CC인증 | GS인증 | 보안적합성 필 | Verified | 국가사이버안전센터 협의체결 | 정보보호관리체계 ISMS | 안전진단 수행기관 | INNOBIZ 기술혁신형 중소기업 | 정보보호대상 (특별상)

대한민국 No.1 위협관리시스템

TESS TMS

TESS TMS / TESS TMS v.6.0 / TESS TMX

KORNIC GLORY

CONTENTS

회사소개

글로벌 IT 보안 전문기업 코닉글로리

2007년 설립되어 IT 시장의 근간이 되는 네트워크 분야에서 인정받는 기업으로 성장하였으며, 국내 최고 수준의 유·무선 보안 기술력을 바탕으로 TMS부분 국내1위(M/S 90% 이상), 국내 최초 WIPS(CC인증 EAL4) 출시 등의 성과를 이루었으며, 기존 네트워크사업과 보안사업을 더욱 강화하여 IT 인프라 구축 및 안전한 유·무선 네트워크 환경을 위한 솔루션 및 서비스를 제공하는 글로벌 IT 보안 전문기업을 목표로 지속적인 성장을 이어가고 있습니다.

주요연혁

2018 12 다크트레이스 파트너
2014 02 라스트라인 단독 총판계약
2012 12 정보보호기술과 합병
2007 05 주식회사 정보보호기술 인수
2007 02 코닉글로리 설립(인적분할)
2001 08 KOSDAQ 상장
1996 08 앤콤정보시스템 설립

사업분야

Security	Solution	R&D
• TESS TMX • TESS TMS • TESS AIRTMS	• 지능형지속위협 대응 – Lastline • 엔터프라이즈 면역체계 시스템 – Darktrace	• 연구 및 개발 프로젝트 • 보안시스템 개발 프로젝트 • 정보보호기술 연구개발 및 산학연구

TESS TMS REFERENCE

주요 부처 및 공공기관 관제센터에
국내 최다 레퍼런스 보유

TMS
시장 점유율
90%이상

주요기관

대전통합전산센터, 광주통합전산센터, ETRI부설연구소, 대통령실, 방송통신위원회, 한국과학기술정보연구원(KISTI), 한국인터넷진흥원(KISA), 우정사업본부, 헌법재판소, 지역정보개발원

17부처

기획재정부, 교육부, 미래창조과학부, 외교부, 통일부, 법무부, 국방부, 행정자치부, 문화체육관광부, 농림축산식품부, 산업통상자원부, 보건복지부, 환경부, 고용노동부, 국토교통부, 해양수산부

16청

통계청, 조달청, 경찰청, 방위산업청, 농촌진흥청, 특허청, 기상청

지방자치단체

경기도청, 경북도청, 전남도청, 제주도청, 충북도청, 광주광역시청, 부산광역시청, 세종특별자치시청, 과천시청, 광명시청, 구리시청, 남양주시청, 당진시청, 부천시청, 상주시청, 서귀포시청, 성주군청, 안양시청, 용인시청, 영주시청, 음성군청, 의성군청, 의왕시청, 진천군청, 제주시청, 제천시청, 청주시청, 충주시청, 칠곡군청, 판교U-city, 하남시청, 광교U-city

공사 / 공단 / 공기업

건강보험심사평가원, 공항철도, 교통기술평가원, 국민건강보험공단, 국민연금관리공단, 국립해양조사원, 대한적십자사, 대한지적공사, 대한주택보증, 대한주택보증무역보험공사, 보건복지정보개발원, 부산항만공사, 선박안전기술공단, 인천국제공항공사, 제주국제자유도시개발센터, 축산물품질평가원, 한국감정원, 한국건설한국공항공사, 한국산업단지공사, 한국수력원자력, 한국수자원공사, 한국시설안전공사, 한국전력거래소, 한국정보통신진흥협회, 한국철도공사, 한국토지주택공사, 한국해양수산연구원, 해양항만청(부산/여수/인천), 해양환경관리공단 외 200여 기관

교육기관

교육과학기술부, 강원도교육청, 경상북도교육청, 광주광역시교육청, 대구광역시교육청, 대전광역시교육청, 부산시교육청, 전라남도교육청, 제주특별자치도교육청, 충청남도교육청, 충청북도교육청, 국립특수교육원

국방관련

사이버사령부, 기무사령부, 방위사업청, 국방기술품질원, 국방연구원, 국방과학연구소, 국방대학교, 정보사령부, 의무사령부, 체육부대, 국군복지단, 자운대

육군본부, 1군사령부, 2작전사령부, 3군사령부, 육군군수사령부, 수도방위사령부, 육군사관학교, 육군3사관학교, 육군보병학교

해군본부, 해군작전사령부, 해군군수사령부, 해병대1사단, 해병대사령부

공군본부, 공군작전사령부, 공군군수사령부, 공군교육사령부, 공군사관학교

금융기관

금융경제원, 코스콤, 시티은행, 외환은행, 한국수출입은행, 한국은행, 금융투자협회, 바클레이즈증권, 리딩투자증권

일반기업

GS홈쇼핑, 보령제약, 현대중공업, 한국무역정보통신, UWAY중앙교육, 현대미포조선, 현대종합상사, 삼성SDS

통신사 / ISP /포탈 / 게임

KT, KTH, LGU+, CADNET, SK네트웍스, CJ시스템즈, mple온라인, NC소프트, 넥슨, 네이버, 다음카카오

병원

일산병원, 연세의료원, 충남대병원, 충북대병원, 경북대병원, 경상대병원, 부산대병원, 제주대병원, 전남대병원, 전북대병원, 강원대병원, 서울대병원, 서울치대병원, 울산대병원

대학

서울대학교, 서울시립대학교, 포항공과대학교, 인하대학교, 단국대학교, 경기대학교, 강원대학교, 공주대학교, 광주교육대학교, 동아대학교, 백석대학교, 부경대학교, 부산대학교, 서울과학기술대학교, 연세대학교, 원광대학교, 전남대학교, 제주대학교, 충북대학교, 강릉원주대학교, 한밭대학교, 한남대학교

해외

앙골라 국가 데이터센터, 모로코 MACERT센터, NHN-Play art LINE

TESS TMS

다양 · 지능화된
사이버 위협에 대한 체계적인
보안관제 및 대응시스템

※ 시장점유율 90%이상인 TESS TMS는 주요 부처 및 공공기관 관제센터에 대한 최다 레퍼런스를 보유하며 그 안전성과 우수성을 인정받고 있습니다.

- 인터넷 웜, 바이러스, 해킹 등 각종 사이버 위협에 대한 조기탐지 및 분석 · 대응시스템
- 사이버 위협에 대한 조기 예/경보를 통하여 피해확산 방지 및 완화를 위한 종합관제 및 대응시스템
- 글로벌 이상징후와 로컬 이상징후 모니터링으로 종합적인 네트워크 분석 수행
- 조직체계에 맞는 보안정책 관리 및 관제 방안 제시
- 신속한 의사결정 기반 마련으로 통합보안관리체계 구축
- 조기 예경보 체계 구축으로 즉각적인 원인분석 및 대처방안 수립

TMS의 업무 흐름도

조기 예/경보

전세계 위협 정보

- 전세계 위협정보서비스를 통해 사전 예/경보 (200개국 240,000개 센서)

국내 위협 상황

- 국가주요기관(국정원, KISA)에서 발령하는 위협등급을 통해 국내 사이버 위협 현황 파악

국가기관 PCRE 패턴 지원
(국가기관용)

종합 관제/원인 분석

가상화 + 종합상황도

- 가상화를 통해 내부 활동 주체의 변화감지
- 종합 상황 지도를 통해 직관적으로 위협 모니터링

트래픽 + 보안 정보

- 실시간 침입탐지
- 트래픽 분석 정보
- 네트워크 이상징후 탐지

Security + Network

- 보안과 트래픽 정보간 상관관계 분석

Anomaly

- Zero-day threat 대비를 위한 최신기법의 이상징후 탐지

의사결정 수단/대응방안 제시

신속한 의사결정 수단

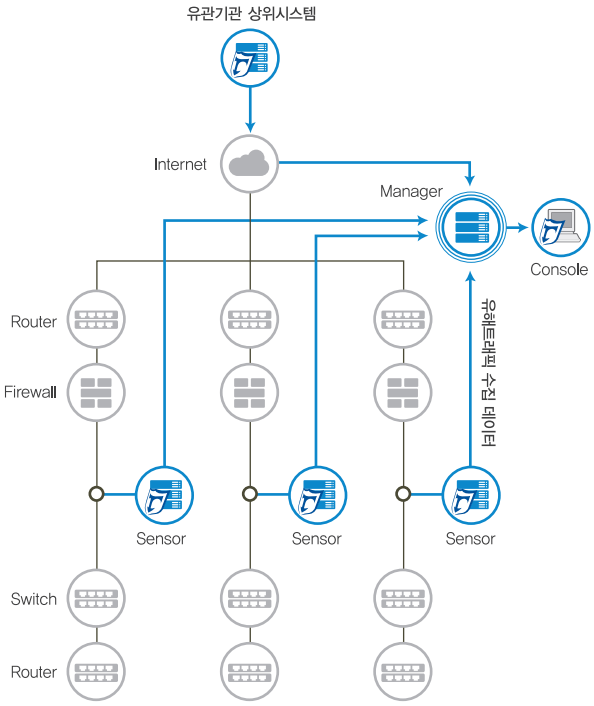
- 공격을 유발시킨 공격자, 트래픽 종류 등을 직관적으로 조회

대응 수단 제시

- 원인분석 결과를 통하여 방화벽, IPS 등 기타 보안 장비를 통해 대응 실시

	방화벽 연동 차단
	라우터 ACL 적용
	기타 보안장비 연동

TMS 제품 구성



위협관리시스템 TESS TMS WEB

- 종합상황도 : 로컬 · 글로벌 위협정보 및 분석을 통해 대응하는 시스템
- 종합적위협상황정보 : 침입탐지 · 유해트래픽 및 상관관계분석 통계 정보
- 조기 예경보 및 취약성 정보 제공으로 종합적 분석 및 판단근거 제시

위협분석 통계정보

위협분석시스템 TESS TAS Manager

- 구간별 침입탐지 및 트래픽 정보 분석
- 네트워크모니터링, 침입탐지분석, 이상징후 분석,공격유형 및 트래픽 분석
- 보안정책, 계정관리 등 운영에 필요한 설정
- DBMS에 DATA 저장

유해트래픽 수집 후 전송

유해트래픽 수집시스템 TESS TAS Sensor

- 전체 트래픽 / 유해트래픽 수집
- 주요구간에 TAP을 이용한 설치
- 실시간 유해트래픽 탐지현황 및 모니터링
- 정규표현식 등 관련 시그니쳐 적용

주요 기능

위협분석	위협분석	글로벌/로컬 실시간 위협 수준 정보, 위협상황추이정보, 전체/기관별 위협 발생 현황 분석, 전체/유해트래픽 추이 분석, 서비스 트래픽/공격유형 탐지(TOP5)정보, 최근 위협정보 및 예경보 발령 조회
	이상징후 탐지	프로파일 기반에 따른 트래픽과 이벤트에 대한 이상징후 탐지/분석 기능
	상관관계 분석	전체/유해트래픽 간 상관분석, 이벤트/트래픽 간 상관분석, 서비스 포트/공격유형 간 상관분석(취약점 정보 및 악성코드 정보 활용)
이벤트	침입탐지 분석	PCRE기반 탐지, 사용자 정의 패턴 탐지, Anomaly 기반 탐지, DoS/DDoS탐지, Worm/Virus탐지, 공격유형/공격자 IP/피해자 IP /피해 포트 별 추이 분석, 침입탐지 RAW DATA 제공
	실시간 모니터링	전체/유해트래픽 현황 모니터링, 비정상행위 현황 모니터링, 위협상황 모니터링, Session 모니터링, 시스템 상태 및 장애 모니터링
트래픽 분석		트래픽 추이 / 트래픽 순위 / 점유율 분석, 프로토콜 / IP/ 서비스 포트 / 프레임 크기 / TCP-Flag 별 트래픽 분석 정보, PPS, BPS 및 INBOUND, OUTBOUND 데이터 정보
운영관리	정책관리	실시간 LiveUpdate, 예/경보 설정, 침입탐지 정책 설정, 임계값 설정, 침입탐지 예외설정, 이상징후 탐지 설정, 감사로그 설정 등
	감사기능	시스템 상태/ DB사용량 등 시스템 감사로그 및 추이 그래프, 정책 이력 리스트, 감사로그 제공
보고서		일간/주간/월간 경향 분석 보고서, 트래픽/침입탐지 분석보고서, TOP10 공격형태, 공격자, 피해자 분석 및 통계 보고서, 예약보고서 기능 제공

TMS의 특장점

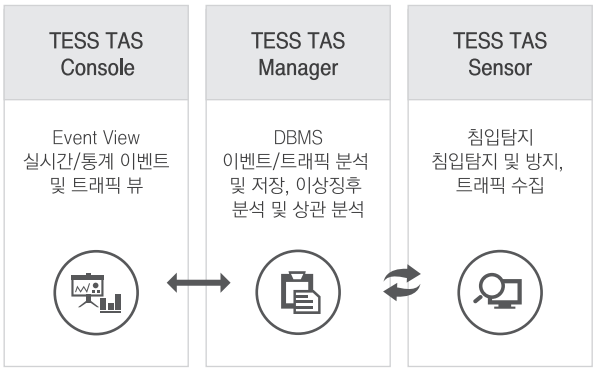
1 국내외 위협 상황 정보

글로벌 위협정보 / 국내 위협정보

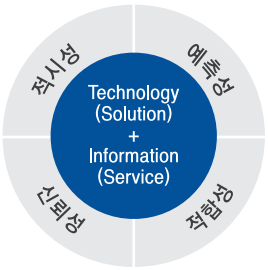
- 시만텍과 연계하여 Global 위협 정보 제공
- 국내외 인터넷 위협 등급 서비스
- 국내외 보안 뉴스 서비스
- 악성코드 및 대응 정보
- 취약점 및 패치 정보 제공

2 안정적인 3-Tier 아키텍처

안정적인 3-Tier 아키텍처



3 신뢰성 있는 정보 제공



- 기술과 정보의 적시성
- 위협 이상징후/상태변화 조기 감지
- 신뢰성 있는 글로벌 위협정보 신속 제공
- 정교한 분석 정보를 통한 최적의 대응

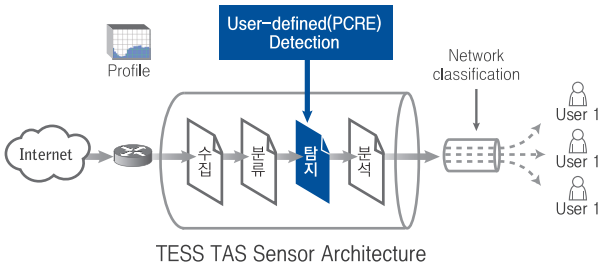
4 위협 탐지 및 트래픽 상관 분석

침입탐지 분석	트래픽 분석
패킷 분석	트래픽 수집
침입탐지/침입방지	트래픽 분류
패킷 분석	트래픽 추이 분석
이벤트 간 상관 분석	트래픽 로깅

상관 분석

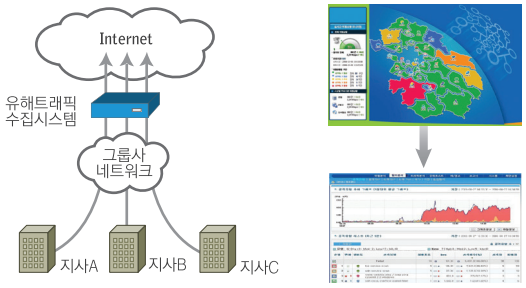
- 이벤트/트래픽 간 상관 분석
- 트래픽 이상 징후 탐지
- 유해트래픽 산정 및 예측
- 위협에 대한 조기 대응

5 트래픽 기반 이상 징후 탐지



- 프로파일 기반의 이상 징후 탐지
- PCRE 기반의 정확한 침입탐지

6 가상화(Virtual & Visual)



- 가상화를 통한 직관적 뷰(View)
- 가상화를 통한 네트워크 관리
- 가상화를 통한 센서 통합
- 통합 설정 및 관리

TESS TMS v6.0

최신 APT 공격과
진화하는 사이버위협 대응을 위한
차세대 위협관리시스템

TMS v6.0 핵심기술

악성파일 탐지엔진

- 네트워크 전송 파일 수집
  - 수집된 파일 및 이벤트 실시간 조회/확인
  - 파일 해시 정보조회 및 악성유무 판별
  - MicroSoft Office File, Hwp, Hwpx, PDF, ZIP, GZIP 등

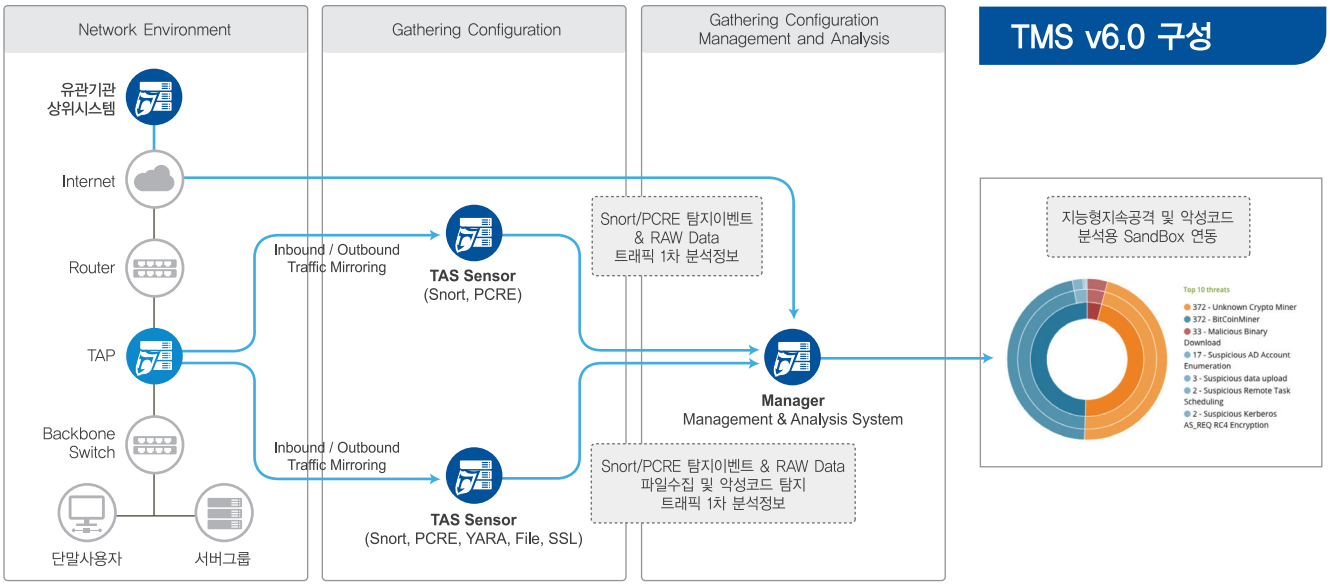
애플리케이션 탐지기술

- HTTP / DNS / TLS 탐지기술 적용
- SMTP 등 메일과 파일전송 응용계층 탐지 지원
- 지속적인 애플리케이션 유형 추가 및 업데이트

TMS v6.0 특장점

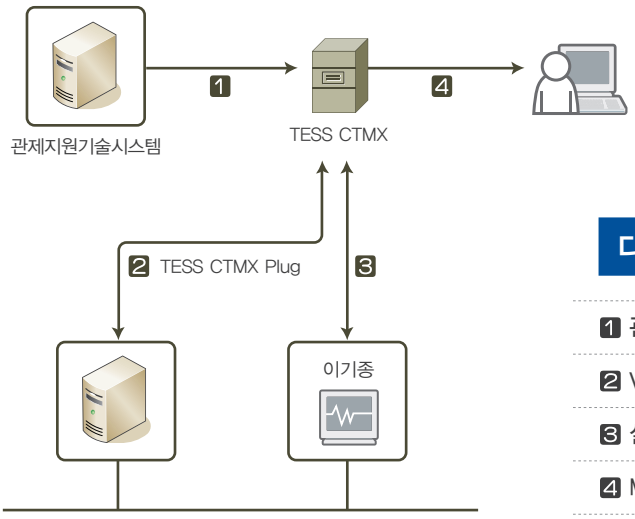
차세대 위협탐지	SandBox 연계	SandBox 연동을 통한 악성코드 및 APT 공격대응
	PCRE / YARA / Application	PCRE / YARA 및 애플리케이션 완벽지원
위협탐지 및 분석	고성능 패킷처리	패킷수집 전용카드 탑재, 멀티코어 & 멀티스레딩
	RAW 데이터 수집	SNORT / PCRE 기반 탐지 및 원본 데이터 수집
	파일수집	트래픽 내 전송되는 파일 자동탐지 및 수집
사용자 인터페이스	Web 기반의 직관적 UI	데이터 시각화 및 통계 데이터에 대한 직관적 UI 제공
	실시간 분석지원 강화	실시간 이벤트 분석 및 편의성 강화
복호화	SSL 통신 복호화	HTTPS 트래픽에 대한 RSA 기반 복호화 지원
	애플리케이션 탐지	패킷탐지 영역을 확대한 애플리케이션 탐지와 자산학습

TMS v6.0 구성



TESS CTMX

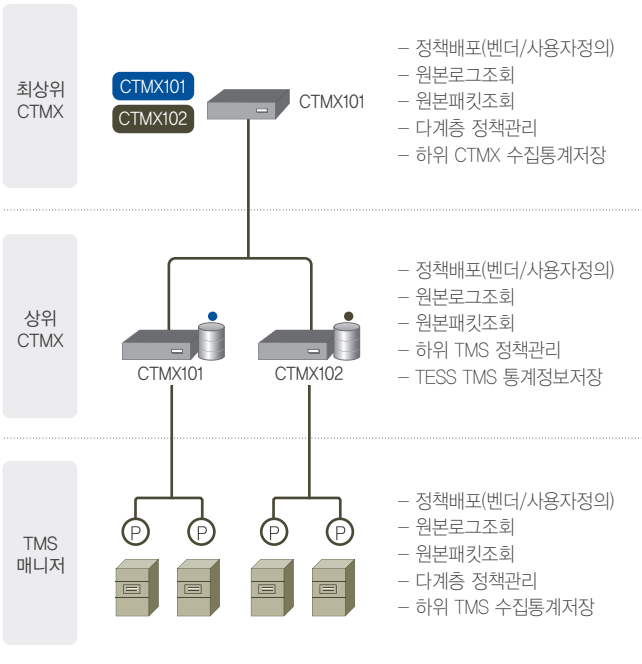
TESS TMS를 통합하고 계층적 관리
다계층 통합관리와
통합정책관리를 위한 TESS CTMX



다계층 관리의 TESS CTMX 동작방식

- **1 관제기술지원시스템 연계 :** 정책 배포 시스템 클라이언트 연동
- **2** Vendor Signature : 코닉글로리 시그니처 통합 배포
- **3 실시간 이벤트 모니터링 :** 24시간 실시간 관제 기능
- **4** MOM(Manager of Manager) : CTMX Station 간 다계층 구성 지원

TESS CTMX 구성 및 주요 기능



1 통합정책관리

– 분산 운영 중인 TMS의 정책을 효과적이고 효율적으로 관리
– 분산된 TESS TMS의 탐지정책을 통합적으로 배포·관리

2 다계층 통합관리

– 물리적으로 분리된 업무에 따라 계층적으로 구성된 네트워크 환경을 업무 및 구성계층에 따른 관리기능을 제공
– 정책배포, 원시로그 및 패킷 조회를 실행하여 물리적으로 원격지에 있는 TESS TMS 및 TESS CTMX의 수집로그를 조회·분석

3 통합위협분석

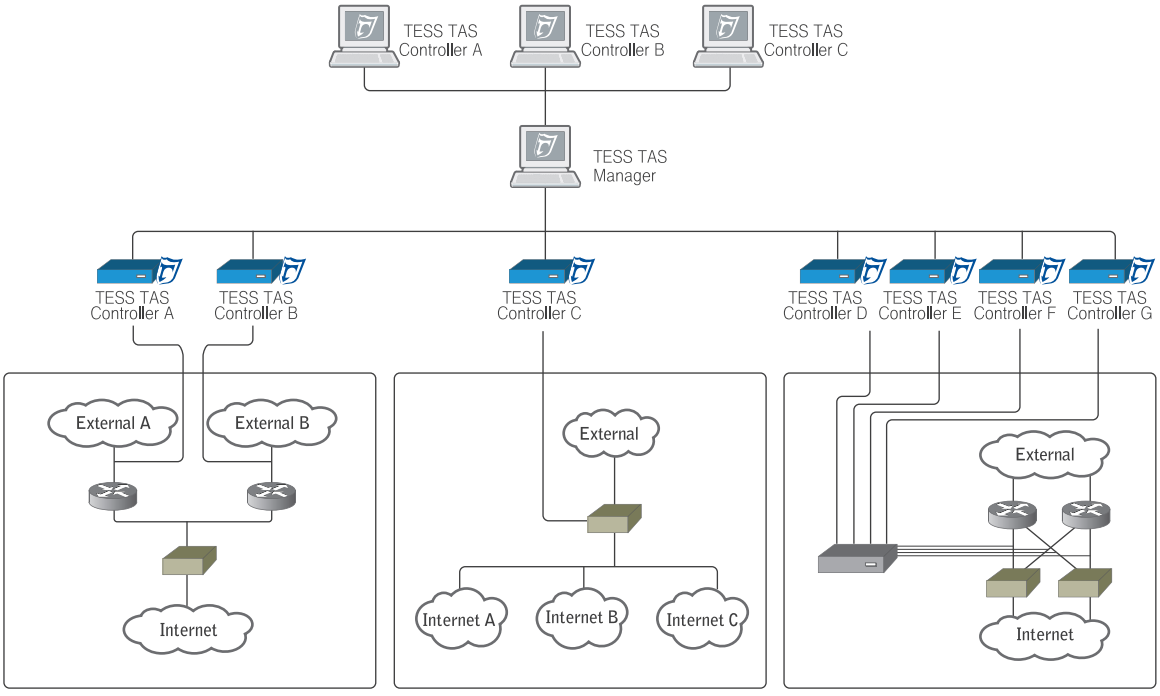
– 글로벌 이상징후와 로컬 이상징후를 모니터링
(시만텍의 글로벌 위협정보 및 위협레벨정보와 TEE TMS에서 탐지된 로컬 위협정보와 트래픽위협정보)
– 지관적 관리를 위한 커스터마이징된 통합대시보드
(고객의 위협관리 요구에 맞도록 고객의 네트워크 보호자산에 대한 지원)

TESS TMS CASE STUDY

다양한 상황별 구축 및 활용사례를 통한 TMS 구성 및 관제업무의 효율성 극대화

- 다수의 다양한 구축경험을 바탕으로 고객에 대한 신뢰성 제공
- 상황별 네트워크 구성사례를 통한 최적화된 안정적 구성지원
- 기능별 활용사례를 통한 단계별 업무대응의 효율성 확대
- Zero-day공격 위협에 대한 대응책과 대응 사례를 통한 관제의 효율성 극대화

[구성사례] 다양한 네트워크 환경 지원



네트워크 환경 1 [일반적인 환경]

- 물리적인 환경과 관리 체계가 동일한 환경
- 모니터링하고자 하는 네트워크에 센서를 설치
- 물리적인 센서 별로 모니터링 실시

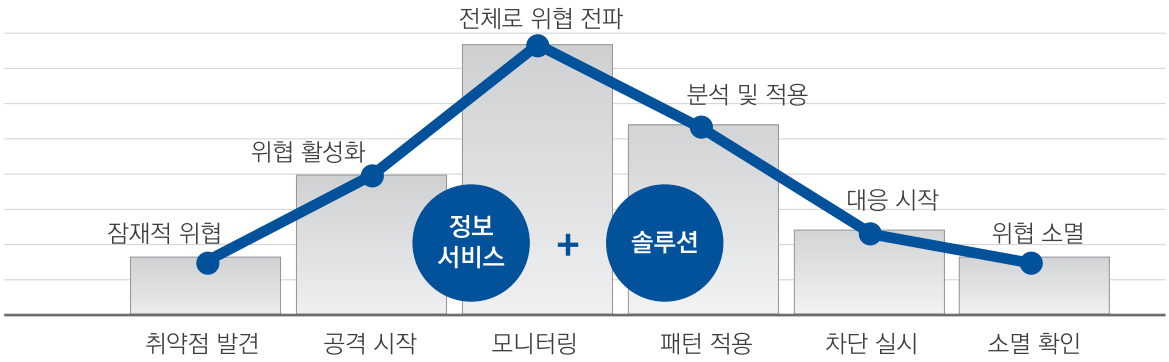
네트워크 환경 2 [회선의 논리적인 분리]

- 다수네트워크를 하나의 물리적인 센서로 모니터링(가상화 지원)
- 네트워크를 가상화하여 물리적인 하나의 회선을 IP, VLAN, URL 등을 기준으로 가상화

네트워크 환경 3 [회선의 논리적인 통합]

- Mesh 구조의 네트워크 모니터링
- 센서를 가상화하여 센서별 모니터링
- 물리적인 여러 개의 센서를 하나의 센서로 가상화

Zero-day 공격 위협에 대한 대응책과 대응사례



- Zero day Thread의 적절한 대응을 위해서는 정보서비스와 솔루션의 대응이 필요
- 실제 Exploit 탐지보다는 취약점 기반의 탐지 및 유연한 탐지 기법 제공
- 신규 사이버 위협에 대처하기 위한 비정상 행위 탐지 기법 적용

TMS를 활용한 DDoS 대응사례

※실제 국가기관 '주의' 경보 발령은 DDoS 발생 후 7/8 02시 40분 발령

1 조기예경보
5월 MS 관련 취약점 사전 리포팅
7월 5일 트래픽 기반 이상징후 예/경보 발령

TMS 조기 예 · 경보(7/6 14시경)

2 위협발생
DDoS 발생
(국가CERT 발령)

TMS'주의' 경보발령(7/6 14:21)

3 정보수집 1차 대응
TMS 긴급탐지 패턴 배포 및 적용
(사용자정의 패턴)

TMS Traffic 추이 분석

4 분석
DDoS 발생
추이 분석

4 분석
공격 참여 시스템 트래픽
발생 추이 분석

TMS 공격자 분석

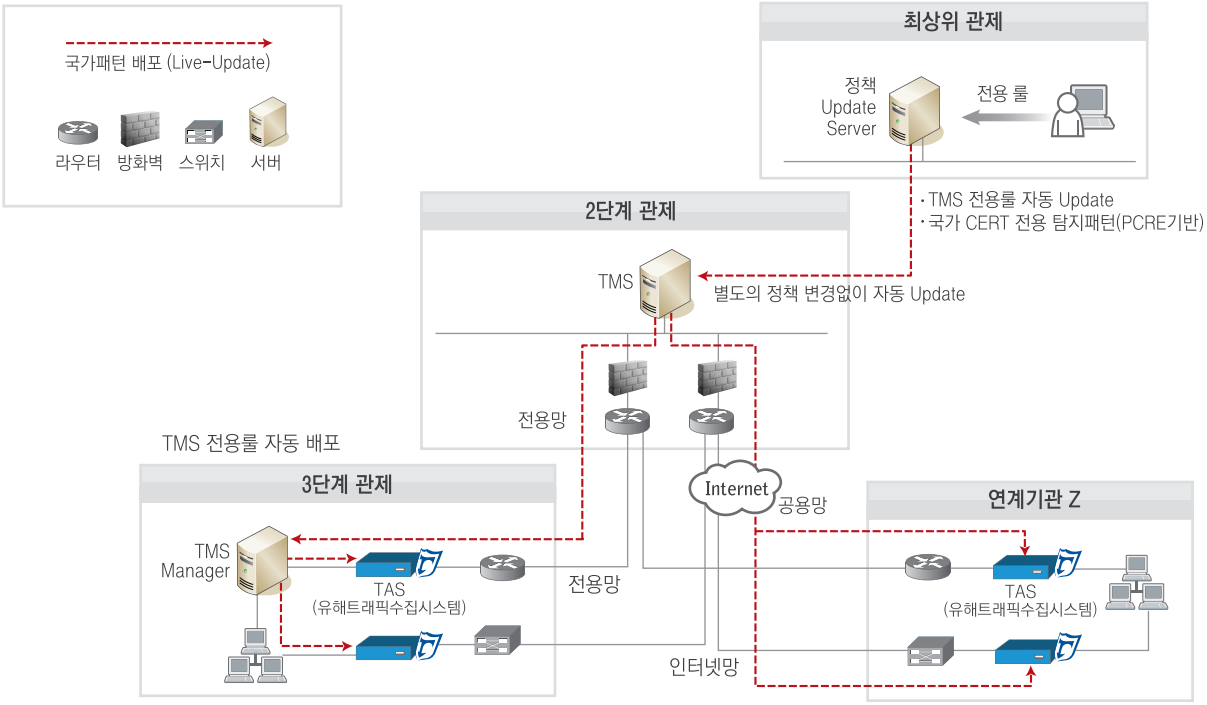
5 정보수집 1차 대응
RAW DATA 분석을 통한 오탐
여부 최종 확인

TMS 피해자 IP 분석

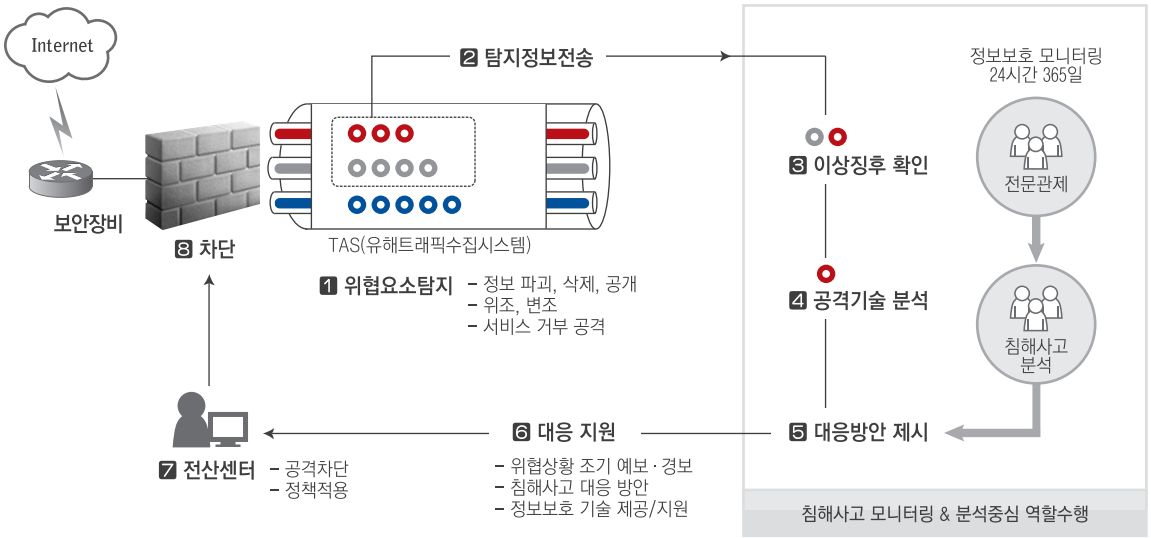
6 위협발생
TMS DATA를 이용한 차단
정책 제작 및 적용 전환

RAW DATA 분석 및 대응 권고

다계층 보안 관제 체계 및 PCRE정책 배포 사례(3단계 관제)



TMS를 이용한 관제 대응 Process



공격 트래픽 공격의심 트래픽 정상 트래픽

- **위험요소 탐지 및 정보 전송** – 실제 위협 요소들을 조기에 탐지하여 탐지 정보를 분석시스템으로 전송
- **실시간 이상징후 확인 및 분석** – 전송된 정보들을 바탕으로 상관 분석 및 이상징후 유무 분석을 통하여 효과적인 공격기술에 대한 대응 방안을 마련
- **상황별 예경보 및 위협요소 해제** – 탐지된 위험에 대한 조기 예보/경보로서 관리자에게 상황을 인지시키며, 신속하고 정확한 대응으로써 위험 요소 제거

제품별 H/W 권장사양

구분	제품명	CPU	MEM	HDD	NIC	인증
통합위협관리시스템	**TESS CTMX**	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45	CC EAL2
위협관리시스템	**TESS TMS v6.0 Manager**	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45	CC EAL4 GS인증
	TESS TMS v6.0 Manager (DBMS 포함)	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45	
유해트래픽 수집시스템	**TESS TAS 1000SC**	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45 1G x 2Port	CC EAL4 GS인증
	TESS TAS 1000SC(R1)	2.1GHz +	16GB +	2TB +	1000Base-T, RJ45 1G x 2Port	
	TESS TAS 1000SC(R2)	2.1GHz +	16GB +	2TB +	1000Base-T, RJ45 1G x 4Port	
	TESS TAS 2000SC	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45 1G x 4Port	
	TESS TAS 2000SC(R1)	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45 1G x 4Port 10G x 2Port(확장)	
	TESS TAS 4000SC	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45 1G x 8Port	
	TESS TAS 4000SC(R1)	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45 1G x 4Port 10G x 2Port(확장) 1G x 4Port(확장)	
	TESS TAS 10000SC	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45 10G x 2Port 10G x 2Port(확장)	
	TESS TAS 20000SC	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45 10G x 4Port	
	TESS TAS 40000SC	2.1GHz +	16GB +	1TB +	1000Base-T, RJ45 10G x 2Port or 4Port	
	TESS TAS 50000SC	2.40GHz +	16GB +	1TB +	1000/10000Base-T x 2Port	

KORNIC GLORY
(주)코닉글로리
06045 서울시 강남구 학동로 155, 원영빌딩 3층~4층 **T.** (02)3476-4200 **F.** (02)3476-4215 www.kornicglory.co.kr