




Microsoft Sentinel 와치리스트 활용 방안

≡ Task ID	
↗ 프로젝트	<u>Development 명재환</u>
↗ 상위작업	
↗ 담당그룹	 <u>DevSecOps</u>
↗ Work Type	<u>Study, Documentation, Case Study.</u>
↗ Task 현황	 <u>Closed</u>
≡ 작업 년/월/주	2022년/8월/1주
↗ Technical Tags	 <u>#Microsoft Sentinel</u>
👤 작업자	⑨ 명재환
⬇ 우선순위	Normal
≡ 유형	Development
# 진척도	
📅 기간	
Σ 소요시간	D 0H
≡ 작업 내용 요약	Microsoft Sentinel의 Watchlist를 활용하여 실제 위협 행위에 대한 활용방안을 연구함
👤 생성자	⑨ 명재환
👤 최종 편집자	⑨ 명재환
🕒 최종 변경일시	@2022년 8월 5일 오후 1:42
↗ Requestor - Cloocus	
↗ Requestor - Customer	
↗ Parent item	

1. 소개

와치리스트는 Sentinel 환경의 이벤트와의 상관 관계를 위해 외부 데이터 원본에서 데이터를 수집할 수 있습니다. 검색, 탐지 규칙, 위협 사냥 및 대응 플레이북에서 감시 목록을 사용할 수 있습니다.

2. 목적

와치리스트를 사용하여 위협을 조사하고 IP 주소, 파일 해시 및 기타 비즈니스 데이터를 빠르게 가져와 인시던트에 신속하게 대응하는 방법을 보여줍니다.

3. 주요 시나리오

1) 위협 탐지: csv 파일에서 위협 IP, 파일 해시 및 기타 데이터를 신속하게 가져와 인시던트에서 신속하게 대응함. 가져온 후에는 경고 규칙, 위협 찾기, 통합 문서, 노트북 및 일반 KQL 쿼리의 조인 및 필터에 대해 감시 목록을 사용할 수 있음













2)비즈니스 데이터를 감시 목록으로 가져오기: 예를 들어 시스템 액세스 권한이 있는 사용자 목록 또는 최근 종료/퇴사한 직원 정보를 가져온 다음 감시 목록을 사용하여 해당 사용자가 네트워크에 로그인하지 못하도록 감지하거나 차단하는데 사용하는 허용 및 거부 목록을 생성함

3)경고 피로도 감소: 허용 목록을 만들어 일반적으로 경고를 트리거하는 작업을 수행하는 권한 있는 IP주소의 사용자와 같은 그룹의 경고를 표시하지 않도록 방지할 수 있음

4)이벤트 데이터 보강: 감시 목록을 사용하여 외부 데이터 원본에서 파생된 이름-값 조합으로 이벤트 데이터를 보강함.

4. 방법

Sentinel 위협 인텔리전스는 TAXII 서버에서 위협 지표를 받아서 표시합니다. 위협 지표는 IP, 도메인, URL 및 파일 해시로 표시됩니다.

<input type="checkbox"/> 이름 ↑↓	값	형식	원본 ↑↓	신5
<input type="checkbox"/> mal_ip: 198.98.59.39	198.98.59.39	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 86.213.75.30	86.213.75.30	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 88.240.59.52	88.240.59.52	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 98.50.153.207	98.50.153.207	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 39.57.56.11	39.57.56.11	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 197.92.136.122	197.92.136.122	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 85.6.232.221	85.6.232.221	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 39.52.55.99	39.52.55.99	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 39.52.44.132	39.52.44.132	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 39.44.116.107	39.44.116.107	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 31.215.185.213	31.215.185.213	 ipv4-addr	EmergingThreatServer	0
<input type="checkbox"/> mal_ip: 1.161.118.53	1.161.118.53	 ipv4-addr	EmergingThreatServer	0

3

Microsoft Excel interface showing a CSV file named 'query_data (1).csv' imported into a worksheet. The data is organized into two columns: A (NetworkIP) and B (Description).

NetworkIP	Description
190.117.226.104	TS ID: 52211901098; iType: mal_ip; State: active; Org: Claro Peru; Source: Emerging Threats C&C Server
181.118.101.22	TS ID: 52392626732; iType: mal_ip; State: active; Org: Arlink S.A.; Source: Emerging Threats C&C Server
78.100.187.118	TS ID: 52513609987; iType: mal_ip; State: active; Org: OOREDOO; Source: Emerging Threats C&C Server
37.18.30.179	TS ID: 53104845252; iType: mal_ip; State: active; Org: Itglobalcom Rus LLC; Source: Emerging Threats C&C Server
185.142.99.39	TS ID: 53459594324; iType: mal_ip; State: active; Org: Televox TV LLC; Source: Emerging Threats C&C Server
186.42.186.202	TS ID: 53573595003; iType: mal_ip; State: active; Org: Corporacion Nacional De Telecomunicaciones - Cnt E; Source: Emerging Threats C&C Server
220.241.38.226	TS ID: 54265296473; iType: mal_ip; State: active; Org: PCCW IMSBiz; Source: Emerging Threats C&C Server
201.190.133.235	TS ID: 54338573428; iType: mal_ip; State: active; Org: Supercanal S.A.; Source: Emerging Threats C&C Server
192.227.232.82	TS ID: 54466231951; iType: mal_ip; State: active; Org: ColoCrossing; Source: Emerging Threats C&C Server
195.123.221.232	TS ID: 54562215042; iType: mal_ip; State: active; Org: Layer6 Networks; Source: Emerging Threats C&C Server
72.69.99.47	TS ID: 54637077765; iType: mal_ip; State: active; Org: Verizon Fios Business; Source: Emerging Threats C&C Server
200.119.11.118	TS ID: 54726034501; iType: mal_ip; State: active; Org: ETB; Source: Emerging Threats C&C Server
103.209.178.208	TS ID: 54762898643; iType: mal_ip; State: active; Org: Kappa Internet Services Private Limited; Source: Emerging Threats C&C Server
37.46.132.101	TS ID: 54838570234; iType: mal_ip; State: active; Org: JSC Server; Source: Emerging Threats C&C Server

Sentinel > 관심 목록에서 생성한 csv파일을 드래그&드래그 또는 파일 찾아보기로 업로드 합니다. 업로드된 정보는 파일 미리보기로 처음 50개 행까지 표시됩니다. 이때 헤더 (NetworkIP)는 검색 키로 사용됩니다.

홈 > Microsoft Sentinel > Microsoft Sentinel | 관심 목록 >

관심 목록 마법사

새 관심 목록 만들기

일반 **원본** 검토 및 만들기

소스 유형
로컬 파일

파일 형식
헤더가 포함된 CSV 파일(.csv)

머리글을 포함하여 행 앞 줄 수
0

파일 업로드 *

query_data.csv

파일 끌어서 놓기 또는 파일 찾아보기

검색키 *

NetworkIP

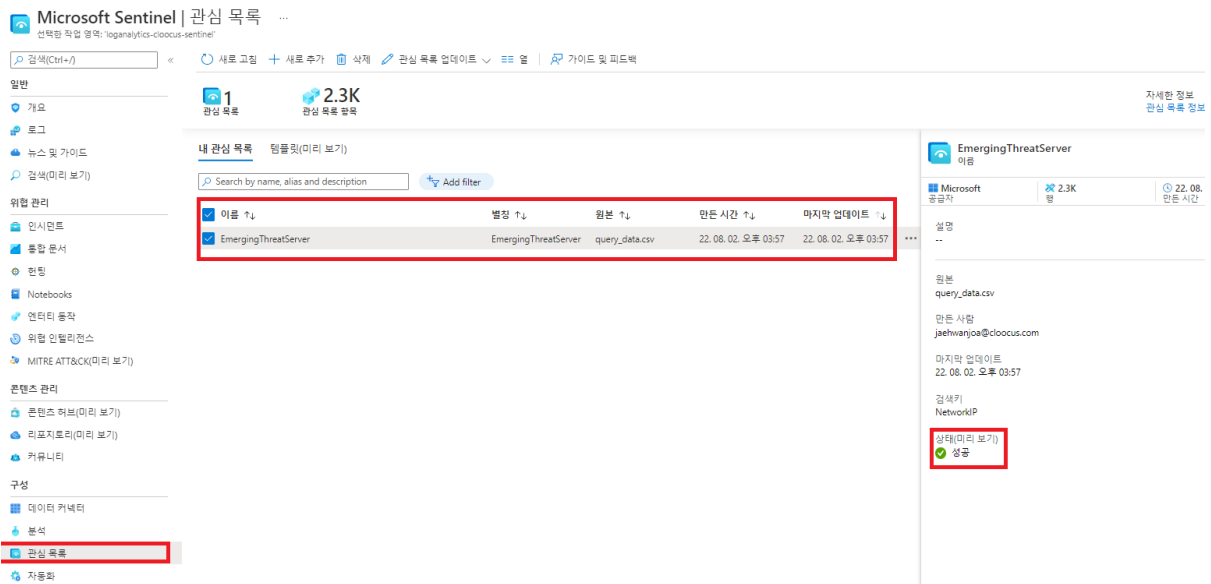
SearchKey는 관심 목록을 사용하여 다른 데이터와 소인할 때 쿼리 성능을 최적화하는 데 사용됩니다. 예를 들어 IP 주소가 포함된 열이 지정된 SearchKey 필드가 되도록 설정 한 후 이 필드를 사용하여 IP 주소로 다른 이벤트 테이블에 조인할 수 있습니다. 자세히 알아보고 SearchKey에 대한 예제를 알아보세요.

파일 미리 보기 | 처음 50개 행과 처음 5개 열

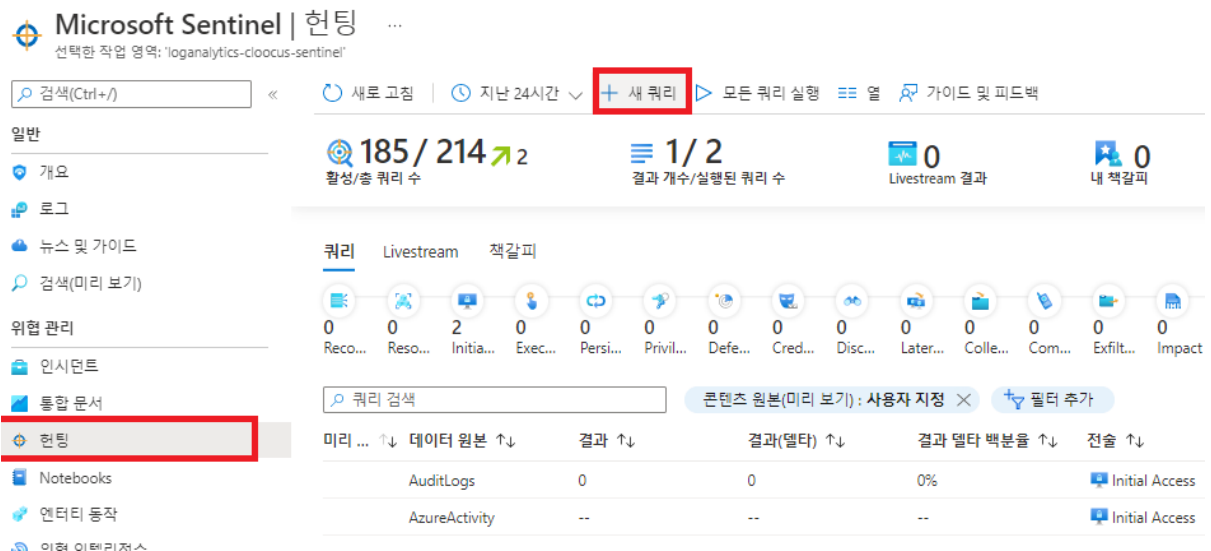
NetworkIP

190.117.226.104
181.118.101.22
78.100.187.118
37.18.30.179
185.142.99.39
186.42.186.202
220.241.38.226
201.190.133.235
192.227.232.82
195.123.221.232
72.69.99.47
200.119.11.118
103.209.178.208
37.46.132.101

와치리스트 생성이 등록되었음을 확인합니다.



생성된 와치리스트를 근거로 헌팅 쿼리를 만듭니다. 위협 인텔리전스의 IP를 통해 Azure 활동을 수행하는 경우 실시간으로 모니터링하며 Azure Activity Log를 활용합니다. 인시던트 분석 규칙대신 헌팅 쿼리를 사용하는 이유는 거의 실시간(라이브 스트림)으로 능동적으로 대응할 수 있기 때문입니다.

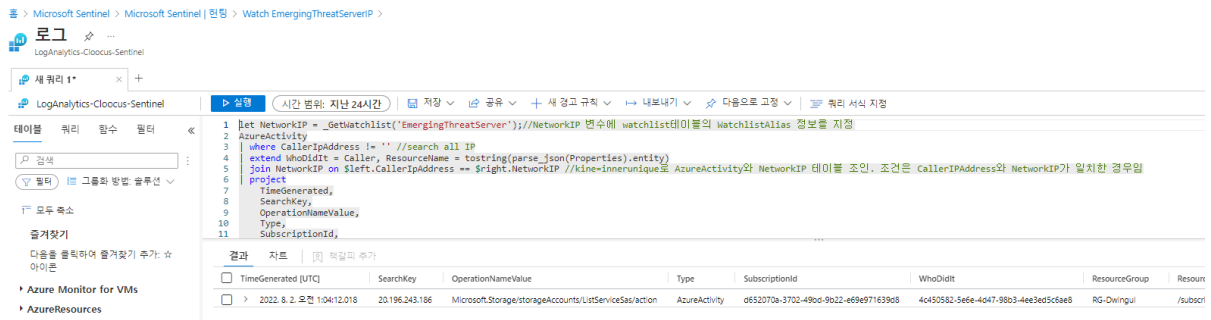


주요 쿼리 구분

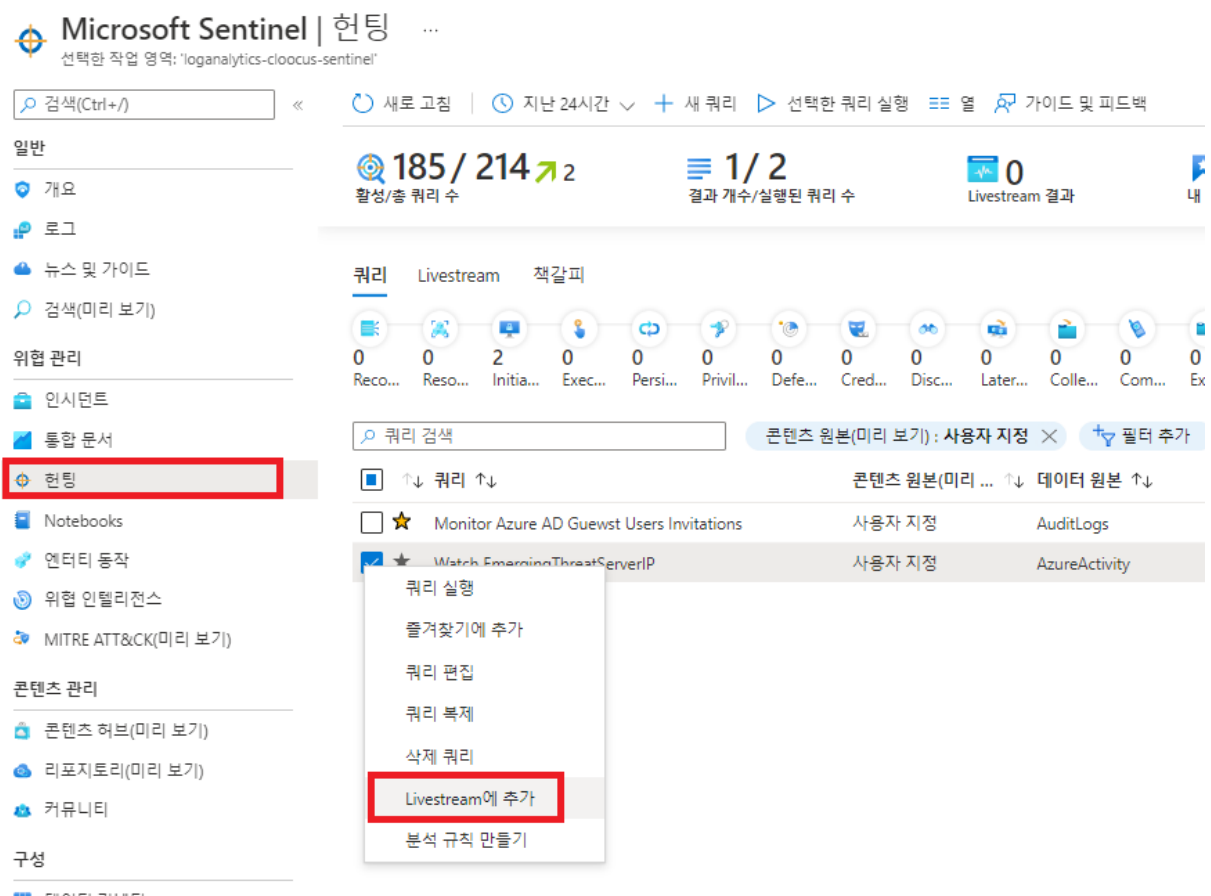
let NetworkIP = _GetWatchlist('EmergingThreatServer');//NetworkIP 변수에 watchlist 테이블의 WatchlistAlias 정보를 지정

AzureActivity | where CallerIpAddress != " //search all IP

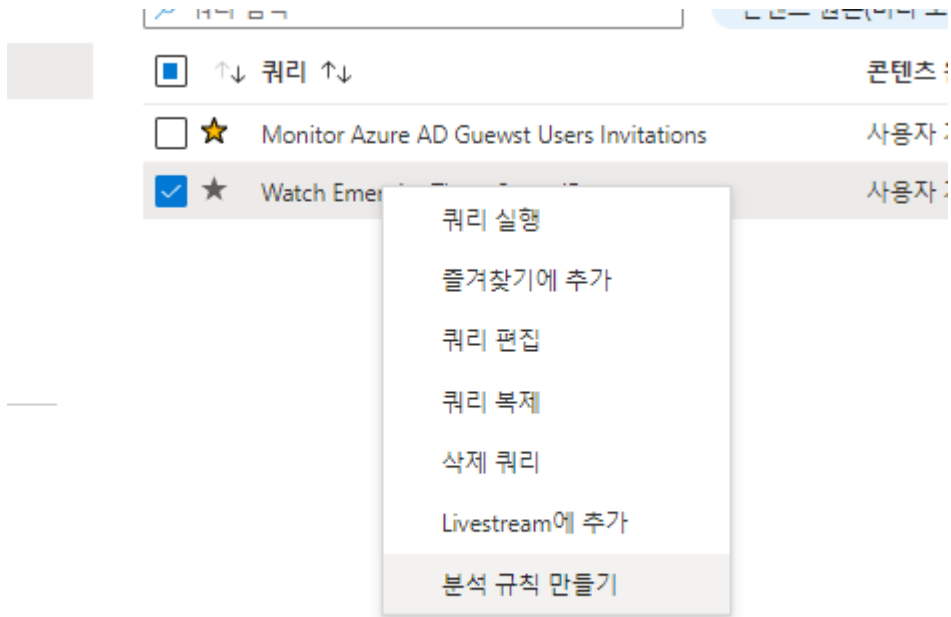
| join NetworkIP on \$left.CallerIpAddress == \$right.NetworkIP //kine=innerunique로 AzureActivity와 NetworkIP 테이블 조인. 조건은 CallerIpAddress와 NetworkIP가 일치한 경우임



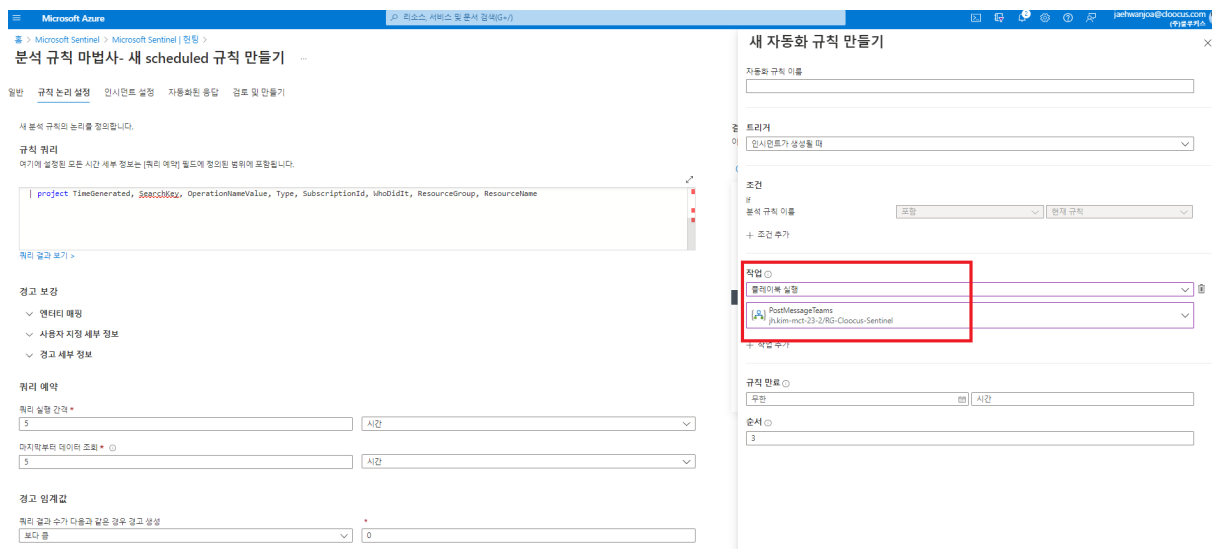
생성된 헌팅 쿼리를 마우스 오른쪽 클릭을 통해 라이브 스트림으로 생성합니다. Azure포털을 로그인하는 IP가 EmergencyThreatServerIP와 일치하는 경우 경고를 생성합니다.



경고가 생성되었다고하면 마우스 오른쪽으로 해당 헌팅 쿼리를 인시던트 분석 규칙으로 승격시킬 수 있습니다.



사전에 만들어진 플레이북을 연계하면 인시던트에 대한 SOAR를 수행할 수 있습니다.



****Watchlist에 csv 파일을 업로드하고 쿼리를 수행할 필요없이, ThreatIntelligenceIndicator 테이블과 비교하려는 테이블을 서로 join하여 쿼리를 수행할 수도 있습니다.**

(직접 비교하여 결과를 보여줄 지표가 없어 SignLogs와 AzureActivity 테이블을 활용함)

피드

▶ 실행
시간 범위: 지난 7일
저장
공유
새 경고 규칙
내보내기
다음으로 고정
쿼리 서식 지정

```

1 let NetworkIP = SigninLogs
2 | where IPAddress == '211.215.58.26';
3 AzureActivity
4 | where CallerIpAddress != ''
5 extend WhoDidIt = Caller, ResourceName = tostring(parse_json(Properties).entity)
6 join NetworkIP on $left.CallerIpAddress == $right.IPAddress
7 project TimeGenerated, IPAddress, OperationNameValue, Type, SubscriptionId, WhoDidIt, ResourceGroup, ResourceName

```

결과
차트
🔍 책갈피 추가

<input type="checkbox"/>	TimeGenerated [UTC]	IPAddress	OperationNameValue	Type	SubscriptionId
<input type="checkbox"/>	> 2022. 8. 2. 오후 11:18:20.110	211.215.58.26	Microsoft.Security/Insights/data...	AzureActivity	d652070a-3702-49bd-9b22
<input type="checkbox"/>	> 2022. 8. 2. 오후 11:18:20.110	211.215.58.26	Microsoft.Security/Insights/data...	AzureActivity	d652070a-3702-49bd-9b22
<input type="checkbox"/>	> 2022. 8. 2. 오후 11:18:20.110	211.215.58.26	Microsoft.Security/Insights/data...	AzureActivity	d652070a-3702-49bd-9b22
<input type="checkbox"/>	> 2022. 8. 2. 오후 11:18:20.110	211.215.58.26	Microsoft.Security/Insights/data...	AzureActivity	d652070a-3702-49bd-9b22
<input type="checkbox"/>	> 2022. 8. 2. 오후 11:18:20.110	211.215.58.26	Microsoft.Security/Insights/data...	AzureActivity	d652070a-3702-49bd-9b22
<input type="checkbox"/>	> 2022. 8. 2. 오후 11:18:20.110	211.215.58.26	Microsoft.Security/Insights/data...	AzureActivity	d652070a-3702-49bd-9b22

이러한 방식으로 ThreatIntelligenceIndicator 에 수집되는 IP 또는 URL과 같은 공격 지표들을 AzureActivity와 같은 다양한 테이블과 join하여 위협을 탐지하도록 활용할 수 있음