CYBERSECURITE ET PARTAGE D'INFORMATIONS: DEFIS ET SOLUTIONS

Abidjan, 30 Mai 2022

AMAN VLADIMIR

CHEF DU CI-CERT

Côte d'Ivoire – Computer Emergency Response Team
v.aman@cicert.ci / aman.vladimir@artci.ci

AGENDA

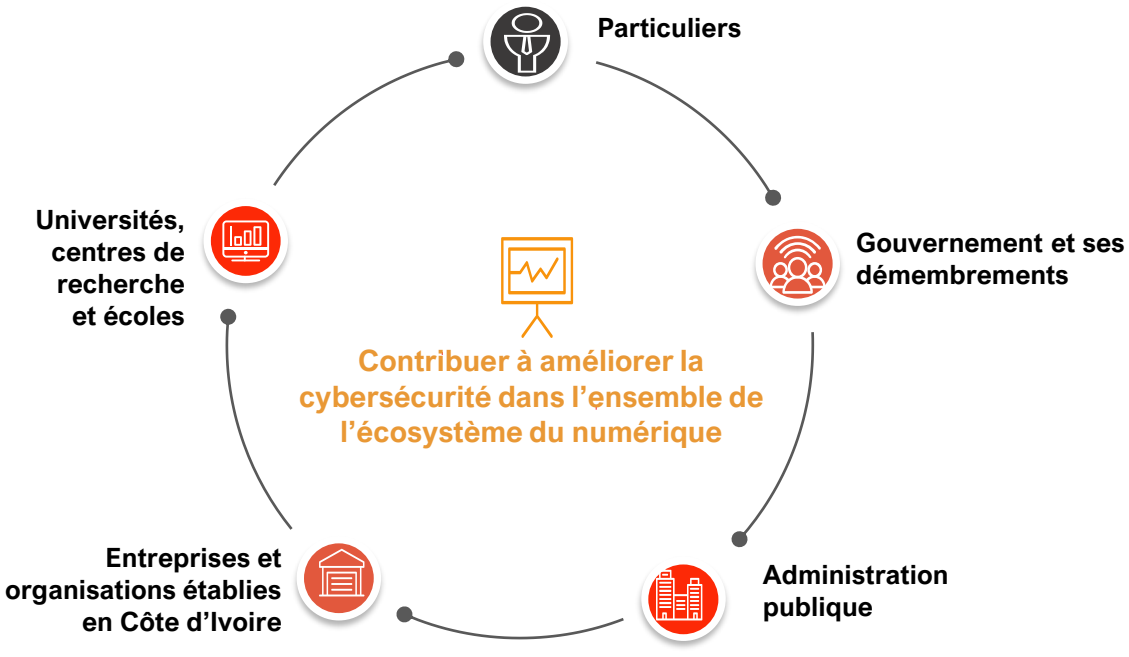
01 A PROPOS DU CI-CERT

02 ENJEUX DU PARTAGE D'INFORMATIONS DE CYBERSECURITE

03 QUELQUES PISTES DE SOLUTIONS

I. A PROPOS DU CI-CERT

Mission & Champs d'action



Article 7, Décret n° 2020-128 du 29 janvier 2020 portant création, organisation et fonctionnement du centre de veille et de réponse aux incidents de sécurité informatique dénommé CI-CERT

Services offerts

SERVICES PROACTIFS

- Monitoring, détection, analyse d'événements de sécurité
- Recherche, analyse et coordination de la publication des vulnérabilités
- Sensibilisation & communication
- Collecte, corrélation et diffusion d'information (Cyber intelligence)

SERVICES REACTIFS

- Collecte et analyse des incidents de sécurité de l'information
- Analyse des artéfacts et preuves numériques
- Coordination du traitement des incidents
- Appui à la gestion de crise

MANAGEMENT DE LA SECURITE

- Formation et appui au développement des capacités
- Appui au développement de politiques opérationnelles
- Appui au développement de SMSI

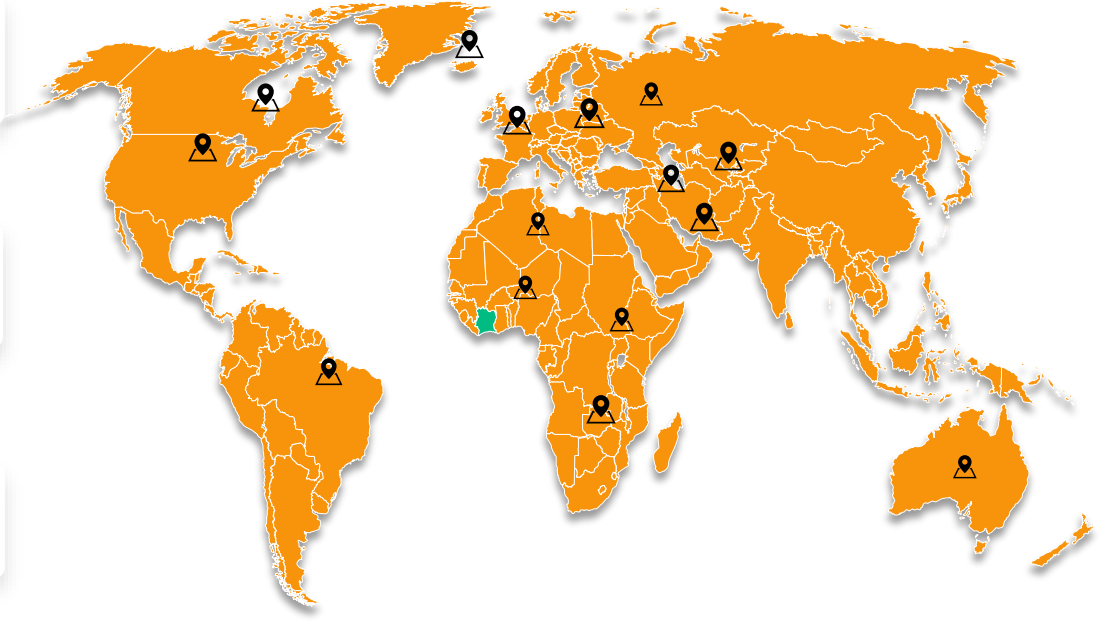
Réseaux de coopération

AU PLAN INTERNATIONAL

AU PLAN REGIONAL

Africa National CSIRT Working Group

AU PLAN NATIONAL



III.

ENJEUX DU PARTAGE D'INFORMATIONS DE CYBERSECURITE

Un cyber environnement fertile aux cybermenaces…

+ 50 Milliards FCFA de pertes financières directes

+ 22.000 dossiers de cybercriminalité traités

+ 4 Millions d'incidents de sécurité détectés et traités

Source: Rapports d'activités CI-CERT

- La surface des cyberattaques augmente en raison des développements technologiques, ce qui rend les cyberattaques plus sophistiquées et les attaquants plus dangereux.
- Les confits croissants entre les états-nation favorisent le développement de cyberarmes à des fins offensives ou défensives qui profitent aux groupes cybercriminels.
- Les cybercriminels sont également plus disposés à partager librement leurs informations, afin que les nouvelles techniques se répandent rapidement parmi les communautés criminelles, pendant que les organisations manifestent un manque « coupable » de communication/coordination
- La cyberdéfense est par nature une activité asymétrique et un combat déséquilibré dans lequel les règles du jeu sont clairement à l'avantage des acteurs menaçants, ce qui rend extrêmement complexe la prévention et la mitigation des cyberattaques.

Clarifications conceptuelles

Cybermenace ou cyber-threat

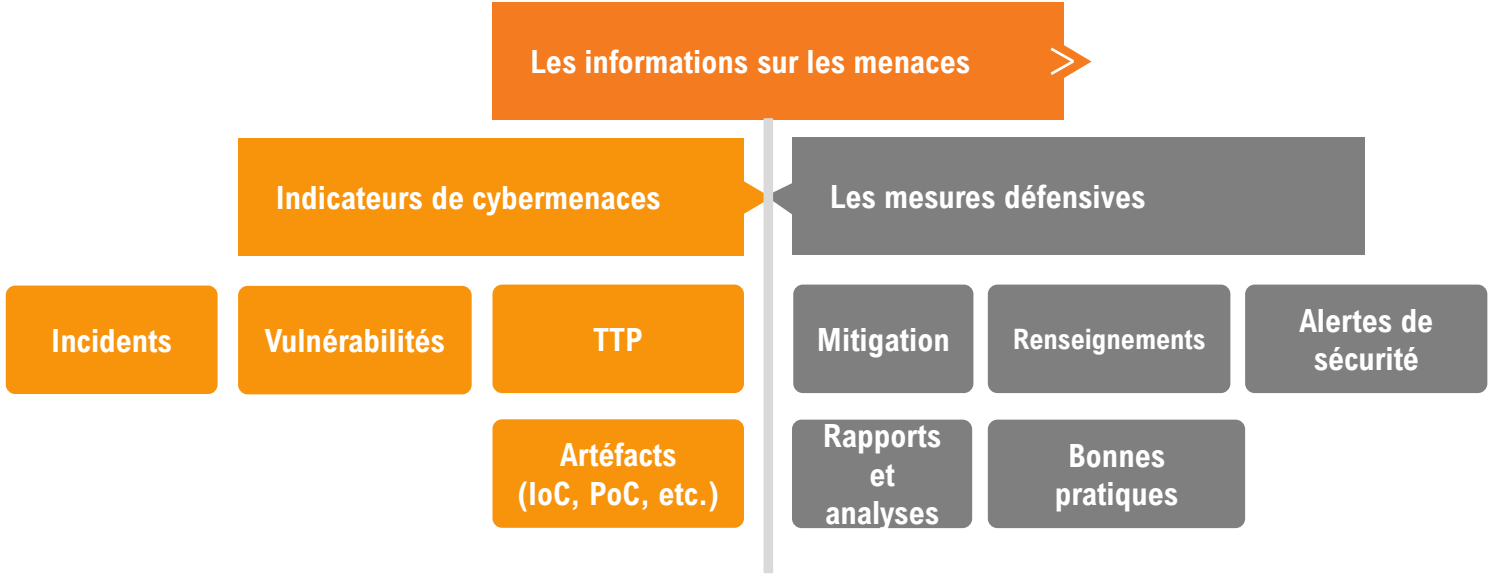
Une cybermenace est « toute circonstance ou tout évén ement susceptible d'avoir un impact négatif sur les opé rations d'une organisation (missions, fonctions, image ou réputation), actifs organisationnels, individus, autres organisations, ou la Nation par le biais d'un système d'i nformation via l'accès non autorisé, la destruction, divul gation ou modification d'informations et/ou déni de serv ice ».

Les informations sur les menaces sont toutes les informations liées à une menace qui pourraient ai der une organisation à se protéger contre une me nace ou détecter les activités d'un acteur.

Informations sur les menaces ou threat informations

Source: NIST Special Publication 800-150
Guide to Cyber Threat Information Sharing

Clarifications conceptuelles



Bénéfices du partage d'information de cybersécurité

01 PLUS GRANDE CAPACITE DE RESISTANCE AUX CYBERATTAQUES

- Amélioration des connaissances collectives et collaboration plus efficace
- Capitalisation sur l'expertise et les capacités analytiques des membres de la communauté de partage
- Meilleure compréhension de l'environnement des menaces et des risques (capacités, intention des acteurs menaçants)
- Meilleures capacités de détection des attaques
- Amélioration de la posture de sécurité et de l'agilité défensive
- Réduction des biais d'analyse situationnelle
- Création de renseignement de meilleure qualité

02 REDUCTION DES COÛTS D'INVESTISSEMENTS EN SECURITE

- Réduction des investissements grâce à la mutualisation des ressources de découvertes et d'identification des facteurs de risques
- Analyse stratégique des investissements facilitée
- Meilleure rationalisation des efforts relatifs au traitement des risques

La nécessité et les avantages du partage d'informations pour une cybersécurité solide et résistante est largement acceptée par toutes les parties prenantes, y compris commerciales et non organisations commerciales, agences gouvernementales et même les particuliers.

Les principaux défis…

01 ÉTABLIR LA CONFIANCE ENTRE LES ACTEURS (G, B, C).

- Garantir le respect de la vie privée et libertés civiles
- Responsabilité pénale et civile des acteurs
- Impacts sur la réputation et perte de confiance
- Risques de susciter plus de cyberattaques
- Impact économique lié au partage d'informations stratégiques
- Assurance qualité des informations partagées
- Equilibre entre Conformité légale et partage d'informations de cybersécurité

Les principaux défis…

02 MOBILISER LES RESSOURCES

- **Coûts des opérations de partage** (infrastructures, outils, personnel, formation, etc.)
- **Assurance d'interopérabilité et automatisation**: les formats de données et les protocoles de transport normalisés sont des éléments de base importants pour faciliter et pérenniser le partage d'informations
- **Savoir parler un langage compréhensible par le management** (axé sur le ROI)
- **Prévisions et investissements stratégiques**

III. QUELQUES PISTES DE SOLUTIONS

Quelques pistes de solutions

- Créer des mécanismes de régulation spécifique au partage d'information de cybersécurité (ex: CISA)
- Mettre en œuvre des programmes de partage d'information de cybersécurité plus interventionnistes pour des acteurs ou catégories spécifiques (ex: Infra Critiques)
- Adopter des standards pour la classification et la protection des informations partagées (ex: TLP Protocol)
- Développer des services de partages d'information de cybersécurité gratuits au niveau des CSIRT nationaux)
- Mettre en œuvre des métriques et des moyens d'évaluation de l'impact économique du partage d'information de cybersécurité
- Encourager l'adoption de solutions open source pour le partage d'informations de cybersécurité (MISP, Zimbra, Wordpress, etc.)
- Encourager le développement des compétences en matière de cyberintelligence et partage d'informations de cybersécurité
- Stimuler la mise en place de consortiums ou communautés d'intérêts pour le partage d'information, tels que les ISAC, ISAO, etc. (ex: FS-ISAC, EU-ISAC)

JE VOUS REMERCIE !

https://www.cicert.ci

(+225) 27 20 34 42 63 | (+225) 27 20 34 43 73

Marcory Anoumabo
18 BP 2203 Abidjan 18

infos@cicert.ci
incidents@cicert.ci