Exercice Adventure builder

https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=146280205

Équipe 01

Équipe 02

Équipe 03

Équipe 04

Équipe 05

Équipe 06

Équipe 07

Équipe 08

Équipe 09

Équipe 10

Équipe 01

1. Sécurité : QAS5 et QAS6– identifier les éléments du scénario, les tactiques et les éléments de l'architecture qui implémenteront celles-ci.

2. Disponibilité : QAS4 et QAS7– identifier les éléments du scénario, les tactiques et les éléments de l'architecture qui implémenteront celles-ci

3. Interopérabilité: Ajouter un scénario de qualité pour l'interopérabilité

4. Utilisabilité : Ajouter un scénario de qualité pour l'usabilité

QAS5: Sécurité

- QAS5. Credit approval and payment processing are requested for a new order. In one hundred percent of the cases, the transaction is completed securely and cannot be repudiated by either party. The business goals are to provide customers and business partners confidence in security and to meet contractual, legal, and regulatory obligations for secure credit transactions.

QAS5. L'approbation du crédit et le traitement du paiement sont demandés pour une nouvelle commande. Dans cent pour cent des cas, la transaction est effectuée en toute sécurité et ne peut être répudiée par aucune des parties. Les objectifs commerciaux sont de fournir aux clients et aux partenaires commerciaux la confiance en la sécurité et de respecter les obligations contractuelles, légales et réglementaires pour les transactions de crédit sécurisées.

Source	Le système bancaire
Stimulus	L'attaquant fraude en donnant des fausses informations pour approuver son crédit.
Artéfact	formulaire de demande de crédit
Environnement	formulaire est connectée en permanence sur le réseau bancaire de l'entreprise . Il est toujours opérationnel
Réponse	le système avertit les responsable d'une tentative de fraude est en train de se produire , crédit refusé
Mesure de la réponse	Le système affiche les tentatives de fraudes chaque 30 secondes . Nb tentative de fraude ?

Tactiques :

- **Détecter les attaques** : Détecter les intrusions
- **Résister aux attaques :** Identifier les acteurs - Authentifier les acteurs - Autoriser les acteurs
- **Réagir aux attaques** : Informer les acteurs - Révoquer l'accès.
- **Récupérer des attaques** : Maintenir une trace d'audit

Éléments de l'architecture :

Équipe 02

1. Sécurité : QAS5 et QAS6– identifier les éléments du scénario, les tactiques et les éléments de l'architecture qui implémenteront celles-ci.à

QAS5: Credit approval and payment processing are requested for a new order. In one hundred percent of the cases, the transaction is completed securely and cannot be repudiated by either party. The business goals are to provide customers and business partners confidence in security and to meet contractual, legal, and regulatory obligations for secure credit transactions.

Source	Humain de l'extérieur de l'organisation
Stimulus	Transaction effectuée avec l'organisation et non répudiée par les parties prenantes.
Artéfact	Données des clients (Carte de crédit)
Environnement	normal
Réponse	Des données sont enregistrées dans la DB (Adventure OPC DB)
Mesure de la réponse	Les données de la transaction sont encryptés

Tactiques:

- Encrypt data (s'assurer que le site web utilise HTTPS et SSL pour ajouter une couche supplémentaire)
- ~~Detect message delay~~

identify actor
authenticate / authorize

QAS6: The OPC experiences a flood of calls through the Web Service Broker endpoint that do not correspond to any current orders. In one hundred percent of the times, the system detects the abnormal level of activity, notifies the system administrator, and continues to service requests in a degraded mode.

Source	Systèmes externes
Stimulus	Multi appels vers le endpoint du Web Service Broker de commandes inexistantes
Artéfact	Endpoint de l'API
Environnement	
Réponse	
Mesure de la réponse	

Tactiques:

-
-

Éléments de l’architecture:

2. Disponibilité : QAS4 et QAS7– identifier les éléments du scénario, les tactiques et les éléments de l’architecture qui implémenteront celles-ci

3. Interopérabilité: Ajouter un scénario de qualité pour l’interopérabilité

4. Utilisabilité : Ajouter un scénario de qualité pour l’usabilité

Équipe 03

1. Sécurité : QAS5 et QAS6– identifier les éléments du scénario, les tactiques et les éléments de l'architecture qui implémenteront celles-ci.
2. QAS5. L'approbation du crédit et le traitement du paiement sont demandés pour une nouvelle commande. Dans cent pour cent des cas, la transaction est effectuée en toute sécurité et ne peut être répudiée par aucune des parties. Les objectifs commerciaux sont de fournir aux clients et partenaires commerciaux la confiance dans la sécurité et de respecter les obligations contractuelles, légales et réglementaires en matière de transactions de crédit sécurisées.
3. QAS6. L'OPC subit un flot d'appels via le point de terminaison Web Service Broker qui ne correspondent à aucune commande en cours. Dans cent pour cent des cas, le système détecte le niveau d'activité anormal, avertit l'administrateur système et continue de traiter les demandes en mode dégradé.

Source	un cl
Stimulus	
Artéfact	Données des clients (Carte de crédit)
Environnement	
Réponse	
Mesure de la réponse	

4. Disponibilité : QAS4 et QAS7– identifier les éléments du scénario, les tactiques et les éléments de l'architecture qui implémenteront celles-ci
5. Interopérabilité: Ajouter un scénario de qualité pour l'interopérabilité
6. Utilisabilité : Ajouter un scénario de qualité pour l'usabilité

Équipe 04

1. Sécurité : QAS5 et QAS6– identifier les éléments du scénario, les tactiques et les éléments de l'architecture qui implémenteront celles-ci.

QAS5:

Credit approval and payment processing are requested for a new order. In one hundred percent of the cases, the transaction is completed securely and cannot be repudiated by either party. The business goals are to provide customers and business partners confidence in security and to meet contractual, legal, and regulatory obligations for secure credit transactions

Source	Nouvelle commande
Stimulus	~~Demande de~~ paiement ou d'approbation de crédit
Artéfact	OPC et ~~Consumer Website~~
Environnement	À tout moment, quel que soit l'état du système
Réponse	La requête est traitée de manière sécuritaire. Trace laissée par la requête
Mesure de la réponse	Nb de cas qui ont été traités correctement (obj: 100%)

Tactiques:

- Authentification des acteurs, par système de token personnel par exemple, pour empêcher la répudiation.
- Autorisation des actions des acteurs selon le niveau de privilège qui leur est associé, pour éviter qu'une demande d'approbation de crédit ou de paiement soit faite à la place de l'utilisateur ou du système.
- Encryption de toutes les connexions et des données d'identification des utilisateurs afin qu'aucun "man-in-the-middle" puisse lire les données transmises.

Éléments de l'architecture:

- ~~OPC~~ et Consumer Website pour la gestion des tokens
- OPC pour la gestion des autorisations
- OPC et Consumer Website pour l'encryption

QAS6:

QAS6. The OPC experiences a flood of calls through the Web Service Broker endpoint that do not correspond to any current orders. In one hundred percent of the times, the system detects the abnormal level of activity, notifies the system administrator, and continues to service requests in a degraded mode.

Source	Système externe non identifié ou ~~Consumer Website~~
Stimulus	~~système externe qui~~ envoie beaucoup de requêtes sur des commandes inexistantes.
Artéfact	OPC
Environnement	À tout moment
Réponse	Le système détecte des niveaux anormaux d'activités, notifie l'administrateur, et réduit le niveau de service (mode dégradé).
Mesure de la réponse	100% du temps, le système détecte le niveau anormal d'activité et l'administrateur est notifié.

Tactiques:

- Détect attacks > Détect service denial -> Détecter si une attaque de déni de service est en cours.
- Resist attacks -> Limit access -> On limite les accès lorsqu'on se rend compte qu'un nombre trop important de requêtes est fait sur des orders inexistants
- React to attacks -> Inform Actors -> On informe les administrateurs quand on reçoit beaucoup de requêtes sur des commandes inexistantes.
- Authentification des acteurs via des tokens sur OPC

Éléments de l'architecture:

- OPC (PoEndpoint Bean) et ~~Consumer Website~~ pour les mécanismes de détection de nombre de requêtes important.
- ~~Consumer Website~~ pour la limitation des accès
- OPC et ~~Consumer Website~~ pour l'authentification

2. Disponibilité : QAS4 et QAS7– identifier les éléments du scénario, les tactiques et les éléments de l'architecture qui implémenteront celles-ci

QAS4:

QAS4. The Consumer Web site sent a purchase order request to the order processing center (OPC). The OPC processed that request but didn't reply to Consumer Web site within five seconds, so the Consumer Web site resends the request to the OPC. The OPC receives the duplicate request, but the consumer is not double-charged, data remains in a consistent state, and the Consumer Web site is notified that the original request was successful in one hundred percent of the times.

Source	Site web Consommateur
Stimulus	Le OPC n'a pas répondu au site web en 5 secondes.
Artéfact	OPC
Environnement	Normal operation
Réponse	Envoyer une 2iem requête identique
Mesure de la réponse	Nb de fois où on envoie une 2iem requete

Tactiques:

Recover from faults -> Preparation and Repair -> Retry : quand on n'a pas reçu de confirmation, on renvoie notre requête au serveur.

Éléments de l'architecture:

OPC qui tient un registre des requêtes en cours et Consumer Website qui recommence ses requêtes.

QAS7:

QAS7:The Consumer Web site is available to the user 24/7. If an instance of OPC application fails, the fault is detected and the system administrator is notified in 30 seconds; the system continues taking order requests; another OPC instance is created; and data remains in consistent state.

Source	Site du consommateur (interne).
Stimulus	Crash d'OPC d'origine logicielle
Artéfact	Instance OPC.
Environnement	À tout moment
Réponse	• Envoie une notification à l'administrateur du système (détection de la faute). • Démarrage d'une nouvelle instance d'OPC
Mesure de la réponse	• Prend environ 30 secondes pour prévenir l'administrateur du système. • Mesure du temps de démarrage d'OPC • Mesure du nombre de crashs par jour

Tactiques:

Redondance passive: démarrage d'une nouvelle instance d'OPC

Éléments de l'architecture:

3. Interopérabilité: Ajouter un scénario de qualité pour l'interopérabilité

Source	Consumer Website
Stimulus	Requête de Consumer Website vers OPC
Artéfact	OPC
Environnement	Avant le démarrage
Réponse	Information sur le succès de la transaction bancaire Confirmation de la réservation du vol Confirmation de la réservation du logement Confirmation de la réservation de l'activité
Mesure de la réponse	L'information est valide à 100% du temps.

Tactiques:

- Orchestrate
- Manager interface: Implémenter une interface afin de communiquer avec les services externes, afin que nous puissions en ajouter de nouveaux rapidement.

Éléments de l'architecture:

Bank, airline, lodging et activity provider. et l'interface créée afin de se connecter aux différents services.

4. Utilisabilité : Ajouter un scénario de qualité pour l'usabilité

Source	
Stimulus	
Artéfact	
Environnement	
Réponse	
Mesure de la réponse	

Tactiques:

Éléments de l’architecture:

Équipe 08

1. Sécurité : QAS5 et QAS6– identifier les éléments du scénario, les tactiques et les éléments de l'architecture qui implémenteront celles-ci.
   QAS5: Credit approval and payment processing are requested for a new order. In one hundred percent of the cases, the transaction is completed securely and cannot be repudiated by either party. The business goals are to provide customers and business partners confidence in security and to meet contractual, legal, and regulatory obligations for secure credit transactions.

Source	Humain (Utilisateur)
Stimulus	Tentative de requête non-autorisé pour une nouvelle commande. Accès non-autorisé aux données d'une nouvelle transaction et/ou aux données personnelles des clients.
Artéfact	Information de paiement ou de crédit pour la commande. Le système OPC. Données du système et données produites par le système (Prix d'une réservation, numéro de carte de crédit).
Environnement	Le système est en ligne, ouvert à tous et entièrement opérationnel.
Réponse	La transaction fonctionne et est sécurisée si les informations de l'utilisateur sont correctes et que l'utilisateur est authentifié et autorisé. La transaction a échoué avec des informations ou une authentification incorrectes.
Mesure de la réponse	100% des attaques ont étés bloquées.

Tactiques:
- Authentifier les utilisateurs de l'application avec 2 facteurs (mot de passe et autre au choix).
- Encrypter les données sensibles (numéro de carte de crédit) et la transaction.
- Détecter les tentatives d'intrusion sur le système.
- Vérifier l'intégrité des messages venant de l'extérieur lors de la transaction.

Éléments de l'architecture:
- La classe OPC
- Le CreditCardService

QAS6: The OPC experiences a flood of calls through the Web Service Broker endpoint that do not correspond to any current orders. In one hundred percent of the times, the system detects the abnormal level of activity, notifies the system administrator, and continues to service requests in a degraded mode.

Source	Système inconnu
Stimulus	Tentative d'accès répété au contenu d'un Order qui n'existe pas.
Artéfact	Les données du systèmes et le Web Service Broker
Environnement	Le système est en ligne, ouvert à tous et entièrement opérationnel.
Réponse	Notification à l'administrateur et le système continue son opération en mode "degraded".
Mesure de la réponse	100% des "flood" sont détectés et les messages sont bien transmis à l'administrateur.

Tactiques:
- Détecter les tentatives de déni de service sur le système OPC.

- Limiter l’accès aux Order avec un timer. Par exemple, on ne peut accéder qu'à un Order toutes les 10 secondes.
- Révoquer l’accès au système à un certain utilisateur/adresse IP qui est identifié comme un attaquant.
- Informer les administrateurs du problème détecté.

Élément de l’architecture:

- WebServiceBroker