

Université Sorbonne Paris Nord

BUT3 Cybersécurité
Département Réseaux et Télécommunications

SAÉ CYBER.03

Assurer la sécurisation et la supervision avancée

Auteurs :

AMMAR Ons et Doumbia Awa

Superviseur :

Dr. OUAMRI Mohamed Amine



Année Universitaire : 2025 – 2026

Remerciements

Nous avons eu l'honneur d'avoir **Mr. OUAMRI Mohamed Amine** comme encadrant de nos travaux durant cette SAE.

Sa supervision et ses conseils nous ont permis de mieux appréhender les différentes étapes de notre projet et de nous confronter à des situations concrètes enrichissantes.

Qu'il trouve ici l'expression de notre vive reconnaissance, notre grande considération et nos remerciements les plus sincères.

Nous espérons que les compétences et les connaissances acquises au cours de cette SAE nous pousseront à poursuivre nos efforts avec davantage d'implication et de motivation dans nos futurs travaux académiques et professionnels.

Ons et Awa

Préface

Ce travail a été réalisé en binôme dans le cadre de notre **SAÉ CYBER.03**, et nous avons eu l'opportunité de collaborer étroitement tout au long du projet.

Nous avons été particulièrement motivés par le défi que représente la compréhension des attaques par écoute clandestine (**Eavesdropping**), et par la création et l'analyse avec un **SIEM Wazuh**

Cette expérience nous a permis de développer notre esprit d'analyse, notre rigueur dans la mise en place de simulations, ainsi que notre capacité à travailler en équipe pour atteindre des objectifs communs.

Nous espérons que ce rapport reflète notre engagement et notre enthousiasme pour ce projet, ainsi que la richesse de l'expérience acquise.

Table des matières

Remerciements	1
Préface	2
Table des figures	4
Introduction	5
1 Mise en place d'une attaque de type Eavesdropping	6
2 Création et Analyse avec un SIEM Wazuh	6
3 Conclusion	6
4 Annexes	7

Table des figures

Introduction

Cette SAE a pour objectif principal de développer nos compétences pratiques en sécurité des systèmes d'information et en analyse des menaces.

Ce rapport présente **deux travaux complémentaires** :

- ① Le premier consiste à mettre en place et analyser une attaque de type ***Eavesdropping*** (écoute clandestine), afin de comprendre ses mécanismes et d'illustrer ses conséquences sur la confidentialité des communications. Cette étape nous a permis **de manipuler un environnement de simulation de l'attaque, d'intercepter et d'analyser des flux réseau, et d'évaluer l'impact de ce type d'attaque sur la sécurité des utilisateurs.**
- ② Le second travail porte sur la création et l'analyse avec un **SIEM** à l'aide de la plateforme open source **Wazuh**. L'objectif était **d'installer, configurer et personnaliser ce système** afin de collecter et centraliser les journaux provenant de différentes sources, et d'analyser les événements de sécurité pour détecter en temps réel les incidents et tester la robustesse du système face à des scénarios d'attaque simulés.

Ainsi, ce projet a permis de lier la compréhension théorique des menaces et attaques à leur analyse pratique, tout en développant des compétences concrètes en cybersécurité, notamment dans l'administration d'un SIEM, la détection et l'analyse des incidents, et la mise en place de mesures de sécurité adaptées.

1 Mise en place d'une attaque de type Eavesdropping

2 Création et Analyse avec un SIEM Wazuh

3 Conclusion

Cette SAE nous a permis d'explorer concrètement le domaine de la cybersécurité à travers la réalisation d'une attaque de type ***Eavesdropping*** et la mise en place d'un **SIEM** avec **Wazuh**. Nous avons pu observer les vulnérabilités possibles dans un réseau **VoIP**, analyser les événements de sécurité et comprendre l'importance de la détection proactive des menaces.

Au-delà des aspects techniques, ce projet a renforcé notre capacité à travailler en équipe, à appliquer une démarche méthodique et à réfléchir de manière critique face à des situations réelles.

Nous espérons que cette expérience constituera une base solide pour nos futurs projets, et qu'elle nous encouragera à continuer à approfondir nos connaissances et compétences en cybersécurité.

4 Annexes