

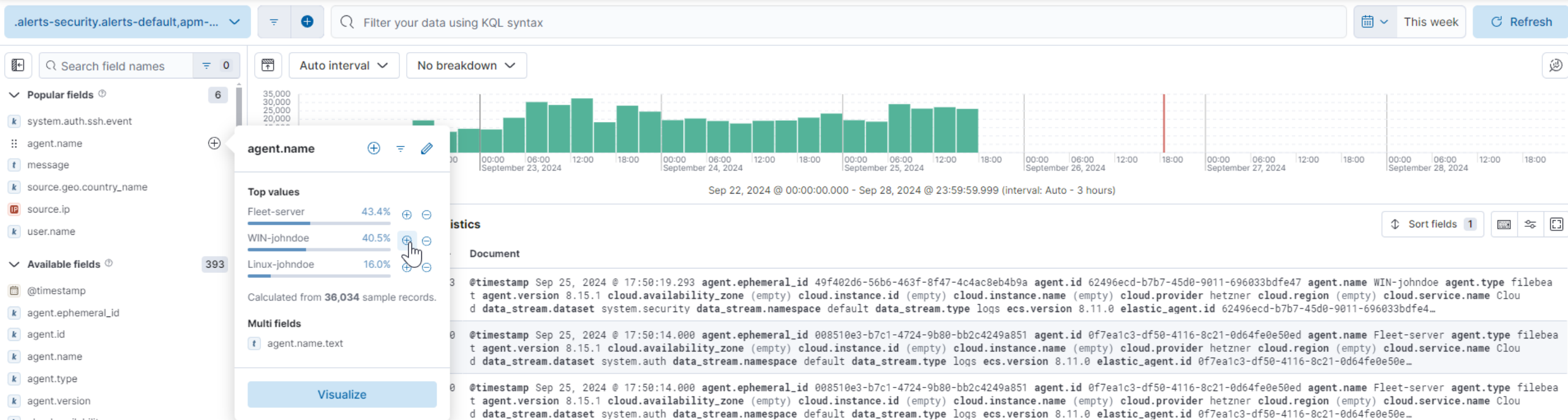
Day 16 - Create Alerts and Dashboards – part 2

Obiettivi

- **Osservare i log di autenticazione dai server Windows/Ubuntu**
- **Creare un alert**

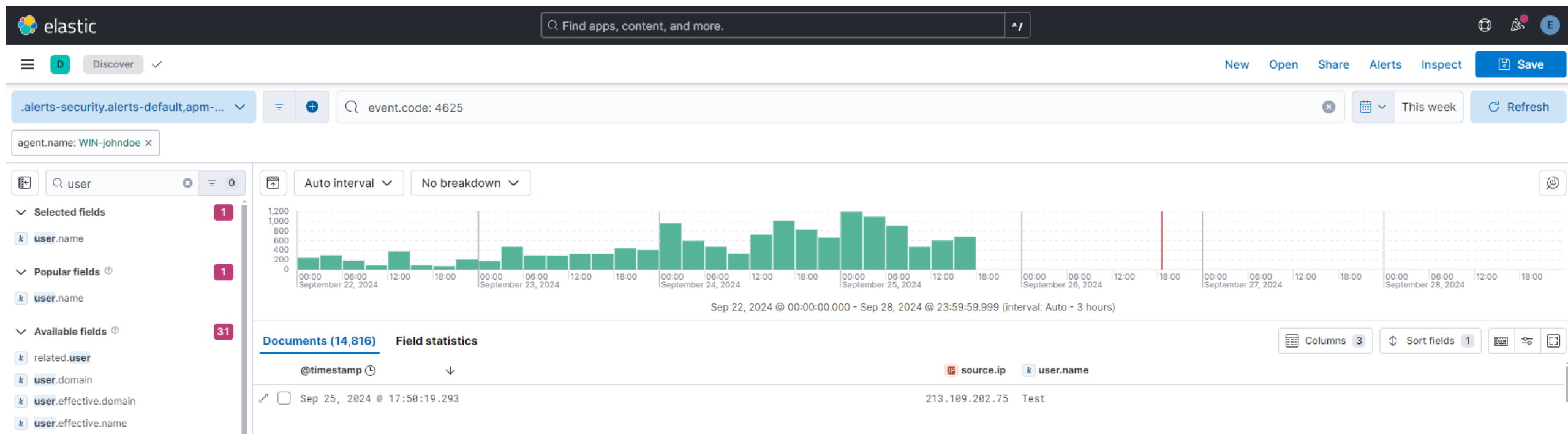
Create Alerts and Dashboards

Filtriamo i dati scegliendo come intervallo temporale questa settimana e isoliamo i dati del server **Windows** con servizio **RDP**.



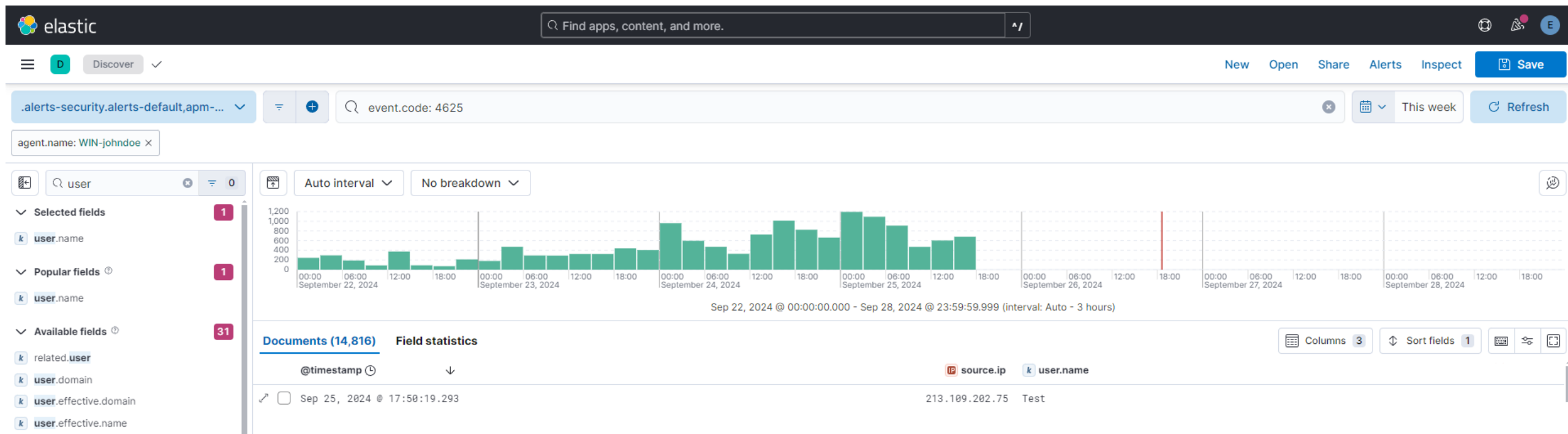
Create Alerts and Dashboards

Questa volta, essendo **Windows**, per isolare i tentativi falliti di autenticazione useremo gli **Event ID** , in questo caso l'**ID** è **4625**, anche in questo caso avremo bisogno di sapere i source ip e user collegati. Procedo col salvataggio della query come in Day 14.



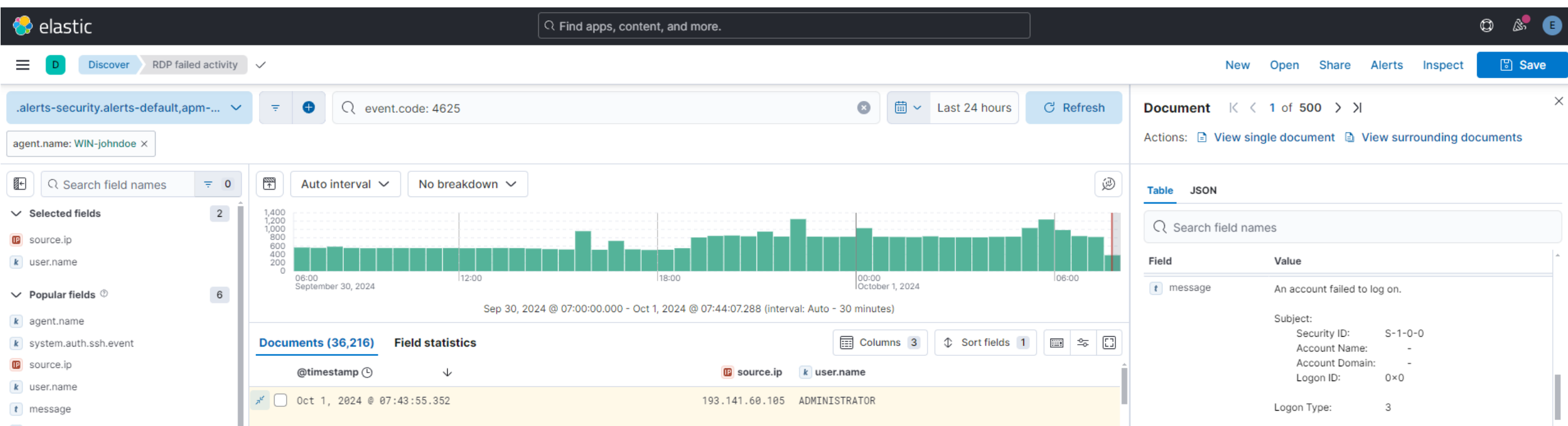
Create Alerts and Dashboards

Salviamo questa ricerca con i campi 'source.ip' e 'user.name' (le possiamo ritrovare cliccando su 'Open').



Create Alerts and Dashboards

Se osserviamo il campo 'Message' vediamo come 'Logon Type' 3. Significa che è un evento di 'network' legato a dei tentativi di autenticazione falliti.



Create Alerts and Dashboards

Creo l'alert come in Day 14 e lo salvo.

Se al momento visualizzo l'alert non avrò molte informazioni.

Elasticsearch query

Alert when matches are found during the latest query run. [Learn more](#)


Select a data view

DATA VIEW .alerts-security.alerts-default,apm-*
transaction*,auditbeat-*,endgame-*,filebeat-*,logs-
,packetbeat-,traces-apm*,winlogbeat-*,-*elastic-
cloud-logs-*

Define your query

agent.name: WIN-johndoe 

Set the group, threshold, and time window 

WHEN count()

OVER all documents

IS ABOVE 5

FOR THE LAST 1 minute

Set the number of documents to send 

SIZE 100


RDP Brute Force Activity - johndoe



|< < 1 of 53 > >|

Overview

Table

Alert Status	active
Feature	 Logs
Last updated	Oct 1, 2024 @ 07:51:57.964
Started	Sep 28, 2024 @ 23:43:44.000
Rule category	Elasticsearch query
Rule	RDP Brute Force Activity - johndoe
Rule tags	—
Evaluation values	—
Evaluation threshold	5
Reason	Document count is 27 in the last 1m in .alerts-security.alerts-default,apm-*-transaction*,auditbeat-*,endgame-*,filebeat-*,logs-*,packetbeat-*,traces-apm*,winlogbeat-*,-*elastic-cloud-logs-* data view. Alert when greater than 5.
Maintenance windows	—

Create Alerts and Dashboards

In 'Security' -> 'Rules' possiamo creare degli alert più precisi, scegliamo 'Detection Rules' -> 'Create New Rule' -> 'Threshold', impostiamo la query nel campo relativo, imposto i required fields, custom highlighted fields, imposto la schedule rule e infine clicco su 'Create & Enable Rule'.

The screenshot shows the 'Index Patterns' tab of an alert configuration interface. It includes a list of index patterns, a custom query field, a group by dropdown, and sections for custom highlighted and required fields.

Index Patterns

apm-*transaction* × auditbeat-* ×

endgame-* × filebeat-* × logs-* ×

packetbeat-* × traces-apm* ×

winlogbeat-* × -*elastic-cloud-logs-* ×

Enter the pattern of Elasticsearch indices where you would like this rule to run. By default, these will include index patterns defined in Security Solution advanced settings.

Custom query [Import query from saved timeline](#)

system.auth.ssh.event: *
and agent.name: "Linux-|
johndoe" and
system.auth.ssh.event:
Failed and user.name:"root"

Group by

All results

Select fields to

Custom highlighted fields Optional

source.ip ×

Required fields ? Optional

source.ip × ip ×

user.name × keyword ×

3 Schedule rule

The screenshot shows the 'Schedule rule' configuration interface. It includes a 'Runs every' section with a dropdown set to 5 minutes, and an 'Additional look-back time' section with a dropdown set to 5 minutes.

Runs every

5 Minut... ▾

Rules run periodically and detect alerts within the specified time frame.

Additional look-back time

5 Minut... ▾

Adds time to the look-back period to prevent missed alerts.

Required Fields: Questi campi servono a fornire un contesto o delle dipendenze per la regola. Anche se non influiscono direttamente sul funzionamento della regola, aiutano a comprendere quali dati sono necessari per il corretto funzionamento. Ad esempio, puoi specificare campi come host.name per garantire che la regola monitori host specifici.

Custom Highlighted Field: Questo campo ti consente di evidenziare un campo specifico all'interno degli avvisi generati dalla regola. È utile per attirare l'attenzione su particolari dettagli rilevanti nel contesto dell'allerta, migliorando la visibilità delle informazioni chiave nel dashboard

Create Alerts and Dashboards

Create le regole le testo effettuando dei tentativi di autenticazione da **Powershell** del mio Pc inserendo delle password errate, come possiamo osservare qui riesco a visualizzare il source ip, da notare che **Elasticsearch** da anche la possibilità di creare una risposta all'attacco tramite EDR.

The screenshot displays the Elastic SIEM interface. At the top, a large purple banner contains the title 'Create Alerts and Dashboards'. Below this, a text box explains the process of creating rules by testing authentication attempts from a PC using PowerShell, noting that Elasticsearch provides the source IP and the ability to create a response via EDR. The main interface shows an alert titled 'SSH Brute Force Attempt - johndoe' with a status of 'Open', a risk score of 21, and no assignees. The alert reason is 'event with source 41.223.231.182 by root created low alert SSH Brute Force Attempt - johndoe'. Below the alert details, there is an 'Investigation' section with a link to the 'Investigation guide'. A large red arrow points from the text box to the alert details. At the bottom, a table lists several alerts, with the first one highlighted in red. The table has columns for Actions, @timestamp, Rule, Assignees, Severity, Risk Score, and Reason.

Actions	@timestamp	Rule	Assignees	Severity	Risk Score	Reason
<input type="checkbox"/> Link Details More	Oct 1, 2024 @ 13:59:10.643	SSH Brute Force Attempt - ...		low	21	event
<input type="checkbox"/> Link Details More	Oct 1, 2024 @ 13:54:07.656	SSH Brute Force Attempt - ...		low	21	event
<input type="checkbox"/> Link Details More	Oct 1, 2024 @ 13:38:58.623	SSH Brute Force Attempt - ...		low	21	event with source 8.218.248.59 by root created low alert SSH Brute Force ...

Highlighted fields:

Field	Value
source.ip	41.223.231.182
user.name	root
kibana.alert.rule.type	threshold
kibana.alert.threshold_result.count	1
kibana.alert.threshold_result.term	root
s.value	41.223.231.182