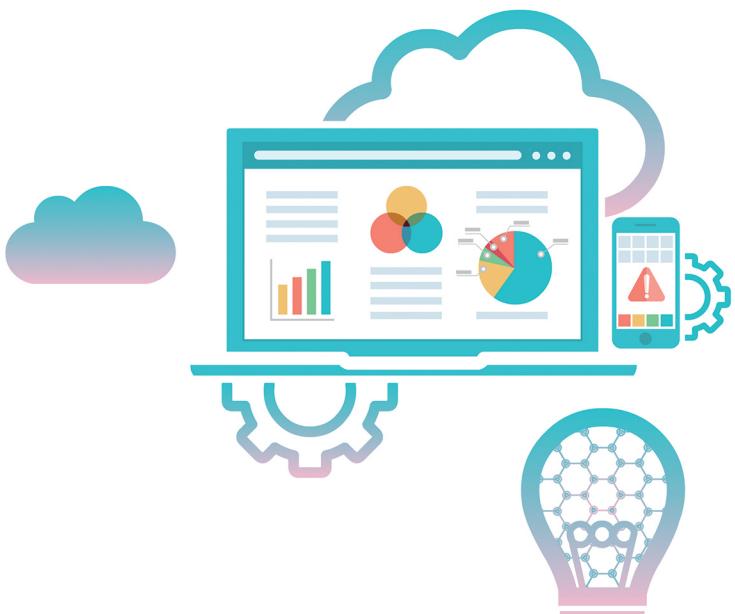




실시간 로그 분석과 머신러닝을 이용하여 해킹을 탐지하는 「차세대 SIEM」

클라우드 SaaS 서비스로 설치부터 서비스 이용까지 5분이면 충분합니다.

우리 서버의 안전한 운영 프루라 「PLURA」와 시작하십시오!



QUBITSECURITY

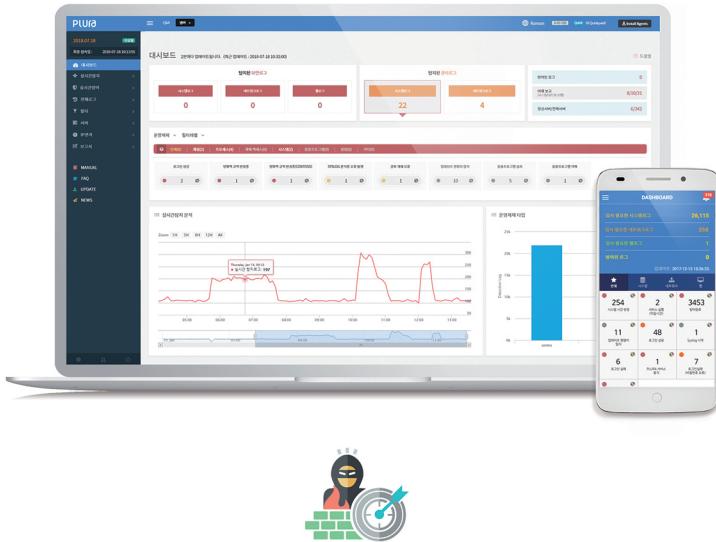
Cloud SaaS Next Generation SIEM

Analyze the logs in real time to detect and block hacking

우리는 왜 해킹 탐지에 번번이 실패할까요?

해킹을 탐지하기 위한 유일한 방법은 로그 분석입니다.
그렇다면 서버에 어떤 로그를 남기고 계신가요?

서버의 로그는 사용자가 설정하지 않으면
중요한 로그는 남지 않습니다.
운영체제는 Hosts 파일을 수정해도, 웹서버는 POST-BODY에
악성코드를 삽입해도 로그를 남기지 않습니다.



프루라「PLURA」를 이용하여 모든 로그를 설정 없이 자동으로 수집하고 분석하세요!
빅데이터 기반 클라우드 SIEM「Security Information & Event Management」

프루라「PLURA」 왜 사용해야 하나요?

현재 진행되고 있는 '사이버 공격'은 사람의 처리 능력으로는 해결할 수 없는 정보를 생성하여 보안 전문가들도 어려움을 겪고 있으며, '기존의 SIEM 시스템'으로도 대응이 쉽지 않습니다.

로그는 기업에 존재하는 위협 정보를 파악하기 위한 가장 기초가 되는 데이터로 정보보안 제품의 바탕을 이루는 요소입니다.
하지만 기업의 시스템, 애플리케이션, 네트워크 등의 다양한 로그와 이벤트 데이터를 자동으로 수집하고 통합하여 이상징후 탐지 시스템을 구축하기 위해서는 **전문인력과 예산**은 필수입니다.

**프루라「PLURA」는 클라우드 SaaS로 초기 도입비용과 설치 기간을 단축할 수 있으며,
전문인력의 지원을 받을 수 있는 차세대 SIEM입니다.**



기존(레거시) 보안제품은 APT 공격과 내부직원에 의한 의도적 유출 탐지가 어렵습니다.

기존 위협탐지 방법은 외부로부터 유입되는 공격의 시그니처를 분석하여 위협을 탐지하는 방향으로 집중되어, 내부 PC 대상의 공격이나 패턴 우회, 내부 직원에 의한 의도적 유출(USB, 프린트, 이메일) 등 APT 공격(사회 공학)에 취약합니다.

“보안은 사슬과 같아서 가장 약한 고리만큼만 안전하다.”

- 브루스 슈나이어 (Bruce Schneier) -

슈나이어가 언급한
취약한 '약한 고리'는 우리 시스템 전체에 걸쳐 있습니다.

전통적인 보안솔루션은 **외부 공격자를 가정하여 서비스 앞 단의 네트워크 보안 강화에 집중**하였습니다.
서버 시스템과 웹 서비스는 관리자의 기대보다 훨씬 취약합니다.

업무망이 인터넷과 분리된 망 분리 환경은 네트워크 공격에 대하여 상대적으로 안정성을 강화하였습니다.
하지만 망 분리 네트워크의 곳곳에 놓인 **연계 솔루션을 제대로 관리해야만 충분한 효과**를 발휘할 수 있습니다.

운영체제(OS), 애플리케이션 그리고 개발들의 지원은 영구적이지 않습니다.
Windows 7, Windows 2008, CentOS 5, Ubuntu 12, Java JDK 1.7등의 지원이 이미 종료되었지만
시스템 어딘가에 아직도 운영 중이라면 순식간에 약한 고리가 될 것입니다.

사용자 데이터스파스워드스쿠기 그리고 난수 생성기 등 암호화를 위하여 사용하는 **암호 모듈과 키 사이즈** 관리는
쉽지 않습니다. 많은 경우 **5~10년 주기의 차세대 시스템을 준비할 때** 변경됩니다.
이와 같은 운영 방식은 약한 고리가 되어 시스템 전체를 약화하게 만듭니다.

SHA-3, TLS 1.3 등 새로운 알고리즘과 프로토콜이 이미 수년 전부터 사용되고 표준화되었지만,
내부 시스템은 과거 **MD5, SHA-1, SSL** 등 오래된 알고리즘과 프로토콜을 사용합니다.

프루라「PLURA」 어떤 서비스인가요?

주요 보안 위협 정보와 이벤트 관리 체계 수립

Cloud SaaS or On-premise? Agent or Agentless? YES!

PLURA-INFRA 서버 보안

윈도우 서버의 이벤트 로그와 시스몬(Sysmon), 리눅스의 시스로그(Syslog)와 오딧로그(Auditlog)로부터 계정 공격, USB 삽입, 데이터 유출 그리고 시스템 설치형 공격인 랜섬웨어 등의 탐지 서비스를 제공합니다.

PLURA-WEB 웹 보안

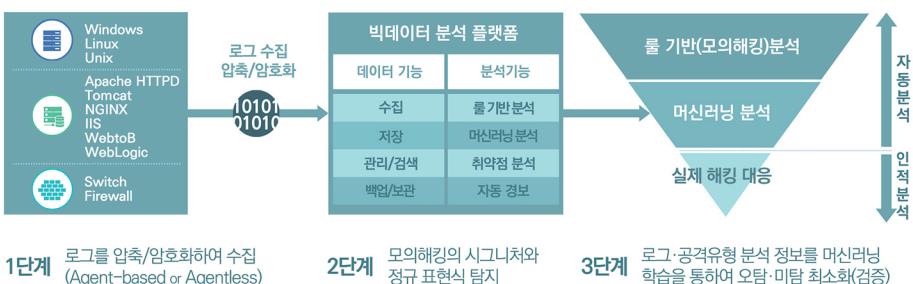
웹 서버 대상 해킹 탐지를 위하여 GET, POST 뿐만 아니라 POST-BODY, RESPONSE-BODY를 'OWASP Top 10' 분류에 따라 공격 유형에 맞추어 예상 피해도와 공격목적별로 탐지 서비스를 제공합니다.

PLURA-NETWORK 네트워크 보안

방화벽(Firewall), 웹방화벽(WAF), 침입탐지(IDS), 침입방지(IPS), 스위치(Switch) 등의 Syslog를 취합하고 분석하여 ARP 스폰핑(Spoofing), 세션(Session) 공격, 설정 변경 등의 해킹을 탐지합니다. 또한, 접속 IP 주소 프로파일링을 통한 자동 분석을 제공합니다.

Vulnerability Check 취약점 점검

운영체제(OS), 웹, 데이터베이스 서버 등의 잘못된 설정과 불필요한 데몬 등의 취약점을 점검하고 관리자가 대응할 수 있도록 조치 방안을 제공합니다.



쉬운 설치와 분석, 적확한 탐지와 협업 시스템 구현

Easy! Quick! Multi! Value!

5분 만에 설치하고 실시간 분석하여 해킹 탐지

에이전트(Agent) 설치 만으로 자동으로 로그 분석이 시작되어 이상 로그를 탐지하여 실시간으로 알려 드립니다.

14일의 체험기간 동안 모든 기능을 경험하세요!

ISMS·ISO 27001 인증 지원

시스템 로그와 웹 로그를 취합·저장·분석·관리하도록 규정하고 있는 'ISMS·ISO 27001' 인증을 지원합니다.

보안 담당자와 시스템 관리자가 동시에 사용

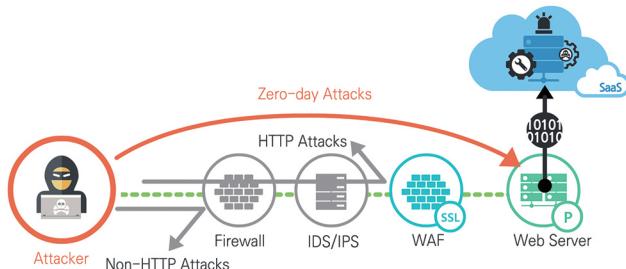
보안을 위한 위험 행위 로그 분석뿐 아니라 커널 애러, 시스템 읽기 오류, 서비스 중지 등

시스템 운영자와 정보보호 담당자가 협업하여 서버에서 발생하는 모든 문제에 대하여 실시간 분석이 가능합니다.

프루라 「PLURA」 어떤 특징이 있나요?

Apache HTTP Server, Tomcat, NGNIX, IIS, WebtoB, WebLogic 등 모든 웹 서버의 POST-BODY 로깅을 통한 실시간 분석과 해킹 탐지

해킹 공격의 80%는 웹 서버를 거쳐 시작됩니다. SQL Injection, XSS(Cross-Site Scripting), Web Shell 이와 같은 공격들은 POST 방식으로 본문(BODY)에 공격 데이터를 삽입하는 형태로 이를 탐지하기 위해서는 웹 로그에서 기본으로 넘겨 되어 있는 GET 분석뿐만 아니라 POST-BODY, RESPONSE-BODY 분석을 통해 웹 방화벽을 통과한 해킹 공격을 탐지하여 웹 서버 해킹에 대응할 수 있도록 제공합니다.



웹 서버 로그 자동 분석 서비스

악의적인 사용자가 어떠한 목적을 가지고 공격했는지
유형원칙(누가·언제·어디서·무엇을·어떻게·왜)에 근거하여 직관적인 정보를 전달합니다.
또한, 해당 공격으로 인한 서버 피해도를 예측하여 침해 사고에 대해 실시간으로 대응할 수 있습니다.

에이전트 설치 없이(Agentless) 웹 트래픽 수집과 해킹 탐지

웹 서버에 프로그램 설치 없이 별도의 어플라이언스 서버에서 웹(HTTP) 트래픽 수집을 통하여 POST-BODY를 분석합니다. 웹 서버의 리소스를 사용하지 않으므로 시스템 부하를 고민하지 않아도 됩니다.

실행 명령어 분석을 통한 해킹 행위 탐지와 차단

서버에서 수행되는 사용자의 명령어(command)를 모니터링하여 악성 프로그램 설치, 다른 서버로의 비인가 접속, 권한 탈취 시도, ARP 스팍핑 등 해킹 공격을 실시간 탐지하고 차단합니다.

MySQL, Redis, HAProxy, OpenVPN 등 모든 서버의 로그 데이터 취합 분석

모든 응용 프로그램의 로그를 취합하고 분석하여 해킹을 탐지합니다.
어떤 응용 프로그램의 로그라도 간단한 설정만으로 바로 분석이 시작됩니다.

상황인식 랜섬웨어 탐지 기술

사용자의 파일을 변조하는 상황(확장자 변환, 랜섬노트 발생, C&C 서버 연결 등)을 종합적으로 판단하여 탐지합니다. 사용자의 파일을 사용하지 못하게 암호화하는 행위를 실시간 탐지합니다.



메일과 앱 푸시를 통한 알림 기능

이메일>Email, 스마트폰 앱 푸시(Push) 알림 기능을 통해 위협 로그 탐지 시 즉시 확인할 수 있습니다.
알림 횟수 설정, 발생 로그의 시간대 등을 사용자가 원하는 방식에 따라 선택할 수 있어 과도한 알림으로부터 업무를 효율적으로 관리할 수 있도록 지원합니다.

흥국화재해상보험 주식회사 Heungkuk Fire & Marine Insurance

1948년 설립, 반세기 동안 대한민국의 보험역사를 굳건히 지키며 고객과 함께 성장하는 대표적인 손해보험 기업

도입 배경

- 기존 ArcSight 솔루션 운영 어려움과 로그 취합의 한계 개선 요구
- 시스템 로그와 웹 로그 분석의 필요성 대두
- ISMS 인증에는 시스템 로그와 웹 로그 취합·분석·관리가 명시되어 있음

도입 효과

- 로그 취합과 분석 시스템 구축 : 시스템, 웹 서버, 네트워크 장비 등
- 모든 시스템에 대하여 실시간 해킹 탐지 시스템 구축
- ISMS 인증 요구 조건 준수

금융보안원 금융보안원



2015년 출범, 금융권 사이버 위협정보 공유와 금융보안을 전담하기 위해서 기존 금융결제원의 금융ISAC, 코스콤의 증권ISAC, 금융보안연구원의 통합기관

도입 배경

- 금융보안원에서 189여개의 금융회사에 제공하는 '서버 자율점검 도구' 시스템 개편

도입 효과

- 운영 시스템의 취약점 점검 서비스 시스템 구축
- 자동점검, 이력관리 등 효율적인 관리를 위해 시스템별 타임라인 상의 설정, 형상 정보들을 클라우드 시스템을 통해 수집하여 해킹에 노출될 수 있는 위험 요소들을 법적 규제 준수 기준에서 점검하고 감사 리포트를 제공
- 설정, 형상 정보들의 변경 이력을 모형화하여 주요 위협이 될 수 있는 취약점을 실시간 감시



www.plura.io

