Ajoutez un certificat fiable à votre système ExtraHop

Publié: 2024-08-09

Votre système ExtraHop ne fait confiance qu'aux homologues qui présentent un certificat TLS (Transport Layer Security) signé par l'un des certificats système intégrés et par tous les certificats que vous chargez. Les cibles SMTP, LDAP, HTTPS ODS et MongoDB ODS, ainsi que les connexions à l'espace de stockage des enregistrements Splunk peuvent être validées par le biais de ces certificats.

Avant de commencer
Vous devez vous connecter en tant qu'utilisateur disposant de privilèges d'installation ou de système et accéder à l'administration pour ajouter ou supprimer des certificats fiables.

Lors du téléchargement d'un certificat sécurisé personnalisé, un chemin de confiance valide doit exister entre le certificat téléchargé et une racine auto-signée approuvée pour que le certificat soit totalement fiable. Téléchargez l'intégralité de la chaîne de certificats pour chaque certificat sécurisé ou (de préférence) assurez-vous que chaque certificat de la chaîne a été téléchargé vers le système de certificats fiables.

> **Important:** Pour faire confiance aux certificats système intégrés et à tous les certificats chargés, vous devez également activer le chiffrement SSL/TLS ou STARTTLS et la validation des certificats lors de la configuration des paramètres du serveur externe.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres réseau section, cliquez sur **Certificats fiables**.
3. Optionnel : Si vous voulez faire confiance aux certificats intégrés inclus dans le système ExtraHop, sélectionnez **Certificats du système de confiance**, puis cliquez sur **Enregistrer**.
4. Pour ajouter votre propre certificat, cliquez **Ajouter un certificat** puis dans Certificat champ, collez le contenu de la chaîne de certificats codée PEM.
5. Dans le Nom dans le champ, saisissez un nom.
6. Cliquez **Ajouter**.