Scores de risque

Publié: 2023-10-24

Un indice de risque numérique associé à un niveau de gravité est attribué aux détections. Les scores de risque vous permettent de trier rapidement les détections en fonction du risque potentiel qu'elles présentent pour votre réseau .

Voici quelques considérations concernant l'utilisation des scores de risque :

- Certaines détections sont éligibles à scores de risque dynamiques, qui sont ajustés en fonction des observations de l'apprentissage automatique.
- Les détections peuvent être filtré ou trié par indice de risque sur la page Détections.
- Règles de notification peut être créé sur la base d'un critère d'indice de risque minimal.
- Les scores de risque accompagnent les marqueurs de détection des dispositifs dans cartes d'activités et sur aperçu de l'équipement pages.

Les sections suivantes fournissent des informations sur la manière dont le système ExtraHop calcule les scores de risque .

Facteurs de risque

Le système ExtraHop attribue à chaque détection un indice de risque basé sur une combinaison de trois facteurs qui évaluent la menace identifiée lors de la détection : probabilité, complexité et impact commercial. Un niveau faible, moyen ou élevé est attribué à chacun de ces facteurs.

Ces facteurs sont combinés pour obtenir un indice de risque numérique pour chaque type de détection. Vous pouvez consulter le niveau de chaque facteur sur le page détaillée de détection.

Probabilité

La probabilité mesure la probabilité qu'une attaque se produise. Les attaques qui nécessitent une planification ou des ressources importantes, telles que l'acquisition de privilèges élevés, ont une probabilité faible. Les attaques qui ciblent des surfaces d'attaque étendues et exposées, ou des vulnérabilités régulièrement exploitées, se voient attribuer une probabilité élevée. Un facteur de risque à probabilité élevée indique une menace commune et fiable, ce qui se traduit par un indice de risque plus élevé.

Complexité

La complexité mesure le niveau de compétence requis pour exécuter une attaque. Les attaques qui nécessitent un minimum de compétences, des techniques peu sophistiquées ou qui peuvent être exécutées à l'aide d'outils accessibles au public se voient attribuer une complexité faible. Les

attaques qui nécessitent un attaquant expérimenté, des outils spécialisés et des techniques avancées se voient attribuer une complexité élevée. Un facteur de risque de complexité élevé indique un délinquant averti capable d'atteindre ses objectifs furtivement, ce qui se traduit par un indice de risque plus élevé.

Impact commercial

L'impact commercial mesure les effets négatifs qu'une attaque peut avoir sur les activités de l'entreprise. Les attaques qui n'affectent pas les opérations commerciales, telles que les scans de reconnaissance et les énumérations, ont un impact commercial faible. Les attaques susceptibles d'entraîner la perte de données ou de systèmes importants, telles que le chiffrement par rançongiciel, ont un impact commercial élevé. Un facteur de risque d' impact commercial élevé indique une attaque susceptible de compromettre les opérations commerciales, ce qui se traduit par un indice de risque plus élevé.

Bien que les scores de risque puissent fournir une estimation de la gravité des risques de sécurité, les scores de risque ne remplacent pas la prise de décision ou l'expertise concernant votre réseau. Révisez toujours sécurité détections pour déterminer la cause première d'un comportement inhabituel et le moment opportun pour agir.

Score de gravité du risque

Les scores de risque sont regroupés selon l'un des niveaux de gravité codés par couleur suivants :

Rouge (80-99)

Les scores de risque rouges sont attribués aux détections qui constituent une grave menace pour votre environnement et doivent faire l'objet d'une recherche immédiate. Par exemple, le rançongiciel, l' exfiltration de données et les failles de vulnérabilité qui peuvent avoir un impact significatif sur votre activité.

Orange (31-79)

Les scores de risque orange sont attribués aux menaces ou aux problèmes de sécurité qui doivent être évalués pour atténuer les dommages potentiels. Par exemple, des détections de reconnaissance telles que des scans et des énumérations, des détections basées sur des renseignements sur les menaces ou des rappels de maintenance concernant des suites de chiffrement SSL/TLS faibles et des certificats de serveur SSL expirés.

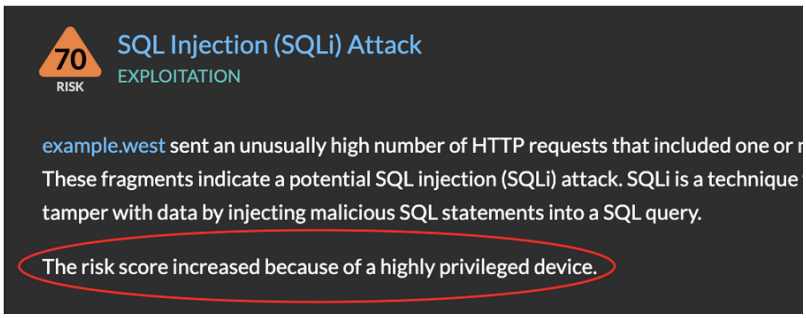
Jaune (1-30)

Les scores de risque jaunes sont attribués aux détections dont le potentiel d'impact sur votre réseau est extrêmement faible.

Scores de risque dynamiques

Si une détection est éligible à un indice de risque dynamique, le service d'apprentissage automatique peut augmenter ou diminuer l'indice de risque pour refléter la présence de participants ou de modèles spécifiques dans votre environnement.

Lorsqu'un indice de risque est ajusté, la carte de détection affiche une explication du changement :



L'indice de risque peut être ajusté pour l'une des raisons suivantes.

Appareils de grande valeur

Les scores de risque sont augmentés lorsque l'un des participants est un équipement à valeur élevée. Un équipement est considéré comme ayant une valeur élevée si le système ExtraHop observe que le dispositif fournit une authentification ou d'autres services essentiels. Les utilisateurs peuvent également spécifier manuellement un équipement avec une valeur élevée, ce qui peut également affecter l'indice de risque.

Niveau de privilège

Les scores de risque sont augmentés lorsque l'un des participants dispose d'un niveau de privilège élevé. Le privilège est une mesure de l'accès d'un utilisateur aux services et aux appareils. Par exemple, un niveau de privilège élevé serait attribué à un équipement associé à un compte administrateur qui accède à des appareils distants ou de grande valeur via des protocoles administratifs tels que le SSH. Si un attaquant compromet un équipement associé à un niveau de privilège élevé, l'impact potentiel sur le réseau est plus important.

Scanners de vulnérabilité

Les scores de risque sont abaissés lorsqu'un ou plusieurs délinquants utilisent un scanner de vulnérabilité.

Taille du transfert

Les scores de risque liés aux détections relatives au transfert de données, telles que l'exfiltration ou la collecte de données, sont augmentés ou abaissés lorsque le volume relatif de données est significativement différent des autres détections du même type.