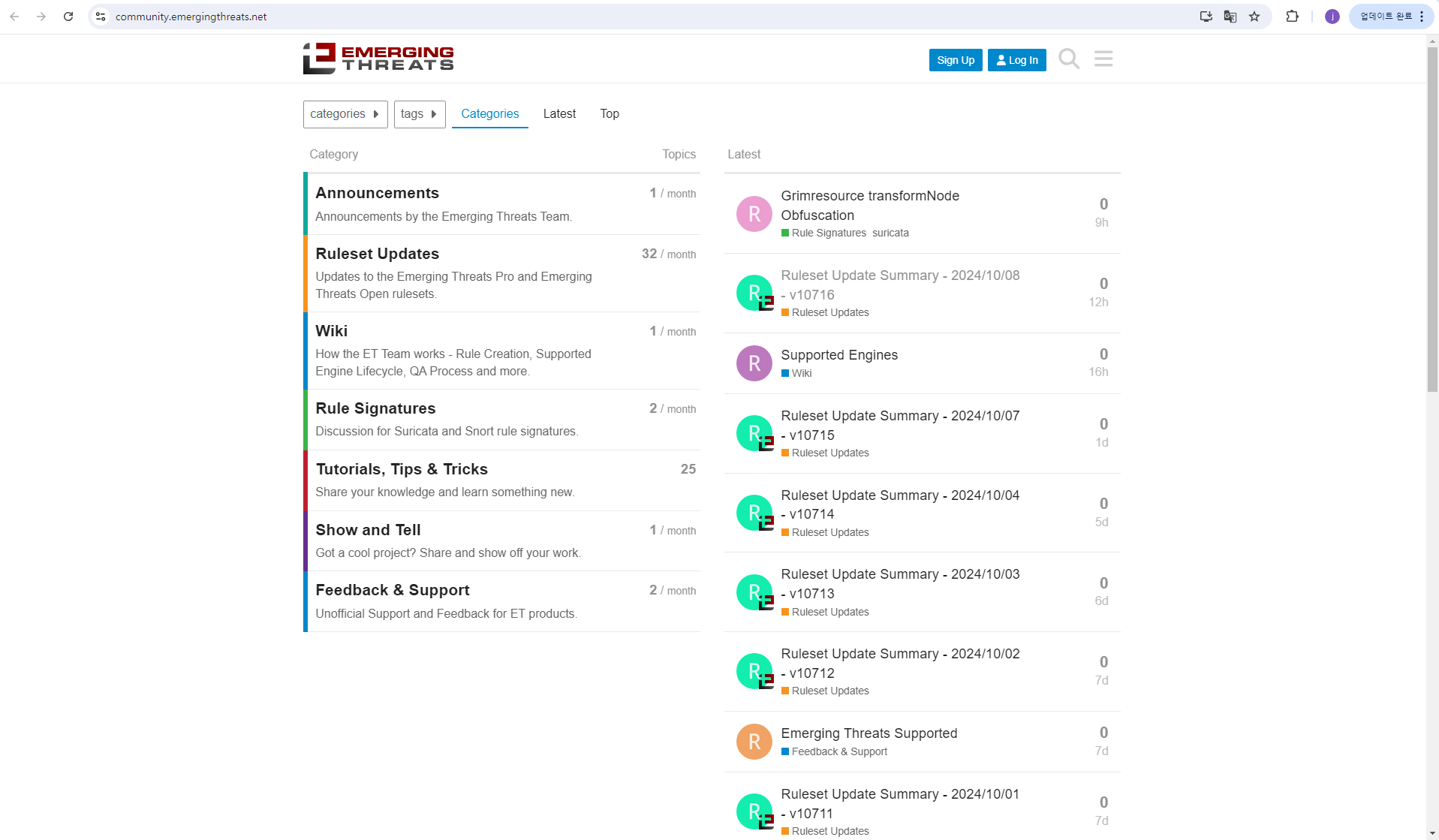
# 수리카타(Suricata) Rules

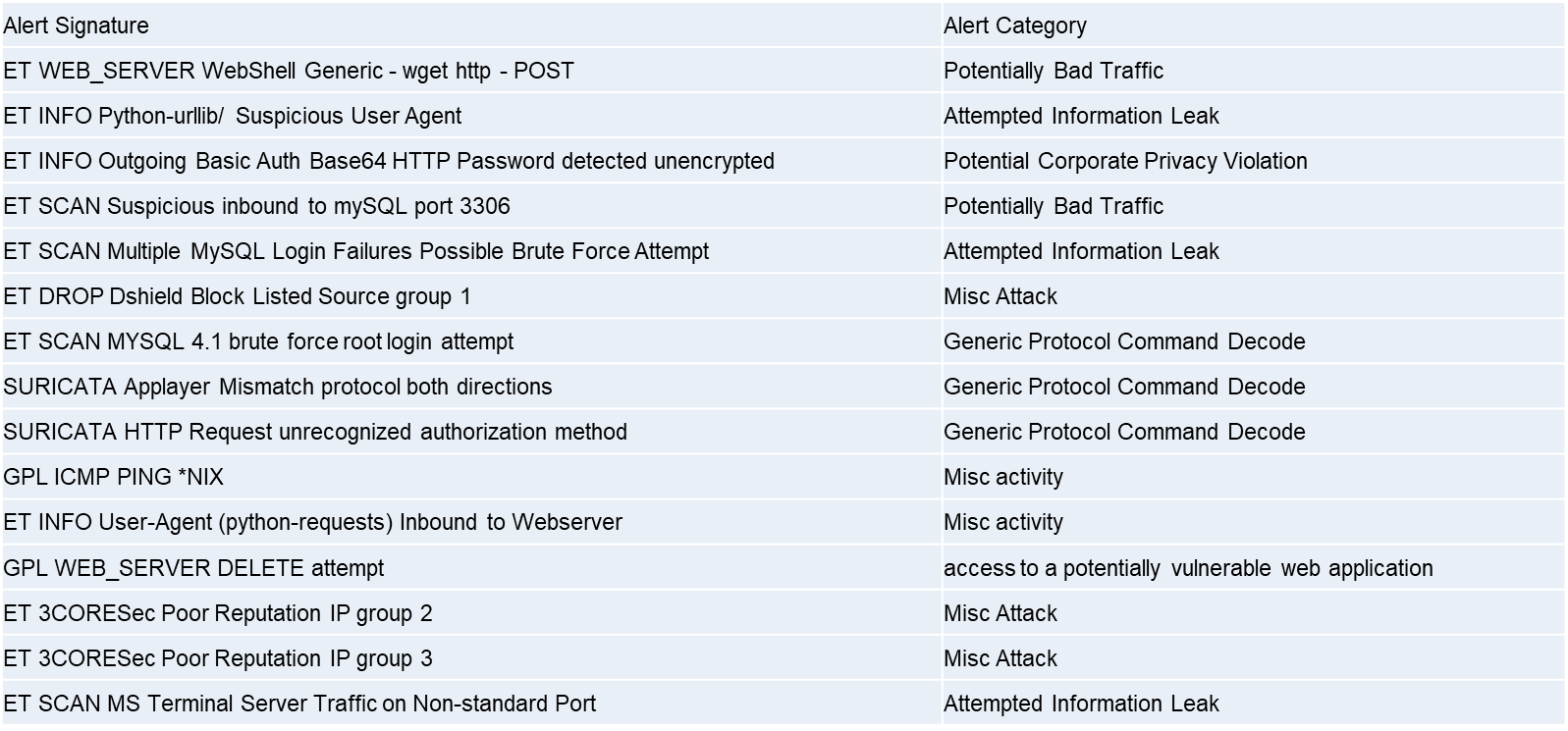
초기 설정되어 있는 2천여개의 Rules 과 Emerging Threats 커뮤니티를 통한 최신의 업데이트 된 중요한 5만여개의 Rules 을 포함하여 수리카타를 운영한다.

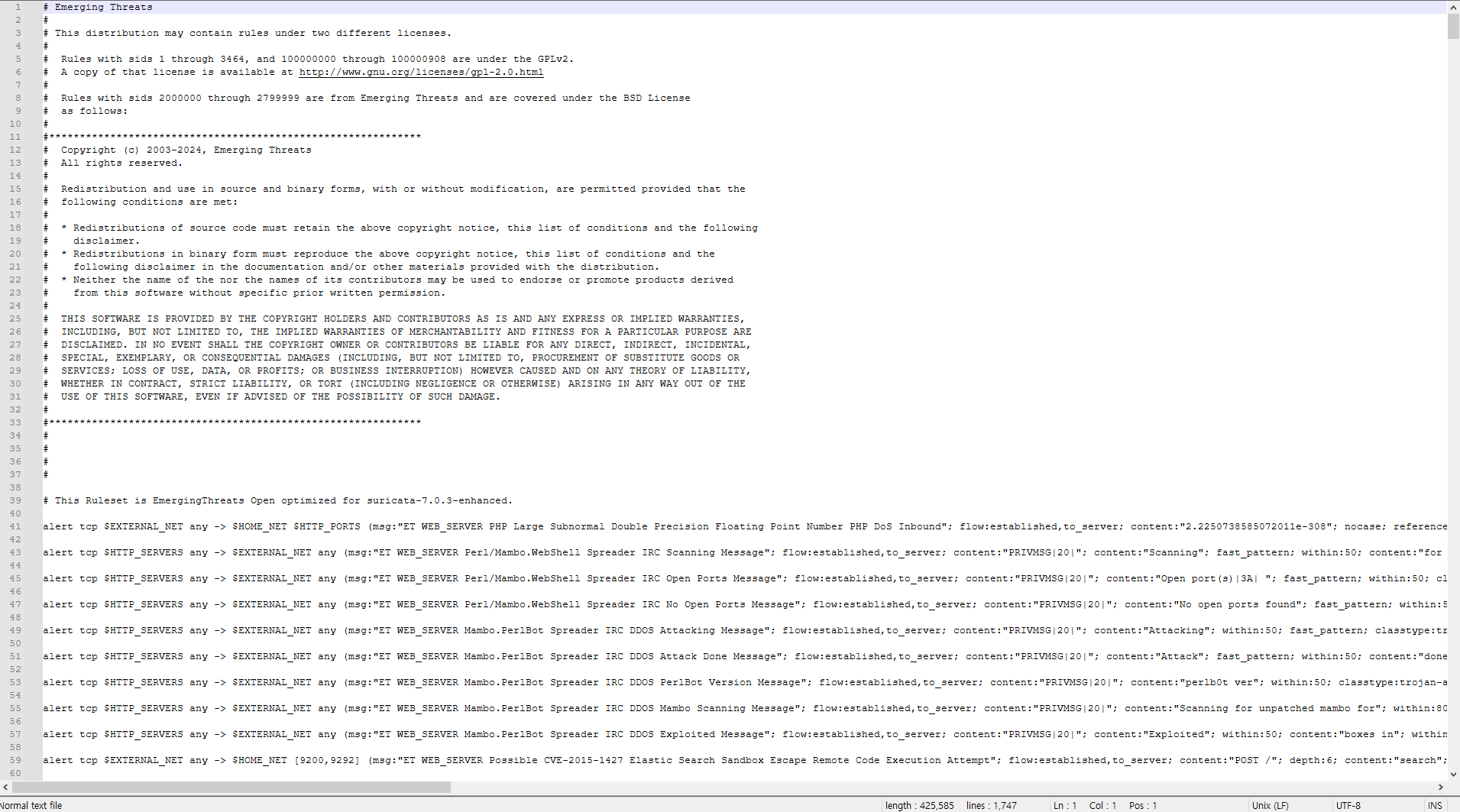
사용자가 직접 Rule을 추가하여 원하는 네트워크 트래픽만 탐지도 가능하다.

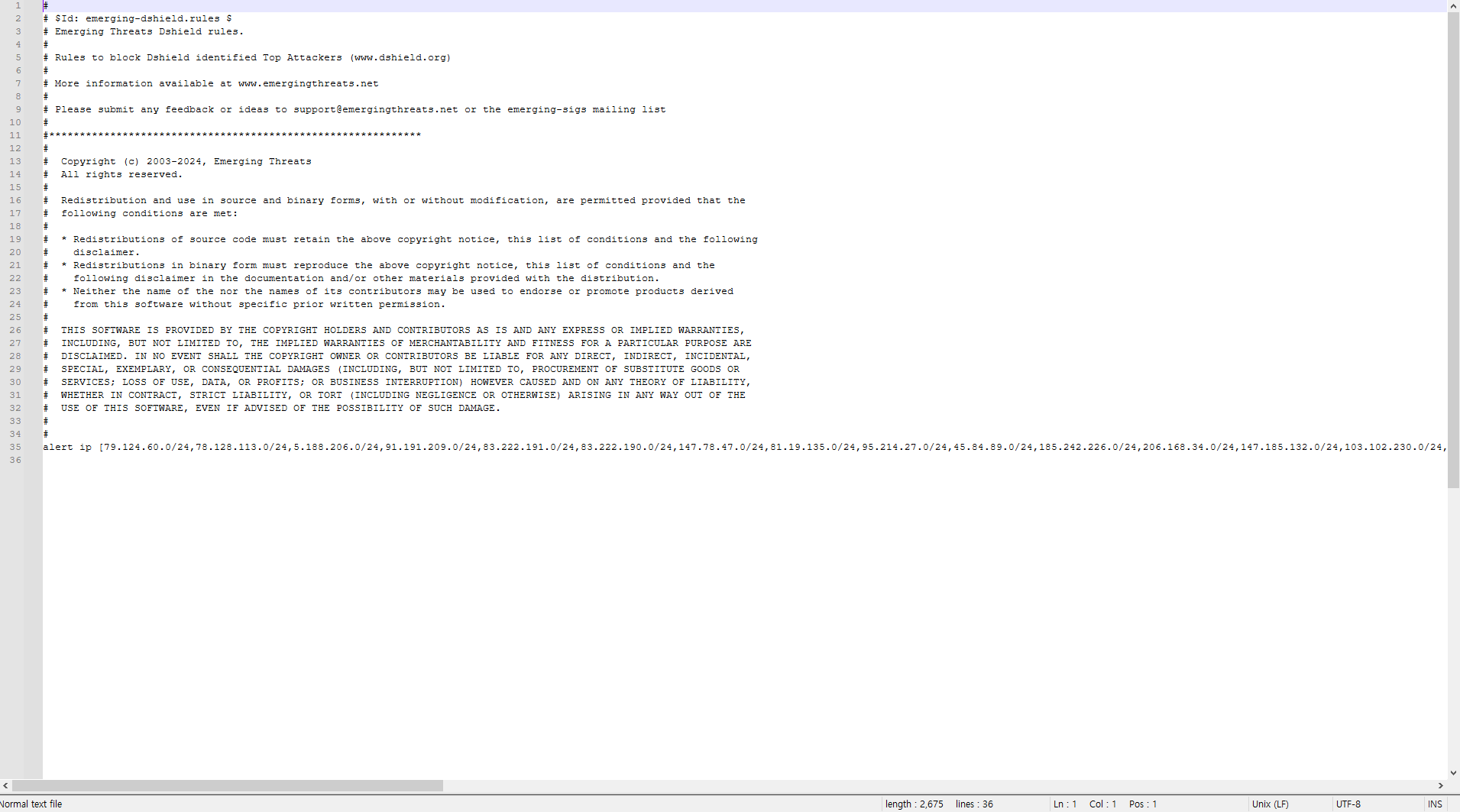
# Emerging Threats

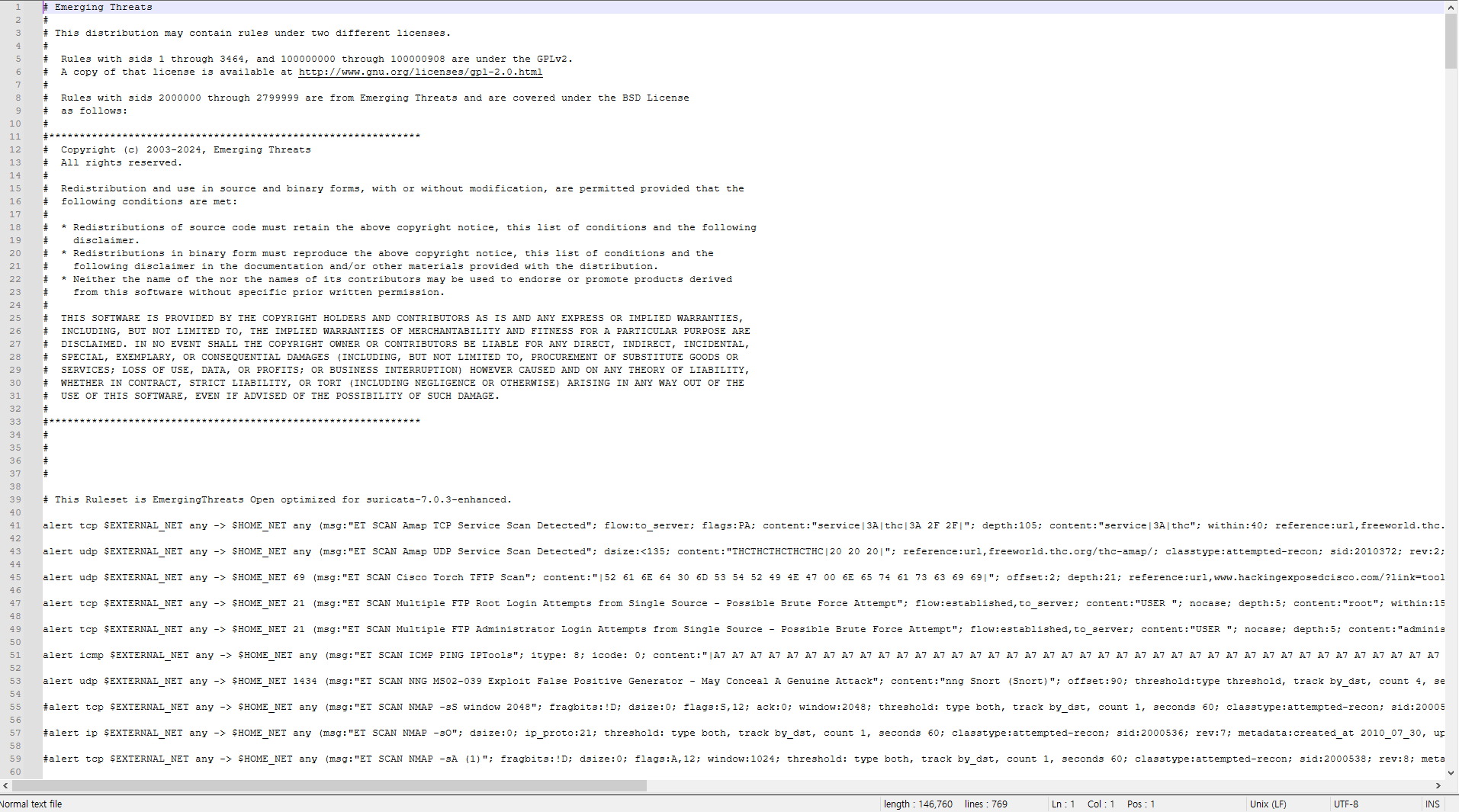


# 주요한 웹서버 Alerts 로그



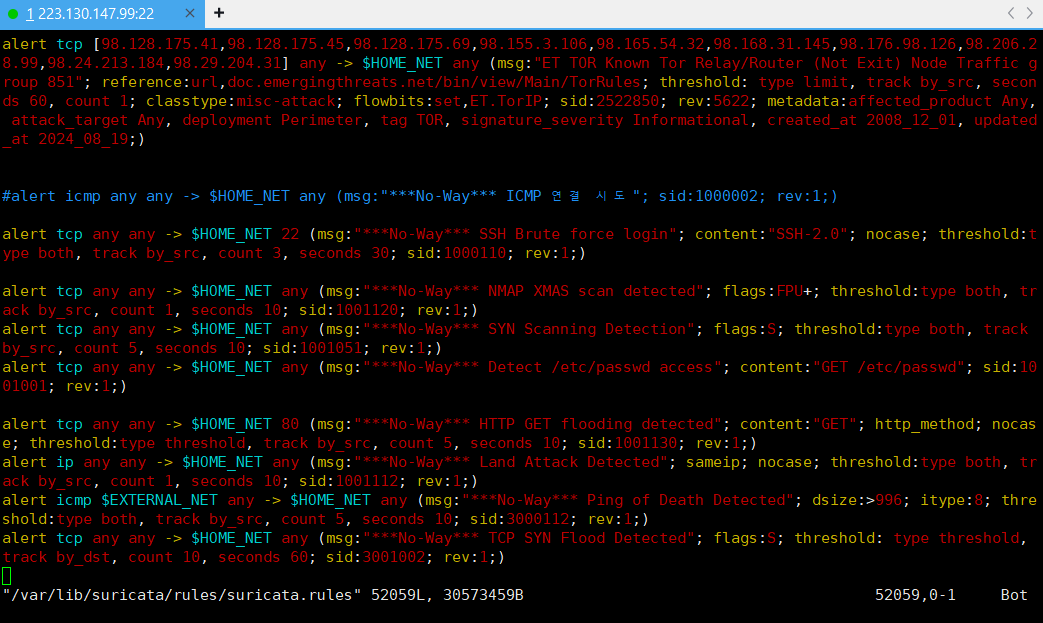






# 수리카타(Suricata) 이벤트 구현

네이버 클라우드에서 IDS 모드로 운영중인 수리카타를 활용하여 여러가지 이벤트를 구현해 보고 관련된 로그들을 분석해 본다.



1 지속적인 로그인 시도 : Credential Stuffing 공격 / 무차별 대입 공격

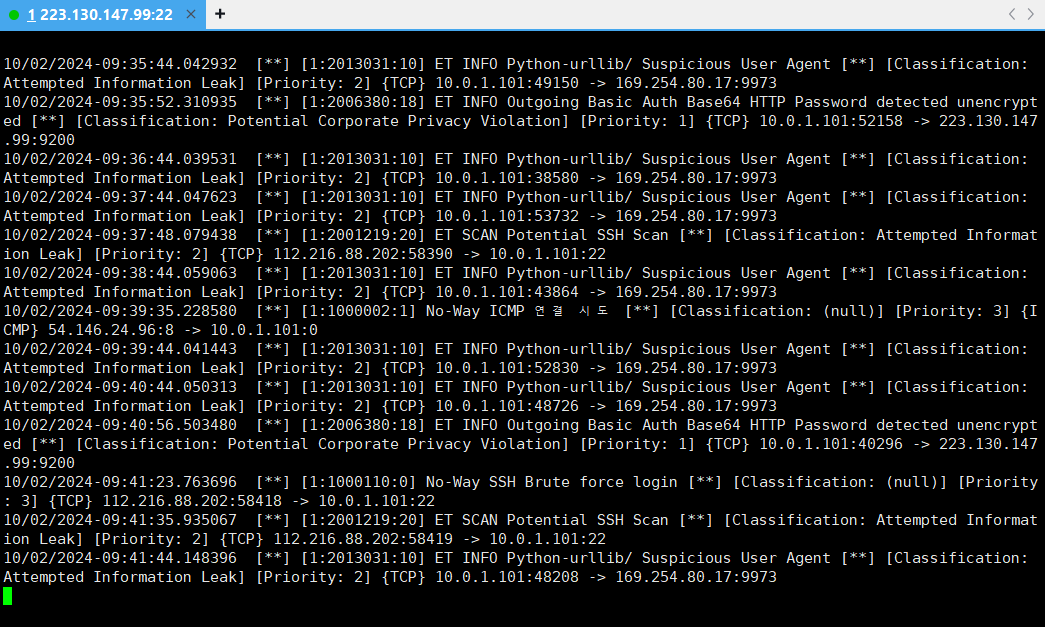
# 다량의 SSH 접속 요청

> 규칙 :

alert tcp any any -> $HOME\_NET 22 (msg:"No-Way SSH Brute force login"; content:"SSH-2.0"; nocase; threshold:type both, track by\_src, count 3, seconds 30; sid:3000110; rev:1;)

> 테스트 : ssh root@223.130.147.99 지속적인 로그인 시도

> Suricata Alert 로그



2 네트워크 스캔 : 포트 스캐닝

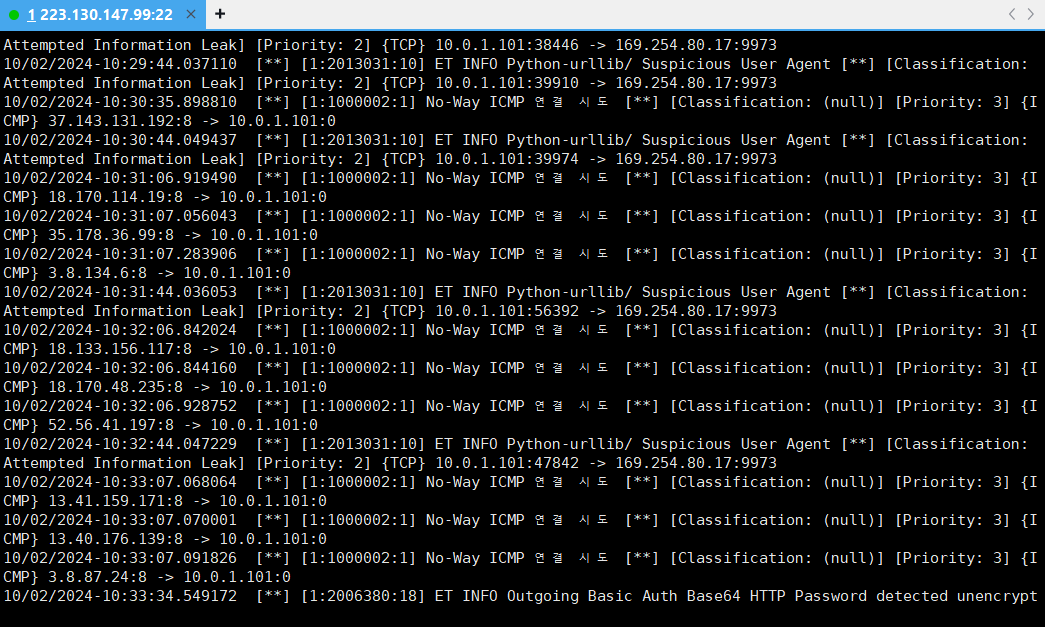
# ICMP Ping Sweep Detection

> 규칙 :

alert icmp $EXTERNAL\_NET any -> $HOME\_NET any (msg:"ICMP Ping Sweep Detected"; dsize:0; itype:8;)

> 테스트 : ping 223.130.147.99

> Suricata Alert 로그



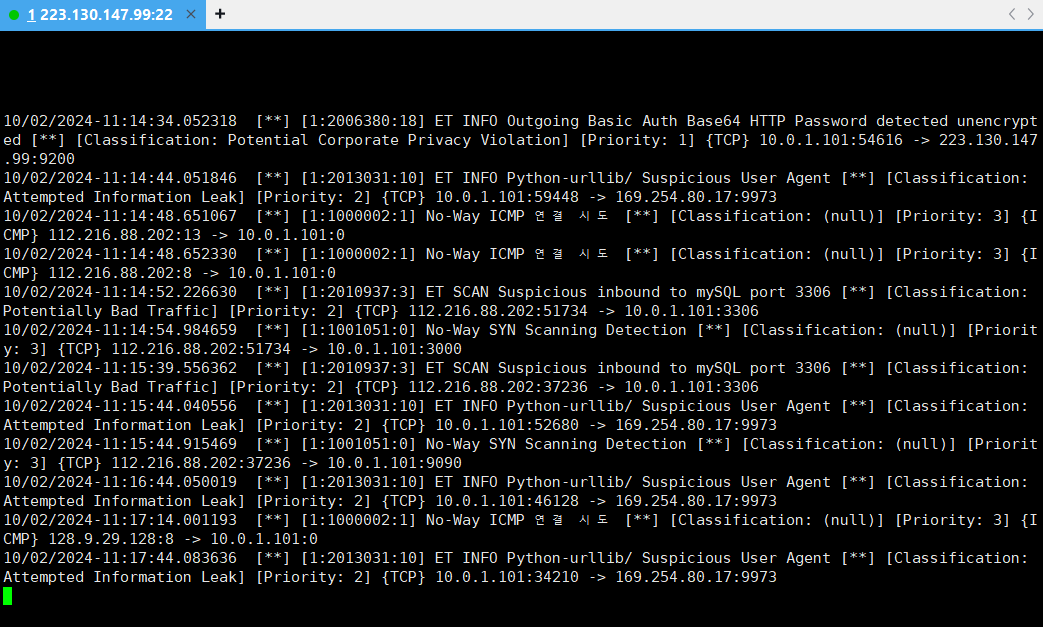
# Nmap Scan : 포트 스캐닝

> 규칙 :

alert tcp any any -> $HOME\_NET any (msg:"No-Way SYN Scanning Detection"; flags:S; threshold:type both, track by\_src, count 5, seconds 10; sid:3,000,051; rev:1;)

> 테스트 : nmap -sS 223.130.147.99

> Suricata Alert 로그



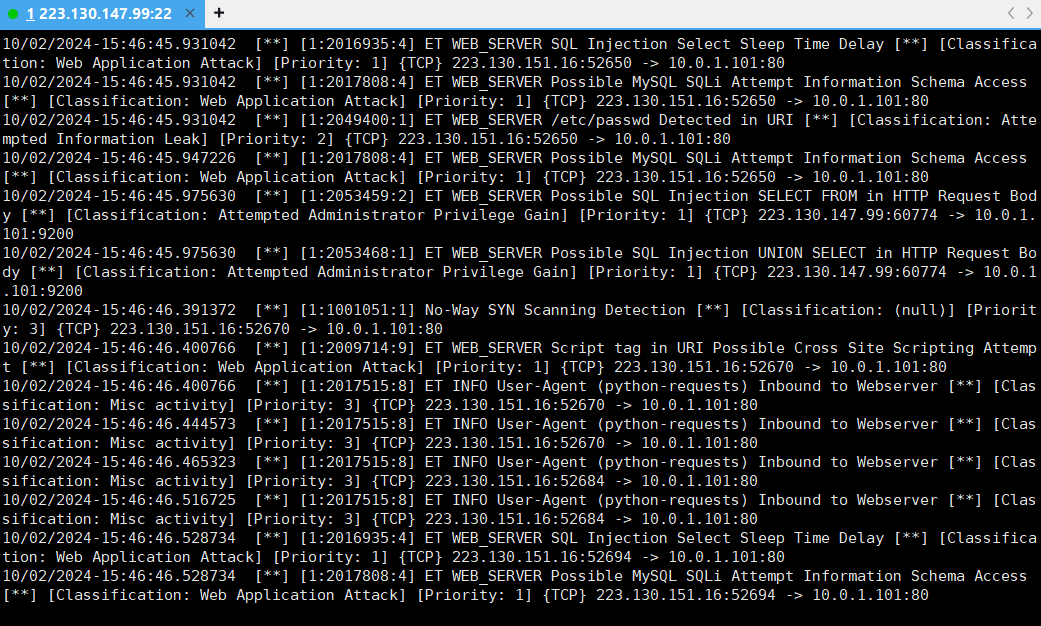
# Web Attack

> 규칙 :

alert tcp any any -> $HOME\_NET 80 (msg:"No-Way Web Attack"; content:"GET /cmd.exe"; nocase; sid:3001012; rev:1;)

> 테스트 : wafw00f http://223.130.147.99/

> Suricata Alert 로그 : 다량의 기본 Rules 검출



3 비정상 패킷 탐지 : Dos / DDoS 공격 등

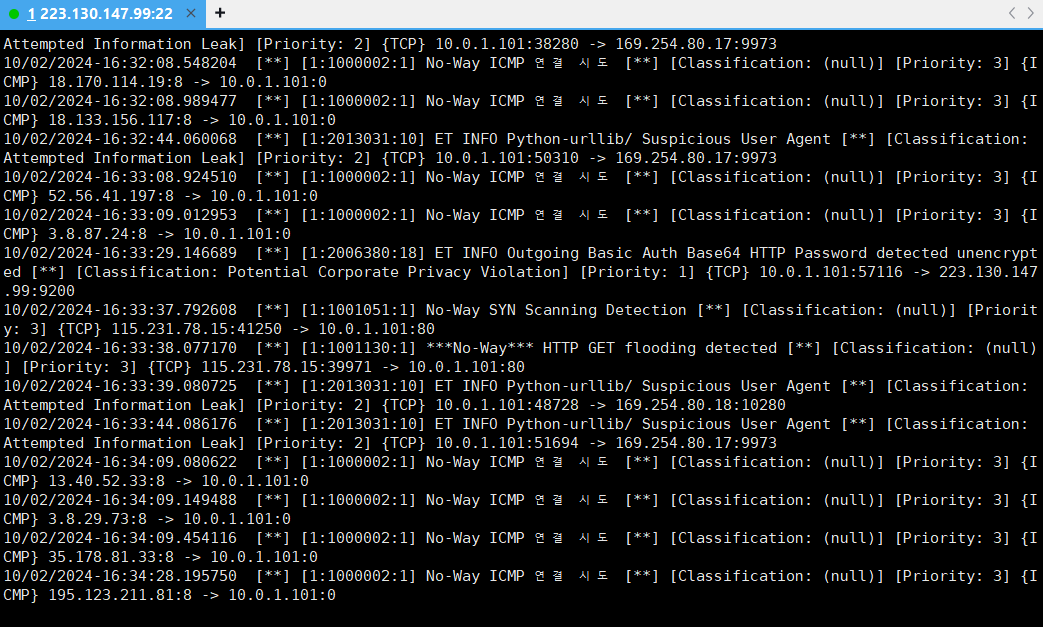
# HTTP Get Flooding

> 규칙 :

alert tcp any any -> any 80 (msg:"\*\*\*No-Way\*\*\* HTTP GET flooding detected"; content:"GET"; http\_method; nocase; threshold:type threshold, track by\_src, count 5, seconds 10; sid:3001130; rev:1;)

> 테스트 : hping3 223.130.147.99 -p 80 -c 10 --fast

> Suricata Alert 로그 : 테스트 로그x, IDS 모드 검출



# 기능 명세서





# 워크플로우

