


Eine Erkennung verfolgen

Veröffentlicht: 2025-02-04

Mit der Erkennungsverfolgung können Sie Benutzer zuweisen, einen Status festlegen und Notizen zu einer Erkennungskarte hinzufügen.

Sie können Ihre Ansicht der Erkennungen auch nach einem bestimmten Status oder einem bestimmten Beauftragten filtern.

 **Video** Sie sich die entsprechende Schulung an: [Erkennungsverfolgung](#)

Bevor Sie beginnen

Benutzer müssen eingeschränkte Schreibmöglichkeiten haben [Privilegien](#) oder höher, um die Aufgaben in diesem Handbuch abzuschließen.

Sie können den Zuständigen in einen beliebigen Benutzer im System ändern, Notizen hinzufügen und den Status einer Erkennung auf einen der folgenden Werte setzen:

Öffnen

Die Erkennung wurde nicht überprüft.

Bestätigen

Die Erkennung wurde festgestellt und sollte bei der Nachverfolgung priorisiert werden.

Im Gange

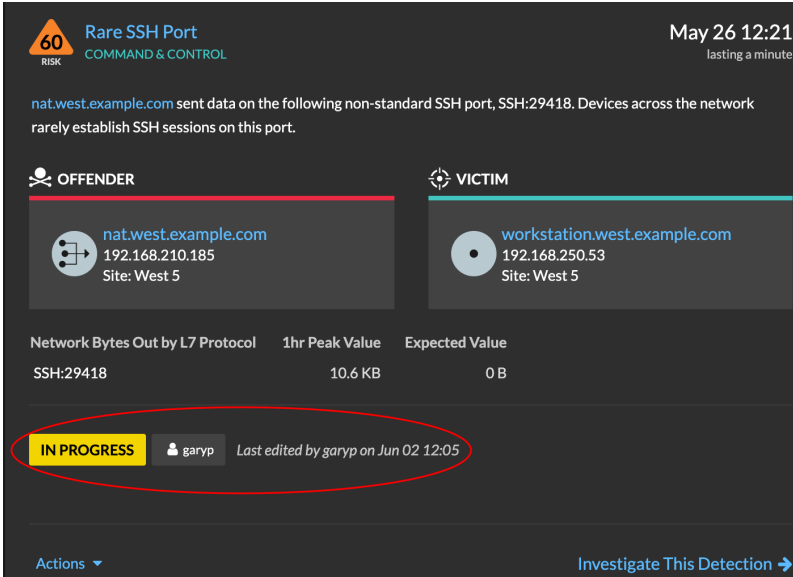
Die Erkennung wurde einem Teammitglied zugewiesen und wird derzeit überprüft.

Geschlossen – Maßnahme ergriffen

Die Erkennung wurde überprüft und Maßnahmen ergriffen, um dem potenziellen Risiko zu begegnen.

Geschlossen – Keine Maßnahmen ergriffen

Die Erkennung wurde überprüft und erforderte keine Maßnahmen.




60 RISK Rare SSH Port
COMMAND & CONTROL

May 26 12:21
lasting a minute

nat.west.example.com sent data on the following non-standard SSH port, SSH:29418. Devices across the network rarely establish SSH sessions on this port.

OFFENDER		VICTIM	
nat.west.example.com	workstation.west.example.com		
192.168.210.185	192.168.250.53		
Site: West 5	Site: West 5		

Network Bytes Out by L7 Protocol	1hr Peak Value	Expected Value
SSH:29418	10.6 KB	0 B

IN PROGRESS  garyp Last edited by garyp on Jun 02 12:05

Actions ▾ [Investigate This Detection](#)

Im Folgenden finden Sie wichtige Überlegungen zu Tracking-Erkennungen:

- Der Status Bestätigt oder Geschlossen verbirgt die Erkennung nicht.
- Der Erkennungsstatus kann von jedem berechtigten Benutzer aktualisiert werden.

- Sie können Erkennungsverfolgung mit ExtraHop und Systemen von Drittanbietern in der [Verwaltung](#) Einstellungen.

Gehen Sie wie folgt vor, um eine Erkennung zu verfolgen:

- Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
- Klicken Sie oben auf der Seite auf **Erkennungen**.
- klicken **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
- Optional: Klicken Sie auf einen Erkennungsstatus, um ihn zur Erkennung hinzuzufügen.

Option	Description
Bestätigen	Die Erkennung wurde festgestellt und sollte bei der Nachverfolgung priorisiert werden.
Im Gange	Die Erkennung wurde einem Teammitglied zugewiesen und wird derzeit überprüft.
Geschlossen – Maßnahme ergriffen	Die Erkennung wurde überprüft und Maßnahmen ergriffen, um dem potenziellen Risiko zu begegnen.
Geschlossen – Keine Maßnahmen ergriffen	Die Erkennung wurde überprüft und erforderte keine Maßnahmen.

The screenshot shows a detection card for 'Rare SSH Port' (RISK 60, COMMAND & CONTROL) dated May 26 12:21. The description states that data was sent on a non-standard SSH port (SSH:29418). The card is divided into OFFENDER (nat.west.example.com, 192.168.210.185) and VICTIM (workstation.west.example.com, 192.168.250.53). A table shows network bytes out by L7 protocol, with SSH:29418 having a 1hr peak value of 10.6 KB and an expected value of 0 B. At the bottom, the status is 'IN PROGRESS' (highlighted with a red circle), assigned to user 'garyp', with a note 'Last edited by garyp on Jun 02 12:05'. An 'Investigate This Detection' link is visible at the bottom right.

- klicken **Spurerkennung...** um den Erkennungsstatus festzulegen, weisen Sie die Erkennung einem Benutzer zu und fügen Sie der Erkennungskarte Notizen hinzu.

Aus dem **Aktionen** Drop-down-Menü, wählen **Spurerkennung...** und dann **Öffnen** um den Status aus der Erkennung zu entfernen; der Beauftragte und die Notizen bleiben sichtbar.

Eine Erkennung von einer Erkennungskarte aus verfolgen

Sie können eine Erkennung verfolgen, indem Sie einen Beauftragten, einen Status und Notizen von einer Erkennungskarte hinzufügen.

Gehen Sie wie folgt vor, um eine Erkennung zu verfolgen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.
2. Klicken Sie oben auf der Seite auf **Erkennungen**.
3. Klicken **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. Optional: Klicken Sie auf einen Erkennungsstatus, um ihn zur Erkennung hinzuzufügen.
5. Klicken **Spurerkennung...** um den Erkennungsstatus festzulegen, weisen Sie die Erkennung einem Benutzer zu und fügen Sie der Erkennungskarte Notizen hinzu.

Aus dem **Aktionen** Dropdown, wählen **Spurerkennung...** und dann **Offen** um den Status der Erkennung zu entfernen; der Beauftragte und die Notizen bleiben sichtbar.



Verfolgen Sie eine Gruppe von Erkennungen anhand einer Erkennungszusammenfassung

In einem Übersichtsfenster auf der Seite „Entdeckungen“ können Sie mehreren Erkennungen gleichzeitig einen Status, eine Person oder eine Notiz zuweisen.

Ein Übersichtsfenster wird angezeigt, wenn Erkennungen in der Zusammenfassungsansicht auf der Seite „Entdeckungen“ nach Typ gruppiert werden.

Gehen Sie wie folgt vor, um eine Gruppe von Erkennungen anhand einer Erkennungszusammenfassung zu verfolgen:

1. Loggen Sie sich in das ExtraHop-System ein über `https://<extrahop-hostname-or-IP-address>`.

2. Klicken Sie oben auf der Seite auf **Erkennungen**.
Standardmäßig sollte sich die Seite in der Zusammenfassungsansicht befinden, in der die Erkennungen nach Typ gruppiert sind. Ist dies nicht der Fall, klicken Sie auf **Zusammenfassende Ansicht**  und dann **nach Typ gruppieren** .
3. Klicken Sie in Ihrer Erkennungsliste auf einen Erkennungstyp.
4. Klicken Sie auf die Kriterien, nach denen Sie filtern möchten: Teilnehmer, Immobilien, Netzwerkstandorte oder Benutzer.
5. Klicken Sie in der unteren linken Ecke des Übersichtsfensters auf **Massenaktionen** Drop-down-Menü und wählen **Alle Erkennungen verfolgen**.
6. Optional: Wählen Sie den Status aus, den Sie auf alle ausgewählten Erkennungen anwenden möchten.
7. Optional: Wählen Sie den Beauftragten aus, den Sie auf alle ausgewählten Erkennungen anwenden möchten.
8. Optional: Wählen Sie aus, ob Sie den vorhandenen Notizen der ausgewählten Funde eine neue Notiz hinzufügen oder alle vorhandenen Notizen überschreiben möchten.
Wenn Sie Ihre Notiz zu vorhandenen Notizen hinzufügen, wird die neue Notiz über vorhandenen Notizen hinzugefügt.
9. Klicken Sie **Speichern**.