Examiner les détections de performances

Publié: 2023-09-19

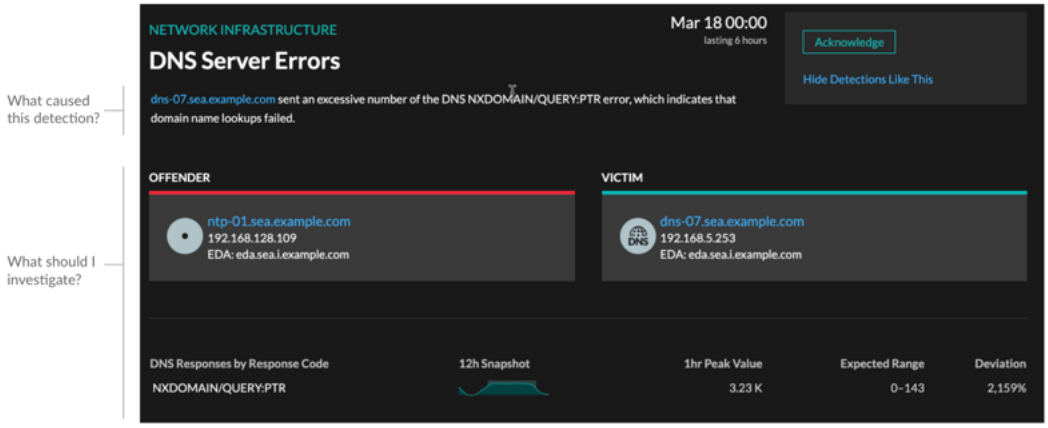
Lorsqu'une détection intéressante apparaît, vous devez vérifier si le comportement détecté indique un problème de faible priorité ou un problème potentiel. Vous pouvez commencer votre enquête directement à partir de la fiche de détection, qui fournit des liens vers les données de l'ensemble du système ExtraHop.

Il existe un certain nombre d'outils qui peuvent vous aider à filtrer votre vue pour voir les détections que vous voulez prioriser pour l'investigation. Pour commencer, recherchez les tendances suivantes :

- Certaines détections se sont-elles produites à des moments inhabituels ou inattendus, comme l'activité des utilisateurs pendant les week-ends ou après les heures de bureau ?
- Des détections apparaissent-elles en groupes importants sur la ligne du temps ?
- Des détections apparaissent-elles pour des points d'extrémité de grande valeur ?
- Les dispositifs détectés participent-ils également à d'autres détections ?

Commencez votre enquête

Examinez le titre et le résumé de la détection pour savoir ce qui l'a provoquée.



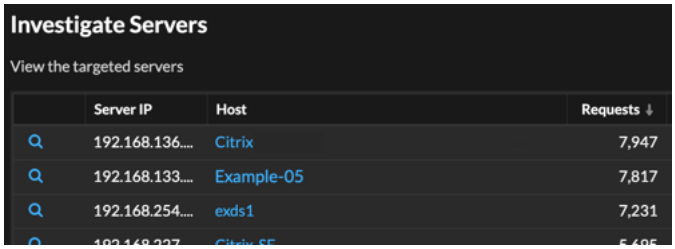
Affinez votre enquête

Les cartes de détails de la détection présentent des données relatives à la détection. La disponibilité des données dépend des appareils et des mesures associés à la détection. Après avoir cliqué sur un lien, vous pouvez revenir à la carte de détection en cliquant sur le nom de la détection dans le chemin de navigation. Chaque option d'investigation est décrite dans les sections ci-dessous.

Examiner les données d'enquête

La plupart des données dont vous avez besoin pour comprendre, valider et examiner une détection sont affichées sur la page des détails de la détection : tableaux des données métriques pertinentes, transactions d'enregistrement et liens vers les paquets bruts.

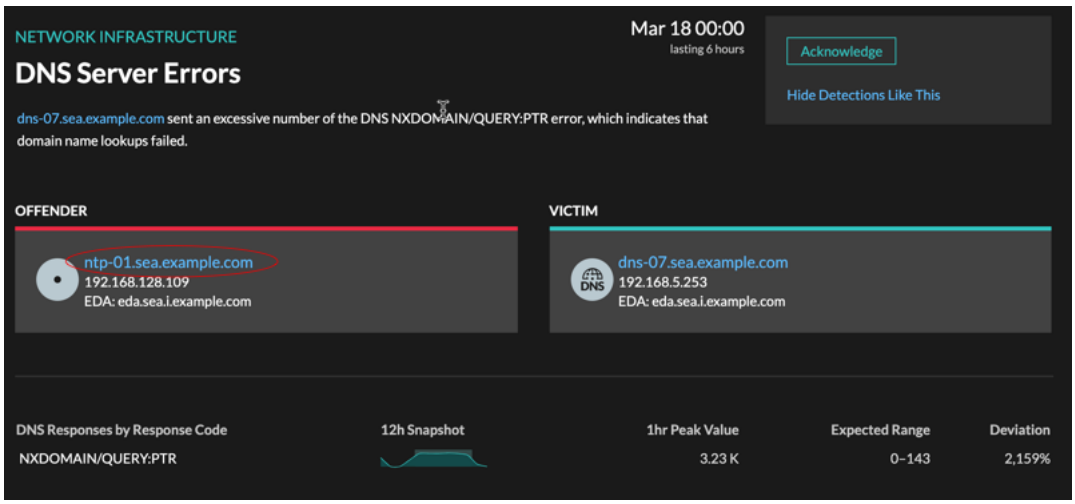
Cliquez sur le nom d'un hôte pour accéder à la page de présentation des périphériques, ou cliquez avec le bouton droit de la souris pour créer un graphique avec ce périphérique comme source et les paramètres pertinents.



Nom du périphérique

Cliquez sur le nom d'un appareil pour accéder à la page Présentation des appareils, qui contient le rôle, les utilisateurs et les balises associés à cet appareil. Dans le volet de gauche, cliquez sur le nom d'un protocole pour afficher toutes les mesures de protocole associées à ce dispositif. La page des protocoles vous donne une image complète de ce que faisait cet appareil au moment de la détection.

Par exemple, si vous recevez une détection concernant des échecs de transaction de base de données, vous pouvez en savoir plus sur les autres activités associées au serveur hébergeant l'instance de base de données.



Disponibilité

Les liens vers les noms de périphériques ne sont disponibles que pour les périphériques qui ont été automatiquement découverts par le système ExtraHop. Les appareils distants situés en dehors de votre réseau sont représentés par leur adresse IP.

Carte d'activité

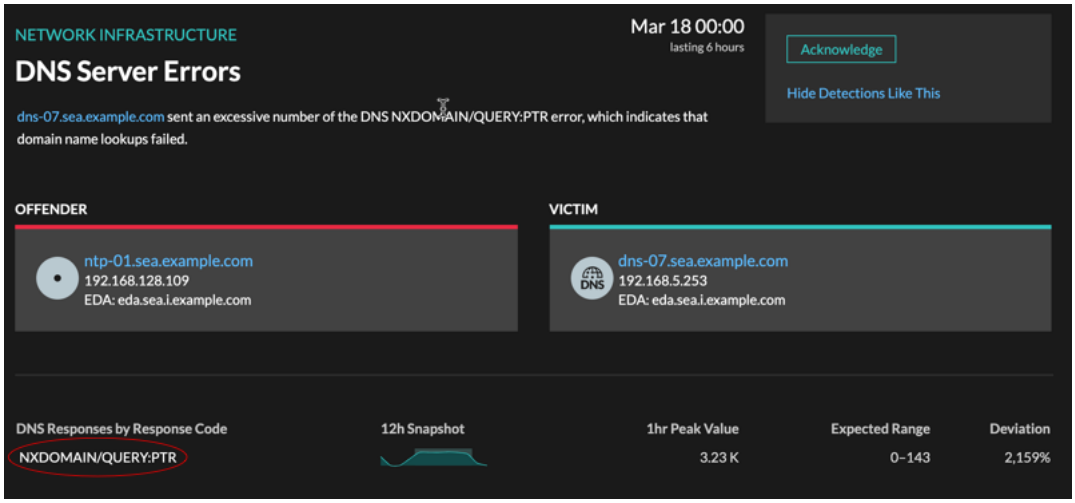
Cliquez sur l'icône Carte d'activité à côté du nom d'un périphérique pour afficher les connexions du périphérique par protocole pendant la durée de la détection. Par exemple, si vous recevez une détection d'erreurs d'authentification LDAP, vous pouvez créer une carte d'activité pour savoir quels périphériques étaient connectés à un serveur LDAP lors de la détection.

Disponibilité

Une carte d'activité est disponible lorsqu'un client ou un serveur unique est associé à une activité de protocole L7 inhabituelle, telle qu'un nombre élevé d'erreurs HTTP ou de délais d'attente pour les requêtes DNS.

Exploration des métriques détaillées

Cliquez sur un lien de métrique détaillée pour approfondir une valeur de métrique. Une page de métriques détaillées s'affiche, répertoriant les valeurs de métriques par clé, telle que l'adresse IP du client, l'adresse IP du serveur, la méthode ou l'erreur. Par exemple, si vous obtenez une détection d'authentification sur un serveur LDAP, vous pouvez effectuer une analyse détaillée pour savoir quelles adresses IP des clients ont soumis des informations d'identification non valides qui ont contribué au nombre total d'erreurs LDAP.

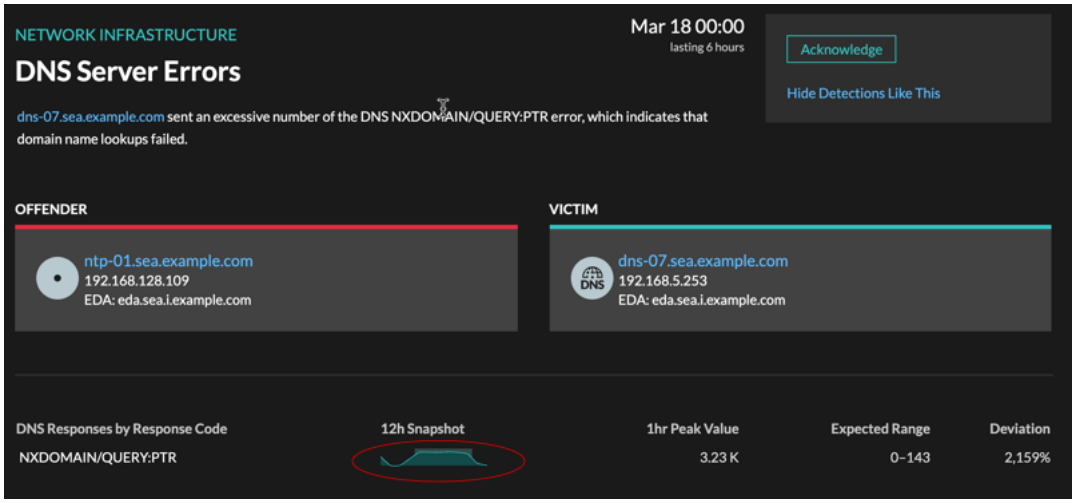


Disponibilité

L'option d'analyse descendante est disponible pour les détections associées aux métriques détaillées topnset.

Diagramme en étoile

Cliquez sur la ligne d'étincelles pour créer un graphique qui inclut la source, l'intervalle de temps et les détails d'analyse de la détection, que vous pouvez ensuite ajouter à un tableau de bord pour une surveillance supplémentaire. Par exemple, si vous recevez une détection concernant des problèmes de serveur web, vous pouvez créer un graphique avec les codes d'état 500 envoyés par le serveur web, puis ajouter ce graphique à un tableau de bord sur les performances du site web.

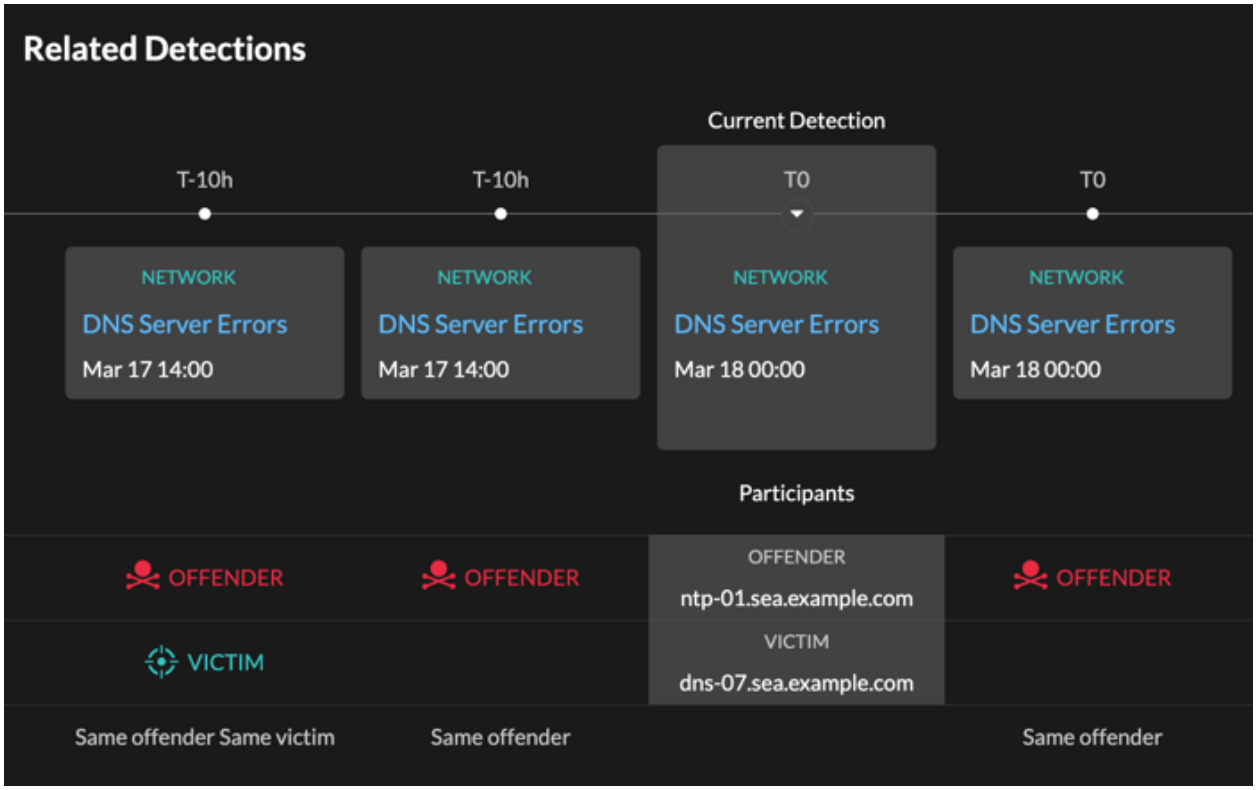


Disponibilité

L'option "sparkline" est disponible pour les détections associées à des mesures.

Détections associées

Cliquez sur une détection connexe pour obtenir des informations sur les problèmes de réseau, d'application et d'infrastructure dans plusieurs détections avec des participants communs. Par exemple, un périphérique identifié comme coupable est la source probable d'un problème, tel qu'un serveur de base de données envoyant un nombre excessif d'erreurs de réponse. Un dispositif identifié comme victime est généralement affecté négativement par le problème, comme les clients qui subissent des transactions de base de données lentes ou qui échouent. Vous pouvez consulter les détails des détections connexes pour déterminer si les événements de détection sont similaires, voir quels autres périphériques sont impliqués et consulter les données métriques.



Disponibilité

La chronologie des détections connexes est disponible s'il existe des détections qui partagent les mêmes participants victimes ou délinquants que la détection actuelle. Les détections connexes peuvent avoir eu lieu avant ou après la détection en cours.