Risikobewertungen

Veröffentlicht: 2023-10-24

Erkennungen wird eine numerische Risikoscore zugewiesen, die einem Schweregrad zugeordnet ist. Mithilfe von Risikobewertungen können Sie Erkennungen schnell anhand ihres potenziellen Risikos für Ihr Netzwerk einstufen.

Hier sind einige Überlegungen zur Arbeit mit Risikoeinstufungen:

- Bestimmte Erkennungen kommen in Frage für dynamische Risikobewertungen, die auf der Grundlage von Beobachtungen des maschinellen Lernens angepasst werden.
- Erkennungen können sein gefiltert oder sortiert nach Risikoscore auf der Seite Erkennungen.
- Regeln für Benachrichtigungen kann auf der Grundlage eines Mindestkriteriums für die Risikoscore erstellt werden.
- Risikobewertungen begleiten Erkennungsmarkierungen für Geräte in Aktivitätskarten und weiter Geräteübersicht Seiten.

Die folgenden Abschnitte enthalten Informationen darüber, wie das ExtraHop-System Risikobewertungen berechnet.

Risikofaktoren

Das ExtraHop-System weist jeder Entdeckung eine Risikoscore zu, die auf einer Kombination von drei Faktoren basiert, mit denen die bei der Erkennung identifizierte Bedrohung bewertet wird: Wahrscheinlichkeit, Komplexität und geschäftliche Auswirkungen. Jedem dieser Faktoren wird ein niedriger, mittlerer oder hoher Wert zugewiesen.

Diese Faktoren werden kombiniert, um eine numerische Risikoscore für jeden Erkennungstyp abzuleiten. Sie können die Stufe jedes Faktors auf der Detailseite zur Erkennung.

Wahrscheinlichkeit

Die Wahrscheinlichkeit misst die Wahrscheinlichkeit, mit der ein Angriff stattfindet. Angriffen, die umfangreiche Planung oder Ressourcen erfordern, wie z. B. der Erwerb erweiterter Rechte, wird eine geringe Wahrscheinlichkeit zugewiesen. Angriffen, die auf große und exponierte Angriffsflächen oder routinemäßig ausgenutzte Sicherheitslücken abzielen, wird eine hohe Wahrscheinlichkeit zugewiesen. Ein Risikofaktor mit hoher Wahrscheinlichkeit weist auf eine gemeinsame und zuverlässige Bedrohung hin, was zu einer höheren Risikoscore führt.

Komplexität

Die Komplexität misst das Qualifikationsniveau, das für die Durchführung eines Angriffs erforderlich ist. Angriffen, die nur minimale Fähigkeiten und unkomplizierte Techniken erfordern oder die mit öffentlich verfügbaren Tools ausgeführt werden können, wird eine Komplexität von gering zugewiesen. Angriffen, die einen erfahrenen Angreifer, spezielle Tools und fortgeschrittene Techniken erfordern, wird eine hohe Komplexität zugewiesen. Ein Risikofaktor mit hoher Komplexität weist auf einen raffinierten Täter hin, der in der Lage ist, Ziele heimlich zu erreichen, was zu einer höheren Risikoscore führt.

Auswirkungen auf das Geschäft

Business Impact misst die negativen Auswirkungen, die ein Angriff auf den Geschäftsbetrieb haben kann. Angriffen, die den Geschäftsbetrieb nicht beeinträchtigen, wie z. B. Aufklärungsscans und Aufzählungen, wird eine geringe Auswirkung auf das Geschäft zugewiesen. Angriffen, die zum Verlust bedeutender Daten oder Systeme führen können, wie z. B. Ransomware-Verschlüsselung, wird eine hohe Auswirkung auf das Geschäft zugeschrieben. Ein hoher Risikofaktor für geschäftliche Auswirkungen weist auf einen Angriff hin, der den Geschäftsbetrieb gefährden kann, was zu einer höheren Risikoscore führt.

Risikobewertungen können zwar den geschätzten Schweregrad von Sicherheitsrisiken angeben, aber Risikoeinstufungen ersetzen nicht die Entscheidungsfindung oder das Fachwissen über Ihr Netzwerk. Immer überprüfen Sicherheit Erkennungen, um die Ursache für ungewöhnliches Verhalten zu ermitteln und zu ermitteln, wann Maßnahmen ergriffen werden müssen.

Schweregrad der Risikobewertung

Die Risikoeinstufungen werden in einen der folgenden farbcodierten Schweregrad eingeteilt:

Rot (80-99)

Rote Risikoeinstufungen werden Erkennungen zugewiesen, die eine ernste Bedrohung für Ihre Umgebung darstellen, und sollten umgehend untersucht werden. Zum Beispiel Ransomware, Datenexfiltration und Ausnutzung von Schwachstelle, die Ihr Unternehmen erheblich beeinträchtigen können.

Orange (31-79)

Orangefarbene Risikobewertungen werden Bedrohungen oder Sicherheitsproblemen zugewiesen, die bewertet werden sollten, um potenziellen Schaden zu minimieren. Zum Beispiel Aufklärungserkennungen wie Scans und Aufzählungen, Erkennungen auf der Grundlage von Bedrohungsinformationen oder Wartungserinnerungen über schwache SSL/TLS-Verschlüsselungssammlungen und abgelaufene SSL-Serverzertifikate.

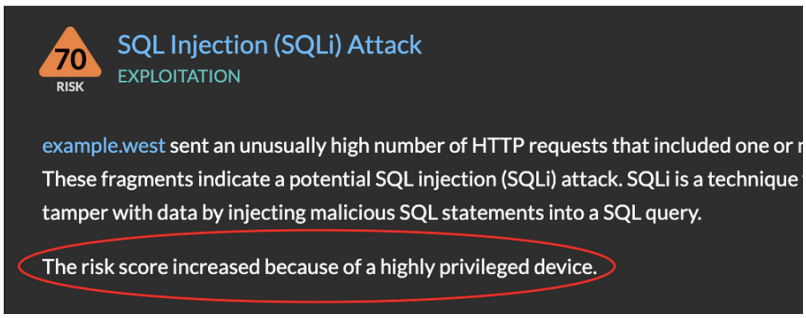
Gelb (1-30)

Gelbe Risikobewertungen werden Erkennungen zugewiesen, die ein extrem geringes Potenzial für Auswirkungen auf Ihr Netzwerk haben.

Dynamische Risikobewertungen

Wenn eine Erkennung für eine dynamische Risikoscore in Frage kommt, kann der Machine Learning Service die Risikoscore erhöhen oder senken, um das Vorhandensein bestimmter Teilnehmer oder Muster in Ihrer Umgebung widerzuspiegeln.

Wenn eine Risikoscore angepasst wird, zeigt die Erkennungskarte eine Erklärung für die Änderung an:



Die Risikoscore kann aus einem der folgenden Gründe angepasst werden.

Hochwertige Geräte

Die Risikobewertung wird erhöht, wenn es sich bei einem der Teilnehmer um ein hoher Wert Gerät handelt. Ein Gerät wird als hoher Wert eingestuft, wenn das ExtraHop-System beobachtet, dass das Gerät Authentifizierung oder andere wichtige Dienste bereitstellt. Benutzer können auch manuell ein Gerät als hohen Wert angeben, was sich auch auf die Risikoscore auswirken kann.

Privilegienstufe

Die Risikobewertung wird erhöht, wenn einer der Teilnehmer über eine hohe Privilegienstufe verfügt. Privilegien sind ein Maß für den Zugriff, den ein Benutzer auf Dienste und Geräte hat. Beispielsweise würde einem Gerät, das mit einem Administratorkonto verknüpft ist, eine hohe Berechtigungsstufe zugewiesen, das über Verwaltungsprotokolle wie SSH auf hochwertige Geräte oder Remote-Geräte zugreift. Wenn ein Angreifer ein Gerät mit einer hohen Rechtestufe kompromittiert, ist die potenzielle Auswirkung auf das Netzwerk höher.

Schwachstellenscanner

Die Risikowerte werden gesenkt, wenn es sich bei einem oder mehreren Tätern um einen Schwachstellenscanner handelt.

Größe der Übertragung

Risikowerte im Zusammenhang mit Erkennungen von Datenübertragungen, wie Datenexfiltration oder Datenvorbereitung, werden erhöht oder gesenkt, wenn sich das relative Datenvolumen erheblich von anderen Erkennungen desselben Typs unterscheidet.