Télécharger des règles IDS personnalisées

Publié: 2024-01-22

Vous pouvez télécharger un ensemble personnalisé de règles IDS vers les capteurs IDS ExtraHop. Le système ExtraHop convertit les règles en types de détection qui génèrent des détections que vous pouvez consulter et examiner.

Ajoutez des règles formatées conformément aux directives de Suricata à un ou plusieurs fichiers .rules et téléchargez-les dans un fichier .zip. Lors du téléchargement, le système ExtraHop traite chaque règle, qui est affichée dans un tableau qui affiche l'ID de signature, le nom de chaque règle et l'un des statuts de règle suivants.

• **Accepté:** Le système ExtraHop a correctement traité la règle.

• **Rejeté:** Le système ExtraHop n'a pas pu traiter la règle. La règle peut contenir une erreur de mise en forme ou contenir une action, un protocole ou une option qui n'est pas actuellement pris en charge par le système ExtraHop. Contacter Assistance ExtraHop pour vous renseigner sur la prise en charge future de la règle.

• **Mise à niveau requise:** UNE une version plus récente du firmware ExtraHop est requise pour soutenir la règle. La version du système requise s' affiche.

Voici quelques considérations concernant les règles IDS personnalisées :

- Les règles IDS personnalisées doivent être formatées comme étant valides Fichier Suricata .rules.
- Un ou plusieurs fichiers Suricata .rules doivent être ajoutés à un seul fichier .zip pour le téléchargement.
- Vous ne pouvez pas télécharger plus de 10 000 règles IDS personnalisées.
- La suppression d'un fichier entraîne la suppression de toutes les règles associées au fichier chargé et peut prendre plusieurs minutes. Les utilisateurs peuvent continuer à voir des détections basées sur ces règles jusqu'à ce que la suppression soit terminée.
- Le remplacement d'un fichier supprime toutes les règles associées au fichier précédemment chargé, puis traite les règles du nouveau fichier.
- Les règles IDS intégrées ne sont ni supprimées ni remplacées lorsque vous gérez vos règles IDS personnalisées. Votre système ExtraHop est connecté à ExtraHop Cloud Services et les dernières règles intégrées sont automatiquement téléchargées sur le système lorsque des versions mises à jour sont disponibles.

  Note: ExtraHop peut revoir les règles téléchargées afin de vérifier l' exactitude des conversions et de guider l'amélioration du produit en termes de conversion, d'exactitude et de performances des règles Suricata.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône Paramètres système puis cliquez sur **Règles IDS personnalisées**.
3. Cliquez **Télécharger un fichier**.
4. Cliquez **Choisissez un fichier**, sélectionnez le fichier .zip de votre choix, puis cliquez sur **Télécharger un fichier**.
   Le processus de téléchargement peut prendre plusieurs minutes. L'état du fichier et ses horodatages sont mis à jour une fois le traitement terminé.

Prochaines étapes

Cliquez **Détections** depuis la page du menu de navigation supérieure pour afficher les détections générées à partir de règles IDS personnalisées. Ces détections indiquent que la règle a été fournie par un fichier IDS personnalisé et inclut l'ID de signature de la règle.