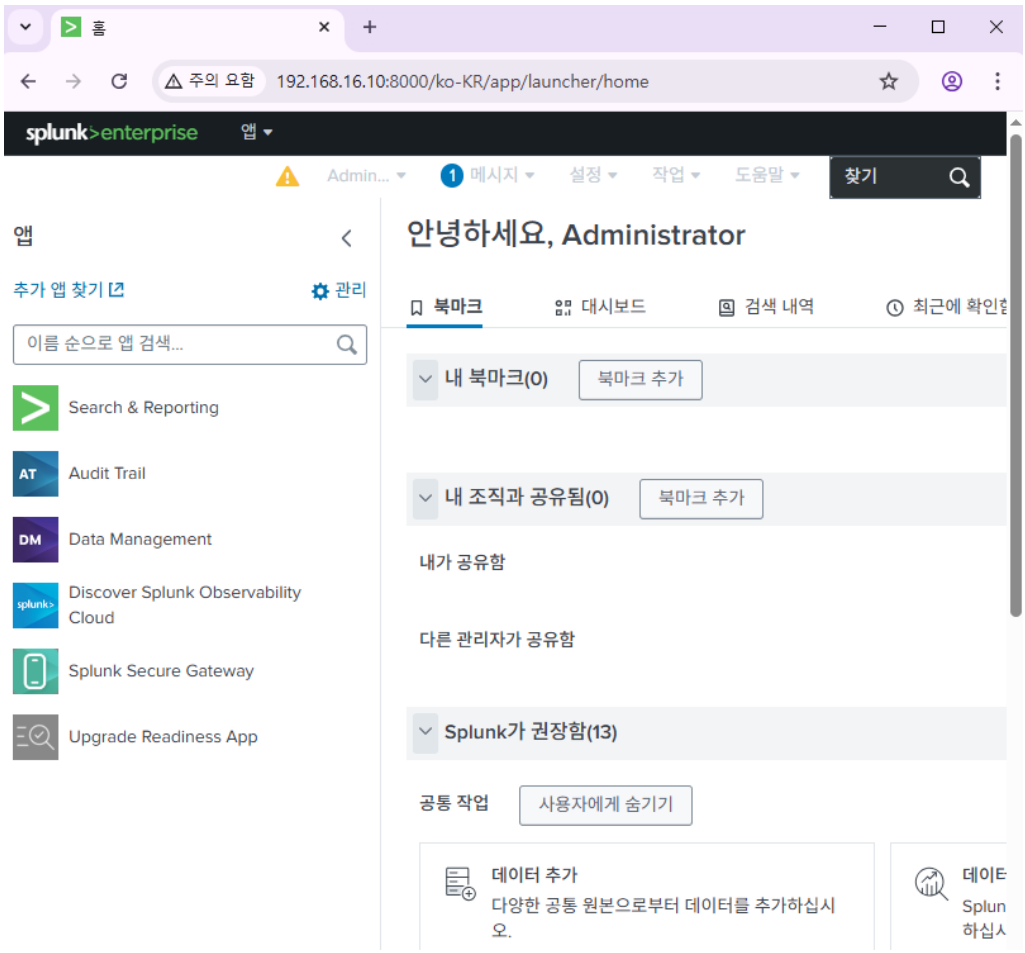
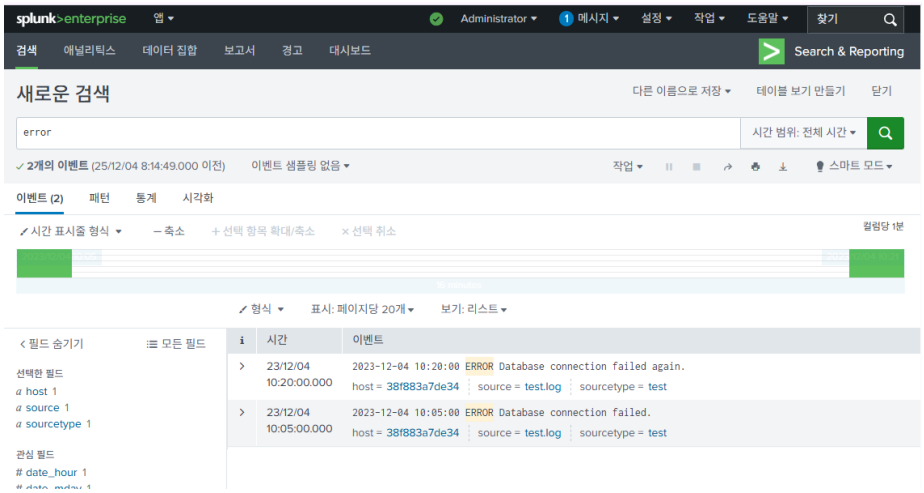
Splunk 로그 구축 이야기

```
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)



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



더미 테스트 로그파일 넣고 데이터 검색해보기

본격적인 웹페이지와의 연결

```
root@localhost ~# wget -O splunkforwarder.rpm "https://download.splunk.com/products/universalforwarde
r/releases/10.0.1/linux/splunkforwarder-10.0.1-c486717c322b.x86_64.rpm" && sudo rpm -i splunkforwarde
r.rpm
--2025-12-04 19:28:31--  https://download.splunk.com/products/universalforwarder/releases/10.0.1/linu
x/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.

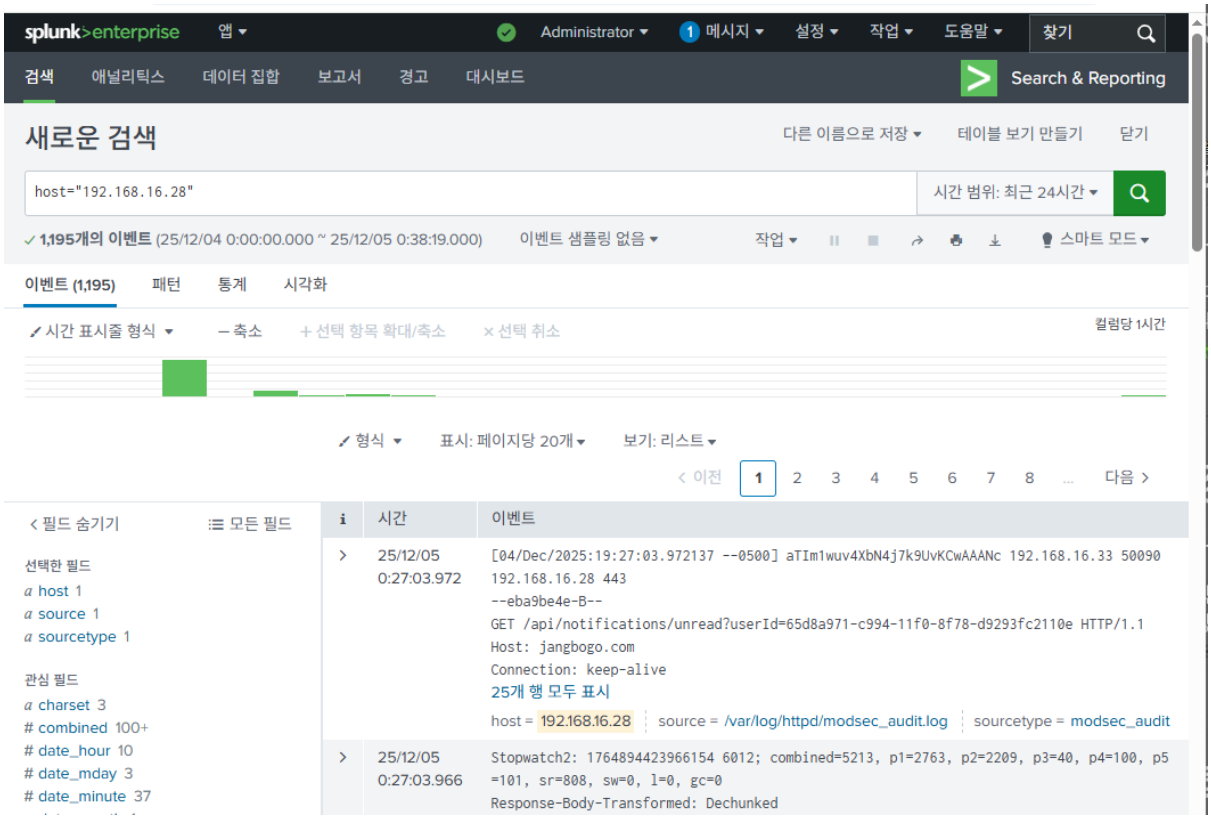
```
root@localhost /o/s/bin# sudo ./splunk add forward-server 192.168.16.10:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: admin
Password:
Added forwarding to: 192.168.16.10:9997.
```

Splunk 가 설치된 우분투 IP 의 9997번 포트로 포워드

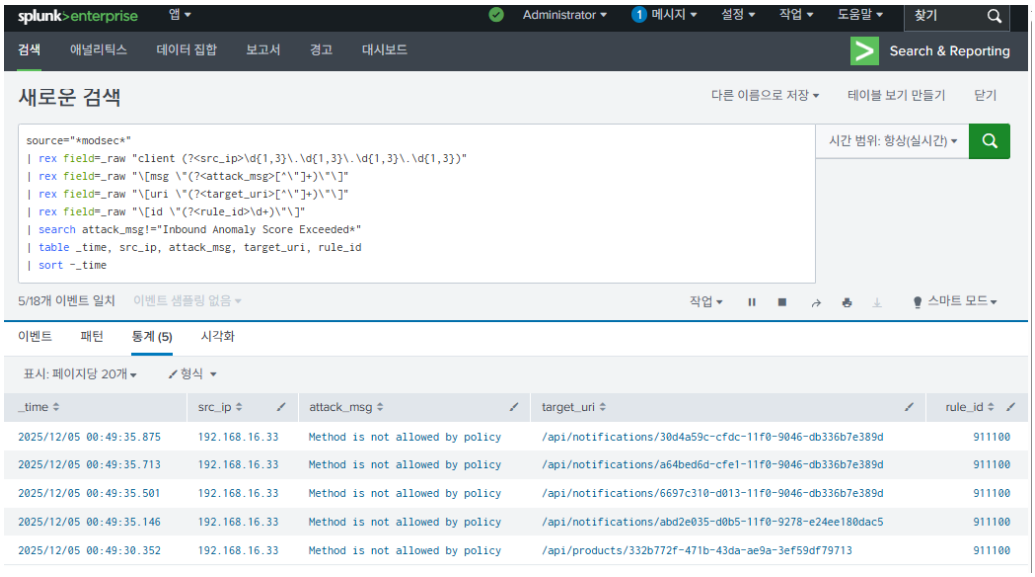
```
root@localhost /o/s/bin# sudo ./splunk add monitor /var/log/httpd/modsec_audit.log
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/httpd/modsec_audit.log'.
```

Splunk 에 로그파일 등록하기.

다시 우분투 splunk 사이트로 돌아오면



로키 리눅스(웹페이지 구축된 머신) 의 로그를 볼 수 있음.



실시간으로 차단되는 유형이 어떤건지 확인해보기.

```
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 공격들 룰 작성 후 로그로 실시간 쌓이는 것을 볼 수 있음.