Logpresso Sonar 4.0 Light

| 빅데이터 및 AI 기반 통합로그분석플랫폼 |

LOGPRESSO

배경

법령을 준수하려면 **통합로그관리 솔루션을 필수적으로 도입**해야 합니다.

정보통신망법 제47조, 제48조의 4

- 정보보호 관리체계(ISMS) 인증 의무화 (제47조)
- 침해사고 원인분석을 위한 접속 기록 등 관련 자료의 보존 (제48조의 4)
- 침해사고 관련정보의 훼손 · 멸실 및 변경 등을 방지할 수 있는 조치 (시행령 제58조)
- 필요 시 암호기술을 적용 (시행령 제58조)

전자금융거래법 제22조

- 5년 이내의 전자금융거래기록 보존 (제22조)

개인정보보호법 제29조

- 개인정보 분실/도난/유출/위조/변조 또는 훼손되지 않도록 내부 관리계획 및 접속기록 보관
- 접속 기록의 안전한 보관, 최소 1년 이상 보존, 월 1회 이상 점검
  (개인정보의 안전성 확보조치 기준 제8조, 개인정보의 기술적·관리적 보호조치 기준 제5조)

신용정보법 제17조, 제19조, 제20조

- 신용정보의 처리 위탁 시 주체 식별 정보 암호화 등의 보호조치 (제17조)
- 제3자의 불법적인 접근, 정보 변경 · 훼손 및 파괴에 대한 기술적 대책 마련 (제19조)
- 개인신용정보 처리 기록을 3년간 보존 (제20조)
- 개인신용정보취급자의 권한 부여, 변경, 말소 기록을 최소 3년 이상 보존
  (금융위원회 신용정보업감독규정 제20조 별표 3)
- 개인신용정보처리시스템의 접속 기록 최소 1년 이상 보존, 월1회 이상 점검
  (금융위원회 신용정보업감독규정 제20조 별표 3)

배경

로그 관리의 어려움

1 로그 처리 복잡도 증가

- 쿠버네티스 (k8s) 및 도커 컨테이너 지원 필요
- 온프레미스, 클라우드 하이브리드 운영
- SaaS 로그 수집 및 분석 필요

2 업무 지연

- 대규모 로그 수집, 저장, 검색, 분석 필요
- 느린 검색, 분석 성능으로 지연 발생
- 처리 요구 시간 내 대응하기 어려움

3 단순 반복 업무

- 반복적인 로그 조회, 검색, 보고서 작성
- API 기반 업무 자동화가 지원되지 않음
- 단순 데이터 가공 작업에 따른 업무 피로 증가

기존 로그 관리는 최신 IT 환경을 지원하지 않고, 성능이 느리며 자동화가 불가능합니다.

솔루션

로그프레소는 최신 IT 아키텍처를 지원하는 통합로그관리 플랫폼을 제공하여 여러분의 문제를 해결해드립니다.

현대화

쿠버네티스, 오픈시프트 등
컨테이너 환경 로그 수집 지원

퍼블릭 클라우드
SaaS, PaaS, IaaS 로그 수집

고성능

270만 EPS, 410MB/s
고속 풀텍스트 인덱싱

전체 1TB, 25억건 기준
2300만 건 검색에 **0.8초**

자동화

100종 이상의
REST API 제공

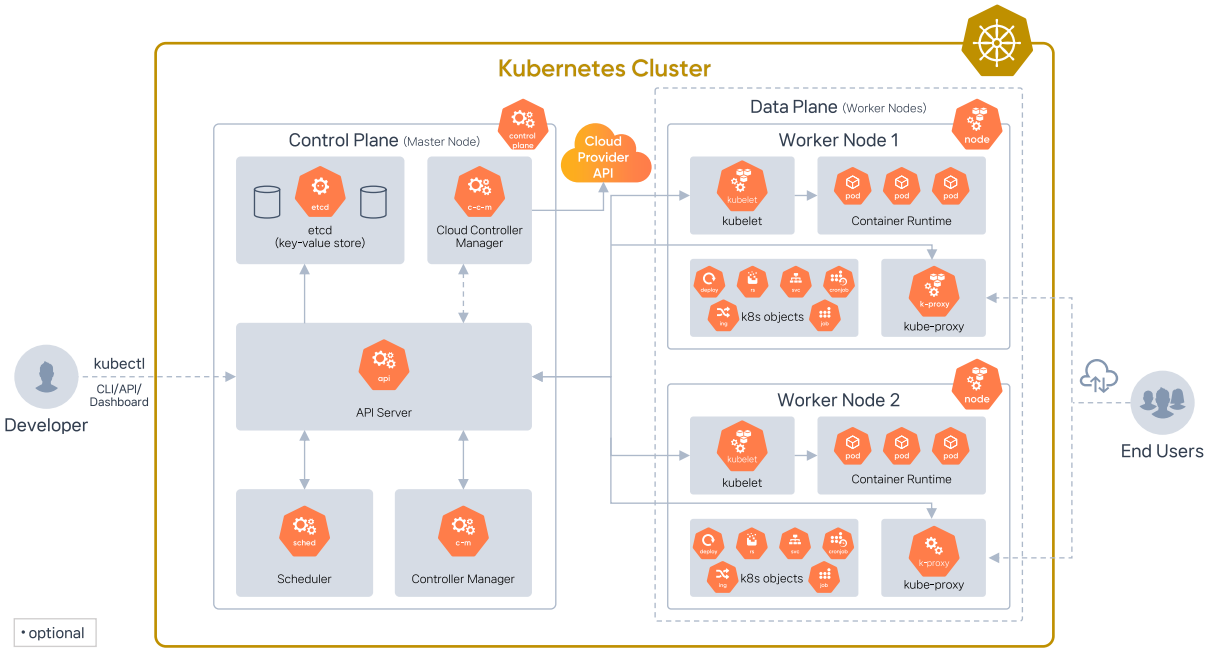
300종 이상의
명령어, 함수로 보고서 작성

현대화

프라이빗 클라우드, 퍼블릭 클라우드, SaaS까지 모든 영역을 포괄하는 통합로그관리 플랫폼을 제공합니다.

SYSLOG, SNMP를 통한 수집이나 베어메탈 머신에 에이전트를 설치하여 로그를 수집하는 전통적 방식 뿐만 아니라, 현대적 마이크로서비스 아키텍처를 지원합니다.

쿠버네티스 환경



DaemonSet으로 쿠버네티스 노드별 로그프레소 센트리 구성

Worker Node의 호스트 볼륨에 기록되는 로그 일괄 수집

클라우드 및 SaaS 환경

금융보안원 NGFCTI

금융보안원 FCTI 서비스의 IP, 도메인, URL 위협정보와 악성파일 MD5, SHA256 정보를 동기화합니다.

SNR/MAE
2023-05-16

네이버 클라우드

네이버 클라우드 앱은 클라우드 액티비티 청구 비용, 서버 운영 상태 등 클라우드 보안형상관리(CSPM)에 필요한 다양한 실시간 모니터링 기능을 제공합니다.

STD/ENT/SNR/MAE
2022-09-11

넷위트니스

RSA 넷위트니스 앱은 REST API를 통해 메타를 수집, 검색하여 완전한 세션 로그를 재조립합니다. 넷위트니스 전용 대시보드, 패킷 검색, PCAP 파일 다운로드, 파일 주출 정보를 제공합니다.

STD/ENT/SNR/MAE
2022-05-19

노션

노션 앱은 REST API를 이용하여 노션 계정목록, 페이지 메타데이터, 블록 정보를 조회하는 기능을 제공합니다.

STD/ENT/SNR/MAE
2022-10-15

마이크로소프트 365

마이크로소프트 365 API를 통해 사용자 계정, 파일, 메일 이용 현황을 모니터링하고 인가되지 않은 자료 접근 및 유출을 탐지합니다.

STD/ENT/SNR/MAE
2022-05-22

마이크로소프트 애저

Azure 앱은 애저 클라우드 API 연동을 통해 활동 로그, 성능지표 모니터링을 제공하고, 클라우드 리소스의 목록과 설정을 관리할 수 있도록 지원합니다.

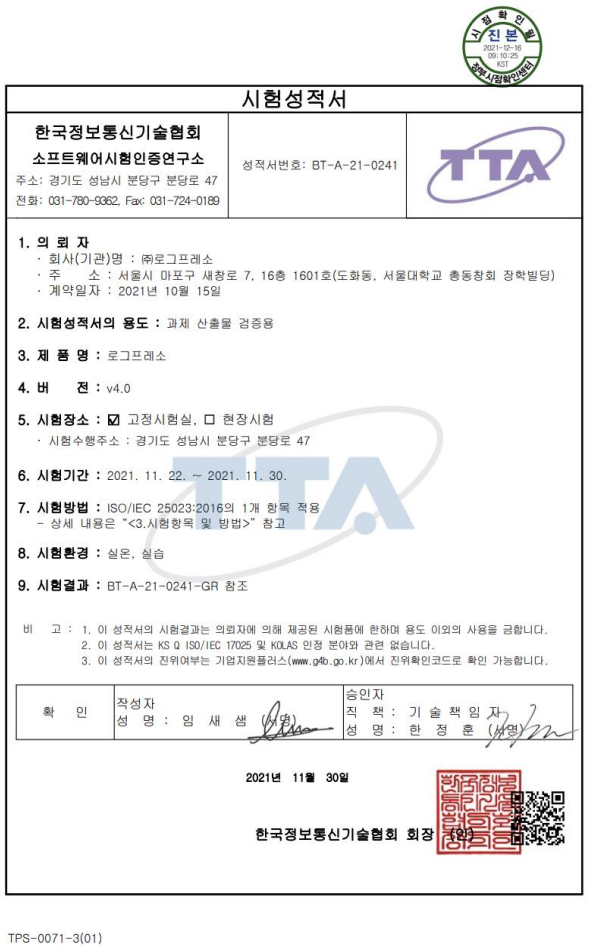
STD/ENT/SNR/MAE
2022-10-04

로그프레소 앱 – 클라우드 및 SaaS 전용 API를 통한 정보 수집 지원

고성능

특허 등록된 AVX2 SIMD 가속 기술이 적용되어 업계 최고의 성능을 제공합니다.

TTA 시험성적서 BT-A-21-0241



시험성적서

한국정보통신기술협회
소프트웨어시험인증연구소
주소: 경기도 성남시 분당구 분당로 47
전화: 031-780-9362, Fax: 031-724-0189

성적서번호: BT-A-21-0241

1. 의 뢰 자
· 회사(기관)명 : ㈜로그프레소
· 주 소 : 서울시 마포구 새창로 7, 16층 1601호(도화동, 서울대학교 총동창회 장학빌딩)
· 계약일자 : 2021년 10월 15일

2. 시험성적서의 용도 : 과제 산출물 검증용

3. 제 품 명 : 로그프레소

4. 버 전 : v4.0

5. 시험장소 : ☑ 고정시험실, ☐ 현장시험
· 시험수행주소 : 경기도 성남시 분당구 분당로 47

6. 시험기간 : 2021. 11. 22. ~ 2021. 11. 30.

7. 시험방법 : ISO/IEC 25023:2016의 1개 항목 적용
- 상세 내용은 "<3.시험항목 및 방법>" 참고

8. 시험환경 : 실온, 실습

9. 시험결과 : BT-A-21-0241-GR 참조

비 고 : 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하며 용도 이외의 사용을 금합니다.
2. 이 성적서는 KS Q ISO/IEC 17025 및 KOLAS 인정 분야와 관련 없습니다.
3. 이 성적서의 진위여부는 기업지원플러스(www.g4b.go.kr)에서 진위확인코드로 확인 가능합니다.

확 인	작성자 성 명 : 임 새 샘 (서명)	승인자 직 책 : 기 술 책 임 자 성 명 : 한 정 훈 (서명)

2021년 11월 30일

한국정보통신기술협회 회장 (인)

TPS-0071-3(01)

270만 PPS 무손실 실시간 인덱싱

실시간 인덱싱 및 저장 수행 시 패킷 손실률이 0%인지 확인

ID	시험항목	시험목표 및 기준	결과	비고
TC1	패킷 손실률 측정1	<시험목표> 패킷 발생 시, 해당 패킷에 대한 실시간 인덱싱 및 저장 수행 시 패킷 손실률이 0%인지 확인 <시험기준> o 기준: 전체 송신 패킷 개수 대비 수신 패킷 개수의 평균 비율 o 산정식: $X = \sum_{i=1}^{n}(A_i/B_i)/n \times 100$ - Ai: i번째 측정에서 손실된 패킷 수 - Bi: i번째 측정에서 송신한 총 패킷 수 - n: 측정 횟수 ※ 패킷 발생은 신청기업에서 제공하는 트래픽 제너레이터 사용 ※ TC1의 시험기준 및 시료는 시험의뢰기업에서 제공함	X = 0 (단위: %)	3회 반복수행 결과값 모두 동일. 시스로그 패킷 평균 사이즈: 160bytes
TC2	패킷 손실률 측정2	<시험목표> 400만 PPS(Packet per Second)로 5억 패킷 발생 시, 해당 패킷에 대한 실시간 패킷 손실률이 0%인지 확인 <시험기준> o 기준: 전체 송신 패킷 개수 대비 수신 패킷 개수의 평균 비율 o 산정식: $X = \sum_{i=1}^{n}(A_i/B_i)/n \times 100$ - Ai: i번째 측정에서 손실된 패킷 수 - Bi: i번째 측정에서 송신한 총 패킷 수 - n: 측정 횟수 ※ 패킷 발생은 신청기업에서 제공하는 트래픽 제너레이터 사용 ※ TC2의 시험기준 및 시료는 시험의뢰기업에서 제공함	X = 0 (단위: %)	3회 반복수행 결과값 모두 동일. 시스로그 패킷 평균 사이즈: 160bytes

X = 0
(단위 : %)

1TB 25억건 0.01초 내 검색

ID	시험항목	시험목표 및 기준	결과	비고
TC5	데이터 검색 속도 측정1	<시험목표> 데이터를 수집하고 인덱싱 후 저장한 상태에서, IP "37.220.35.143"을 검색했을 때 검색에 소요되는 시간을 확인 <시험기준> o 기준: ISO/IEC 25023:2016 - 8.3.1 Time behaviour measures (PTb-3-G: Mean turnaround time) o 산정식: $X = \sum_{i=1}^{n}(B_i - A_i)/n$ - Ai: 작업 i의 시작 시간 - Bi: 작업 i의 완료 시간 - n: 측정 횟수 ※ 기준: 수집된 2,487,068,366건의 데이터 중 특정 IP를 검색하는 쿼리 수행 시간의 ※ TC5의 시료는 시험의뢰기업에서 제	X = 9.8 (단위: ms)	최대: 11 ms 최소: 9 ms 검색결과 건수: 34 건
TC6	데이터 검색 속도 측정2	<시험목표> 데이터를 수집하고 인덱싱 후 저장한 "112.136.154.26"을 검색했을 때 검색 시간을 확인 <시험기준> o 기준: ISO/IEC 25023:2016 - 8.3.1 Time behaviour measures (PTb-3-G: Mean turnaround time) o 산정식: $X = \sum_{i=1}^{n}(B_i - A_i)/n$ - Ai: 작업 i의 시작 시간 - Bi: 작업 i의 완료 시간 - n: 측정 횟수 ※ 기준: 수집된 2,487,068,366건의 데이터 중 특정 IP를 검색하는 쿼리 수행 시간의 평균 ※ TC6의 시료는 시험의뢰기업에서 제공함	X = 807.7 (단위: ms)	최대: 885 ms 최소: 717 ms 검색결과 건수: 23,618,244 건

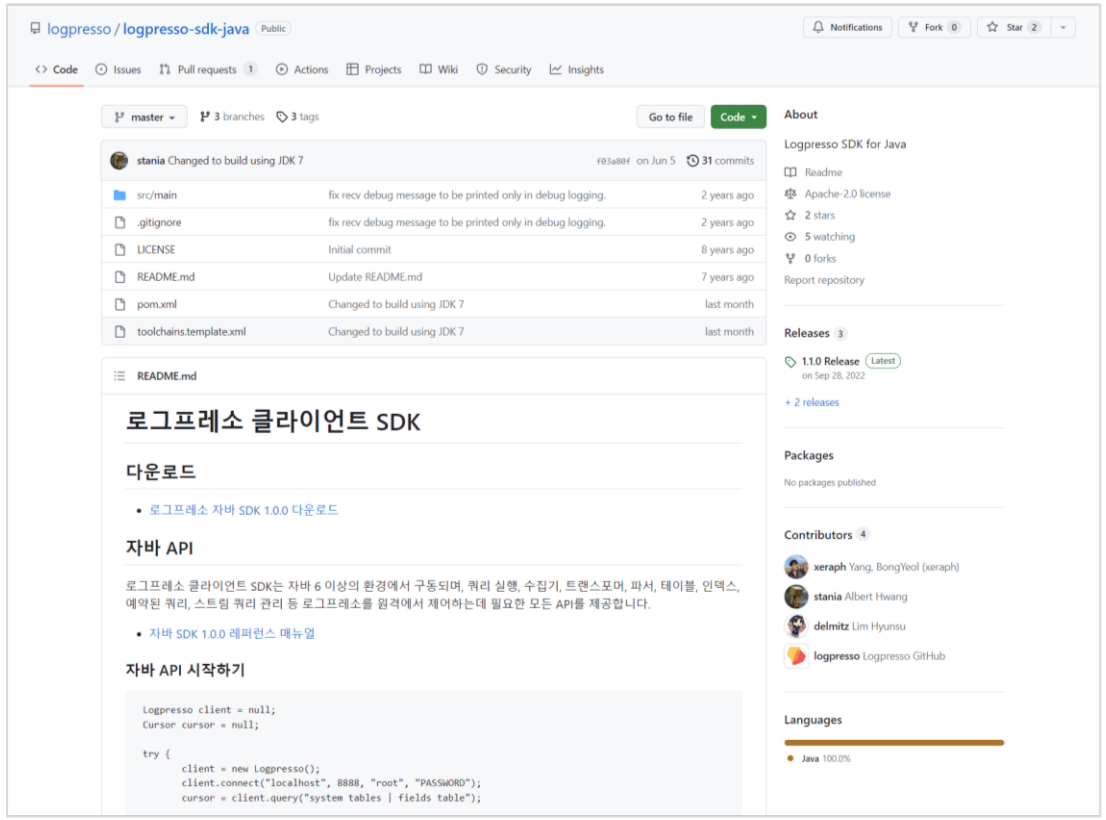
X = 9.8
(단위 :ms)

자동화

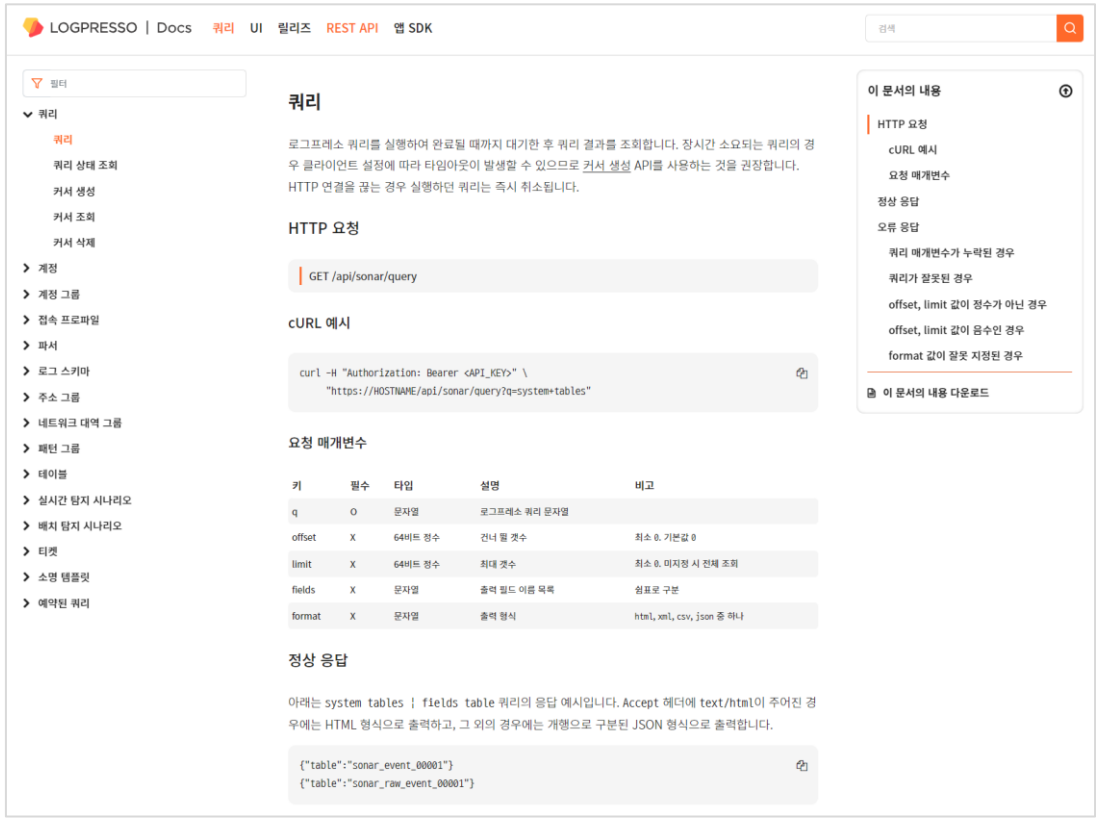
전용 클라이언트 SDK 및 100종 이상의 REST API를 지원합니다.

SOAR(Security Orchestration, Automation, and Response), 보안 포털 등 외부 시스템과 연계하여 자동화 구축 시 원활한 상호운용성을 제공합니다.

클라이언트 SDK



REST API

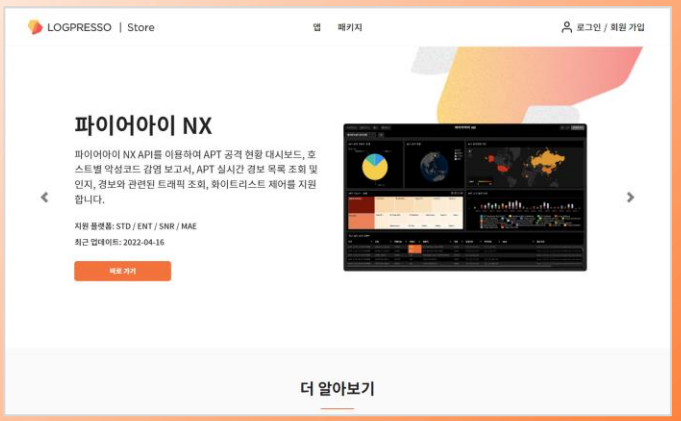


앱 확장성

로그프레소 스토어에서 써드 파티 서비스 및 장비의 데이터 통합과 연동을 지속적으로 제공합니다.

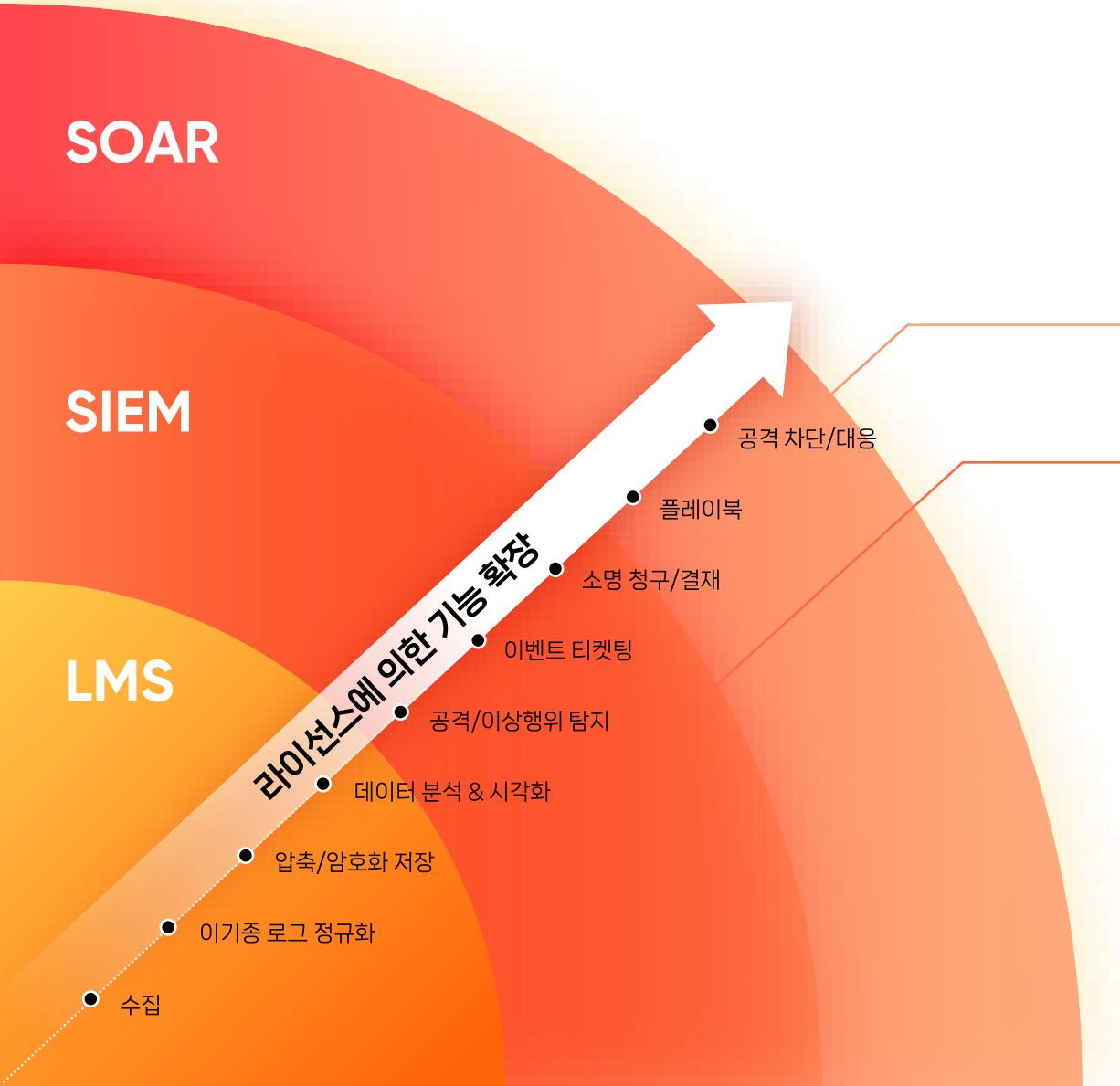
https://logpresso.store에서 150종 이상의 앱을 제공합니다. 앱은 수시로 추가되고 있습니다.

LOGPRESSO | Store



기능 확장성

동일 장비에서 라이선스 변경만으로 **통합로그에서 SIEM, SOAR까지 기능을 확장**할 수 있습니다.



LOGPRESSO

인터페이스

웹 콘솔	REST API	SSH 셸

보안운영 자동화 (SOAR)

플레이북 디자이너	태스크 워크플로우	외부 시스템 제어

통합보안관제 (SIEM)

실시간/배치 시나리오 관리	위협 이벤트 탐지	티켓 및 소명 관리

머신 빅데이터 플랫폼

실시간 풀텍스트 인덱싱	실시간 압축 및 암호화	스트리밍 및 CEP 분석

로그 수집 및 에이전트 관리

파일 및 OS API 데이터 수집	네트워크 원격 로그 수집	에이전트 관리

Apache Felix OSGi Framework - 앱 플러그인 지원

OpenJDK

회사 소개

로그프레소는 보안운영 (SecOps) 플랫폼 전문 기업입니다.

로그프레소는 빅데이터 원천 기술을 보유한 회사로, 통합로그관리(LMS), 통합보안관제(SIEM), 보안운영자동화(SOAR), 디지털 포렌식(DFIR) 솔루션, 위협 인텔리전스(CTI) 서비스를 제공합니다.

회사명	㈜ 로그프레소
설립	2013. 3. 14.
주소	서울특별시 마포구 새창로 7 SNU장학빌딩 16층
사업분야	• 빅데이터 플랫폼 기술 및 개발 • 빅데이터 분석 및 정보보호 솔루션 개발 • 보안관제시스템/서비스 구축 및 컨설팅
제품&서비스	• 로그프레소 소나 라이트 (통합로그관리) • 로그프레소 소나 (통합보안관제) • 로그프레소 마에스트로 (보안운영자동화) • 로그프레소 포렌식 (디지털 포렌식) • 로그프레소 워치 (취약점 진단 서비스) • 로그프레소 CTI (위협 인텔리전스 서비스)
인원	70명

주요 연혁

2013

- 2013. 03.14 이디엄 설립

2017

- BNK부산은행 통합로그 시스템 구축
- 기술혁신형 중소기업 인증 획득
- 특허 등록 (빅데이터 열 지향 처리 및 암호화)

2018

- 특허등록 (빅데이터 필드 인덱싱 방법)
- 조달청 나라장터 종합 쇼핑몰 등록
- KB국민은행 정보보호통합플랫폼 구축
- LS전선 내부정보유출탐지 시스템 구축
- LG화학 인프라 장애 예측 시스템 구축

2019

- ISEC, PASCON 컨퍼런스 발표
- 시드 투자 유치(우리은행)
- BNK부산은행 정보보호 통합플랫폼 구축
- NH농협생명 통합정보보호 모니터링 시스템 구축
- NH농협손보 정보보호 통합플랫폼 구축

2020

- 사명변경 (주식회사 로그프레소)
- BNK시스템 그룹공동망 보안관제 구축
- 특허 등록 (개인정보 유출 탐지 방법)

2021

- LG화학 AI기반 모니터링 시스템 구축
- BNK시스템 정보보호통합플랫폼 구축
- 삼성생명서비스 이상징후탐지시스템 구축
- Logpresso Log4j 취약점 스캐너 배포
- Logpresso Mini 배포

2022

- 하나카드 정보보호모니터링 시스템 구축
- BNK캐피탈 SIEM 구축
- LGCNS Sub-SIEM 구축
- 카카오 엔터프라이즈 SIEM 구축
- BNK경남은행 정보보호통합플랫폼 구축
- 한국재정정보원 차세대 보안관제 구축

2023

- 시리즈A 투자 유치 (KB인베스트먼트,K2인베스트먼트, CJ인베스트먼트)
- 하나금융그룹 통합보안관제 구축

인증 및 특허

로그프레소는 보안운영 플랫폼에 적용된 빅데이터 및 AI 기술에 대해 다수의 특허를 보유하고 있습니다.

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
11	다계층 메모리 구조에 최적화된 데이터 인덱스 방법 및 인덱스된 데이터의 검색 방법	10-2128037	10-2020-0002140
12	네트워크 플로우 데이터를 이용한 네트워크 자산 분류 방법	10-2244036	10-2020-0105865
13	위협 대응 자동화 방법	10-2222377	10-2020-0106709
14	벡터 연산 명령어를 통해 문자열을 고속으로 추출하는 방법	10-2370851	10-2021-0108976

주요 기능

STEP **01**

로그 수집

- 수집 대상 로그
- 에이전트 지원
- 파싱 및 정규화

STEP **02**

로그 저장

- 압축 및 암호화
- 위변조 방지

STEP **03**

로그 분석

- 풀텍스트 검색
- 연관 분석
- 피벗 분석
- 머신러닝
- 대시보드
- 쿼리
- 보고서

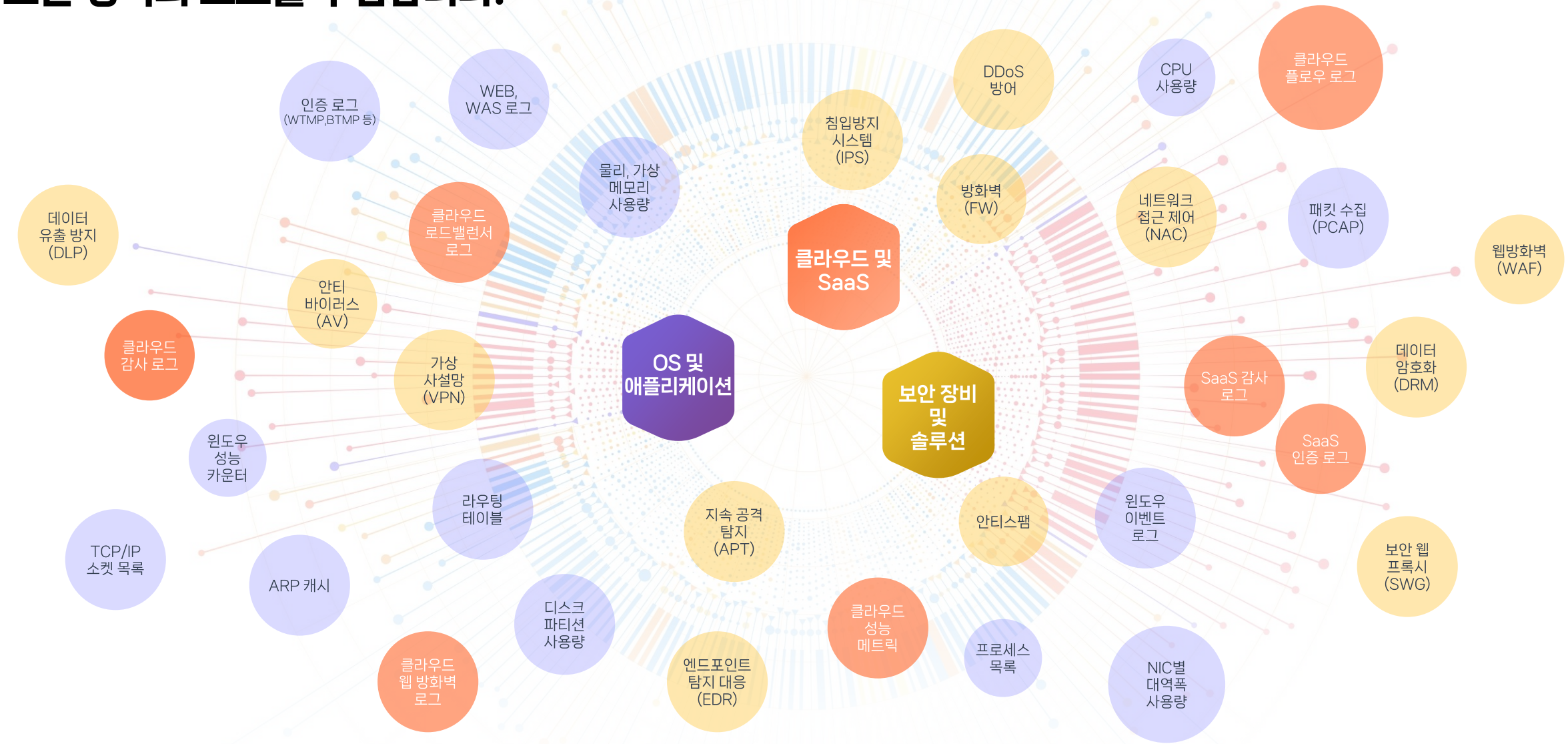
STEP 1

로그 수집 & 파싱

- 수집 대상 로그
- 에이전트 지원
- 파싱 및 정규화

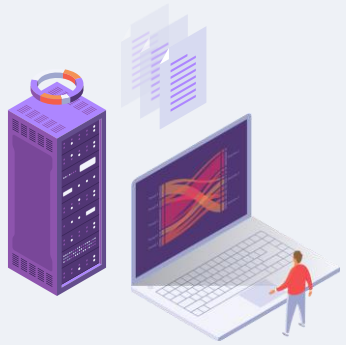
수집 대상 로그

온프레미스 환경부터 클라우드, SaaS 로그에 이르기까지 **모든 영역의 로그를 수집합니다.**



초당 무손실 실시간 인덱싱 및 수집 성능 시험 결과

초당
2,700,000건



ID	시험항목	시험목표 및 기준	결과	비고
TC1	패킷 손실률 측정1	<시험목표> 270만 PPS(Packet per Second)로 5억건의 시스로그 패킷 발생 시, 해당 패킷에 대한 실시간 인덱싱 및 저장 수행 시 패킷 손실률이 0%인지 확인 <시험기준> o 기준: 전체 송신 패킷 개수 대비 수신 패킷 개수의 평균 비율 o 산정식: $X = \sum_{i=1}^{n} (A_i / B_i) / n \times 100$ – Ai: i번째 측정에서 손실된 패킷 수 – Bi: i번째 측정에서 송신한 총 패킷 수 – n: 측정 횟수 ※ 패킷 발생은 신청기업에서 제공하는 트래픽 제너레이터 사용 ※ TC1의 시험기준 및 시료는 시험의뢰기업에서 제공함	X = 0 (단위: %)	3회 반복수행 결과값 모두 동일, 시스로그 패킷 평균 사이즈: 160bytes

시험성적서

한국정보통신기술협회
소프트웨어시험인증연구소
주소: 경기도 성남시 분당구 분당로 47
전화: 031-780-9362, Fax: 031-724-0189

성적서번호: BT-A-21-0241

1. 의 뢰 자
· 회사(기관)명 : ㈜로그프레소
· 주 소 : 서울시 마포구 새창로 7, 16층 1601호(도화동, 서울대학교 총동창회 장학빌딩)
· 계약일자 : 2021년 10월 15일

2. 시험성적서의 용도 : 과제 산출물 검증용

3. 제 품 명 : 로그프레소

4. 버 전 : v4.0

5. 시험장소 : ☑ 고정시험실, ☐ 현장시험
· 시험수행주소 : 경기도 성남시 분당구 분당로 47

6. 시험기간 : 2021. 11. 22. ~ 2021. 11. 30.

7. 시험방법 : ISO/IEC 25023:2016의 1개 항목 적용
– 상세 내용은 "<3.시험항목 및 방법>" 참고

8. 시험환경 : 실온, 실습

9. 시험결과 : BT-A-21-0241-GR 참조

비 고 : 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하며 용도 이외의 사용을 금합니다.
2. 이 성적서는 KS Q ISO/IEC 17025 및 KOLAS 인정 분야와 관련 없습니다.
3. 이 성적서의 진위여부는 기업지원플러스(www.g4b.go.kr)에서 진위확인코드로 확인 가능합니다.

확 인	작성자 성 명 : 임 새 샘 (인)	승인자 직 책 : 기 술 책 임 자 성 명 : 한 정 훈 (서명)

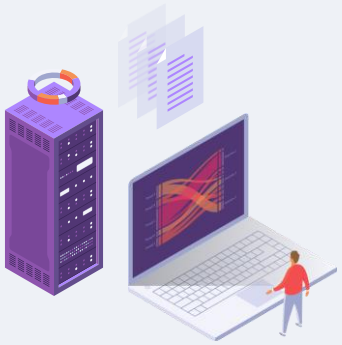
2021년 11월 30일

한국정보통신기술협회 회장 (인)

TPS-0071-3(01)

초당 무손실 수집 성능 시험 결과

초당
4,000,000건



ID	시험항목	시험목표 및 기준	결과	비고
TC2	패킷 손실률 측정2	<시험목표> 400만 PPS(Packet per Second)로 5억건의 시스로그 패킷 발생 시, 해당 패킷에 대한 실시간 저장 수행 시 패킷 손실률이 0%인지 확인 <시험기준> o 기준: 전체 송신 패킷 개수 대비 수신 패킷 개수의 평균 비율 o 산정식: $X = \sum_{i=1}^{n} (A_i / B_i) / n \times 100$ - Ai: i번째 측정에서 손실된 패킷 수 - Bi: i번째 측정에서 송신한 총 패킷 수 - n: 측정 횟수 ※ 패킷 발생은 신청기업에서 제공하는 트래픽 제너레이터 사용 ※ TC2의 시험기준 및 시료는 시험의뢰기업에서 제공함	X = 0 (단위: %)	3회 반복수행 결과값 모두 동일, 시스로그 패킷 평균 사이즈: 160bytes

시험성적서

한국정보통신기술협회
소프트웨어시험인증연구소
주소: 경기도 성남시 분당구 분당로 47
전화: 031-780-9362, Fax: 031-724-0189

성적서번호: BT-A-21-0241

1. 의 뢰 자
· 회사(기관)명 : ㈜로그프레소
· 주 소 : 서울시 마포구 새창로 7, 16층 1601호(도화동, 서울대학교 총동창회 장학빌딩)
· 계약일자 : 2021년 10월 15일

2. 시험성적서의 용도 : 과제 산출물 검증용

3. 제 품 명 : 로그프레소

4. 버 전 : v4.0

5. 시험장소 : ☑ 고정시험실, ☐ 현장시험
· 시험수행주소 : 경기도 성남시 분당구 분당로 47

6. 시험기간 : 2021. 11. 22. ~ 2021. 11. 30.

7. 시험방법 : ISO/IEC 25023:2016의 1개 항목 적용
- 상세 내용은 "<3.시험항목 및 방법>" 참고

8. 시험환경 : 실온, 실습

9. 시험결과 : BT-A-21-0241-GR 참조

비 고 : 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하며 용도 이외의 사용을 금합니다.
2. 이 성적서는 KS Q ISO/IEC 17025 및 KOLAS 인정 분야와 관련 없습니다.
3. 이 성적서의 진위여부는 기업지원플러스(www.g4b.go.kr)에서 진위확인코드로 확인 가능합니다.

확 인	작성자 성 명 : 임 새 샘 (인)	승인자 직 책 : 기 술 책 임 자 성 명 : 한 정 훈 (서명)

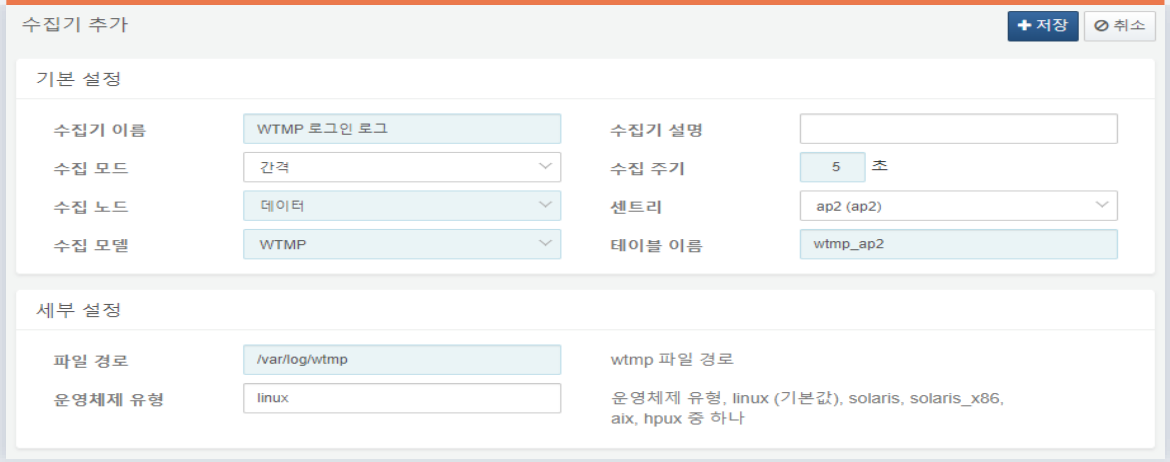
2021년 11월 30일

한국정보통신기술협회 회장 (인)

TPS-0071-3(01)

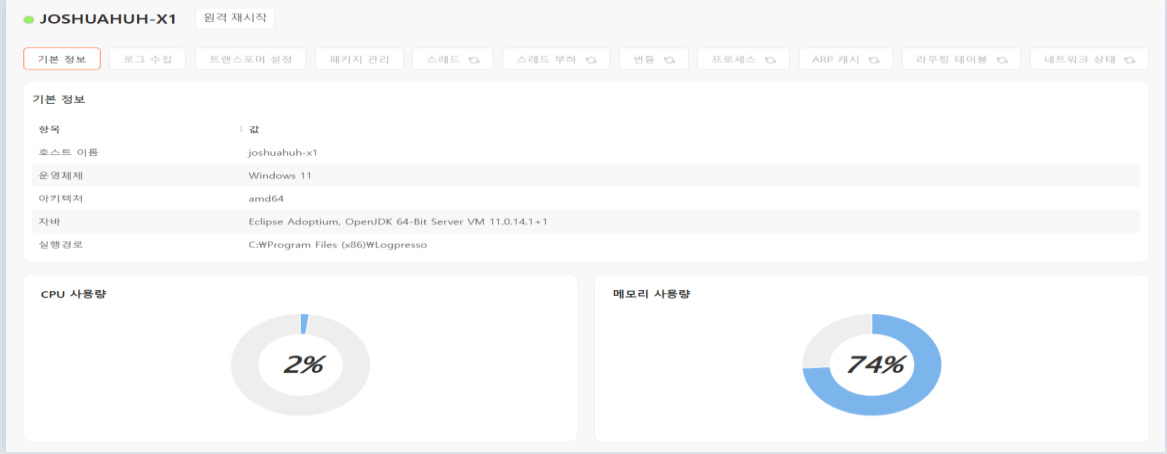
SYSLOG, SNMP, SFTP, JDBC, REST API 등을 통한 원격 수집이 불가능한 경우에는, **리눅스, 윈도우, 유닉스를 모두 지원하는 에이전트**로 데이터를 수집할 수 있습니다.

중앙제어 방식 에이전트 수집 설정



에이전트 성능 및 상태 모니터링

원격 재시작 및 업그레이드

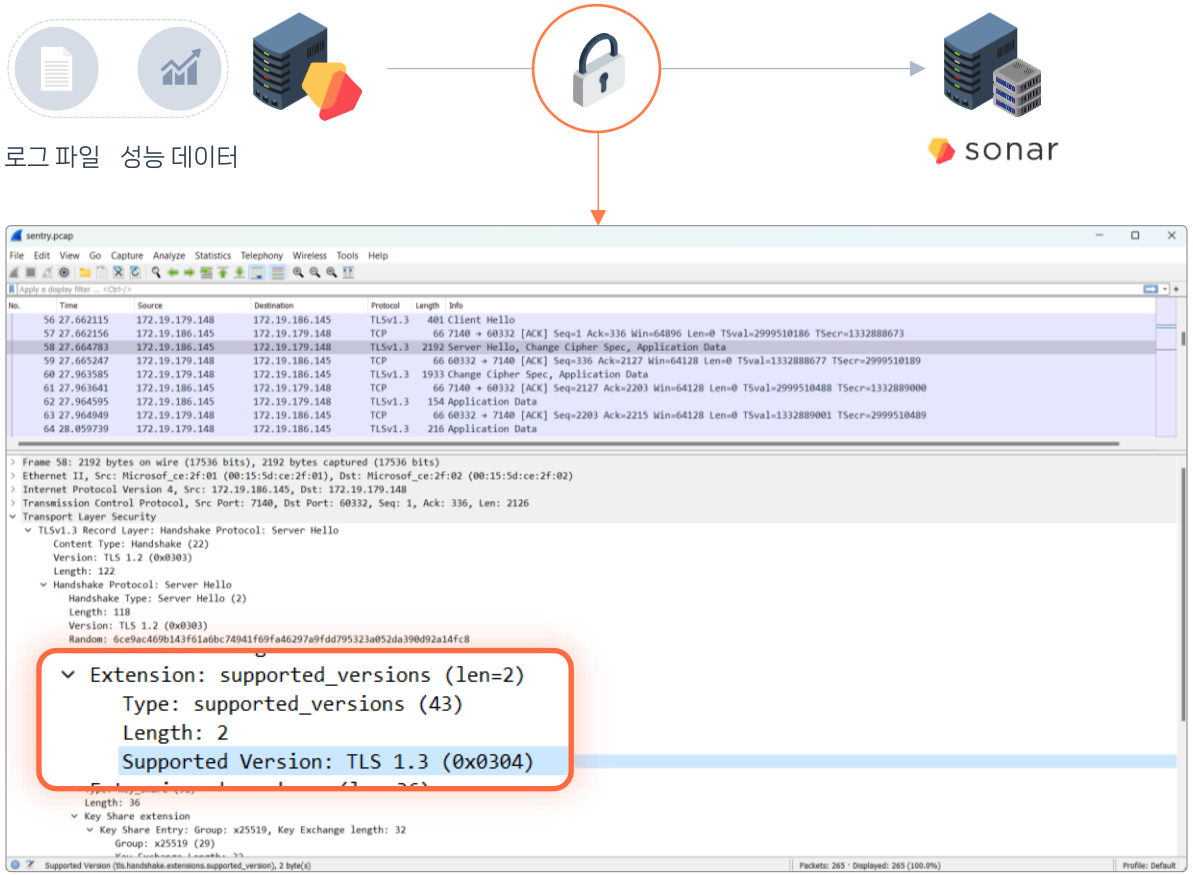


다양한 운영체제 지원

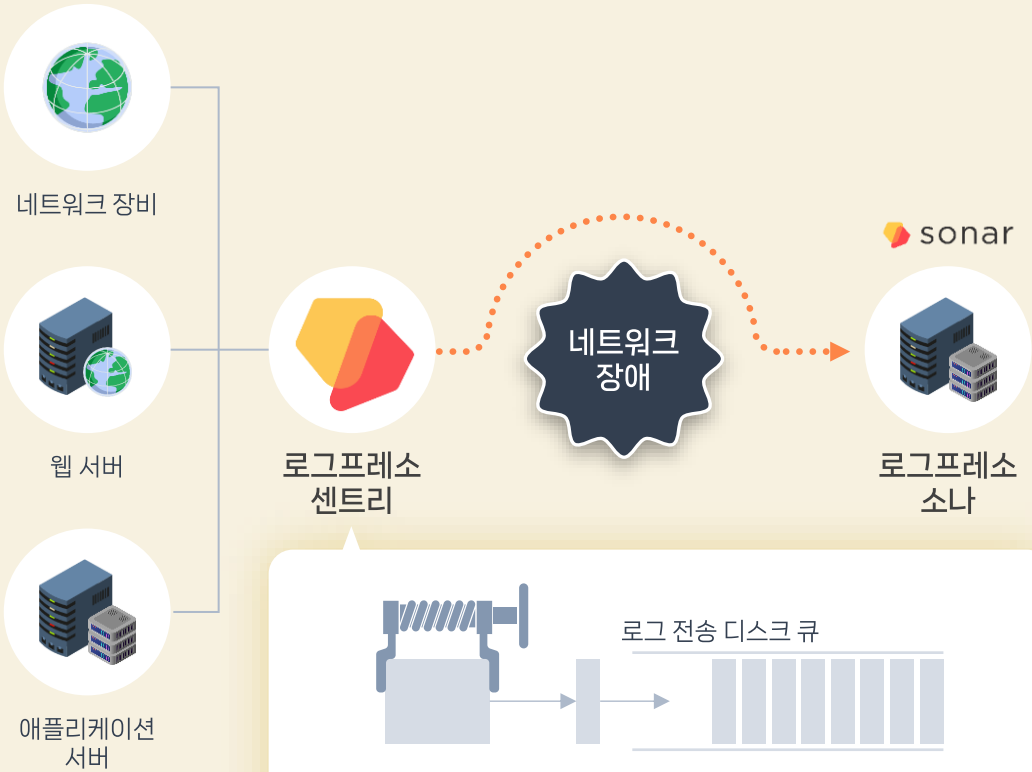
로그프레소 센트리는 수집된 로그를 유실 없이 안전하게 전송합니다.

TLS를 이용한 통신 암호화

로그프레소 센트리 | 로그프레소 소나

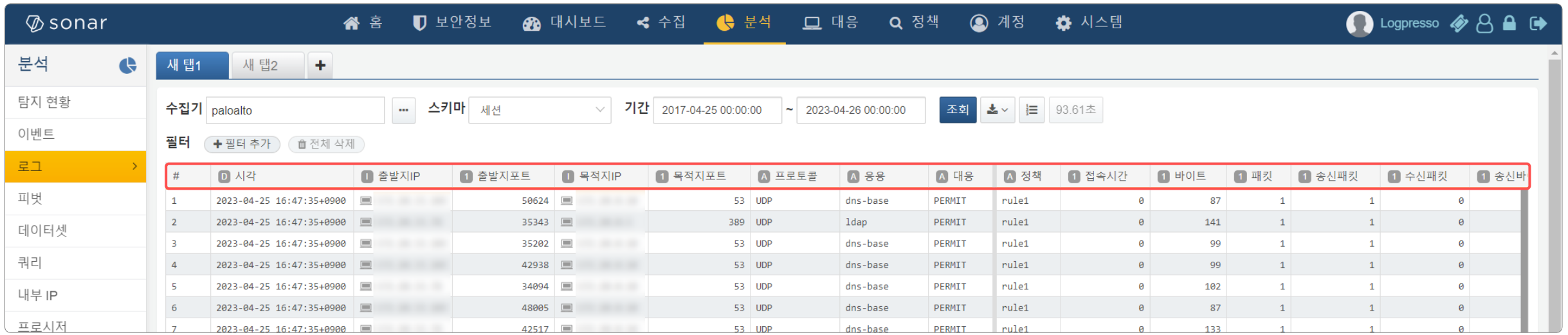


네트워크 장애 시 데이터 유실 대응



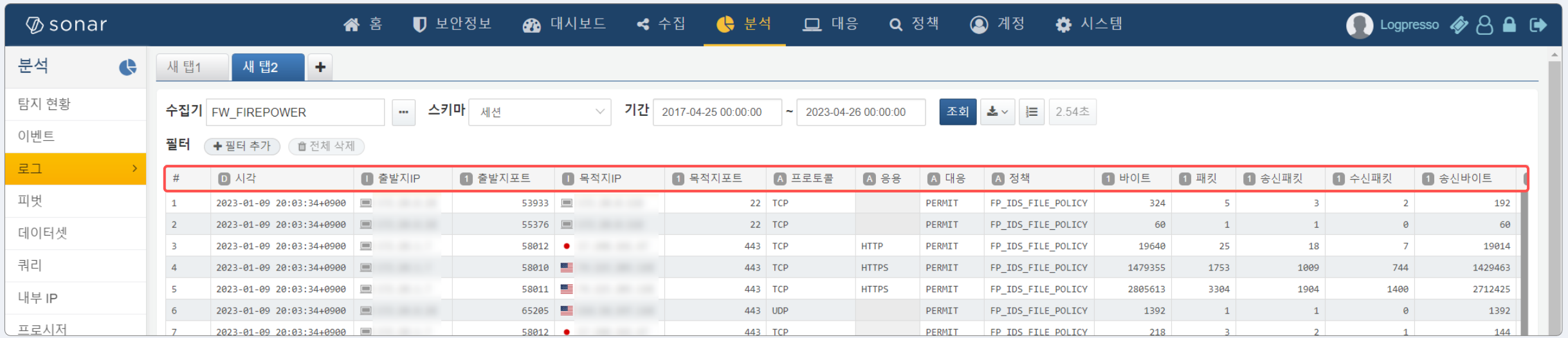
1. 네트워크 장애 복구 시점에 일괄 전송(큐 용량 조절 가능)
2. 데이터 압축으로 네트워크 부하 최소화

동일 유형 이기종 장비의 로그를 한글로 정규화하여 조회할 수 있으므로 일관된 검색이 가능합니다.



▲ 한글로 정규화된 팔로알토 방화벽 로그

한글로 정규화된 시스코 파이어파워 방화벽 로그 ▼



STEP 2

로그 저장

- 압축 및 암호화
- 위변조 방지

특허 기술로 **반드시 필요한 열 벡터만 복호화 및 압축 해제**하여 고속으로 분석합니다.

기존 기술

로그 분석에 필요하지 않은 컬럼까지 모두 포함하여
데이터 블록 전체를 I/O, 복호화, 압축 해제하므로 매우 느림

암호화/압축된 데이터 블록

시각=값, 출발지IP=값, 출발지포트=값, 목적지IP=값, 목적지포트=값, 프로토콜=값, 대응=값

시각=값, 출발지IP=값, 출발지포트=값, 목적지IP=값, 목적지포트=값, 프로토콜=값, 대응=값

시각=값, 출발지IP=값, 출발지포트=값, 목적지IP=값, 목적지포트=값, 프로토콜=값, 대응=값

모든 컬럼을 복호화/압축 해제

로그프레소 특허 기술

로그 분석에 사용할 컬럼만
선택적으로 I/O, 복호화, 압축 해제하므로 매우 빠름

암호화/압축된 데이터 블록

시각	출발지 IP	출발지 포트	목적지 IP	목적지 포트	프로토콜	대응

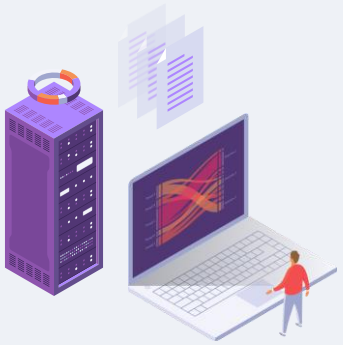
시각, 출발지IP 컬럼만 복호화/압축 해제

1TB 25억 건의 포티게이트 방화벽 로그의 압축 시험 결과

원본 대비

7.54%

압축율은 로그 파일 형식에 따라 상이할 수 있습니다.



ID	시험항목	시험목표 및 기준	결과	비고
TC3	데이터 압축률 측정	<시험목표> 데이터를 수집하고 저장할 때, 실제로 사용하는 저장공간을 확인하여 압축률 확인 <시험기준> o 기준: 약 1TB의 데이터를 저장할 때 실제 사용되는 저장공간을 확인하여 산출된 압축률의 평균 o 산정식: $X = \sum_{i=1}^{n} (A_i / B_i) / n \times 100$ - Ai: i번째 측정에서 테이블 데이터가 저장된 디렉토리의 크기 - Bi: i번째 측정에서 저장한 압축 전 시료 로그 파일 크기 - n: 측정 횟수 ※ TC3의 시험기준 및 시료는 시험의뢰기업에서 제공함	X = 7.54 (단위: %)	3회 반복수행 결과값 모두 동일

시험성적서

한국정보통신기술협회
소프트웨어시험인증연구소
주소: 경기도 성남시 분당구 분당로 47
전화: 031-780-9362, Fax: 031-724-0189

성적서번호: BT-A-21-0241

1. 의 뢰 자
· 회사(기관)명 : ㈜로그프레소
· 주 소 : 서울시 마포구 새창로 7, 16층 1601호(도화동, 서울대학교 총동창회 장학빌딩)
· 계약일자 : 2021년 10월 15일

2. 시험성적서의 용도 : 과제 산출물 검증용

3. 제 품 명 : 로그프레소

4. 버 전 : v4.0

5. 시험장소 : ☑ 고정시험실, ☐ 현장시험
· 시험수행주소 : 경기도 성남시 분당구 분당로 47

6. 시험기간 : 2021. 11. 22. ~ 2021. 11. 30.

7. 시험방법 : ISO/IEC 25023:2016의 1개 항목 적용
- 상세 내용은 "<3.시험항목 및 방법>" 참고

8. 시험환경 : 실온, 실습

9. 시험결과 : BT-A-21-0241-GR 참조

비 고 : 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하며 용도 이외의 사용을 금합니다.
2. 이 성적서는 KS Q ISO/IEC 17025 및 KOLAS 인정 분야와 관련 없습니다.
3. 이 성적서의 진위여부는 기업지원플러스(www.g4b.go.kr)에서 진위확인코드로 확인 가능합니다.

확 인	작성자 성 명 : 임 새 샘 (서명)	승인자 직 책 : 기 술 책 임 자 성 명 : 한 정 훈 (서명)

2021년 11월 30일

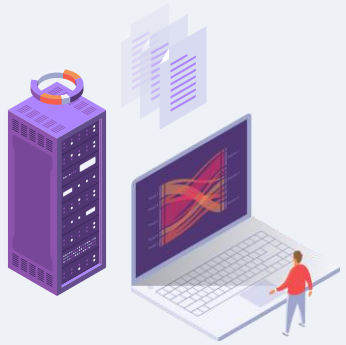
한국정보통신기술협회 회장 (인)

TPS-0071-3(01)

1TB 25억 건의 포티게이트 방화벽 로그에서 IP 주소 검색 시험 결과

평균 검색 속도

0.01s



ID	시험항목	시험목표 및 기준	결과	비고
TC5	데이터 검색 속도 측정1	<시험목표> 데이터를 수집하고 인덱싱 후 저장한 상태에서, IP "37.220.35.143"을 검색했을 때 검색에 소요되는 시간을 확인 <시험기준> o 기준: ISO/IEC 25023:2016 – 8.3.1 Time behaviour measures (PTb-3-G: Mean turnaround time) o 산정식: $X = \sum_{i=1}^{n} (B_i - A_i)/n$ – Ai: 작업 i의 시작 시간 – Bi: 작업 i의 완료 시간 – n: 측정 횟수 ※ 기준: 수집된 2,487,068,366건의 데이터 중 특정 IP를 검색하는 쿼리 수행 시간의 평균 ※ TC5의 시료는 시험의뢰기업에서 제공함	X = 9.8 (단위: ms)	최대: 11 ms 최소: 9 ms 검색결과 건수: 34 건

시험성적서

한국정보통신기술협회
소프트웨어시험인증연구소
주소: 경기도 성남시 분당구 분당로 47
전화: 031-780-9362, Fax: 031-724-0189

성적서번호: BT-A-21-0241

1. 의 뢰 자
· 회사(기관)명 : ㈜로그프레소
· 주 소 : 서울시 마포구 새창로 7, 16층 1601호(도화동, 서울대학교 총동창회 장학빌딩)
· 계약일자 : 2021년 10월 15일

2. 시험성적서의 용도 : 과제 산출물 검증용

3. 제 품 명 : 로그프레소

4. 버 전 : v4.0

5. 시험장소 : ☑ 고정시험실, ☐ 현장시험
· 시험수행주소 : 경기도 성남시 분당구 분당로 47

6. 시험기간 : 2021. 11. 22. ~ 2021. 11. 30.

7. 시험방법 : ISO/IEC 25023:2016의 1개 항목 적용
– 상세 내용은 "<3.시험항목 및 방법>" 참고

8. 시험환경 : 실온, 실습

9. 시험결과 : BT-A-21-0241-GR 참조

비 고 : 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하며 용도 이외의 사용을 금합니다.
2. 이 성적서는 KS Q ISO/IEC 17025 및 KOLAS 인정 분야와 관련 없습니다.
3. 이 성적서의 진위여부는 기업지원플러스(www.g4b.go.kr)에서 진위확인코드로 확인 가능합니다.

확 인	작성자 성 명 : 임 새 샘 (서명)	승인자 직 책 : 기 술 책 임 자 성 명 : 한 정 훈 (서명)

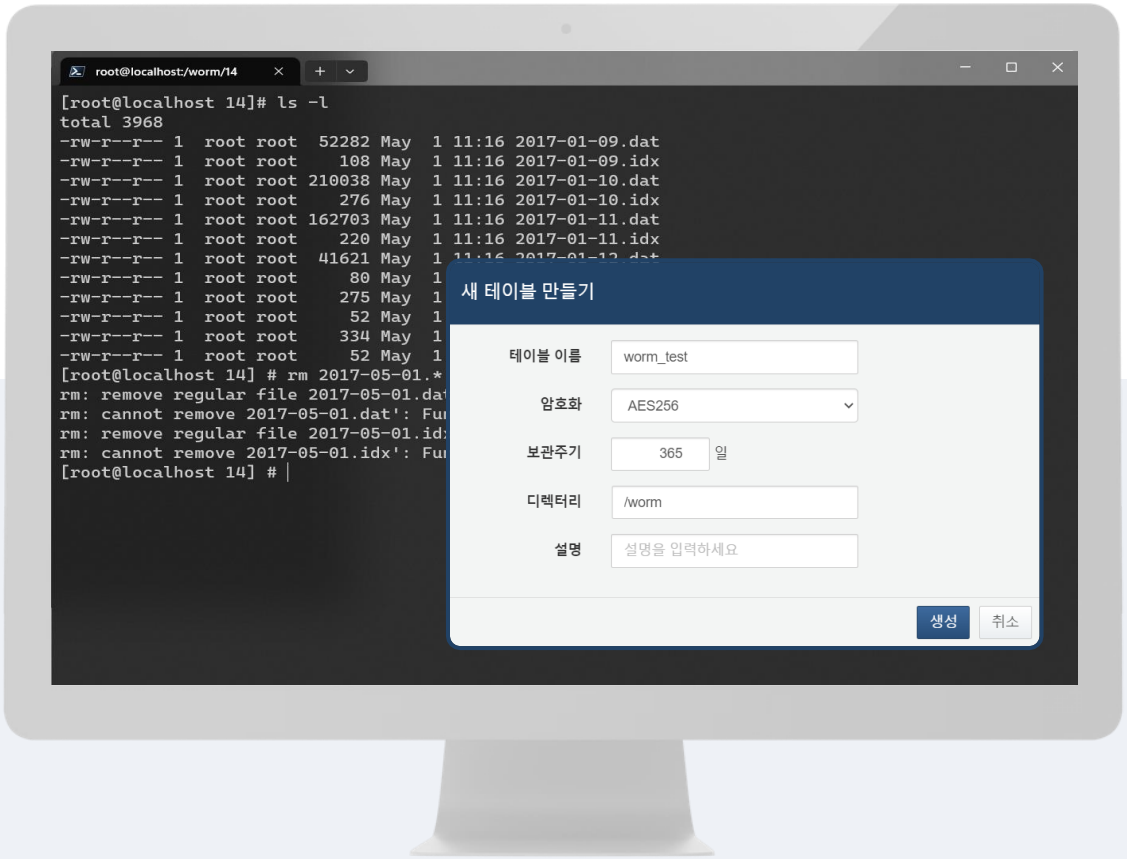
2021년 11월 30일

한국정보통신기술협회 회장 (인)

TPS-0071-3(01)

위변조 방지

리눅스 WORM 파일시스템 드라이버를 제공하여 시스템 관리자 권한으로도 파일 삭제나 위변조가 불가능하도록 지원합니다.



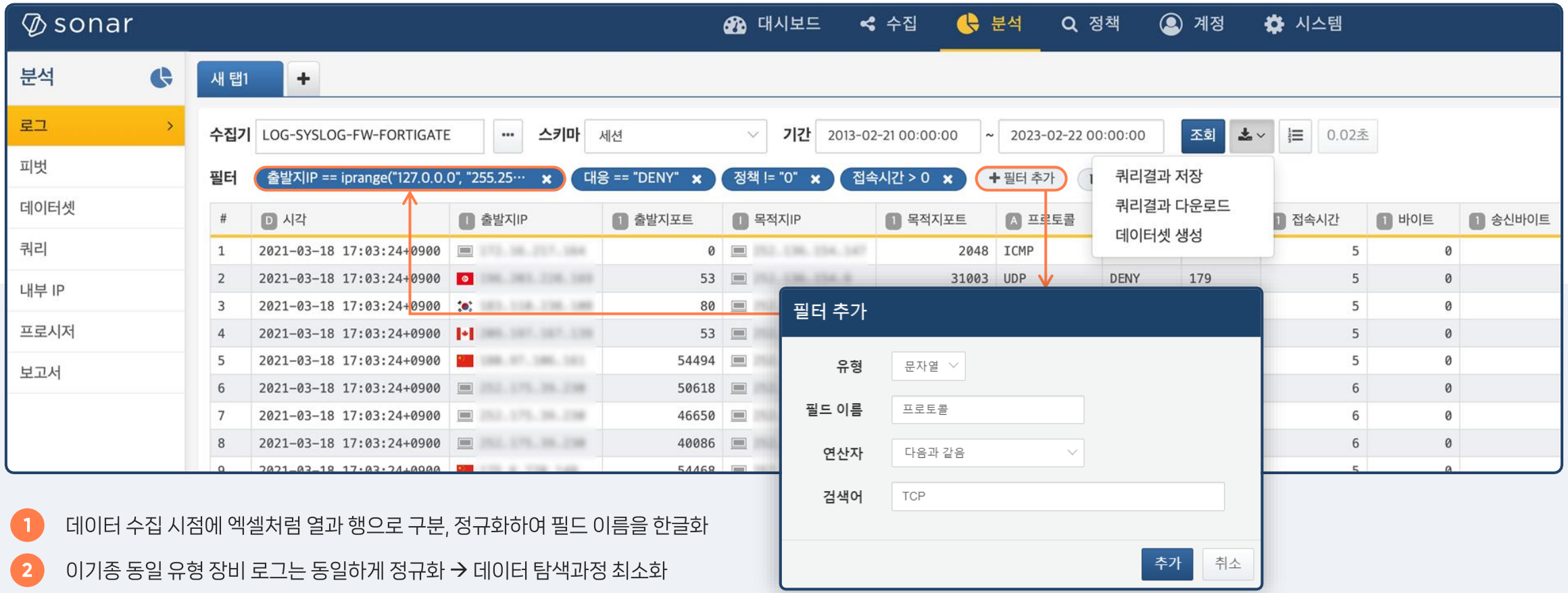
STEP 3

로그 분석

- 풀텍스트 검색
- 연관 분석
- 피벗 분석
- 머신러닝
- 대시보드
- 쿼리
- 보고서

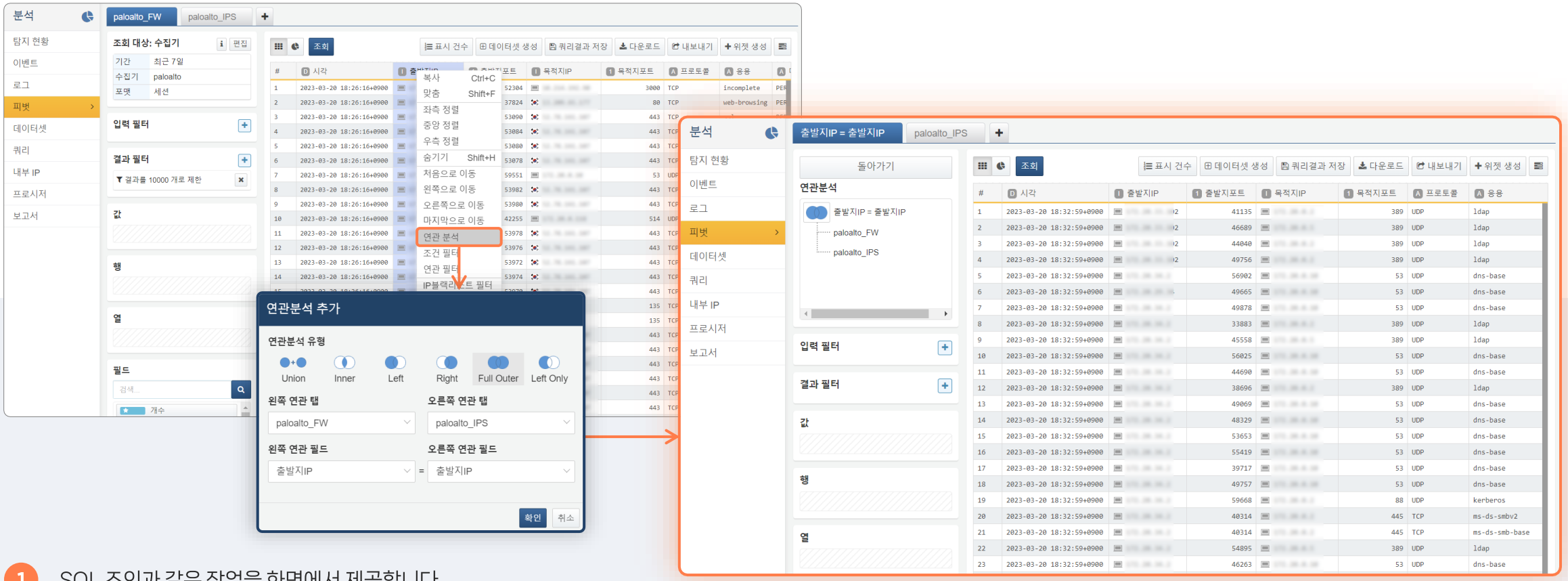
풀텍스트 검색

마우스 클릭만으로 수백 GB의 로그를 1초 이내에 드릴다운 검색하여, **장기간의 해킹 시도 이력이나 서비스 장애 원인을 확인**합니다.



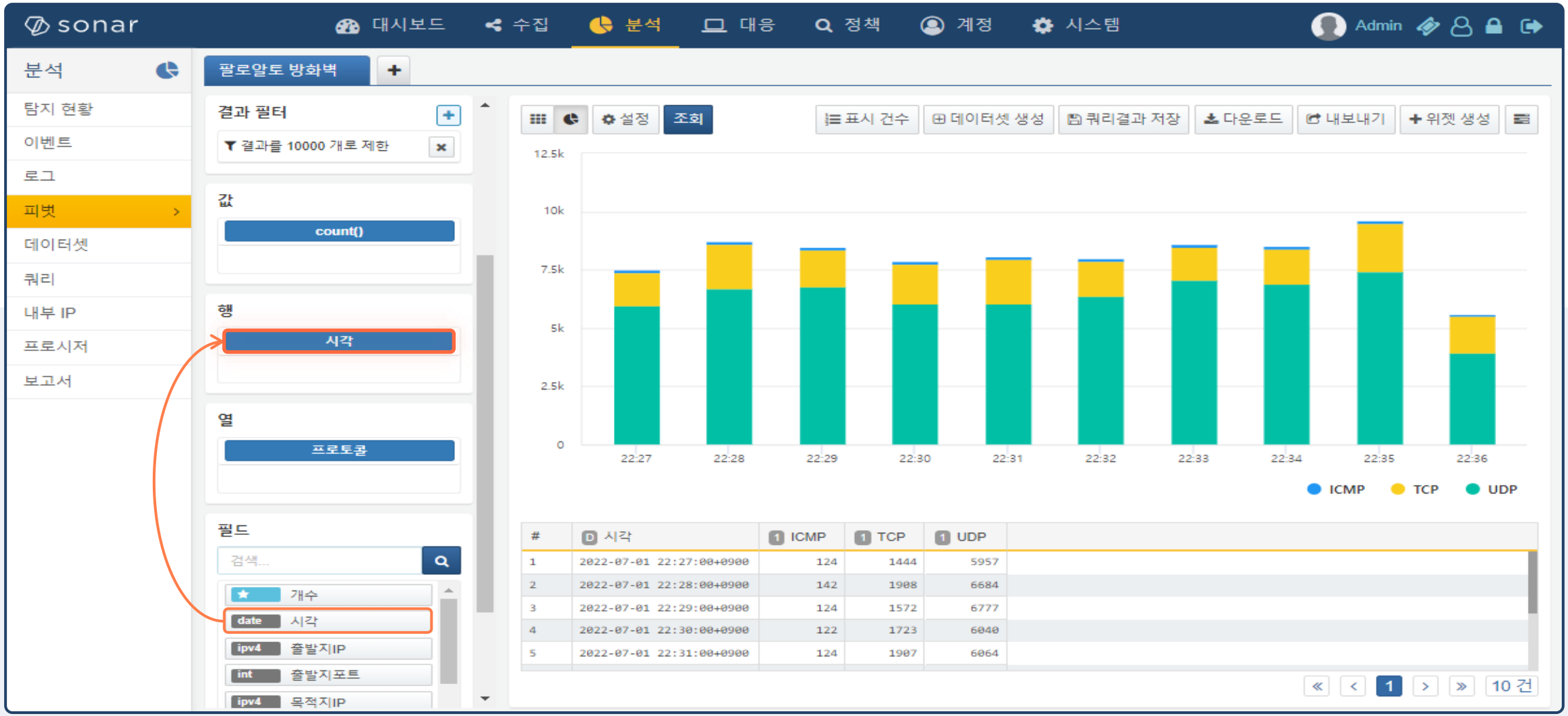
1. 데이터 수집 시점에 엑셀처럼 열과 행으로 구분, 정규화하여 필드 이름을 한글화
2. 이기종 동일 유형 장비 로그는 동일하게 정규화 → 데이터 탐색과정 최소화
3. 한글화된 이름으로 여러 개의 검색 조건을 추가 가능
4. 검색 결과 저장, PC로 다운로드(엑셀, 워드 등), 데이터셋 생성 방식으로 활용 가능

여러 로그를 종합해 **연관 분석**을 하는 작업도 명령어를 익힐 필요 없이 **직관적으로 수행**할 수 있습니다.

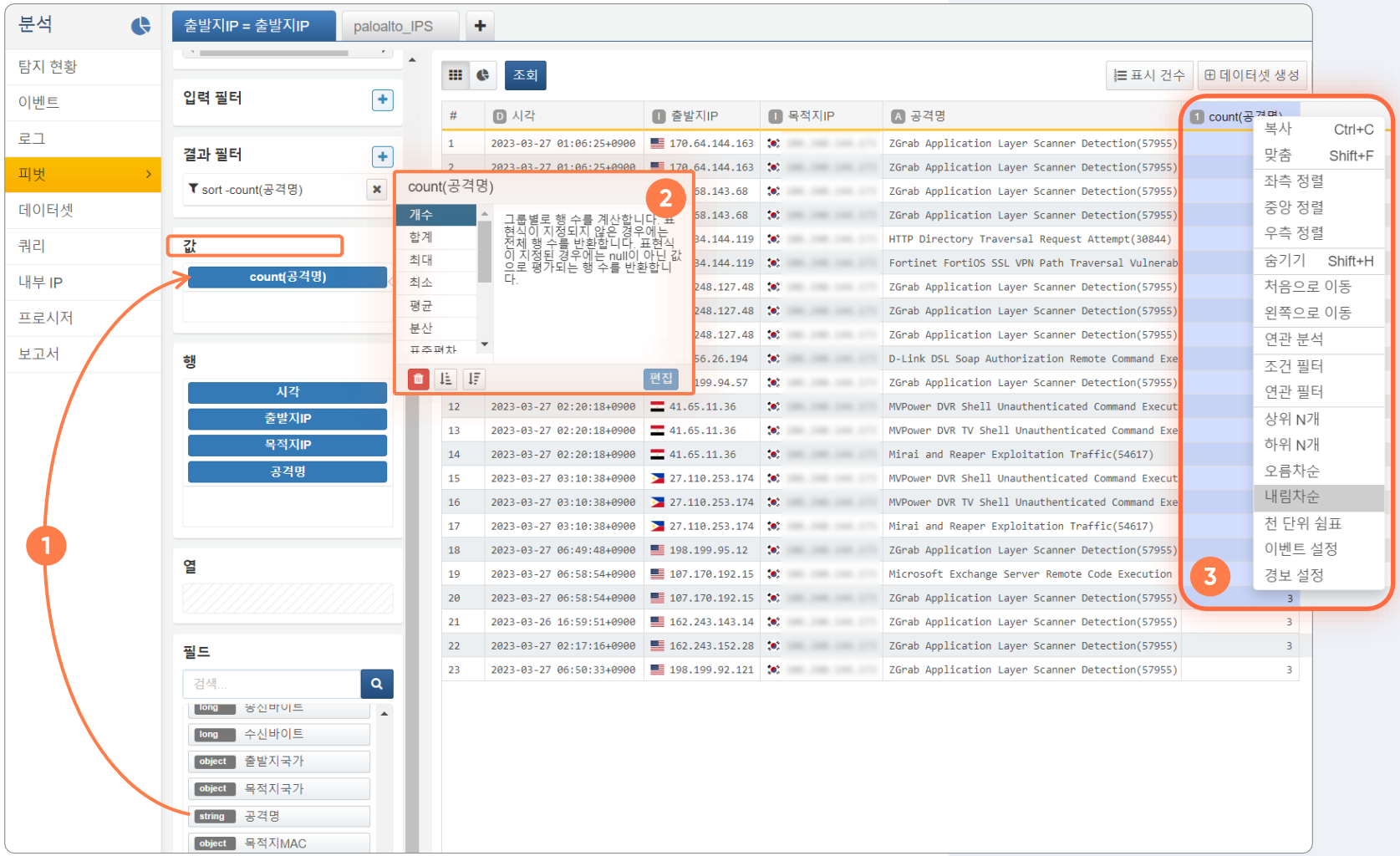


1. SQL 조인과 같은 작업을 화면에서 제공합니다.
2. 서로 다른 형식의 로그를 원본 훼손 없이 분석 시점에 정규화하여 비교할 수 있습니다.
3. 패턴 탐지, 개인정보조회 오남용 탐지, 행위 프로파일링 분석, 시계열 분석, 이상징후 탐지 등에 응용할 수 있습니다.

엑셀을 사용하듯 **드래그 & 드롭**으로 원하는 **모니터링 지표와 차트를 즉시 생성**할 수 있습니다.



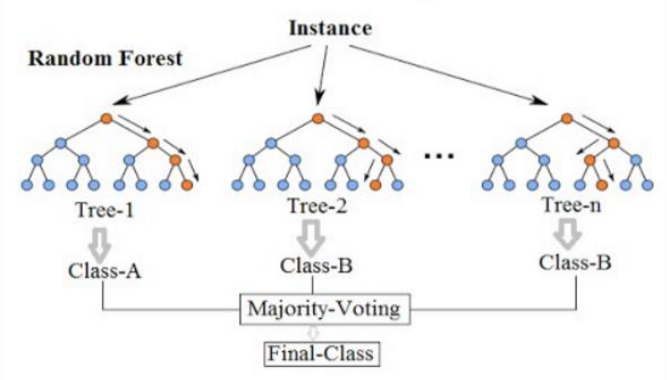
테이블을 구성할 필드를 드래그 & 드롭해서 손쉽게 피벗할 수 있습니다.



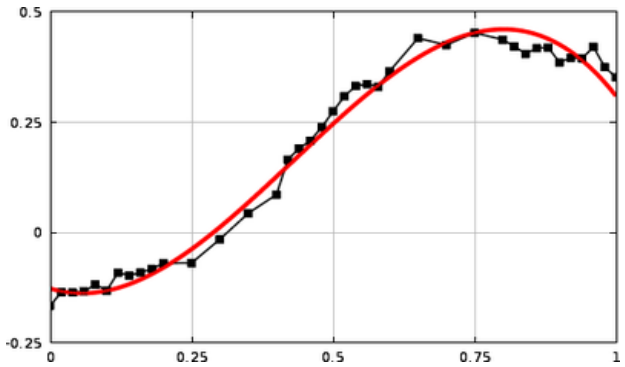
1. 피벗할 필드를 끌어서 원하는 행/열/값에 놓으세요.
2. 조회할 값을 변경할 수 있습니다.
3. 필드나 값을 선택해 필터를 만들거나, 정렬할 수 있습니다.

자체 기술로 인-데이터베이스 머신러닝 모델과 알고리즘을 구현하여 내장하고 있으며, 쿼리에서 호출하여 사용할 수 있습니다.

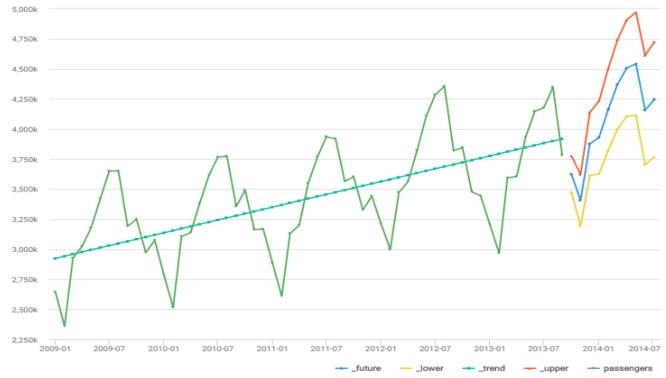
Random Forest Model (rforest 명령)



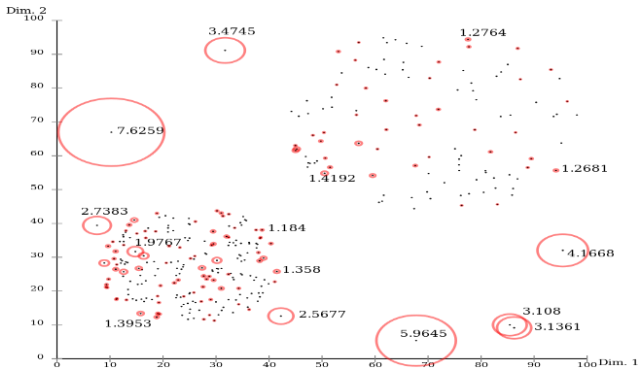
Linear Regression Model (curvefit 명령)



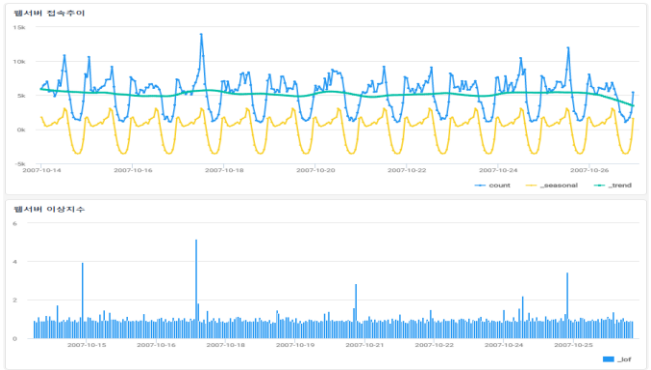
Forecast Model (forecast 명령)



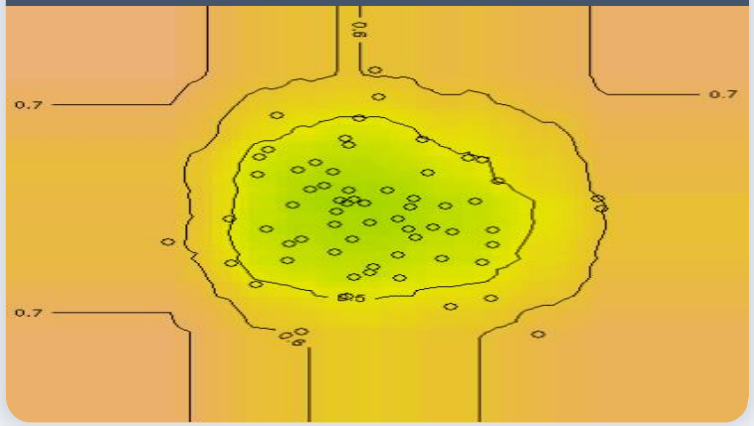
Local Outlier Factor (lof 명령)



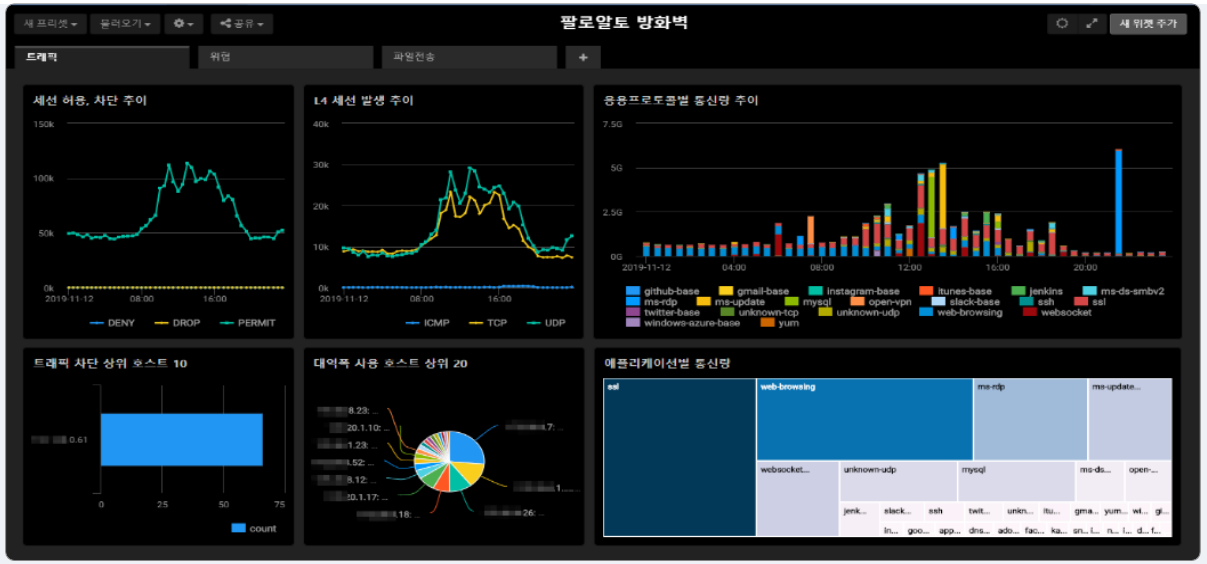
Seasonal-Trend Decomposition (stl 명령)

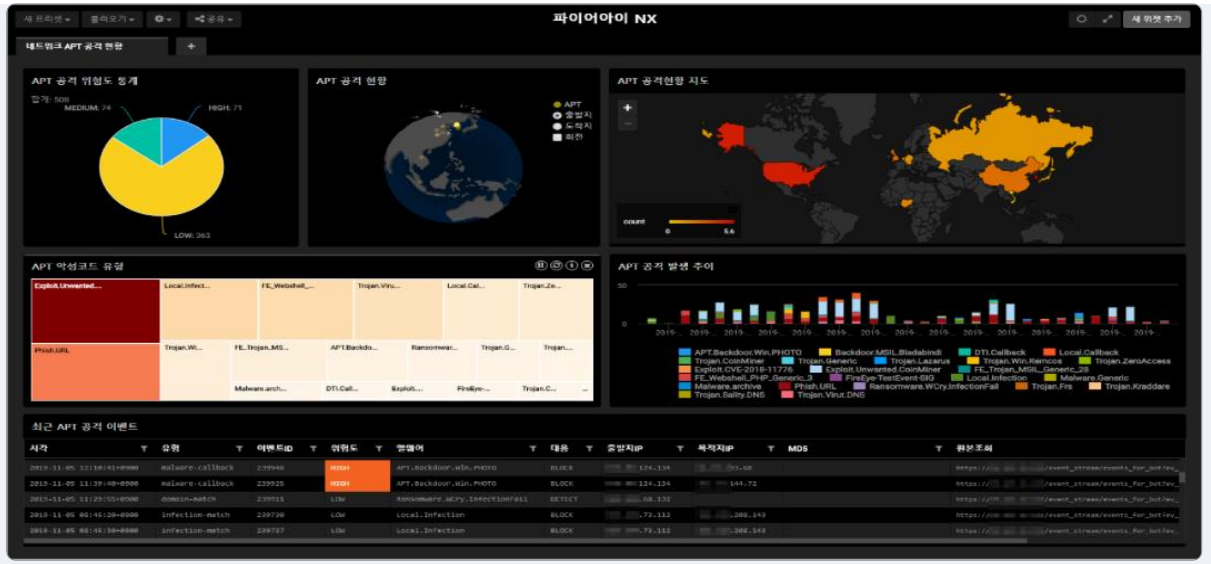


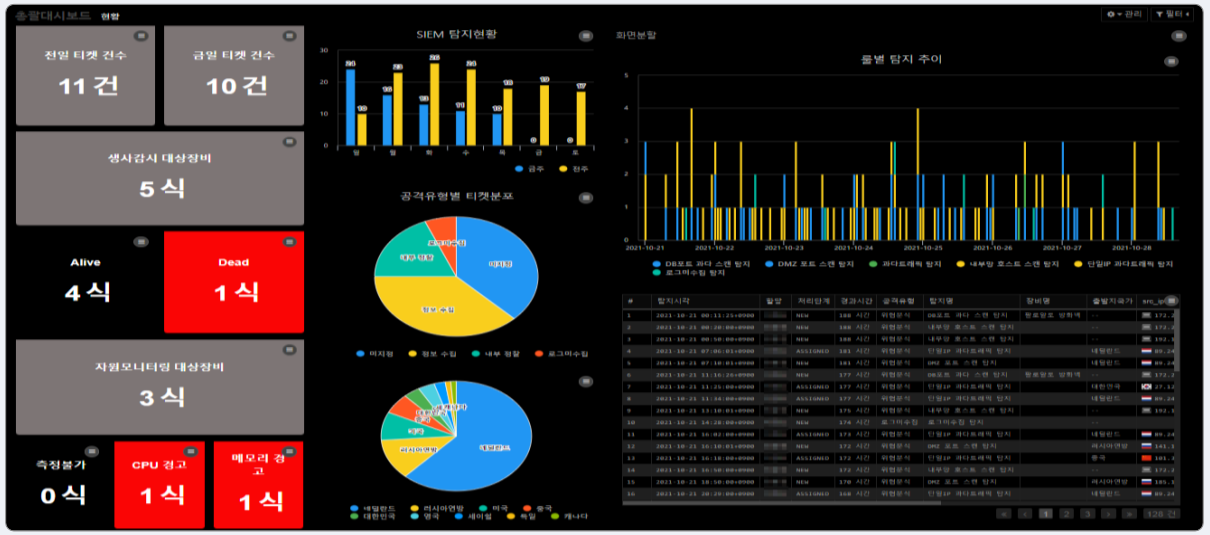
Isolation Forest Model (anomalies 명령)



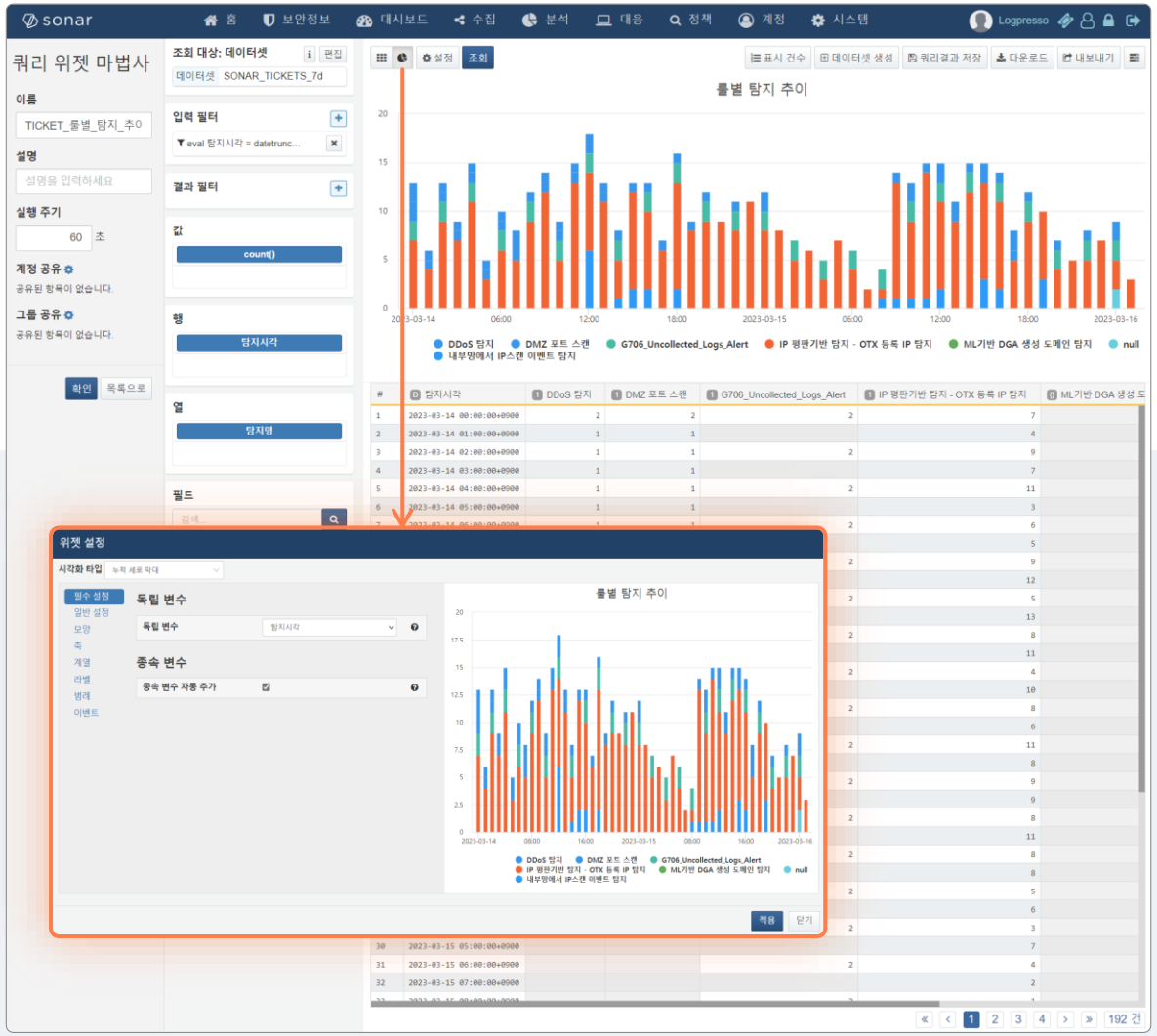
디스플레이 전력 소모를 최소화하고 **가시성을 극대화하는 다크 모드 대시보드**를 제공합니다.

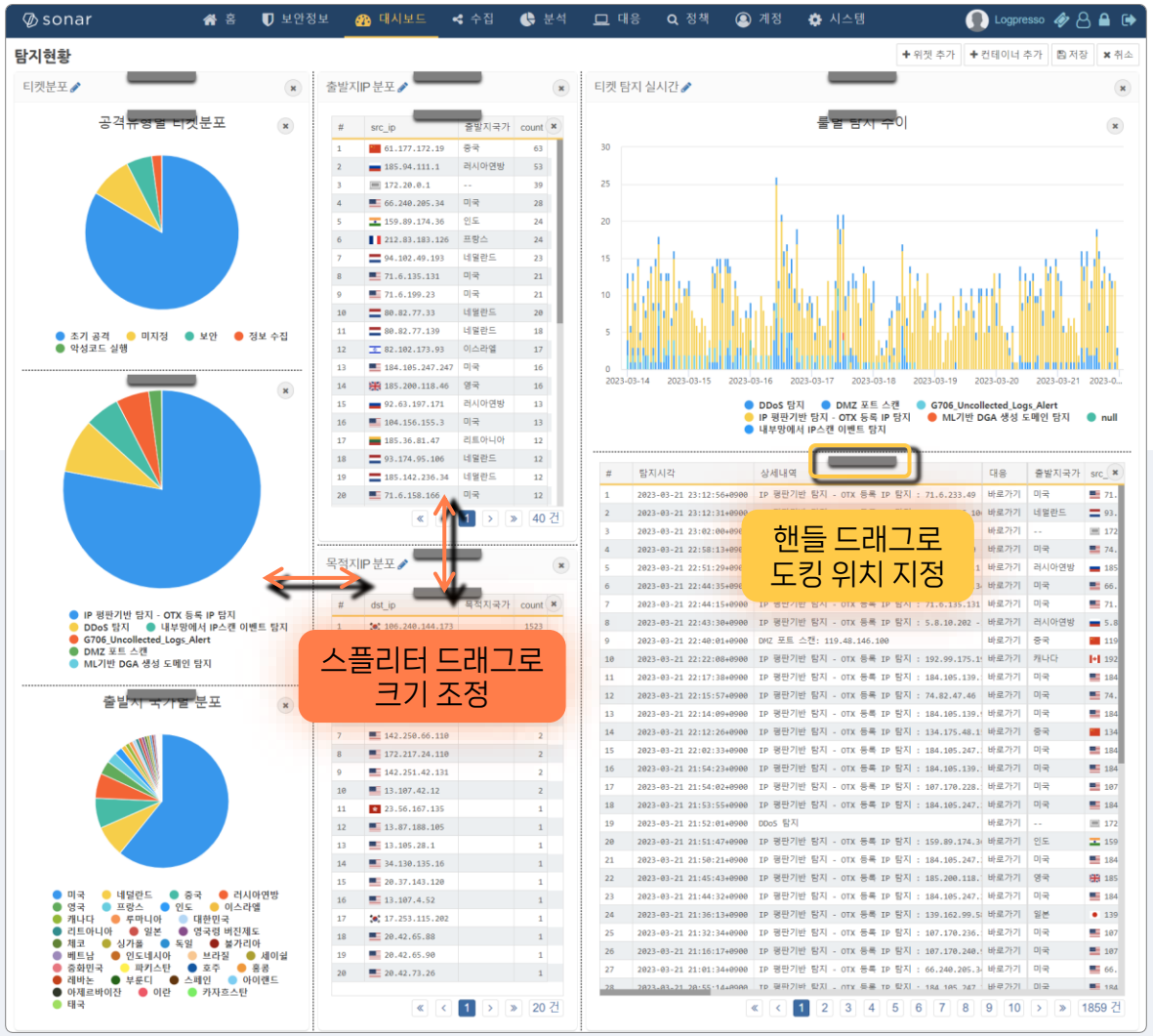






사용자가 원하는대로 대시보드 위젯을 만들고 마우스로 그래그 & 드롭으로 배치하여,
다양한 지표를 **실시간으로 모니터링 및 드릴다운** 분석할 수 있습니다.



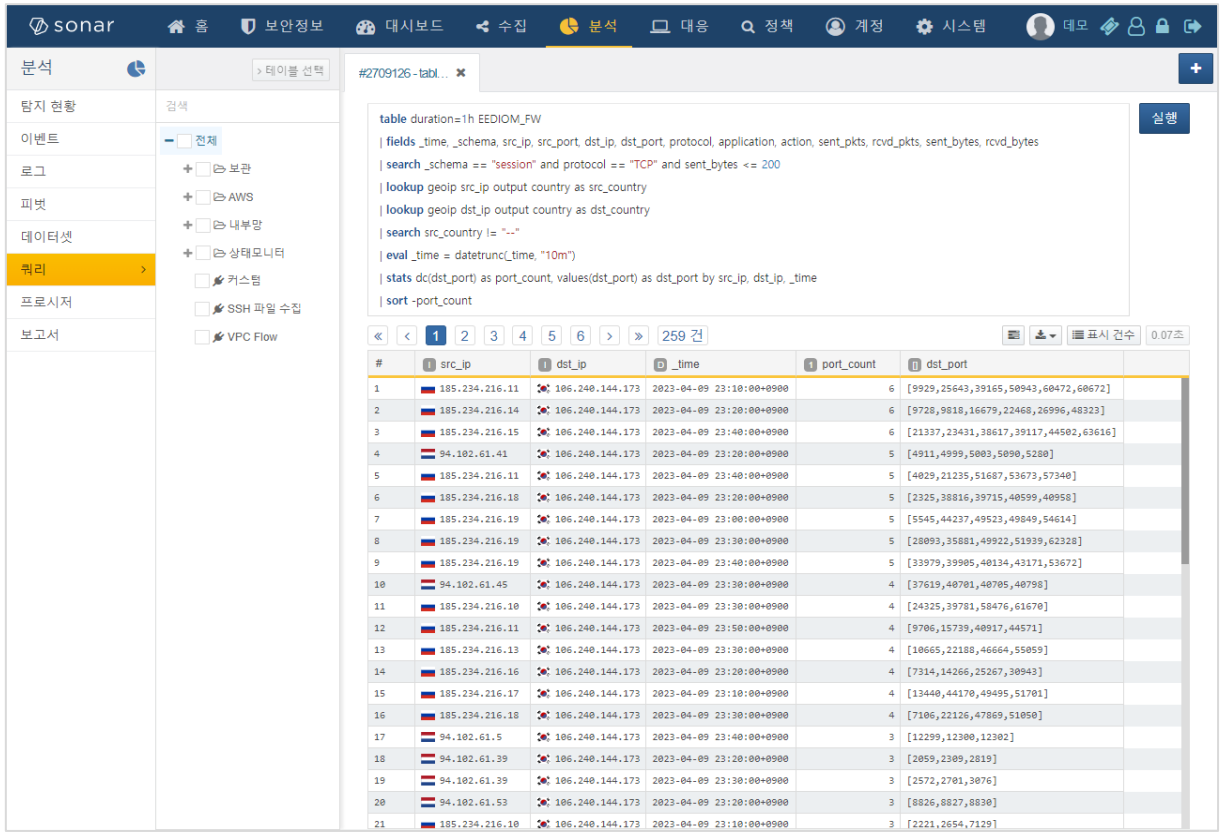


300종 이상의 쿼리 명령어와 함수를 통해 복잡한 비정형 데이터 분석도 손쉽게 처리합니다.

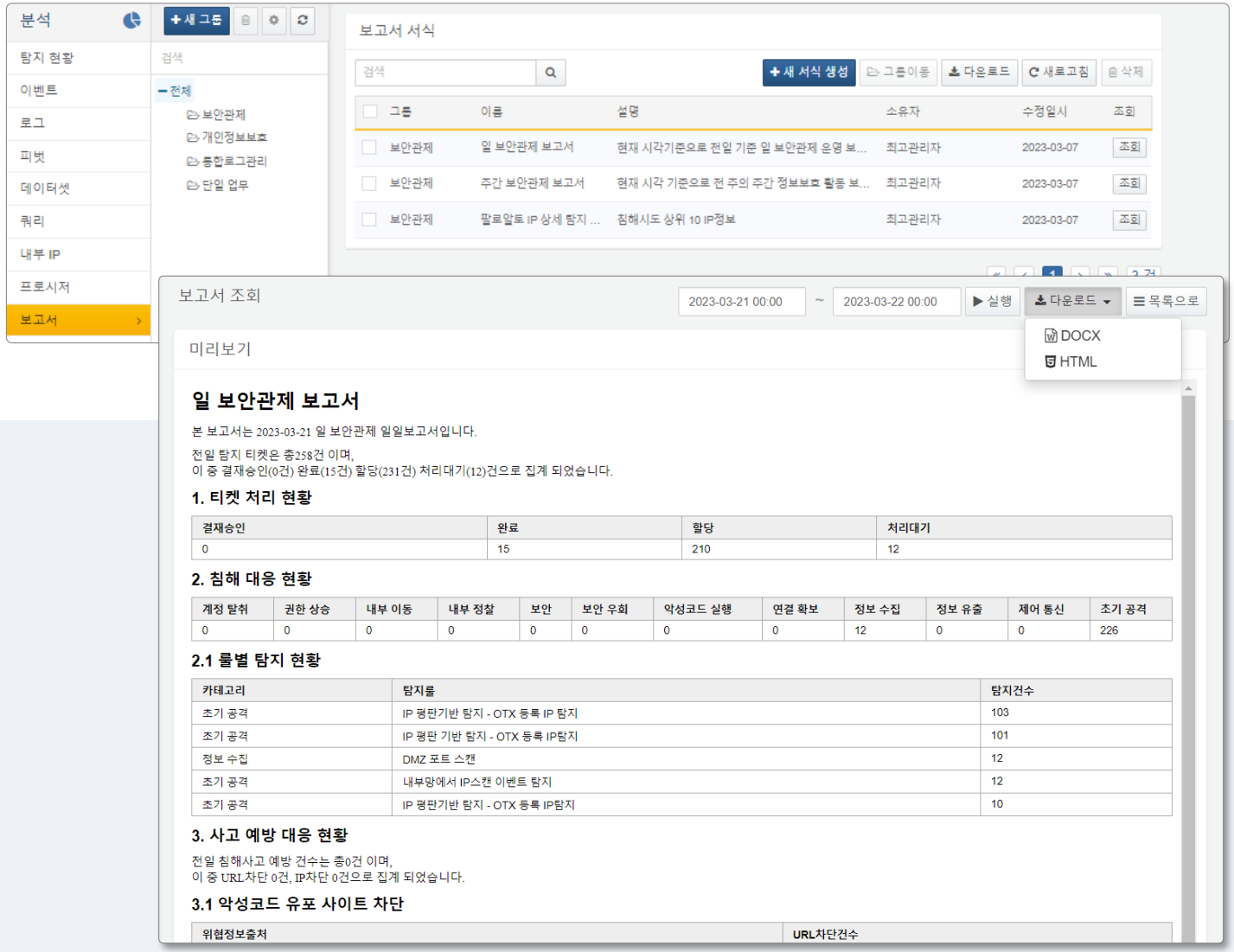
https://docs.logpresso.com에서 모든 기능을 확인할 수 있습니다.

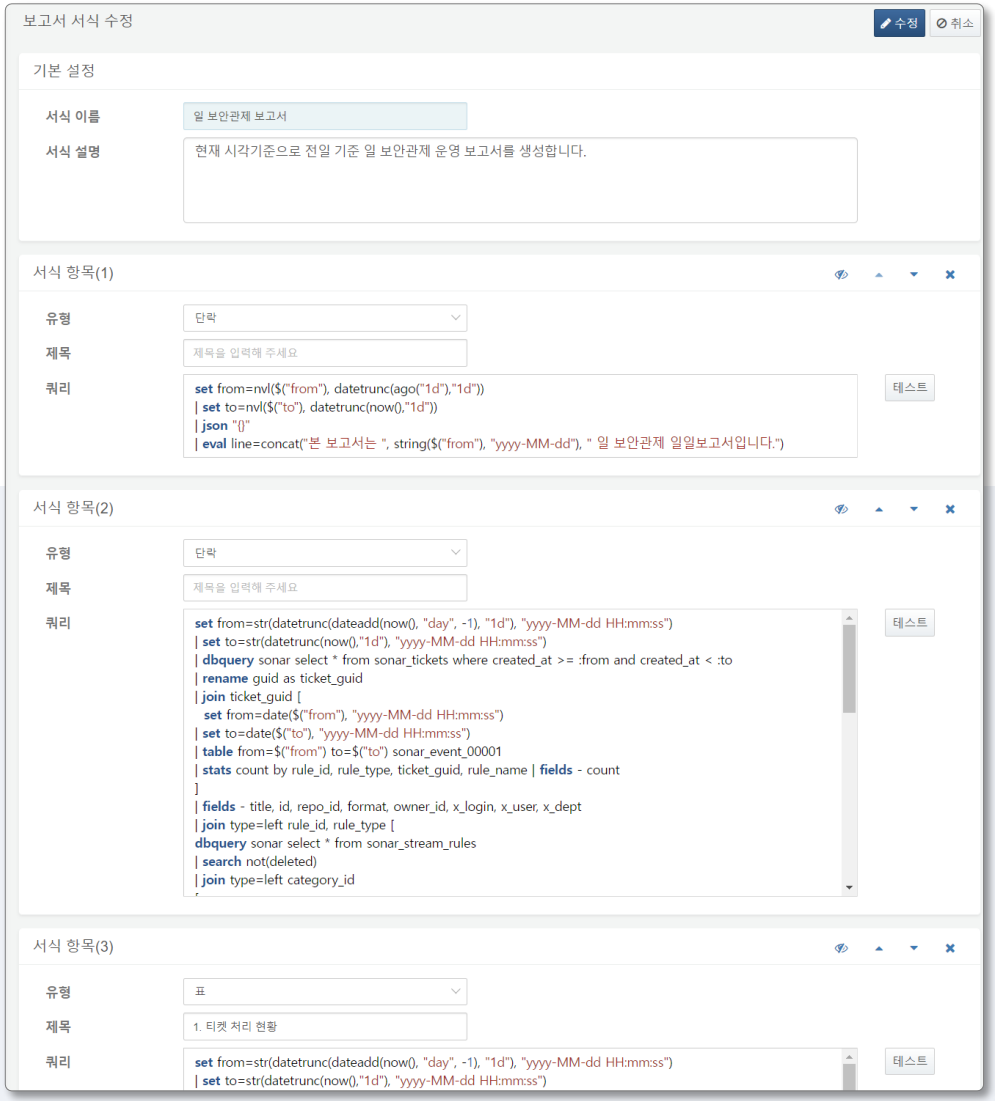
쿼리 매뉴얼 웹 사이트

명령어 자동 완성 및 문법 하이라이트 지원



서식 기능을 사용하여 **원하는 내용의 보고서를 정의하고, 생성된 보고서를 다운로드**할 수 있습니다.





로그프레소가 보유한 **빅데이터 원천기술**을 기반으로 로그 수집, 저장, 분석, 파기의 **전체 과정을 관리**합니다.

클라우드 로그

aws, NAVER CLOUD PLATFORM

에이전트(센트리)

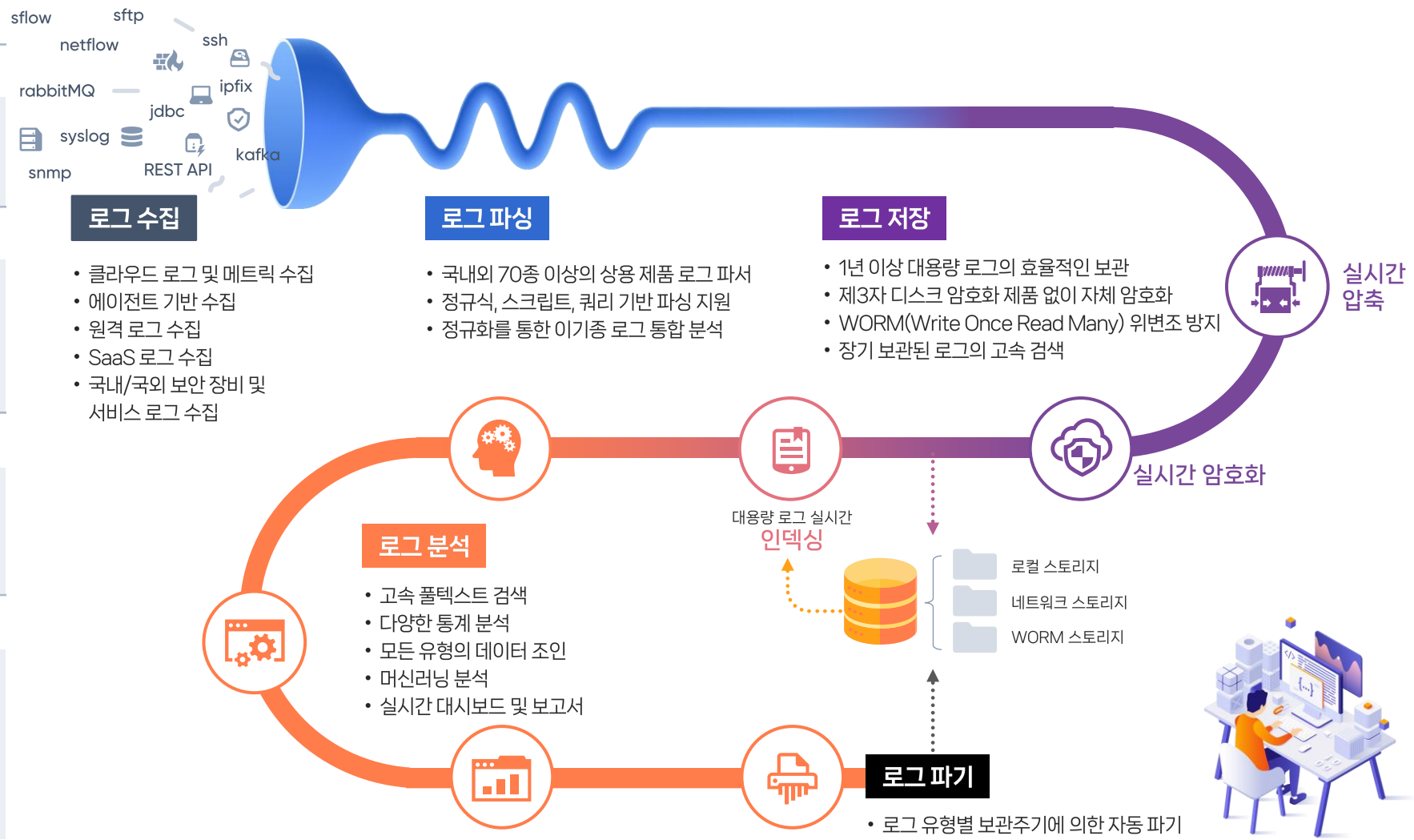
AIX, hp UX, ORACLE Solaris, Windows

SaaS

Google Workspace, GitHub, Microsoft 365

보안 장비/서비스

AhnLab, RAPIDT, RSA



운영 환경

하드웨어 사양은 **원본 로그 1년 보관을 기준으로 하여 다음과 같이 산정**합니다.

타사에 비해 동일 조건에서 적은 수량의 하드웨어를 사용하므로 관리 포인트가 감소하고 총 소유 비용(TCO)을 절감할 수 있습니다.

구분		10GB/일	50GB/일	100GB/일	200GB/일	500GB/일	1TB/일
분석 서버	CPU	인텔 제온 2.6GHz 4core x 2EA	인텔 제온 2.6GHz 8core x 2EA	인텔 제온 2.6GHz 8core x 2EA	인텔 제온 3.0GHz 8core x 2EA	인텔 제온 3.0GHz 8core x 2EA	인텔 제온 3.2GHz 8core x 2EA
	메모리	64GB	128GB	256GB	512GB	256GB	256GB
	디스크	OS: SSD 480GBx2EA DATA: HDD 4TBx2EA (가용 4TB)	OS: SSD 480GBx2EA DATA: HDD 4TBx4EA (가용 12TB)	OS: SSD 480GBx2EA DATA: HDD 8TBx4EA (가용 24TB)	OS: SSD 480GBx2EA DATA: HDD 12TBx4EA (가용 36TB)	OS: SSD 480GBx2EA DATA: HDD 4TBx2EA (가용 4TB)	OS: SSD 480GBx2EA DATA: HDD 4TBx2EA (가용 4TB)
	NIC	1Gbps Dual	1Gbps Dual	1Gbps Dual	1Gbps Dual	10Gbps Dual	10Gbps Dual
수집 서버	CPU	N/A	N/A	N/A	N/A	인텔 제온 3.0GHz 8core x 2EA	인텔 제온 3.2GHz 8core x 2EA
	메모리					512GB	512GB
	디스크					OS: SSD 480GBx2EA DATA: HDD 12TBx5EA (가용 48TB)	OS: SSD 480GBx2EA DATA: HDD 12TBx5EA (가용 48TB)
	NIC					10Gbps Dual	10Gbps Dual
운영체제		RHEL 9+ / Rocky Linux 9+					
비고		분석/수집 일체형 (이중화 시 2대)	분석/수집 일체형 (이중화 시 2대)	분석/수집 일체형 (이중화 시 2대)	분석/수집 일체형 (이중화 시 2대)	분석서버 1대 수집서버 2대 (이중화 시 총 6대)	분석서버 1대 수집서버 4대 (이중화 시 총 10대)

구축 사례

200개 이상의 고객사에서
통합로그분석 (LMS), 통합보안관제 (SIEM), 보안운영자동화 (SOAR)에 활용하고 있습니다.

구축 사례

200개 이상의 고객사에서
통합로그분석 (LMS), 통합보안관제 (SIEM), 보안운영자동화 (SOAR)에 활용하고 있습니다.

금융	KB 국민은행	KB 금융그룹	KB 캐피탈	KDB산업은행	신한은행	제주은행
우리은행	BNK 부산은행	BNK 경남은행	DGB대구은행	JT 저축은행	신 협	저축은행중앙회
NICE신용평가	NICE Payments	KSNET	Smartro	보험연수원 KOREA INSURANCE INSTITUTE	Your Best Credit Partner SGI서울보증	Ksure 한국무역보험공사
SAMSUNG 삼성선물	삼성생명서비스	MG손해보험	NH농협생명	NH농협손해보험	NH투자증권	고려신용정보
Prudential	Rich&Co.	HUG 주택도시보증공사	(주)에이티엠플러스	HYOSUNG FMS	로카모빌리티	핀크
KIWOOMCAPITAL	키움증권	MIRAE ASSET 미래에셋자산운용	MIRAE ASSET 미래에셋증권	하나금융투자	하나카드	KYOBO 교보증권
Daishin 증권	eBEST 이베스트투자증권	KIBO 기술보증기금	손해보험협회	은행연합회		

구축 사례

200개 이상의 고객사에서
통합로그분석 (LMS), 통합보안관제 (SIEM), 보안운영자동화 (SOAR)에 활용하고 있습니다.

제조/건설	SAMSUNG	LG화학	LS전선	DSME 대우조선해양(주)	SK hynix	현대건설
현대중공업	HYUNDAI Rotem	HYOSUNG TNC	kyungshin Holdings	SEBANG Global Moving Network	BMW Korea	
IT	SAMSUNG SDS	롯데정보통신	SK 플래닛	HYOSUNG TNS	kakaoenterprise	GS 네오텍
BNK 시스템	Smilegate Holdings	11번가	여기어때컴퍼니	HANDYSOFT	DAON	한국전자인증
방송	jtbc	KBS	의료/제약	강남세브란스병원 GANGNAM SEVERANCE HOSPITAL	가톨릭대학교 인천성모병원	인하대병원
중앙대학교병원 CHUNG-ANG UNIVERSITY HOSPITAL	JW 중외제약	교육	전남대학교 CHONNAM NATIONAL UNIVERSITY	제주한라대학교	청운대학교 CHUNGWOON UNIVERSITY	한국복지대학교 KOREA NATIONAL UNIVERSITY OF WELFARE
한국폴리텍대학	한양대학교 HANYANG UNIVERSITY	협회/단체	대한상공회의소	삼성꿈장학재단 Samsung Dream Scholarship Foundation	한국교육과정평가원 Korea Institute for Curriculum and Evaluation	The-K 한국교직원공제회 THE KOREAN TEACHERS' CREDIT UNION

Thank You

감사합니다

서울특별시 마포구 새창로 7 SNU장학빌딩 9층 (도화동 565)
02-6730-7249 contact@logpresso.com

LOGPRESSO