PANIC SECURITY

웹 서비스 해킹징후 분석 솔루션

PS BlackBox

2015

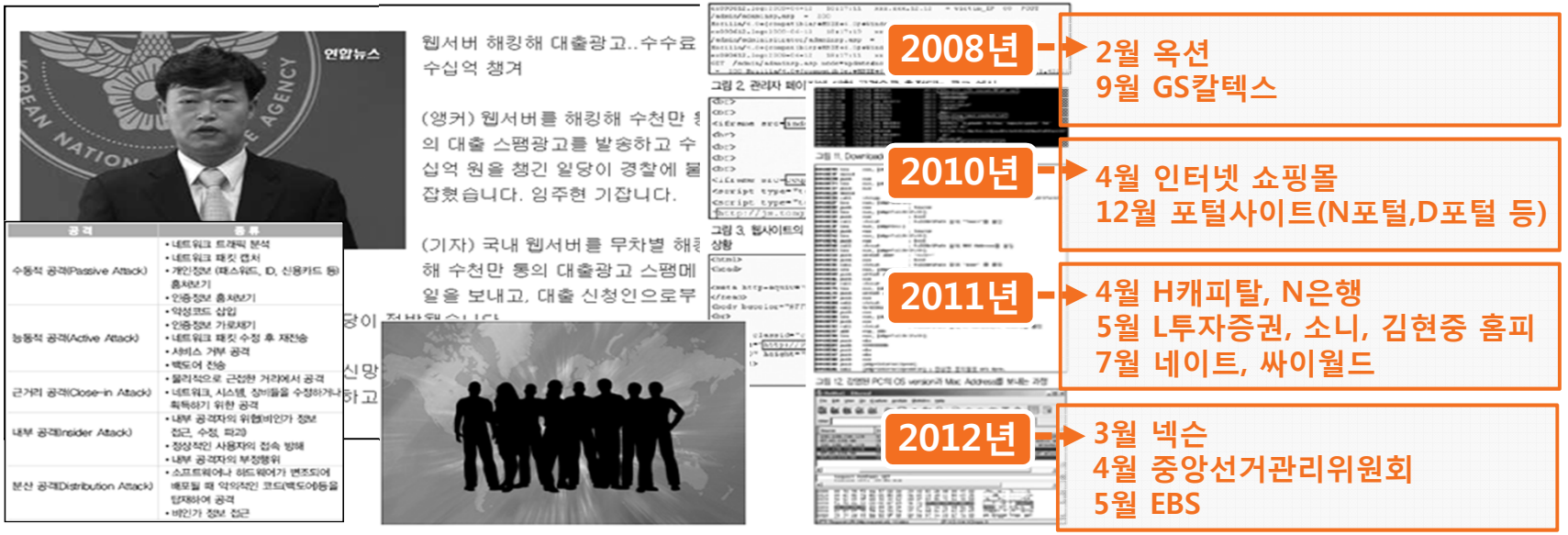
㈜ 패닉시큐리티

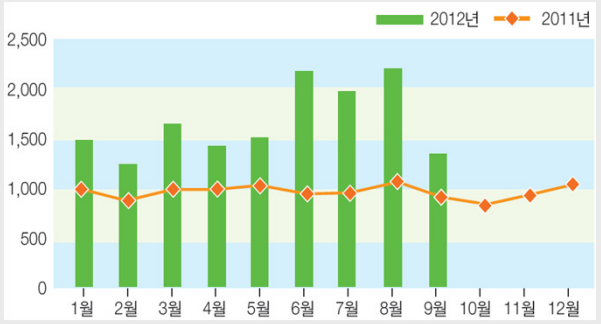
CONTENTS

I. 웹 해킹 징후 분석 개요

1. 웹 서버 해킹 사고 증대

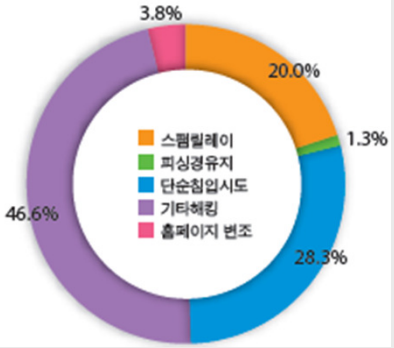
각종 웹 해킹 사고가 증가하고 있어 웹 서버 보안의 중요성이 강조되고 있습니다. 최근 웹 서버 해킹 사고가 언론에 자주 보도되고 있는데, 그 원인은 웹 서버가 사회적으로 중요한 기능을 담당하게 됨에 따라 해커들의 관심도 늘고 있습니다.





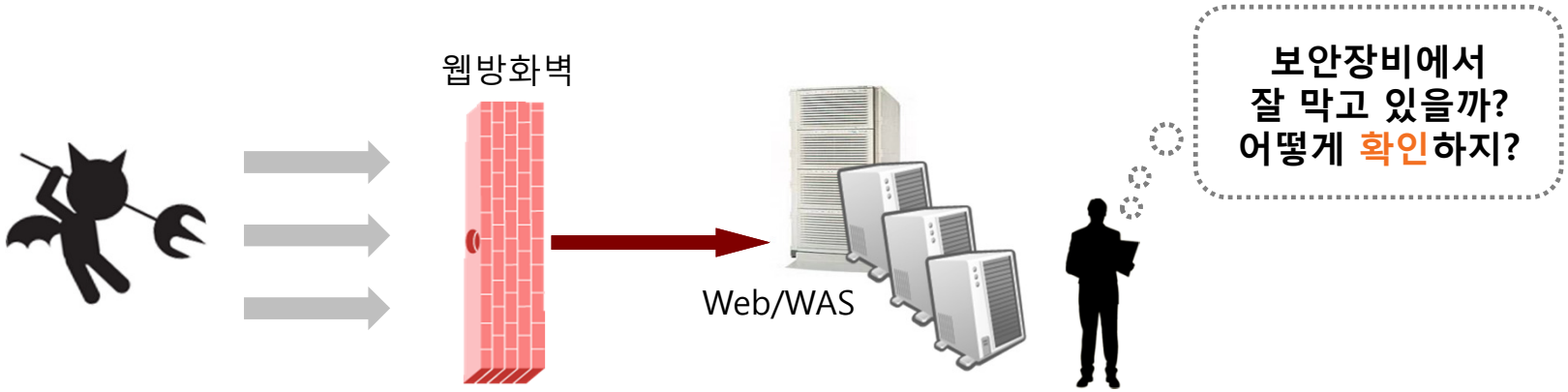
단순침입시도+기타해킹신고 처리

구분	건수
스캠릴레이	434
피싱 경유지	29
단순침입시도	614
기타해킹	1,013
홈페이지 변조	83
총계	2,173



참조
<인터넷 침해 대응센터
2012년 인터넷침해사고 동향 및 분석 월보>

2.1 웹 서비스 보안장비의 한계



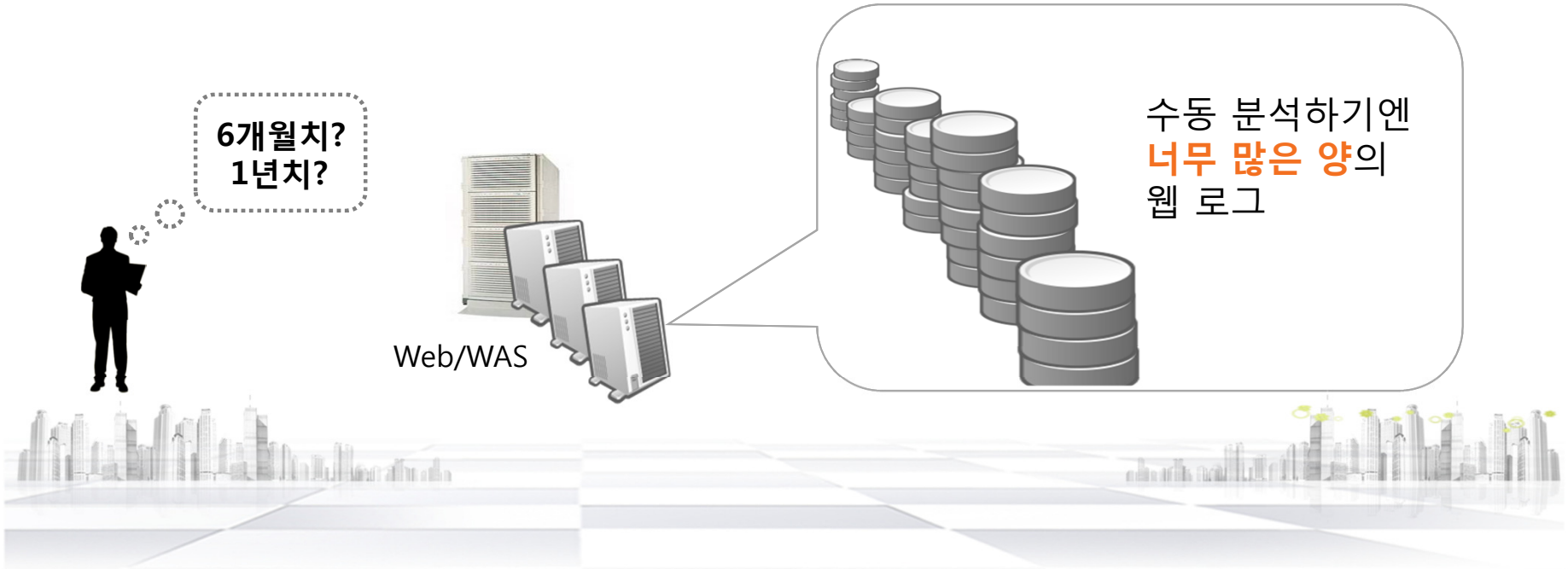
웹 서버 해킹 사고의 지속적인 증대

- 방법 : 홈페이지 변조, 단순침입시도, 피싱 경유, 스팸릴레이, 기타해킹 등
- 사례 : H당, T당, P정부, P청, M업체, J언론, 티아라, C호텔, 메이플스토리, 디아블로, 아르고

웹 서비스 품질(QOS) 보장의 한계

- 실시간 처리를 해야 하므로, 보안 패턴 우회 공격에 대한 심도 있는 분석 한계

2.2 대용량 로그의 법적/제도적 규제



정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행 규칙

- 침해사고방지를 위한 보안프로그램의 설치 및 운영

개인정보의 기술적/관리적 보호조치 기준 (지식경제부)

- **최소 6개월 이상**의 접속기록을 보존 관리하여야 함

2.3 현행 웹 로그 관리의 문제점

매일 쌓이는 대용량의 웹 로그	▪ 하드디스크 용량초과로 인해 주기적으로 삭제하고 있음
웹 로그별 정책상이	▪ 웹 서버 별 독립적으로 웹 로그 관리 ▪ 서버 별 담당자가 다른 경우도 있고 로그 관리 정책도 다름
같은 서버에 여러 개의 웹 사이트가 운영	▪ 하나의 사이트가 침해사고를 당하는 경우 그에 파생되어 다른 웹 사이트에도 침해사고를 쉽게 당함

"정보자산측면에서 웹 로그의 활용 결여"

웹 서버 별 전사적인 정책 전무(관리주기/포맷/정책) 로그의 활용성 저하

웹 로그의 방대한 양으로 단순보관 시 추후 분석이 거의 불가능

3. 웹 서비스 해킹징후 분석의 필요성

웹 서버 해킹 사고 증대

- **웹서버를 통한 중요 정보 해킹증가**
  - H캐피탈, N은행, L투자증권, N포탈등이 웹해킹을 당함
  - 홈페이지 변조, 단순침입시도, 피싱 경유, 스팸릴레이, 기타해킹 등
- **장기간/소량의 공격을 통한 해킹 탐지 우회**

법적/제도적 규제강화

- **정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행 규칙- 지식경제부**
  - 접속기록의 위조, 변조 방지를 위한 조치
  - 침해사고방지를 위한 보안프로그램의 설치 및 운영
- **개인정보의 기술적/관리적 보호조치 기준 (지식경제부)**
  최소 6개월 이상의 접속기록을 보존 관리하여야 한다

웹해킹 사전예방 체계구축

웹 서버 로그 관리

- **로그를 통한 정보수집 부족**
  - 로그별 보관 정책 상이
  - 다양한 웹서버
  - 로그별 담당자 상이
- **현행 웹로그 관리의 문제**
  - 정보자산측면에서 로그가치 결여
  - 웹서버별 전사적인 정책 필요

웹 보안 솔루션의 한계

- **보안장비(IPS, FW, IDS)의 한계**
  - 해킹징후에 대해 디코딩해서 탐지 불가능
  - 과거 로그 기록에 연관분석 분석 기능 없음
  - 설정 값이 변경되면 웹서비스 성능에 막대한 영향을 미침
  - 보안장비를 통과해서 웹서버까지 도달한 요청 기록 분석 안됨
- **웹서비스 품질(QOS) 보장의 한계**
  - 실시간 처리를 해야 하므로, 보안 패턴 우회 공격에 대한 심도 있는 분석 한계

II. 웹 서비스 해킹징후 분석 솔루션 (PS BalckBox)

1. 웹 서비스 해킹징후 분석 솔루션

PS BlackBox는 대용량의 웹로그를 효과적으로 탐지 및 분석하여 장기간에 걸쳐 진행되는 해킹 징후를 파악하는 웹서비스 해킹 징후 분석 솔루션 입니다. 최근 보안위협의 다양화 및 복잡화에 따른 보안 환경변화를 인지하고 법적/제도적 규제강화 및 내부정보유출, 사이버 테러의 급격한 증가에 따른 보안위협에 적극대응하기 위해 위험을 사전 감지할 수 있는 디지털포렌식(Digital Forensics)이 가능합니다.

징후 분석 흐름

1. 웹 로그 관리

- 일관된 정책에 의한 로그 수집 및 저장

2. 해킹 징후 탐지

- 보안 장비를 통과하여 웹서버에 요청된 실제 로그를 기반으로 해킹 징후를 효과적인 탐지

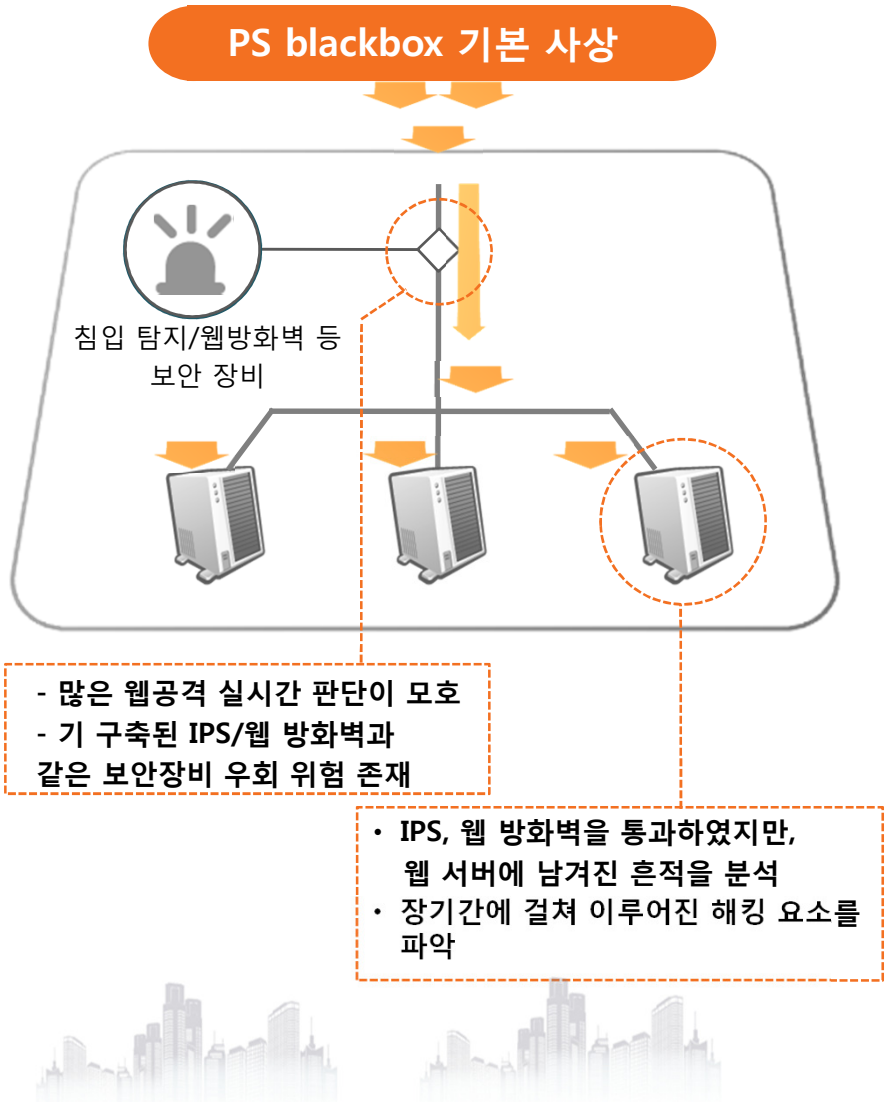
3. 사전 징후 분석

- 주기적인 로그 분석을 통해 사고 전, 의심 행위 탐지 및 대응책 마련

4. 사후 조치 분석

- 웹 해킹 사고 후, 신속한 사고 경위 파악을 통해 취약점 보완 및 보고서 작성

2. 보안장비 vs 웹해킹징후분석 비교

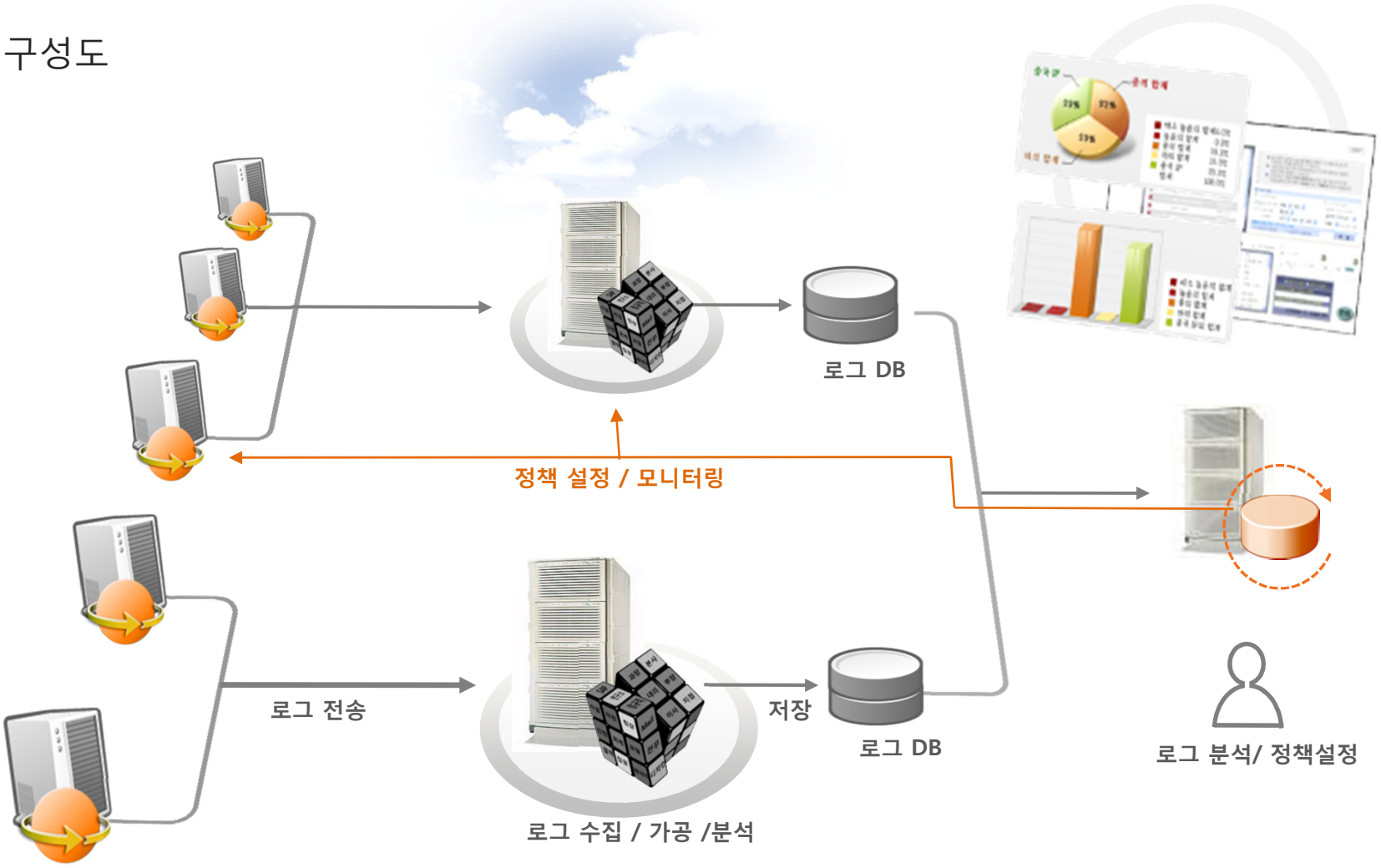


구분	보안장비(IPS, FW, IDS)	PS BlackBox
탐지 방법	실시간	기간에 걸쳐
침입 분석	단일 요청만 분석 (연관분석 불가능)	장기간 로그로 여러 요청 연관 분석
기 능	네트워크 앞단에서 차단	- 보안현황 체크 - 침해사고 대응
공격 재현	기능 없음	탐지된 공격을 자동 재현
웹서비스 영향	설정 값이 많아지면 웹 서비스 성능에 막대한 영향을 미침	서비스 품질(QOS) 제약이 없으므로 심도 있는 패턴 분석
한 계 점	- 웹서비스 영향 - 룰 설정 한계 - 단편적인 탐지	- 즉각적인 차단 불가 - 웹 로그에 의존

상호보완

3. 제품 구성

3.1 구성도



BlackBox - Agent **BlackBox - Spectrum** **BlackBox - Admin**

3.2 구성 요소

구성 모듈	기능 분류	기능 설명
BlackBox Agent	**로그수집**	• 웹 로그 수집 에이전트 • 웹 서버에 설치되어, 블랙박스 정책에 따라 로그를 전송 • 웹 서버 프로세스와 별개로 운용하여, 웹 서버의 안정성에 영향을 주지 않음 • 웹 로그를 기록하는 모든 형태의 웹 서버를 지원함 - Microsoft IIS5, 6 웹 서버 - Apache HTTPD 1.x, 2.x 웹 서버 - 다양한 웹 서버의 로그 형태 지원
BlackBox Spectrum	**로그취합**	• 웹 로그 취합 및 정제화 서버 • 웹 서버의 에이전트와 블랙박스 정책 서버의 정책 및 수집 기능 대행 • 네트워크 환경의 물리적 제약에 따라 전체 블랙박스 시스템의 재배치가 가능하도록 지원
	징후분석(1차)	• 압축된 로그파일 원본을 대용량 저장공간에서 관리하고, 통합 검색 제공 • 로그원본에 대한 인덱스 정보 및 공격 시그니쳐 관리 • 위험 징후 요소에 대한 정보 취합 및 정규화 • 로그에 대한 실시간 패턴 분석
BlackBox Master	**징후분석(2차)**	•압축된 로그파일 원본을 대용량 저장공간에서 관리하고, 통합 검색 제공 • 공격 시그니쳐 관리 • 과거 웹로그와 연관 분석을 통해 징후 상세 분석
	Admin Tool	• 사용이 간편하고, 직관적인 웹 기반 관리자 툴 제공 • 수집 에이전트에 대한 수집 정책 설정 • 수집 에이전트 모니터링 및 수집 현황 제공

4.1 강력한 위험 진단 엔진

공격검증 +

탐지된 위험 패턴의 정확한 검증 절차는
최고수준의 해킹기술을 가진 전문가들이
동일요청 수행 및 이에 대한 응답정보를 통해
검증

패턴 탐지 +

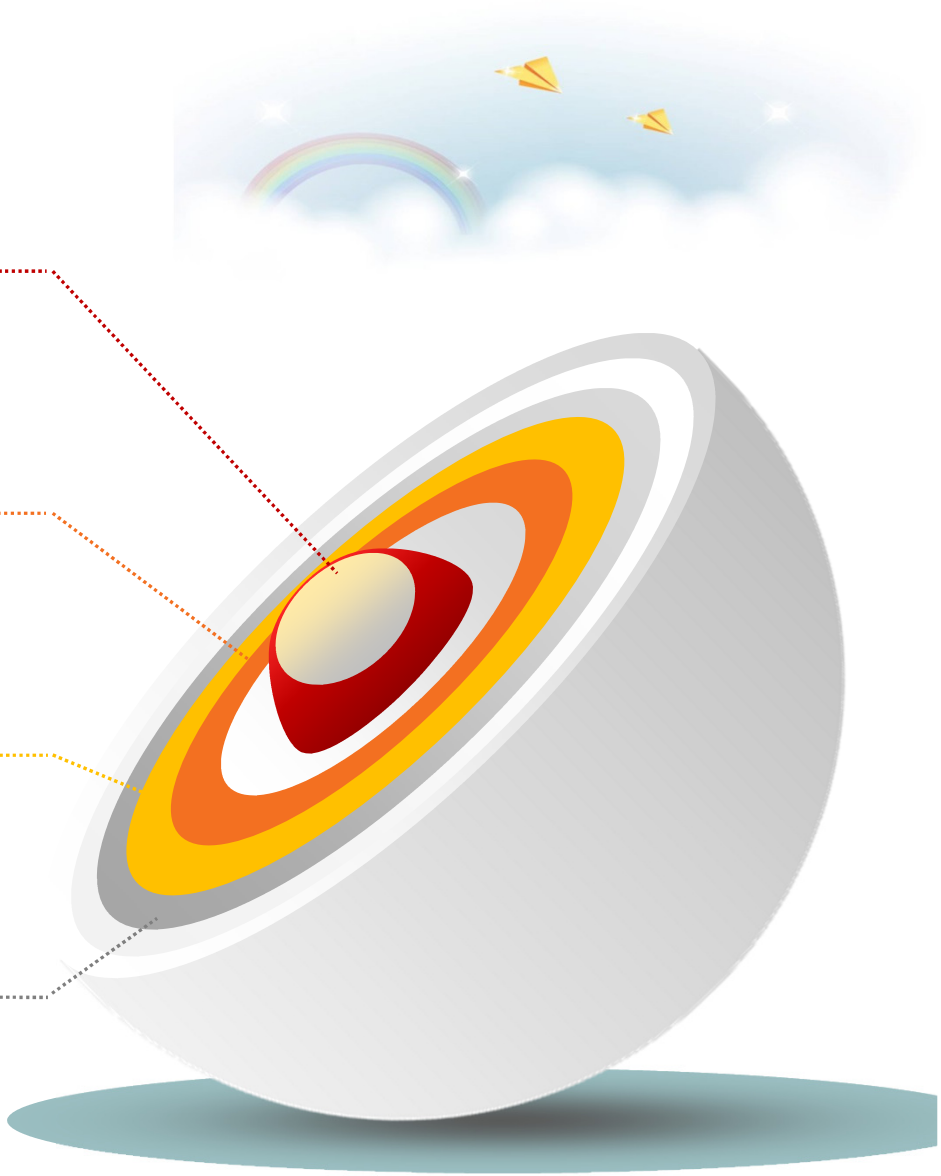
웹 주요취약점 및 사용자 패턴으로 공격
징후 탐지

통합 디코더 +

다양한 형태로 인코딩 되어 우회를 노리는
공격을 멀티디코더 유틸리티로 디코딩
처리해서 분석

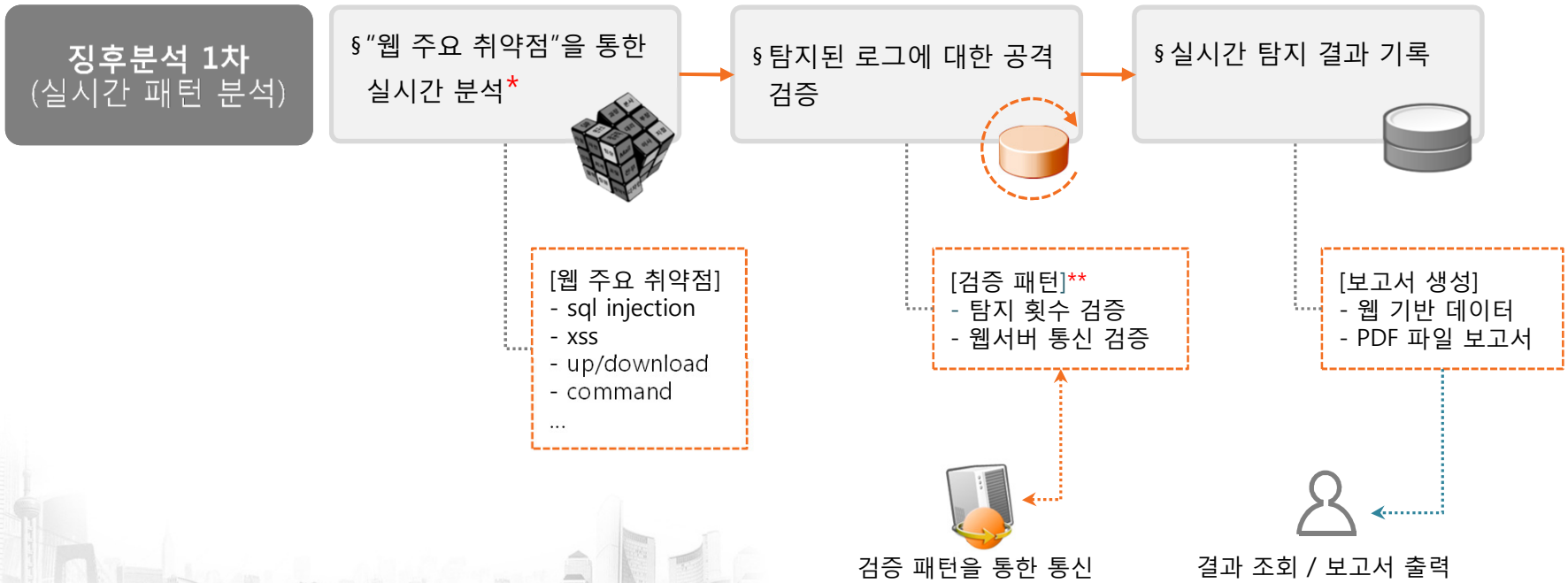
웹 로그 필터 +

불필요한 원본 로그 필터링



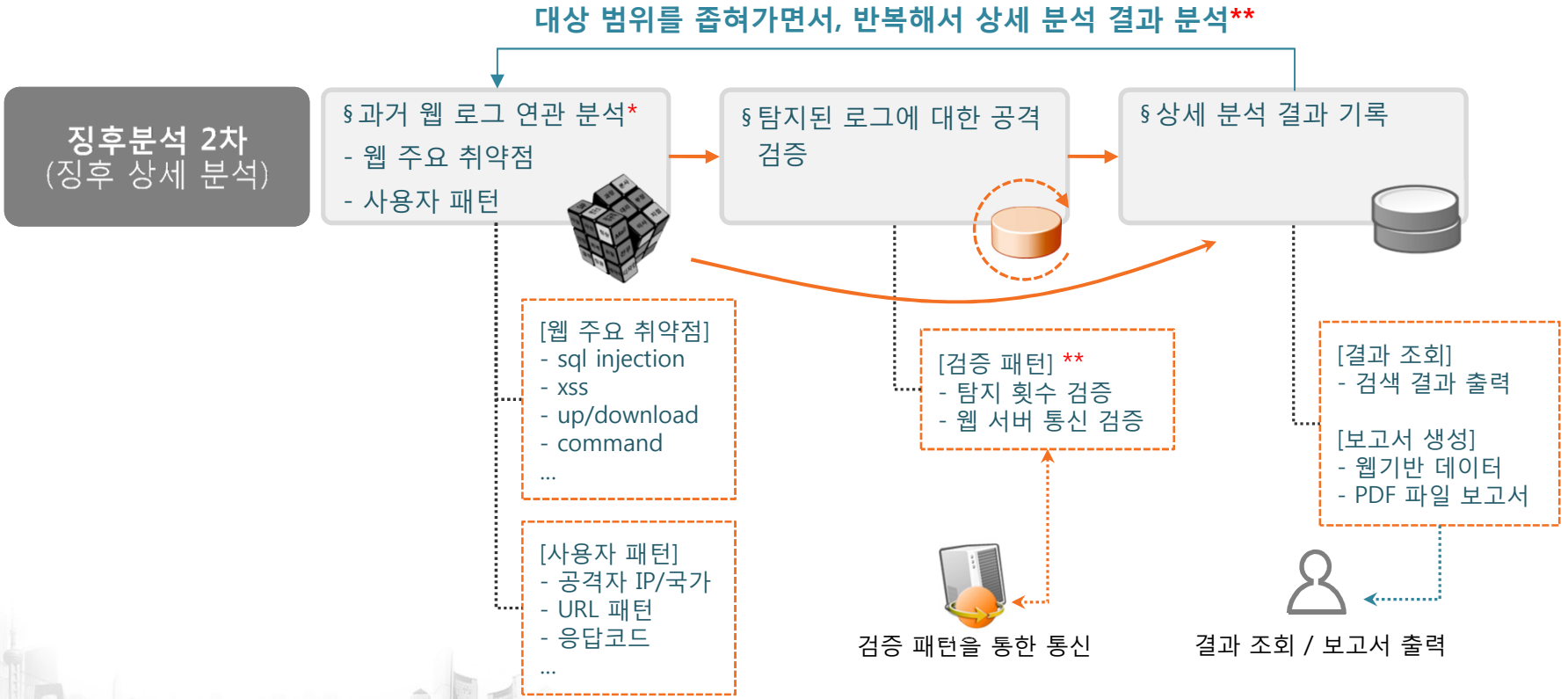
4.2 보안 현황 체크

• **정기적으로 탐지된 징후의 모의공격 재현**



* : 징후분석 시스템에서 제공하는 웹 주요 취약점 패턴에 대한 분석 작업을 수행합니다.
** : 웹 주요 취약점 패턴에 대해 정의된 검증 패턴을 통해서 징후 분석 결과의 신뢰도를 향상시킵니다.
- 동일한 IP로부터 특정 공격이 단위 시간당 n회 이상 반복 수행되었는가? (예: PUT/DELETE 등의 메소드 패턴)
- 탐지된 웹 로그에 대해, 실제 웹 서버가 해당 취약점을 포함하는가? (예: 오탐 제거를 위해 검증이 필요한 패턴)

4.3 침해사고 대응



* : 징후분석 시스템에서 제공하는 웹 주요 취약점 패턴과, 분석자가 검색 시 입력한 사용자 패턴에 대한 분석을 수행합니다.
- 각 패턴에 대한 AND/OR 연산 지원, 웹 로그 원본 또는 이전 상세 분석 결과를 통한 추가 분석

** : 현재의 분석 결과를 통해 추가 징후 분석을 반복적으로 수행합니다.
- 이전 상세 분석 결과를 추가 분석하여, 공격원 및 공격인자를 범위를 좁혀가면서 추적합니다.
- 오랜 시간이 소요되는 징후분석에 대한 작업 효율을 향상시킵니다.

4.4 관리

로그 관리

스펙트럼

- 스펙트럼의 시스템 상태 조회(CPU, Memory, Repository 정보)
- 평균 수집되는 로그의 용량 및 추이를 확인
- 최근 로그 데이터를 그래프로 확인

호스트

- 에이전트별 로그 용량을 그래프와 표로 확인
- 로그의 용량과 수를 확인

에이전트

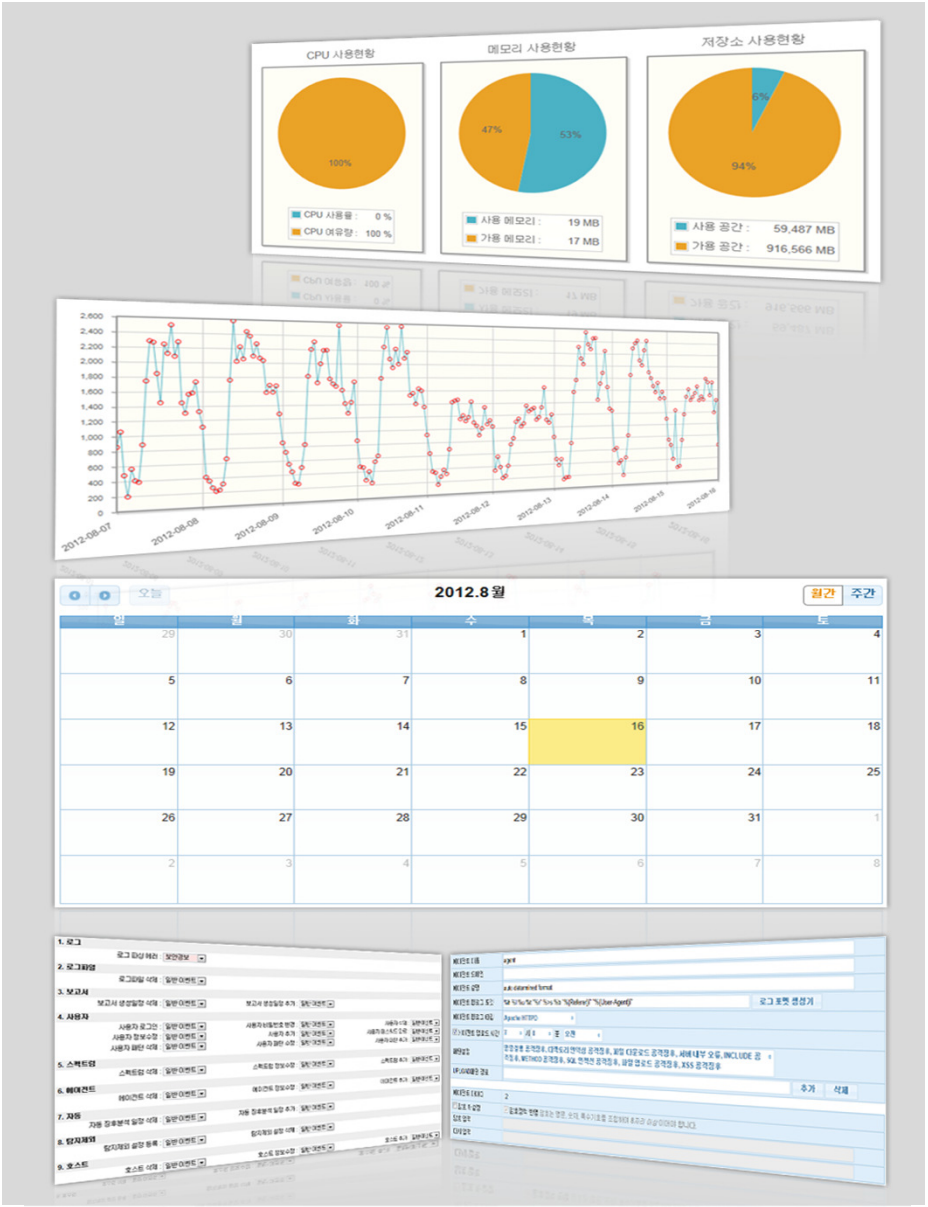
- 수집된 파일 목록과 함께 기타 상세한 정보를 확인
- 가장 많은 로그가 들어오는 호스트 또는 에이전트를 확인
- 평균 수집되는 로그의 용량을 확인

에이전트 관리

- 스펙트럼 등록 및 정보수정
- 웹 서버 등록 및 정보수정
- 에이전트 등록 및 정보 수정

시스템 관리

- 감사 로그 목록 : 웹 징후 분석 시스템의 주요한 작업들을 조회
- 시스템설정 : 웹 로그 자동삭제 / 사용자 로그인 정책
- 보고서 관리: 웹 해킹 징후탐지 결과에 대한 보고서
- 분석일정 : 자동으로 수행되는 웹 해킹 분석을 일정 주기로 수행
- 패턴관리 : BLACKBOX의 사용자 패턴을 관리



4.5 부가모듈

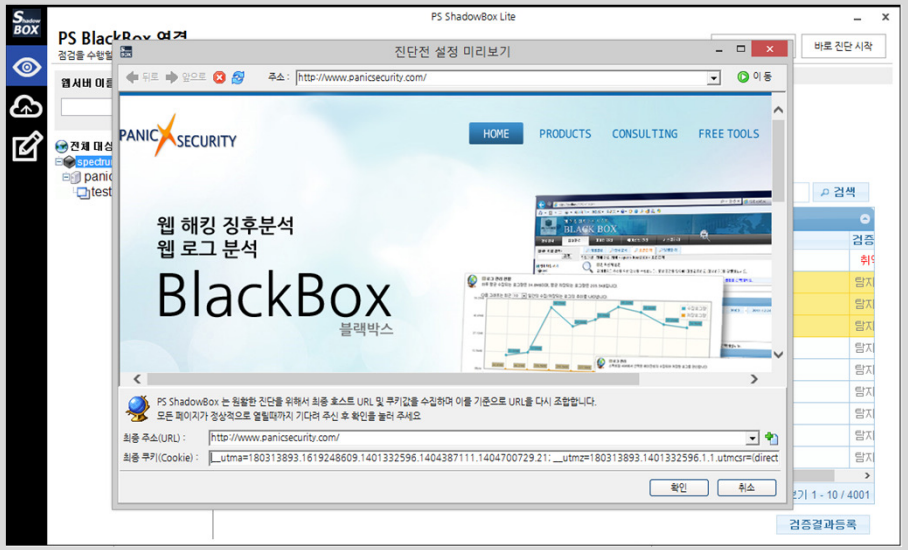
웹 해킹 검증도구 - ShadowBox +

웹해킹 징후탐지 결과에 대해서, 자동 검증도구와 연동 지원

- 웹로그 상에서 **공격징후**가 있는 웹 어플리케이션에 대하여 실제로 취약점이 존재하는지 **"자동" 검증**
- 웹취약점 점검도구(PS ScanW3B)와 동일한 공격 패턴 적용

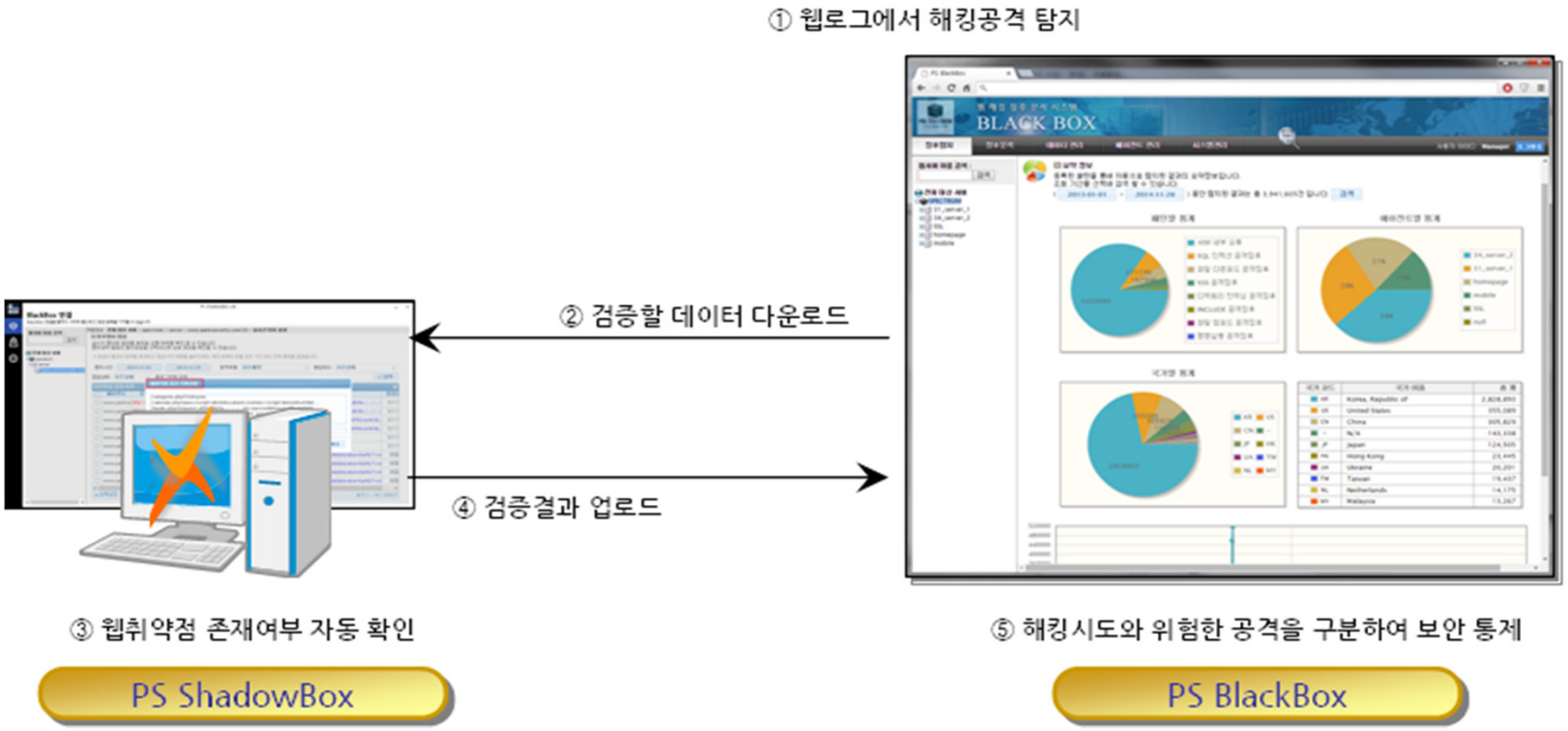
웹해킹 검증결과에 대한 활용

- 웹해킹 징후와 **실제 취약점 존재 여부**를 동시에 확인
- 웹취약점 점검도구(PS ScanW3B)를 통하여 별도의 점검결과 보고서 생성지원



4.5 부가모듈

웹 해킹 검증도구 - ShadowBox +



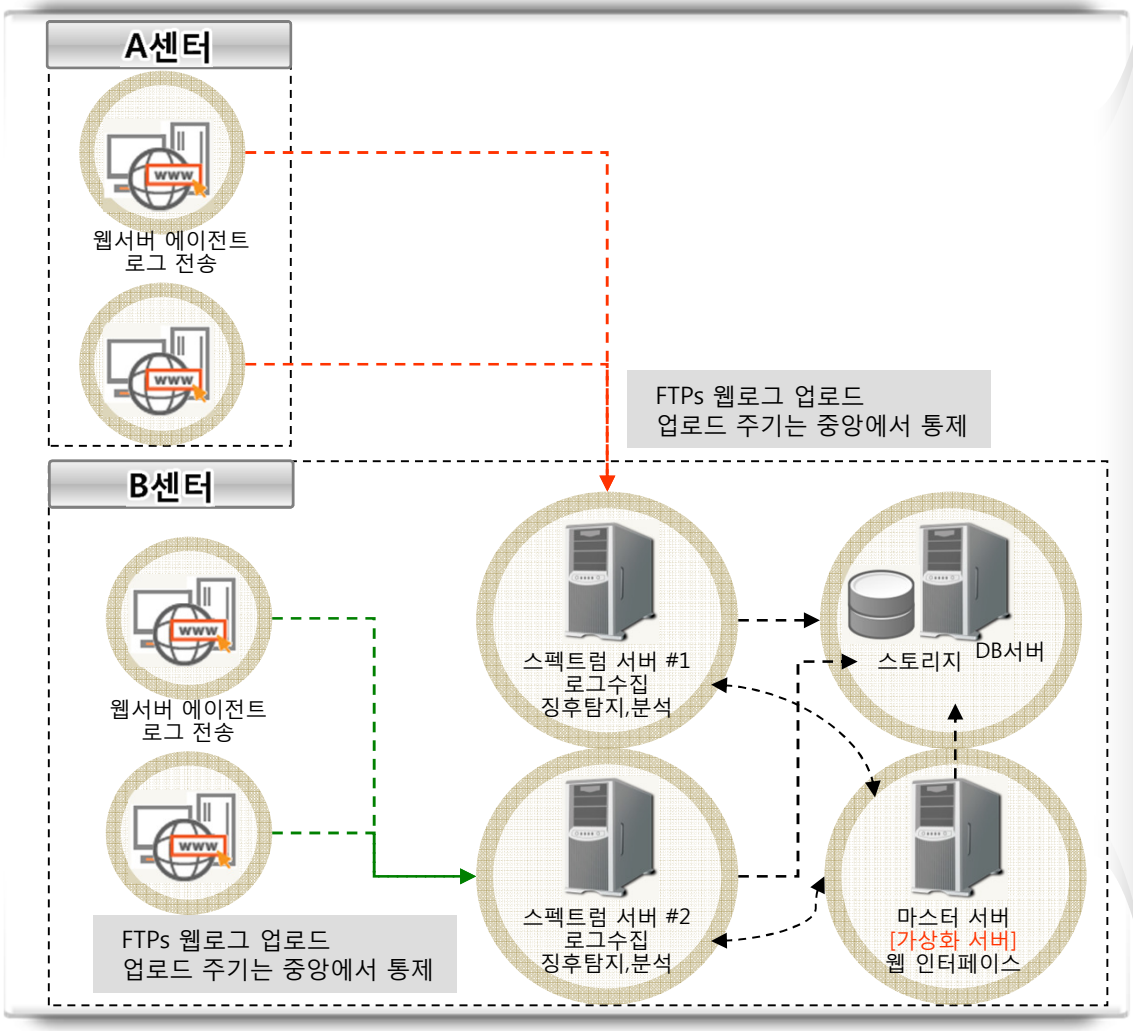
III. 구축 사례

1.1 프로젝트 구축사례

"성공적인 구축을 통한 검증된 기술력"

1.2 관련 프로젝트 구축 사례

[Agnet방식] 삼성화재



thinkNext 삼성화재

시스템 구성

- 대상서버 : 00대 웹서버(000여개 웹서비스)
- 스펙트럼 : 2대/웹서버 로그 수집 및 분석
- DB서버 : 1대 / 데이터 관리
- 마스터 서버 : 1대 / 가상화 서버로 구축
  웹 인터페이스

스토리지 구성

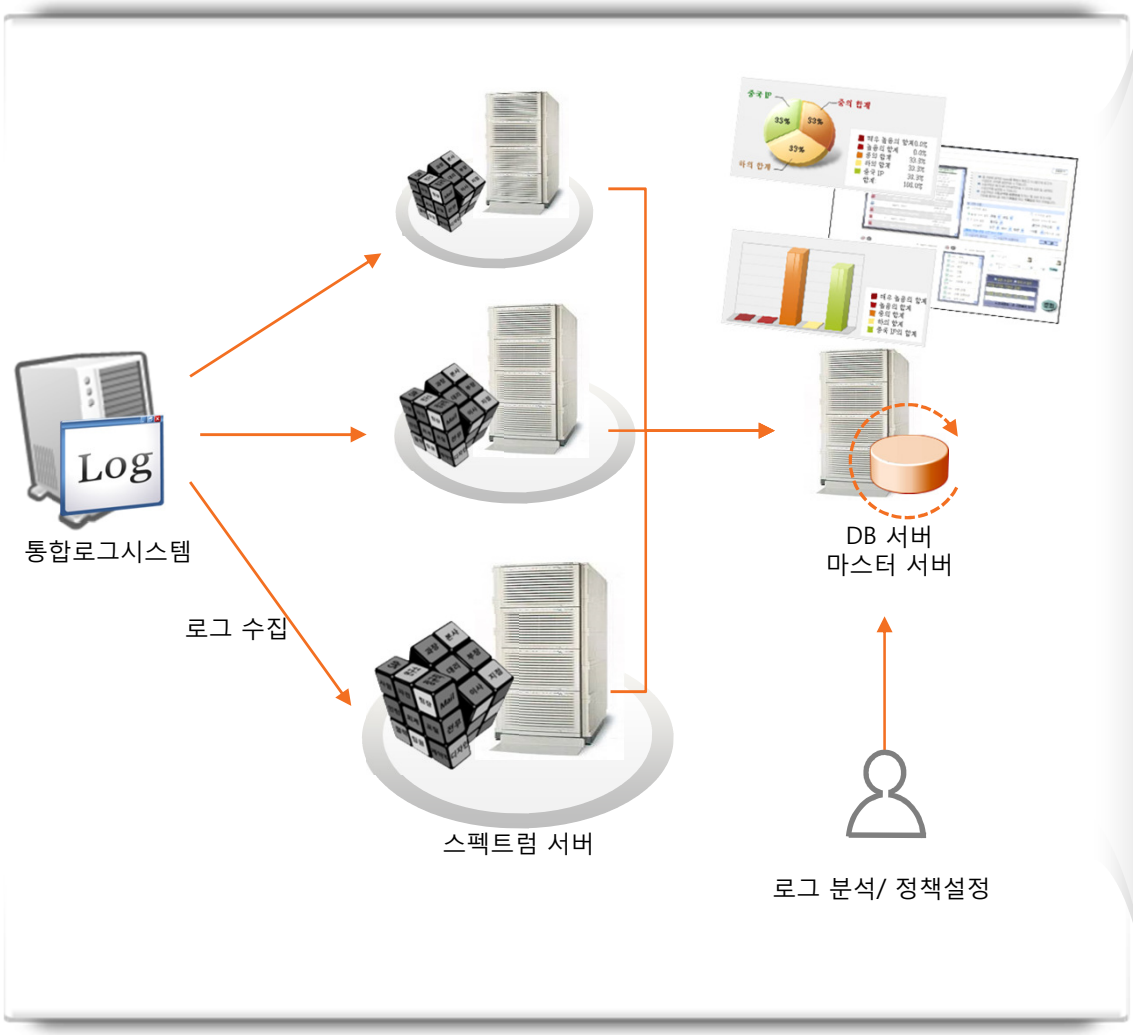
- 스펙트럼 서버 #1 : 3T
- 스펙트럼 서버 #2 : 3T
- DB 서버 : 1T

Agent 구성

- 설치 용량 : 50M
- 업로드 시간 : 매일 00시 이후
  중앙에서 업로드시간 통제
  시간 경과 시 자동중지 익일 재개
- 업로드 방식 : FTPS
- 업로드 속도 : 1Mbyte / second
- 최대 업로드 : 5개 채널

1.2 관련 프로젝트 구축 사례(계속)

[통합로그방식] 삼성카드



삼성카드 SAMSUNG

시스템 구성

- 통합로그시스템 : 기 구축됨
- 스펙트럼 서버
  - 3대/웹 서버 로그 수집 및 분석
- DB서버 / 마스터 서버 : 1대
  - 데이터 관리 / 웹 인터페이스

주요 기능

- 스펙트럼 서버
  - 로그 취합
  - 징후 탐지 및 분석
  - 통합로그시스템과 Plug-in(로그 수집)
- 마스터 서버 : 분석 UI / 시스템 관리
- DB서버 : 데이터 관리

유사 사례

- 서울시청, 삼성전자, 삼성생명

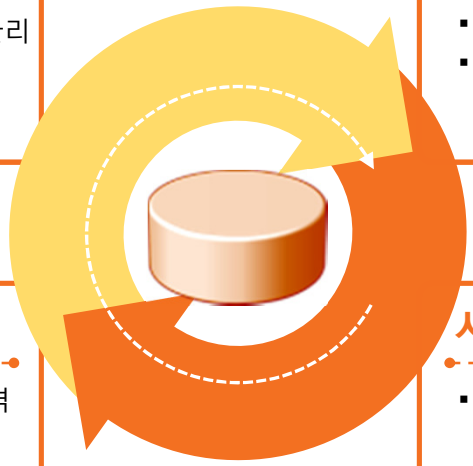
2. 특장점

웹 로그 관리 +

- 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 IPS/웹 방화벽의 방어력이 기대치에 못 미침(보안레벨을 높이면 QOS 저하)
- IPS/웹 방화벽의 **분석력 취약을 보강**
- 보안 장비를 통과하여 웹서버에 요청된 실제 로그를 기반으로 징후를 탐지하여, 각 **장비 별 보안정책 패턴 정책을 강화**



사후 조치 분석

- 보안사고 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"
"위협 요소에 대한 효과적인 검색 및 분석"

IV. 제안사 소개

1. 회사정보

회 사 명	(주)패닉시큐리티	대표자	신용재
주 소	서울시 금천구 가산동 680번지 우림라이온스 612호		
전화번호	TEL : (02) 2027-2890 FAX : (02) 2027-2891		
홈페이지	http://www.panicsecurity.com		
주요제품	**PS ScanW3B** 웹 취약점 진단 도구 솔루션 **PS ScanW3B CS** 기업용 웹 취약점 점검 시스템 **PS BlackBox** 웹해킹 징후분석 시스템		
특이사항	1. 국제 해킹대회 Defcon 예선전 아시아 1위 및 라스베가스 본선 4위 2. 인터넷뱅킹 대상의 메모리해킹 위험성 발표 및 시연 3. 국내 최초 웹취약점 점검툴 개발, 국내 최초 웹해킹징후분석 시스템 개발		
주요고객	**금융기관 :** 대한생명, 국민은행, 삼성카드, LG카드, 중소기업은행, 금융감독원, 금융결제원 등 다수 **공공기관 :** 대법원, 정보통신부, 한국정보보호진흥원, 한국거래소, 서울시, 병무청, 인천교육청 등 다수 **일반기업 :** 삼성전자, KT, 삼성테크윈, 다음, 넥슨, 현대중공업, 현대제철, GS홈쇼핑 등 다수		

2. 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 도구 이며, 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

웹해킹 징후분석 시스템 개발 및 상용화

- 보안장비를 우회하여 웹서버에 도달한 해킹공격이 기록된 대용량 웹로그를 효과적으로 분석함
- 서로 다른 웹서버 종류 및 로그 양식에 대해서 통합 분석, 연관 분석을 지원하여 오랜 기간에 걸친 공격 징후와 피해 범위 파악
- 통합 웹로그 관리시스템 및 빅데이터 시스템에 연동하여 웹해킹 징후를 탐지하고 분석하기 위한 최적의 시스템

감사합니다.

㈜ 패닉시큐리티

주소 : 서울특별시 금천구 가산디지털1로 2 612

www.panicsecurity.com

Tel. 02-2027-2890 / Fax. 02-2027-2891

PANIC SECURITY