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 unique, mais édité par chapitre dans le cadre de ce cours.
Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101 (SEC101 du Cnam). Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cyberdéfense d'entreprise.

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] *Directeur Orange Campus Cyber*
***email** : eric.dupuis@lecnam.net – eric.dupuis@orange.com

Notes de cours SECOPS 2022-2023

Vérifiez la disponibilité d'une version plus récente de
CourseNotes-FR-SEC101-30-VTI-studwork.doc.pdf sur GITHUB CYBERDEF [1]

1. https://github.com/edufaction/CYBERDEF/raw/master/Builder/CourseNotes-FR-SEC101-30-VTI-studwork.doc.pdf

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 à vos pairs. 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**, mais regroupe différentes formes vous pouvez en effet traiter d'un produit, d'une méthode, d'une menace, d'une vulnérabilité

En résumé votre travail devra être :

- 1 document avec un style plutôt Billet BLOG 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...), publié sur le site du CNAM

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 :

- 1 - Travaux trop simpliste et sans valeur d'apport personnel ;
- 2 - Travaux simples ou sans apport personnel ;
- 3 - 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-M3-NOM-PRENOM-Titre-VxRy. (Version / révision si nécessaire)
- Latex : MemModel sur GITHUB (Cyberdef101)

1.4 Remise de Fiches

Vous devez remettre vos documents via l'outil de dépôts et d'analyse de plagiat du CNAM, via le site COMPILATIO.NET [2] Lors du dépôt, le système analysera les similitudes avec des sources ouvertes. Je vous engage donc à citer vos sources, afin qu'à la notation, je puisse éviter d'imputer vos citations comme du plagiat...

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 publiez votre demande sur le FORUM ou 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 Thématique produits et services

Pour les fiches sur les produits et services, vous pouvez livrer votre FICHE, avec un petit dossier supplémentaire (Fichier ZIP au nom du produit contenant) quelques lignes et contenant l'icône du produit nommé **icon.png** afin que vos travaux puissent être directement liés dans le cours publié les prochaines années. Les deux petit fichiers textes :

2. https://interface.compilatio.net/dossier/xn28i

- **description.tex** : fichier contenant un description succincte d'un maximum de 5000 caractères du produit. (Les commandes simples latex sont autorisés dans ce document (mise en forme, tableau, itemize).
- **datas.tex** : Fichier contenant quelques éléments descriptifs du produit ou système. Les éléments descriptifs sont à saisir :
  - `\toolsclass{classe de l'outil}(Facultatif)`
  - `\toolsname{Nom du produit ou de l'outil}(Facultatif : nom du répertoire ou ZIP = produit)`
  - `\toolseditor{Nom de l'éditeur}`
  - `\toolsurl{Url de l'outil}`
  - `\toolversion{Version du produit}(Facultatif)`

Le fichier exemple (téléchargeable) **Qradar.zip** [3] doit donc contenir au moins pour le produit « Qradar » de la classe « SIEM » :

```
\renewcommand\toolseditor{IBM}
\renewcommand\toolsurl{https://www.ibm.com/fr-fr/security/security-intelligence/qradar}
```

Ces fichiers de présentation seront mis en forme dans les supports de cours et d'exemple de produits sous la forme :

Qradar

IBM QRadar	Solution SIEM proposée par IBM, à partir de 2015 se charge de détecter des anomalies, comportements inhabituels et autres attaques en collectant puis en "analysant" l'ensemble des évènements en provenance du SI.

Classe : **SIEM**, Site de référence : **Qradar** [4]
Editeur : **IBM** Analyste : **eduf@ction**

Ces éléments permettent de présenter les produits de manière plus accessible sur le site du CNAM et dans les illustrations du cours

2.3 Les thématiques des fiches TECHNO

Les thématiques des fiches TECHNO et METHODO, dénommées par simplification fiches TECHNO sont classées en deux catégories :

- Les **fiches produits, outils et services** pour chacune des trois thématiques présentées dans le cours, et pour lequel l'outil peut illustrer l'usage d'une technologie ou d'un service de cyberdéfense ;
- Les fiches thématiques **méthodologies, et concepts** dont le sujet peut être choisis dans la liste fournie.

.

3. https://github.com/edufaction/CYBERDEF/raw/master/SecTools/classe.tool.example/siem.Qradar.zip
4. https://www.ibm.com/fr-fr/security/security-intelligence/qradar

2.4 Thématique : Vulnerability Management

2.4.1 Exemples étayés de vulnérabilités

2.4.2 BugBounty

2.4.3 Outils au service des tests d'intrusion

2.4.4 Essentiels 27001 et vulnérabilités

2.5 Thématique : Threat Management

2.5.1 Description d'une attaque virale

2.5.2 Architecture d'un BOTNET

2.5.3 Organisation des bugbounty

2.5.4 Description attaque DDOS

2.5.5 Description du fonctionnement d'un ransomware

2.5.6 Technique de recherche de LEAK dans le darkweb

2.5.7 Sondes de sécurité

2.6 Thématique : Exemples attaques et traitement

Description d'une attaque dans le monde réel avec les mécanismes, stratégies de l'attaquant, le retour d'expérience de l'attaqué et le traitement par les médias.

2.7 Thématique : Incident Management

2.7.1 Description d'une contre attaque DDOS

2.7.2 Description d'une contre attaque de ransomware

2.7.3 Description d'une recherche d'APT

2.7.4 Essentiels 27035

2.7.5 Stratégie d'enquête avec des HoneyPots

2.7.6 Deceptive defense

2.7.7 Essentiels 27001 et incidents

2.7.8 ITIL et gestion des incidents de sécurité

2.8 Thématique : Crisis Management

2.8.1 Essentiels ISO 22301

2.8.2 Annuaire de crise

2.8.3 Comment Gérer une crise ransomware

2.9 Thématique : Gouvernance CyberDef

2.9.1 Architecture d'un SOC

2.9.2 Tableau de Bord Vulnerability Management

2.9.3 Tableau de Bord Incident Management

2.9.4 Tableau de Bord SIEM et SIC

2.10 Thématique : Stratégies CyberDef

2.10.1 Concepts de Deceptive cyberdefense

2.10.2 Utilisation des Honeypots dans la réaction

2.11 Thématiques Transverses

Pour faire évoluer et être au. plus prêt de l'actualité

2.11.1 Bibliographie et book de références par chapitre

2.11.2 Compilation avec abstract d'éléments de lectures

Table des matières