

FIC 2022

L'ESIEA ANIMERA UNE CONFERENCE SUR LA REPONSE AUX INCIDENTS ET L'INVESTIGATION NUMERIQUE (CORIIN)

THEMATIQUE : IOCMITE – QUAND SURICATA RENCONTRE MISP

MARDI 7 JUIN 2022 – 14h

Lille Grand Palais – Forum International de la Cybersécurité

Bonjour,

Dans le cadre du FIC 2022, le Centre d'expert contre la cybercriminalité français (CECIF) anime le mardi 7 juin 2022 au Grand Palais de Lille, premier jour de cet événement de référence, **la huitième conférence dédiée aux techniques de la réponse aux incidents et de l'investigation numérique, CoRIIN 2022.**

Cette journée permettra aux enquêteurs spécialisés, experts judiciaires, chercheurs du monde académique ou industriel, juristes, spécialistes de la réponse aux incidents ou des CERTs de partager et échanger sur les techniques du moment. L'ambition de cette conférence est de rassembler cette communauté encore disparate autour de présentations techniques ou juridiques de qualité, sélectionnées par le comité du CECIF.

A cette occasion, un expert de l'ESIEA, Sébastien Larinier, et Eric Lebond, fondateur de Stamus Networks tiendront une conférence le mardi 7 juin à 14h en salle Flandres (Grand Palais – Lille) sur le sujet suivant : IOCMite - Quand Suricata rencontre MISP. Cette conférence a pour but de présenter différents cas d'usage de l'outil opensource IOCMite. Ce dernier permet de créer des datasets d'indicateur de compromission pour permettre la détection en utilisant Suricata, sonde de détection d'intrusion opensource

L'inscription est obligatoire sur le site du [FIC](#), l'un des événements de la présidence française du Conseil de l'Union européenne sur les questions de sécurité et de confiance numérique. Le thème de cette année : « Shaping Europe's digital Future ».

Le programme complet CoRIIN 2022 :

Matinée

11h : Retour d'expérience sur un Zeppelin

11h30 : DFIR4vSphere: Investigation numérique sur la solution de virtualisation VMWare vSphere

12h : TAPIR : Un parseur d'artefacts pour la réponse aux incidents

12h30 : RETEX Carrefour SOC

Après-midi

14h : IOcmite - Quand Suricata rencontre MISP

14h30 : TinyCheck, détection d'implants passive sur smartphones via l'analyse de flux réseau

15h : Aspects juridiques de la biométrie dans les investigations numériques :
Lorsque le corps devient la clef

15h30 : L'utilisation du scambaiting à des fins préventives
contre les cyberarnaques : le cas des arnaques aux sentiments

16h30 : La montée en puissance des Initial Access Brokers (IABs) - quels constats faut-il en tirer ?

17h : La mutation de l'hébergement "bulletproof"

17h30 : Investigations sur un système de fichiers atypiques ou comment voyager dans le temps avec un groupe APT

Bien à vous,

Myriam



Myriam Boukaïa

Consultante en relations presse

Mob : 07 50 69 52 56

mboukaia@madamemonsieur.agency