

Erkennungen

Veröffentlicht: 2024-04-10

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.

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.

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.

▶ **Sehen Sie sich die entsprechenden Schulungen an:**

- [Sicherheitserkennungen](#)
- [Leistungserkennungen](#)

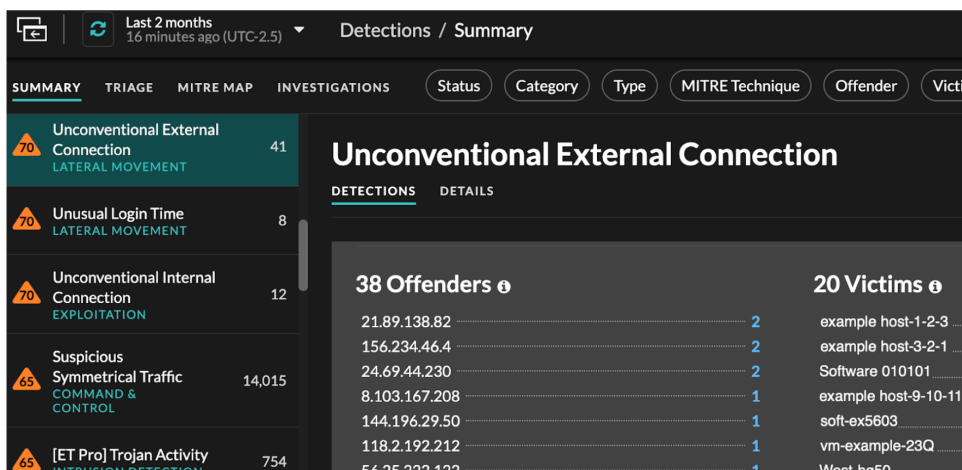
Erkennungen anzeigen

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**.



Unconventional External Connection
LATERAL MOVEMENT

DETECTIONS DETAILS

38 Offenders

21.89.138.82	2
156.234.46.4	2
24.69.44.230	2
8.103.167.208	1
144.196.29.50	1
118.2.192.212	1
56.25.222.122	1


20 Victims

example host-1-2-3	1
example host-3-2-1	1
Software 010101	1
example host-9-10-11	1
soft-ex5603	1
vm-example-23Q	1
West-hq50	1

Sortierung von Erkennungen in der Übersichtsansicht

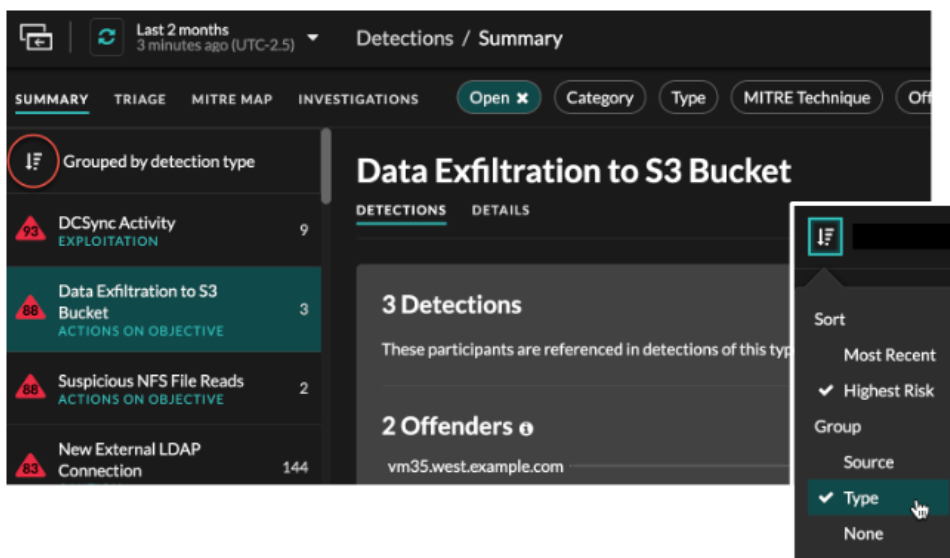
Sie können Erkennungen entweder nach der höchsten Risikoscore oder nach dem jüngsten Ereignis sortieren.

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.



Data Exfiltration to S3 Bucket
ACTIONS ON OBJECTIVE

3 Detections
These participants are referenced in detections of this type

2 Offenders

vm35.west.example.com

Sort

- Most Recent
- Highest Risk

Group

- Source
- Type
- None

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.

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 für die Triage empfiehlt, basierend auf einer kontextuellen Analyse von Faktoren in Ihrer Umgebung.

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, böses 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.

The screenshot shows the MITRE Map interface with the following data:

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 T1136	Hijack Execution Flow	Indicator Removal on Host T1070			

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 **Öffnen** Der Statusfilter wird angewendet auf Erkennungen Seite. Klicken Sie auf **Öffnen** 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 Operationserkennungen 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 Betriebskategorien** Die Optionen sind nach der Anzahl der Funde in der Kategorie sortiert. Härteerkennung 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.

Bedienung 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 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 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 Anruferanfragen 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/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 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 SSL/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 böses 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 Endpunkte von Täter und Opfer werden als Teilnehmer bezeichnet. 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.

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](#)
- [Geräterollen](#)
- Quelle
- 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.

The screenshot shows a detection card for 'VPN Client Data Exfiltration'. On the left, labels point to various parts of the card: 'Risk score and attack chain phase' points to the '70 RISK' indicator; 'Description and root cause of unusual behavior' points to the main text; 'Adjusted risk score' points to the explanation of the risk increase; 'Participant roles and device names' points to the 'OFFENDER' and 'VICTIM' sections; 'Metric data' points to the 'Network Metric' table; and 'Detection tracking and tuning options' points to the 'Actions' dropdown and 'View Detection Details' link.

VPN Client Data Exfiltration
 RISK 70 EXFILTRATION, ACTIONS ON OBJECTIVE
 May 24 08:36
 lasting an hour

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.

OFFENDER
 VPN Client 10
 192.168.237.50
 Site: West 5

VICTIM
 proxy.example.com
 192.168.134.116
 Site: West 5

Network Metric	6h Snapshot	1hr Peak Value	Expected Range	Deviation
Bytes In		356 GB	0 B-623 MB	56,997%

Actions ▾ View Detection Details →

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

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 Details anzuzeigen und auf Links zuzugreifen. Interne Endpunkte zeigen einen Link zur Geräteübersichtsseite an; externe Endpunkte zeigen die Geolokalisierung der IP-Adresse an. **Endpunkt-Suchlinks** 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 Ausgangsendpunkt wird als Teilnehmer betrachtet.

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

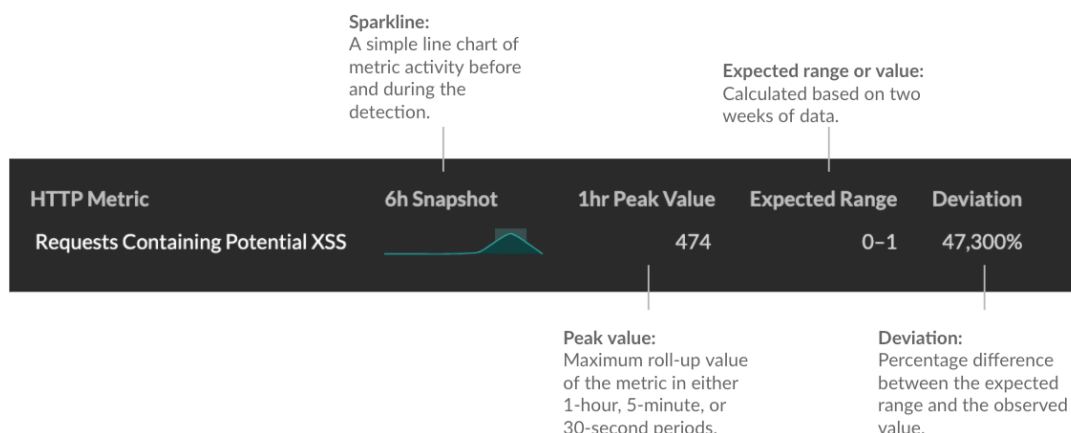
Dauer

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 der Dropdownliste Aktionen, oder klicken Sie auf **Erkennungsdetails anzeigen** um zur Erkennungsdetailseite 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 **Eindämmung von CrowdStrike-Geräten einleiten** das sind Teilnehmer an der Erkennung. (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 Entschlüsselungszeichen angezeigt.

CVE-2021-34527 Windows Print Spooler Exploit Attempt

83 RISK
EXPLOITATION

Dec 8 12:17 • lasting a few seconds

dc05-west received a malicious request that matches an attempt to exploit PrintNightmare, a privilege escalation and remote code execution (RCE) vulnerability in the Windows Print Spooler service. Refer to this [Microsoft Security Update Guide](#) for patch and mitigation information

DETECTED WITH DECRYPTION

Track Detection

Status: No Status | Assignee: Unassigned

Actions:
[Add to an Investigation](#)
[Tune Detection](#)

OFFENDER
externalVM
192.168.226.68

VICTIM
dc05-west
192.168.77.175

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

Erkennungseigenschaften

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.

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

VICTIM
workstation.example.com
192.168.114.49
Site: West1

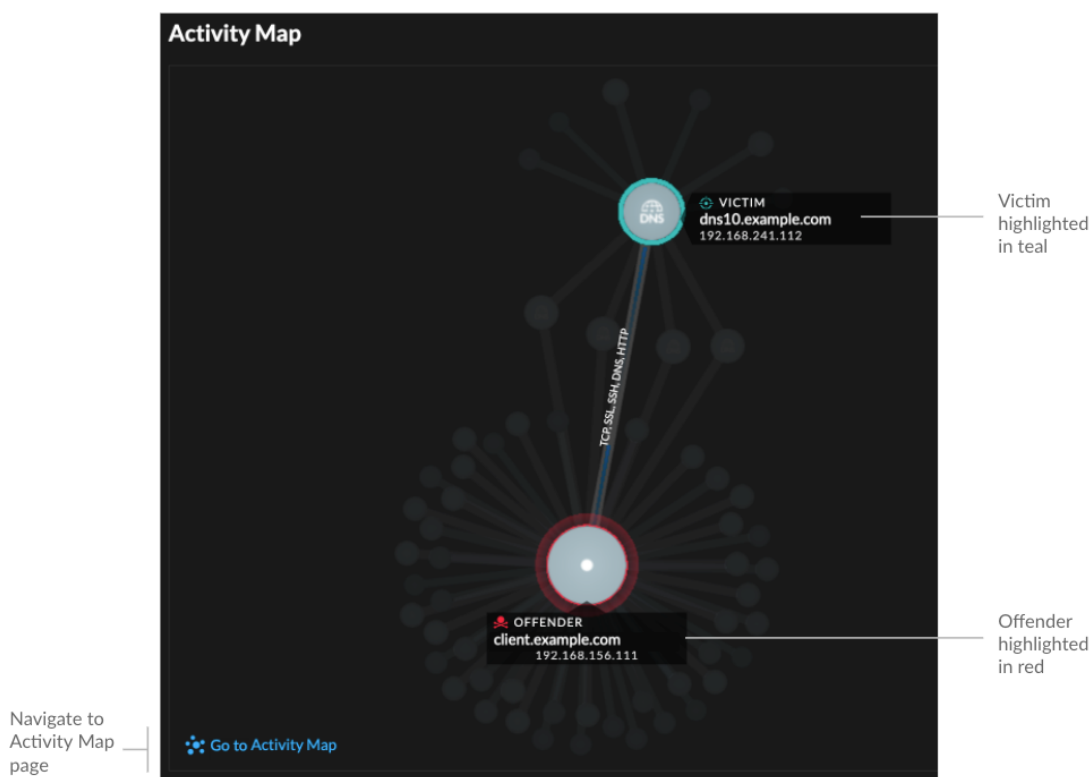
Query Name: A.16.88.248.207.extime.192.168.187.25.east.network
Client Port: 43673
Server Port: 53

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 mit der Erkennung verknüpften Protokoll angezeigt, sodass Sie den Umfang der böswertige 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 enthaltenen **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 Metriktable auf das Symbol [🔍](#) um zugehörige Datensatztransaktionen anzuzeigen. Klicken Sie in einer Datensatztable 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.

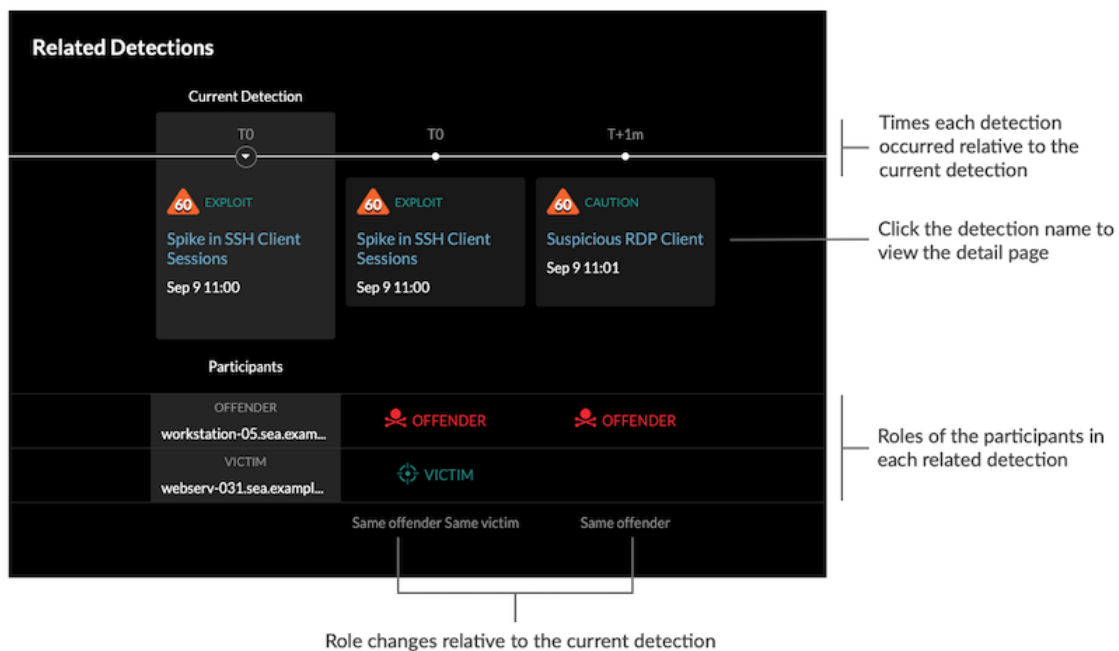
Verhalten vergleichen

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.



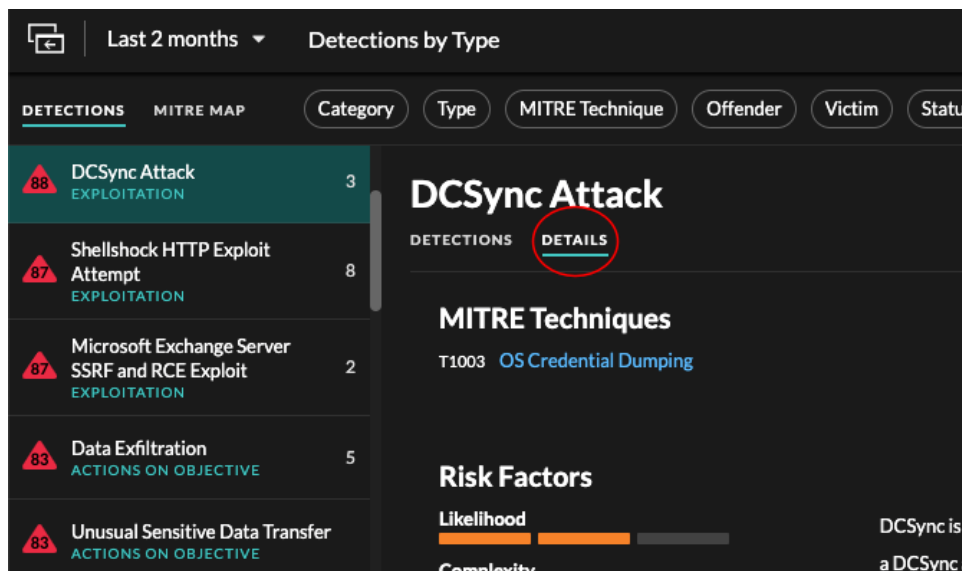
Verwandte Erkennungen, die in einem enthalten sind **empfohlene Untersuchung** sind mit goldenen Links gekennzeichnet und können angeklickt werden, um zur Ermittlungsseite zu gelangen.




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

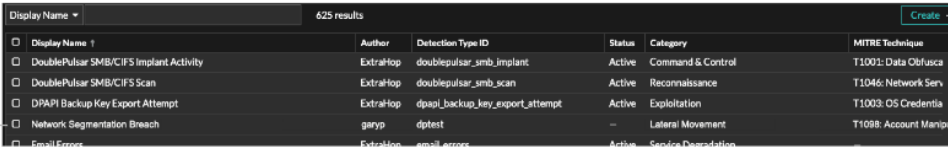


 **Hinweis:** Sie können [Erkennung von Aktionen](#) Detailsseiten mit anderen ExtraHop-Benutzern.

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. .



625 results

Display Name	Author	Detection Type ID	Status	Category	MITRE Technique
<input type="checkbox"/> DoublePulsar SMB/CIFS Implant Activity	ExtraHop	doublepulsar_smb_implant	Active	Command & Control	T1001: Data Obfusca
<input type="checkbox"/> DoublePulsar SMB/CIFS Scan	ExtraHop	doublepulsar_smb_scan	Active	Reconnaissance	T1046: Network Serv
<input type="checkbox"/> DPAPI Backup Key Export Attempt	ExtraHop	dpapi_backup_key_export_attempt	Active	Exploitation	T1003: OS Credentia
<input type="checkbox"/> Network Segmentation Breach	garyp	dnptest	—	Lateral Movement	T1098: Account Manip
<input type="checkbox"/> Email Errors	ExtraHop	email_errors	Active	Service Degradation	

Create a custom detection type

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 Reveal (x) 360).
- Reveal (x) Unternehmenssysteme 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 oder von **Aktionen** Menü auf jeder Erkennungskarte. Ihr ExtraHop-System erstellt außerdem **empfohlene Untersuchungen** als Reaktion auf potenziell böswillige Aktivitäten.

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.

The screenshot shows the 'External Traffic Watch' dashboard. Key sections include:

- Investigation title:** External Traffic Watch
- Authoring information:** Created By: erliche, Created: 1 day ago, Last Updated: a few seconds ago, Investigation ID: 46
- Attack Categories:** Command & Control (4), Reconnaissance (1), Exploitation (0), Lateral Movement (0), Actions on Objectives (0)
- Detections:** 7 detections linked in this investigation. Examples include 'Web Directory Scan' (37) and 'Command-and-Control Endpoint Beaconing' (60).
- Participants:** 17 participants linked in this investigation. Includes 'External Endpoints' and 'High Value Devices'.
- Status and Response Actions:** Status: IN PROGRESS, Assessment: Undecided, Assignee: GPP. Includes a 'Notes' section.

Annotations on the left side of the dashboard:

- Investigation title
- View attack map
- Detection count for each category
- Investigation timeline
- Participants

Annotations on the right side of the dashboard:

- Authoring information
- Update investigation tracking, add or remove detections
- Investigation tracking

Annotation at the bottom:

- Click detections to view detection details

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.

View summary

Investigation timeline

Selected detection

Highlighted detection participants

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 böses 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 böses 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.

C&C with Exfiltration

Recommended Investigation

A device on your network was the victim in a command-and-control (C&C) detection, then became the offender in an exfiltration detection.

Created By

Created

Last Updated

Investigation ID

SUMMARY
ATTACK MAP

Attack Progression
Command & Control **1**
Reconnaissance **0**
Exploitation **0**
Lateral Movement **0**
Actions on C

Detections

2 detections linked in this investigation

Apr 2 10:03 • 3 hours ago

50

Meterpreter C&C Session

COMMAND & CONTROL

125.67.28.39 → webserv.east.example

50

Data Exfiltration

ACTIONS ON OBJECTIVE, EXFILTRATION

webserv.east.example → 151.92.230.221

Participants

2 participants linked in this investigation

External Endpoints

IP

62.144.181.162

test.example.com

External Endpoint

Recurring Participants

webserv.east.example

192.168.16.42

Site: East

Status and Response Actions

Last edited by sean on Apr 02 12:34

Status	Assessment	Assignee
IN PROGRESS	Undecided	garyp

Notes

Reviewed with team. Gary to take lead here. - Sean

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.

98

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.