

Überblick über das Netzwerk

Veröffentlicht: 2024-07-17

In der Netzwerkübersicht werden eine Übersicht der Funde in Ihrem Netzwerk sowie eine Liste der Straftäter nach Anzahl der Entdeckungen angezeigt. Die Netzwerkübersicht aktualisiert die Erkennungskarte und die Täterdaten jede Minute.



Sehen Sie sich die entsprechende Schulung an: [Überblick über Sicherheit, Netzwerk und Perimeter](#)

Erkennungskategorie umschalten

Sie können zwischen Ansichten wechseln, die angezeigt werden **Alle Angriffserkennungen** oder **Alle Leistungserkennungen**, abhängig von den aktivierten Modulen und Ihrem Modulzugriff.

Straftäter bei Fahndungen

Diese Liste zeigt Straftäter, sortiert nach der Anzahl der Erkennungen, bei denen das Gerät oder der Endpunkt als Täter gehandelt hat.

Hier sind einige Möglichkeiten, wie Sie mit der Täterliste interagieren können:

- Klicken Sie in der Liste auf ein Gerät oder einen Endpunkt, um die zugehörigen Erkennungen in der Erkennungsübersicht hervorzuheben und die Geräteeigenschaften anzuzeigen und auf Links zuzugreifen [Endpunktsuche](#) Websites, Erkennungen, Aufzeichnungen oder Pakete.
- Abhängig von der ausgewählten Erkennungskategorie und Ihrem Systemmodul klicken Sie auf **Alle Angriffserkennungen anzeigen** oder **Alle Leistungserkennungen anzeigen** Link um zum Erkennungen Seite, [gefiltert nach Erkennungskategorie und gruppiert nach Quelle](#).
- Wählen Sie den **Erkennungen ohne Opfer anzeigen** Kontrollkästchen, um Erkennungen anzuzeigen, an denen kein beteiligtes Opfer Teilnehmer ist. Beispielsweise schließen SSL/TLS-Scans und bestimmte Warnmeldungen bei verdächtigen Aktivitäten nur einen Täter ein.

Erkennungskarte

In der Erkennungsübersicht werden der Täter und das Opfer für alle Erkennungen angezeigt, die im Umschalter für die Erkennungskategorie ausgewählt wurden.

Kreise werden rot hervorgehoben, wenn das Gerät während des ausgewählten Zeitintervalls bei mindestens einer Erkennung als Täter aufgetreten ist, und blaugrün hervorgehoben, wenn es sich bei dem Gerät um ein Opfer handelt.

Die Teilnehmer sind durch Leitungen miteinander verbunden, die mit dem Erkennungstyp oder der Anzahl der mit der Verbindung verbundenen Erkennungen gekennzeichnet sind, und Geräterollen werden durch ein Symbol dargestellt.

Hier sind einige Möglichkeiten, wie Sie mit der Erkennungskarte interagieren können:

- Klicken Sie auf einen Kreis, um die Geräteeigenschaften anzuzeigen und auf Links zuzugreifen [Endpunktsuche](#) Websites, Erkennungen, Aufzeichnungen oder Pakete.
- Klicken Sie auf eine Verbindung, um die zugehörigen Erkennungen anzuzeigen.
- Bewegen Sie den Mauszeiger über einen Kreis, um Gerätebeschriftungen zu sehen und Geräteanschlüsse hervorzuheben.

Erfahre mehr über [Erkennungen](#).


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](#) .