### node-feed

node-feed 명령어는 수집노드에서 분석 노드와 동기화된 위협 인텔리전스 데이터를 조회합니다. node-feed 명령어는 수집 노드에서만 사용 가능합니다.

node-feed 명령은 SNR #1118 2019-08-01\_18-34 버전부터 사용 가능합니다.

#### 문법

node-feed name=[otx|tor|mdl\_ip|mdl\_domain|malc0de|abusech]

필수 매개변수

**name**

위협 인텔리전스 피드 식별자. otx, tor, mdl\_ip, mdl\_domain, malc0de, abusech 중 선택

#### 설명

피드 식별자는 [matchfeed](https://docs.logpresso.com/ko/query/matchfeed-command) 명령어 설명에 있는 피드 식별자를 참조하십시오.

|  |  |  |  |
| --- | --- | --- | --- |
| 이름 | 유형 | 이름 | 설명 |
| otx | IP 주소 | OTX 피드 | OTX (Open Threat Exchange) 피드를 이용하여 IP 주소 평판 정보를 실시간 대조합니다. |
| tor | IP 주소 | TOR 프록시 | EXIT 라우터 IP 주소를 대조하여 TOR 프록시를 통해 접속하는 IP 주소를 실시간으로 탐지합니다. |
| mdl\_domain | 도메인 | 멀웨어 도메인리스트 | 랜섬웨어 등 악성코드 도메인 피드를 대조하여 내부에서 C&C 도메인으로 접속하면 실시간 탐지합니다. |
| mdl\_ip | IP 주소 | 악성코드 IP 주소 목록 | 랜섬웨어 등 악성코드 IP 피드를 대조하여 내부에서 C&C IP 주소로 접속하면 실시간 탐지합니다. |
| abusech | 도메인 | Abuse.ch | 랜섬웨어가 접속하는 도메인을 실시간으로 탐지합니다. |
| malc0de | MD5 | malc0de | malc0de.com 악성코드 MD5 데이터베이스를 대조하여 악성 바이너리를 탐지합니다. |

#### 사용 예

수집 서버에서 동기화된 OTX 피드 조회

node-feed name=otx

수집 서버에서 동기화된 멀웨어 IP 리스트 조회

node-feed name=mdl\_ip