Les fiches techniques : vos travaux à rendre

Eric DUPUIS[1,2]*

Résumé
Ce document fournit les instructions pour la réalisation des travaux personnels du chapitre sécurité opérationnelle du cours SEC101.
Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document final unique.
Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique.

Mots clefs
Travaux pratiques, études, travaux personnels

[1] *Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France*
[2] *RSSI Orange Cyberdefense*
***email** : eric.dupuis@cnam.fr – eric.dupuis@orange.com

1. Travaux personnels

1.1 généralités

Dans le cadre de ce cours, un seul travail est demandé. C'est un travail personnel, dont l'objectif est de vous faire travailler sur un sujet que vous souhaitez étudier dans le but de le présenter aux autres. Vous pouvez donc choisir un sujet que vous maitrisez ou un sujet que vous ferez découvrir avec un regard de béotien. Ce travail se concrétise par un document à remettre dénommé : **FICHE TECHNO** .

En résumé votre travail devra être :

- 1 document de moins 30 pages (Conseil de 10 à 15 pages)
- Sur un produit, un concept, une méthodologie du monde de la Sécurité Opérationnelle (Vulnérabilités, menaces, incidents, crises, attaques ...)
- Un travail de votre expérience, ou simplement sur une recherche sur internet pour un produit à choisir . . .

Votre analyse sera étayée et critique sur un élément de la sécurité opérationnelle. La notion d'élément SECOPS regroupe de nombreuses thématiques :

- Méthodologique ;
- Technologique ou technique ;
- Conceptuel ;
- Juridique...

Votre rédaction doit faire apparaitre les sources, vous devez surtout développer votre propre vision ou retour d'expérience. Sur ces thématiques, il est important que votre sujet de FICHE TECHNO reste dans le domaine de la sécurité opérationnelle :

- **VEILLE/AUDIT** : Des produits/services de veille et de scan de vulnérabilités informatiques (Qualys, nessus, nmap, checkmarx, appscan ... et bien d'autres ...)
- **SURVEILLE/ALERTE** Des produits/services de gestion d'événement, de supervision et d'alerte (Log, SIEM : Qradar, ArcSight, LogPoint, splunk ... et bien d'autres ...)
- **ANALYSE/REPONSE** : Des produits/services d'analyse post-mortem, et de forensique (Forensic Toolkit, encase ... et bien d'autres ...)

Votre travail est à rendre en fin de session, sous forme informatique (OpenDoc, Formats Microsoft, PDF, Latex...)

1.2 Méthode de notation

Votre travail est noté sur différents critères ci-dessous.

Chaque critère est évalué suivant les valeurs suivantes

- Qualité du positionnement du problème ou du sujet
- Qualité de la conclusion, dont l'ouverture vers d'autres points
- Présence et affichage de votre point de vue : Apports personnels (apports liés à votre propre expérience, ou aux découvertes faites lors de la rédaction de ce travail)

Les valeurs d'évaluation de ces critères sont :

- 0 - Travaux trop simpliste et sans valeur d'apport personnel ;
- 1 - Travaux simples ou sans apport personnel ;
- 2 - Apport étayé et présentation claire ;
- 4 - Apport didactique ;
- 5 - Apport personnel étayé.

1.3 Format

Si le format n'est pas imposé, il est demandé toutefois de suivre un plan permettant de suivre votre démarche et permettant d'être le plus pédagogique possible. Vous pouvez utiliser le modèle de document mis à votre disposition.

- WORD : SEC101-Part3-Modele-Fiche-Techno-VxRy
- Latex : MemModel sur GITHUB (Cyberdef101)

1.4 Remise de Fiches

Vous devez remettre vos documents via l'outils de dépôts et d'analyse de plagiat du CNAM, via le site COMPILATIO.NET [1] Lors du dépôt, le système analysera les similitudes avec des sources ouvertes. Je vous engage donc à citer vos sources.

2. Sujets

2.1 Sélection des sujets

Avant de vous lancer dans vos travaux, il est demander de faire valider votre sujet par l'enseignant. Pour cela simplement envoyer un mail avec votre sujet et vos justificatif de choix.

Vous trouverez ci après quelques différentes thématiques avec des idées de sujet. Chaque sujet est constitué d'un thème, et d'un descriptif optionnel. Ces sujets sont donnés à titre indicatif. Il vous revient d'en proposer un si aucun de ceux présentés vous intéressent.

Votre travail est **à rendre** en fin de session

2.2 sujets produits

Pour les fiches produit, vous devez livrer votre FICHE TECHNO, avec 2 fichiers supplémentaires : l'icône du produit nommé product.ico, et un fichier TEXTE nommé **product.id** contenant les éléments suivants :

- `\producteditorname{Nom de l'éditeur}`
- `\productname{Nom du produit}`
- `\productdescription{description}`
- `\productversion{version du produit}`

Ces éléments permettent de présenter les produits de manière plus accessible sur le site du CNAM.

2.3 Sujets : Vulnerability Management

2.3.1 Exemples étayés de vulnérabilités

2.3.2 BugBounty

2.3.3 Outils au service des tests d'intrusion

1. https://interface.compilatio.net/dossier/q8anf

2.4 Sujets : Threat Management

2.4.1 Description d'une attaque virale

2.4.2 Architecture d'un BOTNET

2.4.3 Organisation des bugbounty

2.4.4 Description attaque DDOS

2.4.5 Description du fonctionnement d'un ransomware

2.4.6 Technique de recherche de LEAK dans le darkweb

2.4.7 Sondes de sécurité

2.5 Sujets : Incident Management

2.5.1 Description d'une contre attaque DDOS

2.5.2 Description d'une contre attaque de ransomware

2.5.3 Description d'une recherche d'APT

2.5.4 Essentiels 27035

2.5.5 Stratégie d'enquête avec des HoneyPots

2.6 Sujets : Crisis Management

2.6.1 ISO 22301

2.6.2 Annuaire de crise

2.6.3 Comment Gérer une crise ransomware

2.7 Sujets : Gouvernance CyberDef

2.7.1 Architecture d'un SOC

2.7.2 Tableau de Bord Vulnerability Management

2.7.3 Tableau de Bord Incident Management

2.7.4 Tableau de Bord SIEM et SIC

2.8 Sujets : Stratégies CyberDef

2.8.1 Concept Deceptive cyberdefense

2.8.2 Utilisation des Honeypots dans la réaction

Table des matières

Table des figures