

AI가 바꾸는 XDR의 풍경

OWASP Seoul
Chapter Night@SF

XDR 운영을 위한 SI 어시스턴트

우리는 보안 업무의 전문가가 되어야 하지, XDR "제품"의 전문가가 될 필요가 없습니다

LOGPRESSO 분석 > SI 어시스턴트

DEMO 위 IP 주소들에 대해 평판 조회

로그

위 IP 주소들에 대해 평판 조회

QUERY

```
json "[*] | eval ip = array(ip("95.214.52.170"), ip("149.50.96.133"), ip("64.140.161.162"), ip("202.120.234.124"), ip("106.247.87.230"), ip("3.16.157.148"), ip("13.211.157.67"), ip("15.156.7.129"), ip("18.141.160.85"))) | explode ip | abuseipdb-check-ip-batch field=ip
```

#	ip	domain	isp	country	abuse_score	report_count	user_count	whitelisted
1	95.214.52.170	mevspace.com	MEVSPACE sp. z o.o.	PL	100	1347	303	false
2	149.50.96.133	mevspace.com	MEVSPACE	PL	100	2894	305	false
3	64.140.161.162	skbroadband.com	SK Broadband Co Ltd	KR	0	0	0	
4	64.140.161.162	webnx.com	WebNX, Inc.	US	0	0	0	false
5	202.120.234.124	cernet.edu.cn	China Education and Research Network	CN	15	3	2	false
6	106.247.87.230	dacom.co.kr	LG DACOM Corporation	KR	0	0	0	
7	3.16.157.148	amazon.com	Amazon Technologies Inc.	US	0	0	0	
8	13.211.157.67	amazon.com.au	Amazon Corporate Services Pty Ltd	AU	0	0	0	
9	15.156.7.129	amazon.com	Amazon Data Services Canada	CA	23	5	4	false
10	18.141.160.85	amazon.com	Amazon Technologies Inc.	SG	0	0	0	

Q&A 무엇이 궁금하신가요? 로고가 답해드립니다.

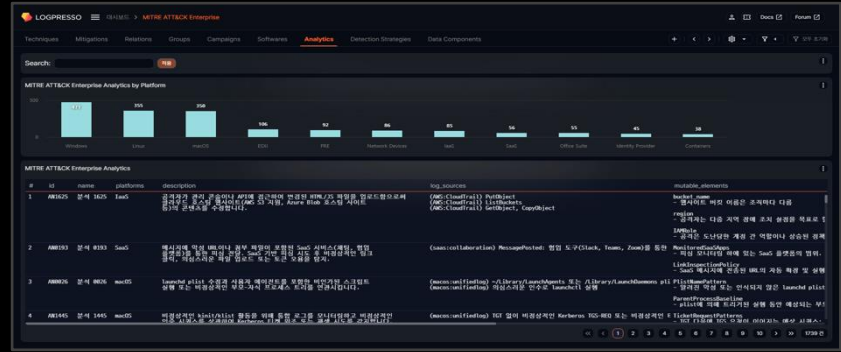
v 5.0

SI는 XDR의 복잡성을 대신합니다

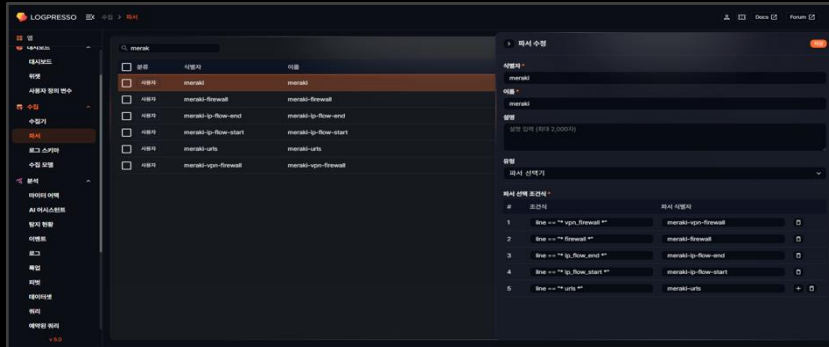
우리가 업무를 정의하면 보고서, 탐지 룰, 파서, 대시보드까지 SI가 알아서 만듭니다



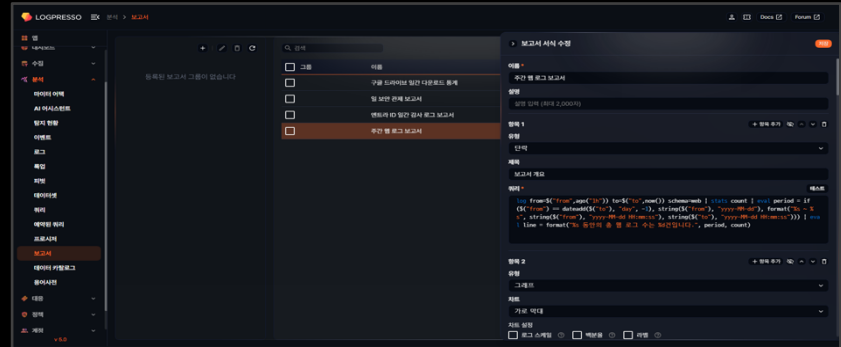
<대시보드 자동 생성>



<탐지 규칙 자동 생성>



<파서 자동 생성>



<보고서 자동 생성>

생성형 AI를 활용한 다양한 기능을 제공합니다

탐지 이벤트의 맥락을 분석하고, 맥락을 고려한 리포트를 생성합니다

The screenshot shows a ticket analysis interface for a TTP event. The ticket title is "티켓 상세 조회 - #90801". The main content area displays a network diagram with nodes representing IP addresses and their connections. Below the diagram, there is a "위협 요약" (Threat Summary) section and a "공격 진행 단계" (Attack Progress Stages) section. The attack progress is divided into three stages: Stage 1: Host Discovery, Stage 2: Usage, and Stage 3: Remote Access. Each stage includes a detailed description of the actions taken, such as RDP connection attempts and SSH connections.

티켓 상세 조회 - #90801

제목 * 172.20.1.1 침해 - 내부 RDP 접근 및 외부 데이터 유출 저장

DEMO 2026-02-23 01:24:54

중요도 상
위험 점수 -
티켓 상태 신규
상태 변환 업무 완료
정오점 미정
사고 여부 미정

태그
태그가 없습니다.

담당자
발달된 담당자가 없습니다.

관계자
발달된 관계자가 없습니다.

첨부 파일
첨부한 파일이 없습니다.

상황 전파
경고 메일

위협 요약
172.20.1.1와 172.20.1.2가 내부 네트워크의 172.20.1.100으로 원격 데스크톱 프로토콜을 사용해 접속 시도했고, 이후 172.20.1.100은 외부 IP(주로 Microsoft, Google, Amazon 등)로 대체 프로토콜을 통해 데이터 유출과 명령 제어를 수행했다.

공격 진행 단계

Stage 1: 숙면 이동
172.20.1.100이 원격 데스크톱 프로토콜 (RDP)을 사용하여 내부 네트워크의 172.20.1.100으로 접속 시도. 이후 172.20.1.100은 외부 IP(주로 Microsoft, Google, Amazon 등)로 대체 프로토콜을 통해 데이터 유출과 명령 제어를 수행했다.

Stage 2: 유출
172.20.1.100이 내부 네트워크의 172.20.1.100으로 원격 데스크톱 프로토콜을 사용하여 접속 시도. 이후 172.20.1.100은 외부 IP(주로 Microsoft, Google, Amazon 등)로 대체 프로토콜을 통해 데이터 유출과 명령 제어를 수행했다.

Stage 3: 원격 액세스
172.20.1.100이 내부 네트워크의 172.20.1.100으로 원격 데스크톱 프로토콜을 사용하여 접속 시도. 이후 172.20.1.100은 외부 IP(주로 Microsoft, Google, Amazon 등)로 대체 프로토콜을 통해 데이터 유출과 명령 제어를 수행했다.

자산, 계정별 TTP 탐지 이벤트 조회

공격 전술(Tactic) 전이 상태 판단

공격 전이도 및 연결 그래프 생성

티켓 제목 및 요약문 생성

증적 포함한 티켓 생성

감사합니다

