umv

ZYON Platform

Web Server Safeguard
WSS AI 웹서버 / WAS 보안솔루션

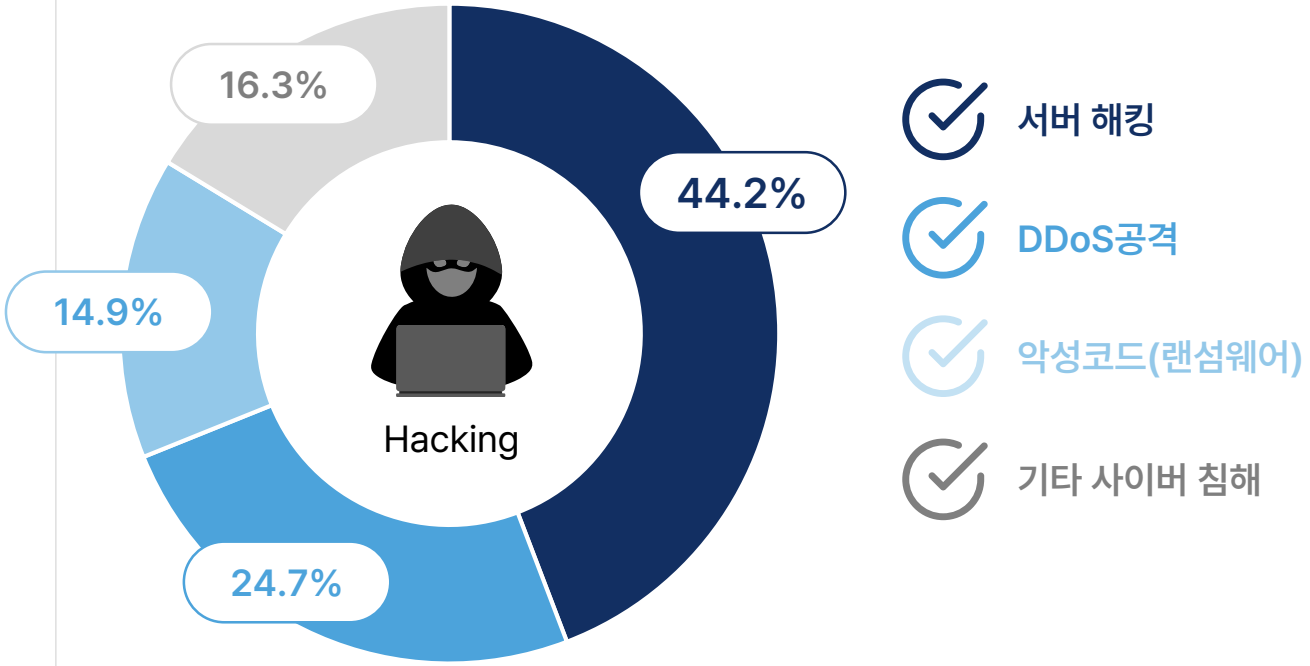
Contents

01. 제안배경

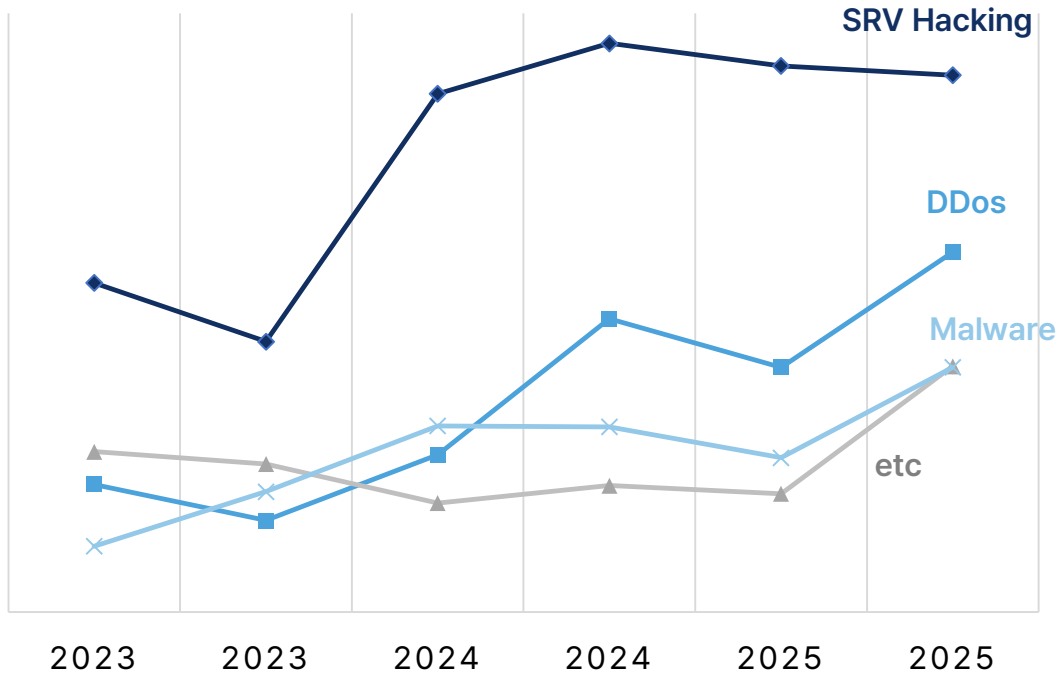
최근 해킹사고 동향

최근 다양한 유형의 해킹 사고 건수가 증가하고 있습니다

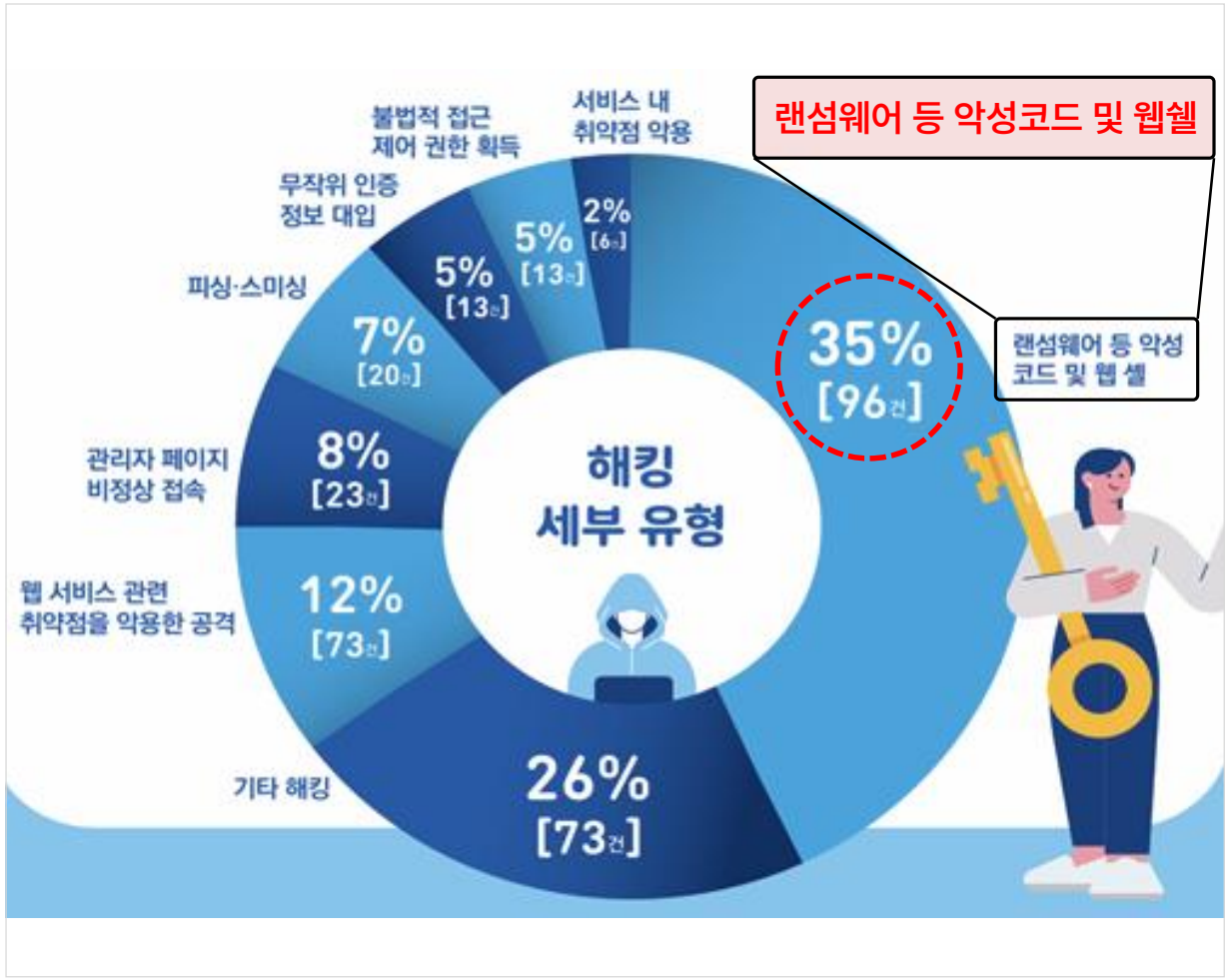
다양한 사이버 침해 공격의 지능화 및 고도화



2023년-2025년 사이버 침해사고 신고 현황



최근 해킹사고 동향

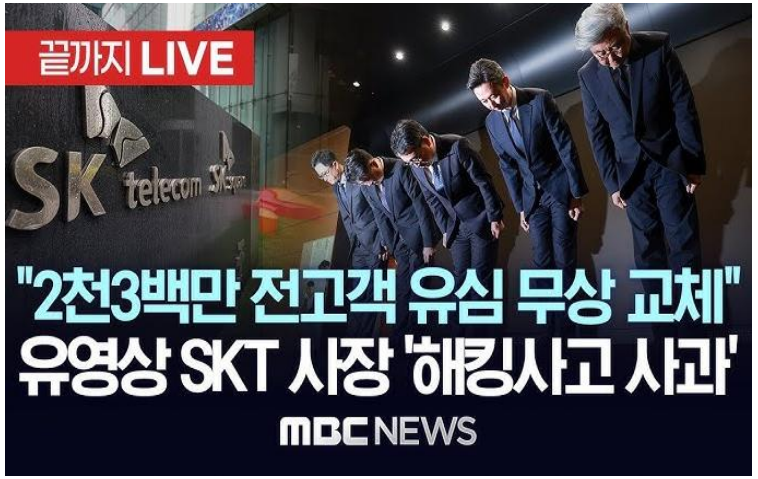


※ 출처 : 개인정보보호위원회

문제인식(1)

(1) 최근 개인정보 유출 사고의 공통 패턴 : 웹쉘 해킹

25.04.25 침해사고 발표



SKT 해킹 사태로 유출된 이용자의 유심 정보가 2천6백만 여건으로 드러났습니다. 조사단은 SKT의 리눅스 서버 3만여대를 모두 4차례 점검한 결과, 모두 23대의 서버가 악성코드에 감염돼 있었고, 최초 침투된 건 3년 전인 22년 6월 15일로, 서버를 장악하는 역할을 하는 '웹쉘'' 코드로 확인 됐습니다. (출처: KBS뉴스)

25.08.31 침해사고 발표

롯데카드는 8월31일 서버를 점검하다 3개 서버에서 2종의 악성코드와 웹서버에 원격으로 접근할 수 있게 하는 도구인 '웹쉘'5종을 발견되었다.
정보가 유출되고 난 뒤 17일이 지나서야 이를 알아차렸다. (출처: SBS뉴스)

25.11.07 침해사고 발표

조사단이 KT 전체 서버를 점검했더니 총 94대 서버에서 웹쉘 및 BPF도어 등에 감염된 것으로 드러났습니다. 웹쉘은 인터넷 연결 접점이 있는 서버의 파일 업로드 취약점을 악용해 서버에 웹쉘을 업로드하고 BPF도어 등의 악성코드를 확산시킨 것으로 확인되어졌습니다. 방화벽, 시스템 로그 등 기록이 없어 공격자의 침투 방법을 판단할 수 없어 어려움을 겪은 것으로 드러났습니다.
(출처: SBS뉴스)

문제인식(2)

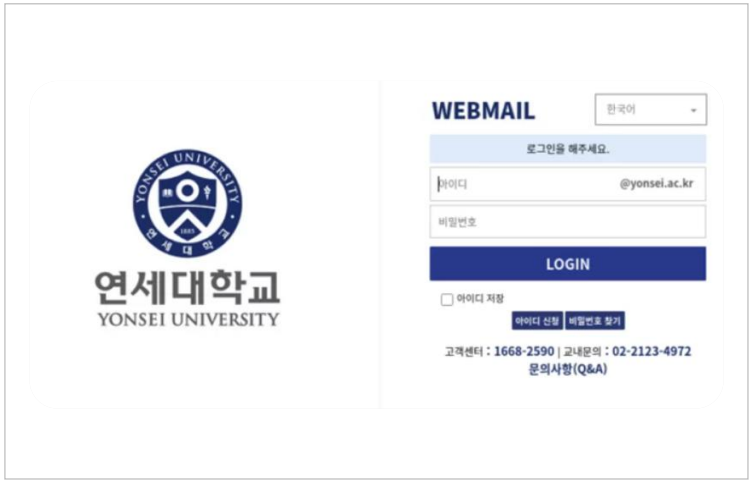
(2) 해킹 사고 관련 기사

계원예술대학교는 웹쉘 공격으로 인한 해킹을 통해 개인정보가 유출됐다. 웹쉘 공격은 해커가 웹서버 취약점을 통해 별도 인증 없이 시스템에 접속, 시스템에 명령을 내릴 수 있는 코드를 실행시켜 해당 웹서버를 조종하는 수법이다. (출처: KBS뉴스)

시기	피해 대상	내 용
25.4.	싱가폴 국영은행 및 중국은행 싱가폴 지점(싱가폴)	- 인쇄밴더(Toppan Next Tech)의 랜섬웨어 피해으로 인해 고객 정보 노출 위협 발생 (공급망 위협)
24.7.	C-edge 테크놀러지(인도)	- 중소은행의 코어뱅킹/결제 공급사의 랜섬웨어 피해으로 인해 지역협동은행 300여 곳 거래 장애 (공급망 위협
24.6.	Patelco Credit Union(미국)	- Ransomhub 랜섬웨어 공격으로 모바일 뱅킹 장기 중단 및 개인 정보 노출
24.5.	Evolve Bank & Trust(미국)	- 직원 악성 링크 클릭을 계기로 LockBit 랜섬웨어 감염과 대규모 데이터 유출 발생
23.11.	ICBC Financial Services(미국)	- LockBit 랜섬웨어 감염으로 미국 국채 결제 마비 발생

▲해외 주요 금융권 피해 사례 [자료:금융보안원]

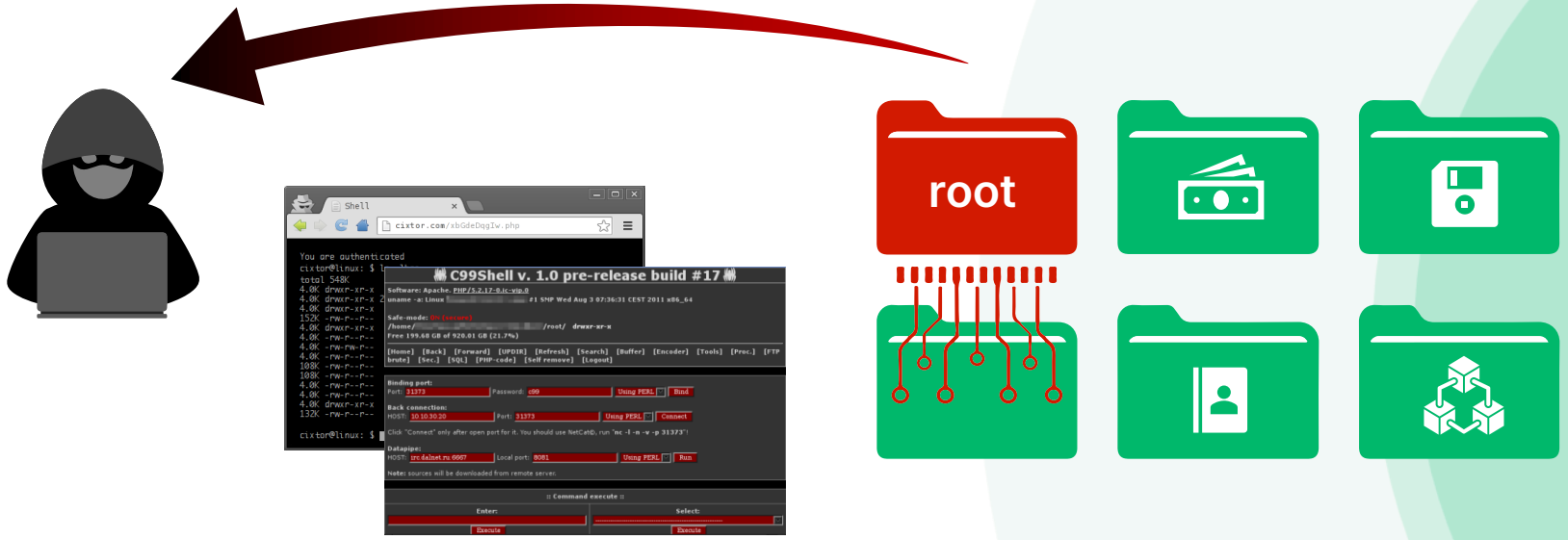
해외 바북이라는 해커집단은 2021년 4월 미국 메트로폴리탄 경찰청을 공격하며 이름을 알렸다. MS 확장 프록시쉘 체인을 악용한 원격코드 실행과 초퍼(Chopper) 웹쉘 및 랜섬웨어 설치 방식을 즐겨 썼고, 내부 침투를 노렸다. (출처: 보안뉴스)



피싱 메일로 교수 PC에 접근한 뒤, 서버에 'Green Dinosaur' 웹쉘을 설치하여 원격 파일 조작 및 데이터 수집에 사용한 점이 확인 (출처: The Hacker News)

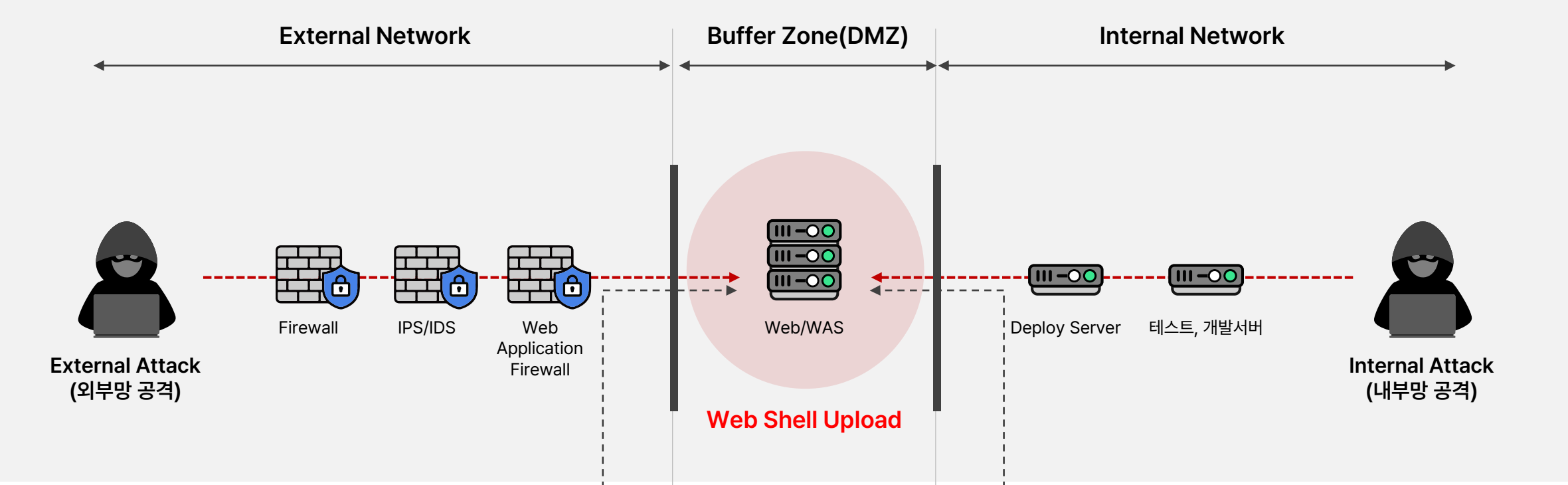
웹쉘(Web shell)이란?

1. 웹서버 취약점을 이용하여 삽입된 명령어 프로그램으로 실행되면 Root 권한에 준하는 서버제어 가능
   웹서비스를 위한 웹서비스 포트(80, 443)는 백도어 역할
2. 웹쉘은 스스로 삭제 기능이 있음으로 실시간 감시가 안될 수 있음
3. 웹쉘은 보안 시스템을 피할 수 있고 최고의 권한으로 별도의 인증 없이 시스템 접속 가능



웹쉘(Web shell)이란?

웹쉘이 진입하는 경로



해커의 웹서버 취약점 분석

마이크로소프트 제로데이 취약점
Log4j 취약점
React2Shell 취약점

네트워크 보안 솔루션 취약점

확장자 우회, 인코딩 우회, 난독화
네트워크 보안장비 취약점 (패킷 단위로 분석)
백신 컴파일된 Binary기반 악성코드 공격

내부 및 외부협력업체 직원에 의한 위험

웹쉘 침투과정

1. **파일 업로드 취약점 이용**

2. **네트워크 보안 솔루션 취약점을 이용한 공격**
   - 확장자 우회, 인코딩 우회, 난독화
   - 네트워크 보안장비 취약점(패킷 단위로 분석)
   - 백신 컴파일된 Binary 기반 악성코드 공격

3. **내부 및 외부협력업체 직원에 의한 위험 요소**

4. **WEB서버 / WAS OS Zero Day 취약점 공격**
   - 마이크로소프트 제로데이 취약점
   - Log4j 취약점 (CVE-2021-44228)
   - React2Shell 취약점 (CVE-2025-55182, CVE-2025-66478)

해킹 아닌 내부자 유출 … 신한카드 개인정보 사고, 모럴헤저드·내부통제 시험대

3년간 방치된 내부 유출 … 가맹점 대표자 19만명 피해
당국 현장검사·전업권 점검 착수 … 내부통제 책임론 확산
신한투자증권 이어 또 내부 리스크 … 그룹 관리체계 시험대

기사입력 2025-12-26 11:45:11 | 박정연 기자 | jypak@newdaily.co.kr

▲ ⓒ신한카드

국내 카드업계 점유율 1위 신한카드에서 내부 직원의 일탈로 가맹점 대표자 19만여 명의 개인정보가 약 3년간 외부로 유출된 사실이 확인됐다. 회사가 장기간 이를 인지하지 못한 채 방치한 가운데 금융당국은 현장검사에 착수했다.

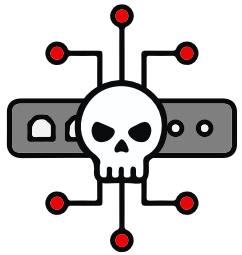
이번 신한카드 개인정보 유출은 롯데카드나 업비트 사례처럼 외부 해킹에 따른 사고와는 성격이 다르다. 해킹의 경우 금융사 역시 피해자라는 해석이 가능하지만, 이번 사고는 내부 직원의 고의적 행위로 발생한 만큼 모럴헤저드와 내부 통제 실패라는 책임을 피하기 어렵다. 여기에 지난해 10월 신한투자증권에서 발생한 1300억원대 손실 사고까지 겹치면

해킹 프로세스

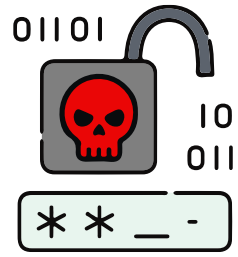
최근 개인정보 유출 사고 공통된 원인분석 결과 **웹쉘**을 통한 **백도어 계열 악성코드 감염**으로 확인

기존 네트워크 보안장비를 뚫고
로그 중독 웹쉘 업로드

해커는 웹쉘을 실행하여
BPF도어 등 정상 파일, 정상 행위로
위장한 악성파일을 쉽게 업로드



내부 네트워크로
이동 및 확장 진행

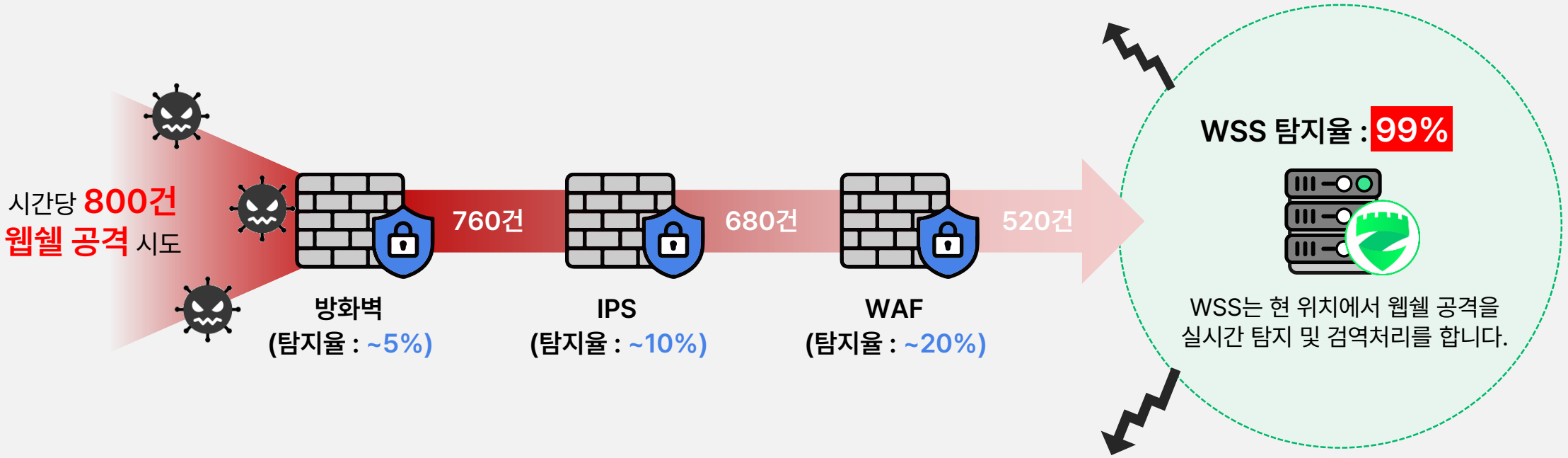


웹서버를 장악한 웹쉘을 통해
개방된 433, 80포트를 백도어로
활용하여 개인정보 탈취 성공

WSS 포지션

웹쉘이 네트워크 보안 솔루션을 통과하여 침투하는 과정

웹쉘 공격 퍼널 : 시간당 공격 시도 대비 침투 성공 건 수*



WSS 포지션

웹쉘 탐지 솔루션 WSS	구분	웹 방화벽(WAF)
웹 서버에 침투한 웹쉘 실시간 탐지 웹쉘 업로드 탐지·차단	기본기능	웹 서버 침입방지 및 차단
웹 디렉터리 내의 웹 프로그램 파일	보안대상	웹 서버의 유입 트래픽
비인가자 소스파일 임의 변경 시 자동탐지 소스파일 저장 및 변경 시 자동복구 기능 제공 파일단위 탐지를 통해 서버 부하 최소화 원본파일(실행파일/데이터파일)에 대한 탐지	웹 위변조 탐지 및 복원	웹 페이지 단위 설정을 통해 컴파일된 HTML 및 데이터 파일 탐지 다수의 페이지에 대한 위·변조 탐지 설정 시 웹서버 및 웹방화벽 부하 발생
WAS 설정 변경 탐지 iFrame 삽입(악성URL 포함) 탐지 및 차단	주요 웹 침입 탐지 및 차단	SQL Injection, XSS, Cookie poisoning, File upload, Buffer overflow 등의 웹 주요 침입에 대한 탐지 및 방어
패턴, 시그니처, Hash, 알고리즘 방식 적용 최초 전체 탐지로 기존 침입한 웹쉘 탐지 가능 웹쉘 코드 업로드 실시간 탐지 · 차단 인코딩된 ASP 웹쉘 코드 탐지 · 차단 웹 방식(FTP 등) 이 아닌 경로를 통해 유입된 웹쉘 탐지 가능	웹쉘 코드 탐지 및 차단	첨부파일 확장자명 차단 패턴 차단은 제한적(소스코드 분석 불가)으로 제공 침입된 웹쉘 및 인코딩 된 웹쉘 탐지 불가
탐지내역 분석을 통한 원격 검역 지원	웹쉘 검색	일부 패턴 보유(100개 미만), 탐지율 30% 미만, 웹쉘 기능 OFF로 설정(과부하 발생)

WSS 포지션

웹쉘 탐지 솔루션 WSS	구분	서버 EDR / 백신
웹서버 · WAS 내부 웹쉘 및 악성 스크립트 대응	Position	서버 OS · 엔드포인트 전반 위협 대응
실시간 웹쉘 탐지 / 업로드 차단 / 위변조 탐지	주요 기능	프로세스 행위 분석 / 악성코드 탐지 / 로그 수집
경량 구조, 서버 성능 영향 최소화	자원 소모	상대적으로 높음 (수집·분석 리소스 필요)
비교적 효율적	비용	상대적으로 높음
설치·운영 단순 / 웹 서버 중심 운영	관리 측면	정책 · 에이전트 · 예외처리 관리 부담 존재
웹쉘 특화 탐지율 높음 / 낮은 오탐 설계 가능	웹쉘 및 악성코드	일반 악성코드 중심 / 웹쉘 업로드 시점 탐지 한계
웹쉘 업로드 및 생성 시점 실시간 탐지	탐지 시점	실행 후 행위 발생 시 탐지

최근 해킹사고 동향보고 사례

시사점(1)

01 웹 기반의 공격의 급증 : 웹쉘 및 서버 해킹이 주 공격 수단

해결책 공격자들은 웹서비스 영역의 취약점을 공략하고 있으며, 웹쉘 기반 침투를 통한 서버 장악 조치 시급

02 기존 WAF와 백신의 한계 : 진화된 공격 대응 어려움

해결책 WAF, 백신 등의 솔루션만으로는 우회 가능한 공격 차단 어려움 행위 기반 감시 시스템 필요

03 EDR의 한계 : 특정공격 실행 이전 대응이 중요

해결책 웹쉘 등의 악성코드 업로드만으로는 탐지가 어려움 실행 시에 감지가능, 사용자 단에 중점을 둠

최근 해킹사고 동향보고 사례

시사점(2)

04 지능형 공격(APT)은 장기 잠복 후 확산을 시도

해결책 초기 침투 시 발견하지 못하면 악성코드가 잠복하여 일정기간 이후 큰 사고로 번질 위험성

05 공공 · 교육기관은 공격자의 핵심 타깃

해결책 대국민 서비스의 연속성과 기관 신뢰도 보호를 위해 사전 탐지와 즉각적인 대응 보안 체계 필요

06 서버 안에 무엇이 새로 생겼는가를 실시간으로 탐지하는 시스템을 구축하는 것이 해킹을 예방하는 길

해결책 파일의 생성, 변경, 삭제 등 실시간 탐지 및 조치가능한 시스템 필요 (보안의 마지막 퍼즐)

02. 제안제품

WSS(Web Server Safeguard)

(1) 국내외 최초 웹쉘 탐지 솔루션

특허 기반 독자적 기술력

(2) 강력한 탐지기법

패턴, 해시, 알고리즘, AI 탐지 제공

(3) AI 소스코드 분석

웹쉘 패턴에 대한 상세 분석 내용 제공

(4) 편리한 부가기능

자동검역, 파일 위변조 탐지 및 복원 기능 등

(5) 클라우드 / 컨테이너 환경 지원

Docker/Kubernetes 환경 완벽 지원

(6) 리소스 최적화

CPU, 메모리 사용량 자동제어

(7) 맞춤형 연동 지원

SOAR, SIEM, EMAIL 등
연동시스템 커스터마이징

(8) 편리한 관리성

유지보수 및 요청사항 적극 반영

특장점 및 강점

(1) 국내외 최초 웹쉘 탐지 솔루션

- 웹쉘 탐지·복원 기술 등 6건 이상 특허 (WSS 파일 변경방지 등)
- 웹쉘 및 악성URL 실시간 탐지
- 금융 공공 구축사례 다수

(2) 강력한 탐지기법

- 미탐 오탐 방지를 위한 개발
- 최신 탐지 어려운 웹쉘 및 패턴/해시값을 웹쉘 알고리즘 탐지 기법으로 탐지
- AI 탐지 기법 개발

(3) AI 소스코드 분석 기능

- AI 소스코드 분석 기능을 통해 탐지 된 웹쉘에 대한 상세 분석 내용 제공

(4) 편리한 부가기능

- 실시간 파일 위변조 탐지&복원
- 홈 디렉토리 자동찾기 기능
- 개인정보 탐지 기능
- 업로드 파일 필터링 기능
- 자동검역 기능 등

(5) 클라우드/컨테이너환경 지원

- AWS, Azure, Kubernetes 완전 대응
- FY17년 삼성전자 Kubernetes 환경 도입 (현재까지 운영중)
- 컨테이너별 에이전트 자동배포

(6) 리소스 최적화

- CPU/Memory 자동 제어, 무중단 운영

(7) 유지보수 및 Requirements 반영

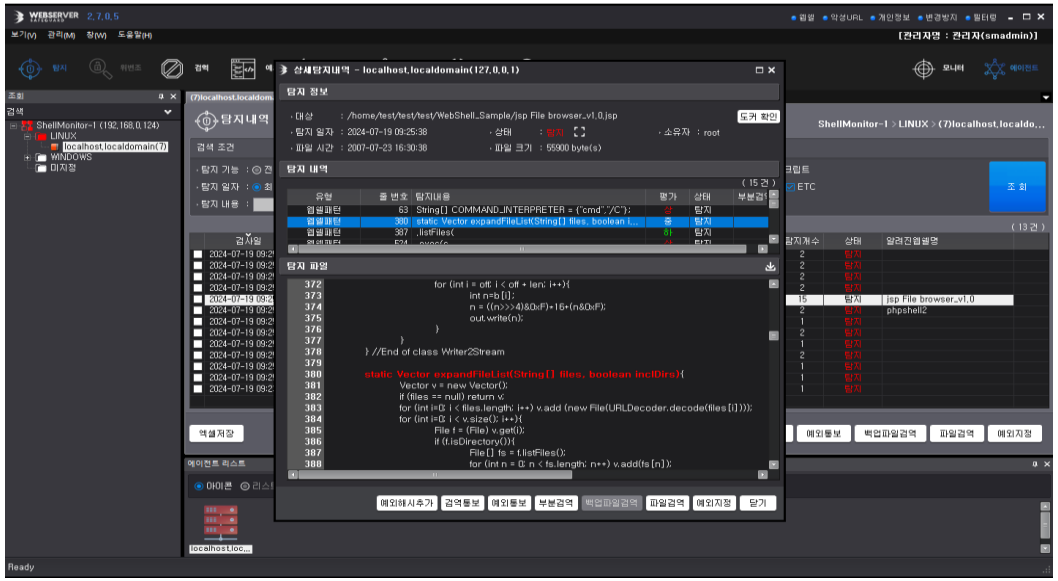
- SIEM, EMAIL, SOAR 등 연동 시스템 지원
- 그 외 연동 시스템 커스터마이징 지원

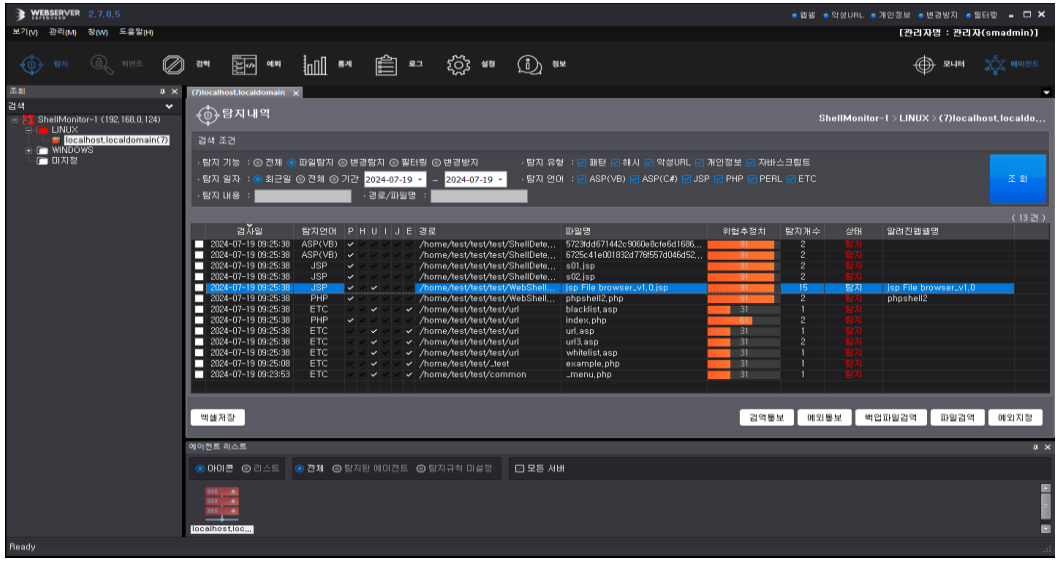
(8) 무중단 탐지

- 신속한 피드백
- 맞춤 유지보수/고객요구사항 분기 또는 연2회 취합(반영)
- 대시보드 및 R&R 지원

상세 기능 : 웹쉘 및 악성 URL 탐지기능

기능명	상세기능	설명
실시간 웹쉘 탐지	탐지	전체 탐지, 실시간 탐지를 통하여 웹쉘 파일 탐지 및 보고
	탐지내역 조치	검역, 예외조치를 통하여 탐지 내역 조치
실시간 악성URL 탐지	탐지	전체 탐지, 실시간 탐지를 통하여 악성URL 파일 탐지 및 보고
	탐지내역 조치	탐지된 URL 검역, 부분검역, 예외조치
	관리기능	그레이, 화이트, 블랙 리스트로 URL 관리

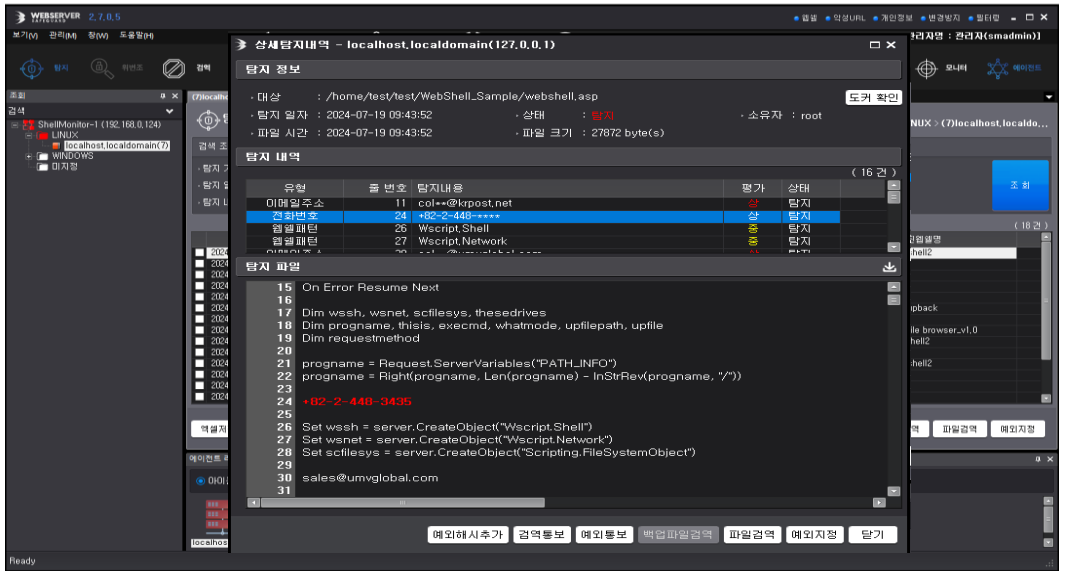




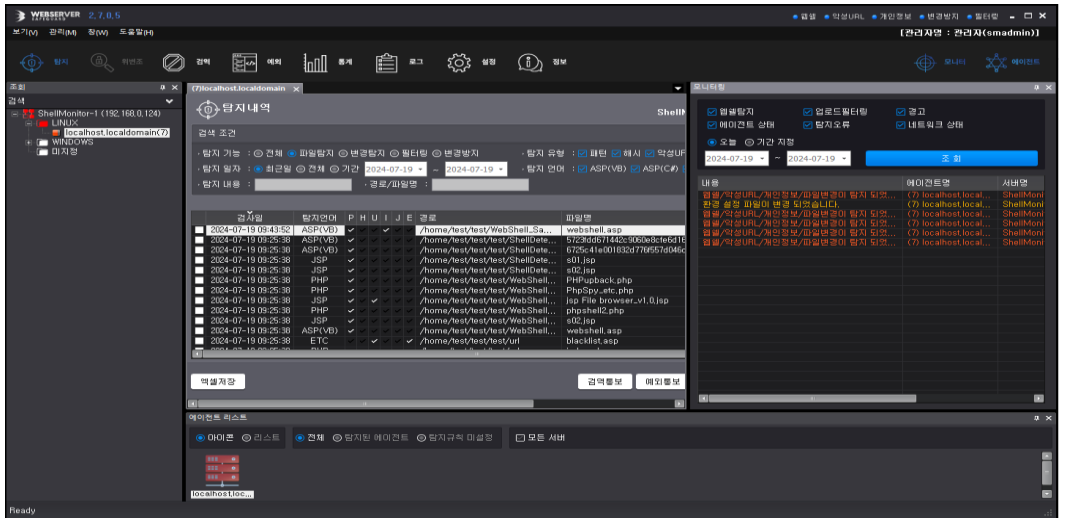
[탐지내역 정보 화면]

상세 기능 : 환경설정 변경탐지 및 기타 기능

기능명	상세기능	설명
웹서버/WAS 환경설정파일 변경방지	웹서버 설정 파일 관리	WEB/WAS 서비스 Scale OUT시 탐지 대상 자동 등록 후 자동 탐지
파일 및 DB 개인정보탐지	개인정보 탐지 (파일)	웹서버 파일 내의 개인정보 탐지 및 보고 (PDF, HWP, DOC, PPT, EXCEL, TXT, etc.)
	개인정보 탐지 (DB)	DB 내의 개인정보 탐지 및 보고
홈 디렉토리 자동찾기	WAS 디렉토리 탐지	웹 루트 디렉토리 자동 탐지
업로드 파일 필터링	파일 필터링	파일 업로드 게시판 허가되지 않은 파일 필터링
침해 대응	공격자 IP탐지	웹쉘 실행 시 웹서버/WAS 로그를 분석하여 실행 IP 보고



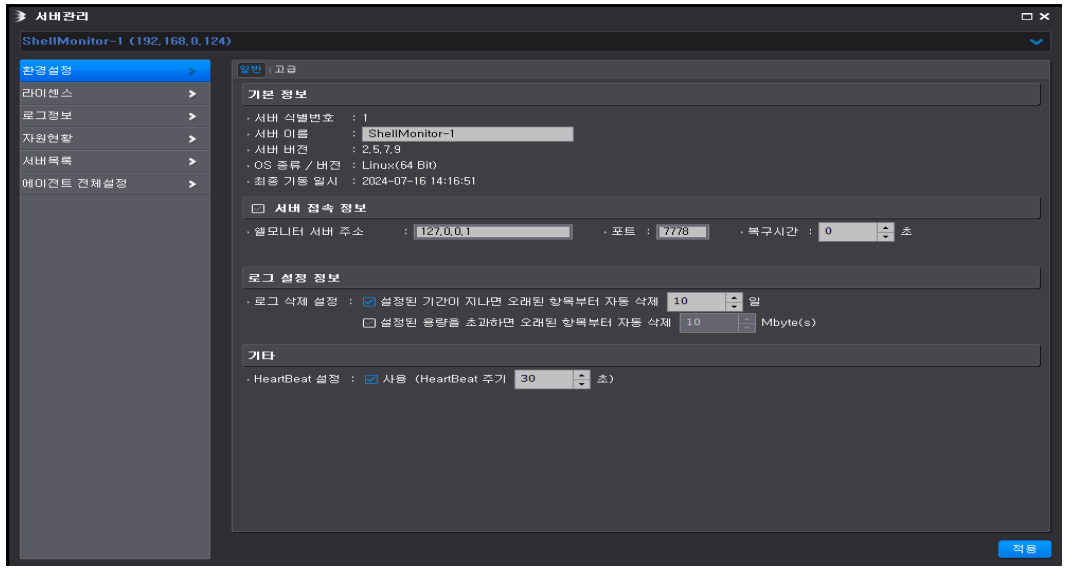
[개인정보 탐지화면]

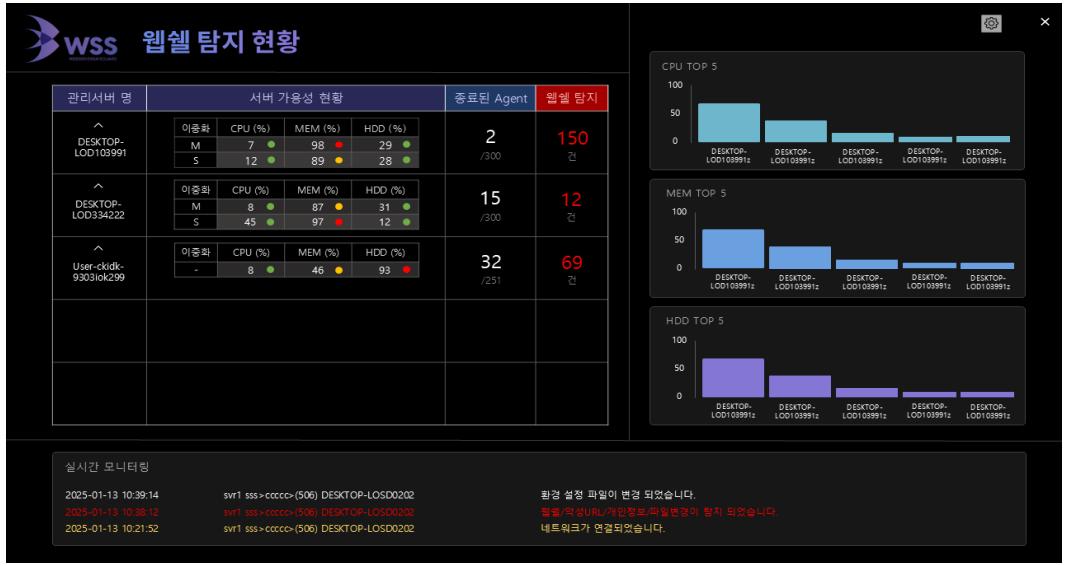


[탐지 알림 화면]

상세 기능 : 관리 기능

기능명	상세기능	설명
관리기능	업데이트 관리	설정자동화, 에이전트, 매니저, 패턴 업데이트 및 버전 관리
	탐지 알림 및 외부 시스템 연동	관제화면, ESM, SMS, EMAIL 등 외부시스템 연동 및 인터페이스 제공(SOAR 연동 API, 웹소켓 API)
	계정 및 사용자 권한관리	계정 및 사용자 별 권한 관리 관리자 권한 방지 기능 추가 예정(26년 상반기)
	통계 및 리포팅 대시보드	보고서 및 통계자료 제공(Excel) 대시보드 제공
	안정성	설치된 웹서버/WAS의 자원 사용 율 조정 관리서버 이중화 지원(Active/Active)

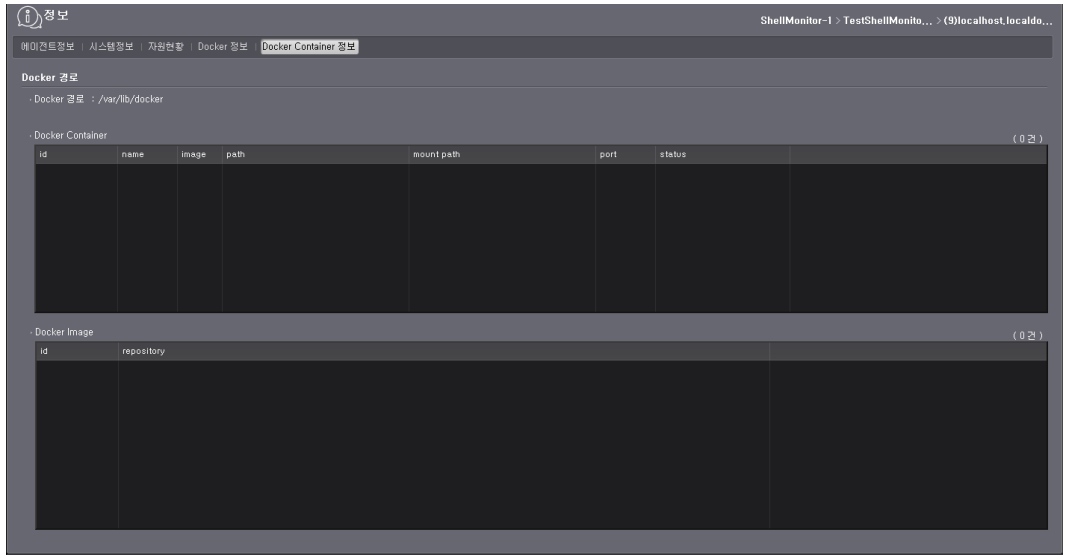




[대시보드 화면]

상세 기능 : 클라우드 지원 기능

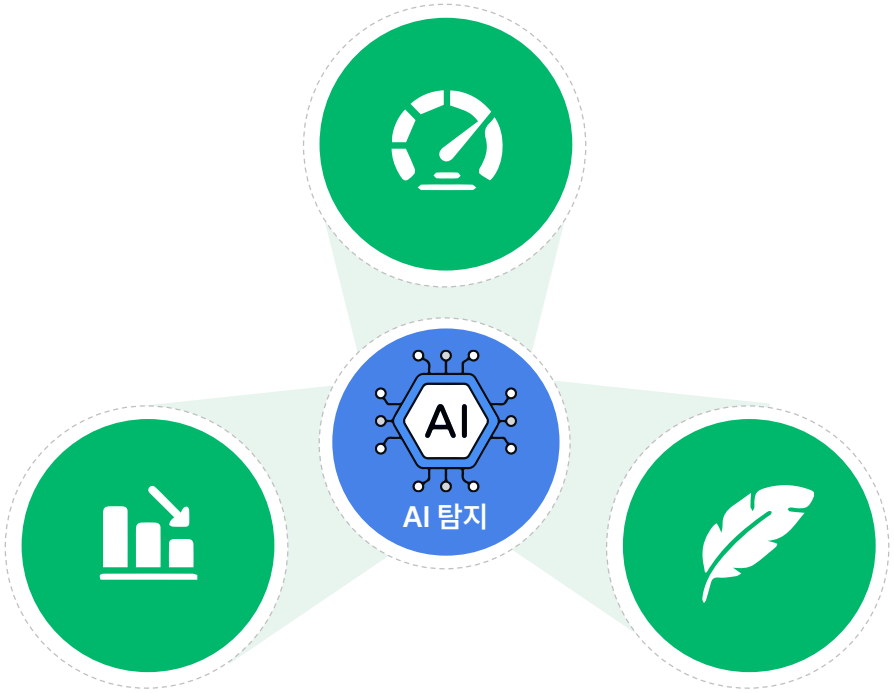
기능명	상세기능	설명
Scale IN/OUT 기능 지원	Scale OUT	WEB/WAS 서비스 Scale OUT시 탐지 대상 자동 등록 후 자동 탐지
	Scale IN	WEB/WAS 서비스 Scale IN 시 삭제 Instance의 탐지/변경/삭제에 대한 이력(로그)을 관리서버로 자동 저장
Docker / Container 도커/ 컨테이너 지원	기본정보제공	Agent 기능에 Docker에 대한 기본정보제공
	에이전트 자동 설치	DaemonSet/SideCar 방식으로 에이전트 자동 설치 제공
	구분 및 처리	탐지된 파일에 대한 Container 구분 및 처리



[Docker Container 정보화면]

[클라우드 가상머신 탐지화면]

상세 기능 : AI 탐지 기능



초고속 분석 및 지능형 탐지

AI기반 탐지엔진과 리소스 최적화로 대용량 파일도 신속하게 처리

알고리즘·패턴·해시+AI 구성으로 신·변종 웹쉘 탐지 및 차단 정확도 최고 수준 달성

Zero Fatigue

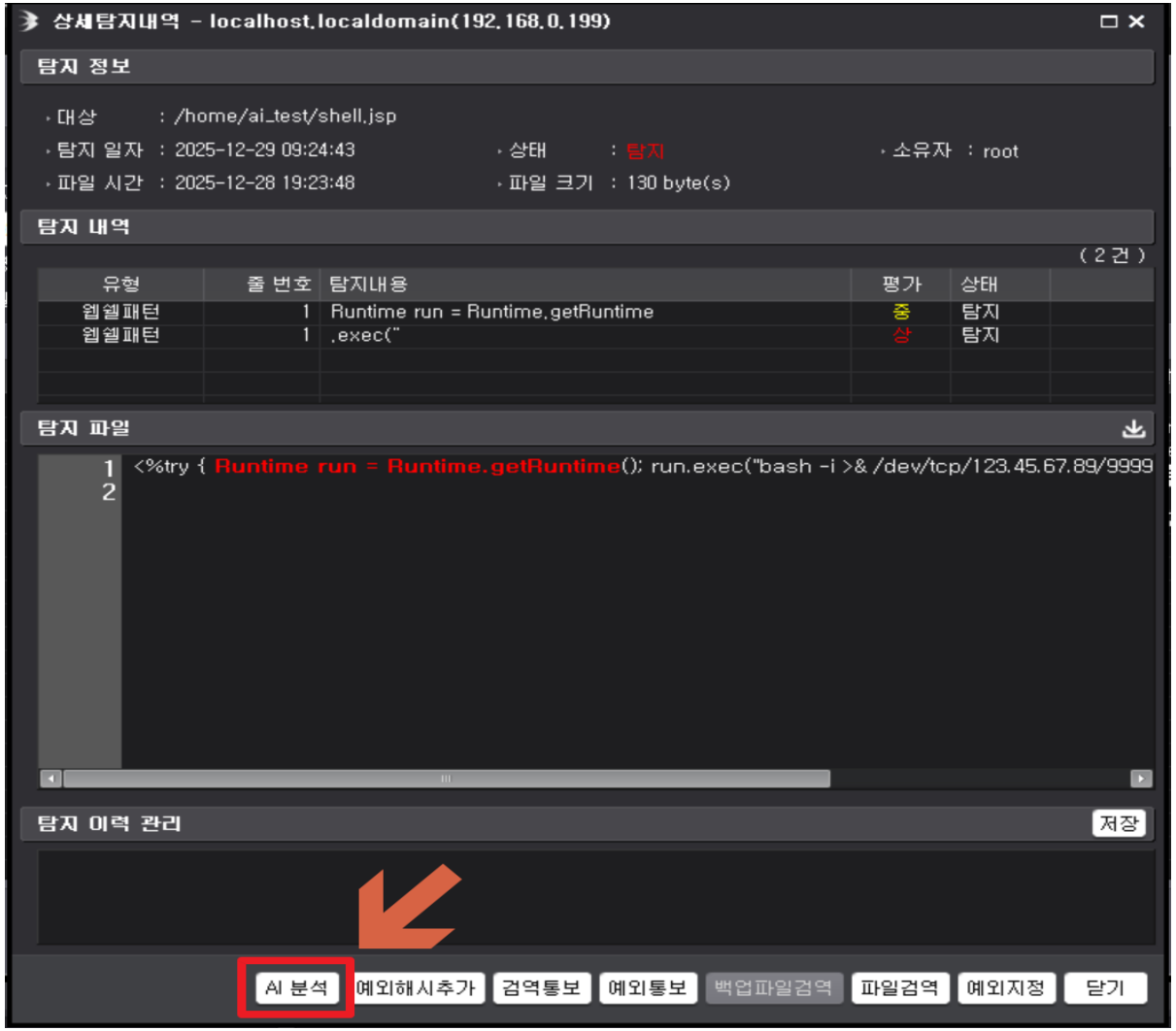
AI 탐지 엔진은 소스코드 전반의 실행 흐름 및 맥락을 분석하고, 실제 악성 행위 여부를 정교하게 판별하여 오탐·미탐 최소화로 관리 효율 극대화

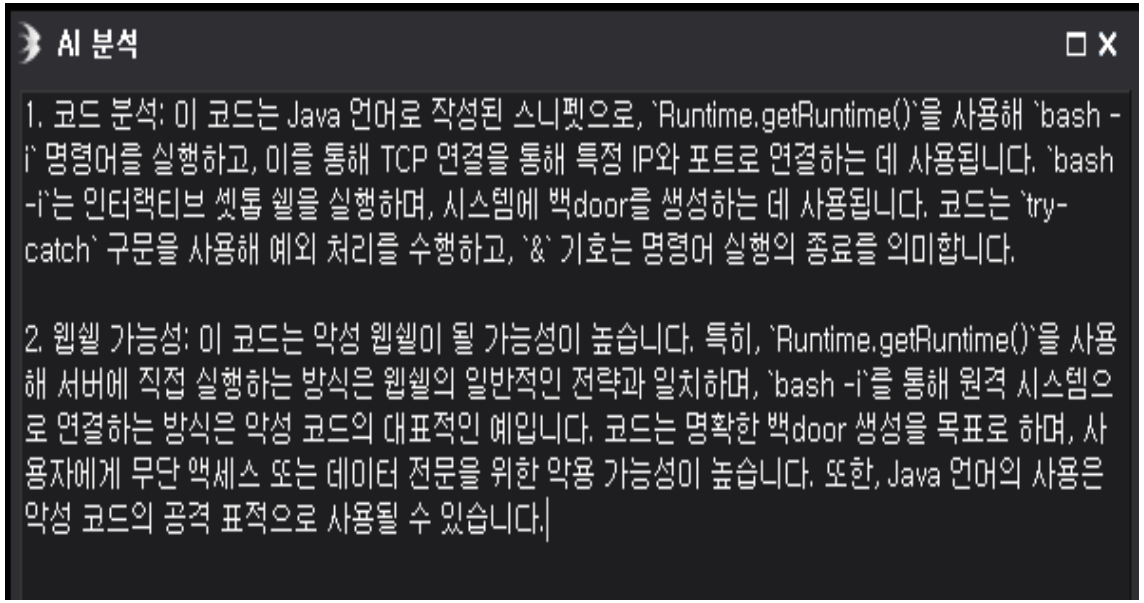
에이전트 경량화

기존 경량 AI 모델에 정교한 파인튜닝을 적용함으로써 연산 효율을 극대화하여, GPU 없이도 CPU 기반 환경에서 안정적으로 동작할 만큼 리소스 사용을 최소화하면서도 고도화된 분석 성능을 확보

10배↑	1/10↓	99.9%
탐지 성능 향상	과탐 · 오탐율 감소	웹쉘 탐지율

상세 기능 : AI 소스코드 분석 기능





[AI 분석] 버튼 및 분석된 결과

[AI 소스코드 분석 상세]

탐지된 웹쉘파일을 AI가 파일의 내용을 직접 읽고 (1) 어떤 기능을 하는 코드인지,

(2) 해킹(웹쉘)에 사용될 가능성이 얼마나 높은지를 쉬운 설명으로 알려줍니다.

솔루션 구성

에이전트, 관리서버, 매니저 프로그램(PC)으로 구성

WSS 에이전트	WSS 관리서버	매니저프로그램(PC)
웹서버/WAS에 설치하는 프로그램 웹쉘 탐지 및 악성 유포지 URL 탐지 웹쉘 탐지 및 필터링 경과 서버 전송 외 JDK 1.5 지원 가능한 Unix, Linux, NT O/S 지원	VM 또는 HW 에 설치하는 서버SW로 WSS Agent에 연결되어 작동 탐지된 이력 및 탐지 정보를 저장 원격 관리 제어 웹쉘 패턴 업데이트 및 에이전트 배포 외	관리자 운영 PC에 설치 (WSS관리서버에 연결) 웹쉘 탐지 실행 모니터링, 원격조치, 환경설정 관리자 권한관리, 통계 & 리포팅 외

실제 도입사례 ①

[S은행]

사업명 웹쉘 탐지 솔루션 재구축 사업 건 (25.12 구매)

개요 원격으로 웹서버/내부WAS에 명령을 수행하는 악성 스크립트 파일, 즉 웹쉘을 방지하고 악성 URL을 통한 바이러스 유포, 파일 시스템 공격 및 암호화, 개인정보유출, 기타 위변조 등의 피해 방지를 목적으로 도입한 사례

효과 타사제품(4개사) 비교우위 선점. 성능 평가, 설치 속도, 유지보수 관련 내용평가를 통해서 WSS 제품으로 선정되어 도입

도입 후 기존 제품 대비 상당히 개선되었다는 평가를 받음

기존 솔루션 대비 다양한 기능 구현 및 신속한 유지보수 대응으로 보안 업무 시 활용 빈도 수가 높아짐

실제 도입사례 ②

[I은행]

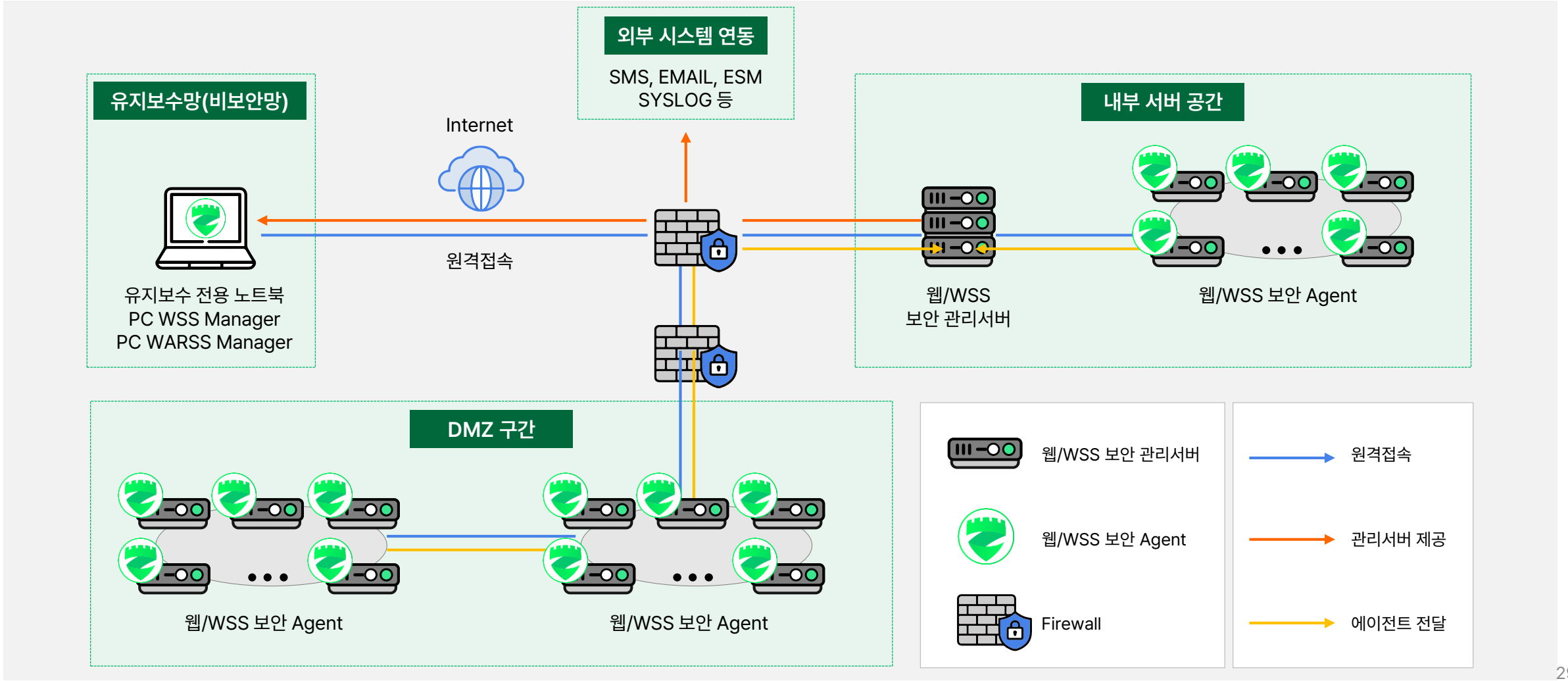
사업명 웹쉘 탐지 솔루션 도입 건 (25.7 구매)

개요 WEB/WAS 서버에 대한 해킹 목적 웹쉘을 탐지·차단하기 위한 솔루션 구축
타사 비교 경쟁을 통해 WSS로 결정 후 도입 한 사례

효과 공정한 비교분석 및 POC를 통해서 WSS의 기능이 가장 우수하다는 판정 되어 도입
특히, 도입 후 요청사항에 대한 대응이 빠르고 CPU리소스 사용률 및 안정성 면에서도 다른 보안제품 대비 뛰어남 평가

실제 도입사례 구성도 ①

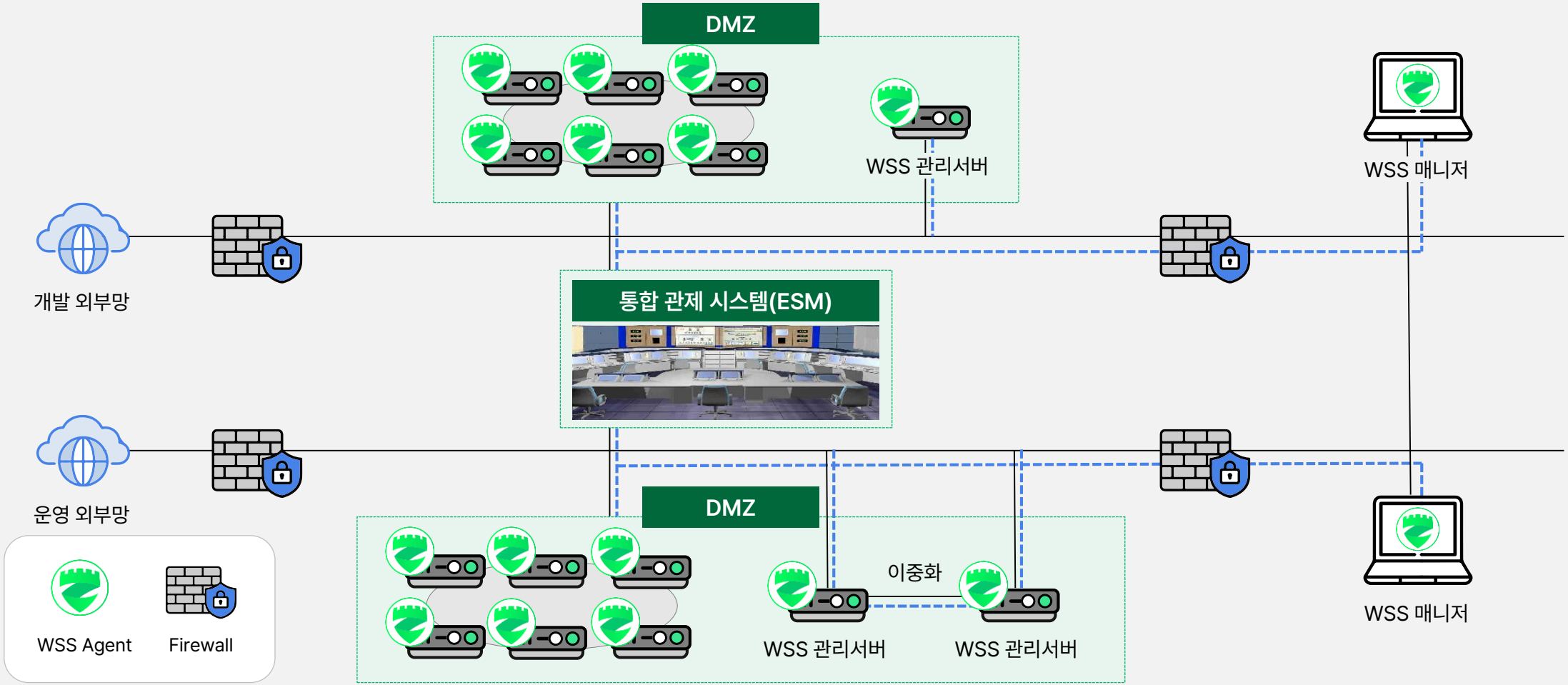
기본 구성도(실제 도입 근거)



실제 도입사례 구성도 ②

00 은행 구성도(25.4월 도입)

IOO 금융사에서는 총 3대의 관리서버와 총 75대의 에이전트 운영이 가능하도록 구축하였습니다.



실제 도입기관 분석

항 목	고객사	초기 구축 시 탐지 개수		실시간 월평균 탐지 개수
구축 6개월 이내	K금융	250개	예외 패턴 적용 및 안정화 단계	10개
	OO결제원	150개		5개
	M금융	120개		4개
	P기업	3,000개		51개
	OO공사	500개		21개
구축 1년 이상	S기업	850개		23개
	H금융	4,000개		23개
	N금융	3,000개		41개
	OO공단	250개		3개
	OO공단	100개		1개

* 외주(협력)업체 : 1차 점검 (탐지 내역 확인, 의심스러운 특정파일 고객사에 전달 등)

* 제 조 사 : 2차 점검 (탐지 내역 확인 및 상세 분석 등)

도입 기대효과

웹쉘 기반 공격에 대한
실시간 선제 대응 가능

기존 보안 체계(WAF, 백신,
EDR)의 탐지 사각지대 보완

개인정보 유출 방지 및
신뢰성과 대국민
서비스 안정성확보

비인가 변경·악성파일 삽입 등
웹서비스 위변조 차단
(2차 공격 차단)

운영 효율성 및 보안 감사
대응력 향상

03. 도입기관

공공기관, 금융, 기업, 대학 · 병원	34

공공기관, 금융, 기업, 대학

공공기관

청와대 · 경찰청 · 외교부 · Ministry of National Defense Republic of Korea · SUPREME COURT OF KOREA · 한국도로공사 · 한국전력 · KARI 한국항공우주연구원 · KORAIL · 한국농어촌공사 · 국방과학연구소 Agency for Defense Development · 행정안전부 국가정보자원관리원 · KOICA · 인천광역시교육청신트리도서관

금융

Hana Financial Group · NH Bank · KDB Bank · SAMSUNG CARD · BCcard · Hyundai Capital · SAMSUNG LIFE INSURANCE · SAMSUNG · KSD 한국예탁결제원 · 롯데손해보험 · iM뱅크 · let: · 신한은행 · meritz · KYOBO 교보생명 · Hyundai Card · 푸본현대생명 · 한국증권금융 · NICE평가정보

기업

amazon web services · Microsoft Azure · SAMSUNG ELECTRONICS · HYUNDAI MOTOR GROUP · LS · Gmarket · AUCTION. · Daiichi-Sankyo · Hanwha · GS · TOYOTA · NICE dun&bradstreet · SK telecom · DAEWOO E&C · CJ CHEILJEDANG · KBS Media · AhnLab · POONGSAN HOLDINGS

대학 · 병원

국립군산대학교 KUNSAN NATIONAL UNIVERSITY · 한국전통문화대학교 KOREA NATIONAL UNIVERSITY OF HERITAGE · 영남이공대학교 Yeungnam University College · 서원대학교 SEOWON UNIVERSITY · 경상국립대학교 GYEONGSANG NATIONAL UNIVERSITY · 한국교원대학교 Korea National University of Education · 국립한밭대학교 · 한국교육개발원 KOREAN EDUCATIONAL DEVELOPMENT INSTITUTE · 경북대학교 KYUNGPOOK NATIONAL UNIVERSITY · 서울과학기술대학교 SEOULTECH · 동원대학교 TONGWON UNIVERSITY · SNUH 서울대학교병원운영 서울특별시보라매병원 · 서울아산병원 Asan Medical Center · SMC 강북삼성병원 · 광주광역시교육청 GWANGJU METROPOLITAN CITY OFFICE OF EDUCATION · 전라남도교육청

umv

㈜유엠브이기술 I www.umvglobal.com I Tel 02-448-3435