Renseignements sur les menaces

Publié: 2023-09-19

Les renseignements sur les menaces fournissent des données connues sur les adresses IP, les domaines, les noms d'hôte et les URI suspects qui peuvent aider à identifier les risques pour votre organisation.

Les ensembles de données de renseignements sur les menaces, appelés collections de menaces, sont disponibles par défaut dans votre système ExtraHop, à partir de sources gratuites et commerciales dans la communauté de la sécurité, et à partir d'intégrations de partenaires avec ExtraHop Reveal(x) 360.

Lorsque le système ExtraHop observe une activité qui correspond à une entrée d'une collection de menaces (appelée indicateur de compromission), une détection est générée pour la connexion à un point d'extrémité suspect et l'entrée suspecte est marquée par une icône de caméra ou d'autres indices visuels.

Recueils de menaces

Le système ExtraHop permet de collecter des menaces à partir de plusieurs sources.

Les renseignements sur les cybermenaces étant fournis par la communauté, il existe de nombreuses sources externes de collecte de données sur les menaces. Les données de ces collections peuvent varier en qualité ou en pertinence par rapport à votre environnement. Pour préserver la précision et réduire le bruit, nous vous recommandons de limiter vos téléchargements à des données de renseignements sur les menaces de haute qualité qui se concentrent sur un type d'intrusion spécifique, comme une collection pour les logiciels malveillants et une autre collection pour les réseaux de zombies.

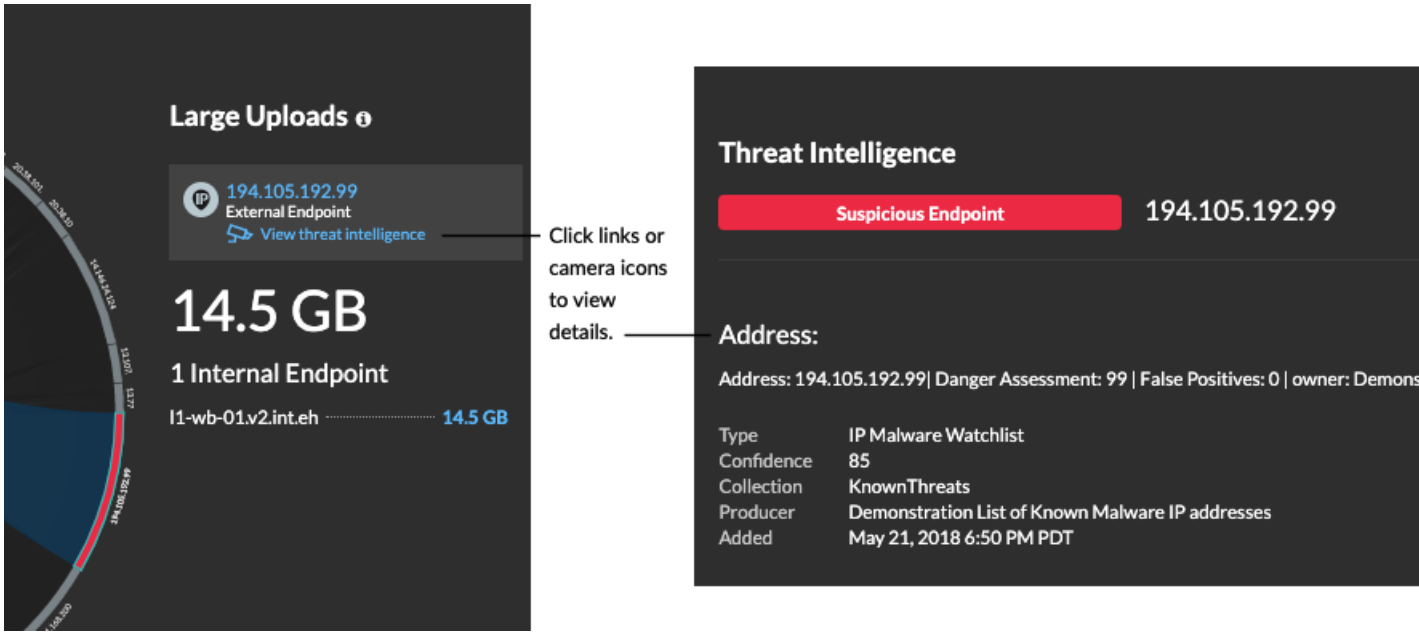
Les collections de menaces créées par ExtraHop sont activées par défaut et mises à jour toutes les 12 heures. Les adresses IP, les domaines, les noms d'hôte et les URI suspects apparaissent dans les graphiques et les enregistrements du système.

Lescollections gratuites et commerciales proposées par la communauté de la sécurité et formatées en Structured Threat Information eXpression (STIX) sous forme de fichiers TAR ou TAR.GZ peuvent être téléchargées manuellement ou via l'API REST vers les systèmes ExtraHop. Les versions STIX 1.0 à 1.2 sont actuellement prises en charge. Vous devez télécharger chaque collection de menaces individuellement vers tous les capteurs connectés.

Les collections de menaces provenant d'intégrations partenaires doivent être importées dans ExtraHop Reveal(x) 360.

Enquêter sur les menaces

Lorsque le système Reveal(x) observe un indicateur de compromission, l'adresse IP, le domaine, le nom d'hôte ou l'URI suspect est marqué d'une icône de caméra ou d'un autre repère visuel afin que vous puissiez enquêter directement à partir des tableaux et des graphiques que vous consultez.



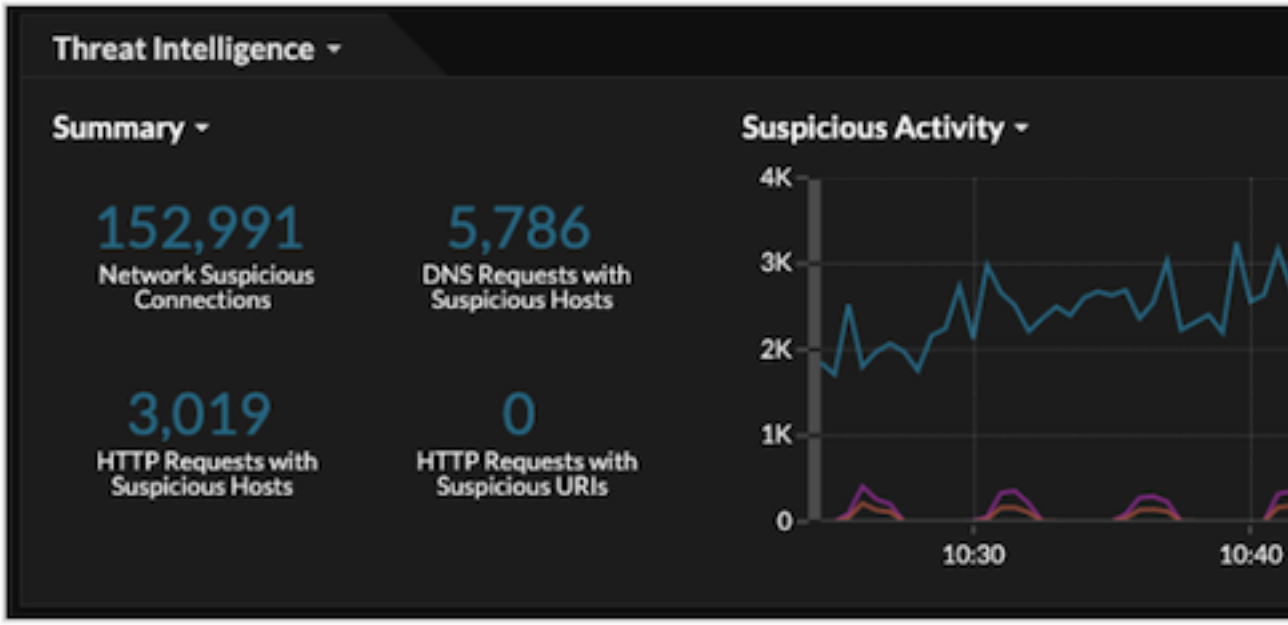
- Si la collection de menaces est ajoutée ou mise à jour après que le système a observé l'activité suspecte, les renseignements sur les menaces ne sont pas appliqués à cette adresse IP, ce nom d'hôte ou cet URI jusqu'à ce que l'activité suspecte se produise à nouveau.
- Si une collection de menaces créée par ExtraHop est mise à jour, le système ExtraHop effectue une détection rétrospective automatisée (ARD), qui recherche de nouveaux domaines qui sont des indicateurs de compromission dans les enregistrements des 7 derniers jours. Si une correspondance est trouvée, le système génère une détection rétrospective.
- Si vous désactivez ou supprimez une collection de menaces, tous les indicateurs sont supprimés des mesures et des enregistrements correspondants dans le système.

Voici quelques endroits du système Reveal(x) qui affichent les indicateurs de compromission trouvés dans vos collections de menaces :

Tableau de bord du renforcement de la sécurité

La région Threat Intelligence (renseignements sur les menaces) contient des indicateurs d'activités suspectes qui correspondent aux données de vos collections de menaces. En cliquant sur un indicateur, tel que Requêtes HTTP avec hôtes suspects, vous pouvez approfondir

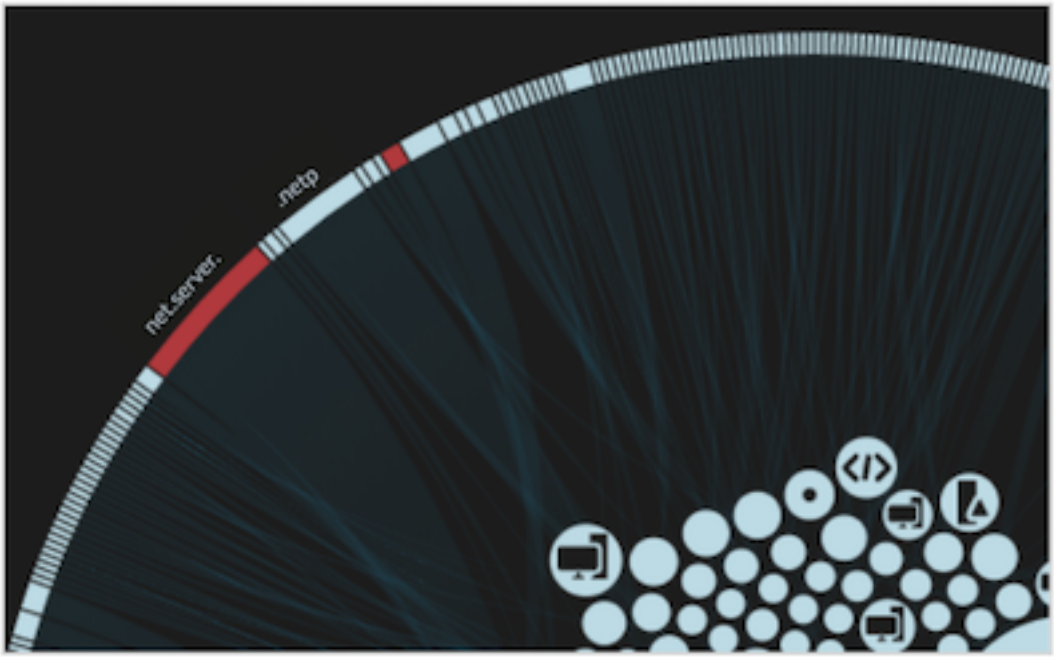
l'indicateur pour obtenir des détails ou interroger les enregistrements pour les transactions



connexes.

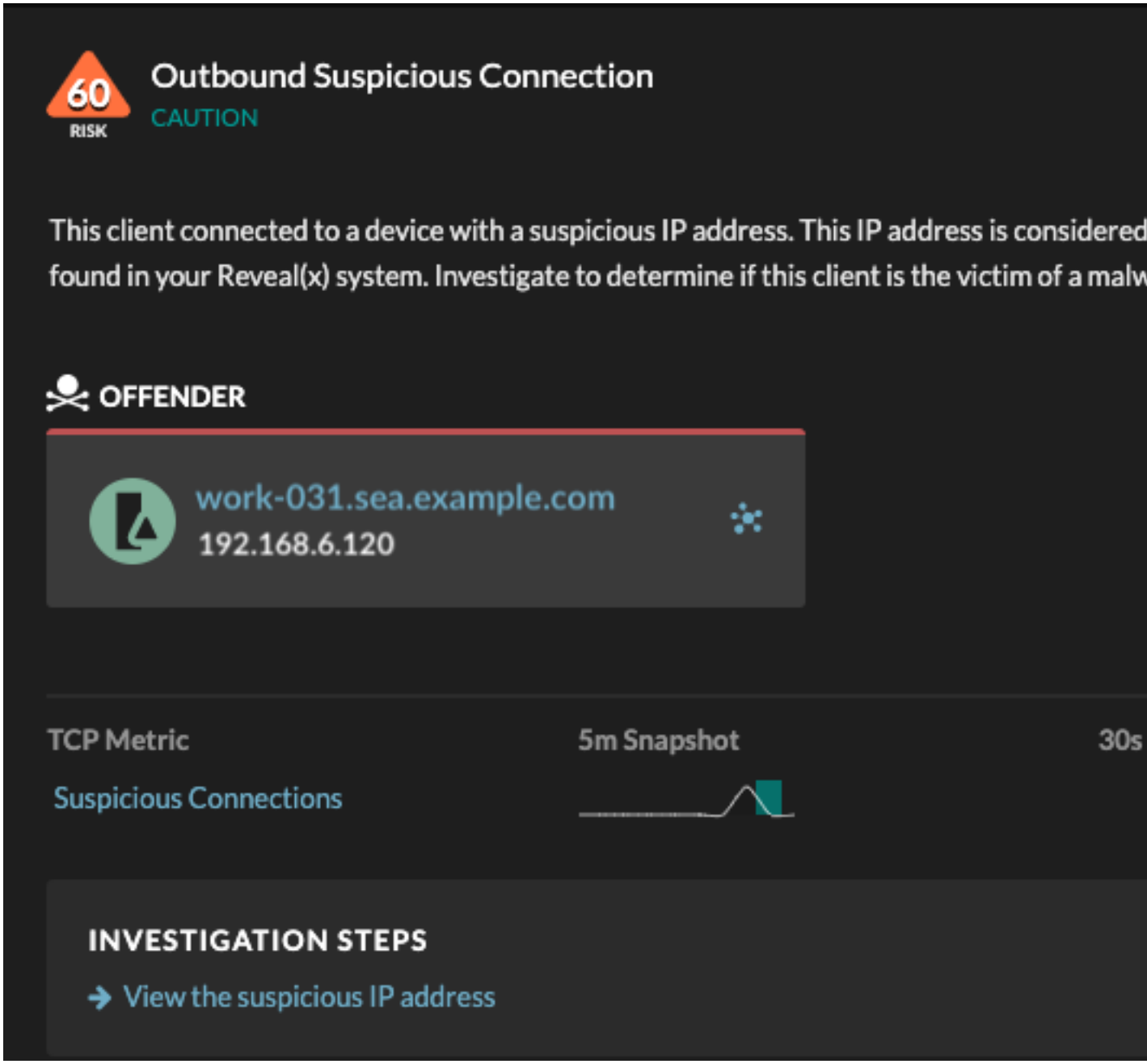
Vue d'ensemble du périmètre

Dans la visualisation du halo, tous les points d'extrémité qui correspondent aux entrées de la collection de menaces sont surlignés en rouge.



Détections

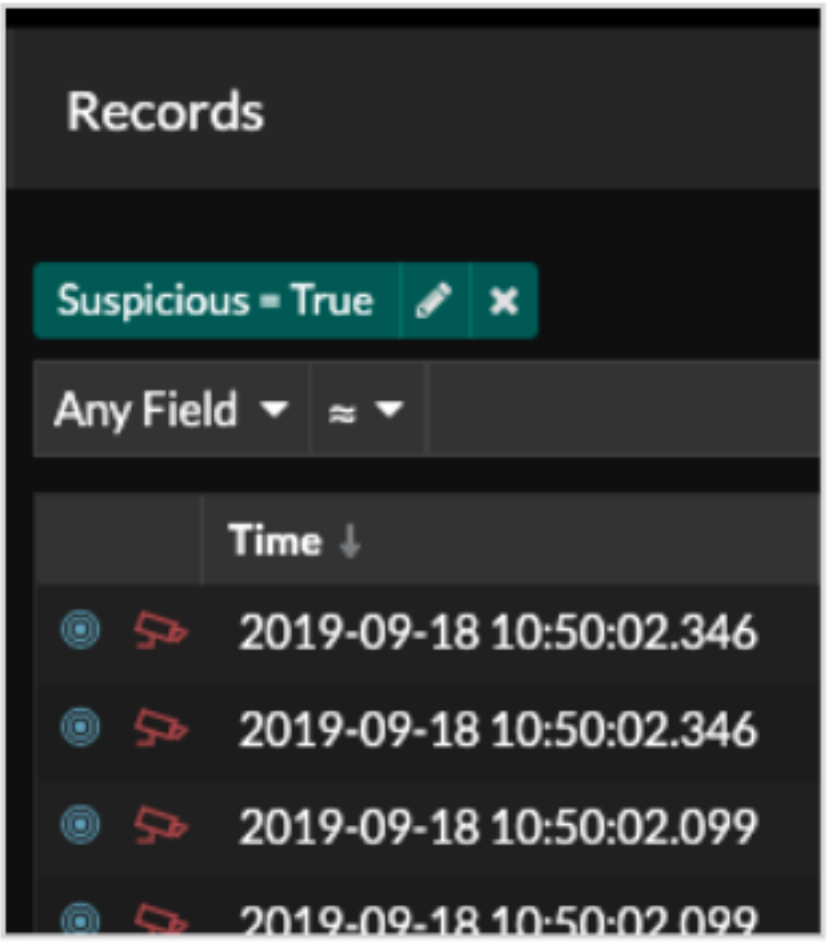
Une détection apparaît lorsqu'un indicateur de compromission provenant d'une collection de menaces est identifié dans le trafic réseau.



Enregistrements

La page Enregistrements vous permet de rechercher directement les transactions qui correspondent aux entrées de la collection de menaces.

- Sous la facette Suspicieux, cliquez sur **Vrai** pour filtrer tous les enregistrements dont les transactions correspondent à des adresses IP, des noms d'hôte et des URI suspects.
- Créez un filtre en sélectionnant Suspicieux, IP suspecte, Domaine suspect ou URI suspecte dans la liste déroulante à trois champs, un opérateur et une valeur.
- Cliquez sur l'icône de la caméra rouge pour afficher les détails des renseignements sur les menaces.



Détections rétrospectives

(Reveal(x) 360 uniquement) Lorsqu'une collection de menaces créée par ExtraHop est mise à jour, le système ExtraHop effectue une détection rétrospective automatisée (ARD), qui recherche les nouveaux domaines qui sont des indicateurs de compromission dans les enregistrements des 7 derniers jours. Si une connexion antérieure à un domaine suspect est identifiée, le système génère une détection rétrospective.

L'horodatage d'une détection rétrospective indique l'heure à laquelle l'activité s'est produite à l'origine et peut ne pas apparaître dans la liste de détection actuelle. Vous pouvez trouver des détections rétrospectives en cliquant sur l'information rétrospective sur les menaces. Vous pouvez également créer une règle de notification de détection qui vous enverra un courrier électronique lorsque ce type de détection se produit.