### SNR#1552 앱 인텔리전스 지원 체계 추가

아래의 기능을 추가했습니다.

* 위협 인텔리전스 피드 저장 방식 변경 및 확장 기능 추가
* matchfeed, node-feed 커맨드 type 옵션 추가
* matchioc() 함수 추가
* 실시간 시나리오 템플릿 추가/변경
* CLI 명령어 추가
* sonar.resetThreatFeed
* sonar.resetNodeSyncStatus
* CLI 명령어 제거
* sonar.isacKey
* sonar.setIsacKey

#### 위협 인텔리전스 피드 확장 기능 추가

앱 설치를 통해 위협 인텔리전스 피드를 확장하는 기능을 추가했습니다. 이에 따라 다양한 데이터 스키마를 수용할 수 있도록 위협 인텔리전스 피드를 로그프레소 테이블에 저장합니다. 마이그레이션 시, **기존 마리아DB의 위협 인텔리전스 피드 테이블이 삭제**됩니다.

위협 인텔리전스 피드 확장 기능을 포함한 앱을 설치하면, sonar\_ioc\_ 접두어로 시작하는 로그프레소 테이블을 생성하고 피드 데이터를 저장합니다.

#### matchfeed, node-feed 커맨드 type 옵션 추가

matchfeed, node-feed 커맨드에 type 옵션을 추가했습니다. name 옵션과 type 옵션을 함께 사용하는 경우, type 옵션이 무시됩니다.

matchfeed [fields=대상필드목록] [invert=t|f] [name=피드이름] [type=피드타입]

**사용 예**

* matchfeed fields=src\_ip name=otx
* src\_ip 필드 값을 **otx 피드**와 매칭
* matchfeed fields=src\_ip type=ip
* src\_ip 필드 값을 **모든 IP 타입의 피드**와 매칭

node-feed [name=피드이름] [type=피드타입]

**사용 예**

* node-feed name=otx
* 쿼리를 실행하는 노드에 동기화된 **otx 피드** 데이터 조회
* node-feed type=ip
* 쿼리를 실행하는 노드에 동기화된 **모든 IP 타입의 피드** 데이터 조회

#### matchioc() 함수 추가

특정 침해지표 유형의 모든 피드에서 값을 검색하는 함수를 추가했습니다.

matchioc(FEED\_TYPE, EXPR)

**반환 값**

FEED\_TYPE 타입의 피드 중에서 EXPR 값이 검색되면 true, 검색되지 않으면 false

#### 실시간 시나리오 템플릿 추가 및 변경

실시간 시나리오 템플릿을 추가 및 변경했습니다. 항목은 아래와 같습니다.

* 추가
* IP 주소가 평판 DB에 포함
* MD5가 특정 평판 DB에 포함
* URL이 평판 DB에 포함
* URL이 특정 평판 DB에 포함
* 변경
* PE 블랙리스트에 포함 -> 대상 해시값과 일치
* PE 평판 DB에 포함 -> MD5가 평판 DB에 포함
* IP 주소가 IP 평판 DB에 포함 -> IP 주소가 특정 평판 DB에 포함

#### CLI 명령어 추가

모든 노드의 위협 인텔리전스 피드 동기화 상태를 초기화하는 CLI 명령어와 특정 노드의 피드 동기화 상태를 초기화하는 CLI 명령어를 추가했습니다.

sonar.resetThreatFeed 피드이름 수집기준날짜 [수집기준ID]

* 모든 노드에서 지정된 위협 인텔리전스 피드의 모든 데이터를 삭제하고 입력한 기준 날짜부터 다시 수집합니다.
* 예시: sonar.resetThreatFeed otx 20180101
* otx 피드 데이터를 초기화하고 2018-01-01부터 수집하도록 기준 날짜를 재설정합니다.

sonar.resetNodeSyncStatus 피드이름 노드GUID 동기화기준날짜 [동기화기준ID]

* 특정 노드에 동기화된 위협 인텔리전스 피드 데이터를 삭제하고 입력한 기준 날짜부터 다시 수집합니다.
* 예시: sonar.resetNodeSyncStatus malc0de abc8777c-c6de-4949-bec4-f31a63ee5ffc 20170818
* 지정된 노드에 동기화된 malc0de 피드의 모든 데이터를 삭제하고 2017-08-18부터 수집하도록 동기화 기준 날짜를 재설정합니다.

#### CLI 명령어 제거

ISAC 키 등록 및 조회 CLI 명령어가 대체되었습니다.

* sonar.isacKey 대신 sonar.globalOptions isac\_api\_key 명령을 사용하세요.
* sonar.setIsacKey ISAC\_API\_KEY 대신 sonar.setGlobalOptions isac\_api\_key ISAC\_API\_KEY 명령을 사용하세요.