CAS D'USAGE CYBERSÉCURITÉ

Orchestrating efficiency, inspiring trust

Cas d'usage – Gestion des actifs

Préoccupations

Comprendre quels sont les actifs présents sur votre réseau et comment ils sont intégrés.

Exigences & Contraintes

Permettre la disponibilité des services réseau tout en supprimant les actifs qui ne sont plus utiles ou qui présentent un risque pour la sécurité. Travailler en collaboration pour comprendre pourquoi chaque actif a été créé et comment il est utile au fonctionnement d'un service spécifique.

Services OFFERTS

- Suivi des actifs pour identifier l'actif, le propriétaire et le but.
- Évaluer les besoins de maintenance, les vulnérabilités, la valeur en tant que point d'attaque et l'élimination si nécessaire de chaque actif.
- Adhésion à des contrôles de sécurité guidés par normes industrielles telles que la norme ISO 27001.
- Révision des contrôles de sécurité pour les adapter aux cas d'utilisation particuliers des actifs de l'organisation.

Quels sont les avantages pour l'organisation ?

L'inventaire des actifs signifie que lorsqu'un actif est impliqué dans un incident de sécurité, les rapports d'incident et les contrôles appropriés sont déjà en place.

La propriété des actifs permettra aux utilisateurs finaux d'assumer la responsabilité de l'atténuation des risques et de la rationalisation des mesures correctives.

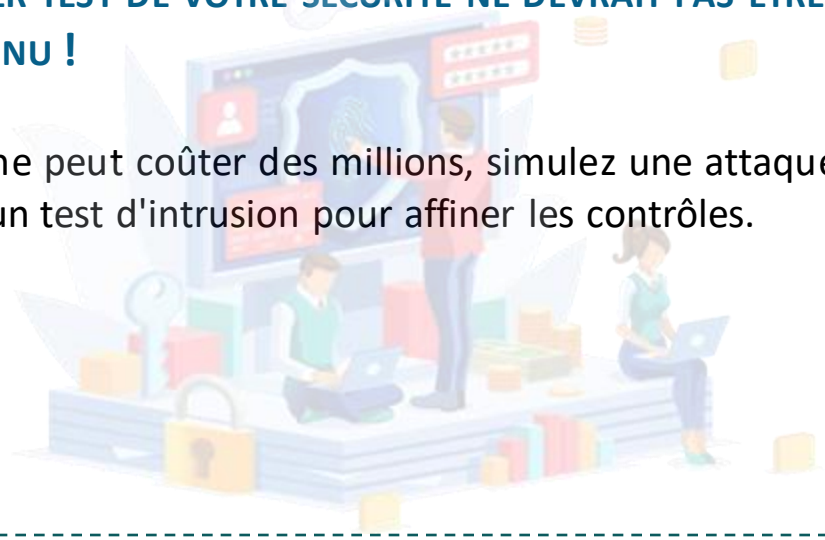
Faciliter l'audit de sécurité et les tests d'infiltration pendant la phase de planification.

Se conformer aux normes de sécurité du secteur, telles que la norme ISO 27001, afin d'instaurer la confiance avec les entreprises partenaires.

Cas d'usage – Tests d'intrusion

Le premier test de votre sécurité ne devrait pas être fait par un inconnu !

Une brèche peut coûter des millions, simulez une attaque externe pendant un test d'intrusion pour affiner les contrôles.



Étapes des tests d'intrusion

- Champ d'application
- Reconnaissance
- Modélisation des menaces
- Exploitation
- Exploitation des postes
- Analyse et rapports

Combler le fossé entre l'équipe de sécurité et les testeurs d'intrusion.

- Définissez un périmètre qui soit à la fois réalisable compte tenu de la taille de votre organisation et de vos ressources, et efficace pour capturer les actifs les plus prioritaires.
- Gérer les limites d'accès des testeurs d'intrusion aux ressources tout en n'entravant pas la disponibilité pour les utilisateurs finaux.
- Veiller à ce que les actifs soient restaurés dans les configurations antérieures à l'exploitation et que les vulnérabilités découvertes soient contrôlées.
- Intégrer l'ensemble de l'équipe de sécurité pour comprendre et communiquer les résultats des rapports de post-exploitation.

Quels sont les avantages pour l'organisation ?

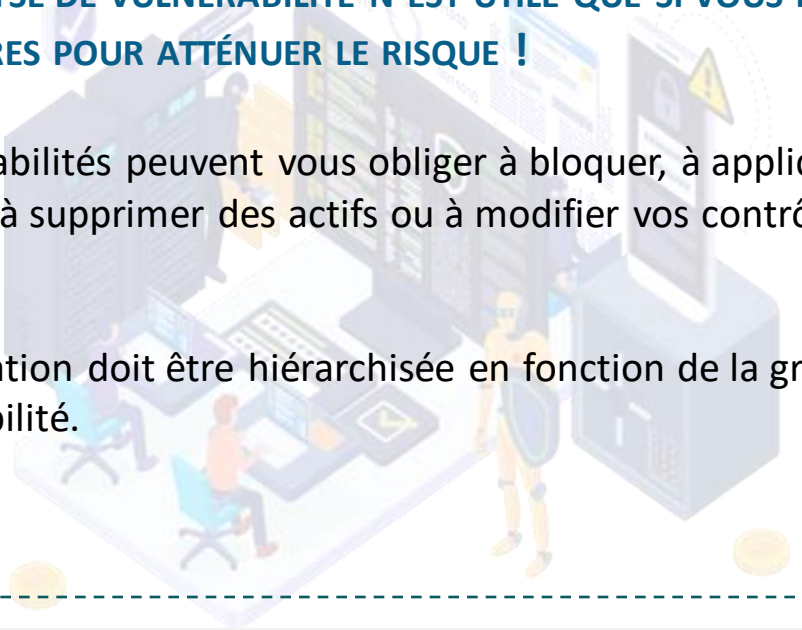
- Veiller à ce que les vulnérabilités soient identifiées avant la prochaine violation.
- Évaluer avec précision la valeur des actifs pour la sécurité du réseau.
- Minimiser le coût des violations de données.

Case d'usage – Gestion des vulnérabilités

Une analyse de vulnérabilité n'est utile que si vous prenez des mesures pour atténuer le risque !

Les vulnérabilités peuvent vous obliger à bloquer, à appliquer des correctifs, à supprimer des actifs ou à modifier vos contrôles actuels.

La remédiation doit être hiérarchisée en fonction de la gravité de la vulnérabilité.



Étapes de la gestion des vulnérabilités

- Identifier
- Évaluer
- Remédier à la situation
- Rapport

Communiquer un rapport sur la vulnérabilité pour permettre aux dirigeants de prendre des décisions.

- Hiérarchisation claire et concise de chaque vulnérabilité sur la base du système CVSS (Common Vulnerability Scoring System).
- Analyses régulières et répétées de la vulnérabilité à l'aide d'outils tels que Nessus Vulnerability Scanner pour effectuer des analyses SCAP et s'assurer que les mesures correctives progressent comme prévu.
- Planification de la remédiation pour permettre aux utilisateurs finaux de continuer à être productifs pendant les heures de pointe.
- Traiter et affiner les contrôles de sécurité en fonction des efforts de remédiation.

Quels sont les avantages pour l'organisation ?

- Veiller à ce que les vulnérabilités soient éliminées avant la prochaine violation.
- Diminuer les temps d'arrêt des services tout en maximisant la sécurité.
- Contrôles documentés basés sur les menaces spécifiques à l'organisation.

Cas d'usage – Managed Detection & Response (MDR)

Préoccupations

Faciliter la découverte active d'incidents de sécurité et l'exécution des réponses et des rapports.

Exigences & Contraintes

Fournir un MDR (Management Detection and Response) par l'utilisation du XDR (Extended Detection and Response) sans entraver la disponibilité des services et en respectant les contraintes de ressources du client.

Quels sont les avantages pour l'organisation ?

- Fournir des ressources qui ne sont pas organiques à l'organisation.
- Exploiter l'IA pour rationaliser une variété de services de sécurité.
- Diminuer le temps de persistance de l'attaque sur votre réseau.

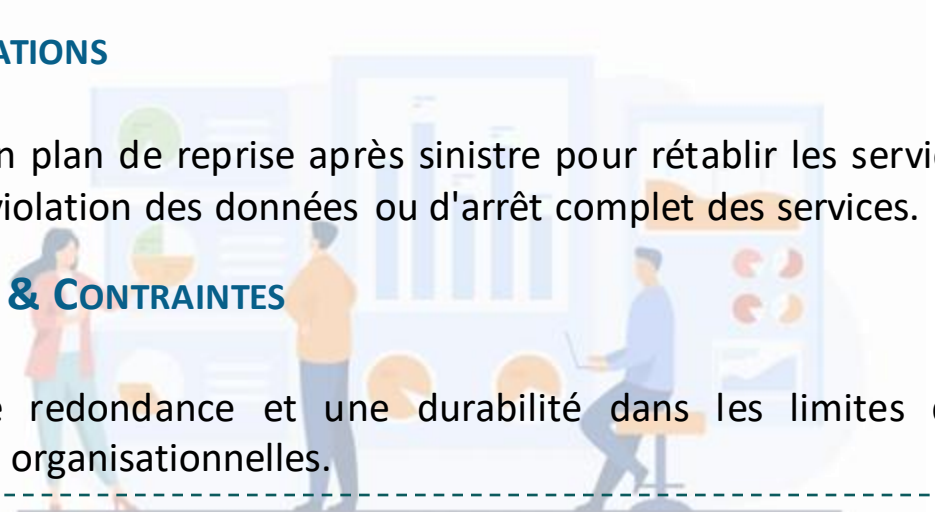
Services OFFERT

- Évaluer & améliorer
- Reduce the number of security tools you are forced to actively monitor, Integrate IDS/IPS with your other monitoring systems to catch suspicious traffic on Layer 2 through 7 of the OSI model
- Réduisez le nombre d'outils de sécurité que vous êtes obligé de surveiller activement. Intégrez les IDS/IPS à vos autres systèmes de surveillance pour détecter le trafic suspect sur les couches 2 à 7 du modèle OSI.
- Fixez des objectifs clairs et gérables pour améliorer votre niveau de sécurité.
- Auditez régulièrement vos procédures de déclaration et de réponse aux incidents.
- Utiliser des outils d'IA et de XDR pour recueillir en temps réel des informations sur les attaques potentielles.
- Utilisez les données générées par XDR pour concentrer les efforts de vos équipes sur les zones problématiques au lieu de chasser dans l'obscurité.

Cas d'usage – Planification de la continuité des opérations

Préoccupations

Élaborer un plan de reprise après sinistre pour rétablir les services en cas de violation des données ou d'arrêt complet des services.



Exigences & Contraintes

Créer une redondance et une durabilité dans les limites des ressources organisationnelles.

Quels sont les avantages pour l'organisation ?

- Réduire les temps d'arrêt après une violation
- Réduire les pertes de données en accédant aux sauvegardes incrémentielles
- Renforcez la confiance de vos clients qui savent qu'ils ne perdront pas l'accès à votre produit en cas de violation.

Services OFFERTS

- **Quel est le coût d'une perte de données pour votre organisation ?**

La réponse à cette question devrait déterminer combien votre organisation est prête à dépenser pour protéger ces données et combien elle est prête à dépenser pour créer une redondance afin de maintenir la disponibilité de ces données.

- **Quelles données doivent être restaurées en cas de violation des données ?**

Toutes les données ne doivent pas être restaurées immédiatement ou pas du tout. Décider de la valeur et de la priorité des données peut réduire le coût du stockage des données et la taille de l'infrastructure nécessaire pour restaurer les services.

- **Quelles menaces sont réalistes pour votre organisation ?**

Se préparer à un tsunami lorsque vos données sont stockées dans un désert peut ne pas être pratique ou utile. Un DRP doit être adapté aux besoins de votre organisation.

- **Comment allez-vous tester votre DRP ?**

Un test régulier de votre plan permettra de s'assurer que chacun est prêt à agir calmement en cas de crise.

Pour toute information complémentaire sur nos offres

Géraldine BLED
Managing Partner / CEO
43, rue des Remparts d'Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Gsm: +33(0)6 12 04 36 01
Email :geraldine.bled@opera-conseil.com

Sébastien AKL
Director of Sales and Business Developement
43, rue des Remparts d'Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Gsm : +33(0)6 13 66 46 83
Email :sebastien.akl@opera-conseil.com

Karine OUAINI
EPM/PPM solution manager
43, rue des Remparts d'Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Email :karine.ouaini@opera-conseil.com

Matheus MENEZES
COO / Salesforce solution manager
43, rue des Remparts d'Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Gsm: +33 (0)6 09 06 95 54
Email :matheus.menezes-pinheiro@opera-conseil.com

Mathew DAVIS
Cyber Security manager
43, rue des Remparts d'Ainay
69002 LYON
Tél : +33(0)4 78 84 08 85
Email :mathew .davis@opera-conseil.com