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: Sehen 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:

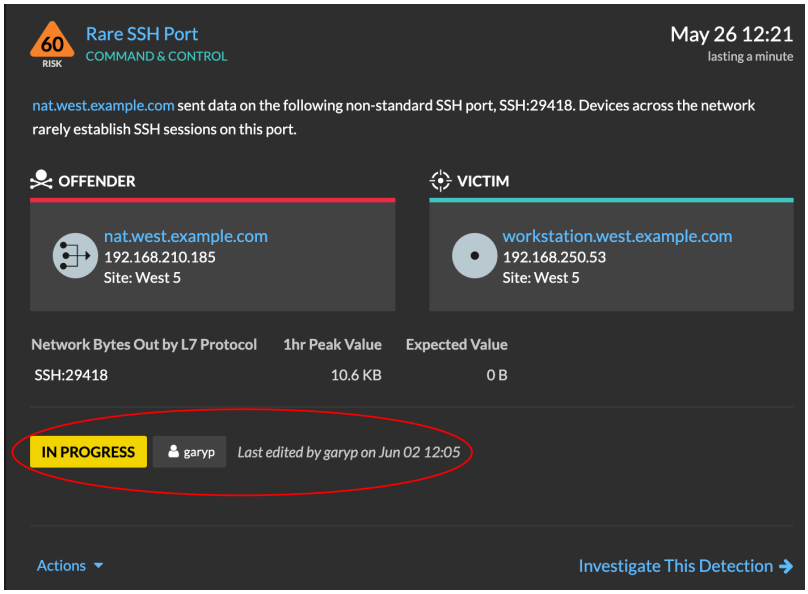
Öffnen
Die Erkennung wurde nicht überprüft.

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.



Im Folgenden finden Sie wichtige Überlegungen zu Tracking-Erkennungen:

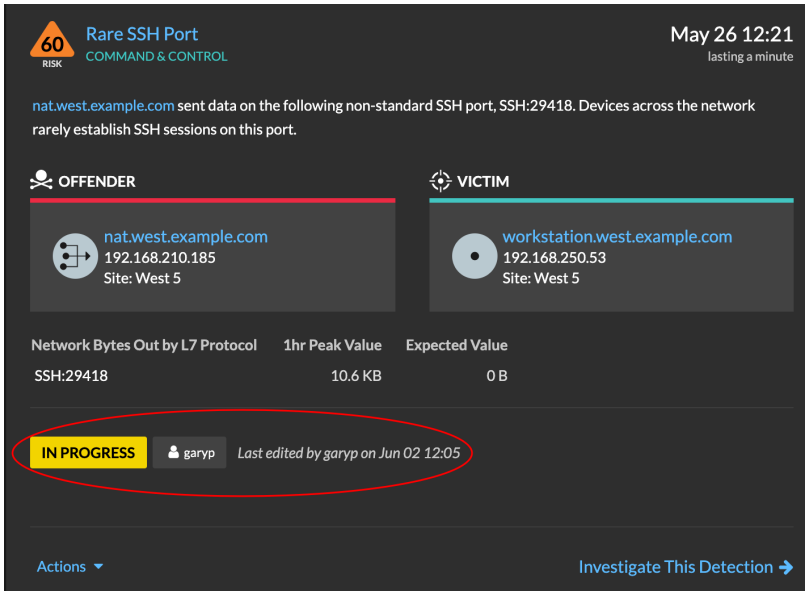
- Der Status Bestätigt oder Geschlossen verbirgt die Erkennung nicht.
- Der Erkennungsstatus kann von jedem berechtigten Benutzer aktualisiert werden.

- Sie können Erkennungsverfolgung mit ExtraHop und Systemen von Drittanbietern in der Verwaltung Einstellungen.

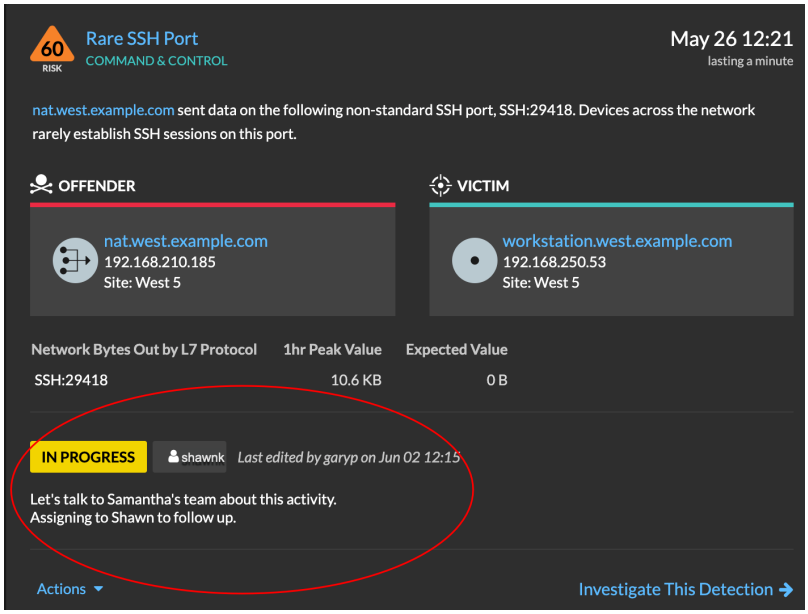
Gehen Sie wie folgt vor, um eine Erkennung zu verfolgen:

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.

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.



5. 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**.