1등급 GOOD Software

Cloud Service Accredited by KACI

K-Innovative Product 혁신제품

EPISC 우수정보보호제품

마이터 어택(MITRE ATT&CK) 기반
통합 정보보안 클라우드 플랫폼

# plura

# XDR

Extended Detection & Response

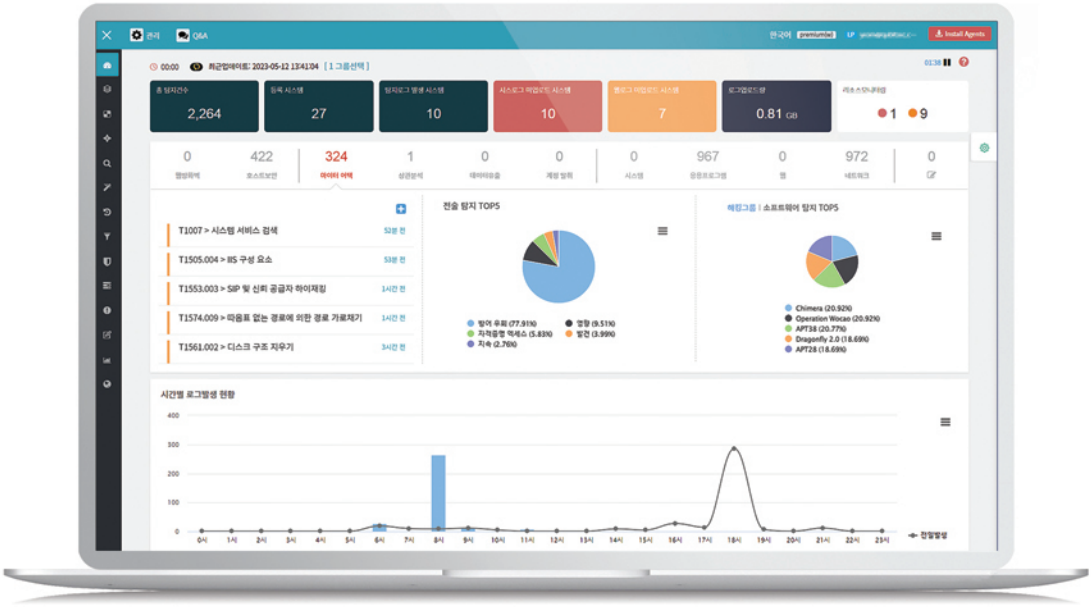
www.plura.io

QUBITSECURITY

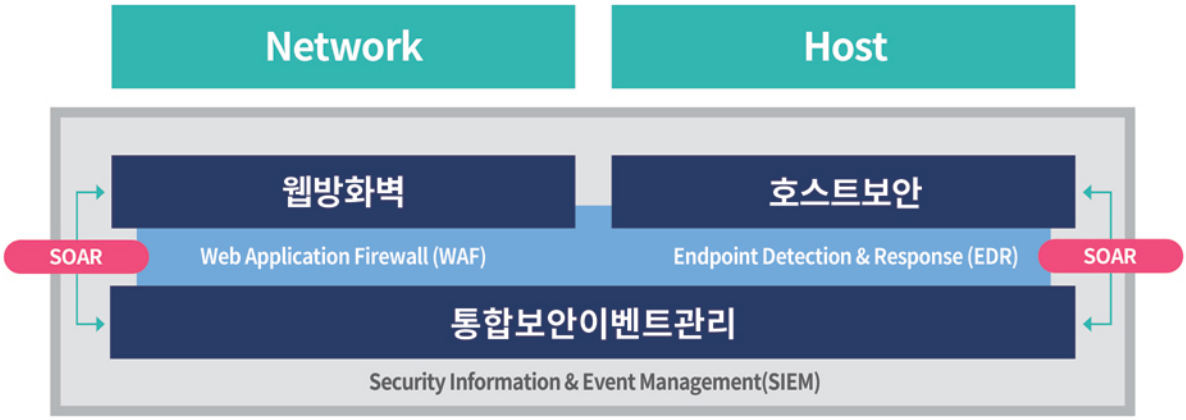
# 실시간 해킹 대응 통합 플랫폼 PLURA-XDR

정보보안은 단일제품이 아닌 플랫폼에서 통합되어야 합니다.
PLURA-XDR은 웹방화벽, 호스트보안, 통합보안이벤트관리
기능을 통합한 정보보안 플랫폼입니다.

## 마이터 어택 기반으로 실질적인 보안 위협 대응 체계 구축




## 각 기능을 수직적으로 통합한 혁신적인 정보보안 플랫폼




**도입 효과**

- 공격에 선제적 대응
- 제로 데이(Zero-Day) 공격에 대응
- 알려지지 않는(Unknown) 공격에 대응
- 응용프로그램 취약점 공격에 대응

# 통합보안이벤트관리 PLURA-SIEM

정보보안 및 네트워크 장비의 상관 분석 기본 기능에
서버와 PC 그리고, 웹의 헤더 및 본문 로그를 분석하여
마이터 어택 기반 해킹공격에 대응하는 혁신 제품입니다.

운영체제는 감사 정책을 설정하지 않으면 로그가 생성되지 않습니다.
웹 서버의 액세스 로그와 함께 본문 로그 수집은 해킹 대응의 출발점입니다.

## 주요 특징

- 제로 트러스트 아키텍처(ZTA) 지원
- 지능형지속위협(APT) 해킹 공격 탐지 및 대응
- 계정 탈취 공격 크리덴셜스터핑 탐지 및 대응
- 웹 요청본문(Post-body), 응답본문(Resp-body) 분석
- SQL 인젝션, 웹셸, 크로스사이트스크립팅(XSS) 분석
- 실시간 탐지 현황 대시보드, 보고서 및 통계 서비스
- 잔디, 텔레그램, 라인, 구글챗을 통한 알람 제공

### 운영체제(OS) 로그

**윈도우 서버** : 이벤트 로그, 시스몬(Sysmon)
**리눅스 서버** : 시스로그(syslog), 오딧(audit) 로그
**유닉스 서버** : 시스로그(syslog), 오딧(audit) 로그

### 웹 서버 로그
(액세스 + 본문 로그)

MS IIS, Apache HTTPD, Tomcat, NGINX,
Node.js, Spring boot 등

## PLURA-SIEM 연동 서비스 기능

- 웹방화벽(PLURA-WAF)
- 호스트보안(PLURA-EDR)
- 접속 IP주소, 로그인(Login), URL 분석 지원
- 상관 분석 지원
- 他社 제품과 syslog 연동
- 탐지 알람 웹훅 및 티켓 시스템 연동
- 전체 로그 수집, 분석, 저장 지원

# 웹방화벽 PLURA-WAF

OWASP TOP 10 웹 해킹 공격 차단
계정탈취 공격인 크리덴셜스터핑 차단
개인정보·민감정보 등 데이터유출 공격 차단

## 웹 본문 분석으로 크리덴셜스터핑과 데이터 유출 차단, Unknown 공격 대응을 위한 SIEM 연동 전체 로깅 지원은 필수입니다.

### 주요 특징

- 제로 트러스트 아키텍처(ZTA) 지원
- SQL 인젝션 공격 차단
- 계정탈취 공격 크리덴셜스터핑 차단
- 전체 웹 로그 분석으로 알려지지 않는 공격 대응
- 응답본문 분석으로 데이터유출 공격 대응
- 요청 및 응답본문 크기 분석으로 이상징후 탐지
- TLS/SSL 인증서 관리
- 정기점검 공지 안내 관리
- 실시간 탐지 현황 대시보드, 보고서 및 통계 서비스
- 잔디, 텔레그램, 라인, 구글챗을 통한 알람 제공

## 공격 탐지는 단일 패킷 뿐 아니라 SIEM 연동을 통한 상관분석으로 웹 공격에 최상의 대응을 제공합니다.

### PLURA-SIEM 연동 서비스 기능

- 계정 로그인 정보 수집, 분석
- 크리덴셜스터핑·볼륨메트릭 수집·분석·저장
- 웹사이트 위·변조 탐지
- 공격 IP주소 수집·분석·저장
- 공격 URL 정보 수집·분석·저장
- 전체 로그 수집·분석·저장

# 호스트보안 PLURA-EDR

마이터 어택(MITRE ATT&CK) 기반으로
호스트(서버와 PC)에 대한 지능형지속위협(APT)
공격을 차단합니다.

제로 데이, 알려지지 않는 공격 등 APT 공격에 대응하기 위하여
반드시 마이터 어택 프레임워크 기반으로 운영 되어야 합니다.

## 주요 특징

- 제로 트러스트 아키텍처(ZTA) 지원
- 행위 분석 기반으로 APT 공격 차단
- DLL 인젝션 공격 대응
- 윈도우 고급감사정책 설정으로 로깅 제공
  (Windows Defender, PowerShell, TaskScheduler 등)
- 윈도우 레지스트리, hosts 파일 변경 탐지 제공
- 리눅스 오딧 설정으로 로깅 제공
- 실시간 탐지 현황 대시보드, 보고서 및 통계 서비스
- 잔디, 텔레그램, 라인, 구글챗을 통한 알람 제공


선제적 대응을 원한다면 마이터 어택 프레임워크에서 시작해야 합니다.

2018 과학기술정보통신부, '우수정보보호 기술·제품' 선정

2019 한국발명진흥원, '우수발명품' 우선구매추천 선정

2020 조달청, '혁신제품' 선정(통합로그관리 PLURA V5)

2021 미국·중국 특허 등록

2022 TTA, GS인증 1등급 획득

Heungkuk 흥국화재 · KB국민카드 · 한화생명 · nexes 주식회사 네패스

SAMSUNG 삼성전자서비스 · SK telecom · LG전자 · CU

CJ 올리브네트웍스 · posco DX · YBM · ETOOS

사랑의교회 SaRang Church · CTS기독교TV · 천주교 서울대교구

코메디닷컴 · 건양대학교병원 KONYANG UNIVERSITY HOSPITAL · 뉴스타파 · KCTC

GI VITA · PIZZA PAPA JOHNS · COMMAX · 전쟁기념관

시흥시 SIHEUNG CITY · 한국해양수산연수원 · GKL 그랜드코리아레저 · Keit 한국산업기술평가관리원


**큐비트시큐리티 주식회사**

서울시 서초구 서초대로 396 18층 (서초동, 강남빌딩)

T. 070-8802-0306

E. sales@qubitsec.com

H. www.qubitsec.com


QUBITSECURITY