Erkennungen optimieren

Veröffentlicht: 2024-07-17

Hier sind einige bewährte Methoden, die Sie implementieren sollten, um Ihre Erkennungen zu verbessern: Fügen Sie Details zu Ihrem Netzwerk hinzu, aktivieren Sie das ExtraHop-System, potenziell verdächtigen Traffic 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 Verkehr in der Regel versteckt ist. Und wenn Ihr Netzwerk über Active Directory verfügt, sind eine Reihe von Erkennungen im verschlüsselten Datenverkehr in der gesamten Domain versteckt.

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 den 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 Cloud-basierten 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, denen Sie vertrauen, z. B. ein CIDR-Block von IP-Adressen, mit denen Ihre Geräte regelmäßig eine Verbindung herstellen. Erkennungen und Systemmetriken durch maschinelles Lernen basieren auf Gerät- und Verkehrsklassifizierungen.

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

Tuning-Regeln erstellen

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

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

Teilen Sie externe Klartext-Daten

Mit dieser Option kann der Machine Learning Service Erfassen Sie IP-Adressen, Hostnamen und Domains die mit verdächtigen Aktivitäten in Verbindung stehen.

Wenn Sie diese Option aktivieren, erweitern Sie einen kollektiven Datensatz potenzieller Bedrohungen, der Ihnen und Ihrem Beitrag zur Sicherheitsgemeinschaft helfen kann.

Erkennungen verfolgen

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 Seite „Erkennungen“ filtern, um gelöste Probleme aus der Ansicht zu entfernen oder die Erkennungen zu überprüfen.