

## Splunk 로그 구축 이야기

```
root@ubuntu ~# systemctl enable --now docker
root@ubuntu ~# usermod -aG docker $USER
root@ubuntu ~# docker run -d \
              -p 8000:8000 \
              -e "SPLUNK_START_ARGS=--accept-license" \
              -e "SPLUNK_PASSWORD=password123" \
              --name my-splunk \
              splunk/splunk:latest
```

Docker 로 이미지 설치 중. (서버는 우분투 리눅스)

The screenshot shows the Splunk Enterprise web interface. At the top, there is a browser header with the URL `192.168.16.10:8000/ko-KR/app/launcher/home`. Below the header, the main title is "splunk>enterprise" followed by "앱". On the left, there is a sidebar titled "앱" with several icons and names: "Search & Reporting", "Audit Trail", "Data Management", "Discover Splunk Observability Cloud", "Splunk Secure Gateway", and "Upgrade Readiness App". Above the sidebar, there is a search bar with the placeholder "이름 순으로 앱 검색...". To the right of the sidebar, the main content area has a title "안녕하세요, Administrator". It features tabs for "북마크", "대시보드", "검색 내역", and "최근에 확인한". Under the "북마크" tab, there are sections for "내 북마크(0)", "내 조직과 공유됨(0)", and "Splunk가 권장함(13)". Each section includes a "북마크 추가" button. At the bottom of the main content area, there are two cards: "데이터 추가" and "데이터 하십니다".

접속은 <http://IP:8000> 로그인은 admin/password123

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with 'splunk-enterprise' and various dropdown menus like 'Administrator', '메시지', '설정', etc. Below the navigation is a search bar with the placeholder 'Search & Reporting'. The main area is titled '새로운 검색' (New Search) and contains a search bar with 'error' typed in. To the right of the search bar are buttons for ' 다른 이름으로 저장' (Save As), '테이블 보기 만들기' (Create Table View), and '닫기' (Close). Below the search bar, it says '2개의 이벤트 (25/12/04 8:14:49.000 이전)' and '이벤트 샘플링 없음'. There are tabs for '이벤트 (2)', '페인', '통계', and '시각화'. Under '이벤트 (2)', there are filters for '시간 표시줄 형식' (Time Format) and '축소' (Collapse). The results table has columns for '시간' (Time), '이벤트' (Event), and '상세' (Details). The first event is from 2023-12-04 10:20:00 with host '38f883a7de34', source 'test.log', and sourcetype 'test'. The second event is from 2023-12-04 10:05:00 with host '38f883a7de34', source 'test.log', and sourcetype 'test'. The bottom left shows a sidebar with field filters like '< 필드 숨기기' and '> 모든 필드'.

더미 테스트 로그파일 넣고 데이터 검색해보기

### 본격적인 웹페이지와의 연결

```
root@localhost ~# wget -O splunkforwarder.rpm "https://download.splunk.com/products/universalforwarder/releases/10.0.1/linux/splunkforwarder-10.0.1-c486717c322b.x86_64.rpm" && sudo rpm -i splunkforwarder.rpm
--2025-12-04 19:28:31-- https://download.splunk.com/products/universalforwarder/releases/10.0.1/linux/splunkforwarder-10.0.1-c486717c322b.x86_64.rpm
Resolving download.splunk.com (download.splunk.com)... 18.64.8.116, 18.64.8.61, 18.64.8.106, ...
Connecting to download.splunk.com (download.splunk.com)|18.64.8.116|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 112013432 (107M) [binary/octet-stream]
Saving to: 'splunkforwarder.rpm'

splunkforwarder.rpm          100%[=====] 106.82M  26.8MB/s    in 4.7s
```

웹페이지에 splunk 설치.

```
root@localhost /o/s/bin# sudo ./splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
    * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
Important: splunk will start under systemd as user: splunkfwd
The unit file has been created.
```

Splunk 허용하기.

```
root@localhost /o/s/bin# sudo ./splunk add forward-server 192.168.16.10:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: admin
Password:
Added forwarding to: 192.168.16.10:9997.
```

Splunk 가 설치된 우분투 IP 의 9997번 포트로 포워드

```
root@localhost /o/s/bin# sudo ./splunk add monitor /var/log/httpd/modsec_audit.log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/httpd/modsec_audit.log'.
```

Splunk에 로그파일 등록하기.

다시 우분투 splunk 사이트로 돌아오면

i	시간	이벤트
>	25/12/05 0:27:03.972	[04/Dec/2025:19:27:03.972137 --0500] aTIm1wuv4XbN4j7k9UvKCwAAAnC 192.168.16.33 50090 192.168.16.28 443 --eba9be4e-B-- GET /api/notifications/unread?userId=65d8a971-c994-11f0-8f78-d9293fc2110e HTTP/1.1 Host: jangbogo.com Connection: keep-alive 25개 행 모두 표시 
>	25/12/05 0:27:03.966	Stopwatch2: 1764894423966154 6012; combined=5213, p1=2763, p2=2209, p3=40, p4=100, p5=101, sr=808, sw=0, l=0, gc=0 Response-Body-Transformed: Dechunked

로키 리눅스(웹페이지 구축된 머신)의 로그를 볼 수 있음.

_time	src_ip	attack_msg	target_uri	rule_id
2025/12/05 00:49:35.875	192.168.16.33	Method is not allowed by policy	/api/notifications/30d4a59c-cfdc-11f0-9046-db336b7e389d	911100
2025/12/05 00:49:35.713	192.168.16.33	Method is not allowed by policy	/api/notifications/a64bed6d-cfe1-11f0-9046-db336b7e389d	911100
2025/12/05 00:49:35.501	192.168.16.33	Method is not allowed by policy	/api/notifications/6697c310-d013-11f0-9046-e24ee180dac5	911100
2025/12/05 00:49:35.146	192.168.16.33	Method is not allowed by policy	/api/products/332b772f-471b-43da-ae9a-3ef59df79713	911100
2025/12/05 00:49:30.352	192.168.16.33	Method is not allowed by policy		

실시간으로  
차단되는 유  
형이 어떤건  
지 확인해보  
기.

```

source="*modsec*"
| rex field=_raw "client (?<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})"
| rex field=_raw "\[msg \"(?<attack_msg>[^"]+)\"]"
| rex field=_raw "\[uri \"(?<target_uri>[^"]+)\"]"
| rex field=_raw "\[id \"(?<rule_id>\d+)\"]"
| search attack_msg!="Inbound Anomaly Score Exceeded"
| table _time, src_ip, attack_msg, target_uri, rule_id
| sort -_time

```

## 이건 필터링

이벤트	패턴	통계 (8)	시각화
표시: 페이지당 20개 ▾ 형식 ▾			
_time	src_ip	attack_msg	target_uri
2025/12/05 05:32:17.547		IDOR Attack Detected (Script/No Referer)	/api/reviews/8bafbbb0-ca75-11f0-8fee-da2f582fe1dc
2025/12/05 05:15:47.039		CSRF Attack Detected (No Valid Headers)	/api/users/update-bio-form
2025/12/05 05:15:03.658		CSRF Attack Detected (No Valid Headers)	/api/users/update-bio-form
2025/12/05 03:34:47.531	192.168.16.33	XSS Attack Detected in Chat Message	/api/chat/message
2025/12/05 03:34:47.387	192.168.16.33	XSS Attack Detected in Chat Message	/api/chat/message
2025/12/05 03:34:47.228	192.168.16.33	XSS Attack Detected in Chat Message	/api/chat/message
2025/12/05 03:34:45.836	192.168.16.33	XSS Attack Detected in Chat Message	/api/chat/message
2025/12/05 03:34:31.556	192.168.16.33	XSS Event Handler detected	/api/reviews

실제 공격들을 작성 후 로그로 실시간 쌓이는 것을 볼 수 있음.