통합보안관제 체계에 관한 연구

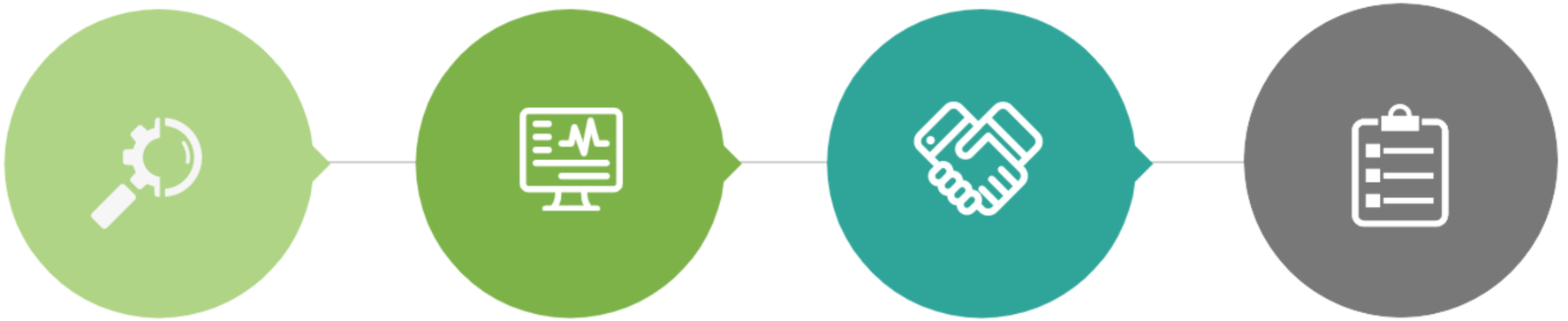
정 보 보 호 학 과 ——— 9 1 7 1 3 9 7 9 김 은 지

[목 차]

01. 통합관제 보안

1. 통합관제 보안 - 업무 5단계

1. 통합관제 보안 - 서비스



원격 관제 서비스

보안장비 중심의 보안 이벤트에 대하여 상시 모니터링을 수행하는 서비스

파견관제 서비스

전문 인력을 파견받아 업무를 수행하는 서비스

자체관제 서비스

자체적으로 운영 및 관리 하는 관제 형태

클라우드 관제 서비스

클라우드 환경에 대한 관제 서비스

02. ESM 보안관제

개요

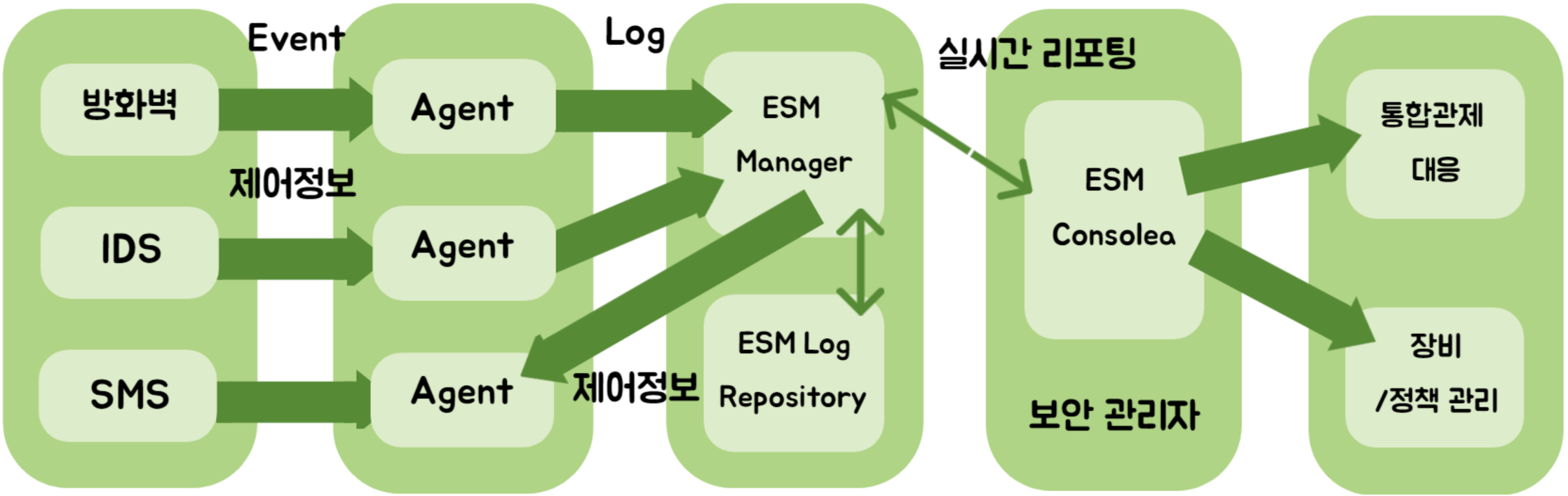
하나의 통합뷰로 관리

유사한보안 정책 통합

후 적용

위험요소를 최소화

구성도


Event
Log
실시간 리포팅
방화벽
IDS
SMS
제어정보
Agent
Agent
Agent
제어정보
ESM
Manager
ESM Log
Repository
ESM
Consolea
보안 관리자
통합관제
대응
장비
/정책 관리

03. SIEM 보안관제

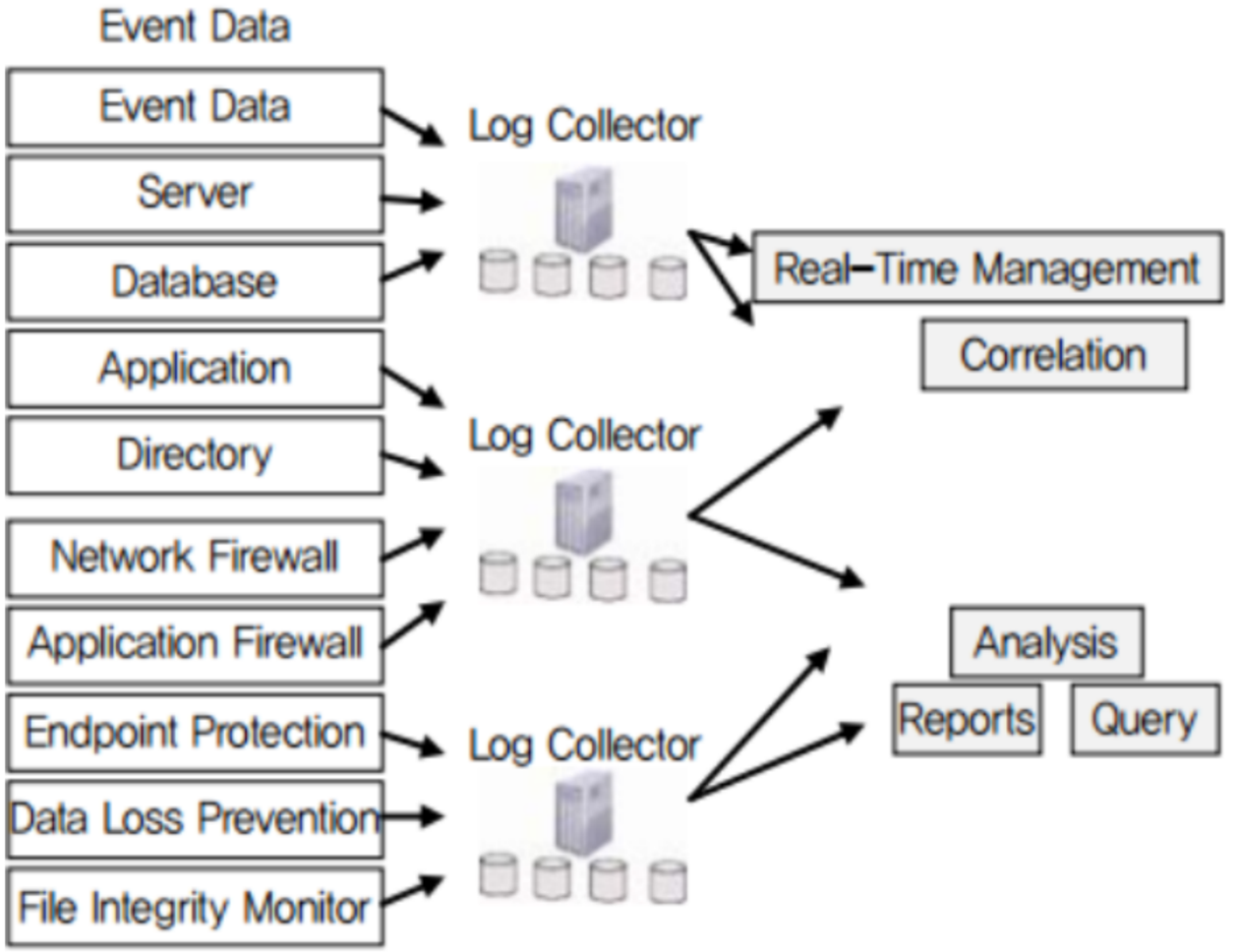
개요

방대한 데이터를 수집 저장

빅데이터 분석 기술로 상관 분석 가능

사이버 공격 측면을 고려 해 적극적인 대응 요구

구성도


Event Data
Event Data
Server
Database
Application
Directory
Network Firewall
Application Firewall
Endpoint Protection
Data Loss Prevention
File Integrity Monitor
Log Collector
Log Collector
Log Collector
Real-Time Management
Correlation
Analysis
Reports
Query

04. 지능형 보안관제

개요

사람이 해야할 일을 자동으로 돌림

비정상 행위 예측 결과가 시각화

비전문가 및 전문가에게 사용의 편리성 제공

지속적인 개선이 이루어짐

구성도


디지털 정보
물리, 정보통신, OT 등에서 발생하는 정보
전처리
빅데이터를 활용
비/지도학습
Rules, CEP, 보안위협, 취약점, 자산중요도
지능형 통합보안관제
시각화

05. 비교

비교 분석 표

항목	관리 분석대상	핵심용도	아키텍처	사용자	탐지오류
ESM	로그, 경고 Event 등	보안 위협 발생시 대처, 가용성 체크	중앙 처리 구조	보안관리자, 관제 요원 위주	비교적 오탐/과탐이 많음 (Event 위주 탐지)
SIEM	네트워크 장비, 보안시스템, 로그, 경고 등	보안 위협 예측 및 모니터링, 신종 보안 위협에 대응	상관 분석 및 리포트	각 업무 시스템별 담당자, 관제요원 등	비교적 오탐/과탐이 적음 (대용량 데이터 위주 탐지)
지능형	보안시스템, 정보통신, OT, 로그, 경고 등	보안 위협 예측 및 모니터링, 신종 보안 위협에 대응	머신러닝	각 업무 시스템별 담당자, 관제요원 등	성향적 오류, 오버피팅 오류가 있음

THANK YOU