Suivez une détection

Publié: 2023-10-24

Le suivi des détections vous permet d'attribuer des utilisateurs, de définir un statut et d'ajouter des notes à une carte de détection.

Vous pouvez également filtrer votre affichage des détections par statut spécifique ou par personne assignée.

Avant de commencer
Les utilisateurs doivent avoir une écriture limitée privilèges ou une version supérieure pour effectuer les tâches décrites dans ce guide.

Vous pouvez attribuer le statut de responsable à n'importe quel utilisateur du système, ajouter des notes et définir l'état d'une détection comme suit :

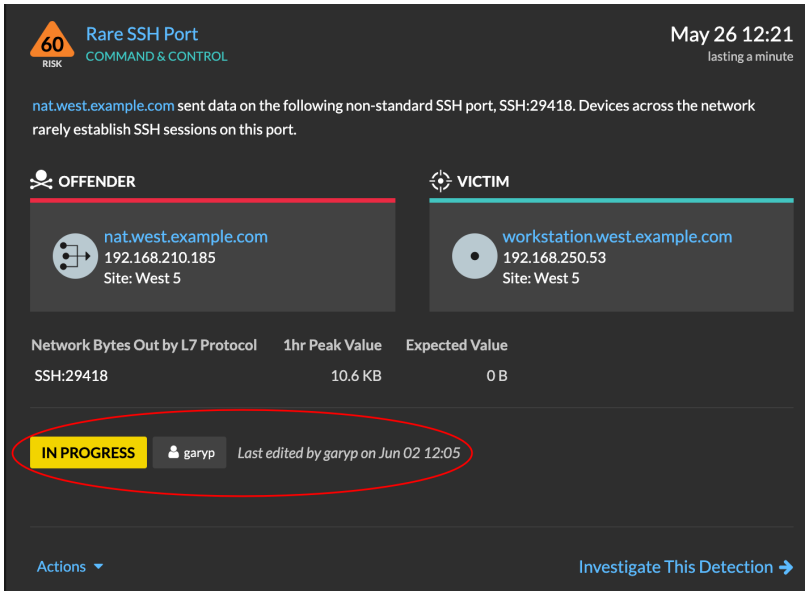
Ouvert
La détection n'a pas été revue.

Reconnaître
La détection a été constatée et doit être priorisée pour le suivi.

En cours
La détection a été attribuée à un membre de l'équipe et est en cours de révision.

Fermé - Mesures prises
La détection a été revue et des mesures ont été prises pour faire face au risque potentiel.

Fermé - Aucune mesure n'a été prise
La détection a été revue et n'a nécessité aucune action.



Voici quelques considérations importantes concernant le suivi des détections :

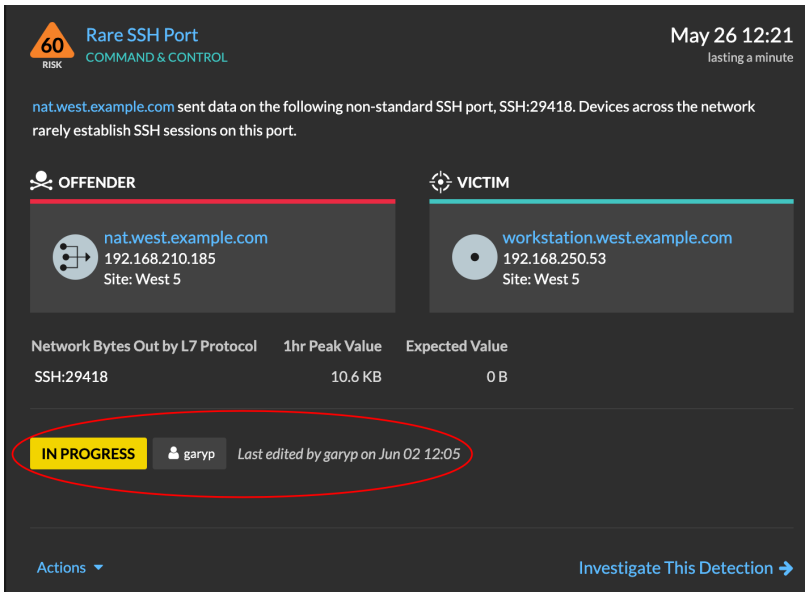
- Le statut Reconnu ou Fermé ne masque pas la détection.
- L'état de détection peut être mis à jour par n'importe quel utilisateur privilégié.
- En option, vous pouvez configurer le suivi des détections avec un système tiers.
- Si vous effectuez actuellement le suivi des détections à l'aide d'un système tiers, vous ne verrez pas le suivi des détections ExtraHop tant que vous n'aurez pas modifié le paramètre dans le Administration paramètres.

© 2023ExtraHop Networks, Inc. Tous droits réservés.

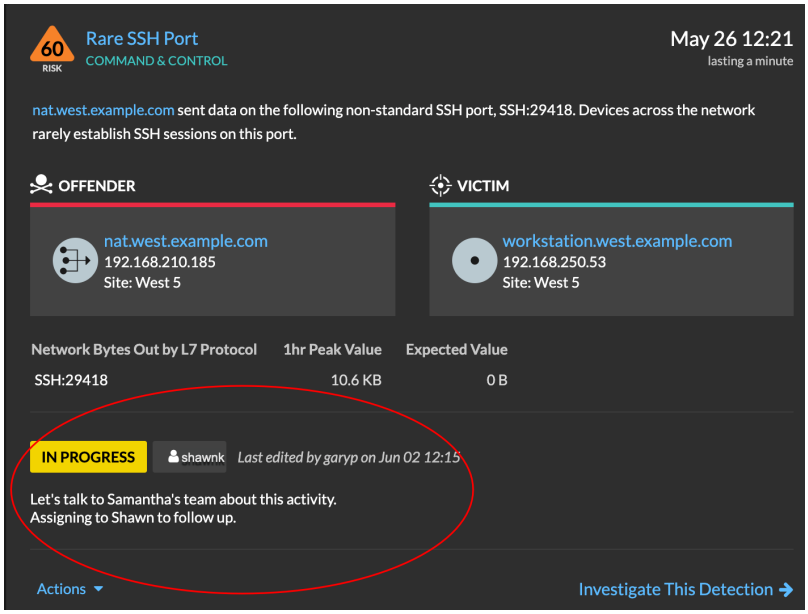
Pour suivre une détection, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez **Des actions** depuis le coin inférieur gauche de la carte de détection.
4. Optionnel : Cliquez sur un état de détection pour l'ajouter à la détection.

Option	Description
Reconnaître	La détection a été constatée et doit être priorisée pour le suivi.
En cours	La détection a été attribuée à un membre de l'équipe et est en cours de révision.
Fermé - Mesures prises	La détection a été revue et des mesures ont été prises pour faire face au risque potentiel.
Fermé - Aucune mesure n'a été prise	La détection a été revue et n'a nécessité aucune action.



5. Cliquez **Détection de pistes...** pour définir l'état de détection, attribuer la détection à un utilisateur et ajouter des notes à la carte de détection.



À partir du **Des actions** menu déroulant, sélectionnez **Détection de pistes...** et puis **Ouvert** pour supprimer le statut de la détection ; le responsable et les notes restent visibles.

Suivez une détection à partir d'une carte de détection

Vous pouvez suivre une détection en ajoutant un responsable, un statut et des notes à partir d'une carte de détection .

Pour suivre une détection, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.
3. Cliquez **Des actions** depuis le coin inférieur gauche de la carte de détection.
4. Optionnel : Cliquez sur un état de détection pour l'ajouter à la détection.
5. Cliquez **Détection de pistes...** pour définir l'état de détection, attribuer la détection à un utilisateur et ajouter des notes à la carte de détection.

   À partir du **Des actions** menu déroulant, sélectionnez **Détection de pistes...** et puis **Ouvert** pour supprimer le statut de la détection ; la personne assignée et les notes restent visibles.

Suivez un groupe de détections à partir d'un résumé des détections

Vous pouvez appliquer un statut, une personne assignée ou une note à plusieurs détections en même temps à partir du panneau récapitulatif de la page Détections.

Un panneau récapitulatif apparaît lorsque les détections sont regroupées par type dans la vue récapitulative de la page Détections.

Pour suivre un groupe de détections à partir d'un résumé des détections, procédez comme suit :

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. En haut de la page, cliquez sur **Détections**.

   Par défaut, la page doit être en mode récapitulatif avec les détections groupées par type. Si ce n'est pas le cas, cliquez sur le Vue récapitulative et ensuite groupe par type.
3. Cliquez sur un type de détection dans votre liste de détections.

4. Cliquez sur les critères selon lesquels vous souhaitez filtrer : participants, propriétés ou localités du réseau.
5. Dans le coin inférieur gauche du panneau récapitulatif, cliquez sur **Suivez toutes les détections**.

   Le lien indiquera le nombre de détections que vous êtes en train de mettre à jour. Par exemple, suivez les 14 détections. Ce lien n'apparaît pas dans le panneau récapitulatif si le filtre d' état masqué est appliqué.
6. Optionnel : Sélectionnez le statut que vous souhaitez appliquer à toutes les détections sélectionnées.
7. Optionnel : Sélectionnez le responsable que vous souhaitez appliquer à toutes les détections sélectionnées.
8. Optionnel : Indiquez si vous souhaitez ajouter une nouvelle note aux notes existantes des détections sélectionnées ou remplacer toutes les notes existantes.

   Lorsque vous ajoutez votre note à des notes existantes, la nouvelle note est ajoutée au-dessus des notes existantes.
9. Cliquez **Enregistrer**.