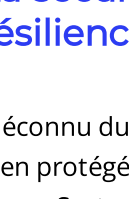
inCyber

Le média de la communauté FIC

Novembre 2021

LA NEWSLETTER inCyber

L'ÉDITO



Par le Général d'armée (2S) Marc WATIN-AUGOUARD

Général d'armée (2S), Fondateur du FIC, Ancien inspecteur général des armées - Gendarmerie nationale, il fut directeur du centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale (CREOGN) jusqu'en 2020.

Alerte sur le STAD le plus sensible !

En 2007, le thème du 1er FIC était prémonitoire : « la cybercriminalité, criminalité du XXIème siècle ! ». Près de 15 ans plus tard, les faits sont là et prouvent bien la migration simultanée, vers le substrat numérique, de la délinquance et de la conflictualité entre États.

La première migration est la suite logique d'un rapport risque pénal/gain escompté très favorable au prédateur ; la seconde offre aux États la possibilité de régler leurs comptes avec une certaine discrétion, privilégiant la « banderille numérique » à la « politique de la canonnière ». Ces deux migrations se croisent, puisque les États ne manquent pas de faire appel à des groupes criminels organisés pour agir à leur place : « *C'est pas moi, c'est ma sœur qu'a cassé le calculateur* », chantait, dans les années soixante Evariste, par ailleurs docteur en particules élémentaires...Certains États en ont fait leur second hymne national ...

Lire l'édito

L'INFO CYBER

CYBER RISQUES

La sécurité du DNS, clé de la résilience d'Internet ?

Méconnu du grand public et pas toujours bien protégé par les entreprises, le Domain Name System (DNS) est pourtant un actif critique de leur système d'information. Mal sécurisé, il peut devenir un vecteur privilégié des cyberattaques. Bien configuré, il s'avère être un outil redoutable contre elles.

Lire l'article

SÉCURITÉ INTÉRIEURE ET DÉFENSE

« Lutte informatique d'influence » : les Armées dévoilent leur nouvelle doctrine

Le 20 octobre, la ministre des Armées et le chef d'état-major des Armées ont présenté le troisième volet de la doctrine militaire des opérations dans le cyberespace. Après les canons de la lutte défensive et offensive, voici ceux de la lutte informationnelle ou « L2I ».

Lire l'article

CYBER RISQUES

L'assurance cyber : un jeu où l'information doit être partagée

La mesure du risque cyber est aujourd'hui imprécise à cause de la fragmentation de l'information, empêchant la constitution de digues financières robustes.

Lire l'article

SÉCURITÉ OPÉRATIONNELLE

L'effacement de données : un processus résilient

Si l'antivirus est devenu un outil de protection couramment utilisé, l'assainissement des matériels et des données en fin de vie n'est pas encore une pratique généralisée chez les entreprises et les particuliers.

Lire l'article

FIC NEWS

Prix de la startup FIC : ouverture prochaine des candidatures !

Le Prix de la startup FIC, organisé pour la deuxième année consécutive avec Atos, a pour objectif d'encourager l'innovation et l'entreprenariat dans le secteur de la cybersécurité. Chaque année, +40 jeunes pousses candidatent auprès du jury constitué d'utilisateurs finaux, de fonds d'investissement, de représentants de l'ANSSI et des ministères de l'Intérieur et des Forces armées.
Nouveautés cette année, outre le renforcement de la dimension européenne (à travers les candidats et les membres du jury), un nouveau prix orienté OT voit le jour. Il permettra de valoriser les startups proposant des innovations / solutions capables de répondre aux enjeux croissants liés à la cybersécurité du monde industriel. Un formulaire de candidature sera disponible sur le site Internet du FIC début décembre. Des sessions d'audition seront ensuite organisées pour les startups sélectionnées. Dans l'attente, n'hésitez pas à consulter les différents témoignages des anciens lauréats.

SUIVEZ-NOUS SUR LES RÉSEAUX !

SAVE THE DATE

Petit-déjeuner : " Obsolescence des équipements et logiciels : véritable enjeu de résilience "

30 novembre 2021

Une étude de 2020 du Global Network Insights Report de NTT témoigne du ralentissement du renouvellement et de la modernisation des équipements en Europe: 48 % sont aujourd'hui vieillissants ou obsolètes, et présentent par conséquent des failles non corrigées et des vulnérabilités logicielles qui sont autant de risques pour la sécurité des organisations. Alors que les modes de travail évoluent sous l'effet de la généralisation du télétravail et que se multiplient les espace "intelligents", plateformes d'échange et autres outils de partage, l'obsolescence des équipements et logiciels constitue un véritable enjeu de résilience. Quels risques font ils peser sur les organisations ? Une maintenance rigoureuse et une PSSI adaptées suffisent-elles à s'en prémunir ? Quelles solutions et quelles bonnes pratiques pour prévenir et y remédier ?

Je m'inscris !

Webinar : " Comment atténuer les risques liés aux cryptomonnaies grâce à une stratégie de conformité fondée sur les données ? "

1er décembre 2021

Malgré l'adoption accrue des cryptomonnaies à travers le monde, certaines institutions financières sont toujours réticentes à bancariser les entreprises de cryptomonnaies, et à investir pour tirer parti de leurs avantages. Et ce notamment en raison de la perception encore largement répandue selon laquelle les cryptomonnaies sont liées à des activités illicites impossible à contrôler.
Cependant, les blockchains offrent en réalité une transparence sans précédent, tant sur les activités liées à la criminalité financière que sur les activités économiques licites.
Joosep Vahtras, Responsable du conseil en conformité de Chainalysis, et Willem van den Brandeler, Chargé de compte, montreront que les données de la blockchain peuvent aussi aider à signaler les crypto-crimes et à élaborer des programmes de conformité fondés sur les données.

Je m'inscris !

LES PARTENAIRES D'INCYBER

Contact : contact@incyber.fr

Avisa Partners - 17 Avenue Hoche - 75008 Paris - FRANCE

inCyber
Le média de la communauté FIC