Analisi

Cloud Insights

NetApp
September 13, 2024

Sommario

Analisi

Forensics - tutte le attività

La pagina All Activity (tutte le attività) consente di comprendere le azioni eseguite sulle entità nell'ambiente workload Security.

Esame di tutti i dati delle attività

Fare clic su **Forensics > Activity Forensics** (analisi > analisi delle attività) e fare clic sulla scheda **All Activity** (tutte le attività) per accedere alla pagina All Activity (tutte le attività). Questa pagina fornisce una panoramica delle attività nel proprio ambiente, evidenziando le seguenti informazioni:

- Un grafico che mostra *Cronologia attività* (accessibile al minuto/ogni 5 minuti/ogni 10 minuti in base all'intervallo di tempo globale selezionato)

  È possibile ingrandire il grafico trascinando un rettangolo nel grafico. L'intera pagina viene caricata per visualizzare l'intervallo di tempo di zoom. Quando si esegue lo zoom avanti, viene visualizzato un pulsante che consente all'utente di eseguire lo zoom indietro.

- Un grafico di *tipi di attività*. Per ottenere i dati della cronologia delle attività in base al tipo di attività, fare clic sul link corrispondente all'etichetta dell'asse X.
- Un grafico delle attività su *tipi di entità*. Per ottenere i dati della cronologia delle attività in base al tipo di entità, fare clic sul link corrispondente all'etichetta dell'asse X.
- Un elenco dei dati di *tutte le attività*

La tabella **tutte le attività** mostra le seguenti informazioni. Nota: Non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare facendo clic sull'icona "ingranaggio" .

- L'ora * in cui è stato effettuato l'accesso a un'entità, inclusi l'anno, il mese, il giorno e l'ora dell'ultimo accesso.
- Il **utente** che ha effettuato l'accesso all'entità con un collegamento a "Informazioni sull'utente".
- L'attività * eseguita dall'utente. I tipi supportati sono:
  - **Cambia proprietà del gruppo** - la proprietà del gruppo è del file o della cartella è stata modificata. Per ulteriori informazioni sulla proprietà del gruppo, consulta "questo link."
  - **Cambia proprietario** - la proprietà del file o della cartella viene modificata in un altro utente.
  - **Cambia permesso** - l'autorizzazione per file o cartelle viene modificata.
  - **Crea** - Crea file o cartella.
  - **Delete** - Elimina file o cartella. Se una cartella viene eliminata, si ottengono gli eventi *delete* per tutti i file in quella cartella e sottocartelle.
  - **Read** - il file viene letto.
  - **Read Metadata** - solo se si attiva l'opzione di monitoraggio delle cartelle. Verrà generato all'apertura di una cartella su Windows o all'esecuzione di "ls" all'interno di una cartella in Linux.
  - **Rinomina** - Rinomina il file o la cartella.

- **Write** - i dati vengono scritti in un file.
- **Write Metadata** - i metadati del file vengono scritti, ad esempio, i permessi modificati.
- **Altra modifica** - qualsiasi altro evento non descritto in precedenza. Tutti gli eventi non mappati vengono mappati al tipo di attività "Altro cambiamento". Applicabile a file e cartelle.

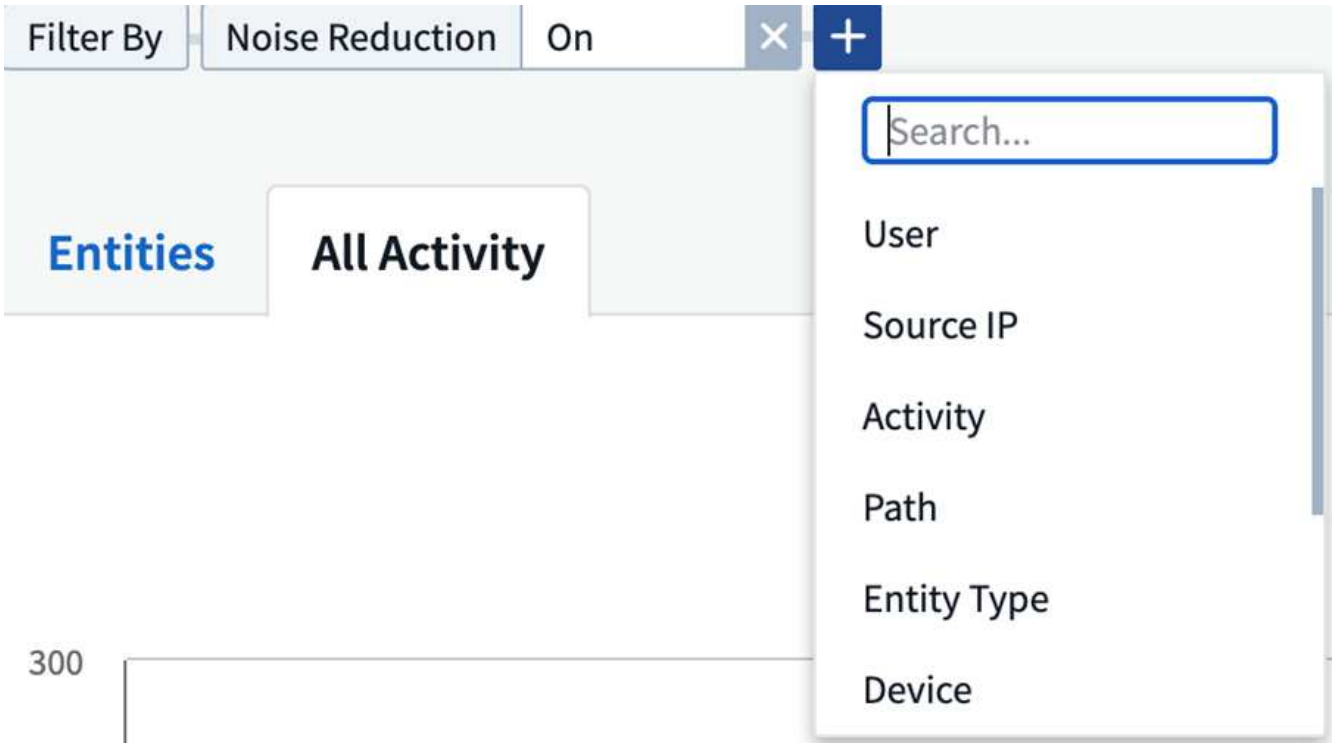
- Il percorso * all'entità con un collegamento a. "Dati di dettaglio dell'entità"
- Il **Entity Type**, inclusa l'estensione dell'entità (ad es. File) (.doc, .docx, .tmp, ecc.)
- Il **dispositivo** in cui risiedono le entità
- Il **protocollo** utilizzato per recuperare gli eventi.
- Il percorso **originale** utilizzato per rinominare gli eventi quando il file originale è stato rinominato. Questa colonna non è visibile nella tabella per impostazione predefinita. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- Il **Volume** in cui risiedono le entità. Questa colonna non è visibile nella tabella per impostazione predefinita. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.

Filtraggio dei dati Forensic Activity History

Per filtrare i dati è possibile utilizzare due metodi.

1. Passare il mouse sul campo nella tabella e fare clic sull'icona del filtro visualizzata. Il valore viene aggiunto ai filtri appropriati nell'elenco *Filter by* principale.
2. Filtrare i dati digitando il campo *Filtra per*:

   Selezionare il filtro appropriato dal widget 'Filtra per' in alto facendo clic sul pulsante **[+]**:



   Inserire il testo di ricerca

   Premere Invio o fare clic all'esterno della casella del filtro per applicare il filtro.

È possibile filtrare i dati delle attività forensi in base ai seguenti campi:

- Il tipo **Activity**.
- **IP di origine** da cui è stato effettuato l'accesso all'entità. È necessario fornire un indirizzo IP di origine valido tra virgolette doppie, ad esempio "10.1.1.1". Gli IP incompleti come "10.1.1.**", "10.1.**.*", ecc. non funzionano.
- **Protocollo** per recuperare le attività specifiche del protocollo.
- **Nome utente** dell'utente che esegue l'attività. Specificare il nome utente esatto da filtrare. La ricerca con il nome utente parziale o con il prefisso '*' non funziona.
- **Riduzione del rumore** per filtrare i file creati nelle ultime 2 ore dall'utente. Viene inoltre utilizzato per filtrare i file temporanei (ad esempio, i file .tmp) a cui l'utente accede.

I seguenti campi sono soggetti a speciali regole di filtraggio:

- **Entity Type**, usando l'estensione dell'entità (file)
- **Percorso** dell'entità
- **Utente** che esegue l'attività
- **Dispositivo** (SVM) in cui risiedono le entità
- **Volume** dove risiedono le entità
- Il percorso **originale** utilizzato per rinominare gli eventi quando il file originale è stato rinominato.

I campi precedenti sono soggetti a quanto segue durante il filtraggio:

- Il valore esatto deve essere compreso tra virgolette: Esempio: "Searchtext"
- Le stringhe con caratteri jolly non devono contenere virgolette: Esempio: Searchtext, 's*searchtext*, filtrerà le stringhe contenenti il carattere 'earchtext'.
- Stringa con un prefisso, ad esempio: Searchtext* , cerca le stringhe che iniziano con 'searchtext'.

Ordinamento dei dati Forensic Activity History

È possibile ordinare i dati della cronologia delle attività in base a *Time, User, Source IP, Activity, Path* e *Entity Type*. Per impostazione predefinita, la tabella viene ordinata in base a un ordine *time* decrescente, il che significa che i dati più recenti verranno visualizzati per primi. L'ordinamento è disattivato per i campi *Device* e *Protocol*.

Esportazione di tutte le attività

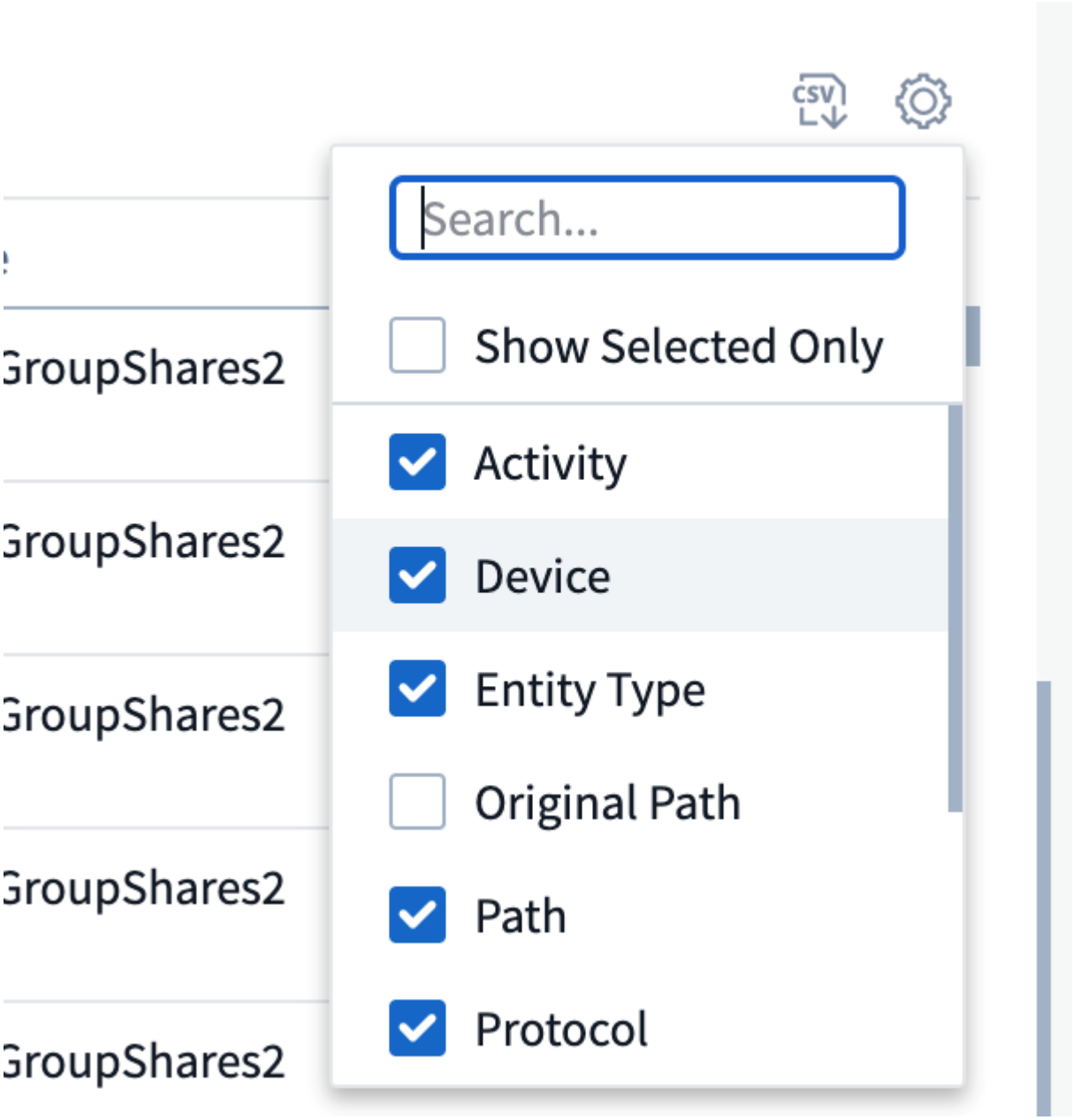
È possibile esportare la cronologia delle attività in un file .CSV facendo clic sul pulsante *Export* sopra la tabella Activity History (Cronologia attività). Si noti che vengono esportati solo i primi 100,000 record. A seconda della quantità di dati, l'esportazione potrebbe richiedere da pochi secondi a diversi minuti.

Un esempio di script per estrarre i dati forensi tramite le API è presente all'indirizzo */opt/netapp/cloudSecure/Agent/export-script/*. Per ulteriori informazioni sullo script, vedere il file Leggimi in questa posizione.

Selezione colonna per tutte le attività

La tabella *All activity* mostra le colonne Select per impostazione predefinita. Per aggiungere, rimuovere o modificare le colonne, fare clic sull'icona a forma di ingranaggio a destra della tabella e selezionare dall'elenco

delle colonne disponibili.



Conservazione della cronologia delle attività

La cronologia delle attività viene mantenuta per 13 mesi per gli ambienti di sicurezza dei workload attivi.

Applicabilità dei filtri nella pagina Forensics

Filtro	Che cosa fa	Esempio	Quali filtri sono applicabili?	Non applicabile per i filtri	Risultato

* (Asterisco)	consente di cercare tutto	Auto*03172022	Utente, PERCORSO, tipo di entità, tipo di dispositivo, volume, Percorso originale		Restituisce tutte le risorse che iniziano con "Auto" e terminano con "03172022"
? (punto interrogativo)	consente di cercare un numero specifico di caratteri	AutoSabotageUser1_03172022?	Utente, tipo di entità, dispositivo, volume		Restituisce AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022AB, AutoSabotageUser1_031720225 e così via
OPPURE	consente di specificare più entità	AutoSabotageUser1_03172022 O AutoRansomUser4_03162022	Utente, dominio, Nome utente, PERCORSO, tipo di entità, Periferica, percorso originale		Restituisce uno qualsiasi di AutoSabotageUser1_03172022 O AutoRansomUser4_03162022
NO	consente di escludere il testo dai risultati della ricerca	NON AutoRansomUser4_03162022	Utente, dominio, Nome utente, PERCORSO, tipo di entità, PERCORSO originale, Volume	Dispositivo	Restituisce tutto ciò che non inizia con "AutoRansomUser4_03162022"
Nessuno	Ricerca i valori NULL in tutti i campi	Nessuno	Dominio		restituisce risultati in cui il campo di destinazione è vuoto

Ricerca percorso / percorso originale

I risultati della ricerca con e senza / saranno diversi

/AutoDir1/AutoFile	Funziona
AutoDir1/Autofile	Non funziona
/AutoDir1/AutoFile (Dir1)	Dir1 la sottostringa parziale non funziona
"/AutoDir1/AutoFile03242022"	La ricerca esatta funziona
Auto*03242022	Non funziona
AutoSabotageUser1_03172022?	Non funziona
/AutoDir1/AutoFile03242022 O /AutoDir1/AutoFile03242022	Funziona

NON /AutoDir1/AutoFile03242022	Funziona
NON /AutoDir1	Funziona
NON /AutoFile03242022	Non funziona
*	Mostra tutte le voci

Risoluzione dei problemi

Problema	Provare
Nella tabella "tutte le attività", sotto la colonna ‘utente’, il nome utente viene visualizzato come: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” o "ldap:default:80038003"	Possibili motivi: 1. Non è stato ancora configurato alcun servizio di raccolta elenchi in linea utenti. Per aggiungerne uno, andare a **sicurezza workload > Collector > User Directory Collector** e fare clic su **+User Directory Collector**. Scegliere *Active Directory* o *LDAP Directory Server*. 2. È stato configurato un User Directory Collector, ma si è arrestato o si trova in stato di errore. Andare a **Collector > User Directory Collectors** e controllare lo stato. Fare riferimento a. "Risoluzione dei problemi di User Directory Collector" sezione della documentazione per suggerimenti per la risoluzione dei problemi. Una volta eseguita la configurazione corretta, il nome verrà risolto automaticamente entro 24 ore. Se il problema persiste, verificare di aver aggiunto il Data Collector utente corretto. Assicurarsi che l’utente faccia effettivamente parte del server Active Directory/LDAP Directory aggiunto.
Alcuni eventi NFS non vengono visualizzati nell’interfaccia utente.	Controllare quanto segue: 1. È necessario eseguire un User Directory Collector per server ad con attributi POSIX impostati con l’attributo unixid attivato dall’interfaccia utente. 2. Qualsiasi utente che esegue l’accesso NFS deve essere visualizzato quando effettua una ricerca nella pagina utente dall’interfaccia utente 3. Gli eventi raw (eventi per i quali l’utente non è ancora stato scoperto) non sono supportati per NFS 4. L’accesso anonimo all’esportazione NFS non verrà monitorato. 5. Assicurarsi che la versione di NFS utilizzata sia inferiore a NFS4.1.

Dopo aver digitato alcune lettere contenenti un carattere jolly come l'asterisco (*) nei filtri delle pagine Forensics *All Activity* o *Entities*, le pagine vengono caricate molto lentamente.	Un asterisco (**) nella stringa di ricerca cerca tutto. Tuttavia, le stringhe con caratteri jolly come <searchTerm>** o *<searchTerm>* causano una query lenta. Per ottenere prestazioni migliori, utilizzare le stringhe di prefisso nel formato *<searchTerm>** (in altre parole, aggiungere l'asterisco (*) *dopo* un termine di ricerca). Esempio: Utilizzare la stringa *testvolume**, invece di **testvolume* o **test*volume*. Utilizza una ricerca basata su prefisso per visualizzare tutte le attività sotto una data cartella in modo ricorrente (ricerca gerarchica). ad esempio */path1/path2/path3* o *"/path1/path2/path3"* elenchiamo tutte le attività in modo ricorrente sotto */path1/path2/path3*. In alternativa, utilizzare l'opzione "Add to Filter" (Aggiungi al filtro) nella scheda All Activity (tutte le attività).
Si verifica un errore di richiesta non riuscita con codice di stato 500/503 quando si utilizza un filtro percorso.	Provare a utilizzare un intervallo di date più piccolo per filtrare i record.
L'interfaccia utente forense sta caricando i dati lentamente quando si utilizza il filtro *path*.	Se il percorso è */AAA/BBB/CCC/DDD*, invece di cercare: AAA/BBB/CCC* OPPURE AAA/BBB/C* Prova a cercare: AAA/BBB/CCC/* Questa ricerca dovrebbe consentire ai dati di caricarsi più velocemente.

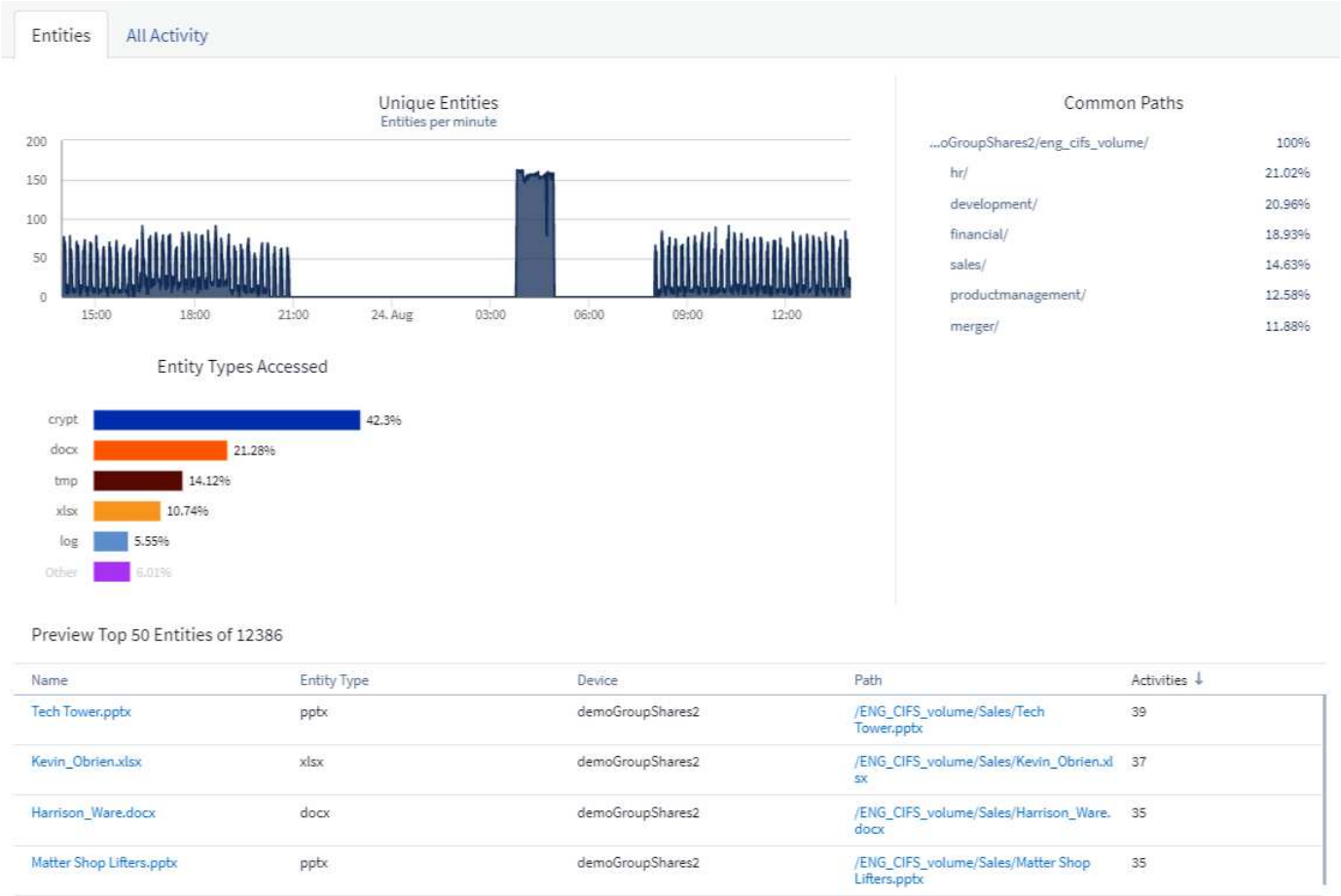
Pagina delle entità forensi

La pagina delle entità Forensics fornisce informazioni dettagliate sull'attività delle entità nell'ambiente.

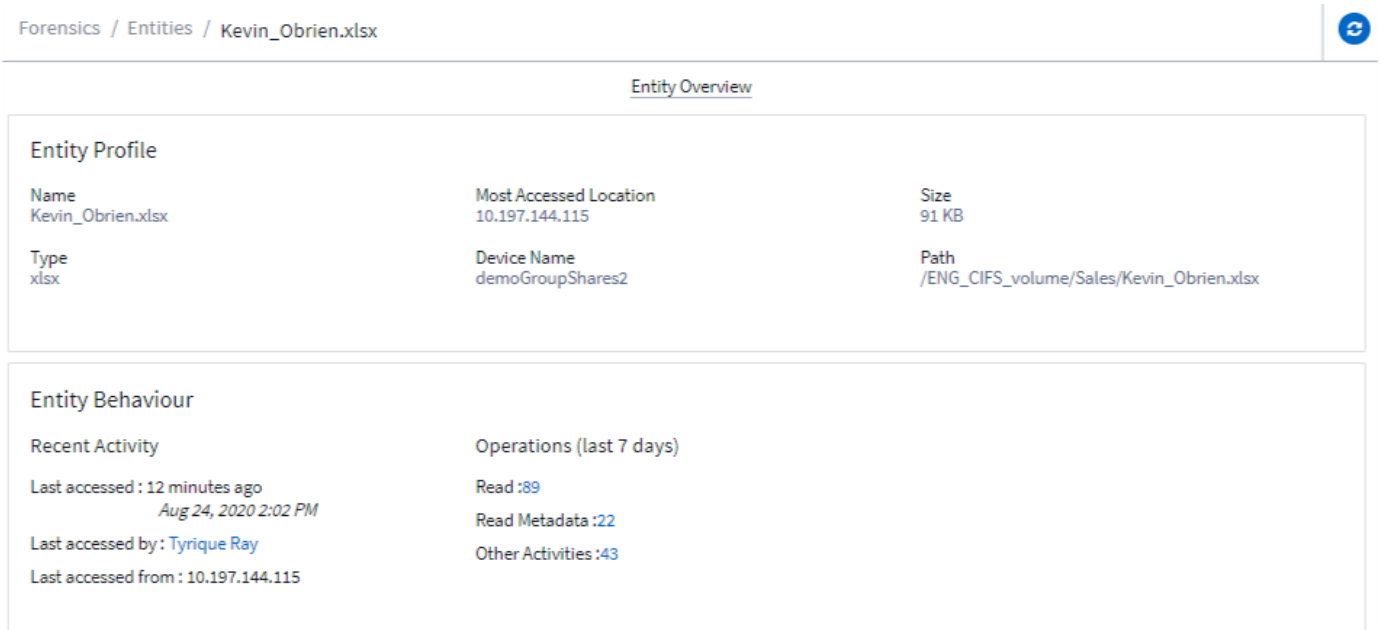
Esame delle informazioni sull'entità

Fare clic su **Forensics > Activity Forensics** e fare clic sulla scheda *Entities* per accedere alla pagina Entities.

Questa pagina fornisce una panoramica dell'attività dell'entità nel proprio ambiente, evidenziando le seguenti informazioni: * Un grafico che mostra *entità univoche* cui si accede al minuto * Un grafico di *tipi di entità a cui si accede* * una suddivisione dei *percorsi comuni* * Un elenco delle *prime 50 entità* rispetto al numero totale di entità



Facendo clic su un'entità nell'elenco, viene visualizzata una pagina panoramica dell'entità, che mostra un profilo dell'entità con dettagli come nome, tipo, nome del dispositivo, indirizzo IP e percorso più utilizzati, oltre al comportamento dell'entità come l'utente, l'IP, e ora dell'ultimo accesso all'entità.



Panoramica dell’utente legale

Le informazioni per ciascun utente sono fornite nella Panoramica utente. Utilizzare queste viste per comprendere le caratteristiche dell’utente, le entità associate e le attività recenti.

Profilo utente

Le informazioni del profilo utente includono le informazioni di contatto e la posizione dell’utente. Il profilo fornisce le seguenti informazioni:

- Nome dell’utente
- Indirizzo e-mail dell’utente
- Manager dell’utente
- Contatto telefonico per l’utente
- Posizione dell’utente

Comportamento dell’utente

Le informazioni sul comportamento dell’utente identificano le attività e le operazioni recenti eseguite dall’utente. Queste informazioni includono:

- Attività recente
  - Ultima posizione di accesso
  - Grafico delle attività
  - Avvisi
- Operazioni per gli ultimi sette giorni
  - Numero di operazioni

Intervallo di refresh

L’elenco utenti viene aggiornato ogni 12 ore.

Policy di conservazione

Se non viene aggiornato nuovamente, l’elenco utenti viene conservato per 13 mesi. Dopo 13 mesi, i dati verranno cancellati. Se l’ambiente workload Security viene cancellato, tutti i dati associati all’ambiente vengono cancellati.