Forensik

Cloud Insights

NetApp
April 16, 2024

Inhalt

Forensik

Forensik - Alle Aktivitäten

Auf der Seite Alle Aktivitäten können Sie die Aktionen verstehen, die für Einheiten in der Workload-Sicherheitsumgebung durchgeführt werden.

Alle Aktivitätsdaten Werden Untersucht

Klicken Sie auf **Forensics > Vorgangsforensics** und klicken Sie auf die Registerkarte **Alle Aktivitäten**, um die Seite Alle Aktivitäten aufzurufen. Diese Seite bietet einen Überblick über Aktivitäten in Ihrer Umgebung und hebt die folgenden Informationen hervor:

- Ein Diagramm mit „*Aktivitätsverlauf*“ (Zugriff pro Minute/pro 5 Minuten/pro 10 Minuten basierend auf dem ausgewählten globalen Zeitbereich)

  Sie können das Diagramm vergrößern, indem Sie ein Rechteck im Diagramm herausziehen. Die gesamte Seite wird geladen, um den vergrößerten Zeitbereich anzuzeigen. Wenn der Zoom vergrößert wird, wird eine Schaltfläche angezeigt, mit der der Benutzer zoomen kann.

- Ein Diagramm mit „*Aktivitätstypen*“. Um die Vorgangshistorie-Daten nach Aktivitätstyp zu erhalten, klicken Sie auf den entsprechenden x-Achse-Label-Link.
- Ein Diagramm der Aktivität auf_Entity Types_. Um Vorgangsdaten nach Entitätstyp zu erhalten, klicken Sie auf den entsprechenden Link für die X-Achse-Bezeichnung.
- Eine Liste der Daten „*Alle Aktivitäten*“

Die Tabelle **Alle Aktivitäten** enthält die folgenden Informationen. Beachten Sie, dass standardmäßig nicht alle dieser Spalten angezeigt werden. Sie können die anzuzeigenden Spalten auswählen, indem Sie auf das Zahnrad-Symbol klicken .

- Die **Zeit**, auf die ein Unternehmen zugegriffen wurde, einschließlich Jahr, Monat, Tag und Uhrzeit des letzten Zugriffs.
- Der * Benutzer*, der mit einem Link auf das Entity zugegriffen hat "Benutzerinformationen".
- Die **Aktivität**, die der Benutzer durchgeführt hat. Folgende Typen werden unterstützt:
  - **Gruppeneigentum ändern** - Gruppeneigentum ist von Datei oder Ordner geändert. Weitere Informationen zu Gruppeneigentum finden Sie unter "Dieser Link."
  - **Eigentümer ändern** - das Eigentum an Datei oder Ordner wird zu einem anderen Benutzer geändert.
  - **Berechtigung ändern** - Datei- oder Ordnerrechte wurde geändert.
  - **Erstellen** - Erstellen Sie Datei oder Ordner.
  - **Löschen** - Datei oder Ordner löschen. Wenn ein Ordner gelöscht wird, werden *delete* Ereignisse für alle Dateien in diesem Ordner und Unterordnern abgerufen.
  - **Lesen** - Datei wird gelesen.
  - **Metadaten lesen** - nur bei Option zur Ordnerüberwachung. Wird beim Öffnen eines Ordners unter Windows erzeugt oder „ls“ innerhalb eines Ordners unter Linux ausgeführt.
  - **Umbenennen** - Umbenennen Sie die Datei oder den Ordner.

- **Schreiben** - Daten werden in eine Datei geschrieben.
- **Metadaten schreiben** - Dateimetadaten werden geschrieben, zum Beispiel, Berechtigung geändert.
- **Andere Änderung** - jedes andere Ereignis, das oben nicht beschrieben wird. Alle nicht zugeordneten Ereignisse werden dem Aktivitätstyp „andere Änderung“ zugeordnet. Gilt für Dateien und Ordner.

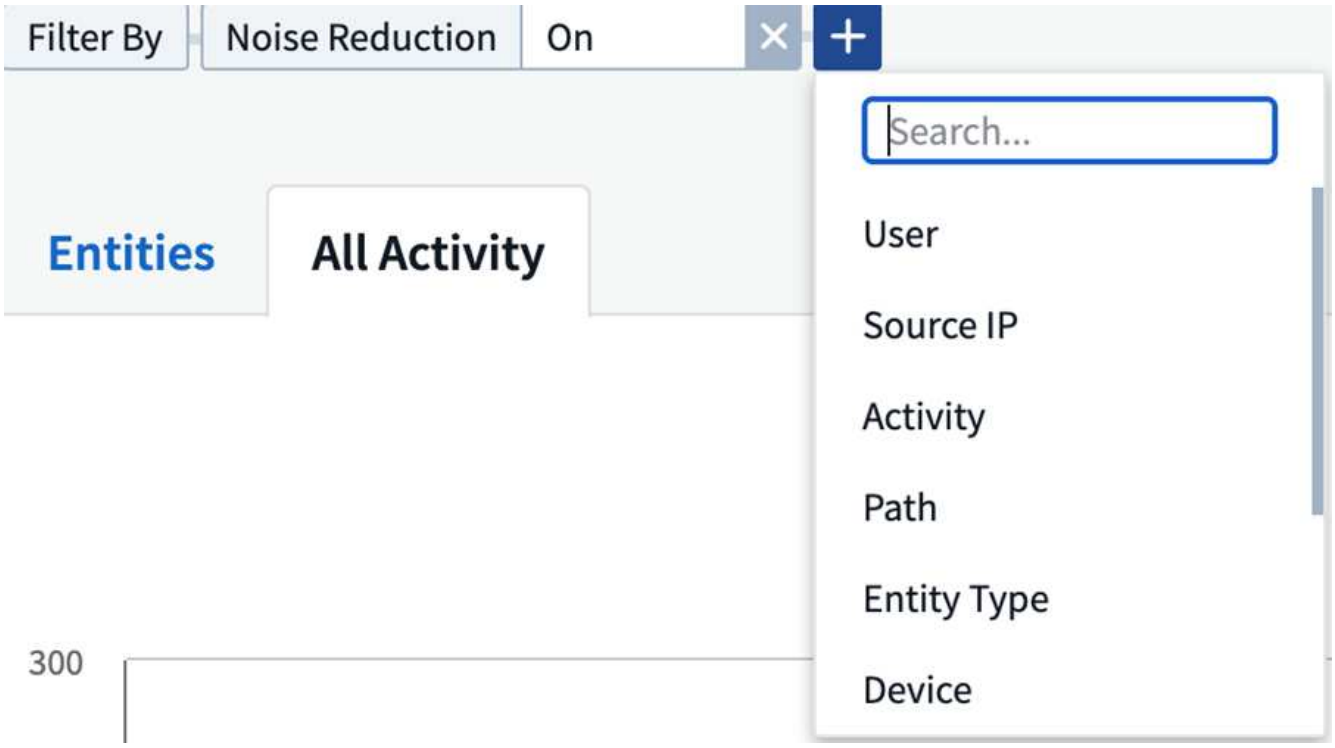
- Der **Pfad** zur Entität mit einem Link zum "Entity Detail-Daten"
- **Entity Type**, einschließlich der Endung Entity (d. h. Datei) (.doc, .docx, .tmp usw.)
- Das **Gerät**, in dem sich die Entitäten befinden
- Das **Protokoll** zum Abrufen von Ereignissen.
- Der **Original-Pfad**, der bei der Umbenennung der Originaldatei verwendet wird. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie die Spaltenauswahl, um diese Spalte zur Tabelle hinzuzufügen.
- Das **Volumen**, in dem sich die Entitäten befinden. Diese Spalte ist in der Tabelle standardmäßig nicht sichtbar. Verwenden Sie die Spaltenauswahl, um diese Spalte zur Tabelle hinzuzufügen.

Filtern Forensischer Vorgangshistorie-Daten

Es gibt zwei Methoden, mit denen Sie Daten filtern können.

1. Bewegen Sie den Mauszeiger über das Feld in der Tabelle, und klicken Sie auf das angezeigte Filtersymbol. Der Wert wird den entsprechenden Filtern in der oberen Liste *Filter by* hinzugefügt.
2. Filtern Sie die Daten, indem Sie das Feld *Filter by* eingeben:

   Wählen Sie den entsprechenden Filter aus dem oberen Widget ‘Filtern nach’ aus, indem Sie auf die Schaltfläche **[+]** klicken:



   Geben Sie den Suchtext ein

   Drücken Sie die Eingabetaste, oder klicken Sie außerhalb des Filterfelds, um den Filter anzuwenden.

Sie können forensische Aktivitätsdaten nach folgenden Feldern filtern:

- Der Typ **Aktivität**.
- **Quell-IP**, auf die das Element zugegriffen wurde. Sie müssen eine gültige Quell-IP-Adresse in doppelten Anführungszeichen angeben, z. B. „10.1.1.1.“. Unvollständige IPs wie „10.1.1.**“, „10.1.**.*“ usw. funktionieren nicht.
- **Protokoll** zum Abrufen protokollspezifischer Aktivitäten.
- **Benutzername** des Benutzers, der die Aktivität ausführt. Sie müssen den genauen Benutzernamen angeben, um sie zu filtern. Die Suche mit teilweisen Nutzernamen oder teilweisen Nutzernamen, vorfixiert oder mit ‘*’ abgestickt, funktioniert nicht.
- **Rauschunterdrückung** zum Filtern von Dateien, die in den letzten 2 Stunden vom Benutzer erstellt werden. Sie wird auch zum Filtern temporärer Dateien (z. B. .tmp-Dateien) verwendet, auf die der Benutzer Zugriff hat.

Die folgenden Felder unterliegen speziellen Filterregeln:

- **Entity Type**, mit Entity (file) Extension
- **Pfad** der Entität
- **Benutzer** die Aktivität durchführen
- **Gerät** (SVM), in dem sich Entitäten befinden
- **Volumen**, in dem sich Entitäten befinden
- Der **Original-Pfad**, der bei der Umbenennung der Originaldatei verwendet wird.

Die vorhergehenden Felder unterliegen beim Filtern folgenden Kriterien:

- Der genaue Wert sollte in Anführungszeichen liegen: Beispiel: "suchtext"
- Platzhalter-Strings dürfen keine Anführungszeichen enthalten: Beispiel: suchtext, *suchtext*, filtert nach Zeichenfolgen, die ‘seartext’ enthalten.
- String mit einem Präfix, Beispiel: suchtext* , sucht alle Strings, die mit ‘seartext’ beginnen.

Forensische Vorgangshistorie-Daten Sortieren

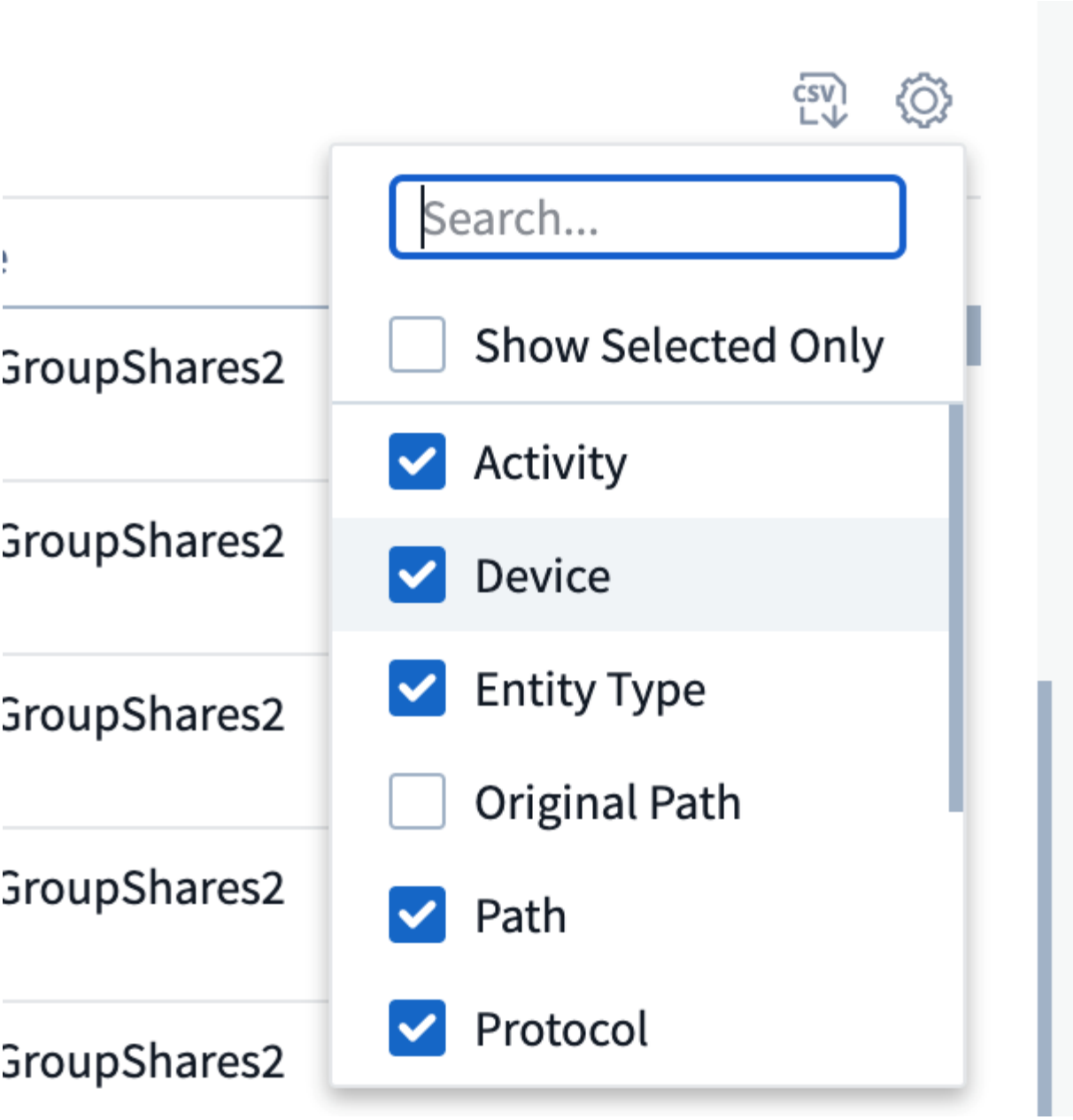
Sie können Vorgangshistorie-Daten nach_Time, User, Source IP, Activity, Path_ und_Entity Type_ sortieren. Standardmäßig wird die Tabelle nach absteigender_Time_-Reihenfolge sortiert, was bedeutet, dass die neuesten Daten zuerst angezeigt werden. Die Sortierung ist für die Felder *Device* und *Protocol* deaktiviert.

Alle Aktivitäten Werden Exportiert

Sie können den Vorgangsverlauf in eine CSV-Datei exportieren, indem Sie über der Tabelle „Vorgangsverlauf“ auf die Schaltfläche „*Export*“ klicken. Beachten Sie, dass nur die 100,000 wichtigsten Datensätze exportiert werden. Je nach Datenmenge kann es einige Sekunden bis zu mehreren Minuten dauern, bis der Export abgeschlossen ist.

Spaltenauswahl für Alle Aktivitäten

In der Tabelle *Alle Aktivitäten* werden standardmäßig ausgewählte Spalten angezeigt. Um die Spalten hinzuzufügen, zu entfernen oder zu ändern, klicken Sie auf das Zahnradsymbol rechts neben der Tabelle und wählen Sie aus der Liste der verfügbaren Spalten aus.



Aufbewahrung Des Aktivitätsverlaufs

Der Aktivitätsverlauf wird 13 Monate lang in aktiven Workload-Sicherheitsumgebungen aufbewahrt.

Anwendbarkeit von Filtern in Forensics Seite

Filtern	Das macht es	Beispiel	In welchen Filtern anwendbar?	Gilt nicht für welche Filter	Ergebnis

* (Sternchen)	Ermöglicht Ihnen die Suche nach allem	Auto*03172022	Benutzer, PFAD, Einheitstyp, Gerätetyp, Volume, Ursprünglicher Pfad		Gibt alle Ressourcen zurück, die mit „Auto“ beginnen und mit „03172022“ enden
? (Fragezeichen)	Ermöglicht die Suche nach einer bestimmten Anzahl von Zeichen	AutoSabotageUser1_03172022?	Benutzer, Einheitstyp, Gerät, Volume		Gibt AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022AB, AutoSabotageUser1_031720225 usw. zurück
ODER	Ermöglicht Ihnen die Angabe mehrerer Elemente	AutoSabotageUser1_03172022 ODER AutoBefreiUser4_03162022	Benutzer, Domäne, Benutzername, PFAD, Einheitstyp, Gerät, Originalpfad		Gibt eine beliebige von AutoSabotageUser1_03172022 ODER AutoBefreiUser4_03162022 zurück
NICHT	Ermöglicht das Ausschließen von Text aus den Suchergebnissen	NICHT automatisch BefreiUser4_03162022	Benutzer, Domäne, Benutzername, PFAD, Einheitstyp, Ursprünglicher PFAD, Volume	Gerät	Gibt alles zurück, was nicht mit "AutoBefreiUser4_03162022" beginnt
Keine	Sucht in allen Feldern nach Null-Werten	Keine	Domäne		Gibt Ergebnisse an, bei denen das Zielfeld leer ist

Pfadsuche/Original-Pfadsuche

Suchergebnisse mit und ohne / werden unterschiedlich sein

/AutoDir1/AutoFile	Funktioniert
AutoDir1/AutoFile	Funktioniert nicht
/AutoDir1/AutoFile (Dir1)	Dir1 partielle Substring funktioniert nicht
„/AutoDir1/AutoFile03242022“	Genaue Suche funktioniert
Auto*03242022	Funktioniert nicht
AutoSabotageUser1_03172022?	Funktioniert nicht

/AutoDir1/AutoFile03242022 ODER /AutoDir1/AutoFile03242022	Funktioniert
NICHT /AutoDir1/AutoFile03242022	Funktioniert
NICHT /AutoDir1	Funktioniert
NICHT /AutoFile03242022	Funktioniert nicht
*	Zeigt alle Einträge an

Fehlerbehebung

Problem	Versuchen Sie Dies
In der Tabelle „Alle Aktivitäten“ in der Spalte ‘Benutzer“ wird der Benutzername wie folgt angezeigt: „ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” oder LDAP:default:80038003“	Mögliche Gründe sind: 1. Es wurden noch keine User Directory Collectors konfiguriert. Um einen hinzuzufügen, gehen Sie zu **Workload Security > Collectors > User Directory Collectors** und klicken Sie auf **+User Directory Collector**. Wählen Sie *Active Directory* oder *LDAP Directory Server*. 2. Ein Benutzerverzeichnissammler wurde konfiguriert, ist jedoch angehalten oder befindet sich im Fehlerzustand. Bitte gehen Sie zu **Collectors > User Directory Collectors** und überprüfen Sie den Status. Siehe "Fehlerbehebung für Benutzerverzeichnissammler" Der Dokumentation für Tipps zur Fehlerbehebung. Nach der ordnungsgemäßen Konfiguration wird der Name innerhalb von 24 Stunden automatisch behoben. Wenn die Lösung immer noch nicht behoben wird, überprüfen Sie, ob Sie den korrekten Benutzer-Data Collector hinzugefügt haben. Stellen Sie sicher, dass der Benutzer tatsächlich Teil des hinzugefügten Active Directory/LDAP Directory Servers ist.
Einige NFS-Ereignisse werden in der UI nicht angezeigt.	Überprüfen Sie Folgendes: 1. Ein Benutzer-Verzeichnis-Collector für AD-Server mit POSIX-Attributen sollte mit dem unixid-Attribut ausgeführt werden, das über UI aktiviert ist. 2. Jeder Benutzer, der NFS-Zugang macht, sollte angezeigt werden, wenn er in der Benutzerseite von UI 3 durchsucht wird. RAW-Ereignisse (Ereignisse, für die der Benutzer noch nicht erkannt wurde) werden für NFS 4 nicht unterstützt. Anonymer Zugriff auf den NFS-Export wird nicht überwacht. 5. Stellen Sie sicher, dass die NFS-Version in weniger als NFS4.1 verwendet wird.

Nachdem Sie einige Buchstaben mit einem Platzhalterzeichen wie Sternchen (*) in die Filter auf den Seiten Forensics *All Activity* oder *entities* eingegeben haben, werden die Seiten sehr langsam geladen.	Ein Sternchen (*) in der Suchzeichenfolge sucht nach allem. Führende Platzhalterzeichenfolgen wie *<searchTerm>* oder *<searchTerm>** führen jedoch zu einer langsamen Abfrage. Um eine bessere Leistung zu erzielen, verwenden Sie stattdessen Präfix-Strings im Format *<searchTerm>** (mit anderen Worten: Fügen Sie das Sternchen (*) *nach* einem Suchbegriff hinzu). Beispiel: Verwenden Sie den String *testvolume** anstatt **testvolume* oder **Test*Volume*. Verwenden Sie eine präfixbasierte Suche, um alle Aktivitäten unterhalb eines bestimmten Ordners rekursiv anzuzeigen (hierarchische Suche). Z.B. */path1/path2/path3* oder *"/path1/path2/path3"* listet alle Aktivitäten rekursiv unter */path1/path2/path3* auf. Alternativ können Sie die Option „zum Filter hinzufügen" auf der Registerkarte „Alle Aktivitäten" verwenden.
Bei der Verwendung eines Pfadfilters tritt ein Fehler „Anfrage fehlgeschlagen mit Statuscode 500/503" auf.	Versuchen Sie, einen kleineren Datumsbereich zum Filtern von Datensätzen zu verwenden.

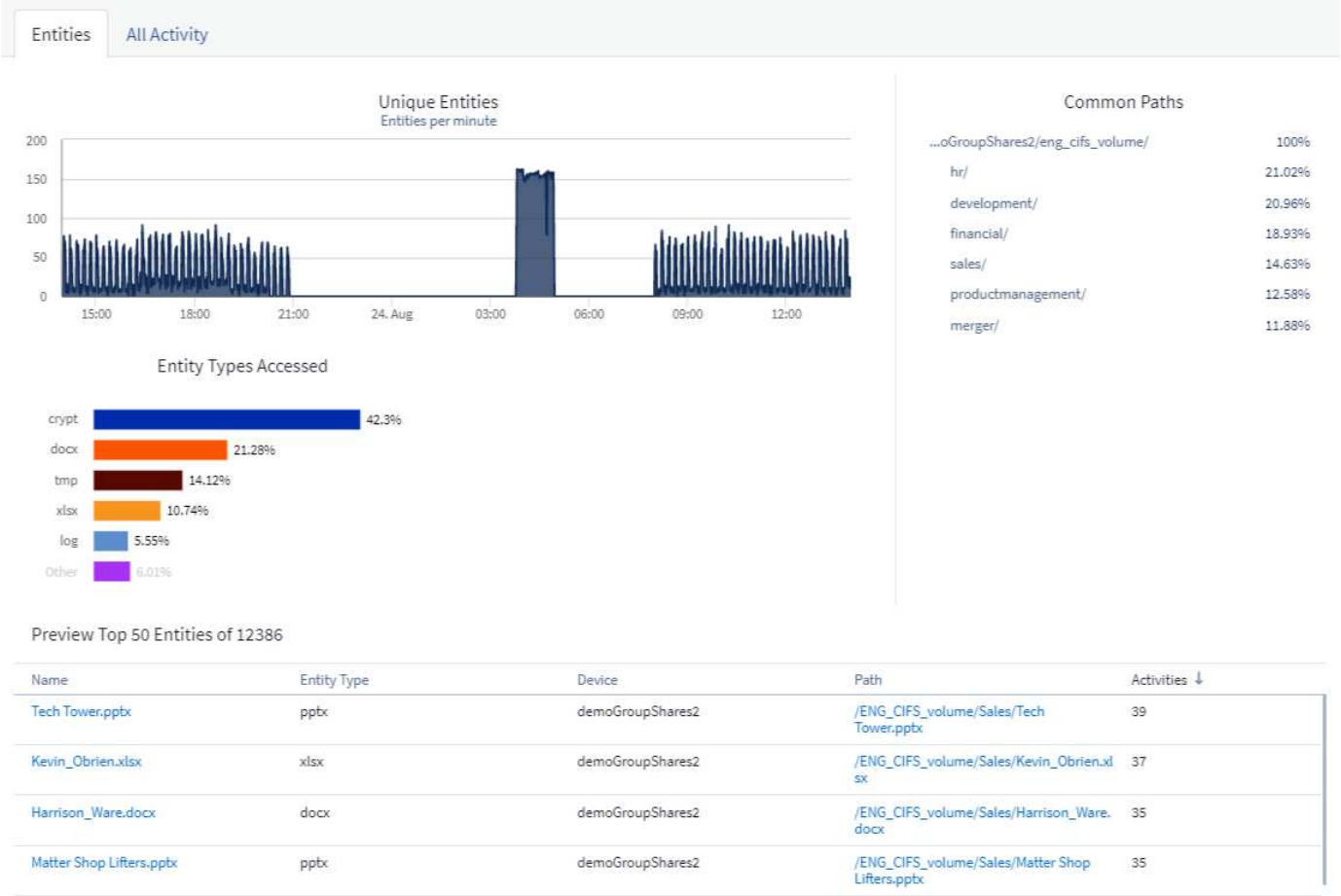
Seite Mit Forensischen Einheiten

Die Seite Forensics Entities enthält detaillierte Informationen über die Aktivität der Entität in Ihrer Umgebung.

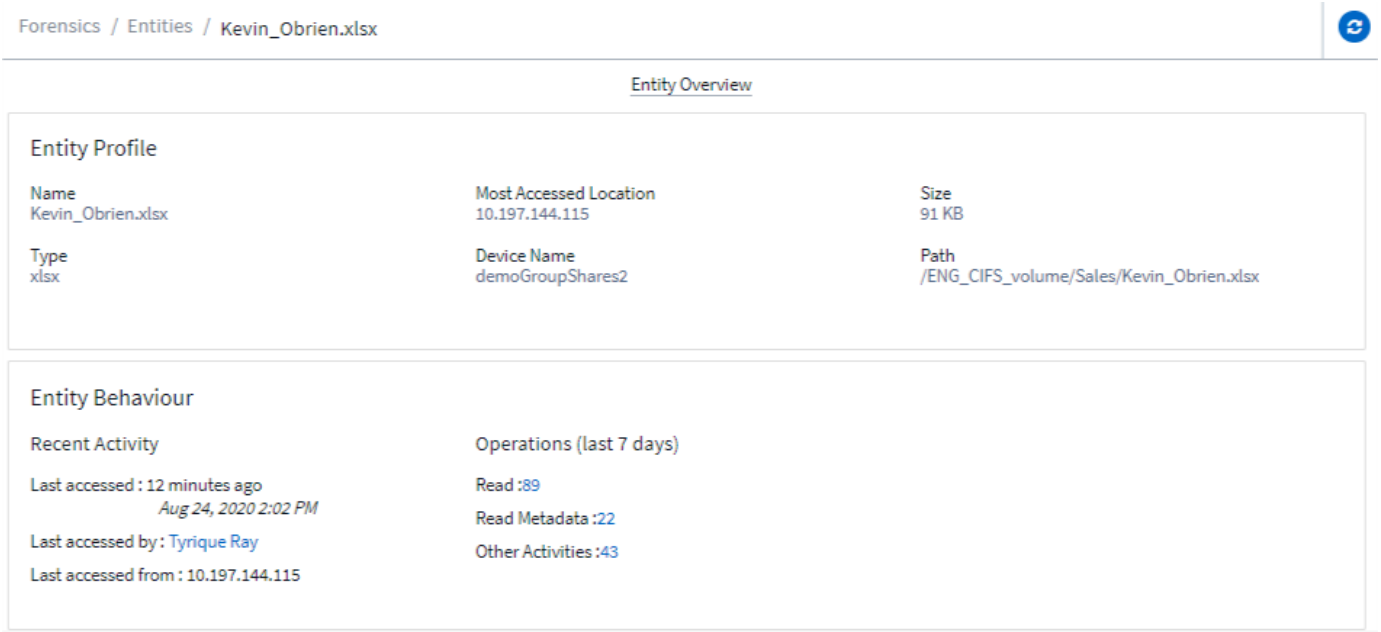
Untersuchung Von Informationen Zur Einheit

Klicken Sie auf **Forensics > Vorgangsforensics**, und klicken Sie auf die Registerkarte *Entities*, um die Seite Entities aufzurufen.

Auf dieser Seite erhalten Sie einen Überblick über die Aktivitäten der Einheit in Ihrer Umgebung, und Sie können die folgenden Informationen hervorheben: * Ein Diagramm mit_eindeutigen Entitäten_ Zugriffsberechtigung pro Minute * Ein Diagramm mit_Entity-Typen, auf die zugegriffen wurde_ * Eine Aufschlüsselung der_Common Paths_ * Eine Liste der *Top 50 Entities* von der Gesamtanzahl der Entitäten



Durch Klicken auf eine Entität in der Liste wird eine Übersichtsseite für die Entität geöffnet, auf der ein Profil der Entität mit Details wie Name, Typ, Gerätename, IP-Adresse und Pfad sowie das Entity-Verhalten wie Benutzer, IP, Und die Zeit, zu der das Unternehmen zuletzt aufgerufen wurde.



Übersicht Über Forensische Benutzer

Informationen zu jedem Benutzer finden Sie in der Benutzerübersicht. Verwenden Sie diese Ansichten, um Benutzereigenschaften, zugehörige Einheiten und aktuelle Aktivitäten zu verstehen.

Benutzerprofil

Zu den Benutzerprofilinformationen gehören die Kontaktinformationen und der Standort des Benutzers. Das Profil enthält folgende Informationen:

- Name des Benutzers
- E-Mail-Adresse des Benutzers
- Benutzermanager
- Telefonkontakt für den Benutzer
- Standort des Benutzers

Benutzerverhalten

Die Informationen zum Benutzerverhalten identifizieren aktuelle Aktivitäten und Vorgänge, die vom Benutzer durchgeführt werden. Zu diesen Informationen gehören:

- Aktuelle Aktivität
  - Letzter Zugriffsort
  - Aktivitätsdiagramm
  - Meldungen
- Betrieb der letzten sieben Tage
  - Anzahl an Operationen

Intervall Aktualisieren

Die Benutzerliste wird alle 12 Stunden aktualisiert.

Aufbewahrungsrichtlinie

Wenn die Benutzerliste nicht erneut aktualisiert wird, wird sie 13 Monate lang aufbewahrt. Nach 13 Monaten werden die Daten gelöscht. Wenn die Workload-Sicherheitsumgebung gelöscht wird, werden alle der Umgebung zugeordneten Daten gelöscht.