## INTRODUCTION

À l’ère de la transformation numérique, les réseaux informatiques occupent une place centrale dans le fonctionnement des entreprises, des institutions et des administrations. Avec l’interconnexion croissante des systèmes et l’augmentation exponentielle des flux de données, les menaces pesant sur la sécurité des réseaux se multiplient. Les cyberattaques, telles que les tentatives d’intrusion, les attaques par déni de service (DoS/DDoS), les malwares ou encore les vols de données sensibles, deviennent de plus en plus sophistiquées et difficiles à détecter en temps réel.

Face à ces enjeux, la mise en place de systèmes de supervision et de surveillance des réseaux s’est imposée comme une nécessité. Les organisations collectent des volumes importants de journaux d’événements (logs) générés par les pare-feux, les systèmes IDS/IPS, les serveurs ou encore les équipements réseau. Cependant, l’analyse manuelle de ces logs est fastidieuse et peut entraîner des erreurs humaines ou des délais de détection trop longs, compromettant ainsi la sécurité globale du système.

Pour répondre à cette problématique, l’intelligence artificielle (IA) offre des solutions prometteuses. L’IA permet d’automatiser l’analyse des comportements réseau et de détecter les anomalies sans intervention humaine directe, réduisant ainsi les faux positifs et optimisant la réponse aux incidents. C’est dans ce contexte que s’inscrit le présent travail.

# **Chapitre 1 : Contexte théorique**

Ce chapitre vise à établir le cadre conceptuel et contextuel du projet. Il présente d’abord l’environnement institutionnel de l’OTIV Mahavonjy Antsiranana, puis explore les notions fondamentales liées à la sécurité des réseaux, aux journaux systèmes (logs) et aux mécanismes de détection d’anomalies. Enfin, il introduit les apports de l’intelligence artificielle comme solution innovante pour améliorer la supervision et la réactivité face aux menaces réseau.

## 1.1 Présentation de l’entreprise : OTIV Mahavonjy Antsiranana

### **1.1.1 Contexte général**

L’**OTIV Mahavonjy Antsiranana** (Ombona Tahiry Ifampisamborana Vola) est une **institution de microfinance mutualiste** créée en 2001. Elle fait partie du réseau OTIV DIANA qui regroupe cinq caisses de base dans la région DIANA (Antsiranana, Ambilobe, Ambanja, Anivorano-Nord, Nosy-Be).

L’OTIV Mahavonjy propose des services financiers accessibles aux populations locales, notament : la collecte d’épargne, l’octroi de crédits à court et moyen terme et des services financiers solidaires.

Le réseau OTIV vise à favoriser l’inclusion financière, notamment pour les populations rurales ou exclues du système bancaire traditionnel.

### **1.1.2 Historique et mission**

Le modèle OTIV s’inspire des caisses Desjardins du Canada, adaptées à Madagascar en 1993 avec le soutien de la Banque mondiale et du Développement International Desjardins (DID).

L’OTIV a comme mission de :

* Recevoir l’épargne des membres et leur accorder des crédits
* Fournir des services financiers adaptés aux besoins locaux
* Favoriser la solidarité et l’entraide économique
* Promouvoir l’éducation financière

### **1.1.3 Organisation de l’OTIV Mahavonjy**

Voici un tableau montrant l’organisation de l’OTIV Mahavonjy

|  |  |
| --- | --- |
| **Forme juridique** | Société coopérative mutualiste |
| **Siège** | Antsiranana (Diego Suarez) |
| **Réseau** | 5 caisses de base et 8 points de service dans la région DIANA |
| **Effectif** | Plus de 36 000 membres en 2024 |

**Tableau 1:** Organisation de l'OTIV Mahavonjy

L’OTIV Mahavonjy fonctionne de manière autonome mais adhère à l’union régionale des OTIV DIANA pour la coordination.

### **1.1.4 Enjeux de sécurité et problématique actuelle**

* **Architecture réseau actuelle**

Voici l’architecture de réseau d’OTIV actuel :

* **Problématique**

Actuellement, la sécurité réseau de l’OTIV Mahavonjy repose principalement sur l’utilisation d’un pare-feu pfSense, configuré pour contrôler le trafic entrant et sortant afin de bloquer les connexions non autorisées. L’organisation utilise également Graylog pour centraliser les journaux d’événements (logs) provenant des équipements réseau et des serveurs. Les alertes de sécurité sont transmises par courriel lorsque des anomalies sont détectées.

Cependant, toutes les vérifications et décisions relatives à la sécurité restent réalisées de manière manuelle. Cette gestion présente plusieurs limites : elle entraîne un risque de retard dans la détection des incidents et augmente la probabilité de laisser passer des menaces, telles que des intrusions, des attaques par force brute, des scans de ports ou des tentatives de déni de service (DoS). L’absence d’un système automatisé rend la supervision lourde exposant le réseau à des risques d’erreur humaine et de réactions tardives face aux attaques.

### **1.1.5 Objectif visé par le projet**

Le projet doit aboutir à la mise en place d’une solution de monitoring des journaux réseaux générés par un pare-feu, capable d’analyser automatiquement des activités suspecte. Ce dispositif a pour but d’aider OTIV Mahavonjy à mieux gérer les incidents réseaux et améliorer la réactivité face aux menaces.

## 1.2 Fondements théorique

### **1.2.1 La sécurité réseau**

La sécurité réseau englobes toutes les activités visant à protéger la fonctionnalité et l’intégrité du réseau et des données. Elle repose sur des couches multiples de défense, appliquant des politiques et contrôles à chaque niveau pour permettre l’accès aux utilisateurs autorisés tout en bloquant les activités malveillantes et les tentatives d’intrusion.

La sécurisation du réseau repose sur plusieurs **principes fondamentaux**, qui doivent impérativement être respectés :

* **Confidentialité :** seules les personnes autorisées peuvent avoir accès aux ressources et bloquer l’accès aux autres.
* **Authenticité :** cet objectif garantis à l’expéditeur que le destinataire est bien celui qui veut lui envoyer des données.
* **Intégrité :** ceci assure que le message n’a pas été modifié.
* **Disponibilité :** l’accès aux ressources du système d’information doit être permanent et sans faille.
* **Non-répudiation :** consiste à assurer qu’aucun des utilisateurs peuvent contester les opérations qu’ils ont réalisées.

#### **1.2.1.1 Technologie pour la sécurisation réseau**

Pour se protéger contre des attaques, il est important d’utiliser des outils de sécurité qui ont pour objectif de minimiser les risques d’intrusions que ça soit dans les machines hôtes ou bien le réseau où se trouve ces machines.

* **Pare-feu (firewall) :** Un pare-feu est un matériel ou un logiciel utilisé pour protéger un réseau local des intrusions extérieures. Il agit comme une barrière de protection et de sécurité empêchant la fuite de certaines informations en dehors du réseau informatique.
* **VPN (Virtual private Network) :** Les réseaux privés virtuels sont utilisés pour établir des connexions sécurisées et cryptées sur des réseaux publics, garantissant la confidentialité des communications.
* **Systèmes de détection d’intrusion (IDS) :** Les IDS surveillent le trafic réseau à la recherche de signatures d'attaques connues ou de comportements suspects, alertant les administrateurs en cas de détection.

### **1.2.2 Monitoring réseau**

Le monitoring de sécurité réseau est un ensemble de pratiques et d'outils visant à surveiller en permanence l'état de la sécurité d'un réseau informatique. Il permet de détecter les activités suspectes, les menaces potentielles, et de réagir rapidement en cas d'incident. Cela inclut la surveillance des équipements réseau, des serveurs, des applications, et des flux de données

* **Outils et protocoles de supervision :**
* **SIEM (Security Information and Event Management) :** est un outil de gestion de la sécurité qui centralise les informations de sécurité réseau.
* **SNMP :** Protocole standard de supervision des équipements réseau. Il permet de surveiller l’état des dispositifs (routeurs, switchs, serveurs) via des agents SNMP.
* **Reniflement des paquets (Packet sniffing) :** Technique qui consiste à capturer et analyser les paquets de données circulant sur un réseau afin de détecter des anomalies ou surveiller les échanges. Exemples d’outils : Wireshark, tcpdump.
* **WMI (Windows Management Instrumentation) :** interface spécifique aux environnements Windows qui permet de collecter des informations système (services, sécurité, état des ressources) sur les postes de travail et serveurs Windows.

### **1.2.3 Généralité sur les logs**

#### **1.2.3.1 Définition**

La gestion des logs est une pratique qui consiste à traiter de grands volumes de messages et de [données de log générées par ordinateur](https://www.splunk.com/en_us/blog/learn/log-data.html). Par définition, les logs, également appelés journaux ou fichiers de journalisation, sont des enregistrements d'événements ou d'activités qui se produisent dans un système informatique, un logiciel, une application ou un réseau. Ils jouent un rôle crucial dans le suivi des actions, la résolution des problèmes, la sécurité, et l'analyse des performances.

#### **1.2.3.2 Types de log**

Pour pouvoir comprendre les données, il faut d’abord comprendre la diversité de logs que l’on peut rencontrer. Chacun d’eux contiennent des informations spécifiques et souvent vitales.

* **Logs de système (syslog) :** enregistrent les événements du système d'exploitation, tels que le démarrage, l'arrêt, les erreurs système et les changements de configuration.
* **Logs d’application :** documentent les activités des applications, comme les erreurs, les transactions, les états de connexion et d'autres informations spécifiques à l'application.
* **Logs réseau :** enregistrent les activités du réseau, telles que les connexions, les transferts de données et les erreurs réseau.
* **Logs de sécurité :** enregistrent les événements de sécurité tels que les tentatives de connexion, les accès aux données sensibles, les modifications de configuration, et les activités suspectes.

#### **1.2.3.3 Importance de gestion de log**

La gestion des logs permet aux entreprises de suivre la trace de toutes les activités qui se déroulent au sein de leur [infrastructure informatique](https://www.splunk.com/en_us/blog/learn/it-infrastructure.html). Et cela peut avoir de nombreux usages au quotidien :

* **Détection des anomalies et des incidents :** Les logs aident à repérer les comportements inhabituels ou les tentatives d'intrusion.
* **Dépannage :** Lorsqu'une erreur survient, les logs sont souvent consultés pour identifier la cause du problème.
* **Audit et conformité :** Les entreprises utilisent les logs pour prouver qu'elles respectent certaines normes de sécurité ou réglementations.
* **Optimisation des performances :** Ils permettent de surveiller les performances des systèmes et d'optimiser les ressources en fonction des événements récurrents.

#### **1.2.3.4 Outil de gestion de log**

Il existe plusieurs outils de gestion de logs, incluant, Wazuh, Splunk et ELK qui permettent de centraliser, rechercher et analyser les logs pour en tirer des informations exploitables. Certains d’entre eux sont open-source et d’autre propriétaire (non-libre).

### **1.2.4 Typologie des incidents et anomalies courante dans un réseau**

Le **monitoring de sécurité réseau** vise à détecter non seulement les attaques malveillantes, mais aussi les anomalies techniques pouvant perturber le fonctionnement normal du système.

Ces événements peuvent être classés en deux grandes catégories :

* **Attaques malveillantes :**
* **Attaque par force brute :** est une attaque qui consiste à essayer toutes les combinaisons possibles d’identifiants jusqu’à trouver la bonne.
* **Attaques DoS et DDoS :** sont les attaques les plus repandues qui visent à perturber la disponibilité d’un service, d’un système ou d’un réseau en submergeant ses ressources avec un volume de requêtes excessif.
* **Attaques MITM (Man-In-The-Middle) :** c’est le fait d’intercepter, d’écouter ou de modifier les échanges entre deux entités sans leur consentement ni leur connaissance, compromettant ainsi la confidentialité, l’intégrité et l’authenticité des données transmises.
* **Scan de port :** l’attaquant teste les ports d’une machine pour identifier ceux qui sont ouverts et détecter des services vulnérables.
* **Anomalies non malveillantes :**
* **Panne matérielle :** Défaillance d’un composant réseau (switch, routeur, serveur), provoquant une interruption de service.
* **Congestion réseau :** Trop de trafic réseau légitime peut saturer les équipements, rendant le réseau lent ou indisponible.
* **Erreur humaine :** Mauvaise configuration, suppression accidentelle de fichiers critiques, ouverture d’un port non sécurisé.

## 1.3 Etat de l’art des solutions existantes

### **1.3.1 Généralité sur Security Information and Event Management (SIEM)**

#### **1.3.1.1 Définitions**

Un SIEM est un outil de gestion de la sécurité qui centralise les informations de sécurité de réseau. Il collecte, analyse et génère des alertes en temps réel pour aider à détecter et répondre rapidement aux menaces. Le SIEM est généralement le composant central de tout centre d'opérations de sécurité (Security Operation center), qui est l'équipe de réponse centralisée traitant des problèmes de sécurité au sein d'une organisation. Les fournisseurs vendent le SIEM sous forme de logiciel, d’appareil ou des services gérer. L’acronyme SIEM a été inventé par Mark Nicolett et Amrit Williams de Gartner en 2005.

#### **1.3.1.2 Avantages**

* **Visibilité totale :** Surveillez l’ensemble de système à partir d’un seul tableau de bord.
* **Détection proactive :** Anticipez les menaces avant qu’elles ne deviennent une crise
* **Simplification de conformité :** gérez facilement les normes et exigences comme RGPD ou ISO.27001

#### **1.3.1.3 Architecture de SIEM**

Event

Analysis & Auditing Information Assurance Incident Response

Windows

Agent ou API Based

Event

Searching / Visualization / Report / Alert

Linux/ Unix/\*Nix Agent Based, API or Streaming

R/SYSLOG Server with Agent or Streaming

Ingest / Index / Data Normalization / Core Database

Network/ IDS/ IPS Stream to R/SYSLOG Server

**Figure 1 :** Architecture générale de SIEM

La figure ci-dessus est répartie en 7 blocs fonctionnels, organisés en 4 grandes catégories essentielles à l’architecture d’un SIEM :

* **Sources d’événement :**
* **Windows Agent or API Based :** ce bloc collecte les événements de sécurité et système des machines Windows via un agent local ou des API (WMI, Event Log API), incluant des journaux tels que les connexions, les erreurs systèmes et les accès.
* **Linux/ Unix /\*Nix Agent based, API or Streaming :** Collecte les logs des systèmes Linux, Unix ou dérivés via un agent local (ex : Wazuh), des API spécifiques ou des flux de streaming comme journalctl ou rsyslog, afin de transmettre les événements au SIEM.
* **Network / IDS / IPS Stream to R/SYSLOG Server :** Collecte les journaux des équipements réseau tels que les pare-feux ou les IDS/IPS et les envoie au format Syslog vers un serveur R/SYSLOG pour centralisation.
* **Serveur Syslog :**
* **R/SYSLOG Server with Agent or Streaming :** Serveur central qui reçoit les logs réseau et système via Syslog (RFC 5424), joue le rôle de relais ou de filtre préliminaire avant de transmettre les données vers le cœur du SIEM.
* **Cœur du SIEM :**
* **Ingest / Index / Data Normalization / Core Database :** Reçoit tous les événements entrants, les classe pour accélérer les recherches, les transforme en un format normalisé (ex : CEF, LEEF) et les stocke dans la base de données centrale du SIEM.
* **Searching / Visualization / Reports / Alerts :** Permet de rechercher et visualiser les données collectées via des dashboards, de générer des rapports (conformité, incidents) et de configurer des alertes automatiques basées sur des règles ou des modèles IA.
* **Utilisateurs & Processus :**
* **Analysis & Auditing / Information Assurance / Incident Response :** Les analystes SOC exploitent les données pour enquêter sur les alertes, assurer la conformité réglementaire et déclencher des actions de réponse aux incidents tels que le blocage d’IP ou l’isolement d’un système compromis.

#### **1.3.1.4 Types de SIEM**

* **SIEM Open source**

Un SIEM open source est un système de gestion des événements de sécurité libre d’accès, permettant de collecter, analyser et corréler des journaux d’activité afin de détecter les menaces et surveiller la sécurité informatique, tout en offrant la possibilité de personnalisation grâce à son code ouvert.

**Tableau 2 :** SIEM Open source

|  |  |
| --- | --- |
| **Nom de SIEM** | **Fonctionnalités clés** |
| **Wazuh** | Filtrer, trier et analyser les logs et événements par plage de temps, champs spécifiques ou termes de recherche |
| **ELK Stack** | Collecter de manière fiable et sécurisée des données provenant de n’importe quelle source, dans n’importe quel format, puis de les rechercher, les analyser et les visualiser. |
| **Graylog** | Collecter, d’indexer et d’analyser les logs dans un emplacement centralisé, facilitant la gestion, la recherche et la visualisation des événements système et réseau |

* **SIEM propriétaire (Commercial) :**

Le SIEM commercial (propriétaire) est un système de gestion des informations et des événements de sécurité (SIEM) développé et commercialisé par une seule entreprise, contrairement aux solutions open source.

**Tableau 3 :** SIEM propriétaire

|  |  |
| --- | --- |
| **Nom de SIEM** | **Fonctionnalités clés** |
| **Splunk** | Collecter, indexer et analyser des données générées par des machines en temps réel. |
| **IBM Qradar** | Détecter, analyser et répondre aux menaces de sécurité en automatisant les tâches grâce à l’intelligence artificielle pour accélérer la gestion des incidents. |

* **SIEM as a Service (SIEMaaS):**

Le SIEM as a Service est une solution de gestion des événements de sécurité proposée sous forme de service cloud.

**Tableau 4 :** SIEM as a Service

|  |  |
| --- | --- |
| **SIEM Open Source** | **Fonctionnalités clés** |
| **Azure Sentinel** | Détecter les menaces, corréler les événements de sécurité et automatiser la réponse aux incidents grâce à une solution cloud native intégrant l’IA et la ML |
| **AlienVault  USM  Anywhere  (AT&T Cy bersecurity)** | Collecter des logs, détecter de vulnérabilités, corréler l'événement et gérer des actifs |

### **1.3.2 Limites des approches traditionnelles**

Les méthodes classiques de supervision réseau présentent plusieurs limitations qui nuisent à l'efficacité globale de la détection et de la réponse aux incidents de sécurité.

* **Détection tardive des menaces :** L’un des principaux inconvénients est le temps de réaction souvent trop long. Une anomalie ou une attaque peut ne pas être repérée à temps, ce qui permet à l’attaquant d’agir sans être interrompu. Par exemple, dans le cas d’un ransomware, un système de détection lent peut laisser l’attaque se propager et chiffrer un grand nombre de fichiers avant toute alerte.
* **Précision des détections :** Les systèmes de détection traditionnels doivent trouver un équilibre entre sensibilité et spécificité. Une configuration trop sensible entraîne de nombreux faux positifs, saturant l’équipe de sécurité avec des alertes inutiles. À l’inverse, une sensibilité trop faible risque de laisser passer des attaques réelles, notamment celles qui sont sophistiquées et discrètes.
* **Analyse difficile de volumes massifs de données :** Les infrastructures réseau modernes génèrent d’importants volumes de données hétérogènes (logs systèmes, flux réseau, historiques d’accès, etc.). La corrélation manuelle de ces données pour identifier une menace persistante (comme une attaque de type APT – Advanced Persistent Threat) est complexe, lente et souvent incomplète avec des outils classiques.
* **Maintenance lourde et évolutivité limitée :** Les systèmes basés sur des règles ou des signatures nécessitent une mise à jour fréquente pour rester pertinents face aux nouvelles menaces. Cette maintenance est non seulement chronophage, mais également coûteuse, et n'offre qu'une protection limitée contre des attaques inconnues ou en mutation.

### **1.3.3 Apports de l’intelligence artificielle en cybersécurité**

#### **1.3.3.1 Etude et comparaison des approches existantes**

Dans le domaine de la détection d’anomalies réseau, plusieurs approches ont été développées, chacune avec ses avantages et ses limites :

* **Approches statistiques**

Ces méthodes reposent sur des modèles probabilistes pour déterminer ce qui constitue un comportement "normal". Par exemple, une distribution gaussienne peut identifier des écarts importants comme étant des anomalies. Bien que simples et transparentes, ces approches sont souvent peu performantes sur des données complexes ou dynamiques.

* **Méthodes basées sur l’apprentissage automatique (Machine Learning)**

Des algorithmes comme les forêts aléatoires (Random Forest), les SVM ou K-Means sont utilisés pour détecter des comportements inhabituels. Ils permettent de généraliser à partir de données historiques, mais leur efficacité dépend fortement de la qualité et de la quantité des données d'entraînement, ce qui peut poser problème en contexte réel.

* **Systèmes basés sur des règles (IDS classiques)**

Ces systèmes déclenchent des alertes lorsqu’une règle prédéfinie est violée. Ils sont rapides et efficaces pour des schémas d’attaque connus, mais sont rigides, nécessitent des mises à jour constantes, et sont inefficaces contre des menaces nouvelles ou complexes.

* **Méthodes de Deep Learning**

Les réseaux de neurones profonds (autoencodeurs, RNN…) sont capables de détecter des anomalies subtiles dans des ensembles de données volumineux et multidimensionnels. Ils offrent une grande précision, mais demandent des ressources importantes en calcul et en données, ainsi qu’un savoir-faire technique élevé pour leur mise en œuvre.

#### **1.3.3.2 Justifications de l’utilisation de l’IA comme solutions**

La complexité croissante des infrastructures réseau, couplée à l’augmentation massive des volumes de données générées par les pare-feux, rend obsolètes les approches traditionnelles de surveillance basées sur des règles fixes ou une supervision humaine. Les méthodes classiques, bien qu’utiles pour détecter des attaques connues (grâce à des signatures ou règles de filtrage), présentent plusieurs limites : elles sont statiques, difficilement évolutives, et souvent inefficaces face à des menaces émergentes ou furtives.

L’intelligence artificielle (IA), et plus spécifiquement l’apprentissage automatique (machine learning), s’inscrit aujourd’hui comme une réponse robuste et scientifiquement fondée à ces limitations. Elle repose sur des modèles mathématiques capables d’apprendre à partir de données historiques, d’extraire des schémas complexes non explicitement définis, et d’effectuer des prédictions en temps réel.

Plusieurs éléments justifient scientifiquement l’usage de l’IA dans le monitoring de la sécurité réseau :

* **Adaptabilité aux menaces inconnues**

Contrairement aux systèmes basés sur des signatures figées, les algorithmes d’apprentissage non supervisé (comme les autoencodeurs, l’isolation forest, ou le clustering) peuvent identifier des comportements atypiques, sans avoir été explicitement programmés pour cela. Cela permet de détecter des attaques dites "zero-day" ou furtives, non documentées à l’avance, avec un taux de détection supérieur aux règles statiques.

* **Réduction des faux positifs**

Les solutions classiques génèrent souvent un grand nombre d’alertes inutiles, ce qui fatigue les équipes de sécurité (fatigue d’alerte). L’IA, en particulier via des techniques de classification supervisée, peut améliorer la précision des détections en apprenant à distinguer des comportements effectivement malveillants de simples anomalies bénignes. Cela permet une hiérarchisation des alertes et une réduction significative des interventions inutiles.

* **Traitement automatique de volumes massifs de données**

La croissance exponentielle du trafic réseau produit une quantité de logs que l’analyse humaine ne peut plus traiter efficacement. Les modèles IA peuvent analyser en temps réel des flux continus de données, extraire des métriques, détecter des tendances, et réagir sans délai, ce qui dépasse largement les capacités humaines ou les scripts statiques.

* **Apprentissage dynamique et contextualisation**

L’un des apports majeurs du machine learning est la capacité d’apprentissage continu. En intégrant des algorithmes capables d’adapter leurs modèles au fil du temps (par exemple, en ligne ou semi-supervisé), le système peut affiner sa compréhension du comportement réseau, s’ajuster à l’évolution des usages, et éviter les dérives liées à des configurations rigides.

* **Passage d’une supervision réactive à proactive**

L’IA permet de dépasser la simple détection d’événements pour aller vers l’analyse prédictive. En étudiant les historiques de logs, elle peut anticiper certaines formes de défaillances, ou détecter des signes avant-coureurs d’attaque. Ainsi, elle soutient une posture défensive proactive et améliore la résilience du système d’information.

## 1.4 Conclusion

Ce chapitre a posé les bases théoriques du projet en présentant le contexte organisationnel de l’OTIV Mahavonjy, les principes de la sécurité réseau, les outils de supervision, ainsi que les limites des approches classiques. Il a également mis en évidence les apports de l’intelligence artificielle dans la détection des anomalies réseau. Ces éléments permettent de mieux comprendre les enjeux du projet et justifient le recours à une solution de monitoring automatisé par IA.

# Chapitre 2 : Méthodologies et environnement expérimental

Afin de valider l’hypothèse selon laquelle l’intelligence artificielle peut améliorer la détection des anomalies réseau à partir des journaux de pare-feu, ce chapitre décrit la démarche expérimentale adoptée dans le cadre du projet. Il présente la méthodologie utilisée, les outils choisis, ainsi que l’environnement technique mis en place pour reproduire des scénarios réalistes de trafic normal et anormal. Cette phase repose sur la création d’une architecture réseau virtualisée, la simulation d’attaques, la collecte automatisée de logs, et l’implémentation de modèles d’apprentissage automatique pour détecter les comportements suspects.

## 2.1 Approches méthodologique

Dans le cadre de ce projet, une **approche expérimentale appliquée** a été adoptée. Elle vise à simuler un environnement réseau sécurisé dans lequel différents types de trafic normaux et malveillants sont générés, journalisés, puis analysés à l’aide de techniques d’intelligence artificielle. L’objectif est de démontrer la capacité d’un système basé sur l’IA à détecter automatiquement des anomalies à partir des logs générés par un pare-feu.

## 2.2 Description de l’environnement

## 2.3 Configuration de la collecte de données

## 2.4 Simulation de trafic

## 2.5 Collecte et prétraitement de données

# Chapitre 3 : Implémentation de la détection automatique

## 3.1 Choix du model