Eine Erkennung verfolgen

Veröffentlicht: 2023-10-24

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

Sie können Ihre Erkennungsansicht auch nach einem bestimmten Status oder Beauftragten filtern.

Bevor Sie beginnen
Benutzer müssen über eingeschränkte Schreibberechtigungen verfügen Privilegien oder höher, um die Aufgaben in diesem Handbuch abzuschließen.

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

Offen

Die Erkennung wurde nicht überprüft.

Bestätigen

Die Erkennung wurde beobachtet und sollte für die Nachsorge priorisiert werden.

In Bearbeitung

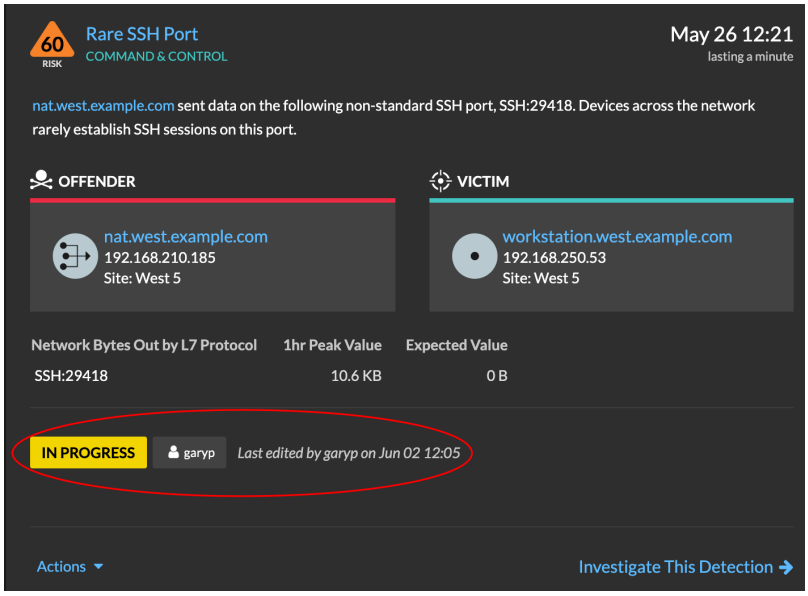
Die Erkennung wurde einem Teammitglied zugewiesen und wird derzeit überprüft.

Geschlossen — Maßnahme ergriffen

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

Geschlossen — Es wurden keine Maßnahmen ergriffen

Die Erkennung wurde überprüft und erforderte keine Maßnahmen.



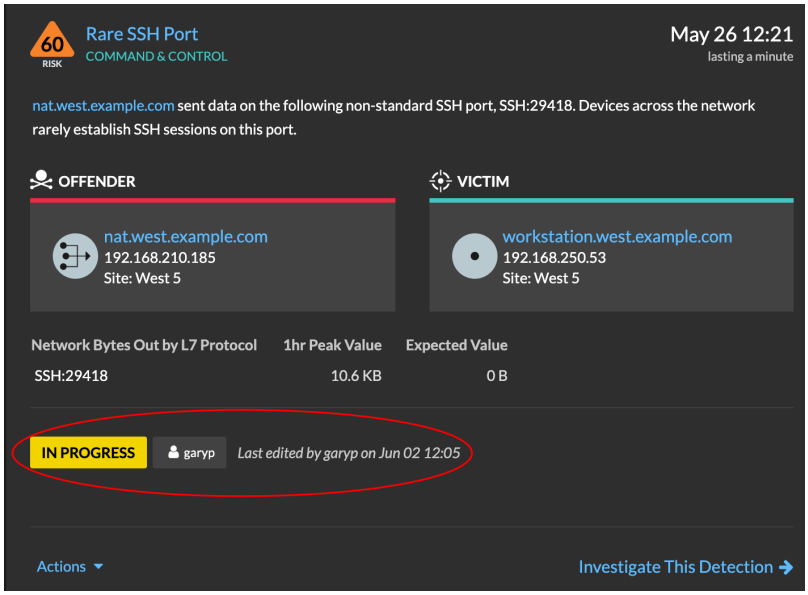
Hier sind wichtige Überlegungen zur Nachverfolgung von Erkennungen:

- Der Status Bestätigt oder Geschlossen verbirgt die Erkennung nicht.
- Der Erkennungsstatus kann von jedem privilegierten Benutzer aktualisiert werden.
- Wahlweise können Sie Konfigurieren Sie das Erkennungs-Tracking mit einem Drittanbietersystem.
- Wenn Sie derzeit Erkennungen mit einem Drittanbietersystem verfolgen, wird die ExtraHop-Erkennungsverfolgung erst angezeigt, wenn Sie die Einstellung in der Verwaltung Einstellungen.

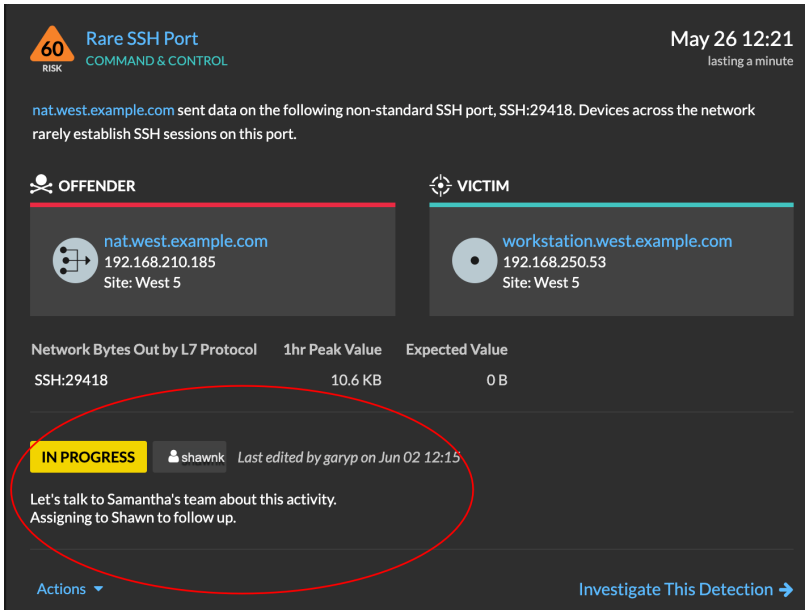
Gehen Sie wie folgt vor, um eine Erkennung zu verfolgen:

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 **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 beobachtet und sollte für die Nachsorge 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 — Es wurden 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** Dropdown, wählen **Spurerkennung...** und dann **Offen** um den Status 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**.