Plura

Excellent Cyber Security Partner

통합 로그 관리

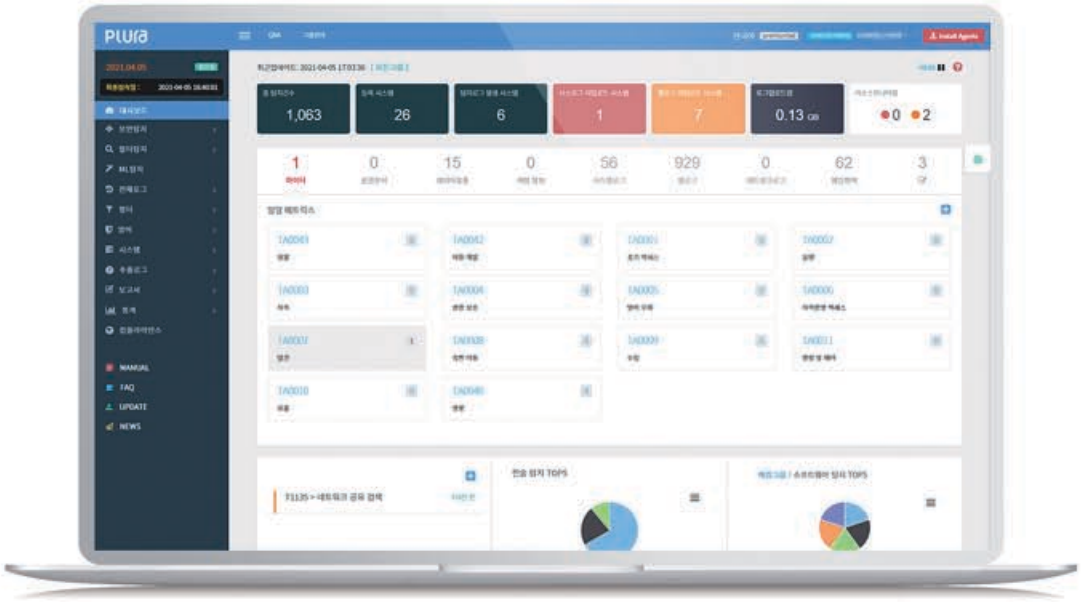
조달청, 혁신제품 지정 인증
(2020-258)

www.plura.io

QUBITSECURITY

통합 로그 관리 시스템

"프루라는 실질적인 이상 행위를 탐지하는 차세대 통합 로그 관리 시스템입니다."



호스트와 애플리케이션으로 로그 관리 영역 확장

"윈도우 고급감사정책, 리눅스 오딧 설정으로 자동화된 로깅 및 실시간 공격 탐지"

프루라(PLURA)는 제한없이 모든 로그를 실시간 수집, 분석합니다.

운영체제 (OS)

Windows의 Event Log, Sysmon,
Linux의 Syslog와 Audit Log 분석

웹 (WEB)

HTTP Header와 본문 전문
(Post-body, Resp-body) 로그 분석

PLURA

정보보안 & 네트워크 장비

방화벽, 웹방화벽, 침입차단시스템,
스위치 등의 syslog 로그 분석

응용프로그램

Tomcat catalina.out, access 로그,
MySQL, Redis, RDP 로그와
NAC , DRM 등의 DB 접속 로그 분석

차세대 보안 운영 시스템

"가장 위험한 사이버 위협 공격을 정확하고 빠르게 탐지하고 대응합니다."

네트워크 경계 보안 장비(방화벽, 웹방화벽, 침입차단시스템)의 공격 차단 실패에 대응하기 위하여
호스트 中心 (운영체제 & 웹 로그) 분석을 통해 실질적인 침해 위협 대응 체계를 구축할 수 있습니다.

APT 공격

마이터 어택(MITRE ATT&CK)
프레임워크 기반 탐지

악성코드 · 랜섬웨어 공격

파워셀 명령어 실행,
스케줄러 등록 등 다양한 이벤트
기반 상관 분석 탐지

크리덴셜 스터핑 공격

요청 헤더와 본문(Post-body),
응답 헤더와 본문(Resp-body)
분석 탐지

데이터 유출 공격

응답 본문 분석으로
고객정보, 민감정보 유출 탐지

APT 공격 탐지

"한층 더 지능적인 방어 체계 수립을 위한 마이터 어택 프레임워크 지원"

마이터(MITRE)에서 제공하는 공격 전술(Tactic)과 기술(Technique)의 개념과 관계를 시각화한
어택(ATT&CK) 매트릭스를 제공합니다. 이를 통해 보안 위협이 침해로 발전하기 전에 위협을 찾을 수 있습니다.

보안 검증 표준 제공

보안 측정을 위한
포괄적인 매트릭스를
제공하며, 최신 보안
위협에 대한 대응방안과
기술을 분류해
인사이트를 제공합니다.

최신 공격 기술 정보 제공

최신 사이버 위협
전술과 조직의 위험 및
이러한 전술에 대한
노출을 명확하게
이해하는데
최상의 도구입니다.

집중된 분석 및 대응 제공

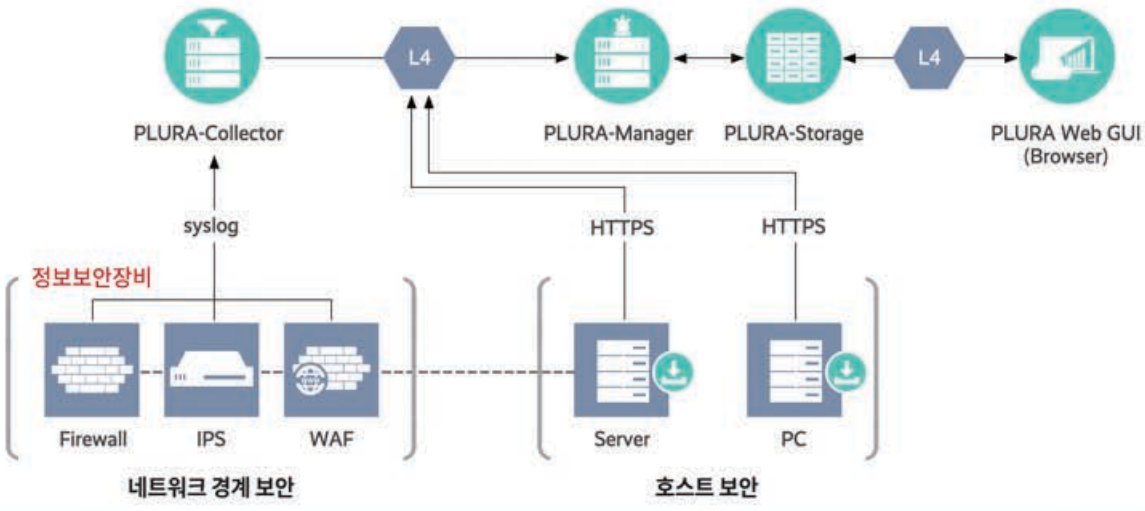
각 경계에서 일어나는
위협 요인을 합치고
공통 위협 요인 간의
공통분모를 만들어 탐지 현황과
탐지기법을 분류하고
표시합니다.

프루라(PLURA) 경쟁력

기존 제품의 한계	PLURA 우수성
네트워크 경계 中心	해킹 최종 목적지인 호스트 中心
로그 수집	로그 자동 생성 / 수집 / 분석
문자열 패턴 매칭 로그 수집 • 분석 솔루션	행위 분석 기반의 공격 탐지 솔루션
전문가가 아니면 사용하기 어려움	자동화를 통한 비전문가도 쉽게 사용 가능
매년 추가 개발과 라이선스 비용을 지불	유지보수 만으로 최신 엔진 업데이트 제공
운영체제 & 웹 서버 로그 분석 지원 없음	운영체제 & 웹 서버 로그 분석으로 공격 탐지
문제 발생 後 사후 분석 시스템	실시간 공격 대응 시스템

로그 수집 방식

에이전트와 에이전트리스 방식 모두 지원 (Agent & Agentless)



- 정보보안장비 연동은 syslog를 이용하여 에이전트리스(Agentless) 방식으로 지원.
- Server와 PC는 에이전트를 설치하여 자동 로깅 및 취합 지원. TTA 에이전트 성능 평가서 제공.
- 전송 구간은 TLS v1.3 암호화 지원.

실시간 로그 수집 및 분석

윈도우의 고급감사정책, 리눅스의 오딧(Audit) 설정,
웹 서버의 요청 본문(Post-body), 응답 본문(Resp-body) 로그 등
공격 관련 로그 자동 생성, 실시간 분석 시스템.

* 윈도우 이벤트 채널 로그 분석 지원 (22종), 시스인터널의 Sysmon 지원
* 윈도우 Registry & File 변경 로그 분석 지원

사용자 상관 분석 기반 보안탐지

사용자가 직접 침해 시나리오를 작성하여 등록/관리하며 서버 內 교차 분석을
통해 랜섬웨어(Ransomware), 데이터 유출(Data breach), 서버 침투 등의
악의적인 공격을 탐지하는 시스템.

* 1,000여 종의 시스템필터와 20여 종의 상관필터 기본 제공

자동화된 분석 및 통계 보고서

일별/주별/월별 분석 보고서와 다양한 통계 분석 기능 제공.

* 마이터 어택, 데이터유출, 크리덴셜스터핑, 업로드 로그 용량, 박스플롯, 워드클라우드, 히트맵 등

사용자 대시보드

공격 탐지/분석 결과에 통합 지표 관리와 업무 효율성을 높이고,
공격 유효성을 빠르게 확인할 수 있는 대시보드 개인화 기능 제공.

ISMS, PCI DSS, ISO 27001, 전자금융감독규정 인증 필수인 로그 취합/분석/관리 최고 서비스

대응하기 어려운 컴플라이언스, 하지만 프루라는 기본 기능입니다.

자동화된 로그 관리 시스템으로 컴플라이언스를 완벽하게 지원하여
정보보호담당자, 시스템관리자의 업무를 90% 이상 경감시켜 드립니다.

ISMS-P ISO PCI DSS COMPLIANT

프루라(PLURA)는 "혁신제품 지정 인증" 제품으로 공공기관의 수의계약 납품 대상이 되며, 공공기관 '혁신구매 목표제' 적용 제품입니다.

혁신제품전용몰 : 프루라(PLURA), 물품식별번호(23882114)

Cigna 라이나생명 | KB 국민카드 | Heungkuk 흥국화재

한국해양수산연수원 | 시흥시 SIHEUNG CITY | GKL 그랜드코리아레저

Keit 한국산업기술평가관리원 | SAMSUNG 삼성전자서비스 | nexes 주식회사 네패스

PIZZA PAPA JOHN'S | MUSINSA soldout | HIPHOPER

CJ 올리브네트웍스 | AJ 전시몰 | ETOOS

건양대학교병원 KONYANG UNIVERSITY HOSPITAL | KCTC | CHUNLAB

T. 070-8802-0306
E. sales@qubitsec.com
H. www.qubitsec.com

큐비트시큐리티 주식회사
서울시 강남구 테헤란로116, 12층 (역삼동 동경빌딩)

QUBITSECURITY