

# Erkennungen

Veröffentlicht: 2024-02-12

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

## Bevor Sie beginnen

Benutzern muss eine Genehmigung erteilt werden [Privilegien](#) um Erkennungen einzusehen.

Wenn ein ungewöhnliches Verhalten festgestellt wird, generiert das ExtraHop-System eine Erkennung und zeigt die verfügbaren Daten und Optionen an. Steuerelemente auf der Seite „Erkennungen“: Oberflächendetektionen, die [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.

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

- Sammeln Sie hochwertige, verwertbare Daten, um die Hauptursachen für Netzwerkprobleme zu ermitteln.
- Finden Sie unbekannte Probleme mit der 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.
- Kennzeichnet verdächtige IP-Adressen, Hostnamen und URIs, die durch Threat Intelligence identifiziert wurden.
- Heben Sie bewährte Methoden zur Stärkung der Sicherheit hervor.

Erfahre mehr über [Optimierung von Erkennungen](#).



**Wichtig:** Erkennungen können Sie zwar über Sicherheitsrisiken und Leistungsprobleme informieren, ersetzen jedoch 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.

## Erkennungen anzeigen

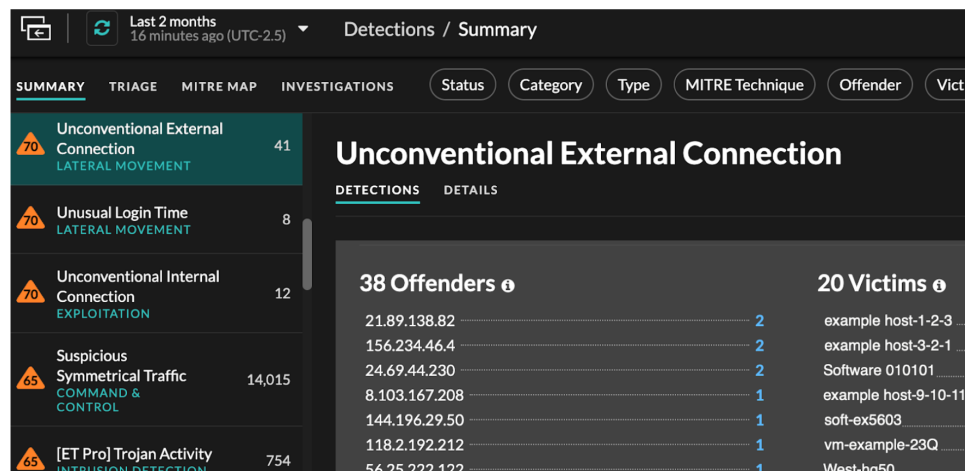
In der oberen linken Ecke der Erkennungsseite gibt es vier Optionen zum Anzeigen von Erkennungen: Zusammenfassung, Triage, MITRE Map und Untersuchungen. Diese Optionen bieten jeweils eine einzigartige Ansicht Ihrer Erkennungsliste.

## Zusammenfassung

Standardmäßig werden Erkennungen auf der Seite Erkennungen in der Übersichtsansicht angezeigt, in der Informationen zu Erkennungen zusammengefasst werden, um Aktivitätsmuster in Ihrer Umgebung hervorzuheben. Sie können Ihre Erkennungsliste in der Übersichtsansicht 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 den Erkennungen Seite. Klicken Sie auf **Offen** filtern, um auf andere zuzugreifen [Optionen filtern](#).



### Sortierung von Erkennungen in der Übersichtsansicht

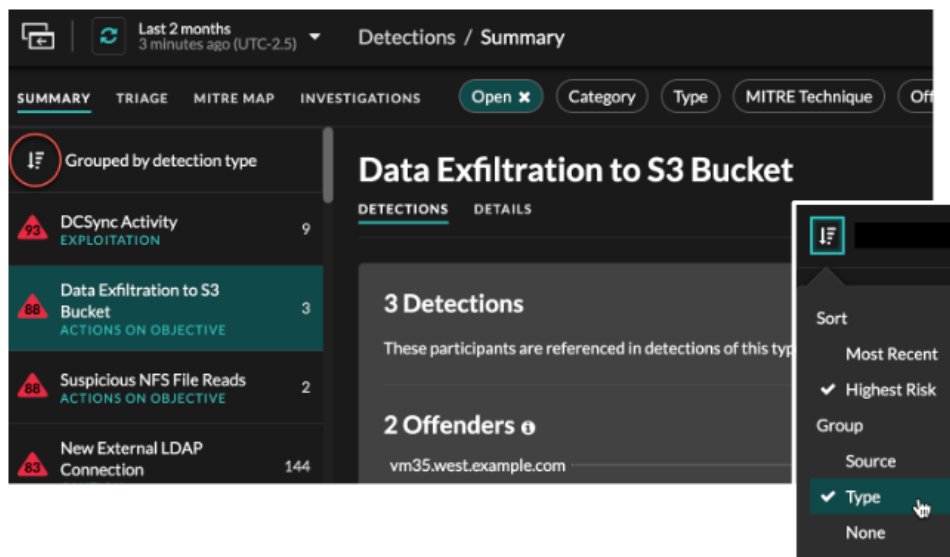
Sie können Erkennungen entweder nach der höchsten Risikoscore oder nach dem jüngsten Ereignis sortieren.

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.

### Gruppierung von Erkennungen in der Übersichtsansicht

Sie können Erkennungen nach Erkennungstyp (z. B. Spike in SSH-Sitzungen) oder nach Erkennungsquelle (z. B. IP-Adresse des Täters) gruppieren, oder Sie können festlegen, dass Ihre Erkennungsliste überhaupt nicht gruppiert wird.



### Nach Typ gruppieren

Beim Gruppieren der Zusammenfassungsansicht nach **Typ**, können Sie Wertelisten anzeigen, die mit Erkennungen verknüpft sind, die während des ausgewählten Zeitintervalls aufgetreten sind, z. B. Teilnehmer, Erkennungseigenschaften oder Netzwerklokalitäten.

Sie können auf Teilnehmerwerte klicken, um mehr über dieses Gerät oder diese IP-Adresse zu erfahren. Klicken Sie auf einen beliebigen Wert, um nur Erkennungen anzuzeigen, die mit diesem Wert verknüpft sind, oder [alle zugehörigen Erkennungen verfolgen](#).

### Teilnehmer

Führt alle Täter und Opfer der ausgewählten Erkennungsart auf. Die Täter- und Opferlisten sind nach der Anzahl der Erkennungen geordnet, bei denen der Teilnehmer auftaucht.

### Immobilienwerte

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

### Lokalitäten im Netzwerk

Führt die Netzwerklokalitäten auf, die Erkennungen des ausgewählten Typs enthalten. Die Liste der Netzwerkortschaften ist nach der Anzahl der Entdeckungen in der Netzwerklokalität sortiert.

Am unteren Rand des Übersichtsfensters befinden sich Links, mit denen Sie [alle Erkennungen verfolgen](#) in der Zusammenfassung enthalten. Du kannst [eine Optimierungsregel erstellen](#) um alle in der Zusammenfassung enthaltenen Erkennungen auszublenden oder versteckte Entdeckungen dieses Erkennungstyps anzuzeigen.

Sie können über den ÜbersichtsBereich hinaus scrollen, um einzelne Erkennungskarten anzuzeigen. Erkennungen, die [für die Triage empfohlen](#) erscheinen zuerst.

### Nach Quelle gruppieren

Wenn Sie die Übersichtsansicht nach Quelle gruppieren, können Sie 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 als Opfer aufgetreten ist. Klicken **Einzelheiten** unter dem Gerätenamen, um eine Liste der Erkennungstypen anzuzeigen, in denen das Gerät aufgetreten ist, und klicken Sie dann auf einen Erkennungstyp, um nach diesem Erkennungstyp zu filtern.

The screenshot displays the 'Detections / Summary' page in the ExtraHop console. On the left, a list of participants is shown, grouped by source device. The 'PCUser10' entry is highlighted, showing 7 detections. Annotations on the left side of the image point to the participant name, the number of detections, and the role (Offender/Victim). The main area shows a detailed view for 'PCUser10' with a 'DETECTIONS' tab selected. A specific detection is highlighted: 'SSL/TLS Connection to a Suspicious Host' with a risk level of 60 (CAUTION) and a timestamp of 'Aug 28 13:16'. Below this, a list of 'Suspicious hostname linked to this detection:' is shown, including 'hostname.com'. The 'OFFENDER' section lists 'PCUser10' with IP '192.168.49.182' and site 'west.example.com'. On the right, a 'DETECTIONS BY TYPE' panel is shown, listing various detection types such as '[ET Pro] Trojan Activity', '[ET Pro] Bad Unknown Traffic', 'Weak Cipher Suite', '[ET Pro] Attempted Admin', 'SSL/TLS Connection to a Suspicious Host', and 'DNS Request to a Suspicious Host'. Annotations on the right side of the image point to the 'DETAILS' link, the detection type list, and a specific detection type.

## Nach Keiner gruppieren

Bei der Gruppierung nach **Keine** Auf der Seite Erkennungen können Sie ein Zeitdiagramm mit der Gesamtzahl der Entdeckungen anzeigen, die innerhalb des ausgewählten Zeitintervalls identifiziert wurden. Jeder horizontale Balken im Diagramm stellt die Dauer einer einzelnen Erkennung dar und ist entsprechend der Risikoscore farblich gekennzeichnet.

- Klicken und ziehen Sie, um einen Bereich im Diagramm hervorzuheben, um einen bestimmten Zeitraum zu vergrößern. Erkennungen werden für das neue Zeitintervall aufgelistet.
- Bewegen Sie den Mauszeiger über einen Balken, um die Bewertung des Erkennungsrisikos anzuzeigen.
- Klicken Sie auf eine Leiste, um direkt zur Seite mit den Erkennungsdetails 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 letztendlich sein Ziel zu erreichen, z. B. sensible Daten zu stehlen. Klicken Sie auf eine Angriffskategorie, um nur Erkennungen in dieser Kategorie anzuzeigen.

## Triage

(nur NDR-Modul) Die Triage-Ansicht zeigt Erkennungen, die ExtraHop auf der Grundlage einer kontextuellen Analyse von Faktoren in Ihrer Umgebung für die Triage empfiehlt.

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 stellt Authentifizierungs- oder grundlegende Dienste bereit, oder ein Asset, das [manuell als hoher Wert identifiziert](#).

### Es handelt sich um einen Haupttäter

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

### Beinhaltet einen seltenen Erkennungstyp

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

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

Du kannst [Erkennungen filtern](#) um nur Erkennungen anzuzeigen, die für die Triage empfohlen werden, und für die Triage empfohlen als Kriterien für eine [Benachrichtigungsregel](#).

Hier sind einige Überlegungen zu den Empfehlungen für die Triage:

- Empfehlungen, die auf hochwertigen Vermögenswerten basieren, sind auf maximal fünf Erkennungen desselben Entdeckungstyps über einen Zeitraum von zwei Wochen beschränkt.
- Zwei Wochen an Sensordaten sind erforderlich, bevor Empfehlungen auf der Grundlage von Faktoren vom Typ „Haupttäter“ oder „Seltenheit“ ausgesprochen werden.

## 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.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
Drive-by Compromise T1189 215 Detections	Command and Scripting Interpreter T1059 1 Detection	Account Manipulation T1098	Boot or Logon Autostart Execution T1547	BITS Jobs T1197	Brute Force T1110 4 Detections	Account Discovery T1087 7 Detections	Exploitation of Remote Services T1210 3 Detections
Exploit Public-Facing Application T1190	Exploitation for Client Execution T1203	BITS Jobs T1197	Boot or Logon Initialization Scripts T1037	Build Image on Host T1612 7 Detections	Credentials from Password Stores T1555	Cloud Service Discovery T1526 11 Detections	Lateral Tool Transfer T1570
External Remote Services T1133	Inter-Process Communication T1559	Boot or Logon Autostart Execution T1547	Create or Modify System Process T1543	Exploitation for Defense Evasion T1211	Exploitation for Credential Access T1212	Domain Trust Discovery T1482	Remote Services T1021 5 Detections
Hardware Additions T1200	Native API T1106	Boot or Logon Initialization Scripts T1037	Event Triggered Execution T1546	Hijack Execution Flow T1574	Forced Authentication T1187	File and Directory Discovery T1083 3 Detections	Taint Shared Content T1080
Phishing T1566 2234 Detections	Scheduled Task/Job T1053 1847 Detections	Browser Extensions T1176 1 Detection	Exploitation for Privilege Escalation T1068	Impair Defenses T1562	Man-in-the-Middle T1557 3 Detections	Group Policy Discovery T1615	Use Alternate Authentication Material T1550
Supply Chain Compromise		Create Account	Hijack Execution Flow	Indicator Removal on Host T1070			

## Tabelle „Untersuchungen“

In der Ansicht Untersuchungen werden alle erstellten Untersuchungen angezeigt.

Klicken Sie auf einen Namen für die Untersuchung, um die Untersuchung zu öffnen. Erfahre mehr über [Ermittlungen](#).

## Erkennungen filtern

Sie können die Seite Erkennungen filtern, sodass nur die Erkennungen angezeigt werden, die Ihren angegebenen Kriterien entsprechen. Beispielsweise interessieren Sie sich möglicherweise nur für Exfiltrationserkennungen, die über HTTP erfolgen, oder für Erkennungen, die mit Teilnehmern verknüpft 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 **Öffnen** Der Statusfilter wird angewendet auf Erkennungen Seite. Klicken Sie auf **Öffnen** filtern, 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 Operationserkennungen filtern oder eine spezifischere Kategorie auswählen, um Ihre Ansicht der Erkennungsseite weiter zu verfeinern. Wenn Sie auf den Kategoriefilter klicken, werden die meisten Kategorien unter dem **Alle Angriffskategorien** und **Alle Betriebskategorien** Die Optionen sind nach der Anzahl der Entdeckungen in der Kategorie sortiert. Härtungserkennungen werden immer am Ende der Liste angezeigt.

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

### Steuerung 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 wertvollen Zielen und Schwächen, die er ausnutzen kann. Diese Erkennungen identifizieren Scans und Aufzählungstechniken.



Bei Erkennungen könnte 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 wurde. Informationen zum Ausblenden von Erkennungen im Zusammenhang mit diesen Geräten finden Sie unter [Erkennungen optimieren](#).

### 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 Ausbeutungstechniken.

### Seitliche Bewegung

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

### Maßnahmen im Hinblick auf Zielsetzung

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

### Vorsicht

Heben Sie Aktivitäten hervor, die keine unmittelbare Bedrohung für den Betrieb darstellen, die aber angegangen werden sollten, um ein gesundes Sicherheitsniveau aufrechtzuerhalten. Diese Erkennungen identifizieren auch Aktivitäten verdächtiger Teilnehmer, die mit Bedrohungsinformationen in Verbindung stehen.

**Betrieb** Erkennungen umfassen die folgenden Kategorien.

### Authentifizierung und Zugriffskontrolle

Heben Sie erfolglose Versuche von Benutzern, Clients und Servern hervor, sich anzumelden oder auf Ressourcen zuzugreifen. Diese Erkennungen identifizieren potenzielle WLAN-Probleme im Zusammenhang mit Authentifizierungs-, 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 von schlechter Qualität für Endbenutzer hervor. Diese Erkennungen identifizieren Anwendungsprobleme, z. B. eine zu hohe 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 Clients daran hindern, eine IP-Adresse vom Server zu erhalten, oder sie 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), Dateiübertragung und E-Mail-Kommunikationsprotokollen hervor. Diese Erkennungen können

auf Dienstverschlechterungen hinweisen, bei denen VoIP-Anrufe fehlgeschlagen sind, und den entsprechenden SIP-Statuscode anzeigen oder darauf hinweisen, dass nicht autorisierte Anrufer versucht haben, mehrere Anrufanfragen zu stellen.

### Aufbewahrung

Heben Sie Probleme beim 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/CIFS-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 schlechte Webserverleistung oder Probleme hervor, die bei der Analyse des Datenverkehrs über das HTTP-Protokoll beobachtet wurden. Diese Erkennungen könnten darauf hindeuten, dass interne Serverprobleme zu einer übermäßigen Anzahl von Fehlern der Stufe 500 führen, sodass Benutzer nicht auf die Anwendungen und Dienste zugreifen können, die sie benötigen.

**Härten** Erkennungen identifizieren Sicherheitsrisiken und Möglichkeiten zur Verbesserung Ihrer Sicherheitslage.

### Härten

Heben Sie bewährte Methoden zur Stärkung der Sicherheit hervor, die durchgesetzt werden sollten, um das Risiko einer Ausnutzung zu verringern. Diese Erkennungen identifizieren Möglichkeiten, die Sicherheitslage Ihres Netzwerk zu verbessern, z. B. die Offenlegung von Anmeldeinformationen zu verhindern und abgelaufene SSL/TLS-Zertifikate von Servern zu entfernen. Nachdem Sie auf eine Härtungserkennung geklickt haben, können Sie zusätzliche Filter anwenden, um bestimmte Erkennungen innerhalb dieses Härtungserkennungstyps anzuzeigen. Erfahre mehr über [Filterung und Abstimmung von Härtungserkennungen](#).

**Einbruchmeldesystem (Intrusion Detection System)** Erkennungen identifizieren Sicherheitsrisiken und böses Verhalten.

### Erkennung von Eindringlingen

Heben Sie Netzwerkverkehr hervor, der mit bekannten Signaturen unsicherer Praktiken, Exploit-Versuchen und Indikatoren für Sicherheitsbedrohungen im Zusammenhang mit Malware und Command-and-Control-Aktivitäten übereinstimmt.

 **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. Datenexfiltration oder abgelaufenen SSL-Serverzertifikaten. Sie können auch eine CVE-Identifikationsnummer in diesen Filter eingeben, um nur Erkennungen für eine bestimmte Sicherheitslücke im Bereich der öffentlichen Sicherheit anzuzeigen.

### MITRE-Technik

Heben Sie Erkennungen hervor, die mit bestimmten MITRE-Technik-IDs übereinstimmen. Das MITRE-Framework ist eine weithin anerkannte Wissensdatenbank für Angriffe.

### Täter und Opfer

Die mit einer Erkennung verbundenen Täter- und Opferendpunkte werden als Teilnehmer bezeichnet. Sie können Ihre Erkennungsliste so filtern, dass nur Erkennungen für einen bestimmten Teilnehmer angezeigt werden, z. B. für einen Täter mit einer unbekannt Remote-IP-Adresse oder für ein Opfer, bei dem es

sich um einen wichtigen Server handelt. Gateway- oder Load Balancer-Geräte, die Externer Endpunkt Endpunktteilnehmern zugeordnet sind, können in diesen Filtern ebenfalls angegeben werden.

### Bevollmächtigter

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](#)
- [Geräterollen](#)
- Quelle
- Site (nur Konsole)
- Ticket-ID-Filter ([Ticketsysteme von Drittanbietern](#) nur)
- Mindestrisikobewertung

## Durch Erkennungen navigieren

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

### Erkennungskarten

Jede Erkennungskarte identifiziert die Ursache der Erkennung, die Erkennungskategorie, den Zeitpunkt der Erkennung sowie die Opfer- und Täterbeteiligten. Sicherheitserkennungen beinhalten eine Risikoscore.

The screenshot shows a detection card with the following components:

- Risk score and attack chain phase:** A risk score of 70 (orange triangle) for 'VPN Client Data Exfiltration'.
- Description and root cause of unusual behavior:** 'VPN Client 10 received an unusual amount of data from internal resources. This behavior indicates that the VPN client might be compromised and transferring unauthorized information out of the network. The VPN client received: 459.7GB from vpncenter.west10.example.com(192.168.72.198) over SSL:443. The risk score increased because of a highly privileged device.'
- Participant roles and device names:** 'OFFENDER' (VPN Client 10, 192.168.237.50) and 'VICTIM' (proxy.example.com, 192.168.134.116).
- Metric data:** A table showing 'Bytes In' with a 6h snapshot graph, 1hr Peak Value of 356 GB, Expected Range of 0 B-623 MB, and Deviation of 56,997%.
- Detection tracking and tuning options:** 'Actions' dropdown and 'View Detection Details' link.
- Timestamp and duration:** 'May 24 08:36 lasting an hour'.


### Risikobewertung

Misst die [Wahrscheinlichkeit, Komplexität und Auswirkungen auf das Geschäft](#) einer Sicherheitserkennung. Dieser Wert bietet eine Schätzung auf der Grundlage von Faktoren zur Häufigkeit und Verfügbarkeit bestimmter Angriffsvektoren im Vergleich zu den erforderlichen Fähigkeiten eines potenziellen Hackers und zu den Folgen eines erfolgreichen Angriffs. Das Symbol ist nach Schweregrad farblich gekennzeichnet: Rot (80-99), Orange (31-79) oder Gelb (1-30).



## Teilnehmer

Identifiziert jeden Teilnehmer (Täter und Opfer), der an der Erkennung beteiligt war, anhand des Hostnamens oder der IP-Adresse. Klicken Sie auf einen Teilnehmer, um grundlegende Informationen und Zugangslinks anzuzeigen. Interne Endpunkte zeigen einen Link zur Seite „Geräteübersicht“ an; externe Endpunkte zeigen die Geolokalisierung der IP-Adresse an. [Links zur Endpunktsuche](#) wie ARIN Whois und ein Link zur IP-Adressdetailseite. 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 ursprüngliche Endpunkt wird als Teilnehmer betrachtet.

 **Hinweis** Wenn HTTPS aktiviert ist, ist eine SSL/TLS-Entschlüsselung erforderlich, um Ursprungsendpunkte anzuzeigen. Erfahre mehr über [SSL/TLS-Entschlüsselung](#).

Bei der Gruppierung nach **Typ**, wird unter dem Erkennungstyp ein Übersichtsfenster angezeigt, das die Erkennungen nach Täter und Opfer aufschlüsselt und es Ihnen ermöglicht, schnell [Teilnehmerfilter anwenden](#).

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

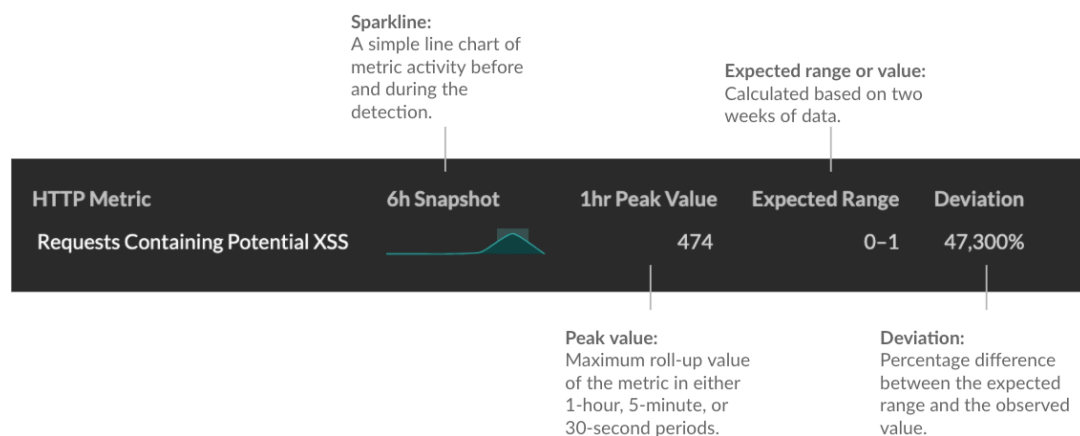
## Dauer

Identifiziert, wie lange das ungewöhnliche Verhalten erkannt wurde, oder zeigt FORTLAUFEND an, wenn das Verhalten derzeit auftritt.

Bei Erkennungen, bei denen bewährte Methoden zur Erhöhung der Sicherheit hervorgehoben werden, werden zwei Daten angezeigt: das erste Mal und das Datum, an dem der Verstoß zuletzt festgestellt 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 der Typ der anomalen Protokollaktivität angezeigt.



## Erkennungsmanagement

Du kannst [Spur](#) oder [stimmen](#) die Erkennung aus der Dropdownliste Aktionen, oder klicken Sie auf **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, Datensatztransaktionen und Links zu Rohpaketen.

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

## Erkennung von Spuren

Du kannst [Spur](#) oder [stimmen](#) die Erkennung, oder klicken **Zu einer Untersuchung hinzufügen** um die Erkennung in ein neues oder vorhandenes einzubeziehen [Untersuchung](#).

Wenn Sie eine konfiguriert haben [CrowdStrike-Integration](#) auf Ihrem ExtraHop-System können Sie [die Eindämmung von CrowdStrike-Geräten einleiten](#) die an der Erkennung beteiligt sind. ( Nur Reveal (x) 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 Entschlüsselungs-Badge angezeigt.

Erfahre mehr über [SSL/TLS-Entschlüsselung](#) und [Entschlüsseln des Datenverkehrs mit einem Windows-Domänencontroller](#).

## Erkennungseigenschaften

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

172.168.225.10

**OFFENDER**  
 dns35.west.example.com  
 192.168.46.64  
 Site: West1

**VICTIM**  
 workstation.example.com  
 192.168.114.49  
 Site: West1

Query Name: A.16.88.248.207.extime.192.168.187.25.east.network  
 Client Port: 43673  
 Server Port: 53

**Related Detections**

Current Detection

### Karte der Aktivitäten

Bietet eine [Aktivitätsdiagramm](#) das hebt die an der Erkennung beteiligten Teilnehmer hervor. Auf der Aktivitätsdiagramm wird der Ost-West-Verkehr des Protokoll angezeigt, das mit der Erkennung verknüpft ist, sodass Sie den Umfang der böartige Aktivität besser einschätzen können. Klicken Sie auf das Opfer oder den Täter, um ein Dropdownmenü mit Links zur Seite „Geräteübersicht“ und anderen Erkennungen aufzurufen, an denen das Gerät Teilnehmer ist.

**Activity Map**

VICTIM  
 dns10.example.com  
 192.168.241.112

Victim highlighted in teal

TCP, SSH, DNS, HTTP

OFFENDER  
 client.example.com  
 192.168.156.111

Offender highlighted in red

Navigate to Activity Map page

Go to Activity Map

## Erkennungsdaten und Links

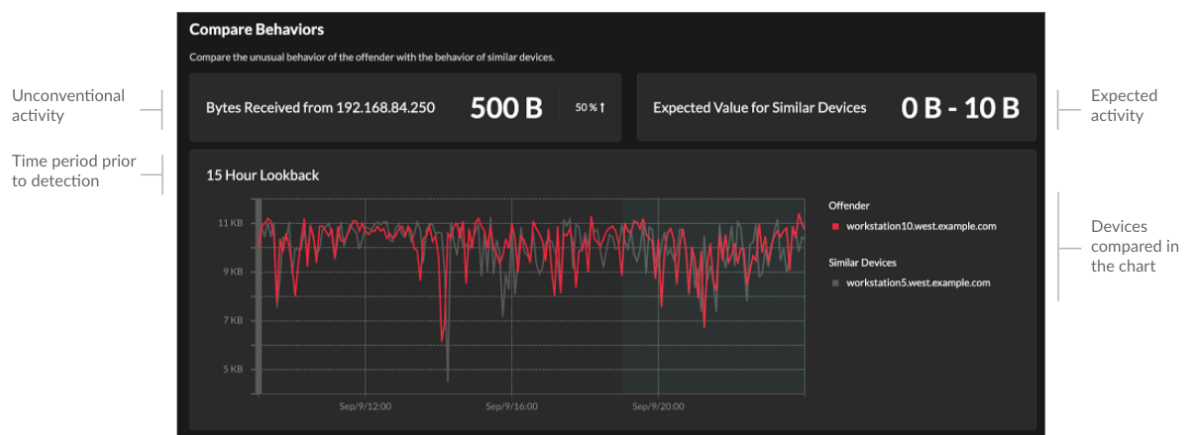
Stellt zusätzliche Daten im Zusammenhang mit der Erkennung bereit, die untersucht werden sollen. Die Datentypen können verwandte Metriken enthalten, Links zu [Datensatz](#) Transaktionsanfragen und ein Link zu einem allgemeinen [Pakete](#) abfragen. Die Verfügbarkeit von Metriken, Datensätzen und Paketen variiert je nach Erkennung. IDS-Erkennungen umfassen beispielsweise Links zu Paketen für alle Protokolltypen, aber Links zu Datensätzen sind nur für L7-Protokolle verfügbar.

Metrische Daten 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.

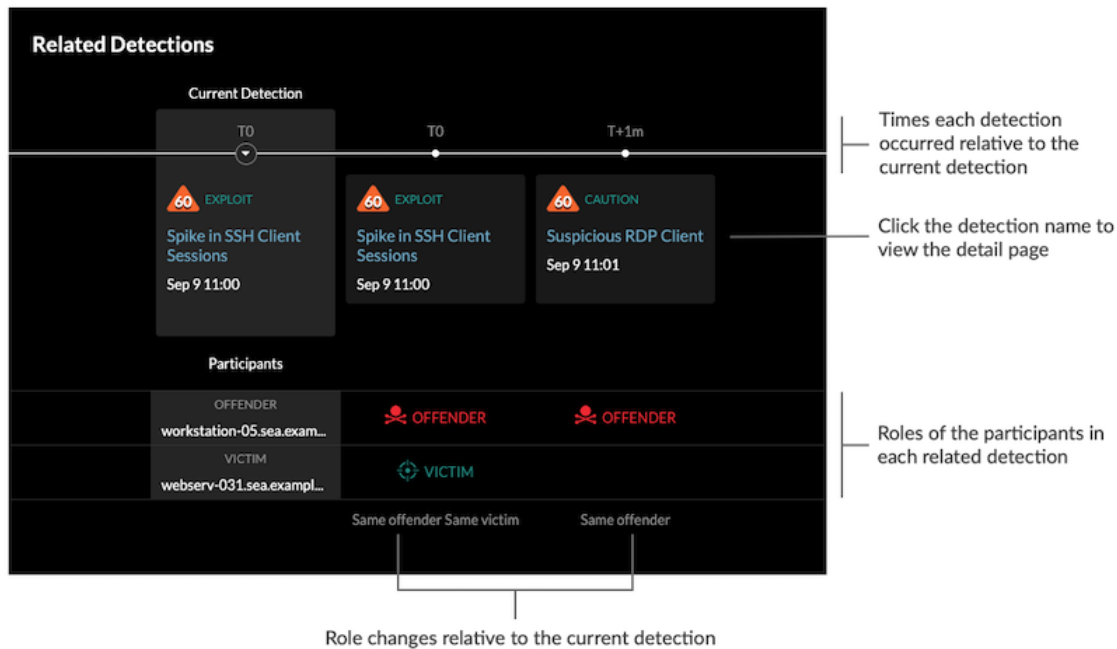
## Verhalten vergleichen

Stellt ein Diagramm bereit, das die Aktivität des Täters neben der Aktivität ähnlicher Geräte in dem Zeitraum anzeigt, in dem die Erkennung erfolgte. Das Diagramm wird für Erkennungen angezeigt, die auf unkonventionelle Aktivitäten eines Gerät sind, und hebt unerwartetes Verhalten hervor, indem es neben dem Verhalten von Geräten im Netzwerk mit ähnlichen Eigenschaften angezeigt wird.



## Verwandte Erkennungen

Bietet eine Zeitleiste mit Erkennungen im Zusammenhang mit der aktuellen Erkennung, anhand derer Sie eine größere Angriffskampagne identifizieren können. Zu den entsprechenden 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 Timeline auf eine zugehörige Erkennung, um die Detailseite für diese Erkennung aufzurufen.



### 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 (1900 Pixel oder mehr) angezeigt, oder Sie können darauf zugreifen, indem Sie darauf klicken **Einzelheiten** unter dem Erkennungstitel, wenn die Erkennungsseite gruppiert wird nach **Typen**.

DETECTIONS

Count	Category	Type
3	DCSync Attack	EXPLOITATION
8	Shellshock HTTP Exploit Attempt	EXPLOITATION
2	Microsoft Exchange Server SSRF and RCE Exploit	EXPLOITATION
5	Data Exfiltration	ACTIONS ON OBJECTIVE
5	Unusual Sensitive Data Transfer	ACTIONS ON OBJECTIVE

**DCSync Attack**

DETECTIONS | **DETAILS**

**MITRE Techniques**

T1003 OS Credential Dumping

**Risk Factors**

Likelihood: [Progress bar]

Complexity: [Progress bar]

**Hinweis:** Du kannst [Erkennung teilen](#) Detailsseiten mit anderen ExtraHop-Benutzern.

## Erkennungskatalog

Der Erkennungskatalog enthält eine vollständige Liste aller im ExtraHop-System verfügbaren Erkennungstypen. Sie können benutzerdefinierte Erkennungstypen auch auf der Seite Erkennungskatalog verwalten.

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

550 results

Display Name	Author	Detection Type ID	Category	MITRE Technique
Multiple SMB/CIFS Errors	ExtraHop	multiple_smb_cifs_errors	Storage	-
NBT-NS Poisoning	ExtraHop	nbt_ns_poisoning	Exploitation	T1557: Man-in-the-Middle
Network Privilege Escalation	ExtraHop	network_privilege_escalation	Lateral Movement	T1021: Remote Services
Network Share Enumeration	ExtraHop	msrpc_network_share_enum	Reconnaissance	T1135: Network Share Discovery
Network Segmentation Breach	garp	network_segmentation_breach	Lateral Movement	T1098: Account Manipulation

Built-in detections with ExtraHop as the author  
 Custom detection with a username as the author

Create a custom detection type

Zusätzlich zum Anzeigenamen und Autor können Sie die Liste der Erkennungstypen nach Erkennungstyp-ID, Erkennungskategorie, mit dem Erkennungstyp verknüpften MITRE-Techniken und Erkennungstypen, die Daten aus dem Fluss unterstützen, filtern Sensoren.

Klicken Sie auf eine integrierte Erkennung, um die Einstellungen für den Erkennungstyp Bereich, in dem der Name, der Typ und die zugehörigen Kategorien der Erkennung angezeigt werden. Um mehr über die Erkennung zu erfahren, klicken Sie auf **Details zum Erkennungstyp**.

### 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 [eine benutzerdefinierte Erkennung erstellen](#).
- 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 tafel. Integrierte Erkennungen, bei denen ExtraHop als Autor aufgeführt ist, können nicht bearbeitet werden.
- Um eine benutzerdefinierte Erkennung zu löschen, klicken Sie auf die Erkennung und dann auf **Löschen** von der Einstellungen für den Erkennungstyp Panel.

## Ermittlungen

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

The screenshot displays the 'External Traffic Watch' interface. On the left, a vertical sidebar contains sections for 'Investigation title', 'Authoring information', 'Updateable notes', 'Investigation timeline', 'Participants', and 'Relative timestamps'. The main area is divided into two panels: a timeline on the left and an investigation map on the right. The timeline lists several detections with their severity scores (e.g., 65, 45, 65, 65) and categories like 'Symmetrical Traffic: Possible Beacons Detected', 'Expired SSL/TLS Server Certificate', and 'Unusual Interactive Traffic from an External Endpoint'. The investigation map shows a network diagram with nodes representing devices and connections between them, with labels like 'SYMMETRICAL TRAFFIC', 'VICTIM Laptop5-Sea', and 'UNUSUAL INTERACTIVE TRAFFIC FROM AN EXTERNAL ENDPOINT'. A caption below the screenshot reads 'Click detections to view detection cards'.

Sie können Untersuchungen auf einer Entdeckungsdetailseite oder über das Menü Aktionen auf jeder Entdeckungskarte erstellen und zu ihnen hinzufügen.

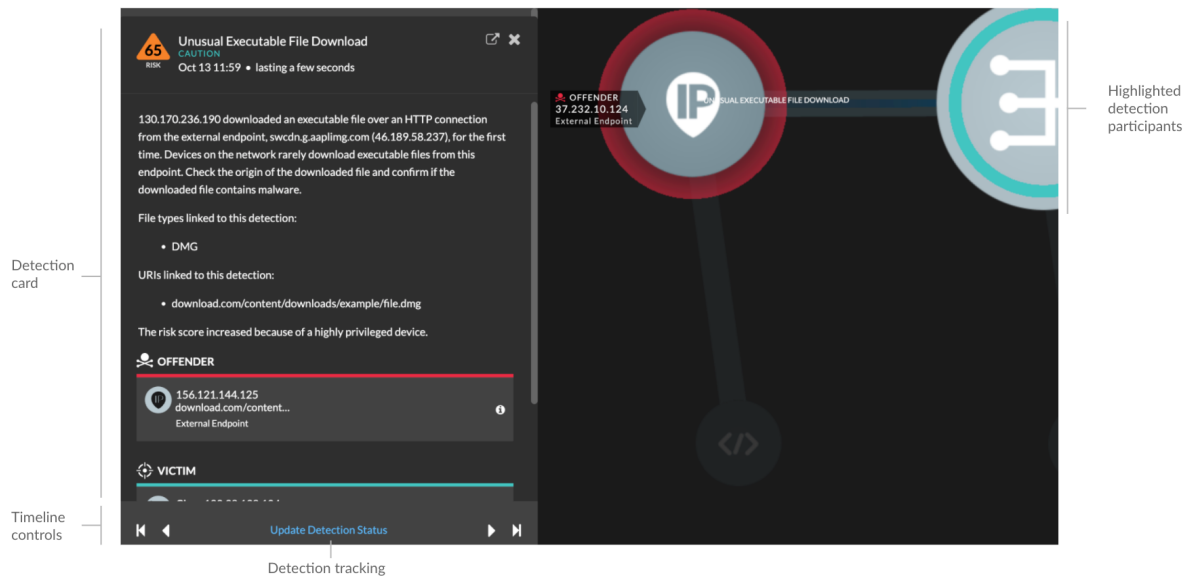
Jede Ermittlungsseite enthält die folgenden Tools:

### Zeitplan für die Untersuchung

Die Zeitleiste wird links auf der Seite angezeigt und listet die hinzugefügten Erkennungen in chronologischer Reihenfolge auf. Neue Entdeckungen, die hinzugefügt werden, werden in der Zeitleiste entsprechend der Uhrzeit und dem Datum der Erkennung sowie relativ zur frühesten Erkennung, die mit T0 gekennzeichnet ist, angezeigt. Erkennungsteilnehmer werden unter dem Erkennungstitel angezeigt, und Informationen zur Erkennungsverfolgung, wie Beauftragter und Status, werden neben den Teilnehmern angezeigt.

Klicken Sie auf eine Erkennung in der Timeline, um die [Erkennungskarte](#) und markieren Sie die Erkennungsteilnehmer auf der Untersuchungskarte. Klicken Sie auf der Karte oder in der Ermittlungskarte auf einen Teilnehmer, um grundlegende Details und Links zur Seite mit der Geräteübersicht sowie zu anderen Erkennungen anzuzeigen, bei denen das Gerät ein Teilnehmer ist.

Klicken Sie in der oberen rechten Ecke der Erkennungskarte auf Gehe zu Symbol, um das zu sehen [Seite mit Erkennungsdetails](#), oder die Symbol, um die Erkennung zu schließen und zur Ermittlungszeitleiste zurückzukehren.



Klicken Sie unter der Erkennungskarte auf **Spurerkennung** zu bearbeiten [Erkennungsverfolgung](#) Informationen. Sie können auf die Timeline-Steuererelemente klicken, um andere Erkennungen in der Untersuchung anzuzeigen.

### Ermittlungskarte

Die Ermittlungskarte zeigt den Täter und das Opfer jeder Erkennung im Rahmen der Untersuchung. Die Teilnehmer sind durch Linien verbunden, die mit dem Erkennungstyp gekennzeichnet sind, und Geräterollen werden durch ein Symbol dargestellt.

- Klicken Sie in der Untersuchungszeitleiste auf eine Erkennung, um die Teilnehmer hervorzuheben. Kreise sind rot hervorgehoben, wenn das Gerät der Täter ist, und blaugrün, wenn das Gerät das Opfer ist. Die Markierungen werden aktualisiert, wenn Sie auf eine andere Erkennung klicken, sodass Sie leichter erkennen können, wann ein Teilnehmer vom Opfer zum Täter wechselt.
- 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 zu navigieren oder [Seite „Geräteübersicht“](#).
- Zeigen Sie mit der Maus auf einen Kreis oder eine Linie, um die Bezeichnung anzuzeigen.

### Hinweise

Klicken **Untersuchung bearbeiten** um Notizen hinzuzufügen oder den Namen der Untersuchung zu ändern. Du kannst weitermachen [einzelne Erkennungen verfolgen](#) nachdem Sie sie zu einer Untersuchung hinzugefügt haben.

### 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.



**98 RISK** Data Exfiltration to S3 Bucket EXFILTRATION Jan 29 00:00  
lasting 3 hours

workstation10-south performed an unusual upload to an Amazon S3 (Simple Storage Service) bucket. This behavior is unusual based on the amount of transferred data and the time of the transfer. workstation10-south might be compromised and an attacker is attempting to exfiltrate data.

The risk score is higher than normal because one of the participants is a critical device.

**OFFENDER**

workstation14-south  
Site: south5

S3 Bytes Out by S3 Bucket Metric	6h Snapshot	1hr Peak Value	Expected Range	Deviation
168438423658-example		571 MB	0 B - 1 B	57,058,367,900%

**S3 Data Watcher**  
Investigation contains this detection.

Erfahren Sie, wie [eine Untersuchung erstellen](#).

## Auffinden von Erkennungen im ExtraHop-System

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



**Hinweis:** Erkennungen bleiben gemäß Ihrem [System-Lookback-Kapazität](#) für 1-Stunden-Metriken mit einer Mindestspeicherzeit von fünf Wochen. Erkennungen bleiben ohne unterstützende Metriken im System, 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 Gerätegruppenübersicht auf den Link Erkennungen, um zur Seite Erkennungen zu gelangen. Die Entdeckungsliste wird nach der Gerätegruppe als Quelle gefiltert.
- Klicken Sie auf der Protokollseite eines Gerät oder einer Gerätegruppe auf den Link Erkennungen, um zur Seite Erkennungen zu gelangen. Die Entdeckungsliste wird nach Quelle und Protokoll gefiltert.
- Klicken Sie auf einer Aktivitätsdiagramm auf ein Gerät, das animierte Impulse rund um die Kreisbeschriftung anzeigt, um [eine Liste der zugehörigen Erkennungen anzeigen](#). Klicken Sie auf den Link für eine einzelne Erkennung, um die Erkennungsdetails anzuzeigen.
- Zeigen Sie in einem Diagramm auf einem Dashboard oder einer Protokollseite mit der Maus auf ein [Erkennungsmarker](#) um den Titel der zugehörigen Erkennung anzuzeigen, oder klicken Sie auf die Markierung, um die Erkennungsdetails anzuzeigen.