LogCOPS™

통합 로그분석 전문도구

Enterprise Log Analysis and Management System

행정정보 보호용 제품
LogCOPS™
통합 로그분석 전문도구
㈜나일소프트

㈜나일소프트
NileSOFT Ltd.

Enterprise Log Analysis and Management System

LogCOPS™

통합 로그분석 전문도구

로깅(Logging)이란?

시스템 작동현황의 축약내용(로그)을 저장매체 또는 출력장치에 기록하는 행위입니다.

로깅의 지원 근거

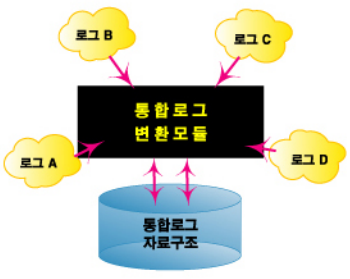
주요 컴퓨터 운영체제 및 프로그램 피키지는 감사 보안체계(C2) 확보를 요구하는 미 국방성의 정보보호 의무규정을 지원하고 있습니다.

로그의 3종류

보 안	시스템에 치명적인 영향 및 신뢰성을 저하시키는 시항과 관련한
시스템	시스템운영체제의 일반적인 작동상황을 기록한 로그
응용 프로그램	일반 응용프로그램이 자신이 수행한 작업 내역을 기록한 로그

통합로그관리기법

서로 다른 이질적인 로그 자료들을 공동자료 구조형식으로 변환하여 저장 관리하는 기법



LogCOPS™ 은 엔터프라이즈 환경에서 여러 호스트들이 생성하는 로그를 한대의 전용 호스트에서 통합하여 관리하는 기능을 가지고 있는 통합로그분석 전문도구입니다. 관리자는 LogCOPS를 통해서 전체 시스템 로그의 검색, 조회 및 시스템의 상태 파악과 원본 로그백업, 보고서 작성 등의 편의기능을 사용함으로서 외부 및 내부의 침해에 대한 감사시스템으로서 활용 할 수 있습니다.

LogCOPS™ 필요성

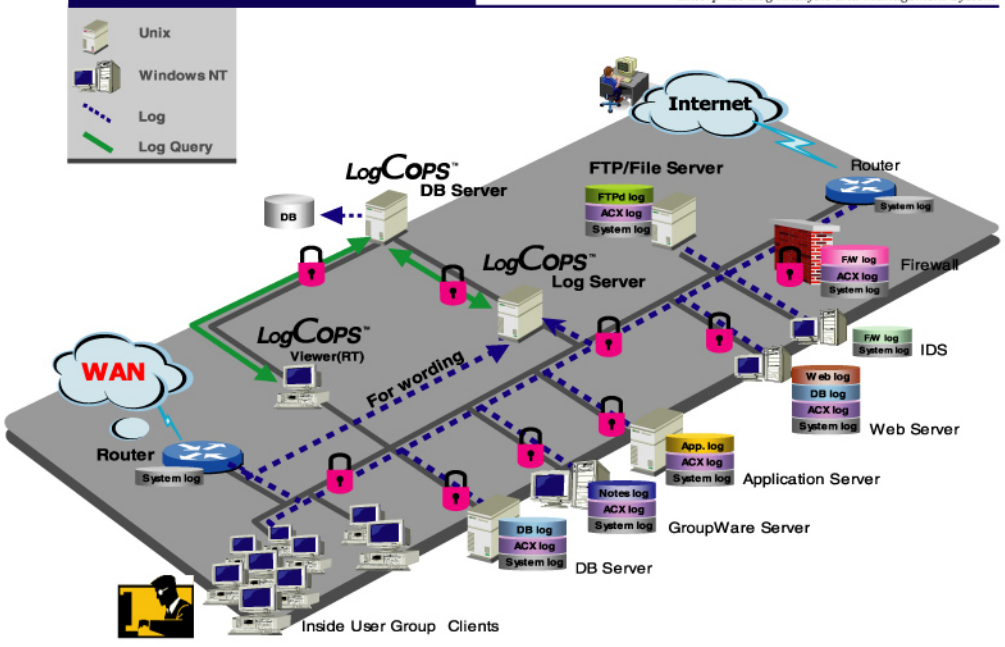
Enterprise Log Analysis and Management System

시스템 관리자가 개별 호스트들의 상태를 일일이 감시하기가 쉽지 않으며 또한 전체 시스템의 상황을 통합하여 파악하기는 더욱 어렵습니다.

대부분의 운영체제들은 침해사건을 감시하기 위한 기본적인 장치를 마련하고 있는데 이는 시스템의 현재 상황을 로그파일에 저장하는 기능입니다. 시스템 로그파일들을 조회해 봄으로서 시스템 관리자는 개별 호스트의 침해사항을 확인해 볼 수 있습니다. 대부분의 서비스 운영 사이트들은 다수의 이기종 플랫폼 호스트들을 광대역 네트워크 환경에서 운영합니다. 이러한 엔터프라이즈 환경에서는 시스템 관리자가 개별 호스트들의 상태를 일일이 감시하기가 쉽지 않으며 또한 전체 시스템의 상황을 통합하여 파악하기는 더욱 어렵습니다.

LogCOPS™ 구성도

Enterprise Log Analysis and Management System



Any Log

어떤 로그파일을 관리하려고 하십니까? 로그파일 포맷을 알고 계시면 로그분석 프로그램 자체를 수정하지 않고 즉시 수용할 수 있습니다.

Any Search

어떤 검색형태로 분석하려고 하십니까? 검색형태만 지정하여 주시면 로그분석 프로그램 자체를 수정하지 않고 즉시 수용할 수 있습니다.

Any Report

어떤 보고서형태로 생성하려고 하십니까? 보고서형태만 지정하여 주시면 로그분석 프로그램 자체를 수정하지 않고 즉시 수용할 수 있습니다.

LogCOPS™ 특징

Enterprise Log Analysis and Management System

◆ 쉽고 간편한 사용 및 설치

- 윈도우 탐색기 형태의 직관적이고 한글화된 사용자 인터페이스 지원
- Install Shield를 이용한 간편한 설치 및 삭제 지원
- 친절하고 자세한 온라인 도움말 지원

◆ 고성능 로그분석 엔진 사용

- 강력하고 효율적인 로그분석 엔진 지원
- 매핑엔진, 검색엔진, 보고서엔진 제공
- DB 서버와 로그서버의 통합 및 분리 지원
- 템플릿 기반의 유연한 확장성 지원

◆ 다양한 로그파일 수용 (Any Log)

- 시스템로그(wtmp, sulog, syslog등 20종 이상) 지원
- 방화벽로그, IDS/IPS로그, 웹로그, 네트워크장비 로그, RDBMS로그, 서버보안로그 등 각종로그 지원
- 일반 사용자 응용프로그램 로그 지원
- 실시간 로그수집과 배치 로그수집 등 다양한 형태 수집방법 지원
- 매핑템플릿, 마법사 및 매핑엔진으로 어떠한 로그파일도 수용

◆ 다양한 검색기능 지원 (Any Search)

- 기본, 사용자, 응용, 패턴 템플릿을 이용한 다양한 검색방법 지원
- 기본, 고급, 연관, 패턴분석 및 챠트 기능 지원
- 다중 로그파일 간 OUTER JOIN 분석 및 고급 SQL 쿼리문 작성 지원
- 검색템플릿, 마법사 및 검색엔진으로 어떠한 검색형태도 수용

◆ 다양한 보고서 지원 (Any Report)

- 검색즉시 보고서, 사전 정의보고서 등 다양한 보고서 지원
- Crystal Report 9.0을 이용하여 작성된 그래프와 표 형태의 강력한 리포트 기능 지원
- Html, Word파일, Excel파일, PDF, Text 등 다양한 파일형식으로의 보고서 변환기능 지원
- 보고서템플릿, 마법사 및 보고서엔진으로 어떠한 보고서도 수용

◆ 다양한 운영체제 및 네트워크 장비 지원

- Solaris, HP-UX, AIX, Unixware, Linux 등 유닉스 운영체제로그 지원
- Windows NT, 2000, 2003 등 윈도우즈 운영체제로그 지원
- Firewall, Router 등 다양한 H/W Appliance 지원

◆ 다양한 이벤트 지원

- 자체 분류 및 제작한 이벤트 지원
- 사용자 정의 이벤트 및 매치스트링 지원
- 실시간 뷰어 혹은 로그검색 시 다양한 형태로 표시

◆ 로그파일 연관관계 추적 지원

- 로그파일 간 연관관계 분석 추적 데이터 제공
- 필요시 사용자가 로그파일 연관관계 정의
- 각종 공격(취약점 공격) 패턴에 대한 로그 검색 가능

◆ 다양한 부가기능 지원

- 로그파일(로그별, OS별)의 매핑, 검색 및 보고서 템플릿 업데이트 지원
- CPU, Memory, Disk 사용량 등 다양한 시스템 상태 정보를 실시간 제공 (*)
- 보안관제 모듈 및 ESM 과의 연동기능 제공 (*)

LogCOPS™ 도입효과

Enterprise Log Analysis and Management System

로그분석효과

실시간 로그 뷰어와 검색 편집기, 패턴템플릿을 사용하여 체계적이고 전문적인 로그 분석이 가능

비용절감효과

정보보호를 위한 로그관리가 필수인 상황과 장기적인 관점에서 로그 관리에 소요되는 인적,물적,시간적 비용을 절감.

로그관리효과

일반 백업이 아닌 로그자료 전용으로 클래스화 된 DB화 및 자동 기능을 지원함으로써 체계적인 저장 관리 지원

표준화 준수효과

LogCOPS 시스템의 규격은 정보통신 기반보호법, 전자금융 안전대책안,BS7799를 준수하므로 도입 시 표준화 준수효과

다양한 로그 관리 ? + 여러 시스템에서 생성된 로그백업 ? + 검색과 보고서 작성 ? + 특정 이벤트 관리 ?

LogCOPS™ 은 엔터프라이즈 환경에서 여러 호스트들이 생성하는 로그를 한대의 전용 호스트에서 통합하여 관리하는 기능을 가지고 있는 통합로그분석 전문도구입니다.

로그관리
중요하고 다양한 로그를 어떻게 관리하고 계십니까 ?

로그백업
여러 시스템에서 생성된 로그를 어떻게 백업하고 계십니까 ?

보고서 작성
다양한 로그에서 원하는 내용을 검색하고 보고서로 만들 수 있습니까 ?

특정 이벤트 관리
로그에서 발생한 특정 이벤트를 관리할 수 있습니까 ?

LogCOPS™ 기능

Enterprise Log Analysis and Management System

로그수집	▸ 실시간, 배치 및 포워딩 로그수집 ▸ 실시간 로그수집 (에이전트 / 콜렉터 기반, 로그 암호화 송수신) ▸ 배치 로그수집 (Active, Passive, Manual 로그수집, secure FTP 사용) ▸ 실시간 로그 뷰 (로그수집 상황 모니터링 , 해킹여부 탐지)
로그저장	▸ WORM, DVD/CD Jukebox 장비 등 다양한 매체에 안전하게 저장 ▸ 서버보안체제 구축으로 로그의 위변조 가능성 차단
로그변환	▸ **Any Log** : 다양한 로그파일 수용 ▸ 시스템로그, 웹로그, 방화벽로그, IDS로그, 라우터로그, 응용프로그램 로그 등 어떤 로그도 수용 ▸ 강력한 로그 매핑엔진 (매핑 템플릿에 따라 로그파일을 DB로 변환) ▸ 로그파일 자동DB변환, 수동DB변환 처리 ▸ 매핑템플릿 마법사 제공
로그검색	▸ **Any Search** : 다양한 로그검색 가능 ▸ 기본, 응용, 사용자정의, 패턴 등 어떤 형태의 검색도 수용 ▸ 강력한 로그 검색엔진 (검색 템플릿에 따라 로그DB를 검색) ▸ 기본검색, 고급검색, 연관검색, 패턴검색, 챠트 등 다양한 검색 제공 ▸ 검색탬플릿 마법사, 패턴 템플릿 마법사, 챠트 마법사 제공 ▸ 다양한 사용자 추적기능 제공
로그보고서	▸ **Any Report** : 다양한 보고서 생성 가능 ▸ 기본, 응용, 사용자정의 등 어떤 형태의 보고서도 수용 ▸ 강력한 로그 보고서엔진 (보고서 템플릿에 따라 보고서를 생성) ▸ 로그검색 즉시 보고서와 사전정의 보고서 등 제공 ▸ 보고서 템플릿 마법사 제공
업데이트 및 관리기능	▸ 수동 및 자동 업데이트 ▸ 각종 DB 관리 기능 (최신 DB유지, DB최적화, DB생성) ▸ 각종 로그관리 기능 (백업관리, 호스트 설정, 사용자 관리, 옵션설정)

LogCOPS™ 로그 템플릿

Enterprise Log Analysis and Management System

매핑 템플릿 (Mapping Template)	로그파일을 로그DB로 변환하기 위한 매핑 형식을 기술한 파일	그룹(Group) 기본(Basic) 사용자 (User-defined)	**패턴 템플릿** (Pattern Template)	로그DB에서 특정 공격패턴을 검색하기 위한 패턴 검색 형식을 기술한 파일	패턴(Pattern) 그룹(Group)
검색 템플릿 (Search Template)	로그DB를 검색하기 위한 검색 형식을 기술한 파일	기본(Basic) 응용 (Application) 사용자 (User-defined)	**보고서 템플릿** (Report Template)	로그DB를 원하는 형태의 보고서를 생성하기 위한 보고서 형식을 기술한 파일	기본(Basic) 사용자 (User-defined) 그룹(Group)

Enterprise Log Analysis and Management System

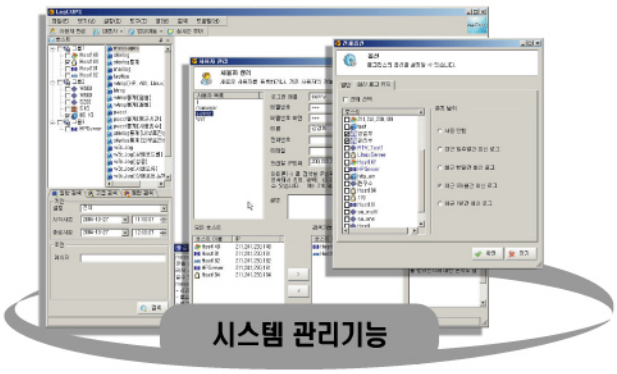
LogCOPS™

아직도 24시간 모니터링하고 계십니까?

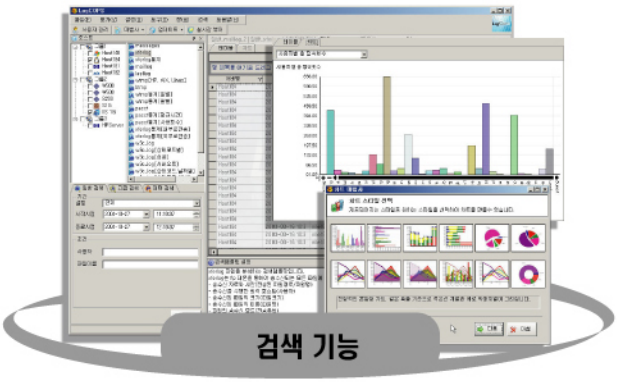
엔터프라이즈 환경에서 여러 호스트들이 생성하는 로그를 한대의 전용 호스트에서 통합하여 관리하는 기능을 가지고 있는 통합로그분석 전문도구는 끊임없이 로그파일들을 지켜봐야만 하는 비효율적인 업무를 가장 효율적이고 편리하게 분석 관리해줍니다.

LogCOPS™ 실행화면

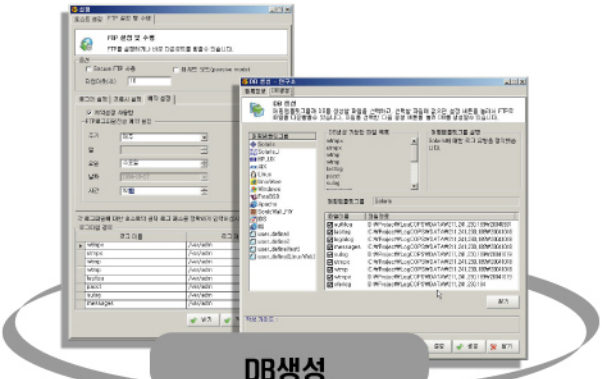
Enterprise Log Analysis and Management System



시스템 관리기능

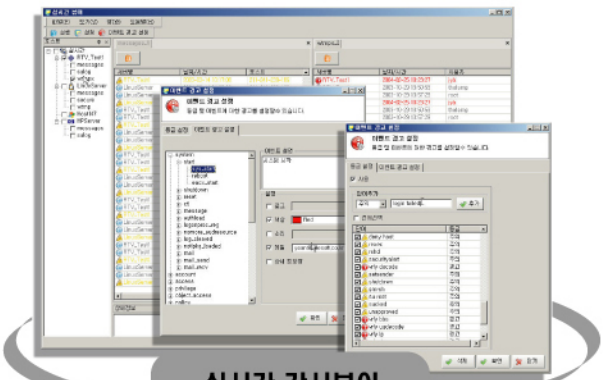


검색 기능

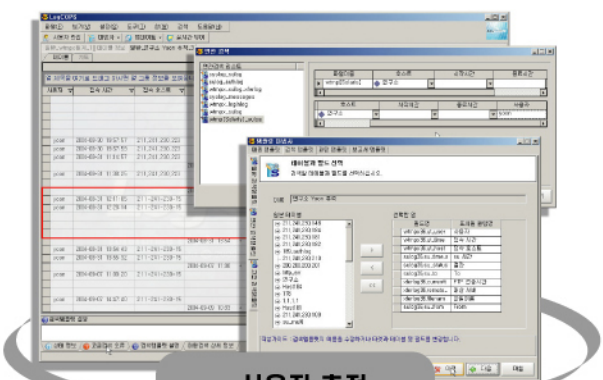


DB생성

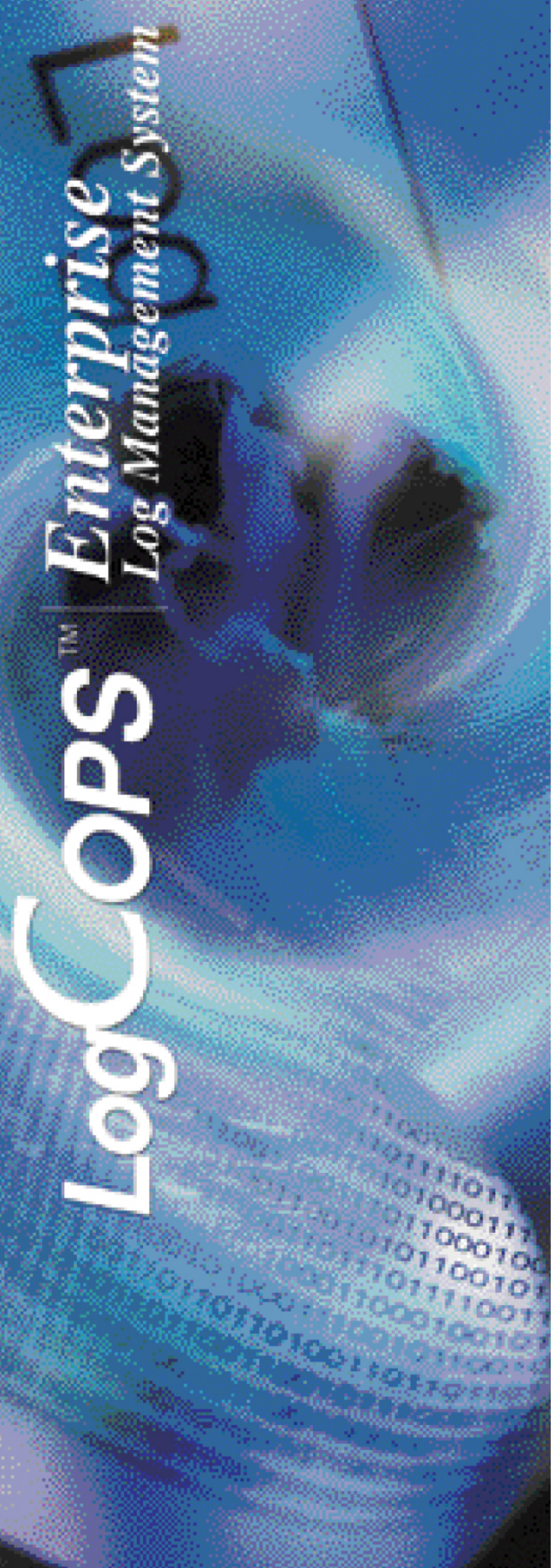
탬플릿과 보고서



실시간 감시뷰어



사용자 추적



정보보호의 대중화! 나일소프트가 함께 하겠습니다.

(주)나일소프트
NileSOFT Ltd.

150-870 서울시 영등포구 여의도동 13-4 동우국제빌딩 4층
전화 : 021 783-0961 팩스 : 02 783-0963
e-mail : webmaster@nilesoft.co.kr