Module 2 : Défenses innovantes – Intégrer l'IA dans la cybersécurité.

Présenté par :
Ir Théodore ZINKPE

APDP
AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES

ASIN
AGENCE DES SYSTÈMES D'INFORMATION ET DU NUMÉRIQUE
RÉPUBLIQUE DU BÉNIN

EMIS sarl

INSTINCT LEADER

Plan de la présentation

1. Contexte et justifications
2. Notions introductives à la cybersécurité et à l'IA
3. Usages concrets de l'IA dans la cybersécurité
4. Exemples d'outils et bibliothèques IA en cybersécurité
5. Exercice pratique : cas de l'analyse de fichiers de log d'Apache et d'une instance Laravel avec des bibliothèques IA

1. Contexte & justification

1. Contexte et justification 1/2

- **Le Bénin est dans une dynamique croissante de digitalisation des administrations publiques** : smartGouv, portail des services publiques, dématérialisation de l'administration publique, etc.
- **Les entreprises et organisations privées béninoises également s'informatisent** de plus en plus : digitalisation des processus métiers, sites internet, etc.
- En un mot, nos administrations, nos entreprises, nos organisations sont de plus en plus connectées et **dépendent dans leur fonctionnement de systèmes d'information**.
- Les dysfonctionnements des systèmes d'information, à la suite d'une attaque informatique par exemple, ont **davantage d'impact et de conséquences sur les activités** des organisations.
- Un rapport de vulnérabilité et d'incident de l'ASIN publié en 2025 révèle sur la période de 2021 à 2024 : **878 vulnérabilités** identifiées : dont 24% élevé, 23% critique. Les secteurs des **finances** (18%) et des **services publics** (37%) étant les plus touchés.

1. Contexte et justification 2/2

- **La cybersécurité devient de plus en plus un enjeu de survie** des organisations qui se modernisent grandement sur le plan numérique par souci de performance et de visibilité.
- Pendant ce temps, les **attaques** informatiques sont plus **nombreuses, plus discrètes et plus complexes** que jamais et entre autres, facilitées par l'IA.
- La cybersécurité basée sur des **règles fixes** ou des **signatures connues** devient **caduque** face à des attaques de plus en plus **sophistiquées** et **polymorphes**.
- A l'ère de la révolution enclenchée par les usages de l'IA, au delà de ces fonctions génératives et des usages habituels, l'IA participe également au renforcement des mécanismes de **cybersécurité pour mieux anticiper et de parer aux attaques** informatiques.

2. Notions introductives

2. Notions introductives à la cybersécurité

- **La cybersécurité :** ensemble des **mécanismes déployés pour protéger** les systèmes informatiques (pc, serveur, espace cloud, smartphone, etc.), les données et les utilisateurs contre les attaques.
- **Le rôle de la cybersécurité :** empêcher l'intrusion, détecter les anomalies, et réagir rapidement.
- la cybersécurité repose sur trois socles : **Confidentialité, Intégrité, Disponibilité.**
- **Dans le cadre de la cybersécurité,** on est amené à gérer des **menaces** qui surviennent, des **vulnérabilités** qui fragilisent la sécurité du système informatique, et le **risque** que ces vulnérabilités soient potentiellement exploitées.
- **Exemple de menaces** : Ransomware, Malware, Phishing, Attaques DDoS, injection de code SQL, etc..

3. Notions introductives à l'IA

- Selon le National Institute of Standards and Technology (NIST):

  l'IA est **un système basé sur une machine** qui, pour un ensemble d'objectifs définis par l'humain, est **capable** de faire des **prédictions**, des **recommandations** ou de **prendre des décisions** influençant des environnements réels ou virtuels.

- Concrètement, elle est utilisée en cybersécurité comme un **outil puissant pour détecter, prévenir et répondre** aux menaces numériques de manière plus efficace que les méthodes manuelles.

- Face à la sophistication croissante des cyberattaques et à l'immense volume de données à analyser, **l'IA offre des capacités d'analyse et d'automatisation essentielles**.

3. Usages concrets de l’IA en cybersécurité

3. Usages concrets de l’IA en cybersécurité

L'IA est un outil transverse qui renforce la défense à tous les niveaux de l’infrastructure numérique: Réseau, Applications, et Données.

Réseaux (NDR)	**Applications (WAAP/DAST)**	**Bases de Données**
Menaces :		
Déplacements internes de l'attaquant, Communication secrète avec l'extérieur	Injections polymorphes, Bot Management	Abus de privilèges, Exfiltration de données

3.1. Sécurité des Applications Web et API (WAAP/DAST/SAST)

L'IA est utilisée dans les solutions de protection des applications Web et des API (Web Application and API Protection - WAAP) pour contrer les menaces comme celles listées dans l'**OWASP Top 10** (Injections, XSS, etc.) et l'**OWASP API Security Top 10**.

3.1. Sécurité des Applications Web et API (WAAP/DAST/SAST) - suite.

Fonction IA	Description simple	Exemple concret	Bénéfice
Détection d'anomalies comportementales (UEBA)	L'IA apprend ce qui est un trafic normal vers une application ou une API et détecte toute activité inhabituelle.	Une tentative d'injection SQL génère un volume de requêtes bizarre → alerte ou blocage	Détection immédiate d'attaques inconnues
Protection contre les bots et abus logiques	L'IA reconnaît les comportements automatisés malveillants (bots intelligents)	Bot qui teste des milliers de mots de passe volés (credential stuffing)	Réduction des fraudes automatiques
Analyse proactive du code et vulnérabilités (SAST / DAST)	L'IA analyse le code et les applications pour trouver des failles avant attaque	L'IA détecte une mauvaise configuration ou faille SQL avant mise en production	Prévention au lieu de réaction
Sécurisation intelligente des API	L'IA surveille les abus, erreurs de configuration et attaques ciblant les API	Un attaquant abuse d'un endpoint mal sécurisé	Renforcement des services exposés
Détection des vulnérabilités critiques (OWASP Top 10)	L'IA détecte les attaques sophistiquées ciblant les vulnérabilités connues.	- Injections SQL/XSS polymorphes détectées par un WAF IA (CNN)	Protection avancée contre les vulnérabilités critiques connues

3.2. Sécurité des données et bases de données

Domaine	Fonction IA	Description simple	Exemple concret	Bénéfice
Surveillance des accès aux données	Surveillance contextuelle et granulaire	L'IA analyse en continu qui accède à quoi, quand et comment	Un utilisateur accède à une base de données hors horaires habituels	Détection rapide des accès suspects
Détection d'abus de privilèges	Analyse du comportement utilisateur	L'IA crée une base de référence du comportement normal des utilisateurs	Un DBA passe soudainement de 10 tables/jour à 50	Identification des menaces internes
Classification automatique des données	NLP et étiquetage intelligent	L'IA identifie les données sensibles dans les bases	Détection automatique de champs contenant des numéros CB	Protection ciblée des données critiques

3.3. Analyse des logs et prédiction

Fonction IA	Description simple	Exemple concret	Bénéfice principal
Analyse en temps réel des logs	L'IA collecte et corrèle automatiquement les logs provenant de serveurs, applications et réseaux.	Détection d'une série de tentatives de connexion échouées sur plusieurs serveurs	Détection rapide d'attaques en cours ou de comportements suspects
Détection d'anomalies dans les logs	L'IA identifie des motifs inhabituels ou des séquences d'événements qui diffèrent de la normale.	Un utilisateur accède à un fichier sensible à une heure inhabituelle	Identification proactive des menaces internes ou externes
Prédiction d'attaques futures	L'IA utilise des modèles de Machine Learning pour anticiper des comportements malveillants.	Prévision d'une attaque DDoS sur un serveur en détectant une hausse inhabituelle de trafic	Prévention et préparation avant que l'attaque ne survienne
Priorisation des alertes	L'IA évalue la criticité des événements et filtre les faux positifs.	1000 alertes journalières regroupées en 10 incidents prioritaires	Gain de temps pour les analystes et focus sur les menaces réelles
Visualisation intelligente des incidents	L'IA génère des dashboards et graphes basés sur la corrélation des logs.	Graphiques montrant l' évolution des tentatives d'accès suspect sur le réseau	Aide à la compréhension rapide et à la décision stratégique

3.4. Sécurité des Réseaux & Infrastructures

Fonction IA	Description simple	Exemple concret	Bénéfice principal
Détection des intrusions réseau (NIDS/NIPS intelligents)	L'IA surveille le trafic réseau pour identifier des comportements inhabituels ou malveillants.	Détection d'une tentative de scan de ports inhabituelle sur le réseau interne	Identification rapide des attaques et prévention des intrusions
Prévention des attaques DDoS	L'IA analyse le trafic en continu pour repérer les pics anormaux et les flux malveillants.	Augmentation soudaine de requêtes sur un serveur web	Maintien de la disponibilité des services et réduction des interruptions
Segmentation et contrôle dynamique du réseau	L'IA ajuste automatiquement les règles de firewall et de segmentation en fonction des menaces détectées.	Isolation automatique d'un segment compromis par un malware	Limitation de la propagation des attaques dans le réseau
Surveillance des périphériques et IoT	L'IA identifie les appareils connectés et détecte des comportements suspects.	Un IoT commence à envoyer du trafic vers des destinations inconnues	Protection des infrastructures sensibles et prévention des compromissions
Analyse prédictive des vulnérabilités réseau	L'IA anticipe les failles potentielles dans les équipements et configurations.	Détection d'un firmware obsolète sur un routeur critique	Planification proactive des mises à jour et réduction des risques

4. Exemples d’outils et bibliothèques IA en cybersécurité

4.1. Outils IA pour la sécurité des Applications Web et API

Outil / Bibliothèque	Type / Fonction IA	Exemple d'usage	Open Source / Commercial
Imperva WAF + AI	WAF IA détectant les injections polymorphes et les abus d'API	Bloque SQLi/XSS avancées et appels API anormaux	Commercial
Data Theorem	Analyse sécurisée des applications et API (SAST / DAST + IA)	Détection de vulnérabilités dans le code et API	Commercial
OWASP ZAP + ML plugin	Test dynamique IA / ML pour trouver failles	Analyse automatique des applications web pour vulnérabilités	Open Source
Bibliothèques Python (Scikit-learn, TensorFlow, PyTorch)	Détection de patterns suspects dans le trafic API	Identification de comportements anormaux dans les requêtes	Open Source

4.2. Outils IA pour la sécurité des données et bases de données

Outil / Bibliothèque	Type / Fonction IA	Exemple d'usage	Open Source / Commercial
IBM Guardium	Surveillance IA des accès aux données et détection d'abus de privilèges	DBA accède à un nombre anormal de tables. Une alerte est donnée.	Commercial
Varonis	IA pour classification automatique et protection des données sensibles	Identification de PII, PCI, PHI dans les bases de données	Commercial
Apache Ranger + ML modules	Surveillance et classification des accès sur Hadoop / bases	Détection d'accès anormal aux données	Open Source
Bibliothèques Python (Pandas + Scikit-learn / TensorFlow)	Détection d'anomalies dans bases de données	Identifier requêtes inhabituelles ou exfiltration	Open Source

4.3. Outils IA pour l'analyse des logs et prédiction

Outil / Bibliothèque	Type / Fonction IA	Exemple d'usage	Open Source / Commercial
Elastic Security (SIEM)	ML pour détection d'anomalies et patterns de menace	Détection exfiltration de données ou attaques réseau	Open Source (core) ; ML avancé payant
Graylog + ML plugin	Analyse avancée des logs et alertes prédictives	Détecte comportements inhabituels et incidents	Open Source
IBM QRadar Advisor with Watson	Corrélation IA des événements de sécurité	Analyse automatique de milliers de logs	Commercial
Prometheus + AI / anomaly detection libraries	Collecte métriques et détection IA / ML	Prédiction de comportement réseau ou serveur anormal	Open Source
Logstash + Elastic Stack ML	Pipeline de logs + détection IA	Détection anomalies et patterns dans les logs	Open Source (core) ; ML avancé payant
Microsoft Defender for Endpoint	Endpoint + Cloud IA	Détecte malware et comportements suspects sur postes Windows	Commercial

4.4. Outils IA pour la sécurité des Réseaux & Infrastructures

Outil / Bibliothèque	Type / Fonction IA	Exemple d'usage	Open Source / Commercial
Darktrace	IA comportementale pour détection d'intrusions réseau	Détection mouvements latéraux et accès inhabituels	Commercial
Vectra AI	Détection IA des comportements suspects réseau	Repère compromission de comptes et attaques invisibles	Commercial
Snort / Suricata + ML modules	IDS/IPS IA pour détection adaptative des intrusions	Identifier attaques réseau inconnues	Open Source
Cisco Secure Network Analytics (Stealthwatch)	Analyse IA du trafic réseau et détection d'anomalies	Détecte malware, DDoS et mouvement latéral	Commercial

5. Exercice pratique : analyse de fichiers de log d'une instance Laravel

Objectifs et bibliothèques correspondant

Objectifs	Bibliothèques utilisées
Analyse descriptive et Catégorisation des erreurs	Pandas, NLTK, Scikit-learn (KMeans)
Définition des niveaux de priorité des erreurs	Pandas, Scikit-learn
Détection d'Anomalies : cas des erreurs inhabituelles	Pandas, Scikit-learn

Stacks de développement :

- Python
- Flask

Commandes pour installer les dépendances :

pip install flask pandas scikit-learn numpy joblib nltk

Rôle des dépendances installées

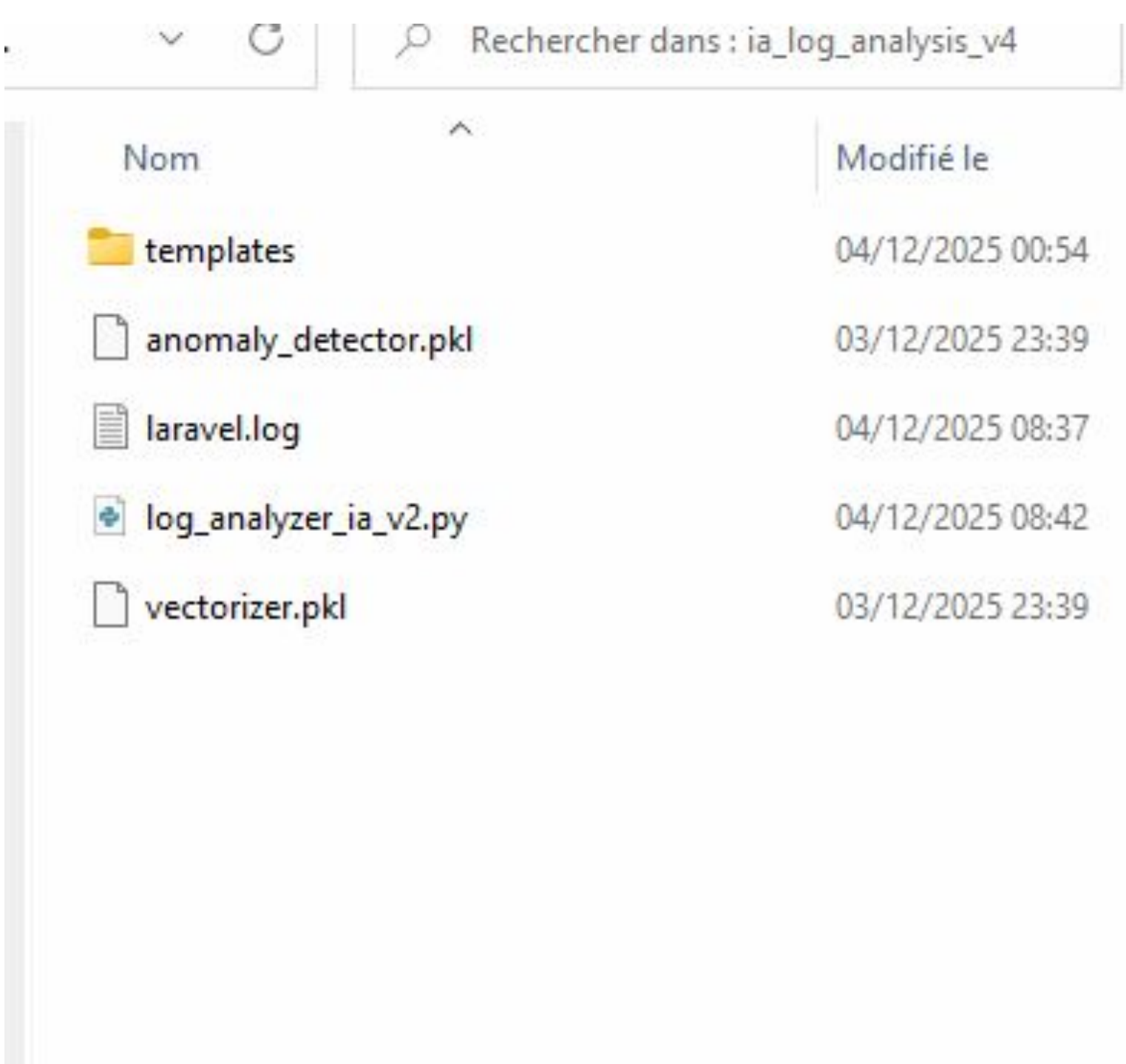
Dépendance	Rôle dans le Script
flask	Le framework web pour créer le serveur et l'interface HTML.
pandas	Essentiel pour la manipulation des données, le nettoyage, et l'analyse structurée des logs (DataFrames).
scikit-learn	La bibliothèque de Machine Learning qui fournit les algorithmes d'IA : **KMeans** (Clustering) et **IsolationForest** (Détection d'Anomalies).
numpy	Utilisé par Pandas et Scikit-learn pour les calculs numériques rapides.
joblib	Utilisé pour sauvegarder et charger le modèle d'anomalie (IsolationForest) sur le disque.
nltk	Utilisé pour le traitement du langage naturel (**NLP**) et le téléchargement des *stopwords* nécessaires au nettoyage des messages de log avant le clustering.

Lien de téléchargement du script

bit.ly/3Y47yVR

Lien du fichier Laravel.log
bit.ly/4oAtumr

python3 log_analyzer_ia_v2.py


Rechercher dans : ia_log_analysis_v4
Nom
Modifié le
templates
04/12/2025 00:54
anomaly_detector.pkl
03/12/2025 23:39
laravel.log
04/12/2025 08:37
log_analyzer_ia_v2.py
04/12/2025 08:42
vectorizer.pkl
03/12/2025 23:39

LOG_FILE_PATH = 'laravel.log'

* Running on all addresses (0.0.0.0)
 * Running on http://127.0.0.1:5000
 * Running on http://91.134.88.105:5000

Module 2 : Défenses innovantes – **Intégrer l'IA dans la cybersécurité.**

– FIN –