IBM Security

IBM Security Software

QRADAR DATA STORE

IBM

보안 빅데이터 시스템 구축 및 컴플라이언스 대응

QRadar Data Store 유즈케이스

**컴플라이언스 준수 목적 모든 로그 보관,
기존 구축 비용 대비 50% 비용 감소**

**실시간 모든 로그 저장으로
선도적인 보안 위협 사냥 수행
(Threat Hunting)**

**앱을 통한 SIEM 기능 확장 및 왓슨
놀리지(Watson's knowledge)
기능 확대**

QRadar Data Store 설명

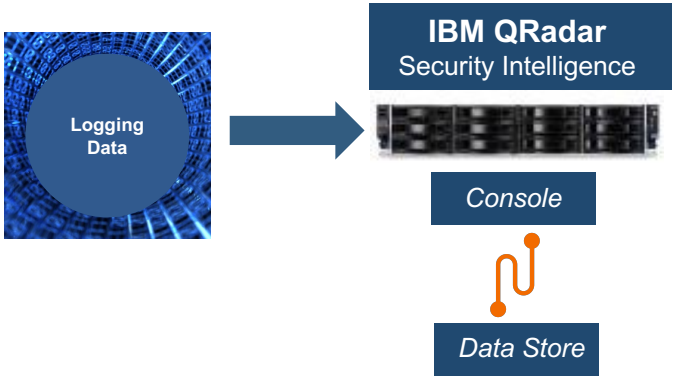
- **필수 사항**
  - QRadar 7.3.1 버전 또는 그 이상의 상위 버전 설치
  - 7.3.1 버전 이상 제품을 사용하고 있는 경우 Data Store 기능을 활성화 하고, 기존 인프라 변경 없이 필요한 라이센스 추가 후 사용 가능

- **라이센스 구매**
  - 대용량 로그를 보관할 하드웨어 또는 가상 시스템 한대 당 1개 “Connection” 라이센스 적용
  - 대용량 로그 보관 시스템: QRadar All-in-One appliance, Event Processor, Data Node
  - 필요 용량에 따라 시스템 확장 지원

- **지원 사항**
  - 로그 수집 및 로그 보관 용량에 대해 라이센스 제한은 없습니다(보관 용량은 하드웨어 또는 가상 시스템의 온/오프 스토리지 용량).
  - 시스템 구성 변경에 따라 라이센스 재조정이 가능 합니다.
  - 대용량 로그 보관에 사용할 시스템 수에 맞춰 필요한 라이센스를 구매 합니다.
  - Data Store 이중화(HA) 구성은 지원하지 않습니다.

QRadar Data Store 구성

- Q> 제품 구성은 어떻게 이뤄지는지?
- A> 기본 구성은 실시간 상관 분석에 필요한 EPS 라이센스 구성 없이 제품 설치 라이센스와 QRadar Data Store connection 라이센스로 IBM QRadar data store 구축이 가능 합니다.



- Q> QRadar Data Store connection 라이센스는 무엇인지?
- A> QRadar 7.3.1 버전 이상에서 라우팅 룰을 적용해 실시간 상관 분석이 필요 없는 로그를 SIEM에 수집 보관하는 라이센스 입니다. Data Store Connection을 통해 수집한 로그는 정규화를 거쳐 보관되기 때문에 QRadar 콘솔 메뉴를 통해 로그 검색 및 보고서 생성을 지원 합니다. 로그 검색/보고서 생성(스케쥴링)/대쉬보드를 지원하고 실시간 상관 분석을 통한 오펜스 생성은 지원하지 않습니다.
- Q> 실시간 상관 분석 확장을 하기 위해 필요한 사항은 무엇인지?
- A> 시스템 인프라 변경 없이 EPS 라이센스 추가를 통해 실시간 상관 분석 기능 확장이 가능 합니다.

QRadar Data Store 기능 설명

IT 보안 빅데이터 시스템 구축 및 컴플라이언스 대응

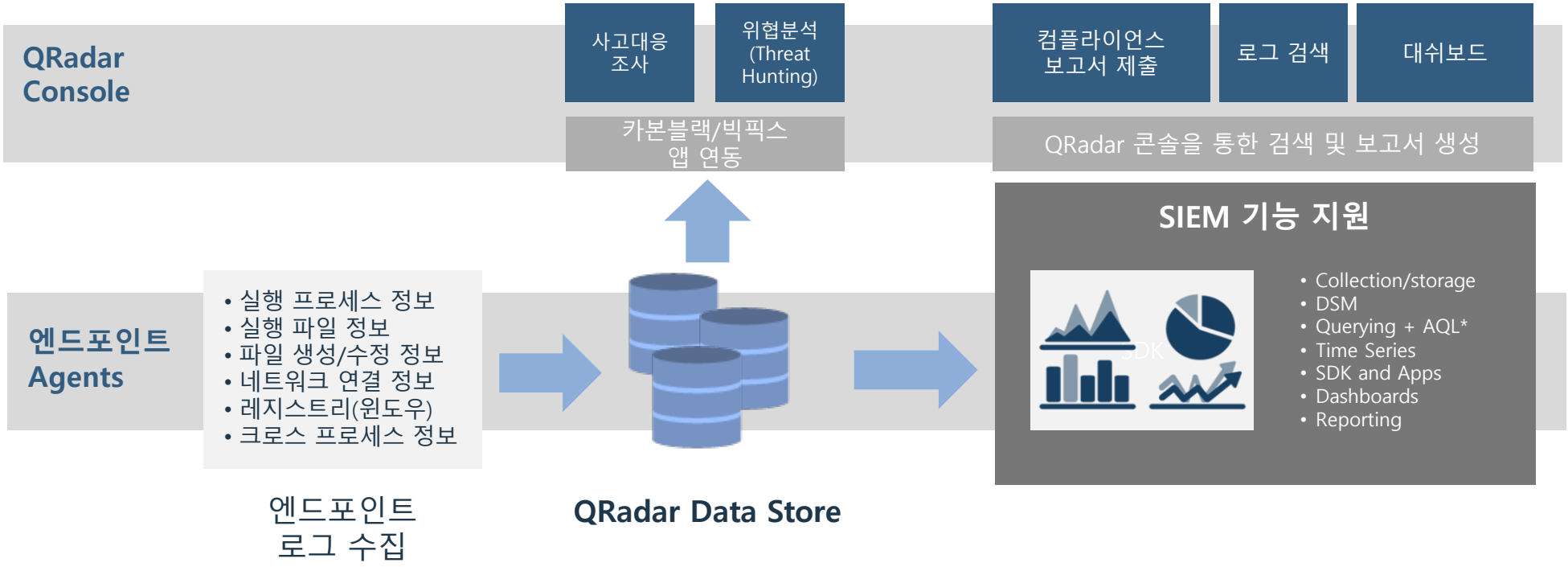
- QRadar Data Store는 저장 용량에 대한 라이센스 제약 없이 로그 수집 보관을 지원 합니다.
- 수집 로그는 QRadar DSM* 엔진을 거쳐 정규화(Normalization) 로그 형식으로 보관 됩니다.
- 수집 로그는 QRadar의 로그 분류에 따라 High Level / Low Level 카테고리로 분류 됩니다.
- 정규화된 로그를 기반으로 고급검색 / 시계열 검색 / 대쉬보드 / 보고서 / Apps 지원 합니다.
- 유연한 라이센스 모델을 활용해 사용자가 제품 구성을 다양하게 활용 할 수 있도록 지원 합니다.
- SDK와 APP 기능 지원하기 때문에 3rd 파티 연동이 가능 합니다.

* Device Support Module

지원 기능	미지원 기능
실시간 로그 수집	실시간 상관 분석 및 히스토리컬 분석
정규화 지원 및 카레고리 분류 (Normalization)	플로우수집(Flows)
DSM* Builder(로그 파싱)	자산관리(Assets)
로그 보관	오펜스생성(Offenses)
Querying + AQL	UBA 기능
시계열 검색 (Time Series)	X-Force 지원
SDK and Apps	Cloud Discovery
대쉬보드 및 보고서 생성	Data Discovery

IBM QRadar Data Store with EDR 유즈케이스

IBM QRadar Data Store를 통해 감사 로그 및 엔드포인트 시스템 로그 수집 보관/검색/대쉬보드 활용



* Ariel Query Language

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANYSYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM