

Briefings sur les menaces

Publié: 2024-01-31

Les briefings sur les menaces fournissent des conseils sur les menaces potentielles qui pèsent sur votre réseau.

Les séances d'information sur les menaces portent sur les événements suivants :

- Événements de sécurité à l'échelle du secteur, au cours desquels le système ExtraHop détecte des détections liées à des compromissions connues.
- Briefings d'analyse de sécurité, qui fournissent une analyse de l'apprentissage automatique spécifique à votre réseau.
- (Reveal (x) 360 uniquement.) Des séances d'analyse rétrospective des menaces, qui permettent de détecter de nouveaux indicateurs de compromission dans les collections actualisées de renseignements sur les menaces organisées par ExtraHop.

Les briefings sur les menaces contiennent des détections de scans, d'exploits et d'indicateurs de compromission (IOC) liés à la menace. Les informations contenues dans chaque briefing varient en fonction du type de menace. Les informations relatives au briefing sont mises à jour dans le cloud à mesure que des informations apparaissent sur les indicateurs de compromission, les vecteurs d'attaque potentiels et les risques connus.

Des informations sur les menaces sont disponibles dans le coin supérieur gauche du [Aperçu de la sécurité](#) page. Cliquez sur n'importe quel titre pour accéder à la page détaillée de ce briefing. La page détaillée est mise à jour à mesure que de nouvelles informations sont découvertes.

Voici quelques moyens de suivre les briefings sur les menaces :

- [Création d'une règle de notification des informations sur les menaces](#) pour recevoir des e-mails lorsqu'une nouvelle information sur les menaces apparaît.
- Cliquez **Créer une enquête** depuis la page détaillée pour ajouter les détections associées au briefing à une enquête.
- Cliquez **Exposé sur les archives** depuis la page détaillée lorsque vous ne souhaitez plus suivre le briefing ; le briefing est automatiquement restauré et un e-mail de notification est envoyé si le briefing est mis à jour. Vous pouvez consulter les anciens briefings dans la section Archivé de la page Threat Briefing. Cliquez **Briefing de restauration** sur la page détaillée pour replacer le briefing dans la section Active de la page Threat Briefing.