Scholanova

Apprendre ensemble

# BTS Services informatiques aux organisations :

Devoir sur Table

---

# Cas CaledoBank

---

2023-2024

# Table des matières

# 1 Cas CaledoBank

## 1.1 Dossier A Centralisation et exploitation des informations de supervision

### 1.1.1 Mission A1 Étudier l'apport de la centralisation des fichiers journaux et des métriques

En complément de la supervision en temps réel, les ingénieurs système et réseau doivent régulièrement effectuer le suivi des données obtenues via les différents systèmes de journalisation aussi bien au niveau des actifs réseaux que des serveurs. Vous avez en charge létude de la solution de centralisation et danalyse des fichiers journaux et des métriques fournies par la suite logicielle Elastic Stack.

**Question A1.1**
Rédiger une courte synthèse expliquant en quoi les outils composant la suite logicielle Elastic Stack répondent aux besoins de la banque CalédoBank.

**Réponse :**
La suite logicielle Elastic Stack, composée de Beats, Logstash, Elasticsearch, et Kibana, répond parfaitement aux besoins de centralisation et d'analyse des journaux et des métriques pour CalédoBank. Beats collecte les données depuis diverses sources, Logstash les transforme et les transporte, Elasticsearch sert de moteur de stockage et d'indexation, et Kibana offre une interface d'analyse et de visualisation. Cette suite permet une analyse efficace, en temps réel, des données, ce qui est crucial pour la détection d'anomalies et la réponse rapide aux incidents, améliorant ainsi la sécurité et la performance du SI de CalédoBank.

Peu de temps après la mise en production de la suite logicielle Elastic Stack, les informations relevées sur le tableau de bord relatif au serveur déchange de fichiers alertent la RSSI. Une augmentation très importante du trafic vers ce serveur a été détectée. Vous devez analyser ce flux de données anormal capturé par un équipement TAP2 positionné avant le serveur.

**Question A1.2**
- Indiquer ladresse IP du serveur de fichiers impliqué, le numéro de port et le protocole applicatif associés.
- Identifier le type dattaque potentiellement subie par le serveur et les éléments qui le démontrent. Puis, indiquer, si selon vous lattaque a réussi ou non. Justifier la réponse.

**Réponse :**
- D'après le journal du serveur déchange de fichiers, l'adresse IP du serveur impliqué est "192.168.134.212", le numéro de port utilisé est "990" (FTPS), et le protocole applicatif associé est FTPS (File Transfer Protocol Secure).
- Le type d'attaque subie semble être une attaque par force brute, comme le démontre la répétition des tentatives de connexion avec différents noms dutilisateur et échecs de connexion. L'attaque ne semble pas avoir réussi, car aucune connexion réussie n'est enregistrée ; toutes les tentatives mentionnées sont des échecs de connexion.

**Question A1.3**
Indiquer deux mesures que vous prendriez, au niveau de la configuration du serveur sans recours à un matériel supplémentaire, pour améliorer le niveau de protection contre ce type dattaque. Justifier la réponse.

**Réponse :** Deux mesures pour améliorer le niveau de protection contre ce type d'attaque sans matériel supplémentaire pourraient être :

- Limitation des tentatives de connexion : Configurer le serveur pour limiter le nombre de tentatives de connexion échouées d'une même adresse IP, réduisant l'efficacité des attaques par force brute.
- Utilisation de mots de passe complexes et politique de renouvellement : Encourager l'utilisation de mots de passe complexes et mettre en place une politique de renouvellement régulier des mots de passe pour diminuer les chances de succès d'une attaque par force brute.

### 1.1.2 Mission A2 Rechercher des vulnérabilités dans linfrastructure système et applicative

Suite à une alerte du réseau CERT.FR, datant du 22 septembre 2020, indiquant une recrudescence dattaques dans le milieu bancaire par le cheval de Troie Emotet, Léa Deschamps, la RSSI de CalédoBank, vous demande de vérifier que le système informatique na pas été infecté et de lui remettre un document indiquant la procédure suivie.

**Question A2.1**
Détailler la recherche de traces permettant détablir si le système informatique est infecté ou non par le cheval de Troie Emotet.

**Réponse :**
Pour détecter si le système informatique est infecté par Emotet, utilisez des outils comme EmoCheck pour identifier les processus malveillants correspondant au dictionnaire Emotet, et consultez des bases de données telles que Feodotracker pour identifier toute communication avec des serveurs de commande et de contrôle connus d'Emotet. Examiner les journaux système et de courriel pour des signes d'activité suspecte, tels que des envois de courriels inattendus ou des fichiers joints malveillants.

Aucun indice ne semble faire penser que le système informatique soit infecté actuellement. Seulement la recrudescence de ce cheval de Troie inquiète Léa Deschamps. Elle vous demande de proposer une stratégie visant à réduire les risques de compromission par ce logiciel malveillant.

**Question A2.2**
Proposer trois mesures à mettre en place afin de réduire les risques de compromission par ce logiciel malveillant. Justifier la réponse.

**Réponse :**
Trois mesures pour réduire les risques de compromission par Emotet incluraient :

- Formation à la sensibilisation : Former les employés à reconnaître les tentatives de phishing et à ne pas ouvrir de pièces jointes ou cliquer sur des liens dans des courriels suspects.
- Mise à jour régulière des systèmes et des logiciels : Appliquer régulièrement des mises à jour de sécurité pour tous les systèmes et logiciels afin de corriger les vulnérabilités qui pourraient être exploitées par Emotet.
- Solutions antivirus et antimalware : Utiliser et maintenir à jour des solutions antivirus et antimalware robustes, capables de détecter et de bloquer Emotet et d'autres malwares.

## 1.2 Dossier B Intégration de lapplication de gestion des crédits à la consommation

CalédoBank, qui jusqualors sous-traitait les demandes de crédit à la consommation à la société rachetée, souhaite intégrer lactivité de gestion des demandes de crédits à la consommation à son système dinformation. La banque souhaite étudier le développement dune application web spécifique permettant de collecter les informations du demandeur de crédit à la consommation et de lui proposer loffre de prêt correspondante. Cette application dénommée CréditPlus sera dans un premier temps liée avec lapplication CréditCal (application de demandes de crédit à la consommation) afin daccéder à sa base de données spécifique et à lapplication interne de gestion des prêts à la consommation de CalédoBank.

### 1.2.1 Mission B1 Vérifier la procédure de demande de crédit à la consommation

La DPD souhaite vérifier que le recueil et le traitement des données envisagés dans le cadre de la nouvelle application web CréditPlus sont conformes au RGPD, elle vous demande de participer à lanalyse dimpact relative à la protection des données.

**Question B1.1**
Identifier, parmi les données personnelles collectées à travers le formulaire de demande de crédit, celles qui paraissent non pertinentes ou qui porteraient atteinte à la vie privée au regard du RGPD.

**Réponse :**
En examinant le formulaire de demande de crédit à la consommation CalédoBank, les données personnelles collectées qui peuvent paraître non pertinentes ou susceptibles de porter atteinte à la vie privée au regard du RGPD incluraient la demande de la "communauté d'appartenance" qui est facultative. Ce type d'information peut être sensible et n'est pas directement nécessaire pour évaluer la solvabilité ou la capacité de remboursement du demandeur, rendant son utilité pour la demande de crédit discutable.

**Question B1.2**
- Relever les droits de lutilisateur du service mentionnés dans le formulaire de demande de crédit.
- Indiquer si ces droits sont tous présents. Justifier la réponse.

**Réponse :**
- Les droits mentionnés dans le formulaire de demande de crédit incluent le droit d'accès, de rectification et d'effacement des données, la limitation du traitement, l'opposition, le droit à la portabilité des données, et le droit de retirer le consentement à tout moment.
- Ces droits couvrent l'essentiel des droits prévus par le RGPD. Cependant, il est important de s'assurer que la mise en uvre pratique de ces droits est claire pour l'utilisateur, notamment la manière de les exercer facilement et la présence d'informations sur le délégué à la protection des données (DPD) pour toute question ou préoccupation.

CalédoBank a identifié les risques sur lapplication de gestion des crédits à la consommation. Vous avez la charge de lanalyse de deux risques :
- risque 1 : vol dune tablette par une personne externe à CalédoBank ;
- risque 2 : un pirate intercepte les données transmises via le réseau Wifi.

**Question B1.3**
Proposer pour chaque risque les niveaux de gravité et de vraisemblance en les justifiant ainsi que les impacts sur les critères de sécurité. Vous vous appuierez sur la méthode préconisée dans le document B5.

**Réponse :**
Pour chaque risque :
- Vol dune tablette :
  - Gravité : Élevée, car cela pourrait mener à une fuite d'informations sensibles des clients.
  - Vraisemblance : Moyenne, compte tenu de l'accès relativement facile aux tablettes.
  - Impact : Atteinte à la confidentialité des données clients.
- Pirate intercepte les données via le réseau Wifi :
  - Gravité : Élevée, car les informations interceptées peuvent inclure des données personnelles sensibles.
  - Vraisemblance : Moyenne à élevée, dépendant de la sécurité actuelle du réseau Wifi.
  - Impact : Atteinte à la confidentialité et à l'intégrité des données.

**Question B1.4**
Proposer, pour chacun des risques identifiés, trois mesures permettant de les diminuer.

**Réponse :**
Pour chaque risque :
- Vol dune tablette :
  - Chiffrement des données stockées sur la tablette.
  - Verrouillage sécurisé des bureaux où les tablettes sont stockées.
  - Formation du personnel sur la sécurité physique et l'importance de surveiller l'équipement.
- Pirate intercepte les données via le réseau Wifi :
  - Utilisation d'un VPN pour chiffrer le trafic de données.
  - Mise à jour du protocole de sécurité Wifi vers WPA3, si possible.
  - Audit régulier de la sécurité du réseau Wifi pour détecter et corriger les vulnérabilités.

### 1.2.2 Mission B2 Dématérialiser la procédure doffre de prêt

Vous avez la charge détudier la possibilité pour le client daccepter loffre de prêt en la signant électroniquement et de convaincre le DSI du bien fondé de cette proposition. Le type dauthentification prévu, permettant daccéder à la signature électronique, est le suivant :
- la connexion à lespace client se réalise via une authentification classique avec un nom d'utilisateur et un mot de passe ;
- pour chaque opération sensible, un code de vérification est ensuite envoyé par SMS sur le téléphone portable de la personne cliente.

Mais la lecture des nouvelles recommandations de lANSSI (document B6.1) alerte Léa Deschamps sur le niveau de sécurité mis en uvre.

**Question B2.1**
Proposer, pour chacun des risques identifiés, trois mesures permettant de les diminuer.

**Réponse :**
L'authentification telle que décrite n'est pas considérée comme forte selon les recommandations de l'ANSSI, car bien qu'elle implique deux facteurs (quelque chose que l'utilisateur connaît : le mot de passe, et quelque chose qu'il possède : le téléphone portable pour recevoir le SMS), la méthode via SMS est considérée comme moins sécurisée en raison de la vulnérabilité aux attaques de redirection de SMS ou de SIM swap.

Vous réalisez un ensemble de tests techniques afin de vous assurer du fonctionnement sécurisé de la procédure de signature par lapplication CréditPlus. Dans un premier temps, vous avez signé un document au format PDF en utilisant un ensemble de commandes sous environnement

Linux sur le serveur web. Vous devez maintenant vérifier que la signature est conforme. Pour cela vous disposez du certificat éphémère produit par lautorité de certification, du document qui a été signé, de la signature et de la syntaxe des commandes nécessaires.

**Question B2.2**
Proposer la démarche à suivre pour vérifier la signature en détaillant les commandes OpenSSL que vous utilisez

**Réponse :**
La vérification de la signature électronique peut impliquer les étapes suivantes :

- Extraire la clé publique du certificat éphémère avec openssl x509.
- Utiliser openssl rsautl avec l'option -verify pour vérifier la signature du document en utilisant la clé publique.
- Comparer l'empreinte originale du document avec celle obtenue après vérification pour s'assurer qu'elles correspondent, en utilisant la commande diff.

Le principe de la dématérialisation de loffre de prêt est adopté. Il est maintenant nécessaire de préparer le changement. La réception dun courriel (mail) par le client est le point de départ de lacceptation de loffre de prêt à distance. Cest pourquoi CalédoBank souhaite minimiser les risques dhameçonnage de ses clients en affichant un avertissement sur le site de CalédoBank lors de la demande initiale de crédit. Le DSI vous confie cette tâche dinformation des clients.

**Question B2.3**
Lister trois éléments à intégrer dans lavertissement précisant les précautions à prendre par le client lors de la réception dun courriel (mail) supposé provenir de CalédoBank.

**Réponse :**
Les éléments à intégrer dans l'avertissement pourraient inclure :

- Vérification de l'adresse de l'expéditeur du courriel pour s'assurer qu'elle correspond à une adresse officielle de CalédoBank.
- Ne jamais fournir de données personnelles ou bancaires via un lien direct contenu dans un courriel.
- Être vigilant quant au contenu et à la forme des courriels : fautes dorthographe, logo de la banque, etc.

### 1.2.3 Mission B3 Sécuriser lhébergement des applications de la zone démilitarisée (DMZ)

La RSSI, Léa Deschamps, a fait appel à une entreprise spécialisée pour réaliser un audit de sécurité concernant lapplication de gestion de crédits qui serait hébergée dans la zone démilitarisée. Leurs conclusions alertent tout particulièrement sur les limites de larchitecture existante en termes de sécurité. Suite à cet audit et à la prise en compte des recommandations de lANSSI, dont un extrait est fourni dans le dossier documentaire, la RSSI propose dans lurgence, sans ajout de matériel supplémentaire, une nouvelle architecture dont le schéma de principe figure dans le document B8.2. Vous avez la charge de produire une synthèse justifiant le bien-fondé de cette proposition à destination du DSI.

**Question B3.1**

- Expliquer en quoi larchitecture actuelle est insuffisante pour garantir un niveau de sécurité au regard des recommandations de lANSSI.
- Justifier en conséquence la nouvelle infrastructure physique proposée.

**Réponse :**

- L'architecture actuelle est insuffisante car elle ne permet pas une séparation efficace entre les différents niveaux de sensibilité des informations et des services exposés. Cela peut augmenter le risque d'attaques réussies et d'exfiltration de données.
- La nouvelle infrastructure physique proposée avec une séparation en trois zones DMZ (interne, intermédiaire, externe) permet une meilleure segmentation du réseau et une réduction des risques de propagation des attaques au sein du système dinformation de CalédoBank.

Après validation de la proposition, vous avez la charge de mettre en uvre cette infrastructure temporaire.

**Question B3.2**

- Proposer, sur la nouvelle architecture, une répartition des sept serveurs virtuels (décrits en fin de document 2) fournissant les services exposés. Justifier la réponse.
- Indiquer les opérations à réaliser sur les pare-feux, tant au niveau de ladressage IP des interfaces quau niveau du principe des règles de filtrage (et non des règles elles-mêmes), pour rendre opérationnelle cette nouvelle topologie. Vous préciserez les adresses IP attribuées aux interfaces des pare-feux.

**Réponse :**

- La répartition des sept serveurs virtuels devrait tenir compte de la nature des services qu'ils offrent et de leur niveau de sensibilité. Par exemple, les serveurs web et proxy dans la DMZ externe, les serveurs d'applications métier dans la DMZ intermédiaire, et les serveurs de bases de données dans la DMZ interne.
- Les opérations sur les pare-feux devraient inclure la configuration des règles de filtrage pour n'autoriser que le trafic nécessaire entre les zones, ainsi que l'attribution d'adresses IP spécifiques aux interfaces des pare-feux pour faciliter la gestion du trafic entre les zones.