Renseignements sur les menaces

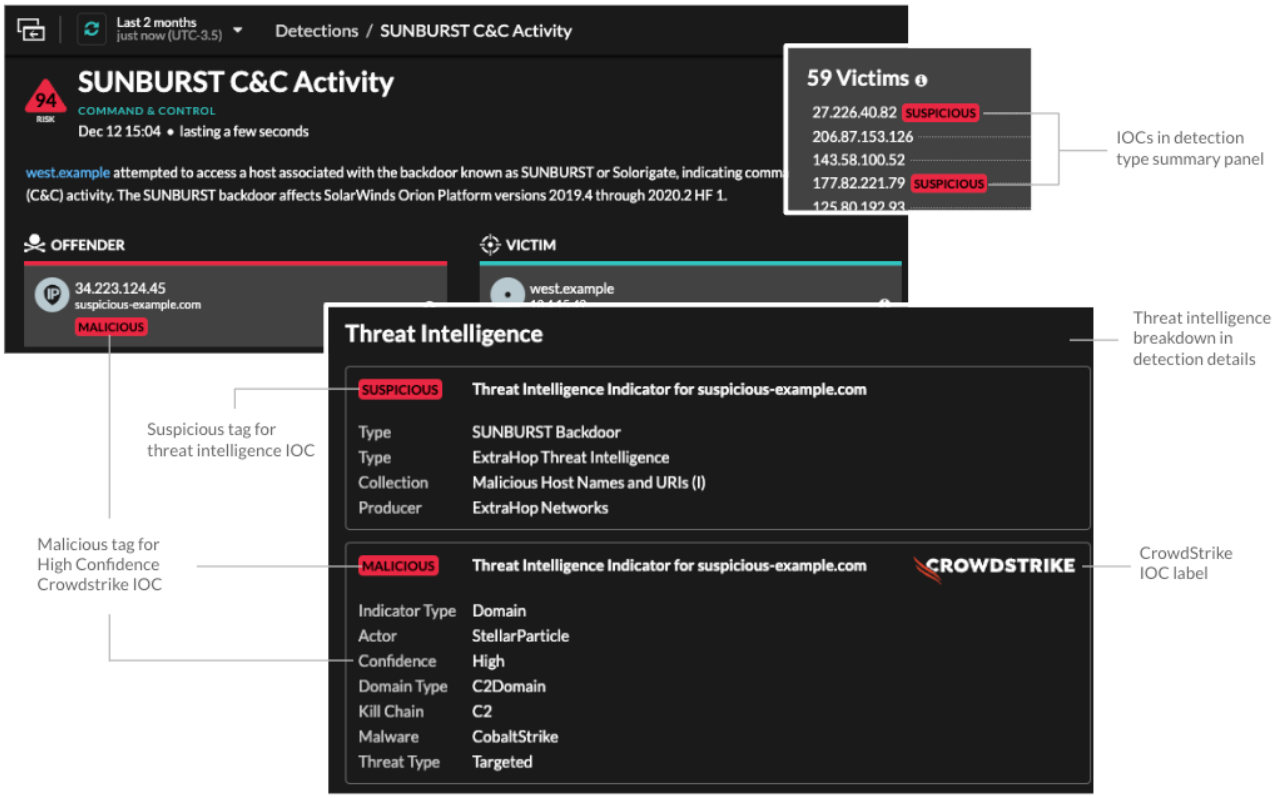
Publié: 2024-04-10

Le renseignement sur les menaces fournit 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.

Vidéos Consultez la formation associée : Renseignements sur les menaces

Les ensembles de données de renseignement sur les menaces, appelés collections de menaces, contiennent des listes de terminaux suspects appelés indicateurs de compromission (IOC).

Les participants correspondant à une collecte des menaces sont marqués comme suspects dans les détections, les résumés des détections, les diagrammes des systèmes et les enregistrements. (Pour les IoC Crowdstrike où le niveau de confiance est élevé, le participant est marqué comme malveillant.) Les enregistrements contenant l'entrée suspecte sont signalés par une icône représentant une caméra. Dans de nombreux cas, une correspondance d'indicateur génère également la détection de la connexion suspecte.



Collections de menaces

Le système ExtraHop prend en charge la collecte de menaces provenant de plusieurs sources.

Collections de menaces intégrées

Des collections de menaces organisées par ExtraHop et CrowdStrike Falçon sont disponibles par défaut dans votre système ExtraHop. Les collections intégrées sont mises à jour toutes les 6 heures. Tu peux activer ou désactiver les collections de menaces intégrées depuis la page Threat Intelligence.

Téléversement de fichiers STIX

Les collections gratuites et commerciales proposées par la communauté de la sécurité et formatées au format STIX (Structured Threat Information eXpression) sous forme de fichiers TAR compressés, tels que .TGZ ou TAR.GZ, peuvent être chargé manuellement ou via l' API REST aux systèmes ExtraHop. Les versions 1.0 à 1.2 de STIX sont actuellement prises en charge. Vous devez télécharger chaque collecte des menaces individuellement sur votre console et sur tous les capteurs connectés.

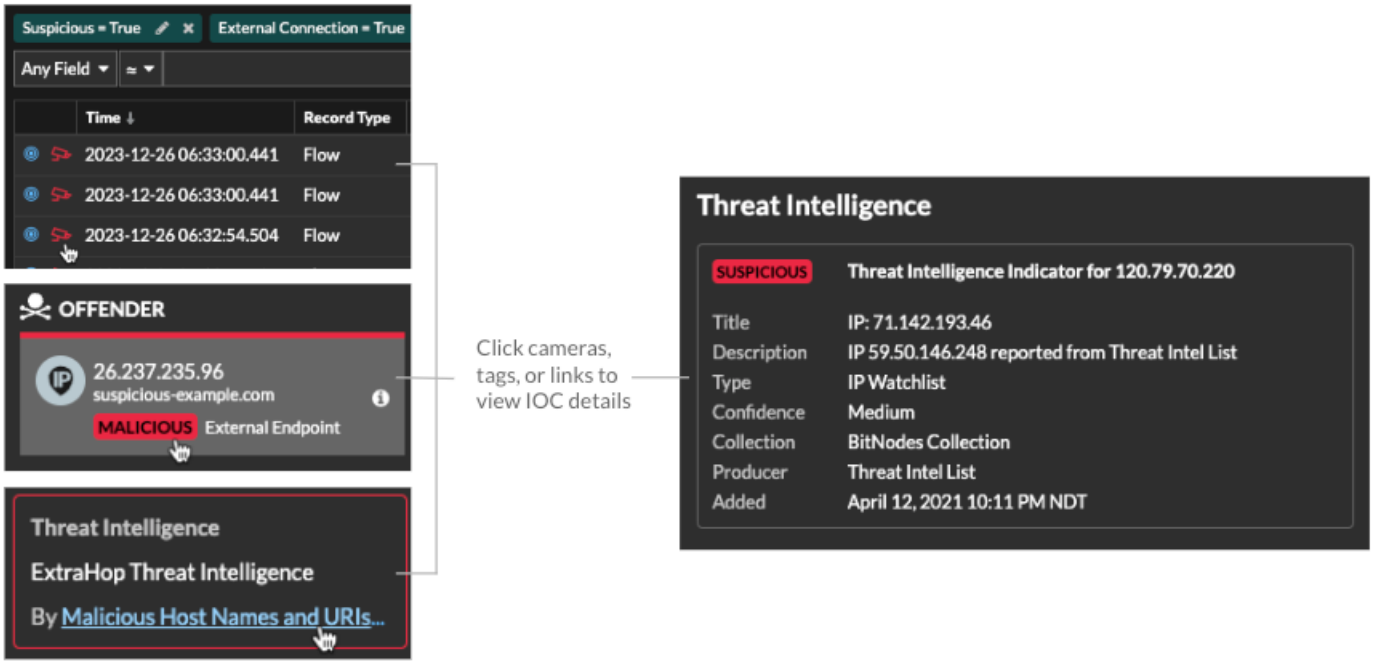
Fil TAXII

Les collections de menaces peuvent être transmises à votre environnement à partir d'une source fiable via le protocole TAXII (Trusted Automated Exchange of Intelligence Information). Un flux TAXII peut fournir un flux constant d'indicateurs de menace mis à jour. Tu peux ajouter un flux TAXII depuis le Renseignements sur les menaces page.

Étant donné que les renseignements sur les cybermenaces sont gérés par la communauté, il existe de nombreuses sources externes pour la collecte des menaces. Les données de ces collections peuvent varier en termes de qualité ou de pertinence par rapport à votre environnement. Pour garantir la précision et réduire le bruit, nous vous recommandons de limiter le téléchargement de vos fichiers STIX 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 programmes malveillants et une autre pour les botnets. De même, nous vous recommandons de limiter les flux TAXII à des sources fiables et de haute qualité.

Enquête sur les menaces

Une fois que le système Reveal (x) a détecté un indicateur de compromission, l' adresse IP, le domaine, le nom d'hôte ou l'URI suspects sont marqués comme suspects ou malveillants dans les résumés de détection et sur les fiches de détection individuelles. Dans les tableaux et les graphiques, les indicateurs de compromission sont signalés par une icône représentant une caméra, ce qui vous permet d'effectuer des recherches directement à partir des tableaux et des graphiques que vous consultez.



- Si la collecte des menaces est ajoutée ou mise à jour après que le système a détecté l' activité suspecte, les renseignements sur les menaces ne sont pas appliqués à cette adresse IP, à ce nom d'hôte ou à cet URI jusqu'à ce que l'activité suspecte se reproduise.
- (Reveal (x) 360 uniquement) Si une collecte des menaces ExtraHop ou CrowdStrike intégrée est mise à jour, le système ExtraHop effectue une détection rétrospective automatisée (ARD), qui recherche les nouveaux domaines, noms d'hôtes, URL et adresses IP qui indiquent une compromission dans

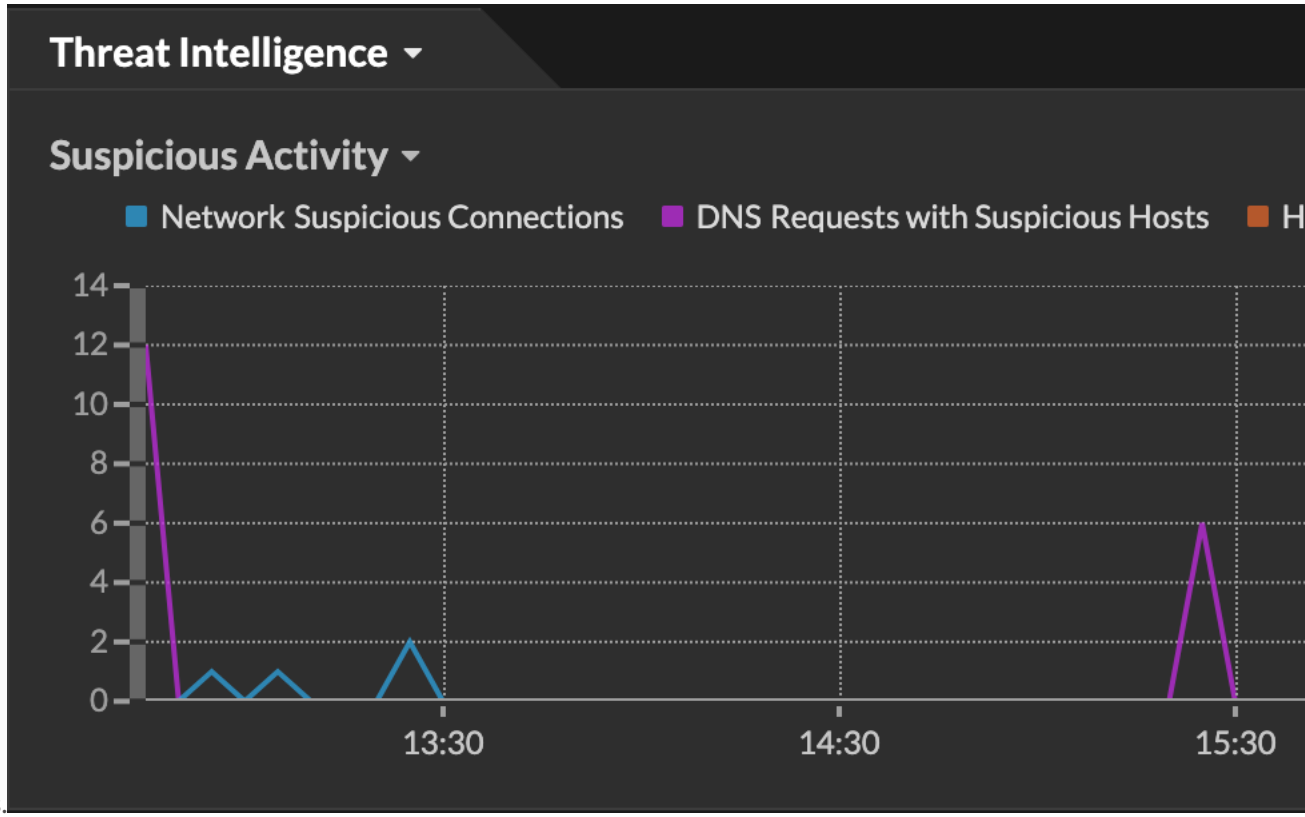
les enregistrements des 7 derniers jours. Si une correspondance est trouvée, le système génère une détection rétrospective.

- Si vous désactivez ou supprimez une collecte des menaces, tous les indicateurs sont supprimés des métriques et des enregistrements associés dans le système. Les détections dont le triage est recommandé sur la base de renseignements sur les menaces resteront dans le système une fois la collecte associée désactivée.

Voici quelques parties du système Reveal (x) qui présentent les indicateurs de compromission détectés dans vos collections de menaces :

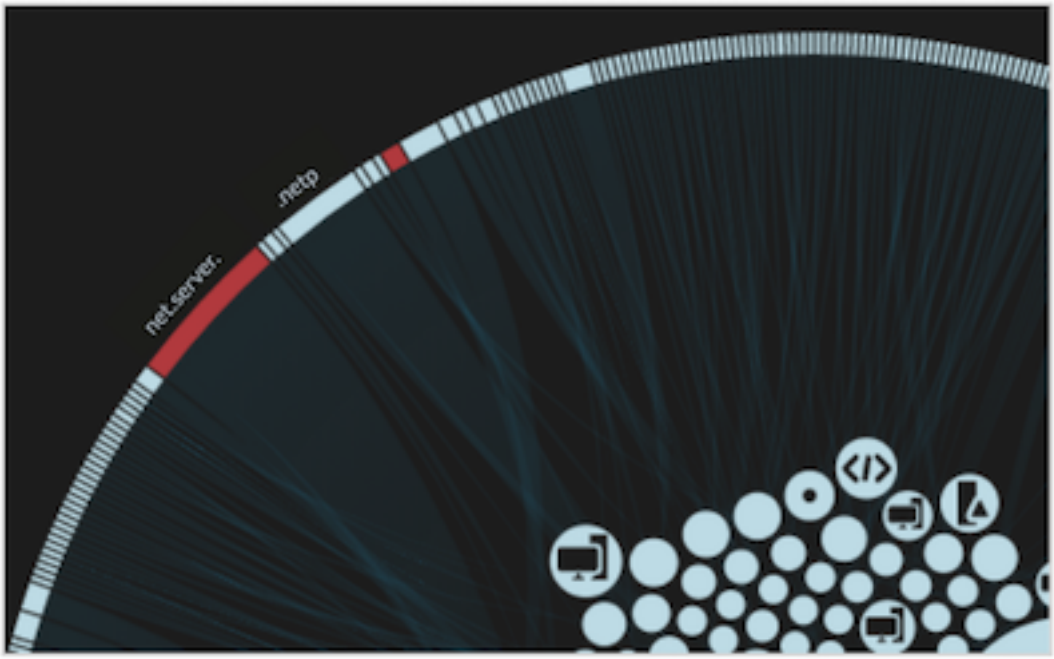
Tableau de bord de renforcement de la sécurité

Le région de renseignement sur les menaces contient des mesures relatives aux activités suspectes qui correspondent aux données de vos collections de menaces. En cliquant sur n'importe quelle métrique, telle que Requêtes HTTP avec des hôtes suspects, vous pouvez effectuer une recherche détaillée sur la métrique ou interroger des enregistrements pour les transactions associées.



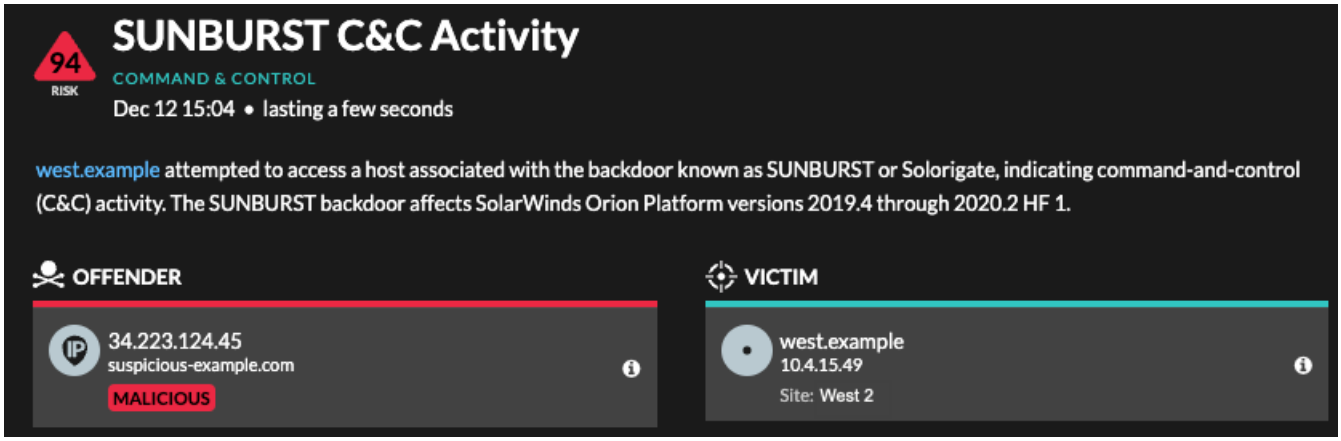
Vue d'ensemble du périmètre

Dans la visualisation du halo, tous les points de terminaison correspondant aux entrées de collecte des menaces sont surlignés en rouge.



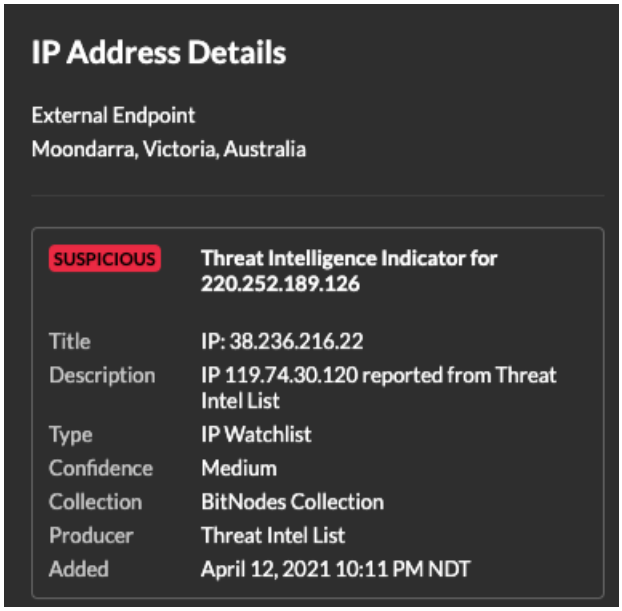
Détections

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



Détails de l'adresse IP

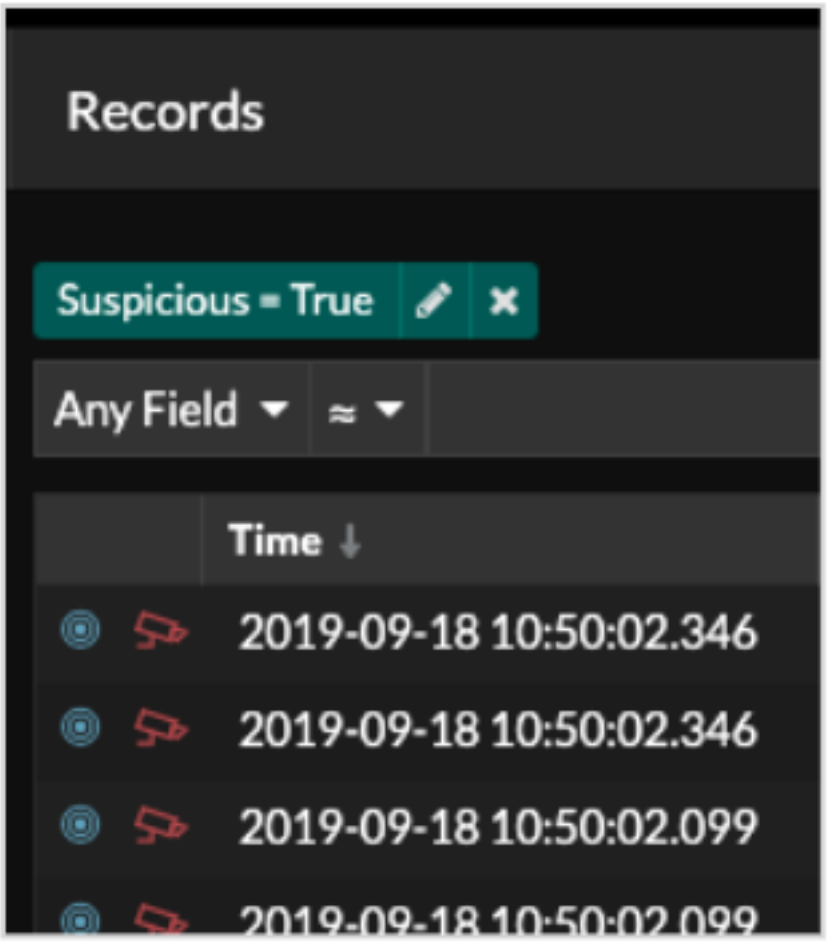
Les pages détaillées des adresses IP affichent des renseignements sur les menaces complets pour les indicateurs de compromission des adresses IP.



Disques

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

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



Détections rétrospectives

(Reveal (x) 360 uniquement) Lorsqu'une collecte des menaces ExtraHop ou CrowdStrike est mise à jour, le système ExtraHop effectue une détection rétrospective automatisée (ARD), qui recherche les nouveaux domaines, noms d'hôtes, URL et adresses IP qui indiquent une compromission dans les enregistrements des 7 derniers jours . Si une connexion passée à un domaine suspect est identifiée, le système génère une détection rétrospective.

L'horodateur d'une détection rétrospective indique l'heure à laquelle l' activité s'est produite initialement et peut ne pas apparaître dans la liste de détection actuelle. Vous pouvez trouver des détections rétrospectives en cliquant sur le Retrospective Threat Intelligence informations sur les menaces. Vous pouvez également créer une règle de notification de détection pour vous envoyer un e-mail lorsque ces types de détections se produisent.