beyondsecurity
by HelpSystems

beyondsecurity
beSECURE

Guide d'utilisation

beyondsecurity
by HelpSystems

Table des matières

Note : Ce guide complet de la plateforme beSECURE en français est basé sur la version anglaise du même guide. Les mots ont été traduits en prenant en compte le contexte, cependant certains mots que vous trouverez en français dans ce guide n'ont pas encore tous été traduits sur la plateforme, ce qui ne saurait tarder. Il s'agit d'une petite partie, néanmoins cela mérite d'être mentionné. Si vous avez la moindre question, n'hésitez pas à contacter le support à l'adresse email suivante : support@beyondsecurity.com

1. Introduction

Le logiciel beSECURE de Beyond Security effectue une cartographie de la sécurité du réseau d'une organisation et simule les attaques provenant d'un réseau interne ou externe. Une fois la cartographie de sécurité terminée, beSECURE génère un rapport détaillé des vulnérabilités qui énumère les failles de sécurité, ainsi que des solutions pratiques et faciles à appliquer pour y remédier. beSECURE est régulièrement mis à jour pour tenir compte des vulnérabilités de sécurité les plus récentes découvertes par l'équipe de R&D de Beyond Security et d'autres organisations.

Les clients qui mettent en œuvre ce service obtiendront une vue en temps réel de l'ensemble de la topographie de sécurité de leur réseau et démontreront leur conformité aux normes de sécurité informatique mondiales émergentes et à la législation sur l'intégrité.

2. Support Technique

L'équipe support de Beyond Security peut répondre aux questions relatives à beSECURE.
Retrouvez les détails ci-dessous :

Téléphone PCI

L'assistance technique est disponible de 7h00 à 17h00 PST du lundi au

vendredi. Par téléphone : 1-800-801-2821 (numéro gratuit aux États-Unis) ou

+972-9-8656850 (en dehors des États-Unis).

3. Accès à la plateforme beSECURE

Pour vous connecter à la plateforme, lancer votre navigateur web et accéder à l’adresse appropriée en fonction de votre location géographique : ·

Serveur américain : https://cloud2.beyondsecurity.com

Serveur européen : https://cloud3.beyondsecurity.com

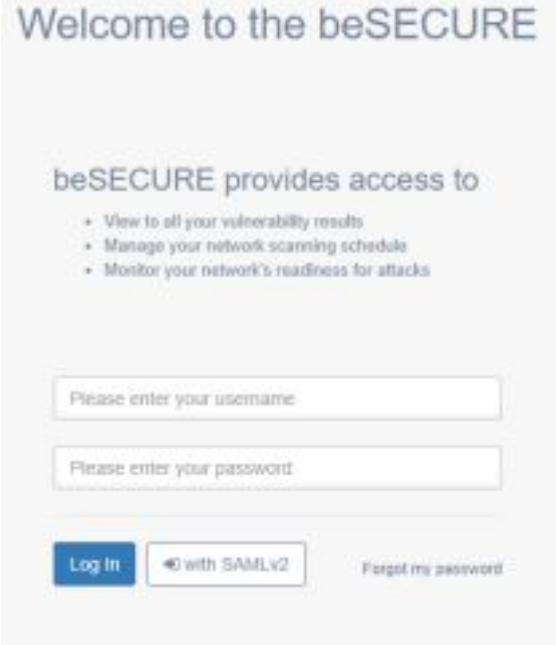
Si vous ne savez pas quelle adresse utiliser, envoyez-nous un courriel à support@beyondsecurity.com ou contactez votre gestionnaire de compte pour obtenir des informations de connexion.

La page d'accueil/de connexion apparaît lorsque :

· L'utilisateur souhaite entrer dans le système pour la première fois

· L'utilisateur s'est déconnecté

· 30 minutes d'inactivité se sont écoulées



Page d'accueil/Login.

Pour se connecter au système beSECURE :

1. Entrez votre nom d'utilisateur et votre mot de passe. (Vous devez avoir reçu ces informations d'un

administrateur système).

2. Cliquez sur Connexion.

Le processus de connexion échoue lorsqu'un utilisateur saisit des informations d'identification incorrecte ou tente d'accéder à un compte désactivé. Lorsque le nom d'utilisateur ou le mot de passe est incorrect, une bannière rouge avec le message "La combinaison nom d'utilisateur/mot de passe fournie est incorrecte" apparaît en haut de la page.

Si le nombre de tentatives de connexion échouées dépasse la limite, le processus de connexion sera désactivé pendant 30 minutes. Par défaut, beSECURE bloque l'accès d'un utilisateur après trois tentatives de connexion infructueuses. Pour plus d'informations sur la modification de ce nombre, voir la section Création d'un profil de sécurité du présent document.

4. Déconnexion

Pour terminer votre session sur la plateforme beSECURE, cliquez sur le nom d'utilisateur en haut à droite de l'écran, puis sur “Déconnexion”. Vous serez alors redirigé vers la page d'accueil.

5. Page d’accueil

La page d'accueil de beSECURE fournit un aperçu des résultats de scan par le biais d'une interface de type “tableau de bord”. Pour accéder à la page d'accueil depuis n'importe quel endroit du système beSECURE, cliquez sur l'élément de menu Accueil ou sur l'icône beSECURE dans la barre latérale.

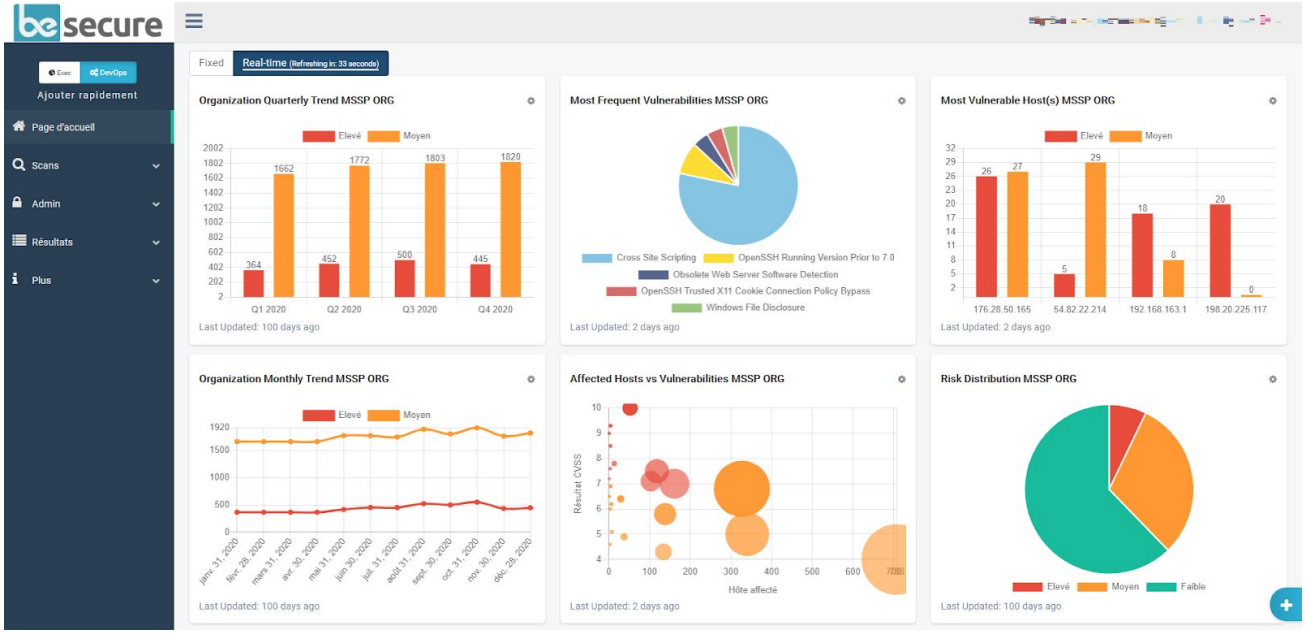
Par défaut, la page d'accueil affiche les informations suivantes :

Hôte(s) le(s) plus vulnérable(s) par organisation	Les hôtes les plus vulnérables pour l'organisation, l'administrateur ou l'entité sélectionnée.
Scans à venir	Des scans programmés pour l'organisation, l'administration ou le lieu sélectionné. Cette section n'apparaît que si les données sont disponibles.
Le type de vulnérabilité le plus fréquent	Le type de vulnérabilité le plus fréquent pour l'organisation, l'administration ou le lieu sélectionné. Les valeurs sont les serveurs web, le cryptage et l'authentification, les applications web, les serveurs SQL et les backports.
Exécution de scans Web	Tout scan d'une page Web en cours pour l'organisation, l'administrateur ou l'entité sélectionnée.
Exécution des scans	Tout scan en cours pour l'organisation, l'administration ou l'entité sélectionnée.
Organisations les plus vulnérables par risque	Les organisations les plus vulnérables par risque. Choisissez parmi toutes les organisations, administrations et les entités.

Organisations les plus vulnérables par score	Les organisations les plus vulnérables par score. Choisissez parmi toutes les organisations, administrations et les

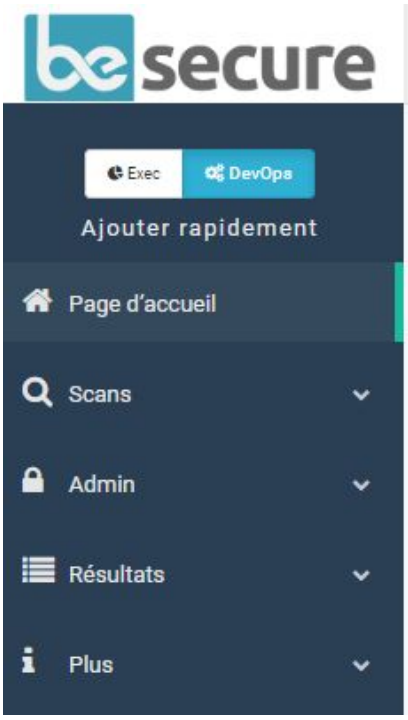
	entités/lieu.
Les vulnérabilités les plus fréquentes	Les vulnérabilités les plus fréquentes pour l'organisation, l'administrateur ou l'entité/lieu sélectionnée.

Vous pouvez modifier les informations affichées dans un rapport en sélectionnant une option différente dans la liste déroulante. Pour supprimer le rapport de la page d'accueil, cliquez sur le X en haut à droite du rapport.



6. Modes

Le système beSECURE regroupe les fonctionnalités du système en deux modes : Le mode exécutif **(Exec) et le mode DevOps**. Le mode exécutif permet d'accéder aux résultats de scans et aux rapports. Il est conçu pour les gestionnaires et autres décideurs. Il s'agit du mode par défaut.



Le mode **DevOps** fournit un accès supplémentaire aux fonctions administratives, telles que la gestion des scans, des comptes d'utilisateurs. Il est conçu pour les gestionnaires du système beSECURE.

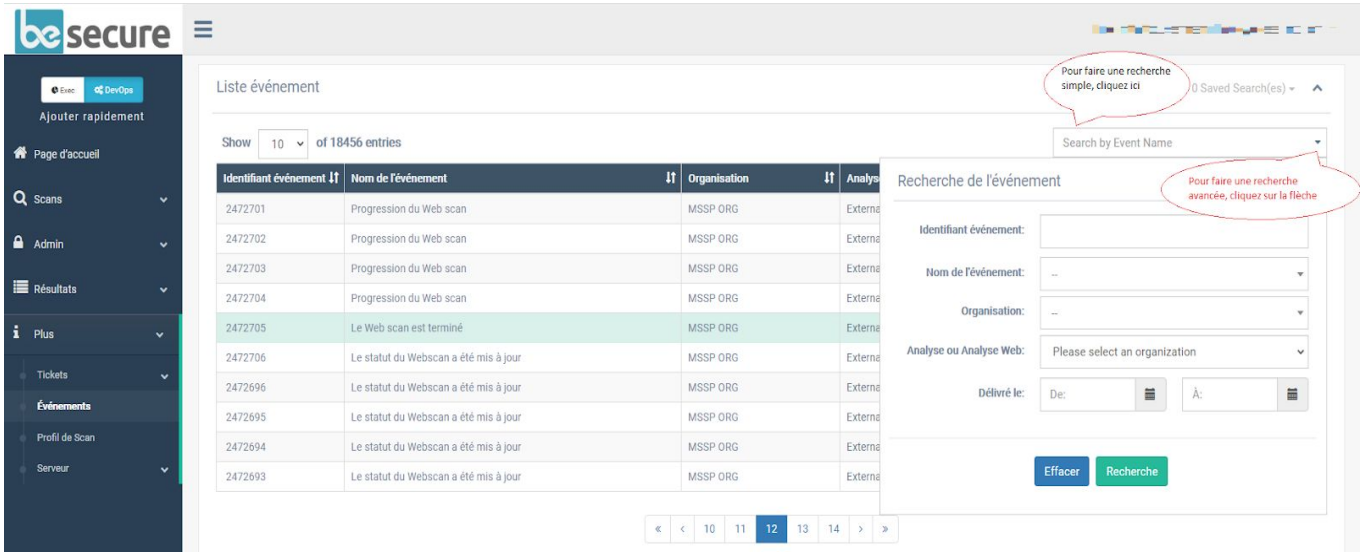
Les utilisateurs ayant un accès complet au mode DevOps peuvent passer d'un mode à l'autre en utilisant le bouton de basculement de mode qui apparaît en haut de la barre latérale.

7. Voir les évènements de la plateforme

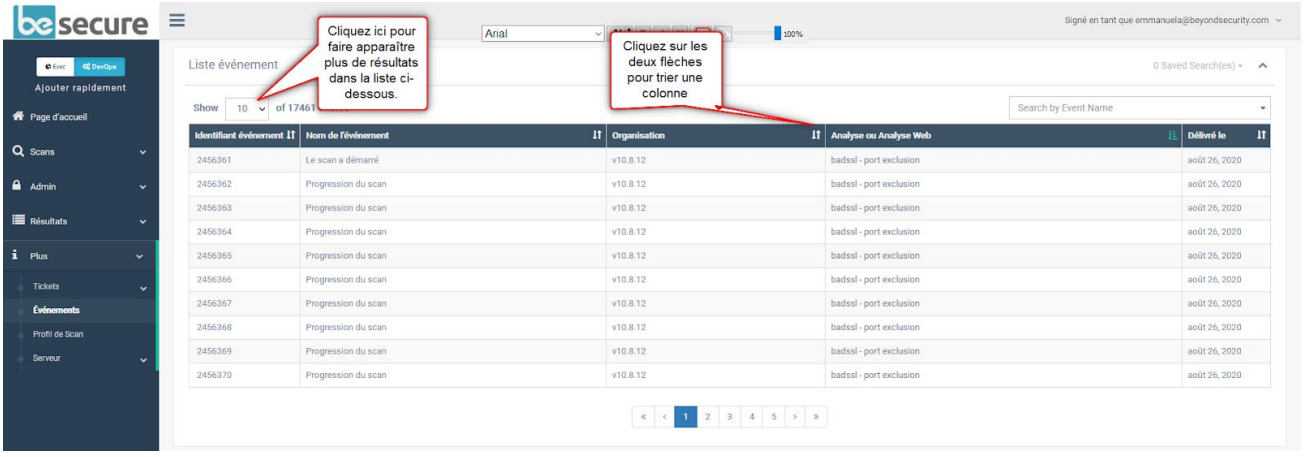
Les événements sont des actions qu'une entité spécifique de réglage du scan a prise. Par exemple, les événements peuvent inclure "scan terminé", "scan commencé", "scan a manqué son horaire" et des actions similaires.

Pour voir les évènements, cliquez sur **Plus › Evènements** dans le menu.

Vous pouvez rechercher un événement spécifique en utilisant le champ de recherche de la page Événements. Par défaut, la recherche s'effectuera dans le champ "Nom de l'événement". Cliquez sur la flèche vers le bas à l'intérieur de la boîte de recherche pour accéder aux options de recherche avancée telles que les champs ID de l'événement, Organisation, Scan ou Web Scan et Date d'émission.

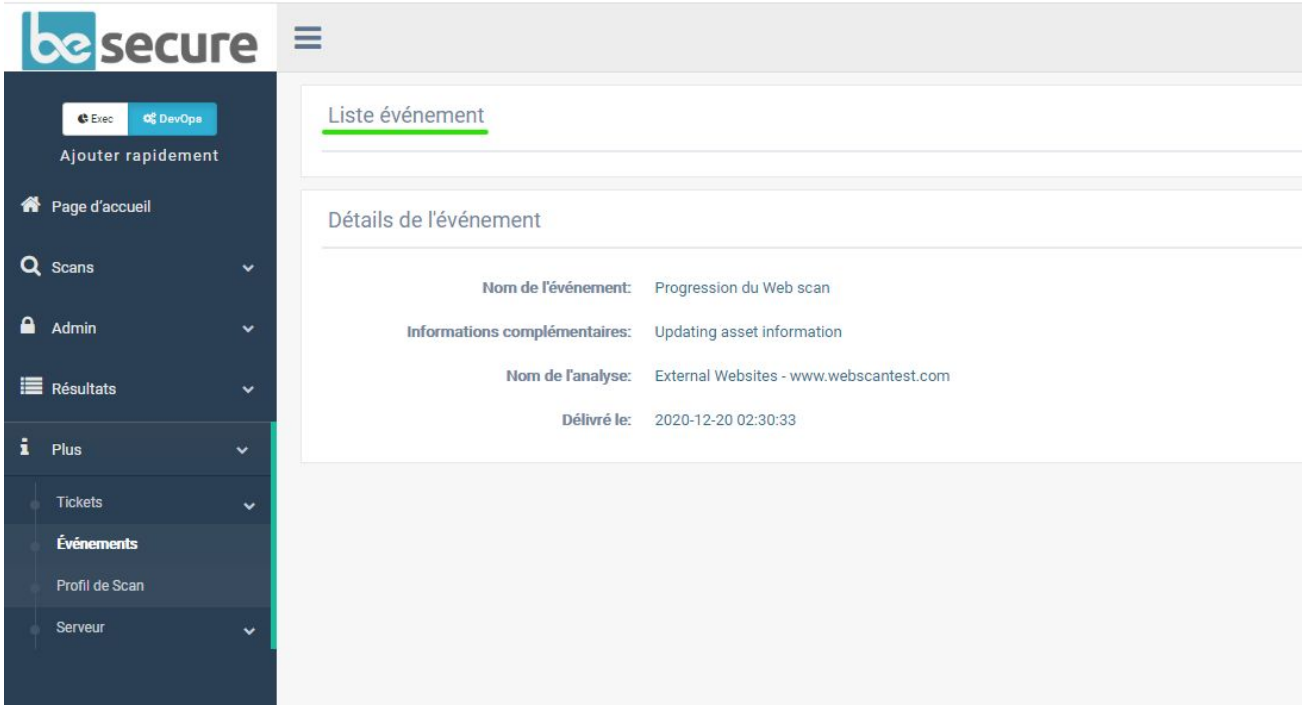


Utilisez la liste déroulante au-dessus des résultats de la recherche pour modifier le nombre de résultats affichés. Vous pouvez également utiliser les flèches dans les en-têtes de colonne pour trier les données. Pour trier par nom d'événement, par exemple, cliquez sur l'icône en forme de flèche dans l'en-tête de cette colonne. Sa couleur passera au vert pour indiquer que les données sont triés sur cette colonne. La séquence verticale de lignes qui apparaît à côté de la flèche verte indique s'il s'agit d'un tri ascendant ou descendant. Pour changer la direction du tri de ascendant à descendant ou vice versa, cliquez sur cette icône. Utilisez les boutons qui apparaissent sous le tableau résultant pour parcourir les résultats de la recherche.



La page Liste des événements.

Cliquez sur un événement pour en voir les détails. La page Détails de l'événement affiche le nom de l'événement, les informations complémentaires (le cas échéant), le nom du scan et la date d'émission.



La page Liste des événements.

Dans l'exemple ci-dessus, le scan s'est terminé le 20 décembre 2020 à 2h30.

8. Système de recherches et Résultats

Les recherches et les résultats sont à la disposition de tous les utilisateurs du système beSECURE. Pour accéder aux recherches et aux résultats, cliquez sur Résultats dans la barre latérale.

8.1. Résumé des résultats

Les résultats synthétisés de beSECURE fournissent des informations de base agrégées sur les vulnérabilités découvertes lors d'une analyse (lors d'un scan). Les rapports indiquent le ou les hôtes, la date d'analyse, le nombre total de vulnérabilités trouvées, le nombre de vulnérabilités à haut risque et à risque moyen, un score global et un indicateur de tendance de la vulnérabilité

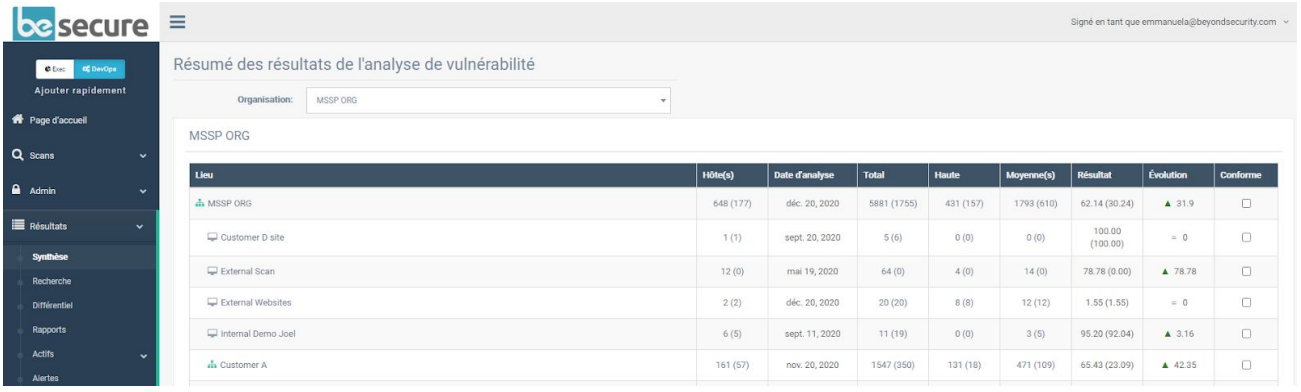
pour chaque emplacement associé au sein de l'organisation.

Pour accéder au résumé des résultats :

1. Connectez-vous au système beSECURE.

2. Cliquez sur Résultats=>Synthèse. La page des résultats du résumé de l'analyse de vulnérabilité s'affiche.

3. Sélectionnez une organisation dans la liste déroulante en haut de la page. Le résumé des résultats pour l'organisation apparaîtra



La page des résultats synthétisée de l'analyse de vulnérabilité.

Cette page affiche une hiérarchie qui montre la structure de l'organisation sélectionnée, ainsi que les informations de vulnérabilité accumulées pour chaque entité.

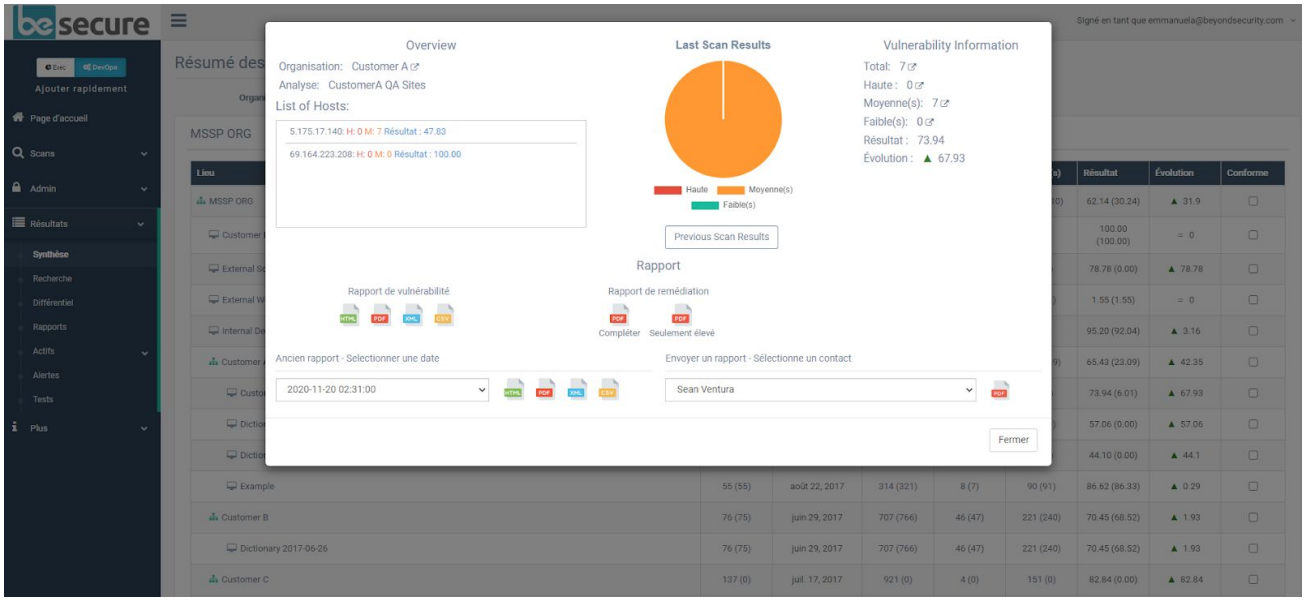
Le résumé montre jusqu'à deux niveaux de la hiérarchie d'une organisation. Le niveau supérieur est l'organisation elle-même (indiquée par une icône verte dans la première colonne de l'organigramme). Les sous-organisations apparaissent en dessous de l'organisation. Ils sont indiqués par une icône de scan (icône d'un ordinateur).

La page affiche les informations suivantes :

Location	La place dans la hiérarchie de l'organisation
Hôte(s)	Le nombre d'hôtes scannés, avec le nombre d'hôtes du scan précédent entre parenthèses. En cliquant sur la première valeur de cette rubrique, vous ouvrirez la page des résultats détaillés de l'analyse de vulnérabilité.
Date d'analyse	La date du dernier scan.
Total	Le nombre total de vulnérabilités trouvées. Le nombre entier entre parenthèses est le nombre de vulnérabilités trouvé lors de l'analyse précédente.
Haute	Le nombre de vulnérabilités à haut risque trouvé. Le nombre entre parenthèses est le nombre de vulnérabilités trouvées lors de l'analyse précédente.
Moyenne(s)	Le nombre de vulnérabilités à risque moyen trouvé. Le nombre entre parenthèses est le nombre de vulnérabilités trouvées lors de l'analyse précédente.

Résultats	Le résultat actuel de l'entité/lieu sur une échelle de 0 à 100, 100 représentant le meilleur score possible et donc un réseau hautement sécurisé. Le chiffre entre parenthèses est le score de l'analyse précédente.
Evolution	Indique si la cible devient plus ou moins sécurisée (après remédiations éventuelles), sur la base d'une comparaison des scores des scans actuels et précédents. Une amélioration du score due à la diminution des vulnérabilités est indiquée par une flèche verte orientée vers le haut. Une baisse du score due à une augmentation des vulnérabilités est indiquée par une flèche rouge, orientée vers le bas. Un score stable est indiqué par un cercle jaune.

En cliquant sur une valeur dans la colonne “Lieu”, la fenêtre “Actions” s'ouvre, donnant accès à des informations et options supplémentaires pour le lieu sélectionné.

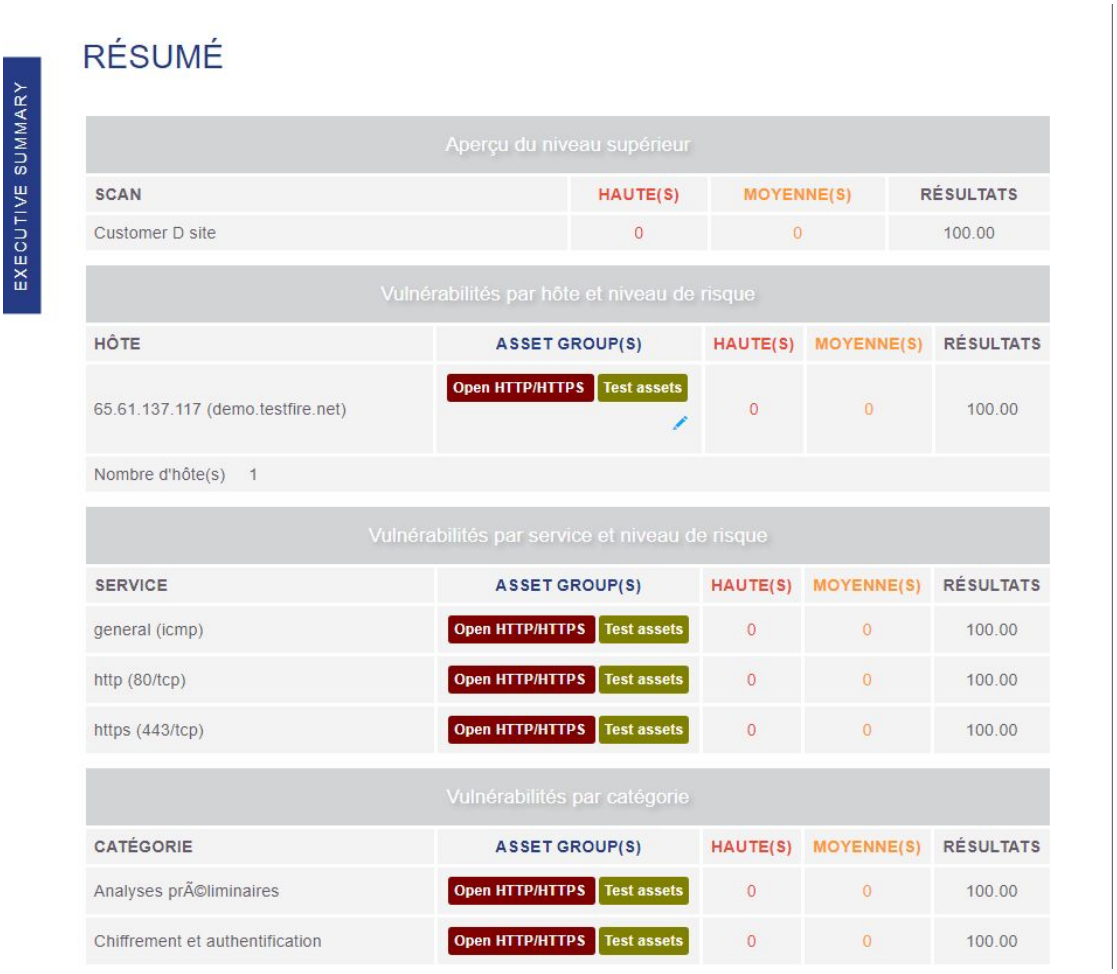


La fenêtre Actions.

La section “Informations générales” de la fenêtre “Actions” affiche l'Organisation, le scan, une liste des hôtes scannés et le score de chaque hôte. Par défaut, la fenêtre “Actions” affiche les informations pour le premier hôte de la liste. Pour modifier les données affichées dans la fenêtre, cliquez sur un autre hôte.

La section “Résultat de la dernière analyse” contient un graphique circulaire qui visualise les proportions de vulnérabilités à risque élevé, moyen et faible pour l'analyse la plus récente de cet emplacement. Vous pouvez comparer le graphique avec les résultats de l'analyse précédente en cliquant sur le bouton “Résultat précédent”. La section “Informations sur les vulnérabilités” affiche les mêmes chiffres que ceux qui figurent sur la page de “Résultats de l'analyse de vulnérabilité”.

La section “Rapport” permet d'accéder aux rapports de vulnérabilité et aux rapports de mesures correctives téléchargeables. Les rapports de vulnérabilité fournissent des détails sur les vulnérabilités trouvées au cours d'une analyse. En plus des chiffres bruts affichés dans la section “Résultats=> synthèse” du système beSECURE, les rapports contiennent également un contexte supplémentaire, des informations explicatives et des solutions possibles.



EXECUTIVE SUMMARY

RÉSUMÉ

Aperçu du niveau supérieur			
SCAN	HAUTE(S)	MOYENNE(S)	RÉSULTATS
Customer D site	0	0	100.00

Vulnérabilités par hôte et niveau de risque				
HÔTE	ASSET GROUP(S)	HAUTE(S)	MOYENNE(S)	RÉSULTATS
65.61.137.117 (demo.testfire.net)	Open HTTP/HTTPS Test assets	0	0	100.00
Nombre d'hôte(s) 1				

Vulnérabilités par service et niveau de risque				
SERVICE	ASSET GROUP(S)	HAUTE(S)	MOYENNE(S)	RÉSULTATS
general (icmp)	Open HTTP/HTTPS Test assets	0	0	100.00
http (80/tcp)	Open HTTP/HTTPS Test assets	0	0	100.00
https (443/tcp)	Open HTTP/HTTPS Test assets	0	0	100.00

Vulnérabilités par catégorie				
CATÉGORIE	ASSET GROUP(S)	HAUTE(S)	MOYENNE(S)	RÉSULTATS
Analyses prÃ©liminaires	Open HTTP/HTTPS Test assets	0	0	100.00
Chiffrement et authentification	Open HTTP/HTTPS Test assets	0	0	100.00

Un rapport sur la vulnérabilité en format HTML.

Les rapports sont disponibles en formats HTML, PDF, XML et XLS. La version HTML du rapport peut être consultée dans n'importe quel navigateur web. Ils s'ouvriront automatiquement dans votre navigateur par défaut. La version PDF est un rapport facile à imprimer. La troisième option est un format XML lisible par machine qui vous permet d'importer les données dans un logiciel de reporting tiers. Le format XLS est un fichier CSV compatible avec Microsoft Excel. Les formats XML et CSV ne contiennent que des données tabulaires. Les graphiques ne sont pas inclus.

Pour générer un rapport de vulnérabilité dans un format téléchargeable, cliquez sur l'icône correspondant au format que vous préférez. Le rapport HTML s'ouvrira dans votre navigateur. Les

autres formats de fichiers se téléchargent automatiquement sur votre machine.

Les rapports de remédiation suggèrent des actions spécifiques qui remédient à certaines vulnérabilités. Par exemple, le rapport suivant suggère deux actions qui remédient à 100% des vulnérabilités trouvées lors d'une analyse d'un lieu particulier.

Un rapport complet sur les mesures correctives ou de remédiation.

Les rapports de remédiation complets suggèrent des actions qui répondent à tous les types de vulnérabilités. Seuls les rapports de remédiation élevés suggèrent des actions qui ne concernent que les vulnérabilités à haut risque. Ces rapports ne sont disponibles qu'en format PDF.

Vous pouvez également envoyer un rapport en format PDF à une personne de contact figurant dans le système beSECURE. Pour ce faire, sélectionnez le contact dans la liste déroulante en bas de la fenêtre, puis cliquez sur l'icône PDF à droite.

Cliquez sur le bouton “Fermer” pour quitter la fenêtre Actions.

Pour plus d'informations sur les rapports, voir la section “Rapports” de ce document.

8.2. Recherche de vulnérabilités

La page de recherche sur les vulnérabilités permet d'effectuer des recherches avancées sur des vulnérabilités spécifiques.

Pour rechercher des vulnérabilités :

1. Connectez-vous au système beSECURE.

2. Cliquez sur Résultats=> Recherche. La page de recherche de vulnérabilités s'affiche. Cette page présente les options de recherche suivantes :

Organisation	L'organisation à rechercher.
Scan	L'analyse qui a permis d'identifier les vulnérabilités. NOTE : Une organisation doit d'abord être sélectionnée.
Nom de la vulnérabilité	Recherche de texte dans le nom descriptif de la vulnérabilité.
Catégorie	La catégorie de vulnérabilité. beSECURE classe les vulnérabilités en fonction de leur domaine d'impact (applications web, cryptage, etc.).
Nom d'hôte / adresse IP	Le nom d'hôte ou l'adresse IP scanné. Utilisez des virgules pour séparer les IP ou nom d’hôte si il y en a plusieurs. Vous pouvez également utiliser le signe du dollar ($) pour indiquer que vous souhaitez une

	correspondance exacte. Par défaut, le système renvoie des correspondances partielles.

Service et port	Le service et le port ont été scannés. Séparez les valeurs par des virgules. Par exemple, si vous entrez 80, 443, vous obtiendrez les résultats pour le port 80 et le port 443.
Numéro du scan	Le numéro attribué au scan. Le numéro de scan pour le premier scan d'une cible sera 1, le deuxième scan portera le numéro de scan 2, et ainsi de suite.
Test ID	L'identifiant du test beSECURE qui a détecté la vulnérabilité lors de l'analyse.
Synthèse	Une description résumée du test beSECURE et les résultats qu'elle a révélés.
Impact	L'impact potentiel de la vulnérabilité, tel que l'accès non autorisé ou la perte de données.
Solution	Solution(s) potentielle(s) pour résoudre le vulnérabilité.

Risque	Le niveau de risque attribué à la vulnérabilité. La première liste déroulante de ce champ permet aux utilisateurs de rechercher les vulnérabilités dont le niveau de risque est égal à, (=), supérieur à (>), inférieur à (<), supérieur ou égal à (>=), ou inférieur ou égal à (<=) le niveau de risque sélectionné dans la deuxième liste déroulante (Élevé, Moyen, Faible ou Aucun).
Résultat CVSS	Le résultat CVSS pour la vulnérabilité.
Age de la Vulnerability	L'âge de la vulnérabilité, en tant que nombre de jours, semaines, mois. Utilisez la liste déroulante à droite du champ de texte pour indiquer si le nombre saisi représente le(s) jour(s), la(les) semaine(s) ou le(s) mois.
Recherche de référence	Recherche d'un élément CVE, CERT, CSC (Cisco) ou KB (Microsoft Knowledge Base) spécifique.
Type d'OS	Le type de système d'exploitation que la cible à distance utilise.
Etiquette	Une valeur définie par l'utilisateur, attribuée à la cible scannée. Les balises permettent de limiter les recherches. Par exemple, l'utilisation d'une balise nommée "DB Server" facilitera la recherche d'informations sur les serveurs de bases de données.

Date d'analyse	Recherche les scans qui se situent dans une plage de dates. Utilisez les widgets du calendrier pour saisir les dates de début et de fin.

Identifiant de la vulnérabilité	L'identification d'une vulnérabilité spécifique.
Inclure les résultats de l'analyse précédente	Si vous voulez inclure les résultats des scans précédents.
Afficher"aucun"risque	Si vous voulez montrer des vulnérabilités qui ne sont pas associées à un niveau de risque.
Afficher Pas de ticket	Si vous voulez montrer des vulnérabilités qui ne sont pas associées à un ticket.
Afficher ignoré	Si vous voulez afficher les vulnérabilités qui ont été marquées "Ignorer".
Retour de sortie dynamique	Si vous voulez activer le champ “Résultats” ci-dessus. Remarques : Les résultats sont disponibles uniquement pour les Web scan.

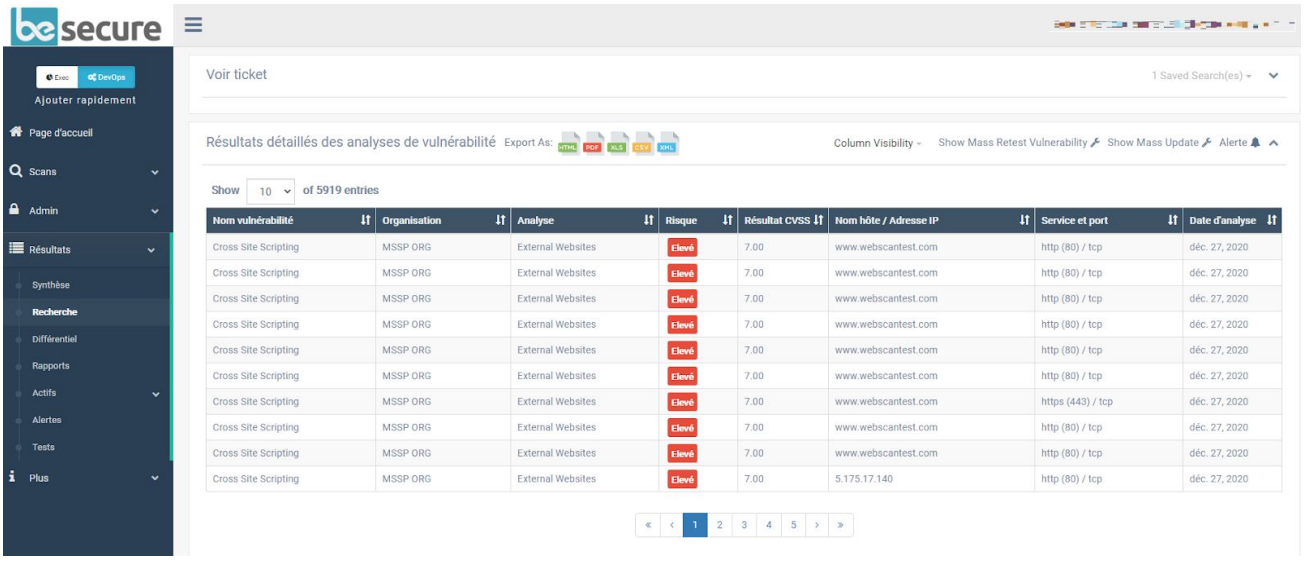
La page de recherche sur la vulnérabilité.

3. Lorsque vous avez fini de saisir les paramètres de recherche, cliquez sur le bouton “Rechercher”. La page de résultats de l'analyse de vulnérabilité apparaît.

Cette page affiche une liste des vulnérabilités qui correspondent aux critères de recherche. Elle présente les informations suivantes sur chaque vulnérabilité :

Nom de la Vulnerabilité	Un nom descriptif pour la vulnérabilité.
Organisation	Le nom de l'organisation associée à la vulnérabilité.
Scan	Le nom du scan qui a trouvé le

	vulnérabilité.
Risque	Le niveau de risque associé à la vulnérabilité. Les valeurs sont : élevé, moyen, faible et aucun.
Résultat CVSS	Le résultat CVSS pour la vulnérabilité.
Nom d'hôte / adresse IP	L'adresse d'hôte ou l'adresse IP de l'hôte concerné.
Service et port	Le service et le port touchés par la vulnérabilité. Séparez les valeurs par des virgules. Par exemple, si vous entrez 80, 443, vous obtiendrez les résultats pour le port 80 et le port 443.
Date de l'analyse	La date à laquelle le scan a eu lieu.



La page des résultats détaillés de l'analyse de vulnérabilité.

Vous pouvez exporter une copie de la liste en cliquant sur l'icône correspondant au format de fichier que vous préférez en haut de la page. La liste peut être exportée au format

HTML, PDF, XML ou XLS.

Cliquez sur une entrée de la liste pour afficher les résultats détaillés de l'analyse de vulnérabilité.

8.2.1. Visualisation des détails de la vulnérabilité

La page “Détails sur la vulnérabilité” présente des informations détaillées sur une vulnérabilité spécifique et les moyens de la résoudre.

Le système présente les informations suivantes sur les vulnérabilités :

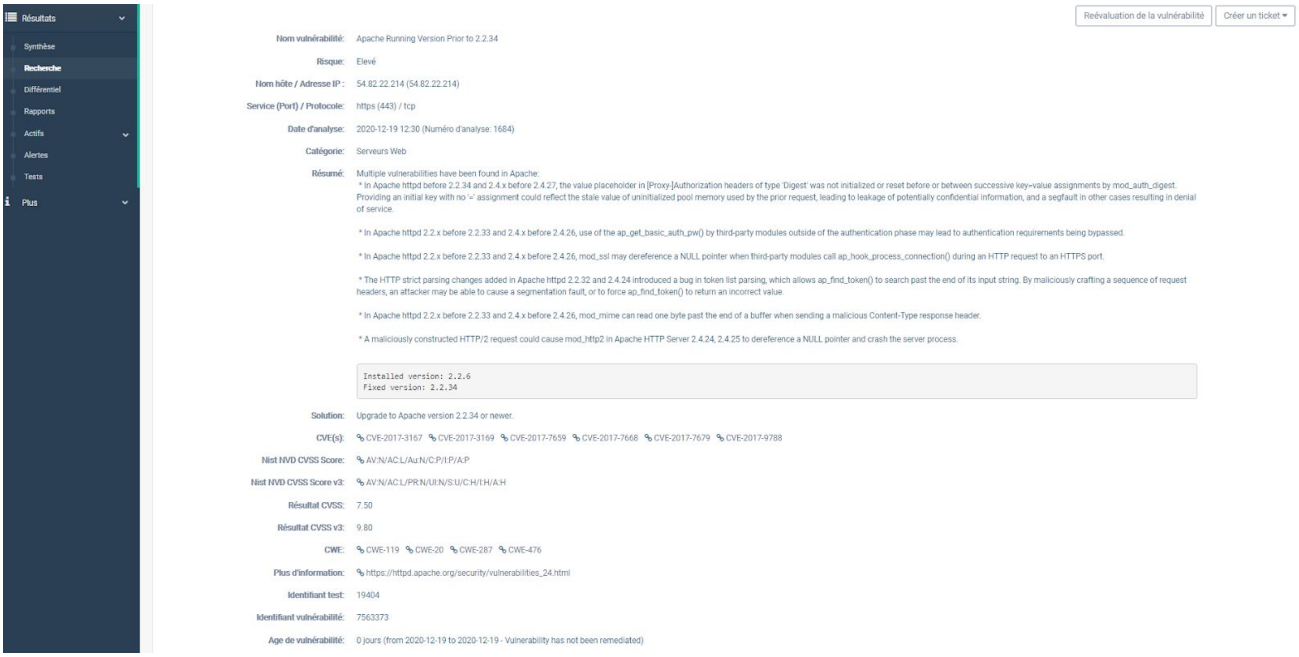
Nom de la vulnérabilité	Un nom descriptif pour la vulnérabilité.
Risque	Le niveau de risque associé à la vulnérabilité. Les valeurs sont : élevé, moyen, faible et aucun.
Nom d'hôte / adresse IP	L'adresse d'hôte ou l'adresse IP de l'hôte concerné.

Service (Port) Protocol	Le service de paramétrage du scan concerné, composé du nom du service, du numéro de port et du protocole de paramétrage du scan.
Date d’analyse	La date et l'heure auxquelles le scan a eu lieu.
Catégorie	La catégorie de vulnérabilité. beSECURE classe les vulnérabilités en fonction de leur domaine d'impact (applications web, cryptage, etc.).

Résumé	Un résumé de la vulnérabilité qui donne de plus amples détails sur la vulnérabilité, les produits (hôtes) touchés et, si possible, les moyens de recréer la situation causée par la vulnérabilité.
Solution	Solution(s) potentielle(s) pour résoudre le vulnérabilité.
CVE(s)	The Common Vulnerabilities and Exposures (CVE) ID numéro pour la vulnérabilité. Cliquez sur la valeur pour voir les détails du CVE sur NIST.gov.
Nist NVD CVSS Score	Le score de gravité de la vulnérabilité selon l'enquête CVSS. Le CVSS est un système indépendant qui attribue une note aux vulnérabilités sur une échelle de 1 à 10. Un score de 10 indique une vulnérabilité critique, tandis que 0 représente un risque négligeable.
Nist NVD CVSS Score v3	Le score de gravité de la vulnérabilité sur l'échelle mise à jour du CVSS Score v3. Cliquez sur la valeur pour voir les détails du CVE sur NIST.gov.

CWE	Le Common Weakness Enumeration ID pour la vulnérabilité. La CWE est une norme industrielle pour indiquer le type de

	vulnérabilité.
Plus d'informations	Fournit des liens vers des sites web externes qui contiennent des informations complémentaires sur la vulnérabilité, notamment le CVE, la base de connaissances de Microsoft et securiteam.com.
Identifiant du Test	L'identifiant du test beSECURE qui a détecté la vulnérabilité lors de l'analyse.
Identifiant de la vulnérabilité	L'identifiant de la vulnérabilité.
Âge de vulnérabilité	L'âge de la vulnérabilité, comme le nombre de jours qui se sont écoulés entre la première et la dernière fois que beSECURE a détecté une vulnérabilité pour un scan spécifique.



La page : Détails sur la vulnérabilité.

Les vulnérabilités sont classées selon trois principaux niveaux de risque. Les vulnérabilités à haut risque peuvent permettre à un attaquant d'obtenir des privilèges élevés sur une machine vulnérable, et doivent être traitées en priorité.

Les vulnérabilités à risque moyen sont des faiblesses qui exposent des données sensibles à un attaquant, soit facilitent un déni de service (DDOS). Les vulnérabilités à faible risque permettent la collecte d'informations préliminaires pour un attaquant, ou présentent des risques qui ne sont pas entièrement liés à la sécurité.

Les politiques de sécurité sont considérées comme à faible risque. Le système classe les résultats qui ne présentent aucune menace pour la sécurité, mais qui contiennent des informations intéressantes sur la cible, dans la catégorie "Aucune".

La page “Détails de la vulnérabilité” donne également accès à la fonctionnalité de ticket. Si un ticket n'existe pas pour une vulnérabilité, vous pouvez en créer un en cliquant sur le bouton “Créer un ticket”. S'il existe un ticket pour une vulnérabilité, un bouton “Afficher le ticket” apparaîtra à la place. Pour plus d'informations, voir la section tickets de ce document.

8.3. Recherche différentielle

Les rapports différentiels vous permettent de suivre les changements entre deux événements de scan pour une organisation. Cette fonctionnalité vous permet de suivre les performances en termes de :

· Les mesures prises pour remédier aux vulnérabilités

· Le temps qui s'écoule avant que les vulnérabilités ne soient traitées

Pour effectuer une recherche différentielle :

1. Connectez-vous au système beSECURE.

2. Cliquez sur Résultats=>Différentiel, dans la barre latérale.

3. Remplissez les champs de recherche suivants (de gauche à droite) :

a) Choisissez votre organisation dans la liste déroulante. Le nombre de scans sauvegardés disponibles apparaît entre parenthèses à côté du nom de l'organisation. Le champ de recherche de droite se remplira avec les scans disponibles pour cette organisation.

b) Choisissez une analyse dans la liste déroulante.

c) Les cases à cocher Haut, Moyen et Bas du champ “Afficher les nouvelles vulnérabilités” sont cochées par défaut. Décochez-les si vous le souhaitez.

d) Les cases à cocher Haut, Moyen et Faible du champ “Afficher les vulnérabilités corrigées” sont cochées par défaut. Décochez-les si vous le souhaitez.

e) Dans le champ “Résultats actuels de”, sélectionnez la date d'une analyse récemment effectuée.

f) Dans le champ “Résultats précédents de”, sélectionnez la date d'une analyse antérieure.

g) Dans le champ “Sélection des résultats”, choisissez une plage de dates pour réduire les résultats à une période plus courte entre les dates d'analyse que vous avez sélectionnées aux étapes 5 et 6 ci-dessus.

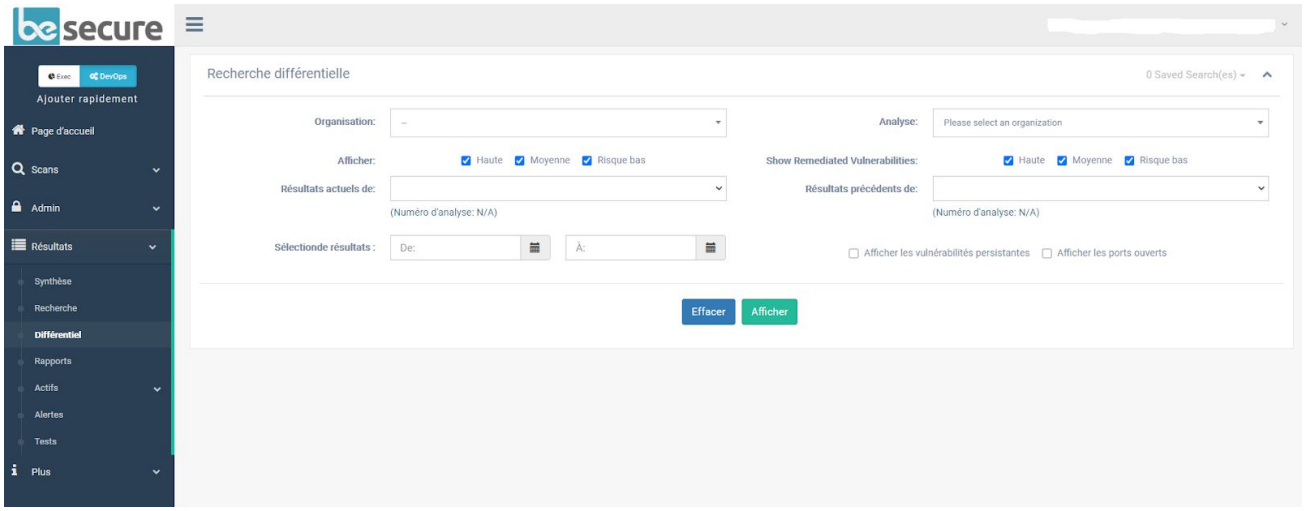
h) Cochez la case “Afficher les vulnérabilités persistantes”, si vous le souhaitez.

i) Cochez la case “Afficher les ports ouverts”, si vous le souhaitez.

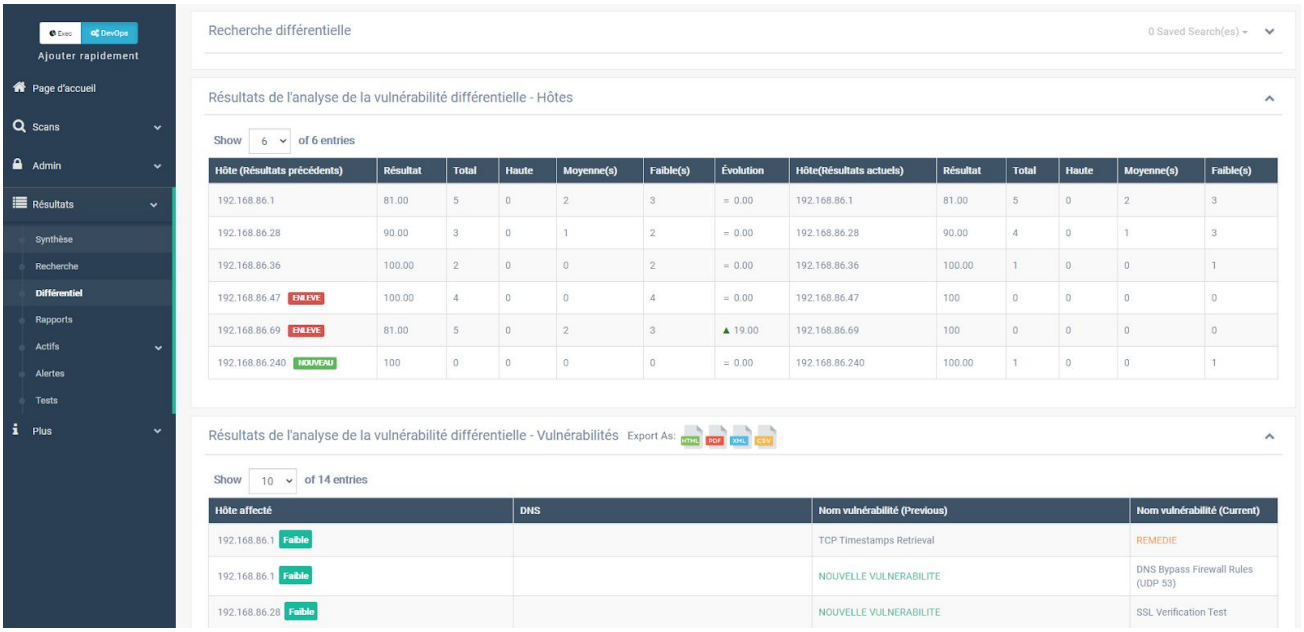
j) Cliquez sur le bouton “Afficher les résultats”, ou sur le bouton Effacer pour

recommencer.

La page de recherche différentielle.



L'écran des résultats montre les résultats par hôte et les résultats par vulnérabilité..



La page de résultats de la recherche différentielle.

La section “Résultats différentiels de l'analyse de vulnérabilité- Hôtes” affiche les informations suivantes :

Hôte (Résultats Précédents)	Ce que l'hôte a scanné lors du scan précédent.
Résultat	Le score global de l'hôte.

Total	Le nombre total de vulnérabilités trouvées.
Haute	Le nombre de vulnérabilités à haut risque trouvées.
Moyenne(s)	Le nombre de vulnérabilités à risque moyen trouvées.
Faible(s)	Le nombre de vulnérabilités à faible risque trouvées.
Evolution	Indique si la cible devient plus ou moins sûre, sur la base d'une comparaison des scores des scans actuels et précédents.

Hôte (Résultats actuels)	L'hôte scanné lors du scan actuel.
Résultats	Le score global de l'hôte.
Total	Le nombre total de vulnérabilités trouvées.
Haute	Le nombre de vulnérabilités à haut risque trouvées.
Moyenne(s)	Le nombre de vulnérabilités à risque moyen trouvées.
Faible(s)	Le nombre de vulnérabilités à faible risque trouvées.

Dans l'image ci-dessous, par exemple, secureiteam.com était l'hôte ou la cible dans les scans précédents et actuels. Les résultats précédents montrent un score global parfait de 100, sans aucune vulnérabilité trouvée. Dans les résultats actuels, cependant, beSECURE a trouvé un total de sept vulnérabilités, et le score global de l'hôte est tombé à 90. La colonne “Evolution” reflète cette baisse de 10 points. Pour plus d'informations sur la manière dont beSECURE calcule les scores, voir la section Scoring de ce document.

La section Hôtes de la page Résultats différentiels de l'analyse de vulnérabilité.

La section Vulnerability Scan Differential Results - Vulnerabilities (Résultats différentiels de l'analyse de vulnérabilité - Vulnérabilités) affiche les informations suivantes :

Hôte affecté	L'hôte scanné. Une étiquette indiquant le risque de vulnérabilité pour l'hôte apparaît à côté du nom de l'hôte.
Nom de la vulnérabilité (Précédente)	Un nom descriptif pour la vulnérabilité trouvée lors de l'analyse précédente. La valeur "Nouvelle vulnérabilité" apparaît si la vulnérabilité n'a pas été découverte lors de l'analyse précédente. La valeur "Remédiée" apparaît si une vulnérabilité découverte lors d'une analyse précédente n'apparaît pas dans l'analyse actuelle.
Nom de la vulnérabilité (actuelle)	Un nom descriptif pour la vulnérabilité trouvée dans l'analyse actuelle.

Pour exporter les résultats au format HTML, PDF, XML ou XLS, cliquez sur l'icône correspondant au format qui apparaît au-dessus du tableau des résultats.

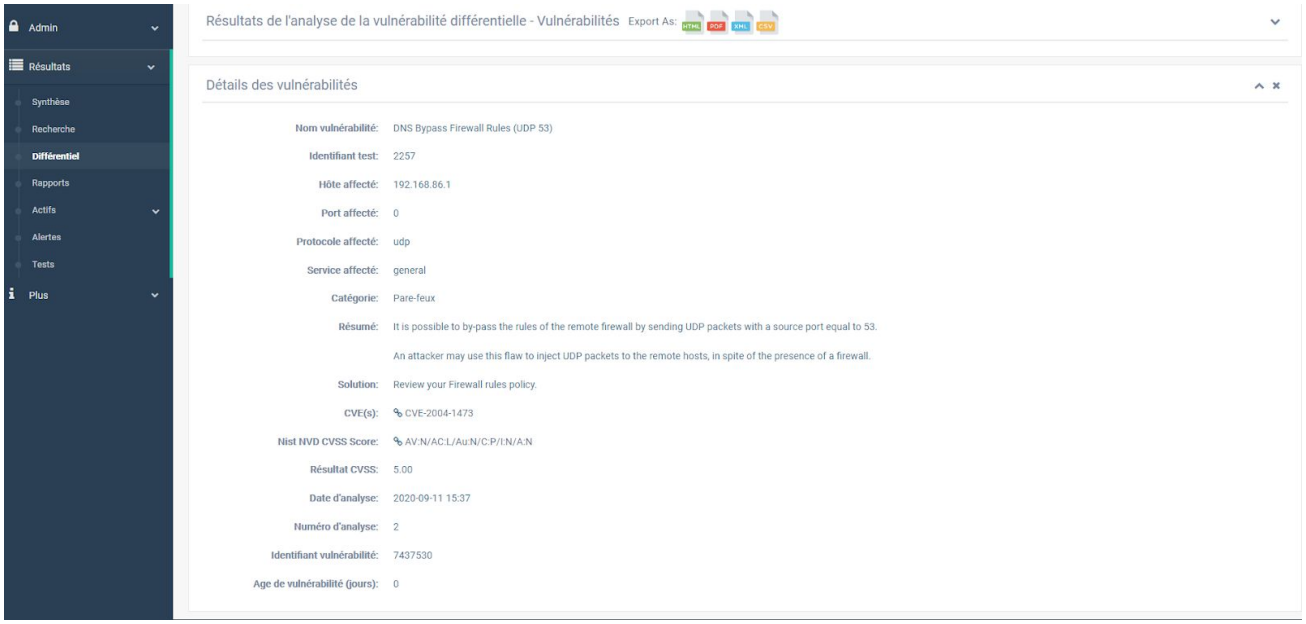
Show 10 of 14 entries

Hôte affecté	DNS	Nom vulnérabilité (Previous)	Nom vulnérabilité (Current)
192.168.86.1 Faible		TCP Timestamps Retrieval	REMEDIE
192.168.86.1 Faible		NOUVELLE VULNERABILITE	DNS Bypass Firewall Rules (UDP 53)
192.168.86.28 Faible		NOUVELLE VULNERABILITE	SSL Verification Test
192.168.86.36 Faible		TCP Timestamps Retrieval	REMEDIE
192.168.86.47 Faible		ICMP Timestamp Request	REMEDIE
192.168.86.47 Faible		SSL Verification Test	REMEDIE
192.168.86.47 Faible		SSL Verification Test	REMEDIE
192.168.86.47 Faible		TCP Timestamps Retrieval	REMEDIE
192.168.86.69 Moyen		Simple Service Discovery Protocol 'M-SEARCH request' DrDoS	REMEDIE
192.168.86.69 Moyen		Network Basic Input/Output System 'Name Resolution (Name Query)' DrDoS	REMEDIE

« ‹ 1 2 › »

La section "Vulnérabilités" de la page "Résultats différentiels de l'analyse de vulnérabilité".

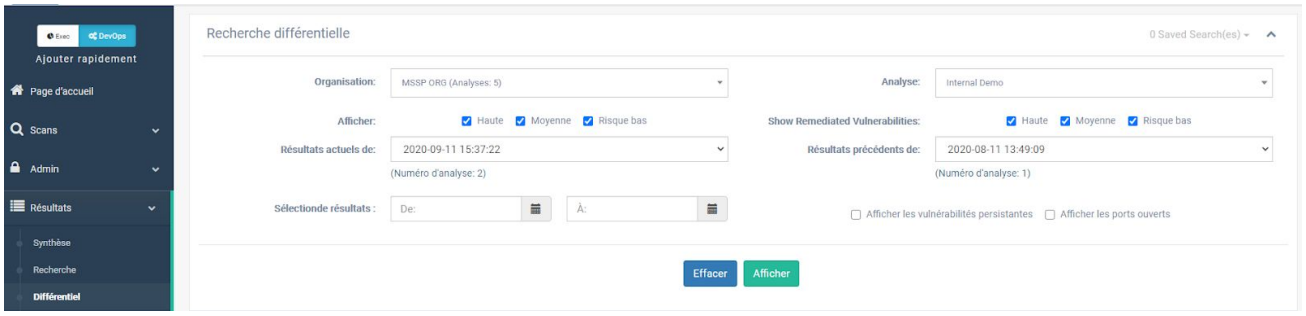
Cliquez sur une ligne pour afficher les détails de la vulnérabilité.



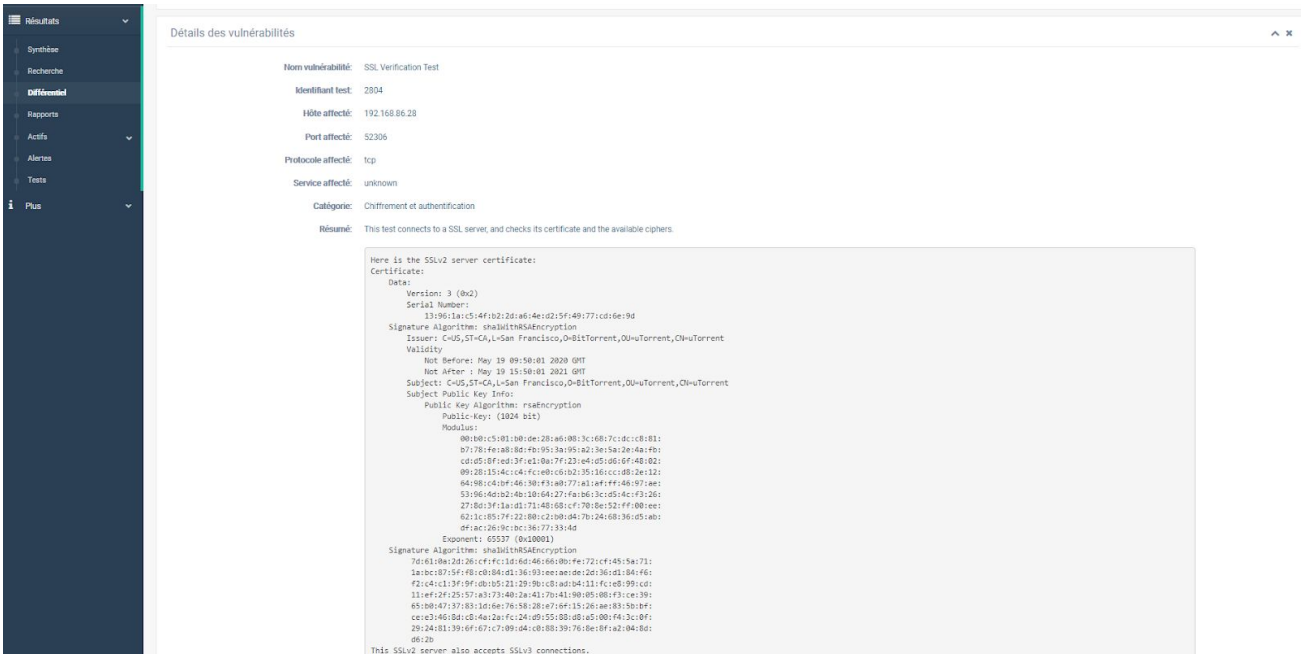
La page Détails sur la vulnérabilité.

Les liens en haut de la page permettent d'accéder à d'autres parties de la section “Résultats différentiels” au sein de la même page. Par exemple, en cliquant sur “Résultats différentiels de

l'analyse de la vulnérabilité - Hôtes”, une fenêtre contenant les résultats de l'hôte s'ouvre. En cliquant sur “Recherche différentielle”, vous ouvrirez une autre fenêtre contenant l'interface de recherche, ce qui vous permettra d'effectuer une autre recherche différentielle dans la même page.



La page de résultats différentiels de l'analyse de vulnérabilité, avec le fenêtre de recherche différentielle élargie. Cliquez sur un résultat pour voir les détails de la vulnérabilité.



The Vulnerability Details page.

La page : Détails sur la vulnérabilité affiche les informations suivantes :

Nom de la vulnérabilité	Le nom de la vulnérabilité.
Identifiant du Test	L'identifiant du test beSECURE qui a détecté la vulnérabilité lors de l'analyse.
Hôte affecté	L'hôte scanné.

Port touché	Le port touché
Protocole affecté	Le protocole concerné (par exemple, tcp).
Service concerné	Le service concerné (par exemple http).
Catégorie	La catégorie dans laquelle se situe la vulnérabilité.
Résumé	Un résumé descriptif de la vulnérabilité.
Solution	Fournit des suggestions sur la manière de remédier à cette vulnérabilité.
Plus d'informations	Liens vers de plus amples informations sur la vulnérabilité.
Date d'analyse	La date du scan.
Numéro/identifiant du Scan	Le numéro attribué au scan. Le numéro de scan pour le premier scan d'une cible sera 1, le deuxième scan portera le numéro de scan 2, et ainsi de suite.
Identifiant (ID) de la vulnérabilité	L'identification de la vulnérabilité.
Âge de la Vulnérabilité (jours)	L'âge de la vulnérabilité, comme le nombre de jours qui se sont écoulés entre la première et la dernière fois qu'elle a été détectée.

8.4. Notation

Le système beSECURE évalue les vulnérabilités, les actifs, les réseaux et les organisations. Le score de vulnérabilité est basé sur la gravité de la vulnérabilité. Le score des actifs est basé sur l'actif. Enfin, le score de l'organisation est basé sur le score moyen de tous les réseaux d'une organisation.

8.4.1. Score de vulnérabilité

beSECURE calcule le score d'une vulnérabilité en fonction de son facteur de risque (élevé, moyen ou faible), ainsi que du système commun de notation de la vulnérabilité (CVSS). Les scores de base numériques du CVSS représentent les caractéristiques de chaque vulnérabilité.

Bien que le CVSS utilise également des classements catégoriels de gravité faible, moyenne et élevée, ces classements qualitatifs sont simplement mis en correspondance avec les scores numériques du CVSS :

· Faible gravité - Une vulnérabilité avec un score de base de l'enquête CVSS de 0,0 à 3,9.
· Gravité moyenne - Vulnérabilité avec un score de base CVSS de 4,0-6,9.
· Gravité élevée - Vulnérabilité dont la note de base de l'enquête CVSS est comprise entre 7,0 et 10,0.

Dans certains cas, certaines des informations généralement utilisées pour générer les

scores CVSS peuvent être indisponibles. Cela se produit généralement lorsqu'un fournisseur annonce une vulnérabilité mais refuse de fournir certains détails. Dans ce cas, les analystes de Beyond Security attribuent des notes CVSS en fonction des informations disponibles.

Définitions des vecteurs CVSS

beSECURE fournit également un vecteur décrivant les composantes utilisées pour calculer le score CVSS. Cela permet aux utilisateurs du score d'avoir confiance en son exactitude et de comprendre la nature de la vulnérabilité. Les vecteurs CVSS comprennent toujours des métriques de base et peuvent contenir des métriques temporelles. Voir le guide de l'utilisateur du système commun de notation de la vulnérabilité pour une description détaillée des mesures CVSS et de leurs valeurs possibles.

Vecteurs CVSS de base

Les vecteurs CVSS contenant uniquement des métriques de base prennent la forme suivante :

(AV : [R,L]/AC : [H,L]/Au : [R,NR]/C : [N,P,C]/I : [N,P,C]/A : [N,P,C]/B : [N,C,I,A])

Les lettres entre parenthèses représentent les valeurs possibles d'une métrique CVSS. Une option est choisie pour chaque ensemble de parenthèses. Les lettres en dehors des parenthèses sont obligatoires et doivent être incluses dans un vecteur CVSS valide. Chaque lettre ou paire de lettres est une abréviation d'une valeur métrique ou d'un paramètre dans le CVSS. Les abréviations sont définies comme suit.

Les abréviations suivantes sont en anglais :

Exemple 1: (AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C)

Exemple 2: (AV:R/AC:L/Au:R/C:C/I:N/A:P/B:N)

Métrique : AV = AccessVector (Related exploit range)

Valeurs Possibles : R = Remote, L = Local

Métrique : AC = AccessComplexity (Required attack complexity)

Possible Values: H = High, L = Low

Métrique : Au = Authentication (Level of authentication needed to exploit)

Valeurs possibles : R = Required, NR = Not Require

Métrique : C = ConfImpact (Confidentiality impact)

Valeurs possibles : N = None, P = Partial, C = Complete

Métrique : I = IntegImpact (Integrity impact)

Valeurs Possibles : N = None, P = Partial, C = Complete

Métrique : A = AvailImpact (Availability impact)

Valeurs Possible : N = None, P = Partial, C = Complete

Métrique : B = ImpactBias (Impact value weighting)

Valeurs Possibles : N = Normal, C = Confidentiality, I = Integrity, A = Availability

Vecteurs temporels CVSS

Les vecteurs CVSS contenant des métriques temporelles sont formés en empruntant les métriques temporelles au vecteur de base. Les métriques temporelles empruntées au vecteur de base prennent la forme suivante :

/E:[U,P,F,H]/RL:[O,T,W,U]/RC:[U,Uc,C]

Example 1: (AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C/E:U/RL:O/RC:U)

Example 2: (AV:R/AC:L/Au:R/C:C/I:N/A:P/B:N/E:P/RL:T/RC:Uc)

Métrique: E = Exploitability (Availability of exploit)

Valeurs Possibles : U = Unproven, P = Proof-of-concept, F = Functional, H = High

Métrique: RL = RemediationLevel (Type of fix available)

Valeurs Possible : O = Official-fix, T = Temporary-fix, W = Workaround, U = Unavailable

Métrique: RC = ReportConfidence (Level of verification that the vulnerability exists)

Valeurs Possibles : U = Unconfirmed, Uc = Uncorroborated, C =Confirmed

beSECURE fournit des liens vers le calculateur CVSS du NVD en créant un hyperlien qui inclut le vecteur CVSS. Cela fonctionne à la fois pour les vecteurs de base et les vecteurs temporels. Les hyperliens prennent la forme suivante.

Exemple d'hyperlien du vecteur de base vers le calculateur CVSS :

http://nvd.nist.gov/cvss.cfm?vector=(AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C)

Example temporal vector hyperlink to CVSS calculator:

http://nvd.nist.gov/cvss.cfm?vector=(AV:L/AC:H/Au:NR/C:N/I:P/A:C/B:C/E:U/RL:O/RC:U)

8.4.2. Score de l'hôte

Les scores des hôtes vont de 0 à 100, les valeurs les plus élevées représentant une plus grande sécurité. Un score de 0 indique que l'hôte peut être facilement compromis, tandis qu'une valeur de 100 indique un hôte sécurisé sans vulnérabilités à risque élevé ou moyen.

Le score d'un hôte ou d'un actif est déterminé en additionnant les scores de toutes les vulnérabilités présentes sur l'hôte, puis en faisant la moyenne de ces scores. Les vulnérabilités à risque élevé, moyen et faible sont pondérées différemment. Les vulnérabilités à haut risque ont un poids plus élevé, tandis que les vulnérabilités à faible risque n'ont pas de poids. La pondération est effectuée selon le calcul suivant :

$$hostscore = (\frac{1}{2})^{(numberofhigh)} * (\frac{9}{10})^{(numberofmedium)}$$

8.4.3. Score du réseau

Le score d'un réseau ou d'un groupe d'actifs est déterminé en faisant la moyenne de tous les scores des hôtes présents. Un poids est ajouté à chaque groupe d'hôtes. Cela vous permet d'attribuer à certains hôtes une importance plus grande qu'à d'autres. Le poids ajouté peut aider les utilisateurs de beSECURE à diminuer l'importance de certains hôtes (tels que les imprimantes) lors du calcul du score global d'un réseau ou d'un groupe d'actifs tout en attribuant une plus grande importance à d'autres hôtes, tels que les serveurs de production. Le score du réseau est calculé de la manière suivante :

$$\frac{\Sigma\left(\frac{(averagescore)*(hostcount)}{(101-weight)}\right)}{\Sigma\left(\frac{(hostcount)}{(101-weight)}\right)}$$

Dans l'équation ci-dessus, on fait la moyenne des poids des hôtes. Plus le poids est élevé, plus l'influence sur le score du réseau est importante. L'attribution d'un poids de 1 ou même de 0 (zéro) à un groupe d'hôtes rendra leur influence respectivement inaperçue ou ignorée.

8.4.4. Score de l'organisation

Le score d'une organisation est basé sur la moyenne récursive des scores de tous les scans/réseaux qui en relèvent. Si une organisation a des sous-organisations, beSECURE inclura également leurs scores dans son algorithme de calcul de la moyenne.

9. Rapports

Alors que les rapports beSECURE sont disponibles dans différentes sections du menu “Résultats”, la sous-section “Rapports” sert d'emplacement central pour la génération et la visualisation de rapports personnalisés.

9.1. Visualisation des rapports

Pour consulter les rapports précédemment demandés :

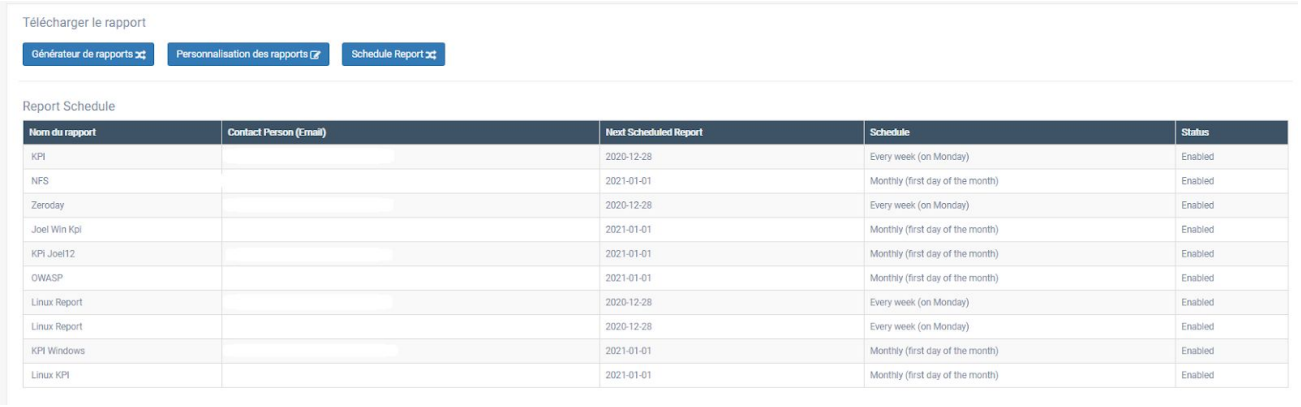
1. Connectez-vous au système beSECURE.
2. Allez à la rubrique "Rapports de résultats".

Une liste des rapports précédemment générés apparaît (le cas échéant). Cette liste contient les informations suivantes sur chaque rapport :

ID	L’ID (identifiant) du rapport
Nom du rapport	Un nom descriptif pour le rapport.
Demandé	La date à laquelle le rapport a été demandé.
Générée	La date à laquelle le rapport a été généré.
Statut	L'état d'avancement du rapport. Les valeurs sont en attente, prêtes et non examinées.

En passant le curseur sur une entrée, une fenêtre contenant plus d'informations apparaît.

Si l'état du rapport est prêt, le fait de cliquer sur le rapport le fera s'ouvrir dans un navigateur ou le télécharger sur votre machine.



La page des rapports.

9.2. Génération des rapports

Pour générer un rapport :

1. Connectez-vous au système beSECURE.

2. Allez à la rubrique "Rapports de résultats". Une liste des rapports précédemment générés apparaîtra (le cas échéant).

3. Cliquez sur le bouton "**Générer le rapport**". La fenêtre Générer le rapport s'ouvre.

4. Remplissez le formulaire qui apparaît. Le formulaire comporte les champs suivants:

Organisation (requis)	L'organisation à scanner.
Scan	L'analyse/scan exécuté précédemment pour en rendre compte.
Date du Scan	La date et l'heure du scan.
Type de rapport (obligatoire)	Le type de rapport à créer (résumé, HIPAA, etc.). La valeur par défaut est un rapport dit ordinaire (complet et exhaustif).
Cacher la section Informations sur l'hôte	S'il faut cacher la section "Informations sur l'hôte" du rapport, qui contient les résultats du scan des ports, les données
	sur le processus d'analyse, et d'autres informations qui ne sont pas liées aux vulnérabilités.

5. Cliquez sur le bouton "Générer". La demande de rapport entrera dans la file d'attente.

Les rapports sont généralement générés dans un délai de cinq minutes.

9.3. Personnalisation des rapports

beSECURE permet aux utilisateurs de contrôler les informations qui figurent dans un rapport.

Pour personnaliser un rapport :

1. Connectez-vous au système beSECURE.

2. Cliquez sur “Résultats”=>”Rapports”. Une liste des rapports précédemment générés apparaîtra (le cas échéant).

3. Cliquez sur le bouton "Personnaliser le rapport". La fenêtre de personnalisation du rapport s'ouvrira.

4. Remplissez le formulaire qui apparaît. Le formulaire comporte les champs suivants:

Nom de la personnalisation	Un nom pour la personnalisation.
Nom du rapport	Nom du rapport
Format (obligatoire)	Le format de sortie du rapport. Les valeurs sont PDF (par défaut) et XML.
Type de rapport	Le type de rapport à créer. Les valeurs sont : Complet (par défaut), Filtré et Différentiel.
Style du rapport (obligatoire)	Le style de rapport à créer (résumé, HIPAA, etc.) est par défaut un rapport complet sans type spécifique.
Cacher la section Informations sur l'hôte	Si vous voulez cacher la section "Informations sur l'hôte" du rapport.

5. Cliquez sur le bouton Modifier pour enregistrer les modifications.

Pour supprimer entièrement la personnalisation du rapport, cliquez sur le bouton Supprimer.

10. Actifs

beSECURE crée un Asset à partir de chaque hôte qui est entré dans le système. Une valeur est attribuée à chaque actif, qui contrôle le poids de l'hôte sur le score du réseau qui contient l'actif et, à son tour, le score de l'organisation qui contient le réseau.

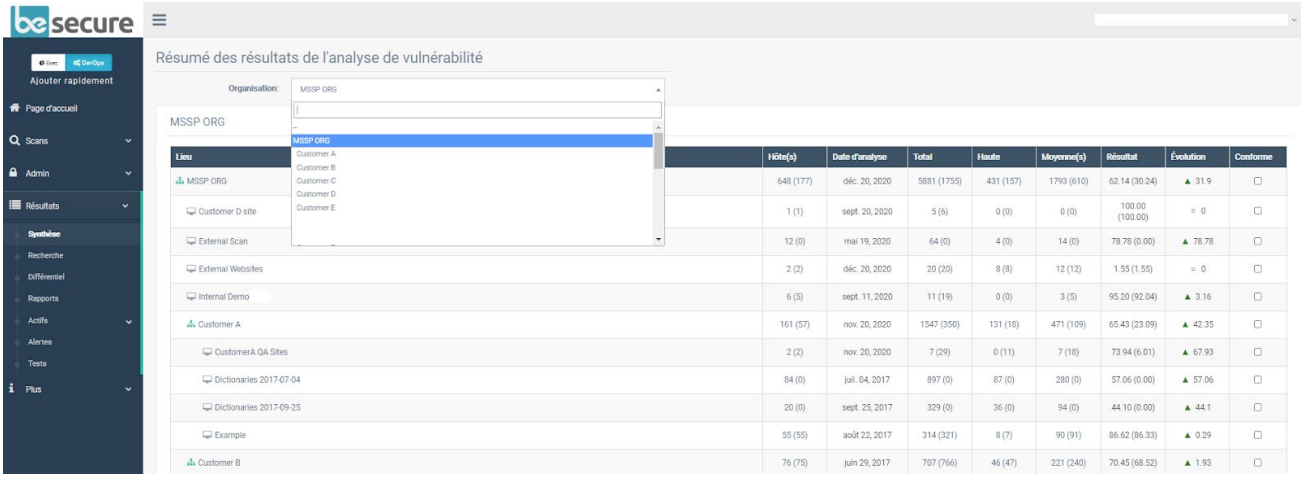
Par défaut, tous les actifs reçoivent une valeur normale. Toutefois, la modification de la valeur attribuée à un actif vous donne un plus grand contrôle sur la pondération et les notes. Les valeurs valides vont de 0 (Ignorer) à 100 (Élevé). Une valeur de Normal représente la valeur médiane de 50, et n'accorde aucun poids particulier à l'hôte en question.

La section “Actifs” fournit également une multitude d'informations sur chaque actif. Pour consulter les actifs :

1. connectez-vous au système beSECURE.

2. Allez dans la zone Résultats ' Actifs. Le menu se développera

3. Cliquez sur Résumé. Une liste des actifs apparaîtra.

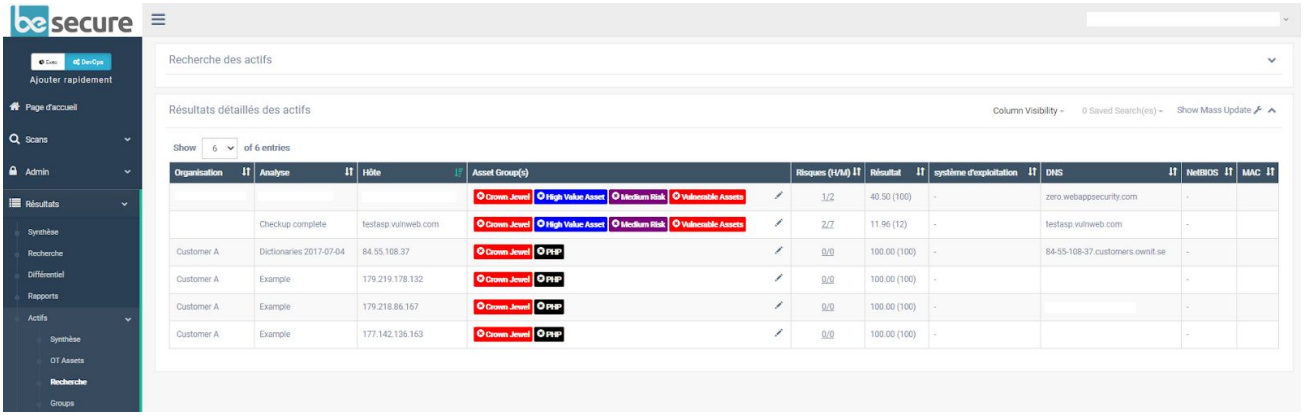


La page de résumé des actifs.

4. Pour filtrer la liste, choisissez une organisation dans la liste déroulante en haut de la page. Vous pouvez également utiliser les boutons de navigation en bas de page pour parcourir la liste. Cliquez sur une entrée pour en voir les détails.

La page des résultats du résumé des actifs apparaîtra. Cette page indique l'emplacement, la valeur, le système d'exploitation, le DNS, le nom NetBIOS, le MAC et l'étiquette pour chaque actif. Pour exporter ces

informations, cliquez sur l'icône correspondant au format de sortie que vous préférez. Les résultats peuvent être exportés sous forme de fichiers HTML, PDF, XML ou XLS.



La page des résultats du résumé des actifs.

Tous les actifs dans l'image ci-dessus ont la valeur par défaut de Normal. Ils affecteront le score du réseau et de l'organisation de la même manière.

Pour modifier la valeur d'un actif afin d'ajuster son poids dans le processus de notation, cliquez sur l'icône d'édition qui apparaît à côté de la valeur, puis choisissez une nouvelle valeur dans la liste déroulante.

La page de recherche des actifs vous permet de localiser un actif spécifique de manière plus efficace. Pour rechercher des actifs : 1. allez dans Résultats ' Actifs ' Recherche. La page de recherche des biens apparaîtra.

2. Entrez les paramètres de recherche. La page "Recherche de biens" comporte les champs suivants :

Organisation	L'organisation associée à l'actif.
Scan/Analyse	Le scan associé à l'actif. Note : Une organisation doit d'abord être sélectionnée.

Afficher la tendance/évolution	Filtre les résultats par tendance de score. Les valeurs s'améliorent, diminuent et restent inchangées.
Valeur	La valeur attribuée à l'actif.
Nom d'hôte / adresse IP	Le nom ou la plage d'adresses IP de l'hôte analysé.
Système d'exploitation	Filtres par le système d'exploitation de la cible.
DNS	Le nom du FQDN ou de l'hôte Internet de la cible
NetBIOS	Le nom NetBIOS.
MAC	L'adresse matérielle de la machine cible.
Tag/Etiquette	Une valeur définie par l'utilisateur et attribuée à l'actif. Les balises permettent de limiter les recherches. Par exemple, l'utilisation d'une balise nommée "DB Server" facilitera la recherche d'informations sur les serveurs de bases de données.
Récursivement	S'il faut chercher de manière récursive. Alors qu'une recherche standard s'effectue au niveau de l'organisation principale, une recherche récursive examinera l'organisation sélectionnée et toutes les sous-organisations qui en relèvent.
Cacher les non-résultats	S'il faut cacher des cibles qui ne sont pas vulnérables.

3. Cliquez sur le bouton "Recherche".

11. Alertes

Une alerte est une recherche définie par l'utilisateur qui déclenche un e-mail à l'utilisateur lorsqu'il

renvoie des résultats. Par exemple, une alerte peut envoyer un courrier électronique chaque fois qu'une vulnérabilité à haut risque est trouvée. La zone des alertes du système beSECURE affiche une liste des alertes que le système a générées.

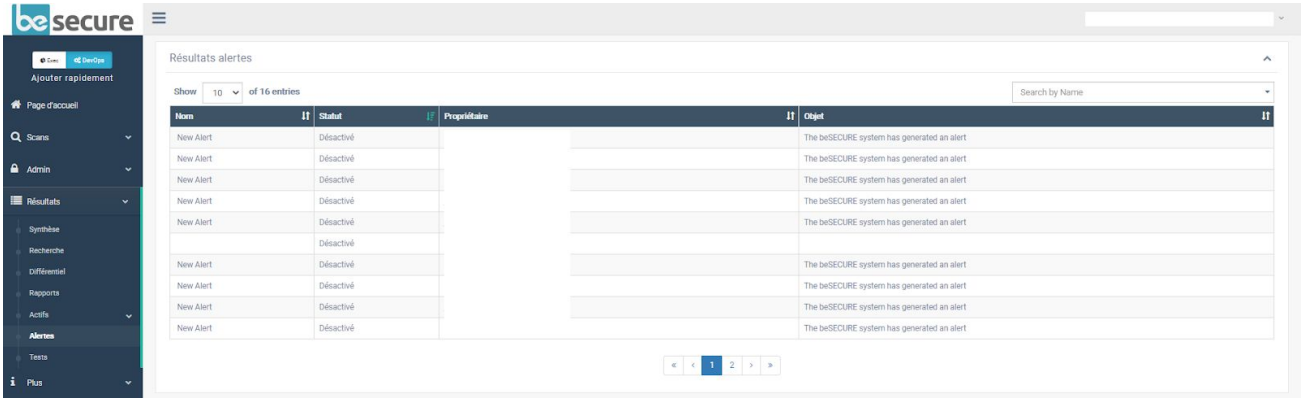
Pour accéder aux alertes :

1. Connectez-vous au système beSECURE.

2. Cliquez sur **Résultats=>Alertes**. Une liste des alertes générées par le système apparaîtra.

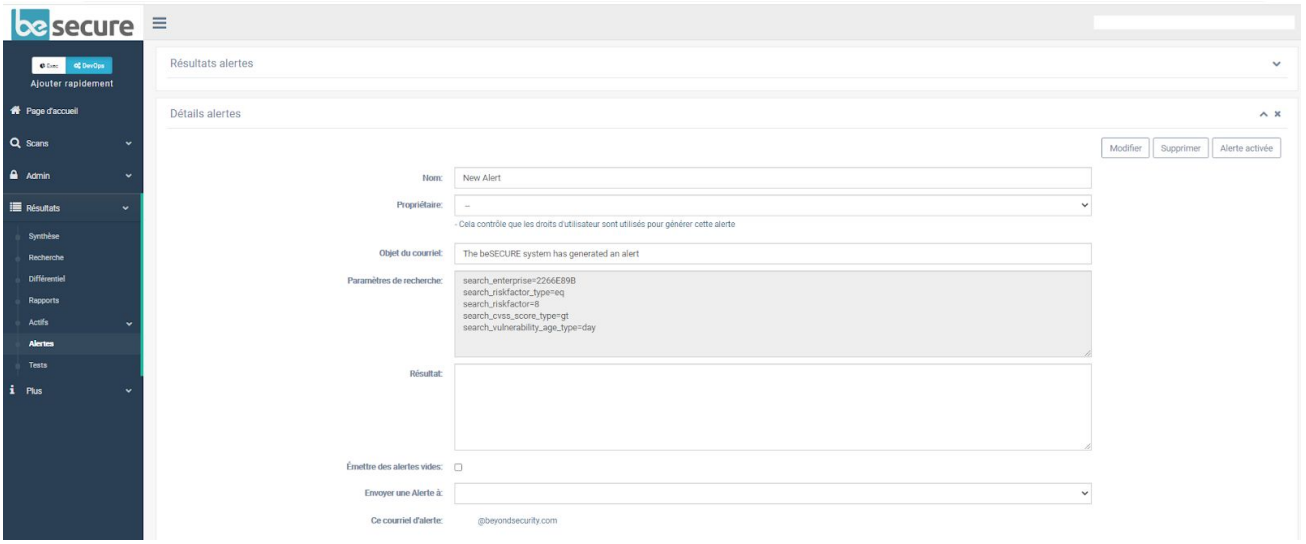
   Cette liste contient les informations suivantes sur chaque alerte :

Nom	Le nom de l'alerte.
Statut	Le statut de l'alerte. Les valeurs sont désactivées et activées.
Propriétaire	L'utilisateur à qui appartient l'alerte.
Sujet	L'objet du message électronique qui a été envoyé à la personne de contact.



La page des résultats des alertes.

3. Cliquez sur une alerte pour en voir les détails.



La page Détails de l'alerte.

La page "Détails de l'alerte" affiche les informations suivantes :

Nom	Le nom de l'alerte.
Propriétaire	L'utilisateur à qui appartient l'alerte.
Objet du courriel	L'objet du message électronique qui sera envoyé à la personne de contact.
Paramètres de recherche	Les paramètres de recherche qui doivent générer l'alerte.
Résultats	Les résultats d'un "test" de l'alerte. Ces informations sont utiles pour le débogage.
Émettre des alertes vides	S'il faut émettre des alertes vides pour indiquer qu'aucun résultat n'a été trouvé.
Envoyer l'alerte à	La personne de contact à laquelle le signalement doit être envoyé

Alerter cet e-mail	L'adresse électronique à laquelle l'alerte doit être envoyée.

Pour modifier l'alerte, modifiez les champs du formulaire, puis cliquez sur le bouton Modifier.

Pour supprimer l'alerte, cliquez sur le bouton Supprimer.

Pour activer l'alerte, cliquez sur le bouton Activer l'alerte.

12. Tests

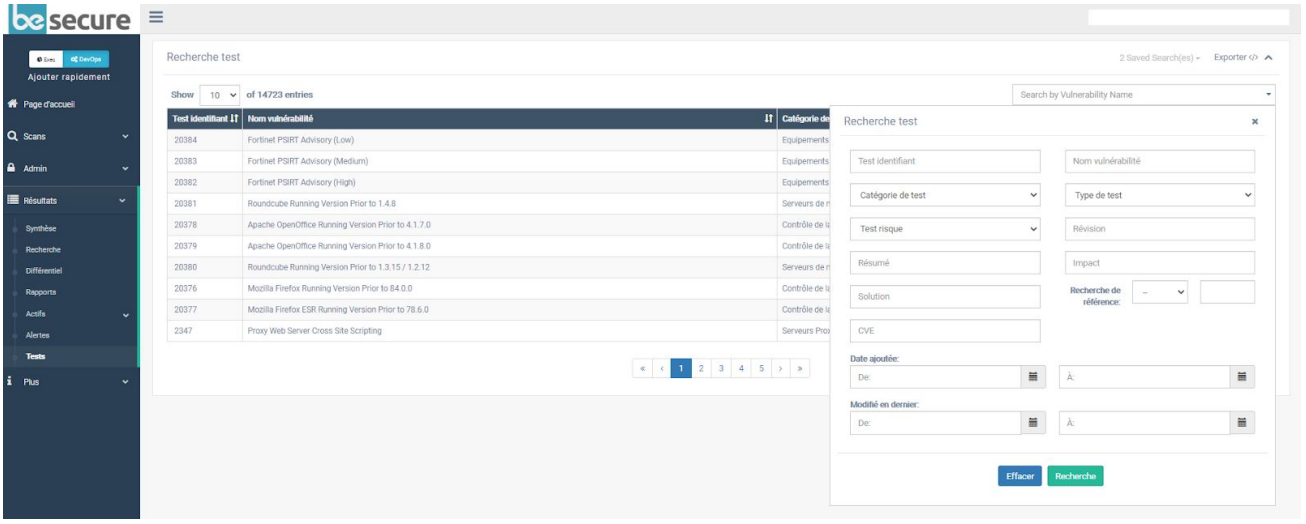
Chaque scan beSECURE exécute plusieurs tests conçus pour détecter les vulnérabilités. La zone Tests du système beSECURE fournit une vue d'ensemble des tests inclus dans un scan.

Pour accéder aux Tests :

1. Connectez-vous au système beSECURE.
2. Cliquez sur Résultats =>Tests. La page de recherche de tests apparaîtra. Cette page fournit les informations suivantes sur chaque test.

Identifiant/ID du Test	L'ID du test qui a détecté la vulnérabilité.
Nom de la vulnérabilité	Un nom descriptif pour la vulnérabilité.
Catégorie de test	La catégorie dans laquelle se situe le test. Chaque catégorie est conçue pour détecter différents types de vulnérabilités.
Test du risque	Le niveau de risque de vulnérabilité que le test est conçu pour détecter. Les valeurs sont : aucune, faible, moyenne et élevée.

Date d'ajout	La date à laquelle le test a été ajouté.
Dernière modification	La date à laquelle le test a été modifié pour la dernière fois.



La page de recherche d'essai, avec le panneau de recherche avancée élargi.

3. Utilisez le champ de recherche pour rechercher un test par nom de vulnérabilité, ou cliquez sur la flèche dans le champ de recherche pour ouvrir les options de recherche avancée. La recherche avancée vous permet de récupérer des tests basés sur les champs suivants :

Identifiant du Test	L'identifiant du test.
Nom de la vulnérabilité	Recherche de texte dans le nom descriptif de la vulnérabilité.
Catégorie de test	La catégorie dans laquelle se situe le test. Chaque catégorie est conçue pour détecter différents types de vulnérabilités.

Type de test	Le type de test. Les valeurs sont Attaque, Déni de service (DoS), Information (collecte de données uniquement ; ne

	ne pas découvrir de vulnérabilités), et Scanner (configurer la manière dont le scanner effectue l'analyse en termes de vitesse, d'utilisation de l'authentification, de paramètres d'analyse web, etc.)
Test du risque	Le niveau de risque de vulnérabilité que le test vise à détecter. Les valeurs sont les suivantes : aucune, faible, moyenne et Haute.
Révision	La version du test (par exemple "1ère génération", "2ème génération", etc.).
Résumé	Une description résumée du test et des résultats qu'il a révélés.
Impact	L'impact potentiel de la vulnérabilité, tel que l'accès non autorisé ou la perte de données.
Solution	Solution(s) potentielle(s) pour résoudre le vulnérabilité.
CVE	Le numéro d'identification des vulnérabilités et expositions communes (CVE) pour la vulnérabilité.

Date d'ajout	La date à laquelle le test a été ajouté.
Dernière modification	La date à laquelle le test a été modifié pour la dernière fois.

Cliquez sur un résultat pour voir les détails de la vulnérabilité associée au test. Pour plus d'informations sur les détails fournis par le système, voir le

4. Voir la section Détails sur la vulnérabilité du présent document.

13. Tickets

Une vulnérabilité peut se voir attribuer un ticket. Contrairement aux vulnérabilités, les tickets sont des éléments pouvant faire l'objet d'une action. Les tickets permettent à tous les utilisateurs du système de suivre le déroulement des actions entreprises pour éliminer une vulnérabilité. Les utilisateurs peuvent mettre à jour le statut d'un ticket, modifier la date d'échéance d'un ticket, ajouter des commentaires, et plus encore dans la zone des tickets.

13.1. Visualisation des tickets

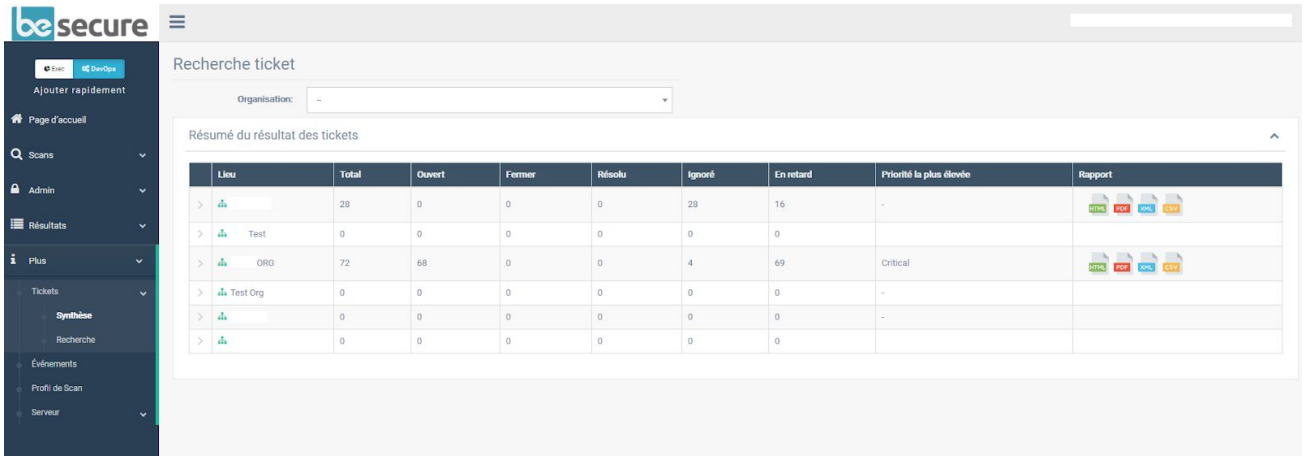
Pour consulter les tickets :

1. Connectez-vous au système beSECURE.
2. Allez à la page Plus ' tickets. Le menu s'agrandira.
3. Cliquez sur Résumé. Cela ouvrira la page Résumé des tickets.

Par défaut, la page Résumé des tickets affiche des informations pour toutes les organisations. Pour afficher les tickets d'une organisation spécifique, sélectionnez une organisation dans la liste déroulante en haut de la page. Les résultats affichent les informations suivantes pour chaque organisation :

Location	L'organisation, le scan ou l'hôte.
Total	Le nombre total de tickets.

Ouvert	Le nombre total de tickets.
Fermé	Le nombre total de tickets.
Résolu	Le nombre total de tickets.
Ignoré	Le nombre total de tickets.
En retard	Le nombre total de tickets.
Priorité la plus élevée	Le niveau de priorité du ticket le plus prioritaire.
Rapport	Contient des icônes permettant de télécharger un rapport de synthèse au format HTML, PDF, XML ou XLS.



La page de résumé des tickets.

Cliquez sur la valeur dans une cellule pour voir tous les tickets correspondants. Dans l'image ci-dessus, par exemple, en cliquant sur le nombre 45, vous obtiendrez une liste de 45 tickets ouverts pour le lieu de la démonstration.

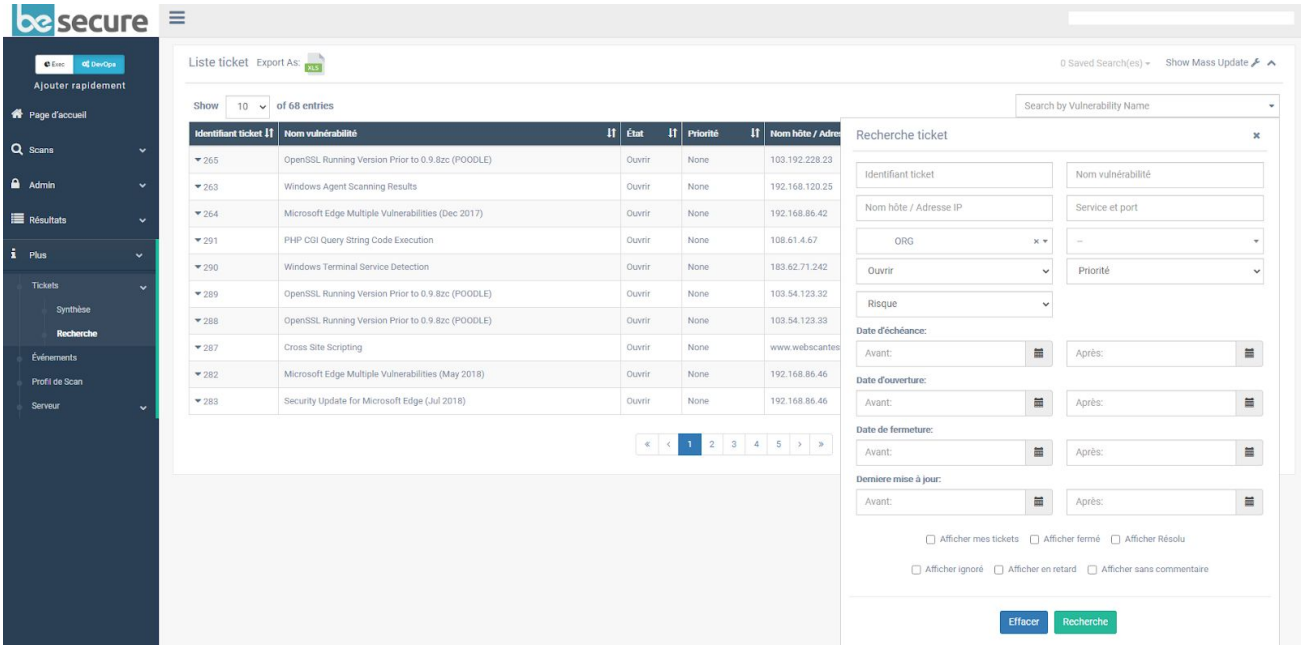
13.2. Recherche de tickets

Pour rechercher des tickets :

1. Allez à la rubrique "Autres" tickets. Le menu s'agrandira.

2. Cliquez sur Rechercher. Cela ouvrira la page Liste des tickets.

Par défaut, la page Liste des tickets affiche tous les tickets d'une organisation. La recherche de base vous permet de faire une recherche par nom de vulnérabilité en entrant du texte dans la zone de recherche en haut à droite. Pour accéder à la recherche avancée, cliquez sur la flèche à la fin de la boîte de recherche. Une fenêtre de recherche avec des options supplémentaires apparaîtra.



La page Liste des tickets, avec la recherche avancée, a été étendue.

L'écran de recherche avancée offre les options suivantes :

ID/identifiant du ticket	La carte d'identité pour le ticket.
Nom d'hôte/adresse IP	Le nom d'hôte ou l'adresse IP de l'hôte associé au ticket.
Organisation	L'organisation associée au ticket.
Statut	Le statut du ticket (ouvert, ignoré, résolu ou fermé). Pour plus d'informations, voir la section tickets de ce document.
Risque	Le niveau de risque associé à la vulnérabilité du ticket. Les valeurs sont : élevé, moyen, faible et

	aucun.
Nom de la vulnérabilité	Un nom descriptif pour la vulnérabilité.

Service et port	Le service et le port touchés par la vulnérabilité. Séparez les valeurs par des virgules. Par exemple, si vous entrez 80, 443, vous obtiendrez les résultats pour le port 80 et le port 443.
Scan	Le scan associé au ticket. Note : Une organisation doit d'abord être sélectionnée.
Priorité	L'urgence du ticket. Les valeurs sont : aucune, faible, modérée, importante et critique.
Date d'échéance	La date à laquelle le ticket est dû. Entrez les dates avant et après pour retourner les tickets dus dans un délai précis.
Date d'ouverture	La date à laquelle le ticket a été ouvert. Entrez les dates avant et après pour rendre les tickets dus dans un délai précis.
Date de clôture	La date à laquelle le ticket a été fermé. Entrez les dates avant et après pour rendre les tickets dus dans un délai précis.
Dernière mise à jour	La date de la dernière mise à jour du ticket. Indiquez les dates avant et après pour rendre les tickets dus dans un délai précis.

Montrer mes tickets	Comprend les tickets attribués à l'utilisateur actuel.
Montrer les tickets fermés	Inclus les tickets qui ont été fermés
Montrer les tickets résolus	Inclus les tickets qui ont été résolus
Montrer les tickets ignorés	Inclus les tickets qui ont été ignorés
Afficher les retards	Comprend les tickets en retard.
Afficher aucun commentaire	Afficher les tickets qui n'ont pas de commentaires décrivant l'action entreprise.

3. Si vous utilisez la recherche avancée, entrez vos critères de recherche et cliquez sur le bouton Recherche.

4. Utilisez les liens Suivant et Précédent au bas de la page pour naviguer dans vos résultats. Cliquez sur un ticket pour afficher la page Détails du ticket.

13.3. Affichage des détails du ticket

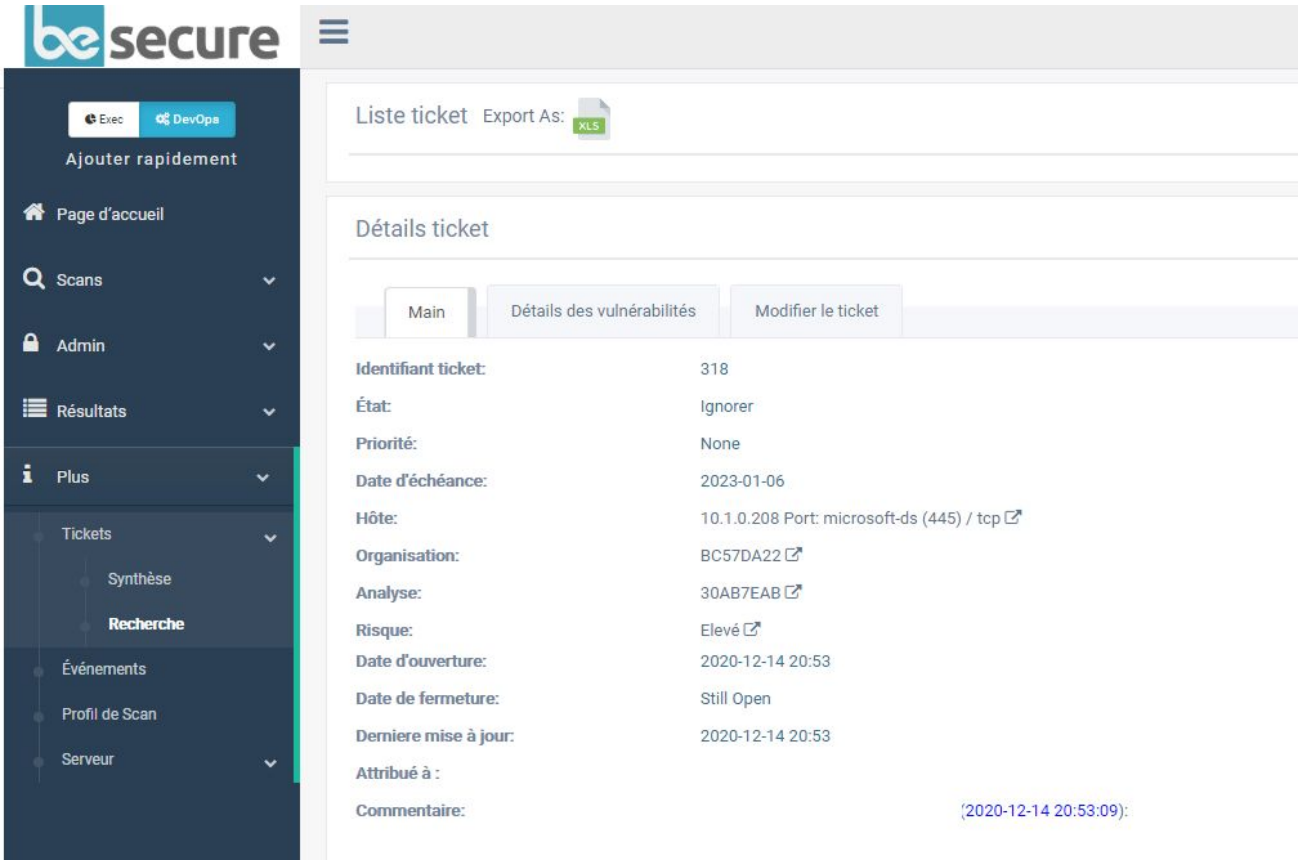
La page “Détails du ticket” affiche les informations suivantes concernant un ticket :

Identifiant/ ID du Ticket	Identifiant du ticket
Statut	Le statut du ticket (ouvert, ignoré, résolu ou fermé). Pour plus d'informations, voir la section tickets du présent document.
Priorité	L'urgence du ticket. Les valeurs sont : aucune, faible, modérée, importante et critique.

Date d'échéance	La date à laquelle le ticket est dû. Entrez les dates avant et après pour rendre les tickets dus dans un délai précis.
Hôte	Le nom d'hôte ou l'adresse IP, le port et le protocole de l'hôte associé au ticket.
Organisation	L'organisation associée au ticket.
Scan	Le scan associé au ticket. Note : Une organisation doit d'abord être sélectionnée.
Risque	Le niveau de risque associé à la vulnérabilité du ticket. Les valeurs sont : élevé, moyen, faible et aucun.

Date d'ouverture	La date à laquelle le ticket a été ouvert. Entrez les dates avant et après pour rendre les tickets dus dans un délai précis.
Date de clôture	La date à laquelle le ticket a été fermé. Entrez les dates avant et après pour rendre les tickets dus dans un délai précis.
Dernière mise à jour	La date de la dernière mise à jour du ticket. Entrez les dates avant et après pour rendre les tickets dus dans un délai précis.
Affecté à	L'adresse email de l'utilisateur à qui le ticket est attribué.

Commentaire	Un champ pour les commentaires facultatifs.



La page Détails des tickets.

Pour revenir à la liste des tickets, cliquez sur Liste des tickets en haut de l'écran.

13.4. Création des tickets

Les tickets sont créés à partir de la page Liste des vulnérabilités, plutôt que dans la zone des tickets. Un ticket peut être créé à partir de chaque vulnérabilité. Un utilisateur qui peut consulter les informations relatives à la vulnérabilité pourra également consulter le ticket.

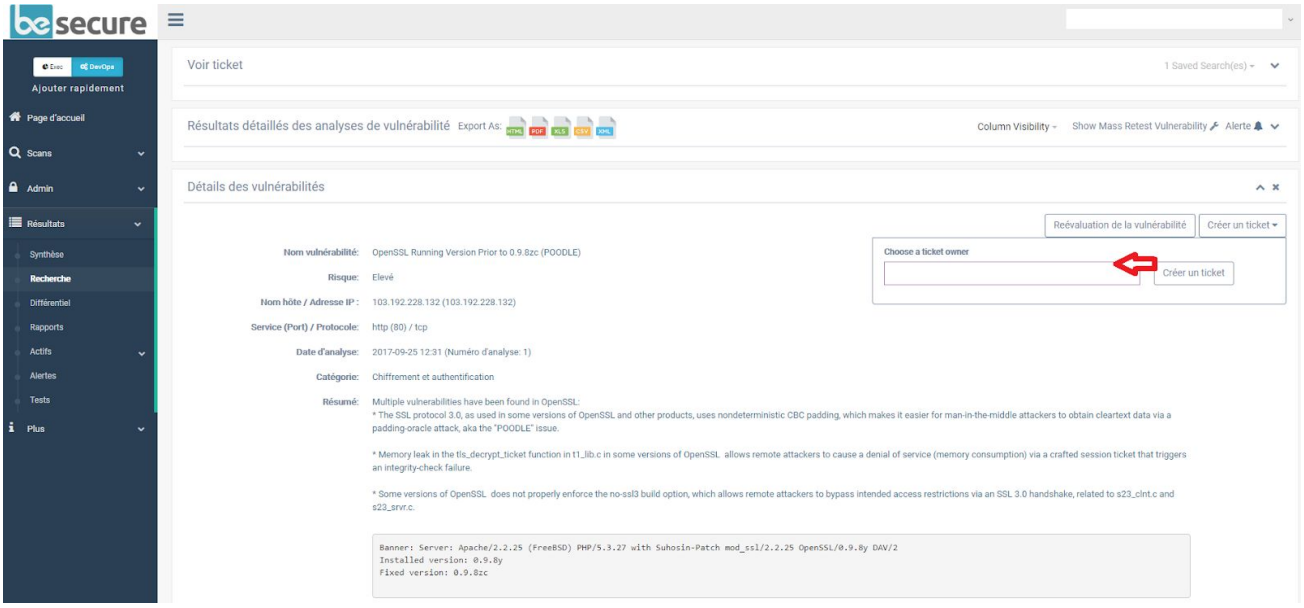
Pour créer un ticket :

1. Suivez les étapes de la section Recherche de vulnérabilités de ce document.

2. Sélectionnez une vulnérabilité dans la liste des résultats.

3. Cliquez sur le bouton Créer un ticket. Le panneau se développe.

4. Choisissez un propriétaire de ticket dans la liste déroulante et cliquez sur le nouveau bouton Créer un ticket.



Créer un nouveau ticket à partir d'une vulnérabilité.

13.5. État du ticket

Un ticket peut avoir l'un des quatre états : Ouvert, Fermé, Résolu, Ignoré, ou En retard. L'état Fermé ne peut être attribué qu'aux tickets dont les vulnérabilités ne sont plus présentes. Les tickets marqués "Ignored" ne sont pas affichés dans le système.

13.6. Priorité des tickets

Un ticket peut également se voir attribuer l'une des priorités suivantes : Aucune, Faible, Modérée, Importante ou Critique. Les tickets critiques apparaîtront en haut de la liste des tickets.

13.7. Date d'échéance des tickets

L'option date d'échéance fixe un délai pour la résolution d'une contravention. Les tickets dont la date d'échéance est dépassée apparaîtront en haut de la liste. En outre, plus la date d'échéance d'un ticket est proche de la date actuelle, plus il apparaîtra en haut de la liste.

14. Fonctions administratives

La zone d'administration du système beSECURE permet aux utilisateurs autorisés de gérer les comptes, les organisations, les contacts, les profils de sécurité, les serveurs, les alarmes et les audits. L'accès à la zone d'administration est limité aux utilisateurs ayant un compte d'utilisateur et d'administrateur. Il est disponible uniquement en mode "DevOps".

14.1. Gestion des organisations

La zone des organisations permet aux utilisateurs et aux administrateurs de créer, modifier et supprimer des organisations et de gérer les logos des organisations.

14.1.1. Création d'une organisation

Créer une nouvelle organisation :

1. Connectez-vous au système avec des privilèges administratifs.

2. Assurez-vous que le rôle DevOps est actif.

3. Allez à la page "Admin ' Organisations". Le menu se développera.

4. Cliquez sur Liste. Une liste des organisations existantes apparaîtra (le cas échéant).

5. Cliquez sur le bouton en bas à droite.

6. Remplissez le formulaire sur la page des détails de l'organisation qui apparaît. Vous devrez au minimum saisir le nom de l'organisation et indiquer si le chevauchement des plages de scan est autorisé ou non. Ces deux champs sont obligatoires. Vous pouvez également sélectionner un nom et un logo de parent. REMARQUE : Le fait de définir le chevauchement des plages de scan sur “Non autorisé” empêche les utilisateurs de scanner deux fois la même machine cible. Cela évite la confusion et les frais supplémentaires pour les scans inutiles.

7. Passez en revue les informations de l'onglet "Rapports".

a. Par défaut, l'utilisateur qui crée l'organisation devient la personne de contact. Toutefois, la personne de contact peut être modifiée à tout moment.

REMARQUE : Si un compte n'est pas associé à l'organisation, seuls les comptes ayant l'autorisation de l'administrateur pourront consulter les informations de vulnérabilité pour cette organisation et ses sous-organisations.

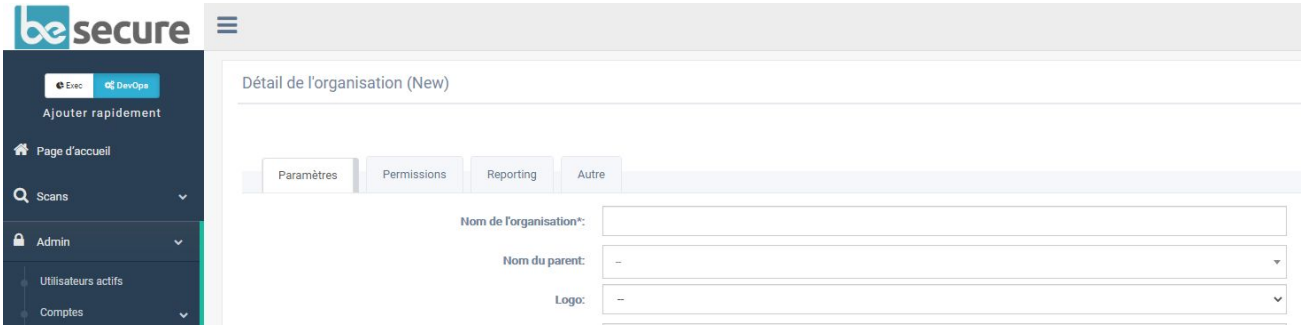
b. Les cases Début de l'analyse et Fin de l'analyse sont également cochées par défaut. Cela signifie que la personne de contact de l'organisation recevra une notification par courrier électronique chaque fois qu'une analyse

commence ou finit. Pour éviter que la personne de contact ne reçoive les notifications, décochez les cases.

8. Remplissez le formulaire de l'onglet Autres (facultatif).

a. Le champ Utilisé par indique les autres scans qui utilisent cette organisation, le cas échéant. b. Le champ Commentaire est un champ de texte libre pour la saisie de notes.

9. Cliquez sur le bouton Créer. La page Détails de l'organisation s'affiche.



La page des détails de l'organisation.

9. Entrez les informations sur l'organisation. Vous devez remplir les champs de base suivants :

Nom de l'organisation (obligatoire)	Le nom de l'organisation. Obligatoire.
Nom du parent	Le nom de la société mère de l'organisation.

Logo	Le logo de l'organisation. Choisissez dans la liste déroulante. Si aucun logo n'est attribué à une organisation, le logo par défaut du système sera utilisé.
Chevauchement des plages de scan (obligatoire	Les valeurs sont autorisées et non autorisées (par défaut). Obligatoire. REMARQUE : Réglage de la plage de scan

	Le chevauchement avec la fonction "Non autorisé" empêche les utilisateurs de scanner deux fois la même machine cible. Cela évite la confusion et les frais supplémentaires pour les scans inutiles.

14.1.2. Modification d'une organisation

Pour modifier une organisation :

1. Connectez-vous au système avec des privilèges administratifs.

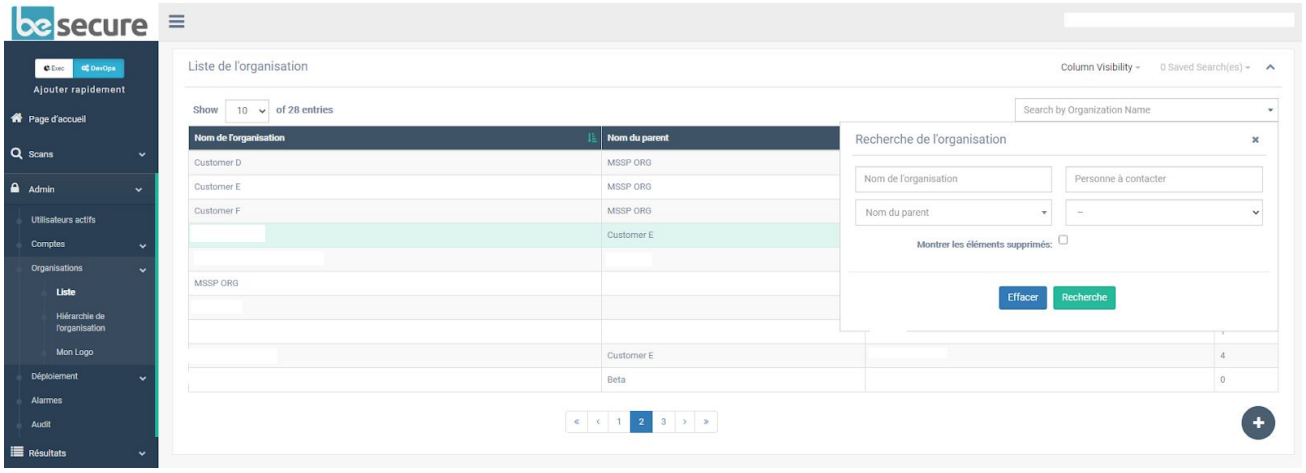
2. Assurez-vous que le rôle DevOps est actif.

3. Allez à la page "Admin ' Organisations". Le menu se développera.

4. Cliquez sur Liste. Une liste des organisations existantes apparaîtra.

5. Entrez le nom d'une organisation dans la zone de recherche en haut de l'écran pour rechercher une organisation spécifique, ou cliquez sur la flèche déroulante dans la zone de recherche pour

ouvrir les options de recherche avancée. La recherche avancée offre des options supplémentaires pour la recherche par personne de contact, par nom de parent et par logo. Si vous souhaitez inclure des organisations supprimées dans votre recherche, cochez la case Rechercher les organisations supprimées. Vous pouvez également utiliser les boutons de navigation en bas de page pour parcourir la liste des organisations.



La page de la liste des organisations, avec la recherche avancée, a été étendue.

6. Cliquez sur un résultat pour ouvrir la page Détails de l'organisation. L'onglet Paramètres est l'onglet par défaut. Les options de cet onglet vous permettent de modifier les paramètres suivants :

Nom de l'organisation (obligatoire)	Le nom de l'organisation.
Nom du parent	Le nom de la société mère de l'organisation.
Logo	Le logo de l'organisation. Choisissez dans la liste déroulante. Si le logo n'apparaît pas dans la liste, cliquez sur Admin=>Organisations=>Mon logo pour le télécharger. Les types de fichiers pris en charge sont les suivants : JPEG, BMP, SVG et GIF. La taille maximale des fichiers pouvant être téléchargés est de 1 Mo. Si une organisation ne dispose pas d'un logo qui lui est attribué, le logo du système par défaut sera utilisé.

Chevauchement des plages de scan (obligatoire)	Les valeurs sont autorisées et non autorisées (par défaut). Obligatoire. REMARQUE : Le fait de régler le chevauchement des plages de scan sur “Non autorisé” empêche les utilisateurs de scanner deux fois le même appareil cible. Cela évite la confusion et les frais supplémentaires pour les scans inutiles.

Modifier les autorisations d'une organisation

L'onglet Permissions détermine quels utilisateurs sont autorisés à modifier, changer et supprimer l'entrée de l'organisation.

Pour ajouter un nouveau propriétaire à une organisation, cliquez sur le nom d'utilisateur dans la partie disponible de la section Propriété. Cette entité sera alors déplacée vers la zone Assigned. Pour supprimer un propriétaire actuel, cliquez sur le X à la fin de la case verte dans la zone Assigned. Cela ramènera cette entité dans la section Disponible.

Pour ajouter une nouvelle association, cliquez sur le nom d'utilisateur dans la partie disponible de la section Associations. Cette entité sera alors déplacée vers la zone Assigned. Pour supprimer un propriétaire actuel, cliquez sur le X à la fin de la case verte dans la zone Assigned. Cela ramènera cette entité dans la section Disponible.

Modification de la personne de contact et des notifications d'une organisation

Vous pouvez modifier la personne de contact et les notifications qu'elle reçoit dans la zone Détails de l'organisation. Pour ce faire, cliquez sur l'onglet Rapports. Cet onglet vous permettra de sélectionner une autre personne de contact dans la liste déroulante, ou de cocher/décocher les

options de notification disponibles pour la personne de contact (lorsqu'un scan commence ou se termine).

14.1.3. Suppression d'une organisation

Le système beSECURE vous permet de supprimer une organisation en cas d'erreur de saisie, de changement de structure de l'entreprise ou d'événement similaire.

Pour supprimer une organisation :

1. Connectez-vous au système avec des privilèges administratifs.

2. Assurez-vous que le rôle DevOps est actif.

3. Allez à la page "Admin ' Organizations". Le menu se développera.

4. Cliquez sur Liste. Une liste des organisations existantes apparaîtra.

5. Entrez le nom d'une organisation dans la zone de recherche en haut de l'écran pour rechercher une organisation spécifique, ou cliquez sur la flèche dans la zone de recherche pour ouvrir les options de recherche avancée. La recherche avancée offre des options supplémentaires pour la recherche par personne de contact, nom du parent et logo. Vous pouvez également utiliser les boutons de navigation en bas de page pour parcourir la liste des organisations. 6. Sélectionnez une organisation dans les résultats de la recherche.

7. Cliquez sur le bouton Supprimer en haut à droite de la page Détails de l'organisation.

REMARQUE : Toute tentative de suppression d'une organisation utilisée par d'autres parties actives dans le système sera refusée et le message d'erreur suivant apparaîtra : "Impossible de supprimer l'élément car il est associé à un ou plusieurs éléments". Cliquez sur le signe "plus" dans la zone de message d'erreur pour afficher les entités du système qui utilisent activement l'organisation.

14.1.4. Restauration d'une organisation

Pour rétablir une organisation qui a été supprimée par erreur :

1. Connectez-vous au système avec des privilèges administratifs.

2. Assurez-vous que le rôle DevOps est actif.

3. Allez à la page "Admin ' Organizations". Le menu se développera.

4. Cliquez sur Liste. Une liste des organisations existantes apparaîtra.

5. Cliquez sur la flèche déroulante dans la boîte de recherche pour ouvrir la recherche avancée.

6. Cochez la case Afficher la suppression.

7. Lancez une recherche pour l'organisation.

8. Sélectionnez l'élément supprimé approprié dans les résultats de la recherche. 9. Cliquez sur le signe plus pour afficher la page des détails de l'organisation. 10. Cliquez sur le bouton "Annuler la suppression".

14.2. Gestion des profils de compte

Un profil de compte définit un rôle d'utilisateur. Chaque nouvel utilisateur se voit attribuer un profil de compte qui détermine ses autorisations sur le système beSECURE. Il existe trois profils de compte par défaut :

Administrateur	Les utilisateurs ayant ce profil de compte ont un accès complet au système.
Utilisateur des scans	Les utilisateurs de scanners ne peuvent gérer que les éléments auxquels l'administrateur ou l'utilisateur qui les a créés leur a spécifiquement donné accès.

Utilisateur des rapports	Les utilisateurs de rapports ont un accès en lecture seule aux résultats de scan, aux actifs et aux tickets.

Un profil de compte peut être associé à une ou plusieurs organisations, et peut posséder plusieurs objets (comptes, scanners, contacts, etc.) dans le système. Cela permet aux utilisateurs possédant ce profil d'accéder aux objets spécifiés. Si un utilisateur se voit accorder la propriété d'un objet qui appartient déjà à son profil, cette propriété ne sera pas effective.

Tous les comptes ayant un profil de compte spécifique auront les mêmes privilèges, associations et propriétés. Par exemple, le groupe A, ayant la propriété du paramètre de scan C, donnera l'autorisation à tout utilisateur appartenant au groupe A. Vous pouvez créer, afficher et modifier les profils de compte dans la zone de fichiers de Account Pro.

14.2.1. Création d'un profil de compte

Pour créer un nouveau profil de compte :

1. Connectez-vous au système avec des privilèges administratifs.

2. Assurez-vous que le rôle DevOps est actif.

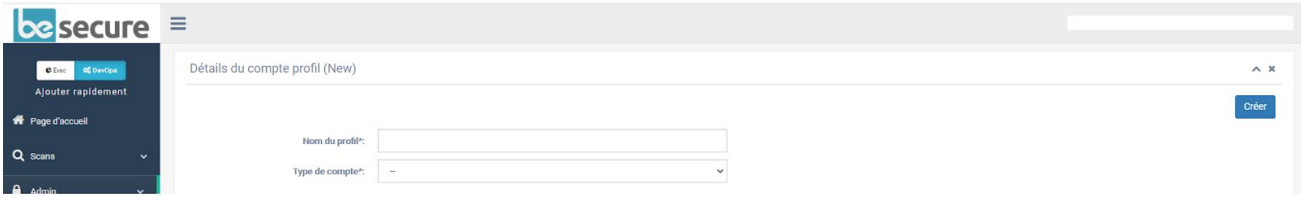
3. Allez dans Admin ' Comptes ' Profils de compte.

4. Cliquez sur le bouton en bas à droite.

5. Remplissez le formulaire d'informations de base qui apparaît. Les champs disponibles sont les suivants :

Nom du profil (obligatoire)	Un nom pour le profil du compte.
Détails du profil du compte	Le type de profil, ou les autorisations associées au profil du compte. Les valeurs sont l'utilisateur rapporteur, l'utilisateur de scan et l'administrateur. Cette valeur ne peut pas être modifiée après la création du profil de compte. Un utilisateur ne peut pas créer un compte avec des privilèges supérieurs aux siens.

6. Cliquez sur le bouton "Créer".



La page Détails du profil du compte.

14.2.2. Modification d'un profil de compte

Pour modifier un profil de compte :

1. Connectez-vous au système avec des privilèges administratifs.

2. Assurez-vous que le rôle DevOps est actif.

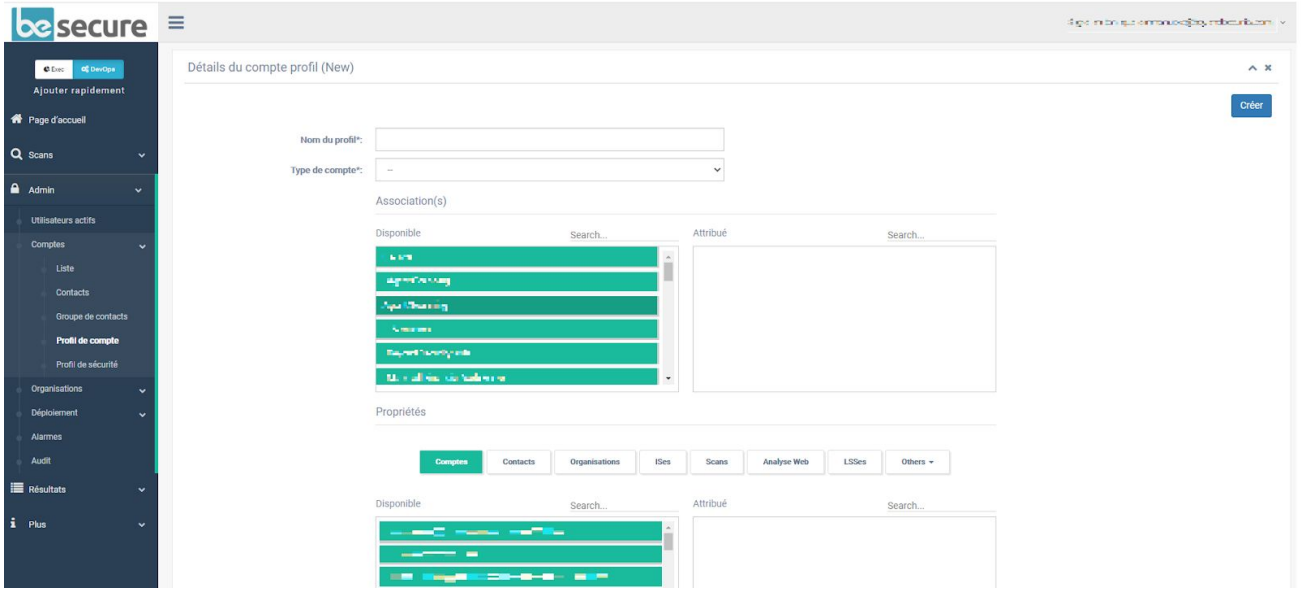
3. Allez dans Admin ' Comptes ' Profils de compte. Une liste des profils de compte existants apparaîtra. Saisissez le texte dans la zone de recherche en haut à droite pour effectuer une recherche par nom de profil. Vous pouvez également utiliser les boutons de navigation en bas de page pour parcourir la liste des profils de compte.

4. Sélectionnez un profil de compte dans la liste.

5. Modifiez les paramètres de base du profil de compte (Nom du profil, Utilisé par et Commentaire) dans l'onglet Paramètres (facultatif).

6. Cliquez sur l'onglet Permissions pour modifier les permissions du profil de compte. Si le profil de compte a un ou plusieurs gestionnaires, ceux-ci apparaîtront dans la zone Assigné. Pour ajouter un nouveau gestionnaire, cliquez sur le nom d'utilisateur dans la partie Disponible de la section Propriété. Cette entité sera alors déplacée vers la zone Assigned. Pour supprimer un gestionnaire actuel, cliquez sur le X à la fin de la case verte dans la zone Assigné. Cela ramènera cette entité dans la section Disponible.

7. Modifiez les associations sous la section Propriété (facultatif). La section Associations détermine quels utilisateurs et administrateurs peuvent accéder aux résultats de l'analyse de leur organisation mère. Un profil de compte sans propriétaire assigné sera automatiquement la propriété de toute compte de l'administrateur dans le système.



L'onglet Permissions de la page Détails du profil du compte.

8. Cliquez sur le bouton Modifier.

14.2.3. Suppression d'un profil de compte

Pour supprimer un profil de compte :

1. Connectez-vous au système avec des privilèges administratifs.

2. Assurez-vous que le rôle DevOps est actif.

3. Allez dans Admin ' Comptes ' Profils de compte. Une liste des profils de compte existants apparaîtra. Saisissez le texte dans la zone de recherche en haut à droite pour effectuer une recherche par nom de profil. Vous pouvez également utiliser les boutons de navigation en bas de page pour parcourir la liste des profils de compte.

4. Sélectionnez un profil de compte dans la liste.

5. Cliquez sur le bouton Supprimer.

REMARQUE : Un profil de compte utilisé par d'autres parties actives dans le système beSECURE ne peut pas être supprimé. Le message d'erreur suivant apparaîtra : "Impossible de supprimer l'élément car il est associé à un ou plusieurs éléments". Cliquez sur le signe "plus" dans la zone de message d'erreur pour afficher les entités qui utilisent activement le profil de compte.

14.2.4. Restauration d'un profil de compte

Pour restaurer un profil de compte qui a été supprimé par erreur :

1. 1. Connectez-vous au système avec des privilèges administratifs.

2. Assurez-vous que le rôle DevOps est actif.

3. Cliquez sur Admin ' Comptes ' Profils de compte. Une liste des profils de compte existants apparaîtra. 4. Cliquez sur la flèche déroulante dans la zone de recherche pour ouvrir la recherche avancée. 5. Cochez la case Afficher les suppressions.

6. Cliquez sur le bouton Rechercher.

7. Sélectionnez l'élément supprimé approprié dans la liste des résultats.

8. Cliquez sur le bouton Annuler la suppression.

14.3. Gestion des profils de sécurité

Un profil de sécurité définit les paramètres de sécurité d'un compte, tels que la force du mot de passe et la durée de la session. Les utilisateurs disposant de privilèges administratifs peuvent consulter des informations sur les profils de sécurité et en créer de nouveaux dans la zone Profils de sécurité.

14.3.1. Création d'un profil de sécurité

Pour créer un profil de sécurité :

1. Assurez-vous que le rôle DevOps est actif.

2. Allez à la page "Admin ' Comptes ' Profils de sécurité".

3. Cliquez sur le bouton en bas à droite et remplissez le formulaire qui apparaît. Le formulaire comporte les champs suivants :

Nom du profil (obligatoire)	Un nom pour le profil de sécurité.
Expiration du mot de passe (obligatoire)	Le nombre de jours avant l'expiration des mots de passe des comptes associés à ce profil de sécurité.
Longueur du mot de passe (obligatoire)	La longueur du mot de passe requise.
Premier changement de mot de passe de connexion (obligatoire)	La valeur par défaut est de 30.
Durée de verrouillage en cas d'échec du mot de passe (obligatoire)	Le nombre de tentatives de connexion échouées avant qu'un compte ne soit verrouillé. La valeur par défaut est de 3.
Commentaire	Un champ pour les commentaires facultatifs.

4. Cliquez sur le bouton "Créer".

Nous espérons que ce guide vous a permis de mieux comprendre le fonctionnement de la plateforme beSECURE. Pour toute question, n'hésitez pas à nous contacter à l'adresse email suivante : support@beyondsecurity.com