

Spécifiez les localités du réseau et les domaines de confiance

Publié: 2024-01-31

En fournissant des détails sur les spécifications de votre réseau, vous pouvez améliorer les mesures et les détections générées par votre système ExtraHop. La page Localités du réseau vous permet de spécifier des adresses IP internes et externes et d'ajouter des domaines fiables auxquels vos appareils se connectent régulièrement.


Voici quelques considérations importantes concernant ces paramètres :

- Si votre déploiement ExtraHop inclut une console, nous vous recommandons de [gestion des transferts](#) de tous les capteurs connectés à la console.
- Pour ExtraHop Reveal (x) 360, ces paramètres sont synchronisés sur tous les capteurs connectés . Vous ne devez pas configurer ces paramètres sur des capteurs individuels.
- Pour ExtraHop Reveal (x) Enterprise, lorsque vous transférez la gestion vers une console connectée, ces paramètres sont synchronisés sur tous les capteurs. Dans le cas contraire, les paramètres de localisation du réseau doivent être configurés sur tous les capteurs et consoles.
- Vous devez avoir une écriture complète [privilèges](#) pour modifier ces paramètres.

 Consultez la formation associée : [Configurer les localités du réseau](#)

Spécifier une localité du réseau

Les localisations du réseau vous permettent de classer le trafic provenant des adresses IP et des blocs CIDR comme étant interne ou externe à votre réseau. Vous pouvez également spécifier un nom pour chaque localité, tel que « DMZ » ou « réseau invité », et filtrer par ce nom dans les appareils et les enregistrements.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système  puis cliquez sur **Localités du réseau**.
3. Cliquez **Ajouter une localité de réseau**.
4. Dans le champ Nom de la localité du réseau, saisissez un nom unique.
5. Dans la section Type de localité du réseau, sélectionnez Interne ou Externe, en fonction de la classification que vous souhaitez appliquer aux adresses IP et aux blocs CIDR.
6. Dans le champ Adresses IP et blocs CIDR, tapez les adresses IP et les blocs CIDR que vous souhaitez ajouter à la localité. Vous devez saisir une plage unique d' adresses ou de blocs.
7. Optionnel : Dans le Descriptif champ, saisissez des informations sur la localité du réseau.
8. Cliquez **Enregistrer**.
9. Pour ajouter d'autres entrées, cliquez sur **Ajouter une localité de réseau**.

Prochaines étapes

- Filtrez les appareils en sélectionnant Interne ou Externe comme type de localité réseau dans le filtre à trois champs.
- Filtrez les appareils en spécifiant le nom de la localité du réseau dans le filtre à trois champs.
- Explorez une métrique par client, serveur ou adresse IP et sélectionnez Interne ou Externe comme localité du réseau dans le filtre à trois champs.
- Filtrez les enregistrements en spécifiant l'un des filtres suivants :
 - Nom de la localité du réseau
 - Nom de la localité du réseau client
 - Nom de la localité du réseau du serveur
 - Nom de la localité du réseau de l'expéditeur

- Nom de la localité du réseau du récepteur

Ajouter un domaine sécurisé

Certaines détections sont générées lorsqu'un équipement établit une connexion à un domaine externe. Si vous savez qu'un domaine est légitime, ajoutez-le à la liste des domaines approuvés et les futures détections ciblant les activités malveillantes du domaine seront supprimées pour ce domaine.

Pour les détections associées à un domaine, vous pouvez également [ajouter un domaine sécurisé directement depuis une carte de détection](#).



Note: Si votre système ExtraHop inclut une console et que ce système est configuré pour gérer les paramètres de réglage, ces domaines sécurisés s'appliqueront à tous les capteurs connectés.

Network Localities Save

CIDR Blocks

Network localities enable you to specify a range of IP addresses in CIDR notation that is internal or external to your network. If you have a Command appliance, you must configure these settings on the Command appliance and on all connected sensors.

Network ✕
 Internal External

Description

[Add CIDR](#)

Trusted Domains

Add a trusted domain to suppress detections that specifically target activity with potentially-malicious domains.

2 domains Remove All

✕
 ✕

[Add Domain](#)

This Command appliance manages shared settings for 1 of 2 connected sensors.

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Localités du réseau**.
3. Sous Domaines fiables, cliquez **Ajouter un domaine**.
4. Entrez un nom de domaine fiable.
Le nom de domaine doit correspondre exactement au domaine que vous souhaitez supprimer. Les Wildcards et les Regex ne sont pas pris en charge. Pour ajouter plusieurs noms de domaine fiables, cliquez sur **Ajouter un domaine**. Entrez un seul nom de domaine par champ.
5. Cliquez **Enregistrer**.