


Eine Erkennung verfolgen

Veröffentlicht: 2024-01-31

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.

In Bearbeitung

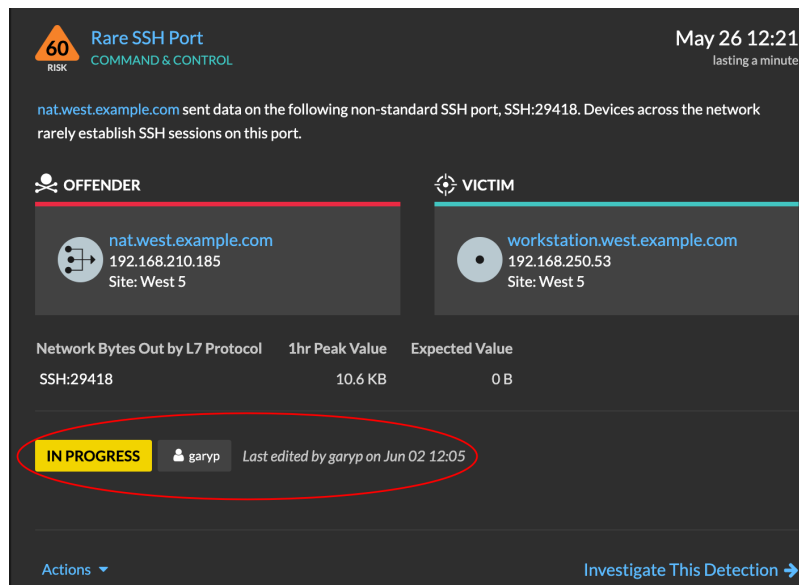
Die Erkennung wurde einem Teammitglied zugewiesen und wird derzeit überprüft.

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 with the following details:

- Risk Level:** 60 (RISK)
- Category:** COMMAND & CONTROL
- Timestamp:** May 26 12:21 (lasting a minute)
- Description:** 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:** nat.west.example.com (192.168.210.185, Site: West 5)
- Victim:** workstation.west.example.com (192.168.250.53, Site: West 5)
- Network Bytes Out by L7 Protocol:** SSH:29418
- 1hr Peak Value:** 10.6 KB
- Expected Value:** 0 B
- Status:** IN PROGRESS (highlighted with a red circle)
- Assigned To:** garyp
- Last Edited:** 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.
- Optional können Sie [Konfigurieren Sie das Erkennungs-Tracking mit einem Drittanbietersystem](#).

- Wenn Sie derzeit Erkennungen mit einem Drittanbietersystem verfolgen, wird das ExtraHop-Erkennungs-Tracking erst angezeigt, wenn Sie die Einstellung in der [Verwaltung](#) Einstellungen.

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 Sie **Aktionen** aus der unteren linken Ecke der Erkennungskarte.
4. 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.
In Bearbeitung	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 erforderliche keine Maßnahmen.

The screenshot shows a detection card titled "Rare SSH Port" with a risk level of 60 (RISK) and a category of "COMMAND & CONTROL". The detection occurred on May 26 at 12:21, lasting for a minute. The description states: "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."

The card is divided into two sections: "OFFENDER" and "VICTIM".

- OFFENDER:** nat.west.example.com (IP: 192.168.210.185, Site: West 5)
- VICTIM:** workstation.west.example.com (IP: 192.168.250.53, Site: West 5)

Below these sections is a table of network statistics:

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

At the bottom of the card, there is a status bar showing "IN PROGRESS" (highlighted with a red circle in the image), assigned to user "garyp", with a note "Last edited by garyp on Jun 02 12:05".

At the very bottom, there are "Actions" and a link to "Investigate This Detection".

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

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

nat.west.example.com
192.168.210.185
Site: West 5

VICTIM

workstation.west.example.com
192.168.250.53
Site: West 5

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

IN PROGRESS shawnk Last edited by garyp on Jun 02 12:15

Let's talk to Samantha's team about this activity.
Assigning to Shawn to follow up.

Actions ▾ Investigate This Detection →

Aus dem **Aktionen** Dropdown, 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 Erkennungsübersicht

In einem Übersichtsfenster auf der Seite Erkennungen können Sie mehreren Erkennungen gleichzeitig einen Status, einen Beauftragten oder eine Notiz zuweisen.

Ein Übersichtsfenster wird angezeigt, wenn Erkennungen in der Übersichtsansicht auf der Seite Erkennungen nach Typ gruppiert sind.

Gehen Sie wie folgt vor, um eine Gruppe von Erkennungen anhand einer Erkennungsübersicht 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 Übersichtsansicht befinden, wobei die Erkennungen nach Typ gruppiert sind. Wenn dies nicht der Fall ist, klicken Sie auf [Ansicht „Zusammenfassung“](#) 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, Eigenschaften oder Netzwerkorte.
5. Klicken Sie in der unteren linken Ecke des Übersichtsfensters auf **Alle Erkennungen verfolgen**.
Der Link enthält, wie viele Erkennungen Sie aktualisieren. Beispiel: Alle 14 Erkennungen verfolgen. Dieser Link wird nicht im Übersichtsfenster angezeigt, wenn der Filter Status Versteckt angewendet wird.
6. Optional: Wählen Sie den Status aus, den Sie auf alle ausgewählten Erkennungen anwenden möchten.
7. Optional: Wählen Sie den Verantwortlichen aus, den Sie auf alle ausgewählten Erkennungen anwenden möchten.
8. Optional: Wählen Sie aus, ob Sie den vorhandenen Notizen der ausgewählten Entdeckungen eine neue Notiz hinzufügen oder alle vorhandenen Notizen überschreiben möchten.
Wenn Sie Ihre Notiz zu vorhandenen Notizen hinzufügen, wird die neue Notiz über den vorhandenen Notizen hinzugefügt.
9. klicken **Speichern**.