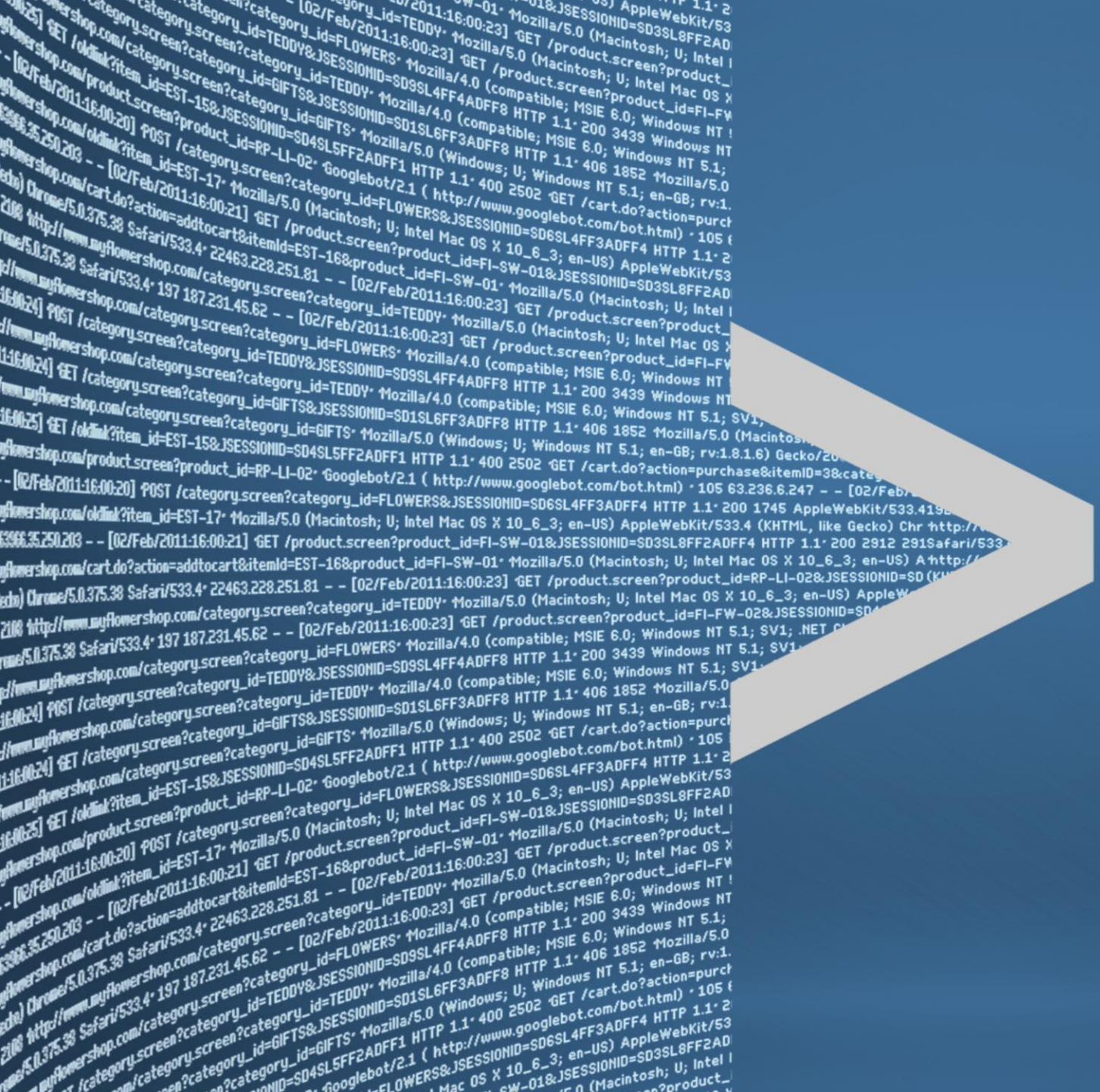
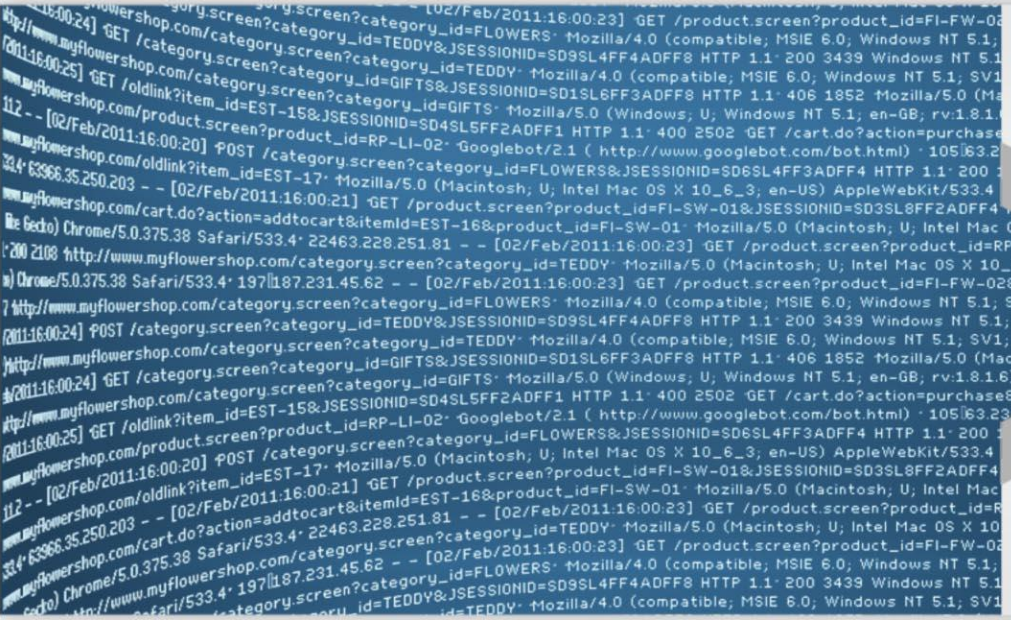


Splunk Bootcamp User Session 1 Day (V6.2)

MOS

MOS Asia Inc.

splunk> MOS



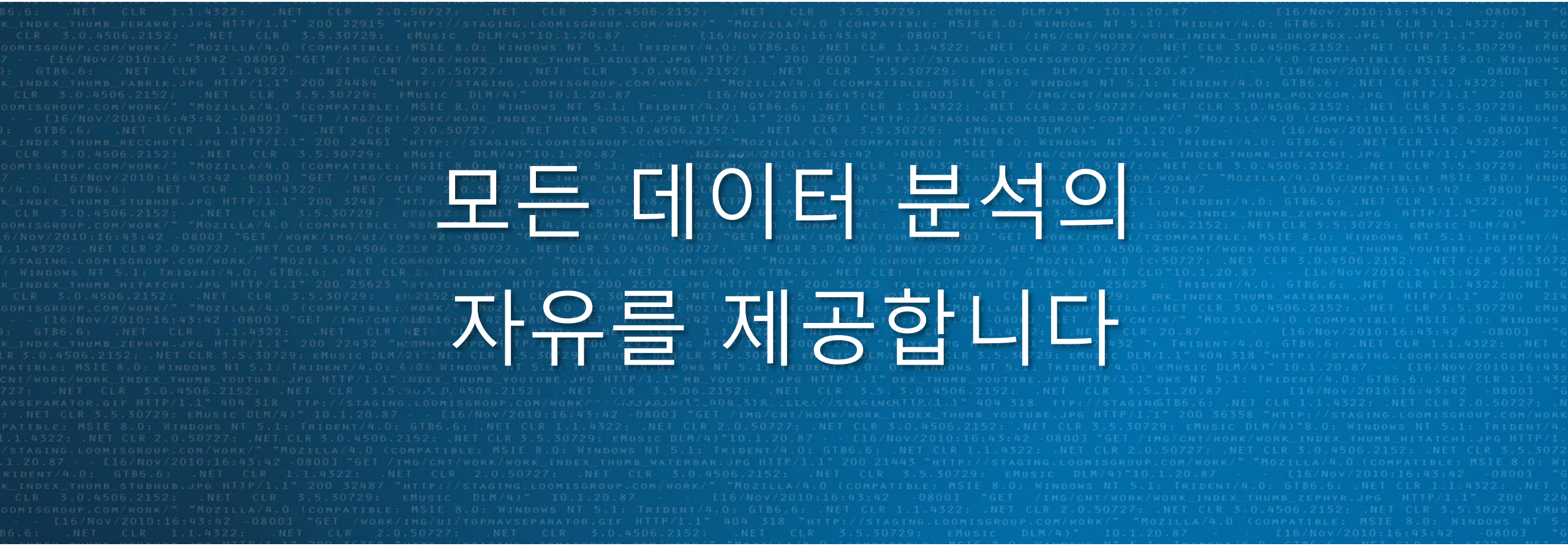
Introduction

splunk>

splunk> Mission

Splunk User Session에 오신 여러분을 환영합니다

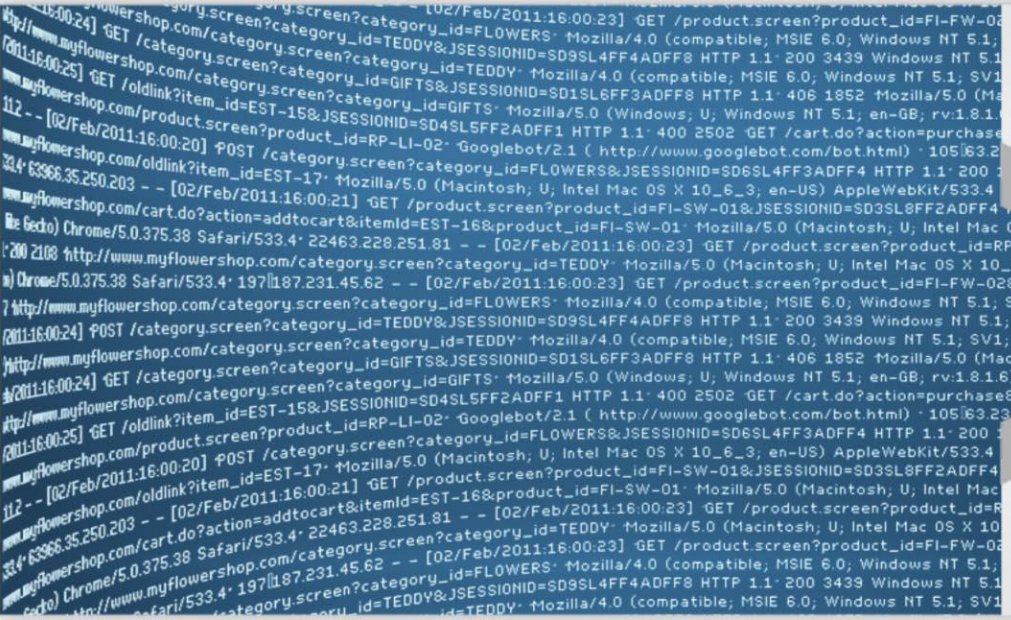
splunk> Mission



Splunk BootCamp User Session Goals

- **Splunk** 개념 이해
- **Splunk** 를 사용한 검색
- **Splunk** 데이터 수집, 정규화 및 실습
- 검색한 정보로 보고서 및 차트 생성
- DashBoard 와 Apps 생성

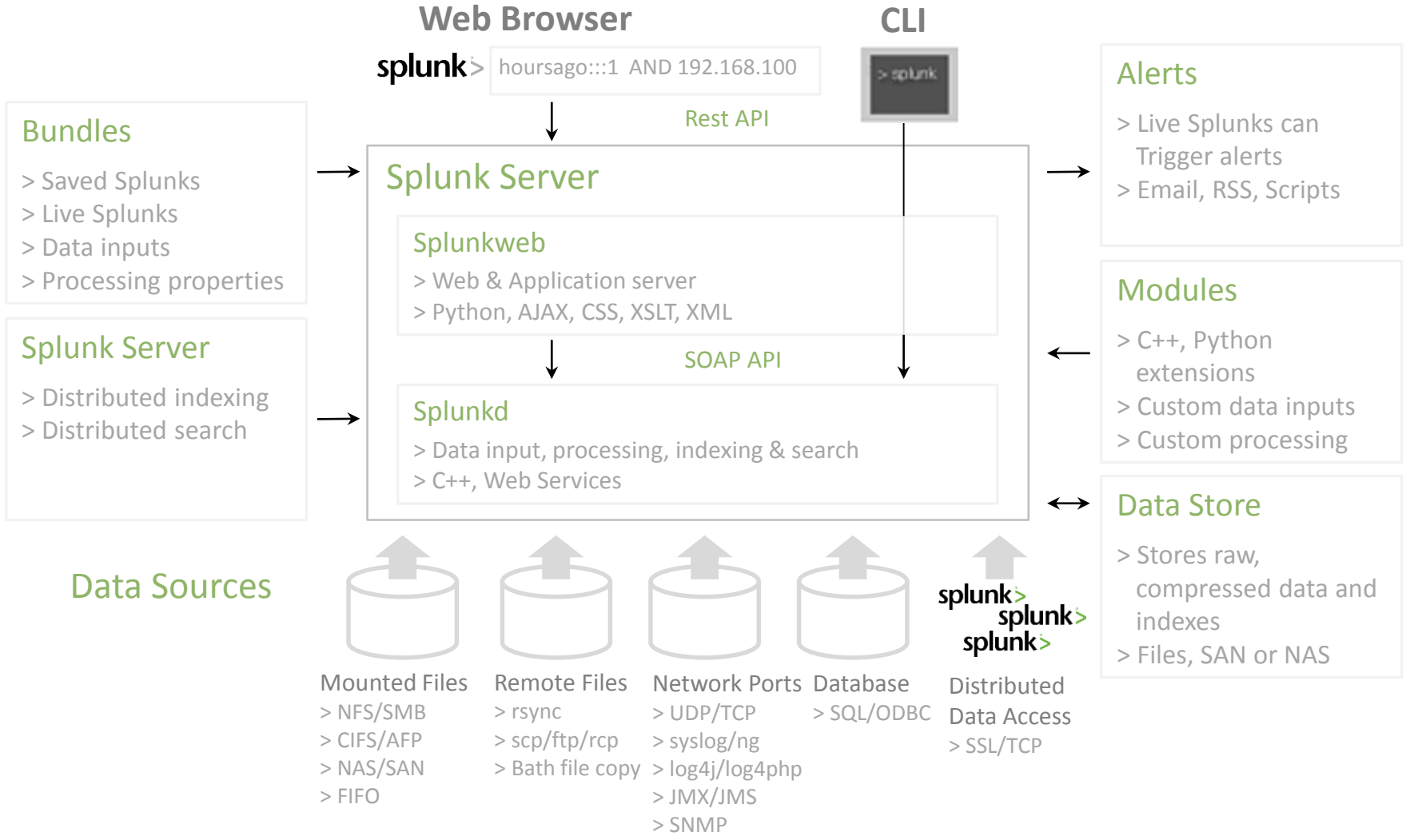
splunk> MOS



Splunk 소개

splunk>

Splunk Architecture



Splunk 소개

원격 소스에서 데이터 수집

Splunk Forwarder는 여러 소스에서 데이터를 실시간으로 수집

로컬 데이터 소스(애플리케이션, 센서, End Point 장치)를 모니터링하고, 일정에 따라 상태 명령의 출력을 수집함

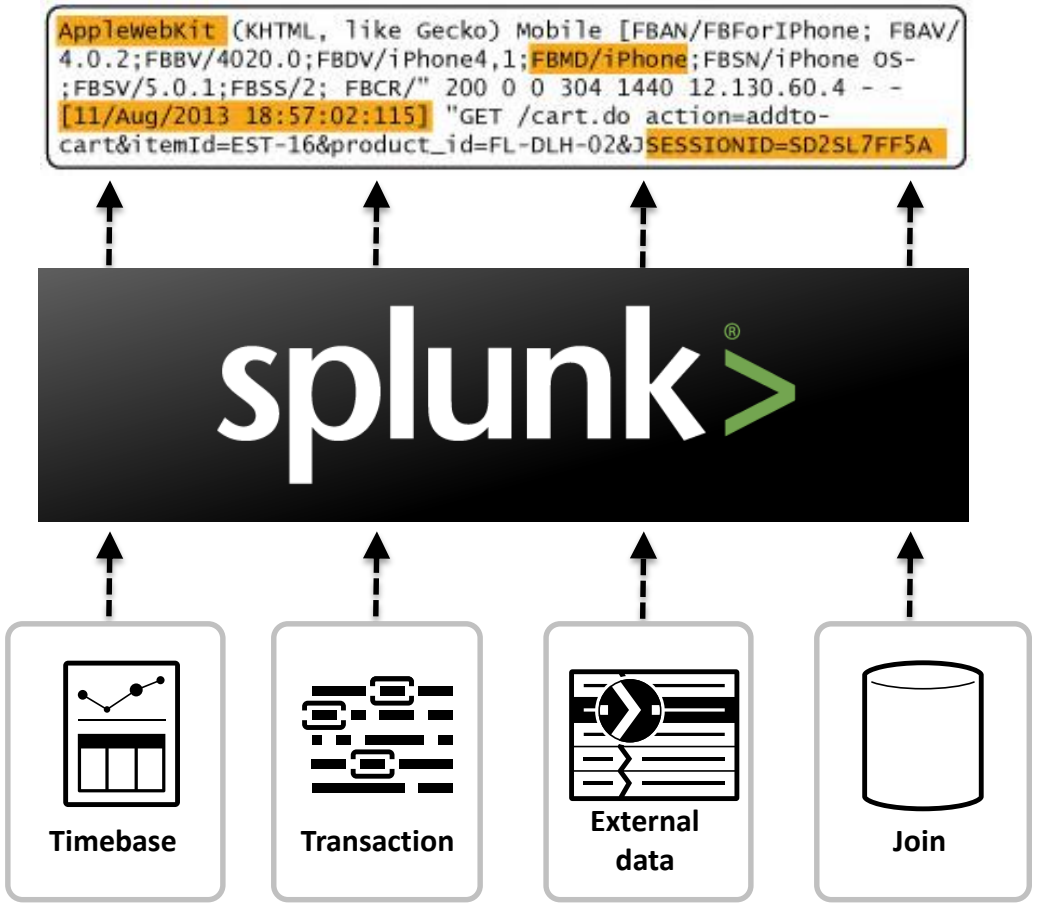
Forwarder는 중앙 관리 방식의 경량 형 장치로 추가 비용 없이 빠르게 배포 가능

Splunk 소개

복잡한 이벤트의 상관

Splunk는 다양한 데이터 소스에서 파생되는 복잡한 이벤트의 상관관련 검색 및 분석이 가능함

- 시간 상관 : 시간, 근접성을 기반으로 관계 식별
- 트랜잭션 상관 : 일련의 관련 이벤트를 단일 트랜잭션으로 추적하여 기간, 상태 또는 기타 분석을 수행
- 외부데이터 상관 : Splunk Data와 외부 데이터의 관계를 분석할 수 있는 LOOKUP 기능 제공
- 내부 및 외부 상관 : SQL과 유사한 조인 지원

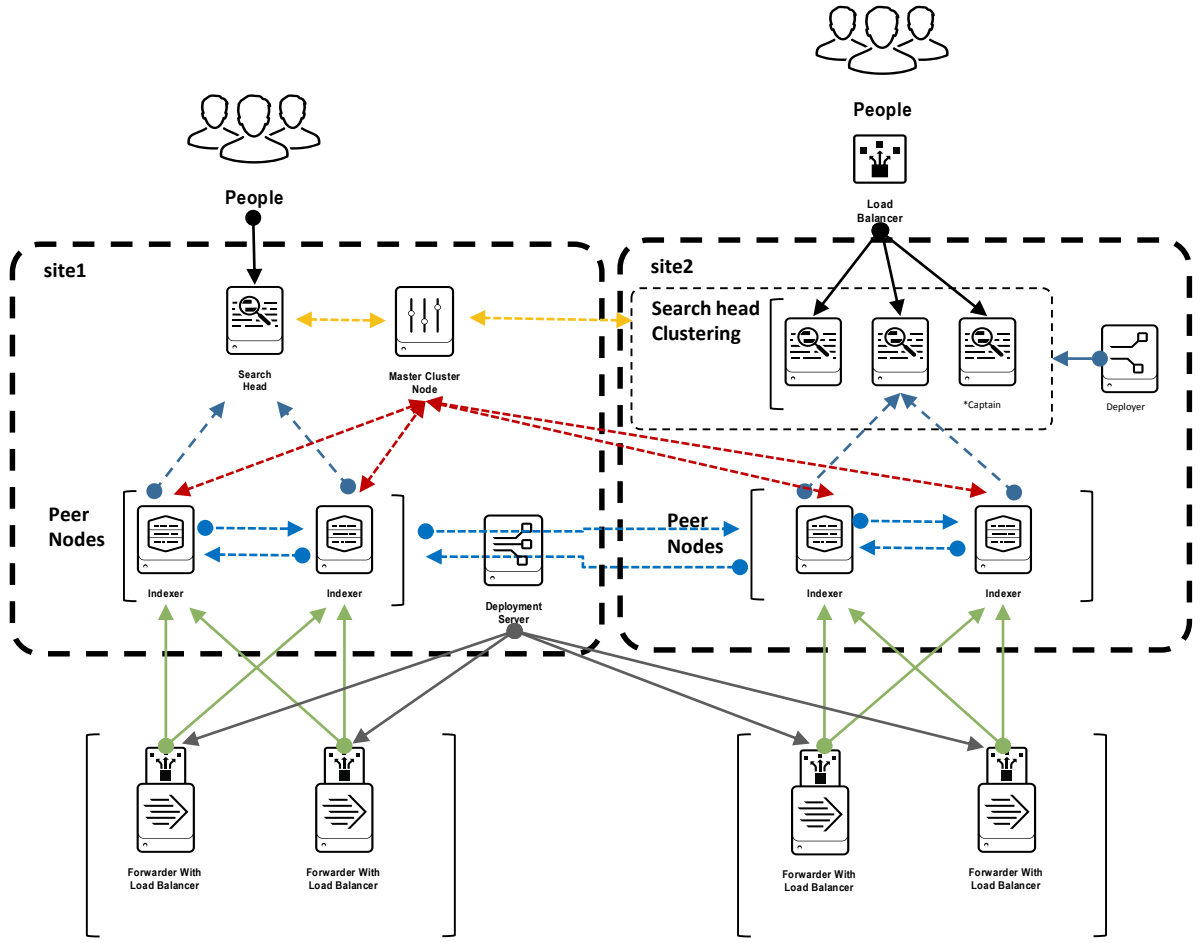


Splunk 소개

Enterprise급 가용성 및 규모

Splunk Enterprise를 확장하여 매일 수백 TB의 데이터를 수집하고 인덱싱 할 수 있음

- Splunk Enterprise Clustering 및 다중 사이트 Clustering 기술은 지속적인 가용성을 제공
- 단일 서버 또는 사이트가 중단되더라도 머신 데이터 (machine data)로부터 중요한 Insight 을 얻을 수 있음
- 자동 부하 분산은 워크로드와 응답 시간을 최적화하고 기본 Fail-Over 를 지원
- 보고서 작성 및 분석 기능을 통해 빠른 Insight 도출이 가능함
- Agent 관리를 위한 Deploy-Master
- Search Head Clustering

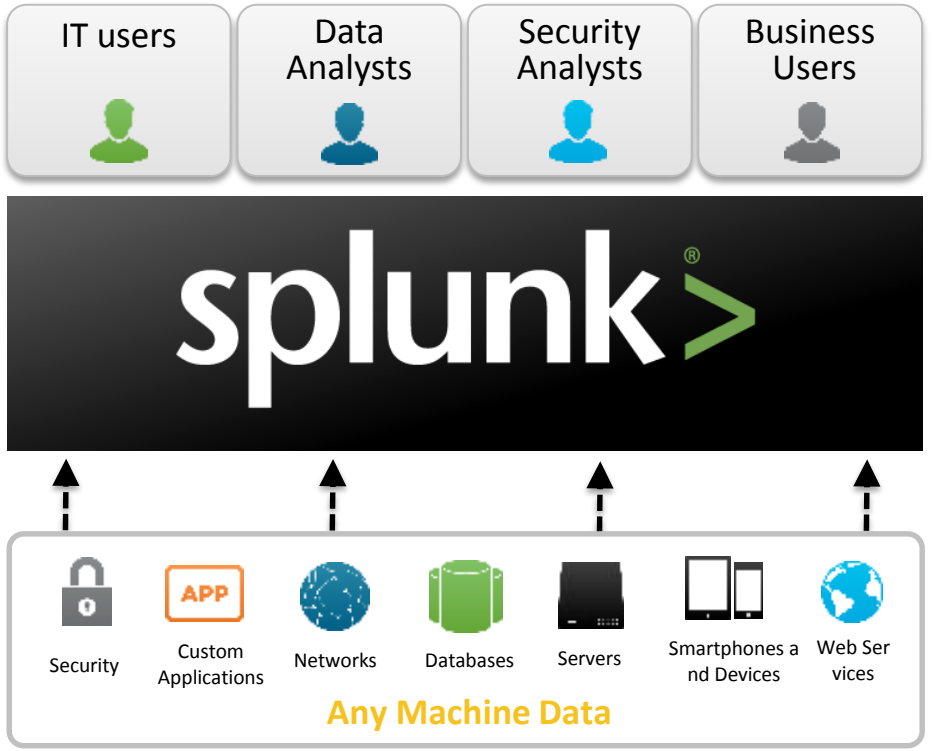


Splunk 소개

세분화된 역할 기반 보안 제공

Splunk Enterprise가 제공하는 기능

- 강력한 보안 (CC인증 획득)
- 안전한 데이터 처리
- 역할 기반 액세스 제어
- 웹 사용자 인터페이스
- CLI를 통한 인터페이스
- Splunk Enterprise REST API를 통한 시스템 작업

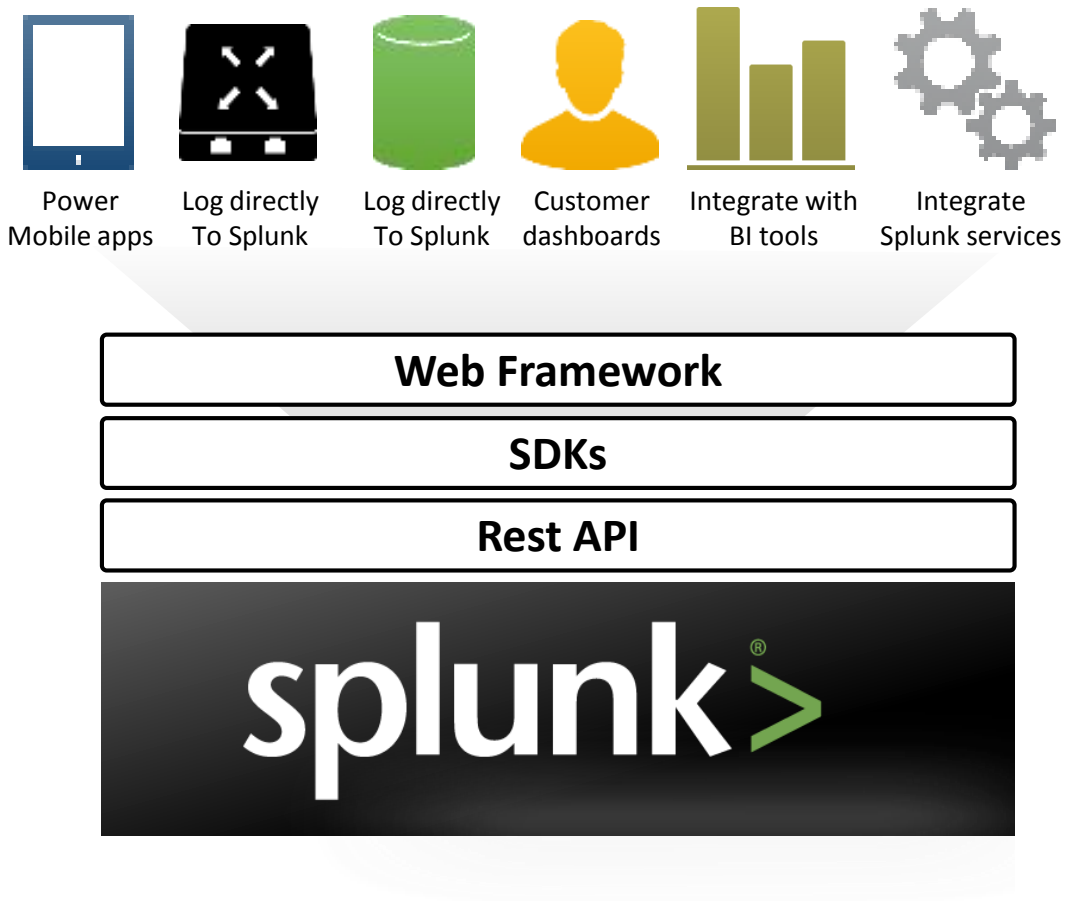


Splunk 소개

기업 개발자용 플랫폼

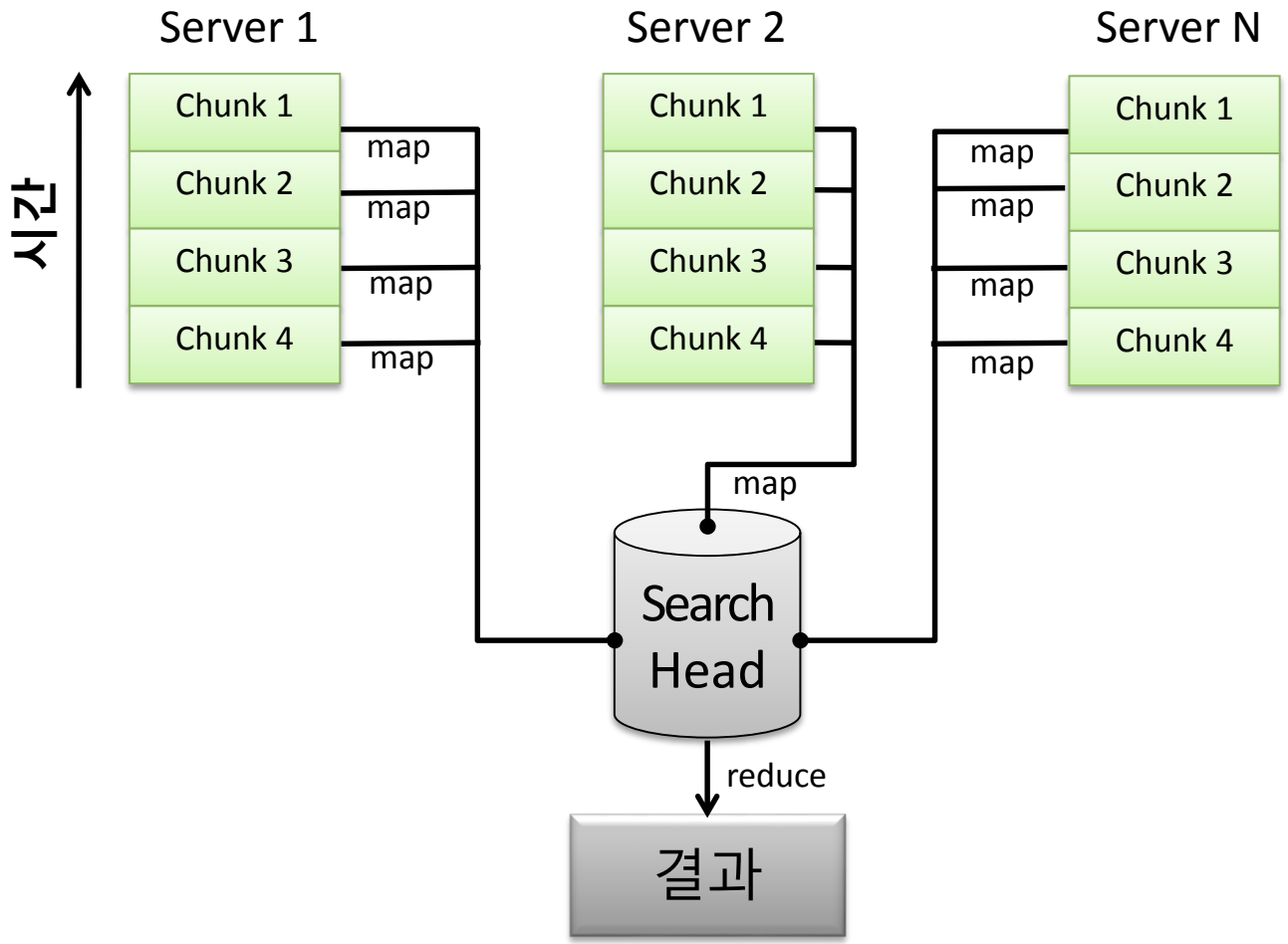
Splunk Web Framework
- JavaScript
- HTML5
- JQUERY
- XML, XLST
- CSS3
- Django
- etc

SDK(Software Development Kits)
- Java
- JavaScript
- C#
- Python
- PHP
- Ruby



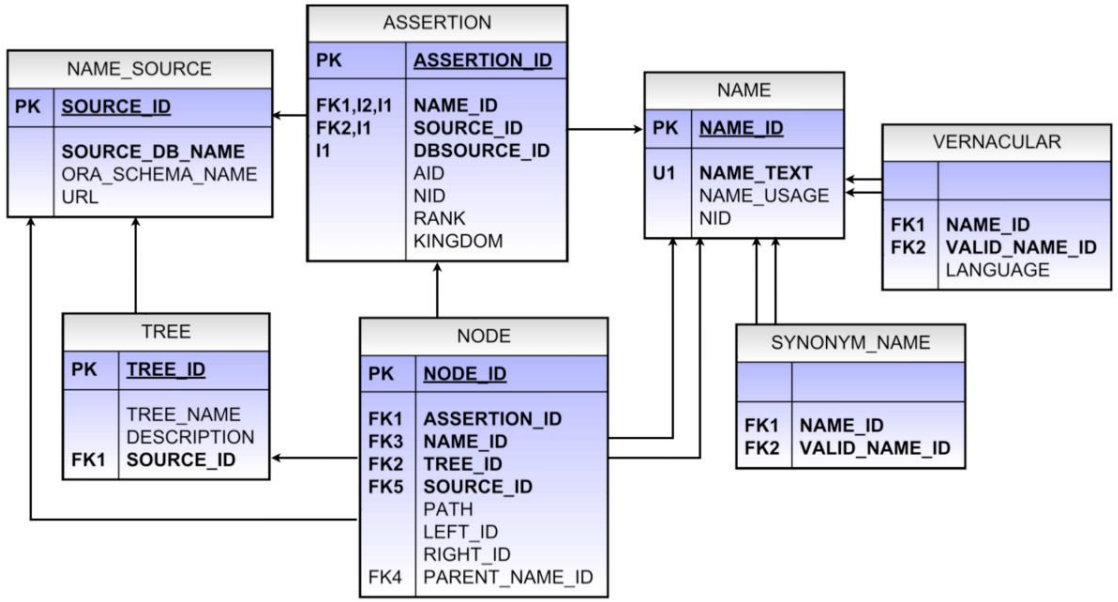
Splunk 소개

Map Reduce 기반의 Architecture



Splunk 와 기존 기술 비교

기존 기술 RDBMS/SQL – Early-structure Binding

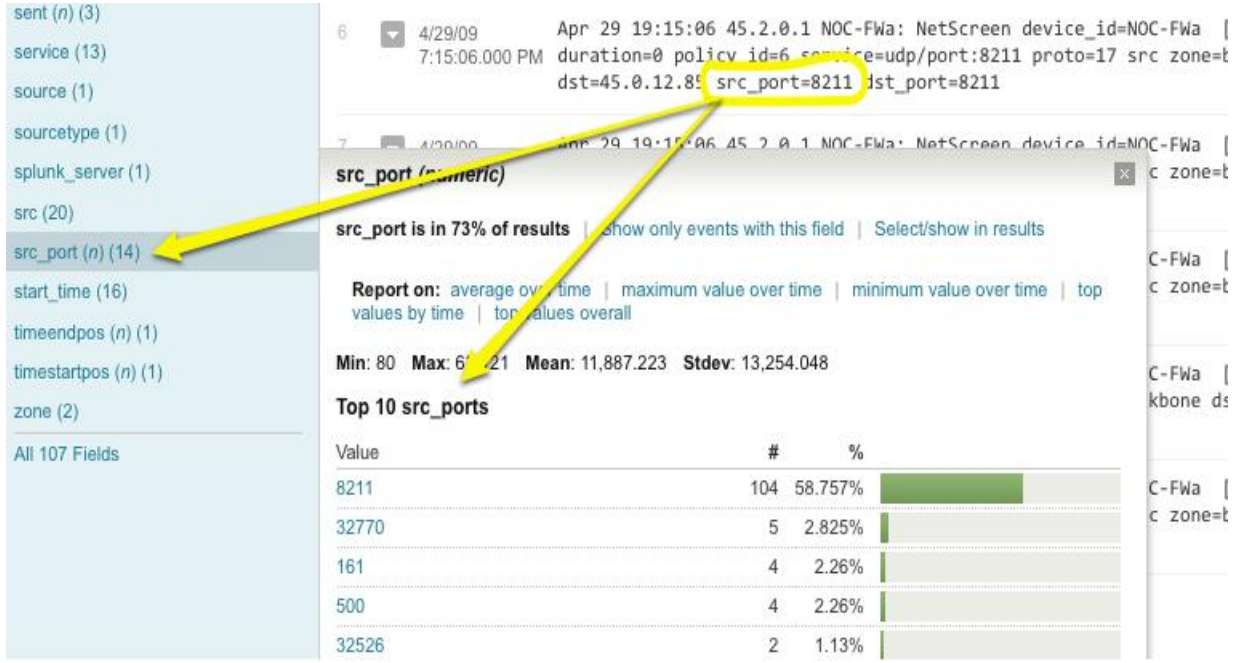


구조	데이터
✓ Schema – 시스템 구축과 디자인 ✓ Queries – 디자인 시점에 정확한 이해를 통한 최적의 Query 정의	✓ 단일유형 – 설정된 구조에 맞게 입력하거나 변환이 요구됨 ✓ 여러 DB의 구조적 요건을 맞추어야 함

SELECT customers.* FROM customers
WHERE customers.customer_id NOT IN(SELECT customer_id FROM orders WHERE year(
orders.order_date) = 2004)

Splunk 와 기존 기술 비교

splunk> 빅 데이터 기술 - Late-structure Binding



구조	데이터
✓ Schema 가 요구되지 않음 ✓ 데이터의 속성이 검색과 함께 정의 됨 ✓ Queries 나 검색은 그때그때 다이나믹하게 구성	✓ 여러 이종의 데이터 수용 – 모든 종류의 Raw데이터 수용 ✓ 지속적인 변경을 수용 ✓ Conversion 이나 데이터 규격에 따른 제약 조건이 없음.

eventtype=firewall accept OR allow | top src_port

홈페이지 안내

- **MOSA 홈페이지** http://www.splunkmos.com
- **FACEBOOK** http://www.facebook.com/mos.since2003
- **Twitter** https://twitter.com/mos_korea
- **교육 신청** edu@mobile-os.com
- **Blog** http://blog.naver.com/mos_splunk
- **기술 문의** support@mobile-os.com

- **Splunk 공식** http://www.splunk.com/
- **Splunk wiki** http://wiki.splunk.com/
- **Splunk apps** http://apps.splunk.com/
- **Splunk docs** http://docs.splunk.com