Importate su Splunk i dati di esempio “tutorialdata.zip”:
● Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.
● Scrivi una query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente “djohnson” e mostrare il timestamp e l'ID utente.
● Scrivi una query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP “86.212.199.60”. La query dovrebbe mostrare il timestamp, il nome utente e il numero di porta.
● Crea una query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.
● Crea una query Splunk per trovare tutti gli Internal Server Error.

Query 1 : ● Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.

```
source="tutorialdata.zip:*" "Failed password"
| rex "^(?<timestamp>.{3} .{3} \d+ \d{4} \d{2}:\d{2}:\d{2}) .+\[(?<error_code>[^]]+)\]: Failed password for(?: invalid user)? (?<username>[^ ]+) from (?<src_ip>[^ ]+) port (?<port>\d+)"
| table timestamp, error_code, username, src_ip, port
```

Questa query è utile per analizzare i log di accesso ai sistemi, in particolare per identificare tentativi di accesso falliti.

timestamp	error_code	username	src_ip	port
Thu Nov 01 2024 04:37:13	5276	appserver	194.8.74.23	3351
Thu Nov 01 2024 04:37:13	4675	local	203.45.206.135	1133
Thu Nov 01 2024 04:37:13	2591	email	203.45.206.135	2262
Thu Nov 01 2024 04:37:13	3250	irc	89.106.20.218	4299
Thu Nov 01 2024 04:37:13	1315	jira	69.175.97.11	4033
Thu Nov 01 2024 04:37:13	5989	sys	212.58.253.71	3031
Thu Nov 01 2024 04:37:13	5023	amanda	109.169.32.135	4272
Thu Nov 01 2024 04:37:13	1773	helpdesk	95.130.170.231	2227
Thu Nov 01 2024 04:37:13	3847	system	183.60.133.18	4291
Thu Nov 01 2024 04:37:13	4628	sys	183.60.133.18	3058
Thu Nov 01 2024 04:37:13	4829	jboss	223.205.219.67	3786
Thu Nov 01 2024 04:37:13	4269	oracle	223.205.219.67	4378
Thu Nov 01 2024 04:37:13	4511	varnish	94.229.0.21	3522
Thu Nov 01 2024 04:37:13	4619	vmware	64.66.0.20	1225
Thu Nov 01 2024 04:37:13	4270	ftp	64.66.0.20	3416
Thu Nov 01 2024 04:37:13	3027	backup	112.111.162.4	1404
Thu Nov 01 2024 04:37:13	2557	backup	112.111.162.4	2527
Thu Nov 01 2024 04:37:13	2536	irc	91.208.184.24	3311
Thu Nov 01 2024 04:37:13	5948	sapadmin	91.208.184.24	2875

Query 2 : ● Scrivi una query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente “djohnson” e mostrare il timestamp e l'ID utente.

```
source="tutorialdata.zip:*" "Accepted password for djohnson"
| rex "Accepted password for (?<username>[^ ]+) from (?<src_ip>[^ ]+) port \d+"
| table _time, username, src_ip
```

Questa query serve a estrarre e visualizzare informazioni sugli accessi riusciti dell'utente "djohnson" dai log, fornendo dettagli su quando e da quale indirizzo IP si è connesso.

_time	username	src_ip
2024-11-01 04:37:13	djohnson	10.3.10.46
2024-11-01 04:37:13	djohnson	10.3.10.46
2024-11-01 04:37:13	djohnson	10.3.10.46
2024-11-01 04:37:13	djohnson	10.3.10.46
2024-11-01 04:37:11	djohnson	10.3.10.46
2024-11-01 04:37:11	djohnson	10.3.10.46
2024-11-01 04:37:11	djohnson	10.3.10.46
2024-11-01 04:37:10	djohnson	10.3.10.46
2024-11-01 04:37:10	djohnson	10.3.10.46
2024-11-01 04:37:10	djohnson	10.3.10.46
2024-11-01 04:37:10	djohnson	10.3.10.46
2024-10-31 04:37:13	djohnson	10.3.10.46
2024-10-31 04:37:13	djohnson	10.3.10.46
2024-10-31 04:37:11	djohnson	10.3.10.46
2024-10-31 04:37:10	djohnson	10.3.10.46
2024-10-31 04:37:10	djohnson	10.3.10.46
2024-10-31 04:37:10	djohnson	10.3.10.46
2024-10-31 04:37:10	djohnson	10.3.10.46
2024-10-30 04:37:13	djohnson	10.3.10.46
2024-10-30 04:37:13	djohnson	10.3.10.46

Query 3 : ● Scrivi una query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP “86.212.199.60”. La query dovrebbe mostrare il timestamp, il nome utente e il numero di porta.

```
source="tutorialdata.zip:*" "from 86.212.199.60"
| rex "Failed password for(?: invalid user)? (?<username>[^ ]+) from (?<hostname>[^ ]+) port (?<port>\d+)"
| table _time, username, port
```

Questa query serve a estrarre e visualizzare informazioni sui tentativi di accesso falliti dall'indirizzo IP specificato, mostrando i dettagli rilevanti come il timestamp, il nome utente e il numero di porta utilizzato.

_time	username	port
2024-10-31 04:37:13	administrator	2959
2024-10-31 04:37:13	gopher	2771
2024-10-31 04:37:11	admin	3673
2024-10-31 04:37:11	mailman	4339
2024-10-30 04:37:13	hammer	1323
2024-10-30 04:37:11	ncsd	4022
2024-10-30 04:37:11	fpass	3420
2024-10-30 04:37:11	root	3683
2024-10-30 04:37:11	mail	3805
2024-10-29 04:37:13	administrator	3447
2024-10-29 04:37:13	harrison	1609
2024-10-29 04:37:13	nobody	3374
2024-10-29 04:37:13	git	3214
2024-10-29 04:37:13	ventrilo	4391
2024-10-29 04:37:13	operator	4720
2024-10-28 04:37:11	mysql	3458
2024-10-26 04:37:13	sunny	4644
2024-10-26 04:37:13	appserver	4979
2024-10-25 04:37:13	nagios	3362
2024-10-25 04:37:13	root	2753

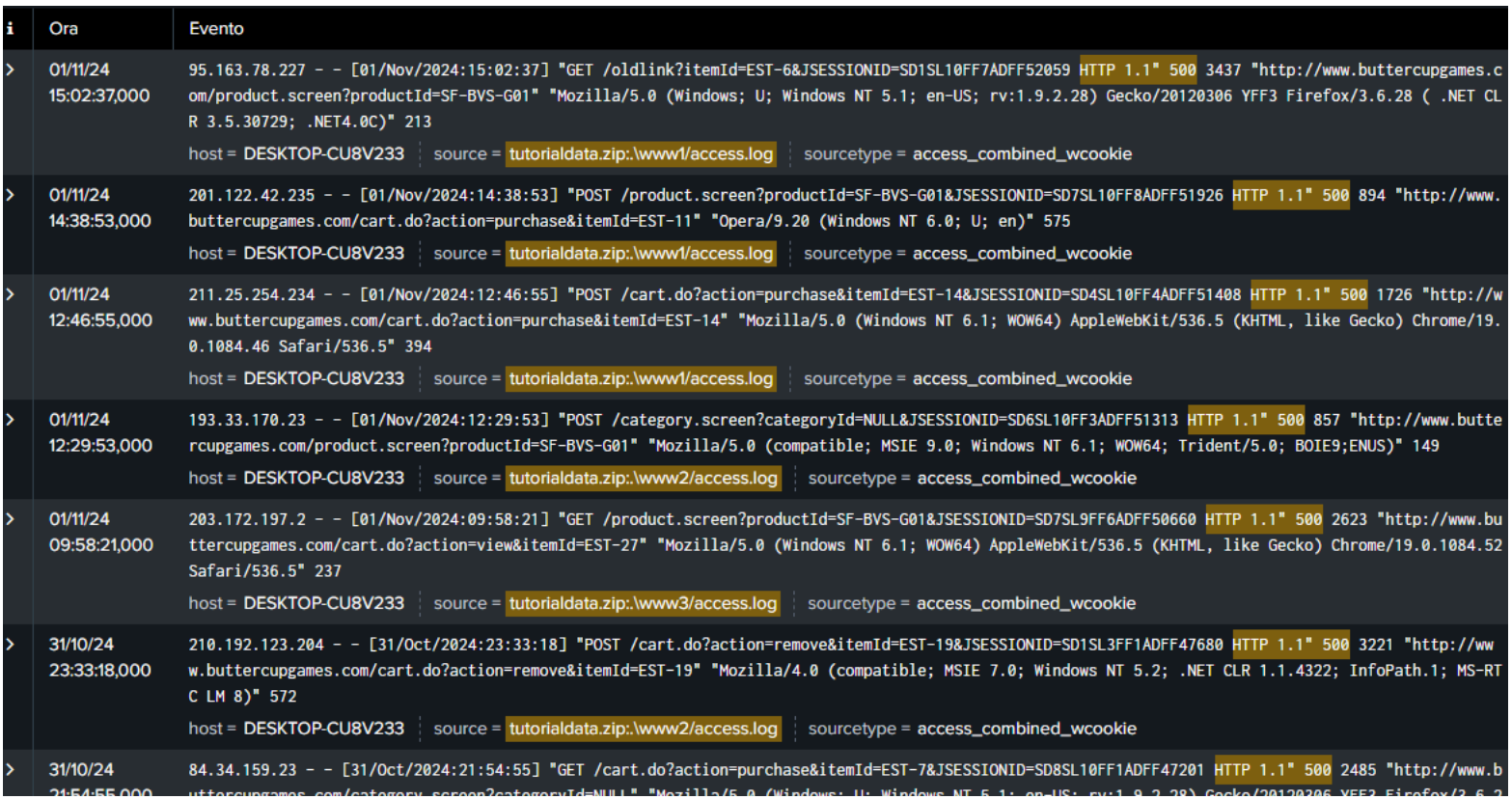
Query 4 : ● Crea una query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.

```
source="tutorialdata.zip:*" "Failed password"
| rex "Failed password for(?: invalid user)? [^ ]+ from (?<src_ip>[^ ]+) port \d+"
| stats count as error_code by src_ip
| where error_code > 5
| table src_ip, error_code
```

107.3.146.207	25
108.65.113.83	33
109.169.32.135	47
110.138.30.229	20
110.159.208.78	15
111.161.27.20	14
112.111.162.4	13
117.21.246.164	27
118.142.68.222	10
12.130.60.4	15
12.130.60.5	14
121.254.179.199	22
121.9.245.177	21
123.118.73.155	10
123.196.113.11	18
123.30.108.208	16
124.160.192.241	21
125.17.14.100	13
125.7.55.180	27
125.89.78.6	23

Query 5 :● Crea una query Splunk per trovare tutti gli Internal Server Error.

source="tutorialdata.zip:*" "HTTP 1.1\" 500"



i	Ora	Evento
>	01/11/24 15:02:37,000	95.163.78.227 - - [01/Nov/2024:15:02:37] "GET /oldlink?itemId=EST-6&JSESSIONID=SD1SL10FF7ADFF52059 HTTP 1.1" 500 3437 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 213 host = DESKTOP-CU8V233 source = tutorialdata.zip:.\www1/access.log sourcetype = access_combined_wcookie
>	01/11/24 14:38:53,000	201.122.42.235 - - [01/Nov/2024:14:38:53] "POST /product.screen?productId=SF-BVS-G01&JSESSIONID=SD7SL10FF8ADFF51926 HTTP 1.1" 500 894 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-11" "Opera/9.20 (Windows NT 6.0; U; en)" 575 host = DESKTOP-CU8V233 source = tutorialdata.zip:.\www1/access.log sourcetype = access_combined_wcookie
>	01/11/24 12:46:55,000	211.25.254.234 - - [01/Nov/2024:12:46:55] "POST /cart.do?action=purchase&itemId=EST-14&JSESSIONID=SD4SL10FF4ADFF51408 HTTP 1.1" 500 1726 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 394 host = DESKTOP-CU8V233 source = tutorialdata.zip:.\www1/access.log sourcetype = access_combined_wcookie
>	01/11/24 12:29:53,000	193.33.170.23 - - [01/Nov/2024:12:29:53] "POST /category.screen?categoryId=NULL&JSESSIONID=SD6SL10FF3ADFF51313 HTTP 1.1" 500 857 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 149 host = DESKTOP-CU8V233 source = tutorialdata.zip:.\www2/access.log sourcetype = access_combined_wcookie
>	01/11/24 09:58:21,000	203.172.197.2 - - [01/Nov/2024:09:58:21] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD7SL9FF6ADFF50660 HTTP 1.1" 500 2623 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-27" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.52 Safari/536.5" 237 host = DESKTOP-CU8V233 source = tutorialdata.zip:.\www3/access.log sourcetype = access_combined_wcookie
>	31/10/24 23:33:18,000	210.192.123.204 - - [31/Oct/2024:23:33:18] "POST /cart.do?action=remove&itemId=EST-19&JSESSIONID=SD1SL3FF1ADFF47680 HTTP 1.1" 500 3221 "http://www.buttercupgames.com/cart.do?action=remove&itemId=EST-19" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 572 host = DESKTOP-CU8V233 source = tutorialdata.zip:.\www2/access.log sourcetype = access_combined_wcookie
>	31/10/24 21:54:55,000	84.34.159.23 - - [31/Oct/2024:21:54:55] "GET /cart.do?action=purchase&itemId=EST-7&JSESSIONID=SD8SL10FF1ADFF47201 HTTP 1.1" 500 2485 "http://www.b

Conclusioni dei Log

Q1 - **Identificazione di Tentativi di Accesso Malintenzionati**:La presenza di numerosi eventi di "Failed password" suggerisce che potrebbero esserci tentativi di accesso non autorizzati al sistema. Analizzando i log, possiamo identificare gli indirizzi IP responsabili di un numero elevato di tentativi di accesso falliti. Questo può indicare un attacco di forza bruta.

Q2 - Gli accessi riusciti (come nel caso dell'utente **djohnson**) possono fornire informazioni preziose sul comportamento degli utenti. Analizzare i tempi e le modalità degli accessi può aiutare a comprendere le abitudini degli utenti e a migliorare l'esperienza complessiva. Ad esempio, se ci sono picchi di accesso in determinati orari, potrebbe essere utile ottimizzare le risorse del server in quei momenti.
Q3 - **Identificazione di Attività Sospette**:Gli accessi falliti provenienti da indirizzi IP specifici, come 86.212.199.60, possono indicare tentativi di attacco di forza bruta. Analizzare la

frequenza dei tentativi di accesso da questo IP e confrontarli con gli accessi riusciti può rivelare potenziali vulnerabilità nel sistema di autenticazione.

Q4 - **Rilevamento di IP Malevoli**:Identificare gli indirizzi IP che effettuano più di 5 tentativi di accesso falliti è fondamentale per la sicurezza del sistema. Potrebbe essere necessario implementare misure di sicurezza come il blocco degli IP sospetti o l'attivazione di un sistema di avviso automatico per tentativi ripetuti di accesso.

Q5 - **Errori Interni del Server**:L'analisi degli errori HTTP 500 suggerisce che ci sono problemi significativi sul server. Questi errori possono derivare da bug nel codice, configurazioni errate o sovraccarico del server. Monitorare la frequenza e il contesto di questi errori può aiutare a identificare la causa principale e migliorare la stabilità dell'applicazione.