Überblick über die Sicherheit

Veröffentlicht: 2023-11-13

In der Sicherheitsübersicht werden mehrere Diagramme angezeigt, in denen Daten zu Erkennungen aus unterschiedlichen Perspektiven hervorgehoben werden. Diese Diagramme können Ihnen dabei helfen, das Ausmaß der Sicherheitsrisiken einzuschätzen, Untersuchungen ungewöhnlicher Aktivitäten einzuleiten und Sicherheitsbedrohungen zu mindern. Erkennungen werden je nach Metrik alle 30 Sekunden oder jede Stunde analysiert.

Für Triage empfohlen

Dieses Diagramm zeigt Ihnen eine Liste der 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.

Erkennungstypen

Dieses Diagramm zeigt die Anzahl der verschiedenen Erkennungstypen, die in den Kategorien Attack, Hardening und Operations während des ausgewählten Zeitintervalls aufgetreten sind. Wenn Sie das Zeitintervall ändern, können Sie sehen, wie viele Erkennungstypen während dieser Zeit aufgetreten sind. Klicken Sie auf eine Zahl, um die Seite Erkennungen zu öffnen, die gefiltert ist, sodass die Erkennungen für jeden Typ in der ausgewählten Erkennungskategorie angezeigt werden.

Erkennungen nach Angriffskategorie

Dieses Diagramm bietet einen schnellen Überblick über die Arten von Angriffen, denen Ihr Netzwerk ausgesetzt sein könnte, und zeigt die Anzahl der Erkennungen an, die in jeder Kategorie während des ausgewählten Zeitintervalls aufgetreten sind. Aktionen bei objektiven Erkennungen sind nach Typ sortiert, damit Sie die schwerwiegendsten Erkennungen priorisieren können. Klicken Sie auf eine beliebige Zahl, um eine gefilterte Ansicht der Erkennungen zu öffnen, die der ausgewählten Zahl entsprechen Angriffskategorie.

Häufige Straftäter

Dieses Diagramm zeigt die 20 Geräte oder Endgeräte, die bei einer oder mehreren Erkennungen als Täter gehandelt haben. Das ExtraHop-System berücksichtigt die Anzahl der verschiedenen Angriffskategorien und Erkennungstypen sowie die Risikobewertung der Erkennungen, die mit den einzelnen Gerät verknüpft sind, um festzustellen, welche Geräte als häufige Angreifer 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 dem Gerät zugeordnet sind. Klicken Sie auf den Gerätenamen, um ihn anzuzeigen Geräteeigenschaften.

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 der Geschäftsleitung

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

Seitenauswahl

Klicken Sie oben auf der Seite auf die Site-Auswahl, um Daten für eine oder mehrere Websites in Ihrer Umgebung anzuzeigen. Sehen Sie sich den kombinierten Datenverkehr in Ihren Netzwerken

© 2023ExtraHop Networks, Inc. Alle Rechte vorbehalten.

an oder konzentrieren Sie sich auf einen einzelnen Standort, um Gerätedaten schnell zu finden. Die Seitenauswahl gibt an, wann alle oder einige Websites offline sind. Da Daten von Offline-Websites nicht verfügbar sind, zeigen die mit Offline-Websites verknüpften Diagramme und Geräteseiten möglicherweise keine oder nur begrenzte Daten an. Der Site-Selector ist nur verfügbar von Konsole.

(nur NDR-Modul) Executive Report

Klicken **Bericht für die Geschäftsleitung erstellen** um eine PDF-Datei zu erstellen. Der Executive Report bietet eine Zusammenfassung der wichtigsten Erkennungen und Risiken für Ihr Netzwerk in der letzten Woche. Der Executive Report enthält nur Informationen für die ausgewählten Standorte.