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 Crèvecœur, Alain Faure et Patrick Cardot
Modérateur : Jimena Saez

Événement spécial – 31 mars 2022

Nos Experts

Francesco Molino
Canada

Patrick Cardot
France

Xavier Crèvecœur
France

Alain Faure
Belgique

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

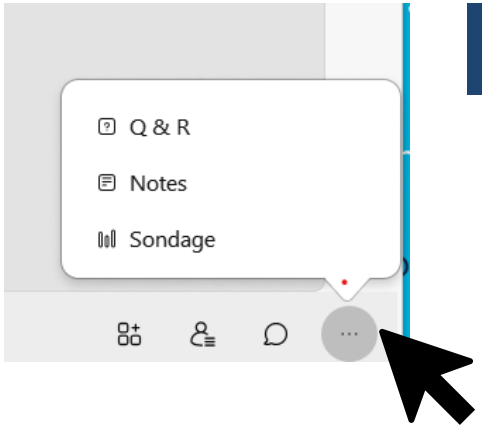
Agenda

- 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



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Introduction

Participez !

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

Casquette brodée

Gobelet thermique en acier

Wireless Phone Charger Deluxe

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Bloc 1 – Questions et Réponses

- Protection Mail
- Les attaques
- Les mesures de protection

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

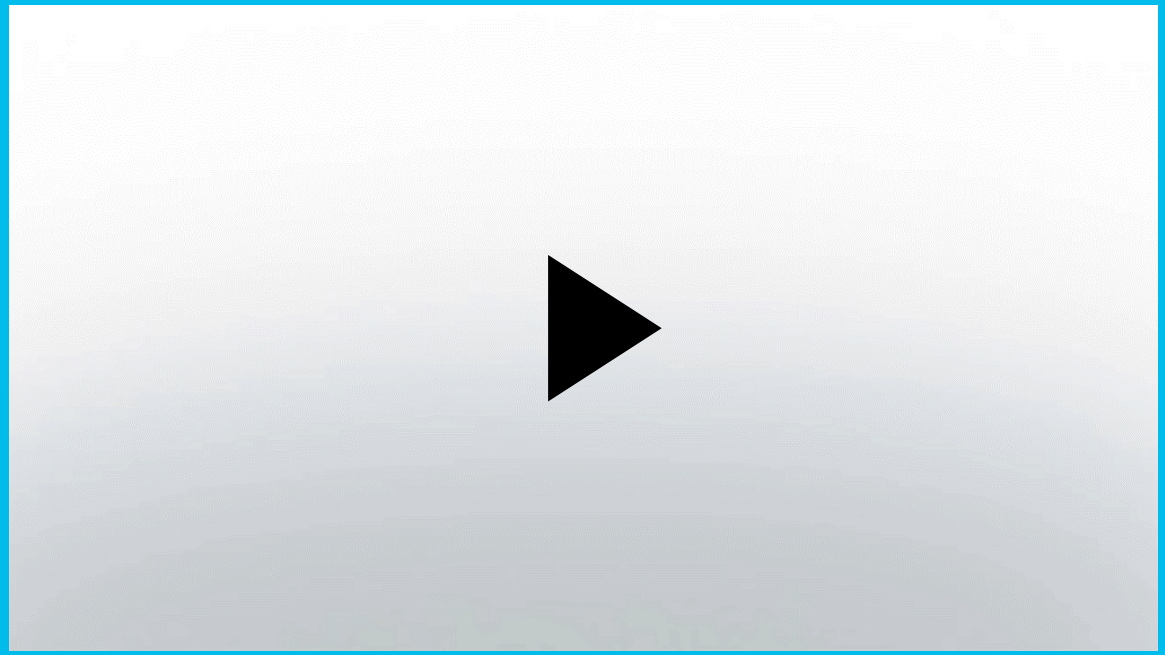
© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Interview à Jérôme HENNECART

Sécurité informatique
Ethical Hacking : Apprendre l'attaque pour mieux se défendre (6e édition)
ACISSI, Damien BANCAL, Franck EBEL, Frédéric VICOGNE, 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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Vidéo – Interview Jérôme Hennecart



https://bit.ly/INT-FRmar22

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Bloc 2 – Questions et Réponses

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Polling Question 3

Un firewall est aussi appelé...

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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 !!!)

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

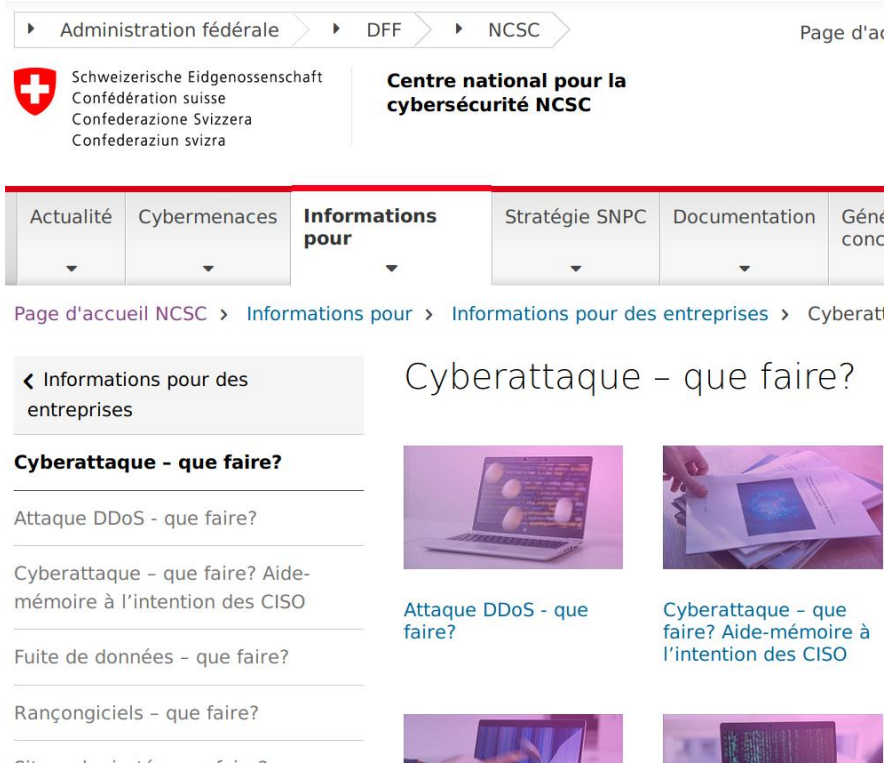
Réactions 2/4 – Ne pas éteindre les machines

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).



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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.

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Signalez ! : Belgique

Signalement des attaques : https://cert.be/fr/signaler-un-incident

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Signalez ! : France

2 – Des conseils et solutions

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

ET / OU

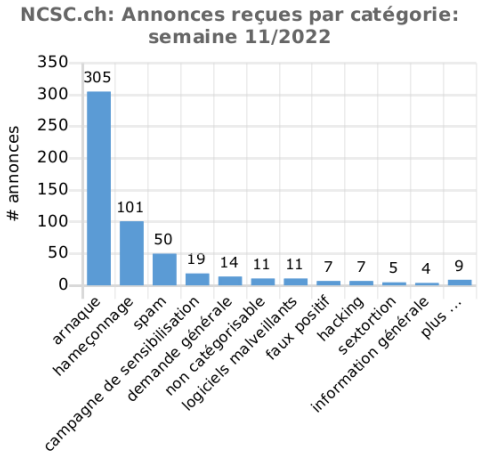
Vous pouvez faire une demande de mise en relation avec un professionnel spécialisé. »

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

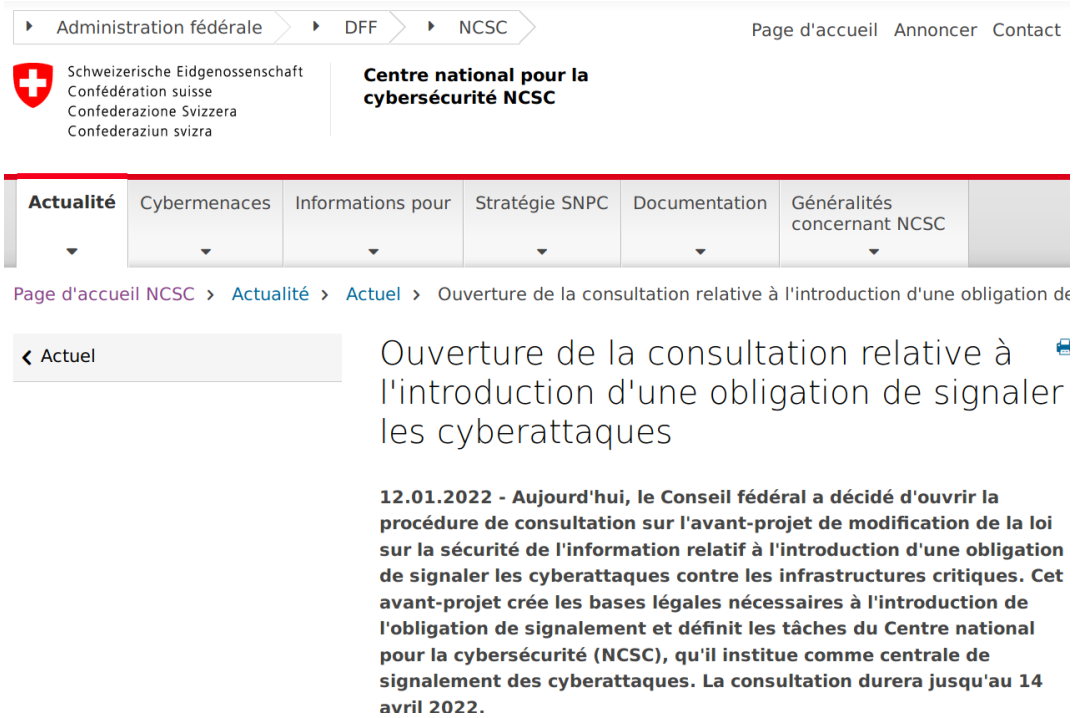
Signalez ! : Suisse

Signalement des attaques : https://www.report.ncsc.admin.ch/fr/



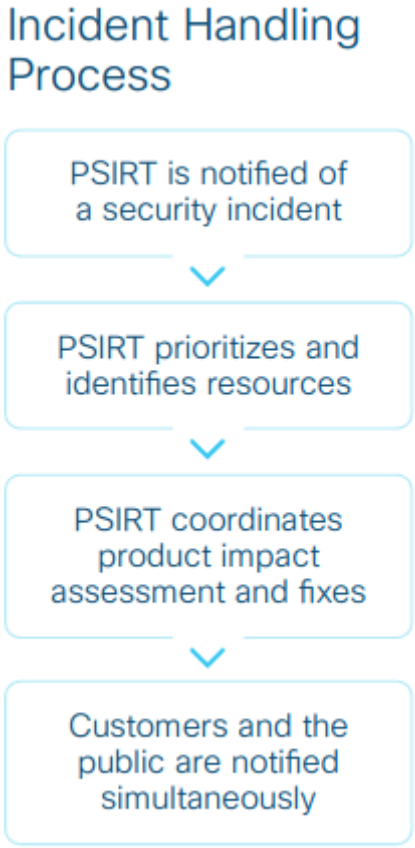
© 20

ential



Recevoir des notifications de Cisco

Cisco.com/security
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/



© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

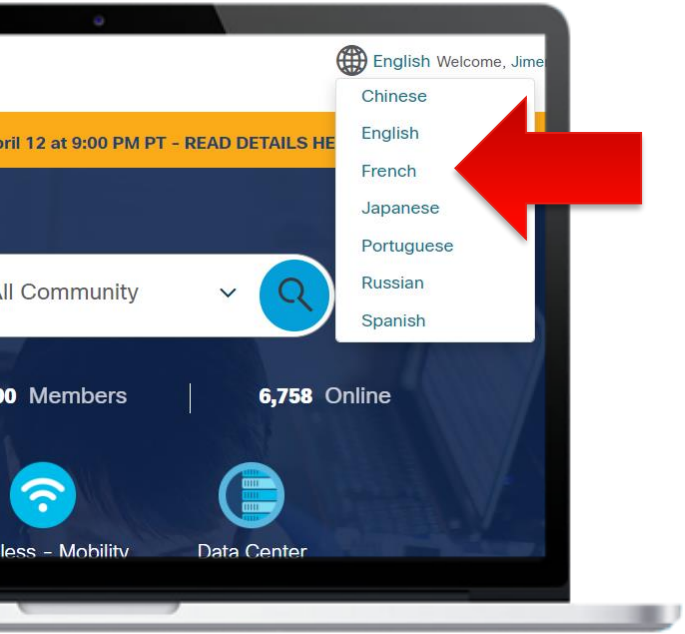
Bloc 3 – Questions et Réponses

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

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tour de Table

Où que vous soyez restez connecté…



- Facebook CiscoSupportCommunity
- Twitter @cisco_support
- YouTube CiscoSupportChannel
- LinkedIn Cisco Community
- Instagram CiscoSupportCommunity

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Répondez à notre enquête !

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The bridge to possible