



## 로그생명주기 전 과정을 지원하는 대용량 실시간 통합로그관리시스템

# LogCops

LogCops는 대용량으로 발생하는 로그를 실시간으로 수집, 검색, 분석, 보관 및 폐기하기 위한 소프트웨어 기반 통합로그분석시스템입니다

각종 시스템, 웹, 방화벽/VPN/IPS 혹은 응용프로그램, 개인정보접근이력 등의 로그를 로그생명주기 (로그생성, 수집, 분석, 보관, 폐기) 전 과정에 맞추어 관리하고, 이 모든 과정을 실시간으로 처리 할 수 있습니다. 또한, SIEM(Security Information & Event Management) 기능을 제공하여 데이터 통합 분석을 통해서 다양한 보안위협 시나리오를 설정하여 운영 할 수 있습니다.



### 로그 생명 주기



### LogCops 상세 특징

- 실시간으로 모든 뷰, 검색, 보고서, 시각화, 대시보드, 경고를 처리
- AGENT, SYSLOG, SNMP, FTP, DB추출 등 다양한 수집방식 지원
- 대용량 로그 데이터의 실시간 처리 및 분석 지원
- 수십TB 로그를 대상으로 즉시 혹은 수초 이내 검색하는 최고의 검색 성능
- 사용자 시나리오 기반 검색 시스템 지원
- 이종 데이터간 JOIN (INNER, LEFT, RIGHT, CROSS 등) 기능 제공
- 이종 데이터간 정규식(POSIX 표준 포함) 검색 기능 지원
- 검색된 결과에서 재 검색하는 무제한 결과내 검색 가능
- 다수개의 필드를 이용한 Group By 검색 기능
- 다수개의 필드를 이용한 Pivot 검색 기능
- 동종 혹은 이종 로그간의 연관 검색 기능
- IP 및 LOGID에 대해 다양한 가상필드 확장 기능
- 사용자기반 설정을 이용하여 다양한 분석 보고서 생성
- 뷰, 검색, 보고서, 시각화, 대시보드, 경고에 대한 다양한 설정이 가능한 고급선택 기능
- EXCEL, WORD, HTML, TEXT 등 다양한 파일형태로 보고서 생성 및 이출(Export) 가능
- 동종 및 이종로그, 단일 및 다중로그를 합산 혹은 분리 처리할 수 있는 기능
- 로그의 보관기한, 장소 및 복제(1차 및 2차)의 선택적 및 체계적 설정 기능
- WORM장비에 선택적 보관
- 원본로그를 압축율 12:1로 압축화(기본) 보관 및 암호화(선택) 보관
- 간편하고 직관적인 웹 서비스 GUI
- 중앙 집중식 로그관리
- 사용자별, 장비별, 로그별, 기능별 엄격한 권한분리
- 사용자 정의기반의 다양한 대시보드 구성 기능
- 관제템플릿을 제공하여 다양한 보안위협 시나리오 설정 및 경고 설정

### LogCops 실행화면

- 대시보드, 실시간 검색, 실시간 분석 등 다양한 시스템 구성화면 및 사용자 중심의 간편하고 직관적인 웹서비스 GUI 지원



▲ 대시보드 화면

▲ 수집시스템 현황 화면

## LogCops 시스템 소개



### 대용량 통합로그관리시스템 및 SIEM

각종 서버, Web, WAS, 정보보호 장비, 응용프로그램, 개인정보 접근이력에서 발생하는 로그를 실시간(Real-Time)으로 수집하고, 수집된 로그를 실시간으로 검색 및 분석 할 수 있으며, 관제 템플릿을 제공하여 보안위협에 대한 이상징후를 탐지합니다.



### 사용자 행위 감사로그 기록 및 재생

서버 자산에 접근한 모든 사용자 행위를 녹화(Recording) 및 재연(Replay) 기능을 제공하며 별도의 관련 솔루션 도입을 대체 할 수 있습니다.



### 로그생명주기를 지원하는 통합 시스템

로그가 생성된 후 수집, 가공, 검색, 분석, 보관 및 폐기에 이르는 로그생명주기(Log life Cycle)의 일부분을 지원하는 부분 솔루션(Partial-Solution)이 아니라 전과정을 자동화하여 관리 할 수 있는 통합 시스템(Integrated System)입니다.



### 다양한 활용방안을 제공하는 다목적 솔루션

실시간 시스템 감사 모니터링, 포렌식(Forensics), 로그관련 각종 법규 및 지침 준수, 보안 및 정보보호 등 감사 및 컴플라이언스에 부합할 수 있는 다목적 솔루션(Multi-Purpose Solution)입니다.

## LogCops 시스템 효율성

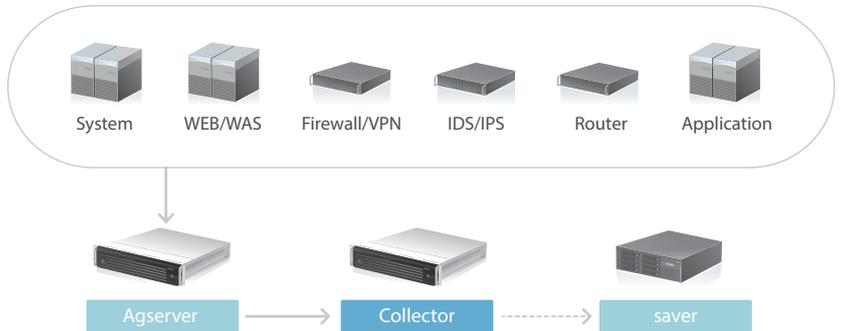
- 로그데이터를 실시간으로 안전하게 저장
- 중앙 집중화 된 로그관리로 효율적인 디스크 관리
- 보안사고 발생시 책임추적 가능
- 저장된 로그파일의 법정 증거자료로 활용가능
- 장기적인 로그분석으로 강력한 보안대응체제 구축
- 강화된 로그관련 법규 준수
- 로그 위·변조 방지를 위한 무결성 및 기밀성 보장

## 로그관련 국내 법규, 지침, 규정 및 인증

국제 표준	국제 표준
FISMA	Federal Information Security Management Act of 2002
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act of 1996
SOX	Sarbanes-Oxley Act of 2002
PCI DSS	Payment Card Data Security Standard
ISMS	Information Security Management System
GDPR	General Data Protection Regulation
한국	한국
	정보통신 기반 보호법 13조 1항(침해사고의 통지)
	정보통신 서비스 정보보호지침 제 3조 5항 (복구 대책)
	주요정보통신 기반시설 보호지침 제 4조(침해사고 예방조치)
	전자 금융 대책 안 로그백업 및 보관기간
	ISMS-P

## LogCops 시스템 구성

Product	Environment	Misc.
Collector	Back-end Collector with Memory Queue, Linux, HW Appliance	Collector Agserver
Agserver	Front-end Collector, Linux, HW Appliance	Option
Saver	NAS/SAN/Shared File System, Linux, HW Appliance	Option



## LogCops 시스템 규격 및 사양

Model	LCA-7010	LCA-7020	LCA-7050	LCA-AGS
Appliance	Collector 	Collector 	Collector 	Agserver 
CPU	6-Core * 1	8-Core * 2	10-Core * 2	6-Core * 2
Memory	32GB (64GB)	64GB (128GB)	128GB 이상	32GB 이상
Disk	Usable 5TB 이상	Usable 10TB 이상	Usable 40TB 이상	Usable 1TB 이상
NIC	1Gb 2-port	1Gb 2-port	1Gb 2-port	1Gb 2-port
Power	Redundant Power Supply	Redundant Power Supply	Redundant Power Supply	Redundant Power Supply
Form factor	Rack type (2U)	Rack type (2U)	Rack type (2U)	Rack type (1U or 2U)

\*상기 규격은 사전 고지 없이 일부 변경될 수 있습니다.