

leportail

By **xmco**

Module serenity

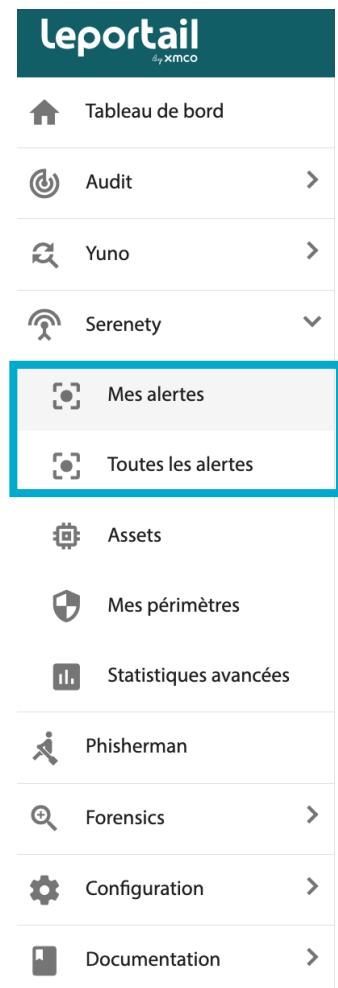
By xmco

Suivi de vos alertes de cybersurveillance

3

Consulter le plan d'action (1/2)

Le **plan d'action** vous permet d'accéder à l'ensemble des bulletins émis par le CERT-XMCO depuis le lancement de la cyber-surveillance Serenity.



Consulter le plan d'action (2/2)

Le **plan d'action** vous permet d'accéder à l'ensemble des bulletins émis par le CERT-XMCO depuis le lancement de la cyber-surveillance Serenety.

The screenshot shows the Serenety alert management interface. On the left, a sidebar lists various modules: Tableau de bord, Audit, Yuno, Serenety (selected), Mes alertes (highlighted), Toutes les alertes (highlighted), Assets, Mes périmètres, Statistiques avancées, Phisherman, Forensics, Configuration, and Documentation. The main area has two tabs: 'Définitions des filtres de sélection' (left) and 'Gestion des filtres (sélection, application, réinitialisation)' (right). The left tab shows a filter configuration with 'Intégrer les plans d'action de:' dropdown set to 'Ouvert' (checked), and a search bar with 'Sélectionner un opérateur' set to 'égal à' and 'Tracker' set to 'Alertes Serenety, Infos Se...'. The right tab shows a toolbar with icons for 'Ajouter un filtre', search, clear, export, edit, and settings. Below these tabs is a table listing 10 alerts, each with columns for PDF icon, ticket number, criticality (color bar), title, status, impact, assigned to, and publication date. Arrows point from the sidebar's 'Mes alertes' and 'Toutes les alertes' buttons to the respective tabs in the main interface.

	Export PDF	Référence	Criticité	Périmètre	Titre	Statut	Impact	Assigné à	Publication
<input type="checkbox"/>		578745		Serenety USA	A publicly available Trello project related to XMDEMO discloses business-related information	Nouveau	0	Demo MANAGER	22/09/21
<input type="checkbox"/>		578744		Serenety USA	Data linked to XMDEMO have leaked during Umanis' compromise on November 14, 2020	Nouveau	0	Demo MANAGER	22/09/21
<input type="checkbox"/>		578743		Serenety Groupe	Scope evolution (February 2021)	Nouveau	0	Demo MANAGER	22/09/21
<input type="checkbox"/>		578742		Serenety Groupe	4 accounts related to XMDEMO have been identified in the Cit0day collection	Nouveau	0	Demo MANAGER	22/09/21
<input type="checkbox"/>		578741		Serenety France	Annonce d'une vulnérabilité critique affectant les équipements Pulse Connect Secure : 1 serveur affecté	Nouveau	3	Demo MANAGER	22/09/21
<input type="checkbox"/>		578740		Serenety France	Analyse de la vulnérabilité critique référencée CVE-2020-5135 affectant SonicWall	Nouveau	0	Demo MANAGER	22/09/21
<input type="checkbox"/>		578739		Serenety France	A project containing log files and private keys belonging to XMDEMO have been identified on Github	Nouveau	0	Demo MANAGER	22/09/21
<input type="checkbox"/>		578738		Serenety Groupe	A new domain related to XMDEMO has been identified : xnndemo.ru	Nouveau	0	Demo MANAGER	22/09/21
<input type="checkbox"/>		578737		Serenety USA	A TriplePlay administrative interface with default credentials has been identified on admin.tripleplay.fr (1.1.1)	Nouveau	0	Demo MANAGER	22/09/21



Différents **trackers** sont disponibles pour catégoriser les différents types de tickets d'actions proposés au travers de Serenety (en particulier **Alertes** et **Info**)

Création / sélection d'une **Vue filtrée**

Modification multiples des tickets d'actions, **Export (XLS)**, et **Personnalisation de l'affichage**

Traiter un ticket d'action Serenity (1/4)

Serenity > Serenity - DEMO

Plan d'actions Technologie(s) déployée(s) Composant(s) technique(s) Statistiques Utilisateur(s) Détails Préférences de Veille Fichiers

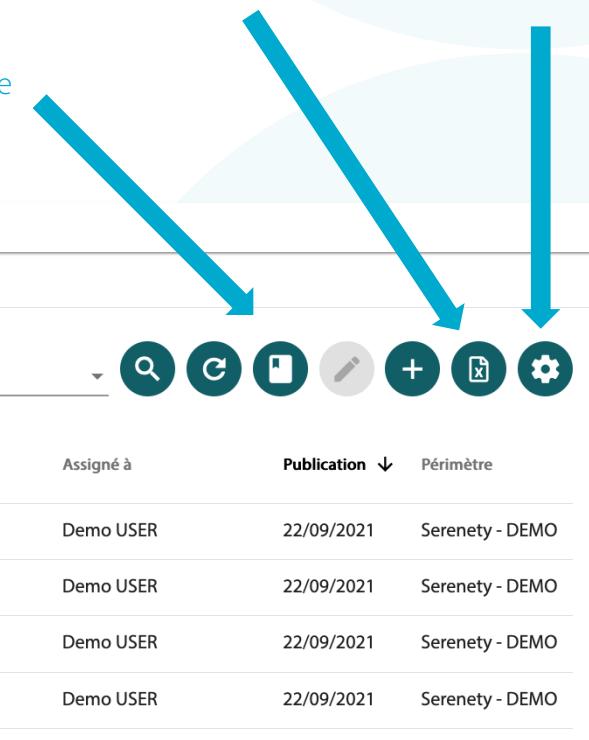
Intégrer les plans d'action de : Serenity - DEMO Sélectionner un opérateur Tracker Alertes Serenity, Infos Se... Ajouter un filtre

<input type="checkbox"/> Export PDF	Référence	Criticité	Titre	Statut	Assigné à	Publication	Périmètre
<input type="checkbox"/>	PDF 578749	●●●	Trois domaines contenant le nom XXXX ont été identifiés	Nouveau	Demo USER	22/09/2021	Serenity - DEMO
<input type="checkbox"/>	PDF 578748	●●●	Une interface d'administration vulnérable PHPMyAdmin a été identifiée sur le site X.X.X (*cdn.com)	Nouveau	Demo USER	22/09/2021	Serenity - DEMO
<input type="checkbox"/>	PDF 578747	●●●	Une interface d'administration vulnérable Oracle Weblogic a été identifiée sur le site X.X.X (*cdn.com)	En cours	Demo USER	22/09/2021	Serenity - DEMO
<input type="checkbox"/>	PDF 578746	●●●	Un code source contenant des informations sensibles a été publié par un collaborateur d'Assises sur GitHub	Nouveau	Demo USER	22/09/2021	Serenity - DEMO

Recherche sauvegardée

Export XLS

Personnalisation du tableau



Étape 1
Cliquez sur le ticket d'action à modifier

Vous pouvez modifier éditer chacun des tickets d'action Serenity afin d'adapter leur niveau de criticité et de faciliter leur traitement dans votre contexte spécifique.

Une fois le bulletin marqué comme étant résolu, un consultant du CERT-XMCO vérifiera l'application des recommandations et, le cas échéant le clôturera.



Traiter un ticket d'action Serenety (2/4)

☰ ← | [21_02_DEMO] Serenety - DEMO > Alert 578749

Trois domaines contenant le nom XXXX ont été identifiés

Date de publication : 22/09/2021

Criticité :

Statut : Nouveau

Assigné : USER Demo

Périmètre : Périmètre passif

Catégorie : DNS

Composants techniques : Aucun

Impact : 0

Échéance : Aucune

Observateurs : Aucun

Identification : Automatique

Sous-catégorie : Exposition - Interface d'administration (technique)

Placeholder

Historique et Commentaire(s) 1

Mis à jour par Demo MANAGER le 18/11/2021 à 10:16:02

• Assigné : Demo MANAGER -> Demo USER

PDF Exporter

Éditer

Étape 2
Cliquez sur Éditer

Historique des actions réalisées

Traiter un ticket d'action Serenety (3/4)

☰ ← | [21_02_DEMO] Serenety - DEMO > Alerte 578749

Titre
Trois domaines contenant le nom XXXX ont été identifiés

Placeholder

Commentaire

Étape 3
Ajoutez un commentaire dans la zone prévue à cet effet, sous la description du bulletin.
Ajoutez des images, utilisez les styles disponibles, ...

PDF Exporter Visualiser

☰ ↗

Dépôt de fichier activé

Étape 4
Cliquez sur la Disquette pour enregistrer



Vous pouvez modifier la criticité d'un bulletin, son statut, définir une échéance à laquelle il devra être traité, l'assigner au bon interlocuteur et éventuellement définir des observateurs, spécifier le système étant impacté, ou encore préciser si ce ticket d'action vous intéresse ou non dans le cadre de l'activité de votre équipe.

Traiter un ticket d'action Serenity (4/4)

The screenshot shows the 'Traitement d'un ticket d'action Serenity' (Treatment of a Serenity action ticket) interface. It includes fields for assignee ('MANAGER Demo'), due date, status ('Nouveau'), criticality ('Faible'), category ('Exposition'), and sub-category ('Exposition - Nouvelles menaces'). It also shows observers ('Observateurs') and a perimeter ('Périmètre Serenity France'). A large blue arrow points from the status/criticality section towards the bottom right, indicating the path to save changes.

Assigné: MANAGER Demo

Échéance:

Statut: Nouveau

Criticité: Faible

Catégorie: Exposition

Sous-catégorie: Exposition - Nouvelles menaces

Observateurs:

Périmètre: Serenity France

Type de périmètre: Périmètre actif

OK **Annuler**

Étape 4
Cliquez sur la Pile

Étape 7
Cliquez sur la Disquette pour enregistrer

Étape 5
Mettez à jour les éléments de suivis (statut, criticité, assignation, ...) et assignez le bulletin au CERT-XMCO ou à un collègue responsable du traitement du ticket.

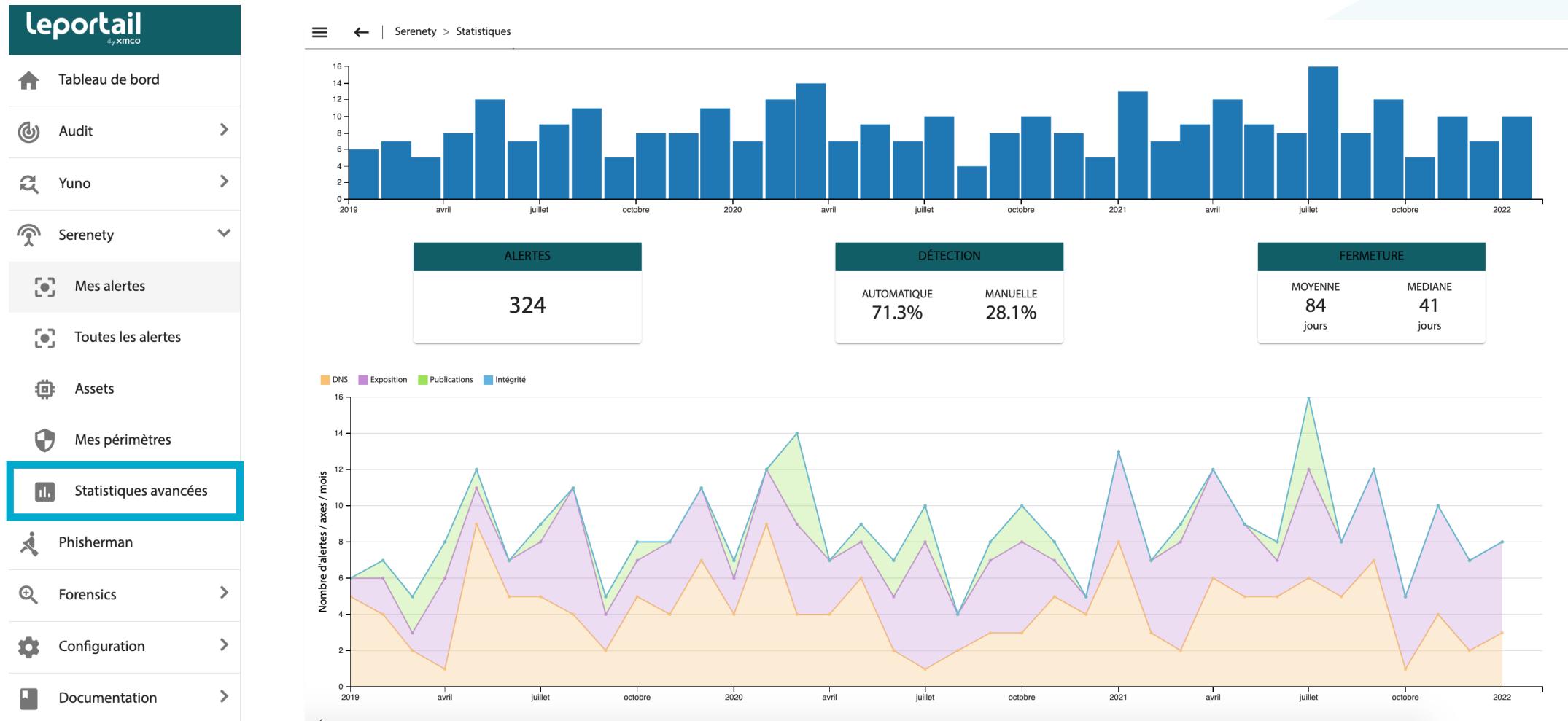
Étape 6
Validez les modifications et enregistrez les via le bouton de mise à jour (disquette).



Vous pouvez modifier la criticité d'un bulletin, son statut, définir une échéance à laquelle il devra être traité, l'assigner au bon interlocuteur et éventuellement définir des observateurs, spécifier le système étant impacté, ou encore préciser si ce ticket d'action vous intéresse ou non dans le cadre de l'activité de votre équipe.

Consulter les statistiques

La page des **statistiques** vous permet d'obtenir des informations et indicateurs sur les bulletins reçus depuis le lancement du service



Consulter la liste des assets surveillés

La [page des assets](#) vous permet de connaître précisément les éléments de votre périmètre surveillés par Serenity.

The screenshot displays the Le Portail interface, specifically the 'Assets' section. On the left, a sidebar lists various modules: Tableau de bord, Audit, Yuno, Serenity (with a dropdown arrow), Mes alertes, Toutes les alertes, Assets (highlighted with a blue border), Mes périmètres, Statistiques avancées, Phisherman, Forensics, Configuration, and Documentation. The main content area is titled 'Inventaire des assets' and contains the following information:

- Filtres de recherche:** Shows counts for DNS (171), IP (62), and Mot-clé(s) (48).
- Search and Sort:** Includes a 'Recherche' input, a 'Type' dropdown, a 'Trier par' dropdown, and an 'Appliquer' button.
- Asset List:** A table with 7 rows, each representing an asset entry. The columns include:
 - Type: Mot-clé(s)
 - Type: Mot-clé(s)
 - 163. [REDACTED]
 - 163. [REDACTED]
 - 163. [REDACTED]
 - 163. [REDACTED]
 - 163. [REDACTED]Dates in the table indicate last modification times: 03/02/2022, 03/02/2022, 08/02/2022, 03/02/2022, 07/02/2022, 07/02/2022, and 07/02/2022. Each row has a refresh icon.

xmco

We deliver cybersecurity expertise