Überblick über die Sicherheit

Veröffentlicht: 2024-07-17

In der Sicherheitsübersicht werden mehrere Diagramme angezeigt, in denen Daten zu Erkennungen aus unterschiedlichen Perspektiven dargestellt werden. Mithilfe dieser Diagramme können Sie den Umfang der Sicherheitsrisiken einschätzen, Untersuchungen zu ungewöhnlichen Aktivitäten einleiten und Sicherheitsbedrohungen eindämmen. Erkennungen werden je nach Metrik alle 30 Sekunden oder jede Stunde analysiert.

Video: Sehen Sie sich die entsprechende Schulung an: Überblick über Sicherheit, Netzwerk und Perimeter

Für Triage empfohlen

Dieses Diagramm zeigt Ihnen eine Liste von Erkennungen, die ExtraHop auf der Grundlage einer kontextuellen Analyse Ihrer Umgebung empfiehlt. Klicken Sie auf eine Erkennung, um die Erkennungskarte in Triage-Ansicht auf der Seite „Erkennungen“.

Ermittlungen

Dieses Diagramm zeigt die Anzahl der Untersuchungen, die während des ausgewählten Zeitintervalls erstellt wurden. Die Zählung beinhaltet Untersuchungen, die von ExtraHop empfohlen oder von Benutzern erstellt wurden. Klicken Sie auf das Diagramm, um das zu sehen Tabelle der Untersuchungen auf der Seite „ Erkennungen“.

Erkennungen nach Angriffskategorie

Dieses Diagramm bietet einen schnellen Überblick über die Arten von Angriffen, für die Ihr Netzwerk möglicherweise gefährdet ist, und zeigt die Anzahl der Erkennungen an, die in jeder Kategorie während des ausgewählten Zeitintervalls aufgetreten sind. Die Aktionen bei objektiven Erkennungen sind nach Typ aufgelistet, damit Sie die schwerwiegendsten Erkennungen priorisieren können. Klicken Sie auf eine beliebige Zahl, um eine gefilterte Ansicht der Erkennungen zu öffnen, die mit der ausgewählten Zahl übereinstimmen Kategorie des Angriffs.

Häufige Straftäter

Dieses Diagramm zeigt die 20 Geräte oder Endgeräte, die bei einer oder mehreren Erkennungen als Straftäter fungierten. Das ExtraHop-System berücksichtigt die Anzahl der verschiedenen Angriffskategorien und Erkennungstypen sowie die Risikobewertung der mit jedem Gerät verbundenen Erkennungen, um festzustellen, welche Geräte als häufige Straftäter gelten.

Die Größe des Geräterollensymbols gibt die Anzahl der verschiedenen Erkennungstypen an, und die Position des Symbols gibt die Anzahl der verschiedenen Angriffskategorien an. Klicken Sie auf ein Rollensymbol, um weitere Informationen zu den Angriffskategorien und Erkennungstypen anzuzeigen, die mit dem Gerät verknüpft sind. Klicken Sie auf den Gerätenamen, um ihn anzuzeigen Eigenschaften Gerät.

Erfahren Sie mehr über Netzwerksicherheit mit dem Dashboard zur Erhöhung der Sicherheit.

Bedrohungsinformationen

Threat Briefings bieten in der Cloud aktualisierte Hinweise zu branchenweiten Sicherheitsereignissen. Erfahren Sie mehr über Bedrohungsinformationen.

Standortauswahl und Bericht über Sicherheitsoperationen

Auf dieser Seite können Sie die Websites angeben, von denen Sie Daten anzeigen möchten. Benutzer mit Zugriff auf das NDR-Modul können einen Security Operations Report erstellen, um die Ergebnisse zu teilen.

Seitenauswahl

Klicken Sie oben auf der Seite auf die Seitenauswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Traffic in Ihren Netzwerken an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl zeigt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, werden in den Diagrammen und Geräteseiten, die Offlineseiten zugeordnet sind, möglicherweise keine oder nur begrenzte Daten angezeigt. Der Site-Selector ist nur von einem verfügbar Konsole.

(nur NDR-Modul) Sicherheitsbetriebsbericht

Der Security Operations Report enthält eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk. klicken **Bericht generieren** um das Zeitintervall und die Standorte anzugeben, die in den Bericht aufgenommen werden sollen, klicken Sie dann auf **Generieren** um eine PDF-Datei zu erstellen. klicken **Bericht planen** um einen Security Operations Report zu erstellen, der per E-Mail an die Empfänger gesendet wird gemäß die konfigurierte Frequenz.