LES PARTIES PRENANTES

RÔLES ET RELATIONS AVEC LE CIRT-BF

03/05/2013

RENCONTRE D'ECHANGE AVEC LES PARTIES PRENANTES DU CIRT-BF

Hôtel Palm Beach

aristide.zoungrana at arcep.bf

Définition partie prenante

- Acteur, individuel ou collectif (groupe ou organisation), activement ou passivement concerné par une décision ou un projet ; c'est-à-dire dont les intérêts peuvent être affectés positivement ou négativement à la suite de son exécution (ou de sa non-exécution). Source: Wikipedia, mai 2013
- « Constituency »: terme aussi utilisé dans le monde des CIRTs, pour désigner la base de clientèle d'un CIRT
- « Client particulier » ou partenaire ou adhérant … au CIRT

AGENDA

- Rappel mission générale d'un centre de cybersécurité
- Avantages d'adhérer au CIRT-BF
- Profil des parties prenantes
- Relation des parties prenantes avec le CIRT-BF
- Relation avec les Centres de cybersécurité (CCS) extérieurs
- Cadre de la coopération
- Confidentialité

Rappel mission générale du CIRT-BF

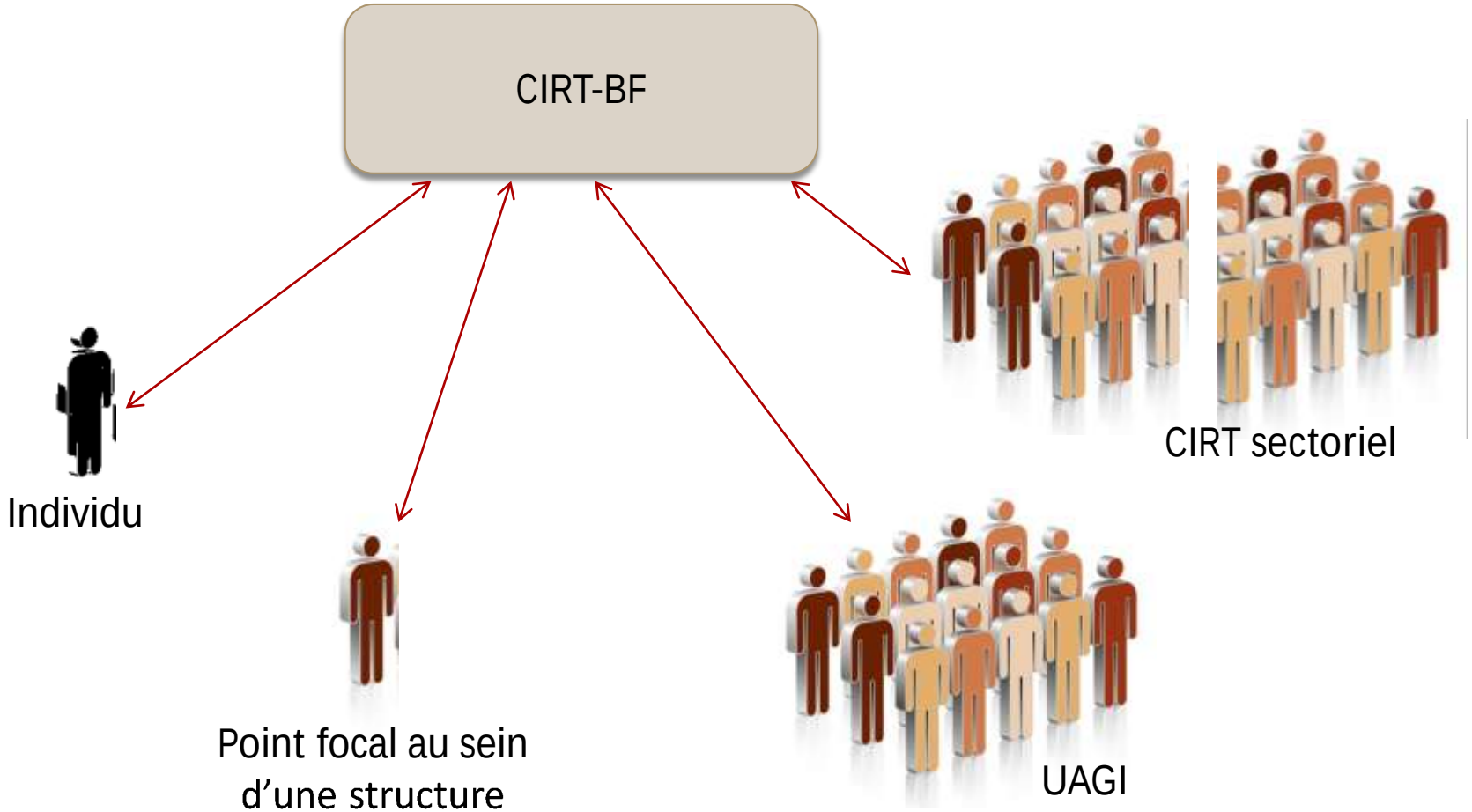
- Sécuriser le cyberespace en assistant ses adhérents en matière de sécurité informatique dans le domaine de la prévention, la détection et la résolution d'incidents de sécurité, en vue de réduire les risques et incidents de sécurité informatique

- Ambition du CIRT-BF:
  - Ambition d'être une cellule nationale de confiance pour la collecte et la diffusion d'informations relatives aux menaces, aux vulnérabilités, aux incidents affectant les réseaux d'ordinateurs…

Avantages d'adhérer au CIRT-BF

- Centralisation de la coordination en matière de cybersécurité
- Disponibilité d'une expertise nationale et internationale: bénéficier de l'expérience des parties prenantes, pour les parties prenantes
- Suivi des évolutions dans le domaine de la sécurité informatique
- Partager une même culture de sécurité informatique

Profil des parties prenantes

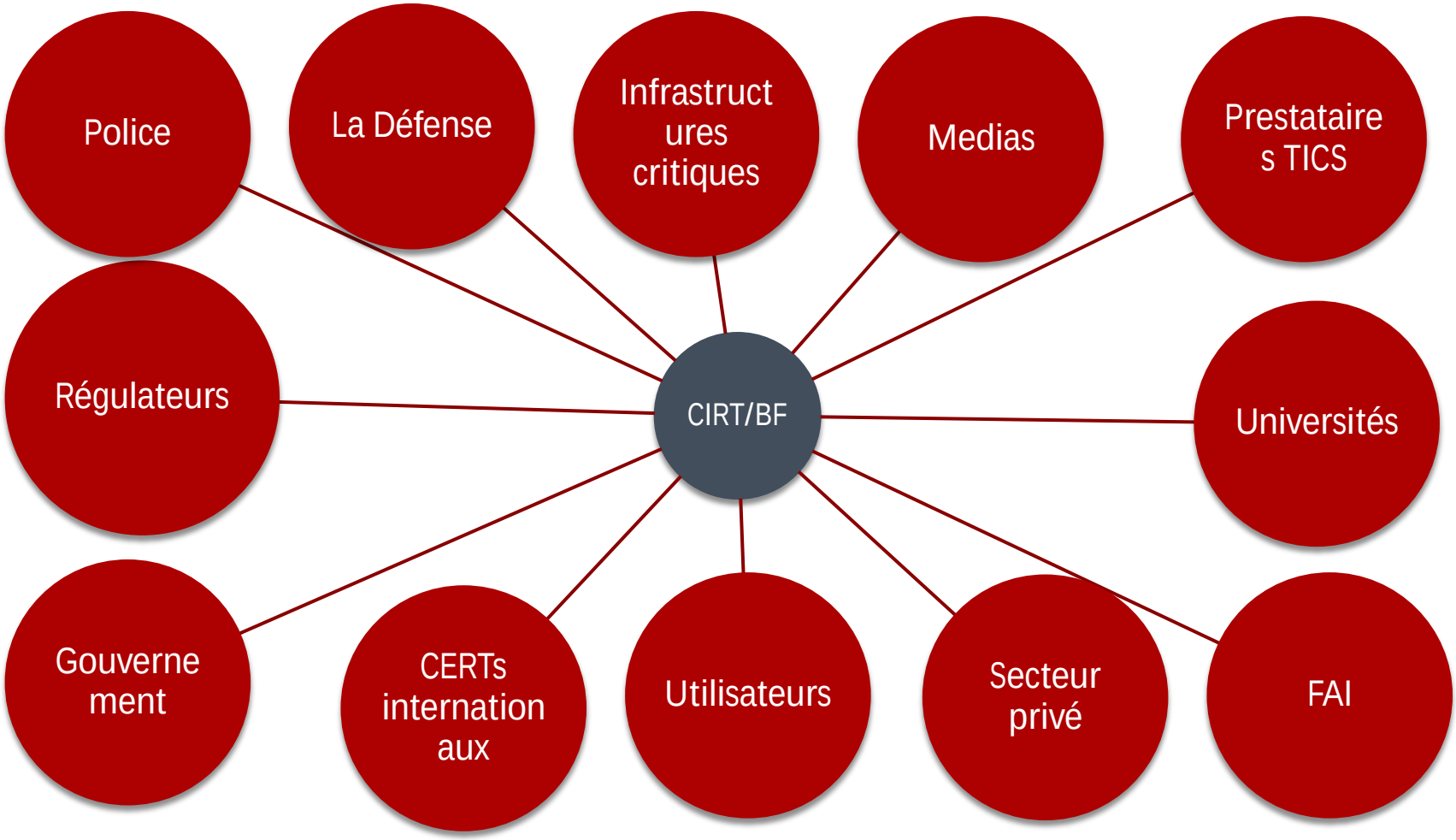


UAGI: Unité d'Analyse et de Gestion des Incidents

Profil des parties prenantes

- Pour le cas du Burkina Faso:
- Phase de démarrage de la coopération avec les structures
  - Environ 40 structures ciblées pour cette phase
  - Concerne les fournisseurs de ressources clés et d'infrastructures critiques du Burkina
- Ouverture de plus de services au grand public à moyen/long terme
  - Contrainte de plus de main d'œuvre pour la gestion du grand flot d'informations…

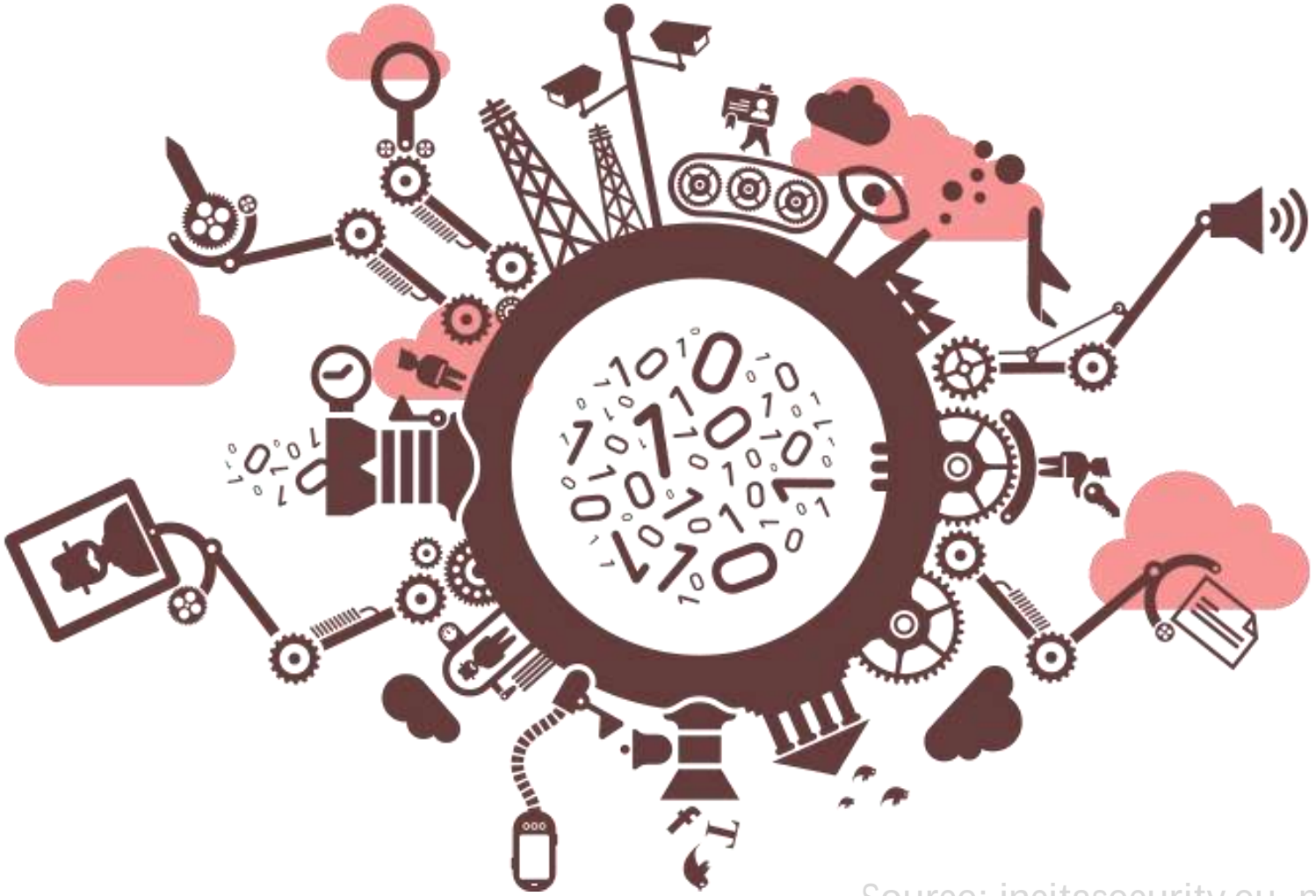
Profil des parties prenantes



Profil des parties prenantes

- Profils souhaités pour les points focaux
  - Ingénieurs informaticiens dans la mesure du possible
  - Managers senior en informatique
  - Experts en sécurité informatique, RSSI
  - Programmeurs
  - Experts en investigation, en analyse d'incidents/vulnérabilités…
  - Administrateurs systèmes et réseaux
  - Spécialistes en télécommunications
  - Gestionnaires de base de données
  - Etc.
- Bien entendu, toute personne/profil de par sa position ou son autorité en matière de sécurité de l'information, au sein d'une structure, nous est utile

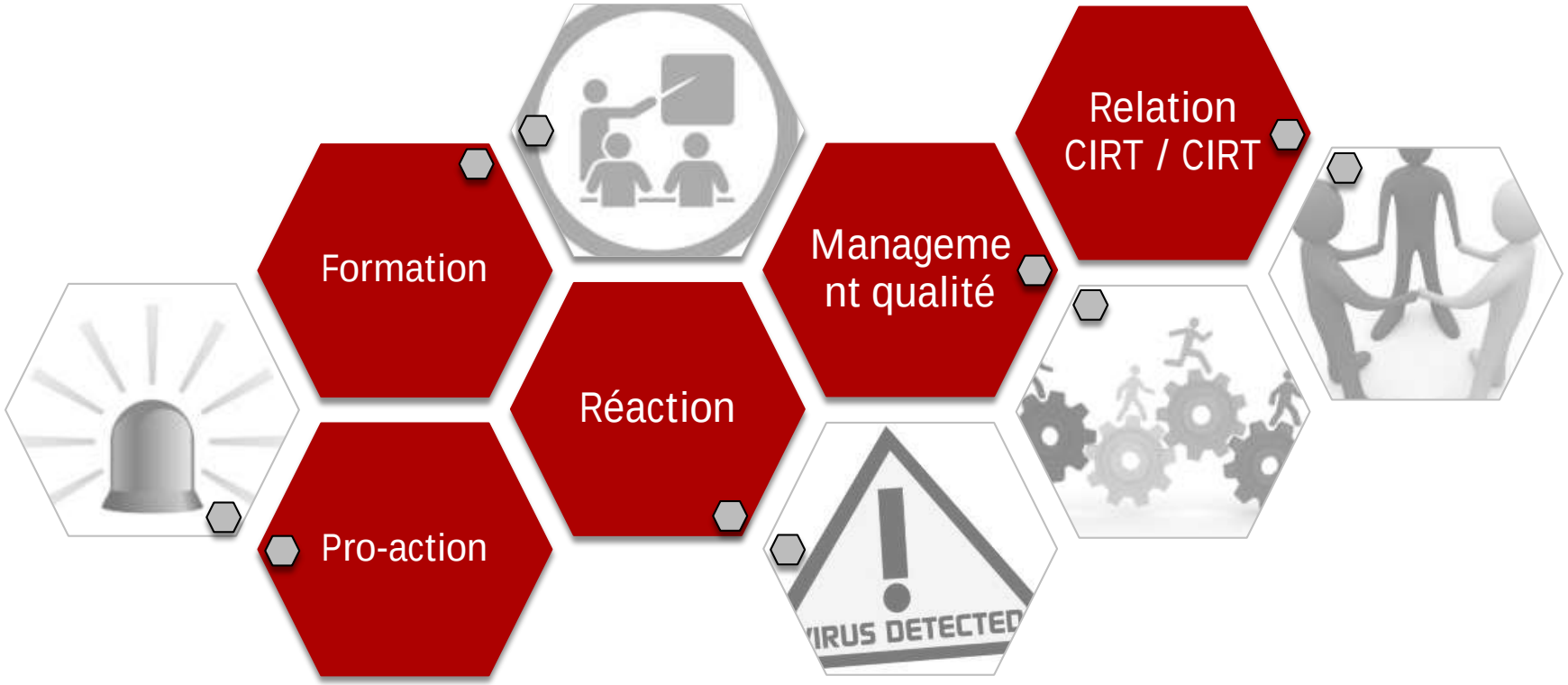
Relation avec le CIRT-BF



Source: incitasecurity.eu, mai 2013

Relation avec le CIRT-BF

Services à activer dans le temps par le CIRT-BF



Relation avec le CIRT-BF

- Services proactifs
  - Annonces, diffusion d'alertes et de toute information relative à la sécurité
  - Configuration et maintenance des outils de sécurité, des applications et des infrastructures
  - Développement d'outils de sécurité
  - Mise en place d'outils/services de détection d'intrusion
  - Assistance protection/dissémination des informations
  - Veille technologique
  - Audit de sécurité

Relation avec le CIRT-BF

- Services réactifs
  - Alertes et avertissements
  - Gestion des incidents
    - Analyse des incidents
    - Appui de réponse aux incidents
    - Réponse en cas d'incidents, sur le site physique
    - Coordination des interventions en cas d'incident
  - Gestion des vulnérabilités/failles/faiblesses d'un SI
    - Analyse, réponse, coordination

Relation avec le CIRT-BF

- Services de management de la sécurité des systèmes d'information
  - Mise en place de système d'analyse de risques
    - Système de Management de la Sécurité de l'Information (SMSI)
  - Plan de continuité et de reprise après incidents
  - Consultation en sécurité
  - Renforcement de la sensibilisation sur les bonnes pratiques en sécurité informatique
  - Education / Formation
  - L'évaluation de produit et certification

Relation avec le CIRT-BF

- Relation entre les CIRTs du Burkina
- Le CIRT/BF vous laisse la latitude de créer des CIRTs Internes (spécialisés banque…)
- Se veut le point central de dialogue avec les autres acteurs nationaux et les acteurs internationaux
  - Sert de point de contact de sécurité (PoC) pour un pays

Relation avec le CIRT-BF

- Autres apports des parties prenantes envers le CIRT/BF
  - Abonnement/financement d'activités
  - Apport dans les domaines juridiques, techniques…

Relation avec les CCS extérieurs

- CCS: Centre de cyber-sécurité
- Le CIRT-BF: point focal du Burkina pour les autres CCS extérieurs
- Vous entendrez parler aussi de:
  - CERT Computer Emergency Response Team
  - CSIRT Computer Security Incident Response Team
  - CIRC Computer Incident Response Capability
  - CIRT Computer Incident Response Team
  - IRC Incident Response Center or Incident Response Capability
  - IRT Incident Response Team
  - SERT Security Emergency Response Team
  - SIRT Security Incident Response Team
  - CSC Cyber Security Center

Relation avec les CCS extérieurs

- Quelques centres nationaux
  - CI-CERT: www.cicert.ci
  - ghCERT (Ghana)
  - EG-CERT www.egcert.eg
  - CSIRT-KENYA www.csirt.or.ke
  - CERT-MU (Maurice) www.cert-mu.org.mu
  - CERT MORROCO www.macert.ma
  - Afrique du Sud: ECS-CSIRT + CSIRTFNB (Banque)
  - CERT Sudan www.cert.sd
  - tunCERT www.ansi.tn

Relation avec les CCS extérieurs

- Quelques grandes structures fédératives
  - IUT
  - Impact
  - First
  - AfricaCERT
  - APCERT
  - ENISA (European Network and information Security Agency ou Agence européenne chargée de la sécurité des réseaux et de l'information)
  - Etc.

Relation avec les CCS extérieurs

- IUT (Union Internationale des Télécoms)
  - Prise de résolution commune
  - Assistance technique aux pays
  - Aide les pays à réaliser les objectifs du Programme mondial cybersécurité (GCA) de l'UIT

Relation avec les CCS extérieurs

- Impact
  - International Multilateral Partnership Against Cyber Threats
- Agence spécialisée des Nations Unies pour la cybersécurité, à travers un partenariat avec l'IUT
- Plus de 200 pays ayant bénéficié du soutien
- Services
  - Expertise en matière de cybersecurité
  - Global Response Centre (GRC) offre:
  - Electronically Secure Collaborative Application Platform for Experts (ESCAPE): plateforme virtuelle de collaboration alimentée par les industries, les académies…, et utilisée par les partenaires pays
  - Centre de formation et de développement des compétences
  - On y retrouve des organismes comme Kaspersky, F-secure, Ec-Council (Certification CEH..), Sans institute (Certification + université de formation)

Relation avec les CCS extérieurs

- First
  - Global Forum for Incident Response and Security Teams
  - Forum des Equipes de Réponse aux Incidents de Sécurité
- Services
  - Accès à des documents de bonnes pratiques
  - Publications et webservices
  - Forum de discussion thématique
  - Conférence annuel sur la réponse aux incidents

Relation avec les CCS extérieurs

Le réseau FIRST. Source: www.first.org . Avril 2013

Relation avec les CCS extérieurs

- AfricaCERT [africacert.org]
- Plateforme africaine de prévention et de lutte contre les attaques informatiques
- Inauguré en 2012 en partenariat avec AfriNIC et l'OIF (Organisation internationale de la Francophonie)
- Services proposés
  - Coordination des actions de lutte contre la cybercriminalité en Afrique
  - Formation et de renforcement de capacités
  - Assistance et mise à disposition d'expertise-conseil pour la création des CERTs nationaux
  - Sensibilisation des décideurs politiques, économiques, académiques et sociaux aux enjeux de la cybercriminalité

Relation avec les CCS extérieurs

- En résumé:
- Passerelle de coordination des analyses et des réponses aux problèmes de sécurité informatique
- Passerelle de veille technologique
- Accès à des bibliothèques sur les meilleures pratiques en matière de sécurité des systèmes d'information
- Rencontres/conférences techniques
- Formations

Récapitulatif des services offerts

Services proactifs

Annonces
Veille technologique
Audits de sécurité
Configuration et maintenance de sécurité
Développement d'outils de sécurité
Détection d'intrusion
Protection/dissémination des informations

Services réactifs

Alertes et avertissements

Gestion des incidents (analyse, réponse, coordination)
Gestion des vulnérabilités (analyse, réponse, coordination)

Management sécurité

Analyse de risques (SMSI)
Plan de continuité et de reprise après incidents
Consultation en sécurité
Renforcement de la sensibilisation
Education / Formation
L'évaluation de produit et certification

Relation avec les Centres de cyber-**sécurité en local comme à l'international**
Passerelle pour les services réactifs / proactifs.. étrangers, formation..

Récapitulatif des services offerts

- Discussions permanentes en vue de mieux choisir les services qui répondent aux besoins des parties prenantes

Services	Importance basse	Moyen	Haute
Alertes	X		PP
Gestion incidents		X	PP
Supervision			X PP
…			

X: Importance vue par le CIRT-BF

PP: Importance d'implémentation ou d'activation d'un service, voulue ou demandée par les Parties prenantes

Mode de communication

- Communication entre un point focal et un membre de l'équipe CIRT-BF
- Outils
  - Flux RSS
  - Souscription à une liste de diffusion
  - Liste de discussion
  - Mail (Utilisation d'un certificat électronique et/ou PGP)
  - Téléphone
  - Formulaire de déclaration d'incidents en ligne
  - Plateforme collaborative
  - Etc.

Cadre de la coopération

- Coopération/échange informelle dans de nombreux cas
  - Notamment entre parties prenantes ou avec le CIRT-BF
- Mémorandum d'entente
  - Document légal décrivant un accord bilatéral entre les parties. Elle exprime une convergence de volonté entre les parties, indiquant une ligne commune d'action prévu, plutôt que d'un engagement juridique
- Accord de non-divulgation
  - Contrat entre deux parties au moins qui décrit les documents confidentiels ou des connaissances que les parties souhaitent partager avec un autre pour certaines fins, mais souhaitent limiter l'utilisation généralisée
  - Contrat par lequel les parties s'engagent à ne pas divulguer des informations couvertes par l'accord
  - Crée une relation de confiance entre les parties afin de protéger des secrets commerciaux…
- Etc.

Confidentialité

- Le CIRT-BF conforme aux règles d'usage de la profession et des lois nationales et internationales sur les données
- Ainsi le CIRT-BF respecte scrupuleusement les mesures suivantes:
  - Confidentialité des informations techniques découvertes: tout au long du processus de sécurisation
  - Confidentialité sur les vulnérabilités et autres failles dites « 0Day » tant que le fournisseur n'a pas émis de «Correctif » ou «Moyen Préventif » de sécurisation
  - A ne pas divulguer ni communiquer à quiconque en dehors de l'entité impactée aucune information confidentielle (sous quelque forme que ce soit et par quelque moyen que ce soit) liée à la faiblesse de son système
  - Confidentialité, à l'égard de tiers, des données nominatives et cela conformément à la loi CIL..
  - A communiquer sur son site web la « sécurisation réussie » de l'entité impactée sans donner de détails techniques

Confidentialité

- Afin de préserver la confidentialité et la non-répudiation, le mode de chiffrement PGP lors des échanges par email avec les entités alertées
- Les clés publiques et les modes de communication seront publiés ultérieurement sur le site web du CIRT/BF
- Si l'organisme impacté ne dispose pas du chiffrement PGP, le CIRT-BF s'alignera sur le moyen utilisé

Merci pour votre attention!

QUESTIONS, REPONSES, APPORTS ?

« La sécurité n'est pas un produit mais un processus »

Bruce Schneier, Cryptologue

La sécurité, c'est l'affaire de tous.

Il appartient à chacun d'apporter sa pierre à l'édifice.

N'hésitez pas à nous contacter: cirt@cirt.bf et www.cirt.bf

Par Aristide R. ZOUNGRANA
aristide.zoungrana at arcep.bf