Erkennungen

Veröffentlicht: 2025-02-04

Das ExtraHop-System wendet Techniken des maschinellen Lernens und eine regelbasierte Überwachung Ihrer wire data an, um ungewöhnliche Verhaltensweisen und potenzielle Risiken für die Sicherheit und Leistung Ihres Netzwerk zu identifizieren.

Bevor Sie beginnen
Benutzern muss Folgendes gewährt werden Privilegien um Erkennungen anzuzeigen.

Wenn anomales Verhalten erkannt wird, generiert das ExtraHop-System eine Erkennung und zeigt die verfügbaren Daten und Optionen an. Steuerelemente auf der Seite „Erkennungen“ führen zu folgenden Oberflächenerkennungen: für die Triage empfohlen und helfe dir filtern und sortieren Ihre Ansichten, sodass Sie sich schnell auf Erkennungen im Zusammenhang mit kritischen Systemen konzentrieren können .

Erfahre mehr über Optimierung von Erkennungen.

Wichtig: Obwohl Erkennungen Sie über Sicherheitsrisiken und Leistungsprobleme informieren können, ersetzen Erkennungen nicht die Entscheidungsfindung oder das Fachwissen über Ihr Netzwerk. Immer überprüfen Sicherheit und Performance Erkennungen, um die Ursache für ungewöhnliches Verhalten zu ermitteln und zu ermitteln, wann Maßnahmen ergriffen werden müssen.

Module und Erkennungen

Die Arten von Erkennungen, die Sie in Ihrem ExtraHop-System sehen, hängen von Ihrem Zugriff auf lizenzierte Module ab. Mit dem Modul Netzwerk Performance Monitoring (NPM) können Benutzer Erkennungen im Zusammenhang mit der Netzwerkleistung anzeigen. Mit dem Netzwerk Detection and Response (NDR) -Modul können Benutzer Erkennungen im Zusammenhang mit der Netzwerksicherheit anzeigen.

Mit dem NPM-Modulzugriff können Erkennungen Ihnen auf folgende Weise bei der Wartung Ihres Netzwerk helfen:

- Erfassen Sie hochwertige, verwertbare Daten, um die Ursachen von Netzwerkproblemen zu ermitteln.
- Finden Sie unbekannte Probleme mit Leistung oder Infrastruktur.

Mit dem Zugriff auf das NDR-Modul können Erkennungen Ihnen helfen, Ihr Netzwerk auf folgende Weise zu schützen:

- Identifizieren Sie bösartiges Verhalten, das mit verschiedenen Angriffskategorien oder MITRE-Techniken in Verbindung steht.
- Sehen Sie sich verwandte Erkennungen an oder erstellen Sie Ihre eigenen Untersuchung um Erkennungen zu gruppieren und potenzielle Angriffskampagnen zu verfolgen.
- Kennzeichnen Sie verdächtige IP-Adressen, Hostnamen und URIs, die anhand von Bedrohungsinformationen identifiziert wurden.
- Heben Sie bewährte Methoden zur Erhöhung der Sicherheit hervor.

Video: Sehen Sie sich die entsprechenden Schulungen an:

- Sicherheitserkennungen
- Leistungserkennungen

So werden Erkennungen generiert

Das ExtraHop-System identifiziert Erkennungsaktivitäten anhand von drei unterschiedlichen Methoden: regelbasierte Trigger, Machine-Learning-Modelle und Intrusion Detection System (IDS) -Erkennungen.

Regelbasierte Erkennungen

Regelbasierte Erkennungen identifizieren fragwürdige Netzwerkaktivitäten, indem sie bekannte Muster verdächtigen Datenverkehrs abgleichen.

Regelbasierte Erkennungen werden sofort durch Muster ausgelöst, die mit CVE-Exploit-Versuchen, gängigen Angriffstools, Command-and-Control-Frameworks und Möglichkeiten zur Netzwerkhärtung wie abgelaufenen Zertifikaten oder Schwache Verschlüsselung übereinstimmen.

Du kannst auch eine benutzerdefinierte Erkennung erstellen um Ihre eigenen Erkennungskriterien festzulegen.

Erkennungen durch maschinelles Lernen

Modelle für maschinelles Lernen führen eine Langzeitanalyse des Netzwerkverkehrs durch, um ungewöhnliches Verhalten zu identifizieren.

Die maschinellen Lernmodelle von ExtraHop passen sich dynamisch an Änderungen in Ihrem Netzwerk an und legen neue Grundlinien für das erwartete Verhalten einzelner Geräte sowie Gruppen ähnlicher Geräte fest. Die Modelle für maschinelles Lernen fügen den Erkennungen auch Informationen hinzu, indem sie die Risikobewertungen dynamisch anpassen und hoher Wert Geräte durch Überwachung Gerät Geräteverhaltens identifizieren.

IDS-Erkennungen

Intrusion Detection System (Intrusion Detection System) -Erkennungen treten auf, wenn der Netzwerkverkehr den Signaturen in einem IDS-Regelsatz entspricht.

IDS-Erkennungen erfordern lizenzierte Intrusion Detection System- und NDR-Module und ein IDS-Sensor.

Erkennungsteilnehmer

Teilnehmer sind die Endpunkte, die an der Aktivität beteiligt sind, die eine Erkennung generiert.

Informationen über die Teilnehmer werden aus allen Aktivitäten im Zusammenhang mit der Erkennung gesammelt und auf einem Erkennungskarte wenn eine Erkennung generiert wird.

Erkennungsteilnehmer können interne oder externe Endpunkte sein und werden anhand Gerät Gerätenamens, Hostnamens oder der IP-Adresse identifiziert. Wenn ein Teilnehmer ein anderes Gerät wie einen Load Balancer oder ein Gateway passiert hat, werden sowohl der Teilnehmer als auch das Gerät auf der Teilnehmerkarte angezeigt, aber nur der Ausgangsendpunkt wird als Teilnehmer betrachtet.

IP-Adressen der Teilnehmer

Die IP-Adressen der Teilnehmer werden anhand der Aktivität erfasst, die mit einer Erkennung verbunden ist. Externe Endpunkte werden immer durch eine IP-Adresse dargestellt.

IP-Adressen für erkannte Geräte und externe Endpunkte können sich dynamisch ändern. Die IP-Adresse auf einer Teilnehmerkarte ist in der Regel die IP-Adresse des Täters oder Opfers zum Zeitpunkt der Erkennung. Wenn während der Erkennungsaktivität für ein Gerät keine IP-Adresse beobachtet wird, zeigt die Teilnehmerkarte die letzte IP-Adresse an, die dem Gerät zugeordnet war. Ein Informationsetikett ⓘ wird neben IP-Adressen angezeigt, die bei der Erkennung nicht beobachtet wurden. Auf dem Übersichtsseite für ein Gerät, können Sie alle IP-Adressen anzeigen, die im Laufe der Zeit mit dem Gerät verknüpft wurden.

Nutzernamen der Teilnehmer

Benutzernamen werden aus Aktivitäten im Zusammenhang mit Erkennungen gesammelt, bei denen die Teilnehmer über ein Protokoll kommunizieren, das einen Benutzernamen enthält.

Benutzernamen werden aus dem Protokoll abgerufen, das mit der Erkennung verknüpft ist.

Ein Erkennungsteilnehmer verknüpft nur einen Benutzer mit der Erkennung, aber es kann sein, dass dem Gerät in der Vergangenheit mehrere Benutzer zugeordnet wurden. Sie können den Mauszeiger über einen Teilnehmer bewegen, um den Benutzer zu sehen, der mit der Erkennung verknüpft ist. Klicken Sie dann, um zur Seite „Assets“ zu gelangen und ihn anzuzeigen alle mit dem Gerät verbundenen Benutzer.

Hinweis Benutzernamen können nur in den folgenden Protokollen beobachtet werden: FTP, Kerberos, LDAP, NTLM, RDP, RPC, SMB.

Beschriftungen der Teilnehmer

Die Teilnehmer werden je nach Kontext der Erkennung als Täter und Opfer eingestuft. In der Regel ist der Täter der Teilnehmer, der die Aktivität initiiert hat, die zur Erkennung geführt hat. Bei bestimmten Erkennungen wird das Opfer jedoch als der auslösende Teilnehmer identifiziert, z. B. bei Command-and-Control-Aktivitäten, bei denen ein kompromittiertes Gerät eine Anfrage an einen vom Angreifer kontrollierten Server sendet.

Um die Richtung der Erkennungsaktivität weiter zu verdeutlichen, werden die Teilnehmer auch als Client oder Server für Erkennungen im Zusammenhang mit L7-Protokollen und für andere Protokolle wie NTLM als Sender oder Empfänger gekennzeichnet. Clients und Absender sind in der Regel die Quelle des Datenverkehrs; Server und Empfänger sind das Ziel des Datenverkehrs.

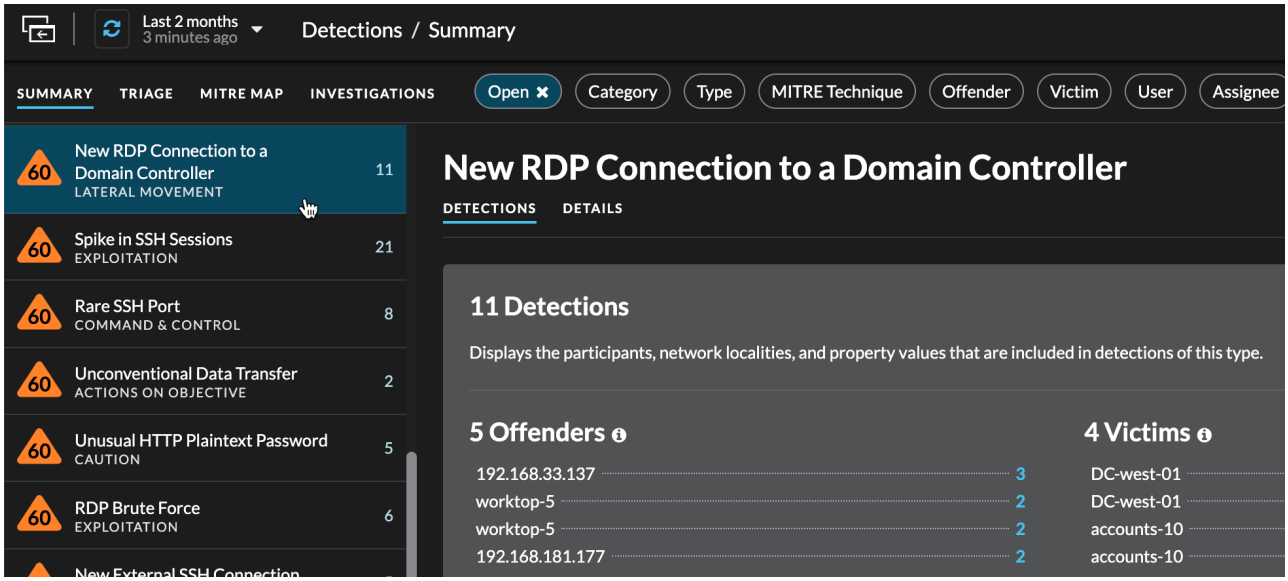
Erkennungen anzeigen

In der oberen linken Ecke der Erkennungsseite gibt es vier Optionen zum Anzeigen von Erkennungen: Zusammenfassung, Triage, MITRE Map und Untersuchungen. Diese Optionen bieten jeweils eine einzigartige Ansicht Ihrer Erkennungsliste.

Zusammenfassung

Standardmäßig werden Erkennungen auf der Seite „Entdeckungen“ in der Zusammenfassungsansicht angezeigt, in der Informationen zu Erkennungen zusammengefasst werden, um Aktivitätsmuster in Ihrer Umgebung hervorzuheben. Sie können Ihre Erkennungsliste in der Zusammenfassungsansicht sortieren und gruppieren, um sich auf häufig auftretende Erkennungstypen und die aktivsten Teilnehmer zu konzentrieren.

Hinweis Standardmäßig ist der **Offen** Der Statusfilter wird angewendet auf Erkennungen Seite. Klicken Sie auf **Offen** Filter, um auf andere zuzugreifen Filteroptionen.

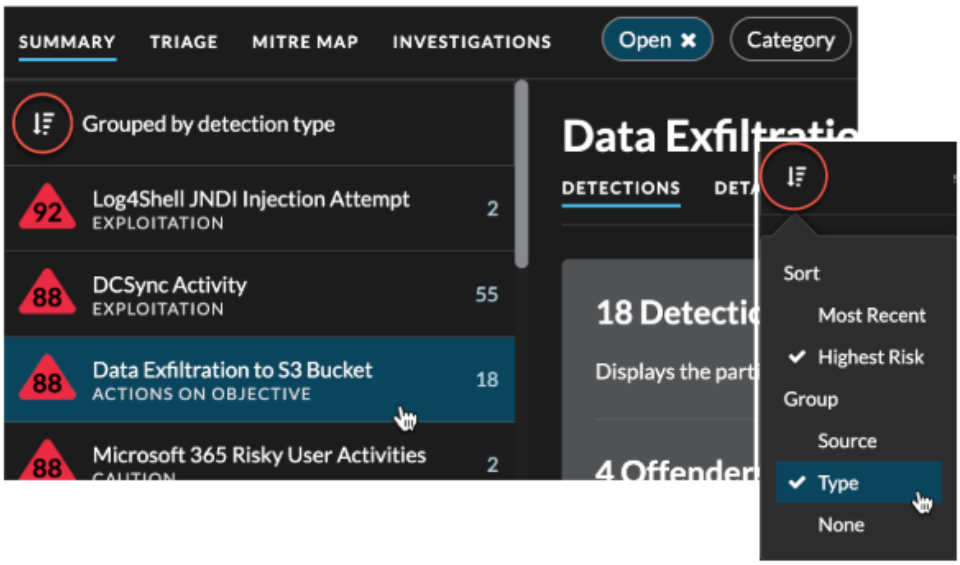


Sortierung von Erkennungen in der Übersichtsansicht
Sie können Erkennungen entweder nach der höchsten Risikoscore oder nach dem jüngsten Ereignis sortieren.

Wenn sie nach Risikobewertung sortiert sind, sind dies Erkennungen für die Triage empfohlen erscheinen zuerst, gefolgt von Entdeckungen mit der höchsten Risikoscore.

Wenn sortiert nach **Aktuellste**, Erkennungen mit der letzten Endzeit werden zuerst angezeigt. Wenn noch zwei Erkennungen andauern, wird die Erkennung mit dem letzten Aktualisierungszeitpunkt zuerst angezeigt. Klicken Sie auf das Sortiersymbol über der Erkennungsliste, um eine Option auszuwählen.

Gruppieren von Funden in der Zusammenfassungsansicht
Sie können Erkennungen nach der Art der Erkennung (z. B. Spike in SSH-Sitzungen) oder nach der Erkennungsquelle (z. B. der IP-Adresse des Täters) gruppieren, oder Sie können festlegen, dass Ihre Erkennungsliste überhaupt nicht gruppiert werden soll.



Nach Typ gruppieren

Bei der Gruppierung der Zusammenfassungsansicht nach **Typ**, können Sie Listen mit Werten anzeigen, die mit Funden verknüpft sind, die während des ausgewählten Zeitintervalls aufgetreten sind, z. B. Teilnehmer, Erkennungseigenschaften oder Netzwerkstandorte .

Sie können auf Teilnehmerwerte klicken, um mehr über das Gerät oder die IP-Adresse zu erfahren. Klicken Sie auf einen beliebigen Wert, um nur Erkennungen anzuzeigen, die mit diesem Wert verknüpft sind, oder Verfolgen Sie alle zugehörigen Erkennungen.

Teilnehmer

Listet alle Täter und Opfer des ausgewählten Erkennungstyps auf. Die Täter- und Opferlisten sind nach der Anzahl der Funde sortiert , bei denen der Teilnehmer auftaucht.

Immobilienwerte

Listet die Eigenschaftswerte auf, die dem Erkennungstyp zugeordnet sind. Die Liste der Eigenschaftswerte ist nach der Anzahl der Funde sortiert, in denen der Eigenschaftswert vorkommt.

Lokalitäten des Netzwerks

Listet die Netzwerkstandorte auf, die Funde des ausgewählten Typs enthalten. Die Liste der Netzwerkstandorte ist nach der Anzahl der Funde in der Netzwerklokalität sortiert.

Nutzer

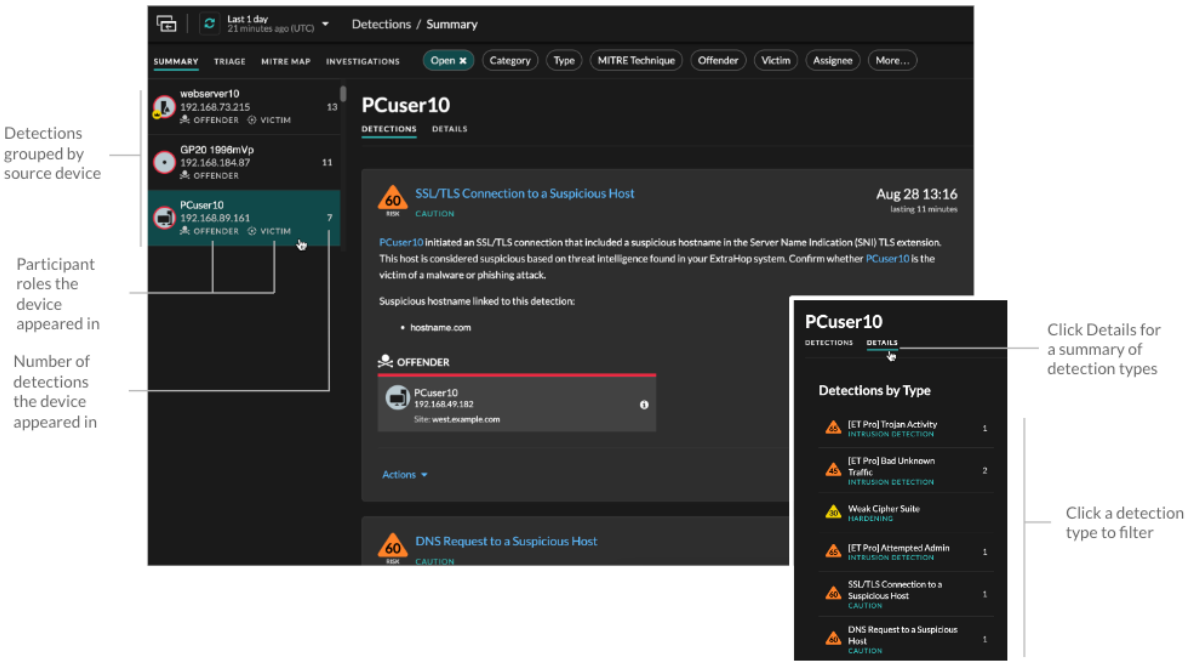
Listet die Benutzernamen der Teilnehmer auf, die dem Erkennungstyp zugeordnet sind. Benutzerinformationen sind nur in bestimmten Protokollen verfügbar und werden nicht bei allen Erkennungen angezeigt.

Du kannst alle Funde verfolgen im Übersichtsbereich, oder fügen Sie alle Funde zu einem Untersuchung aus dem **Massenaktionen** Drop-down-Menü am unteren Rand des Übersichtsfensters. Du kannst klicken eine Tuning-Regel erstellen um Erkennungen auf der Grundlage der im Übersichtsbereich enthaltenen Informationen auszublenden.

Sie können über den Übersichtsbereich hinaus scrollen, um einzelne Erkennungskarten anzuzeigen. Erkennungen, die für die Triage empfohlen erscheinen zuerst.

Nach Quelle gruppieren

Bei der Gruppierung der Zusammenfassungsansicht nach **Quelle**, Sie können die Teilnehmer anzeigen, die die Quelle einer Erkennung sind, wobei die Anzahl der Erkennungen neben dem Namen des Teilnehmers angezeigt wird. Klicken Sie auf eine Quelle, um die Erkennungen anzuzeigen, bei denen das Gerät entweder als Täter oder Opfer aufgetreten ist. klicken **Einzelheiten** unter dem Gerätenamen, um eine Liste der Erkennungstypen anzuzeigen, in denen das Gerät aufgetreten ist. Klicken Sie dann auf einen Erkennungstyp, um nach diesem Erkennungstyp zu filtern.



Gruppieren nach None

Bei der Gruppierung nach **Keine** Auf der Seite „Erkennungen“ können Sie ein Zeitdiagramm mit der Gesamtzahl der innerhalb des ausgewählten Zeitintervalls identifizierten Funde anzeigen. Jeder horizontale Balken im Diagramm steht für die Dauer einer einzelnen Erkennung, und der Balken ist entsprechend der Risikoscore farblich gekennzeichnet.

- Klicken und ziehen Sie, um einen Bereich im Diagramm hervorzuheben und einen bestimmten Zeitraum zu vergrößern. Erkennungen werden für das neue Zeitintervall aufgelistet.
- Zeigen Sie mit der Maus auf einen Balken, um den Erkennungsrisikowert anzuzeigen.
- Klicken Sie auf eine Leiste, um direkt zur Erkennungsdetailseite zu gelangen.

Unter der Zeitleiste wird in einem Flussdiagramm die Anzahl der Erkennungen angezeigt, die jeder Angriffskategorie zugeordnet sind. Kategorien werden zu einer Angriffskette zusammengefasst, die den Verlauf der Schritte beschreibt, die ein Angreifer unternimmt, um letztlich sein Ziel zu

erreichen, beispielsweise den Diebstahl sensibler Daten. Klicken Sie auf eine Angriffskategorie, um nur Erkennungen in dieser Kategorie anzuzeigen.

Triage

(nur NDR-Modul) In der Triage-Ansicht werden Erkennungen angezeigt, die ExtraHop für die Triage empfiehlt, basierend auf einer kontextuellen Analyse von Faktoren in Ihrer Umgebung, auch bekannt als Smart Triage.

Erkennungskarten, die für die Triage empfohlen werden, sind mit einem gelben Etikett gekennzeichnet und listen die Faktoren auf, die zu der Empfehlung geführt haben.

Beinhaltet einen hochwertigen Asset

Das Asset bietet Authentifizierung oder wichtige Dienste, oder ein Asset, das manuell als hoher Wert identifiziert.

Beinhaltet einen Top-Täter

Das Gerät oder die IP-Adresse hat an zahlreichen Erkennungen und einer Vielzahl von Erkennungstypen teilgenommen.

Beinhaltet einen seltenen Erkennungstyp

Der Erkennungstyp ist in letzter Zeit nicht in Ihrer Umgebung aufgetreten. Ungewöhnliche Erkennungstypen können auf einzigartiges, bösartiges Verhalten hinweisen.

Beinhaltet einen verdächtigen Hostnamen oder eine verdächtige IP-Adresse

Der Hostname oder die IP-Adresse lautet in einer Bedrohungssammlung referenziert das ist auf Ihrem System aktiviert.

Beinhaltet eine empfohlene Untersuchung

Die Erkennung ist Teil einer potenziellen Angriffskette in einem empfohlene Untersuchung.

Erkennungen, die für die Triage empfohlen werden, werden in der Zusammenfassungsansicht priorisiert und erscheinen unabhängig von der Sortierung ganz oben in Ihrer Erkennungsliste.

Du kannst Erkennungen filtern um nur Erkennungen anzuzeigen, die für die Triage empfohlen werden, und „Empfohlen für Triage“ als Kriterium für eine Benachrichtigungsregel.

Im Folgenden finden Sie einige Überlegungen zu Empfehlungen für die Triage:

- Empfehlungen, die auf hoher Wert Ressourcen basieren, sind auf maximal fünf Erkennungen desselben Erkennungstyps über einen Zeitraum von zwei Wochen begrenzt.
- Zwei Wochen an Sensordaten sind erforderlich, bevor Empfehlungen auf der Grundlage von Faktoren ausgesprochen werden, bei denen es sich um die häufigsten Straftäter oder um seltene Erkennungsfaktoren handelt.
- Empfehlungen auf der Grundlage von Bedrohungsinformationen sind auf zwei Erkennungen desselben Erkennungstyps für denselben Bedrohungsindikator über einen Zeitraum von dreißig Tagen beschränkt.

MITRE karte

Klicken Sie auf das **MITRE Karte** anzeigen, wenn Sie Ihre Erkennungen nach Angriffstechnik anzeigen möchten.

Jede Kachel in der Matrix steht für eine Angriffstechnik aus der MITRE ATT&CK® Matrix for Enterprise. Wenn eine Kachel hervorgehoben ist, erfolgte die mit dieser Technik verbundene Erkennung während des ausgewählten Zeitintervalls. Klicken Sie auf eine beliebige Kachel, um Erkennungen zu sehen, die dieser Technik entsprechen.

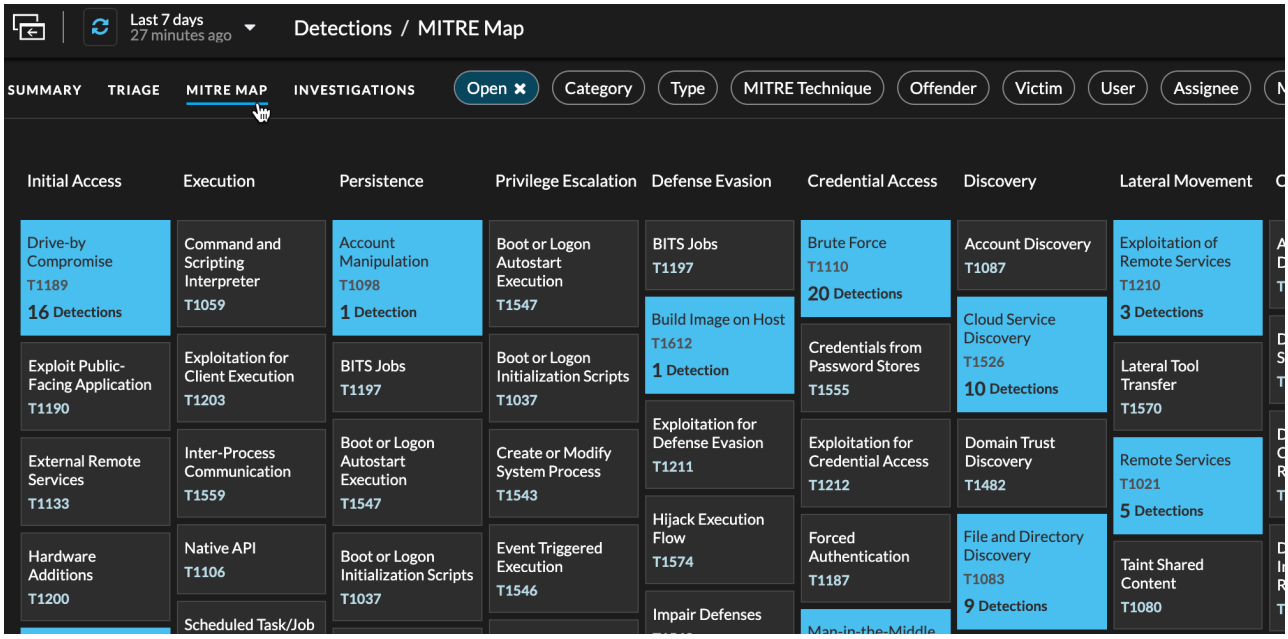


Tabelle „Untersuchungen“

In der Ansicht Untersuchungen werden alle vom Benutzer erstellten und empfohlenen Untersuchungen angezeigt, die während des ausgewählten Zeitintervalls erstellt wurden.

Klicken Sie auf einen Ermittlungsnamen, um die Untersuchung zu öffnen. Erfahre mehr über Ermittlungen.

Erkennungen filtern

Sie können die Seite „Entdeckungen“ filtern, um nur die Erkennungen anzuzeigen, die Ihren angegebenen Kriterien entsprechen. Beispielsweise könnten Sie nur an Exfiltrationserkennungen interessiert sein, die über HTTP erfolgen , oder an Erkennungen, die Teilnehmern zugeordnet sind, bei denen es sich um wichtige Server handelt.

Status

Sie können Erkennungen mit einem bestimmten Erkennungsstatus filtern, z. B. Bestätigt, In Bearbeitung oder Geschlossen. Standardmäßig ist der **Offen** Der Statusfilter wird angewendet auf Erkennungen Seite. Klicken Sie auf das **Offen** Filter, um auf andere Filteroptionen zuzugreifen.

Sie können das auswählen **Versteckt** Status, um nur Erkennungen anzuzeigen, die derzeit versteckt von Tuning-Regeln.

Kategorie

Sie können nach Angriffs- oder Leistungserkennungen filtern oder eine spezifischere Kategorie auswählen, um Ihre Ansicht der Seite „Entdeckungen“ weiter zu verfeinern. Wenn Sie auf den Kategoriefilter klicken, werden die meisten Kategorien unter dem **Alle Angriffskategorien** und **Alle Leistungskategorien** Die Optionen sind nach der Anzahl der Funde in der Kategorie sortiert. Härteerkennungen werden immer am Ende der Liste angezeigt.

Zu den Erkennungen von Angriffen gehören die folgenden Kategorien, die den Phasen der Angriffskette entsprechen.

Befehl und Steuerung

Ein externer Server, der eine Verbindung zu einem kompromittierten Gerät in Ihrem Netzwerk hergestellt und aufrechterhalten hat. C&C-Server können Malware, Befehle und Payloads senden,

um den Angriff zu unterstützen. Diese Erkennungen identifizieren, wenn ein internes Gerät mit einem Remotesystem kommuniziert, das anscheinend als C&C-Server fungiert.

Aufklärung

Ein Angreifer sucht nach hochwertigen Zielen und Schwächen, die er ausnutzen kann. Diese Erkennungen identifizieren Scans und Aufzählungstechniken.

Hinweis Bei Erkennungen kann ein bekannter Schwachstellenscanner wie Nessus und Qualys identifiziert werden. Klicken Sie auf den Gerätenamen, um zu bestätigen, ob dem Gerät bereits eine Vulnerability Scanner-Rolle im ExtraHop-System zugewiesen ist. Informationen zum Ausblenden von Erkennungen im Zusammenhang mit diesen Geräten finden Sie unter Erkennungen abstimmen.

Ausbeutung

Ein Angreifer nutzt eine bekannte Schwachstelle in Ihrem Netzwerk aus, um Ihre Ressourcen aktiv auszunutzen. Diese Erkennungen identifizieren ungewöhnliche und verdächtige Verhaltensweisen im Zusammenhang mit Ausnutzungstechniken.

Seitliche Bewegung

Ein Angreifer hat Ihr Netzwerk infiltriert und bewegt sich auf der Suche nach höherwertigen Zielen von Gerät zu Gerät. Diese Erkennungen identifizieren ungewöhnliches Geräteverhalten im Zusammenhang mit Datenübertragungen und Verbindungen im Ost-West-Korridor.

Zielgerichtete Maßnahmen

Der Angreifer ist kurz davor, sein Ziel zu erreichen, das vom Diebstahl sensibler Daten bis hin zur Verschlüsselung von Dateien bis hin zum Lösegeld reichen kann. Diese Erkennungen identifizieren, wenn ein Angreifer kurz davor ist, ein Kampagnenziel zu erreichen.

Vorsicht

Heben Sie Aktivitäten hervor, die keine unmittelbare Gefahr für den Betrieb darstellen, aber angegangen werden sollten, um eine gesunde Sicherheitslage aufrechtzuerhalten. Diese Erkennungen identifizieren auch Aktivitäten verdächtiger Teilnehmer, die mit Bedrohungsinformationen in Verbindung stehen.

Leistung Erkennungen umfassen die folgenden Kategorien.

Authentifizierung und Zugriffskontrolle

Markieren Sie erfolglose Versuche von Benutzern, Clients und Servern, sich anzumelden oder auf Ressourcen zuzugreifen. Diese Erkennungen identifizieren potenzielle WLAN-Probleme im Zusammenhang mit Authentifizierung-, Autorisierungs- und Auditprotokollen (AAA), übermäßige LDAP-Fehler oder decken Geräte mit eingeschränkten Ressourcen auf.

Datenbank

Heben Sie Zugriffsprobleme für Anwendungen oder Benutzer auf der Grundlage der Analyse von Datenbankprotokollen hervor. Diese Erkennungen identifizieren Datenbankprobleme, z. B. Datenbankserver, die eine übermäßige Anzahl von Antwortfehlern senden , die zu langsamen oder fehlgeschlagenen Transaktionen führen können.

Desktop- und Anwendungsvirtualisierung

Heben Sie lange Ladezeiten oder Sitzungen mit schlechter Qualität für Endbenutzer hervor. Diese Erkennungen identifizieren Anwendungsprobleme, z. B. eine übermäßige Anzahl von Zero Windows, was darauf hindeutet, dass ein Citrix-Server überlastet ist.

Netzwerk-Infrastruktur

Heben Sie ungewöhnliche Ereignisse über die TCP-, DNS- und DHCP-Protokolle hervor. Diese Erkennungen können auf DHCP-Probleme hinweisen, die verhindern, dass Clients eine IP-Adresse vom Server abrufen, oder zeigen, dass Dienste Hostnamen aufgrund übermäßiger DNS-Antwortfehler nicht auflösen konnten.

Verschlechterung des Dienstes

Heben Sie Serviceprobleme oder Leistungseinbußen im Zusammenhang mit Voice over IP (VoIP), Dateiübertragungs- und E-Mail-Kommunikationsprotokollen hervor. Diese Erkennungen zeigen

möglicherweise Dienstverschlechterungen an, bei denen VoIP-Anrufe fehlgeschlagen sind, und geben den entsprechenden SIP-Statuscode an, oder zeigen, dass nicht autorisierte Anrufer versucht haben, mehrere Anrufanfragen zu stellen.

Aufbewahrung

Heben Sie Probleme mit dem Benutzerzugriff auf bestimmte Dateien und Freigaben hervor, die bei der Auswertung des Netzwerkdateisystemverkehrs festgestellt wurden. Diese Erkennungen könnten darauf hinweisen, dass Benutzer aufgrund von SMB-Problemen am Zugriff auf Dateien auf Windows-Servern gehindert wurden oder dass NAS-Server (Netzwerk Attached Storage) aufgrund von NFS-Fehlern nicht erreicht werden konnten.

Web-Applikation

Heben Sie eine schlechte Webserverleistung oder Probleme hervor, die bei der Verkehrsanalyse über das HTTP-Protokoll beobachtet wurden. Diese Erkennungen zeigen möglicherweise, dass interne Serverprobleme zu einer übermäßigen Anzahl von Fehlern auf der Ebene 500 führen, sodass Benutzer nicht auf die Anwendungen und Dienste zugreifen können, die sie benötigen.

Aushärten Erkennungen identifizieren Sicherheitsrisiken und Möglichkeiten zur Verbesserung Ihrer Sicherheitslage.

Aushärten

Heben Sie bewährte Methoden zur Erhöhung der Sicherheit hervor, die durchgesetzt werden sollten, um das Risiko einer Ausnutzung zu minimieren. Diese Erkennungen identifizieren Möglichkeiten zur Verbesserung der Sicherheitslage Ihres Netzwerk, z. B. zur Verhinderung der Offenlegung von Anmeldeinformationen und zum Entfernen abgelaufener TLS-Zertifikate von Servern. Nachdem Sie auf eine Härteerkennung geklickt haben, können Sie zusätzliche Filter anwenden, um bestimmte Erkennungen innerhalb dieses Härteerkennungstyps anzuzeigen. Erfahre mehr über Filtern und Abstimmung von Härteerkennungen.

System zur Erkennung von Eindringlingen (Intrusion Detection System) Erkennungen identifizieren Sicherheitsrisiken und bösartiges Verhalten.

Erkennung von Eindringlingen

Heben Sie den Netzwerkverkehr hervor, der bekannten Signaturen unsicherer Praktiken, Exploit-Versuche und Indikatoren für Sicherheitslücken im Zusammenhang mit Malware und Command-and-Control-Aktivitäten entspricht.

Wichtig: Während IDS-Erkennungen Links zu Paketen für alle Protokolltypen beinhalten, sind Links zu Datensätzen nur für L7-Protokolle verfügbar.

Typ

Filtern Sie Ihre Erkennungsliste nach einem bestimmten Erkennungstyp, z. B. nach Datenexfiltration oder abgelaufenen SSL-Serverzertifikaten. Sie können auch eine CVE-Identifikationsnummer in diesen Filter eingeben, um nur Erkennungen für eine bestimmte öffentliche Sicherheitslücke anzuzeigen.

MITRE-Technik

Markieren Sie Erkennungen, die bestimmten MITRE-Technik-IDs entsprechen. Das MITRE-Framework ist eine weithin anerkannte Wissensdatenbank für Angriffe.

Täter und Opfer

Die mit einer Erkennung verbundenen Täter- und Opferendpunkte sind bekannt als Teilnehmer. Sie können Ihre Erkennungsliste so filtern, dass nur Erkennungen für einen bestimmten Teilnehmer angezeigt werden, z. B. für einen Täter, der eine unbekannte Remote-IP-Adresse hat, oder ein Opfer, das ein wichtiger Server ist. Gateway- oder Load Balancer-Geräte, die Externer Endpunkt Endpunktteilnehmern zugeordnet sind, können ebenfalls in diesen Filtern angegeben werden.

Nutzer

Filtern Sie Erkennungen nach Nutzername mit der Erkennung verbunden.

Abtretungsempfänger

Filtert Erkennungen nach dem Benutzer, der der Erkennung zugewiesen ist.

Mehr Filter

Sie können Ihre Erkennungen auch nach den folgenden Kriterien filtern:

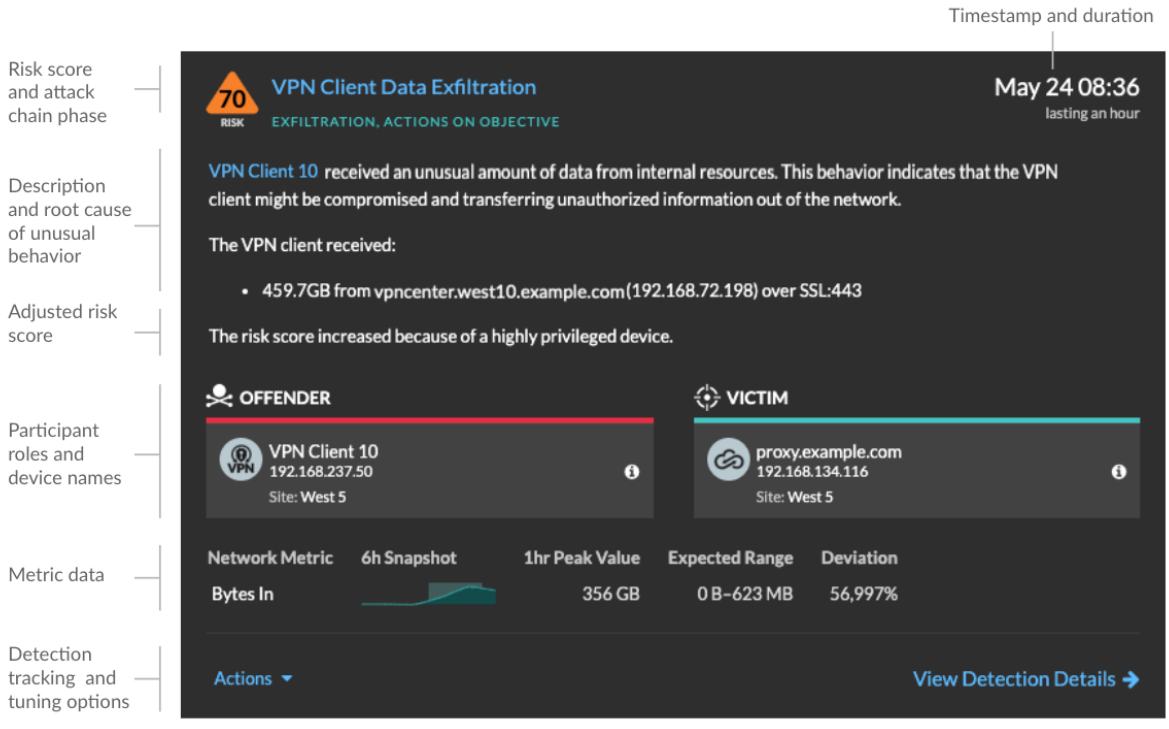
- Für Triage empfohlen
- Rolle des Geräts
- Teilnehmer
- Site (nur Konsole)
- Ticket-ID-Filter (Ticketverfolgung durch Dritte nur)
- Mindestrisikobewertung

Durch Erkennungen navigieren

Nachdem Sie ausgewählt haben, wie Ihre Erkennungsliste angezeigt, gruppiert und gefiltert werden soll, klicken Sie auf eine beliebige Erkennungskarte, um zur Erkennungsdetailseite zu gelangen.

Erkennungskarten

Jede Erkennungskarte identifiziert die Ursache der Entdeckung, die Erkennungskategorie, den Zeitpunkt der Erkennung sowie die Teilnehmer des Opfers und des Täters. Sicherheitserkennungen beinhalten eine Risikoscore.



Risiko-Score

Misst die Wahrscheinlichkeit, Komplexität und geschäftliche Auswirkungen einer Sicherheitserkennung. Diese Bewertung liefert eine Schätzung, die auf Faktoren wie Häufigkeit

und Verfügbarkeit bestimmter Angriffsvektoren im Vergleich zu den erforderlichen Fähigkeiten eines potenziellen Hackers und den Folgen eines erfolgreichen Angriffs basiert. Das Symbol ist nach Schweregrad als rot (80-99), orange (31-79) oder gelb (1-30) farblich gekennzeichnet.

Teilnehmer

Zeigt jedes an Teilnehmer an der Erkennung beteiligt.

Teilnehmerkarten zeigen Informationen an, die während der Erkennungsaktivität über den Teilnehmer gesammelt wurden, wie Hostname, IP-Adresse oder Benutzer. Die verfügbaren Informationen können sich je nach Entdeckungstyp und sonstigem Kontext ändern.

Klicken Sie auf einen Teilnehmer, um grundlegende Details anzuzeigen und auf Links zuzugreifen. Interne Endpunkte zeigen einen Link zur Seite Geräteübersicht an; externe Endpunkte zeigen die Geolokalisierung der IP-Adresse an. Endpunkt-Suchlinks wie ARIN Whois und ein Link zur IP-Adressdetailseite.

Hinweis: Eine TLS-Entschlüsselung ist erforderlich, um die Ausgangsendpunkte anzuzeigen, wenn HTTPS aktiviert ist. Erfahre mehr über TLS-Entschlüsselung.

Bei der Gruppierung nach **Typ**, wird unter dem Erkennungstyp ein Übersichtsfeld angezeigt, das die Erkennungen nach Tätern und Opfern aufschlüsselt und Ihnen ermöglicht, schnell Teilnehmerfilter anwenden.

Bei der Gruppierung nach **Quelle**, die internen Geräterollensymbole sind rot hervorgehoben, wenn das Gerät bei einer Erkennung ein Täter war, und blaugrün, wenn das Gerät ein Opfer war. Du kannst klicken **Einzelheiten** unter dem Quellennamen, um eine Zusammenfassung der Entdeckungen anzuzeigen, an denen diese Quelle Teilnehmer war. Diese Gerätedetails werden neben der Erkennungskarte auf Breitbildschirmen (1900 Pixel oder mehr) angezeigt.

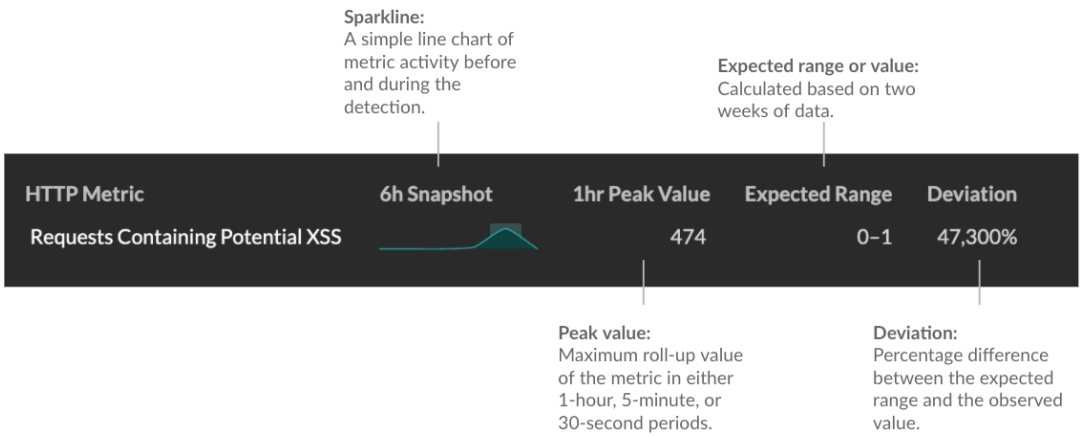
Dauer

Gibt an, wie lange das ungewöhnliche Verhalten erkannt wurde, oder zeigt FORTLAUFEND an, wenn das Verhalten gerade auftritt.

Bei Erkennungen, die auf bewährte Methoden zur Erhöhung der Sicherheit hinweisen, werden zwei Daten angezeigt: das erste und das Datum, an dem der Verstoß zuletzt identifiziert wurde.

Metrische Daten

Identifiziert zusätzliche Metrikdaten, wenn das ungewöhnliche Verhalten mit einer bestimmten Metrik oder einem bestimmten Schlüssel verknüpft ist. Wenn Metrikdaten für die Erkennung nicht verfügbar sind, wird die Art der anomalen Protokollaktivität angezeigt.



Erkennungsmanagement

Du kannst Spur oder stimmen die Erkennung aus dem **Aktionen** Drop-down-Menü oder fügen Sie die Erkennung zu einem Untersuchung. Klicken Sie **Erkennungsdetails anzeigen** um zur Seite mit den Erkennungsdetails zu navigieren.

Seite mit Erkennungsdetails

Die meisten Daten, die Sie benötigen, um eine Erkennung zu verstehen und zu validieren, werden auf der Erkennungsdetailseite angezeigt: Tabellen mit relevanten Metrikdaten, Aufzeichnungstransaktionen und Links zu Rohpaketen.

Auf die Informationen der Erkennungskarte folgen alle verfügbaren Abschnitte für die Erkennung. Diese Abschnitte variieren je nach Art der Erkennung.

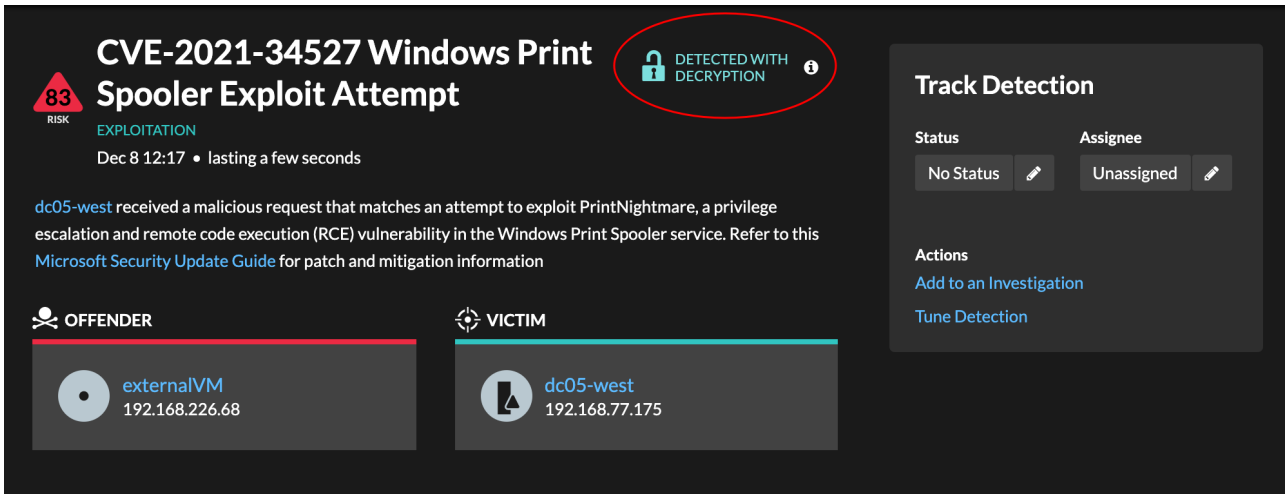
Spurerkennung

Du kannst Spur oder stimmen die Erkennung, oder klicken Sie **Zu einer Untersuchung hinzufügen** um die Erkennung in eine neue oder bestehende aufzunehmen Untersuchung.

Wenn Sie eine konfiguriert haben CrowdStrike-Integration auf Ihrem ExtraHop-System können Sie die Eindämmung von CrowdStrike-Geräten einleiten das sind Teilnehmer an der Erkennung. (Nur RevealX 360.)

Entschlüsselungsabzeichen

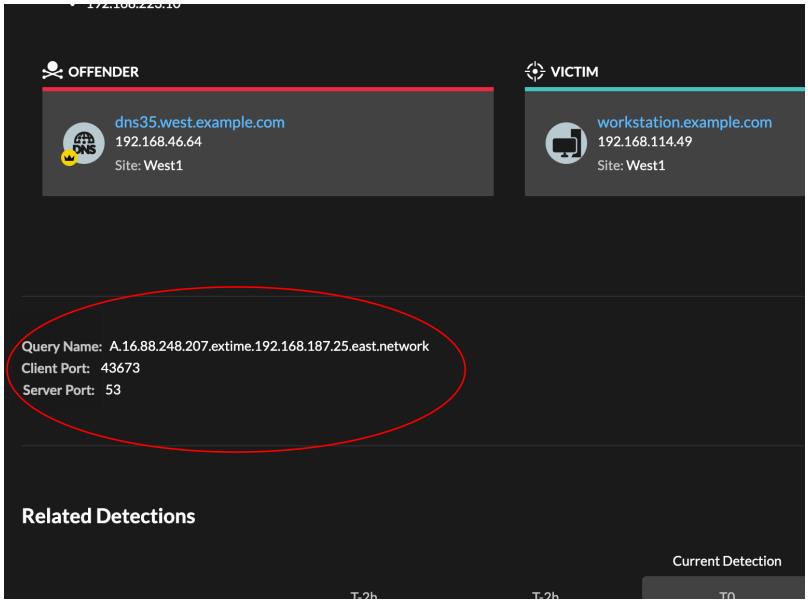
Wenn das ExtraHop-System verdächtiges Verhalten oder einen potenziellen Angriff in entschlüsselten Verkehrsaufzeichnungen feststellt, wird auf der Erkennungsdetailseite rechts neben dem Erkennungsnamen ein Entschlüsselungskennzeichen angezeigt.



Erfahre mehr über TLS-Entschlüsselung und Entschlüsseln des Datenverkehrs mit einem Windows-Domänencontroller.

Eigenschaften

Stellt eine Liste der Eigenschaften bereit, die für die Erkennung relevant sind. Zu den Erkennungseigenschaften können beispielsweise eine Abfrage, eine URI oder ein Hacking-Tool gehören, das für die Erkennung von zentraler Bedeutung ist.



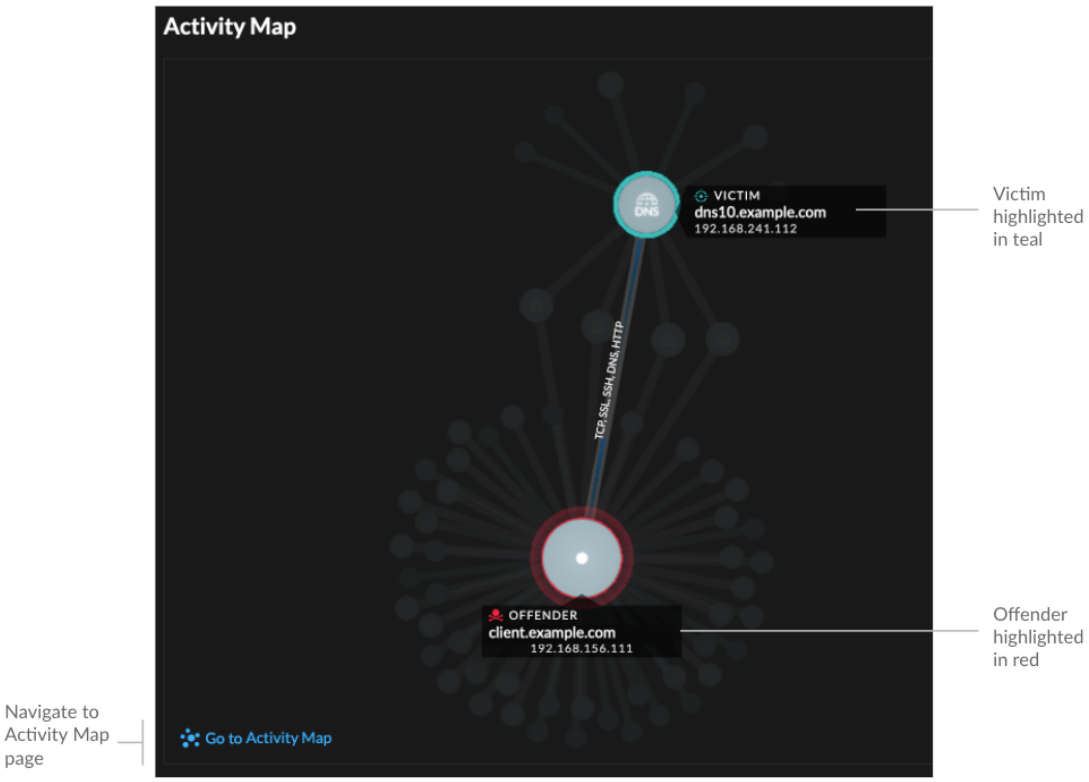
Loggen

Stellt ein mit Zeitstempel versehenes Protokoll der mit der Erkennung verbundenen Aktivitäten bereit.

Informationen über eine Erkennung werden selten aus einer einzelnen Anfrage oder Antwort gesammelt, sondern aus dem gesamten Verkehrsfluss zwischen Endpunkten. Das Erkennungsprotokoll listet jedes Update auf, das mit der Erkennung verknüpft ist. Jeder Eintrag im Protokoll stellt eine Aktualisierung des Verkehrsflusses dar, der zu der Erkennung geführt hat.

Karte der Aktivitäten

Bietet eine Aktivitätsdiagramm das hebt die Teilnehmer hervor, die an der Erkennung beteiligt waren. Auf der Aktivitätsdiagramm wird der Ost-West-Verkehr des mit der Erkennung verknüpften Protokoll angezeigt, sodass Sie den Umfang der bösartige Aktivität besser einschätzen können. Klicken Sie auf das Opfer oder den Täter, um ein Drop-down-Menü mit Links zur Geräteübersichtsseite und anderen Erkennungen aufzurufen, an denen das Gerät Teilnehmer ist.



Erkennungsdaten und Links

Stellt zusätzliche Daten im Zusammenhang mit der zu untersuchenden Entdeckung bereit. Die Datentypen können verwandte Metriken, Links zu enthalten Datensatz Transaktionsabfragen und ein Link zu einer allgemeinen Pakete abfrage. Die Verfügbarkeit von Metriken, Datensätzen und Paketen variiert je nach Erkennung. IDS-Erkennungen umfassen beispielsweise Links zu Paketen für alle Protokolltypen, aber Links zu Datensätzen sind nur für L7-Protokolle verfügbar.

Metrikdaten und Datensatztransaktionen werden in Tabellen angezeigt. Klicken Sie in einer Metriktabelle auf das Symbol um zugehörige Datensatztransaktionen anzuzeigen. Klicken Sie in einer Datensatztabelle auf das Symbol um die zugehörige Paketabfrage für eine Transaktion anzuzeigen.

Hinweis: EIN Recordstore muss für die Anzeige von Transaktionen und fortlaufenden Transaktionen konfiguriert sein PCAP muss für das Herunterladen von Paketen konfiguriert sein.

Verhalten vergleichen

Stellt ein Diagramm bereit, in dem die Aktivität des Täters neben den Aktivitäten ähnlicher Geräte im Zeitraum angezeigt wird, in dem die Erkennung stattgefunden hat. Das Diagramm wird für Erkennungen im Zusammenhang mit unkonventionellen Aktivitäten eines Gerät angezeigt. Unerwartetes Verhalten wird hervorgehoben, indem es neben dem Verhalten von Geräten im Netzwerk mit ähnlichen Eigenschaften angezeigt wird.

Verwandte Erkennungen

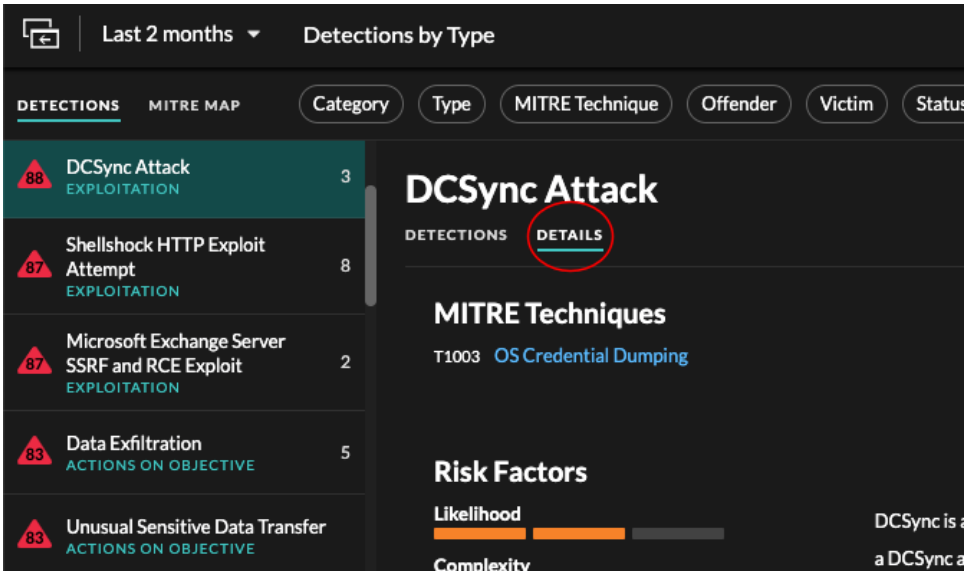
Bietet eine Zeitleiste der Erkennungen im Zusammenhang mit der aktuellen Erkennung, anhand derer Sie eine größere Angriffskampagne identifizieren können. Zu den zugehörigen Erkennungen gehören die Rolle des Teilnehmer, die Dauer, der Zeitstempel und alle Rollenänderungen, wenn der Täter bei einer Erkennung zum Opfer einer anderen Erkennung wird. Klicken Sie in der Zeitleiste auf eine zugehörige Erkennung, um die Detailseite für diese Erkennung anzuzeigen.

Verwandte Erkennungen, die in einem enthalten sind empfohlene Untersuchung sind mit goldenen Links gekennzeichnet und können angeklickt werden, um zur Ermittlungsseite zu gelangen.

Einzelheiten zur Erkennung

Enthält eine ausführliche Beschreibung der Erkennung, z. B. zugehörige MITRE-Techniken, Risikofaktoren, Angriffshintergründe und -diagramme, Abhilfemaßnahmen und Referenzlinks zu Sicherheitsorganisationen wie MITRE.

Diese Details werden neben der Erkennungskarte auf Breitbildschirmen angezeigt, oder Sie können auf sie zugreifen, indem Sie auf **Einzelheiten** unter dem Erkennungstitel, wenn die Erkennungsseite nach gruppiert wird **Typen**.



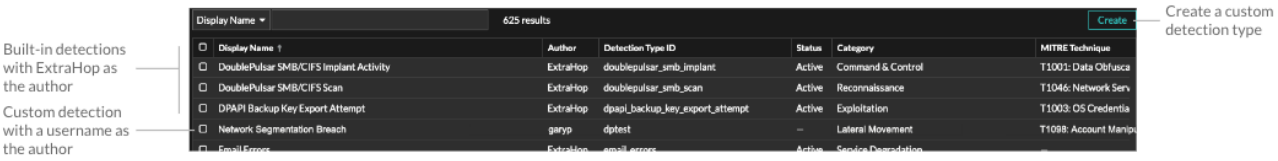
Für einige Erkennungstypen ist ein So funktioniert dieser Detektor Dieser Abschnitt enthält Antworten auf häufig gestellte Fragen dazu, warum eine Erkennung in Ihrem ExtraHop-System erscheint.

Hinweis: Du kannst Erkennung von Aktien Detailseiten mit anderen ExtraHop-Benutzern.

Erkennungskatalog

Der Erkennungskatalog enthält eine vollständige Liste aller Erkennungstypen im ExtraHop-System, einschließlich Erkennungstypen, die derzeit inaktiv sind oder überprüft werden. Sie können benutzerdefinierte Erkennungstypen auch auf der Seite Erkennungskatalog verwalten.

Sie können auf die Seite Erkennungskatalog zugreifen, indem Sie auf das Symbol Systemeinstellungen klicken. .



Zusätzlich zum Anzeigenamen und Autor können Sie die Liste der Erkennungstypen nach ID, Status, Kategorie, MITRE-Techniken, die dem Erkennungstyp zugeordnet sind, und Erkennungstypen filtern, die Daten aus dem Fluss unterstützen Sensoren.

Klicken Sie auf eine von ExtraHop verfasste Erkennung, um die Einstellungen für den Erkennungstyp Bereich, in dem der Name des Erkennungstyps, die ID, der Autor, der aktuelle Status des Erkennungstyps, das Datum, an dem der Erkennungstyp erstmals für die Produktion freigegeben wurde (sofern verfügbar), und die zugehörigen Kategorien angezeigt werden. Um mehr über die Erkennung zu erfahren, klicken Sie auf **Details zum Entdeckungstyp**.

Status des Entdeckungstyps

Dieser Status gibt an, ob eine Erkennung in Ihrer Umgebung verfügbar ist.

Aktiv

Aktive Erkennungstypen sind für alle Sensoren verfügbar und können in Ihrer Umgebung zu Erkennungen führen.

Inaktiv

Inaktive Erkennungstypen wurden von allen Sensoren entfernt und erzeugen keine Erkennungen mehr. Wenn ein Erkennungstyp inaktiv wird, werden bestehende Erkennungen dieses Typs weiter anzeigen.

Im Rückblick

In Review werden die Erkennungstypen auf einer begrenzten Anzahl von ExtraHop-Systemen evaluiert, bevor sie für alle Sensoren verfügbar sind. Diese Erkennungstypen werden einer gründlichen Prüfung auf Effizienz und Genauigkeit unterzogen, bevor sie einer zunehmenden Anzahl von Sensoren zur Verfügung gestellt werden. Der Überprüfungszeitraum kann bis zu mehreren Wochen dauern. Nach Abschluss der Überprüfung wird der Status des Entdeckungstyps auf Aktiv aktualisiert.

Im Folgenden finden Sie einige wichtige Überlegungen dazu, ob Erkennungen eines bestimmten Typs in Ihrer Umgebung sichtbar sind:

- Wenn aktive Erkennungen nicht wie erwartet angezeigt werden, erfordert der Erkennungstyp möglicherweise Entschlüsselung oder unterstützt möglicherweise keine Durchflusssensoren (nur RevealX 360).
- RevealX Enterprise-Systeme müssen verbunden sein mit Cloud-Dienste um regelmäßige Updates für den Erkennungskatalog zu erhalten. Ohne eine Verbindung zu Cloud Services Updates sind verzögert bis die Firmware aktualisiert ist.

Benutzerdefinierte Erkennungen

Sie können benutzerdefinierte Erkennungen auf der Seite Erkennungskatalog anzeigen und verwalten.

- Um einen benutzerdefinierten Erkennungstyp zu erstellen, klicken Sie auf **Erstellen** in der oberen rechten Ecke der Seite. Die Erkennungstyp-ID für den neuen Erkennungstyp muss mit der ID übereinstimmen, die im benutzerdefinierten Erkennungsauslöser enthalten ist. Erfahre mehr über Erstellen einer benutzerdefinierten Erkennung.
- Um eine benutzerdefinierte Erkennung zu bearbeiten, klicken Sie auf die Erkennung und bearbeiten Sie den Anzeigenamen, den Autor, die Erkennungskategorien und die zugehörigen MITRE-Techniken in der Erkennungstyp bearbeiten Panel. Sie können keine Erkennungen bearbeiten, bei denen ExtraHop als Autor aufgeführt ist.
- Um eine benutzerdefinierte Erkennung zu löschen, klicken Sie auf die Erkennung und dann auf **Löschen** aus dem Einstellungen für den Erkennungstyp Panel.
- Bei benutzerdefinierten Erkennungen wird unter Status immer ein Bindestrich (-) angezeigt.

Ermittlungen

(nur NDR-Modul) Mithilfe von Untersuchungen können Sie mehrere Funde in einer einzigen Zeitleiste und Karte hinzufügen und anzeigen. Anhand einer Zusammenfassung verbundener Erkennungen können Sie feststellen, ob verdächtiges Verhalten eine gültige Bedrohung darstellt und ob die Bedrohung von einem einzelnen Angriff oder Teil einer größeren Angriffskampagne stammt.

Sie können Untersuchungen von einer Entdeckungsdetailseite aus erstellen und zu ihnen hinzufügen, **Aktionen** Menü auf einem individuelle Erkennungskarte, oder die **Massenaktionen** Menü auf einem Zusammenfassung der Erkennung. Ihr ExtraHop-System erstellt außerdem empfohlene Untersuchungen durch Smart Investigations, bei denen es sich um Untersuchungen handelt, die automatisch als Reaktion auf potenziell bösartige Aktivität erstellt werden.

Jede Ermittlungsseite enthält die folgenden Tools:

Zeitplan der Untersuchung

Die Untersuchungszeitleiste wird auf der linken Seite der Seite angezeigt und listet die hinzugefügten Funde auf, beginnend mit der neuesten Erkennung. Neue Funde, die der Untersuchung hinzugefügt werden, werden in der Zeitleiste entsprechend der Uhrzeit und dem Datum der Erkennung angezeigt. Erkennungsteilnehmer werden unter dem Erkennungstitel angezeigt, und Informationen zur Erkennungsverfolgung, wie Beauftragter und Status, werden neben den Teilnehmern angezeigt.

Angriffskategorien

Die Kategorien der hinzugefügten Funde werden oben auf der Ermittlungsseite angezeigt.

Die Kette der Angriffskategorien zeigt die Anzahl der Funde in jeder Kategorie an, nicht die Reihenfolge, in der die Erkennungen aufgetreten sind. Einen genauen Überblick darüber, wie die Erkennungen im Laufe der Zeit aufgetreten sind, finden Sie im Zeitplan der Untersuchung.

Untersuchungen anzeigen

Oben auf der Ermittlungsseite gibt es zwei Optionen, um die Untersuchung anzuzeigen: Zusammenfassung und Angriffskarte. Beide Optionen bieten einen einzigartigen Überblick über Ihre Untersuchung.

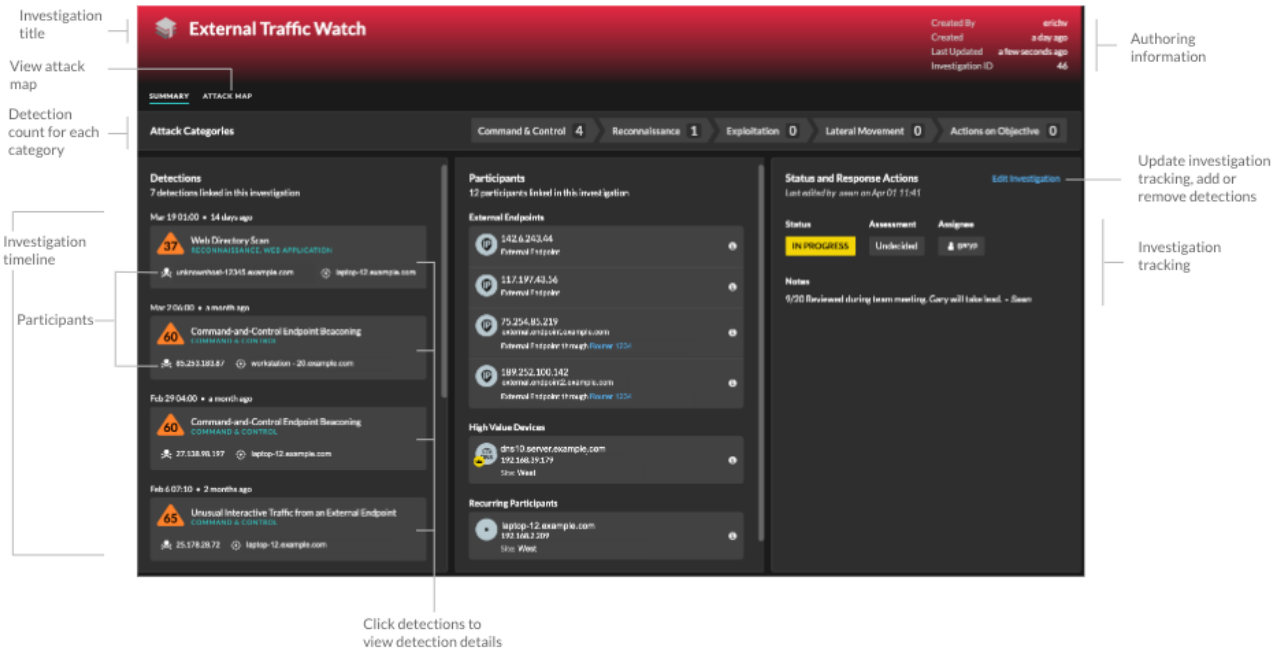
Zusammenfassung

Standardmäßig beginnen Ermittlungen in **Zusammenfassung** Ansicht, die den Zeitplan für die Erkennung, eine aggregierte Teilnehmerliste und ein Panel zur Verfolgung des Status und der Reaktionsmaßnahmen für die Untersuchung enthält.

Sie können in der Untersuchungszeitleiste auf eine Erkennung klicken, um sie anzuzeigen Erkennungsdetails, klicken Sie dann auf das X-Symbol, um die Erkennungsdetails zu schließen und zur Zusammenfassung der Untersuchung zurückzukehren. Sie können auch auf Gehe zu klicken

Symbol in der oberen rechten Ecke, um die Seite mit den Erkennungsdetails in einem neuen Tab anzuzeigen.

Im Panel „ Teilnehmer“ werden die Teilnehmer an der Untersuchung nach externen Endpunkten, hoher Wert Geräten und wiederkehrenden Teilnehmern gruppiert. Dabei handelt es sich um Teilnehmer, die bei mehreren Funden in der Untersuchung vorkommen. Klicken Sie auf einen Teilnehmer, um Details anzuzeigen und auf Links zuzugreifen.

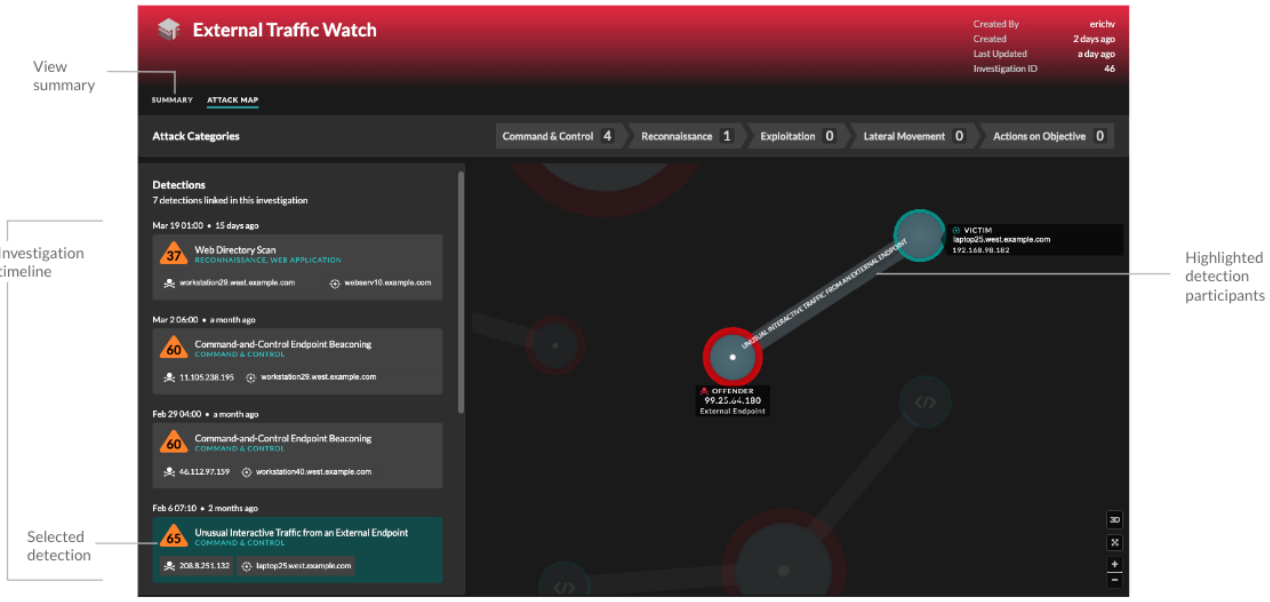


In der Status - und Reaktionsmaßnahmen Panel, klicken **Untersuchung bearbeiten** um den Namen der Untersuchung zu ändern, den Status oder die endgültige Bewertung der Untersuchung festzulegen, einen Beauftragten anzugeben oder Anmerkungen hinzuzufügen .

Sie können fortfahren Verfolgen Sie einzelne Erkennungen nachdem Sie sie zu einer Untersuchung hinzugefügt haben.

Angriffskarte

In **Angriffskarte** Ansicht, der Täter und das Opfer von jeder Erkennung in der Untersuchung werden auf einer interaktiven Karte neben dem Zeitplan der Untersuchung angezeigt.



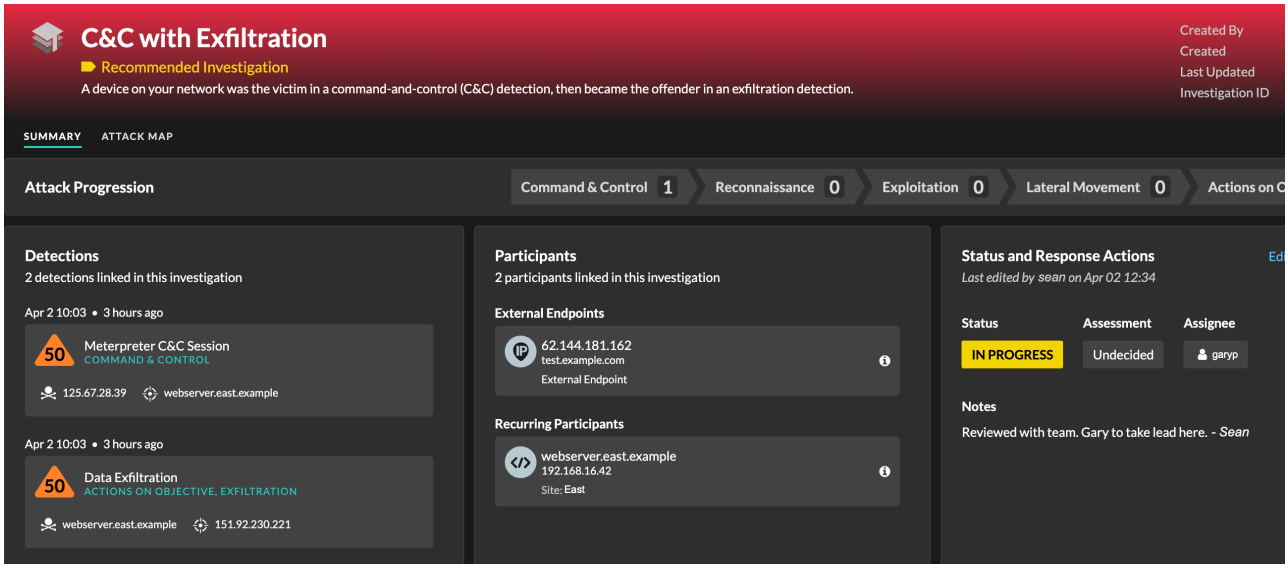
Die Teilnehmer sind durch Linien verbunden, die mit dem Erkennungstyp beschriftet sind, und die Geräterollen werden durch ein Symbol dargestellt.

- Klicken Sie in der Zeitleiste der Untersuchung auf eine Erkennung, um die Teilnehmer hervorzuheben. Kreise werden rot hervorgehoben, wenn das Gerät bei mindestens einer Erkennung im Rahmen der Untersuchung als Täter aufgetreten ist, und blaugrün hervorgehoben, wenn es sich bei dem Gerät um ein Opfer handelt. Die Markierungen werden aktualisiert , wenn Sie auf eine andere Erkennung klicken, damit Sie leichter erkennen können, wann ein Teilnehmer vom Opfer zum Täter wird.
- Klicken Sie auf einen Kreis, um Details wie den Hostnamen, die IP-Adresse oder die MAC-Adresse des Gerät anzuzeigen oder um zu den zugehörigen Erkennungen oder dem Seite „Geräteübersicht“.
- Zeigen Sie mit der Maus auf einen Kreis oder eine Linie, um das Etikett anzuzeigen.

Empfohlene Untersuchungen

Der ExtraHop Machine Learning Service überwacht die Netzwerkaktivität auf Kombinationen von Angriffstechniken, die auf bösartiges Verhalten hinweisen könnten. Wenn eine Kombination identifiziert wird, erstellt das ExtraHop-System eine empfohlene Untersuchung, sodass Ihre Sicherheitsteams die Situation beurteilen und schnell reagieren können, wenn bösartiges Verhalten bestätigt wird.

Wenn beispielsweise ein Gerät Opfer einer Erkennung in der Kategorie Command-and-Control wird, bei einer Exfiltrationserkennung aber zum Täter wird, empfiehlt das ExtraHop-System eine C&C mit Exfiltrationsuntersuchung.



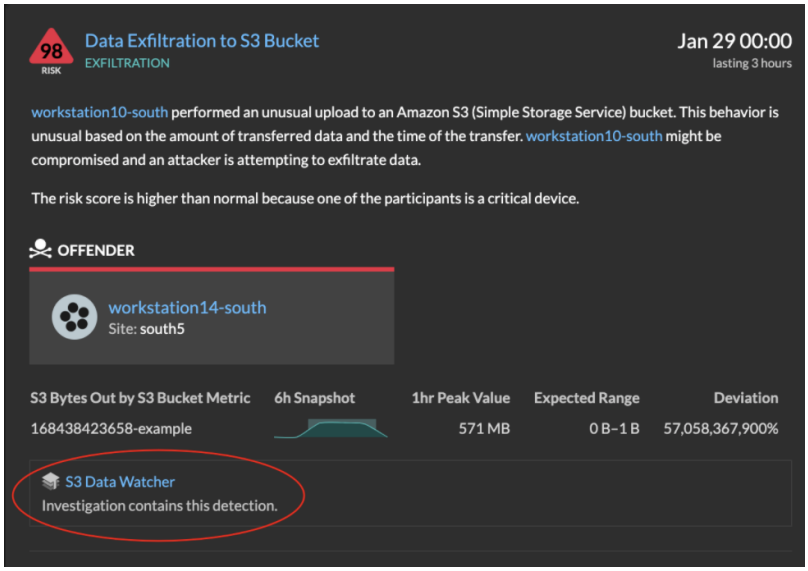
Sie können mit empfohlenen Untersuchungen auf die gleiche Weise interagieren wie von Benutzern erstellte Untersuchungen, z. B. indem Sie Erkennungen hinzufügen oder entfernen, einen Beauftragten angeben und einen Status und eine Bewertung festlegen.

Empfohlene Untersuchungen finden Sie in der Tabelle der Untersuchungen. Sie können die sortieren Erstellt von Spalte, um Untersuchungen zu finden, die von ExtraHop erstellt wurden.

Durch Ermittlungen navigieren

Nachdem eine Erkennung zu einer Untersuchung hinzugefügt wurde, wird unten auf der Erkennungskarte und auf der Seite mit den Erkennungsdetails ein Link zu der Untersuchung angezeigt.

Klicken Sie auf den Namen, um die Untersuchung zu öffnen, und klicken Sie dann auf der Ermittlungsseite auf den Namen der Entdeckung, um zur Erkennungsdetailseite zurückzukehren.



Erfahren Sie, wie eine Untersuchung erstellen.

Auffinden von Funden im ExtraHop-System

Die Seite „Erkennungen“ bietet zwar schnellen Zugriff auf alle Funde, aber im gesamten ExtraHop-System gibt es Indikatoren und Links zu Erkennungen.

Hinweis: Erkennungen bleiben im System entsprechend Ihrer System-Lookback-Kapazität für 1-Stunden-Metriken mit einer Mindestspeicherzeit von fünf Wochen. Erkennungen verbleiben im System ohne unterstützende Metriken, wenn Ihre System-Lookback-Kapazität weniger als fünf Wochen beträgt.

- Klicken Sie auf einer Seite mit der Geräteübersicht auf Erkennungen, um eine Liste der zugehörigen Erkennungen anzuzeigen. Klicken Sie auf den Link für eine einzelne Erkennung, um die Seite mit den Erkennungsdetails anzuzeigen.
- Klicken Sie auf einer Seite mit der Gerätegruppen-Übersicht auf den Link Erkennungen, um zur Seite „ Erkennungen“ zu gelangen. Die Erkennungsliste wird nach Teilnehmern gefiltert, die Mitglieder der Gerätegruppe sind.
- Klicken Sie auf einer Aktivitätsdiagramm auf ein Gerät, das animierte Impulse rund um die Kreisbeschriftung anzeigt, um eine Liste der zugehörigen Funde anzeigen. Klicken Sie auf den Link für eine einzelne Erkennung, um die Erkennungsdetails anzuzeigen.
- Bewegen Sie den Mauszeiger in einem Diagramm auf einem Dashboard oder einer Protokollseite über Erkennungsmarker um den Titel der zugehörigen Erkennung anzuzeigen, oder klicken Sie auf die Markierung, um die Erkennungsdetails anzuzeigen.