Samsung SDS

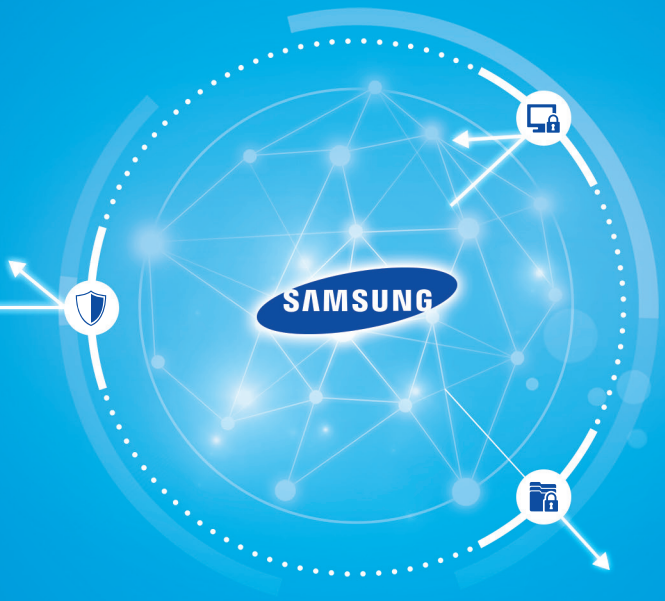
Cyber Security Offerings

삼성은 20년간 그룹 보안운영 경험을 통해 축적된 노하우와 고유의 보안관리 원칙을 기반으로 기업에 맞는 최적의 『컨설팅–솔루션–서비스』 제공

원칙1
Intruder Root–out

외부 해킹 공격으로부터 정보시스템 보호

24x365 보안관제
- 홈페이지 해킹
- DDoS 공격
- 악성코드 감염
- APT 공격 등



원칙2
Insider Lock–in

내부 취약점 제거

정보유출 차단 및 모니터링

암호화된 문서공유, 모바일오피스 등 안전한 정보유통환경 제공

원칙3
"White Elephant" Strategy

데이터 암호화 및 권한관리로 정보유출을 대비

PC, 서버內 주요정보 보호

솔루션 포트폴리오

컨설팅	솔루션					서비스
IT취약점 진단	네트워크	방화벽	IPS	DDoS차단		방화벽 관제
보안관제 수준진단	인증	FIDO[1]				홈페이지 관제
기업보안관리 수준진단	PC/서버	PC보안	PC 문서보안	서버 문서보안		악성코드 관제
	모바일	EMM[2]				APT 관제
	위협관리	홈페이지 관제	악성코드 관제	APT 관제	SCAN	TMS
	기타	대용량 파일 고속전송	인프라관제			

※ 이 외 솔루션은 삼성SDS 전문 파트너社를 통해 제공

[1] FIDO(Fast IDentity Online): 생체정보 기반의 사용자 인증 [2] EMM(Enterprise Mobility Management): 기업형 모바일 관리 솔루션

Samsung SDS
Cyber Security Offerings

	명칭		설명
컨설팅	IT취약점 진단		전문해커 모의해킹을 통한 IT시스템 보안진단
	보안관제 수준진단		보안관제체계 진단을 통한 보안 관제 고도화
	기업보안관리 수준진단		삼성고유의 보안수준진단을 통한 보안관리 성숙도 측정
솔루션	네트워크	방화벽	비인가 네트워크 차단
		IPS	네트워크 유해 트래픽 침입차단
		DDoS차단	DDoS(서비스 거부공격) 탐지 및 차단
	위협관리	홈페이지 관제	웹서버內 악성 웹쉘 업로드 時 탐지/격리
		악성코드 관제	유입되는 파일에 대한 악성여부 탐지
		APT 관제	내외부間 네트워크 분석을 통한 APT공격 탐지
		SCAN	웹, 서버, DB에 대한 보안 취약점 점검
		TMS	네트워크 보안장비 모니터링 및 통합관리
	인증	FIDO	지문, 얼굴 인식 등 생체정보 기반의 사용자 인증
	PC/서버	PC보안	외부 저장장치, 네트워크 사용 등 통제
		PC 문서보안	전자 문서 암호화, 사용권한 등 통제
		서버 문서보안	서버內 전자 문서 암호화 및 사용권한 통제
	모바일	EMM	기업형 모바일 보안관리 및 정보보호
	기타	대용량 파일 고속전송	소프트웨어 기반 대용량 파일 고속전송
		인프라관제	서버/네트워크 등 장비성능 및 장애 모니터링
서비스	방화벽 관제		과다통신, 좀비PC 탐지 및 조치권고
	홈페이지 관제		홈페이지 공격/해킹 탐지 및 조치권고
	악성코드 관제		악성파일 유입탐지 및 조치권고
	APT 관제		Advanced Persistent Threat 탐지 및 조치권고

삼성SDS

IT취약점 진단

모의해킹을 통한 IT시스템 보안취약점 진단 및 개선 가이드 컨설팅

필요성

IT시스템 보안취약점 진단의 요구 증가

최신 해킹공격 기법에 대한 대응수준 파악
발생 가능한 해킹위협 및 내부 보안사고 사전예방
보안취약점 원인분석을 통한 조치방안 도출

서비스 개념

최신 해킹기법에 대한 대응수준을 파악할 수 있도록 IT 인프라 및 응용 시스템에 대한 침투 테스트를 수행하고 원인 분석을 통한 보안위협 선제 대응체계 제공

주요 특징

삼성 고유의 체크리스트 기반의 IT시스템 모의해킹 서비스

- 16개영역 333개 통제항목으로 구성된 ITSI[1] 기반 IT인프라 취약점 점검
- White Hacker에 의한 모의해킹 및 대응수준 진단
- APT/악성코드 테스트를 통한 보안관제 및 대응절차 진단

자동 및 수동 진단 병행을 통한 효율성 극대화

- 진단경험을 바탕으로 자체 개발한 웹취약점 스캐너 활용
- 시나리오별 정보유출 시도, 로직 추측, 파라미터 변조 등 공격자 입장에서 확인된 취약점을 이용하여 침투 테스트 실행

보안 가이드 제공

- 진단 결과에 따른 조치가 가능하도록 보안가이드 제공
- 운영자, 보안담당자 대상 보안교육 제공

[1] IT Security Index: 각종 보안법률, 국내외 보안기관 보안공지 취약점 등을 반영한 보안 취약점 진단 점검 항목 Checklist

주요 서비스

모의해킹 대상 시스템 분석

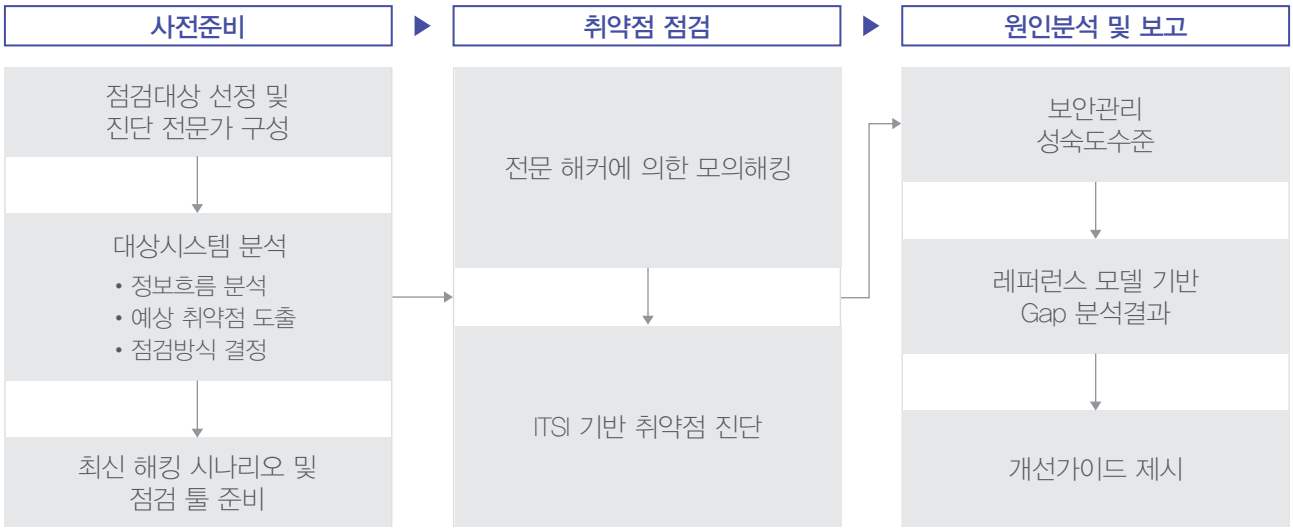
정보흐름 분석 및 예상 취약점 도출
취약점 점검대상 시스템 정의

모의해킹 및 취약점 점검

시스템/서비스 대상으로 해커와 동일한 입장에서 모의해킹
악성코드/APT공격 형태의 자료유출 및 내부접근 가능성 점검
취약점 점검 프로그램을 통한 취약점 확인 및 추가 모의해킹

개선과제 수립

취약점 및 원인분석에 대한 진단결과 보고서
진단영역별 주요원인에 대한 조치방안 제시
우선순위에 따른 Quick Fix/단기/장기 개선과제 제시



기대효과

다양한 공격기법을 통한 정보유출 방지

발견된 취약점을 이용한 위협 시나리오 인지
기업 중요정보 및 고객 개인정보 유출을 위한 최신 공격 대응

개선가이드에 따른 IT시스템 보안 강화

도출된 개선사항을 바탕으로 보안강화 과제계획 수립 및
보안관리 체계 고도화

삼성SDS

보안관제 수준진단

보안관제 체계 진단을 통한 보안관제 수준진단 및 고도화 컨설팅

필요성

보안관제 체계진단의 필요성

웹해킹, 웹쉘, DDoS, 악성코드, APT 등에 대한 위협 지속 증가
침해사고 대응 메뉴얼 등 운영 프로세스 수립 필요
보안위협 대응을 위한 보안관제체계 고도화 및 개선 모델 수립 필요

서비스 개념

검증된 보안관제 진단 Framework를 통해 기 구축된 또는 신규 구축 보안관제 아키텍처에 대한 수준 진단 및 개선 지원 서비스

주요 특징

삼성고유 보안관제 수준진단 서비스

- 관제정책, 조직역량, 관제프로세스, 관제플랫폼 4개영역, 8개 도메인으로 구성된 SMCI[1] 기반 보안관제 아키텍처 체계진단

현장 실사 중심의 수준진단 및 문제점 도출

- 실무자 인터뷰, 로그 샘플링 분석, 보안장비 운영 실사 등을 통한 보안관제 주요 기능별 미흡 사항 도출
- 보안관제 프로세스맵, 보안관제 영역별 구축시 고려사항 등 개선안 제시

목표 수준 정의 및 가이드라인 제시

- 개선안에 따른 세부 목표 및 실행과제 리스트 제시
- 개선과제 이행 경과 점검 및 지원

[1] SMCI (Security Monitoring & Control Index): 국제표준 및 삼성 노하우가 집약된 보안관제 수준 진단 지표

주요 서비스

보안관제 아키텍처 수준진단

관제정책, 수행조직/역량, 운영 프로세스 등 상세 현황파악
보안로그 분석 미흡으로 인한 미탐지 해킹 흔적 유무 조사

보안관제 개선안 수립

Best Practice 대비 Gap 분석 및 도메인간 균형도 분석
구현 용이성, 효과성, 연관성을 고려하여 개선 과제 우선순위 도출

보안관제 역량 전달

방화벽, 침입방지, DDoS, 좀비PC차단 등 기본과정 제공
보안관제의 역할, 이벤트 로그분석, 영역별 모의훈련 등 심화과정 제공

현황 분석	보안관제 진단	개선방안 수립	전문가 Advisory
보안관제 규정/지침	영역별 실사 및 인터뷰	보안시스템 개선방안 • 보안솔루션 • 보안관제 시스템	개선방안 이행점검
관제 Rule	탐지 누락분석	보안관제체계 개선방안 • 정보흐름 분석 • 예상 취약점 도출 • 점검방식 결정	관제 운영 가이드
보안 시스템 로그	보안관제 모의훈련		관제 전문가 양성 교육

기대효과

현 보안관제 수준의 객관적 평가

정책관리, 탐지 Rule 관리, 사고대응 등 도메인간 균형도 및 도메인별 Gap 분석

최적의 보안관제 체계 구성

인력, 역량, 관제 프로세스, 관제 플랫폼 등 TO-BE 모델 제시

신규 보안위협 선제적 대응

최신 침해 공격에 대한 탐지룰 및 대응 프로세스 보유

삼성SDS

기업보안관리 수준진단

보안관리 성숙도 측정을 위한 수준진단 컨설팅

필요성

기업 전반에 대한 보안관리 수준진단 요구 증가

보안위협 대응을 위한 전사적 보안관리체계 구축필요
보안정책, 조직, 사고대응 등 보안 거버넌스 全영역 강화 필수
보안관리 시스템의 '도입'보다 효과적인 '운영'이 중요

서비스 개념

보안정책 관리, 보안조직 관리, 보안 시스템 취약점 관리에 대한 현장 중심의 심층적인 현황 파악을 통한 기업의 보안관리 거버넌스 강화 및 수준 진단 서비스 제공

주요 특징

삼성고유 보안수준 진단툴 기반 정기적인 수준진단 서비스

- 6개영역 173개 통제항목으로 구성된 ESMI[1] 기법 활용
- 정기진단으로 개선과제 실행결과 확인

현장실사 중심의 진단 서비스

- 문서중심의 Yes/No 방식 진단이 아닌 현장중심 진단
- 5단계의 세분화된 성숙도 측정

보안전문가의 모의해킹 진단

- 모의해킹을 통한 진단결과 보고서, 원인분석 및 보안 가이드 제공
- 삼성고유 진단 체크리스트 및 자동 점검툴을 이용한 취약점 진단

[1] ESMI (Enterprise Security Maturity Index): 삼성 고유의 보안관리 영역별 성숙도 측정지표

주요 서비스

6개 영역 보안관리 수준진단

보안정책

보안정책 운영
컴플라이언스 준수
정보자산 분류 및 관리

IT보안

솔루션 운영
IT시스템 보안점검
PC보안
서버보안
DB보안
통신망보안
어플리케이션 보안

보안조직

보안조직 운영
보안협의체 운영

사고대응

보안사고 예방 및 대응
재해복구 관리

보안의식제고

임직원 보안관리
협력사 보안관리
보안서약서 관리

물리보안

통제구역 관리
출입보안
영상보안
통신보안

Best Practice 대비 Gap 비교 및 개선안 수립

보안관제 우수기업 대비 Gap 분석
보안관리 수준 개선을 위한 가이드 제시

주기적 사후 진단 및 개선관리 지원

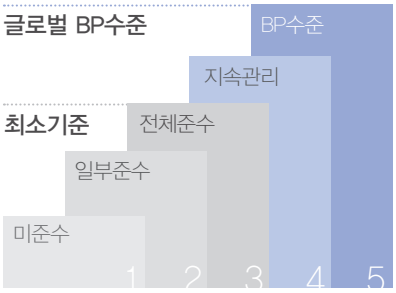
개선여부, 수준 확인을 위한 사후 진단 수행(권장 1년)

현황분석 ▶ **성숙도 평가** ▶ **개선방향 도출**

ESMI 기준

관리체계	보안취약점	운영역량
보안정책		
보안조직		
의식제고		
사고대응		
IT보안		
물리보안		

5단계 평가



산출물

보안관리 성숙도수준

레퍼런스 모델 기반 Gap 분석결과

개선가이드 제시

기대효과

전사 보안관리 수준 개선을 위한 Baseline 수립

보안관리 영역별 수준 가시화
지속적인 보안관리를 위한 개선기준 설정

전사적 보안 거버넌스 강화

보안조직/프로세스/시스템 內 취약요소 제거
보안사고 사전예방 및 피해 최소화

삼성SDS

방화벽
(SECUI MF2)

최신 네트워크 보안위협에 대응하는 차세대 통합네트워크 보안 솔루션

필요성

통합 네트워크 보안장비 도입 필요

다양하고 통합적인 보안 기능을 사용하면서 고성능 유지
IPv6 지원 및 IPTV 보안 등 최신 이슈 해결
NAC, 취약점 점검툴 등 다양한 보안기능의 확장 및 운영 가능
효과적인 원 포인트 시스템 관리 필요

솔루션 개념

사용자 기반 애플리케이션 행위 제어, 정보유출방지, DDoS 공격 대응, 웹취약점 분석 등 변화하는 네트워크 보안 위협에 능동적 대응

주요 특징

애플리케이션, 사용자 기반의 식별 및 제어 기능

• Port, Protocol 정보와 독립적인 인터넷 애플리케이션 식별 및 제어

개인정보 및 기업정보 유출방지 기능 제공

• Built-in 및 사용자 정의 키워드 지원 및 내용 검색
• HTTPS 등 암호화된 패킷 검색 지원

URL 평판 DB로 악성코드 배포 사이트 접근 차단

• Cloud 기반의 악성 URL 차단 정보 업데이트

검증된 Anti-DDoS 엔진 탑재로 공격 방어 기능

• Traffic limit, Behavior, Signature, Zero-day Attack 방어
• Anti-DDoS 전용 장비 엔진 적용

SSL VPN 및 Mobile VPN으로 스마트워크 환경 지원

• 외부 접속용 SSL VPN, 다양한 Mobile VPN 기능

주요 기능

Web Filter

URL 주소 입력을 통한 우회 방지 (URL의 IP 주소 자동 업데이트)
외부 Proxy 서버 자동 업데이트로 인한 우회 접속 Http Request 차단

Web Contents Filtering

금지 패턴 차단, URL 내 확장자(exe, dll 등) 차단
명령어 삽입, SQL,XSS 공격 차단 기능
검색엔진 색인을 위한 웹 로봇 탐지 / 차단

Anti-Virus/ Anti-Spam

환경에 따른 Stream-Based와 File-Based 방식의 Anti-Virus DB 선택 가능
Global Anti-Spam 솔루션으로 다국어 키워드 필터 지원
RBL(Real-time Blocking List) 기능

SMART HA, NAT

Router, Bridge 모드 혼용 사용 가능한 HA 제공
Policy Based NAT 기능을 통한 유연성 확보

VPN(IPSec/SSL/Mobile)

국제 표준 인증 프로토콜과 암호화 알고리즘 지원
Multi-Tunnel, Bonding, Load balancing 기능

Application Control

다양한 인터넷 애플리케이션 제어 기능
애플리케이션 별 User ID로 행위 제어

IPS/DDoS

Anti-DDoS 전용장비 엔진 적용
내부 좀비 PC 탐지 및 차단

Specifications

구분		MF2 110	MF2 300	MF2 1100	MF2 2100	MF2 3100	MF2 6000
CPU		2 Core	2 Core	2 Core	4 Core	10 Core	6 Core x 2
Memory		2 GB	4 GB	4 GB	8 GB	16 GB	24 GB
HDD		–	250GB	500GB	1TB	2TB	2TB
Through-put	Firewall Max	600 Mbps	1 Gbps	5 Gbps	12 Gbps	30 Gbps	40 Gbps
	VPN Max	300 Mbps	300 Mbps	1.5 Gbps	2 Gbps	4 Gbps	5.5 Gbps
	VPN Tunnel	1,000	2,500	10,000	20,000	30,000	40,000
Network Interface	10/100/1000 BASE-TX	6	6	8	Max 24	Max 24	Max 24
	1000 BASE-X	–	–	2	Max 24	Max 24	Max 24
	10G BASE-R	–	–	–	–	Max 12	Max 12
	BYPASS	Support					
	Mgmt Ports	–	–	–	1	1	1
	Console	1(RJ-45)					
Dimension[WxDxH]		201x191x45	430x238x44	430x449x44	431x522x88	431x600x88	431x657x88
Power Supply		Adapter	Single	Single	Redundant	Redundant	Redundant
Temperature		0 ~ 40°c					
Humidity		10 ~ 90% [non condensing]					

삼성SDS SAMSUNG

삼성SDS

IPS
(SECUI MFI)

내부 IT자원에 대해 예방진단부터 유출방지까지 제공하는 차세대 통합 침입방지 솔루션

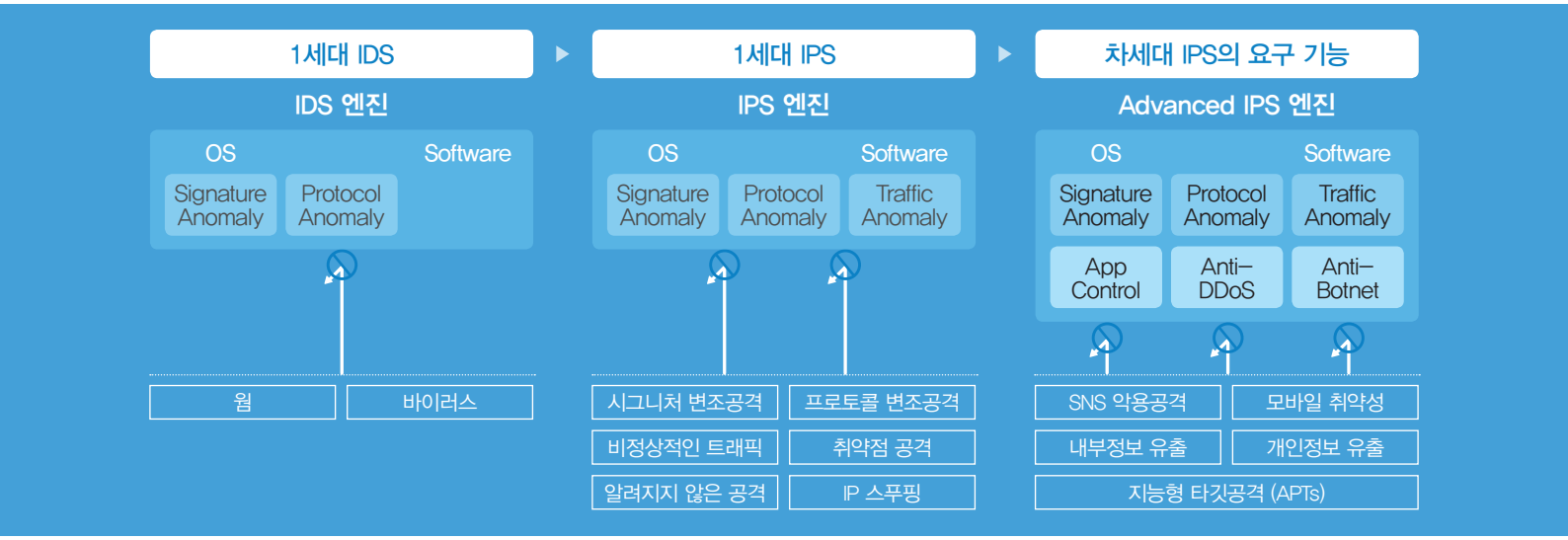
필요성

최신 보안 위협에 능동적 대응을 위한 솔루션 필요

다양하고 진화된 공격 위협의 증가로 인한 피해범위 확산 대응
최신 공격 위협에 취약한 1세대 IPS의 한계 극복
능동적 침입방지 시스템 보안 기능 요구 증대

솔루션 개념

일반적인 시그니처 기반 IDS/IPS의 한정된 개념을 탈피하여 다양한 지능형 공격에 대한 예방진단, 위협탐지, 공격차단, 유출방지 기능까지 제공



주요 특징

SC FDE(SECUI Clustering-based Flow Distribution Engine)

- 대칭형 다중처리(SMP)와 클러스터링 기술이 결합된 최신 하드웨어 아키텍처 및 부하분산처리기술 적용

SM ADPI(SECUI Multi-stage Advanced Deep Packet Inspection)

- DDoS 공격, Exploit, Web 취약점 공격 탐지, 애플리케이션 제어 기능
- Full Stack Inspection으로 애플리케이션까지 인식 및 정밀 방어 기술

SMART UPDATE

- Black List IP 정보 및 취약점 정보, 악성코드 배포지 정보 제공
- 클라우드 기반 분석 시스템 연동 및 실시간 업데이트

주요 기능

통합엔진(IPS + Anti-DDoS)

Full Stack Inspection으로
애플리케이션까지 인식 및 정밀
방어 엔진 적용

Signature기반 방어

고속 패턴매칭을 통한 공격 차단 및
유해 트래픽 확산 방지

Protocol 취약점 방어

L3/L4 계층의 프로토콜 취약점을
이용한 공격 차단

Virtual Domain

내부, DMZ별 보호 프로파일을 별도
지정하여, 유연성 있는 보안 정책
적용

다양한 시스템 구성 및 솔루션 연동

다양한 Fail-Over 기능 지원을 통한
안정성 보장
SECUI SCAN 연동 및 타사 악성코드
탐지 솔루션 연동 지원
(FireEye, Trend Micro, Symantec)

DDoS 공격 방어

임계치 기반 탐지, 행위 기반 탐지,
공격 패턴 자동학습
세션기반 탐지 엔진 탑재

통합 대시보드 및 실시간 모니터링

직관적인 공격 현황 및 실시간 현황
검색 지원

응용계층 취약점 방어

L7 계층의 취약점 및 서비스 거부
공격 방어 및 차단

SSL Inspection

암호화된 트래픽 탐지를 위한
SSL Inspection 기능을 제공하여
보안성 향상

Specifications

구분		MFI 2100	MFI 4100	MFI 20000
CPU		4 Core	10 Core	8 Core x 2
Memory		16 GB	32 GB	32 GB
HDD		1TB	2TB	2TB
Throughput	64 byte	2 Gbps	4 Gbps	20 Gbps
	Max	10 Gbps	20 Gbps	120 Gbps
Network Interface	1G Copper	8 [Max 24]	8 [Max 24]	– [Max 32]
	1G Fiber	8 [Max 12]	8 [Max 12]	– [Max 24]
	10G Fiber	–	– [Max 6]	8 [Max 24]
Dimension [WxDxH]		2U [431x600x88]	2U [431x600x88]	3U [431x664x132]
Power Supply		Redundant [460 Watts]	Redundant [600 Watts]	Redundant [1010 Watts]

삼성SDS

DDoS 차단
(SECUI MFD)

다계층, 다단계 방어 엔진을 탑재한 지능화된 DDoS 공격 탐지/차단 솔루션

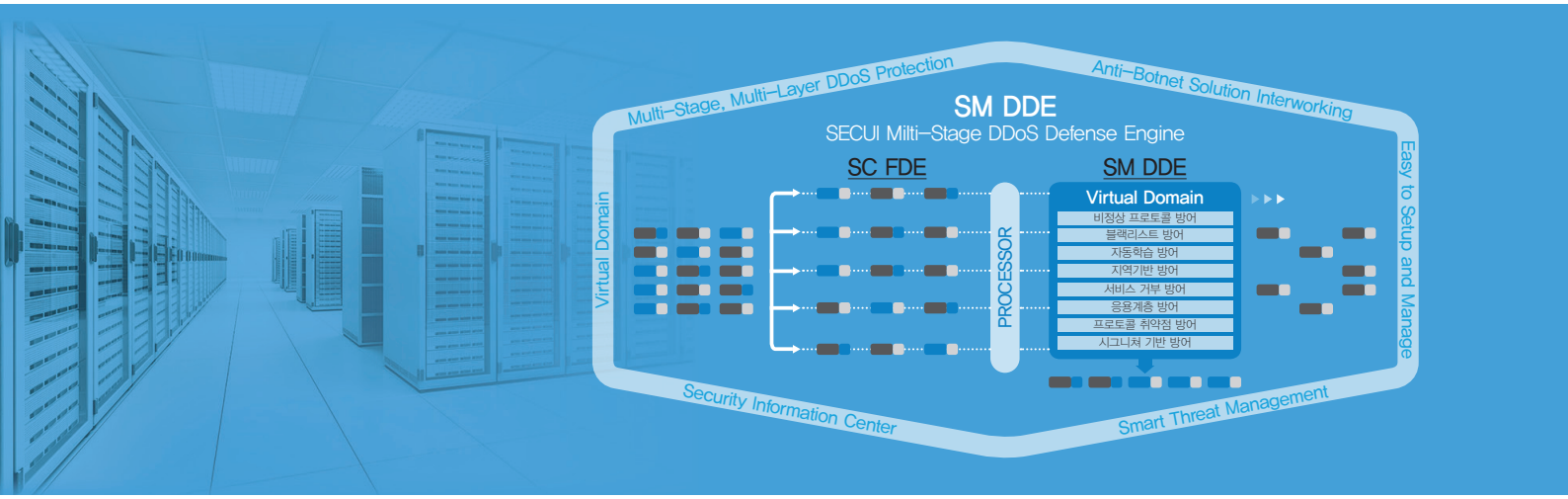
필요성

조직적이고 지능화된 공격에 능동적인 DDoS 대응 필요

다양한 형태의 DDoS 공격방어로 서비스 연속 보장
실시간 공격 / 트래픽 분석에 의한 예경보 시스템 구현

솔루션 개념

고유의 클러스터링 및 부하분산처리 기술과 접목된 다계층, 다단계 DDoS 공격 방어 엔진을 기반으로 다양한 DDoS 공격을 정밀하게 탐지 및 차단



주요 특징

고성능 멀티코어 하드웨어

- 64비트 SECUI OS와 고성능 멀티코어 지원 및 Wired-Speed 제공
- 트래픽 분산 처리 및 멀티코어 최적화 기술(SC FDE[1])

정밀한 DDoS 공격 탐지 및 차단

- 다단계/다계층 DDoS 공격 탐지 및 차단(SM DDE[2])
- Snort, PCRE(표준 정규화) 정책 등록 지원, Anti-Botnet 솔루션 연동 차단

유연한 시스템 구성 및 가상 도메인 설정

- 보호 도메인, 보호 프로파일 지원, In-Line 및 Out-of-Path 구성

통합 모니터링

- 실시간 대시보드, 보안정책 검색, 상세 로그 및 Report

[1] SC FDE(SECUI Clustering-based Flow Distribution Engine): 부하분산처리기술

[2] SM DDE(SECUI Multi-stage DDoS Defense Engine): 애플리케이션 계층 프로토콜 취약점을 이용한 DDoS 공격 탐지/차단 엔진

주요 기능

SM DDE(SECUI Multi-Stage DDoS Defense Engine)

비정상 프로토콜 방어, 블랙리스트 기반 방어, 자동학습 방어, 지역기반 방어,
서비스 거부 방어, 응용계층 방어, 프로토콜 취약점 방어, 시그니처 기반 방어
자동 학습을 통한 차단 및 국가별 DDoS 공격 방어
IP 계층부터 애플리케이션 계층까지 다양한 DDoS 공격 정밀 탐지 및 차단

Virtual Domain

가상 도메인으로 네트워크 환경에 적합한 유연한 DDoS 방어 정책 적용

Anti-Botnet Solution Interworking

악성코드 탐지 및 차단 솔루션 연동으로 침해 사고 예방
DDoS 공격 시도 차단 및 내부 정보유출 방지

Smart Threat Management

SECUI TMS 연동을 통한 보안 위협 조기 예경보 체계 구축

Security Information Center

DDoS 전용 시그니처 및 블랙리스트 정보의 지속적인 업데이트

Easy to Setup and Manage

통합 대시보드 및 실시간 모니터링으로 직관적인 공격 현황 제공
보안정책 검색 및 로그 기반의 간편 보안 정책설정 제공

Specifications

구분		MFD 2000	MFD 4000	MFD 20000
CPU		4 Core	10 Core	8 Core x 2EA
Memory		16 GB	32 GB	32 GB
HDD		1TB	2TB	2TB
DDoS 방어 성능		2 Gbps	4 Gbps	40 Gbps [MAX 100 Gbps]
Network Interface	1G Copper	8 [Max 32]	8 [Max 32]	– [Max 32]
	1G Fiber	8 [Max 16]	8 [Max 16]	– [Max 24]
	10G Fiber	–	– [Max 8]	8 [Max 24]
Dimension [WxDxH]		2U [431x600x88]	2U [431x600x88]	3U [431x644x132]
Power Supply		Redundant [460 Watts]	Redundant [600 Watts]	Redundant [1010 Watts]

삼성SDS

홈페이지 관제

웹쉘 업로드 탐지 및 웹 로그 분석을 통한 실시간 웹쉘 공격 탐지/차단 전용 솔루션

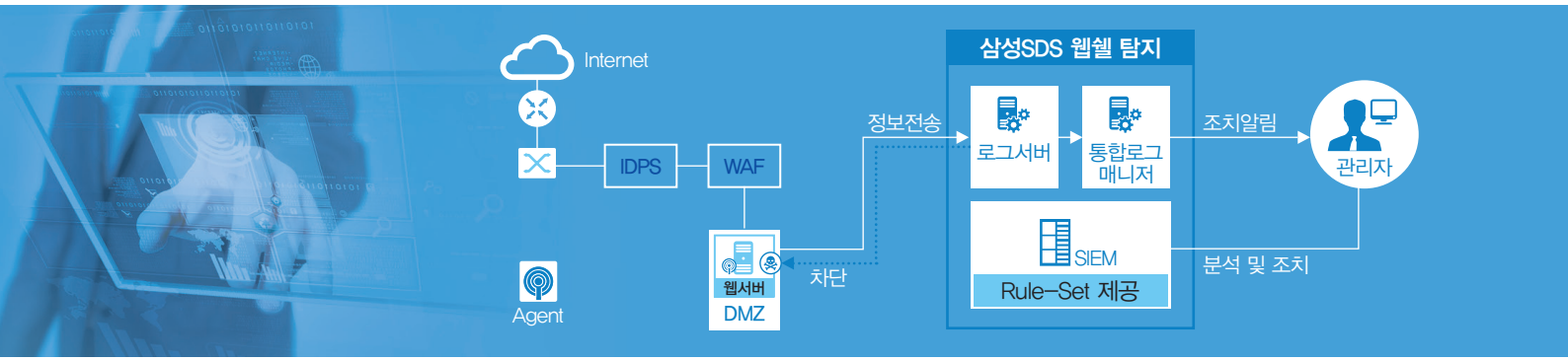
필요성

다양하고 복잡한 웹 서비스 확대 따른 기존 보안솔루션의 한계

기업 마케팅 홈페이지부터 모바일 웹서비스로 다양한 용도로 확대
서버 중요 데이터 저장으로 웹서비스 중요성 증가
웹 해킹 후 DB 및 웹 어플리케이션 서버 등으로 해킹 피해 증가

솔루션 개념

기존 보안솔루션으로 탐지 불가능한 지능화된 웹서비스 공격을 대응하기 위해 웹쉘 탐지 및 통합 로그 분석 서비스 제공



주요 특징

변종 웹쉘 및 로그 분석을 통한 해킹징후 차단

- 패턴 탐지, 시그니처 탐지, 휴리스틱 탐지(전용엔진) 방식으로 변종 웹쉘 대응
- 통합로그 매니저를 통한 로그 수집에 대한 정책설정, 조치 지원
- Rule-Set기반 웹 로그 해킹징후 실시간 분석 및 차단

실시간 탐지 및 탐지 성능 최적화

- 자원사용율(CPU, 메모리) 제어를 통한 신속한 탐지 및 실시간 탐지 지원
- 최적화된 탐지패턴 및 웹쉘 시그니처 자동검역을 통한 탐지율 극대화

다양한 공격 기법 대응

- ASP, JSP, PHP 등 다양한 웹 스크립트 탐지 지원 및 패턴 업데이트
- 인코딩, 난독화, 코드분할 공격 등 분석이 어려운 우회공격 기법 탐지

엔터프라이즈 환경지원

- 대량의 웹 서버 중앙 집중 관리 및 무중단 서비스 지원
- 다양한 외부 연동 지원 (ESM, SMS, EMAIL, SMP, 형상관리서버 등)

주요 기능

실시간 웹쉘 탐지/검역

실시간 탐지를 통한 웹쉘 파일 탐지, 검역 및 예외조치
웹쉘 실행 시 웹서버/WAS로그를 분석하여 공격자 IP 보고

실시간 악성URL 탐지

탐지된 URL 검역, 부분검역 및 예외조치
그레이, 화이트, 블랙 리스트 URL 관리

웹서버/WAS 환경설정 위변조 탐지

임의 또는 악의적인 웹 서버 설정파일 변경 시 관리자 보고
웹서버 파일 및 DB내의 개인정보 탐지 및 보고

관리기능

계정 및 사용자별 권한 관리
관제화면, ESM, SMS, Email 등 외부 시스템 연동 인터페이스 제공
관리서버 이중화 지원 (Active/Active)
에이전트, 매니저, 패턴 업데이트 및 버전관리
보고서 및 통계 자료 제공

웹쉘탐지	악성URL탐지	위변조탐지	관리기능	가상머신(VM)전용기능
웹쉘탐지	블랙 리스트 기반 탐지	변경방지	권한관리	SCALE IN/OUT 지원
검역처리	화이트 리스트 기반 탐지	변경탐지	에이전트관리	이력관리
예외처리	그레이 리스트 기반 탐지	업로드필터링	업데이트관리	네트워크 보안관리
	URL/URI 관리	WAS설정파일 변경탐지	홈디렉토리 자동찾기	이벤트 중복관리

구성형태

01 **단독 솔루션 구축형**	고객사 내부 네트워크에 홈페이지 관제 솔루션을 도입하여 운영하는 형태
02 **보안관제 서비스 연동 구축형**	고객사의 웹서버/WAS에 에이전트를 설치 후 외부 원격 관제를 통한 서비스 형태
03 **클라우드 기반 프리미엄 서비스형**	클라우드 컴퓨팅 서비스를 이용하는 VM별로 에이전트를 설치하여 해당 관리자가 운영하는 형태

삼성SDS

악성코드 관제

내부로 유입되는 모든 악성파일 및 C&C서버와의 통신을 탐지하는 솔루션

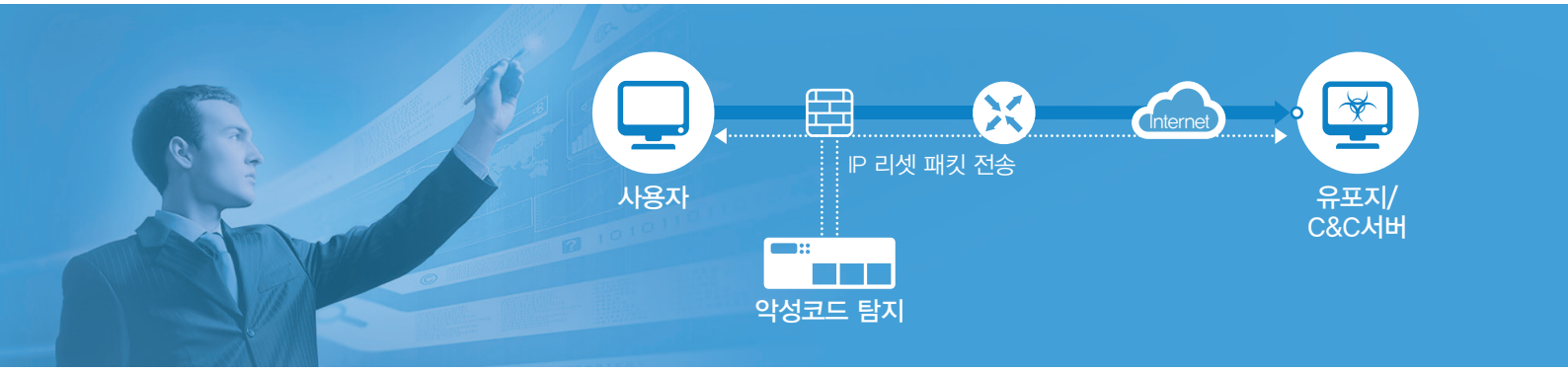
필요성

악성코드가 침해사고에 핵심적인 요소로 존재

최신 보안 위협은 다양한 기술과 공격 방식을 이용해 지속적으로 특정 대상에 공격을 가하며, 그 중심에는 신종 악성코드가 존재

솔루션 개념

내부 임직원 PC로 유입되는 모든 악성파일을 정적/동적 분석을 하고 악성코드 유포지 및 C&C서버 통신내역을 확인하여 차단하는 솔루션



주요 특징

시그니처 기반 탐지부터 악성코드까지 탐지

- 시그니처(Signature)기반 탐지를 통해 유해사이트, C&C 통신 탐지
- 클라우드 정보 활용을 통한 평판(Reputation)기반 탐지
- 행위기반 분석을 통해 시그니처 및 탐지 룰 없이 zero-day 악성코드를 탐지

다중 차단 방식의 이상트래픽 탐지 및 차단

- 전용 에이전트 설치 여부와 상관없이 C&C 서버 접속 및 악성코드 배포사이트 차단
- C&C 트래픽 탐지 이벤트, 악성코드 유포 사이트 접속 탐지 이벤트 등 차단 이벤트 대상 탐지
- TCP RESET 패킷, ICMP Unreachable 패킷, Garbage DNS Response 패킷 등을 Client/Server 전송하여 차단

실시간 위협 모니터링

- 악성코드 탐지 및 분석에 대한 명확한 가시성 제공
- 신종 악성코드 및 의심 파일/이벤트에 집중 모니터링 제공

주요 기능

위협 및 이상 트래픽 탐지 및 분석

주요 인터넷 서비스 프로토콜 수집 및 분석 (HTTP, SMTP, SMB, FTP 등)
파일 유입 및 유출에 대한 양방향 트래픽 모니터링
가상 머신 기반 분석을 통한 신종 악성코드 분석
비실행형(non-PE / MS office 등) 악성코드 분석
VM 분석 과정 및 C&C 탐지 내역에 대한 PCAP 파일 다운로드

위협 대응 및 치료

악성코드 감염 PC에 의한 유해 사이트 접근 및 C&C 통신 탐지 및 차단
탐지된 악성코드 감염 의심 호스트에 대해서 악성코드 자동/수동 치료

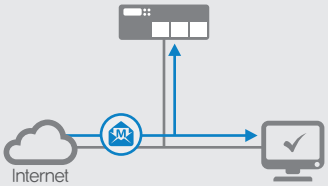
통합 모니터링 및 로그 관리

대시보드를 통한 보안 현황 및 주요 이벤트 정보 제공
실시간 악성코드 유입 현황 및 이상 트래픽 발생 여부 확인
이벤트 종류, IP 주소, 행위 내역 등에 대한 상세 로그
자동 및 수동 DB 백업 기능
통합로그관리시스템(SIEM) 연동을 위한 syslog 포워딩 기능

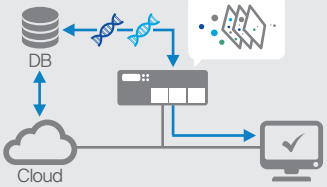
동작 방식

「분석-탐지-확인-차단」 프로세스에 의한 악성코드 침해사고 대응

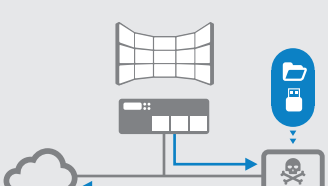
1단계 | 유입되는 모든 파일 분석



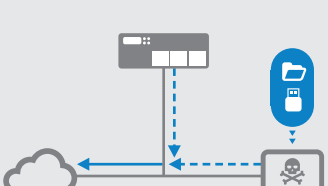
2단계 | 분석을 통한 위협 탐지



3단계 | 분석 결과 확인



4단계 | 이상 트래픽 탐지 및 차단



삼성SDS SAMSUNG

삼성SDS

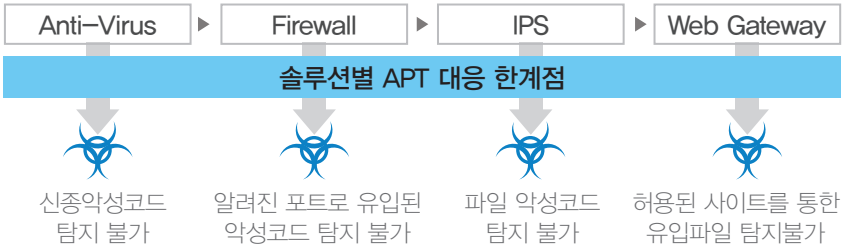
APT 관제

APT 악성코드 감염 PC의 비정상적 행위에 대한 탐지를 통해 정보 유출과 시스템 장애를 사전에 방지하는 솔루션

필요성

기존 보안솔루션의 지능형 악성코드 대응 한계

전통적인 보안 솔루션만으로는 신종 악성코드 중심의 지능화된 위협에 대응하기에는 한계



솔루션 개념

알려진 악성코드 뿐만 아니라 신종/변종 등 지능형 악성코드에 대한 단계적인 분석을 진행하고 알려진 C&C 통신 및 이상 트래픽에 대한 추가 분석

주요 특징

지능형 공격에 대한 특성을 다각도로 분석

- 모든 트래픽을 수집하여 정상 트래픽과 비정상 트래픽 구분
- 악성코드 유포 시점부터, 악성코드 감염 후 행동까지 확인

정상적인 파일/통신으로 위장하는 공격 대응

- 악의적으로 확장자를 변조한 실행파일 다운로드 탐지
- 알려진 프로토콜을 활용한 악의적인 공격 탐지

네트워크 통신 정밀 분석을 통한 위협 탐지

- C&C 서버와 같은 알려진 APT 도메인의 주기적인 통신행위 탐지
- 익명의 프록시 서버 및 Tor[1] 사용과 같은 추적 회피 행위 탐지

[1] Tor: 분산형 네트워크 기반의 익명 인터넷 통신 시스템

주요 기능

트래픽 수집

네트워크의 모든 패킷 수집 및 고속검색 기능 제공

트래픽 분석

트래픽을 통한 악성코드 상세분석 기능
다양한 프로토콜/어플리케이션 분석 및 비 표준 프로토콜 분석
악성코드를 통한 내부정보 유출 행위 탐지

악성코드 분석

자동화된 악성코드 분석 및 위험도 평가
행위분석 기반 신규 악성코드 탐지 가능
악성코드 분석결과와 트래픽 연계 분석

통합 대시보드

실시간 경보 및 추이, Top N 그래프 등 통합 대시보드 제공
발견된 위협에 대한 즉각적 인지 가능

동작 방식

「인터넷 트래픽 수집 – 악성코드 분석 – 이상행위 통신 차단」 프로세스에 의한 지능형 공격 대응

인터넷 트래픽 수집

인터넷 트래픽 수집
- 트래픽 전체 내용 수집
- 유출입 파일 수집

트래픽 고속검색 환경 제공

악성코드 분석

실행파일 자동검사를 통한
악성코드 유입탐지

악성 사이트 접속 탐지/분석
- 악성코드 유포사이트 탐지
- 명령서버 통신 트래픽 분석

악성코드 감염PC 탐지

이상행위 통신 차단

위험도에 따른 악성코드 조치
- 유포/명령서버 통신 차단
- 감염PC 사업장 통보

긴급 악성코드 통신 차단
예) 국가적 해킹사고 발생 등

삼성SDS SAMSUNG

삼성SDS

SCAN
(SECUI SCAN)

중앙센터 및 지방사업장들의 취약점 통합관리가 가능한 중앙관제형 취약점 점검 스캐너

필요성

다양한 해킹 공격 위협 대응을 위한 자동화된 통합 취약점 점검 필요

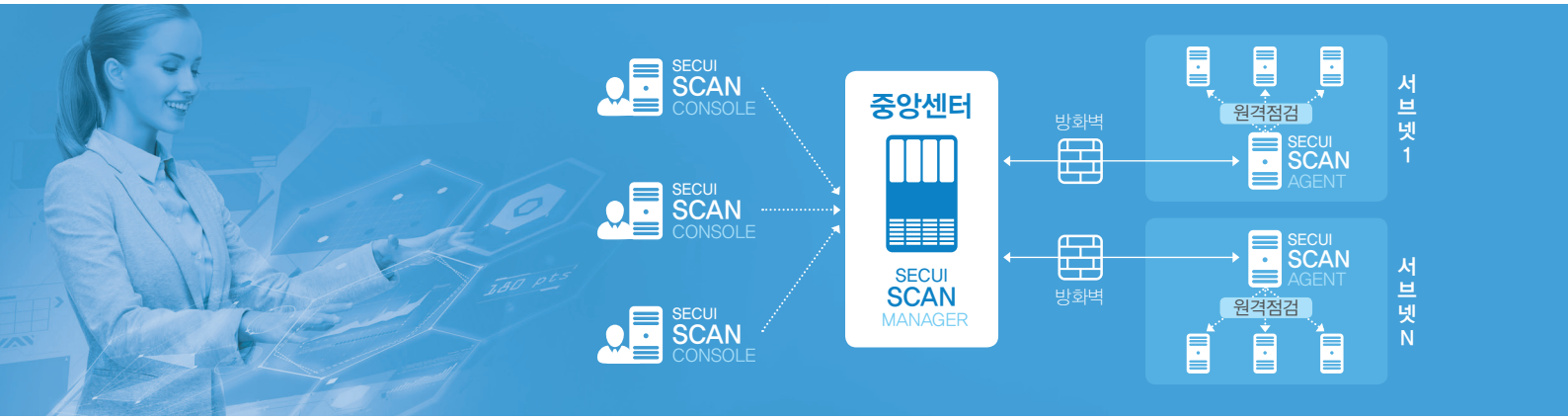
기업의 네트워크, 정보시스템, 웹 서버의 시스템이 증가함에 따른 다양한 보안 취약점 제거 필요

기업의 보안사고를 예방하기 위한 기업내 사전 보안취약점 점검을 통한 능동적인 보안관리가 필요

솔루션 개념

3-Tier방식의 중앙관제형 점검 툴로 중앙관제센터에서 관리 대상 서브넷들의 통합관리가 가능한 네트워크, 웹, 개인정보탐지 통합 스캐너

Console: 점검 작업 실시간 모니터링을 위한 사용자 User Interface
Manager: 중앙관제센터에 설치되며, Agent 점검 결과 통합관리
Agent: 실제 점검 기능을 갖추고 있는 스캐닝 엔진을 탑재한 프로그램



주요 특징

강력한 취약점 점검

• 다양한 운영체제, 네트워크 장비 등에 대한 시스템 점검 제공

편리한 사용방식

• 취약점별 상세설명 제공 및 선행 점검항목 자동선택

강력한 정책편집

• 사용자의 목적과 환경에 맞는 정밀한 정책설정 가능

기술적 위험과 변화에 대한 능동적인 대처

• 서브넷별 주요 네트워크 분리를 통한 웜 확산 방지 기능 제공

주요 기능

다양한 취약점 스캐닝

Windows, Linux, Unix 등의 일반 운영체제를 비롯해 각종 네트워크 장비, 보안장비에 대한 광범위한 점검
다양한 네트워크 프로토콜의 취약점 점검
서비스 거부 취약점에 대한 점검정책 별도 분리

웹 서버 자체의 알려진 취약점 점검

웹 어플리케이션 상의 각종 취약점(SQL Injection, XSS 등) 점검
각종 웹 패키지 소프트웨어(ZeroBoard 등) 알려진 취약점 점검
웹 상에 유출된 개인정보 탐지 및 숨겨진 웹 폴더 추축 점검
JavaScript 처리엔진과 Flash 파일처리기를 내장한 Crawling 기능제공

개인정보 탐지 기능

개인정보가 포함된 웹페이지를 찾아 리포팅
정규 표현식을 활용한 사용자 정의 점검패턴 지원

중앙 관제형 스캐너

중앙 관제형 스캐너를 통해 분산된 네트워크의 통합점검 지원
사용자별 점검권한 및 점검대역 부여
한 사용자가 각기 다른 정책을 가진 복수개의 점검 작업 동시수행 가능
다중 에이전트를 이용한 병렬 점검 기능

Specifications

제품	구분	상세 분류	
SECUI SCAN V3.0	3-Tier / Stand Alone	SECUI SCAN V3.0 UNLIMITED	모든 IP 대역에 대해 점검할 수 있는 버전 점검 가능 IP 대역 : 예) 1.1.1.1 ~ 255.255.255.254 용도 : 보안 관련 컨설팅 업체 진단/컨설팅 및 대규모 네트워크 관리
		SECUI SCAN V3.0 A CLASS	A Class : 지정된 IP Class A 대역에 대해 점검할 수 있는 버전 점검 가능 IP 대역 : 예) x.1.1.1 ~ x.255.255.254 용도 : 대규모 사업장에서 사용
		SECUI SCAN V3.0 B CLASS	B Class : 지정된 IP Class B 대역에 대해 점검할 수 있는 버전 점검 가능 IP 대역 : 예) x.x.1.1 ~ x.x.255.254 용도 : 중대형 규모의 사업장에서 사용
		SECUI SCAN V3.0 C CLASS	C Class : 지정된 IP Class C 대역에 대해 점검할 수 있는 버전 점검 가능 IP 대역 : 예) x.x.x.1 ~ x.x.x.254

※ 3-Tier 형식은 추가 Agent 구매 가능

삼성SDS

TMS
(SECUI TMS)

다수 보안장비에 대한 통합적으로 정책설정, 모니터링, 패치 등의 기능을 제공하는 위협관리 솔루션

필요성

통합 위협관리 및 모니터링의 필요성

SECUI 계열 솔루션에 대한 관리/모니터링을 통해 업무효율성 보장
(통합 정책설정, 상세 모니터링, 패치 및 백업관리)

최신 글로벌 위협에 대한 경보 및 실시간 대응

솔루션 개념

SECUI 장비에 대한 통합 관리/모니터링을 제공함으로써 보안장비의 장애발생 위협을 사전에 대처하는 위협관리 솔루션

주요 특징

통합 설정 및 위협 관리 기능

- SECUI MFI, SECUI MF2 등 제품에 대한 위협 정보 현황 분석 및 예경보 설정을 통한 위협 관리

통합 관리 기능

- 통합 정책 / 모니터링 / SECUI 보안 솔루션의 패치 기능
- 장애 및 위협에 대한 빠른 대응 및 업무 효율성 증가

실시간 장비 상태 모니터링 기능

- 보안장비 상태의 통합 정보 실시간 제공을 통한 운영친화 대시보드
- 2D/3D Topology Map, 상태 TOP 10 정보, 통합 트래픽 모니터링 기능 제공

주요 기능

통합 설정

개별 장비 설정과 설정 복제 적용
통합 스크립트 실행

실시간 상태 확인

실시간 통합 위협 탐지 이벤트 상태 모니터링 기능

모니터링

보안 이벤트 및 시스템 상태 모니터링 기능 제공

통합 이벤트 관리

이벤트에 대한 분석된 티켓 발송 (E-mail,SMS) 기능 및 조치 입력 기능

정책 및 객체 관리

TMS에 등록된 장비의 정책 동시 적용 기능
정책 및 객체 변경 관리 기능

TMS U Mode

다수의 SECUI TMS를 효율적으로 관리하는 통합 모드
하위 TMS의 로그 검색 및 모니터링

위협 분석

특정 시간, 날짜 등의 기간으로 통계 기반 분석 기능 제공
분석 데이터에 따른 저장 및 Export 기능 제공

이벤트 정책

다양한 이벤트 정책에 의한 상관 분석 기능
특정 이벤트에 대한 긴급 대응 팝업 / 이벤트 평가

로그 관리

다수의 로그 쿼리를 통한 패킷 플로우 분석
로그 압축 저장을 통한 증가된 디스크 사용률

보고서

통합보고서, 시스템 운영보고서, 장비 보고서
자동 스케줄 및 자동 발송(E-mail, SMS) 기능

Specifications

분류	TMS 1000	TMS 2000
CPU	4 Core	4 Core x 2
Memory	8 GB	16 GB
HDD	3TB x 2	3TB x 2
NIC	1 Copper x 4 port	1 Copper x 4 port
Dimension [WxDxH]	482.4 x 663.3 x 42.8	482.4 x 663.3 x 87.3
Rack Mount [size]	1U	2U

삼성SDS

FIDO[1]
(Fast IDentity Online)

생체인식 기반 보안 인증 체계 및 편리한 사용자 인증 절차를 제공하는 보안인증 솔루션

필요성

안전하고 간편한 인증의 필요성

디지털 컨버전스 시대의 안전한 사용자 인증 필수
복잡한 인증 과정으로 인한 사용자 피로도 증가
구매결제 포기, 인증 절차 만족도 저하 등으로 인한 기업 경쟁력 저하

솔루션 개념

PKI[2] 인증체계를 기반으로, 스마트 기기의 생체인식센서와 TEE[3] (Secure Storage)를이용하여, 편리성과 안전성을 획기적으로 개선한 검증된 보안인증 솔루션

주요 특징

FIDO Certified™ 인증 획득

- FIDO Alliance의 FIDO Certified™ 공식인증을 획득한 UAF Client/Server 제품군 보유
- FIDO 제품군 최초 CC(Common Criteria) 인증 획득

멀티모달 생체인증 기능 제공

- 지문 外 얼굴 인식 기반의 생체인증 추가 지원을 통한 보안성 강화 및 단말 커버리지 확대

최고 수준의 보안 환경 제공

- Who you are(생체인증) + What you have(단말) + PKI 기반 인증방식 적용으로 최상위 레벨의 보안환경 제공

주요 Mobile OS 지원 (Android, iOS)

- 삼성 Galaxy 시리즈와 애플 iPhone 지원을 통해 고객의 신속한 사업지원

[1] FIDO (Fast IDentity Online): PKI 인증체계를 기반으로 스마트 기기의 생체인식 기능과 Secure Storage를 온라인 인증에 적용해 간편하고 안전한 인증 방식을 제공하는 보안인증 솔루션

[2] PKI: Public Key Infrastructure, 공개키 암호화 방식의 인증체계

[3] TEE: Trusted Execution Environment, 단말 OS가 아닌 분리된 OS를 제공하는 환경

[4] UAF: Universal Authentication Framework, FIDO 1.0에서 규정한 국제 표준 인증 방식

[5] ASM: Authenticator Specific Module, 인증장치와 인증정보를 주고 받는 인터페이스

주요 기능

생체인증 + PKI 기반의 온라인 인증 체계 제공

도용 불가능한 생체인식 기반 인증 제공
금융 거래 시 부인 방지 및 데이터 무결성 보장

생체 정보 이용을 통한 간편한 사용자 인증 절차 제공

비밀번호, 복잡한 결제 정보 입력, 보안카드, OTP, 공인인증서를 대체하는 편리한 사용자 인증 절차 제공

지문+홍채 등과 같은 다중요소 인증 지원 가능

전 세계 스마트폰 시장점유율 1위 삼성 Galaxy Series 탑재

삼성 Galaxy Series 내 삼성SDS FIDO 솔루션 기본 탑재

활용 시나리오

Fast IDentity Online(FIDO)는 사용자 인증이 필요한 다양한 활용 분야에서 편리하고 안전한 방식의 인증을 제공하여 기업과 기업의 고객 모두에게 새로운 가치 제공

쇼핑몰	은행	증권
결제 부인 방지 및 One Touch 간편한 결제 가능	금융 보안 사고 예방 및 편리한 사용자 인증 제공	금융 보안 사고 예방 및 편리한 사용자 인증 제공
사내시스템	**Smart Car**	**Smart Home**
임직원 외 시스템 접속 통제 및 사내 데이터 보호	운전자에게 편리하고 안전한 원격제어 환경 제공	안전한 원격제어 환경 제공 및 에너지 소비 효율 개선 가능

삼성SDS

PC보안
(ESCORT)

PC의 외부 저장장치 및 네트워크 사용 등의 통제를 통한 내부 정보유출 차단 솔루션

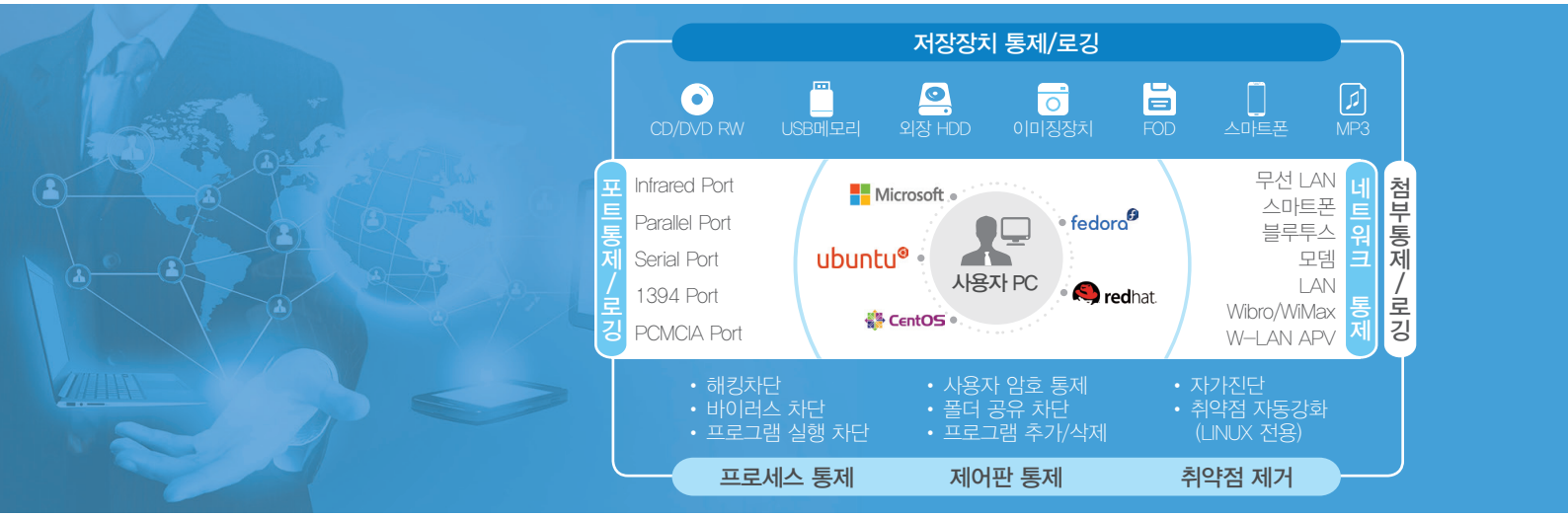
필요성

불법적인 정보유출을 차단하기 위해 저장장치 및 네트워크의 통제 필요

USB 등 외부 저장장치를 이용한 정보유출 차단
비인가 Wi-Fi 등 네트워크를 통한 회사 자산유출 방지
보안에 취약한 PC 사용통제 및 자가점검 기능 필요

솔루션 개념

PC의 저장장치, 네트워크 사용통제 및 보안 취약점 제거를 통해 PC에서 발생 가능한 정보 유출을 사전에 차단하여 회사의 정보자산 보호



주요 특징

리소스 부하 영향 최소화

• PC, 서버, 네트워크 최소 리소스 사용

예외처리 자동화

• 업무 프로세스 연계를 통한 사용자 예외처리 자동화

인사/자산 등 정보시스템 연동

• 사용자 정보기반 표준 인터페이스 제공을 통한 통제 정책 적용

자체 보호기능 가동

• 다단계 보호장치를 통한 제품 보호

세부 통제 정책 제공

• 사내/사외/개인/그룹별 세부 통제 정책 운영 가능

주요 기능

정보유출 차단 및 로깅

외부저장장치 사용통제 및 로깅
첨부파일 통제 및 로깅
무선통신, 블루투스 통제

보안 취약점 제거 및 로깅

부팅/화면보호기 취약 암호 통제
필수 S/W 설치 유도
정책위반 PC의 N/W 사용 차단

IP관리 및 사용이력 로깅

위치정보 및 Segment 정보 관리
다양한 IP환경 지원 : DHCP, VPN, 공용

다양한 PC 환경 지원

MS-Windows10 이상
Linux 환경 (GUI/CLI 모드지원)
※지원되는 Linux OS, RHEL(6.0 이상), Ubuntu (8.10 이상), CentOS (6.00이상), Fedora (10 이상)

정보유출피해 방지

- 이동식 저장장치 통제 Device 장착 통제
- 제어판 통제
- 프로그램 사용 통제
- PC사용자 실명관리
- 무선 AP 접속, 네트워크 포트 통제
- 파일첨부 통제
- 네트워크 드라이브 통제
- 인터넷 이력/접속 통제
- 멀티 OS설치 현황 파악

취약점 방지

- 부팅암호 취약점 강화
- 화면보호기 취약점 강화
- 폴더공유 취약점 강화
- 백신 취약점 강화
- Windows 계정암호 취약점 강화
- 전원 관리

IP관리

- IP 통제 관리
  - IP변경 통제
  - 사용자/사업장/Segment/ 위치정보 별 IP 관리
  - 등록/반납/기간만료
- 인터넷 접속 통제

자산관리

- S/W 현황 관리
- S/W 라이선스 관리
- S/W 배포
- S/W 설치유도
- H/W 현황 및 이력 관리
- H/W 통계

지원 환경

PC 보호 운영지원 서비스

교육, 점검, Help Desk 운영으로 안정적인 PC보안 서비스 제공
24×365 기술지원을 통한 고객 밀착 서비스

삼성SDS

PC 문서보안
(NASCA PC-DRM)

전자 문서 암호화 및 사용권한 등 PC 문서보안 솔루션

필요성

PC 문서 암호화 및 사용통제의 필요성

해커가 PC에 저장된 문서를 탈취하여도 해당 문서의 정보확인 불가
조직/사용자별 권한설정을 통해 사내 임직원간 정보유출 차단
문서 생성/수정/삭제를 기록하여, 이력관리 가능

솔루션 개념

문서 개봉/저장 시 사용자 인증 및 권한통제, 암호화 및 복호화를 적용하여 문서 생성부터 삭제까지 정보자산 Life Cycle 관리

주요 특징

다양한 전자문서 및 사용환경 지원

- 주요 3대 브라우저 (IE, Chrome, Firefox) 사용환경 지원
- 다양한 형식의 문서 편집기 파일 (MS-Office 등) 및 이미지 파일 지원

사용자 편의 기능 향상

- 다양한 권한그룹 설정 기능 제공: 가상그룹, 복수부서, 멀티사용자
- 사용자 인증을 통한 타인 PC에서의 문서 활용 가능

안정적인 서비스 제공

- 24×365 Help Desk, S/W 영향성 점검 및 년간 무상 정기점검 서비스
  운영자 및 관리자 교육 제공

주요 기능

접근 및 활용 통제 기능

전자문서, 이미지, CAD 및 동영상 S/W에 대한 DRM 처리
커스터마이징 없이도 자동 DRM 처리: 서버문서 다운로드 시 DRM 처리
보안문서 외부발송 지원: 복호화 문서 발송, 암호화 문서 발송
문서활용 내역 로깅: 개봉, 저장, 삭제, 캡처, 내용복사, 인쇄

사용자 편의 기능

새로운 S/W에 DRM 적용 시 DRM Agent 패치 없이 즉시 적용
타인 PC에서도 본인 인증 (그룹웨어)을 통한 문서 활용
PC 문서 DRM, 서버 문서 DRM, 화면통제 DRM을 조합한 통합환경 제공

지원 환경

지원 문서 S/W

MS Office
(MS WORD 2003/2007/2010/2013, MS EXCEL2003/2007/2010/2013,
MS POWERPOINT 2003/2007/2010/2013)

아래아 한글 2004/2005/2007/2010/2014

Acrobat PDF Reader 8/9/10/11, Acrobat Standard/Professional

Acro Edit/UltraEdit/Edit Plus

Adobe Photoshop, Adobe Illustrator

Corel(Jasc) PaintShop Pro

윈도우 그림판/윈도우 Picture and Fax Viewer/윈도우 Photo Gallery

삼성SDS

서버 문서보안
(NASCA 서버-DRM)

정보시스템에 존재하는 중요문서에 대한 암호화 및 권한통제를 통해 내부 시스템 정보유출 차단

필요성

정보시스템 서버에 대한 외부의 정보 유출 시도 공격 대응 방안 필요

알려지지 않은 취약점 등을 이용한 악성 공격 행위로부터 정보시스템 서버 내 중요 문서 유출에 대한 보안 대응 방안

해킹된 내부 정보시스템의 보안을 위한 화면 통제 대응 방안

솔루션 개념

업무 시스템에 등록되어 있는 문서 종류 및 정책에 따라 실시간으로 사용자의 권한을 조회하여 문서 열람 여부 정책 적용

주요 특징

화면통제 DRM

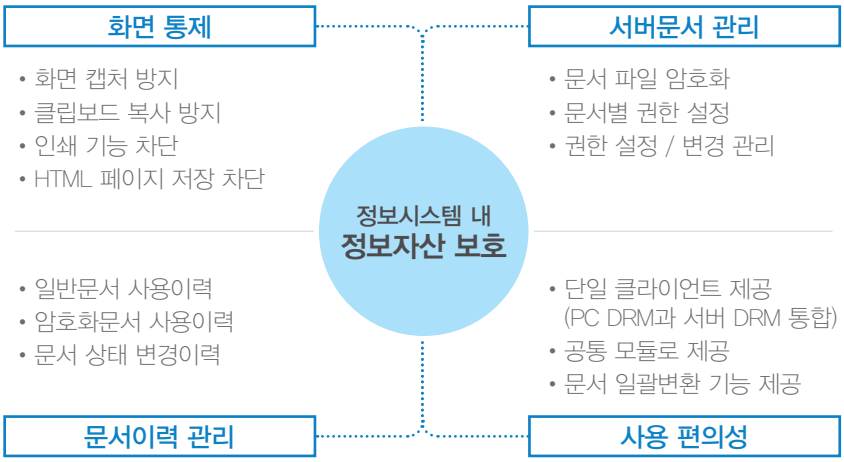
- 키보드 및 캡처 프로그램에 의한 화면 캡처 차단
- 해당 화면의 클립보드 복사 기능 차단
- 인쇄기능 차단(Context Menu 차단)
- HTML 페이지 저장 기능 차단

서버문서 DRM

- 문서 보관 기준에 따라, 문서 업로드 시 자동으로 암/복호화 처리
- 정보시스템 인증 외에 문서에 대한 서버 DRM 인증 추가
- 정보시스템 서버와 연결이 가능해야 문서개봉 가능

※ DRM: Digital Rights Management

주요 기능



화면통제 및 서버문서 DRM

PrtScr / Ctrl+C / 마우스 우클릭 차단
100여종의 캡처 프로그램 실행 차단
캡처 영역 Gray Mask 처리
Shell Context Menu의 '복사', '부가기능' 메뉴 차단
인쇄 기능 차단, Page를 파일로 저장 차단 (MHT, HTML, TXT 등)
Drag & Drop을 이용한 파일 생성 차단
개발자도구, 소스보기 차단

다양한 업무 S/W 지원

MS Office: 2003/2007/2010/2013
Adobe Reader: 7/8/9/10/11
Adobe Writer: 7/8/9/10/11
Image File: Windows Paint, Windows Default Image Viewer
Text File: MemoPad, WordPad
기타 Office: 한컴오피스, 훈민정음

다양한 서버환경 지원

ASP.NET: Windows Server 2003, 2008, 2012(32bit, 64bit)
UNIX: AIX, SOLARIS, HP-UX
Linux: REDHAT, UBUNTU

삼성SDS

EMM
(Enterprise Mobility Management)

기업의 다양한 업무 환경에 맞추어 단말부터 앱, 컨텐츠에 이르는 전체 모바일 업무 환경을 보호 및 관리할 수 있도록 하는 기업형 모바일 관리 솔루션

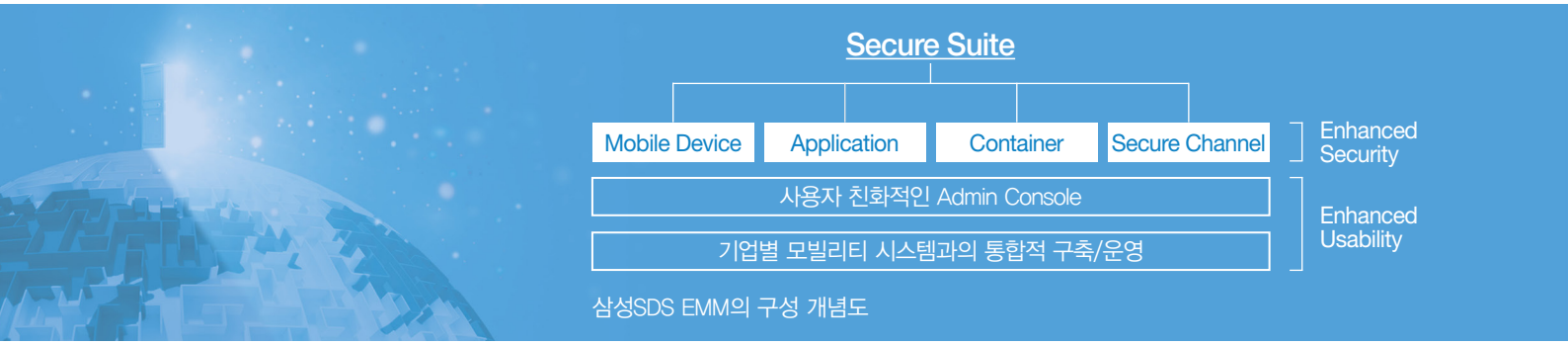
필요성

Enterprise Mobility 트렌드에 따른 보안 이슈 증가

모바일 워크 스타일, 협업 문화 등 업무 환경변화에 따른 모바일 기기내 기업정보 유출 등 기업 보안 위협 증가

솔루션 개념

단말에서부터 애플리케이션, 데이터에 이르기까지 모든 레이어에서 구현이 가능한 솔루션으로 OS에 관계없이 단일화된 하나의 콘솔을 통한 보안 운영 가능



삼성SDS EMM의 구성 개념도

주요 특징

EMM 업계 최초 미국 Common Criteria 획득

- 미국 연방정부의 보안요구사항(MDMPP 1.1)과 정보처리 표준규정(FIPS 140-2)의 보안 기준 기반 개발
- EMM 업계 최초로 미국 국가안전보장국(NSA) 산하 국가정보보증협회(NIAP)에서 미국 Common Criteria를 획득 및 미국 국가안전보장국(NSA)의 기밀정보 취급용 상업 솔루션 (Commercial Solutions for Classified Program) 목록에 EMM업계 최초 등재

안전하고 신뢰성 높은 양방향 Push 서비스 제공

- 전송률 100%, 메시지 순서 보장, 중복전송 방지 등 신뢰성 높은 고품질 양방향 Push 서비스 제공
- 통신 패킷 및 통신 채널 보안 제공을 통한 안전한 데이터 전송 제공

EMM Guardian 기능으로 단말 공장 초기화에도 안전

- 단말의 공장 초기화, EMM 삭제를 통한 EMM 무력화 방지 기능 제공

기업용 모바일 보안 웹브라우저(Secure Browser) 활용으로 기업 정보 유출 차단

- 기업의 보안정책이 적용된 모바일 웹브라우저를 통한 정보 유출과 바이러스 감염 방지

사전 정의한 이벤트 발생 시 보안 정책 즉각 적용

- 사전 정의된 이벤트 정책에 따른 모바일 운영 제어 및 효율성 제고

주요 기능

단말기 관리

부서, 개인별 보안정책 차별적용 및 기업 정보 관리
카메라, 스크린캡처 등 차단여부를 제어
원격제어 및 데이터 암호화

애플리케이션 관리

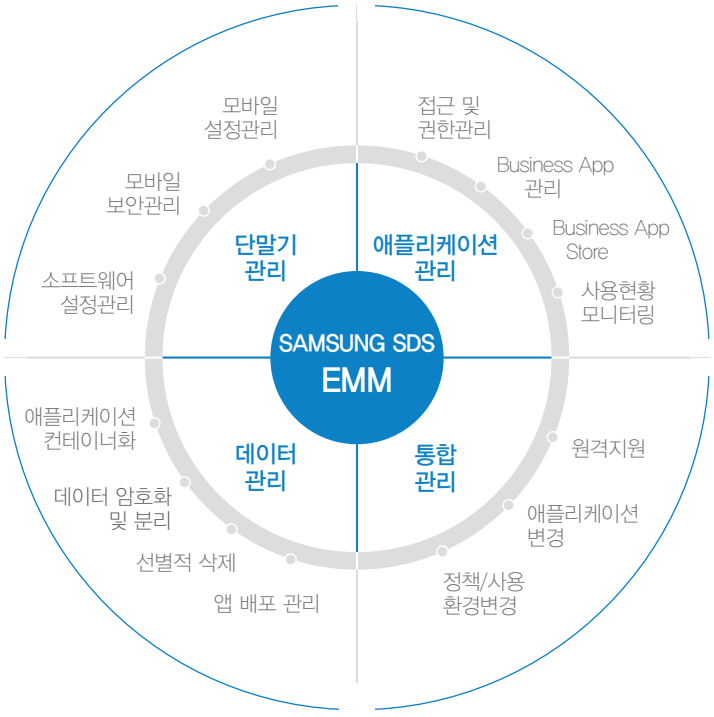
업무용 모바일 애플리케이션의 조직체계연동을 통한 사용자 접근 및 권한 관리
업무공간 접근을 위한 전용폴더 제공
사용현황 모니터링을 통한 운영 정책 수립 지원

데이터 관리(컨테이너)

컨테이너 상에서 앱 데이터를 암호화하여 분리 저장
단말기의 분실 혹은 판매 시 업무영역만 선별 삭제
사용자 권한에 기반한 모바일 앱 목록 관리

통합관리

애플리케이션 제어를 통한 기업 모바일 앱 배포 및 관리
단말기 도난 등 보안 유출 위협 발생시 원격기능 제공
사용자별 보안정책관리 기능 제공



EMM 주요기능

삼성SDS

대용량 파일 고속전송 (RAPIDANT)

저비용으로 네트워크의 효율적 사용 및 전송속도 개선이 가능한 소프트웨어 기반의 대용량 파일고속전송 솔루션

필요성

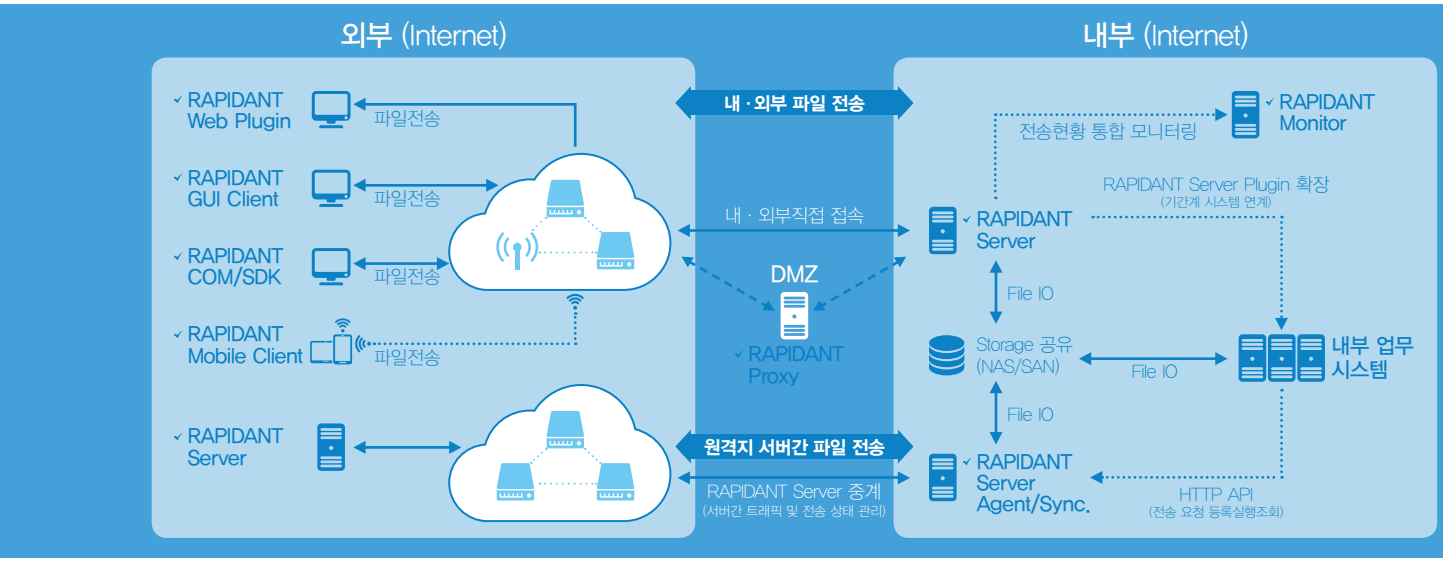
데이터의 고품질/대용량化에 따라 기존보다 빠르고 안전한 파일전송 방식 필요

방송 – SUHD 等 컨텐츠 화질 증가로 인한 전송용량 증가
제조 – 파트너社와 협업 증가로 대용량 설계 도면 전송 필요
의료 – 대량의 의료자료 및 Bio 데이터 수집 증가

솔루션 개념

✔ RAPIDANT 모듈

네트워크 운영 환경의 재구성 없이 적용 가능한 서버–클라이언트 구조로 보안 향상을 위한 RAPIDANT Proxy를 통한 파일 전송



주요 특징

소프트웨어 설치만으로 최대 100배 빠른 전송가능

- TCP/UDP 방식 모두 지원
- 대용량/다량의 파일 고속 전송

이중 검증을 통한 데이터 무결성 보장

- 데이터 손실 또는 전송 실패 시 자동화된 재전송 기능 제공
- 파일 전송 시 SSL, AES 128bit 암호화 지원

자동 동기화를 통한 사용 편의성 향상

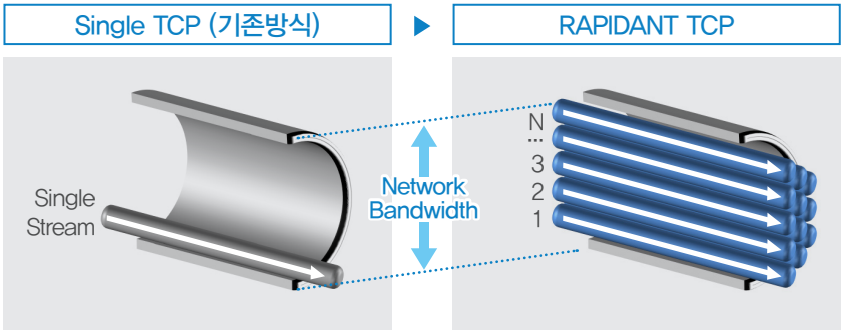
- 원격지 파일 시스템간의 변경사항에 대한 자동 동기화
- 실시간 모니터링 및 리포팅 기능 제공을 통한 성능 분석 및 전송관리

주요 기능

RAPIDANT TCP

다수(N)의 스트림을 동시에 사용하여 데이터 전송 속도를 획기적으로 개선

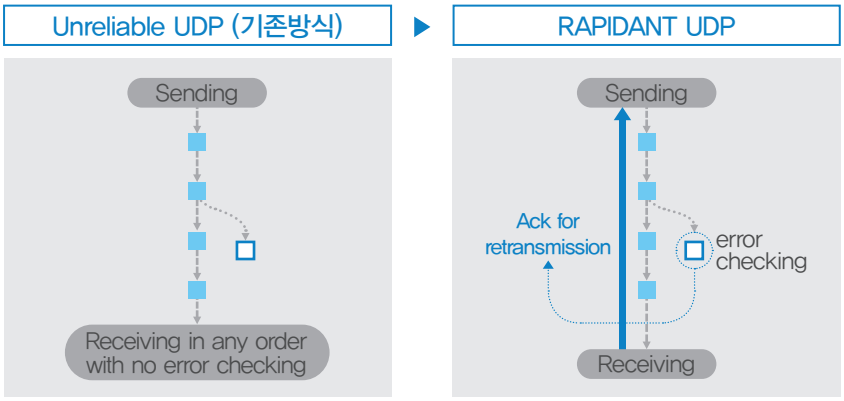
네트워크 혼잡이 발생하면 전송속도를 줄이는 비율이 1/(2N)이 되어 Single TCP 대비 전송률을 줄이는 비율이 낮음



RAPIDANT UDP

Application Layer에서 “Acknowledgement” 알고리즘을 적용하여 UDP의 단점을 보완하고 전송 데이터의 신뢰성을 보장

네트워크 상황을 고려한 전송률 제어를 통해 Wi-Fi, LTE 등 무선 네트워크에 최적화 기능 제공



삼성SDS

인프라관제
(MAXIGENT)

비즈니스와 인프라를 통합 관리하는 차세대 통합관제 시스템

필요성

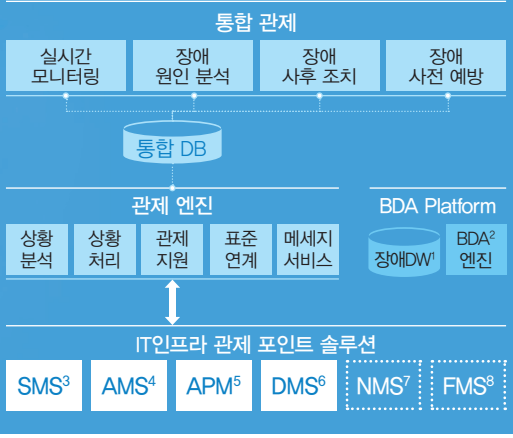
비즈니스 서비스와 IT자산의 통합관리 솔루션 필요

서비스와 시스템의 유기적인 연계를 통해 효과적인 통합관리 가능
시스템 장애 예측을 통한 비즈니스 가용성 향상

솔루션 개념

IT 자원의 이상 징후를 감지하여 장애 발생을 사전에 예방하며, 장애 발생시 신속한 감지와 정확한 장애 원인 분석으로 빠른 복구 지원

솔루션 구성도



[1] DW: Data Warehouse
[2] BDA: Big Data Analytics
[3] SMS: System Management Software
[4] AMS: Application Monitoring Software
[5] APM: Application Performance Management
[6] DMS: Database Monitoring Software
[7] NMS: Network Management System
[8] FMS: Facility Management System
'16년 출시 예정

주요 특징

비즈니스와 인프라의 통합관리

- 업무시스템에 영향을 미치는 KPI를 Rule 기반으로 관리할 수 있도록 함으로써 비즈니스와 인프라의 통합관리 지원

ProActive 장애 관리 기법

- 장애 발생시 장애의 위치와 파급효과를 실시간, 직관적으로 파악
- 통계적 기법을 적용하여 장애 징후를 감지할 수 있도록 사전대응 지원

통합관리를 위한 유연한 구조

- 다양한 자원으로부터 정형/비정형 데이터에 대한 표준인터페이스 제공
- 유연한 연계 구조를 통해 NMS, APM 등 포인트 솔루션이나 기타 관제시스템 등으로 모니터링 영역 확장 가능

검증된 방법론 적용 및 최적화된 관제 모델 제시

- 관제시스템 구축시 다양한 경험을 통해 축적된 자체 방법론 적용
- 고객사 관제 수준진단을 통해 고객사 환경에 최적화된 관제 모델 제시

주요 기능

SMS (System Management Software)

서버, DB, 네트워크 등 다양한 IT인프라에 대한 관리 정보를 자동으로 수집하여 통합적으로 모니터링하고 장애 원인을 분석하여 해결 방안 제시

- 모니터링 솔루션으로 인한 시스템 부하 최소화 (CPU 사용률 2% 이하 : AIX 6.1 기준)
- 이력데이터 스냅샷을 통한 직관적 사후 분석
- Web방식의 사용자 친화적 UI 구성

AMS (Application Monitoring Software)

비즈니스 어플리케이션을 서비스 관점에서 계층적으로 모니터링하여 장애에 대한 진단, 원인 분석과 해결 방안 제시

- Rule Engine 기반의 운영데이터 점검 자동화
- 수집 스케줄의 초 단위 상세 설정/관리
- Self-Health 체크 기능으로 시스템 안정성 향상

APM (Application Performance Management)

웹 서버, 웹 어플리케이션에 대한 실시간 트랜잭션 분석을 통해 성능 병목 및 장애 원인을 분석하여 해결 방안 제시

- J2EE 기반의 WEB/WAS 실시간 성능 모니터링
- 성능 병목 부분 집중 분석
- 실시간 트랜잭션 분석 및 관리

DMS (Database Monitoring Software)

데이터베이스에 대한 통합 모니터링을 통하여 장애 원인을 분석하고 구성, 성능, 용량 등 종합적인 관리 체계 제시

- OWI[1]에 기반한 근본 원인 추적 및 규명
- Agent 없이 성능 정보 수집
- 통합적 / 실시간 성능 분석 및 증가 추이 예측

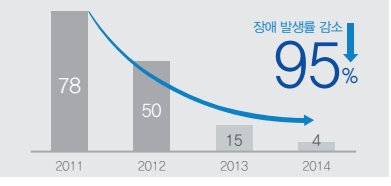
[1] OWI: Oracle Waits Interface

적용 사례

IT 인프라 운영 업무 생산성 향상

Rule Set 기반 이상 징후 감지로 장애 발생률 감소 사례

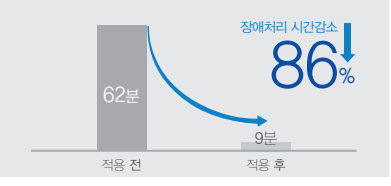
글로벌 업체인 A전자는 장애 발생시 천문학적인 비용이 소요되어 사전 예방 중심의 IT자원 운영이 필요했습니다. 삼성SDS IT Infrastructure Monitoring 도입 후 Rule Set 기반의 사전 예방 활동으로 장애 발생률이 **95% 감소**했습니다.



장애 조치 시간 및 비용 절감

KDB[2]에 의한 빠른 조치로 장애 처리시간 감소 사례

국내 1위의 B생명은 장애 발생시 고객에 직접 피해가 발생해 기업 이미지 실추에 막대한 영향을 끼칩니다. 삼성SDS IT Infrastructure Monitoring 도입 이후 KDB를 활용한 신속한 조치로 장애 처리시간을 **86% 감소**시켰습니다.



[2] KDB: Knowledge DB (실제 경험한 다양한 장애 유형의 이상 징후와 해결책을 DB화하여 유사 사례 발생시 빠르고 정확한 해결책 제시)

삼성SDS SAMSUNG

삼성SDS

방화벽 관제서비스

웜/바이러스 감염에 의한 유해 트래픽 발생과 비정상적 방화벽 트래픽 탐지 및 대응 서비스

필요성

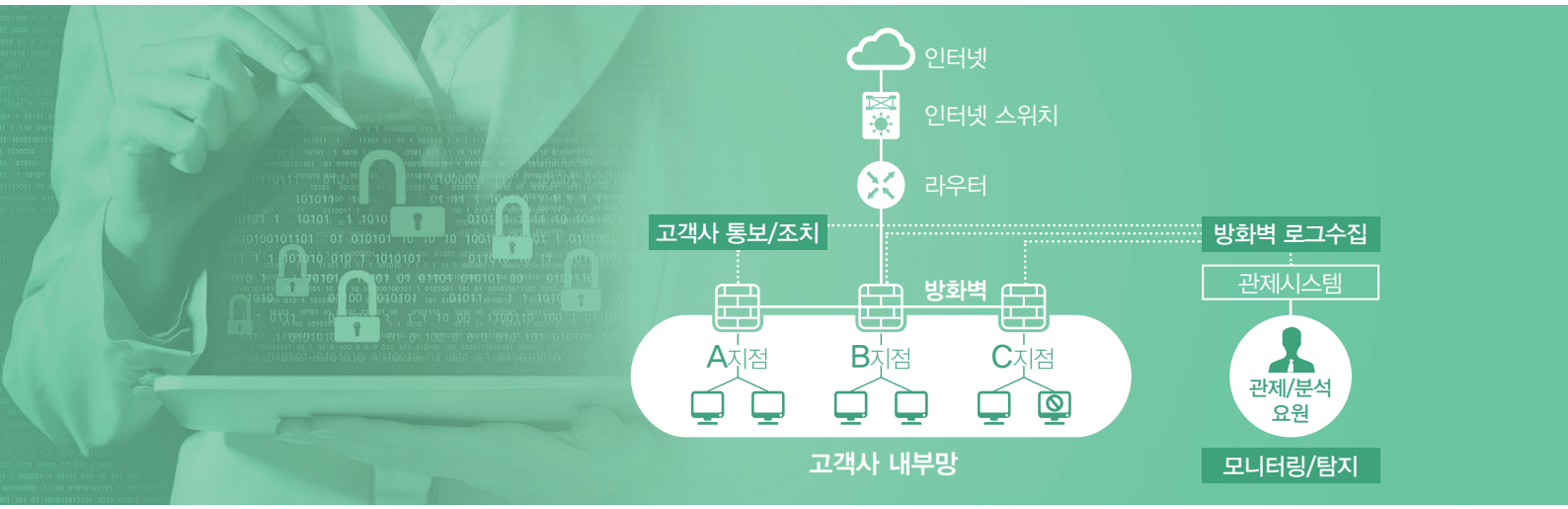
고도화되고 다각화된 네트워크 위협에 대응 필요

방화벽의 정책 설정 및 장비 운영관리 수준에서 벗어나, 방화벽 로그 분석 및 유해 트래픽 탐지 등 고도화된 방화벽 관제 필요

웜/바이러스성 트래픽, 비정상 과다 세션, 방화벽 세션 추이 급증/급감, 미수신 등 다양한 방화벽 이상 유무 확인을 통한 위협 대응 필수화

서비스 개념

방화벽의 모든 트래픽을 대상으로 웜/바이러스 및 비정상 과다 트래픽 등 유해 트래픽 유발 PC를 탐지하고 대응하는 서비스



주요 특징

추이 비교 및 비정상 트래픽 분석을 통한 실시간 위협 탐지

- 탐지된 정보는 평상시 대비 사용량(전일/전주 기준) 추이 비교 및 세션 과다발생 원인분석을 통해 위험도를 판단 및 통보

탐지된 위협에 대한 효율적인 조치 및 지원 서비스

- 긴급/일반 건으로 고객에게 실시간으로 통보
  긴급: 비정상 과다 세션 트래픽 발생 시 유선/메일 통보
  일반: 웜/바이러스성 트래픽 및 특이사항 탐지 시 경보 메일 발송
  (로그 미수신, 방화벽 이상유무 등 포함)
- 보안관제요원에 의한 유해 트래픽 발원지, 발생내역 등 분석 및 경보 발행

주요 서비스

웜/바이러스성 유해 트래픽

웜/바이러스 발생 서비스 포트(예: NetBIOS[1], IRC[2])를 이용한 이상 트래픽 탐지

비정상 과다 세션 탐지

비정상 대량 세션 및 악성 여부 탐지
Application 오작동 트래픽 탐지

방화벽 이상 유무 탐지

고객사 방화벽 세션 추이 급증, 급감, 미수신 등 탐지
평상시 사용량(전일/전주 기준) 추이 비교
세션 과다 발생 원인 분석

탐지된 이벤트에 대한 위험도 분류 및 통보

위험도 분석 후 긴급건(예: 비정상 과다 트래픽)에 대한 유선/메일 통보,
일반건(예: 웜/바이러스성 트래픽)에 대한 경보 메일 발송

사후 조치 및 결과 확인

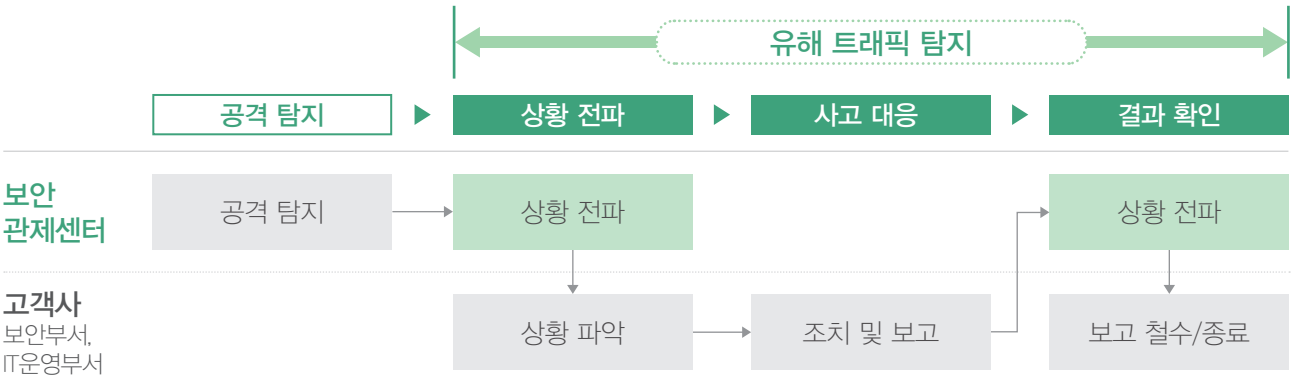
고객사 방화벽 및 보안 시스템의 해당 트래픽 차단 조치 요청
OS 보안 패치, 백신 업데이트 포함한 상황별 조치 요청 및 조치 결과 보고

[1] NetBIOS
(Network Basic Input/Output System):
IBM에서 정한 네트워크 규약

[2] IRC (Internet Relay Chat):
서버간 직접 연결로 통신하는 프로그램

서비스 프로세스

**유해 트래픽 탐지시 보안관제센터와 고객사 유관부서 간
정형화된 프로세스를 통해 단계별적인 대응체계를 운영**



삼성SDS SAMSUNG

삼성SDS

홈페이지 관제서비스

웹해킹[1] 공격 행위를 탐지 및 조치하고자 재발방지를 위한 예방활동을 제공하는 서비스

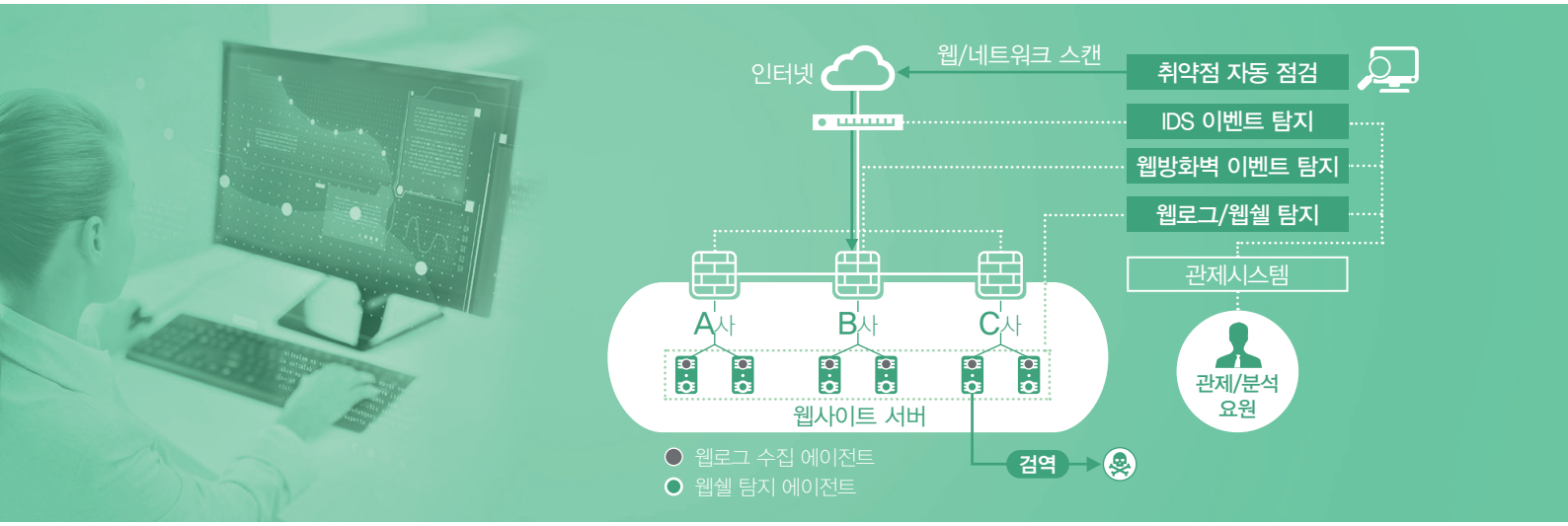
필요성

웹해킹에 대비하기 위한 「예방 – 탐지 – 조치」의 통합서비스 필요

예방: 최신 취약점 정보를 활용한 웹/네트워크 취약점 정기 진단
탐지: IDS, 웹방화벽, 웹쉘 및 웹로그 에이전트를 통한 통합분석
조치: 해킹탐지시 관제/분석요원의 정밀분석 및 잔존 취약점 점검

서비스 개념

사이버 사업장을 대상으로 하는 홈페이지 위변조, 정보탈취 등과 같은 외부 위협에 사전예방–탐지 및 대응–사후조치를 지원하여 홈페이지를 안전하게 보호하는 서비스



주요 특징

최신 웹해킹 공격에 대한 상시 자동 탐지 제공

- 홈페이지 해킹시도, 홈페이지 위변조, 웹소스내 악성URL 삽입 등 탐지
- 「수집 – 분석 – 룰셋개발 – 관제적용」 프로세스에 의한 Zero-day 공격 등 신종 웹 위협 탐지
- 공격 위험도에 따른 유형별 대응 조치

정기적인 취약점 자동점검을 통한 해킹사고 예방

- 네트워크 취약점 자동 점검 (부적절한 설정 및 OS 취약점 탐지 등)
- 웹 취약점 자동 점검 (입력값 검증 부재 등 웹 애플리케이션 취약점 탐지 등)

[1] 웹해킹: 웹사이트의 취약점을 공격하여 웹페이지를 통해 권한이 없는 시스템에 접근하거나 데이터 유출 및 파괴와 같은 행위 수행

주요 서비스

웹로그 분석

외부에서 고객사 웹사이트로 접속시, 웹서버 내부에 기록된 웹로그를 실시간 수집 및 분석

Google 정보유출 탐지

구글 검색 기능을 활용하여 설계도, 계약서, 개인정보 등 고객사 중요 정보의 유출을 탐지

웹쉘 탐지

해킹 공격에 의해 웹 서버 홈디렉토리 內 악성 웹쉘 업로드 時 실시간 탐지

상용웹쉘[2] 및 악의적으로 활용될 수 있는 구문이 포함된 파일 탐지 및 검역

침입 웹사이트 취약점 정밀 분석

최근 발생한 공격 대상으로 분석전문가의 상세수동 점검 및 조치 가이드 제공

웹트래픽 분석

외부에서 고객사 웹사이트로 접속시, 발생하는 웹트래픽을 웹방화벽 및 IDS를 통해 실시간 수집 및 분석

OWASP Top 10[1] 기준 공격패턴 탐지

웹사이트 화면 위변조 탐지

위 · 변조 정보를 수집 후 고객사 웹사이트 여부를 확인하고 원인 분석

저장된 웹사이트 화면 이미지를 비교 분석하여 위변조 탐지

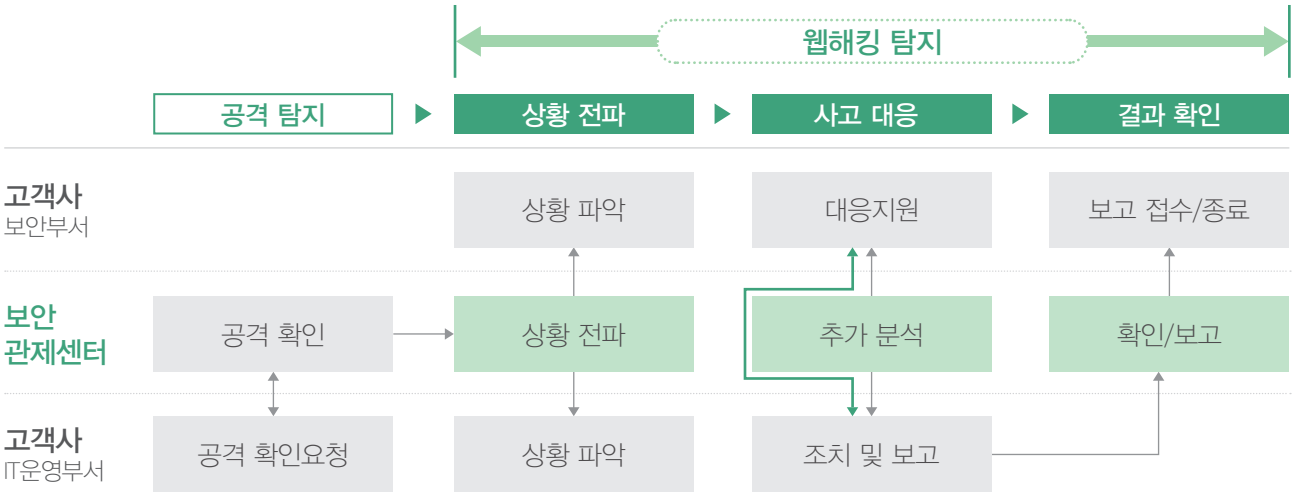
화면 비교를 통해 위변조 탐지시 HTML 웹소스 분석을 통해 소스 변조 및 악성URL 삽입 여부 탐지

[1] OWASP Top 10: 오픈소스 웹 애플리케이션 보안 프로젝트로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하여 발표한 10대 웹 애플리케이션의 취약점

[2] 상용웹쉘: 해커에 의해 제작된 악성 파일로, 블랙마켓에서 거래되거나 Google 검색을 통해 유포되는 널리 알려진 웹쉘

서비스 프로세스

웹해킹 공격 탐지시 보안관제센터와 고객사 유관부서 간 정형화된 프로세스를 통해 단계별로 신속하고 정확하게 상황 전파 및 대응 실시



삼성SDS SAMSUNG

삼성SDS

악성코드 관제서비스

인터넷을 통해 내부로 유입되는 악성코드를 탐지하여 정보유출을 방지하는 서비스

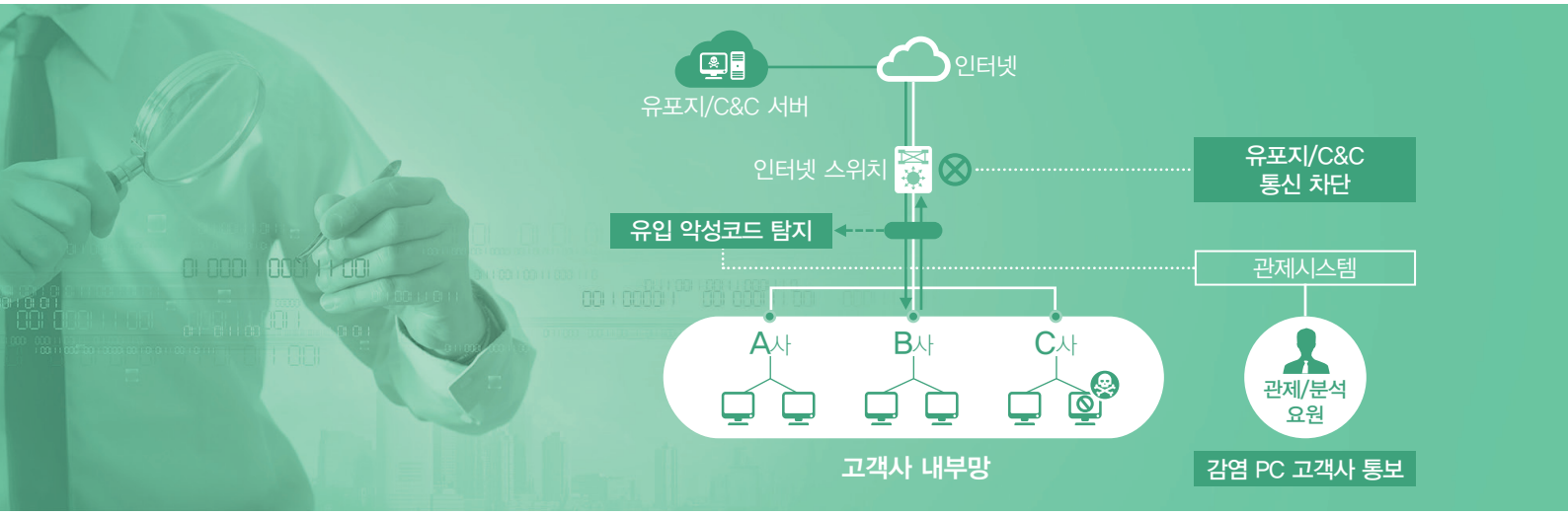
필요성

악성코드 감염 탐지 및 대응을 위한 「탐지 – 차단 – 조치」의 서비스 필요

탐지: 외부에서 내부PC로 유입되는 악성코드 및 유포지 탐지
차단: 악성코드 유포지 차단 및 C&C 접속시도 차단
조치: 감염PC에 대한 경보 및 조치 가이드 제공 서비스

서비스 개념

인터넷을 통해 내부PC로 유입되는 악성코드를 탐지하여 유포지 및 C&C서버[1]와의 통신을 차단하고 정보 유출을 방지하는 보안관제 서비스



주요 특징

하이브리드 기반 분석 기법

- 악성코드 정적분석과 동적분석 결합
- 행위간 연관분석 및 평판분석
- 취약점을 이용한 문서형 악성코드 탐지

실시간 위협 모니터링

- 모든 탐지 및 분석 대상의 악성여부에 대한 명확한 가시성 제공
- 관심 이벤트(파일, IP, URL)에 대한 집중 모니터링

악성코드 발생 현황 분석 정보 제공

- 악성코드 탐지 추이, 주요 유포지/C&C서버 탐지 현황 분석 정보

[1] C&C 서버 (Command and Control Server): 악성코드가 감염된 PC에 명령을 내리고 데이터를 수신하는데 사용되는 서버

주요 서비스

알려진 악성코드뿐만 아니라 악성으로 의심되는 파일까지 검사/탐지

1단계: 알려진 악성코드 유입 탐지
시그니처 기반 패턴 매칭 방식
2단계: 변종/신종 악성코드 탐지
파일 평판 분석 및 행위 분석 방식

악성코드 유포지 탐지 및 차단

악성코드가 업로드된 사이트 접속을 통해 다운로드 URL/IP 탐지
악성코드 감염경로 분석 및 검증 후 URL/IP 실시간 차단 적용

C&C서버 통신 차단

다수 소스에서 발표된 신종 악성코드 정보 및 자체 수집된 C&C서버 정보 기반으로 악성 URL/IP 차단 적용

탐지된 악성코드에 대한 위험도 분류 및 통보

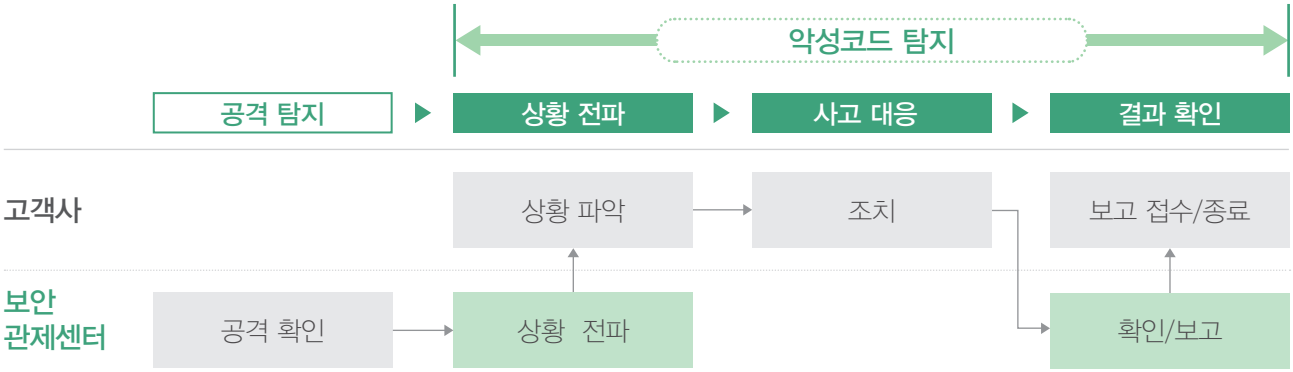
위험도 분석 후 긴급건/일반건으로 고객사에 실시간 통보

백신엔진 업데이트

신종 악성코드 탐지시 백신업체에 의뢰하여 업데이트 조치
진단명 및 신규 백신 버전 정보 제공

서비스 프로세스

악성코드 탐지시 보안관제센터와 고객사 유관부서 간 정형화된 프로세스를 통해 단계별로 신속하고 정확하게 상황 전파 및 대응 실시



삼성SDS

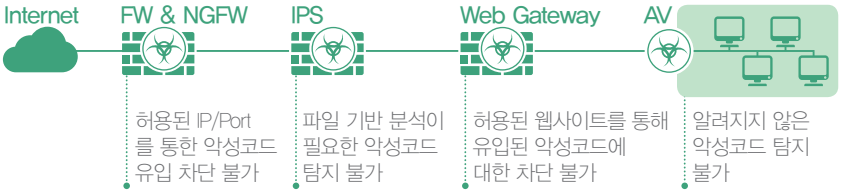
APT[1] 관제서비스

비정상 행위, 공격행위 은닉 등 고도화된 타깃 공격에 대한 대응 서비스

필요성

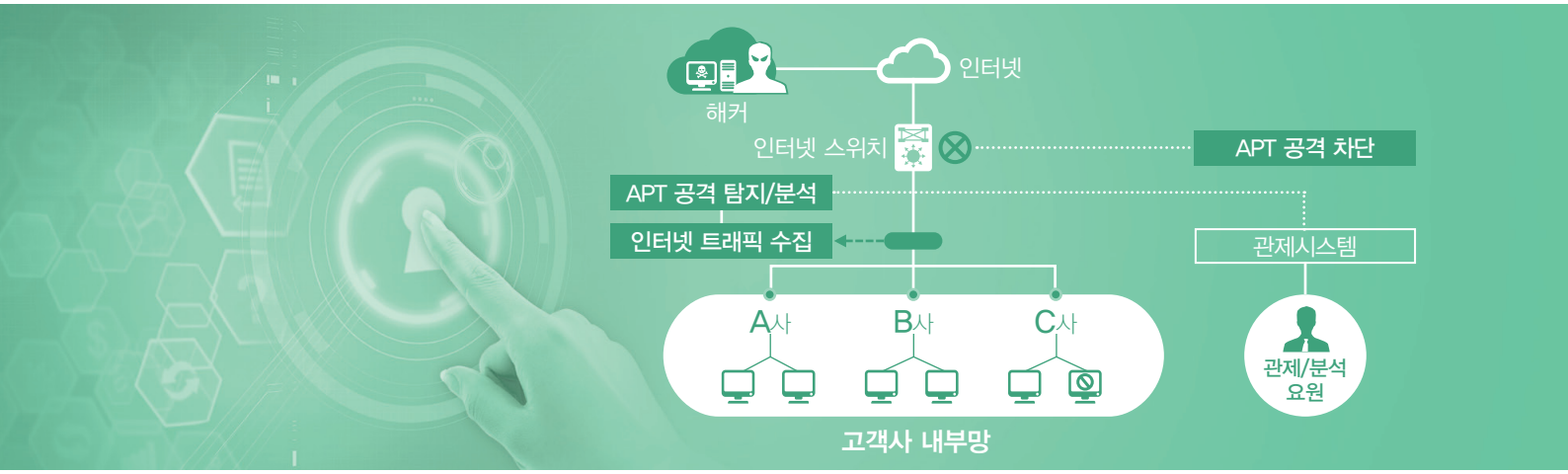
기존 보안솔루션의 타깃 공격에 대한 대응 한계

APT 해킹은 사회공학기법, 각종 은닉 기술 등을 활용하여 백신, 방화벽, IPS와 같은 기존 보안솔루션으로는 대응에 한계 존재



서비스 개념

APT 공격에 의한 내부 감염PC의 비정상적인 행위를 분석하여
정보유출 행위를 신속히 탐지하고 차단하기 위한 보안관제 서비스



주요 특징

정교한 의심파일 및 의심트래픽 탐지 및 분석

- PE형식의 실행파일 및 문서파일에 대한 의심파일 추출 후 동적분석을 통해 악성코드 유무 판별
- APT 위협정보에 접속 또는 감염이 의심되는 트래픽에 대한 정밀분석
- 내부 사용자의 자료 유출 탐지

APT 상세 현황 분석 정보 제공

- 탐지유형, 분석현황, 경보현황, 차단현황 등 상세 리포트 제공
- 전체 악성 파일 유입 및 의심트래픽 분석/통계 정보 제공

[1] APT (Advanced Persistent Threat): 타깃을 정해 고도의 공격 기법들이 성공할 때까지 지속적으로 시도하는 공격

주요 서비스

Full Packet 수집

기업 ↔ 인터넷간 송수신 되는 모든 네트워크 통신내역을 수집
비정상 통신 패킷추출 (예: https를 사용하는 평문통신 패킷)

Packet 분석

난독화된 네트워크 트래픽 복호화
자체 보유 악성IP/URL 접속현황 분석
대용량, 지속적인 정보 전송현황 분석

파일 평판 분석

정상 파일 여부 확인
파일 속성, 작성자, 작성일 등 Header 정보와 유포지의 악성여부 확인

동적/정적 평판 분석

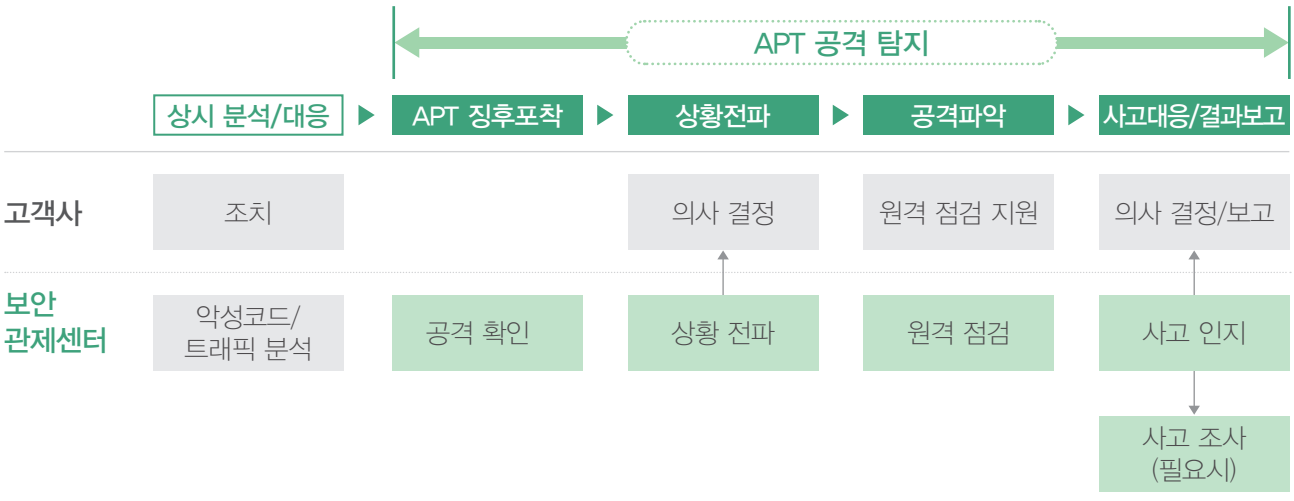
파일, 프로세스, 레지스트리, 네트워크, API 등 OS행위 분석
행위간 상관분석
메모리 분석/어셈블리 코드 분석

APT 공격 차단 및 고객사 통보

의심파일 및 의심트래픽 분석결과 확인된 유포지, 경유지, C&C서버, 정보유출서버 차단

서비스 프로세스

APT 공격 탐지시 보안관제센터와 고객사 유관부서 간 정형화된 프로세스를 통해 단계별로 신속하고 정확하게 상황 전파 및 대응 실시



삼성SDS SAMSUNG