

Étudier les détections de sécurité

Publié: 2024-08-08

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.

The screenshot shows a detection card with the following details:

- Risk Level:** 65 EXPLOITATION (High Risk)
- Time:** Today 09:00 (lasting an hour)
- Action:** Acknowledge button and Hide Detections Like This link.
- What caused this detection?:** webserv-031.sea.example.com received an unusually large number of short SSH sessions, which could be caused by planned maintenance, or could indicate a potential brute force attack. The risk score increased because of device importance.
- What should I investigate?:**
 - OFFENDER:** workstation-05.sea.example.com (192.168.123.113)
 - VICTIM:** webserv-031.sea.example.com (192.168.80.9)
- SSH Metric:** Short Sessions
- 6h Snapshot:** A line graph showing a spike in short sessions.
- 1hr Peak Value:** 248
- Expected Range:** 0-1
- Deviation:** 24,700%

Affinez votre investigation

Les fiches détaillées de détection présentent les données associées 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 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 des appareils, ou cliquez avec le bouton droit pour créer un graphique avec cet équipement comme source et les mesures pertinentes.

Investigate Servers

View the targeted servers

	Server IP	Host	Requests ↓
🔍	192.168.136...	Citrix	7,947
🔍	192.168.133...	Example-05	7,817
🔍	192.168.254...	exds1	7,231
🔍	192.168.227...	Citrix-55	5,485

Nom de l'appareil

Cliquez sur le nom d'un équipement pour accéder à la page Présentation de l'appareil, qui contient le rôle, les utilisateurs et les balises 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 la détection d'un scan de reconnaissance, vous pouvez savoir si le rôle d'analyseur de vulnérabilités est attribué à l'équipement associé au scan.

65 EXPLOITATION
Today 09:00
lasting an hour

Spike in SSH Server Sessions

webserv-031.sea.example.com received an unusually large number of short SSH sessions, which could be caused by planned maintenance, or could indicate a potential brute force attack.

The risk score increased because of device importance.

OFFENDER
workstation-05.sea.example.com
192.168.123.113


VICTIM
webserv-031.sea.example.com
192.168.80.9

SSH Metric	6h Snapshot	1hr Peak Value	Expected Range	Deviation
Short Sessions		248	0-1	24,700%

Disponibilité

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

Carte des activités

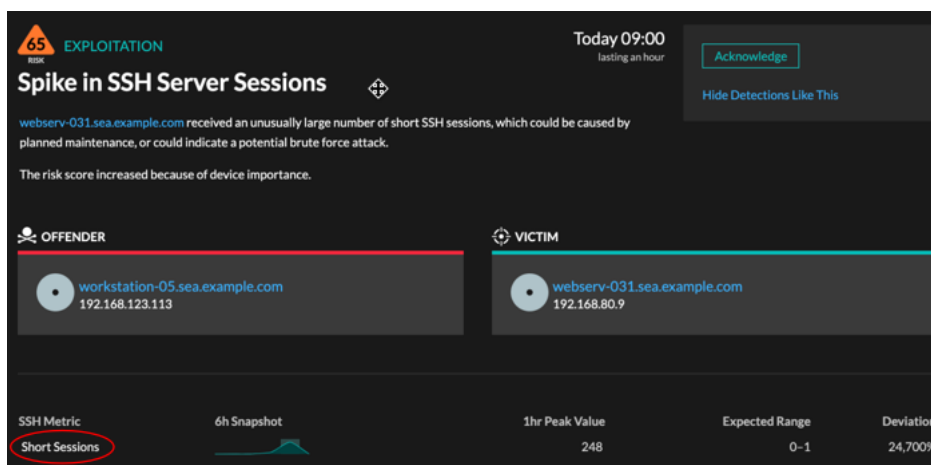
Cliquez sur l'icône de la carte d'activité  à côté du nom d'un équipement pour voir les connexions de l'équipement par protocole au moment de la détection. Par exemple, si vous recevez une détection de mouvement latéral, vous pouvez savoir si l'équipement suspect a établi des connexions via un protocole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

Disponibilité

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

Analyse métrique détaillée vers le bas

Cliquez sur le lien d'une métrique détaillée pour accéder à une valeur métrique vers le bas. Une page de mesures détaillées apparaît, qui répertorie les valeurs 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 par scan de reconnaissance, effectuez une exploration vers le bas pour savoir quelles adresses IP des clients étaient associées au nombre anormalement élevé de codes d'état 404 lors de la détection.

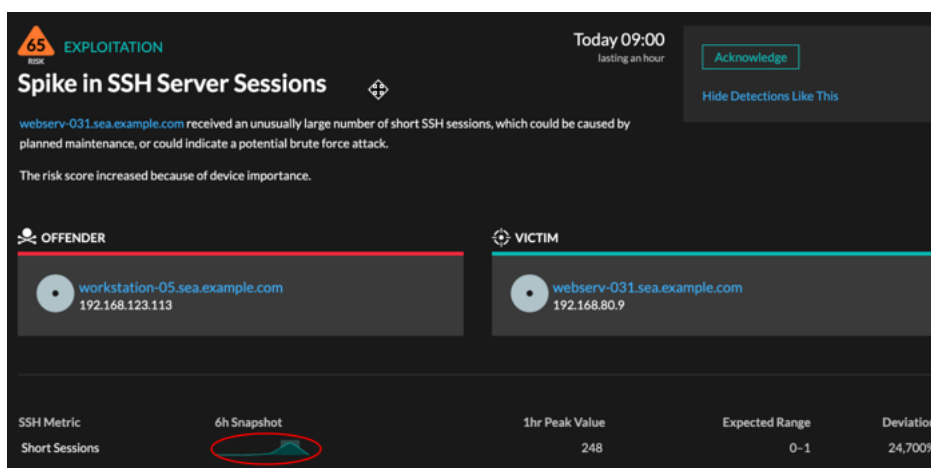


Disponibilité

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

Sparkline

Cliquez sur la ligne d'étincelle 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 concernant la gestion des sessions.

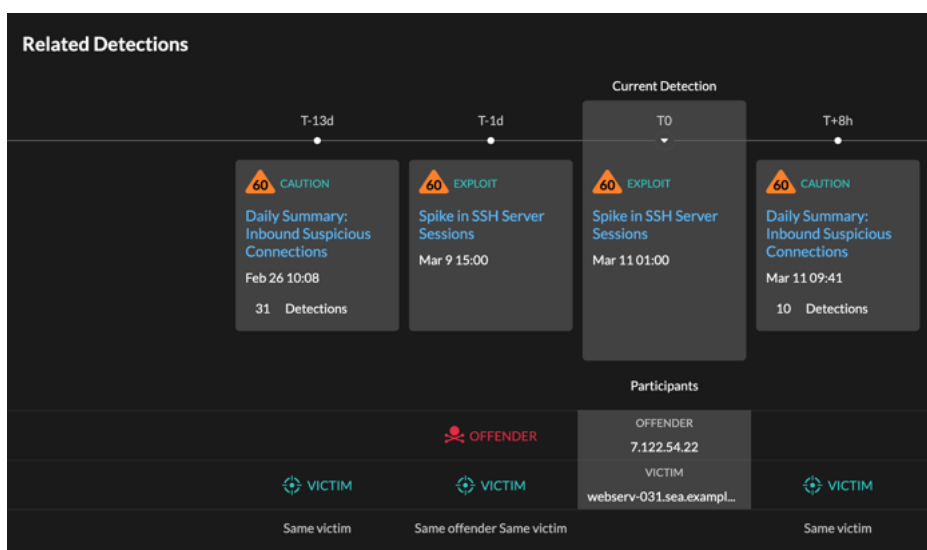


Disponibilité

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

Détections associées


Cliquez sur l'une des détections associées pour obtenir des informations sur les comportements suspects et les attaques émergentes résultant de plusieurs détections impliquant des participants partagés. Par exemple, une victime de la détection en cours 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 concernés.



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 avoir eu lieu avant ou après la détection en cours.

Renseignements sur les menaces

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

Le renseignement sur les menaces fournit des données connues sur les adresses IP, les noms d'hôte et les URI suspects qui peuvent aider à identifier les risques auxquels votre organisation est exposée. Ces ensembles de données, appelés collections de menaces, sont disponibles par défaut dans votre système RevealX 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 RevealX pour que vous puissiez voir ces indicateurs.