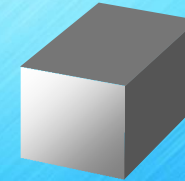


웹 침해사고 징후분석을 위한 “BlackBox”



제품 소개서

2011

Table of Contents

▶ I. 회사 소개

II. 현황 및 필요성

III. 제품 소개

1. 회사 소개

| | |
|-----------|--|
| 회 사 명 | (주)패닉시큐리티 |
| 설 립 일 자 | 2004년 05월 01일 |
| 주 요 구 성 원 | 정보보호전문업체(정통부 지정) 재직 경력 및 언더그라운드 해커로 구성 |
| 보 유 기 술 | 모의해킹, 웹 어플리케이션 취약점 분석, 취약점 코드 설계, 무선보안 기술 |
| 연 락 처 | 신 용 재 이사 Tel : (017) 549-5765, (02) 2027-2890 E-mail: kstep@panicsecurity.com |
| 홈 페이지 | http://www.panicsecurity.com |
| 특 이 사 항 | <ul style="list-style-type: none">▪ 구성원 전체가 해커 출신이며, 최고 수준의 기술적 취약점 분석 능력 보유▪ 다수의 모의해킹 및 기술적 취약점 분석 프로젝트 수행 경험<ul style="list-style-type: none">- 국가 K기관 : 무선랜 보안 컨설팅 수행 경험- L사 쇼핑몰 : 모의해킹을 통한 기술적 취약점 분석 수행 경험 등 다수▪ 웹 어플리케이션 취약점 점검 도구 PS ScanW3B 개발 – 국내 최초 개발. 국내 점유율 1위▪ 인터넷 뱅킹의 메모리 해킹 위험성 발표 및 최초 시연. 방지 대책 발표 (PS TVS)<ul style="list-style-type: none">▪ 금융보안연구소 및 금융결제원에서 최초 발표 / 시연▪ 국제해킹대회 Defcon Ctf에서 아시아 1위로 온라인 예선전 통과 (08년 5월)<ul style="list-style-type: none">▪ 미국 라스베가스에서 전세계 8개팀이 겨루는 본선 대회에서 전체 4위 (08년 8월) |

2. 회사 연혁

| 기간 | 회 사 연 혁 | 해당 기관 |
|-------------|---|--------|
| ▪ 2004. 05. | 주식회사 패닉시큐리티 설립 | N/A |
| ▪ 2004. 07. | 대법원 등기정보시스템 보안컨설팅 | 대법원 |
| ▪ 2004. 09. | 국내 최초 웹 어플리케이션 취약점 자동화 분석 도구 PS ScanW3B 출시 | |
| ▪ 2005. 04. | 벤처기업 지정 (신기술 기업) | 기술보증기금 |
| ▪ 2005. 05. | 무선랜 (Wi-Fi) 침입탐지(IDS) 보안장비 개발 과제 | 중소기업청 |
| • 2006. 03 | 금융감독원 연간 유지보수 계약 - 분기별 취약점 분석 | 금융감독원 |
| • 2006. 04 | 한국정보보호진흥원(KISA) 연간점검 - 분기별 취약점 분석 | KISA |
| • 2006. 07 | “홈페이지 개발자를 위한 훈련공간” 구축 위탁과제 | KISA |
| • 2006. 09 | 국가정보원 보안 적합성 검토 필 | 국가정보원 |
| • 2007. 03 | 벤처 기업 재 지정 | 기술보증기금 |
| • 2007. 05 | 인터넷 뱅킹의 메모리 해킹 최초 발표 및 시연. 대책 발표 (PS TVS) | 금융감독원 |
| • 2008. 05 | 국제 해킹대회 온라인 예선 국내 1위로 본선 진출 (Taekwon-V 연합팀) | DEFCON |
| ▪ 2008. 08 | 국제 해킹대회 본선 세계 4위 (Taekwon-V 연합팀) | DEFCON |

3. 주요 사업 내역

정보보호 컨설팅 사업 (기술적 취약점 분석에 중점)

- 서울대, KAIST 출신 및 정보보호전문인력(정보통신부 지정)경험이 있는 해커출신 연구원으로 구성.
- 다수의 모의해킹(PT, Penetration Test) : KISA, 금융감독원, 은행/보험/카드, 통신, 홈쇼핑 및 다수의 공공기관
- 컨설팅 등의 단순 유선랜 기반 모의해킹 뿐만이 아닌 특화된 정보보호 컨설팅 수행.

국내 최초의 웹 어플리케이션 취약성 진단 도구 개발 및 상용화

- PS ScanW3B은 국내 최초의 순수 국내기술로 제작된 웹 어플리케이션 취약성 진단 도구이며, 해커출신 전문
- 컨설턴트가 개발에 참여하여, 웹 어플리케이션 자동화 취약성 진단 및 분석도구를 통한 현실적 대안의 제시.
- 국내 최대 레퍼런스 보유 – 금융, 통신, 공공 시장에서 압도적인 점유율

국내 최초 ActiveX 취약점 진단 도구 개발 및 상용화

- 국내 웹환경의 특징은 여러가지 ActiveX를 포함하고 있으나, 이에 대한 취약점 검증은 거의 이루어지지 않고 있음
- 취약한 ActiveX가 있을 경우, 홈페이지를 방문한 사용자는 자신도 모르게 악성코드가 PC에 설치될 수 있음
- 국내 최초로 ActiveX의 취약점 점검을 자동화 한 도구

블랙박스 – 웹 침해사고 징후분석 솔루션

- 대용량의 웹로그를 중앙에서 수집/보관/관리
- 웹 해킹의 경우 6개월 ~1년 이전부터 여러가지 웹사이트 정보 분석이 이루어지며 정확한 해킹 시작 시점과 해킹의 피해 범위를 파악하기 위해서는 웹로그 분석이 필수적
- 대부분의 기관은 웹로그 양이 방대하므로 오랜기간 보관을 하지 않으며, 보관한다 하더라도 분석에 너무 많은 시간이 소요됨

Table of Contents

I. 회사 소개

.....

▶ II. 현황 및 필요성

.....

III. 제품 소개

.....

1. 제품 배경

✓ 웹서버 해킹 사고 증대

| 공격 | 종류 |
|----------------------------|--|
| 수동적 공격(Passive Attack) | <ul style="list-style-type: none"> 네트워크 트래픽 분석 네트워크 패킷 캡처 개인정보 (패스워드, ID, 신용카드 등) 훔쳐보기 인증정보 훔쳐보기 |
| 능동적 공격(Active Attack) | <ul style="list-style-type: none"> 악성코드 삽입 인증정보 가로채기 네트워크 패킷 수정 후 재전송 서비스 거부 공격 백도어 전송 |
| 근거리 공격(Close-in Attack) | <ul style="list-style-type: none"> 물리적으로 근접한 거리에서 공격 네트워크 시스템 장비들을 수정하거나 획득하기 위한 공격 |
| 내부 공격(Insider Attack) | <ul style="list-style-type: none"> 내부 공격자의 위협비인가 정보 접근, 수정, 파괴 정상적인 사용자의 접속 방해 내부 공격자의 부정행위 |
| 분산 공격(Distribution Attack) | <ul style="list-style-type: none"> 소프트웨어나 하드웨어가 변조되어 배포될 때 악의적인 코드(백도어)들을 탑재하여 공격 비인가 정보 접근 |

웹서버 해킹해 대출광고.. 수수료 수십억 챙겨

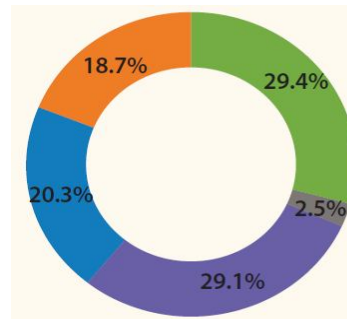
(앵커) 웹서버를 해킹해 수천만 통의 대출 스팸광고로 바꾼다고



그림 2 관리자 페이지에 대한 공격으로 추정되는 로그 0

해킹에 의해 다른 코드가 정상적인

해킹에 의해 다른 코드가 정상적인



해킹사고 접수·처리 건수 유형별 분류

- 스팸릴레이 29.4%
- 피싱 경유지 2.5%
- 단순침입시도 29.1%
- 기타해킹 20.3%
- 홈페이지 변조 18.7%

참조 <인터넷 침해 대응센터

2010년 12월 인터넷침해사고 동향 및 분석 월보>

2. 현황 - 부족한 웹보안 대응 체계

✓ 웹보안 솔루션의 한계



✓ 대용량 웹로그 : 6개월치? 1년치?



3. 웹로그 관리 현황

✓ 현행 웹로그 관리의 문제점

매일 쌓이는
대용량의 웹 로그

- 하드디스크 용량초과로 인해 주기적으로 삭제하고 있음

웹서버 별 독립적으로
저장되는 웹 로그

- 서버별로 산재되어 관리가 되지 않음
- 서버별 담당자가 나뉘어질 경우, 로그 관리주기도 다름

같은 HW에 여러개의 웹 사이트가
운영되는 경우 (가상호스트)

- 하나의 사이트가 침해사고를 당하는 경우 그에 파생되어 다른 웹 사이트에도 침해사고를 쉽게 당하는 경우가 빈번함



웹로그의 방대한 양으로 단순
보관시 추후 분석이 거의 불가능

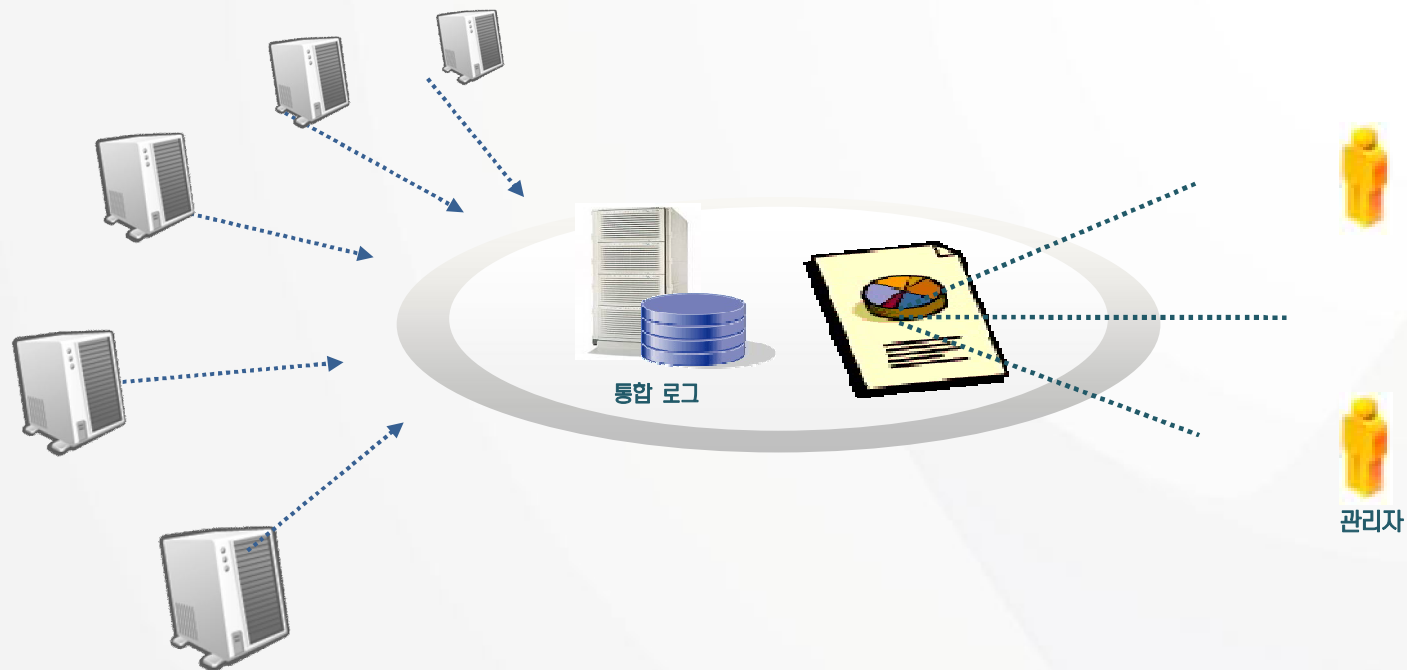
- 일반적으로 최소 6개월 이상의 로그보관 및 관리가 필요
- DDos 공격 등을 통해 평소보다 과대한 로그 발생시, 로그 관리에 장애요소가 됨

**“정보자산측면에서
로그의 가치 결여”**

웹서버별 전사적인 정책 전무(관리주기/포맷/정책)
로그의 활용성 저하

4. 웹로그의 가치

✓ 웹로그의 통합 관리



“로그 = 정보자산”

분산된 웹로그의 취합을 통한 일관된 로그 정책 수립
방대한 양의 웹로그 분석 환경 제공
웹로그 분석을 통한 사용자의 위험 행위 인지

5. 웹 로그 활용의 필요성

✓ 웹 로그 관리/분석이 핵심



웹 로그의 통제

- 압축 보관을 통한 최적화 저장
- 향후 로그 분석을 위한 데이터 베이스화
- 로그서버 구성을 통해 분산된 웹 로그의 통합관리
- 여러 웹 서버의 로그 연관 관계를 파악
- 로그 백업 및 삭제에 대한 일괄 정책 수립



위험도 분석 향상

- 기 구축되어 있는 ISP/웹 방화벽의 방어력이 기대치에 못 미침(보안레벨을 높이면 QOS 저하)
- IPS/웹 방화벽의 **분석력 취약을 보강**
- 보안 장비를 통과하여 웹서버에 요청된 실제로그를 기반으로 징후를 탐지하여, 각 **장비별 보안정책 패턴 정책을 강화**



사후 조치 분석

- 보안 사고 발생시, 과거 데이터 분석을 통한 공격 유형 및 유입 경로 파악
- **신속한 사고 경위 파악**을 통해 취약점 보완 및 보고서 작성



사전 징후 분석

- 주기적인 로그 분석을 통해 **의심 행위 탐지** 및 대응책 제공
- **개별 웹로그가 아닌, 기관 내 전체 웹로그 분석에 의한 포괄적 위험도 분석**
- 위험에 대한 사전 대응으로 웹서버 안전성 향상



“일관된 정책에 의한 로그 수집 및 저장”
“위험 요소에 대한 효과적인 검색 및 분석”

Table of Contents

I. 회사 소개

.....

II. 현황 및 필요성

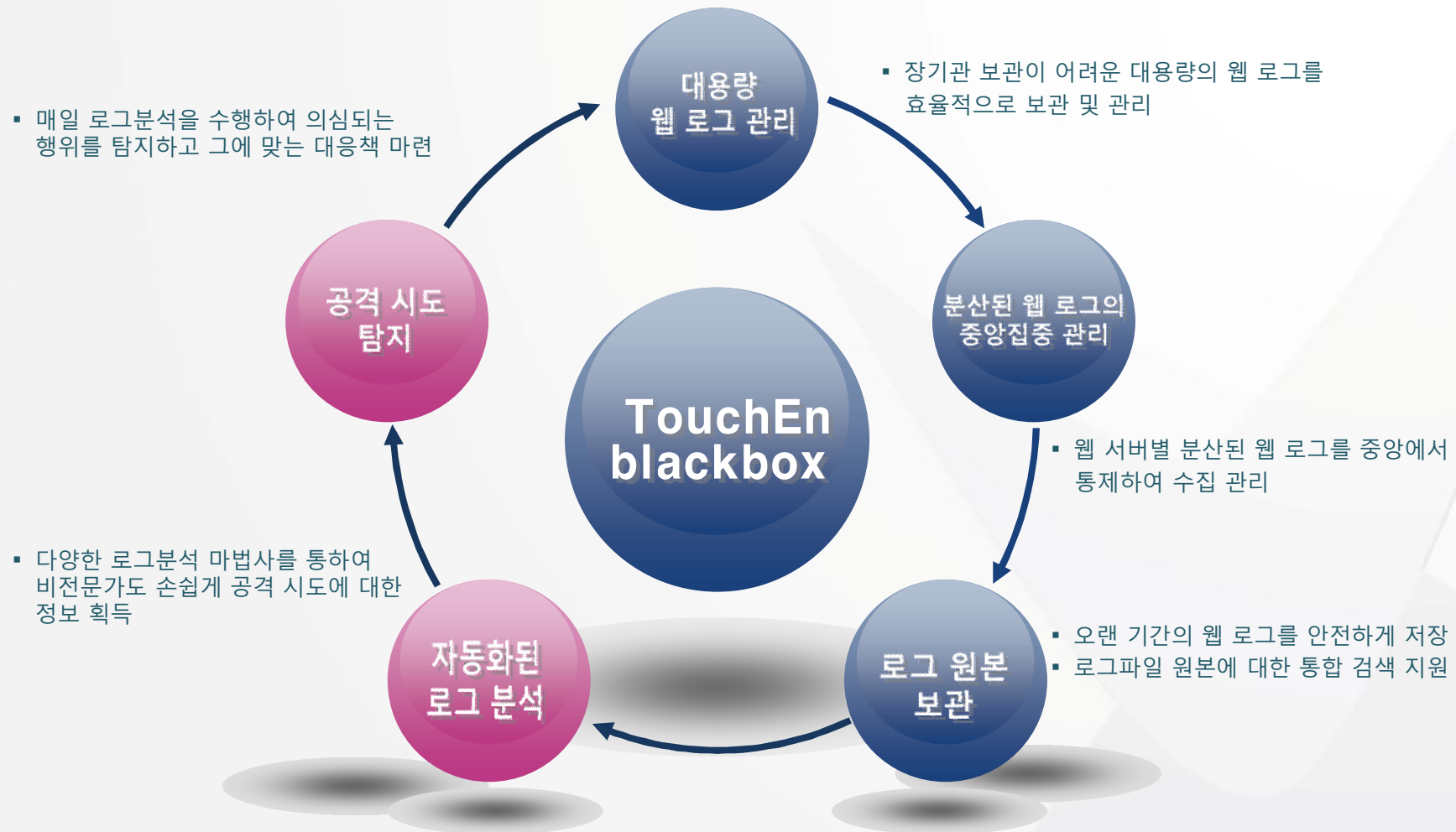
.....

▶ III. 제품 소개

.....

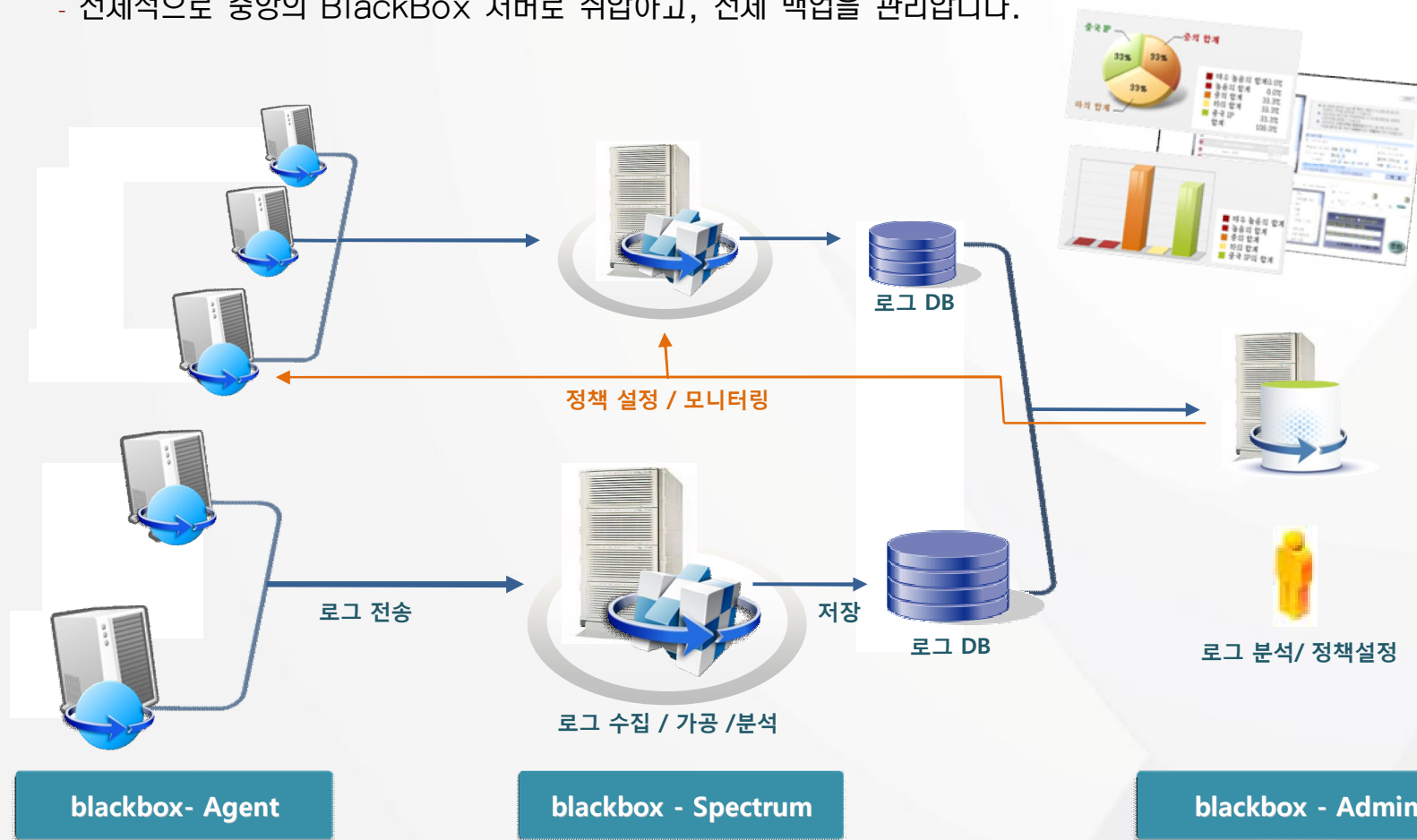
1. Black Box 제품 개요

✓ Blackbox 개요



2. BlackBox 전체 구성도

- 여러 대의 웹서버에 대한 로그를 그룹별로 취합할 수 있습니다. 네트워크 환경에 따라 구성을 변경할 수 있습니다.
- 전체적으로 중앙의 BlackBox 서버로 취합하고, 전체 백업을 관리합니다.



3. BlackBox 주요 구성 모듈

BlackBox Admin Server

- 블랙박스 Admin 정책 서버
- 압축된 로그파일 원본을 대용량 저장공간에서 관리하고, 통합 검색 제공
- 로그원본에 대한 인덱스 정보 및 공격시그니처 관리
- 웹서버에 설치된 전체 Agent 정책을 중앙에서 통제하고 관리함

BlackBox Spectrum Server

- 블랙박스 스펙트럼 서버
- 웹서버의 Agent와 블랙박스 정책 서버의 정책 및 수집 기능 대행
- 네트워크 환경의 물리적 제약에 따라 전체 블랙박스 시스템의 재배치가 가능하도록 지원

CASE1 통합로그가 구축 되어 있을 경우

- 통합로그 시스템에서 BlackBox 스펙트럼 서버로 전달

CASE2 통합로그가 구축 되어 있지 않을 경우

- 웹서버에 Agent를 설치하여 BlackBox 스펙트럼 서버로 전달

4. 주요 기능 및 특징

✓ 제품의 특징

1

전체 웹서버의 웹로그를 연관 분석하여, **위험 징후에 대해 사전도출**

2

중앙 집중식 로그 정책 수립으로 관리 편의성 향상
제품 모니터링 및 로그 수집 현황 제공으로 안정적인 운영 환경 보장

3

로그 분석 및 정제화 단계에서의 신속한 분석 엔진 / 정제화된 로그의 상관 관계 분석을 통한
강력한 탐지 엔진 – **이중화 엔진 탑재**

4

위험 징후 탐지시 SMS / e-mail 를 통해 관리자에게 신속하게 **위험 정보 알림**

5

네트워크 기반의 **자동 웹로그 수집** 및 수개월~수년에 이르는 기간의 로그를 백업
테라바이트 급 **대용량 로그 보관**을 통해 웹서버 로그의 중앙집중적 관리 시스템

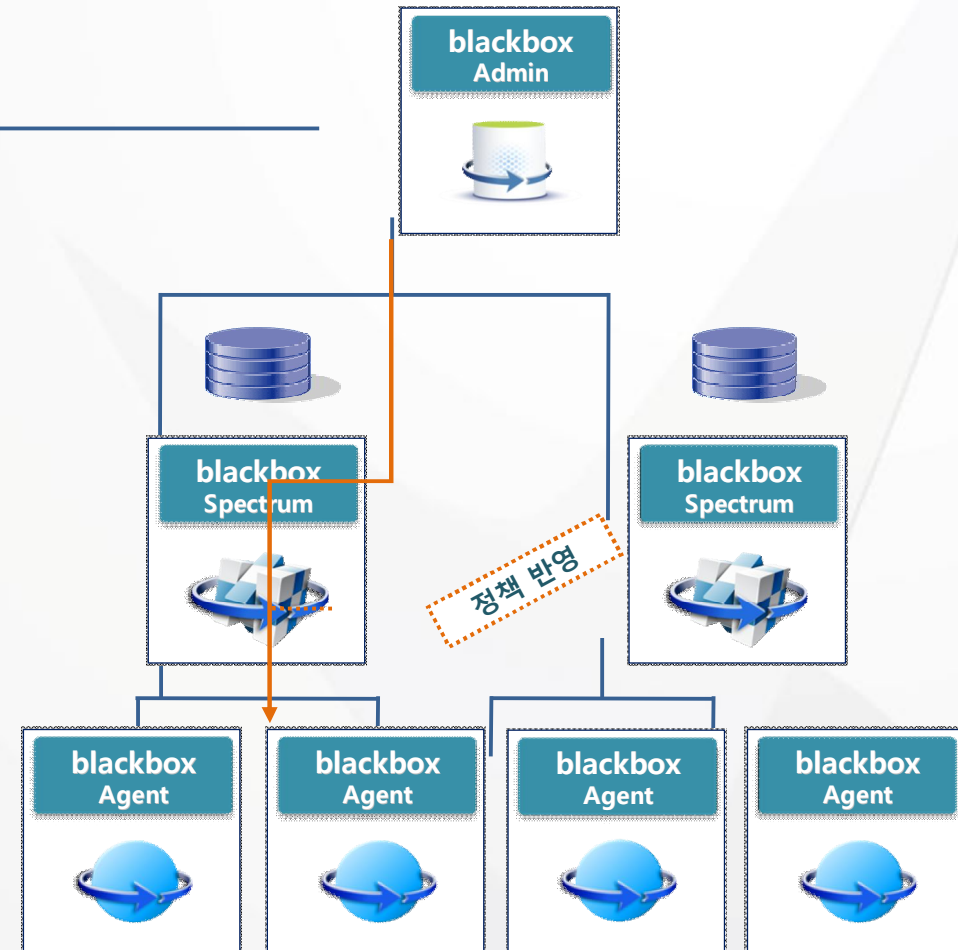
6

웹서버의 성능 및 안정성에 영향을 미치지 않는, **독립 프로세스형** 로그 수집 Agent 지원
환경에 따라 별도의 설치가 없는 Agent-less 방식 지원

4. 주요 기능 1

✓ 로그 검색 및 정책 설정

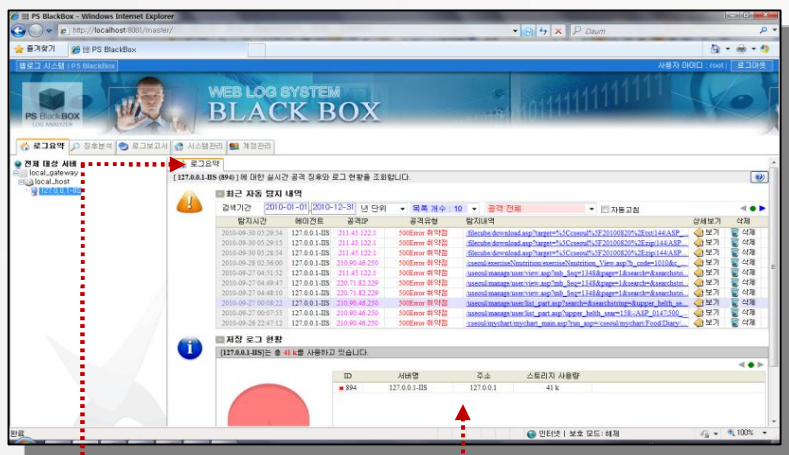
- 웹기반 패턴 검색 도구 - 웹 로그에 대해서 다양한 검색기능을 지원
- 웹기반 정책 설정 도구 - 수집 대상 서버 및 로그 수집 주기 설정



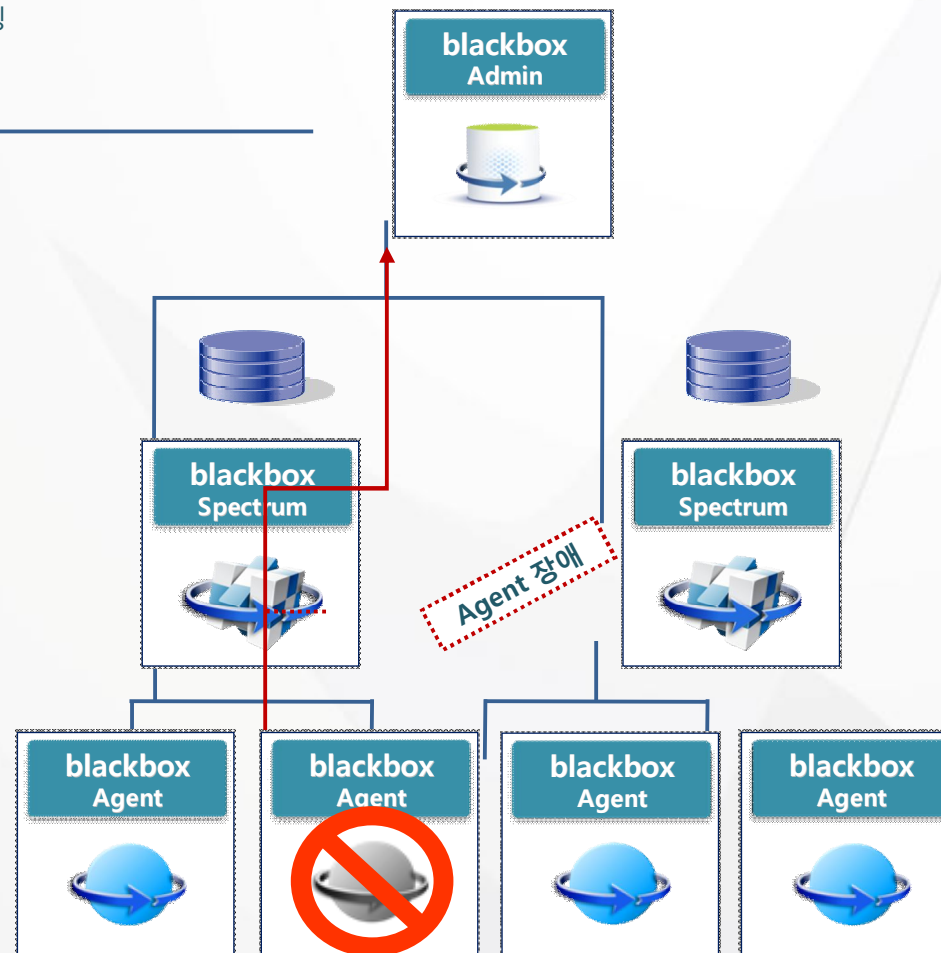
4. 주요 기능 2

✓ 로그 수집 모니터링 및 현황

- 로그 수집 모니터링 - 로그 수집의 안정적인 운영을 위한 제품 상태 모니터링
- 로그 수집 현황 - 웹서버별 전송된 로그 크기/시간/결과에 대한 모니터링



- 제품 모니터링
- 웹서버별 로그 수집 현황



PANIC  SECURITY

- 웹 로그에 대해서 다양한 검색기능을 지원

결과 내 분석 | 0.67, 기간:2010-07-01~2010-07-15 / 개수:232

» 사용자 옵션 설정

분석 옵션 | 클라이언트 IP | 124.227.141.230 | [추가] [삭제]

| 탐지시간 | 에이전트 | 공격IP | 공격유형 | 탐지내역 | 상세보기 |
|---------------------|---------------|-----------------|------------|---|------|
| 2010-07-08 17:43:56 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /gtk/news/news_view.php?idx=7755%20aND%208%3D8 | [보기] |
| 2010-07-08 17:43:56 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /gtk/news/news_view.php?idx=7755%20aND%208%3D3 | [보기] |
| 2010-07-08 17:44:00 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/att/att_view.php?idx=1008&ba_gubun=2010%20aND%208%3D8 | [보기] |
| 2010-07-08 17:44:00 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/en/hallyu_view.php?idx=1009%20aND%208%3D8 | [보기] |
| 2010-07-08 17:44:01 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/en/hallyu_view.php?idx=1009%20aND%208%3D3 | [보기] |
| 2010-07-08 17:44:02 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/att/att_view.php?idx=1008&ba_gubun=2010%20aND%208%3D3 | [보기] |
| 2010-07-08 17:44:03 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/att/att_view.php?idx=1008&ba_gubun=2010%27%20aND%20%278... | [보기] |
| 2010-07-08 17:44:04 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/shop/districts_view.php?idx=7842%20aND%208%3D8 | [보기] |
| 2010-07-08 17:44:05 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/shop/districts_view.php?idx=7842%20aND%208%3D3 | [보기] |
| 2010-07-08 17:44:04 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /index.php?ptIdx=2%20aND%208%3D8 | [보기] |
| 2010-07-08 17:44:06 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/att/att_view.php?idx=1008&ba_gubun=2010%27%20aND%20%278... | [보기] |
| 2010-07-08 17:44:06 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /index.php?ptIdx=2%20aND%208%3D3 | [보기] |
| 2010-07-08 17:44:07 | 115.84.164... | 124.227.141.230 | SQL인젝션 취약점 | /cav/att/att_view.php?idx=1008&ba_gubun=2010%09aND%098%3D8 | [보기] |

5. 도입 효과 1

BlackBox 적용



BlackBox 미적용

- ① 에이전트 작업요청
- 백업 시기 확인
 - 주기적 반복 요청

자동화된
업무플로우

블랙박스 서버

- ② 에이전트 작업명령
- 백업 대상 파일 목록 지정
 - 압축 방식 및 HMAC 정보 지정
 - FTPS 인증 및 백업 정보 지정
 - 백업 후처리(파일삭제 등) 지정

- ④ 로그 처리
- 압축 원본의 무결성 확인 및 자동 분류
 - 웹로그의 자동 파싱
 - 중요 URL 및 공격 시도 분류

⑤ 로그 검색

- 웹로그 원본의 통합 검색
- 전체 웹서버들에 대한 패턴 검색
- 장기간에 걸친 로그를 통해 이상징후 파악



“2년 전부터 /hack.asp가 존재했고,
이를 통해 수개월간 중국 IP를 통해
데이터 유출이 이루어진 것으로
파악되었습니다.”

① 웹서버별 개별 백업

- 웹서버마다 다른 백업 주기/형식
- 웹서버 용량 한계에 따른 임의삭제
- 담당자 업무 이관시 백업정책 변경
- 웹로그 관련 보안정책 지시 및 이행여부 파악 곤란

② 과거 웹로그 검색

- 웹서버별 개별 로그위치 파악
- 웹서버별 로그양식 파악
- 로그 종류별 개별 검색 작업 및 검색결과의 취합
- 웹로그를 찾을 수 없거나, 삭제된 경우에 추적 불가능

③ 침해사고에 대한 문제 파악

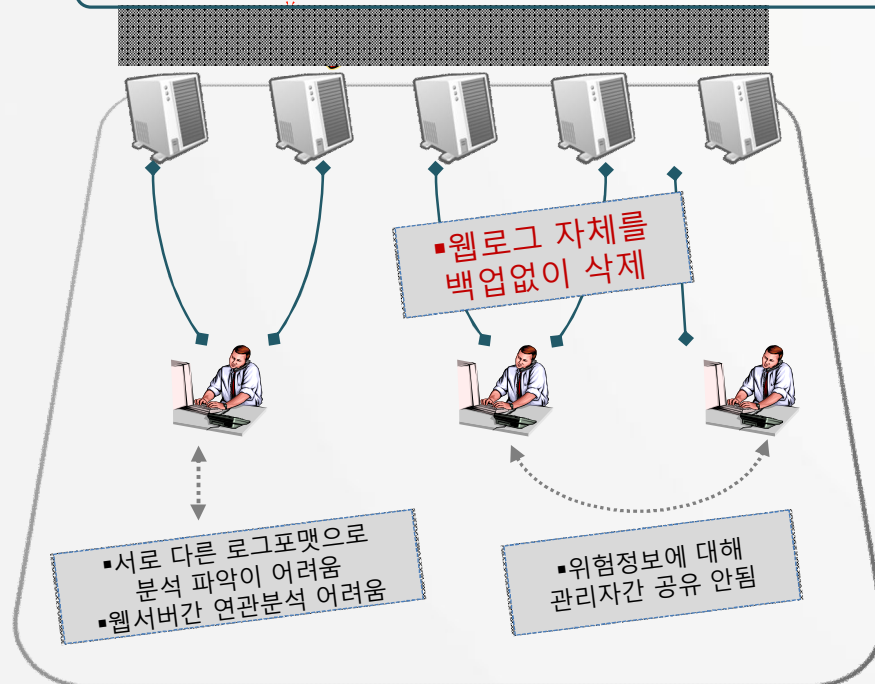
- 과거 전체 웹서버 로그에 대한 분석에 긴 시간이 소요
- 신속하고 정확한 분석이 어려움

“데이터의 정확한 유출 경로 확인을 위해
최근 수주동안 분석이 이루어졌으며,
언제부터인지 모르지만 /hack.asp가
중국에서 최근 수차례 접근되었습니다.”

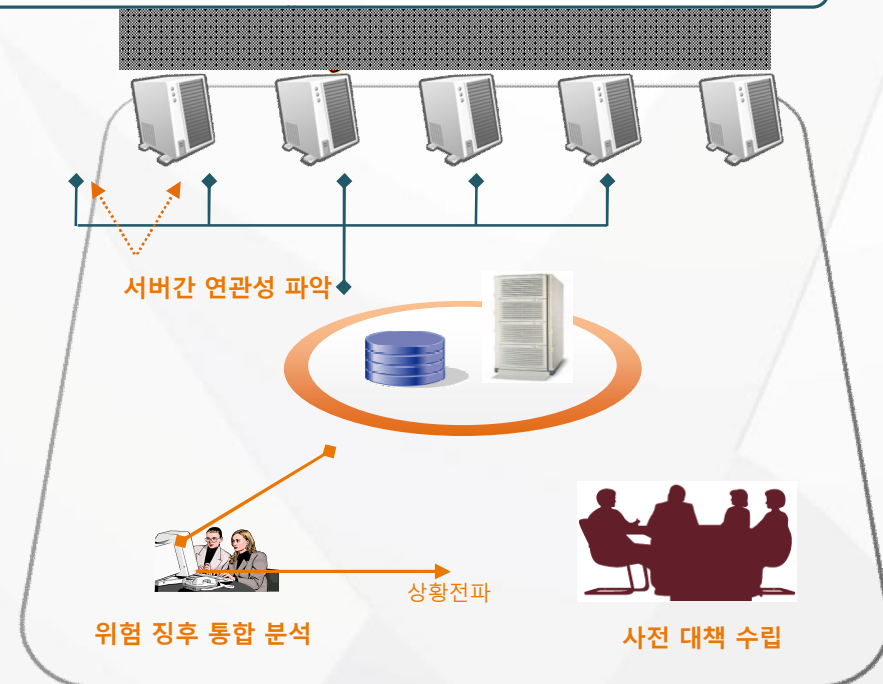
5. 도입 효과 2

✓ 사전 위험 분석

해킹을 위해 6개월에서 1년전부터 웹 사이트에 대한 다각적인 정보 분석이 진행



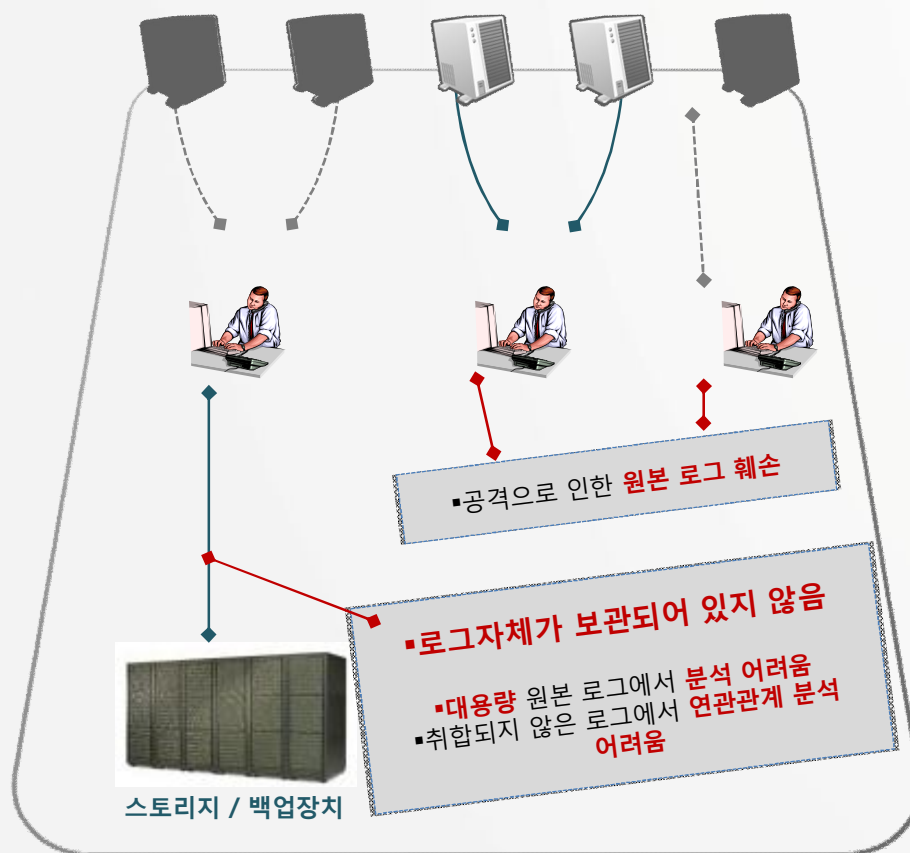
도입 전



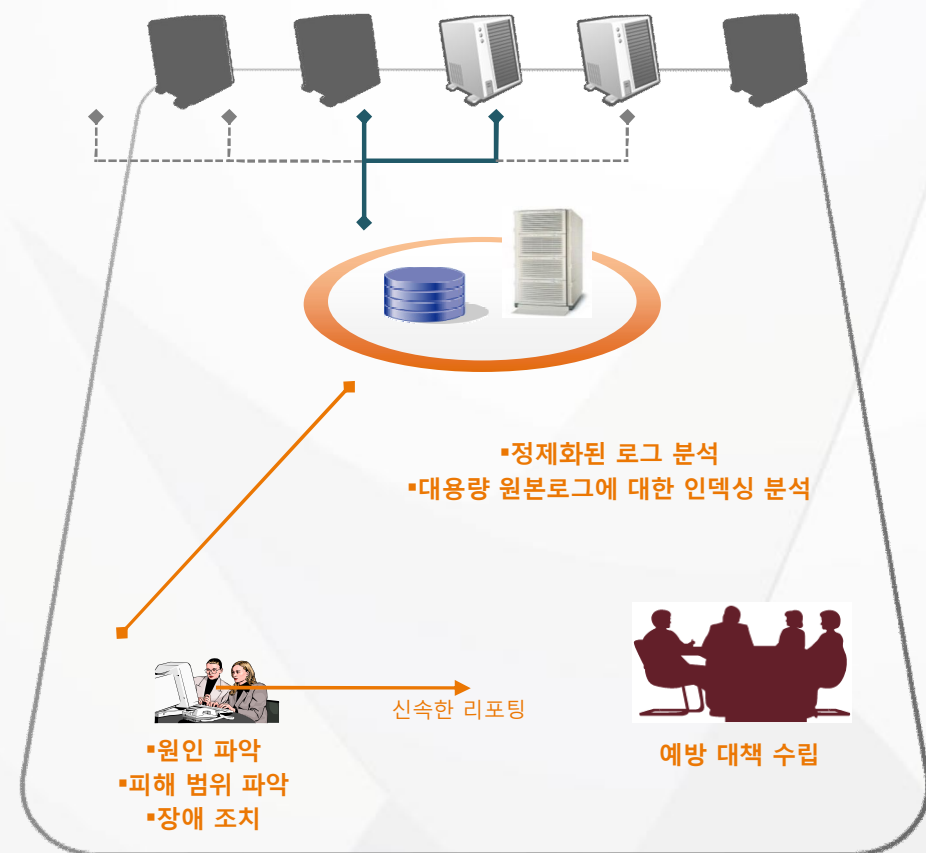
도입 후

5. 도입 효과 3

✓ 사후 대응 분석



도입 전



도입 후

6. 기능 및 효과 요약

| | 구 분 | 기 능 | 효 과 |
|-------|------------------------|--|--|
| 사후 대응 | 가공로그 통합보관 | <ul style="list-style-type: none"> - 여러대의 웹서버에 분산된 로그를 모아서 관리 - 로그 압축 / 전송 등의 스케줄링 - 개별 관리되던 로그를 자동으로 수집/통제 | <ul style="list-style-type: none"> - 신소한 침해사고분석 대응 - 전체적인 분석 용이 |
| | 공격 시도 및 피해 범위 분석 | <ul style="list-style-type: none"> - 원본 로그와 인덱싱 정보로 구분되어 관리 및 보관 됨 - 공격 유형 별, 의심 IP 별, 공격 기간 별 다양한 분석 마법사 제공 | <ul style="list-style-type: none"> - 막대한 양의 로그를 분석해야 하는 시간과 비용 절감 - 비전문가도 손쉽게 분석 |
| | 과거 웹로그 검색 | <ul style="list-style-type: none"> - 원본 로그는 변경 되지 않도록 압축 및 안전하게 보관 - 빠른 분석을 위해 별도 인덱싱 정보 활용 | <ul style="list-style-type: none"> - 법적인 증거자료 마련 |
| 사전 대응 | 공격 탐지 | <ul style="list-style-type: none"> - 의심되는 여러가지 시도를 탐지하여 사전에 대응책 마련 - 공격 패턴 업데이트 | <ul style="list-style-type: none"> - 공격 시도의 징후를 미리 인지하여 적절한 대응책 마련이 가능 |
| | 리포트 | <ul style="list-style-type: none"> - 매일/매주/매월 등의 리포트 생성 | <ul style="list-style-type: none"> - 여러가지 통계 자료로 위험 IP 등의 정보 취득 |

7. 적용 기술

공격 탐지 기술

웹 해킹 및 취약점 점검으로 축적된 공격 탐지 기술
국내 최초 웹취약점 점검 도구의 개발 경험 및
다수의 모의해킹 시연 기술 보유

연관성 분석 기술

웹 서버 사이의 로그 연관성 분석을 통하여
보다 신뢰성 있는 공격 징후를 포착.

사고 분석 기술

침해사고 발생 시 오랜시간 백업된 대용량의 로
그파일을 (형식에 관계없이) 신속하게 분석 – 이
를 위해 주기적인 가공로그 확보

- 웹 보안을 위한 여러가지 대책을 보강 : **상시 웹로그 분석**

→ 침해 사고가 나기 전에 징후를 포착하여 더 견고한 보안 룰을 설정할 수 있게 함 !

→ 만약 침해 사고가 나더라도, 피해 범위와 원인을 분석할 수 있는 기본 백데이터를 제공 함



(주)패닉시큐리티는
고객의 만족과 보안 향상을 위해
최선의 노력을 다 하겠습니다.

감사합니다.

<http://www.panicsecurity.com>