LOGPRESSO MAESTRO 소개

보안 오케스트레이션 및 자동화 대응 플랫폼

배경

지금까지 수십 종, 수백 대의 보안시스템이 도입되면서 제한된 인원으로 대규모의 시스템을 효율적으로 운영하는데 많은 어려움을 겪고 있습니다. 이제 보안 운영 프로세스 자동화를 통해 업무 효율화와 품질 향상을 동시에 달성할 수 있습니다.

시스템 복잡도 증가

- 60종 이상의 단위보안시스템
- 수작업에 의한 운영 한계

과다한 경보 발생

- 일 150건 이상의 티켓 발생
- 일 10만건 이상의 이벤트 발생

반복적 업무 수행

- 평판 조회, 검색 등 수작업
- 개별 시스템 접속 및 차단 반복

전문 인력 부족

- 고도로 훈련받은 전문가 부족
- 높은 업무 피로 및 잦은 퇴사

대응 시간 지연

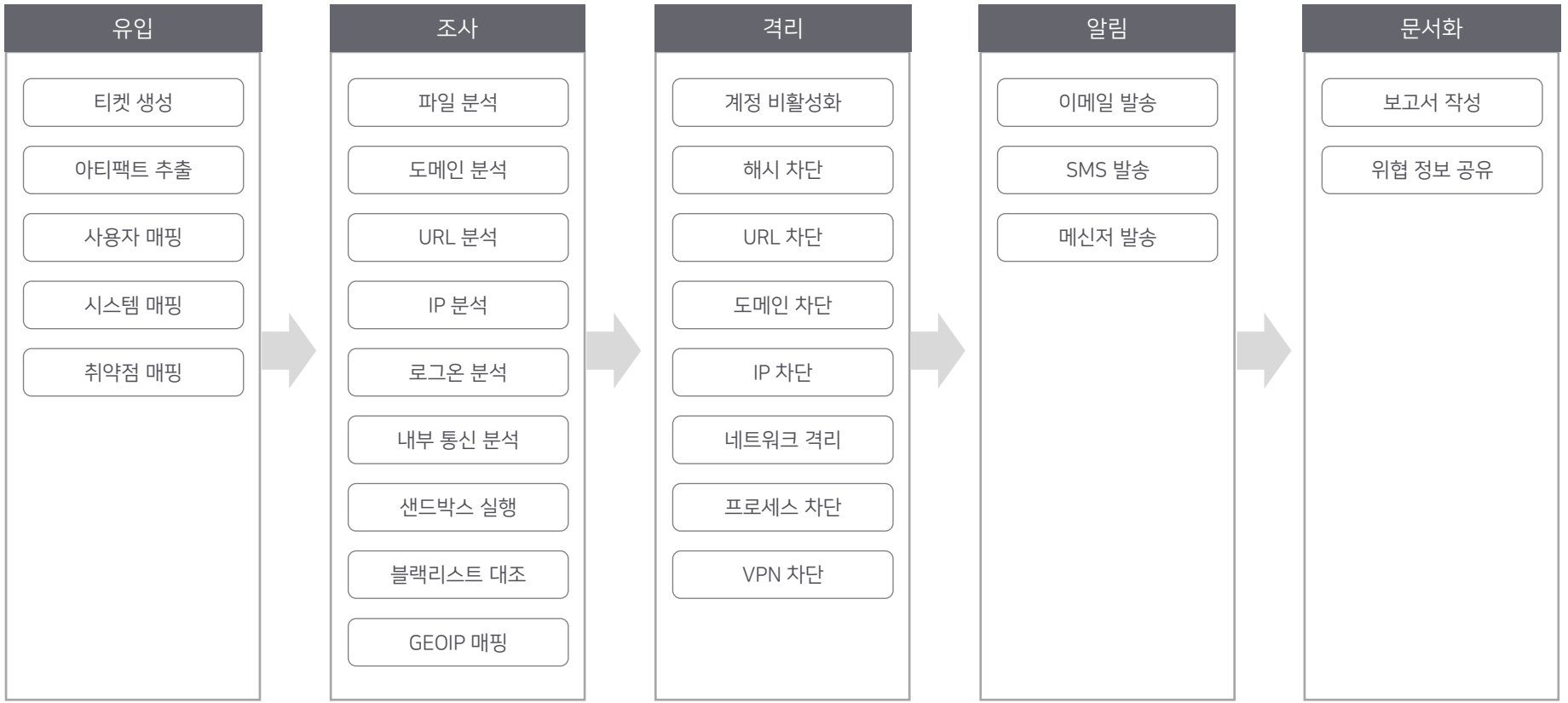
- 많은 경보로 인해 분석 지연
- 수작업 차단으로 휴먼 에러

고도화되는 위협

- 단순 위협은 자동으로 처리
- 고수준 위협에 역량 집중 필요

기존 위협 대응 절차

보안팀의 운영 업무는 SIEM이 위협을 탐지한 시점부터 시작됩니다. 티켓이 생성되면 관련된 기본 정보를 확인하고, 위협이 침해사고에 해당하는지 확인하기 위하여 위협 인텔리전스 대조와 각 단위 보안시스템의 로그를 기반으로 연관 분석을 진행합니다. 실제 침해로 판명되면 IP, HASH 등 핵심 지표를 기준으로 차단, 격리, 복구를 수행하고, 대응 보고서를 작성해야 하나의 위협 분석 및 대응 프로세스가 완결됩니다.



기존 업무 소요 시간

기존 SOC 체계에서는 위협 경보에 대한 모든 분석, 대응 단계를 수작업으로 진행해야 하므로 많은 시간이 소요됩니다. SIEM 솔루션에 보안 로그를 통합하여 이벤트를 탐지하고 있으나, 위협 분석 및 대응을 수행하려면 서로 다른 웹서비스 및 솔루션 콘솔에 접속하여 개별적으로 작업을 수행해야 합니다.

위협 조사 예

위협 인텔리전스 체크 — 5분

- 바이러스토탈, 시큐디움 인텔리전스, AbuseIPDB 등 교차 확인

내부 블랙리스트 체크 — 1분

- 기존 블랙리스트에 해당 IP, HASH, 이메일 주소 등 등록 여부 확인

이전 침해시도 내역 확인 — 3분

- 일련의 침해시도를 확인하여 공격 진행 경과와 차단 여부 검토

공격 대상 내부자산 정보 확인 — 2분

- 호스트명, 운영체제, 운영 서비스 및 버전, 담당자 등 관련 정보 확인

취약점 대조를 통해 공격 영향 확인 — 3분

- 자산에 대한 취약점 진단 내역과 공격을 대조하여 공격 영향도 확인

차단 및 침해여부 분석 예

공격 IP, URL, HASH 차단

- 각 보안시스템에 접속하여 격리 및 차단 정책 반영

OS, DB 계정 생성 여부 확인

- 공격자가 사후 접속을 위해 생성한 관리자 계정이 있는지 확인

서비스 포트 오픈 여부 확인

- 기존에 사용하지 않던 서비스 포트가 열렸는지 확인

보안 설정, 로그 위변조 여부 확인

- 보안 설정을 해제하거나 로그 삭제 혹은 위변조 정황이 있는지 확인

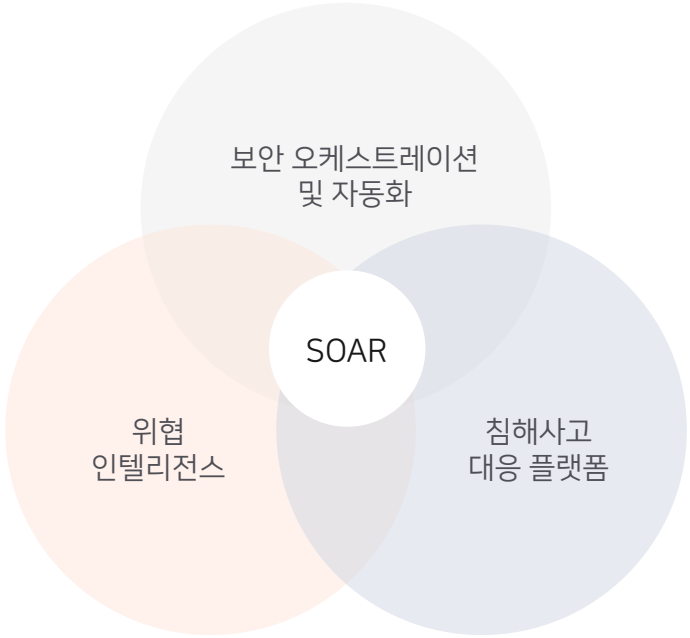
웹쉘, 루트킷 설치 여부 확인

- 외부 명령을 실행하기 위한 웹쉘이나 루트킷 설치 여부 확인

"매일 100건 이상의 위협 경보, 1건에 최소 15분 이상 소요, 일 24시간 이상 필요"

SOAR 개요

SOAR는 사람, 기술, 프로세스를 조율하고 자동화하여 위협 대응 업무의 효율성과 일관성을 개선합니다. 보안 시스템 간 워크플로우를 자동화하고, 위협 유형별로 미리 정해진 프로세스에 따라 업무를 진행하며, 여러 위협 인텔리전스를 수집, 상관 분석하여 대응에 필요한 정보를 제공합니다.



SOAR = SOA + TIP + SIRP

SOA (Security Orchestration & Automation)
- 단위 보안시스템 통합 및 워크플로우 자동화

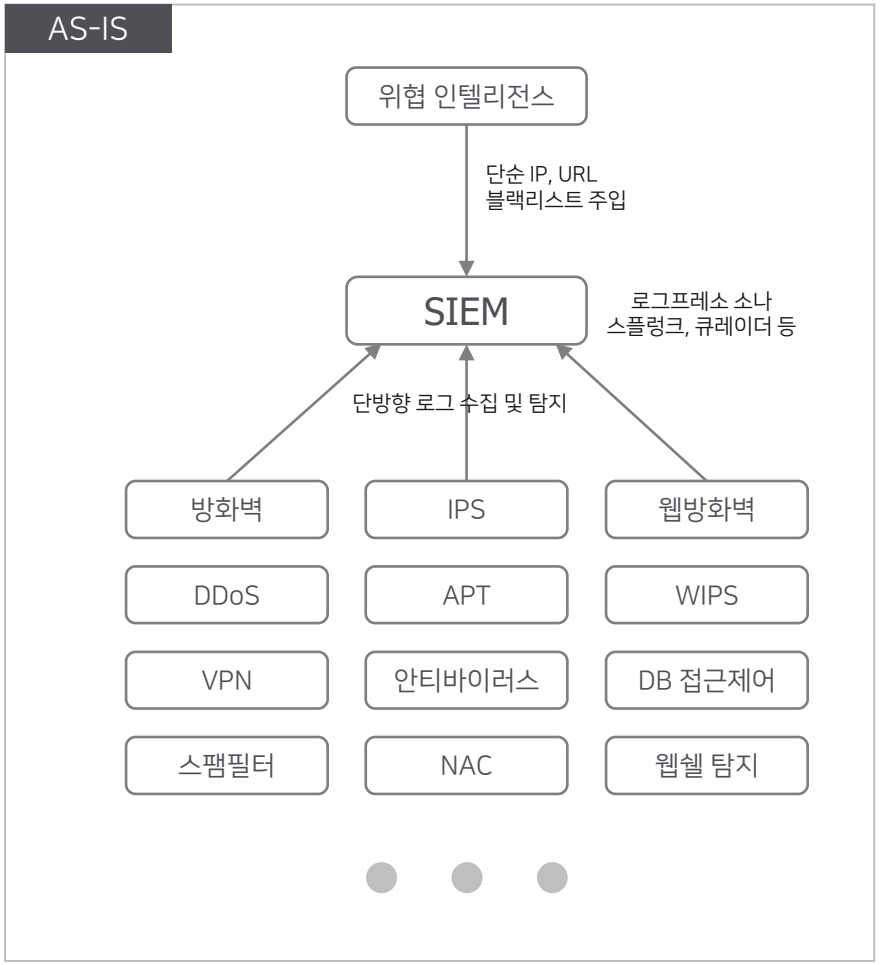
TIP (Threat Intelligence Platform)
- 위협 인텔리전스 기반 의사결정 지원

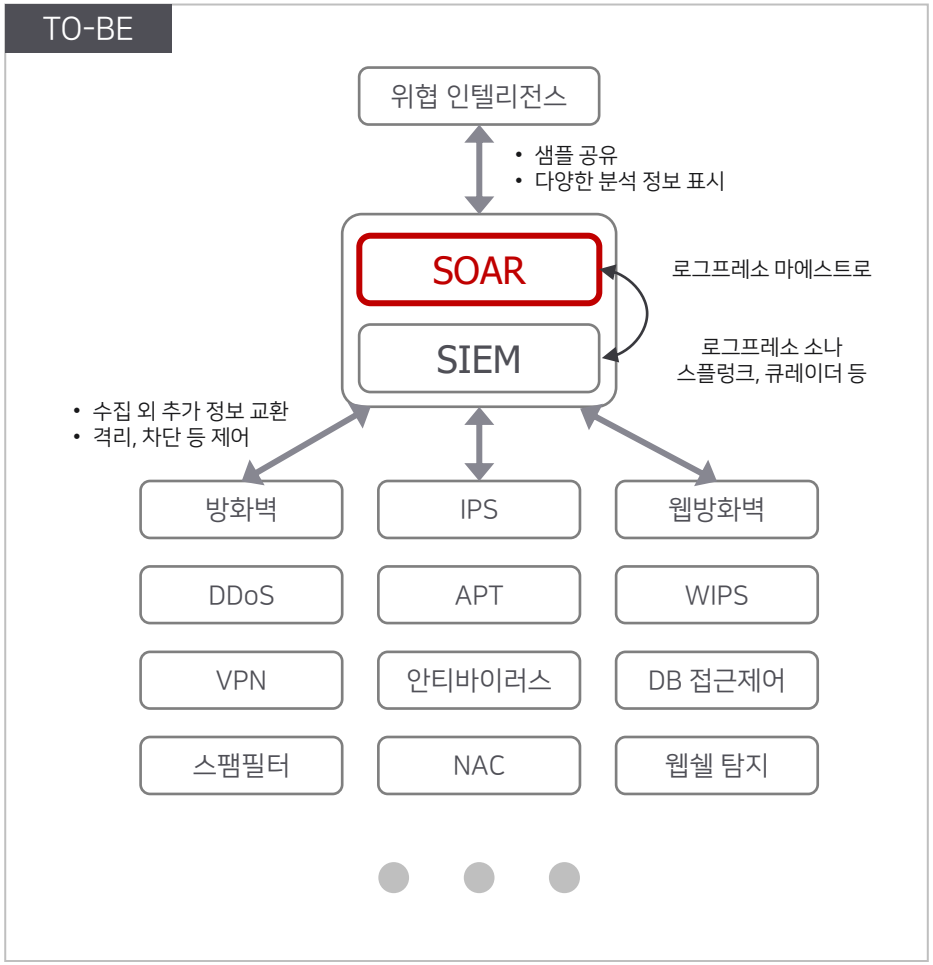
SIRP (Security Incident Response Platform)
- 위협 유형별 업무 프로세스 관리

위협 탐지 → 분석 및 추적 → 대응 → 우선순위 조정

SOAR 아키텍처

SOAR (Security Orchestration, Automation, Response) 솔루션은 수집, 탐지 뿐 아니라, API를 통한 제어 개념을 포함하여 전체 보안 시스템을 유기적으로 통합, 자동화하기 때문에 보안 운영 효율을 극대화 할 수 있습니다.





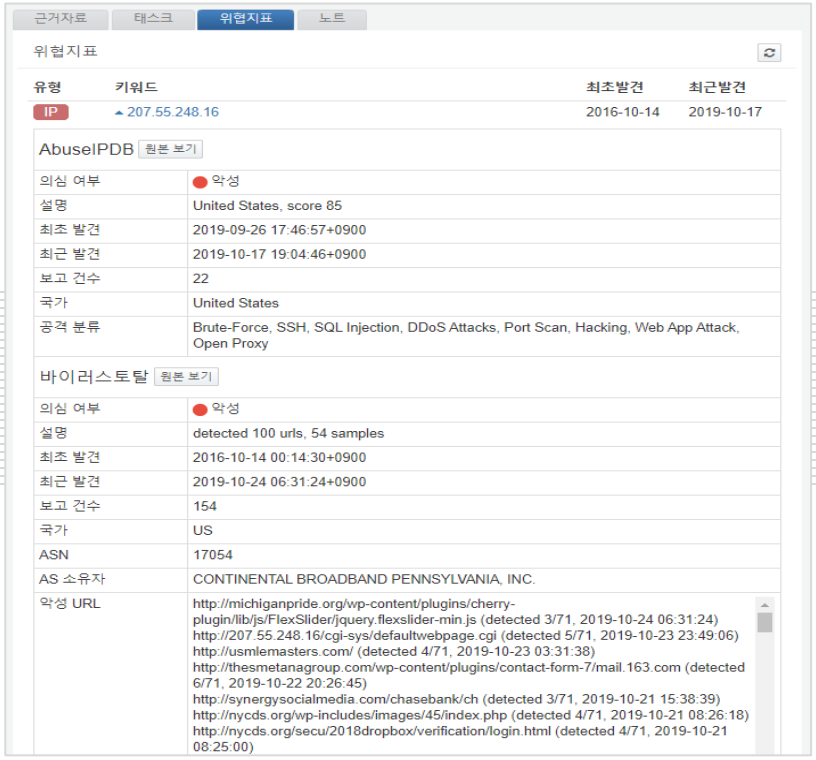
완전한 보안 API 통합

로그프레소 마에스트로는 단순 로그 수집에 그치지 않고 보안 솔루션 API를 기반으로 앱을 개발하여 풍부한 분석 정보와 시스템 제어 능력을 제공합니다. 특히 글로벌 솔루션 뿐 아니라 국내의 보안 솔루션 제조사와 협업하여 완전히 통합된 보안 오케스트레이션과 자동화를 지향합니다.

금융보안원 FINANCIAL SECURITY INSTITUTE	• 요주의 IP, 악성코드 유포지 등 IoC • 금융위 전파사항, 금융전산위기경보 • 보안관제 특이사항, 피싱/파밍 신고
RSA NETWITNESS®	• 기간별 메타 및 세션 정보 조회 • 파일 전송 MD5, SHA1 조회 • 패킷 원본 바이너리 검색
SECUDIUM INTELLIGENCE	• 유해 IP, URL, MD5 IoC • 파일 정적/동적 분석 정보 조회 • CVE 취약점 정보 조회
FIREEYE™	• 호스트별 감염, 콜백, 차단 통계 조회 • 호스트 IP별 악성코드 탐지 내역 • APT 관련 통신 세부내역 검색 • 화이트리스트 IP 추가/삭제
Genians	• 자산 식별정보 (IP, OS 버전, NIC 등) • 취약점 진단 내역 및 서비스 포트 조회 • 태그 기반 네트워크 격리 및 해제 제어
RAPID7	• 자산 목록 및 위험도 • 취약점 진단 내역 • 원격 진단 시작
AXGATE	• 보안정책, 주소, 서비스 등 객체 관리 • 블랙, 화이트리스트 조회 및 설정
paloalto NETWORKS	• 방화벽 IP 그룹 조회 및 변경 • 방화벽 정책 배포 명령
BLUEMAX NGF	• 호스트, 네트워크, 그룹 객체 등 관리 • 방화벽 정책 설정 및 적용
SolidStep	• 자산, 그룹, 사용자, 진단 결과 조회 • 진단 실행 및 취소, 조치 이력 조회

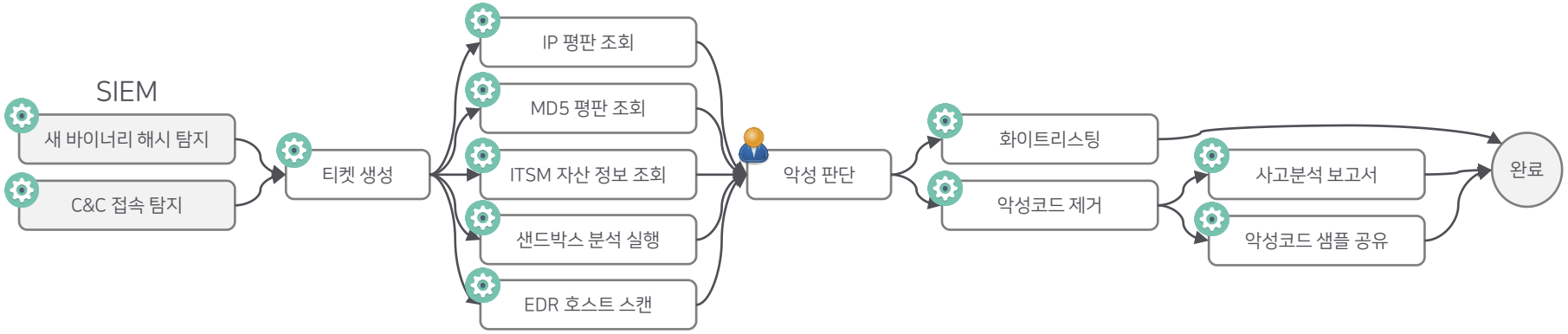
위협 분석 및 대응 가이드

위협 대응 프로세스를 시스템 자동화 단계와 사람이 수행하는 단계로 구분하여 정의할 수 있으며, 위협 대응 과정에서 취합된 정보에 따라 다음 수행 단계를 동적으로 확장하여 표시합니다. IP, 해시, 도메인, 레지스트리 키 등 위협지표를 자동 취합하여 제시하며 빠르고 정확한 대응 수행을 지원합니다.



플레이북 - 맬웨어 대응 예시

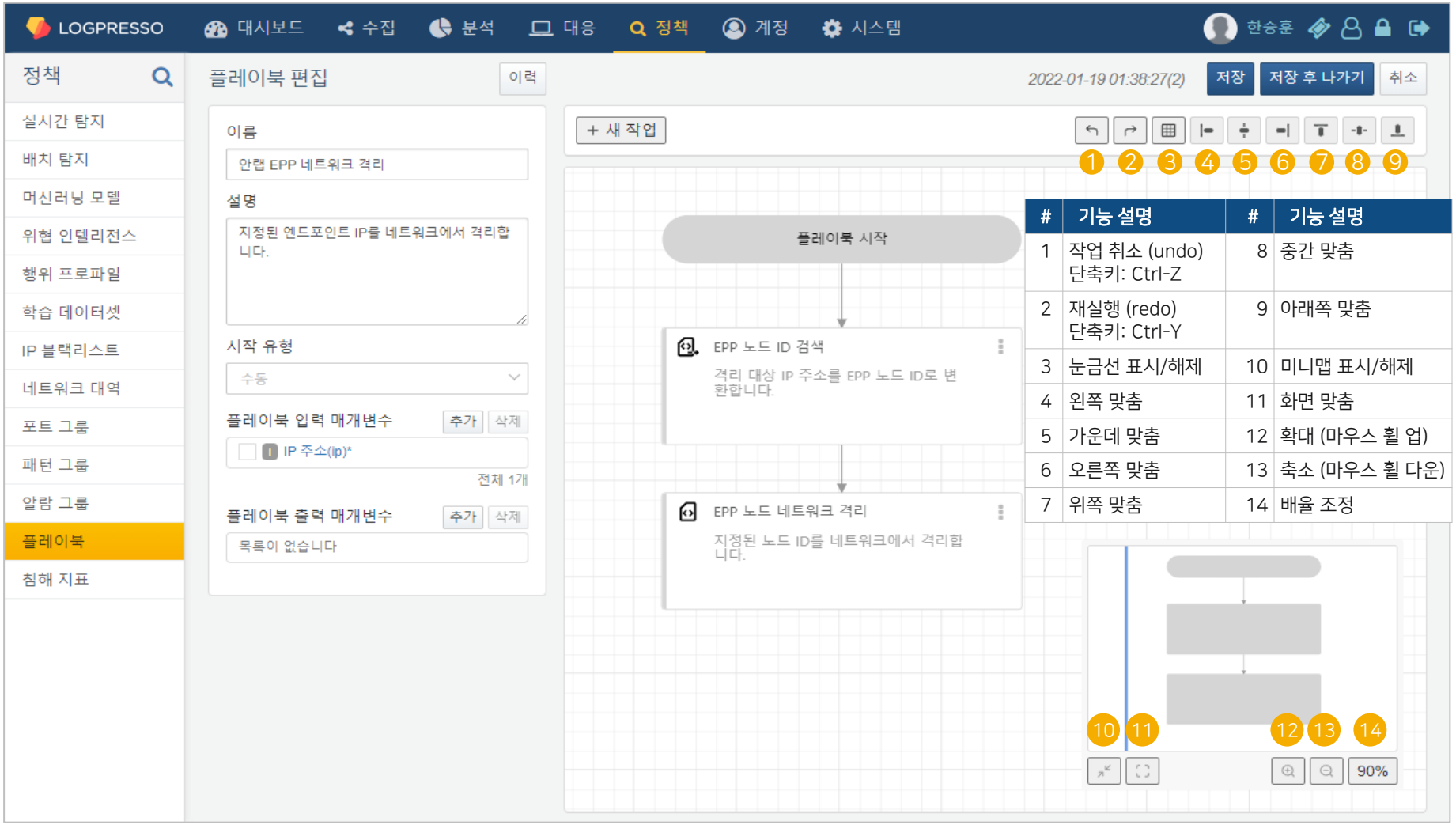
티켓 유형에 따라 사전 정의된 플레이북이 구성되고 시스템에 할당된 태스크가 자동으로 수행됩니다. 모든 분석 자료가 자동 취합되어 준비된 상태에서 보안팀이 바이너리의 악성여부 판단만 확정해주면, 이후 악성코드 제거나 예외 처리 등의 단계가 일괄 실행됩니다.



작업	작업 설명	자동화 방안
IP 평판 조회	내부에서 접속한 공인 IP가 다른 조직에서도 공격 이력이 있는 악성 IP인지 위협 인텔리전스를 조회합니다.	티켓의 IP 주소 목록을 자동으로 추출하여 위협 인텔리전스 API를 호출합니다. 위협 인텔리전스별 특화된 정보를 위협 분석 정보로 취합합니다.
MD5 평판 조회	새 바이너리 해시가 알려진 바이너리인지, 악성 바이너리인지 위협 인텔리전스를 조회합니다.	티켓의 MD5 해시 목록을 자동으로 추출하여 위협 인텔리전스 API를 호출합니다. 위협 인텔리전스별 특화된 정보를 위협 분석 정보로 취합합니다.
ITSM 자산 정보 조회	현재 의심 바이너리가 발견된 호스트의 정보를 확인하여 네트워크 차단에 대한 위험성을 평가합니다. 예를 들어 중요 서비스 IP를 격리하면 대고객 장애가 발생할 수 있습니다.	액티브 디렉터리 기반의 인프라를 운영하는 경우, LDAP 프로토콜을 통해 자산 정보를 디렉터리에서 자동으로 조회할 수 있습니다. ITSM을 내부에 별도로 구축한 경우에는, DB나 API 호출을 통해 자산 정보를 취합합니다.
샌드박스 분석 실행	의심 바이너리를 샌드박스 솔루션에서 실행하여 행위분석 보고서를 확인합니다. (프로세스 실행, 레지스트리 기록, 파일 드롭 등)	Cisco Threat Grid, Joe Sandbox 등 샌드박스 솔루션에 자동으로 의심 바이너리를 업로드하여 분석(detonate)하고, 행위분석 결과를 취합합니다.
EDR 호스트 스캔	동일한 바이너리가 다른 호스트에서도 발견되는지 설치 혹은 전파 내역을 확인합니다.	EDR 서버를 통해 EDR 에이전트가 설치된 모든 호스트에 자동으로 파일 검색 명령을 내리고, 비동기적으로 검색 결과를 취합합니다.
화이트리스팅	정상 바이너리로 확인되면 MD5를 예외 처리합니다.	EDR 서버에 예외 처리 명령을 자동으로 전달합니다.
악성코드 제거	악성코드로 확인되면 발견된 모든 호스트에서 제거합니다.	EDR 서버에 제거 명령을 자동으로 전달합니다.
사고분석 보고서	사고분석 보고서를 작성하여 내부 보고합니다.	각 작업의 자동 혹은 수동 실행 내역을 시간대별로 자동 생성하여 첨부합니다.
악성코드 샘플 공유	외부 인텔리전스나 유관 기관에 악성코드 샘플을 공유합니다.	금융보안원 FCTI 등 외부 인텔리전스에 샘플을 자동으로 업로드합니다.

플레이북 디자이너

위지윅 방식으로 손쉽게 플레이북 워크플로우를 구성할 수 있습니다. 태스크를 클릭하면 연결점이 활성화되고 이를 드래그하여 연결하면 작업 의존성이 설정됩니다. 태스크 복제, 작업 취소 (Undo), 재실행 (Redo), 다중 선택 및 정렬 맞춤 기능, 버전 이력과 같은 편의 기능을 제공합니다.



#	기능 설명	#	기능 설명
1	작업 취소 (undo) 단축키: Ctrl-Z	8	중간 맞춤
2	재실행 (redo) 단축키: Ctrl-Y	9	아래쪽 맞춤
3	눈금선 표시/해제	10	미니맵 표시/해제
4	왼쪽 맞춤	11	화면 맞춤
5	가운데 맞춤	12	확대 (마우스 휠 업)
6	오른쪽 맞춤	13	축소 (마우스 휠 다운)
7	위쪽 맞춤	14	배율 조정

태스크 유형

실행 태스크
마에스트로 혹은 보안 솔루션/서비스별 앱으로 확장된 플레이북 명령어를 실행합니다.

분기 태스크
비교 혹은 불리언 표현식의 평가 값에 따라 T 혹은 F로 실행 경로를 분기합니다.

수식 태스크
로그프레소 함수와 연산자를 사용한 표현식의 평가 값을 새로운 플레이북 변수에 할당합니다.

사용자 입력 태스크
불리언, 문자열, 문항 선택 3가지 유형으로 사용자 입력을 받아 새로운 플레이북 변수에 할당합니다.

승인 태스크
사용자의 의견과 함께 승인/반려 여부를 받아 실행 경로를 분기합니다.

대기 태스크
지정된 초 단위 시간을 대기합니다.

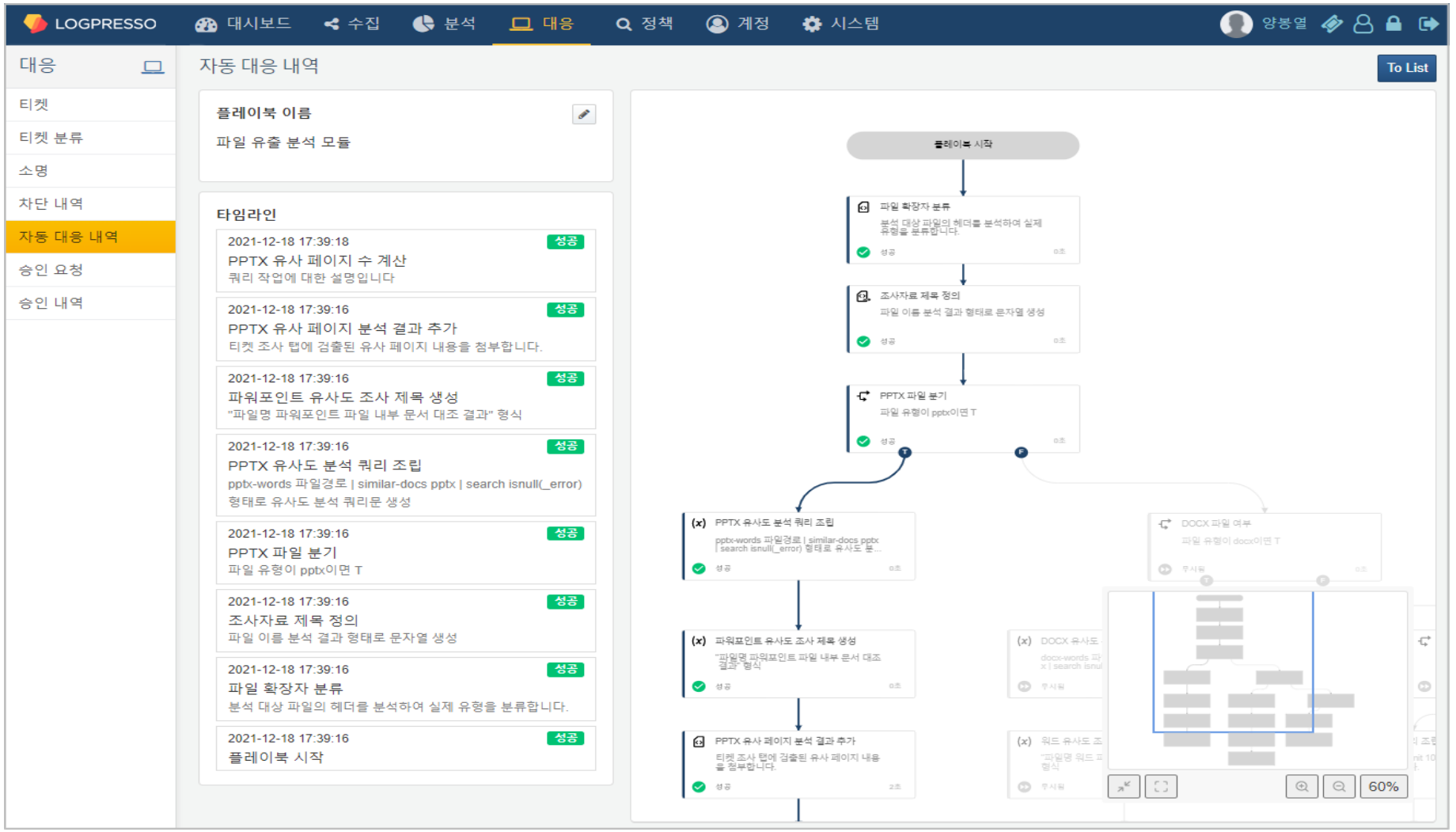
이메일 전송 태스크
플레이북 변수를 삽입하여 제목 및 내용을 동적으로 생성하고 이메일을 전송합니다. (텍스트, 마크다운, HTML 지원)

플레이북 호출 태스크
다른 플레이북을 호출합니다. 모듈화된 플레이북의 재활용과 루프 변수 지정을 통한 반복 호출을 지원합니다.

쿼리 태스크
로그프레소 쿼리를 실행하여 결과를 플레이북 변수에 할당합니다. 쿼리 결과가 2건 이상인 경우, 각 플레이북 변수에 필드별 배열이 할당됩니다.

자동 대응 내역

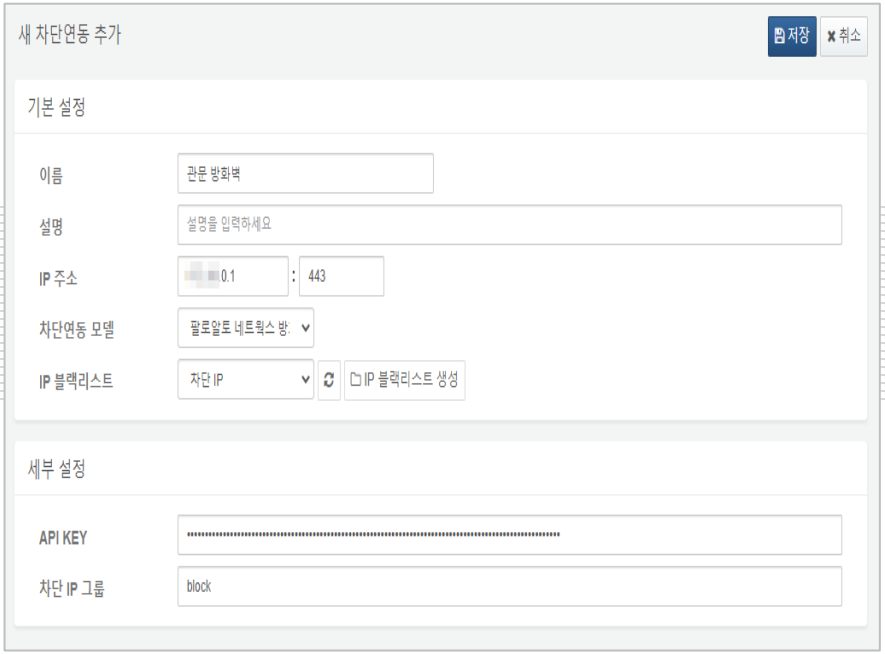
각 플레이북 실행 내역은 자동 대응 내역 메뉴에서 플레이북이 실행되는 동안 실시간으로 태스크 진행 상태를 확인할 수 있습니다. 각 태스크를 우클릭하면 태스크의 시작 종료 시점, 입출력 매개변수, 에러 코드를 확인할 수 있습니다.

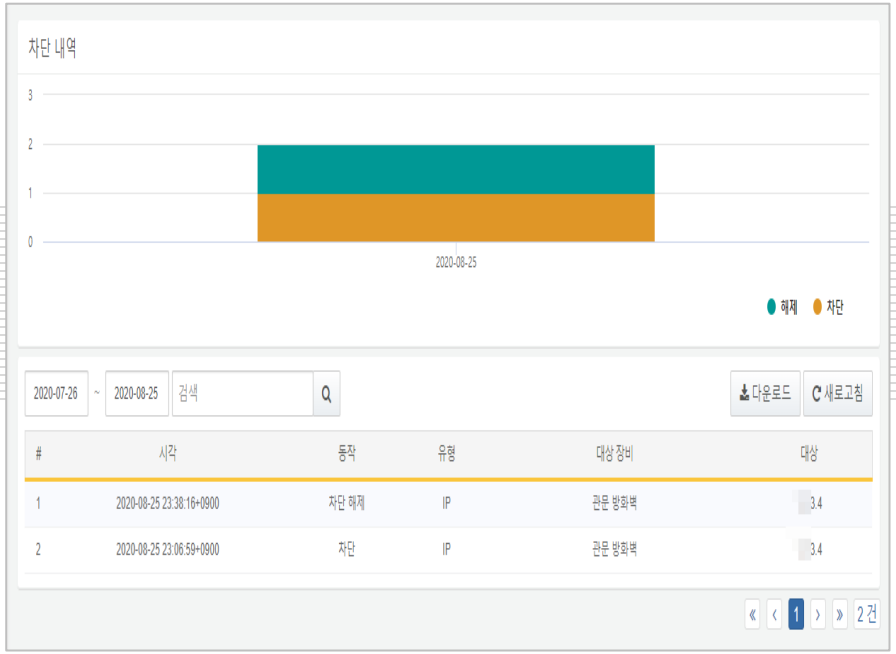


IP 차단 자동화

국내외 방화벽 장비에서 지원하는 API를 이용하여 차단 블랙리스트를 자동으로 동기화합니다. 별도로 방화벽 콘솔에 접속하여 설정하지 않더라도 플랫폼에서 공격이 반복되는 악성 IP 주소를 차단할 수 있습니다.

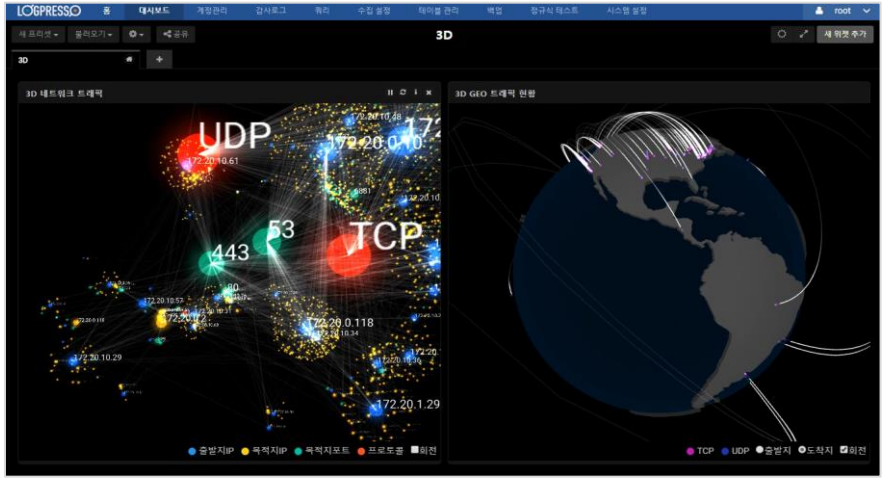
블랙리스트 추가 (자동/수동) → 차단 연동 모듈에서 인식 → 신규 차단 IP를 장비에 반영 → 네트워크 차단 동작

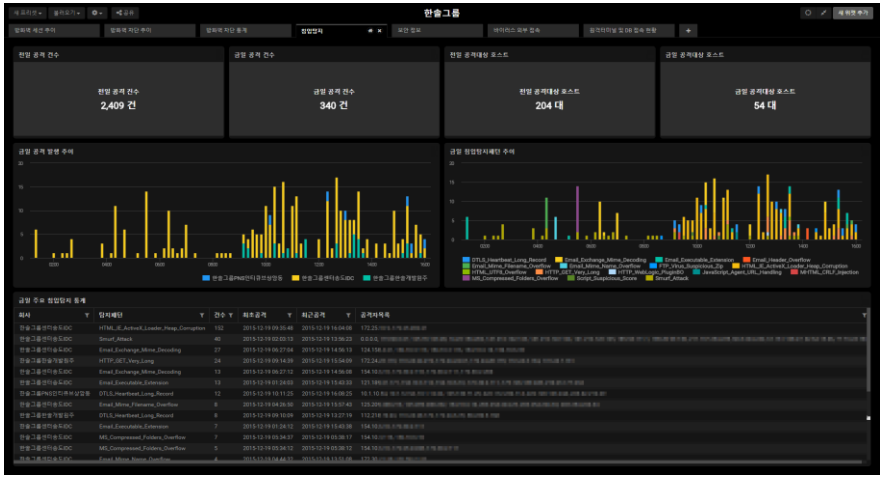


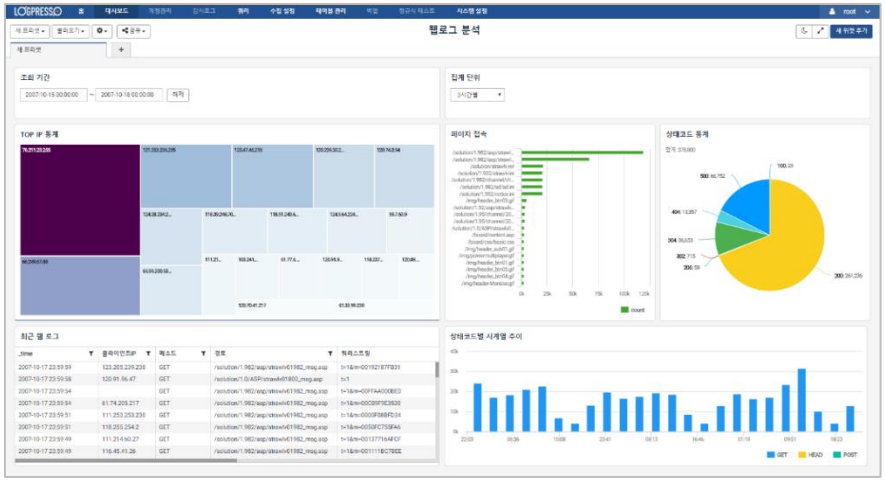


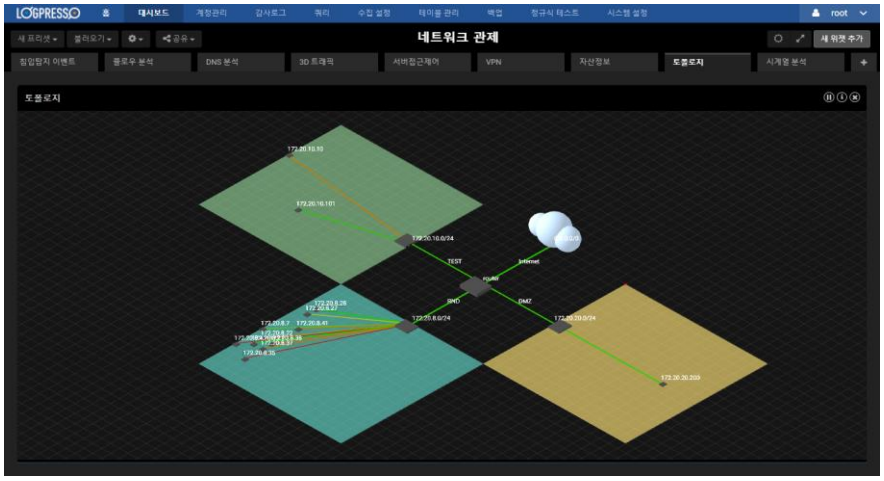
인터랙티브 대시보드

차트, 그리드에 대해 클릭, 드래그 시 필터가 추가되면서 다른 위젯들도 해당 조건을 반영하여 실시간으로 드릴다운된 결과를 표시합니다. 특정 시간대나 IP 등 다단계로 범위를 좁혀가면서 여러 탭에서 다차원으로 데이터를 검토할 수 있으므로 위협원의 행위를 여러 각도에서 쉽고 빠르게 파악할 수 있습니다.





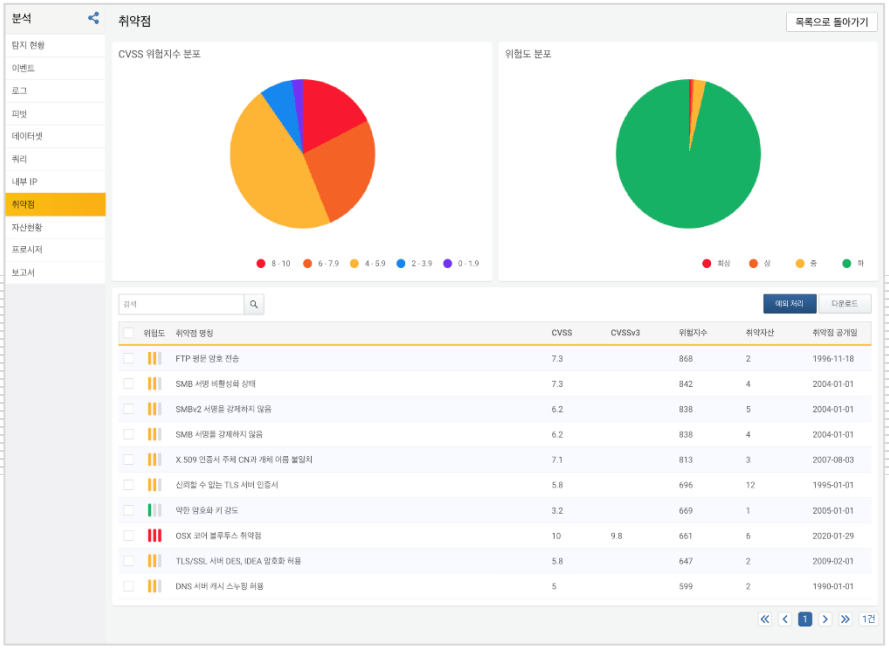


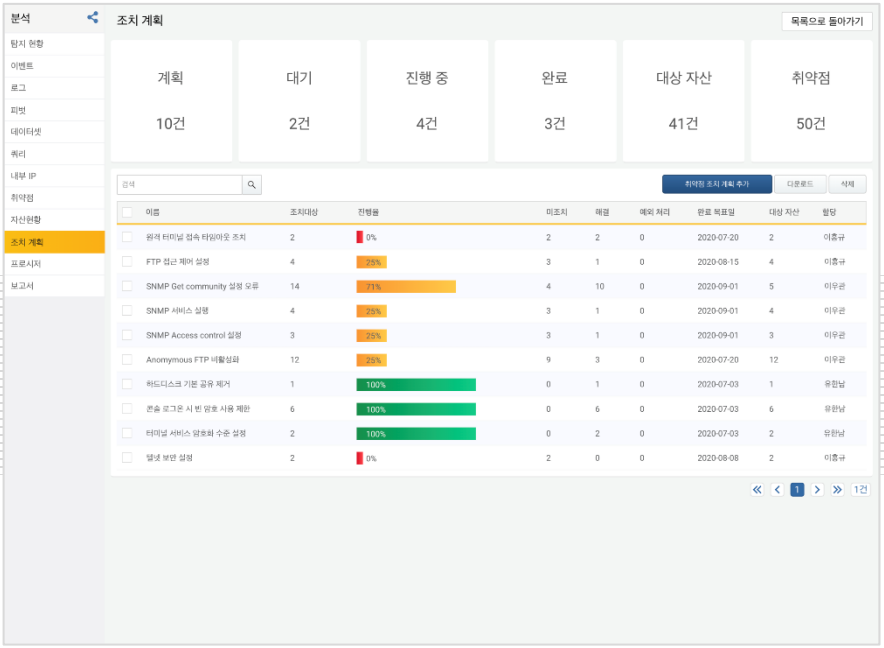


자산 및 취약점 관리

RAPID7 인사이트VM, SSR 솔리드스텝 등 취약점 진단 솔루션에서 제공하는 API를 통해 자산별 취약점 정보를 통합하여 위협 발생 시 자산 및 취약점 정보를 제시합니다. 담당자별 취약점 조치 계획을 수립하고 일정에 따라 취약점 조치가 진행되는지 가시적으로 관리할 수 있도록 지원합니다.

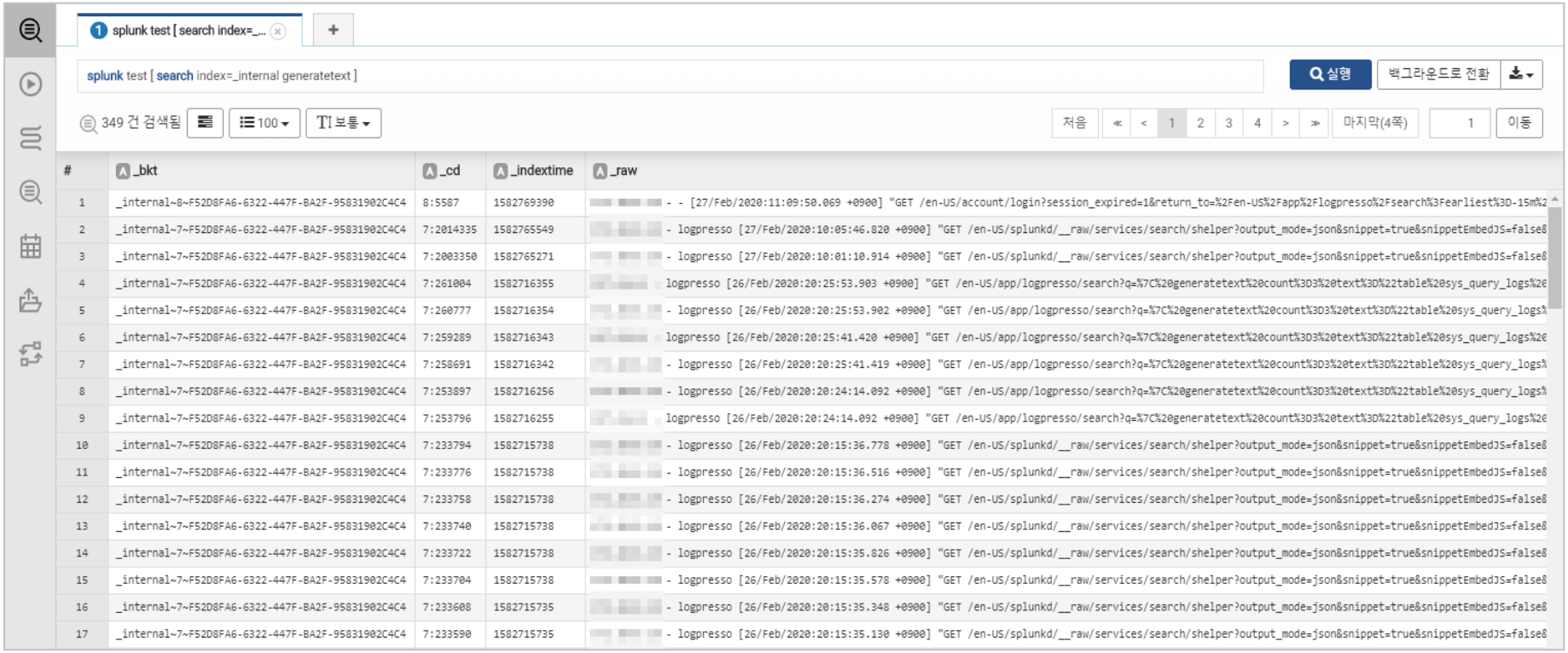
취약점 진단 정보 수집 → 취약점 조치 계획 수립 → 취약점 조치 모니터링 → 재진단 및 취약점 제거 확인





로그프레소의 스플렁크 앱

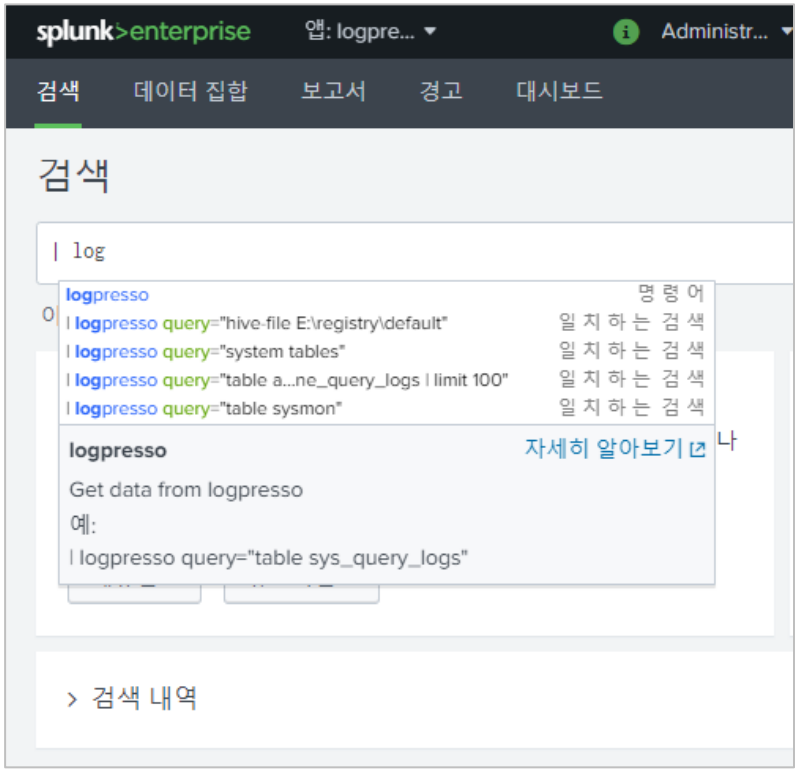
로그프레소에 스플렁크 앱을 추가 설치하면 다음과 같이 스플렁크 인스턴스에 원격으로 쿼리를 실행할 수 있습니다.

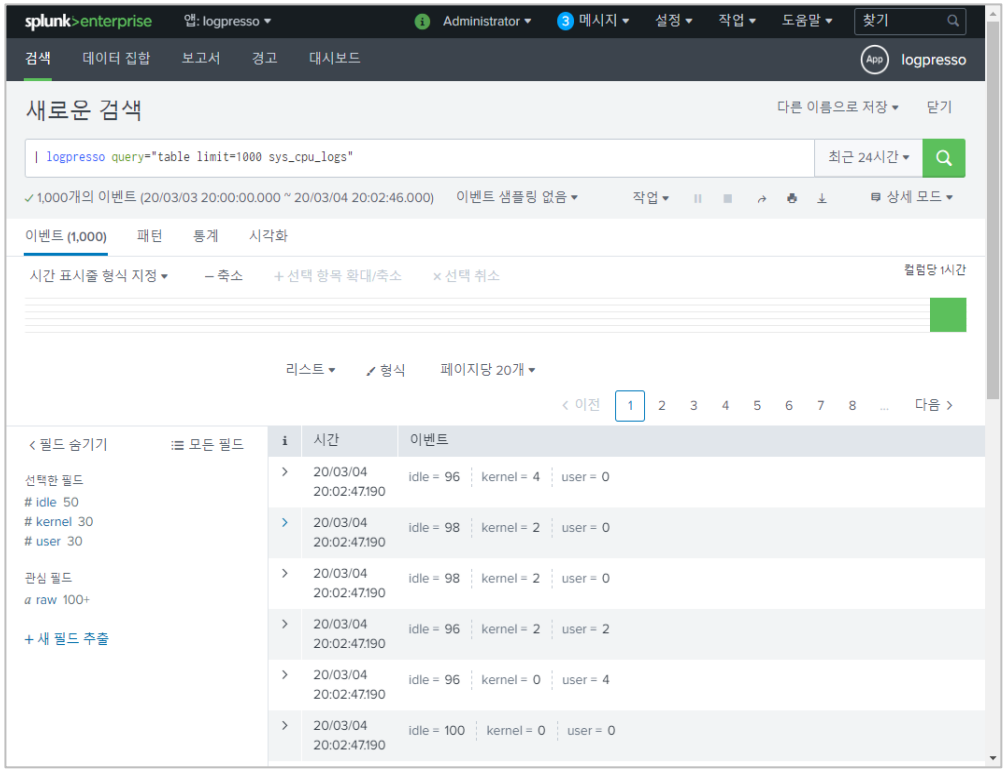


#	_bkt	_cd	_indextime	_raw
1	_internal~8~F52D8FA6-6322-447F-BA2F-95831902C4C4	8:5587	1582769390	- - [27/Feb/2020:11:09:50.069 +0900] "GET /en-US/account/login?session_expired=1&return_to=%2Fen-US%2Fapp%2Flogpresso%2Fsearch%3Fearliest%3D-15m%2
2	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:2014335	1582765549	- logpresso [27/Feb/2020:10:05:46.820 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
3	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:2003350	1582765271	- logpresso [27/Feb/2020:10:01:10.914 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
4	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:261004	1582716355	logpresso [26/Feb/2020:20:25:53.903 +0900] "GET /en-US/app/logpresso/search?q=%7C%20generatetext%20count%3D3%20text%3D%22table%20sys_query_logs%20
5	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:260777	1582716354	- logpresso [26/Feb/2020:20:25:53.902 +0900] "GET /en-US/app/logpresso/search?q=%7C%20generatetext%20count%3D3%20text%3D%22table%20sys_query_logs%
6	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:259289	1582716343	logpresso [26/Feb/2020:20:25:41.420 +0900] "GET /en-US/app/logpresso/search?q=%7C%20generatetext%20count%3D3%20text%3D%22table%20sys_query_logs%20
7	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:258691	1582716342	- logpresso [26/Feb/2020:20:25:41.419 +0900] "GET /en-US/app/logpresso/search?q=%7C%20generatetext%20count%3D3%20text%3D%22table%20sys_query_logs%
8	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:253897	1582716256	- logpresso [26/Feb/2020:20:24:14.092 +0900] "GET /en-US/app/logpresso/search?q=%7C%20generatetext%20count%3D3%20text%3D%22table%20sys_query_logs%
9	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:253796	1582716255	logpresso [26/Feb/2020:20:24:14.092 +0900] "GET /en-US/app/logpresso/search?q=%7C%20generatetext%20count%3D3%20text%3D%22table%20sys_query_logs%20
10	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:233794	1582715738	- logpresso [26/Feb/2020:20:15:36.778 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
11	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:233776	1582715738	- logpresso [26/Feb/2020:20:15:36.516 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
12	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:233758	1582715738	- logpresso [26/Feb/2020:20:15:36.274 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
13	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:233740	1582715738	- logpresso [26/Feb/2020:20:15:36.067 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
14	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:233722	1582715738	- logpresso [26/Feb/2020:20:15:35.826 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
15	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:233704	1582715738	- logpresso [26/Feb/2020:20:15:35.578 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
16	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:233608	1582715735	- logpresso [26/Feb/2020:20:15:35.348 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&
17	_internal~7~F52D8FA6-6322-447F-BA2F-95831902C4C4	7:233590	1582715735	- logpresso [26/Feb/2020:20:15:35.130 +0900] "GET /en-US/splunkd/__raw/services/search/shelper?output_mode=json&snippet=true&snippetEmbedJS=false&

스플렁크의 로그프레소 앱

스플렁크에서 로그프레소 쿼리를 원격으로 실행하는 스플렁크 앱을 제공합니다. pylogpresso 라이브러리를 사용하여 로그프레소 서버와 통신합니다.





기대 효과

로그프레소 마에스트로의 보안 오케스트레이션 및 자동화를 통해 보안 운영 업무의 효율성, 단위 처리 시간, 품질 수준을 크게 향상시킬 수 있습니다.

대량의 위협 발생에 대한 자동화 분석으로 처리 효율 6배 이상 향상

대응 프로세스 표준화를 통해 일관된 업무 품질 달성

분석 및 차단 시간 단축으로 MTTR (Mean Time To Respond) 향상

반복 업무로 인한 피로도 감소 및 고위험군 위협 분석 집중력 향상

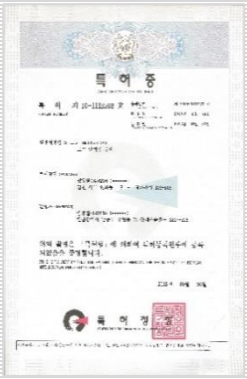
API 통합으로 기 도입한 단위 보안시스템의 활용을 극대화하여 ROI 향상

인증 및 특허

로그프레소는 CC인증 EAL2와 GS인증 1등급을 획득하였으며, 빅데이터 원천 기술 연구개발을 바탕으로 다수의 특허를 보유하고 있습니다.

– CC인증 EAL2 –

– GS인증 1등급 –



번호	발명의 명칭	등록번호	출원번호
1	로그 인덱싱 방법	10-1112568	10-2010-0101170
2	이벤트 처리 시스템의 이벤트 처리 방법 (CEP)	10-1459018	10-2014-0042232
3	자바 프로그램 실행 시 유저 데이터그램 프로토콜 패킷을 수집하는 방법	10-1487859	10-2014-0004988
4	빅데이터 입력 및 처리 방법 (스트림 쿼리)	10-1542526	10-2014-0033821
5	메시지의 필드 인덱싱 방법 (타입 최적화)	10-1770271	10-2015-0113619
6	열-지향 레이아웃 파일 생성 방법 (스키마리스)	10-1780652	10-2016-0029589
7	열-지향 레이아웃 파일 생성 방법 (암호화)	10-1809018	10-2016-0047960
8	메시지의 필드 인덱싱 방법 (쿼리 기반 토크나이저)	10-1921123	10-2017-0088290
9	개인정보처리와 관련한 로그 데이터 생성 방법 및 그 로그 데이터를 이용한 개인정보 유출 탐지 방법	10-2055706	10-2019-0014214
10	행위 확률 기반 웹 서버 공격 탐지 방법 (AI 위협헌팅)	10-2096785	10-2019-0090210

감사합니다

서울특별시 마포구 새창로 7 SNU장학빌딩 16층 (도화동 565)
02-6730-7249 contact@logpresso.com

LOGPRESSO