
RICHTER
CYBER

RICHTER

DATE : Le jeudi 5 avril 2018
HEURE : de 8 h 30 à 19 h
LIEU : À l'hôtel Hyatt Regency à Montréal (1255, rue Jeanne-Mance, Montréal, QC H5B 1E5)

Cybercriminalité

Survol des incidents de sécurité marquants de l'année 2017 et les leçons à en tirer

Nos panellistes

Jean-François se spécialise dans l'architecture et la sécurité des gros réseaux. Au cours de ses mandats, il a, entre autres, joué un rôle majeur dans le design et le déploiement du nouveau réseau des HEC, UdeM, Centre de Recherche du CHUM, épaulé la STM (Société de Transport de Montréal), plusieurs universités, commissions scolaires, prisons, hôpitaux, la Bibliothèque et archives nationales du Québec et endurci le réseau d'un porte-avion français. Il à récemment effectué plusieurs audits de sécurité dans les secteur financier et de la pétrochimie. Jean-François a aussi occupé plusieurs postes en sécurité réseau, ingénierie et consultation pour Desjardins, CGI, Group Telecom, et SINC/Avance Services Réseaux. Ancien Paramédic en soins avancés, il carbure aux défis et missions de type SWAT. **Jean-François a fondé Satori en 2005**, et ce groupe de conseillers sénior offre des services-conseils principalement dans de multiples domaines.

Loren est **architecte sécurité chez Ubisoft**. Il est un analyste de sécurité expérimenté en évaluation des risques de sécurité technique, analyse de vulnérabilité, tests de pénétration et révision d'architecture de sécurité. Loren travaille actuellement comme analyste DFIR afin de détecter des incidents, faire l'analyse des vidanges de mémoire et aider à répondre aux incidents.
Ses travaux récents comprennent des examens de l'architecture de sécurité et des tests de vulnérabilité des principales applications « Software as a Service » (SAAS), ainsi que de nombreuses applications commerciales d'envergure. Le but était de faire la correspondance entre les vulnérabilités techniques et la réalité commerciale des entreprises en priorisant l'impact des risques et en aidant les services informatiques à trouver des solutions innovantes et rentables. Loren a aussi mené des exercices de pénétration « Red Team ». Une vaste expérience en tant qu'architecte de la sécurité informatique dans 3 grands domaines: jeux vidéo, télécommunications, opérations bancaires

Yves est un **consultant indépendant et expert en sécurité informatique, expert technique sur les normes PCI**, orateur, et auteur du livre PCI DSS made easy (version anglaise actualisée en décembre 2017, et présentement en traduction vers le français) qui explique la conformité à la norme PCI DSS (aussi disponible en 4 volumes numériques sur les plateformes Amazon Kindle and Apple iBooks stores). Yves a plus de 16 ans d'expérience professionnelle en technologie de l'information, ayant alterné entre des rôles en consultation, en développement logiciel et en sécurité informatique. Il a travaillé en français, anglais et espagnol, en Europe, au Canada, au Mexique et aux États-Unis. Yves possède les certifications de CISSP (Certified Information Systems Security Professional) et PCIP (PCI Professional) et est en un membre de OWASP (The Open Web Application Security Project).
Yves est titulaire d'un baccalauréat en génie informatique de l'Université de Sherbrooke et d'un MBA de l'Université de Notre Dame aux États-Unis.

Gabriel est le **président et co-fondateur de Delve Labs** ainsi que le président et co-fondateur de l'événement NorthSec.
Initialement impliqué dans la gestion et l'optimisation des processus de développement logiciel, il décide en 2011 de devenir consultant en sécurité pour occuper la fonction d'expert en test d'intrusion dans diverses entreprises du Québec. Appuyé sur cette expérience, il lance en 2014 sa propre entreprise, Delve Labs, ayant pour mission de révolutionner le domaine de la découverte de vulnérabilités en s'appuyant sur l'intelligence artificielle. Occupant maintenant un rôle plus administratif, il continue à s'intéresser aux grands courants qui régissent l'évolution de la cybersécurité et tente d'apporter des solutions novatrices aux entreprises d'ici et d'ailleurs.

Système de sondage

http://www.101vote.com/

Protégé via ZKIP

Avez-vous déjà été confrontés à de la cyber-criminalité ?

A. Oui directement, mon entreprise a été attaquée !

B. Oui directement, mais l'attaque n'a pas vraiment fonctionné ?

C. Non, pas vraiment, mais en fait je ne sais pas trop…

D. Non, je suis sûr que tout va bien !

E. Je ne dirais rien !

F. Je ne sais pas ce qu'est la cyber-criminalité…

Question 1 : quel type d’attaque ?

A. Virus, Maliciel (Malware), Botnet

B. Rançongiciel (Ransomware)

C. Hameçonnage (Phishing)

D. Déni de service ou déni de service distribué (DoS ou DDoS)

E. Toutes ou plusieurs des réponses ci-dessus

F. Je ne sais pas…

Que dire de l’aspect local de la cybercriminalité ?

Question 2 : quel impact majeur sur vos affaires ?

A. Indisponibilité de systèmes ou d'applications

B. Perte monétaire directe

C. Perte de réputation

D. Utilisation non-prévue de personnel

E. Utilisation non-prévue de services professionels tiers

F. Perte ou fuite de données

Question 3 : selon vous combien coûte une attaque moyenne ?

A. + de 1M$

B. De 500k$ à 1M$

C. De 100 à 500k$

D. De 50 à 100k$

E. - de 50k$

F. Aucune idée

Des exemples de la perte directe de valorisation ou de capital ?

Comment doivent se gérer les pénalités ?

Comment doivent se gérer les pénalités ?

À quel contrôle n’avez-vous pas du tout pensé ?

A. Plan de sortie du fournisseur infonuagique

B. Gestion des incidents et cyber-crises avec le fournisseur infonuagique

C. Gestion de la preuve digitale infonuagique

D. Gestion des clefs maîtres (réelles) de chiffrement des données

E. Augmentation des prix ou modèles de licences substantielles

F. Je crois avoir pensé à tout !

Quels sont les enjeux des régulations et régulateurs ?

Comment gérer cette hygiène face à la cyber-criminalité?

Vous sentez-vous prêt à gérer une cyber-crise liée directement à de la criminalité ?

A. Oui totalement !

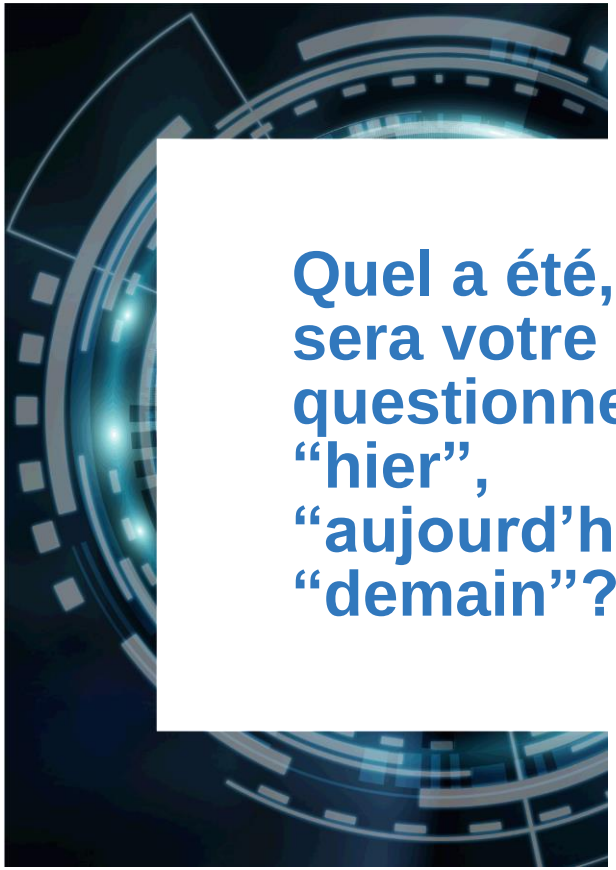
B. Oui, pas trop mal.

C. Moui, pas sûr…

D. Bof, pas vraiment…

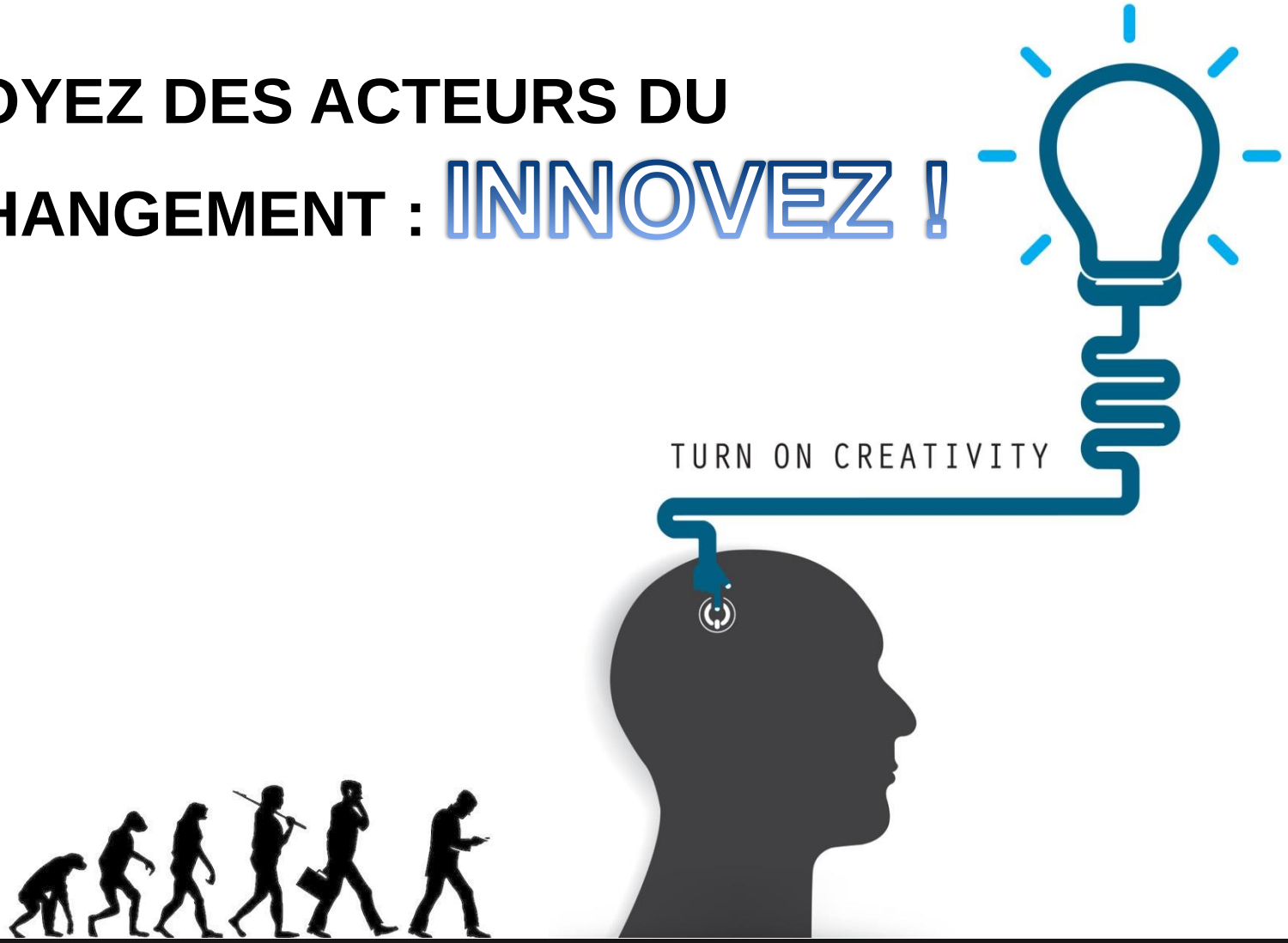
E. Non, assez pessimiste.

F. Non, pas du tout, au secours !



Quel a été, est et sera votre plus gros questionnement “hier”, “aujourd’hui” et “demain”?

SOYEZ DES ACTEURS DU CHANGEMENT : INNOVEZ !



MERCI

Richter S.E.N.C.R.L.
1981, McGill College
Montréal QC H3A 0G6

181, Bay St., bureau 3320
Bay Wellington Tower
Toronto ON M5J 2T3

www.richter.ca

Visitez-nous sur :

Facebook
LinkedIn
Twitter