Beijaflore

Pénurie d'experts ou opportunité ?

Jeudi 06 OCT 2016

#careeropportunity #recruitment
#cybersecurity #skillset #training #IISP

Observatoire des pratiques RH dans l'univers des experts SSI

Antoine ANCEL
RSSI
SNCF RESEAU

Cyril HAZIZA
CISO EMEA
L'OREAL

Maxime de JABRUN
Vice President
BEIJAFLORE

- Une étude menée auprès de
  - Chasseurs de tête, DRH, Enseignants en école et université
  - RSSI et DSI
  - Responsables d'équipe conseil et d'expertise
- Sur le terrain en France et à Singapour (marché du travail dérégulé)
- Et en analysant les principaux rapports sur le sujet
  - Bridging the cyber security skills gap
  - Cyber Security workforce competencies
  - Hacking skills shortage

Sommaire

- Mythes et réalités de la pénurie
- Recruter des « experts » en sécurité…
  - Pour quels métiers ? Où les trouver ?
  - Comment les évaluer et les former ?
- Une solution : décloisonner !

Le Center for Strategic International Studies confirme la pénurie
82% des décideurs sondés en juillet (FR, GER, ISRL, JPN, MEX, UK, USA, AUS)

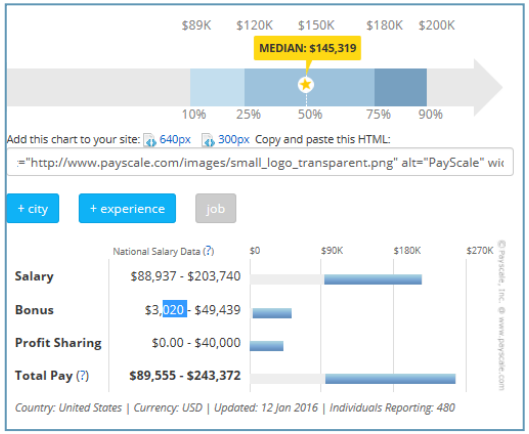
- Carence d'1 million de spécialistes sécurité d'ici 2020

- Recrutement actif et professionnalisé
  - En France, une sollicitation par semaine
  - Un expert en sécurité débutant change de poste tous les 12 à 15 mois à Singapour
  - un profil Sécurité prend déjà 25% de temps de plus qu'un IT
  - Les chasseurs se spécialisent sur le créneau de la cyber sécurité

→ « L'agent sportif » pour les experts seniors en sécurité, un nouveau métier ☺

La rémunération augmente

- Les profils sécurité disposent d'un premium sur les IT d'environ 10% aux USA
- Leur rémunération a augmenté de 11 à 15% à Singapour cette année



Pour nuancer ce propos anxiogène

- Plusieurs RSSI déclarent avoir recruté facilement pour 1 position à pourvoir
- Les organisations sécurité du secteur financier sont déjà plus développées et moins exposées à cette pénurie
- 90% des sondés du CSIS pense que la technologie, en particulier le machine learning, permettra de combler en partie le besoin
- Les universités et écoles d'ingénieurs s'organisent avec l'industrie pour fournir des formations pratiques

Sommaire

- Mythes et réalités de la pénurie
- Recruter des « experts » en sécurité…
  - Pour quels métiers ? Où les trouver ?
  - Comment les évaluer et les former ?
- Une solution : décloisonner !

Je veux recruter un expert sécurité
Qu'est ce qu'un expert en sécurité ?

- Les spécialistes techniques sont les plus rares
  - analystes SOC, auditeurs techniques
- D'autres expertises peuvent être gérées différemment

- Equation magique

→ Succès = Compétence + Aptitude^2 + Motivation^3

- Un expert sécurité = un sismologue des SI ~~cowboy dogmatique~~
  - Curieux, créatif, intuitif
  - Culture scientifique (math, systémique ou IT) → rigueur, analyse
  - Communiquant à l'écrit et à l'oral
  - Aimant comprendre le fonctionnement des choses
  - Ténacité et intelligence relationnelle

Je peux donc recruter dans d'autres métiers pour compléter mon dispositif sécurité

Enjeu

Alignement Métier

Amélioration

Expertise Technique

Risque, Continuité,
Data Privacy, Sensibilisation

Programme / Projets
Politiques et processus

Architecte sécurité
Auditeur technique
Analyste SOC

MOA
Opérateur métier

Chef de projet /
PMO

Architecte IT
Développeur
Ingénieur réseau
ou système

Exemple de programme de formations pour reconvertir une équipe IT et la projeter sur 4 ans

Introduction to Cyber Security	SEC 401 Bootcamp	SEC 505 Windows	ICS 410 SCADA essentials	Vuln Scan + SIEM solution basic certification

Threat Management

Foundations	SEC 504 –GCIH Incident Handling	SEC 503 Network intrusion detection	FOR 408 Endpoint - Windows forensics	Vuln Scan + SIEM solution advanced certification
Practitioner	SEC 542 Web pentest	SEC 560 Infra pentest	ICS 515 SCADA Active response and defend	MGT 535 Incident management
Expert	SEC 642	SEC 660	FOR 508 Digital Forensics and response	FOR 585 Smartphone forensics

Pourquoi un modèle de compétences ?
Pour spécialiser les profils et couvrir l'ensemble de vos besoins

Pour fidéliser, montrez ce qu'ils vont apprendre

→ transparence et projection

Pour attirer d'autres talents, démystifiez les prérequis

→ Tête bien faîte à former plutôt que des moutons à 5 pattes

Pour faciliter le dialogue avec les équipes RH

→ évaluation et formations ad hoc

Quels modèles de compétences ?

Les modèles souverains

- L'ANSSI / SecNum*edu*
  - Compétences/Métiers
  - Labellisation de formation

- US DoL – CS competency model
  - S'appuie sur NICE

Un standard neutre

- Institute of Information Security Professionals (www.iisp.org)
  - Indépendant, reconnu à l'international
  - Questionnaire d'évaluation simple et complet sur 9 catégories d'expertise

Et après un premier job en sécurité ?

- Un deuxième pour les passionnés
- Risque / contrôle pour l'expertise
- Transformation pour le savoir-faire
- Digital pour l'aptitude geek/métier/pédagogie
- IT pour diffuser le savoir sécurité

Sommaire

- Mythes et réalités de la pénurie
- Recruter des « experts » en sécurité…
  - Pour quels métiers ? Où les trouver ?
  - Comment les évaluer et les former ?
- Une solution : décloisonner !

1 minute Security Manager – créer un tissu efficace sur le terrain

0.3% des ETP

Certifié
ISACA CSX

- 1 utilisateur « geek »
- 1 ambassadeur pour 20 utilisateurs
- Agit en proximité physique
- à hauteur de 15 jh par an

Quotidiennement (1 à 10 minutes)

- Observe les comportements et rappelle les bonnes pratiques
- Remonte les anomalies et projets au CISO / DPO

Mensuellement (4h)

- Revoit les accès, entrées/sorties
- Diffuse les communications de la filière « sécurité »

Annuellement (1 semaine)

- Réalise une session de sensibilisation
- Classifie les données / revoit les impacts des risques
- Revoit les profils d'accès
- Suit une formation

Comment réussir la sensibilisation des utilisateurs ?

- Quel rythme ?
  - Trop discret et les gens oublient la sécurité
  - Trop fréquent et la sécurité devient un bruit de fond… spam ?
  - → Une fois par mois

- Quels formats ?
  - Oubliez les mails !
  - Newsletter mettant en avant les collaborateurs
  - Campagne de test/phishing,
  - Lunch-n-learns, Affiches décalées
  - Vidéo témoignage des dirigeants sur réseaux sociaux
  - → Alternez les approches

- Règle d'or: une excellente relation avec votre équipe de communication interne
- Décomplexer les collaborateurs (parler de droits plutôt que de devoirs)
- Et après ? gamification, portail elearning, visites terrain/démo, challenge de hack

En conclusion, pour faire face à la pénurie, la filière sécurité doit se professionnaliser (RH) et se décloisonner

- Aptitudes et envie priment sur les compétences
  - Élargir le vivier en se concentrant sur les soft skills et former sur les hard skills
- Les experts ne sont pas les meilleurs pour tous les postes sécurité
  - Les business analysts sont meilleurs que les experts pour le dialogue métier
  - Les chefs de projet IT sont meilleurs que les experts pour transformer
- La formation est un puissant outil de fidélisation et développement
- Un bon modèle de compétence permet d'éliminer le syndrome du mouton à 5 pates
- Décloisonner permet de limiter le besoin de ressources spécialisées
  - Ambassadeurs sécurité
  - Plan de sensibilisation/éducation efficace
- Capital humain sécurité = régalien (interne) + as a service (externe)

Prochaine étape

Approfondir l'étude pour la France

Publication d'un livre blanc

CESIN

Valeurs
connaître, expérimenter, travailler ensemble, développer, se former, collaborer, promouvoir, influencer
270 membres

Fin du document

Sources

- *Financier Worldwide Magazine – oct 2016*
  - **Bridging the cyber security skills gap**
  - http://www.financierworldwide.com/bridging-the-cyber-security-skills-gap#.V_OSfWdPpdp
- Lance Spitzner, Director, SANS Securing the Human
  - **How often is too often?**
  - https://www.linkedin.com/pulse/security-awareness-communications-how-often-too-lance-spitzner?trk=hp-feed-article-title-publish
- Phoenix university / (ISC)2 -
  - **Cyber Security workforce competencies** report
  - https://www.isc2cares.org/uploadedFiles/University-of-Phoenix-ISC2-cybersecurity-report.pdf
- Intel Security / Center for Strategic and International Studies – jul 2016
  - **Hacking skills shortage**
  - https://www.csis.org/events/hacking-skills-shortage
  - http://www.mcafee.com/es/resources/reports/rp-hacking-skills-shortage.pdf
- Burning Glass – 2014
  - **The Growth of Cybersecurity Jobs**
  - http://www.burning-glass.com/research/cybersecurity/
- ISACA and CSX - January 2015
  - **Global Cybersecurity Status Report**
  - http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf
  - **Global Information Security Workforce Study**," Frost and Sullivan, April 16, 2015.
  - https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf