Dashboard zur Erhöhung der Sicherheit

Veröffentlicht: 2024-02-12

Mit dem Security Hardening-Dashboard können Sie allgemeine Informationen über potenzielle Sicherheitsbedrohungen in Ihrem Netzwerk überwachen.

Jedes Diagramm im Security Hardening-Dashboard enthält Visualisierungen von Sicherheitsdaten, die über den ausgewähltes Zeitintervall, nach Region organisiert.

Hinweis Von einer Konsole aus können Sie das Security Hardening-Dashboard für jeden Paketsensor anzeigen. Klicken Sie in der Navigationsleiste neben dem Namen des Sensor auf den Abwärtspfeil, um das Security Hardening-Dashboard für andere Sensoren anzuzeigen.

Das Security Hardening-Dashboard ist ein integriertes System-Dashboard, das Sie nicht bearbeiten, löschen oder einer gemeinsamen Sammlung hinzufügen können. Sie können jedoch ein Diagramm kopieren aus dem Security Hardening-Dashboard und füge es zu einem benutzerdefiniertes Dashboard, oder du kannst eine Kopie des Dashboard erstellen und bearbeiten Sie es, um Kennzahlen zu überwachen, die für Sie relevant sind.

Die folgenden Informationen fassen jede Region und ihre Diagramme zusammen.

Bedrohungsinformationen

Beobachten Sie die Anzahl der Verbindungen und Transaktionen, die verdächtige Hostnamen, IP-Adressen oder URIs enthalten, die in Bedrohungsinformationen. Klicken Sie in der Legende auf einen blauen Metrikwert oder einen Metriknamen, um nach einer verdächtigen Metrik zu suchen. Eine Detailseite mit einem roten Kamerasymbol wird angezeigt neben dem verdächtigen Objekt. Klicken Sie auf das rote Kamerasymbol, um mehr über die Quelle der Bedrohungsinformationen zu erfahren.

Hinweis Bedrohungsanalyse-Metriken zeigen aus einem oder mehreren der folgenden Gründe einen Nullwert an:

- Ihr ExtraHop Reveal (x) -Abonnement beinhaltet keine Bedrohungsinformationen.
- Sie haben die Bedrohungsinformationen für Ihr ExtraHop Reveal (x) -System nicht aktiviert.
- Sie haben benutzerdefinierte Bedrohungssammlungen nicht direkt in Ihre hochgeladen Sensoren. Wenden Sie sich an den ExtraHop-Support, wenn Sie Hilfe beim Hochladen einer benutzerdefinierten Bedrohungssammlung auf Ihre von ExtraHop verwaltete Sammlung benötigen Sensoren.
- Es wurden keine verdächtigen Gegenstände gefunden.

SSL - Sitzungen

Beobachten Sie die Anzahl der aktiven SSL-Sitzungen mit Schwache Verschlüsselung Verschlüsselungssammlungen in Ihrem Netzwerk. Sie können sehen, welche Clients und Server an diesen Sitzungen teilnehmen und mit welchen Verschlüsselungssammlungen diese Sitzungen verschlüsselt sind. DES-, 3DES-, MD5-, RC4-, Null-, Anonym- und Export-Cipher Suites gelten als schwach, da sie einen Verschlüsselungsalgorithmus enthalten, der bekanntermaßen anfällig ist. Daten, die mit einer Schwache Verschlüsselung Verschlüsselungssuite verschlüsselt wurden, sind potenziell unsicher.

Sie können auch die Anzahl der SSL-Sitzungen beobachten, die mit TLS v1.0 eingerichtet wurden, und welche Clients an diesen Sitzungen teilnehmen. Bekannte Sicherheitslücken stehen im Zusammenhang mit TLS v1.0. Wenn Sie eine hohe Anzahl von TLS v1.0-Sitzungen haben, sollten Sie erwägen, Server so zu konfigurieren, dass sie die neueste Version von TLS unterstützen.

SSL - Zertifikate

Beobachten Sie, welche SSL-Zertifikate in Ihrem Netzwerk selbstsigniert sind, Platzhalter sind, abgelaufen sind und bald ablaufen. Selbstsignierte Zertifikate werden von der Entität signiert, die

das Zertifikat ausstellt, und nicht von einer vertrauenswürdigen Zertifizierungsstelle. Selbstsignierte Zertifikate sind zwar günstiger als Zertifikate, die von einer Zertifizierungsstelle ausgestellt wurden, aber sie sind auch anfällig für Man-in-the-Middle-Angriffe.

Ein Platzhalterzertifikat gilt für alle Subdomains der ersten Ebene eines bestimmten Domänenname. Das Platzhalterzertifikat *.company.com schützt beispielsweise www.company.com, docs.company.com und customer.company.com. Wildcard-Zertifikate sind zwar günstiger als Einzelzertifikate, aber Wildcard-Zertifikate bergen ein höheres Risiko, wenn sie kompromittiert werden, da sie für eine beliebige Anzahl von Domänen gelten können.

Schwachstellen-Scans

Beobachten Sie, welche Geräte Anwendungen und Systeme in Ihrem Netzwerk scannen, um nach Schwachstellen und potenziellen Zielen, wie z. B. hoher Wert Geräten, zu suchen. In der linken Tabelle können Sie erkennen, welche Geräte die meisten Scananfragen senden. Dabei handelt es sich um HTTP-Anfragen, die mit bekannten Scanneraktivitäten verknüpft sind. Im rechten Diagramm können Sie sehen, welche Benutzeragenten mit den Scananfragen verknüpft sind. Der User-Agent kann Ihnen dabei helfen, festzustellen, ob Scananfragen mit bekannten Schwachstellenscannern wie Nessus und Qualys verknüpft sind.

DNS

Beobachten Sie, welche DNS-Server in Ihrem Netzwerk am aktivsten sind und wie viele Reverse-DNS-Lookup-Fehler auf diesen Servern insgesamt aufgetreten sind. Ein Reverse-DNS-Lookup-Fehler tritt auf, wenn ein Server als Antwort auf eine Client-Anfrage nach einem Pointer-Record (PTR) einen Fehler ausgibt. Fehler bei Reverse-DNS-Lookups sind normal, aber eine plötzliche oder stetige Zunahme von Ausfällen auf einem bestimmten Host kann darauf hindeuten, dass ein Angreifer Ihr Netzwerk scannt.

Sie können auch die Anzahl der Adresszuordnungs- und Textdatensatzabfragen in Ihrem Netzwerk beobachten. Ein starker oder plötzlicher Anstieg dieser Arten von Abfragen kann ein Indikator für einen potenziellen DNS-Tunnel sein.