Ajoutez un certificat fiable à votre système ExtraHop

Publié: 2024-04-10

Votre système ExtraHop ne fait confiance qu'aux pairs qui présentent un certificat TLS (Transport Layer Security) signé par l'un des certificats système intégrés et par tout certificat que vous téléchargez. 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 d'administration du système et des accès pour ajouter ou supprimer des certificats sécurisés.

Lors du téléchargement d'un certificat sécurisé personnalisé, un chemin de confiance valide doit exister entre le certificat téléchargé et une racine autosignée fiable 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 dans le système de certificats sécurisés.

Important: Pour faire confiance aux certificats système intégrés et aux certificats téléchargés, 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 Réglages réseau section, cliquez **Certificats fiables**.
3. Optionnel : Le système ExtraHop est livré avec un ensemble de certificats intégrés. Sélectionnez **Certificats du système de confiance** si vous souhaitez faire confiance à ces certificats, puis cliquez sur **Enregistrer**.
4. Pour ajouter votre propre certificat, cliquez sur **Ajouter un certificat** puis collez le contenu de la chaîne de certificats codée PEM dans Certificat champ
5. Entrez un nom dans le Nom champ et cliquez **Ajouter**.