CYBERSÉCU@LIM

10 OCTOBRE 2018

CONCOURS ÉTUDIANT CYBERSÉCURITÉ

Faculté des Sciences et Techniques - Limoges

Présentation des thèmes et inscriptions

Amphi JOLIET - 17h30

50 ANS Université de Limoges

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA HAUTE-VIENNE

Silpc
Informatique hospitalière

30 ANS 3iL INGENIEURS

Des actions de sensibilisations à la Sécurité de l'Information

Un concours pour valoriser l'enseignement supérieur local

CYBERSÉCU@LIM

Des créations de supports pédagogiques*

Une forte collaboration des acteurs locaux

** À usage non commercial*

- ***A l'initiative de la Préfecture de la Haute-Vienne et du GIP SILPC***
- ***Organisé en partenariat avec l'université de Limoges et le Groupe 3IL***

50 ANS Université de Limoges

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA HAUTE-VIENNE

Silpc
Informatique hospitalière

30 ANS 3iL INGENIEURS

Ordre du jour

- Enjeux et dispositifs juridiques
  - *N.BELILI, chargé de mission auprès du préfet de la haute Vienne*
  - *E. MAZATAUD, Direction Départementale de la Sécurité Publique de la Haute-Vienne (Police nationale)*
  - *D.FRESSARD, Gendarmerie Nationale*
- Présentation du Concours *(cybersecuatlim.groupe3il.fr)*
  - *Présentation du règlement*
  - *Planning et dates à retenir*
  - *Thèmes proposés par Comité d'organisation*
  - *Dotations*
  - *Inscriptions*

Actions de sensibilisation à la sécurité de l'information

à destination des utilisateurs *(PME/PMI/Hôpitaux/EHPAD/…)*

par des mises en situations concrètes

préparées et réalisées par des étudiants lors de la participation à un concours

50 ANS Université de Limoges

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA HAUTE-VIENNE

Silpc
Informatique hospitalière

30 ANS 3iL INGENIEURS

Qui : *Les étudiants justifiant :*

- *d'un BAC+2 validé*
- *d'une inscription de scolarité en Limousin en cours de validité*
- *d'une adresse de courriel @etu.unilim.fr ou @3il.fr*

Quoi :

- *restituer un projet de cybersécurité qui prendra la forme d'un ou plusieurs message(s) pédagogique(s) vidéo, en équipe, durant un temps déterminé (20 minutes Maxi) et sur un thème donné.*

  (un diaporama et/ou un fichier vidéo (d'une durée maximale de 5 minutes) et un POC (proof of concept) technique si le thème choisi le nécessite)

Comment :

- *En constituant des équipes de 3 personnes maximum (limitation à 20 équipes)*
- *En désignant un(e) chef(fe) d'équipe interlocuteur des organisateurs*
- *En s'inscrivant individuellement en remplissant un formulaire à transmettre par email à cybersecuatlim@silpc.fr*

  Conseil : Décrivez au dos du formulaire comment vous envisagez de traiter le/les thèmes choisis (3 maxi) - Ceci pourra être pris en compte pour l'affectation définitive du thème.
- *En se rapprochant d'un enseignant référent (Chaque équipe **devra** être obligatoirement rattachée à un enseignant référent)*

DES RÈGLES (EXTRAIT DU RÈGLEMENT) :

***Respect** de la législation française dans le cadre de ce concours et de la protection d'autrui :*

- *Droits d'auteurs et forme de plagiat (citer les sources)*
- *Tout comportement s'apparentant à de la cybercriminalité ou de l'escroquerie pourra provoquer une disqualification du concours par décision des organisateurs.*
- *…*

Les participants s'engagent également à respecter le règlement intérieur

THÉMATIQUE(S) DU CONCOURS

- *Chaque projet doit s'inscrire dans une des thématiques proposées et devra faire l'objet d'une validation par les organisateurs*
- *Chaque équipe a la possibilité de choisir 3 thèmes par ordre de préférence, noté de 1 à 3 sur le formulaire d'inscription*
- *Les équipes qui n'auront pas de projet ou dont le projet n'a pas été validé par les organisateurs hériteront du projet des organisateurs*

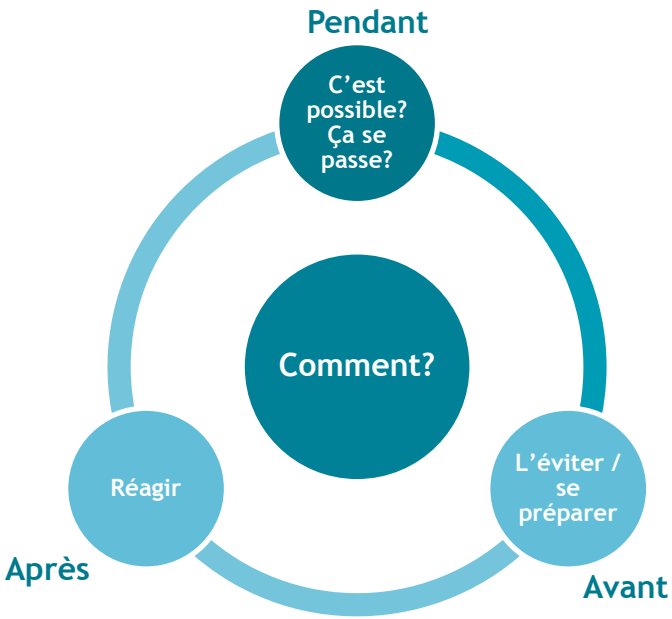
FORMAT, NOTATION ET PRIX :

Chaque équipe disposera de 20 minutes MAXIMUM pour présenter son projet, avec éventuellement quelques questions du jury. Les équipes sont libres de présenter leur projet à leur manière mais devront rendre à l'issue des restitutions, un support vidéo de 5 minutes maximum incluant des messages pédagogiques.

Les critères de notation (basé sur 20 points) sont les suivants :

- *Mise en situation (POC technique, scénario...) - 10 points*
- *Originalité du format et valeur pédagogique - 10 points*

Être Victime d'une Cyber Attaque



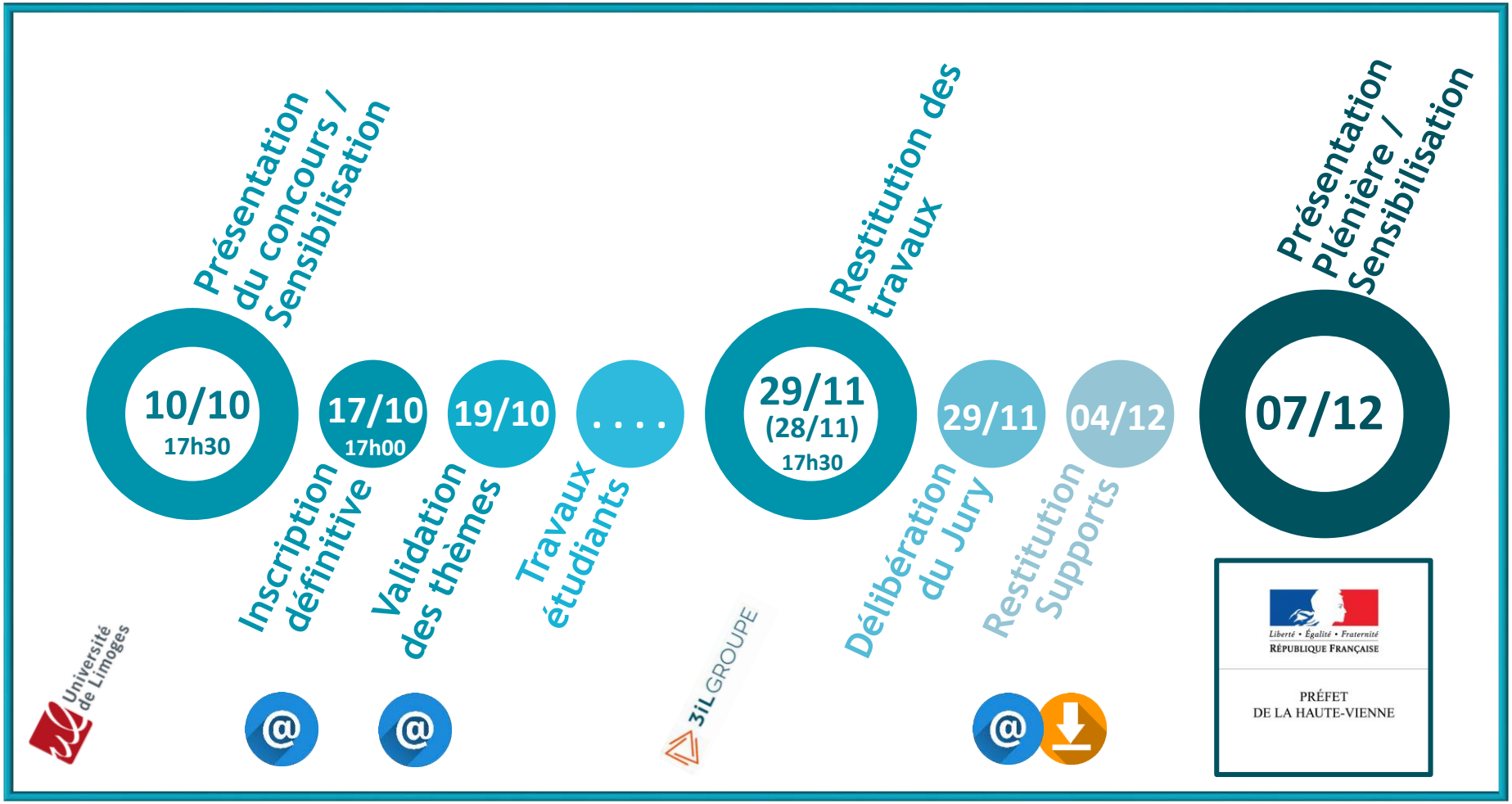
JURY :

- *RSSI – Chargé de Mission de la Préfecture de la Haute-Vienne*
- *Représentants Université & 3il : Équipes Pédagogiques*
- *Help Desk du GIP SILPC*
- *Représentant Établissement de Santé*
- *Représentant PME/PMI locale*
- *Cellule de communication (du Comité d'Organisation)*
- *Un professionnel représentant d'un sponsor du concours*

DOTATION

- *+ de 2000 € de lots à gagner*
  (Par exemple : Nintendo switch, Casques Audio, …)
- *Les meilleures équipes seront sélectionnées pour présenter leur projet le 7 décembre et seront récompensées lors de la remise des prix à la Préfecture*

Présentation du Concours / Déroulement



http://cybersecuatlim.groupe3il.fr/
cybersecuatlim@silpc.fr

50 ANS Université de Limoges

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET
DE LA HAUTE-VIENNE

Silpc
Informatique hospitalière

30 ANS 3iL INGENIEURS

Thèmes Proposés

1	Cryptovirus / Ransomware
2	HotSpot Public
3	Vol / Perte / Partage *(support USB, Portable, …)*
4	Keylogger Materiel
5	Mise à jour *(OS, Logiciels)*
6	Mots de Passe *(Complexité/Stockage/Mémorisation dans les outils)*
7	Sécurité des objets connectés/Domotique
8	Ingénierie Sociale
9	Paiement en Ligne
10	Téléchargement *(Illégal, outils gratuits)*
11	Les services "Gratuits" *(Cloud, Réseaux Sociaux, Condition Générale d'utilisation)*
12	La Messagerie
13	Usurpation d'identité / Verrouillage de session
14	Données de Santé *(Echange avec Médecin / RDV / Résultat de Labo…)*
15	La Mobilité *(Téléphone)*
16	Renouvellement des équipements
17	DarkWeb / DeepWeb
18	Géolocalisation
19	Identité Numérique
20	BYOD *(périphériques corrompus amenés par l'utilisateur)*
21	Utilisation d'équipements professionnels dans un cadre privé
22	Imprimantes photocopieurs
23	Webcam/micro/téléphones *(Utilisation à l'insu de son propriétaire)*
24	Objets publicitaires
25	Espionnage industriel
26	IoT industriel *(scada…)*
27	Sécurité physique des bâtiments (badges)

Exemple Ransomware

Référence : https://secnumacademie.gouv.fr/

SecNumacadémie.gouv.fr
Formez-vous à la sécurité du numérique

Être victime d'un composant logiciel malveillant dont l'objectif est de prendre en otage vos données

Thèmes Proposés

- POC Technique
- Support de Restitution
- Vidéo

Pendant

- Par navigation ou usage messagerie (Pièce jointe)
- Exécution d'un composant de chiffrement

Après

- Isolement des composants impactés
- Ne pas éteindre
- Connaissance Crypto Monnaie
- Situation face à demande de rançon
- Dépôt de plainte / Déclaration incidents (https://www.cybermalveillance.gouv.fr)
- Comment restauré
- Conservation des preuves
- Faire appel à des experts

Avant

- Sauvegarde
- Mise à jour logiciels/OS
- Droits Utilisateurs
- Anti-virus
- Vigilance Usage de la messagerie / Navigation

50 ANS Université de Limoges

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA HAUTE-VIENNE

Silpc
Informatique hospitalière

30 ANS 3iL INGENIEURS

- 7 SEMAINES
- UNE VINGTAINE DE THÉMATIQUES
- VALORISER SES COMPÉTENCES
- FAVORISER LA CRÉATION DE RESSOURCES PÉDAGOGIQUES POUR UN LARGE PUBLIC
- + DE 2000 € DE LOTS À GAGNER !

CyberSecu@Lim

Valoriser vos formations

Pour nous contacter :

Référents Enseignants

Benjamin Chervy
Courriel : chervy@3il.fr

Emmanuel Conchon
Courriel : emmanuel.conchon@unilim.fr

Damien Sauveron
Courriel : damien.sauveron@unilim.fr

GIP SILPC

Patrice Boisseuil
Courriel : patrice.boisseuil@silpc.fr
Emilie Guenant
Cellule Communication
Courriel : emilie.guenant@silpc.fr

Merci pour votre participation

N’hésitez pas à relayer l’évènement