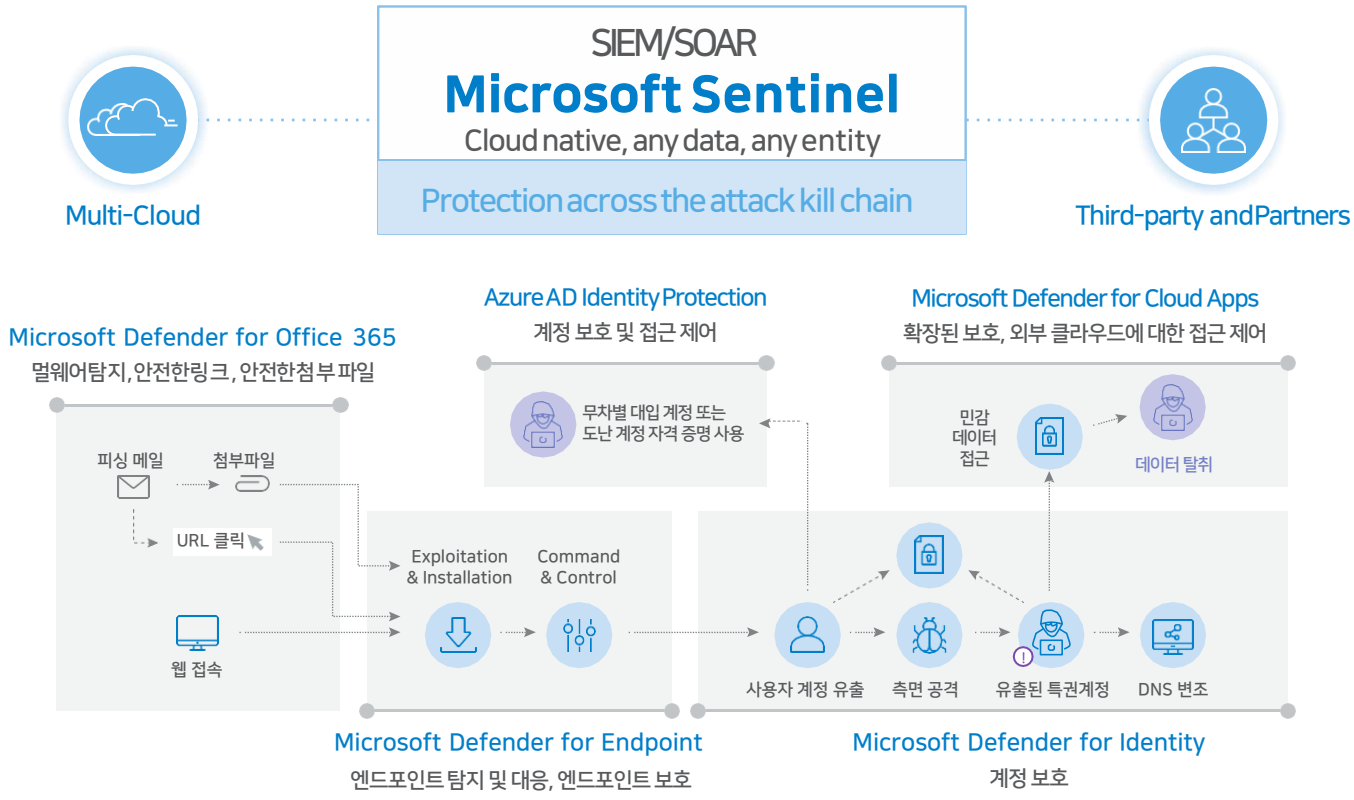
Metanet Tplatform

Microsoft Sentinel Workshop

Microsoft Sentinel Workshop 개요

이틀 간의 Microsoft Sentinel 워크샵을 통해 고객사이트에 강화된 클라우드 보안 가시성 확보 및 보안 강화를 제시하고, 아울러 Microsoft 365 라이선스 확보 또는 업그레이드를 통해 보안위협에 대응할 수 있고 워크로드 보호를 위한 보안이 한층 강화된 Azure Service들을 제시하고자 합니다.



Workshop 커리큘럼I

Workshop은 이틀에 걸쳐서 진행되며, 기본적인 내용부터 시작하여 고급 기능까지 활용할 수 있는 수준을 목표로 진행됩니다.

Day1 — 워크샵 Kick-off (1 hours)

Goals:
- Kick-off meeting
  - -MS 및 MTP보안 서비스 소개
    ex) 보안관제 서비스 등
  - -범위 및 제공 문서 정의
  - -사용할 툴/환경 정의
  - -향후 일정 및 계획 소개

Day1 — Sentinel서비스 소개 (2) (2 hours)

Goals:
- KQL(kusto Query Language) 소개
- MS Sentinel 위협 인텔리전트
- MS Sentinel 위협 헌팅

Day2 — 워크샵 Kick-off (1 hours)

Goals:
- 데모8 위협지표 관리
- 데모9 규칙생성
- 데모10 플레이북 생성
- 데모11 스케쥴 쿼리 생성
  ~
- 데모15 Sentinel 노트북 생성

Day1 — Sentinel서비스 소개 (1) (2 hours)

Goals:
- MS Sentinel Overview
- MS Sentinel 작업영역 생성
- MS Sentinel 데이터 수집

Day2 — Sentinel 데모(1) (2 hours)

Goals:
- 데모1 작업영역 생성하기
- 데모2 데이터 수집 커넥터 연결하기
- 데모3 화면구성
- 데모4 KQL의 기본 쿼리
  ~
- 데모 7 KQL 다중 테이블 작성

Day2 — Wrap up (1 hours)

Goals:
- 데모 결과 요약 및 정리
- 향후 일정 계획 수립
- 다음 단계 일정 조율

Workshop 커리큘럼II

Workshop 후에 고객은 Sentinel을 통하여 고객 환경에서 실질적으로 필요한 부분에 대해 리포트로 지정하여 확인할 수 있습니다. 또한, 현재의 보안 수준이 컴플라이언스나 사내 규정과 비교하여 미흡한 부분을 직관적으로 인지한 후에 필요한 조치를 취할 수 있습니다.

워크샵 사전 준비

Microsoft Sentinel 작업 영역 생성

데이터 수집 Connector연결
- AWS(Amazon Web Services)
- Microsoft Defender for Cloud
- Microsoft 365 Defender
- Windows 보안 이벤트
- CEF(Common Event Format)
- 사용자 지정 커넥터

데이터 분석
- 예약된 쿼리 규칙 만들기
- NRT(Near-Real-Time)규칙 만들기
- Anomaly 규칙 만들기
- UEBA 규칙 만들기
- (User & Entity Behavior Analytics)

Kusto Query Language
- 화면 구성 살펴보기
- 기본 쿼리문
- 결과 분석 - 연산자 활용
- 차트 결과 나타내기
- 다중 테이블 작성하기

위협 인텔리전스
- 위협 인텔리전스 플랫폼 연결
- 위협 인디케이터 작업

데이터 시각화 및 모니터링
- 데이터 시각화
- Azure Monitor
- 통합 문서 활용

위협 헌팅
- Notebooks 활용
- Bookmark 활용
- Livestream 활용

통합문서 (Workbooks)만들기
- 기본 제공 통합 문서
- 사용자 정의 통합 문서

영업문의 _ mtp.security@metanet.co.kr

Metanet Tplatform

Microsoft Sentinel소개

Microsoft Sentinel에 Microsoft 365 서비스의 인시던트를 통합하고 보안을 강화하여 Microsoft 365 서비스를 보다 안정적이고 안전한 환경에서 제공받을 수 있습니다.

Microsoft 365 서비스 활성화 및 보안 강화를 위한
Microsoft Sentinel & Microsoft 365 통합

인시던트 통합

- 두 포털 간에 보안 인시던트 동기화 상태 유지
- 인시던트에는 관련된 모든 경고, Entity 및 관련 정보 포함
- 심사 및 예비 조사를 수행할 수 있는 충분한 컨텍스트 제공

사건 해결 시간 단축

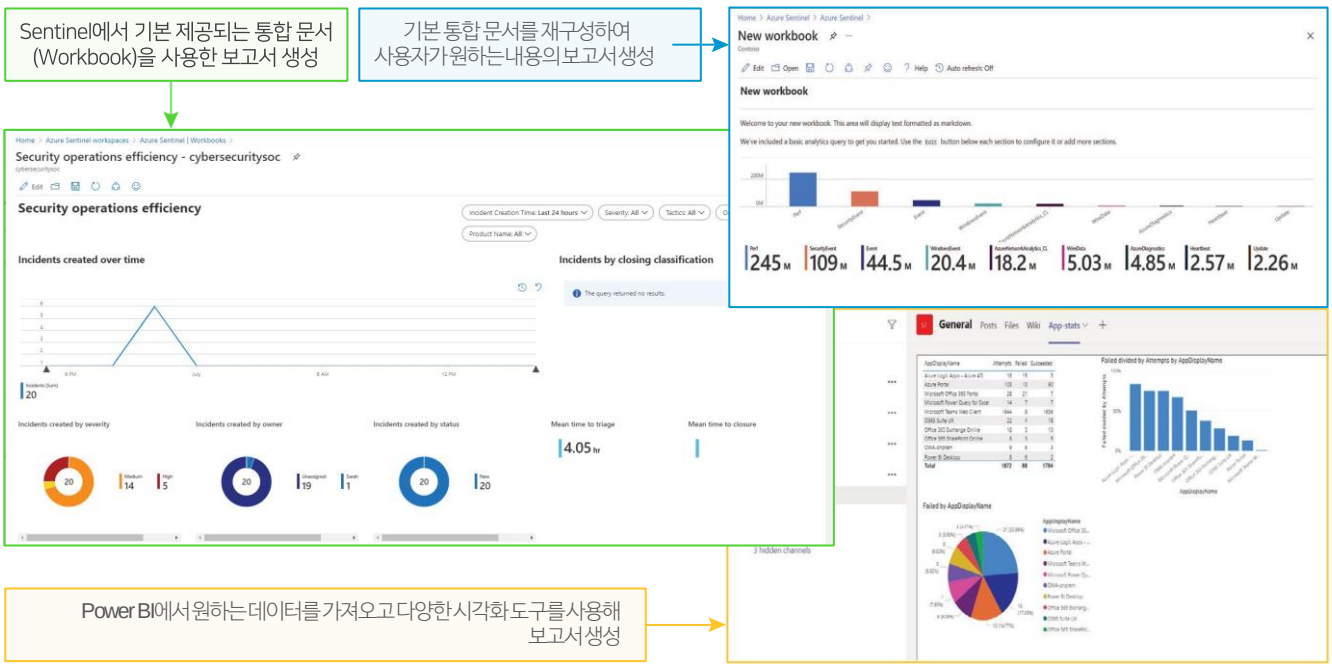
- 전체 조직의 기본 인시던트 큐의 일부로 Microsoft Sentinel에서 관리할 수 있는 가시성 제공
- Microsoft 365 인시던트의 상관 관계 지정
- Microsoft 365 제품의 경고를 강화하고 그룹화하여 SOC의 인시던트 큐 크기를 줄임으로써 해결 시간 단축

고급 헌팅 이벤트 수집

- 기존 엔드포인트용 Microsoft Defender/Office 365 고급 헌팅 쿼리를 변경없이 Microsoft Sentinel에 적용
- 원시 데이터를 사용하여 경고, 헌팅 및 조사에 대한 추가 인사이트 제공
- Microsoft Sentinel의 다른 데이터 원본 이벤트와 상호 연결

Workshop 결과예시

Workshop 후에 고객은 Sentinel을 통하여 고객 환경에서 필요로 하는 항목에 대한 정보만 리포트로 지정하여 확인할 수 있습니다. 또한, 현재의 보안 수준이 컴플라이언스나 사내 규정과 비교하여 미흡한 부분을 직관적으로 인지한 후에 필요한 조치를 취할 수 있습니다.



Metanet Cloud SOC 소개

Metanet Tplatform은 Metanet 그룹의 정보보안 관련 전문 핵심 기술력을 기반으로 서비스 및 컨설팅 능력을 갖추고 신기술에 대한 신속한 대응 및 기술지원으로 항상 고객에게 최상의 솔루션과 서비스를 제공합니다.

MSSP*

Microsoft

한국 마이크로소프트

Cloud Implemetation

클라우드 컨설팅 | Migration | Optimization | 클라우드 보안

Cloud Service

프라이빗 & 퍼블릭 클라우드

국내 최초 마이크로소프트 MSSP 파트너 | 인프라 솔루션 공급 | 클라우드 인프라/플랫폼 | 온프레미스-클라우드 보안 | 시스템 운영/유지보수

Managed Security Service Provider

Microsoft Sentinel Workshop 목표

고객은 워크샵을 통해서 Sentinel의 지능형 보안 분석 및 위협 인텔리전스를 이용한 온프레미스 및 클라우드 환경 전반에 걸친 활성 화된 위협을 탐지하고 신속하게 위협을 차단하며, 자동화된 위협 대응 방법에 대해서 익힐 수 있습니다.

요구 분석

SIEM* 도입 시 고객의 요구 사항 및 우선 순위

* Security Information and Event Management

범위 정의 및 도입

Microsoft 및 타사 솔루션이 통합된 프로덕션 환경에서 범위 정의 및 Microsoft Sentinel 도입 방안

원격 관제*

경보 및 로그 수집과 원격 관제

*선택적구성 요소 논의

위협 인텔리전스

이메일, ID 및 데이터 전반에 걸쳐 온프레미스, 클라우드 환경에 대한 위협을 발견하고 응답을 자동화하는 방법

권장 절차

Microsoft Sentinel의 프로덕션 구현 방법과 추진 절차

Workshop 기대효과

클라우드 네이티브 SIEM으로써 Microsoft Sentinel만의 장점을 알게 되고 잠재적 위협에 대한 충분한 이해와 우선 순위를 지정하여 배포 로드맵과 목표에 따른 추진 절차를 정의함으로써 도입 추진 전략을 마련할 수 있습니다.

through Microsoft Sentinel Workshop

01	클라우드 네이티브 SIEM의 장점 이해
02	잠재적 위협에 대한 깊은 이해를 바탕으로 우선 순위 지정
03	배포 로드맵 정의
04	요구 사항과 목표에 따라 추진 절차 정의

Why deliver the Microsoft Sentinel Workshop

01	맞춤형	특정 보안 요구사항 집중
02	시연	데모* 또는 예제화면을 통한 시연
03	솔루션 도입 계획	실행가능한 계획 수립

*고객환경or테스트필드