

Test de sécurité gratuit IBM

Mémento

Fonctions de base et procédures correctives

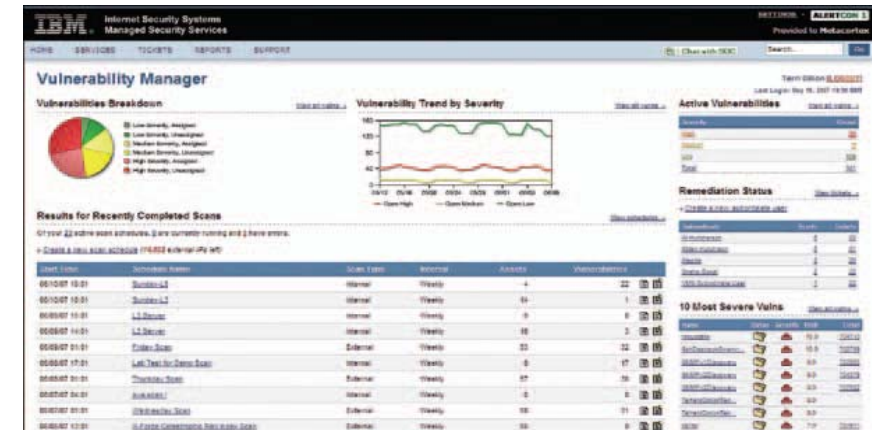
Connexion au VSOC (Virtual Security Operations Center)

Ouvrez votre navigateur et accédez à l'adresse : <https://portal.mss.iss.net>

1. Entrez votre identifiant.
2. Entrez votre mot de passe.
3. Cliquez sur Sign In



La page d'accueil du portail clients du VSOC apparaît.



4. Dans le menu, cliquez sur **Services** ⇒ **Vulnerability Management** pour accéder au menu Vulnerability Management Services (VMS).

Déconnexion du VSOC

1. Pour quitter le portail clients du VSOC, cliquez sur **Logout**, en haut de la page en cours.
2. Pour revenir à la page d'accueil du portail, cliquez sur **Home** au début de la barre de menu.

Contactez le centre

Pour plus de détails sur le fonctionnement de VMS, consultez les guides utilisateur détaillés accessibles via l'option **Document Repository** du menu **Support**.

L'IBM ISS Security Operations Center peut être contacté par e-mail en anglais : mss.support@iss.net ou par téléphone en français au : 01-57-32-32-41

Programmation d'une analyse

Le service VMS d'IBM Internet Security Systems vous permet de déterminer le moment et les modalités d'exécution des analyses (suivant les options souscrites). Les onglets du programmeur (Scan Scheduler) fournissent des informations complètes sur les analyses programmées (Active Scan Schedules) et les sessions en cours (Running Jobs), terminées (Completed) et problématiques (Errored).

1. Cliquez sur **Services** ⇒ **Vulnerability Management** ⇒ **Scan Scheduler**.

2. Cliquez sur le lien **Create a new scan**.

3. Actualisez les champs suivants :

- **Schedule Name** (nom de l'analyse) : ex., Scan 1
- **Description** : ex., Discovery Scan (analyse de découverte)
- **Scan Type** (type d'analyse) : ex., Interne ou Externe
- **Recurrence** (fréquence) : ex., One Time
- **Start Date** (date de démarrage) : ex., 05/05/07
- **Preferred Time** (heure préférée) : ex., 05:00 EST
- **Policy Type** (type de politique) : ex., DO Light Discovery
- **Target** (cible) : ex., S Portal Dev
- **IP Sub-range** (plage d'adresses) : (facultatif)

4. Actualisez les champs de notification. Indiquez les adresses e-mail individuelles ou alias de listes de diffusion des personnes à avertir de l'exécution de l'analyse.

5. Cliquez sur **Save Schedule**. L'analyse que vous venez de programmer sera listée dans l'onglet **Active Scan Schedule**.



Confirmation des ressources

L'étape qui suit une recherche de failles de sécurité consiste généralement à passer en revue et à confirmer les ressources (assets). Cette opération vous permet d'associer les failles à des tickets et de commencer à réduire votre exposition au moyen d'actions correctives.

1. Cliquez sur **Services** ⇒ **Vulnerability Management** ⇒ **Asset Inventory**.

• **Filtre d'affichage** – Des options vous permettent de filtrer les ressources affichées (toutes, non confirmées, ignorées ou vulnérables).

2. Cochez la case affichée en regard d'une ou plusieurs ressources.

3. Cliquez sur le bouton **Confirm** :

- **Confirm** : Confirme la ressource sélectionnée.
- **Merge** : Combine des ressources aux caractéristiques similaires.
- **Delete** : Supprime des ressources dont la gestion n'est plus nécessaire.
- **Ignore** : Ignore les ressources sélectionnées.

4. La page **Confirm Selected Assets** apparaît.

5. Actualisez les champs suivants :

- **Name** : Alias défini par l'utilisateur pour désigner la ressource.
- **Owner** : Responsable sécurité du système (peut être un Security Admin ou un Subordinate User). Pour créer un Subordinate User, reportez-vous à la section Préférences utilisateurs.
- **Criticality** : Sélectionnez le degré de criticité de la ressource.
- **Description** : Décrivez la fonction de la ressource.

6. Cochez la case **Update all Remaining Assets with the Same Information**.

7. Cliquez sur le bouton **Submit**.

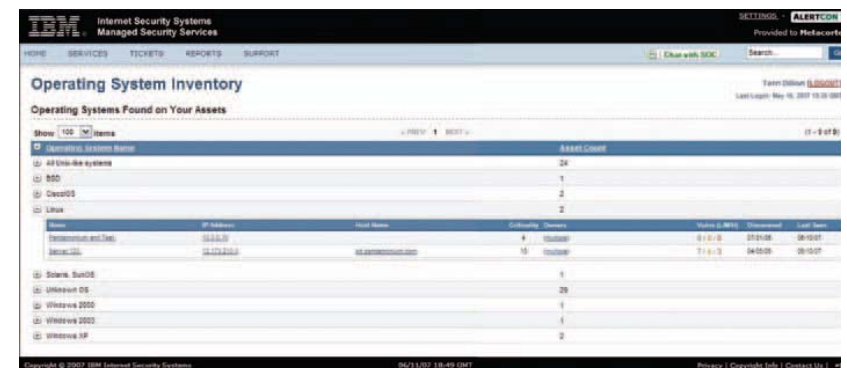


Confirmation des systèmes d'exploitation

La page Operating System Inventory indique le nombre de ressources tournant sous les différents systèmes d'exploitation répertoriés.

1. Cliquez sur **Services** ⇒ **Vulnerability Management** ⇒ **Operating System Inventory**.

2. Cliquez sur le signe « + » pour développer la liste et voir les caractéristiques des ressources tournant sous chacun des systèmes d'exploitation.



Confirmation des services

La page Service Inventory indique le nombre de ressources exécutant un service donné sur un port donné.

1. Cliquez sur **Services** ⇒ **Vulnerability Management** ⇒ **Service Inventory**.
2. Cliquez sur le signe « + » pour développer la liste et voir les caractéristiques des ressources exécutant chacun des services.



Procédures correctives

L'examen des vulnérabilités « ouvertes » est la première étape à effectuer pour identifier les problèmes nécessitant des mesures correctives. Les tickets de correction couvrent un ensemble logique de failles de sécurité et sont automatiquement assignés aux différents responsables des ressources concernées par ces tickets. Ils servent de base à la répartition des tâches entre les Subordinate Users (utilisateurs auxiliaires) et permettent de suivre l'avancement des actions de gestion des vulnérabilités.

1. Cliquez sur **Services** ⇒ **Vulnerability Management** ⇒ **Remediate Vulnerabilities**.
2. Cochez la case située en regard de la vulnérabilité à corriger.
3. Cliquez sur le bouton Remediate pour afficher la page **New Vulnerability Remediation Ticket**.



4. Entrez la date limite (**Due Date**).
5. Déterminez la **priorité** du ticket.
6. Indiquez dans le champ **Description** la cause de ce ticket et les éventuelles instructions à fournir à ceux à qui il est assigné.
7. Cliquez sur le bouton **Save Ticket**. La page **Ticket Details** apparaît.

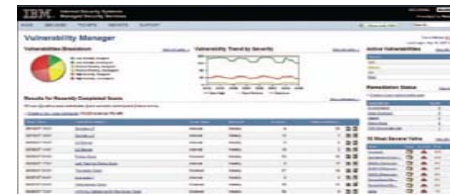


8. Entrez les informations à lire par les responsables des ressources avant de traiter les vulnérabilités listées.
9. Si vous le souhaitez, demandez un correctif virtuel en cliquant sur **Request a Virtual Patch Application** (facultatif - nécessite un agent de prévention des intrusions ISS).
10. Cliquez sur le bouton **Save Ticket**.
11. Cliquez sur le bouton **Remediate** pour afficher la page **New Vulnerability Remediation**.

Préférences utilisateurs

Après avoir défini les utilisateurs et leurs rôles, vous pouvez avoir besoin de consulter ou d'actualiser les préférences utilisateurs via le portail clients.

1. Cliquez sur le lien **Settings**, affiché en haut de toutes les pages du portail.



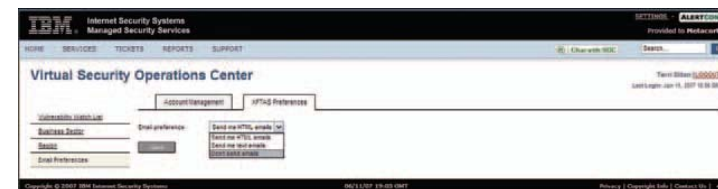
Sélectionnez Settings

2. Sélectionnez **My Profile** pour mettre à jour vos informations personnelles (numéros de téléphone, adresses e-mail, mots de passe, etc.).
3. Un administrateur (Security Admin) habilité peut activer le lien **Users** pour modifier ou actualiser les informations utilisateurs – paramètres e-mail pour les notifications quotidiennes d'évaluation des menaces, numéros de téléphone, adresses e-mail, mots de passe, etc.



Cliquez ici pour créer un utilisateur

4. Sélectionnez **Sites** pour modifier ou consulter les informations relatives aux emplacements physiques des équipements et des ressources.
5. Cliquez sur l'onglet **XFTAS Preferences** pour définir ou consulter vos préférences pour la notification des vulnérabilités dans le cadre du service XFTAS.



6. Cliquez sur le bouton **Save** pour valider les modifications éventuelles (réservé aux administrateurs habilités).

Remarque : Les administrateurs habilités peuvent créer des utilisateurs auxiliaires, les Subordinate Users, auxquels il est possible d'assigner des tickets VMS pour la correction des vulnérabilités. Les droits d'accès de ces utilisateurs se limitent à la consultation.

Copyright© 2007 IBM Internet Security Systems. Tous droits réservés dans le monde entier. Internet Security Systems et Proventia sont des marques d'IBM Internet Security Systems. Les autres marques ou dénominations peuvent appartenir à des tiers. Les caractéristiques et les contenus sont susceptibles d'être modifiés sans avertissement.
Diffusion : Générale : 0707