Étudier les détections de sécurité

Publié: 2023-09-30

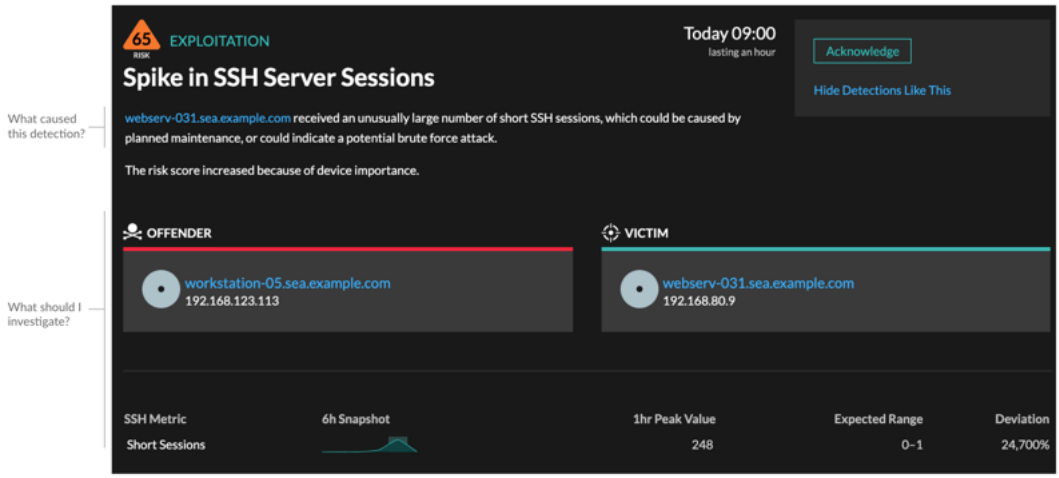
Lorsqu'une détection intéressante apparaît, vous devez déterminer si le comportement détecté indique un problème peu prioritaire ou un risque de sécurité potentiel. Vous pouvez démarrer votre enquête directement à partir de la carte de détection, qui fournit des liens vers les données du système ExtraHop.

Il existe un certain nombre de outils qui peuvent vous aider à filtrer votre vue pour voir les détections que vous souhaitez prioriser dans le cadre d'une enquête. Pour commencer, observez les tendances suivantes :

- Des détections se sont-elles produites à des moments inhabituels ou inattendus, tels que l'activité des utilisateurs le week-end ou en dehors des heures de bureau ?
- Des détections apparaissent-elles dans de grands groupes sur la chronologie ?
- Des détections apparaissent-elles pour des points de terminaison de grande valeur ?
- Y a-t-il des détections présentant des scores de risque élevés ?
- Les appareils utilisés lors de la détection participent-ils également à d'autres détections ?
- Les indicateurs de compromission sont-ils identifiés à partir d'une collecte des menaces associée à la détection ?

Commencez votre investigation

Consultez le titre et le résumé de la détection pour découvrir la cause de la détection.



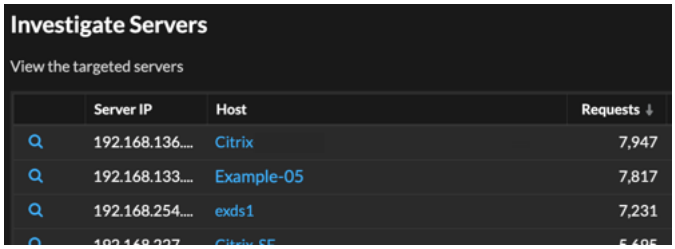
Affinez votre investigation

Les fiches détaillées de détection présentent des données associées à la détection. La disponibilité des données dépend des appareils et des métriques 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 étudier une détection sont affichées sur la page détaillée de la détection : tableaux contenant les données métriques pertinentes, transactions d'enregistrement et liens vers des paquets bruts.

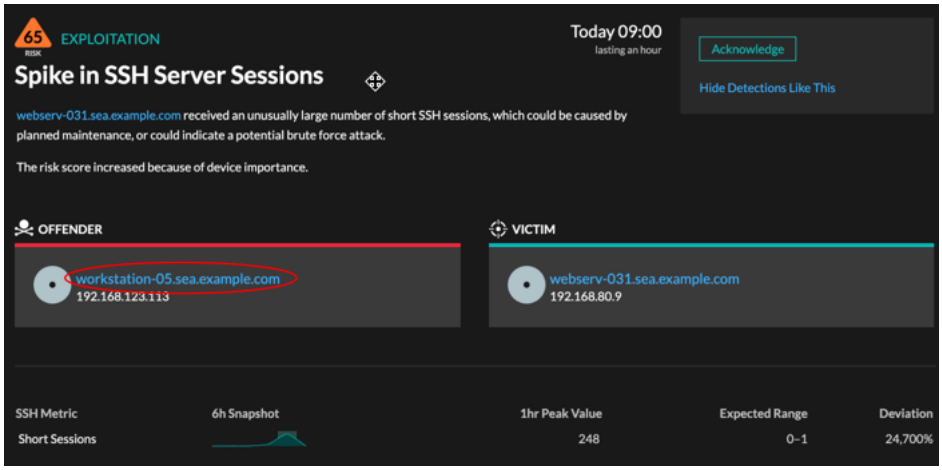
Cliquez sur le nom d'un hôte pour accéder à la page de présentation du périphérique, ou cliquez avec le bouton droit de la souris pour créer un graphique avec cet équipement comme source et les mesures pertinentes.



Nom de l'appareil

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

Par exemple, si vous obtenez une détection par analyse de reconnaissance, vous pouvez savoir si le rôle de scanner de vulnérabilités est attribué à l'équipement associé à l'analyse.



Disponibilité

Les liens vers les noms d'appareils ne sont disponibles que pour les appareils 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 des activités

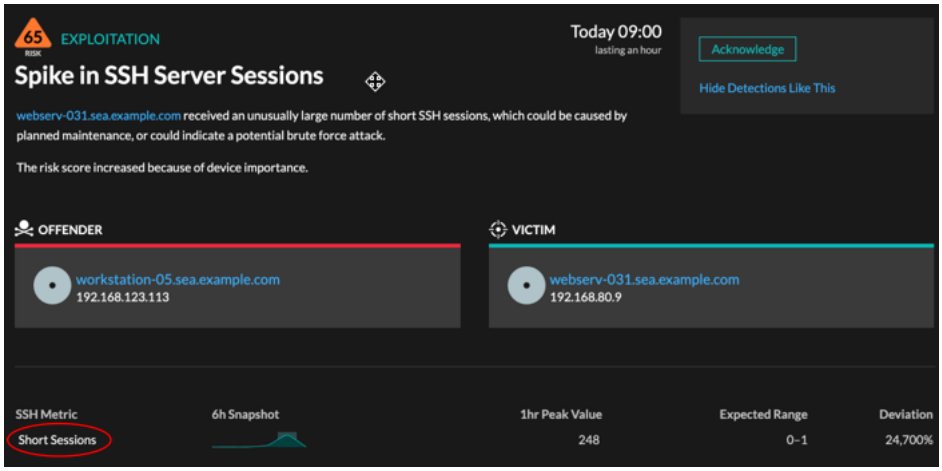
Cliquez sur l'icône de la carte d'activité à côté du nom d'un équipement pour voir les connexions des équipements par protocole au moment de la détection. Par exemple, si vous obtenez une détection de mouvement latéral, vous pouvez savoir si l'équipement suspect a établi des connexions via un protocole de contrôle à distance avec d'autres clients, serveurs informatiques ou contrôleurs de domaine de votre réseau.

Disponibilité

Une carte dactivités est disponible lorsqu'un seul client ou serveur est associé à une activité inhabituelle liée au protocole L7, telle qu'un nombre élevé d'erreurs HTTP ou des délais d'expiration des requêtes DNS.

Exploration métrique détaillée

Cliquez sur un lien métrique détaillé pour accéder à une valeur métrique vers le bas. Une page détaillée des mesures apparaît, qui répertorie les valeurs métriques par clé, telles que l'adresse IP du client, l'adresse IP du serveur, la méthode ou l'erreur. Par exemple, si vous obtenez une détection par analyse de reconnaissance, effectuez une analyse détaillée pour savoir quelles adresses IP des clients ont été associées au nombre anormalement élevé de codes d'état 404 lors de la détection.

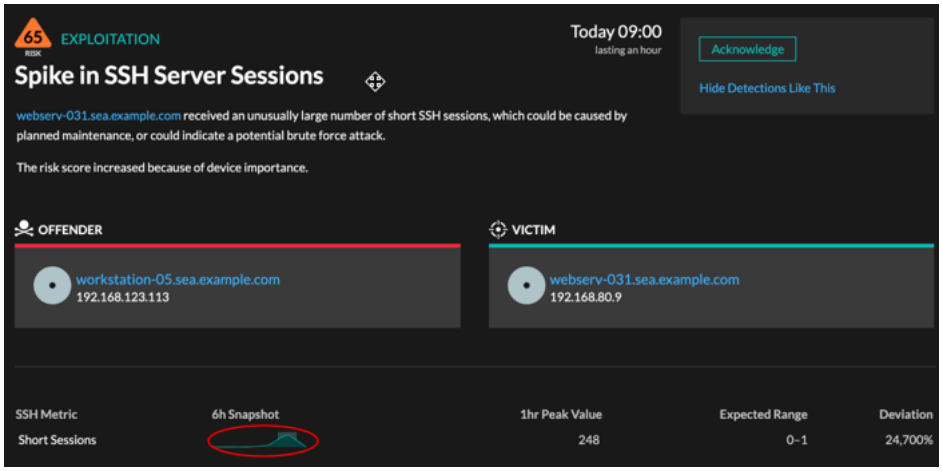


Disponibilité

L'option d'exploration vers le bas est disponible pour les détections associées à topnset métriques détaillées.

Sparkline

Cliquez sur le sparkline pour créer un graphique qui inclut la source, l'intervalle de temps et les détails détaillés de la détection, que vous pouvez ensuite ajouter à un tableau de bord à des fins de surveillance. Par exemple, si vous recevez une détection concernant un nombre inhabituel de sessions à distance, créez un graphique avec les sessions SSH pour ce serveur, puis ajoutez-le à un tableau de bord sur la gestion des sessions .

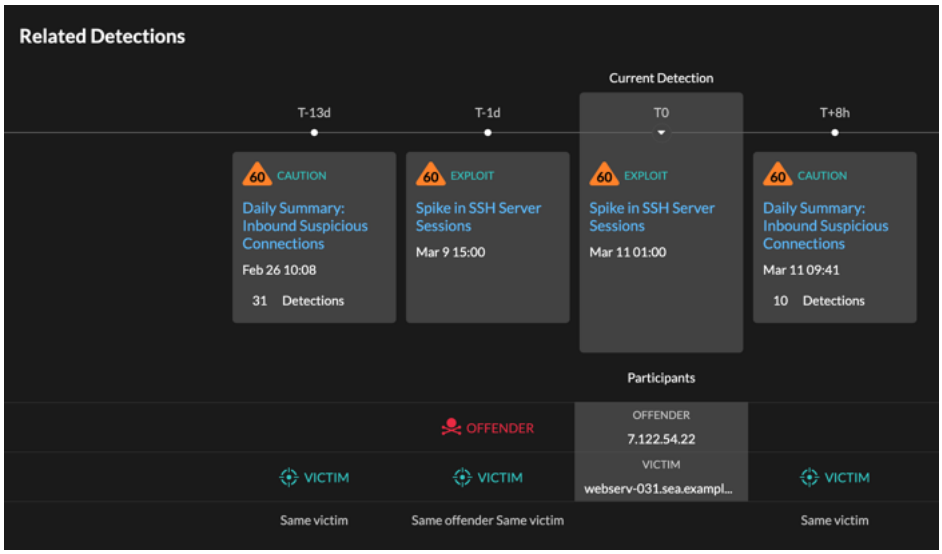


Disponibilité

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

Détections associées

Cliquez sur une détection associée pour obtenir des informations sur les comportements suspects et les attaques émergentes issues de plusieurs détections impliquant des participants communs. Par exemple, une victime en cours de détection qui participe en tant que délinquant à une détection ultérieure peut indiquer que l'équipement est compromis. Vous pouvez consulter les détails de détection associés pour déterminer si les événements de détection sont similaires et pour voir quels autres appareils sont impliqués.



Disponibilité

La chronologie des détections associée est disponible si certaines détections concernent la même victime ou le même délinquant que la détection en cours. Les détections associées peuvent s'être produites avant ou après la détection en cours.

Renseignements sur les menaces

Cliquez sur une icône de caméra rouge pour accéder à des renseignements sur les menaces détaillés 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 entreprise. 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

Les renseignements sur les menaces doivent être activés sur votre système Reveal (x) pour que vous puissiez voir ces indicateurs.