



The bridge to possible

# Table ronde avec nos Experts (Partie 2)

## Sécurité des Infrastructures Informatiques

Comment agir en cas d'urgence – Procédures et meilleures pratiques.

Experts : Francesco Molino, Xavier Crèvecoeur, Alain Faure et Patrick Cardot

Modérateur : Jimena Saez

Événement spécial – 31 mars 2022

# Nos Experts



Francesco  
Molino  
Canada



Patrick  
Cardot  
France



Xavier  
Crèvecoeur  
France



Alain  
Faure  
Belgique

# Agenda

- Introduction
- Bloc 1 – Email Security
- Que faire une fois hacké ?
- Bloc 2 – Comment réagir
- Interview (vidéo)
- Bloc 3 – Sécurité
- Tour de Table (Tous)



## Bloc Questions

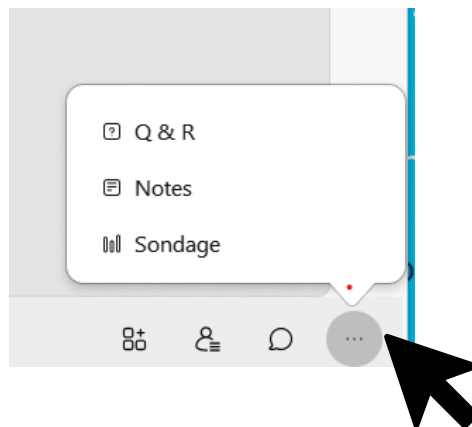
- Questions pour l'expert
- Questions de l'audience
- Intervention des autres panelistes

## Tour de Table

- Sujets en général
- Échange d'idées

## Interview

- Diffusion d'une vidéo



# Introduction

Participez !

Répondez à l'enquête  
et partagez-nous  
votre avis ou posez  
des questions.



Gobelet thermique en acier



Casquette brodée



Wireless Phone Charger Deluxe



NoWire Mouse Pad is 10W fast Qi charger and mouse mat

# Polling Question 1

En matière de mots de passe quelle est la meilleure bonne pratique ?



Un mot de passe...

- Très long
- Complexe
- Que l'on peut mémoriser
- Avec des étoiles


# Bloc 1 – Questions et Réponses

- Protection Mail
- Les attaques
- Les mesures de protection

# Polling Question 2

Une arnaque  
au président est ...



1. Une tentative d'arnaque sur la plus haute instance de l'entreprise
2. Une technique d'évasion qui consiste à corrompre un président imprudent
3. Une technique par laquelle un fraudeur usurpe l'identité d'un dirigeant 
4. Une falsification d'un bulletin de vote



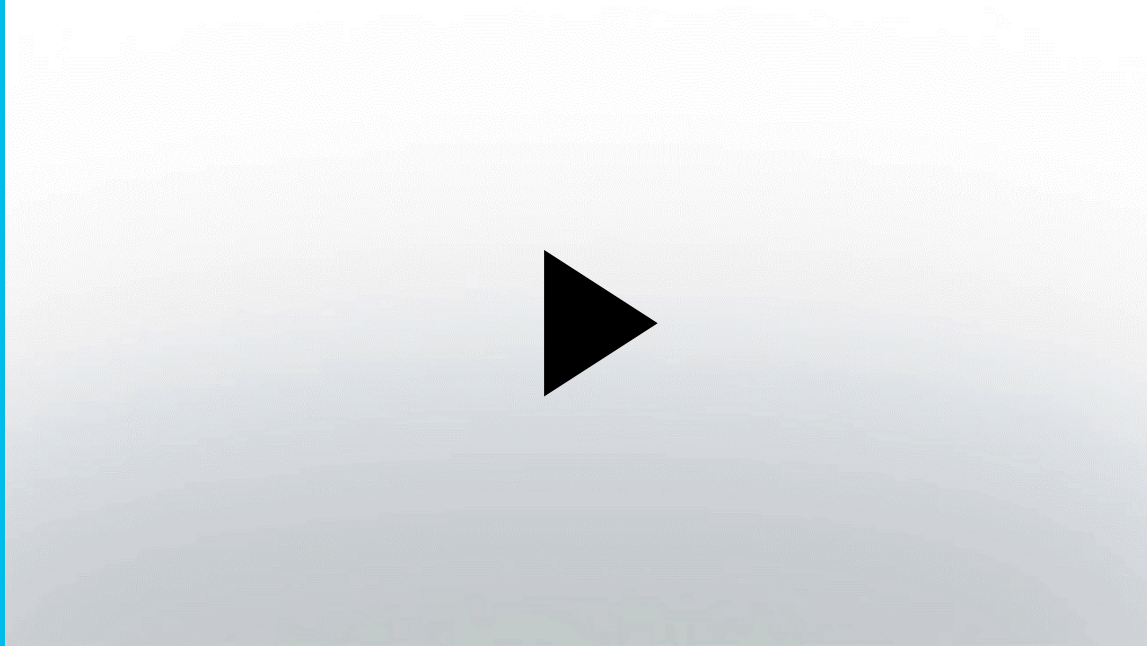
# Interview à Jérôme HENNECART



## Sécurité informatique Ethical Hacking : Apprendre l'attaque pour mieux se défendre (6e édition)

ACISSI, Damien BANCAL, Franck EBEL, Frédéric VICOONE, Guillaume FORTUNATO, Jacques BEIRNAERT-HUVELLE, Jérôme HENNECART, Joffrey CLARHAUT, Laurent SCHALKWIJK, Raphaël RAULT, Remi DUBOURGNOUX, Robert CROCFER, Sébastien LASSON  
ISBN : 978-2-409-03366-7

# Vidéo – Interview Jérôme Hennecart



<https://bit.ly/INT-FRmar22>

# Bloc 2 - Questions et Réponses

- Surveiller les vulnérabilités
- Anticiper la menace
- Mises à jour firmware

# Polling Question 3

Un firewall est aussi appelé...



1. Un paravent
2. Un paratonnerre
3. Un parapluie
4. Un pare-feu

# Que faire une fois hacké ?

Notes - Sécurité

Alain Faure - CCIE #8935 R&S

# Directives de sécurité

## 1. Vérifiez vos **sauvegardes**

Firmware, configurations, fichiers divers dans les équipements, etc. et faites en si ce n'est pas le cas. Surtout il faut les conserver hors de tout système reprogrammable et hors réseau. Ex : bandes, documentation papier.

## 2. Vérifiez régulièrement l'**intégrité**

En partie automatisé... des firmwares, logiciels etc. (des virus, attaques qui ont pu être prépositionnés)

## 3. Renouvelez votre politique de **mot de passe**. C'est le moment !

Pas moins de 15 caractères sur l'infrastructure (maj. min. chiffres, signes). Conservez les mots de passe sur du papier et non pas dans les logiciels (fussent t-ils agréés !!! )

# Réactions 1/4 – Coupez l'accès réseau

## En urgence :

- ✓ Déconnectez les câbles
- ✓ Préplanifiez cette opération (et choisir où couper)

## Importance :

- ✓ D'un réseau spécifique d'administration matériel et séparé : non VLAN
- ✓ De la documentation papier



# Réactions 2/4 – Ne pas éteindre les machines

## En urgence :

- ✓ Mais les déconnecter toutes du réseau
- ✓ Ne plus toucher jusqu'à expertise

## Importance :

- ✓ Ayez les coordonnées d'un expert en sécurité externe (car en interne la vulnérabilité n'a pas été adressée).

The screenshot shows the website of the Swiss Federal Cyber Security Centre (NCSC). The header includes the navigation path: Administration fédérale > DFF > NCSC. The logo of the Swiss Confederation is visible, along with the text: Schweizerische Eidgenossenschaft, Confédération suisse, Confederazione Svizzera, Confederaziun svizra. The main title is "Centre national pour la cybersécurité NCSC". Below the header is a horizontal menu with categories: Actualité, Cybermenaces, Informations pour (selected), Stratégie SNPC, Documentation, and Général. A breadcrumb trail reads: Page d'accueil NCSC > Informations pour > Informations pour des entreprises > Cyberattaques. The main content area is titled "Cyberattaque – que faire?". It lists several articles: "Attaque DDoS - que faire?", "Cyberattaque - que faire? Aide-mémoire à l'intention des CISO", "Fuite de données - que faire?", and "Rançongiciels - que faire?". Each article is accompanied by a small image: a laptop with a DDoS attack visualization, a hand holding a document, and a person using a laptop.



# Réactions 3/4 – Récupérer les logs

## En urgence :

- ✓ Par les interfaces d'administration locales aux machines.
- ✓ Routeurs, Switches, serveurs, PC utilisateurs, téléphones.

## Importance :

- ✓ Du NTP (temps)
- ✓ D'un serveur Syslog durci

### **logging host**

Logs messages to a UNIX syslog server host.

For *host*, specify the name or IP address of the host to be used as the syslog server.

To build a list of syslog servers that receive logging messages, enter this command more than once.

For complete syslog server configuration steps, see the "[Configuring UNIX Syslog Servers](#)" section.

# Réactions 4/4 – Traiter les supports mémoire

## En urgence :

- ✓ Une fois la machine éteinte selon une procédure d'urgence (qui peut être une coupure de courant brutale pour éviter des modifications intempestives), tenter une récupération pour les données importantes.

## Importance :

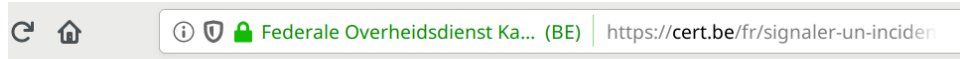
- ✓ Coordonnées expert en récupération de data sur disques.



# Signalez ! : Belgique

Signalement des attaques :

<https://cert.be/fr/signaler-un-incident>



NL FR DE EN



À propos Signaler un incident Conseils Actualités Offres d'emplo

## | SIGNALER UN INCIDENT



**Premiers secours en cas de  
cyberattaque**

# Signalez ! : Canada

*« Les signalements ne mènent pas toujours à une enquête mais dans certains cas, nous pouvons être en mesure d'aider à récupérer ce qui a été perdu ou endommagé. »*

<https://www.antifraudcentre-centreantifraude.ca/>

<https://www.antifraudcentre-centreantifraude.ca/report-signalez-fra.htm>



The screenshot shows the top of the website <https://signalement.centreantifraude.ca>. It features a "BÊTA" badge and a message: "Ceci est une nouvelle version du service mais votre rapport sera né". Below this are the logos for the "Gouvernement du Canada" and "Government of Canada". A yellow banner contains a warning icon and the text "En savoir plus sur les fraudes liées à la COVID-19". The main heading is "Signalez une fraude informatique". Below the heading, it states: "Votre signalement aidera la Gendarmerie royale du Canada (GRC) et le Ce d'incidents." There is a section titled "Signaler en ligne" with a text box containing: "Signalez un incident si vous, quelqu'un que vous connaissez ou une entreprise a perdu ou pourrait avoir perdu de l'argent, des données ou des informations personnelles, ou a été touché par un rançongiciel." and an information icon. A dark blue button labeled "Rapport complet" is positioned below the text box.

# Signalez ! : France

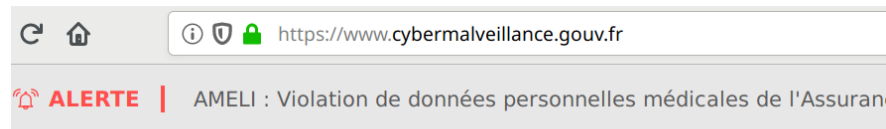
## 2 - Des conseils et solutions

« Des conseils et solutions vous sont proposés pour résoudre votre problème.

ET / OU

Vous pouvez faire une demande de mise en relation avec un professionnel spécialisé. »

<https://www.cybermalveillance.gouv.fr/>



# ASSISTANCE ET PRÉVENTION RISQUE NUMÉRIQUE AU SERVICE DES PUBLICS

LES MENACES ET BONNES PRATIQUES

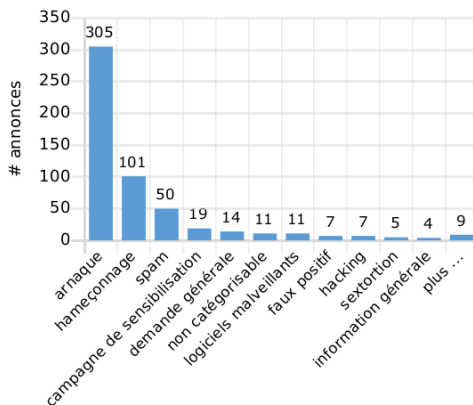
L'ACTUALITÉ DE LA  
CYBERMALVEILLANCE

# Signalez ! : Suisse

Signalement des attaques :

<https://www.report.ncsc.admin.ch/fr/>

NCSC.ch: Annonces reçues par catégorie: semaine 11/2022



Administration fédérale > DFF > NCSC

Page d'accueil Annoncer Contact

 Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

**Centre national pour la cybersécurité NCSC**

Actualité Cybermenaces Informations pour Stratégie SNPC Documentation Généralités concernant NCSC

Page d'accueil NCSC > Actualité > Actuel > Ouverture de la consultation relative à l'introduction d'une obligation de

< Actuel

## Ouverture de la consultation relative à l'introduction d'une obligation de signaler les cyberattaques

**12.01.2022 - Aujourd'hui, le Conseil fédéral a décidé d'ouvrir la procédure de consultation sur l'avant-projet de modification de la loi sur la sécurité de l'information relatif à l'introduction d'une obligation de signaler les cyberattaques contre les infrastructures critiques. Cet avant-projet crée les bases légales nécessaires à l'introduction de l'obligation de signalement et définit les tâches du Centre national pour la cybersécurité (NCSC), qu'il institue comme centrale de signalement des cyberattaques. La consultation durera jusqu'au 14 avril 2022.**

# Recevoir des notifications de Cisco

[Cisco.com/security](https://cisco.com/security)

[psirt@cisco.com](mailto:psirt@cisco.com)

<https://tools.cisco.com/security/center/rss.x?i=44>

<https://www.cisco.com/c/en/us/support/web/tools/cns/notifications.html>

<https://developer.cisco.com/psirt/>

## Receiving Security Vulnerability Information from Cisco

There are several ways to stay connected and receive the latest security vulnerability information from Cisco.

Cisco Security: [cisco.com/security](https://cisco.com/security)

Contact PSIRT: [psirt@cisco.com](mailto:psirt@cisco.com)

RSS feeds: <http://tools.cisco.com/security/center/rss.x?i=44>

My Notifications: <https://www.cisco.com/c/en/us/support/web/tools/cns/notifications.html>

Cisco PSIRT openVuln API: <https://developer.cisco.com/site/PSIRT/>

© 2021 Cisco and/or its affiliates. All rights reserved.



## Incident Handling Process

PSIRT is notified of a security incident



PSIRT prioritizes and identifies resources



PSIRT coordinates product impact assessment and fixes



Customers and the public are notified simultaneously

# Polling Question 4

Qu'est-ce qu'une attaque par force brute ?



1. Secouer violemment la victime pour avoir son mot de passe
2. Tester une multitude de mot de passe jusqu'à trouver le bon
3. Pousser un utilisateur de sa chaise pour lui piquer son PC
4. Casser le chiffrement d'un fichier à l'aide d'une CPU très puissante

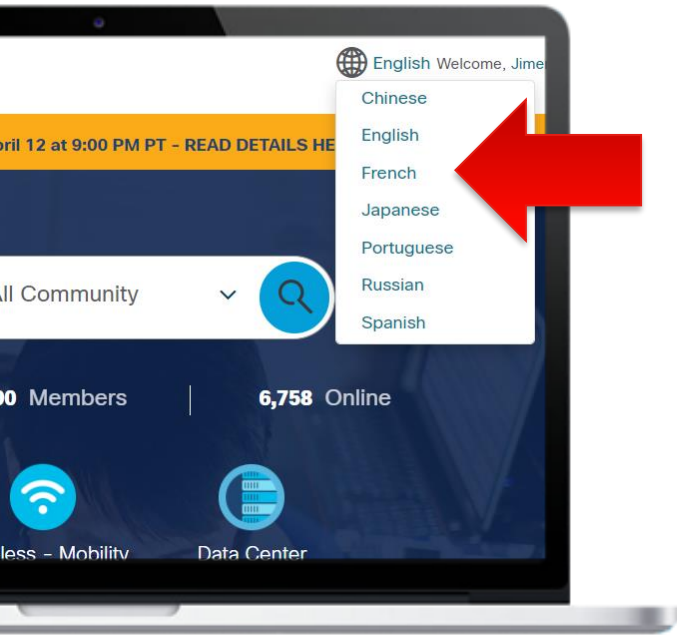


# Bloc 3 – Questions et Réponses

- Attaque DDoS
- Phishing
- Détection de codes malveillants de sabotage (wiper)

Tour de Table

# Où que vous soyez restez connecté...



- Facebook [CiscoSupportCommunity](#)
- Twitter [@cisco\\_support](#)
- YouTube [CiscoSupportChannel](#)
- LinkedIn [Cisco Community](#)
- Instagram [CiscoSupportCommunity](#)



Répondez à notre enquête !



The bridge to possible