

IT GAME Bachelor 2025

KEYCE Academy



Table des matières

Table des matières 2

Contexte du Projet..... 3

Objectifs du projet..... 3

Description Détaillée des Tâches 4

 1. Récupération Automatique des Données4

 2. Analyse Technique des Logs4

 3. Dashboard Interactif4

 4. Conception du Produit (Proof of Concept).....4

Présentation des résultats 5

Critères d'évaluation 5

Informations Techniques 6



Contexte du Projet

Votre équipe intervient pour la société Pallad, une entreprise soucieuse de renforcer la sécurité informatique de ses clients. Pallad vous fournit un accès à distance à des logs d'activité via une API dédiée. Votre mission est de récupérer ces logs, les analyser et proposer une solution innovante, complète et commercialisable en cybersécurité.

Objectifs du projet

- Récupérer et analyser les fichiers logs fournis par l'API.
- Identifier clairement les cyberattaques en utilisant les bonnes pratiques du secteur.
- Concevoir et développer une solution de cybersécurité commerciale sous forme de Proof of Concept (POC).



Description Détaillée des Tâches

1. Récupération Automatique des Données

Connectez-vous à l'API fournie pour télécharger automatiquement les fichiers logs.

2. Analyse Technique des Logs

Analysez les fichiers PCAP de façon automatisée.

Intégrez une vérification automatisée des adresses IP (ex : VirusTotal, AbuseIPDB).

Détectez et catégorisez les attaques selon le référentiel MITRE ATT&CK, en modélisant clairement les étapes :

- Initial access
- Execution
- Persistence
- Privilege escalation
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Collection

3. Dashboard Interactif

Développez un tableau de bord interactif permettant de visualiser vos analyses :

- Afficher clairement les indicateurs clés : IP malveillantes, heure des incidents, machines ciblées, etc.
- Permettre une visualisation intuitive des données analysées.
- Permettre de suivre automatiquement l'évolution des données et des attaques détectées.

4. Conception du Produit (Proof of Concept)

Proposez une solution complète incluant :

- Branding du produit (nom, identité visuelle, logo).
- Présentation marketing attractive.
- Déterminez un prix réaliste et justifié pour votre solution (analyse des solutions concurrentes, positionnement de votre produit).



Présentation des résultats

La présentation de la solution se déroulera de la façon suivante :

- Une présentation orale de 15 minutes maximum, durant laquelle chaque membre de l'équipe devra obligatoirement prendre la parole.
- Durant cette présentation, vous devrez clairement détailler :
 - La méthodologie et l'automatisation mise en place.
 - Le fonctionnement détaillé du dashboard interactif développé.
 - La stratégie marketing adoptée (branding, étude de marché, pricing).
- Une session de 10 minutes de questions-réponses suivra immédiatement votre présentation.

Critères d'évaluation

Qualité Technique

- Fiabilité et précision de l'analyse technique des logs.
- Efficacité et robustesse de l'automatisation mise en place.

Ergonomie du Dashboard

- Interface intuitive et esthétique.
- Pertinence des informations affichées.

Qualité de la Présentation Orale

- Clarté et structuration de la présentation.
- Participation équilibrée et pertinente de chaque membre de l'équipe.
- Capacité à répondre efficacement aux questions posées lors de la session Q&A.

Pertinence Commerciale

- Attractivité du branding et des supports marketing.
- Réalisme de l'étude de marché et de la justification du pricing proposé.

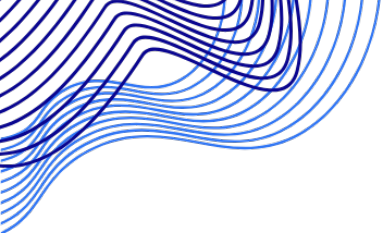


Informations Techniques

Adresse API fournie :

<http://93.127.203.48:5000/pcap/latest>

Cette adresse est UNIQUEMENT accessible depuis le réseau interne de l'école.



pa||pd

CYBERSÉCURITÉ. AUDIT. CONSEIL.