

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 Serenety.


leportail


by xmco


 Tableau de bord


 Audit >


 Yuno >


 Serenety v


 Mes alertes


 Toutes les alertes


 Assets


 Mes périmètres


 Statistiques avancées


 Phisherman

 Forensics >

 Configuration >

 Documentation >

 Cliquez sur **Mes Alertes** pour accéder aux **bulletins qui me sont assignés**

 Cliquez sur **Toutes les alertes** pour accéder à **tous les bulletins publiés**

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.

- 2 vues préfiltrées sont proposées :
- **Mes alertes** : limitées aux alertes qui vont sont assignées
 - **Toutes les alertes**

Tableau de bord

Audit

Yuno

Serenety

Mes alertes

Toutes les alertes

Assets

Mes périmètres

Statistiques avancées

Phisherman

Forensics

Configuration

Documentation

Serenety > Mes alertes

Intégrer les plans d'action de : ☐ Ouvert ☒

Sélectionner un opérateur

Tracker

☒ égal à

Alertes Serenety, Infos Se...

<input type="checkbox"/>	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 MANA...	22/09/2021
<input type="checkbox"/>		578744		Serenety USA	Data linked to XMDEMO have leaked during Umanis' compromise on November 14, 2020	Nouveau	0	Demo MANA...	22/09/2021
<input type="checkbox"/>		578743		Serenety Groupe	Scope evolution (February 2021)	Nouveau	0	Demo MANA...	22/09/2021
<input type="checkbox"/>		578742		Serenety Groupe	4 accounts related to XMDEMO have been identified in the Cit0day collection	Nouveau	0	Demo MANA...	22/09/2021
<input type="checkbox"/>		578741		Serenety France	Annonce d'une vulnérabilité critique affectant les équipements Pulse Connect Secure : 1 serveur affecté	Nouveau	3	Demo MANA...	22/09/2021
<input type="checkbox"/>		578740		Serenety France	Analyse de la vulnérabilité critique référencée CVE-2020-5135 affectant SonicWall	Nouveau	0	Demo MANA...	22/09/2021
<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 MANA...	22/09/2021
<input type="checkbox"/>		578738		Serenety Groupe	A new domain related to XMDEMO has been identified : xnndemo.ru	Nouveau	0	Demo MANA...	22/09/2021
<input type="checkbox"/>		578737		Serenety USA	A TriplePlay administrative interface with default credentials has been identified on admin.tripleplay.fr (1.1.1.1)	Nouveau	0	Demo MANA...	22/09/2021

Définitions des filtres de sélection

Gestion des filtres (sélection, application, réinitialisation)



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)

Export XLS

Personnalisation du tableau

Recherche sauvegardée

Menu

←

Serenety > 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

égal à

Tracker

Alertes Serenity, Infos Se...

Ajouter un filtre

Recherche

Actualiser

Export PDF

Personnalisation

Plus

Tableau

Paramètres

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

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 > Alerte 578749

Trois domaines contenant le nom XXXX ont été identifiés

PDF Exporter

Éditer

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

← **Étape 2**
Cliquez sur **Editer**

← **Historique** des actions réalisés

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

☰

←

[21_02_DEMO] Serenity - DEMO > Alerte 578749

PDF Exporter

Visualiser

Titre

Trois domaines contenant le nom XXXX ont été identifiés

Placeholder

Commentaire

↺ ↻ B I H “ </> 🔗 🖼️ | ☰ ☷ − 📊 | 🖼️ 📄 ✂️ 👁️

Étape 3

Ajoutez un commentaire dans la zone prévue à cet effet, sous la description du bulletin.

Ajoutez des images, utilisez les styles disponibles, ...

Dépôt de fichier activé



Étape 4
Cliquez sur la **Disquette** pour enregistrer

i

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 Serenety (4/4)

PDF Exporter

Visualiser

PDF Exporter

Visualiser

Périmètre

Serenety France

X

Assigné

MANAGER Demo

X

Échéance

Statut

Nouveau

En cours

Résolu

Risque accepté

Criticité

Faible

Moyenne

Élevée

Urgent

Catégorie

DNS

Exposition

Publications

Intégrité

Sous-catégorie

Exposition - Interface d'administration (LMS)

Exposition - Ports ouverts

Exposition - Certificats TLS

Exposition - Version obsolète

Exposition - Nouvelles menaces

Composant(s) Technique(s)

vpn1.xmdemo.fr

Observateurs

Identification

Manuel

Automatique

Type de périmètre

Périmètre actif

Périmètre passif

Hors périmètre

Ceci ne m'intéresse pas

OK

Annuler

Étape 4

Cliquez sur la Pile

Étape 7

Cliquez sur la Disquette pour enregistrer

Étape 5

Mettez à jours 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).

i

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

leportail

by xmc

🏠

Tableau de bord

🔍

Audit

>

🔄

Yuno

>

📶

Serenity

▼

📶

Mes alertes

📶

Toutes les alertes

⚙️

Assets

🛡️

Mes périmètres

📊

Statistiques avancées

👤

Phisherman

🔍

Forensics

>

⚙️

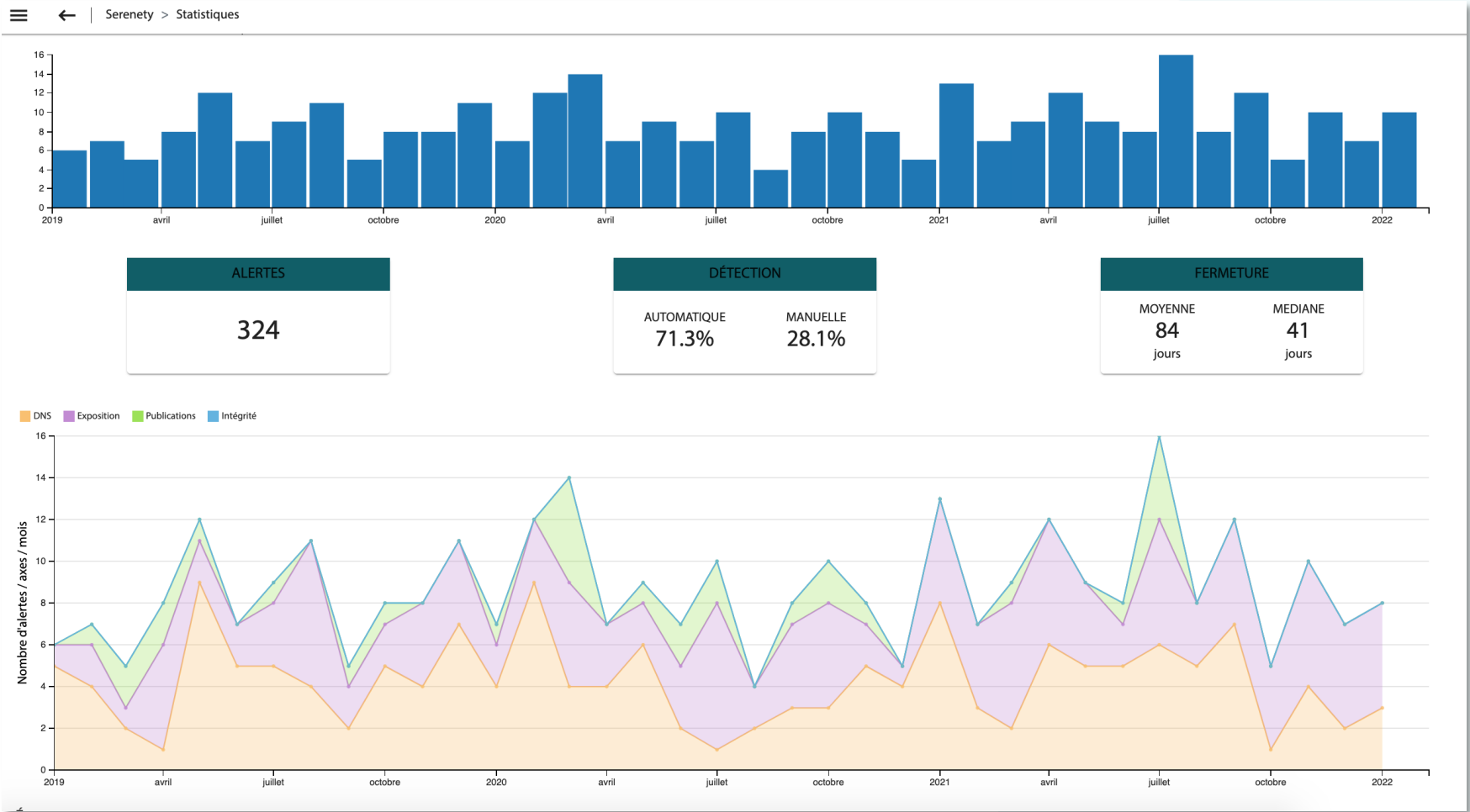
Configuration

>

📖

Documentation

>



Consulter la liste des assets surveillés

La **page des assets** vous permet de connaître précisément les éléments de votre périmètre surveillés par Serenety.

leportail

Tableau de bord

Audit

Yuno

Serenety

Mes alertes

Toutes les alertes

Assets

Mes périmètres

Statistiques avancées

Phisherman

Forensics

Configuration

Documentation

Serenety > Liste des assets

Inventaire des assets

Cette page liste l'ensemble des assets surveillés par Serenety.

DNS
171

IP
62

Mot-clé(s)
48

Recherche

Type

Trier par

Appliquer

Type : Mot-clé(s)	Dernière modification : 03/02/2022
Type : Mot-clé(s)	Dernière modification : 03/02/2022
163.1	Dernière modification : 08/02/2022
Type : IPV4	
163.	Dernière modification : 03/02/2022
Type : IPV4	
163.	Dernière modification : 07/02/2022
Type : IPV4	
163.	Dernière modification : 07/02/2022
Type : IPV4	
163.	Dernière modification : 07/02/2022
Type : IPV4	

1-25 sur 282

xmco

We deliver cybersecurity expertise