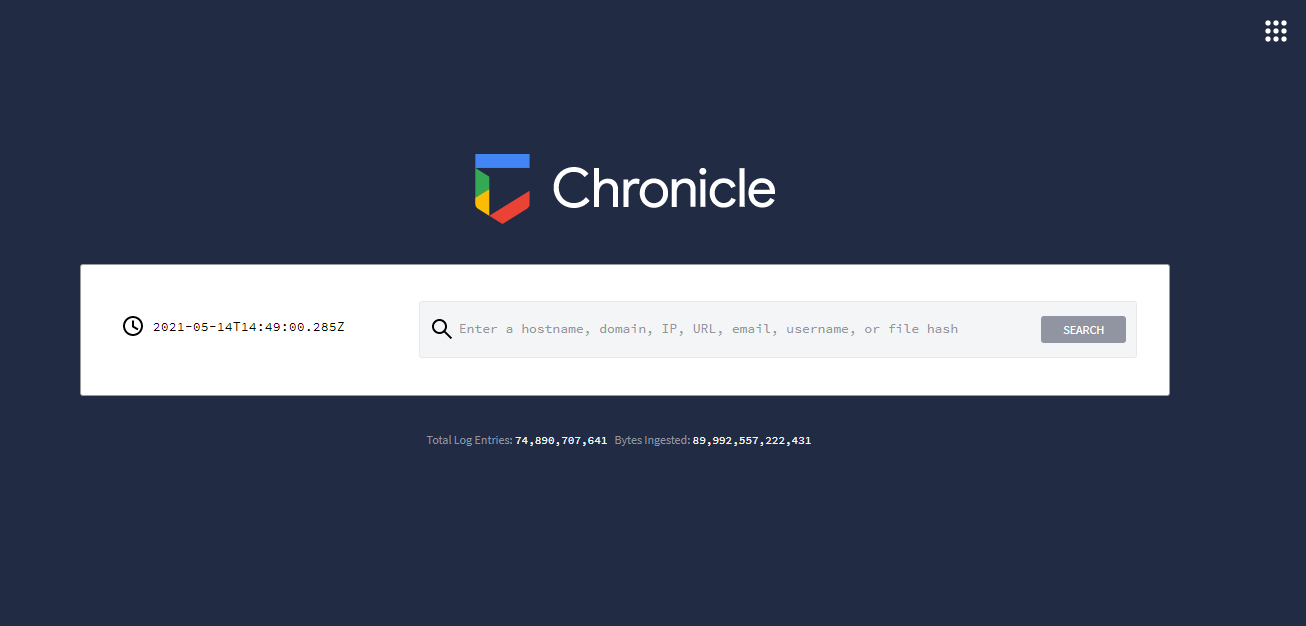
**CHRONICLE**

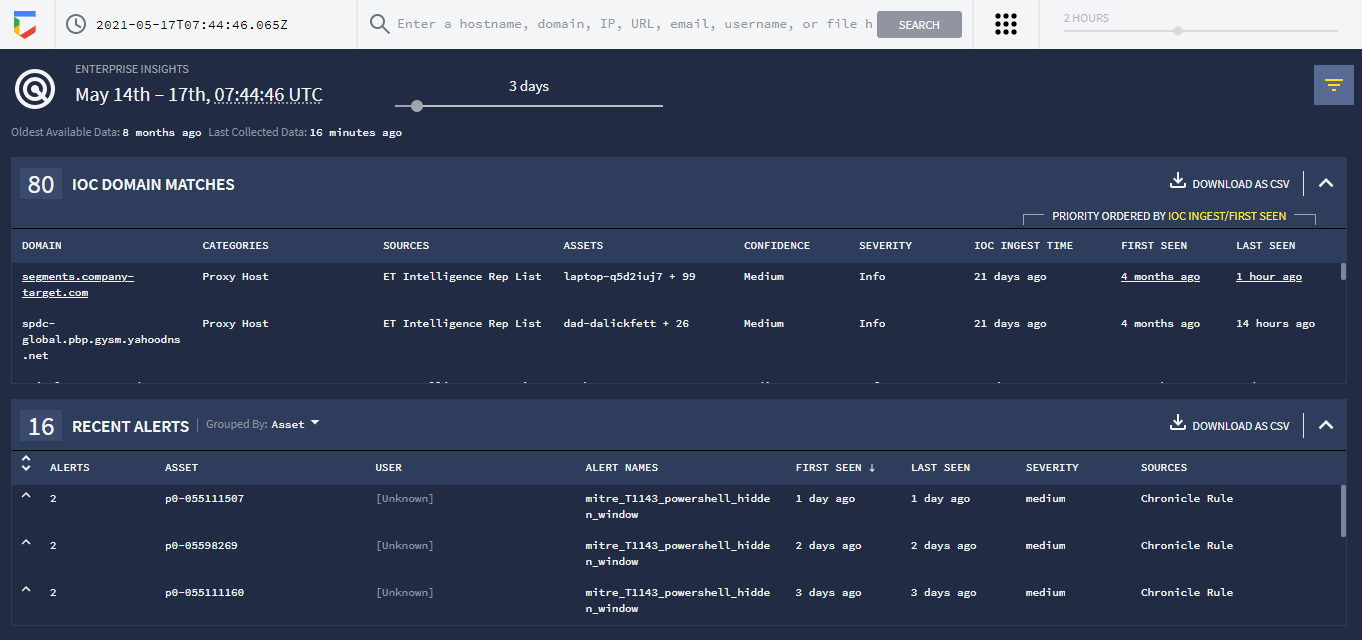
Per poter accedere a Chronicle, inserire le proprie credenziali e visitare l’url **https://<customername>.backstory.chronicle.security**

**IMPORTANTE:** Gli orari visibili su Chronicle sono in UTC. Calcolare quindi la corrispondente ora italiana.

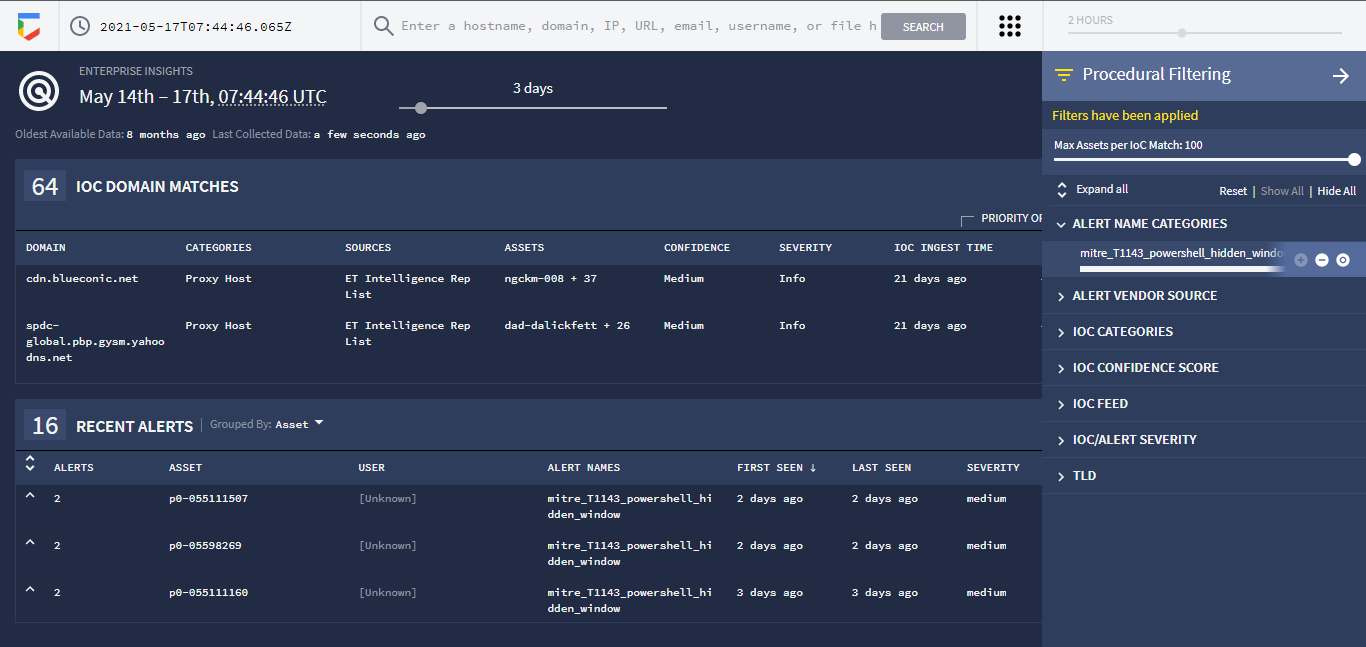


**1)** **Enterprise Insights**

Nell’interfaccia **Enterprise Insights** sono presenti i domini e gli assets rilevati dal monitoring della propria azienda e che richiedono una maggiore attenzione. E’ possibile accedervi cliccando il simbolo  in alto a destra nella home page e selezionando poi **Enterprise Insights**.



E’ possibile applicare dei filtri ai risultati in evidenza premendo sul simbolo  in alto a destra nella schermata degli insights. Tramite i simboli  che si trovano accanto ad ogni voce evidenziata nei filtri, rispettivamente si può ripristinare un filtro in caso sia stato disattivato, disattivare un filtro o escludere ogni altro filtro eccetto quello selezionato.



Sotto la voce **IOC Domain Matches** vengono evidenziati i domini che l’azienda ha etichettato ed impostato come sospetti, e che sono stati visitati dagli utenti. Facendo scorrere a destra o sinistra l’indicatore  è possibile aumentare o diminuire il lasso di tempo dello storico delle evidenze rintracciate.

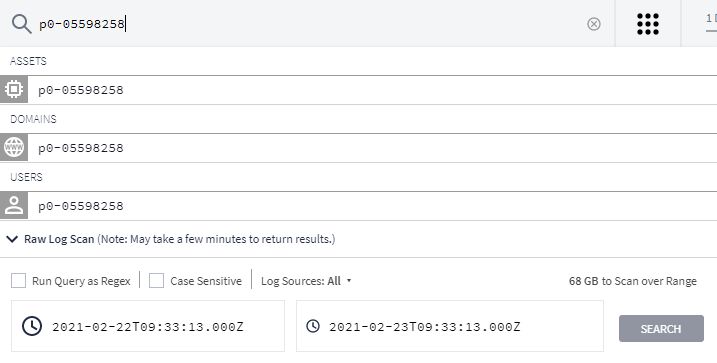
Gli alert possono essere ordinati per:

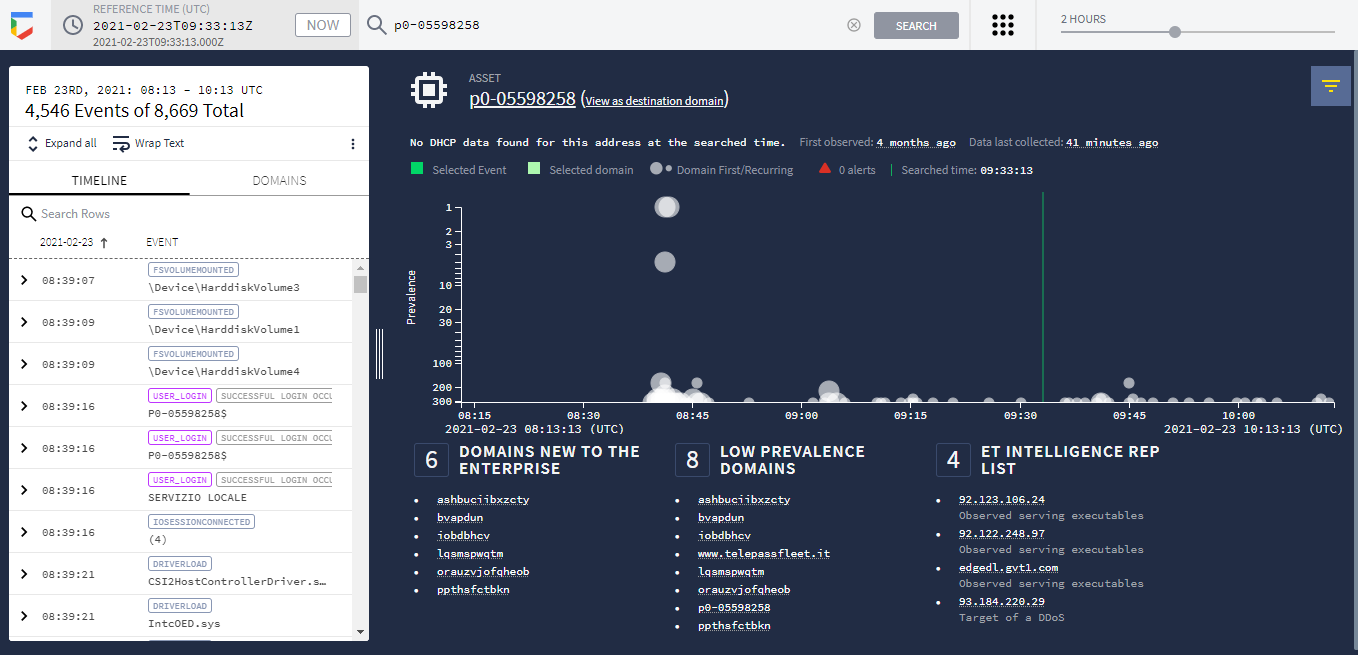
* IOC Ingest Time – il tempo scorso dalla prima volta che Chronicle impostato l’IOC
* First Seen – Il tempo scorso dalla prima volta che l’IOC è stato rintracciato nell’azienda
* Last Seen – Il tempo scorso dall’ultima volta che l’IOC è stato rintracciato nell’azienda

Sotto la voce **Recent Alerts** è possibile consultare gli alert generati più recentemente. In questa sezione sono presenti anche gli alert generati dalle Rules di Chronicle (vedi sezione Chronicle Rules).

**2) Indagine sugli assets**

**2.1)** Chronicle offre la possibilità di investigare sull’attività di un asset in particolare. Inserendo nella barra di ricerca l’hostname, l’IP da cui è stata svolta attività o il MAC address del device sotto osservazione è possibile ottenere un elenco delle azioni svolte dall’asset. Premere quindi su **Search** e cliccare l’asset sotto la voce **Assets** che appare di conseguenza. **NOTA: Perché l’asset desiderato appaia sotto Assets, è necessario che questo esista effettivamente.**

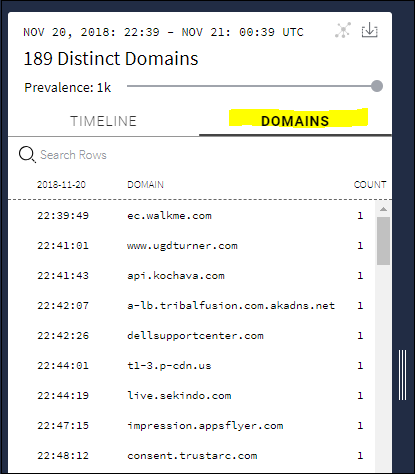




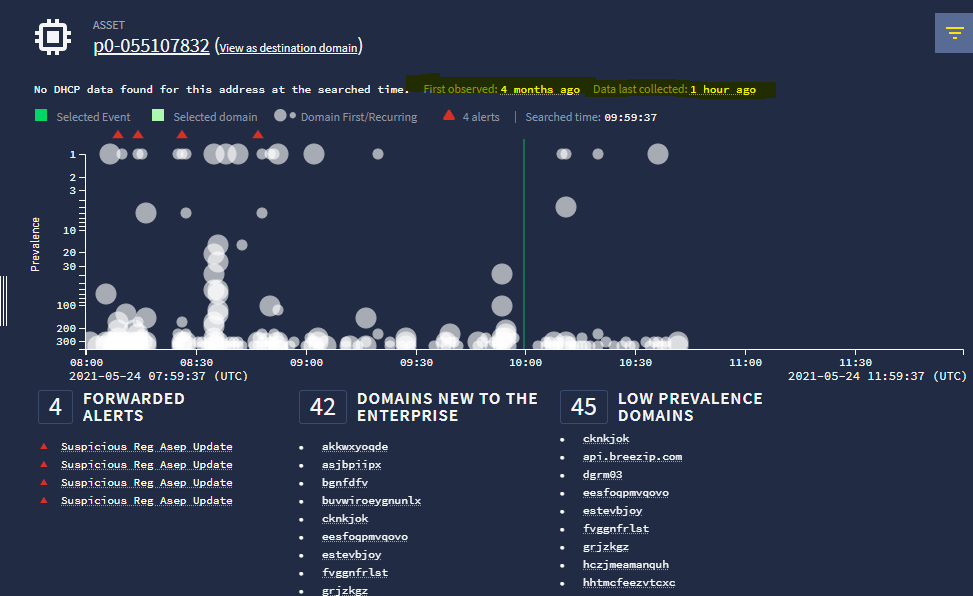
In alto a destra è presente la **Timeline Sidebar (indicata con il numero 1 nell’immagine successiva)**, che di default è impostata su due ore. Spostando il cursore della barra a sinistra o a destra è possibile rispettivamente diminuire o aumentare il **time range di indagine (2 nell’immagine)** sull’asset ricercato. In alto a sinistra si trova il **Reference Time (3 nell’immagine)**, e subito sotto il time range sotto indagine calcolato in base al tempo impostato nella Sidebar. Notare che impostando un determinato numero di ore nella Sidebar, il time range risultante sarà tale da avere la Reference Time esattamente nel mezzo. (e.g.: Se sono le 10:00 e impostiamo 2 ore nella Sidebar, il time range di indagine andrà dalle 9 alle 11. Se impostiamo 5 ore nella Sidebar, il timerange andrà dalle 7:30 alle 12:30)



Accanto alla sezione **Timeline**, che evidenzia le attività svolte dall’asset nell’impostato time range, è presente la sezione **Domains**, dove è possibile consultare i domini a cui l’asset si è connesso.

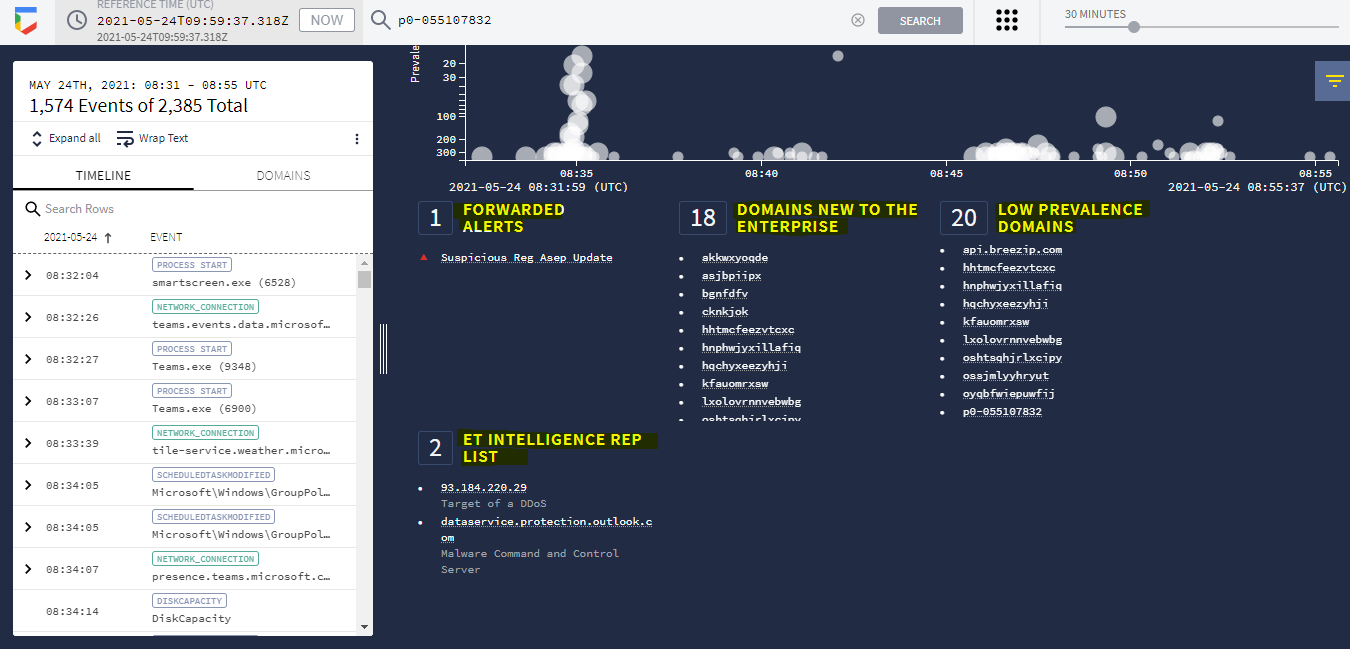


Al centro della schermata è possibile notare il **Prevalence Graph**: ogni cerchio grigio rappresenta l’insieme dei domini al quale l’asset si è connesso. I cerchi grandi indicano le prime connessioni ai domini, mentre quelli piccoli rappresentano le successive volte in cui l’asset si è connesso ai medesimi domini. I domini che più spesso vengono visitati si trovano verso la parte più bassa del grafico, mentre quelli più insoliti sono indicati nella parte alta, insieme ai triangoli rossi che rappresentano domini visitati potenzialmente pericolosi. Sopra al grafico è possibile notare alcune informazioni riguardanti l’asset sotto indagine, come la prima volta in cui si hanno evidenze di attività.



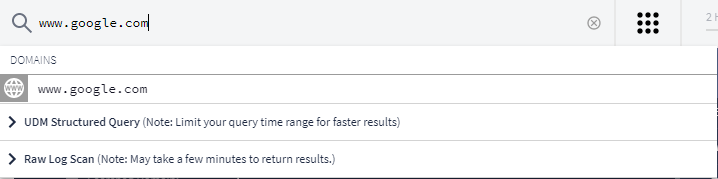
Nella parte sottostante al Prevalence Graph gli **Asset Insight Blocks** sono presenti delle voci che evidenziano i domini e gli alert che richiedono attenzione:

* **Forwarded Alerts**: sotto questa voce si trovano gli alert che necessitano di una indagine più approfondita in quanto generati da domini sospetti.
* **Domains new to the enterprise:** indica i domini che sono stati visitati dall’asset e che non sono mai stati visitati in generale da nessuno all’interno dell’enterprise. Questa verifica avviene a seguito di un controllo del database del DNS aziendale.
* **Low Prevalence Domains:** indica i domini che sono stati visitate poche volte dall’asset sotto indagine (numero di volte compreso tra 1 e 10).
* **ET Intelligence Rep List:** indica le corrispondenze tra gli IOC incontrati durante l’attività dell’asset e la Emerging Threats (ET) Intelligence Rep List pubblicata da Proofpoint, Inc.



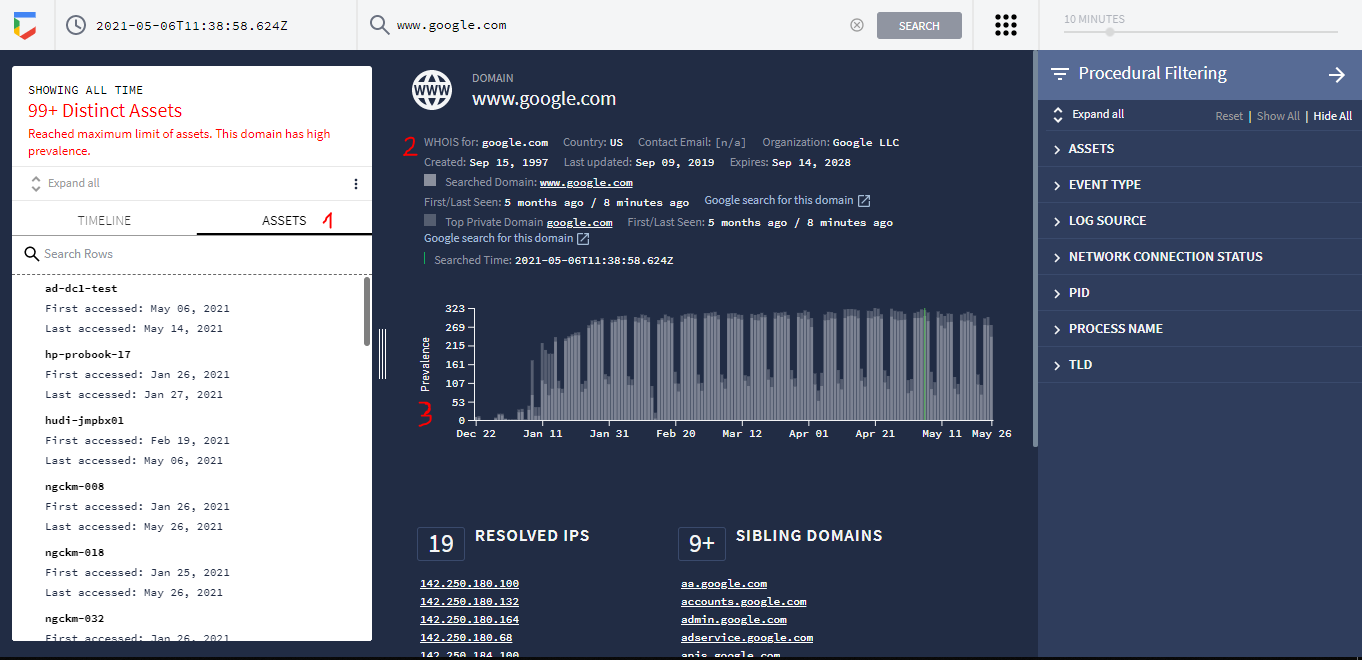
Sugli alert evidenziati è possibile eseguire il **Procedural Filtering**, per il quale si rimanda alla spiegazione nel paragrafo **1) Enterprise Insights.**

**2.2)** Chronicle offre la possibilità di ricercare specifici domini, indicando da quali asset sono stati visitati. Per farlo, inserire l’url nella barra di ricerca, premere Search e poi l’indirizzo che compare sotto la voce Domains nella tendina che si apre sotto alla barra di ricerca.



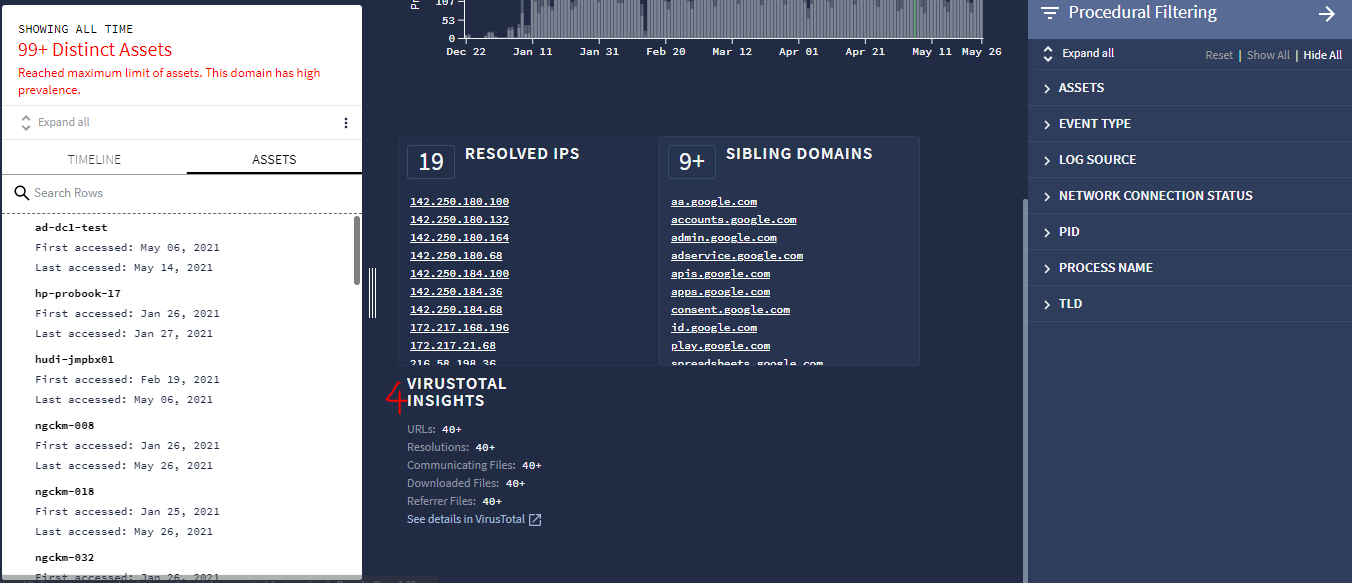
Nella schermata che si aprirà al termine della ricerca, è possibile consultare utili indicatori al fine del miglioramento dell’indagine.

Nella parte sinistra è presente la sezione **Asset (numero 1 nell’immagine successiva)**, che indica gli asset che hanno visitato l’url ricercato. Vengono mostrati i dati provenienti da **WHOIS (numero 2)**, che mostrano informazioni riguardo al dominio, oltre alla reputazione che questo ha. La **Prevalence (numero 3)** mostra il grafico degli asset che nel tempo hanno visitato il dominio.

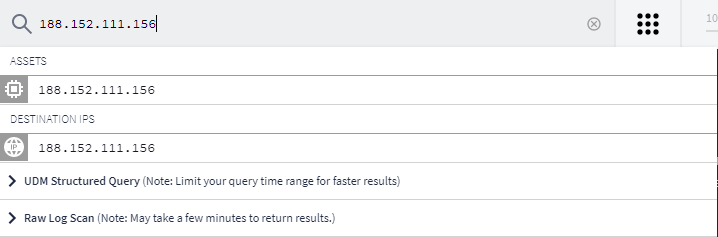


Sono presenti ulteriori campi sotto al Prevalence Graph, quali **Resolved IPs**, **Sibling Domains** e **VirusTotal Insights (numero 4 nell’immagine successiva).**

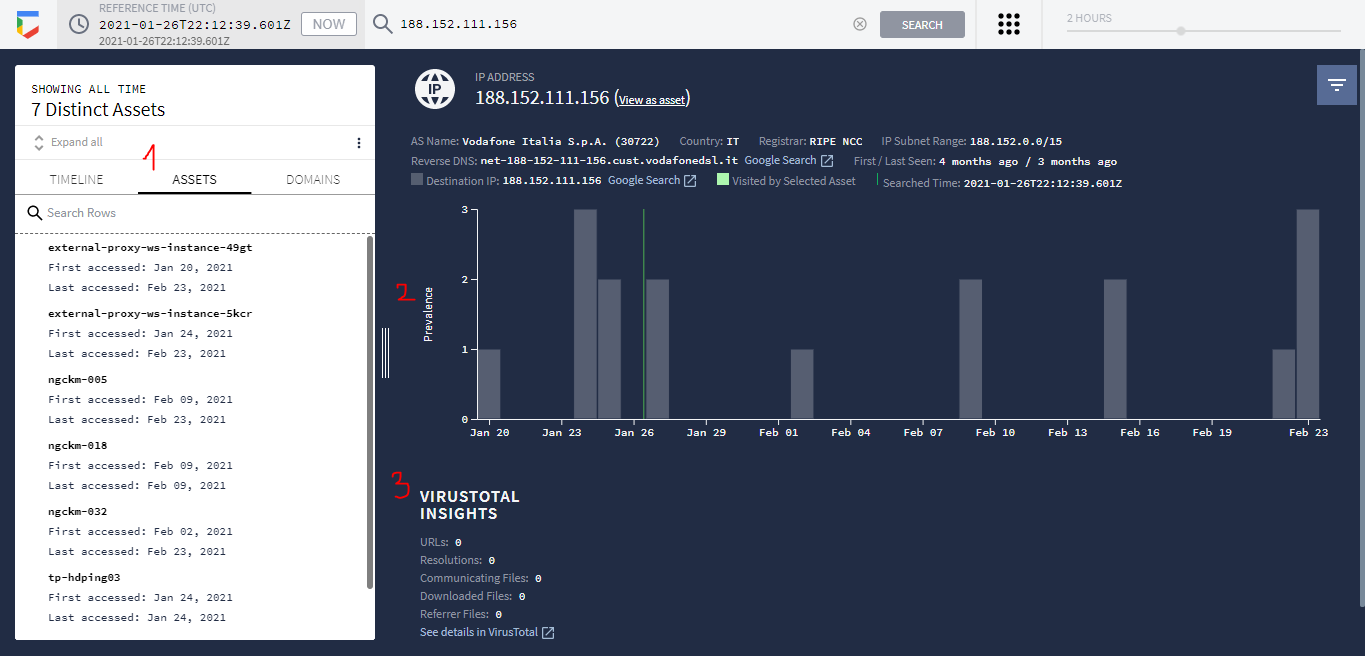
* Resolved IPs: indica gli IP degli host che hanno visitato il dominio sotto indagine
* Sibling Domains: indica i domini che sono simili o che contengono quello ricercato
* VirusTotal Insights: indica informazioni provenienti da VirusTotal



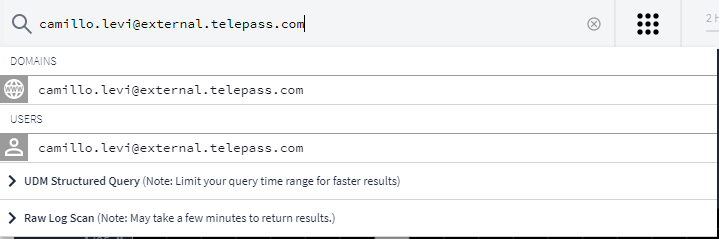
**2.3)** Chronicle offre la possibilità di effettuare ricerche su IP specifici. Per farlo, inserire l’IP nella barra di ricerca, premere Search e poi premere sull’IP che appare sotto la voce **Destination IPS**.



La sezione **Assets (numero 1 nell’immagine successiva)** indica gli asset che si sono connessi all’IP ricercato. Il **Prevalence Graph (numero 2)** indica gli assets che nel tempo si sono connessi all’IP ricercato. **VirusTotal Insights (numero 3)** indica informazioni provenienti da VirusTotal.



**2.4)** Chronicle offre la possibilità di effettuare ricerche su utenti specifici. Per farlo, inserire l’indirizzo dell’utente nella barra di ricerca, premere Search e poi l’indirizzo che appare sotto la voce **Users**.



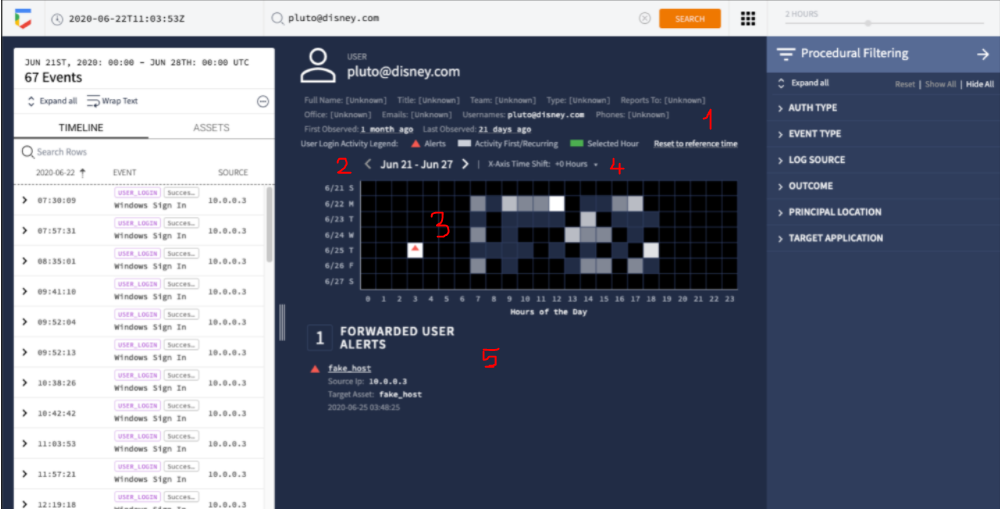
Nella schermata di indagine che si apre, sono presenti alcuni valori che possono aiutare nell’indagine.

* **User Information (numero 1 nell’immagine successiva)**: fornisce informazioni riguardo all’utente
* **Date Selection (numero 2)**: indica una settimana. Quindi premendo la freccia a destra o sinistra si può decidere di quale settimana mostrare le attività
* **Gradient Heat Map (numero 3)**: ogni cella rappresenta un’ora di attività, e il colore indica la frequenza di attività. Nera: assenza di attività. Bianca: attività solitamente presente. Grigio: sfumatura più chiara indica molta attività, arrivando a sfumature scure che indicano poca attività. NOTA: attività come creazione/compilazione di documenti Word ecc non sempre sono indicati.
* **X-Axis Time Shift (numero 4)**: questa impostazione è di aiuto se si vogliono svolgere indigini che comprendano un lasso di tempo a cavallo tra due giorni. Impostando il X-Axis per esempio a -1 Hour, verrà indicata l’attività svolta durante la prima ora dei giorni successivi. Quindi se inizialmente era indicata l’attività dalle ore 0 alle ore 23 di ogni giorno della settimana stabilita nel Date Selection, impostando lo X-Axis a -1 Hour avremo visione delle attività dalle ore 1 (di ogni giorno) alle ore 0 (dei giorni successivi). Con X-Axis a -2 Hour avremo visione dalle ore 2(di ogni giorno) alle ore 1 (dei giorni successivi).

Ulteriore esempio di chiarimento: l’attività svolta il lunedì (orario 0-23) della settimana impostata è sotto osservazione. Impostando a -1 Hour lo X-Axis, verrà tolta un’ora all’estremo sinistro e aggiunta all’estremo destro, di fatto diventando orario 1 (del lunedì) – 0 (della notte del martedì).

Questa impostazione risulta molto utile se si vuole avere sulla stessa riga l’attività svolta da un’utente la notte tra un giorno e quello successivo.

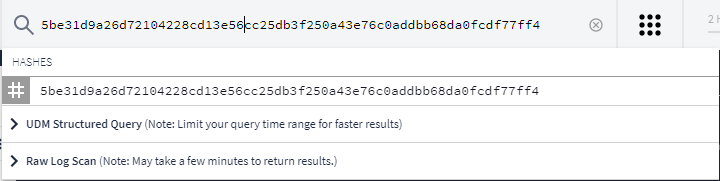
* **User Alerts (numero 5)**: in questa sezione vengono indicati gli alert riscontrati durante l’attività dell’utente nella settimana impostata.



**2.5)** Chronicle offre la possibilità di effettuare ricerche su file in particolare. Ciò è possibile farlo in tre modi: attraverso l’hash, la ricerca dell’asset oppure tramite il Raw Log Scan (per il quale si rimanda alla sezione Raw Log Scan).

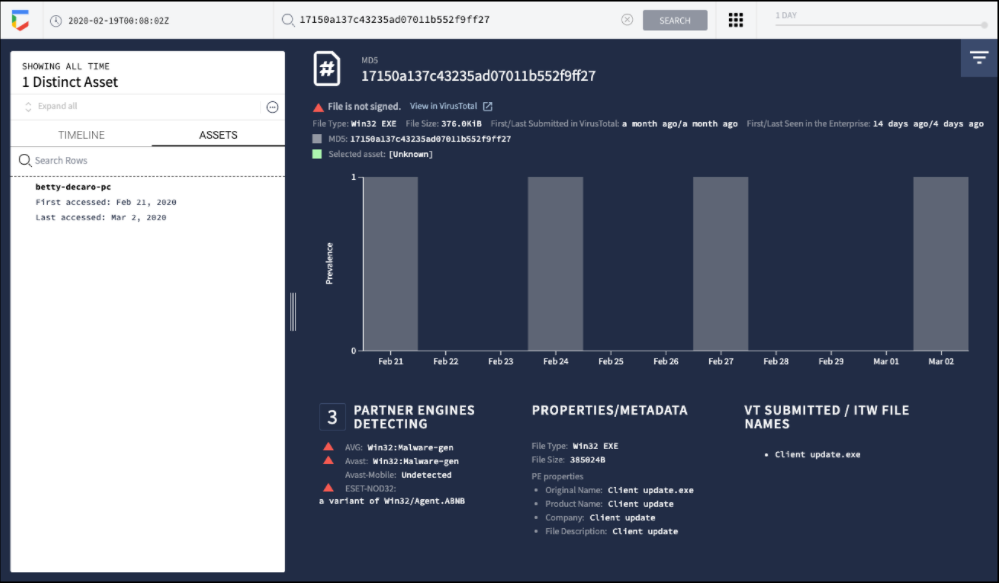
**Ricerca per hash**:

Per effettuare una ricerca per hash, incollare l’hash nella barra di ricerca, cliccare su Search e poi cliccare l’hash che compare sotto la voce **Hashes**.

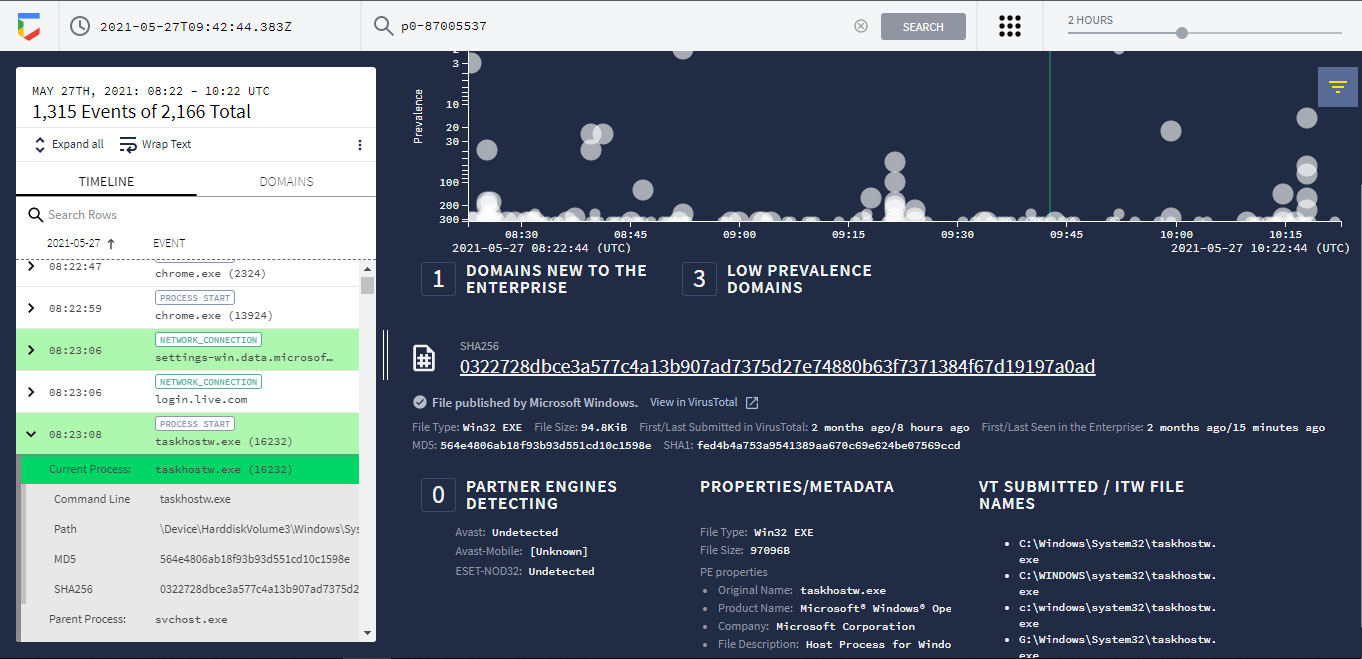


Al termine della ricerca, si avrà la possibilità di consultare gli asset che hanno interagito col file legato all’hash ricercato andando nella sezione **Assets**, o di consultare la timeline delle attività di interazione col suddetto nella sezione **Timeline**. Nella parte bassa dell’interfaccia, si avranno tre diverse voci:

* **Partner Engines Detecting:** altri security vendors che hanno individuate l’hash ricercato
* **Properties/Metadata:** Proprietà conosciute del file
* **VT Submitted/ITW File Names:** File che combaciano con l’hash ricercato secondo VirusTotal



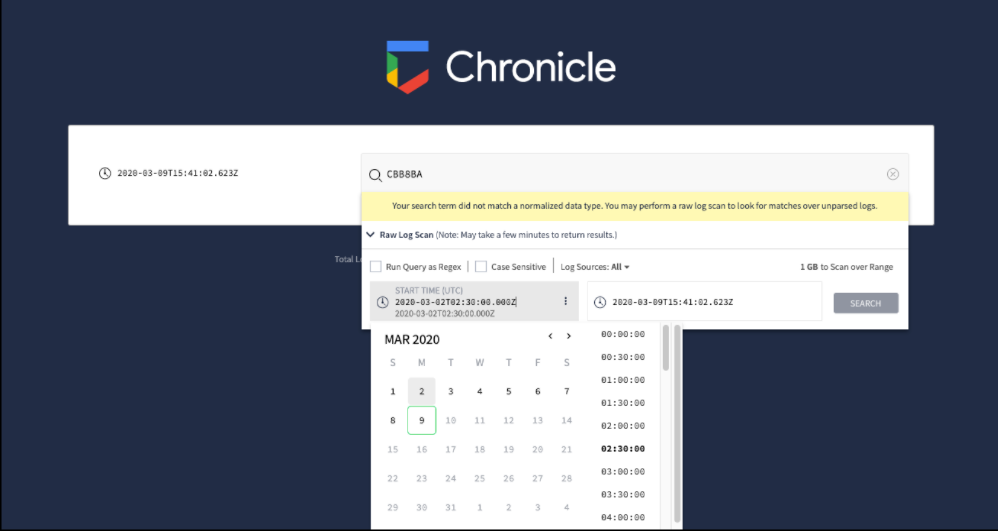
**Ricerca per Asset:** Cercare l’asset di cui vogliamo effettuare un controllo delle attività legate a un file. Nella parte sinistra, rimanere nella sezione **Timeline** e cercare il file desiderato. A questo punto ingrandire il log dell’attività che indica il file cercato premendo sulla freccia alla sinistra. Premere quindi il file accanto alla voce **Current Process**. Sotto al Prevalence Graph appariranno le informazioni riguardanti il file appena cliccato.



**3) Raw Log Scan**

Chronicle offre la possibilità di effettuare una ricerca in un range personalizzabile. Inserendo l’oggetto nella barra di ricerca e premendo Search, l’ultima opzione nel menù a tendina che si aprirà sarà **Raw Log Scan**. Impostare quindi il time range di ricerca. In questo modo verrà ricercato qualsiasi evento che nel log comprenda la stringa ricercata (NOTA: Tramite Raw Log Scan è possibile inserire il nome di un file e ricercarlo come stringa all’interno dei log di attività di un asset).

Se l’oggetto inserito nella barra di ricerca non viene riconosciuto da Chronicle (e.g.: utenti non registrati, file sconosciuti ecc), l’unica opzione sarà indagare tramite Raw Log Scan.



**4) Regular Expressions**

Chronicle offre la possibilità di effettuare delle query all’interno della barra di ricerca in modo da poter interrogare i log degli eventi Windows. Se necessario è possibile anche concatenare query in modo da imporre delle condizioni.

**ATTENZIONE:** Se si vuole fare uso di espressioni regolari, inserire la query nella barra di ricerca, premere Search, selezionare Raw Log Scan e spuntare la casella **Run Query as Regex.** Negli esempi sottostanti verrà dato per scontato che l’opzione di cui sopra sia stata spuntata.

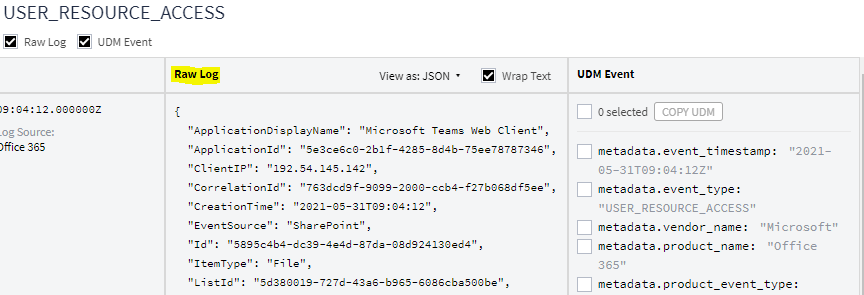
Esempio:

1. **"EventID":"4738" –** Questa query mostra tutti i log in cui compare l’event ID numero 4738, che indica un evento di cambio dati di una utenza, come per esempio il cambio della password. Per l’elenco degli event ID da poter ricercare su Chronicle si rimanda al link [Appendix L - Events to Monitor | Microsoft Docs](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor) .
2. **"target\_account.account\_name": "xxx" – (dove xxx indica il numero di matricola di un utente) –** Questa query mostrerà come risultato tutti gli eventi che hanno avuto come target account l’utenza con numero di matricola xxx .
3. **EventID\"\:\s\*\"xxx.\*?target\_account.account\_name\"\:\s\*\"yyy\" –** Questa query mette in AND due condizioni, che quindi si devono verificare entrambe nello stesso momento. Nello specifico, l’esempio di cui sopra ricercherà un evento con event ID xxx e che abbia avuto come target l’utente con numero di matricola yyy.
4. **(?:\"EventID\"\:\s\*\")(?:4738|4724) –** Questa query mostrerà come risultato tutti i log che hanno come event ID 4738 OPPURE 4724.

Negli esempi c) e d) è possibile cambiare il tipo di dato che si vuole andare a cercare. Per esempio in c) è possibile cambiare la parte di target\_acount.account\_name con un altro dato da cercare all’interno dei log, così come nel d) è possibile cambiare il dato EventID con un’altra informazione.

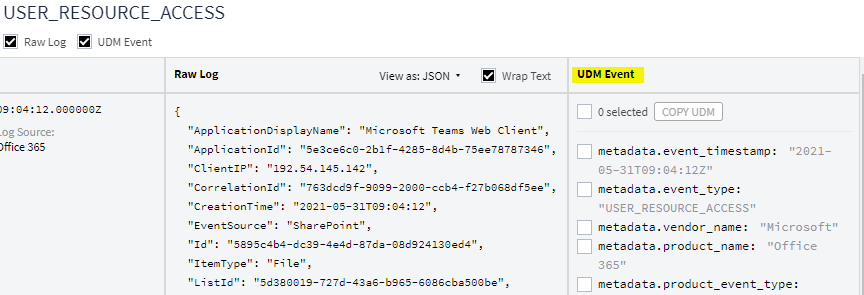
Per ulteriori esempi di query si rimanda alla documentazione di Chronicle.

**NOTA**: Le interrogazioni presenti nelle query di cui sopra vengono effettuate sui dati presenti nel Raw Log di ogni evento. Per le interrogazioni sui dati presenti nella sezione di UDM Event si rimanda al prossimo capitolo (5).



**5) UDM Structured Query**

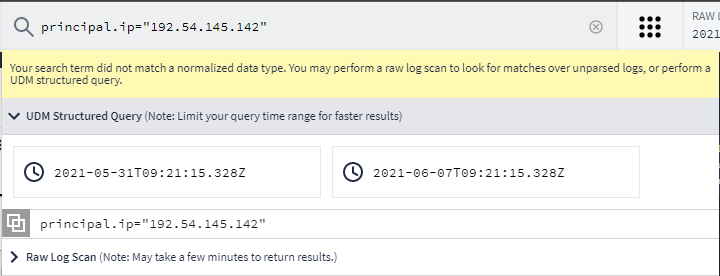
E’ possibile effettuare interrogazioni di ricerca utilizzando i dati nella sezione UDM Event di ogni log.



Per capire come impostare query in questa modalità, è opportuno mostrare degli esempi:

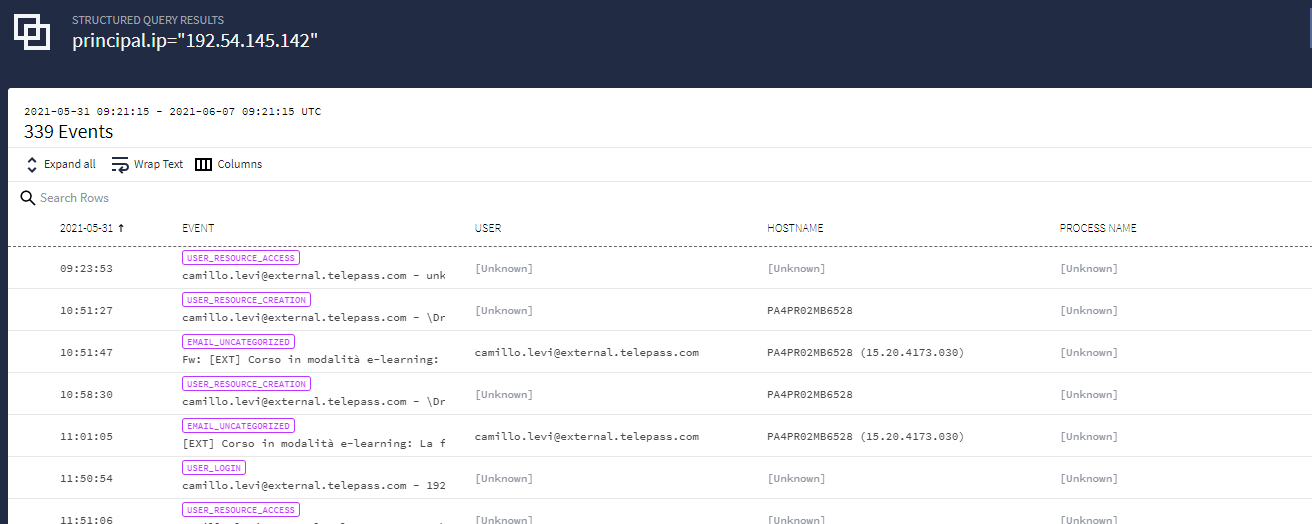
[**NOTA:** Tramite questa tipolologia di query è possibile utilizzare i connettivi logici AND e OR, anche concatenandoli quando necessario].

1. **principal.ip="192.54.145.142"** – Poniamo di voler effettuare indagini sui logs di attività provenienti dall’IP 192.54.145.142. Nella sezione UDM Event di un log di attività (effettuata da quell’indirizzo IP) è presente la dicitura principal.ip[0] : "192.54.145.142" .  
   Inserire quindi nella barra di ricerca la query in esempio, eliminando le parentesi quadre, il numero all’interno e i due punti, sostituendo il tutto con “=”. Premendo su Search, si apriranno le opzioni a tendina. Sopra a quella di Raw Log scan (capitolo 3) è presente la ricerca per UDM Structured Query.

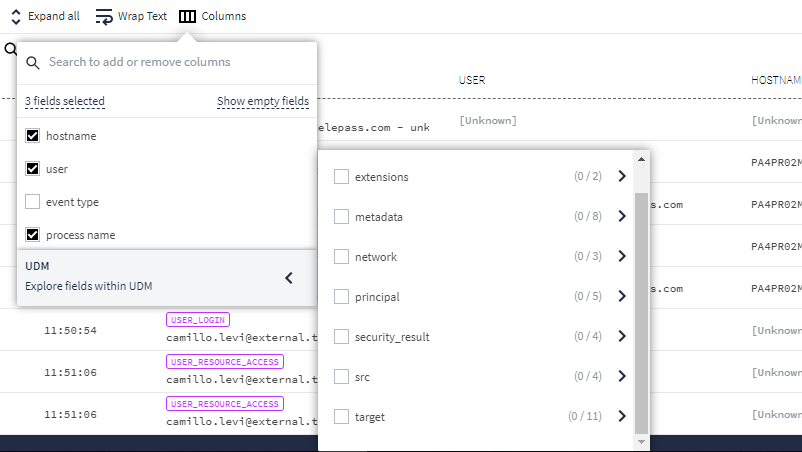


Impostare quindi il time range in cui si vuole che venga effettuata la ricerca e, per farla partire, premere sulla query appena sotto agli orari.

Si aprirà quindi la schermata col risultato della ricerca.

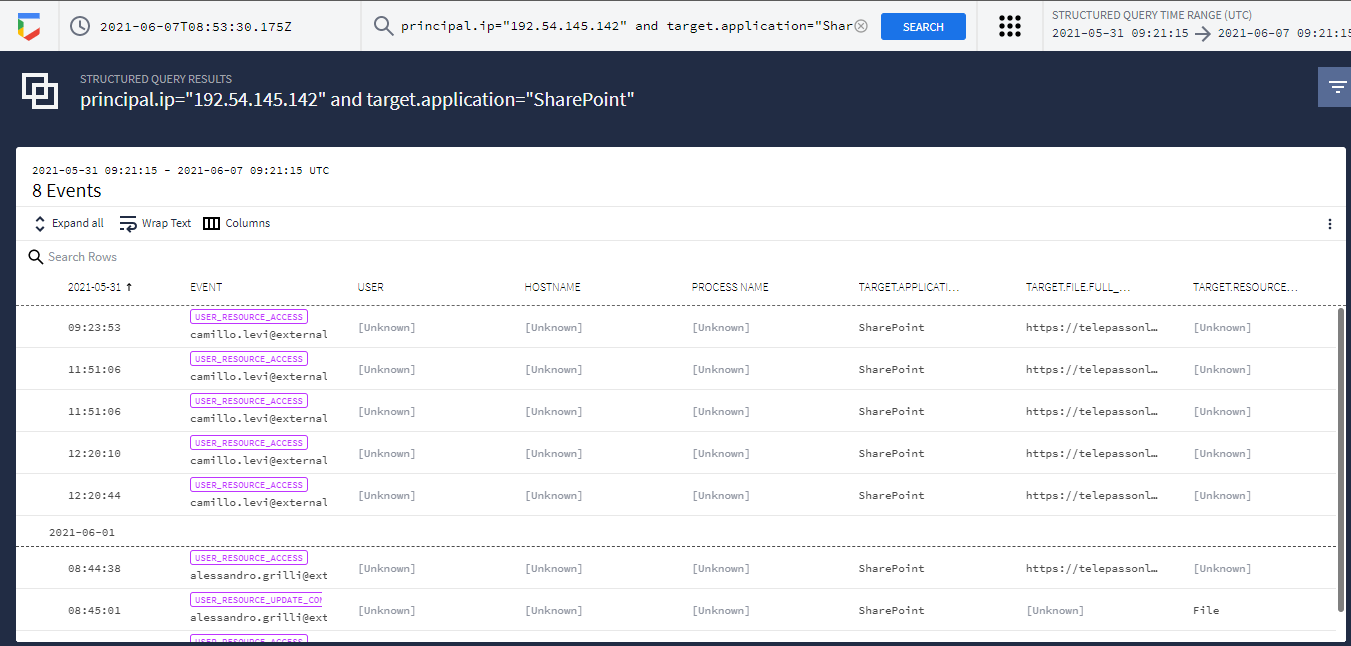


Le caratteristiche di ogni log saranno visibili nelle colonne accanto all’evento. Queste sono modificabili premendo e spuntando i campi voluti. Sono presenti ulteriori caratteristiche, premendo su Explore Fields within UDM.



Per approfondire ulteriormente un log di attività, è sempre disponibile il tasto  nella parte finale, a destra, di ogni riga.

1. **principal.ip="192.54.145.142" and target.application="SharePoint" –** La query in esempio, data la presenza del connettivo AND, mostrerà come risultato tutti i log che ,all’interno dell’UDM Event, presentano principal.ip[0] : "192.54.145.142" E (quindi nello stesso log) target.application : "SharePoint". La stessa tipologia di query è possibile effettuarla sostituendo OR al posto di AND. In quel caso, si hanno come risultato tutti i log che, nel time range selezionato, presentano all’interno dell’UDM Evento la dicitura principal.ip[0] : "192.54.145.142" OPPURE ) target.application : "SharePoint". Nell’immagine di esempio sottostante è stata spuntato anche il campo Target, in modo che fossero visibili le caratteristiche di indagine.



1. **(principal.ip="146.112.42.38" or principal.ip="192.54.145.142") and target.application="SharePoint" –** In questa query viene utilizzata la concatenazione di connettivi logici. La presenza delle parentesi tonde è obbligatoria nel momento in cui possono essere presenti ambiguità nella ricerca. Nell’esempio riportato, se non fossero state utilizzate le parentesi tonde, Chronicle non avrebbe saputo a quale condizione dare la precenza: i due IP sono in OR e il loro risultato è in AND con la target application? Oppure il secondo IP è in AND con la target application e il suo risultato è in OR col primo IP?

La presenza delle parentesi risolve questo problema, dando priorità al connettivo desiderato; senza di queste, non sarebbe possibile avviare la UDM Structured Query inserita.

Quindi, il risultato della query in esempio mostrerà ogni evento che, all’interno della sezione di UDM Event, presenti uno dei due IP ricercati E la target.application selezionata.

**NOTA:** Se al posto dell’OR tra i due IP fosse stato messo un AND, la query non sarebbe partita. Questo perché è impossibile che ci sia un log con due principal IP diversi.

**6) Chronicle Rules**

Chronicle permette agli utenti di poter creare delle regole di allerta che vengono generate e notificate al verificarsi di determinati eventi.

Per aprire la **Rules Dashboard** premere l’icona  e selezionare View Rules.

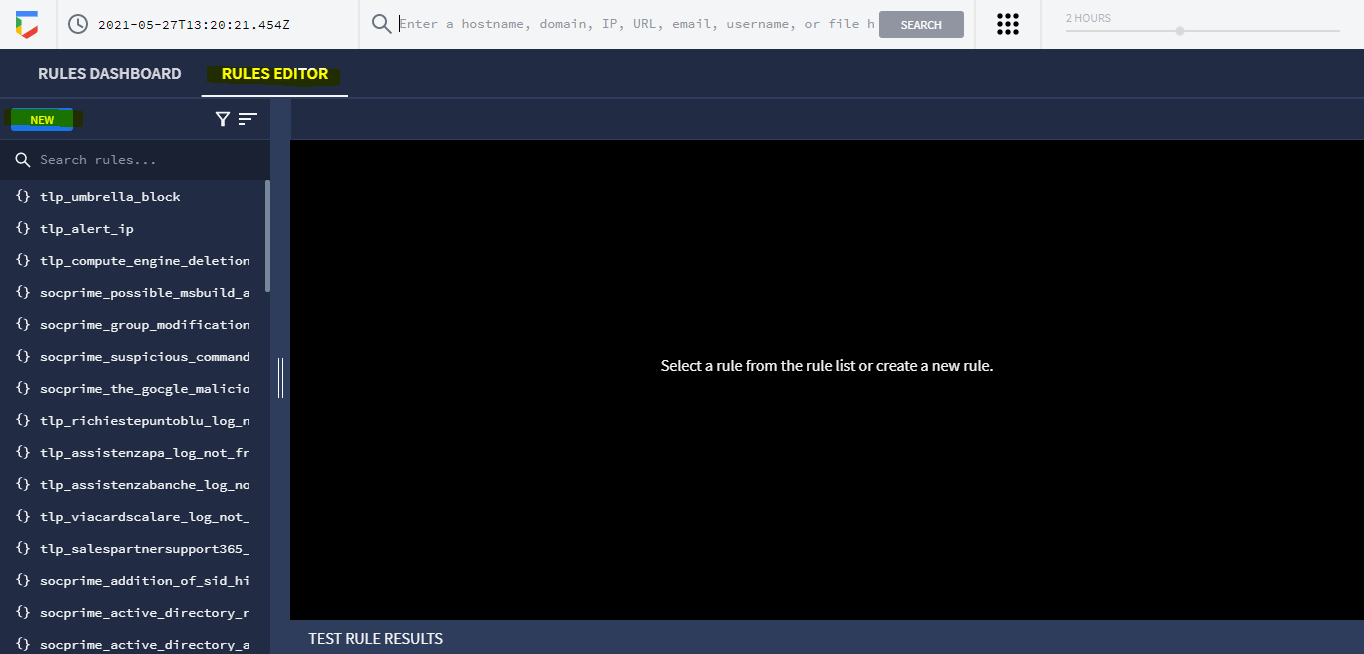
Si aprirà la schermata delle Rules di Chronicle, e di default verrà mostrata la dashboard.



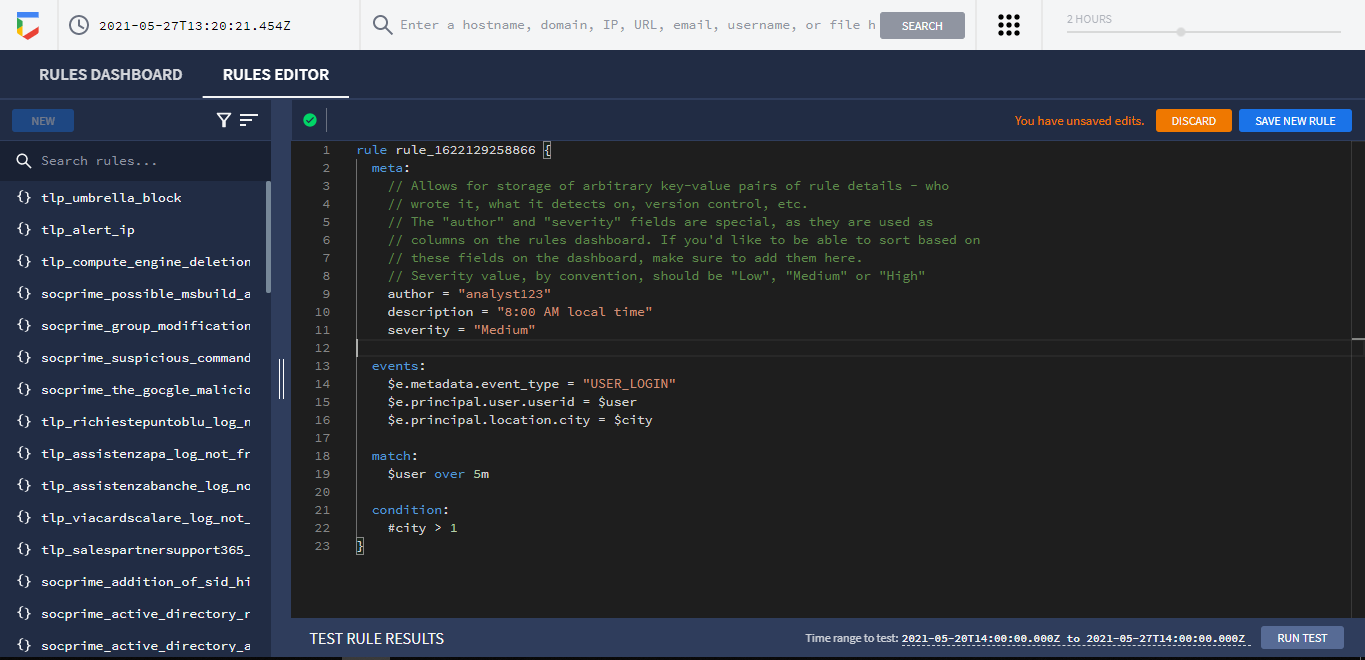
Qui sono consultabili tutte le regole che sono state create, con relativi orari di ultima detection.

Nel corso del paragrafo verranno chiariti i vari campi indicati per ogni regola.

Per creare una nuova regola, premere la sezione **Rules Editor**, dove sarà possibile modificare regole già create e presenti. Premere quindi **New.**



Apparirà il codice di default di una regola. Cancellarlo per poter scrivere quella nuova



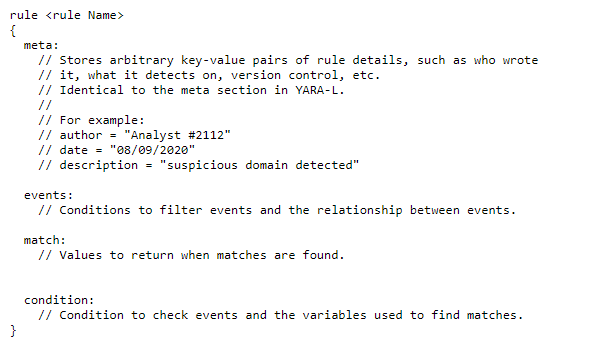
**Creazione e struttura di una Rule**:

Le regole su Chronicle sono scritte in linguaggio YARA-L 2.0, che col nuovo Detection Engine risulta incompatibile con YARA, sviluppato da VirusTotal. Le eventuali regole scritte in YARA sono da riscriversi in YARA-L 2.0. Il codice viene prima compilato, e solamente in caso di assenza di errori è possibile eseguirlo.

Una Rule è divisa in:

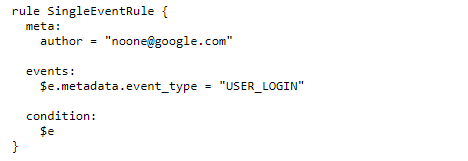
* **Meta:** dove generalmente è presente una descrizione della regola implementata, con l’aggiunta di autore, data, versione, severity, descrizione sintetica e altri dettagli che contestualizzano la regola, consultabili negli esempi o nella documentazione di Chronicle.
* **Events:** Evento/i sui quali verranno verificate le condizioni stabilite nel Match e nella Condition
* **Match (Optional):** Condizione sugli eventi che viene controllata dopo la Condition e che se verificata genera l’alert. Questa sezione è opzionale nel caso in cui si volesse verificare una condizione singola.
* **Condition:** Condizione che viene verificata sugli eventi descritti in Events.

Di seguito la struttura standard di una Rule con relativi commenti delle sezioni interne.



Al fine di comprendere al meglio la sintassi di YARA-L 2.0 e la sua applicazione nelle Rules, si prendano in considerazione gli esempi riportati di seguito. Per la parte sulla generazione degli Alert delle Rules si rimanda alla sezione **Test, Save e Alerting delle Rules**.

**a) Singolo evento - 1**



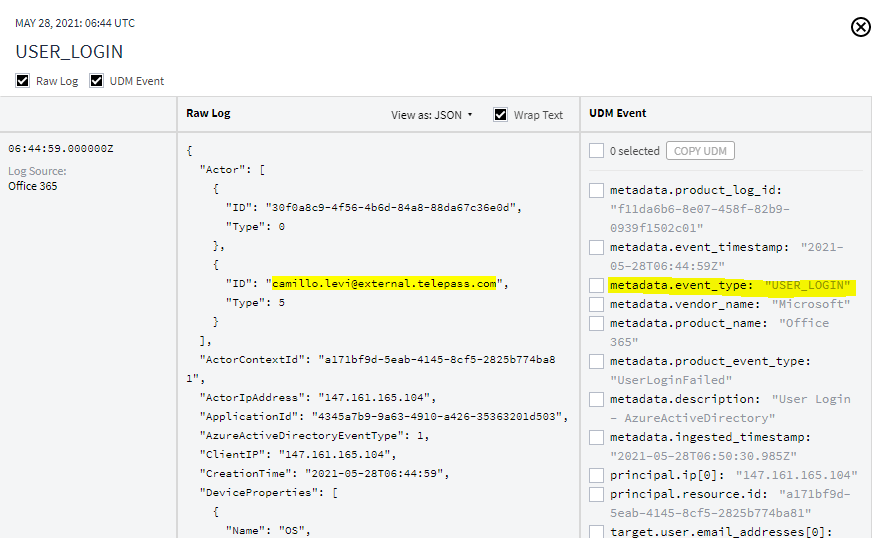
Questa regola genera un avviso ogni volta che un utente effettua una login. La sezione “meta” contiene l’autore della regola, la parte “events” contiene l’evento di login mentre la “condition” verifica che l’evento scritto in “events” si sia verificato, generando conseguentemente l’avviso.

Entrando nello specifico della sezione “events” di questo esempio, è utile capire la sintassi del linguaggio:

* **$e** – è il modo per indicare un evento. Lo si può vedere come l’assegnazione di una variabile all’evento stesso. Per riferirsi all’evento, come verrà visto inseguito, si usa l’espressione $e.

Quando ci saranno più eventi a cui riferirsi, saranno presenti le diciture $e1, $e2 ecc.

* **metadata.event\_type** – Come è possibile notare nella successiva immagine, nella scheda UDM Event di ogni log di Chronicle sono presenti informazioni sulle quali è possibile effettuare una verifica nella parte “condition” della Rule stessa. In questo caso, l’evento al quale si fa riferimento è un qualsiasi log di attività (di Chronicle) che abbia come event\_type una LOGIN. Di seguito l’esempio di un LOGIN con relativo UDM Event su Chronicle.



E’ possibile verificare una condizione su qualsiasi dato all’interno della scheda UDM Event di un log di attività.

La “condition” della Rule di esempio effettua una verifica sull’effettivo event\_type del log.

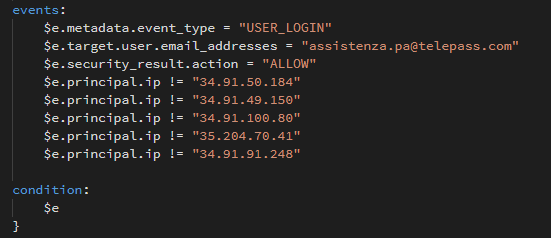
In particolare, scrivere $e nella sezione della condition equivale a impostare come fattore di avviso il il verificarsi dell’evento chiamato “e” (più banalmente, if $e = true).

Quindi, al verificarsi dell’evento $e, che come dichiarato nella sezione degli “events” in questo caso si tratta di una USER\_LOGIN, verrà generato un avviso. Ogni volta che verrà generato un log di attività di LOGIN, di conseguenza, la condizione della Rule sarà verificata. Per la parte sulla generazione degli Alert delle Rules si rimanda alla sezione **Test, Save e Alerting delle Rules**.

**b) Singolo evento - 2**

In questo esempio è stata volontariamente omessa la parte “meta”.

Questa regola genera un avviso ogni volta che l’utente assistenza.pa@telepass.com effettua con successo una login proveniente da IP diversi da quelli citati nel codice.



Nella sezione “events” sono state specificate più informazioni su cui effettuare la verifica:

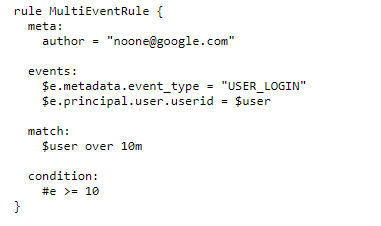
* **$e.metadata.event\_type = “USER\_LOGIN” -** come descritto nell’esempio precedente indica che log deve essere di tipo USER\_LOGIN
* **$e.target.user.email\_addresses = “xxx” -** altra caratteristica che deve avere l’evento è che l’indirizzo email che ha effettuato la login corrisponda a xxx, nella figura assistenza.pa@telepass.com
* **$e.security\_result.action = “ALLOW” -** pone un’altra restrizione al log. In particolare questo deve essere di LOGIN andato a buon fine
* **$e.principal.ip != “34.91.50.184” e seguenti** – questa riga di codice impone che l’evento debba provenire da IP diversi da quelli descritti. Ciò è riscontrabile dai caratteri “!=” che stanno ad indicare “diverso da”

La condition **$e** sta ad indicare che il generico evento “e”, descritto in “events”, debba verificarsi con successo. Dal momento che ogni caratteristica dell’evento nella sezione “event” è stata descritta sull’evento “e”, e che la condition è “$e”, significa che tutte le caratteristiche descritte in “events” debbano valere sullo stesso evento.

Quindi verrà generato un avviso dalla Rule ogni volta in cui su Chronicle sarà presente un log di attività con queste caratteristiche: Login con successo dall’account assistenza.pa@telepass.com proveniente da IP diversi da quelli citati.

**c) Multi-evento 1**

Di seguito è riportato un esempio di Rule Multi-evento. In particolare, questa genera un avviso ogni volta che lo stesso utente effettua una login per almeno 10 volte nell’arco di 10 minuti.



Esaminando la sezione “events”:

* **$e.metadata.event\_type = “USER\_LOGIN” –** I log sotto osservazione sono quelli che come tipologia hanno una login.
* **$e.principal.user.userid = $user –** In questo modo, si sta assegnando alla variabile $user lo userid dell’evento sotto osservazione. In questo modo, quando si andranno ad enumerare vi sarà unicità del valore.

La sezione “match” viene controllata prima delle condition, e tutte le variabili di cui si vuole fare uso devono essere dichiarate all’interno di “events”. **NOTA:** Nella sezione “match” vanno inserite le Match Variables. Di seguito è riportata la definizione cui fa riferimento la documentazione di Chronicle:



Da questa definizione si evince che le variabili nella sezione “match” sono dei campi che contengono più valori all’interno.

L’esempio contiene la riga di codice:

* **$user over 10m –** In questo caso, come finestra temporale vengono fissati 10 minuti. Questo significa che vengono presi in considerazione solo gli eventi di tipo USER\_LOGIN che tra di loro hanno una distanza temporale minore di 10 minuti, raggruppati per userid ($user) distinti. La keyword “over” serve per indicare il lasso di tempo che si vuole considerare.

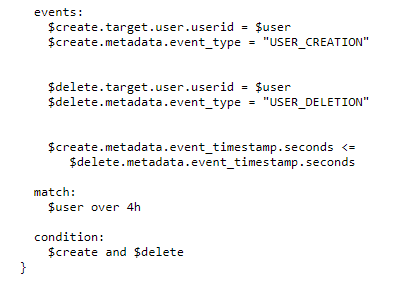
E’ presente poi la sezione “condition”:

* **#e >= 10 –** Il carattere “#” serve per effettuare un count dei distinti valori o eventi rappresentati dalla variabile. In questo caso, la variabile “e” rappresenta un evento di tipo USER\_LOGIN. Questo significa che, perché la condizione descritta in “condition” sia verificata, l’evento nominato “e” debba avvenire un numero di volte maggiore o uguale a 10. **NOTA:** la variabile impostata nella sezione “match” serve per effettuare una join sugli eventi che vengono presi in considerazione (in questo caso quelli di tipo USER\_LOGIN distanziati da meno di 10 minuti, raggruppati per distinti userid) e che vengono contati nella sezione “condition” della Rule.

**c) Multi-evento 2**

Nel seguente esempio è stata volontariamente omessa la sezione “meta” della Rule.

La regola genera un alert nel momento in cui una utenza viene creata e poi cancellata nell’arco di tempo di 4 ore.



Esaminando la sezione “events”:

* si noti che non è presente la notazione “$e1” o “$e2” per indicare gli eventi. Questo perché nell’esempio vengono cercati due gruppi di eventi differenti, in questo caso gli eventi di creazione ($create) e cancellazione ($delete). Negli events è presente anche la riga **$create.metadata.event\_timestamp.seconds<=$delete.metadata.event\_timestamp.seconds**: ciò sta ad indicare che i gruppi di eventi su cui si stabiliscono le condizioni debbano comprendere prima la creazione e poi la cancellazione, in questo ordine.
* Lo userid viene inserito nella variabile **$user**, che ha la funzione di join tra i due gruppi di eventi ricercati.

Esaminando la sezione “match”:

* **$user over 4h**: gli eventi che corrispondono alla creazione e alla cancellazione dello user (cioè con lo stesso $userid, in cui la creazione viene prima della cancellazione) devono essere separato da un lasso di tempo massimo di 4 ore affinché venga generato l’alert dalla regola.

Esaminando la sezione “condition”:

* **$create and $delete**: la condizione è che l’evento (esista un evento di tipo create all’interno del gruppo create) di creazione sia true, quindi che esista effettivamente, e (and) che l’evento di cancellazione sia true, quindi che esista effettivamente anche questo.

Quindi vengono ricercati i gruppi di eventi di creazione e di cancellazione tali per cui questi esistano, si verifichino in quell’ordine, e all’interno di questi vengono verificate le condizioni sull’utenza, che deve essere la stessa, e il lasso di tempo in cui si sono verificati, che corrisponde a 4 ore. Quando tutte queste condizioni sono verificate, la regola genererà un alert.

**6.1) Test, Save e Alerting delle Rules**

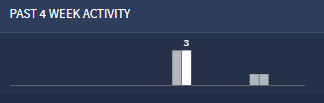
Una volta che il codice è stato scritto e non risultano errori di compilazione (verificabile dalla presenza del simbolo  in alto a sinistra), è consigliabile testare la regola creata.

Premere quindi  in basso a destra. Il lasso di tempo in cui viene testata la regola corrisponde al time range presente a sinistra del tasto Run Test. E’ possibile cambiarlo premendo sugli orari evidenziati.

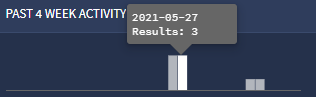
Quando il test avrà portato ai risultati voluti, verificabile dai log di test che vengono generati una volta che questo si è concluso, premere su  in alto a destra per salvare la regola (premere  per cancellarla).

A questo punto, la regola appena creata sarà visibile andando nella sezione **Rules Dashboard** accanto al Rules Editor (raggiungibile premendo  accanto alla barra di ricerca o nella home di Chronicle).

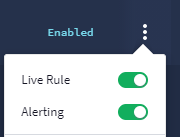
A destra rispetto al nome della regola è presente il grafico degli avvisi generati nelle ultime 4 settimane.



Ogni colonna rappresenta l’insieme degli eventi che hanno fatto scattare la regola in un determinato giorno. Per una rapida indagine è possibile posizionare il cursore sopra ad una colonna per mostrare le occorrenze di allerta e la data in cui si sono presentate.



Continuando a destra, sono presenti la data e l’ora dell’ultimo avviso generato dalla regola (**Last Detection**), l’autore della regola (**Author**), la severity impostata (**Severity**), l’opzione di alerting (**Alerting**), il risultato del **Retrohunt** e lo status della regola (**Live Status**).

[**NOTA**: per cambiare le impostazioni delle opzioni Alerting e Live Status, si deve premere su  alla fine della riga della corrispondente alla regola di cui si vogliono effettuare i cambiamenti. Impostare il cursore sulla destra – diventerà verde – per settare la caratteristica su ON; impostarlo a sinistra per settarla su OFF  ]

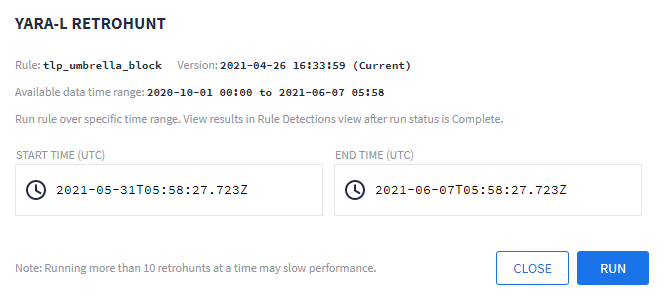
E’ necessario chiarire le ultime tre caratteristiche sopra descritte:

* **Alerting**: se l’opzione è impostata su ON, quando la regola genererà un alert, questo sarà visibile nella sezione Recent Alert degli Enterprise Insights (capitolo 1).
* **Retrohunt**: questa opzione permette, dal momento che le nuove regole generano avvisi nel momento in cui vengono creati nuovi logs di attività, di generarne esaminando i logs già presenti nel database di Chronicle. Premere quindi sui tre punti verticali alla fine della riga, e cliccare su **YARA-L Retrohunt.**



Si aprirà la schermata di impostazione del time range in cui si vuole far eseguire la regola.

Verranno quindi esaminati i logs generati nel lasso di tempo impostato. Per cambiare lo Start Time o l’End Time, premere su questi e inserire la data voluta. Una volta effettuata la retrohunt, si potranno visionare i risultati.



* **Live Status**: se impostato su ON, la regola esamina i logs che vengono generati, e a tutti gli effetti questa è in funzione. Impostarlo su OFF se si vuole che la regola non generi alerts.

Per ulteriori esempi/dettagli si rimanda alla documentazione di Chronicle.