LOGPRESSO | AbuseIPDB

IP 주소 평판 조회 및 악성 IP 주소 신고

개요

- AbuseIPDB는 IP 평판 조회 및 악성 행위 신고 기능 제공
- 로그프레소는 AbuseIPDB REST API를 통해 위협 정보 조회 및 신고 기능을 플랫폼에 통합
- IP 주소 평판 조회, IP 블랙리스트 조회, 악성 행위 신고 지원
- 플레이북에 따른 IP 평판 확인 후 자동 차단을 수행하거나 악성 행위 신고 가능

로그프레소 + AbuseIPDB

인터넷에 연결된 웹/애플리케이션 서버는 취약점을 찾는 자동화된 공격에 수시로 노출됩니다. 이러한 공격은 지속적인 보안 경보를 유발합니다. 자동화된 공격을 보안담당자의 수작업에 의존해 처리하면 업무 피로도가 높아 정작 주의 깊게 관찰해야 할 위협을 놓치기 쉽습니다.

로그프레소 플랫폼은 AbuseIPDB 서비스와 연동하여 경보 발생 시점에 IP 주소의 평판 정보를 조회합니다. IP 주소의 평판 지수가 지정된 임계값 이상이면 자동으로 공격자의 IP 주소를 차단하거나, IP 블랙리스트를 가져와 선제적으로 악성 IP 주소를 차단할 수도 있습니다.

반복된 로그인 시도, 포트 스캔, SQL 인젝션과 같은 공격 행위와 IP 주소를 자동으로 AbuseIPDB에 신고함으로써 인터넷을 더 안전하게 하는데 일조할 수 있습니다.

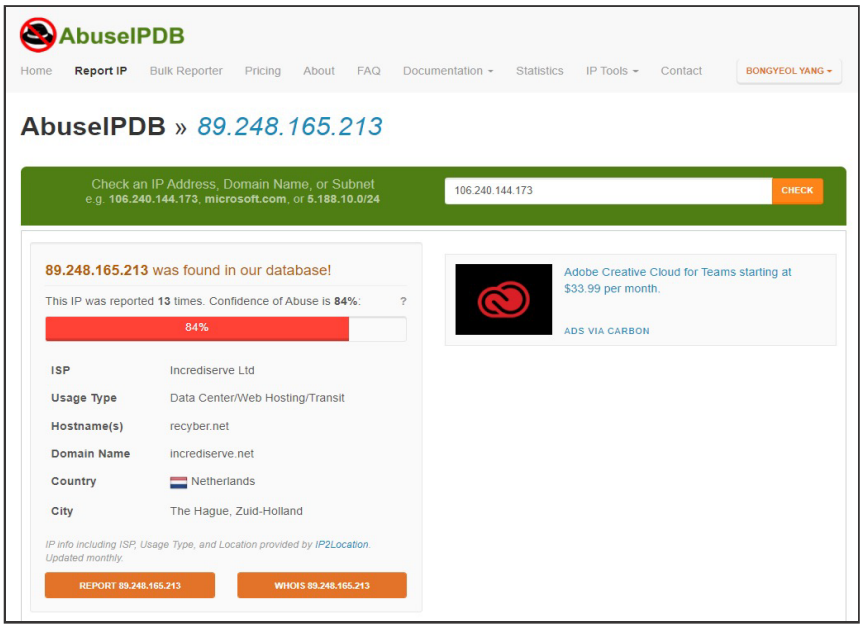
이제 자동화된 IP 평판 조회와 차단 대응을 기반으로 편리한 보안 운영 환경을 만들어보세요.

지원 플랫폼

- 로그프레소 소나
- 로그프레소 마에스트로

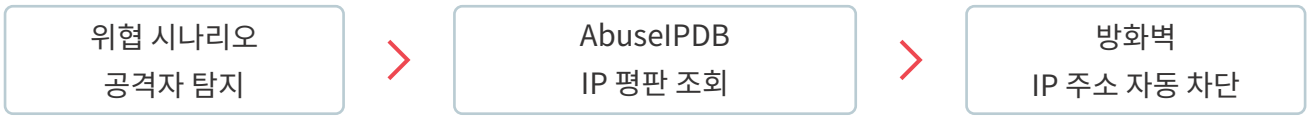
연계 제품

- AbuseIPDB (APIv2)



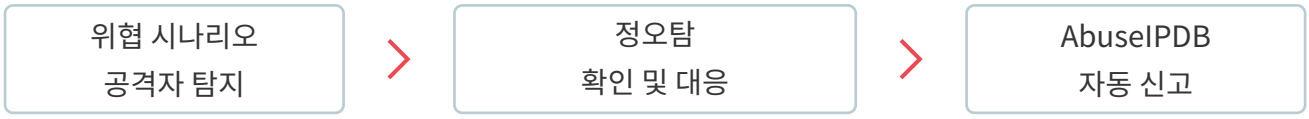
공격자 IP 주소 차단 자동화

AbuseIPDB의 어뷰징 평판 지수는 0-100 사이의 값을 갖습니다. 다수의 사용자가 IP 주소를 악성으로 보고하면 보수적으로 지수값이 증가하며, 악성 행위 없이 시간이 지나면 점점 감소하게 설계되어 있습니다. 따라서 위협 탐지 후 어뷰징 평판 지수가 지정된 임계값 이상일 때 자동으로 방화벽에서 IP 주소를 차단하여 업무 부담을 감소시킬 수 있습니다.



IP 주소 기반 악성 행위 신고

AbuseIPDB 서비스는 23가지 유형으로 세분하여 악성 IP 주소 신고를 받습니다. 예를 들어 반복된 SSH, FTP 로그인 실패, SQL 인젝션 시도, 포트 스캔, 스팸 발송 행위 등 지정된 분류의 위협이 탐지되면 이를 AbuseIPDB에 자동으로 신고하여 위협 정보를 공유합니다.



3종의 전용 쿼리 확장

AbuseIPDB 전용 쿼리를 통해 로그프레소 플랫폼에서 API 연동을 지원합니다.

명 령 어	기 능
abuseipdb-check-ip	IP 평판 조회
abuseipdb-report-ip	IP 악성 행위 신고
abuseipdb-blacklist	IP 블랙리스트 조회