Enquêter sur les détections de sécurité

Publié: 2023-09-19

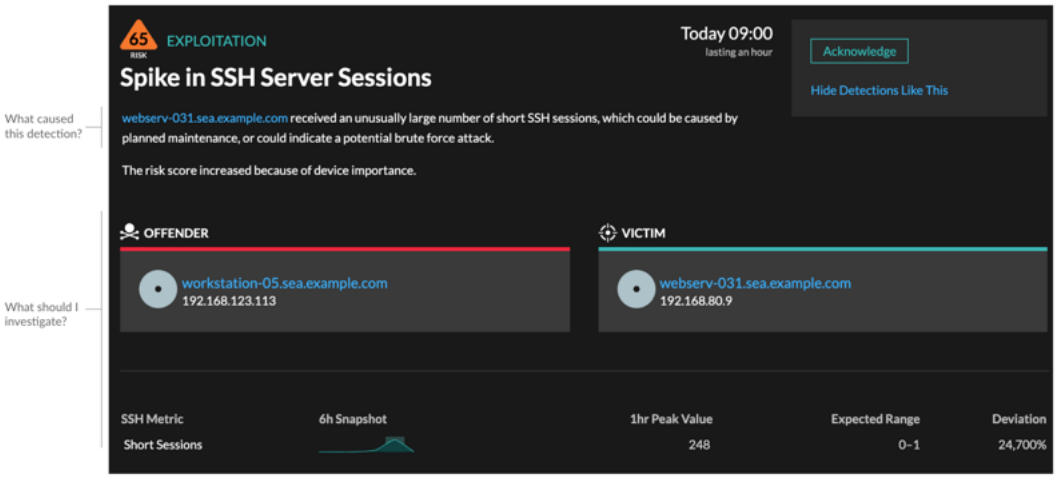
Lorsqu'une détection intéressante apparaît, vous devez vérifier si le comportement détecté indique un problème de faible priorité ou un risque de sécurité potentiel. Vous pouvez commencer votre enquête directement à partir de la fiche de détection, qui fournit des liens vers les données de l'ensemble 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 ?
- Certaines détections apparaissent-elles en groupes importants sur la ligne du temps ?
- Des détections apparaissent-elles pour des points finaux de grande valeur ?
- Certaines détections présentent-elles des scores de risque élevés ?
- Les dispositifs détectés participent-ils également à d'autres détections ?
- Des indicateurs de compromission ont-ils été identifiés à partir d'une collection de menaces associée à la détection ?

Commencez votre enquête

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



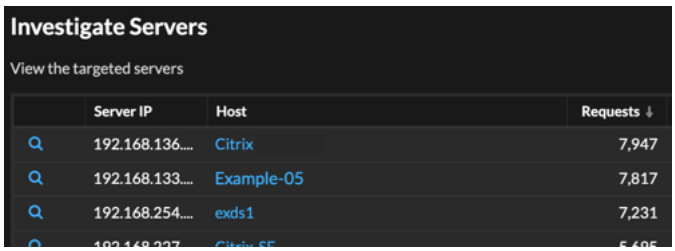
Affinez votre enquête

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 fiche 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.

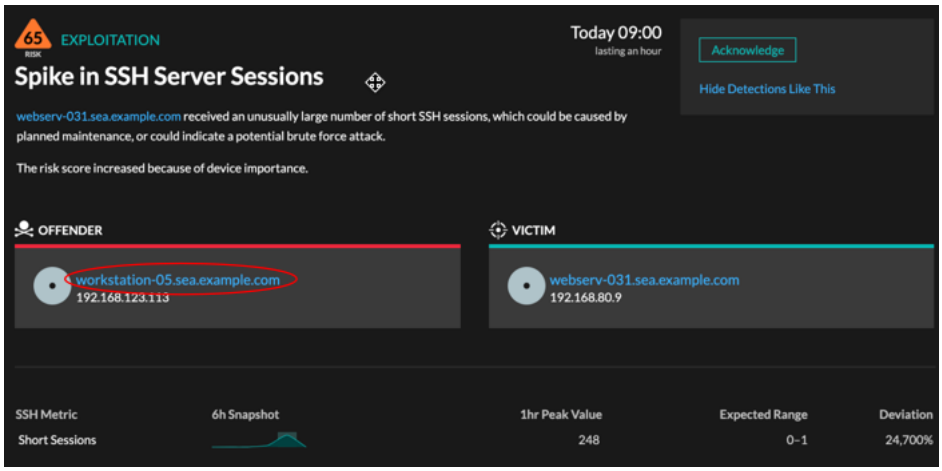
Cliquez sur le nom d'un hôte pour accéder à la page de présentation des périphériques, ou cliquez avec le bouton droit de la souris pour créer un graphique avec ce périphérique comme source et les paramètres pertinents.



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 du protocole vous donne une image complète de ce que faisait ce dispositif au moment de la détection.

Par exemple, si vous obtenez une détection d'analyse de reconnaissance, vous pouvez savoir si le dispositif associé à l'analyse est affecté au rôle d'analyseur de vulnérabilité.



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 obtenez une détection de mouvement latéral, vous pouvez savoir si le périphérique suspect a établi des connexions via un protocole

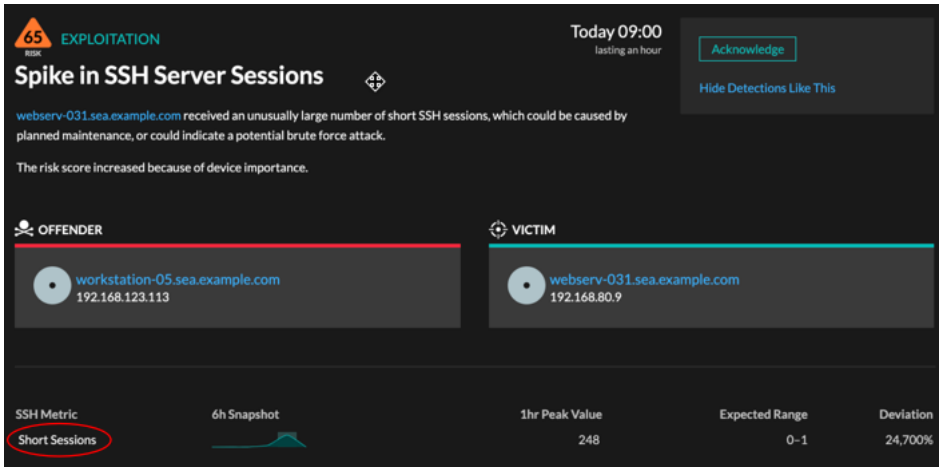
de contrôle à distance avec d'autres clients, serveurs informatiques ou contrôleurs de domaine sur votre réseau.

Disponibilité

Une carte d'activité est disponible lorsqu'un client ou un serveur unique est associé à une activité inhabituelle du protocole L7, 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 de balayage de reconnaissance, effectuez une analyse détaillée pour savoir quelles adresses IP de client étaient associées au nombre anormalement élevé de codes d'état 404 lors de la détection.

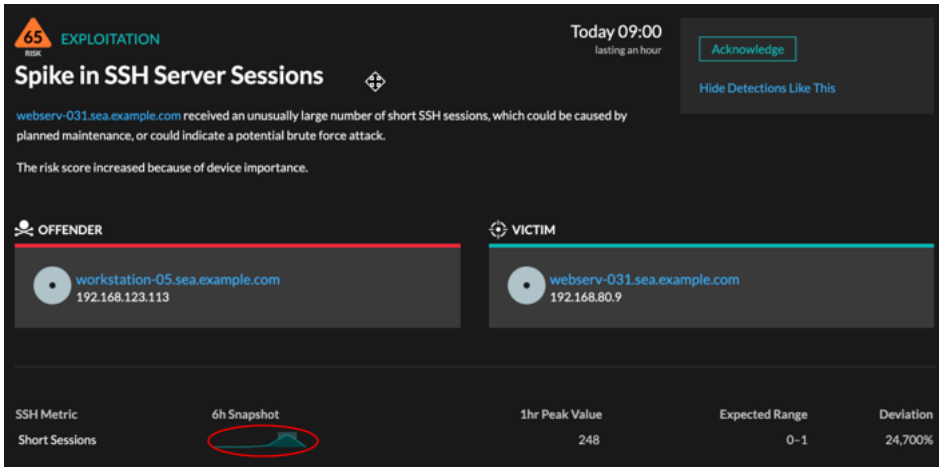


Disponibilité

L'option d'exploration 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 de la détection, que vous pouvez ensuite ajouter à un tableau de bord de surveillance. Par exemple, si vous recevez une détection concernant un nombre inhabituel de sessions distantes, créez un graphique avec les sessions SSH pour ce serveur, puis ajoutez ce graphique à un tableau de bord sur la gestion des sessions.

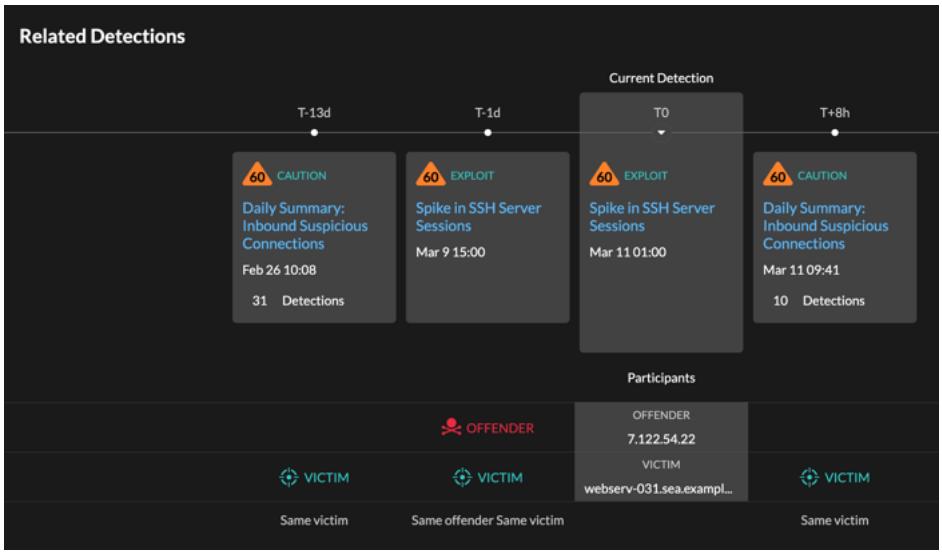


Disponibilité

L'option "sparkline" est disponible pour les détections associées à des mesures et d'une durée supérieure à une heure. Pour les mesures d'une seconde, un graphique en étoile est disponible lorsque la durée est supérieure à 30 secondes.

Détections connexes

Cliquez sur une détection connexe pour obtenir des informations sur les comportements suspects et les attaques émergentes dans le cadre de plusieurs détections avec des participants communs. Par exemple, une victime dans la détection actuelle qui participe en tant qu'auteur dans une détection ultérieure peut indiquer que l'appareil est compromis. Vous pouvez afficher les détails des détections connexes pour déterminer si les événements de détection sont similaires et pour voir quels autres appareils sont impliqués.



Disponibilité

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

Renseignements sur les menaces

Cliquez sur l'icône d'une caméra rouge pour accéder aux renseignements détaillés sur les menaces concernant un indicateur de compromission.

Les renseignements sur les menaces fournissent des données connues sur les adresses IP, les noms d'hôte et les URI suspects qui peuvent aider à identifier les risques pour votre organisation. Ces ensembles de données, appelés collections de menaces, sont disponibles par défaut dans votre système Reveal(x) et auprès de sources gratuites et commerciales de la communauté de la sécurité.

Disponibilité

Le renseignement sur les menaces doit être activé sur votre système Reveal(x) pour que vous puissiez voir ces indicateurs.