FALCON : un outil pratique et utile pour la communauté ASR

Jean-Luc Evrard
Institut de biologie moléculaire des plantes
STRASBOURG

Marc Herrmann
Délégation Alsace du CNRS
STRASBOURG

Virgile Jarrige
Faculté Pharmacie de Strasbourg
ILLKIRCH-GRAFFENSTADEN

Thomas Keller
Observatoire astronomique de Strasbourg
STRASBOURG

Yasmina Ramrani
Laboratoire image, ville, environnement
STRASBOURG

Sébastien Schmitt
Laboratoire des sciences de l'ingénieur, de l'informatique et de l'imagerie
STRASBOURG

Résumé

FALCON est une base de connaissance de « fiches de sécurité », autrement dit des procédures synthétiques, pratiques et opérationnelles. Ces fiches ont pour but d'apporter une aide utile et rapide au traitement d'un problème de sécurité des systèmes d'information. Dans un premier temps, les thèmes sont extraits de la formation SIARS2 délivrée par le CNRS, garantissant ainsi la pertinence des sujets abordés. La liste des thématiques reste toutefois ouverte pour s'adapter au mieux à l'actualité de la sécurité informatique et aux besoins des utilisateurs.

L'idée du projet est de centraliser les procédures, notes techniques, vade-mecum, pense-bêtes et autres modes opérationnels rédigés par les collègues ASR à travers l'hexagone. Nous partageons un même métier et de ce fait, nous partageons les mêmes outils, les mêmes interrogations, nous partageons par moment des difficultés identiques, et rencontrons les mêmes obstacles à franchir pour sécuriser un service web, chiffrer un ordinateur, dépanner un accès VPN, traiter un incident de sécurité, etc. Dès lors, nous souhaitons partager également les solutions.

FALCON pourrait ainsi devenir un référentiel SSI utile à tout ASR dans l'exercice quotidien de son métier, à la condition d'alimenter et de consolider la base de connaissance par les contributions de plusieurs collègues prêts à partager leurs précieuses notes.

Mots-clefs

Sécurité, fiches pratiques, projet collaboratif

1. Introduction

L'équipe du projet FALCON est composée de six ASR du CNRS et de l'université de Strasbourg. Bien que motivée et volontaire, elle ne possède pas l'ensemble de l'expertise technique de nos métiers devenus composites. Il serait bien présomptueux de penser le contraire. Le temps aussi est un paramètre crucial : rédiger, vérifier, publier et maintenir des dizaines de procédures, en plus de tout le travail quotidien, n'est humainement pas réalisable. Par conséquent, la réponse sera donc collective ou ne sera pas.

L'équipe du projet FALCON a mis en place un espace collaboratif, un protocole de contribution et un ensemble de modèles pour permettre de recueillir et publier des fiches pratique de sécurité. Elle s'engage à animer le projet, à encourager la communauté de rédacteurs pour faire profiter tout le monde des expériences de chacun.

Il nous paraît raisonnable de pouvoir obtenir une petite contribution de quelques dizaines de collègues volontaires et généreux. Leurs champs de compétences cumulés constituent sans doute le plus grand patrimoine immatériel de notre communauté.

Nous avons tous, à un moment ou un autre, consigné une procédure de chiffrement, un script nmap, une suite de commandes Powershell, un paramétrage de switch, d'un service réseau, le processus de durcissement d'un OS, la création d'un accès VPN, la marche à suivre en cas incident, etc.

Le but est de retrouver ces indispensables, et parfois complexes, informations le moment venu et, *in fine*, gagner un temps précieux et compté. Mais voilà, la vraie vie est souvent cruelle, un post-it qui s'égare, une feuille volante retrouvée trop tard, des informations incomplètes, une procédure obsolète, on se retrouve à nouveau démuni. On est donc confronté à une perte de temps, une procédure à refaire avec une frustration garantie.

L'idée du projet FALCON est de regrouper, toiletter puis publier toutes ces petites pépites stockées sur vos bureaux, dans vos ordinateurs ou dans un coin de votre tête. Tous ces mémentos, pense-bêtes, aide-mémoire, *vade-mecum*, procédures, modes opératoires seront mis à disposition de toute la communauté dans le but de faciliter au quotidien la vie des ASR.

2. Présentation générale

Le site du projet est accessible à l'url http://falcon-cnrs.unistra.fr

Après authentification avec un compte CRU (Renater) ou Janus (CNRS), vous avez accès à l'intégralité des fiches publiées au format PDF et bénéficiez des facilités de recherche et de tri offertes par la plateforme.

FALCON est hébergé sur une plateforme SharePoint, afin de nous concentrer sur le contenu. Bien loin d'être une solution parfaite, cet outil offre cependant un moteur de recherche, des possibilités d'automatisation et surtout une possibilité d'édition en ligne à partir de Windows (on avait dit pas parfaite), les utilisateurs Linux et MacOS ne sont pas oubliés évidemment l'édition est aussi possible hors ligne et également avec LibreOffice.

3. Pourquoi des fiches ?

Une action de formation présente un état de l'art ponctuel des technologies, outils ou encore bonnes pratiques de nos métiers. Une veille active, souvent individuelle, est nécessaire pour maintenir à jour les solides connaissances acquises.

D'autre part, les choix pédagogiques (découpage des chapitres, ratio théorie/pratique, mélange méthodologie/outil) encapsulés dans des « bonnes pratiques », le tout adressé à un public hétérogène, influent d'une part la réappropriation personnelle du contenu, d'autre part l'utilité pratique et la pérennité des informations reçues.

Le choix de proposer des « fiches pratiques » repose sur ces deux principes : conserver la partie appliquée de la formation et tenter de maintenir à jour les informations restituées.

a. Que contient une fiche ?

Les fiches pratiques s'adressent aux ASR, sous-entendu à un public d'initiés maitrisant les concepts basiques d'un système d'information. Il en découle dans les fiches un niveau d'explication et de détails adaptés, il ne sera par exemple pas nécessaire de rechercher une exhaustivité compulsive dans l'enchainement des copies d'écrans. Les fiches tiennent en moins de 10 pages, le format est volontairement peu contraignant pour faciliter la rédaction des fiches et permettre des tutoriels clairs avec suffisamment d'illustration de lignes de commande au format texte afin de permettre le copier/coller.

Une fiche est valable dans un contexte bien défini et bien encadré. Pour le chiffrement d'ordinateur par exemple, il y aura autant de fiches unitaires qu'il y a de systèmes d'exploitation et d'outils de chiffrement différents. Il en résulte des fiches plus synthétiques et plus nombreuses. Elles seront alors moins longues à rédiger et plus facile à maintenir.

b. Classement des fiches

Plusieurs approches sont possibles pour répartir les fiches pratiques dans des sous-ensemble structurés : découpage par thématique (réseau, système d'exploitation, base de données, web,…), par équipement (serveur Windows/Linux, PC, pare-feu, commutateur,…), par services (authentification, filtrage, VPN,…), ou d'autres encore. Les choix de structuration influent sur la manière de retrouver les informations cherchées, la pertinence et la rapidité des éléments affichés.

Le choix retenu est de ne pas figer une fiche dans un ensemble fermé, en la référençant par des mots clé. Cela permet de multiplier les entrées sur la fiche et augmente les chances de retrouver l'information cherchée. Le moteur de recherche indiquera toutes les fiches contenant dans le corps du texte le ou les mots clé demandés. Nous utilisons pour cela le moteur de recherche natif dans SharePoint. Les premiers tests montrent que cet outil est amplement suffisant dans l'immédiat, il est bien évidemment possible d'améliorer la syntaxe de recherche si besoin.

4. Rédaction des fiches

a. Qui rédige ?

Les premières fiches ont été rédigées par les six ASR à l'origine du projet. Il va sans dire que ces rédacteurs originels, si motivés et enthousiastes soient-ils, n'ont ni les connaissances techniques ni le temps de rédiger les centaines de fiches pratiques potentiellement utiles à notre communauté.

A l'instar de feu le projet Plume, cette initiative est basée sur une contribution multiple et répartie. Une somme de « petites » contributions parait la seule option réaliste pour garantir la pertinence des contenus et leur validité. Nous disposons collectivement de toute l'expertise nécessaire pour obtenir une base de connaissance consistante. Le tout est de mobiliser et de motiver nos collègues.

b. Publication des fiches

Les fiches rédigées seront relues par l'équipe du projet FALCON sans altération du contenu. Seules des modifications de mise en forme pourront être apportées. En cas de doute sur un élément de la fiche, l'auteur sera sollicité pour faire évoluer sa contribution, le cas échéant. Les fiches seront ensuite indexées, converties et publiées sur le site. L'accès à ce dernier nécessite, pour le moment, une authentification via la large fédération d'identité de Renater.

c. Mise à jour des fiches

Seul l'auteur de la fiche est responsable de cette dernière et est habilité à modifier son contenu. Il peut le faire de sa propre initiative dès qu'il le juge nécessaire. L'équipe du projet FALCON veille à surveiller l'obsolescence, réelle ou supposée, des fiches. Elle alertera l'auteur en cas de doute sur la validité du contenu.

Nous ne gérons ni de date fixe de révision ni de suivi de version, là encore pour faciliter la gestion globale du projet. Les fiches comportent une date d'édition dans l'entête. Cette date, croisée avec le contenu thématique de la fiche, nous donnera une indication sur la confiance de validité. La durée de légitimité étant très variable en fonction du sujet abordé.

5. Comment contribuer ?

L'idée est de faciliter au maximum le travail du contributeur pour alimenter le référentiel. Une simple demande par courriel fera de vous un contributeur. Le menu "contribution" sur le site du projet sera débloqué et mettra à votre disposition quelques ressources documentaires. Le contributeur aura à sa disposition un *vade-mecum* de rédaction, un modèle de fiche pré-formatée et la possibilité de renseigner la fiche en ligne. Il pourra piocher une fiche dans notre liste de fiches en attente de contributeur ou en proposer une nouvelle si aucune d'elles ne l'inspire. Une fois la fiche modèle récupérée, vous pouvez la remplir. Attention, vous êtes seuls garant des informations et procédures décrites dans la fiche. Vous pouvez évidemment rédiger à plusieurs, voire éventuellement désigner un relecteur pour votre fiche, sans que ce dernier point soit une obligation.

6. Avenir du projet ?

Ce projet nous semble une réponse à une problématique commune mais son déploiement reste une grande inconnue pour nous. Il nous parait assez évident que cet outil pourrait rendre d'innombrables services à un large public, et même à tous les ASR. Son aboutissement dépend de notre capacité à le promouvoir, notre volonté collective de se poser un instant et de rédiger une modeste, mais ô combien utile, contribution.

« *Il dépend de celui qui passe que je sois tombe ou trésor, que je parle ou me taise. Ceci ne tient qu'à toi, ami n'entre pas sans désir.* » Paul Valéry