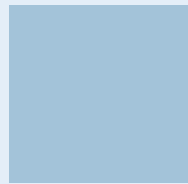


# Azure Sentinel

## SecureON for Sentinel

### : 2wk Assessment



# INDEX

- 01 / Azure Sentinel 이란
- 02 / Azure Sentinel 연동 방법
- 03 / Azure Sentinel 핵심 기능
- 04 / Sentinel Workshop

# 01

**Azure Sentinel 이란?**

# Azure Sentinel이란?

- 클라우드 SIEM : Digital Transformation 시대에 발맞춘 SIEM 솔루션

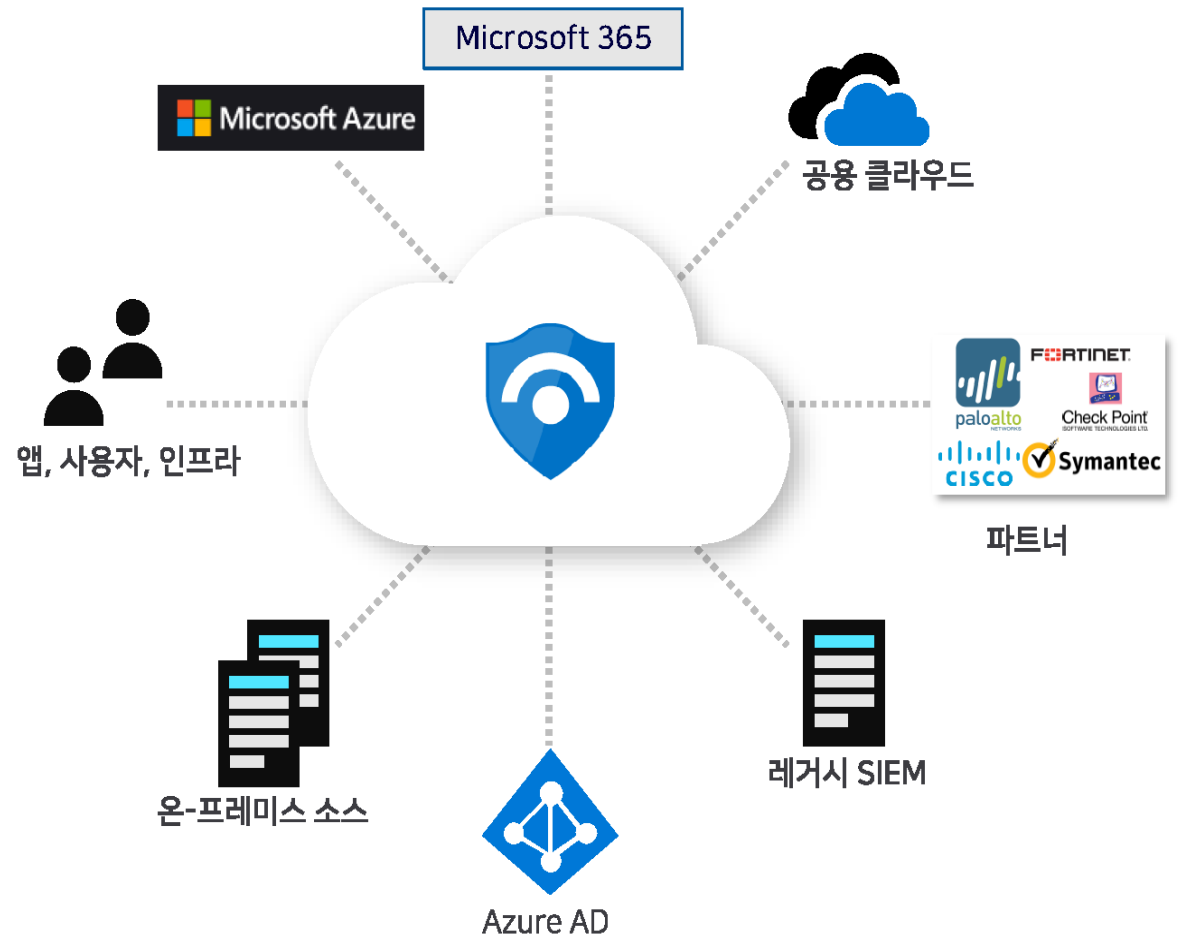
Microsoft 솔루션으로 **사전 통합**

많은 파트너 솔루션을 위한 **커넥터**

모든 소스에 대한 **표준 로그 포맷** 지원

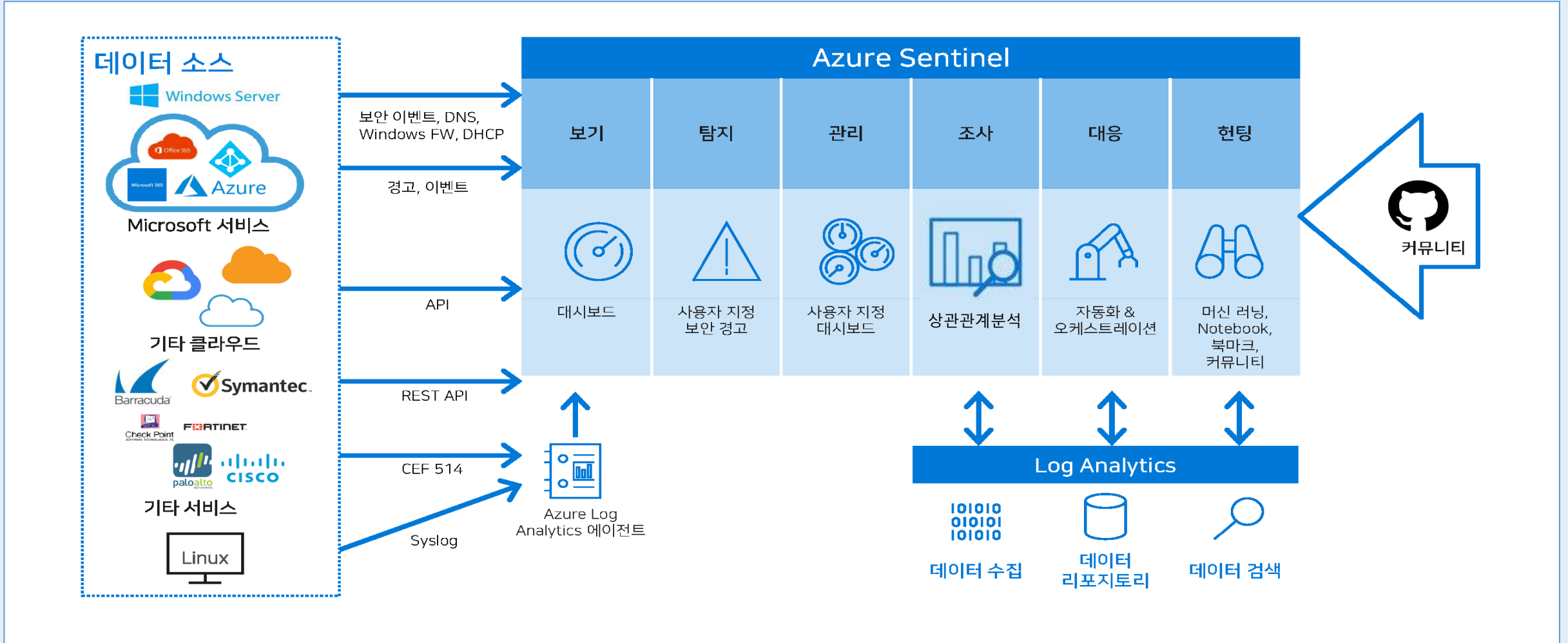
일일 수집량이 **10 petabyte 이상**인 입증된 로그 플랫폼

**Legacy SIEM** 솔루션 대비 **비용 48% 절감**



# Azure Sentinel이란?

- 연동 및 기능 : 연동가능한 데이터 소스와 센티널의 기능



# 02

## Azure Sentinel 연동 방법

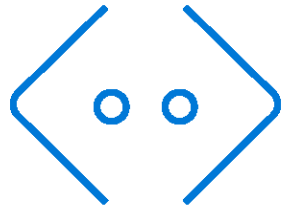
# Azure Sentinel 연동방법

- 연동 종류 : 커넥터를 통한 직접 연결 및 Agent기반 연결



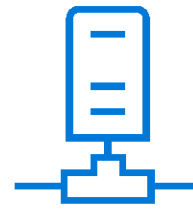
## 직접 연결

데이터 커넥터 내에서 연결하고 Sentinel로 스트리밍할 로그를 선택



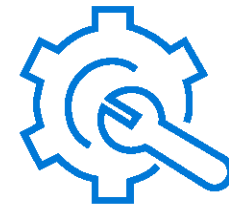
## 에이전트

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 위협 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

The screenshot displays the configuration page for the Office 365용 Microsoft Defender connector in Azure Sentinel. The page is divided into two main sections: '필수 구성 요소' (Prerequisites) and '구성' (Configuration).

**필수 구성 요소 (Prerequisites):**

- Office 365용 Microsoft Defender(미리 보기)과(와) 통합하려면 다음이 있는지 확인합니다.
- ✓ **작업 영역:** 읽기 및 쓰기 권한.
- ✓ **테넌트 권한:** 작업 영역 테넌트의 '전역 관리자' 또는 '보안 관리자'.
- ✓ **라이선스:** Office 365용 Microsoft Defender 플랜 2(Office 365 E5, Office 365 A5 및 Microsoft 365 E5 라이선스에 포함되어 있으며 별도로 구매할 수 있음)

**구성 (Configuration):**

Microsoft Sentinel에 Office 365용 Microsoft Defender 경고 연결  
Office 365용 Microsoft Defender을(를) 연결하면 Office 365용 Microsoft Defender 서비스에서 수집되는 데이터가 Microsoft Sentinel 작업 영역을 구성한 위치에서 저장 및 처리됩니다.

Office 365용 Microsoft Defender

**Office 365용 Microsoft Defender(미리 보기) 경고는 Microsoft 365 Defender 커넥터를 통해 연결되며 자동으로 인시던트로 그룹화됩니다. 인시던트는 인시던트 큐에서 확인할 수 있습니다.**

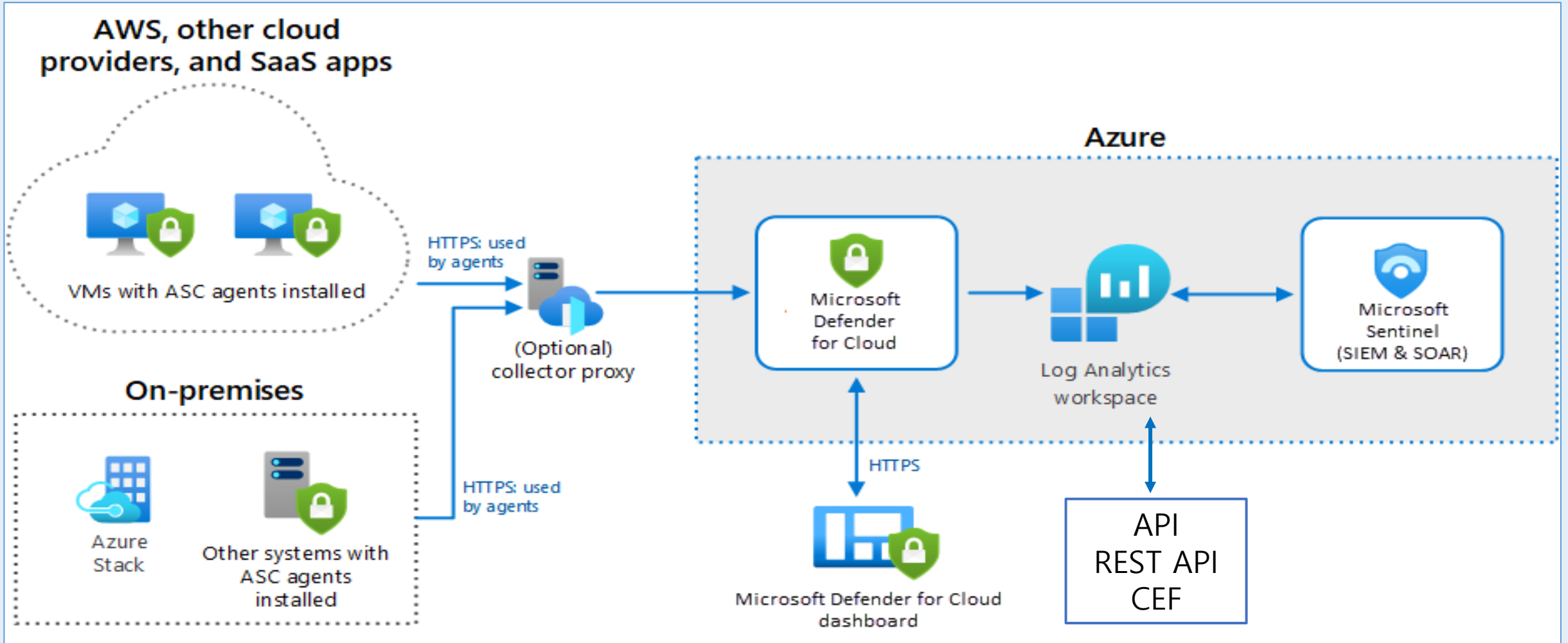
**Create incidents - Recommended!**  
Create incidents automatically from all alerts generated in this connected service.

**Left Panel Details:**

- 연결됨 상태:** Microsoft 공급자, --, 마지막 로그가 수신됨
- 설명:** Office 365용 Microsoft Defender은(는) 메일 메시지, 링크(URL) 및 협업 도구에서 제기되는 악성 위협으로부터 조직을 보호합니다. Office 365용 Microsoft Defender 경고를 Microsoft Sentinel(으)로 수집하면 메일 및 URL 기반 위협에 대한 정보를 전체 위협 분석에 통합하고 그에 따라 대응 시나리오를 빌드할 수 있습니다.
- 가져올 수 있는 경고의 유형은 다음과 같습니다:**
  - 잠재적인 악성 URL 클릭이 탐지된 경우
  - 배달 후 제거된 맬웨어가 포함된 메일 메시지
  - 배달 후 제거된 피싱 URL이 포함된 메일 메시지
  - 사용자가 맬웨어 또는 피싱이라고 보고한 메일
  - 의심스러운 메일 전송 패턴이 탐지된 경우
  - 메일 전송이 제한된 사용자
- 이러한 경고는 Office 고객이 Office 보안 및 준수 센터에서 확인할 수 있습니다.**
- 마지막 데이터가 수신됨:** --
- 관련 콘텐츠:** 통합 문서 0, 쿼리 1, 분석 규칙 템플릿 2
- 데이터 수신됨:** Log Analytics로 이동
- 그래프:** 데이터 수신량을 보여주는 선 그래프 (4월 5일, 4월 7일, 4월 9일)

# 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

Azure  
Sentinel

## 플레이북

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

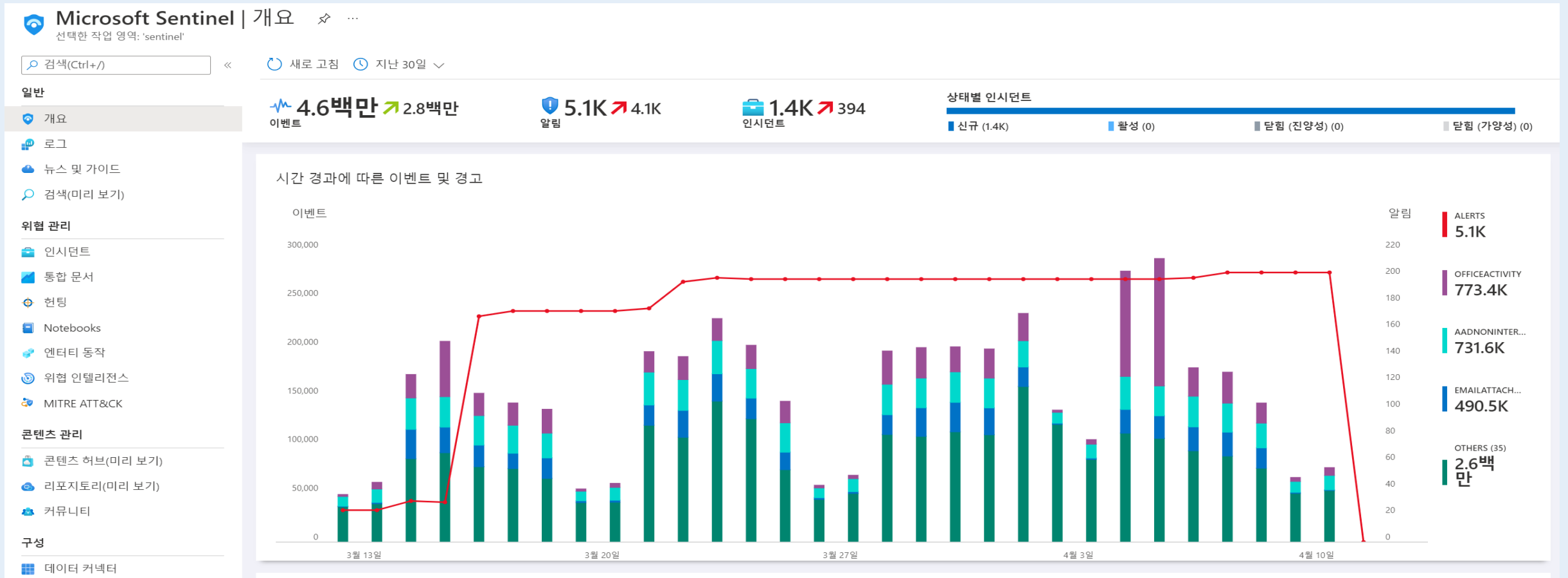
## 통합문서

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

# Azure Sentinel 핵심 기능

- Sentinel 관리 페이지 : 수집된 로그량과 발생한 인시던트에 대해 확인 가능

## 데이터 수집량 및 이벤트



# Azure Sentinel 핵심 기능

- 헌팅 : MITRE ATT&CK 매트릭스 실시간 이벤트 확인

## MS제공 기본 헌팅 쿼리

178 / 223 ↗2      0 / 0      0      2

활성/총 쿼리 수      결과 개수/실행된 쿼리 수      Livestream 결과      내 체크리스트

쿼리      Livestream      체크리스트

3      0      38      38      56      26      21      16      12      13      24

Reconn...      Resourc...      Initial Ac...      Execution      Persiste...      Privilege...      Defense ...      Credenti...      Discovery      Lateral ...      Collection

쿼리 검색      필터 추가

<input type="checkbox"/>	↑↓ 쿼리 ↑↓	공급자 ↑↓	데이터 원본 ↑↓
<input type="checkbox"/> ★	Changes made to AWS IAM policy	Microsoft	AWSCloudTrail
<input type="checkbox"/> ★	Consent to Application discovery	Microsoft	AuditLogs
<input type="checkbox"/> ★	Rare Audit activity initiated by App	Microsoft	AuditLogs
<input type="checkbox"/> ★	Rare Audit activity initiated by User	Microsoft	AuditLogs
<input type="checkbox"/> ★	Azure storage key enumeration	Microsoft	AzureActivity
<input type="checkbox"/> ★	DNS lookups for commonly abused TLDs	Microsoft	DnsEvents
<input type="checkbox"/> ★	DNS - domain anomalous lookup increase	Microsoft	DnsEvents
<input type="checkbox"/> ★	DNS Full Name anomalous lookup increase	Microsoft	DnsEvents

## 라이브스트림 대화형 세션

177 / 222 ↗8      0 / 0      0      1

활성/총 쿼리 수      결과 개수/실행된 쿼리 수      Livestream 결과      내 체크리스트

쿼리      Livestream      체크리스트

쿼리 검색      상태: 모두

상태	쿼리 ↑↓	다음 이후 실행 ↑↓	결과 ↑↓	마지막 결과 ↑↓
실행 중	Different Region	22. 03. 15. 오후 02:42	0	0

## 체크리스트로 관리자 공유

▶ 실행      시간 범위: 사용자 지정      저장      공유      새 경고 규칙      내보내기

```

1 let aadFunc = (tableName: string) {
2   table(tableName)
3   | where ResultType == 0
4   | where isnotempty(Location)
5   | summarize
6     CountOfLocations = dcount(Location),
7     Locations = make_set(Location),
8     BurstStartTime = min(TimeGenerated),
9     BurstEndTime = max(TimeGenerated)
10  | by UserPrincipalName, Type
11  | where CountOfLocations > 1

```

결과      차트      열      **체크리스트 추가**      시간 표시 (UTC+00:00)      그룹 열

완료됨. 사용자 지정 시간 범위의 결과를 표시하는 중입니다.

timestamp [UTC]	AccountCustomEntity	Account_0_Name	UserPrincipalName
2022. 3. 15. 오전 2:31:58...	ju975@cnthoth.com	ju975@cnthoth.com	ju975@cnthoth.com

# Azure Sentinel 핵심 기능

- 분석 : 위험요소 분석을 스케줄로 정책 구성

## 분석 정책 상태

74 활성 규칙

심각도별 규칙

높음 (11) | 중간 (10) | 낮음 (0) | 정보 제공 (53)

활성 규칙 | 규칙 템플릿

검색 | 필터 추가

<input type="checkbox"/> 심각도 ↑↓	↑↓ 이름 ↑↓	규칙 유형 ↑↓	상태 ↑↓	전술
<input type="checkbox"/> 높음	Advanced Multistage Attack Detection	Fusion	사용	+8
<input type="checkbox"/> 높음	Azure WAF matching for Log4j vuln(CVE-2021-44228)	Scheduled	사용 안 함	Initial Access
<input type="checkbox"/> 높음	Azure WAF matching for Log4j vuln(CVE-2021-44228)	Scheduled	사용 안 함	Initial Access
<input type="checkbox"/> 높음	Create incidents based on Microsoft Defender for Endpoint alerts	Microsoft Security	사용	
<input type="checkbox"/> 높음	Create incidents based on Microsoft Defender for Office 365 alerts	Microsoft Security	사용	
<input type="checkbox"/> 높음	Log4j vulnerability exploit aka Log4Shell IP IOC	Scheduled	사용 안 함	Command and Control
<input type="checkbox"/> 높음	Log4j vulnerability exploit aka Log4Shell IP IOC	Scheduled	사용 안 함	Command and Control
<input type="checkbox"/> 높음	User agent search for log4j exploitation attempt	Scheduled	사용 안 함	Initial Access
<input type="checkbox"/> 높음	User agent search for log4j exploitation attempt	Scheduled	사용 안 함	Initial Access
<input type="checkbox"/> 높음	Vulnerable Machines related to log4j CVE-2021-44228	Scheduled	사용 안 함	
<input type="checkbox"/> 높음	Vulnerable Machines related to log4j CVE-2021-44228	Scheduled	사용 안 함	
<input type="checkbox"/> 중간	사외 파일 다운로드 현황 확인	Scheduled	사용	
<input type="checkbox"/> 중간	alert	Scheduled	사용	Reconnaissance
<input type="checkbox"/> 중간	login fail	Scheduled	사용	Initial Access
<input type="checkbox"/> 중간	New Analytics	Scheduled	사용	Discovery

## 심각도 선택

심각도

높음

정보 제공

낮음

중간

높음

## 전술 선택

전술과 기술

5개 선택됨

Reconnaissance

T1595 - Active Scanning

T1592 - Gather Victim Host Information

T1589 - Gather Victim Identity Information

T1590 - Gather Victim Network Information

T1591 - Gather Victim Org Information

T1598 - Phishing for Information

T1597 - Search Closed Sources

# Azure Sentinel 핵심 기능

- 분석 : 위험요소 분석을 스케줄로 정책 구성

## 스케줄 세부 설정

### 경고 보강

- ✓ 엔터티 매핑
- ✓ 사용자 지정 세부 정보
- ✓ 경고 세부 정보

### 쿼리 예약

쿼리 실행 간격 \*

마지막부터 데이터 조회 \* ①

### 경고 임계값

쿼리 결과 수가 다음과 같은 경우 경고 생성

### 이벤트 그룹화

**i** 이벤트당 알림 한도가 곧 증가할 예정입니다.

규칙 쿼리 결과가 경고로 그룹화되는 방법 구성

- 모든 이벤트를 단일 경고로 그룹화
- 각 이벤트에 대해 경고 트리거

## 인시던트 및 경고 선택

### 인시던트 설정

Microsoft Sentinel 경고를 검토해야 하는 인시던트로 그룹화할 수 있습니다. 이 분석 규칙으로 트리거되는 경고에서 인시던트를 생성할지 여부를 설정할 수 있습니다.

이 분석 규칙으로 트리거되는 경고에서 인시던트 만들기

사용  사용 안 함

### 경고 그룹화

이 분석 규칙으로 트리거되는 경고가 인시던트로 그룹화되는 방법을 설정합니다. 경고를 인시던트로 그룹화하면 응답하는 데 필요한 컨텍스트를 제공하고 단일 경고의 잡음이 감소합니다.

이 분석 규칙에서 트리거된 관련 경고를 인시던트로 그룹화


사용  사용 안 함

## 자동화 선택

### 경고 자동화

이 분석 규칙에서 새 경고가 생성될 때 실행할 플레이북을 선택합니다. 플레이북은 경고를 있습니다.

이름

 alert\_playbook



# Azure Sentinel 핵심 기능

• 자동화 : 경고 및 인시던트에 대해 관리자 알림 및 사용자 격리

## 자동화 정책 상태

2  
자동화 규칙

0  
사용 가능한 규칙

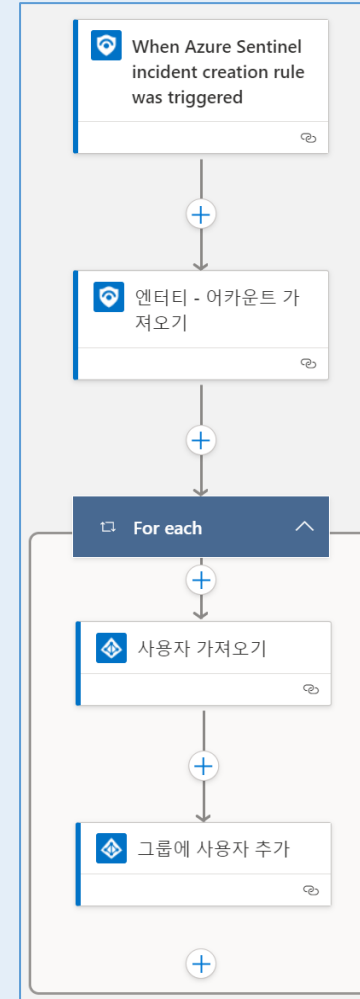
15  
사용 가능한 플레이북

자동화 규칙    활성 플레이북    플레이북 템플릿(미리 보기)

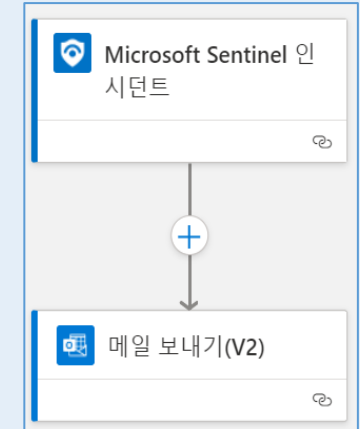
분석 규칙: 모두
작업: 모두
만든 사람: 모두
마지막으로 수정한 사람: 모두

순서	표시 이름	분석 규칙 이름	작업	만료 날짜
2	Test_AzurePortal Login attempt fa...	Test_AzurePortal Login attempt fa...	플레이북 'Test_Groupmovetest'...	2022. 3. 11. 오후 6:44:58
4	loginfail	login fail	플레이북 'user_group_move' ...	무한

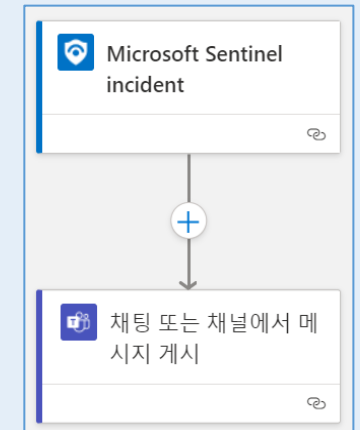
## 차단 그룹 이동



## 관리자 메일 전송



## 팀즈 채팅 전송



# Azure Sentinel 핵심 기능

- **인시던트** : 분석 규칙을 통해 생성되는 이벤트

## 인시던트 생성 현황

**1.4K**  
인시던트 열기

**1.4K**  
새 인시던트

**0**  
활성 인시던트

**심각도별 인시던트 열기**  
■ 높음 (0)

심각도 : 모두
상태 : 2개 선택됨

자동 새로 고침 인시던트

<input type="checkbox"/> 심각도 ↑↓	인시던트 ID ↑↓	제목 ↑↓	알림
<input type="checkbox"/> 중간	2491	test	1
<input type="checkbox"/> 중간	2490	OneDrive_Upload_Rule	1
<input type="checkbox"/> 중간	2489	사외 파일 다운로드 현황 확인	1
<input type="checkbox"/> 중간	2488	OneDrive_Upload_Rule	1
<input type="checkbox"/> 중간	2487	사외 파일 다운로드 현황 확인	1

## 인시던트 관리자 지정

**New Analytics**  
인시던트 ID: 2484

할당되지 않음 신규 중간  
소유자 상태 심각도

허담  
 heodam@cnthoth.com

도현석  
 hsdo@cnthoth.com

김형수  
 00693@skgas.co.kr

**Groups**

HelpdeskAgents

Teams for U  
 teamsforu@cnthoth.onmicrosoft.com

박경우 테스트(팀이름변경)  
 msteams\_0ba231@cnthoth.com

사내IT  
 ITTeam@cnthoth.com

Operation파트  
 CNT\_OperationPart@cnthoth.com

적용

취소

## 메모 기능 제공

인시던트 링크

[https://portal.azure.com/#asset/Microsoft\\_Azure](https://portal.azure.com/#asset/Microsoft_Azure)

---

☰ 마지막 주석

---

도현석님 결과 내용 전체 공유 바랍니다.

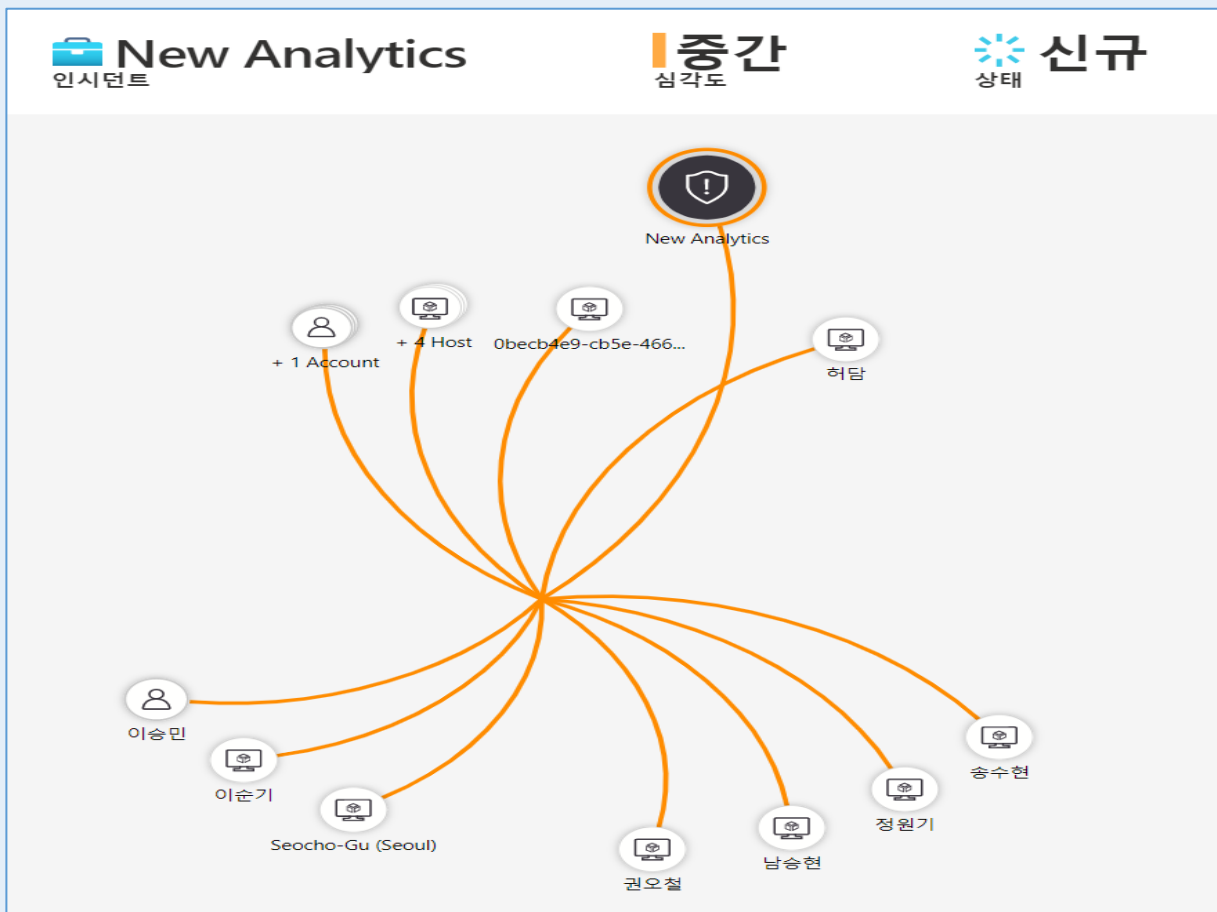
CT씨앤티

18

# Azure Sentinel 핵심 기능

- 조사 : 인시던트 발생 시 상관관계 분석 가능

## 상관관계 분석 내용



## 특정사용자 상관관계 분석

This screenshot shows the 'Related alerts' dropdown menu for a specific user. The menu is titled '허담' and lists various alert types with their counts and '이벤트 >' links. The items are:

- Assigned IPs (0) 이벤트 >
- Related alerts (27) 이벤트 >
- Parent processes running... 이벤트 >
- 자세히 ▾
- Accounts which logged ont... 이벤트 >
- Related bookmarks (0)
- Least prevalent processes... 이벤트 >
- Processes on Host blocked... 이벤트 >
- Processes running on Host... 이벤트 >
- User accounts created or ... 이벤트 >
- Services created on host (0) 이벤트 >
- Accounts triggering Micro... 이벤트 >
- Least prevalent inbound W... 이벤트 >

# Azure Sentinel 핵심 기능

- 통합문서 : 생성된 인시던트나 사용 이력을 대시보드로 구성

## 기본 제공 템플릿 형식

12  
저장된 통합 문서

118  
템플릿

1  
업데이트

내 통합 문서    템플릿

**안전하지 않은 프로토콜** | ⚠ v2.1 업데이트 가능(현재 실행 중인 버전: v2.0)

MICROSOFT

**데이터 수집 상태 모니터링**

MICROSOFT

**로그 소스 및 분석 규칙 적용 범위**

MICROSOFT SENTINEL COMMUNITY

**보안 경고**

MICROSOFT

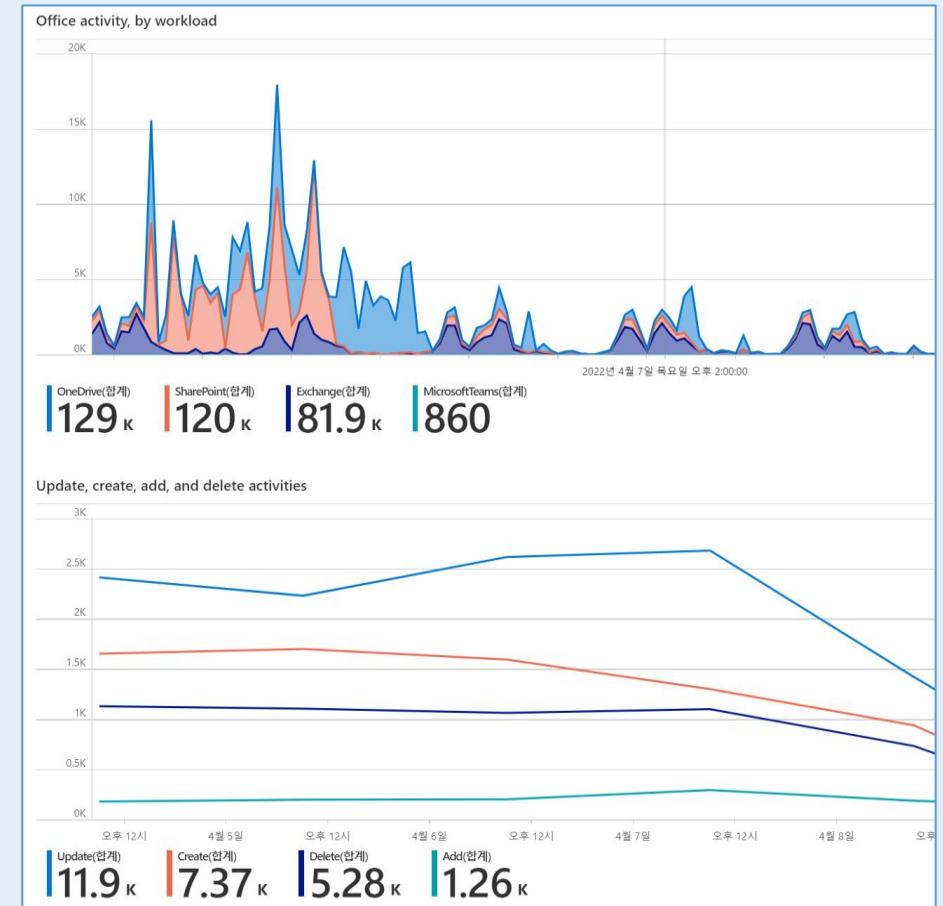
**보안 상태**

MICROSOFT

**보안 운영 효율성**

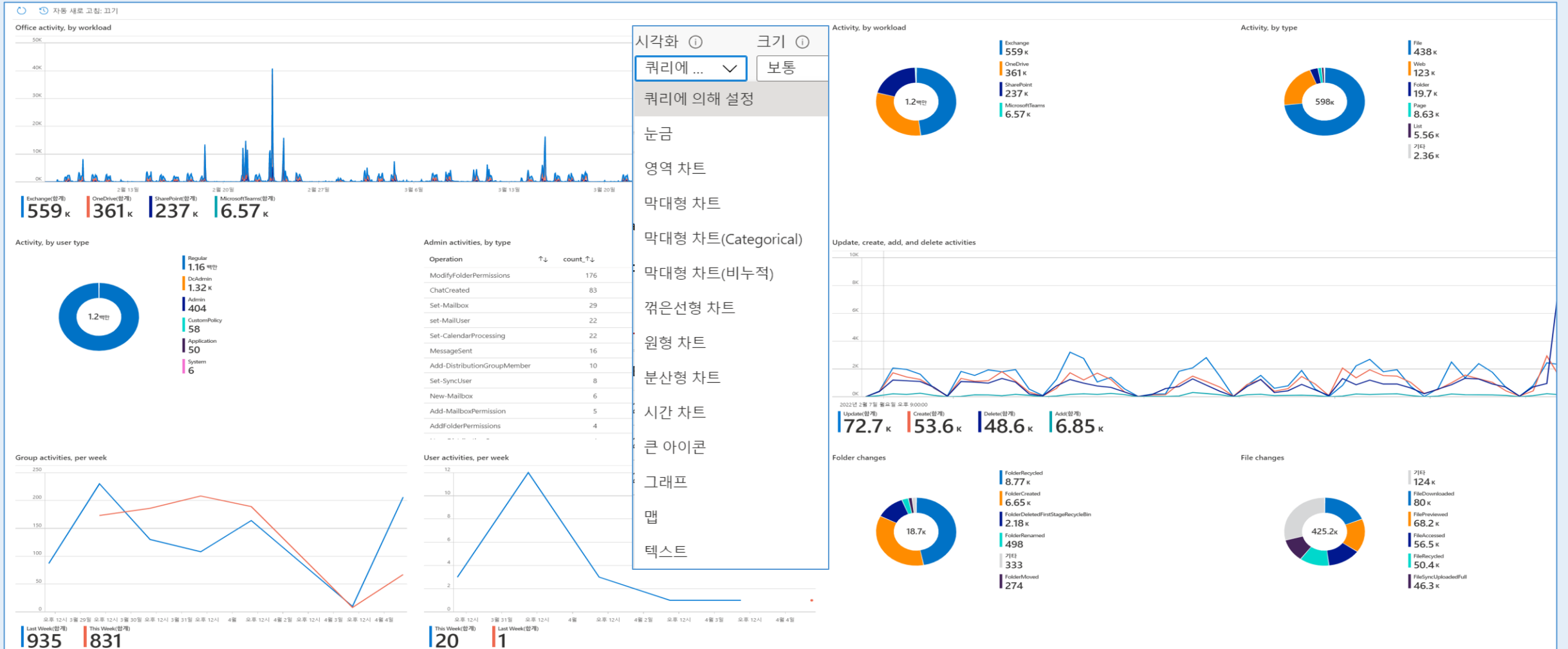
MICROSOFT

## 항목별 커스터마이징 가능



# Azure Sentinel 핵심 기능

- 통합문서 : 각 항목별 데이터를 환경에 따라 시각화 구성





**04**

**Sentinel Workshop**



# 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 보안 솔루션의 보안 정책에 대한 인사이트 확보
- 사용자, 회사 데이터를 활용한 보안 정책 수립과 관리 도구의 활용 방법
- 보안 관리자가 위험 요소에 대한 즉각적인 처리 및 가시성 확보를 위한 대시보드 구성 SOAR를 통한 즉각적인 대처 방안 (편의성 증대/보안 강화)

# 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.	



**THANK YOU**