Plura

Excellent Cyber Security Partner

AUTOMATICALLY REAL-TIME LOG ANALYSIS

NEXT GENERATION SIEM “PLURA”

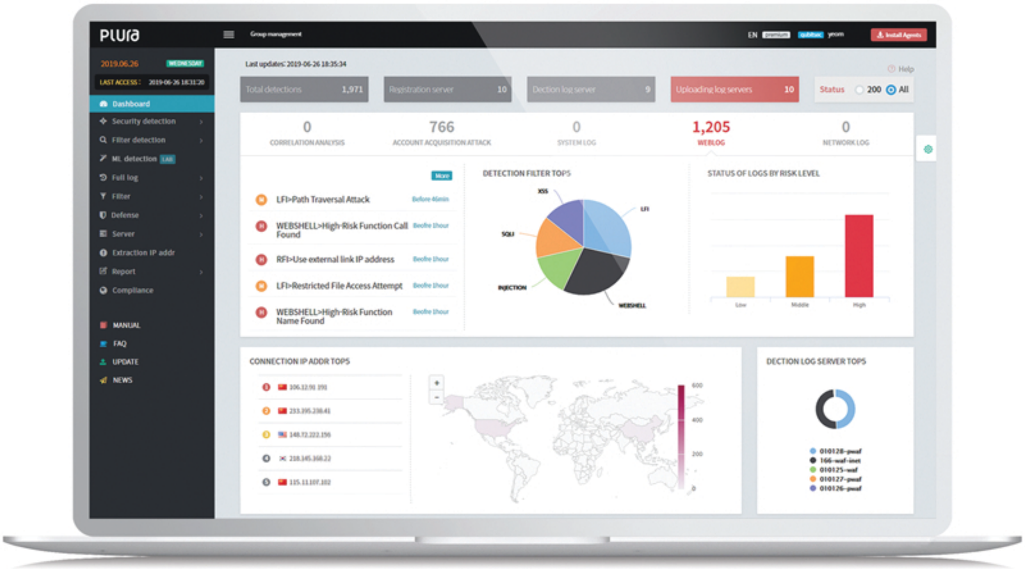
TO DETECT HACKING

www.plura.io

QUBITSECURITY

SECURITY INFORMATION AND EVENT MANAGEMENT

PLURA ensures the visibility of the entire system
(log generating, collecting, processing, searching, analyzing, storing, and discarding).
Helping information protection personnel focus their work on detecting signs of substantial anomalies
"Next generation SIEM" that can respond quickly to incidents and security threats.



LAST ACCESS : 2019-06-26 18:31:20

Last updates: 2019-06-26 18:35:34

Total detections 1,971

Registration server 10

Dection log server 9

Uploading log servers 10

Status ○ 200 ● All

0	766	0	1,205	0
CORRELATION ANALYSIS	ACCOUNT ACQUISITION ATTACK	SYSTEM LOG	WEBLOG	NETWORK LOG

- M LFI>Path Traversal Attack Before 46min
- H WEBSHELL>High-Risk Function Call Found Beofre 1hour
- H RFI>Use external link IP address Beofre 1hour
- M LFI>Restricted File Access Attempt Beofre 1hour
- H WEBSHELL>High-Risk Function Name Found Beofre 1hour

1 106.12.91.191
2 233.195.238.41
3 148.72.222.156
4 218.145.168.22
5 115.11.107.102

- 010128-pwaf
- 166-waf-inet
- 010125-waf
- 010127-pwaf
- 010126-pwaf

Available On-premise and Cloud SaaS

FEATURES

User Correlation Analysis

Provide a correlation analysis
system that enables users to create, register,
and manage infringement scenarios.

Machine Learning Detection

Intelligent APT attack response system
through machine learning analysis
of Big Data.

Web Log Analysis Support

A system that compensates
for the attacks that failed
to block by WAF.

Real-Time Protection (Blocking)

A system that detects and
defends hacking attacks
through real-time log analysis.

Compliance

Provide automatic mapping
of PCI DSS, ISO 27001, ISMS-P
compliant items and detection logs.

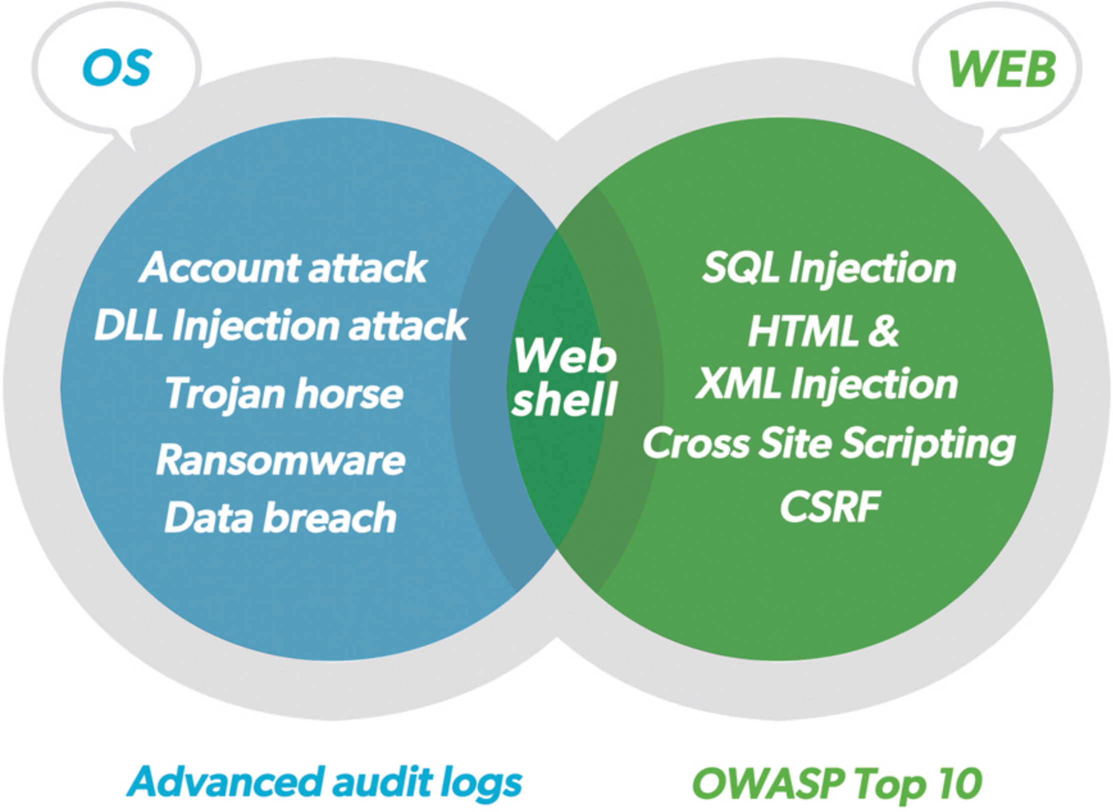
Notification & Ticketing

Instant notification
with Email and Webhook (Hangout, Slack).
Ticketing (Redmine, MantisBT, Jira) support.

Built-in hacking detection engine through Windows, Linux and Web server log analysis!

Over 300 filters detect hacks such as account attacks, DLL injections and ransomware from the operating system (Windows, Linux) logs.

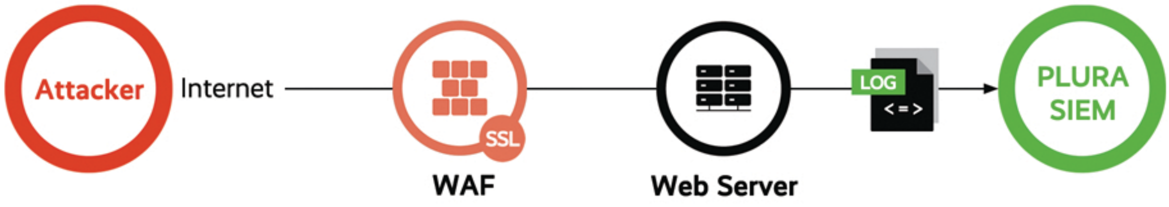
Real-time automatic analysis of web server logs detects Credential stuffing, Volume metrics, Homepage forgery attack detection, and hacks such as SQL injection and Cross-site scripting (XSS) based on OWASP Top 10 classification.



Accurate detection through audit log analysis!

Advanced Audit Policy on Windows Server, Desktop and Audit Log Analysis on Linux Server detects detailed security threats from inside operating system (OS).

Provide system-wide visibility, including Webshell activity through WAF.



DLL Injection Hack Attack Detected

An automatic detection system that completely replaces manual detection using Windows Sysinternals Process Explorer.

Automatic Detection of Bypass Attacks with AI

An intelligent analysis system for overcoming false positives and false negatives which is the limit of passive analysis of security analysts, by applying machine learning analysis technology to web system attack behavior detection.

Sysmon Log Analysis Support

More advanced and accurate Windows Server Log Analysis! Support log analysis by Windows Sysinternals Sysmon to provide differentiated log analysis.

USB Channel Log Analysis Support

Support Windows USB device channel analysis to provide event log management for USB device attachments and detachments.

Best service for log collection, analysis, management that require PCI DSS, ISO 27001 certification!

Compliance is difficult, but PLURA provides basic feature.
Automated log management system fully supports compliance, reducing the work of system administrators and information security officers by more than 90%!

「PLURA」 Cloud SaaS Service

PLURA Cloud SaaS automates the entire process of collecting and analyzing various logs and events, so it takes three minutes from installation to data analysis.

meet plura.io　Join > Install Agents > Start PLURA

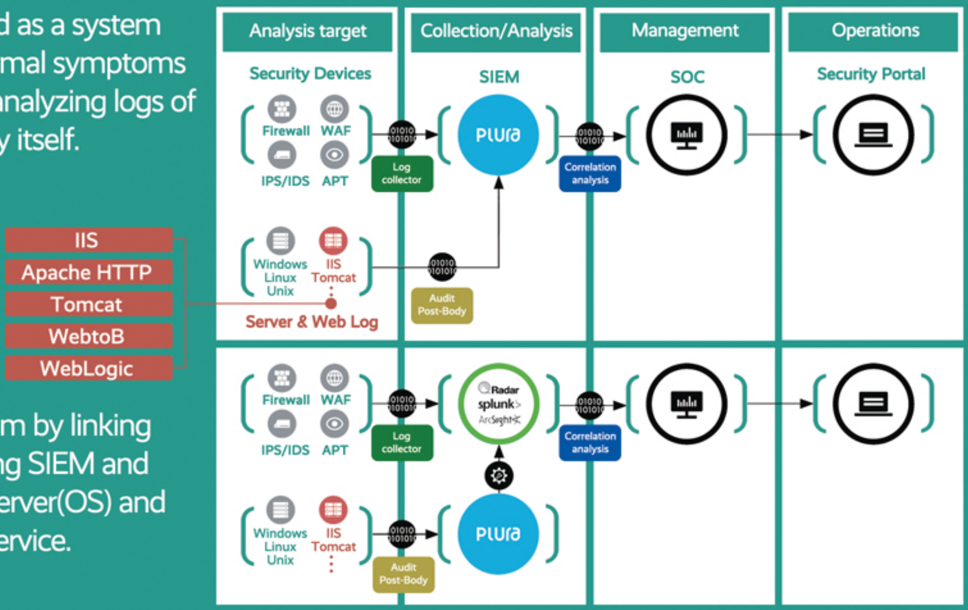
「PLURA」 Package (On-Premise)

Cloud SaaS products are delivered as an on-premise package.

SORT	DESCRIPTION
PLURA-Manager	Log collection, Real time log analysis, Security threat detection, Dashboard, Report.
PLURA-Web Console	Collect, analyze and detect log management by user accessing through Web UI.
PLURA-Agent	Windows Server & Desktop: Collect 20 kinds of event channel logs. * Advanced audit policy setting support. Linux Server: Syslog, Audit log collection. Web Server: GET & POST log collection. * Request Post-body, Response Resp-body logging support.
PLURA-Syslog Collector Server	Information Security Products, Network Equipment : Log transfer server that collects Syslog and sends to PLURA Manager.

「PLURA」 Operating Method

01 PLURA is operated as a system that detects abnormal symptoms by collecting and analyzing logs of all devices alone by itself.



02 Operate as a system by linking provided by existing SIEM and PLURA with the server(OS) and web log analysis service.

2019

- Selected as the recommended business of superior invention priority purchase, Patent Office.
- Selected in the 5th Shinhan Future's Lab & the 1st Shinhan Future's Lab Indonesia.
- "Grand Prize" of 2nd Seoul Innovation Challenge, Seoul City.

2018

- 2018 Selected as the company of Excellent Information Protection Technology and Product, Ministry of Science and ICT & KISA.
- Patent registered: "System and method for detecting attack based on real-time log analysis".
- Signed a contract to supply 「Server Self-Checking Tool」, with Financial Security Institute.
- Tokyo office opened.

2017

- 2017 K-ICT Cloud Awarded, the Ministry of Science and ICT.
- National Productivity Award, the Minister of Trade, Industry and Energy.
- PPS(Public Procurement Service) Venture Start-up Innovative Product Registration(23213052).

2016

- 2nd Selected as K-Global 300, the Ministry of Science and ICT.
- K-Startup, KBS TV, Awarded, the Minister of National Defense.
- 'PLURA' GS Certification Level 1, TTA.

2015

- Selected as a TIPS, Small and Medium Business Administration.

2014

- Established Qubit Seurity Inc.

EPISC
우수정보보호제품
Excellent Potential Information Security Company

Ministry of Science and ICT

KISA KOREA INTERNET & SECURITY AGENCY

en.qubitsec.com
plura@qubitsec.com

QUBITSECURITY