Forensik

Data Infrastructure Insights

NetApp
December 19, 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 die Aktivitäten Ihres Mandanten und hebt die folgenden Informationen hervor:

- Ein Diagramm mit *Aktivitätsverlauf* (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.

- Eine Liste der *All Activity*-Daten.
- In einer Dropdown-Liste „Gruppieren nach“ können Sie die Aktivität nach Benutzern, Pfad, Entitätstyp usw. gruppieren
- Über der Tabelle steht eine Schaltfläche für gemeinsamen Pfad zur Verfügung, auf die Sie klicken können, um das Fenster mit Details zum Entity-Pfad zu öffnen.

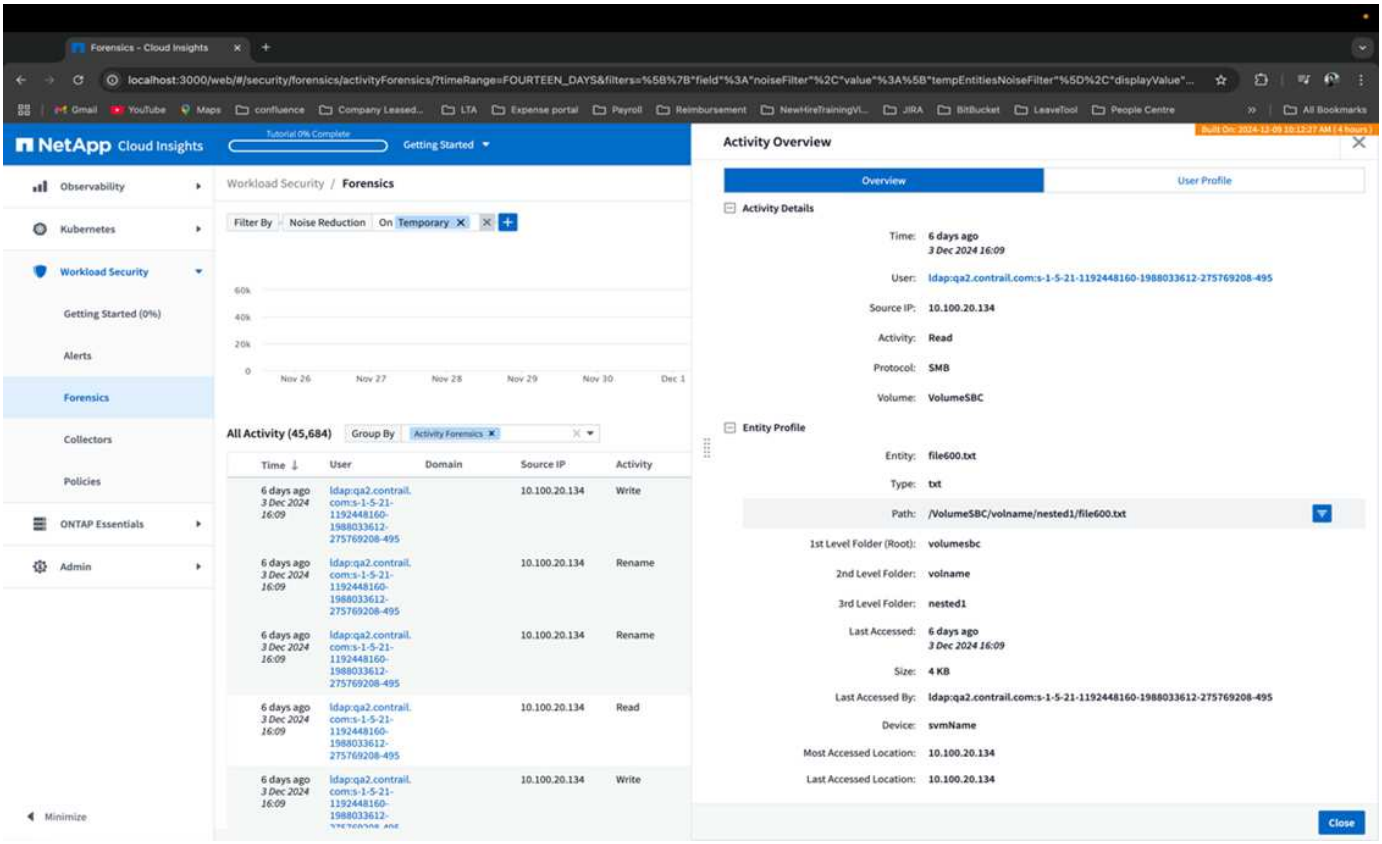
Die Tabelle **Alle Aktivitäten** enthält die folgenden Informationen. Beachten Sie, dass standardmäßig nicht alle dieser Spalten angezeigt werden. Sie können Spalten auswählen, die angezeigt werden sollen, indem Sie auf das Zahnradsymbol klicken.

- Die **Zeit**, auf die ein Unternehmen zugegriffen wurde, einschließlich Jahr, Monat, Tag und Uhrzeit des letzten Zugriffs.
- Der **user**, der auf die Entität mit einem Link zum als Slide-out Panel zugegriffen "Benutzerinformationen"hat.
- Die **Aktivität**, die der Benutzer durchgeführt hat. Folgende Typen werden unterstützt:
  - **Gruppeneigentum ändern** - Gruppeneigentum ist von Datei oder Ordner geändert. Weitere Informationen zur Gruppenbeteiligung 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** ist *entity* Pfad.
- Der * 1st Level Folder (Root)* ist das Stammverzeichnis des Entity-Pfades in Kleinbuchstaben.
- Der **2nd Level Folder** ist das Verzeichnis der Entity PATH der zweiten Ebene im Kleinbuchstaben.
- Der Ordner **3rd Level** ist das Verzeichnis 3rd Level des Entity PATH im Kleinbuchstaben.
- Der Ordner **4th Level** ist das Verzeichnis der Entity PATH der vierten Ebene in Kleinbuchstaben.
- Die Erweiterung **Entity Type**, einschließlich 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.

Wenn Sie eine Tabellenzeile auswählen, wird ein Schiebefenster geöffnet, in dem das Benutzerprofil auf einer Registerkarte und die Vorgangs- und Entitätsübersicht auf einer anderen Registerkarte angezeigt werden.



Die standardmäßige *Group by*-Methode ist *Activity Forensics*. Wenn Sie eine andere *Group by*-Methode auswählen, z. B. Entity Type—die Entity_Group by_-Tabelle wird angezeigt. Wird keine Auswahl getroffen, wird *Group by* **all** angezeigt.

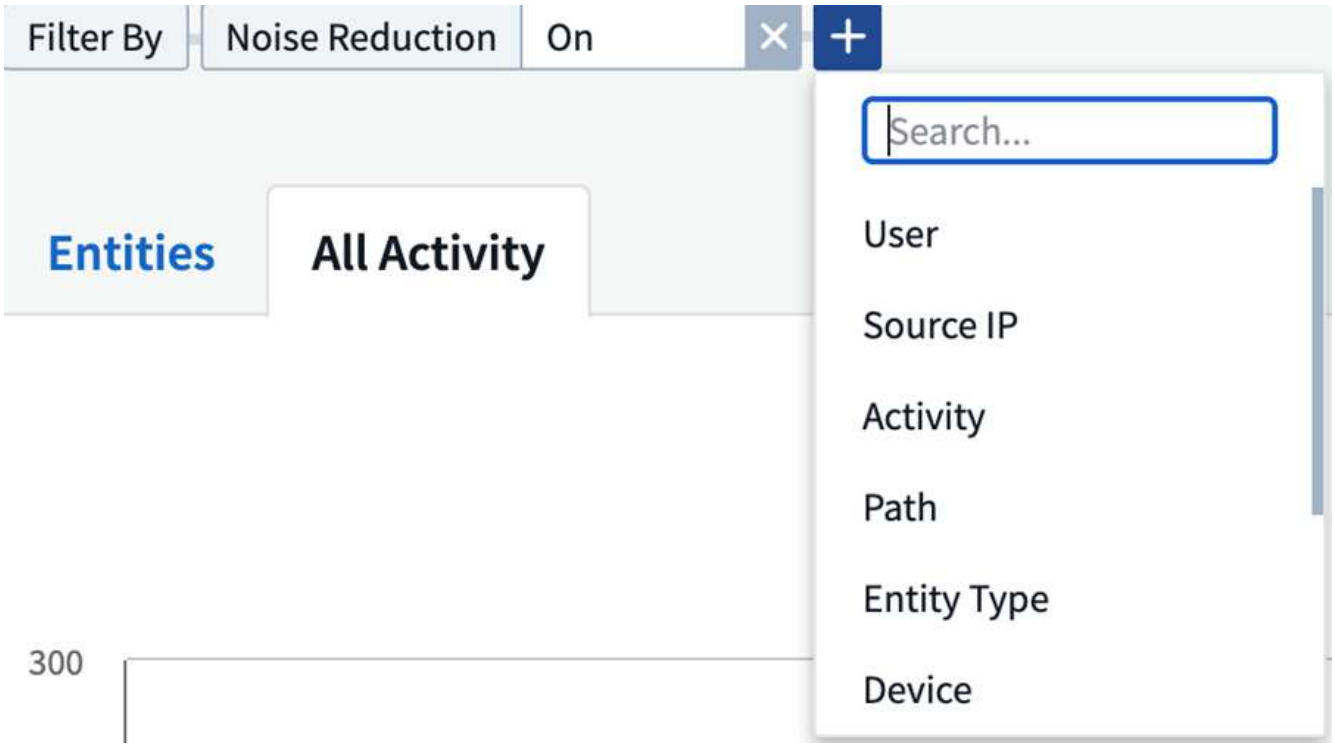
- Die Vorgangsanzahl wird als Hyperlink angezeigt. Wenn Sie diese Option auswählen, wird die ausgewählte Gruppierung als Filter hinzugefügt. Die Tabelle der Aktivität wird basierend auf diesem Filter aktualisiert.
- Wenn Sie den Filter ändern, den Zeitraum ändern oder den Bildschirm aktualisieren, können Sie nicht zu den gefilterten Ergebnissen zurückkehren, ohne den Filter erneut einzustellen.

Filtern Forensischer Vorgangshistorie-Daten

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

- Der Filter kann über das Schiebefeld hinzugefügt werden. Der Wert wird den entsprechenden Filtern in der oberen Liste *Filter by* hinzugefügt.
- 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.
- **Domain** des Benutzers, der die Aktivität ausführt. Sie müssen die **genaue Domain** angeben, um zu filtern. Die Suche nach einer partiellen Domäne oder einer partiellen Domäne mit Präfix oder Suffix mit Platzhalter ('*') funktioniert nicht. *None* kann angegeben werden, um nach fehlender Domain zu suchen.

Die folgenden Felder unterliegen speziellen Filterregeln:

- **Entity Type**, mit Entity (File) Extension - es ist vorzuziehen, den genauen Entity-Typ in Anführungszeichen anzugeben. Beispiel: _ „Txt“_.
- **Pfad** der Entity - Verzeichnispfad-Filter (Pfadstring endet mit /) für schnellere Ergebnisse werden bis zu 4 Verzeichnisse empfohlen. Beispiel: *“/Home/userX/nested1/nested2/“*. Weitere Informationen finden Sie in der folgenden Tabelle.
- 1st Level Folder (Root) - Stammverzeichnis des Entity Path als Filter. Wenn beispielsweise der Entity-Pfad /Home/userX/nested1/nested2/ lautet, kann Home ODER "Home" verwendet werden.
- 2nd Level Folder - Verzeichnis 2nd Level der Entity Path Filter. Wenn beispielsweise der Entity-Pfad /Home/userX/nested1/nested2/ lautet, kann userX ODER "userX" verwendet werden.
- Ordner der dritten Ebene – Verzeichnis der Pfadfilter der dritten Ebene.
- Wenn beispielsweise der Entity-Pfad /Home/userX/nested1/nested2/ lautet, kann nested1 ODER „nested1“ verwendet werden.
- Ordner der 4. Ebene – Verzeichnis der Filter für Entity Path auf vierter Ebene. Wenn beispielsweise der Entity-Pfad /Home/userX/nested1/nested2/ lautet, kann nested2 ODER „nested2“ verwendet werden.
- **User** die Aktivität durchführen - es ist vorzuziehen, den genauen Benutzer in Anführungszeichen anzugeben. Beispiel: _ „Administrator“_.
- **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.

Beispiele Für Forensik-Filter Für Aktivitäten:

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Performance-Assessment	Kommentar
Pfad = „/Home/userX/nested1/nested2/“	Rekursive Abfrage aller Dateien und Ordner unter dem angegebenen Verzeichnis	Schnell	Verzeichnissuchen bis zu 4 Verzeichnisse werden schnell sein.

Vom Benutzer angewendeter Filterausdruck	Erwartetes Ergebnis	Performance-Assessment	Kommentar
Pfad = „/Home/userX/nested1/“	Rekursive Abfrage aller Dateien und Ordner unter dem angegebenen Verzeichnis	Schnell	Verzeichnissuchen bis zu 4 Verzeichnisse werden schnell sein.
Pfad = „/Home/userX/nested1/Test“	Rekursive Abfrage aller Dateien und Ordner unter dem angegebenen Pfad regex(Test* könnte Datei ODER Verzeichnis ODER beides bedeuten)	Langsamer	Die Suche nach Verzeichnis+Datei ist langsamer als bei Verzeichnissuchen.
Pfad = „/Home/userX/nested1/nested2/nested3/“	Rekursive Abfrage aller Dateien und Ordner unter dem angegebenen Verzeichnis	Langsamer	Mehr als 4 Verzeichnissuchen sind langsamer zu suchen.
Alle anderen nicht pfadbasierten Filter. Benutzer- und Entitätstyp-Filter, die in Anführungszeichen empfohlen werden, z. B. Benutzer=„Administrator“ Entitätstyp=„txt“		Schnell	

HINWEIS:

1. Die Anzahl der Aktivitäten, die neben dem Symbol „Alle Aktivitäten“ angezeigt wird, wird auf 30 Minuten gerundet, wenn der ausgewählte Zeitraum mehr als 3 Tage umfasst. In einem Zeitraum von _1. September 10:15 bis 7. September 10:15 werden die Aktivitätszahlen vom 1. September 10:00 bis 7. September 10:30 Uhr angezeigt.
2. Ebenso werden die im Diagramm „Aktivitätsverlauf“ angezeigten Zählwerte auf 30 Minuten abgerundet, wenn der ausgewählte Zeitraum mehr als 3 Tage umfasst.

Forensische Vorgangshistorie-Daten Sortieren

Sie können Daten aus dem Aktivitätsverlauf nach *Zeit, Benutzer, Quell-IP, Aktivität,*, *Entity Type*, 1st Level Folder (Root), 2nd Level Folder, 3rd Level Folder und 4th Level Folder 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.

Benutzerhandbuch für asynchrone Exporte

Überblick

Die Funktion „asynchrone Exporte“ in „Storage Workload Security“ wurde für die Verarbeitung großer Datenexporte entwickelt.

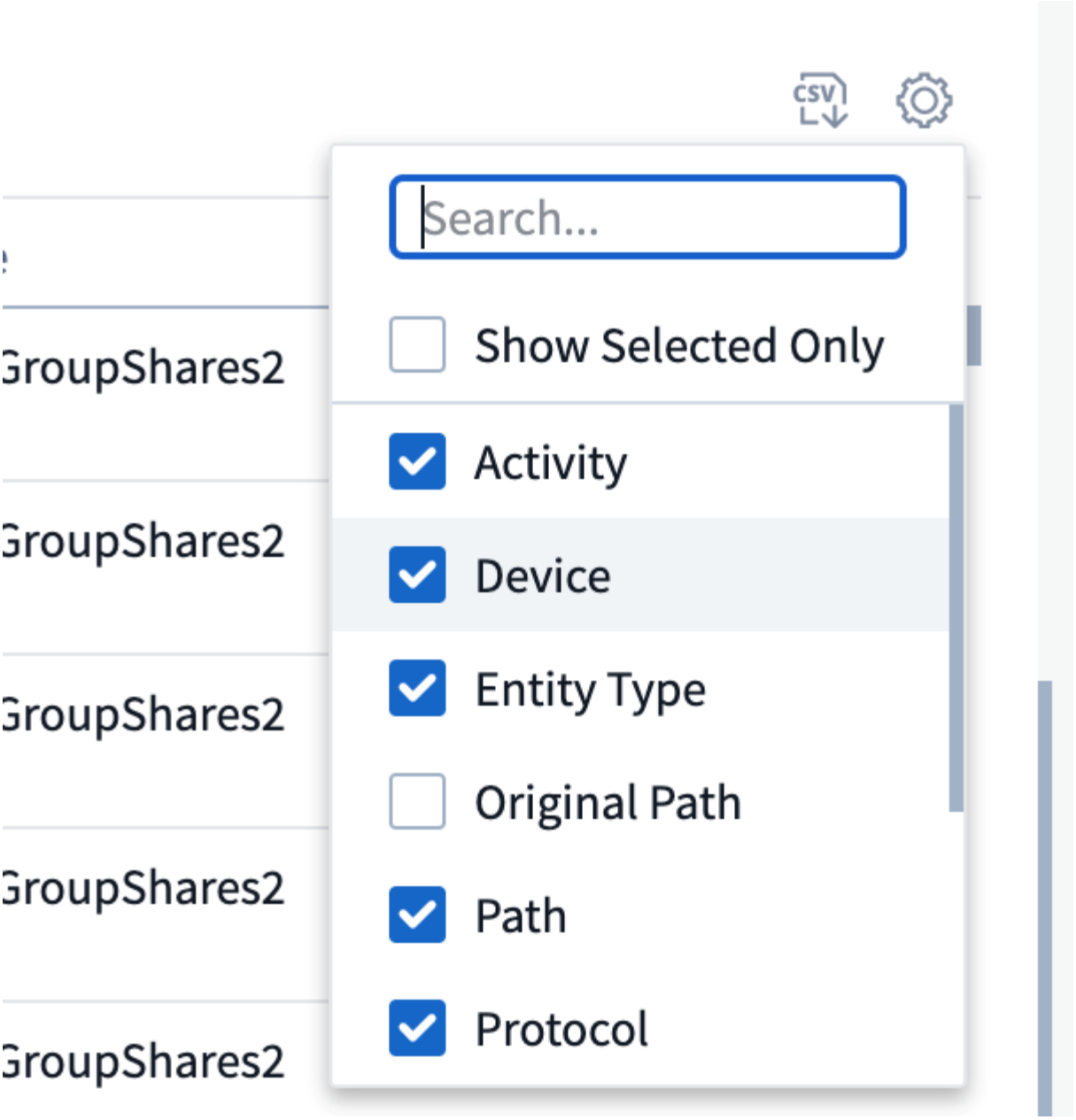
Schritt-für-Schritt-Anleitung: Daten mit asynchronen Exporten exportieren

1. **Export starten**: Wählen Sie die gewünschte Zeitdauer und Filter für den Export aus und klicken Sie auf den Export-Button.
2. **Wait for Export to complete**: Die Verarbeitungszeit kann von ein paar Minuten bis zu einigen Stunden betragen. Unter Umständen müssen Sie die Seite „Forensik“ einige Male aktualisieren. Sobald der Exportauftrag abgeschlossen ist, wird die Schaltfläche "Letzten Export CSV-Datei herunterladen" aktiviert.
3. **Download**: Klicken Sie auf den Button "Download Last created Export file", um die exportierten Daten im .zip-Format zu erhalten. Diese Daten können heruntergeladen werden, bis der Benutzer einen anderen asynchronen Export initiiert oder 3 Tage vergangen sind, je nachdem, was zuerst eintritt. Die Schaltfläche bleibt aktiviert, bis ein anderer asynchroner Export gestartet wird.
4. **Einschränkungen**:
    - Die Anzahl asynchroner Downloads ist derzeit auf 1 pro Benutzer und 3 pro Mandant begrenzt.
    - Die exportierten Daten sind auf maximal 1 Million Datensätze begrenzt.

Ein Beispielskript zum Extrahieren forensischer Daten über API ist auf dem Agenten unter */opt/NetApp/CloudSecure/Agent/Export-script/* vorhanden. Weitere Informationen zum Skript finden Sie in der Infodatei an dieser Stelle.

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	Gilt für diese Filter	Gilt nicht für diese Filter	Ergebnis
* (Sternchen)	Ermöglicht Ihnen die Suche nach allem	Auto*03172022 Wenn der Suchtext Bindestrich oder Unterstrich enthält, geben Sie den Ausdruck in Klammern an, z. B. (svm*) für die Suche nach svm-123	Benutzer, Einheitstyp, Gerät, Volume, ursprünglicher Pfad, Ordner 1 Stufe, Ordner 2 Ebenen, Ordner 3 Ebenen, Ordner 4 Ebenen		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, Entitätstyp, Gerät, Volume, 1stLevel-Ordner, 2ndLevel-Ordner, 3rdLevel-Ordner, 4thLevel-Ordner		Gibt AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022B, AutoSabotageUser1_031720225 usw. zurück
ODER	Ermöglicht Ihnen die Angabe mehrerer Elemente	AutoSabotageUser1_03172022 ODER AutoBefreiUser4_03162022	Benutzer, Domäne, Einheitstyp, Ursprünglicher Pfad		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, Entitätstyp, ursprünglicher Pfad, Ordner mit 1 Stufe, Ordner mit 2 Ebenen, Ordner mit 3 Ebenen, Ordner mit 4 Ebenen	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/AutoFile03242022“	Nur die exakte Suche funktioniert; gibt alle Aktivitäten mit exaktem Pfad wie /AutoDir1/AutoFile03242022 zurück (Fall unsensibel)
„/AutoDir1/“	Funktioniert; gibt alle Aktivitäten mit Verzeichnis 1. Ebene zurück, die mit AutoDir1 übereinstimmen (unsensibel)
„/AutoDir1/AutoFile03242022/“	Funktioniert; gibt alle Aktivitäten mit Verzeichnis 1. Ebene mit AutoDir1 und Verzeichnis 2. Ebene mit AutoFile03242022 zurück (Fall nicht sensibel)
/AutoDir1/AutoFile03242022 ODER /AutoDir1/AutoFile03242022	Funktioniert nicht
NICHT /AutoDir1/AutoFile03242022	Funktioniert nicht
NICHT /AutoDir1	Funktioniert nicht
NICHT /AutoFile03242022	Funktioniert nicht
*	Funktioniert nicht

Lokale Root-SVM-Benutzeraktivitäten ändern sich

Wenn ein lokaler Root-SVM-Benutzer eine Aktivität ausführt, wird die IP des Clients, auf dem die NFS-Freigabe gemountet ist, jetzt im Benutzernamen berücksichtigt, der sowohl auf forensischen Aktivitäten als auch auf Benutzeraktivitäts-Seiten als Root@<ip-address-of-the-client> angezeigt wird.

Beispiel:

- Wenn SVM-1 von Workload Security überwacht wird und der Root-Benutzer dieser SVM die Freigabe auf einem Client mit der IP-Adresse 10.197.12.40 mountet, lautet der auf der Seite für forensische Aktivitäten angezeigte Benutzername *root@10.197.12.40*.
- Wenn dieselbe SVM-1 in einen anderen Client mit der IP-Adresse 10.197.12.41 eingebunden wird, lautet der auf der Seite für forensische Aktivitäten angezeigte Benutzername *root@10.197.12.41*.

*• Dies wird getan, um NFS-Root-Benutzeraktivität durch IP-Adresse zu trennen. Zuvor wurde die gesamte Aktivität als vom *root*-Benutzer durchgeführt betrachtet, ohne IP-Unterscheidung.

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 User Directory Collector wurde konfiguriert, jedoch wurde er angehalten oder befindet sich im Fehlerzustand. Bitte gehen Sie zu **Collectors > User Directory Collectors** und überprüfen Sie den Status. Tipps zur Fehlerbehebung finden Sie im "Fehlerbehebung für Benutzerverzeichnissammler" Abschnitt der Dokumentation. 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-Zugriff ausführt, sollte auf der Benutzerseite von UI 3 aus gesehen werden. 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 Verzeichnissuche, um alle Aktivitäten unterhalb eines bestimmten Ordners rekursiv zu sehen (hierarchische Suche). Beispiel: „/path1/path2/path3/“ listet alle Vorgänge rekursiv unter /path1/path2/path3 auf. Alternativ können Sie die Option „zum Filter hinzufügen“ unter 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.

Die forensische Benutzeroberfläche lädt Daten langsam, wenn der *PATH*-Filter verwendet wird.	Verzeichnispfad-Filter (Pfadstring endet mit /) für schnellere Ergebnisse werden bis zu 4 Verzeichnisse empfohlen. Z.B. wenn der Verzeichnispfad /AAA/BBB/CCC/DDD ist, versuchen Sie nach „/AAA/BBB/CCC/DDD/“ zu suchen, um Daten schneller zu laden.

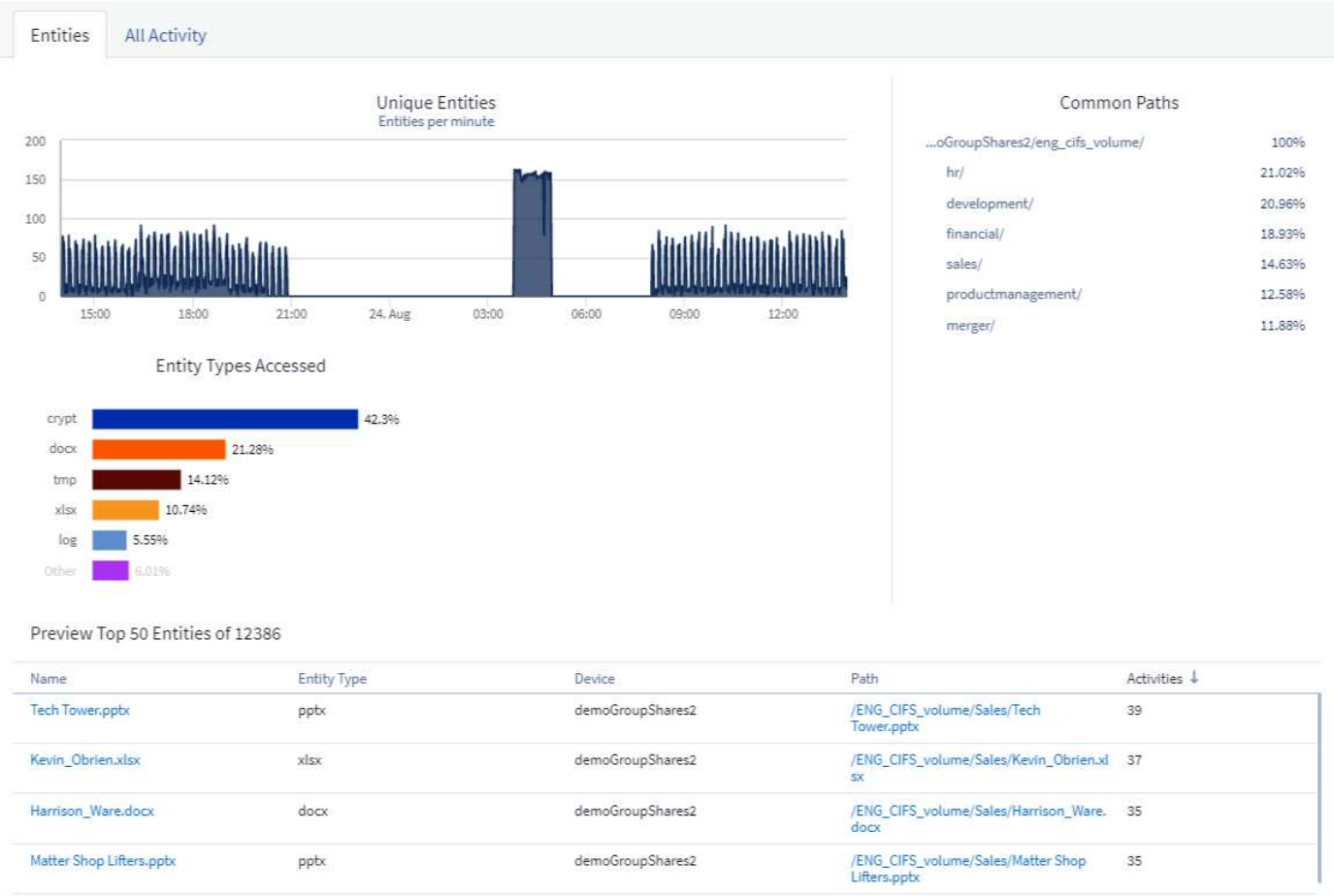
Seite Mit Forensischen Einheiten

Auf der Seite Forensics Entities finden Sie detaillierte Informationen über die Entitätstätigkeit auf Ihrem Mandanten.

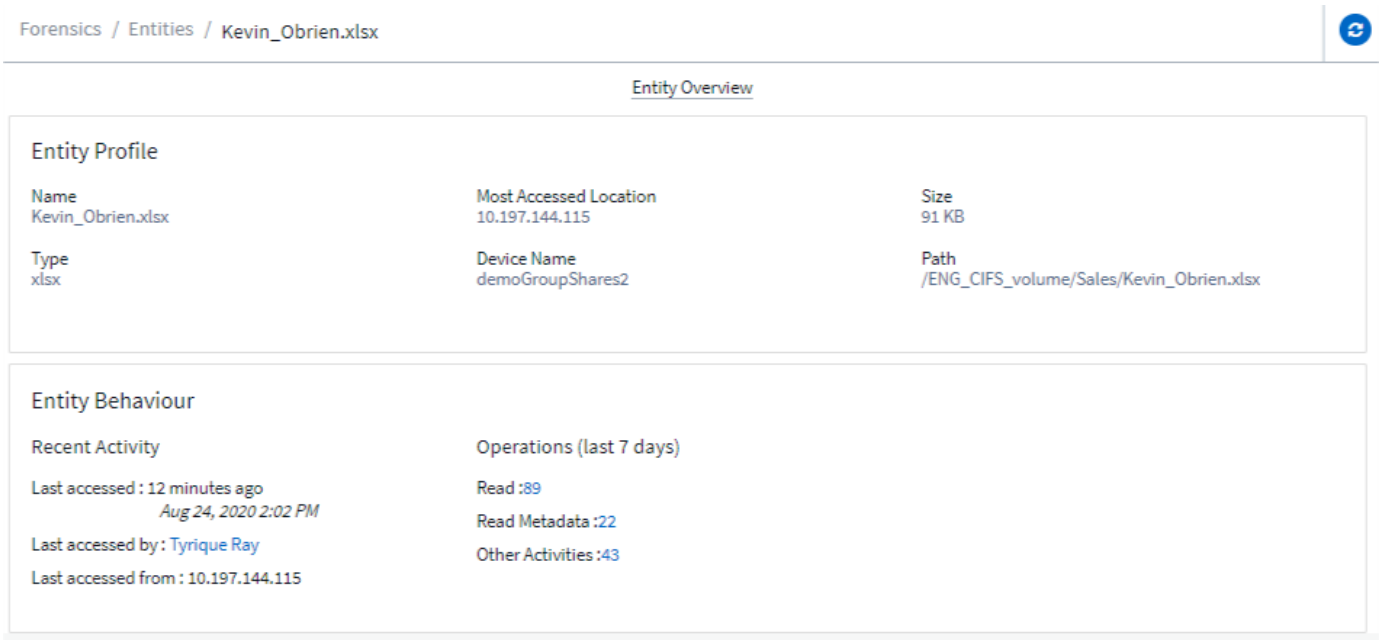
Untersuchung Von Informationen Zur Einheit

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

Diese Seite bietet einen Überblick über die Entity-Aktivitäten auf Ihrem Mandanten, wobei folgende Informationen hervorgehoben werden: * Ein Diagramm mit *Unique Entities* Zugriffe pro Minute * Ein Diagramm mit *Entity-Typen zugegriffen* * Eine Aufschlüsselung der *Common Paths* * Eine Liste der *Top 50 Entities* aus der Gesamtzahl der Entities



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.