

Renseignements sur les menaces

Publié: 2024-07-03

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.

📺 **Vidéo** 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.

The screenshot displays the 'SUNBURST C&C Activity' detection page. It features a risk score of 94 (Command & Control) and a summary of the activity. A '59 Victims' panel lists several IP addresses, with two marked as 'SUSPICIOUS'. A 'Threat Intelligence' panel provides a detailed breakdown for a 'suspicious-example.com' indicator, including its type (SUNBURST Backdoor), collection (Malicious Host Names and URIs (I)), and confidence (High). A 'CrowdStrike IOC label' is also visible.

SUNBURST C&C Activity
 94 RISK
 COMMAND & CONTROL
 Dec 12 15:04 • lasting a few seconds

west.example attempted to access a host associated with the backdoor known as SUNBURST or Solorigate, indicating comm. (C&C) activity. The SUNBURST backdoor affects SolarWinds Orion Platform versions 2019.4 through 2020.2 HF 1.

59 Victims

- 27.226.40.82 SUSPICIOUS
- 206.87.153.126
- 143.58.100.52
- 177.82.221.79 SUSPICIOUS
- 125.80.192.93

Threat Intelligence

SUSPICIOUS Threat Intelligence Indicator for suspicious-example.com

Type	SUNBURST Backdoor
Type	ExtraHop Threat Intelligence
Collection	Malicious Host Names and URIs (I)
Producer	ExtraHop Networks

MALICIOUS Threat Intelligence Indicator for suspicious-example.com **CROWDSTRIKE**

Indicator Type	Domain
Actor	StellarParticle
Confidence	High
Domain Type	C2Domain
Kill Chain	C2
Malware	CobaltStrike
Threat Type	Targeted

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 Falcon 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 RevealX a observé 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.

The screenshot shows the ExtraHop interface with the following elements:

- Table of Suspicious Connections:**

Time ↓	Record Type
2023-12-26 06:33:00.441	Flow
2023-12-26 06:33:00.441	Flow
2023-12-26 06:32:54.504	Flow
- OFFENDER Card:**
 - IP: 26.237.235.96
 - Domain: suspicious-example.com
 - Label: MALICIOUS External Endpoint
- Threat Intelligence Card:**
 - Indicator: Threat Intelligence Indicator for 120.79.70.220
 - Title: IP: 71.142.193.46
 - Description: IP 59.50.146.248 reported from Threat Intel List
 - Type: IP Watchlist
 - Confidence: Medium
 - Collection: BitNodes Collection
 - Producer: Threat Intel List
 - Added: April 12, 2021 10:11 PM NDT

A callout box with the text "Click cameras, tags, or links to view IOC details" points to the camera icons in the table and the threat intelligence card.

- 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.
- (RevealX 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

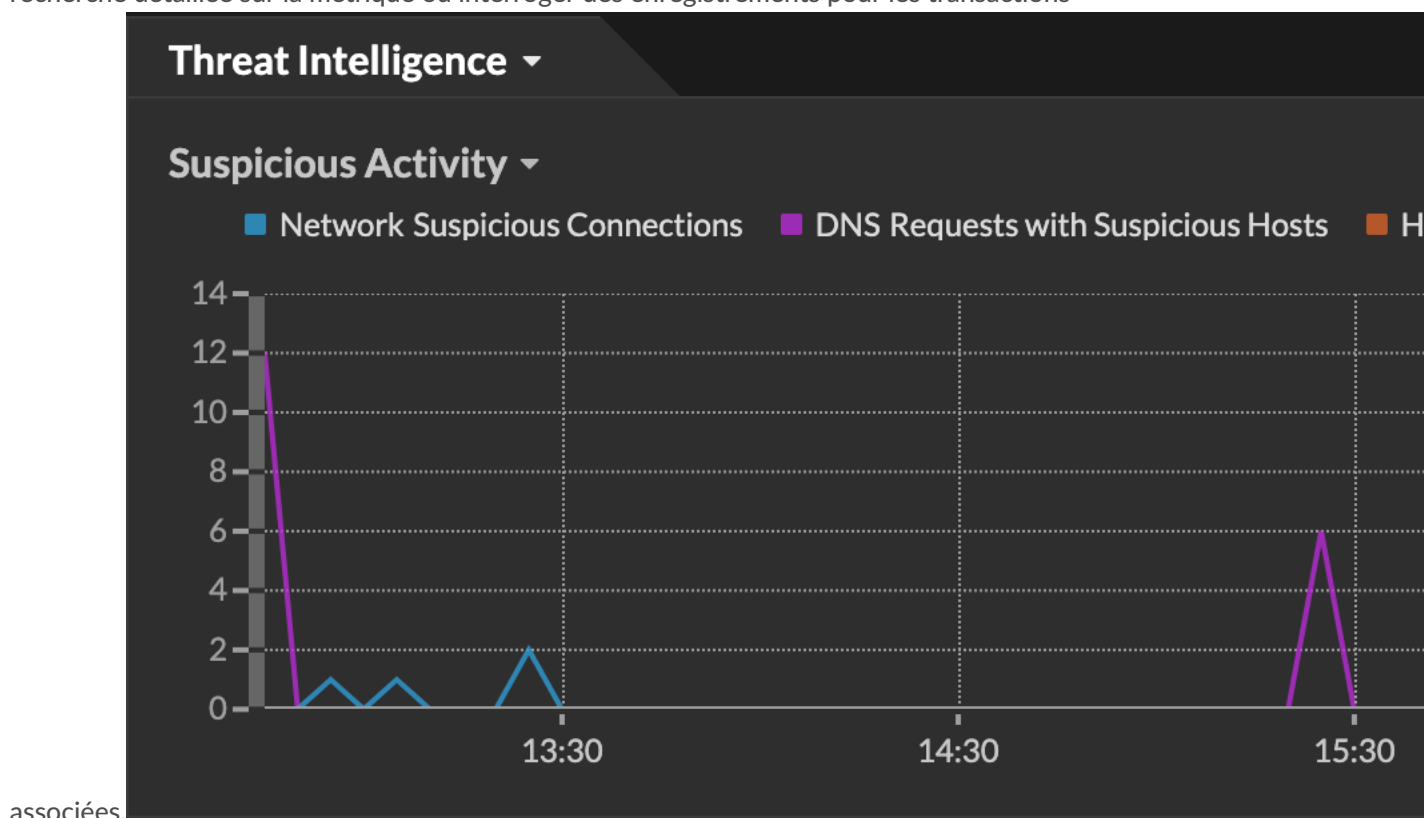
les enregistrements des 7 derniers jours. Si une correspondance est trouvée, le système génère une détection rétrospective.

- 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 sections du système RevealX qui présentent les indicateurs de compromission détectés dans vos collections de menaces :

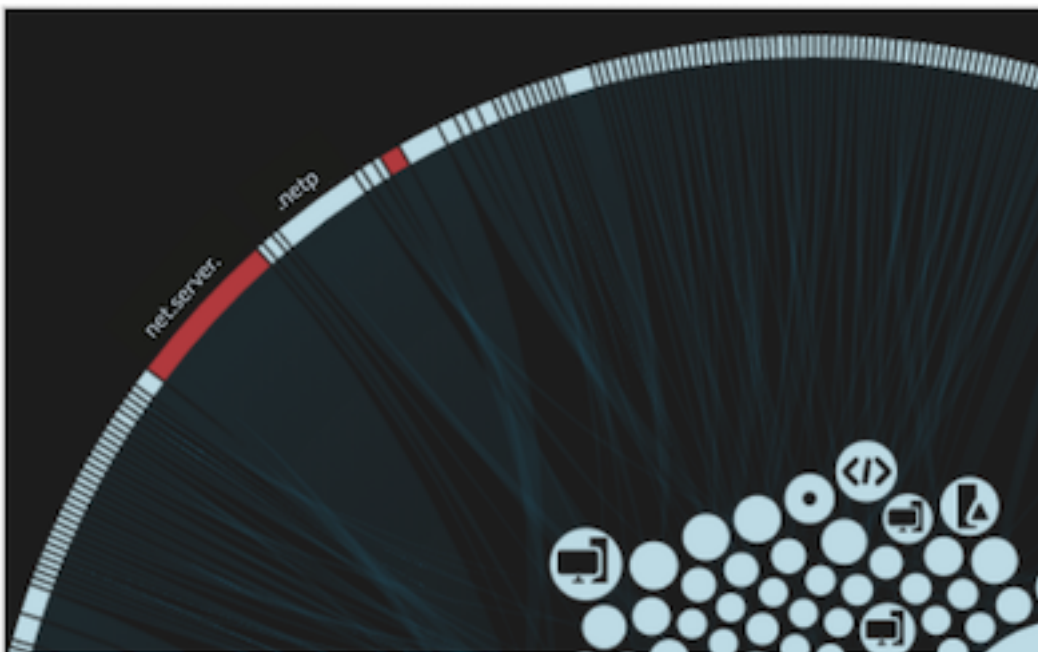
Tableau de bord de renforcement de la sécurité

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



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.

94

RISK

SUNBURST C&C Activity

COMMAND & CONTROL

Dec 12 15:04 • lasting a few seconds

[west.example](#) attempted to access a host associated with the backdoor known as SUNBURST or Solorigate, indicating command-and-control (C&C) activity. The SUNBURST backdoor affects SolarWinds Orion Platform versions 2019.4 through 2020.2 HF 1.

☠

OFFENDER

IP

34.223.124.45

suspicious-example.com

MALICIOUS

🎯

VICTIM

IP

west.example

10.4.15.49

Site: West 2

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.


IP Address Details

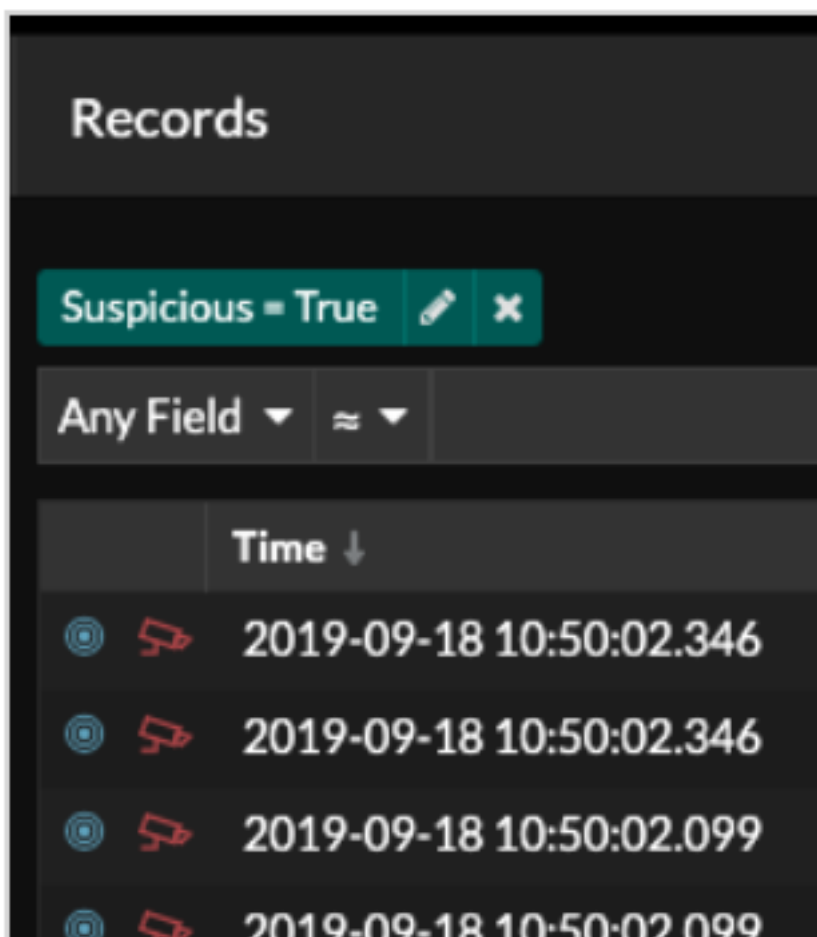
External Endpoint
Moondarra, Victoria, Australia

SUSPICIOUS	Threat Intelligence Indicator for 220.252.189.126
Title	IP: 38.236.216.22
Description	IP 119.74.30.120 reported from Threat Intel List
Type	IP Watchlist
Confidence	Medium
Collection	BitNodes Collection
Producer	Threat Intel List
Added	April 12, 2021 10:11 PM NDT

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

(RevealX 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.