Optimierung von Erkennungen

Veröffentlicht: 2024-02-16

Hier sind einige bewährte Methoden, die Sie anwenden sollten, um Ihre Erkennungen zu verbessern: Fügen Sie Details zu Ihrem Netzwerk hinzu, aktivieren Sie das ExtraHop-System, um potenziell verdächtigen Datenverkehr zu erkennen, und filtern Sie Ihre Seitenaufrufe nach Ihren Prioritäten.

Die meisten dieser Einstellungen bieten Kontext zu Ihrem Netzwerk, den Sie bereitstellen können, um sowohl maschinelles Lernen als auch regelbasierte Erkennungen zu verbessern. Diese Einstellungen werden manchmal übersehen und können die Qualität Ihrer Erkennungen beeinträchtigen.

Entschlüsselung konfigurieren

Verschlüsselter HTTP-Verkehr ist ein häufiger Angriffsvektor, auch weil Angreifer wissen, dass der Datenverkehr normalerweise versteckt ist. Und wenn Ihr Netzwerk über Active Directory verfügt, verbergen sich eine Reihe von Erkennungen im verschlüsselten Datenverkehr in der gesamten Domäne.

Wir empfehlen dringend, die Entschlüsselung für zu aktivieren SSL/TLS und Active Directory.

Tuning-Parameter konfigurieren

Diese Einstellung verbessert die Genauigkeit regelbasierter Erkennungen. Du das ExtraHop-System mit Details versorgen über Ihre Netzwerkumgebung, um einen Kontext zu den beobachteten Geräten bereitzustellen.

Beispielsweise wird eine regelbasierte Erkennung generiert, wenn ein internes Gerät mit externen Datenbanken kommuniziert. Wenn Datenverkehr zu einer externen Datenbank erwartet wird oder die Datenbank Teil einer legitimen cloudbasierten Speicher- oder Produktionsinfrastruktur ist, können Sie einen Optimierungsparameter festlegen, um den Datenverkehr zur genehmigten externen Datenbank zu ignorieren.

Netzwerkstandorte konfigurieren

Mit dieser Einstellung können Sie intern oder extern klassifizieren Endpunkte und Domänen, denen Sie vertrauen, z. B. eine vertrauenswürdige Domain, mit der Ihre Geräte regelmäßig eine Verbindung herstellen. Erkennungen durch maschinelles Lernen und Systemmetriken basieren auf Gerät- und Verkehrsklassifizierungen.

Wenn Ihre Geräte beispielsweise regelmäßig eine Verbindung zu einer unbekannten, aber vertrauenswürdigen Domain herstellen, die als externe IP-Adresse klassifiziert ist, werden Erkennungen für diese Domain unterdrückt.

Erkennungen optimieren

Mit diesen Einstellungen können Sie Erkennungen ausblenden oder unterdrücken nachdem das System sie generiert hat. Wenn Sie eine Erkennung sehen, die keinen Mehrwert bietet, können Sie das Rauschen in Ihrer Gesamtansicht reduzieren.

Wenn eine Erkennung beispielsweise anhand eines Täters, eines Opfers oder anderer Kriterien generiert wird, die für Ihr Netzwerk nicht von Belang sind, können Sie alle früheren und zukünftigen Erkennungen mit diesen Kriterien ausblenden.

Externe Klartext-Daten teilen

Mit dieser Option kann der Machine Learning Service IP-Adressen, Hostnamen und Domains sammeln die mit verdächtigen Aktivitäten verbunden sind.

Wenn Sie diese Option aktivieren, erweitern Sie einen kollektiven Datensatz potenzieller Bedrohungen, die Ihnen helfen und einen Beitrag zur Sicherheitsgemeinschaft leisten können.

Erkennungen nachverfolgen

Mit dieser Option können Sie Weisen Sie einem Benutzer eine Erkennung zu, fügen Sie Notizen hinzu und aktualisieren Sie den Status von bestätigt bis geschlossen. Anschließend können Sie die

Erkennungsseite filtern, um gelöste Probleme aus der Ansicht zu löschen oder um nach Erkennungen zu suchen.