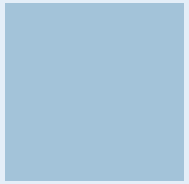
SECURE ON
Adoption & Managed Service

Azure Sentinel
SecureON for Sentinel
: 2wk Assessment



씨앤토트

INDEX

01

Azure Sentinel 이란?

Azure Sentinel이란?

• **클라우드 SIEM** : Digital Transformation 시대에 발맞춘 SIEM 솔루션

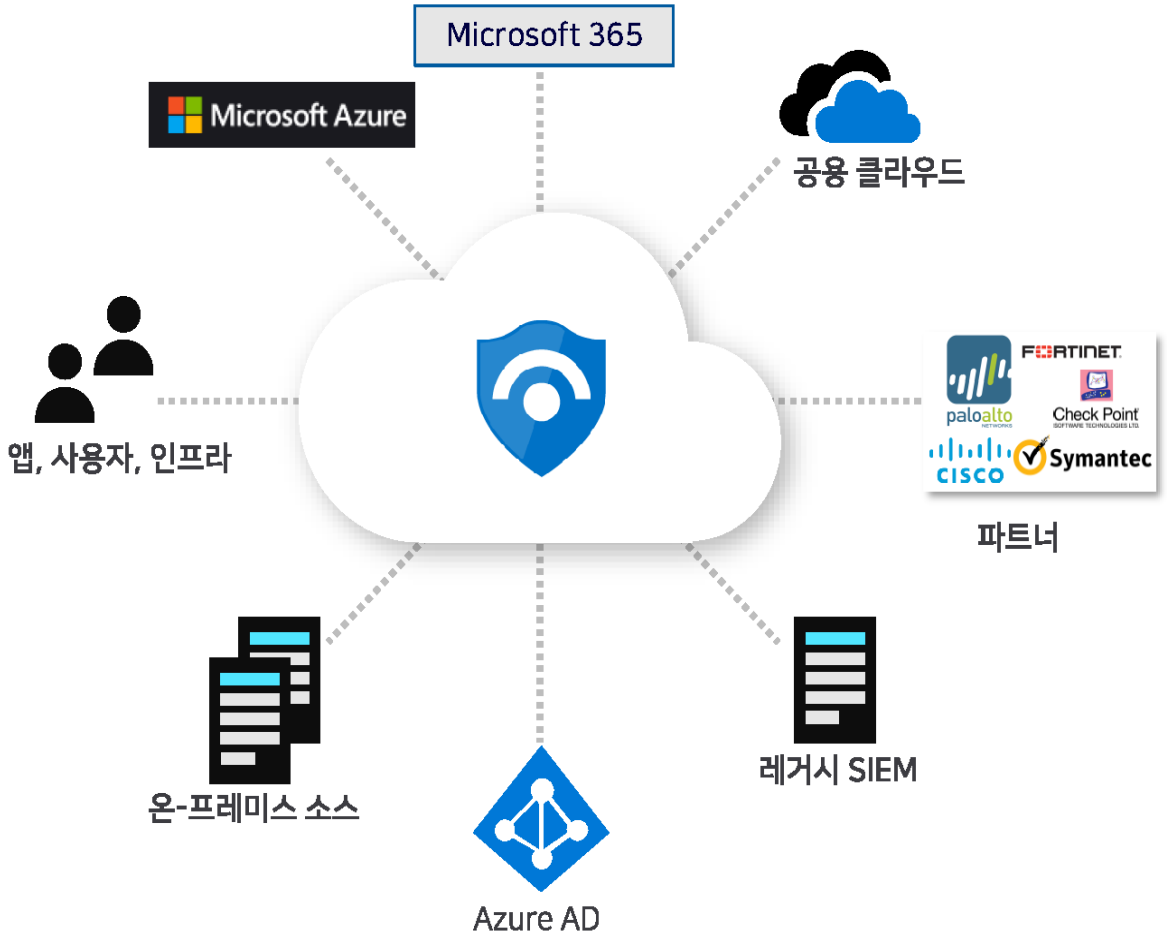
Microsoft 솔루션으로 **사전 통합**

많은 파트너 솔루션을 위한 **커넥터**

모든 소스에 대한 **표준 로그 포맷** 지원

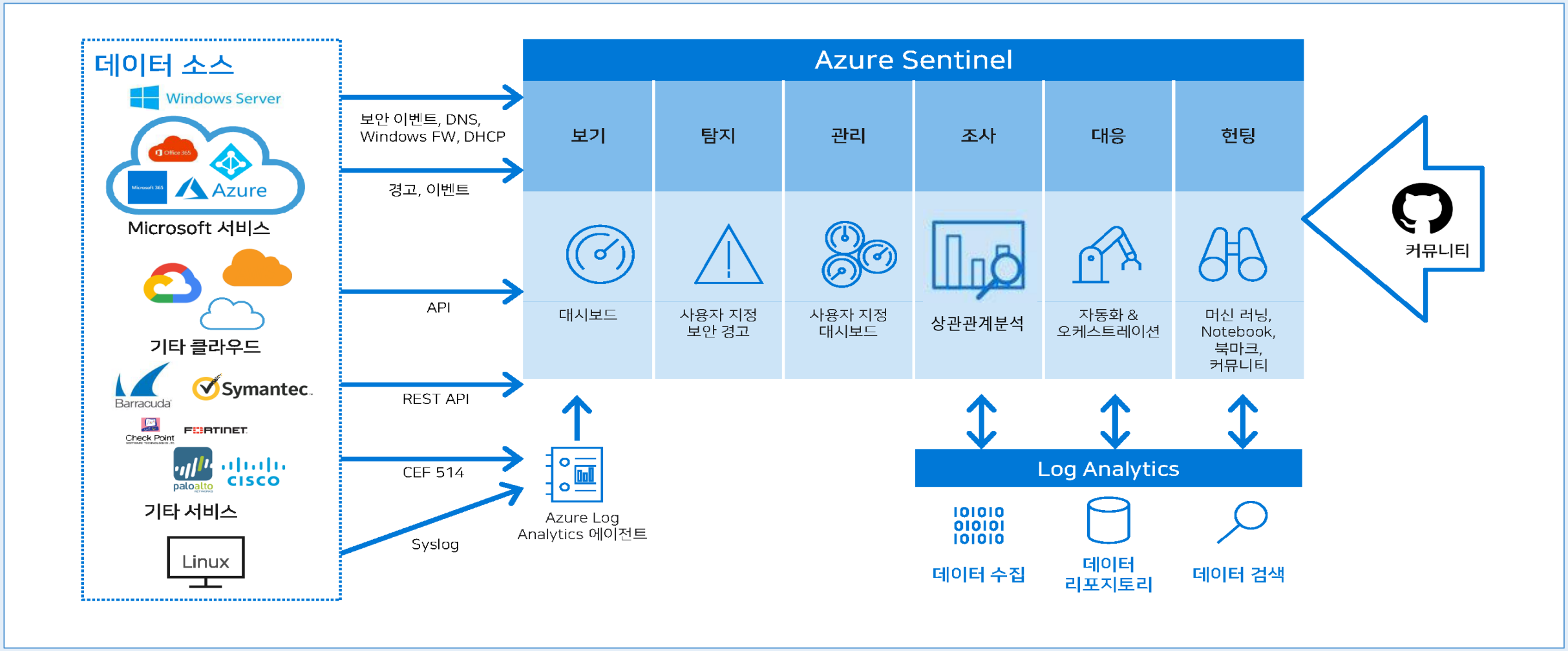
일일 수집량이 **10 petabyte 이상**인 입증된 로그 플랫폼

Legacy SIEM 솔수션 대비 비용48% 절감



Azure Sentinel이란?

- **연동 및 기능** : 연동가능한 데이터 소스와 센티널의 기능



02

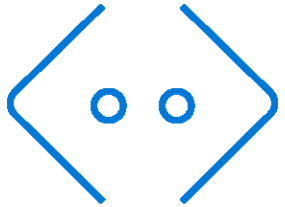
Azure Sentinel 연동 방법

Azure Sentinel 연동방법

- **연동 종류** : 커넥터를 통한 직접 연결 및 Agent기반 연결

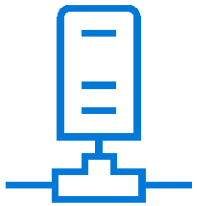
직접 연결

데이터 커넥터 내에서 연결하고 Sentinel로 스트리밍할 로그를 선택



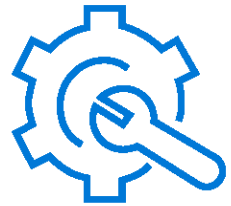
에이전트

데이터 커넥터를 구성하기 위해 Windows 혹은 Linux 용 Log Analytics 에이전트를 반드시 설치해야 함



에이전트가 있는 Syslog 서버

데이터 커넥터를 구성하기 위해 Log Analytics 에이전트가 있는 Syslog 서버가 필요함



직접 API

로그 소스에 연결하기 위해 수동 구성이 필요함

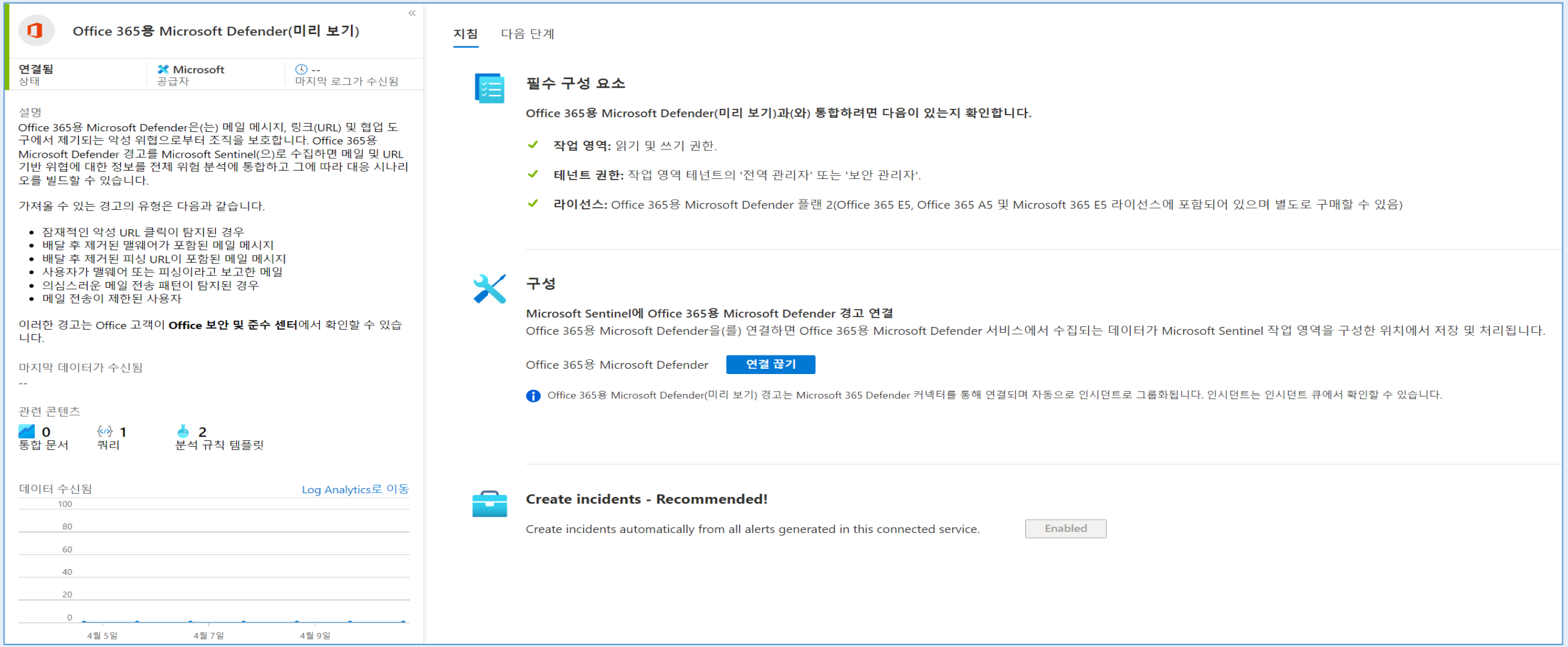
Azure Sentinel 연동방법

- **데이터 커넥터** : Microsoft 제품 및 3rd Party 솔루션에 대한 손쉬운 연동

Microsoft 365 내부 위험 관리 (미리 보기) Microsoft	Amazon Web Services Amazon	F5 BIG-IP F5 Networks
Microsoft 365 Defender (미리 보기) Microsoft	Amazon Web Services S3 Amazon	F5 Networks F5 Networks
Microsoft Defender for Cloud Microsoft	Apache HTTP Server (미리 보기) Apache	Facebook의 작업 영역 (미리 보기) Facebook
Microsoft Defender for Cloud Apps Microsoft	Apache Tomcat (미리 보기) Apache	Forcepoint CASB (미리 보기) Forcepoint
Microsoft Defender for Identity Microsoft	Aruba ClearPass (미리 보기) Aruba Networks	Forcepoint CSG (미리 보기) Forcepoint
Microsoft PowerBI (미리 보기) Microsoft	Atlassian 구성 감사 (미리 보기) Atlassian	Forcepoint DLP (미리 보기) Forcepoint
Microsoft Project (미리 보기) Microsoft	Atlassian Jira 감사 (미리 보기) Atlassian	Forcepoint NGFW (미리 보기) Forcepoint
Office 365 Microsoft	Azure 활동 Microsoft	Fortinet Fortinet

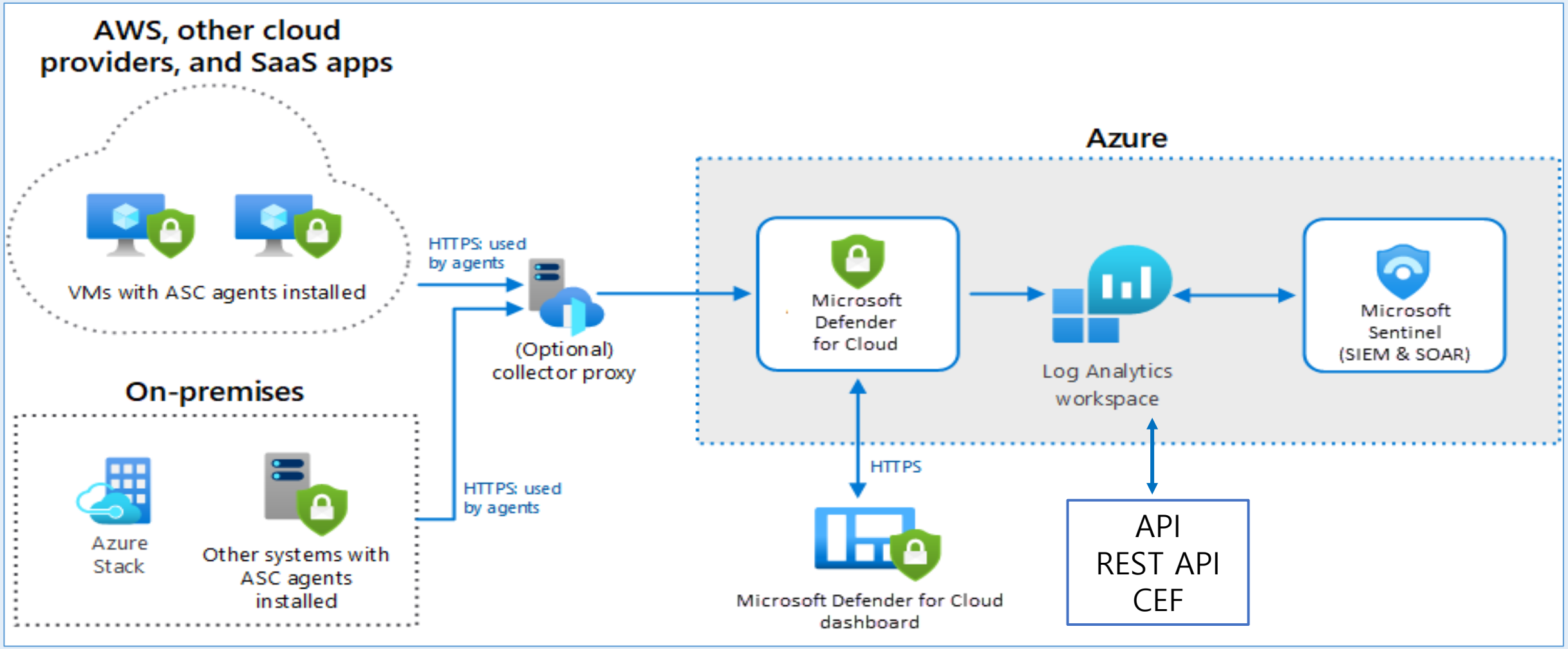
Azure Sentinel 연동방법

- **데이터 커넥터** : 연동에 필요한 필수 구성과 정보



Azure Sentinel 연동방법

- **Agent** : 커넥터로 제공되지 않는 장비들을 Agent 설치로 관리



03

Azure Sentinel 핵심 기능

Azure Sentinel 핵심 기능

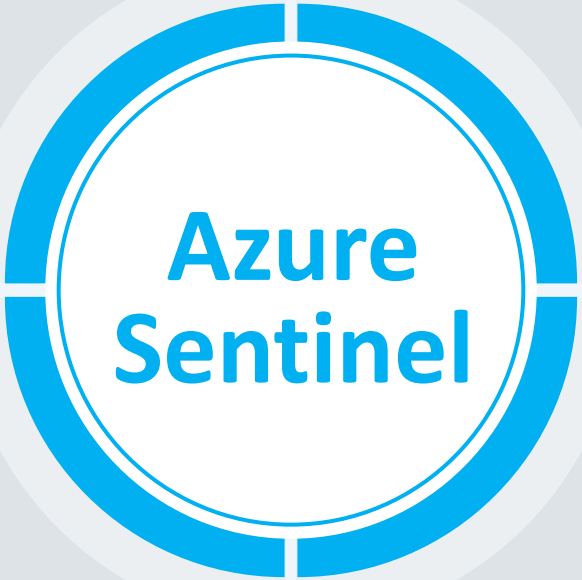
- 기업 환경에 맞게 수집된 수많은 이벤트를 분석
- 위험도에 따른 자동화 대응과 대시보드 커스터마이징

헌팅

✓ 위험요소에 대한 즉각적인 검색
✓ MITRE 매트릭스로 사전 위협 조사
✓ 이벤트에 대한 Livestream 모니터링

분석 및 인시던트

✓ 경고를 트리거하여 인시던트 생성
✓ 위험요소에 대한 검색 규칙을 예약
✓ 상관관계 분석 및 이상 징후 식별



플레이북

✓ 인시던트 발생시 Playbook으로 대응
✓ 관리자에게 메일, 채팅으로 알림
✓ 위험 노출시 자동화 대응 구성

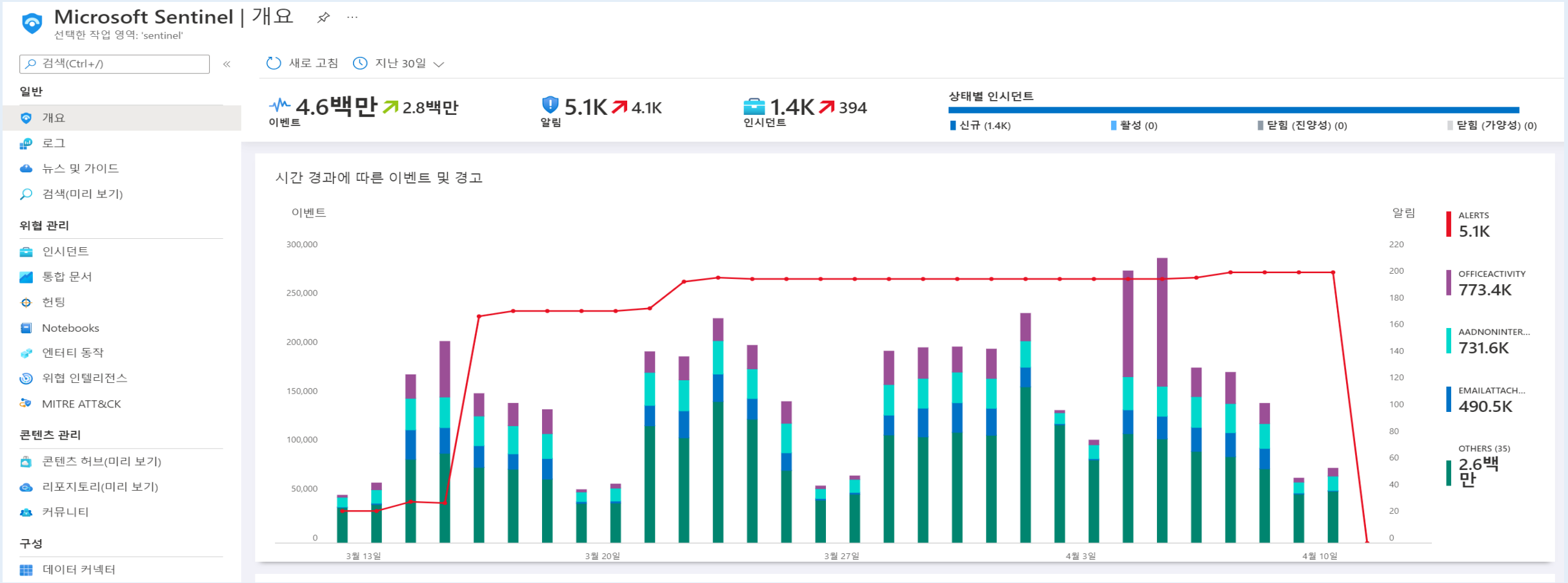
통합문서

✓ 수집한 데이터 전체 가시화
✓ 관리자 설정 대시보드
✓ 다양한 시각화 지원

Azure Sentinel 핵심 기능

- **Sentinel 관리 페이지** : 수집된 로그량과 발생된 인시던트에 대해 확인 가능

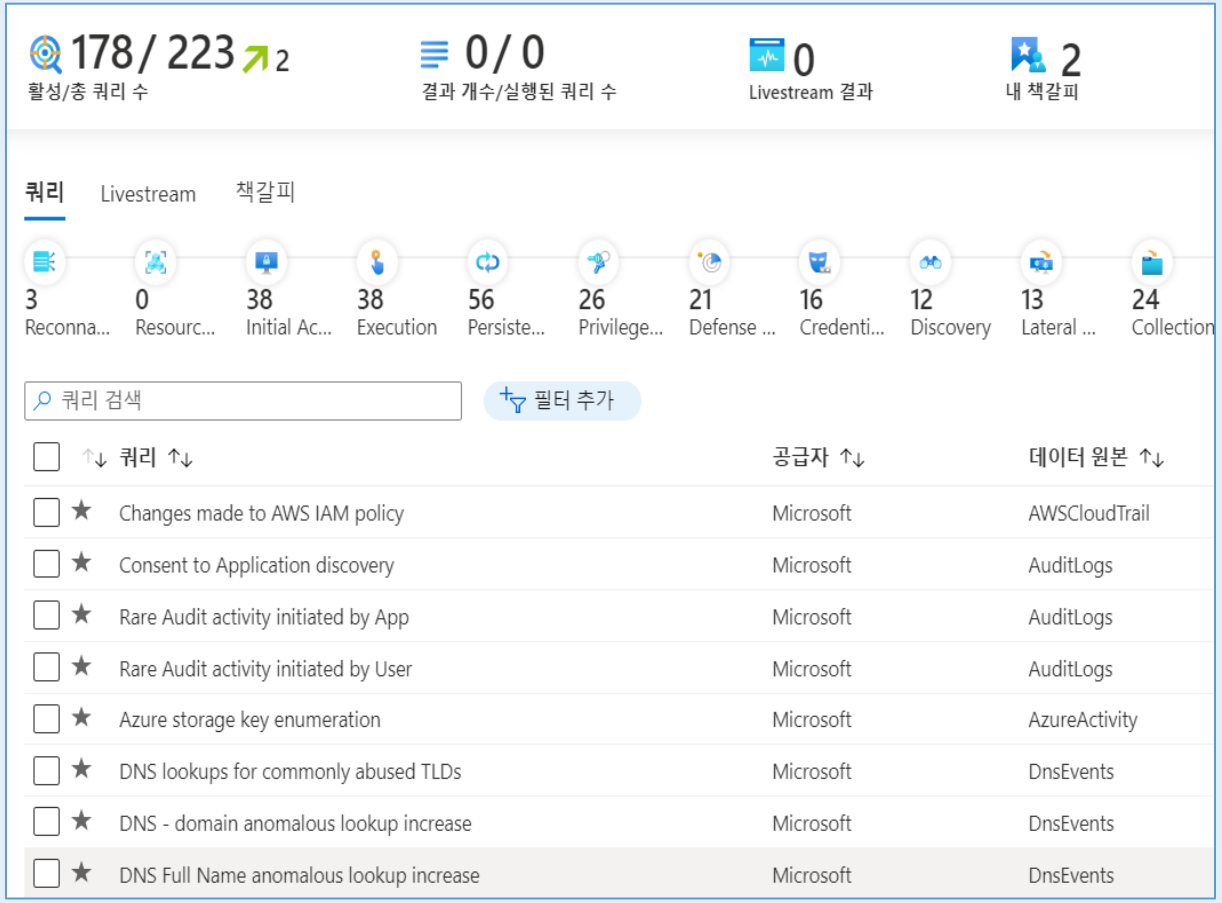
데이터 수집량 및 이벤트



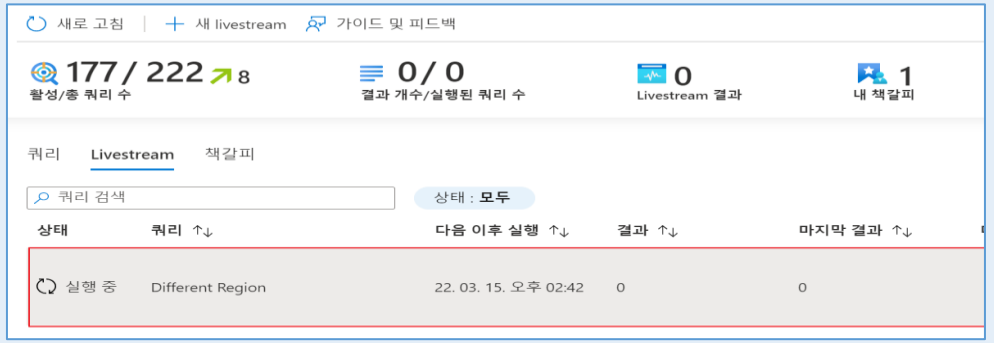
Azure Sentinel 핵심 기능

- **헌팅** : MITRE ATT&CK 매트릭스 실시간 이벤트 확인

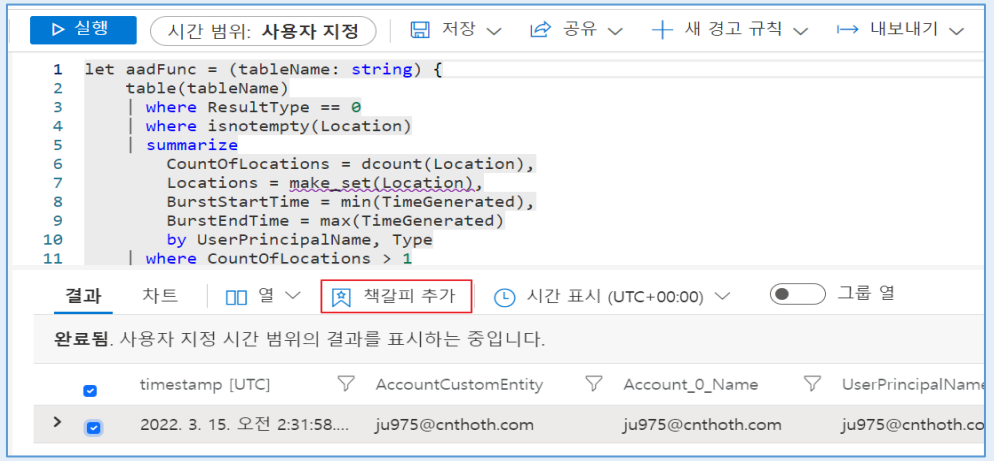
MS제공 기본 헌팅 쿼리



라이브스트림 대화형 세션



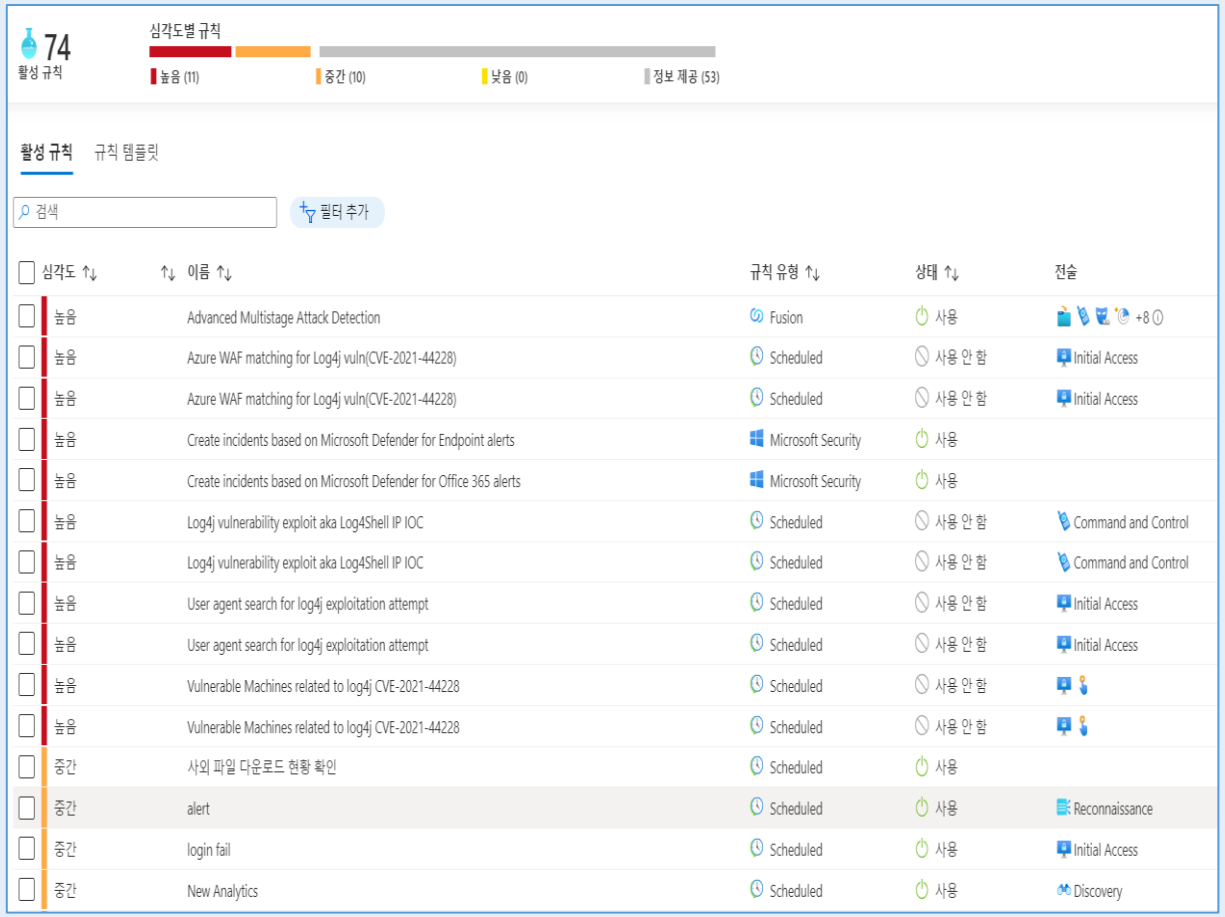
책갈피로 관리자 공유



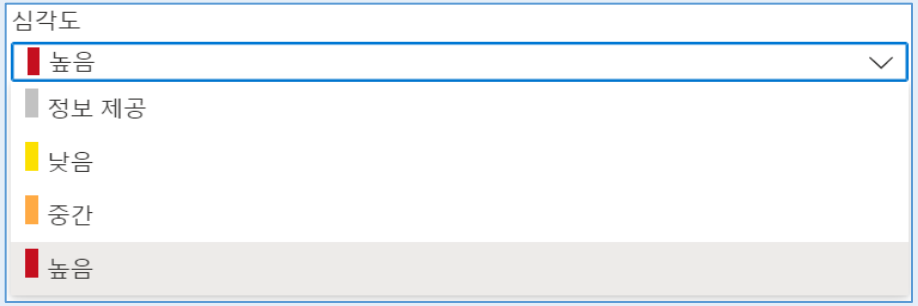
Azure Sentinel 핵심 기능

- **분석** : 위험요소 분석을 스케쥴로 정책 구성

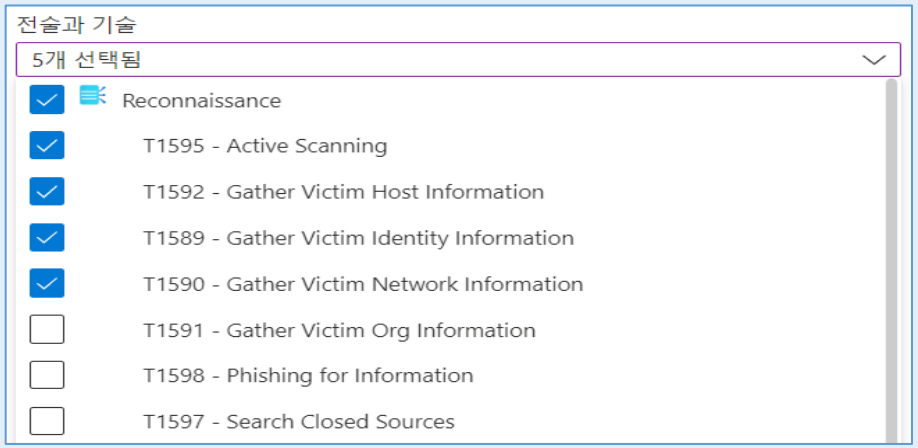
분석 정책 상태



심각도 선택



전술 선택

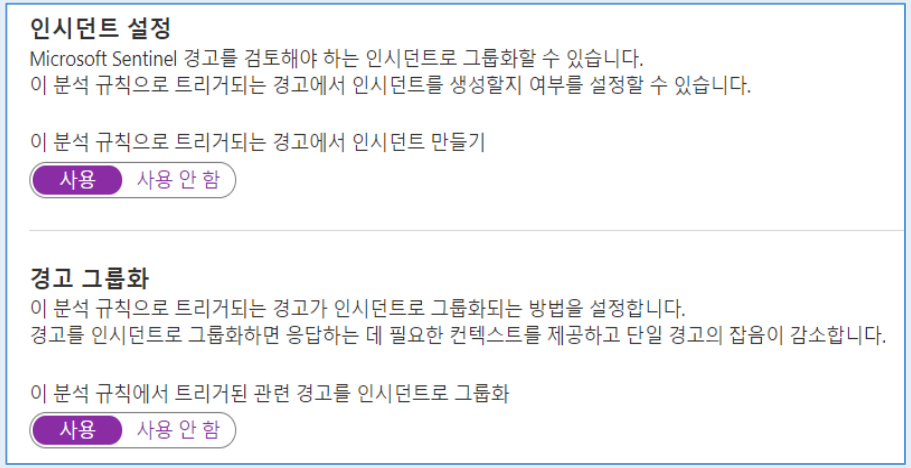


Azure Sentinel 핵심 기능

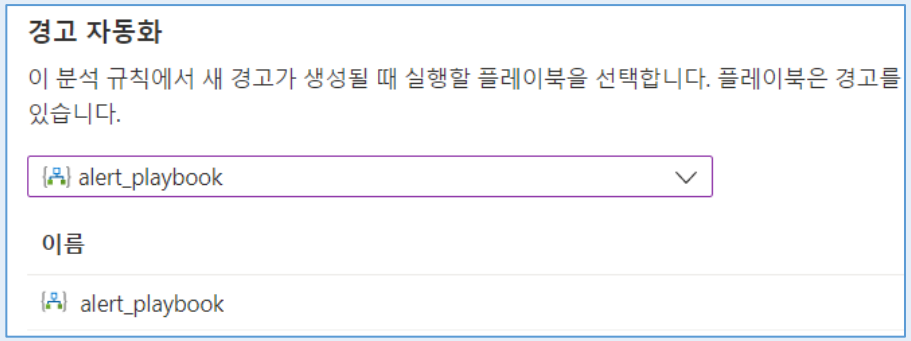
• **분석** : 위험요소 분석을 스케쥴로 정책 구성

스케쥴 세부 설정

인시던트 및 경고 선택



자동화 선택

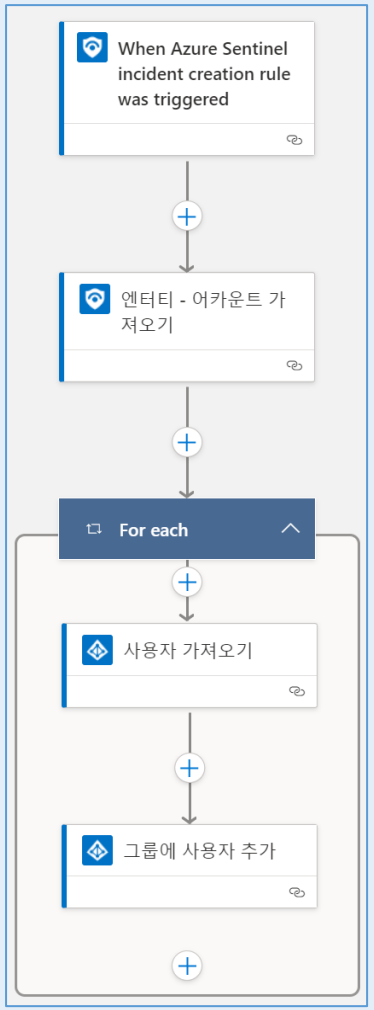


Azure Sentinel 핵심 기능

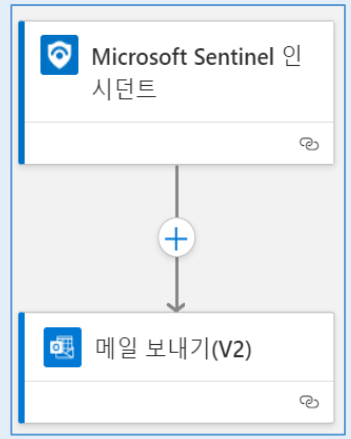
- **자동화** : 경고 및 인시던트에 대해 관리자 알림 및 사용자 격리

자동화 정책 상태

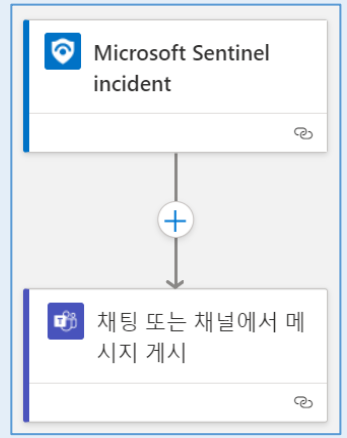
차단 그룹 이동



관리자 메일 전송



팀즈 채팅 전송

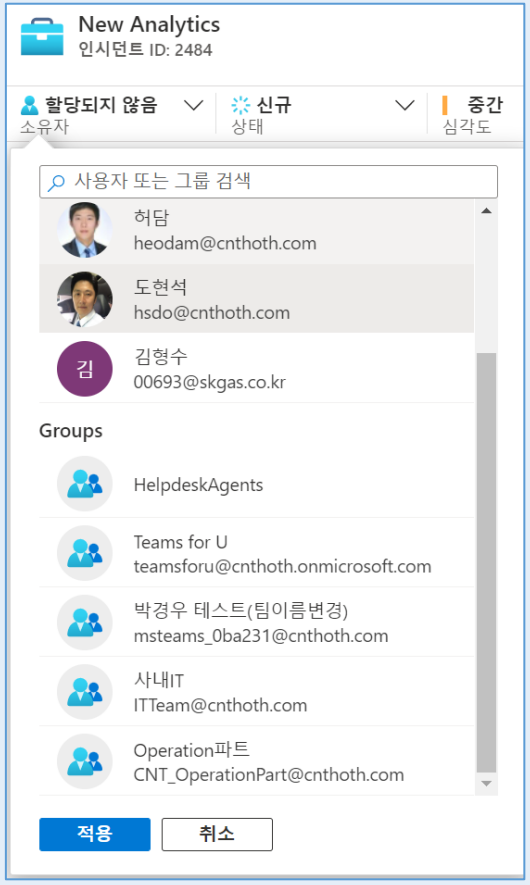


Azure Sentinel 핵심 기능

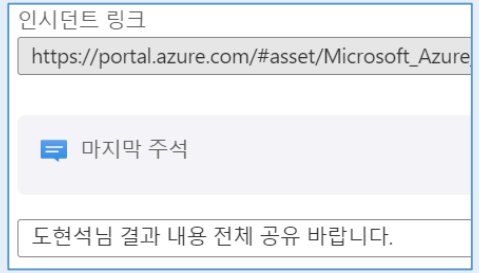
• **인시던트** : 분석 규칙을 통해 생성되는 이벤트

인시던트 생성 현황

인시던트 관리자 지정



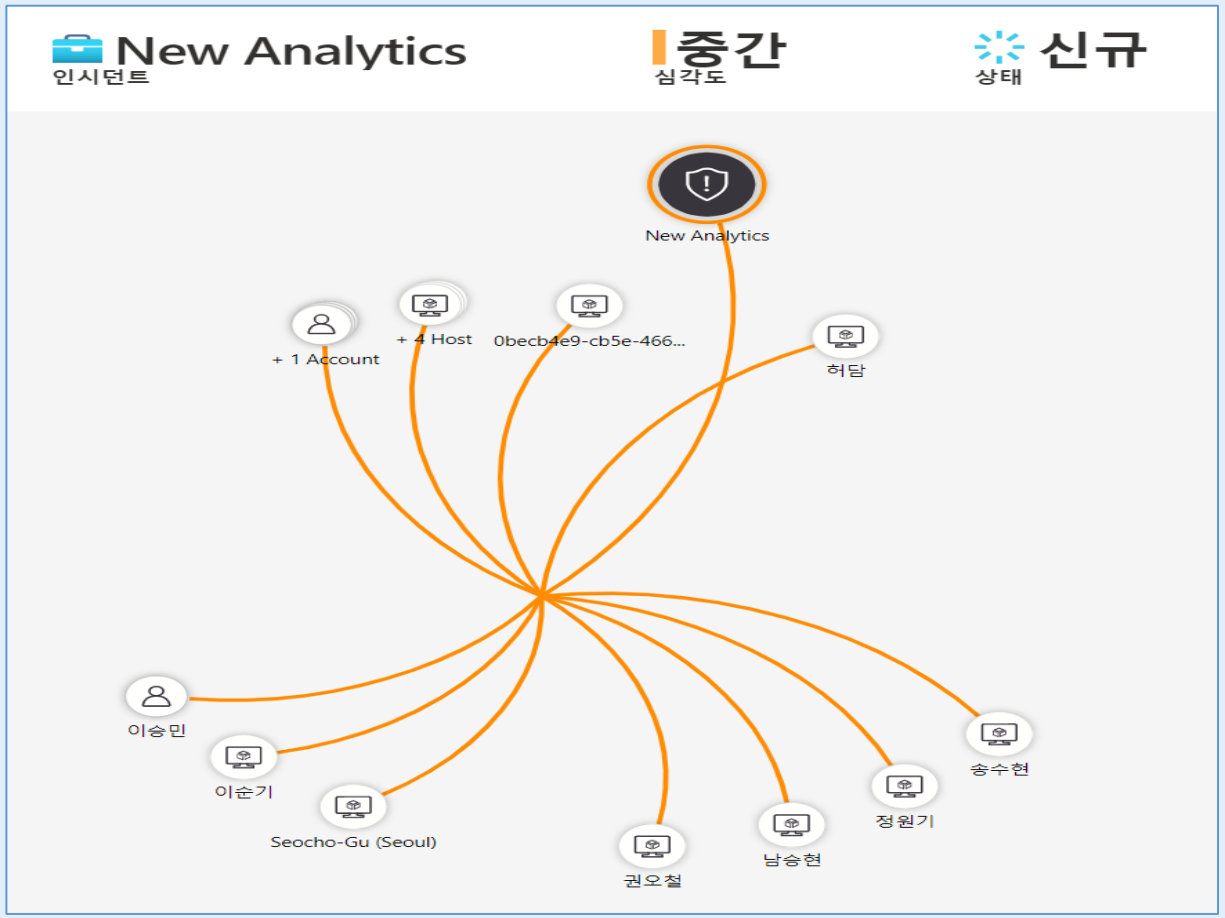
메모 기능 제공



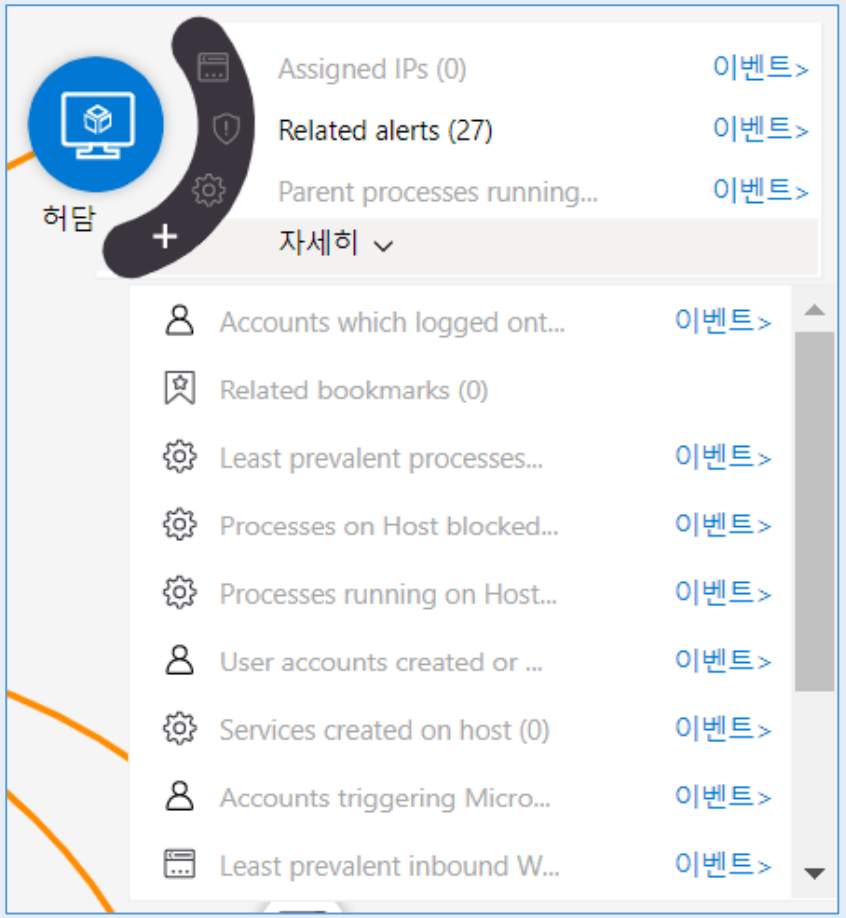
Azure Sentinel 핵심 기능

• **조사** : 인시던트 발생 시 상관관계 분석 가능

상관관계 분석 내용



특정사용자 상관관계 분석

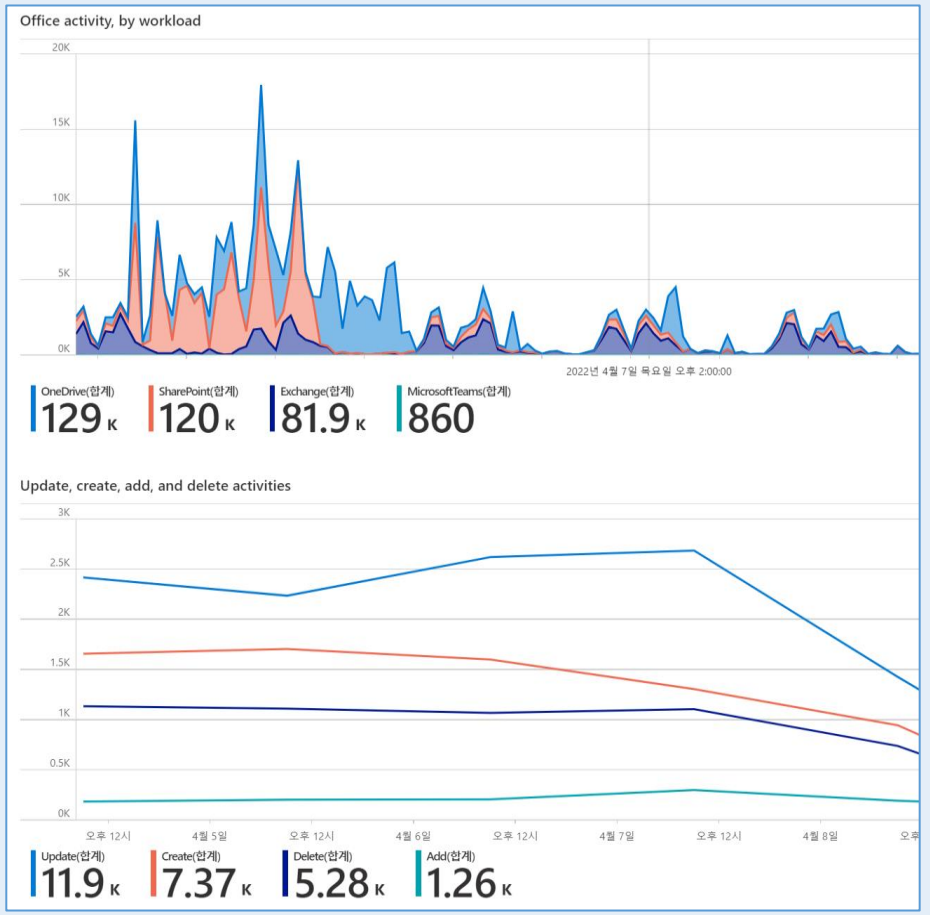


Azure Sentinel 핵심 기능

- **통합문서** : 생성된 인시던트나 사용 이력을 대시보드로 구성

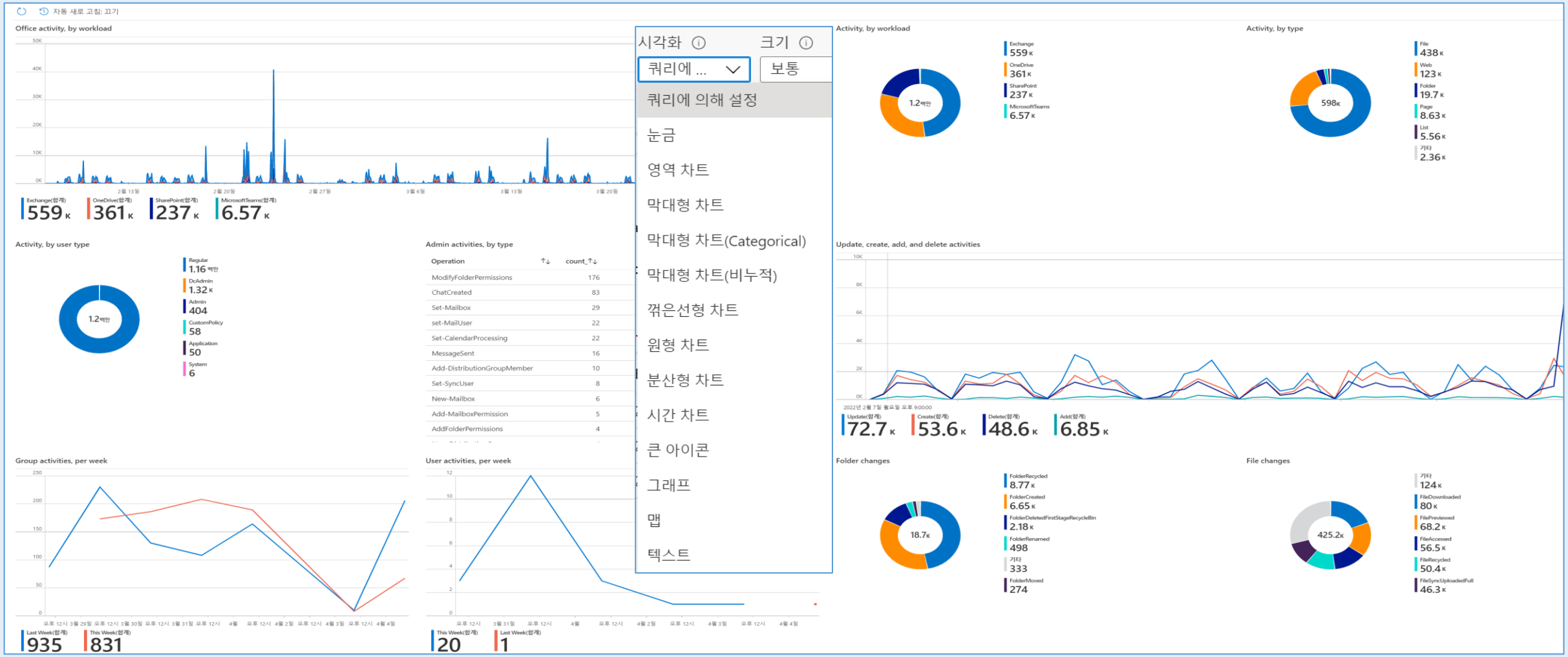
기본 제공 템플릿 형식

항목별 커스터마이징 가능



Azure Sentinel 핵심 기능

- **통합문서** : 각 항목별 데이터를 환경에 따라 시각화 구성



04

Sentinel Workshop

씨앤토트

Cloud Native SIEM Solution

Azure Sentinel Workshop (2 Weeks)

Microsoft Sentinel은 확장 가능한 클라우드 네이티브, **SIEM(보안 정보 및 이벤트 관리)** 및 **SOAR(보안 오케스트레이션, 자동화 및 응답)** 솔루션입니다. Microsoft Sentinel은 엔터프라이즈 전반에 걸쳐 지능형 보안 분석 및 위협 인텔리전스를 제공하여 공격 탐지, 위협 가시성, 사전 예방적 사냥 및 위협 대응을 위한 단일 솔루션을 제공합니다

온보딩
Azure Sentinel 활성화

데이터 연결
분석을 위한 데이터 수집 진행
데이터 커넥터, Agent 및 syslog

분석 계획 수립
사용자 위험 행위 분석 계획
위험 요소 분석 계획

결과 공유
추천 방안 제시 및 향후 계획 수립

필수 권한 및 구성

Azure Sentinel을 시작하기 위한 필수 권한 및 구성

- 활성 Azure 구독. 계정이 없는 경우 시작하기 전에 무료 계정을 만듭니다.
- Sentinel 서비스를 생성하기 위해 리소스 그룹 소유자 및 보안관리자 필요
- 생성 후 Sentinel, Log 분석 작업 영역에 기여자 권한, 판독기 권한 필요
- 특정 데이터 커넥터 원본을 연결하기 위한 추가 권한이 필요 할 수 있음

기대효과

데이터 분석을 통한 위험 요소 분석 및 보안 강화 할 수 있도록 적절한 시나리오를 검토합니다.

- Azure Sentinel을 활용한 관리 개선 방안 도출
- 사용자 및 보안솔루션의 보안 정책에 대한 인사이트 확보
- 사용자, 회사 데이터를 활용한 보안 정책 수립과 관리 도구의 활용 방법
- 보안 관리자가 위험요소에 대한 즉각적인 처리 및 가시성 확보를 위한 대시보드 구성
  SOAR를 통한 즉각적인 대처 방안
  (편의성 증대/보안 강화)

씨앤토트

Sentinel 구성을 통한 보안, 위험 요소 제어, 고급 분석 활용

Azure Sentinel Workshop

Agenda

진행 항목	설명	예상 기간
사전 미팅 및 Azure Sentinel 온보딩	미팅을 통한 기업 환경 분석 및 분석 범위 정의 필수 권한 계정으로 Azure Sentinel 및 Log Analytics 작업 영역 온보딩	1 - Day
데이터 수집	제공되는 커넥터를 활용하여 데이터 연동 Agent 설치를 통한 서버 데이터 수집 Syslog 서버에 Agent 설치를 통한 데이터 수집 충분한 데이터 수집까지 시간 소요	5 – Day
분석 계획 수립	수집된 데이터를 기반으로 분석 계획 수립 기업 환경에 따른 위험도 정의 위험도에 따른 알림, 인시던트 생성 SOAR 구성	5 – Day
MITRE ATT&CK 정책 활성화	기업 환경에 맞춰 MITRE ATT&CK 위험요소 탐지 정책을 활성화	1 – Day
대시보드 구성	위험요소 가시성 확보를 위한 통합 대시보드 커스터마이징 요청 사항에 맞춰 디자인 구성	1 – Day
결과 공유	현재 환경 개선과 향후 성공적인 Sentinel 관리를 위한 결과 보고서 공유	1 - Day
비고	**실제 작업 일정은 기업 환경에 따라 변경 될 수 있습니다.**	

SECURE ON
Adoption & Managed Service

THANK YOU

secureon@cnthoth.com
www.cnthoth.com