삼성SDS

방화벽 관제서비스

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

필요성

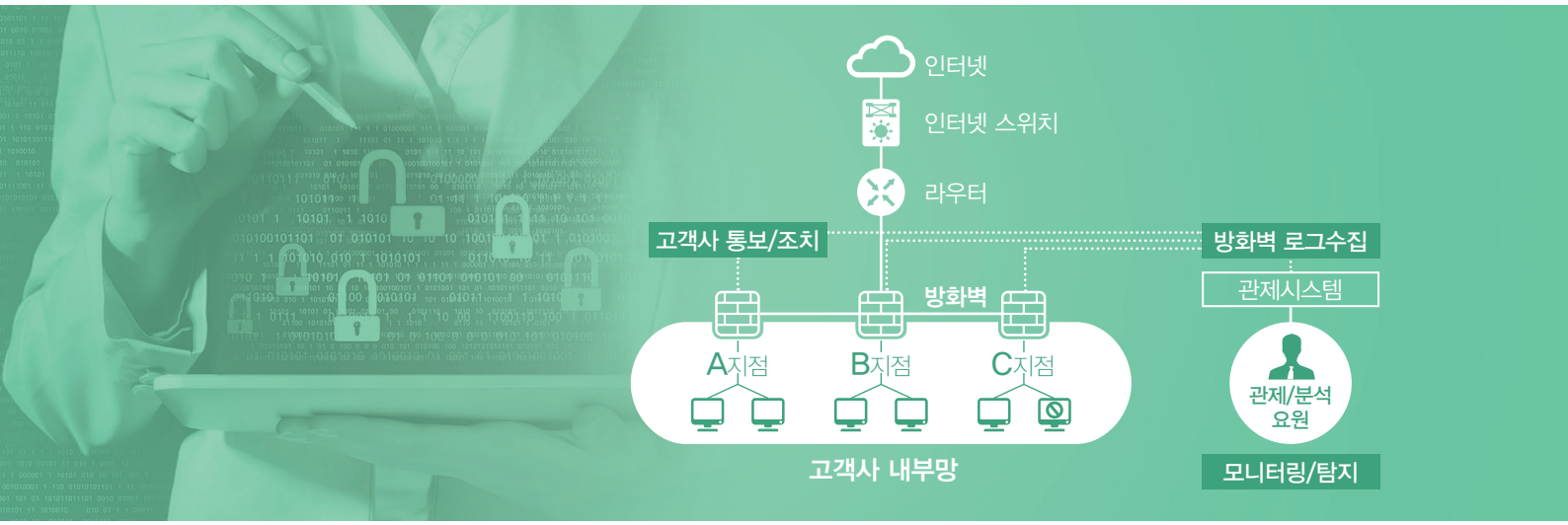
고도화되고 다각화된 네트워크 위협에 대응 필요

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 트래픽탐지

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

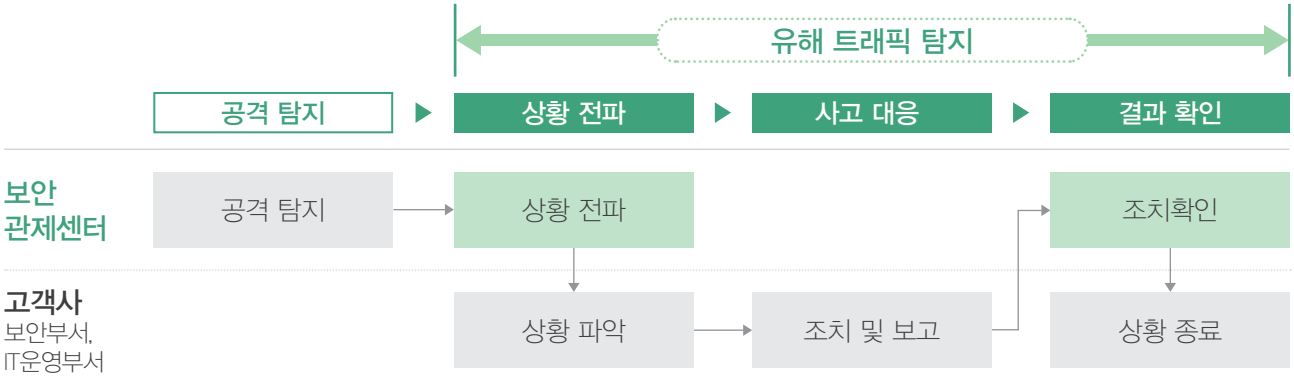
- 고객사 방화벽 및 보안 시스템의 해당 트래픽 차단 조치 요청
- OS 보안 패치, 백신 업데이트 포함한 상황별 조치 요청 및 조치 결과 보고

[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



Copyright © 2018 Samsung SDS. All rights reserved.

SAMSUNG SDS