AhnLab

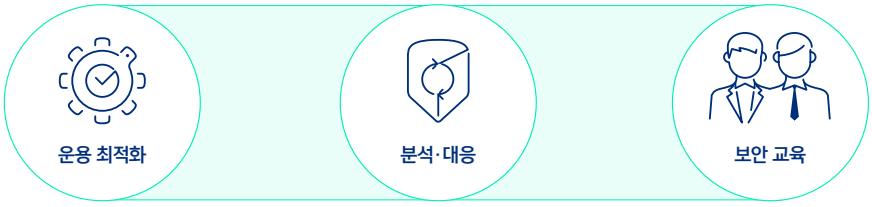
Professional Service

스마트한 보안 관리자의 선택

시스템 사전 점검·관리부터 보안 사고 대응까지,
전문가에 의한 차별적인 보안 운용 서비스

서비스 개요

안랩 프로페셔널 서비스(AhnLab Professional Service)는 제한적인 리소스로 최신 보안 위협에 대응해야 하는 기업 보안 관리자를 위한 '전문가 보안 위협 관리 서비스'입니다. 보안 솔루션 운용, 보안 위협 분석 대응, 정보보안 교육 등 3개 영역, 7가지 서비스로 구성된 전문 서비스를 개별 또는 연계하여 제공함으로써 기업의 보안 부담은 최소화하고 사전 예방 효과는 극대화합니다.



보안 솔루션 운용 최적화
효과적인 보안 솔루션 관리
장애 최소화 및 사전 예방 효과

보안 위협 분석 및 대응
시스템 진단을 통한 잠재 위협 제거
보안 사고 원인 규명 및 예방책 제시

맞춤형 정보보안 교육
임직원 보안 인식 제고
보안 솔루션 이해 · 활용 강화

서비스 배경

기업의 IT 환경은 나날이 복잡다단해지고, 랜섬웨어 등 신종 보안 위협이 지속적으로 증가함에 따라 보안 솔루션 또한 고도화되고 있습니다. 그러나 다양한 위협에 대응하기 위해 다수의 보안 솔루션을 도입하다 보니 관리자의 부담은 늘고, 보안의 효용성은 떨어지는 경우가 대부분입니다.

01. 보안 솔루션 데이터 분석 서비스

안랩 보안 솔루션의 안정적인 운용을 위해 전문가가 정기적으로 원격 또는 방문하여 점검하고 최적화하는 서비스입니다. 정기적인 점검 활동을 통해 보안 위협 요인에 대한 예방 조치와 보안 솔루션의 장애를 미연에 방지함으로써 안정적인 보안 운영이 가능합니다.

* AhnLab EPP, AhnLab MDS 이용 고객사에 한함

서비스 방식

- 안랩 전문가가 정기적으로 현장 방문 또는 원격으로 보안 솔루션 점검
  - 방문 점검 또는 원격 점검

주요 내용

- 점검 항목에 대한 보고서 및 개선 방안(Best Practice) 제공
- 예상되는 장애 및 보안 위협 요인에 대한 후속 예방 조치 수행

기대 효과

- 시스템 장애 사전 예방 및 안정적인 보안 솔루션 운용
- 정책 설정 등 비즈니스 환경에 최적화된 보안 시스템 운영 환경 확보

02. 전문가 온디멘드 서비스

고객의 중요 및 긴급 요청에 대해 안랩의 전문가가 현장에서 신속하게 이슈 대응 및 조치 방안을 제공하는 고급 기술지원 서비스입니다. 안랩의 직접적인 기술지원을 통해 민감한 보안 이슈를 해소함으로써 안정적인 비즈니스 운영이 가능합니다.

서비스 방식

- 안랩 전문 기술지원 엔지니어의 현장 지원

주요 내용

- 고객사 요청 시, 안랩의 전문 엔지니어가 현장에서 보안 이슈 대응

기대 효과

- 신속하고 전문적인 이슈 해결
- 비즈니스 중단 방지 또는 최소화

03. 보안 감사 사전 점검 서비스

컴플라이언스 등과 관련된 기업 및 기관의 리소스 부담을 최소화하고 성공적인 보안감사 수행 및 리스크 관리에 기여하는 서비스입니다. 감사 대상의 보안 규정을 파악하고 실질적인 이행(조치) 방안을 제시합니다.

* 안랩 엔드포인트 보안 관리 솔루션 보유 고객에 한함

서비스 방식

- 안랩의 공인된 전문 엔지니어가 일정 기간 고객사에 상주하여 서비스 수행

주요 내용

- 보안감사 항목 현황 점검
- 보안 규정 관련 기술적 조치 수행 – AhnLab EPP Management 서버에 한함
- 점검 및 기술적 조치 수행에 대한 결과 보고서 제공 – 보안감사 자료로 활용 가능

기대 효과

- 보안감사에 따른 고객사 리소스 부담 최소화
- 적절한 이행(조치)을 통한 보안감사 및 컴플라이언스 준수

01. 의심 시스템 진단 서비스

기업 및 기관의 인프라에 연결된 시스템들을 분석하여 은닉하고 있는 보안 위협을 사전에 탐지하고 대응 방안을 제공하는 서비스로, 보안 사고를 사전에 예방함으로써 기업의 리스크 관리에 기여합니다.

서비스 방식

- 안랩의 자체적인 시스템 로그 수집 유틸리티를 이용해 보안 위협 분석 수행

주요 내용

- 보안 위협 및 시스템 취약점 종합 진단
- 악성으로 의심되는 파일 수집 및 V3 엔진을 이용한 대응
- 확인된 보안 위협에 대한 분석 및 대응 방안 제공
- 서비스 이용 범위에 따라 PC 전수 보안 위협 점검 제공

기대 효과

- 보안 사고 예방 · 탐지 · 대응(복구) 등 위험 관리 방안 확보
- 보안 정책 설정 등 비즈니스 환경에 최적화된 시스템 운영 환경 구축

02. 악성코드 전문가 분석 서비스

기업 및 기관 내부로 유입된 악성코드(파일)의 기능 및 특성에 대해 국내 최고의 악성코드 전문 분석가들이 직접 상세하게 분석하여 최적의 대응 방안을 제공하는 서비스입니다.

서비스 방식

- 고객사 요청 시 안랩 분석 전문가의 상세 분석 제공

주요 내용

- 파일의 주요 기능, 동작 및 특징 분석
  - 파일 다운로드, 파일 복제/생성, 네트워크 연결, 레지스트리 변경 등
- 악성코드로 판명될 경우 솔루션 기반의 대응 방안 제공(V3 및 MDS 기준)
- 서비스 이용 범위에 따라 기본 보고서 또는 상세 분석 보고서 제공
  - 기본 보고서는 윈도우 계열 파일 포맷에 대한 분석 정보만 제공

기대 효과

- 내부로 유입된 악성코드의 상세한 정보 파악 및 대응 방안 마련

03. A-FIRST 포렌식 서비스

안랩의 차별적인 위협 분석 기술력과 전문성을 기반으로 보안 침해사고를 분석하여 최적의 대응 방안을 제시하는 '전문 디지털 포렌식 서비스'입니다. 기업 및 기관의 자체 확인이 어려운 공격 유입 경로를 분석하고 디지털 증거를 수집해 침해사고의 원인과 피해 범위, 유출 경로 등을 파악하고, 그에 따른 조치를 제공함으로써 효과적인 피해 복구 및 재발 방지에 기여합니다.

서비스 방식

- 고객사 요구 시 협의 후 안랩의 디지털 포렌식 전문가 분석 진행
  - 고객사 현장 분석 또는 안랩 본사 분석

주요 내용

- 주요 점검 대상(PC, 서버, 메모리, 로그) 분석 및 디지털 증거 수집
- 디지털 포렌식 분석 및 결과에 따른 조치 방안 제시
- 악성코드에 의한 침해사고로 확인 시, '악성코드 전문가 분석 서비스'로 연계 가능

기대 효과

- 보안 침해사고에 따른 영향도 분석을 통한 리스크 관리 가능
- 공격 유입 경로 파악 및 분석을 통한 지능형 위협(APT) 등 보안 사고 재발 방지

01. 정보보안 교육 서비스

기업 및 기관의 특성에 따라 최적의 보안 정보를 제공해 내부 임직원의 보안 인식 제고에 기여하는 맞춤형 정보보안 교육 서비스입니다. 풍부한 경험을 보유한 안랩의 전문 강사진이 기업 및 기관의 비즈니스에 특화된 정보보안 교육을 제공함으로써 임직원의 정보보안 인식을 강화하는 것은 물론, 사내 보안 인력의 효과적인 솔루션 운영에 기여합니다.

제공 방식

- 고객사 요청 시 안랩 전문 강사진의 보안 교육 강의 진행
  - 교육 내용, 규모, 장소 등에 대한 사전 협의 가능

주요 내용

- 맞춤형 교육 과정 구성
- 안랩 제품 및 서비스와 연계된 전문가 교육

기대 효과

- 사용자(임직원)의 정보보안 인식 제고
- 보안 솔루션 활용도 향상

도입 사례

ISP 업체인 A사는 '보안 고도화 사업'의 일환으로 백신, PC 취약점 조치 솔루션, 엔드포인트 중앙 관리 솔루션 등을 새로 도입하기로 결정했습니다. A사는 보안 솔루션의 설치에 앞서 내부 업무 및 안정적인 대고객 서비스 제공을 위해 전반적인 솔루션 구축 설계와 각 솔루션의 정책 설정 최적화를 진행했습니다.

서비스 도입 배경 및 요구 사항

- 백신 및 다수의 엔드포인트 보안 솔루션 신규 도입을 위한 구축 설계
- 각 보안 솔루션의 정책 최적화 및 운영 안정화

이용 서비스

- 보안 솔루션 데이터 분석 서비스

서비스 도입 효과

- 민감한 서비스를 제공하는 비즈니스 환경에 최적화된 보안 체계 마련
- 보안 솔루션 설정 및 운영 리소스 절감 효과

국내외 다수의 건설 현장을 보유하고 있는 종합건설업체인 B사는 랜섬웨어와 지능형 위협(APT)에 대비하기 위해 우선 사내 시스템의 보안 상태를 면밀하게 점검하고자 하였습니다. 이에 '의심 시스템 진단 서비스'를 진행하여 점검 결과에 따라 필요한 조치를 수행하고 보안 정책 가이드도 마련했습니다.

서비스 도입 배경 및 요구 사항

- 랜섬웨어 및 APT 대응을 위한 사내 보안 현황 점검
- 전체 서버 및 일부 PC에 대한 악성코드 존재 여부 확인 및 조치

이용 서비스

- 의심 시스템 진단 서비스

서비스 도입 효과

- 일부 시스템 내 은닉형 악성코드 탐지 및 조치 (치료/삭제)
- 일부 시스템에 설치된 PUP 제거를 통한 시스템 성능 향상
- 시스템 및 업무별 보안 정책 가이드 수립을 통한 보안 강화
- 분석 보고서를 토대로 필요 솔루션 추가 도입 검토 중

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901

AhnLab