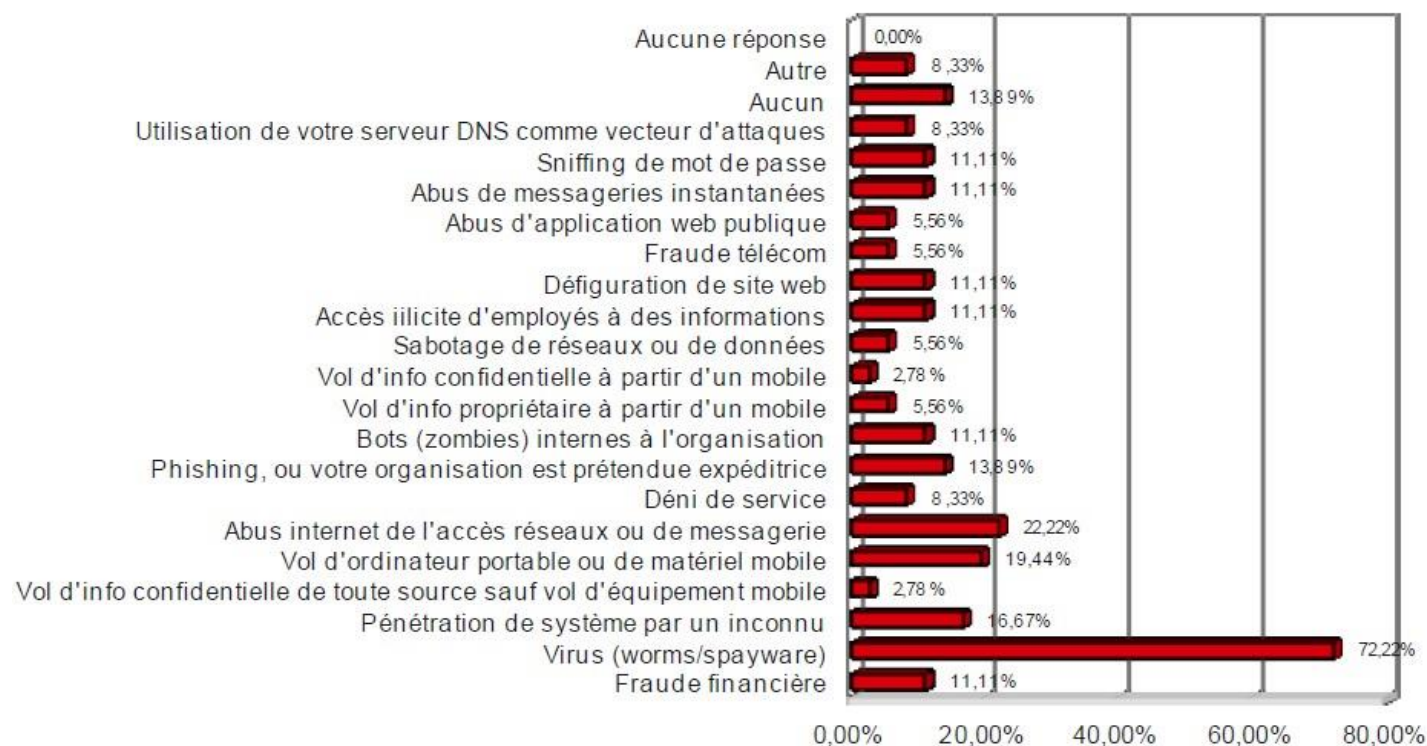
q Sur le plan national

- L'adoption en 2004 d'une stratégie d'opérationnalisation du plan de développement de l'infrastructure nationale de l'information et de communication
- L'élaboration d'un plan national de cybersécurité en 2010
- une augmentation des cas d'incidents causés sur les systèmes d'informations du gouvernement et des entreprises

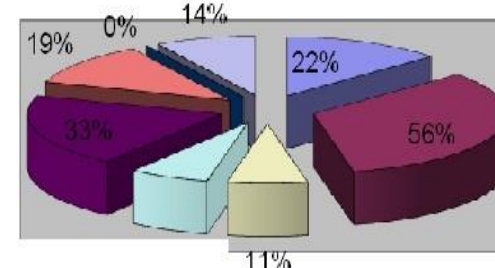


II. CONTEXTE DE CREATION DU CIRT-BF

Résultats d'enquête effectuée par l'ARCEP en 2010 : types et fréquences d'incidents rencontrés



IMPACTS DES INCIDENTS DE SECURITE
Tous secteurs confondus



II. CONTEXTE DE CREATION DU CIRT-BF

- “ Ces faits ont amené les premiers responsables de notre pays à adhérer aux différentes initiatives et même de s’y impliquer
 - ❑ Le 12 novembre 2008, le Président du Faso réaffirme son soutien au Programme GCA lors de la cérémonie d’ouverture de la session de haut niveau du Conseil de l’Union Internationale des Télécommunications
 - ❑ Le 25 Octobre 2011 à Genève, le Président du Faso est désigné comme Président du Conseil d’Administration d’IMPACT, l’agence d’exécution de l’IUT dans le domaine de la cybersécurité
- “ C’est naturellement que le BURKINA FASO a bénéficié de l’appui de l’UIT pour l’établissement d’un CSIRT national.
- “ La mission d’établissement est alors confiée à IMPACT et une équipe projet comprenant l’UIT, IMPACT et l’ARCEP (Sponsor) est mise en place
- “ L’implémentation du CIRT-BF s’est faite avec la participation de prestataires locaux pour l’acquisition et l’installation de la plateforme
- “ A la date d’aujourd’hui, le CIRT-BF est en phase de démarrer ses activités.

III. MISSIONS, ORGANISATION ET FONCTIONNEMENT DU CIRT-BF

A. MISSIONS PRINCIPALES DU CIRT-BF

Les missions principales du CIRT-BF sont les suivantes :

1. Coordonner et aider les organismes gouvernementaux et sociétés privées à mettre en œuvre des services proactifs afin de réduire les risques d'incidents de sécurité informatique, ainsi que répondre à de tels incidents lorsqu'ils se produisent
2. Mener des sensibilisations afin d'informer la population locale sur les effets néfastes des cybermenaces et de la cybercriminalité
3. Fournir des avis et conseils en temps opportun à tous les acteurs du secteur des communications électroniques sur les bonnes pratiques

III. MISSIONS, ORGANISATION ET FONCTIONNEMENT DU CIRT-BF

B. MISSIONS DÉTAILLÉES

- 1) Analyser et gérer les incidents de sécurité et fournir une assistance de gestion de crise en réponse aux menaces ou attaques
- 2) Donner les alertes et faciliter les échanges et discussions entre les acteurs pour une gestion efficace des incidents
- 3) Coordonner avec les UAGI (Unités d'Analyse et de Gestion des Incidents) sectorielles et autres organisations du public, du privé et les citoyens pour fournir les informations d'alerte spécifiques et des mesures de protection appropriées à mettre en place
- 4) Coordonner les actions de réponse avec les organisations sœurs au niveau régional et international
- 5) Promouvoir et aider dans la mise en œuvre des plans de continuité et de contingence

III. MISSIONS, ORGANISATION ET FONCTIONNEMENT DU CIRT-BF

B. MISSIONS DÉTAILLÉES

- 6) Sensibiliser les internautes sur les problèmes de sécurité et les aider à une utilisation rationnelle du cyberspace pour une bonne protection de celui-ci
- 7) Permettre un travail communautaire des experts et des professionnels pour une meilleure sécurité des systèmes d'information
- 8) Mettre en place une veille technologique en matière de la sécurité des systèmes d'information
- 9) Adhérer à des organisations internationales telles que le GRC, le FIRST, IMPACT et autres pour une meilleure coordination de réponse au niveau régional et international
- 10) Réaliser périodiquement des rapports et statistiques sur la cybersécurité

III. MISSIONS, ORGANISATION ET FONCTIONNEMENT DU CIRT-BF

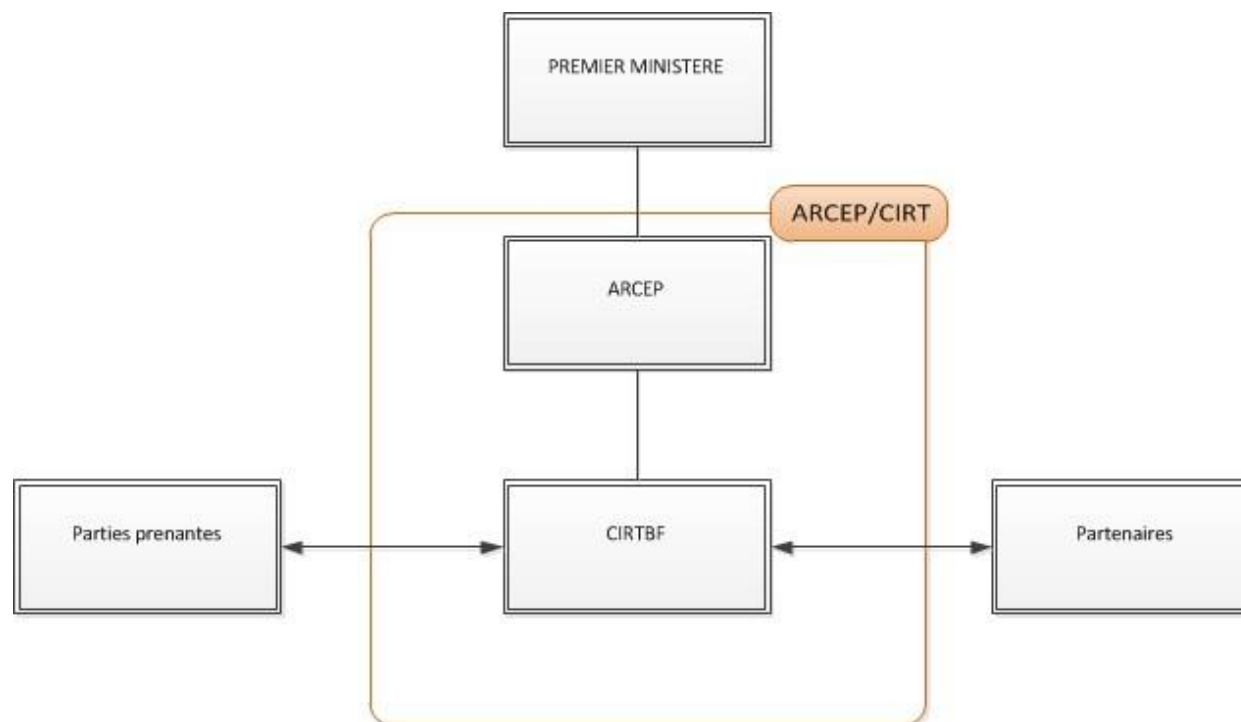
C. ORGANISATION

En attendant une formalisation de sa création, le CIRT-BF est placé sous la tutelle de l'ARCEP.

” *Tutelle administrative*

” *Tutelle technique*

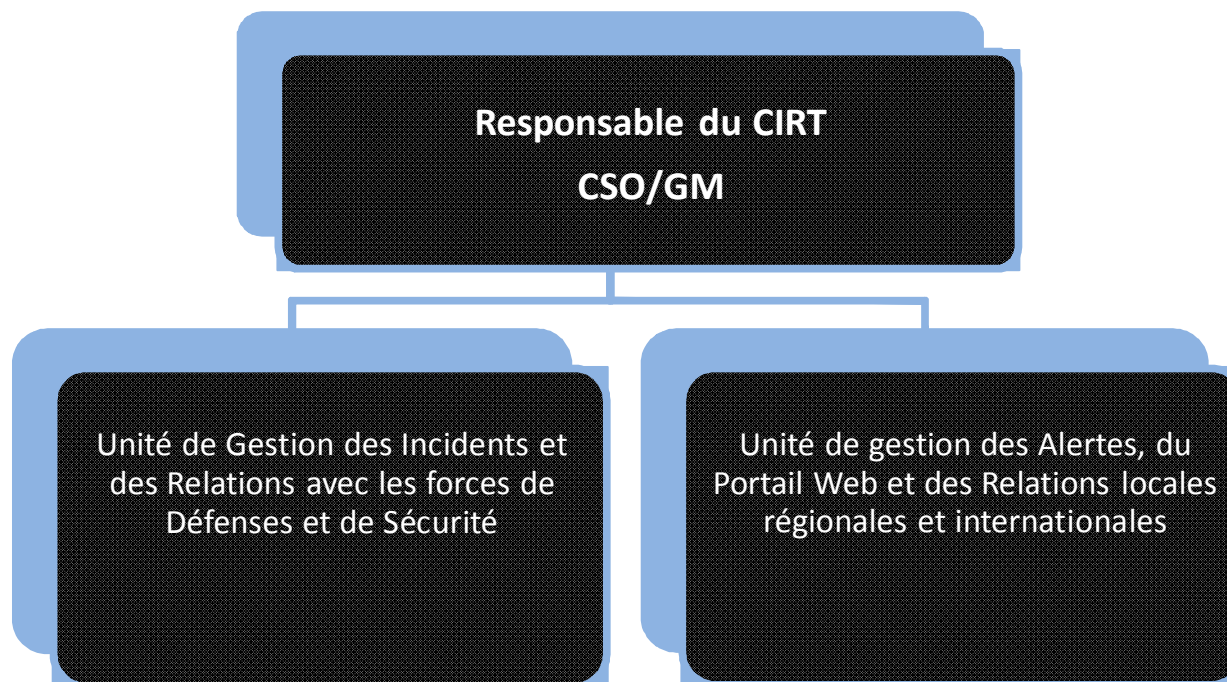
” *Tutelle financière*



III. MISSIONS, ORGANISATION ET FONCTIONNEMENT DU CIRT-BF

C. ORGANISATION

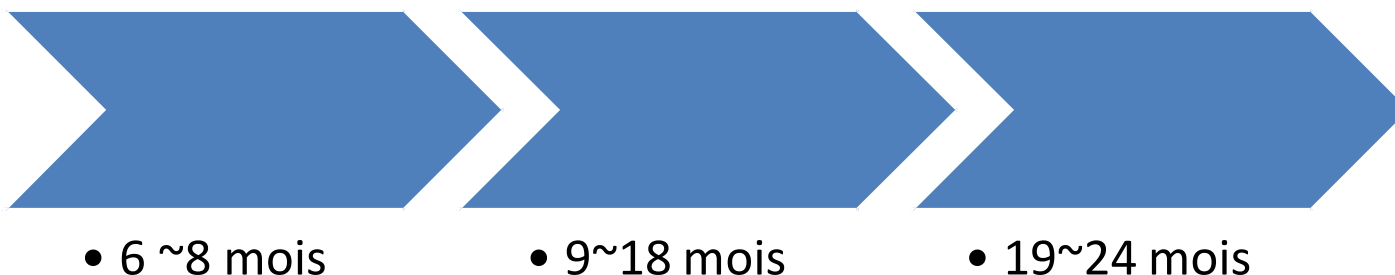
En interne, le CIRT-BF est structuré dans sa phase initiale comme suit



III. MISSIONS, ORGANISATION ET FONCTIONNEMENT DU CIRT-BF

D. FONCTIONNEMENT

- “ Le CIRT-BF est doté de moyens adéquats pour offrir **des services** à ses **parties prenantes** et **assurer une collaboration avec ses partenaires nationaux et internationaux**
- “ La mise en place des **services** se fera de façon **graduelle** :



- “ Les services basiques sont offerts gratuitement aux parties prenantes

III. MISSIONS, ORGANISATION ET FONCTIONNEMENT DU CIRT-BF

D. FONCTIONNEMENT

	Services réactifs	Services proactifs	Services de Management de la sécurité des SI
Phase 1	<ul style="list-style-type: none"> “ Réponse aux incidents “ Emissions de messages d’alertes “ Réponses aux vulnérabilités 	<ul style="list-style-type: none"> “ Information et sensibilisation “ Formation 	-----
Phase 2	<ul style="list-style-type: none"> “ Coordination des réponses aux incidents “ Coordination des réponses aux vulnérabilités et analyse des risques 	<ul style="list-style-type: none"> “ Analyse des vulnérabilités “ Veille technologique 	<ul style="list-style-type: none"> “ Sensibilisation avancée “ Formation
Phase 3	-----	<ul style="list-style-type: none"> “ Analyses pour les enquêtes criminelles “ Evaluation et audits de sécurité 	<ul style="list-style-type: none"> “ Analyse des risques “ Consulting en sécurité

IV. PERSPECTIVES

” Ancrage

- . *Intégrer le CIRT-BF à l'ANSSI*

” Couverture

- . *Appuyer la création et la collaboration avec des CSIRT sectoriels*
- . *Augmenter le nombre de parties prenantes et surtout faire adhérer les opérateurs des services et des infrastructures de base*

” Services

- . *Offrir plusieurs services aux parties prenantes*
- . *Rendre le CIRT-BF fonctionnel 24h/24 et 7j/7*

” Personnel

- . *Renforcer le nombre et la qualité du personnel*

” Renforcement des capacités des parties prenantes

- . *Offrir des formations...*

IV. PERSPECTIVES

” Collaboration internationale

- . Continuer la collaboration avec IMPACT (accès au GRC, ESCAPE ...) et l'UIT



- . Adhérer au réseau FIRST



- . Etablir des relations de coopération avec les équipes nationales de réponses aux incidents informatiques des autres pays
- . Appuyer la création d'un Centre Africain de coordination des activités des CSIRT nationaux des pays africain

CONCLUSION

- Le CIRT-BF est un puissant instrument offert aux structures gouvernementales, aux entreprises, aux opérateurs et au-delà, l'ensemble des utilisateurs du cyberspace national pour les aider à résoudre les incidents liés à l'utilisation des TIC
- Le CIRT-BF déploiera les ressources nécessaires pour offrir des services de qualité aux parties prenantes
- Le succès de la lutte contre les incidents dépendra de la collaboration de tous

Merci pour votre écoute !



Site web : <http://www.cirt.bf>

Email (infos): [cirt\(at\)cirt.bf](mailto:cirt@cirt.bf)

Reporter un incident : [incidents\(at\)cirt.bf](mailto:incidents@cirt.bf)