TER SYSTEME INDUSTRIELS
M1 FSI 2024/2025

COMPTE RENDU DE REUNION

COMPTE RENDU

(Réunion 003)

RÉSUME DU DOCUMENT

Ce document présente le compte rendu de la troisième réunion de travail du projet CyberSécurité OT, tenue le 20 mai 2025 dans le cadre du TER (Travail d'Étude et de Recherche).

La réunion a permis au groupe Cybersécurité OT d'assister à la présentation du groupe Hacking Ethique et inversement.

Plusieurs points ont été abordé, notament le manque de maturité et de serieux de la part du groupe Cybersécurité OT, 3 des 6 membres du groupe s'étant présenté en retard.

M. AGOPIAN souligne les points positifs et les axes d'améliorations.

Enfin, le professeur encadrant donne lieu à une suite d'échanges pendant lesquels il décrit ses attentes quant à la prochaine présentation qui aura lieu le mardi 27 mai 2025 et nous parle de plusieurs éléments cruciaux.

1 Propriétés du document

CLASSIFICATION DU DOCUMENT	Privée
RÉFÉRENCE DU DOCUMENT	CR003_OT_24_25
DATE D'ÉMISSION DU DOCUMENT	22/05/2025
VERSION DU DOCUMENT	3
AUTEURS	DOUZI Youssef
PROPRIÉTAIRE DU DOCUMENT	AGOPIAN Roland – Aix Marseille

Tableau 1 – Propriété du document

2 Historique des révisions

VERSION	DATE	AUTEUR	RÉSUMÉ DES MODIFICATIONS
1	21/05/2025	DOUZI Youssef	Version Initiale (1)
2	22/05/2025	DOUZI Youssef	Version 2
3	22/05/2025	DOUZI Youssef	Version finale (3)

Tableau 2 - Historique des révisions

3 Diffusion

NOM	FONCTION
AGOPIAN Roland	Professeur Encadrant Pédagogique
PARNET Cyril	Chef de Projet
BERREBIHA Nasserdine	Sous-Chef de projet
YABDA Redouane	Membre de l'équipe
DIA Mouhamadou Afiss	Membre de l'équipe
DOUZI Youssef	Membre de l'équipe
KASMI Badreddine	Membre de l'équipe

Tableau 3 - Distribution

4 Approbation

NOM	FONCTION	SIGNATURE	DATE
PARNET Cyril	Chef de Projet	CP	22/05/2025
BERREBIHA Nasserdine	Sous-Chef de projet	NB	22/05/2025
YABDA Redouane	Membre de l'équipe	RY	22/05/2025
DIA Mouhamadou Afiss	Membre de l'équipe	MaD	22/05/2025
DOUZI Youssef	Membre de l'équipe	YD	22/05/2025
KASMI Badreddine	Membre de l'équipe	KB	22/05/2025

Tableau 4 - Approbation

5 Présentation du document

Ce document constitue le compte rendu de la troisième réunion de travail du projet CyberSécurité OT, qui s'est déroulée le mardi 20 mai 2025 dans le cadre du Travail d'Étude et de Recherche (TER).

Il a pour objectif de retranscrire les échanges entre les participants, de présenter les décisions prises, et de documenter les actions à mener à la suite de cette réunion. La réunion s'est déroulée en deux phases :

Première partie : avec la présence de M. AGOPIAN, enseignant-encadrant du TER, de l'équipe du projet CyberSécurité OT et également de celle du projet Hacking Ethique. Tous les membres étaient présents.

Deuxième partie : Le groupe Hacking Ethique s'en va et le reste des étudiants ainsi que M. AGOPIAN continuent leurs échanges.

6 Déroulement de la réunion

6.1 Lieu

La réunion a eu lieu dans la salle de travail du Bâtiment 7, côté A, 3ème étage. La salle était équipée d'un écran pour la présentation. Malheureusement dû à une simulation d'exercice incendie dans le batiment, la réunion s'est terminée à l'exterieur, au niveau du point de rassemblement du campus de Saint Charles.

6.2 Présentation du groupe Hacking Éthique

Le groupe Hacking Ethique composé de 6 étudiants a présenté un travail de recherche sur l'hacking éthique qui abordait notamment les différences entre ce dernier et l'hacking standard ; les différentes phases par lesquelles passent un hackeur éthique dans le cadre de ses missions ; une étude de cas fictive et également une petite partie sur les tests d'intrusion dans le milieu OT.

La présentation était très fluide, les étudiants savaient bien de quoi ils parlaient, le support visuel était très bien réalisé. Aucune remarque particulière n'a été émise si ce n'est l'oubli de nombre de diapositives maximum qui devait être visible sur le support.

Monsieur AGOPIAN souligne la perspicacité des questions du groupe cybersécurité OT, notamment celle sur les certificats numériques et nous informe donc qu'il prendra un moment dans les prochaines réunions pour nous en parler en profondeur.

6.3 Présentation du groupe cybersécurité OT

Le groupe cybersécurité OT a ensuite présenté leur travail sur les attaques ciblant les milieux industriels en abordant l'évolution des attaques ; les causes et les facteurs de cette évolution ; la typologie des attaques ; un cas concret qui est l'attaque Stuxnet et finalement les moyens pouvant être mis en oeuvre pour pallier ces attaques.

Plusieurs remarques ont été réalisé à la suite de cette présentation :

- Un très gros manque de dynamisme et de maturité de la part de certains membres du groupe
- Beaucoup de fautes d'orthographes sur les diapositives
- Certains étudiants répetaient dans leur partie des choses qui avaient déjà été dites auparavant, laissant une impression de manque de travail d'équipe et de cohésion
- Un souci de logique dans la construction de la présentation

Les étudiants ont pris en compte ces critiques et ont échangé avec le professeur en donnant leur avis et leur point de vue. Ce qui en ressort est que malgré l'implication et le bon travail de certains étudiants, la présentation dans son ensemble est très mauvaise, et les points cités précédemment doivent être pris en compte pour la prochaine fois.

6.4 Valeur ajoutée

M. AGOPIAN parle d'une chose très importante qui est la valeur ajoutée. En effet dans un monde où l'intelligence artificielle se développe de plus en plus, beaucoup de métiers tendent à disparaitre et il est important pour un étudiant de se poser la question de quelle serait sa valeur ajoutée par rapport à une IA. En réalité, M. AGOPIAN explique qu'à travers ce projet de TER en cybersécurité, les étudiants vont acquérir une compréhension des langages OT et IT et seront notamment capable de proposer des mesures compensatoires lorsque confrontés à un problème, là où l'IA ne pourra pas.

6.5 Mesures compensatoires

La réunion a par ailleurs permis d'aborder le thème des **mesures compensatoires**. Ce sont des solutions mises en place quand une mesure de sécurité standard n'est pas possible. Elles peuvent être **techniques**, mais aussi **humaines**. Par exemple, si on ne peut pas mettre de capteur sur une cuve d'eau pour détecter une ouverture, on peut demander aux agents de nuit d'être attentifs aux bruits suspects qui pourraient indiquer une ouverture malveillante.

6.6 Classification du document

M. AGOPIAN souligne l'importance de la classification d'un document. Un document peut être classé comme publique, privé, interne etc... En effet le traitement, la diffusion ou encore la transmission seront différents selon la classification du document. Cette classification permet de savoir **comment traiter et protéger le document**. Par exemple, un document public peut être partagé librement, alors qu'un document privé ou confidentiel doit être **protégé et partagé uniquement avec les bonnes personnes**. C'est important pour éviter les fuites d'informations sensibles et respecter certaines règles de sécurité.

CLASSIFICATION	SIGNIFICATION
Publique	Le document peut être visionné de tous, notamment du groupe Hacking Ethique
Privée	Le document peut être visionné uniquement par les personnes présentes dans la liste de diffusion

6.7 L'importance du versionning

M. AGOPIAN et l'ensemble du groupe échangent ensuite sur l'importance du versionning d'un document. Il en ressort que ce dernier permet de suivre, gérer et archiver les différentes versions d'un document au fil du temps. Le versionning est également très utile dans des contextes collaboratifs ou techniques. Lorsqu'un problème survient (ex : cyberattaque, bug, mauvaise mise à jour), un **plan d'action** est déclenché pour restaurer le système dans une version antérieure plus stable et **le versionning est ce qui rend ce plan possible et efficace.**

6.8 L'approche par conformité

Un autre point qui a été abordé est **l'approche par conformité**. Elle consiste à appliquer des **mesures de sécurité** définies par des **normes**, des **standards** ou des **référentiels** officiels, comme ceux du **NIST**, de **l'ANSSI**, ou encore les normes **ISA/IEC**. Elles sont mises en place pour respecter un cadre réglementaire ou des exigences métier et permet notmamment de se protéger sur le plan juridique en montrant que l'organisation ou l'entreprise suit les bonnes pratiques.

6.9 Attentes pour la réunion numéro 4

M. Agopian demande une **présentation de 50 minutes** lors de la prochaine réunion, sur le thème des **normes standards** et de l'approche par conformité en général. Points à aborder :

- Norme ISA/IEC 62443
- Réferentiel NIST
- Réferentiel ANSSI
- MITRE Pyramide de Pain

M. Agopian demande également aux étudiants de commencer à s'informer sur les simulateurs de systèmes industriels, et notamment des simulations d'attaques sur ces systèmes.

6.10 Bonnes pratiques pour améliorer le compte rendu

M. AGOPIAN clôture la réunion en donnant quelques remarques sur le compte rendu précedent :

- Ne jamais écrire une date qui n'est pas pleinement qualifiée (ex : 4 mai)
- Compléter la première page du compte rendu en précisant l'année et le type de master afin de faciliter la recherche future du document
- Trouver une bonne nomenclature pour les documents également afin de faciliter la recherche de ces derniers

Il précise également la possibilité de se référencer en utilisant les numéros de semaines.

6.11 Informations supplémentaires

M. AGOPIAN souligne deux points :

- L'amélioration de l'écriture du compte rendu numéro deux par rapport au premier.
- Un dernier avertissement pour les retardataires.

7 Acronymes et définitions

Table des acronymes

ACRONYME	SIGNIFICATION
ISA	International Society of Automation
IEC	Internation Electrotechnical Comission
NIST	National Institute of Standards and Technology
MITRE	MITRE Corporation
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Informations

Table 5 – Table des acronymes