



SEC 101

Analyse de risques
Politiques et architectures de sécurité
Sécurité opérationnelle

le cnam
Bretagne

30.1 - Les fiches techniques : vos travaux à rendre

Éléments de sécurité opérationnelle en cyberdéfense d'entreprise

Eric DUPUIS

eric.dupuis@lecnam.net eric.dupuis@orange.com

<http://www.cnam.fr>

Conservatoire National des Arts et Métiers
Chaire de Cybersécurité

Publication Notes de cours SECOPS 2023-2024 du
14 décembre 2023, 11 h 30 CET



Abstract

⚙️ Hashtags : Travaux pratiques, études, travaux personnels

Ce document fournit les instructions pour la réalisation des travaux personnels du chapitre sécurité opérationnelle du cours SEC101.



Sommaire

1. Travaux personnels

2. Sujets





Le travail demandé





Votre travail

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 maîtrisez 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



Votre travail

- 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



Thèmes

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





Domaines

- **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)



l'évaluation et la notation





Critères

- 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)



Evaluation

- 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.





Fiche TECHNO

Généralités

Le sujet et le contenu de vos travaux



Travaux à valider

Avant de vous lancer dans vos travaux, il est demandé 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 justificatifs 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



Les thèmes

produits et concepts

- 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.



des questions ?

contacter eric.dupuis@lecnam.net

CYBERDEF



101

*Tous les documents publiés dans le cadre de ce cours sont perfectibles,
ne pas hésiter à m'envoyer vos remarques !*




Contributions

Les notes et les présentations sont réalisées sous \LaTeX .

Vous pouvez contribuer au projet du cours CYBERDEF101. Les contributions peuvent se faire sous deux formes :



- Corriger, amender, améliorer les notes publiées. A chaque session des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de vos expertises dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace :
(edufaction/CYBERDEF101) ^a.

a. <https://github.com/edufaction/CYBERDEF101>



Mises à jour régulières

Eduf@ction eric.dupuis@lecnam.net

Vérifiez la disponibilité d'une version plus récente de

CourseNotes-FR-SEC101-30-VTI-studwork.prz.pdf sur GITHUB CYBERDEF ¹



2023 eduf@ction - Publication en Creative Common BY-NC-ND

