오픈소스를 활용한 보안위협 대응 플랫폼

THE TRUST BEYOND
THE SECURITY

SK infosec

Contents

1. 2017년 IT 관심 Keyword

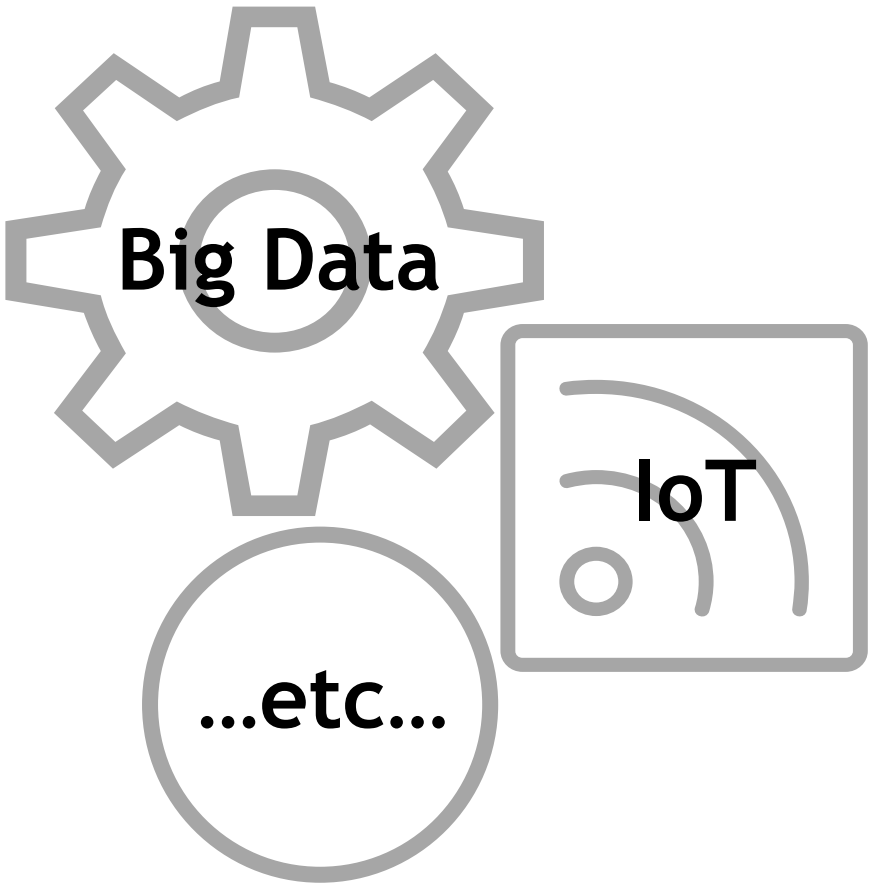
2017년 : Data, Threat, Cloud, Risk, IoT…

2016년 : Submission Titles

⬆ Data, IoT, Machine ⬇ Cyber, Learn ○ Threat, Cloud, Risk

2. 다양한 IT Infra와 진보된 보안위협

배경



이슈

- Big Data 수집/ 분석
- 실시간 데이터 처리
- Correlation Analysis

1. SIEM Architecture

Data Collector

- Security Equipment
  - Firewall
  - IDS
  - IPS
  - DDoS
- Routers
- Switches
- Server
- Workstation
- Applications
  - Antivirus
- Etc.

Data Analyzer

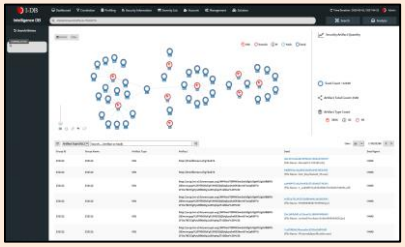
Event Data	Contextual Data
Security Devices	Vulnerability Scans
Network Devices	User Information
Servers	Asset Information
Applications	Threat Intelligence

Data Normalization &
Correlation Logic Rules

Analysis

Monitoring

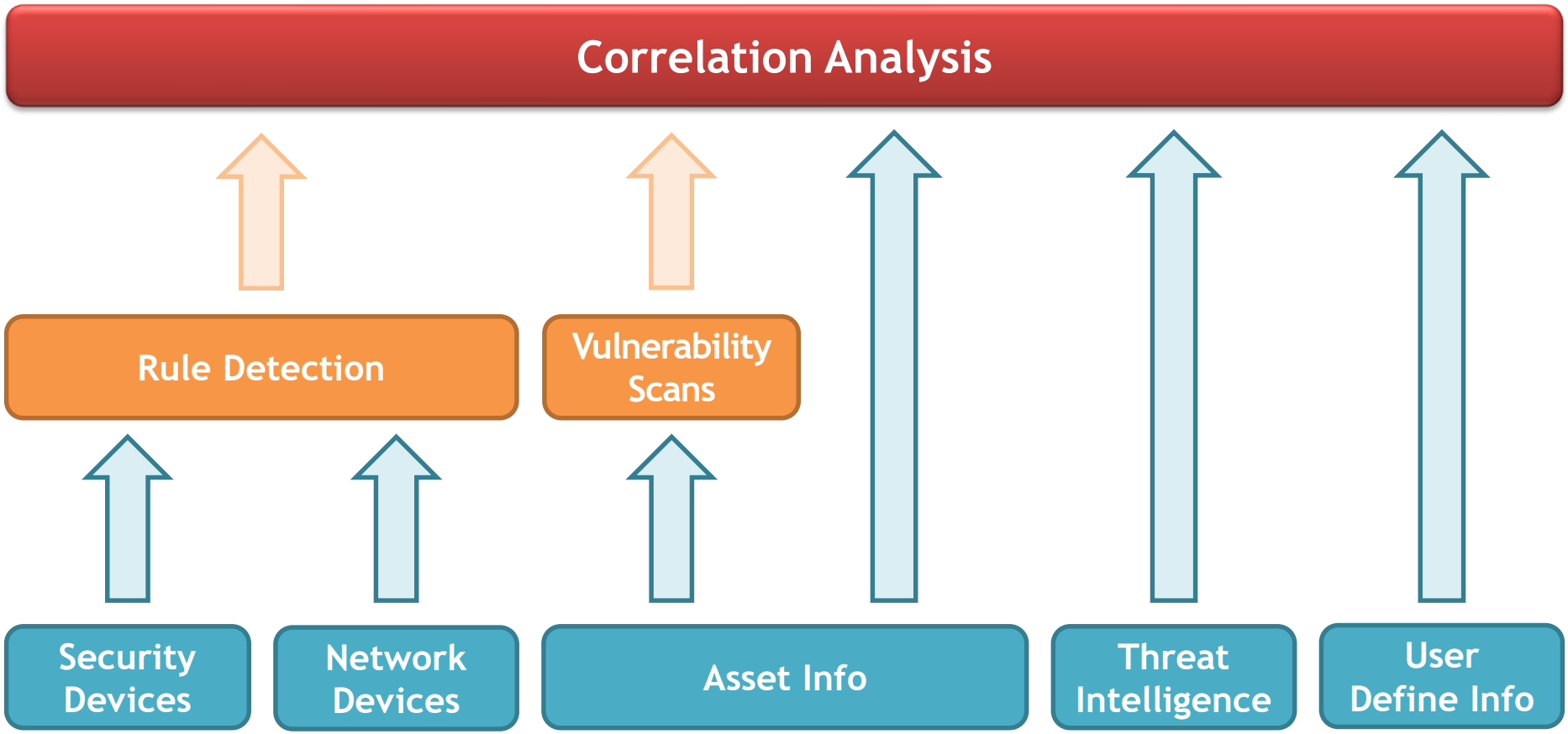
Dashboard



Report

Alarm

2. SIEM: Correlation Analysis



3. SIEM: 도입 방법 및 선택

솔루션 도입

자체 개발

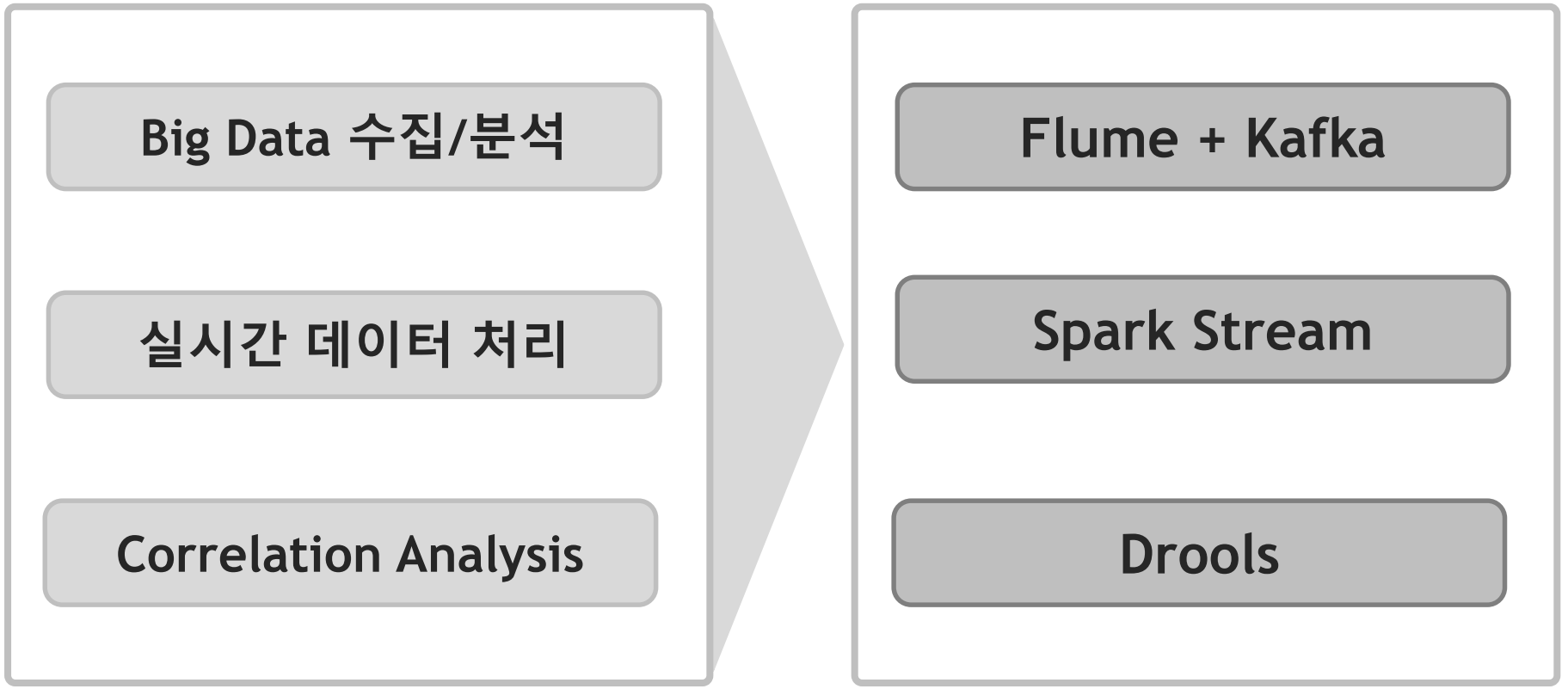
오픈소스 활용한 구축 ✓

1. 오픈 소스 도입 이유

1위	벤더 기술 종속성 탈피
2위	자유로운 코드 수정
3위	소프트웨어의 기능성
4위	소프트웨어의 혁신성
5위	코드의 품질과 보안성

『출처 : NorthBridge/BlackDuck SW. 2017 Open Source 360° Survey』

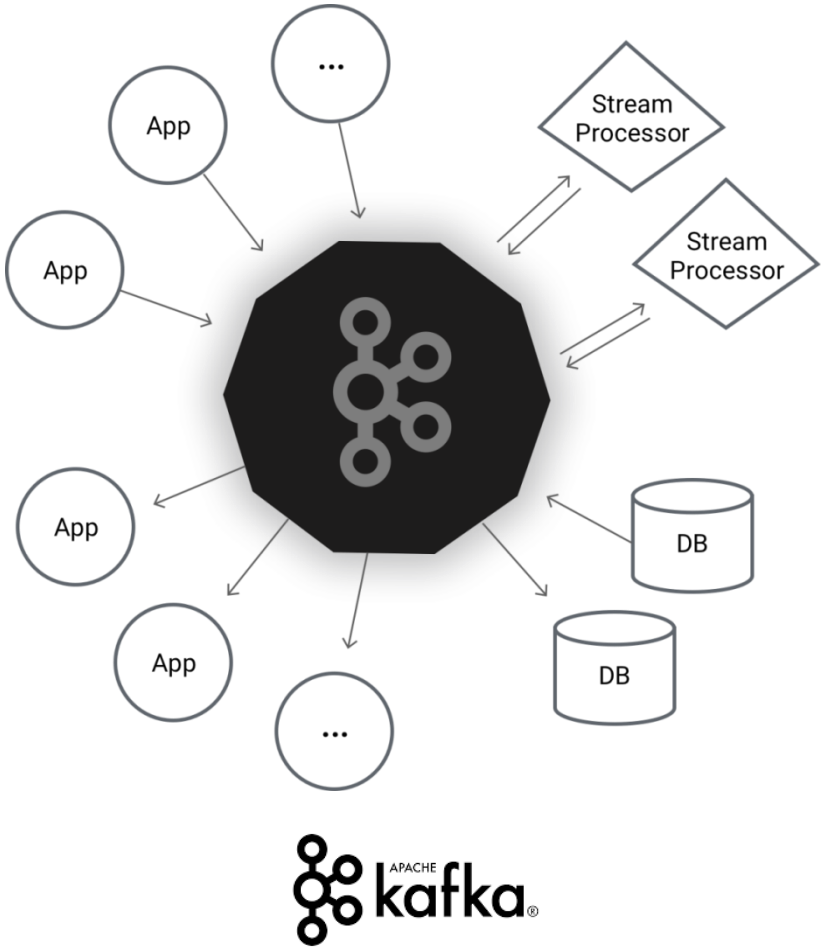
2. OSS 플랫폼 선정


Big Data 수집/분석
실시간 데이터 처리
Correlation Analysis
Flume + Kafka
Spark Stream
Drools

2. 수집 플랫폼 - Flume

- Reliability
- Scalability
- 다양한 Data Source
- 데이터 정제
- 다양한 전송타입

3. 수집 플랫폼 - Kafka



- Persistency
- Scalability
- 고성능 설계
- Zero-Copy

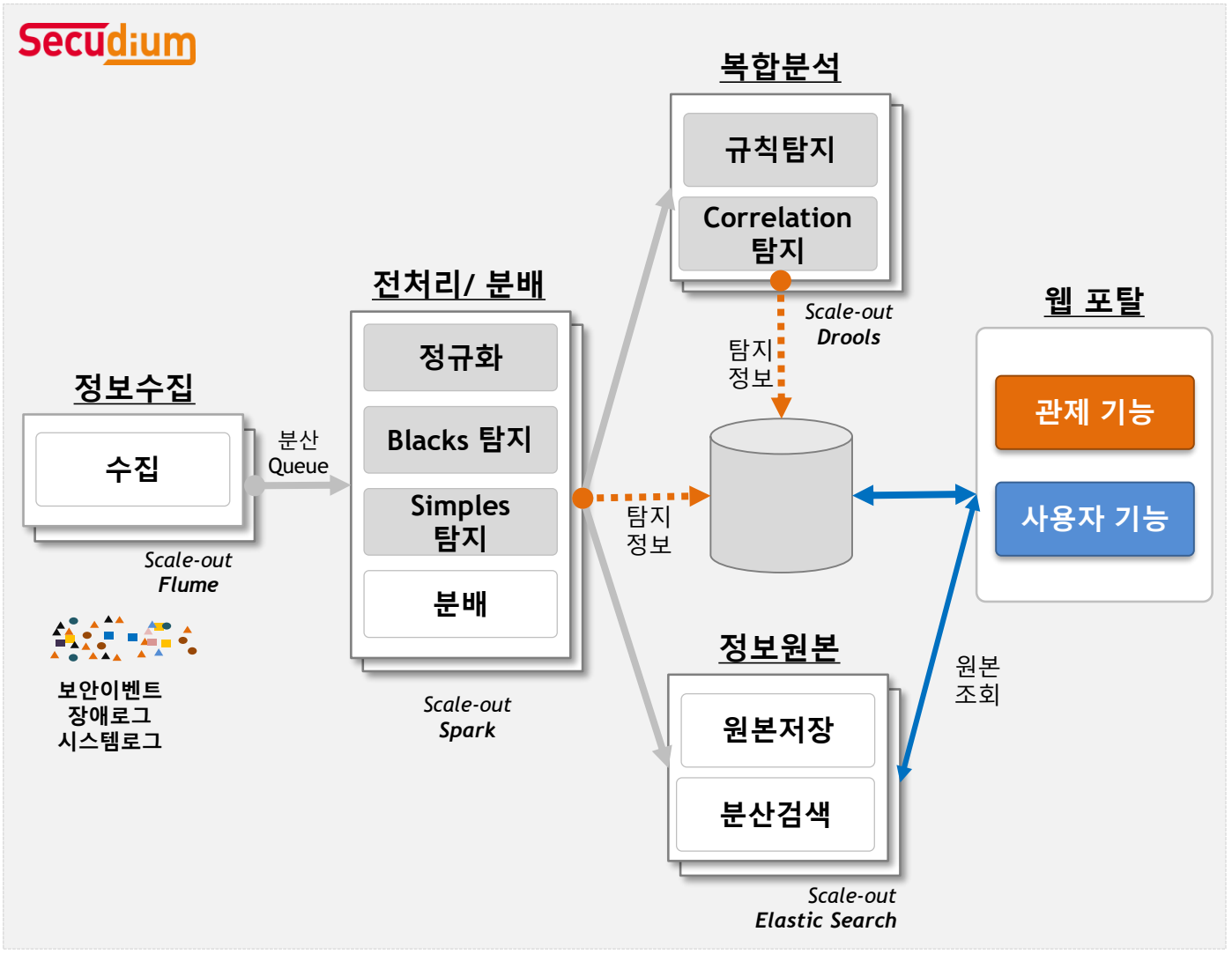
4. 실시간 처리 플랫폼 - Spark Streaming

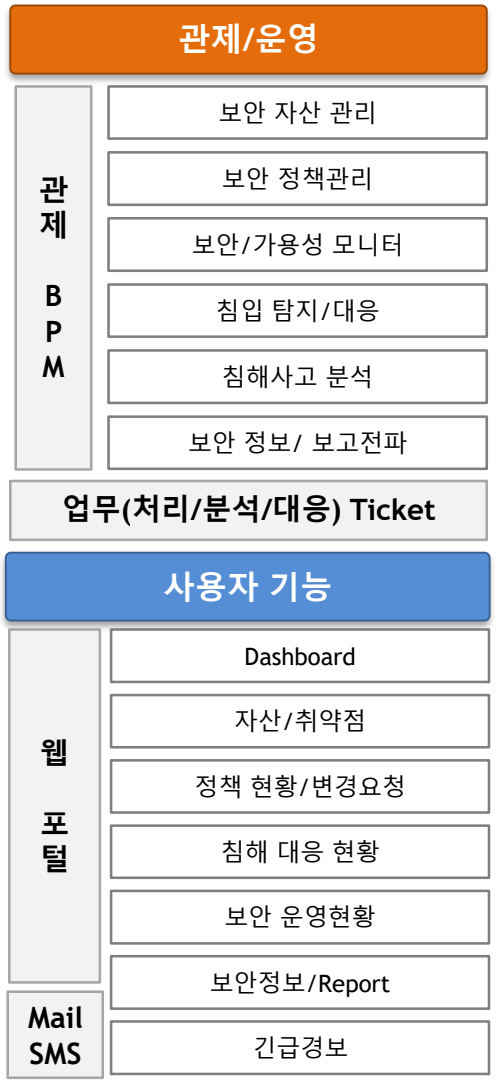
- Dynamic load balancing
- Dynamic scaling
- 빠른 속도
- 다양한 개발언어 지원
- UI enhancements

5. CEP 플랫폼 - Drools

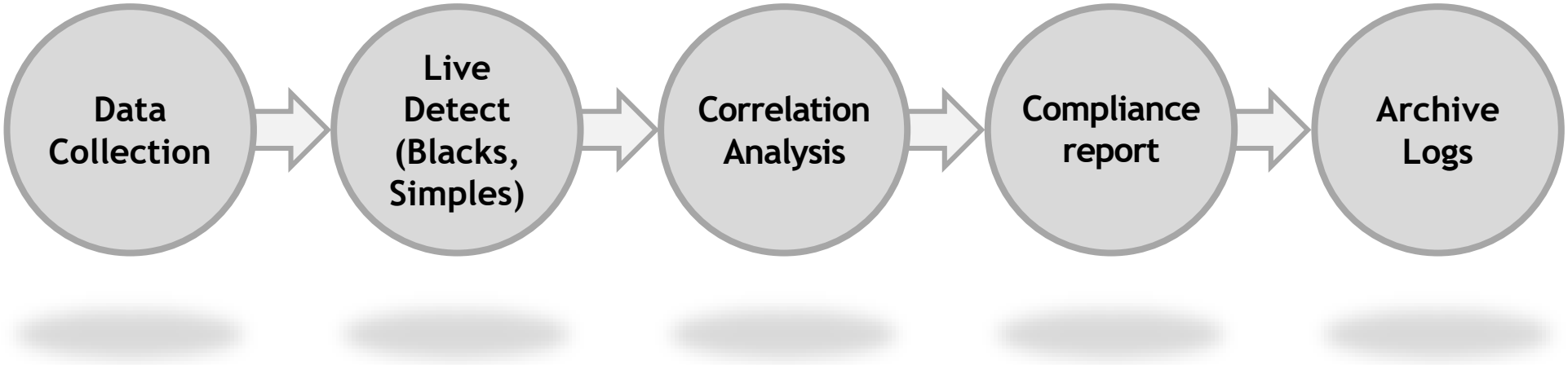
- 성숙된 Rule Engine
- 쉬운 Rule 편집 기능
- 통합 Rule 관리 기능
- WEB UI의 Workbench
- 확장 가능한 구조

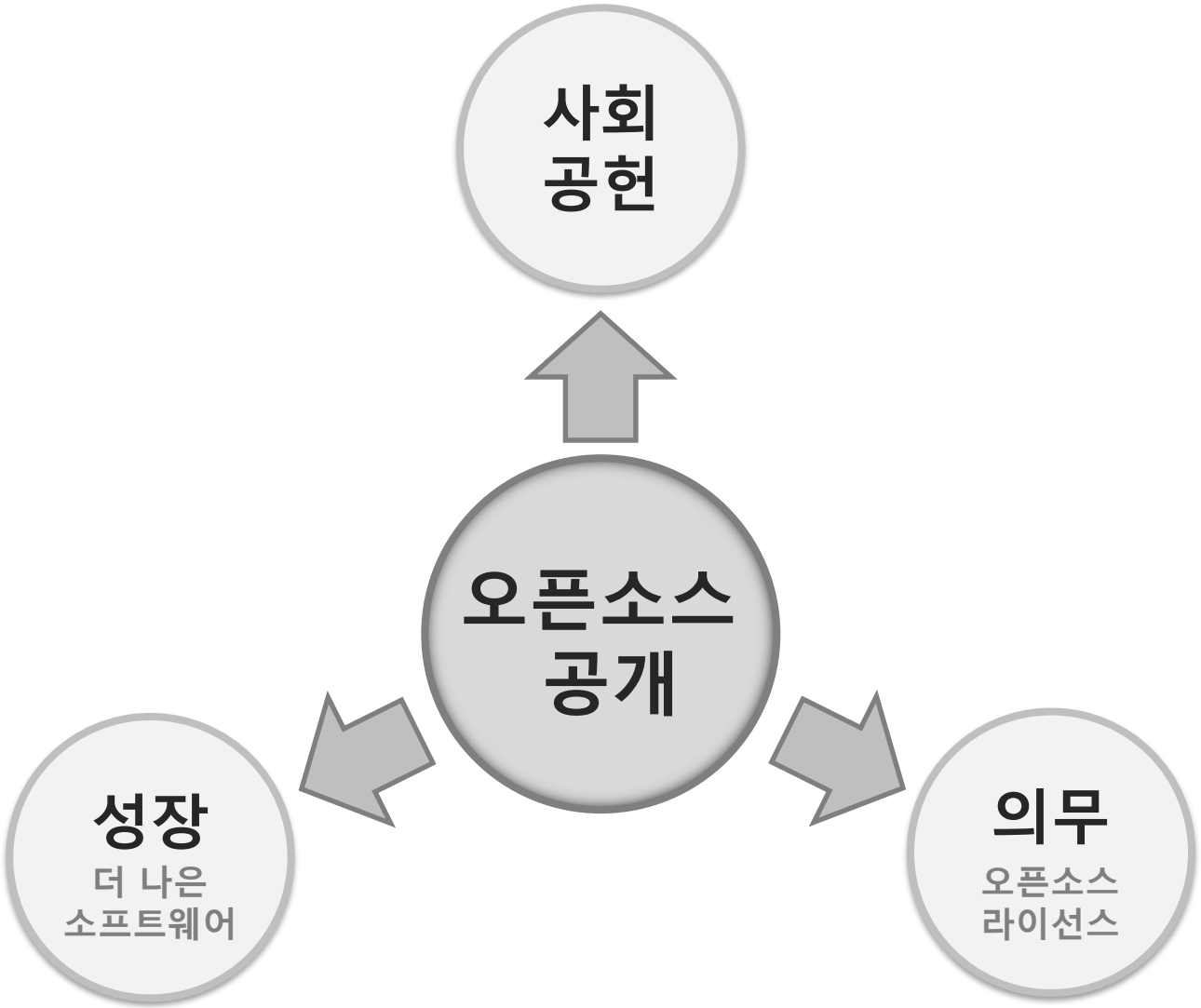
1. Architecture



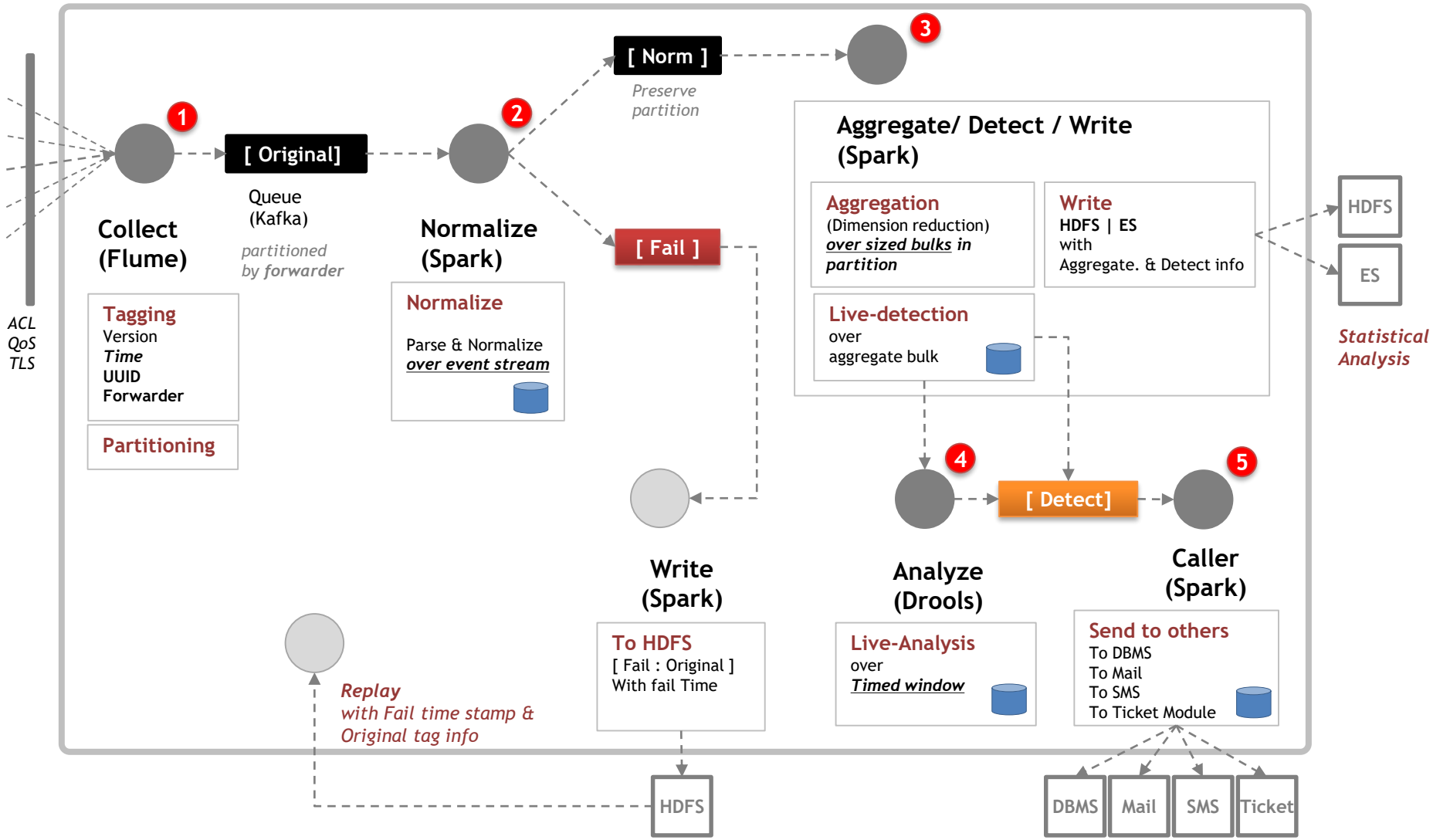


2. Data Detect Workflow




사회
공헌
오픈소스
공개
성장
더 나은
소프트웨어
의무
오픈소스
라이선스

2. Secudium OSS - Engine Data Flow



Thank You for Watching!

SK infosec