cloud excellence

CLOUDZEN × Microsoft Azure

CLOUDZEN Offering

Microsoft Sentinel 기반 보안 Monitoring PoC

Microsoft

ZENITH & COMPANY

목차

Microsoft Sentinel 개요

제로 트러스트 환경과 정의에 부합하는 클라우드 핵심 보안 모니터링 환경 및 통합 분석을 위한 비용 최소화된 보안 모델을 제공합니다.

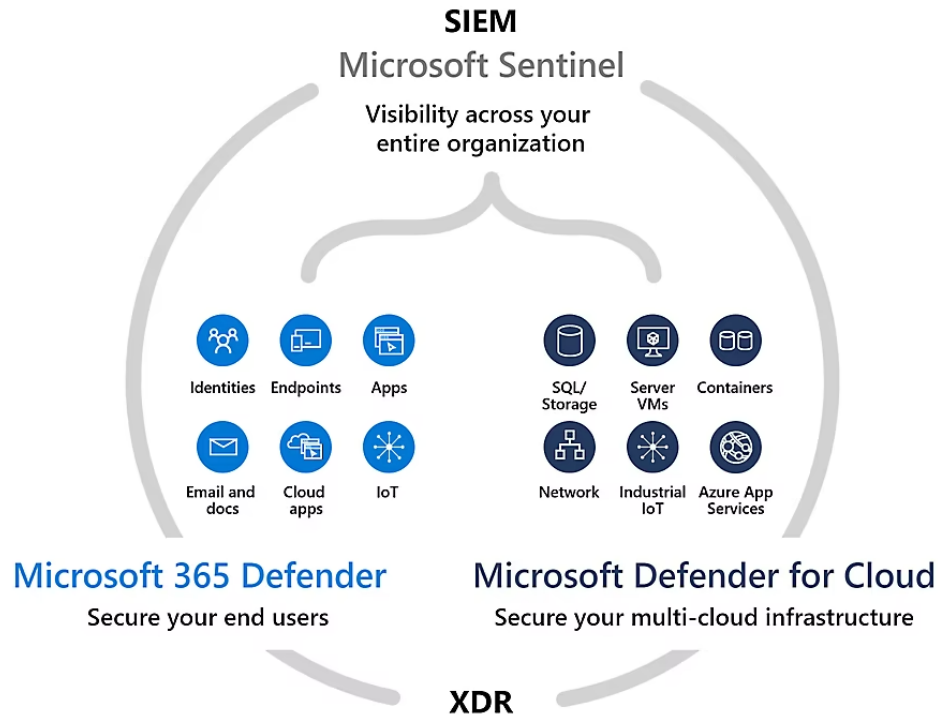
SIEM 개념 및 역할

SIEM (Security Information and Event Management)

- 정의 : 기업의 여러 원본에서 이벤트 로그 데이터를 수집하고 보안 위협을 탐지, 분석, 대응하는 솔루션
- 기능
  1. 여러 원본에서 이벤트 로그 데이터를 수집
  2. 로그 기반 실시간 분석
  3. 정상적인 범위를 벗어나는 활동을 식별하여 적절한 조치

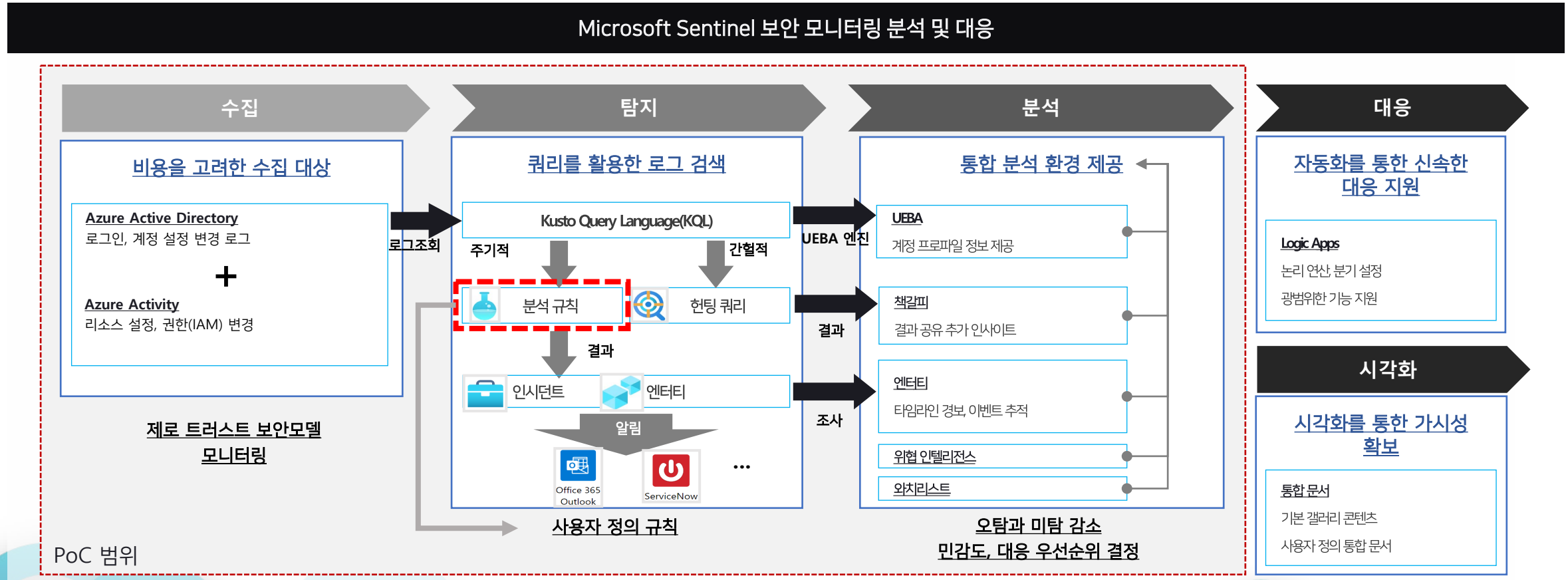
SIEM 및 XDR을 통한 최신 공격 방어

- Microsoft Defender for Cloud 와 Microsoft 365 Defender를 사용하여 클라우드와 End Point 사용자를 보호
- Microsoft Sentinel을 사용하여 전체 조직의 위협을 탐지하고 자동화를 통한 신속한 대응



PoC 진행 절차

보안 모니터링은 수집 대상 선정, 로그 분석을 통한 탐지 및 통합 분석 환경을 제공하는 3단계 절차로 진행합니다.



PoC 수행 일정, 대상, 비용

Microsoft Sentinel 환경 구성을 시작으로 완료 보고까지 총 2주간의 일정으로 진행합니다.

PoC 수행 일정

구분	1주차	2주차
Microsoft Sentinel 배포	→	
Azure AD, 활동 로그 수집 설정	→	
분석 규칙 및 경보 설정	→	
경보 테스트 및 통합 분석	→	→
PoC 완료 보고		→

PoC 대상 경보 리스트

계정 관리
- 수명 주기가 짧은 계정

계정 설정
- 정책을 위반하는 계정 생성
- 단일 인증 로그인 또는 설정
- 계정 유형 변경

계정 권한
- 관리자 또는 민감한 권한 할당

로그인
- 변칙 로그인: 업무 시간외 또는 해외 접속
- 로그인 실패: 다단계 인증 또는 비활성 계정

활동 로그
- 구독 또는 리소스 그룹 범위 작업 발생

PoC 비용

Offering	Azure 비용	인건비	Offering 비용	고객혜택	수행기간
Sentinel PoC	Sentinel 무료 평가판 범위내 무상으로 진행 - 1개월이내, 일일 최대로그 10GB	Azure 계약 고객 대상 무상 진행	0원	800만원	2주

감사합니다.

CLOUDZEN

Microsoft Partner
Microsoft

2019 Partner of the Year Winner
Korea

Microsoft Partner
Microsoft

Gold DevOps
Gold Data Analytics
Gold Cloud Platform
Gold Application Integration
Gold Application Development

Microsoft Partner
Microsoft

Gold Cloud Productivity
Gold Windows and Devices
Gold Collaboration and Content
Gold Enterprise Mobility Management
Gold Small and Midmarket Cloud Solutions

Microsoft Partner
Microsoft

Gold Datacenter
Gold Communications
Gold Project and Portfolio Management
Silver Security
Silver Messaging

고객의 성공을 위한

The right partner, The right solution

클라우드젠

서울특별시 강남구 테헤란로16길17 제니스빌딩 8층-11층 06235
marketing@zenithn.com

ZENITH & COMPANY