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 최적화, 보안 위협 분석 대응, 전문가 기술지원의 3개 영역, 9가지 서비스로 구성된 전문 서비스를 개별 또는 연계하여 제공함으로써 기업의 요구에 부합하는 최적의 보안 서비스를 제공합니다.

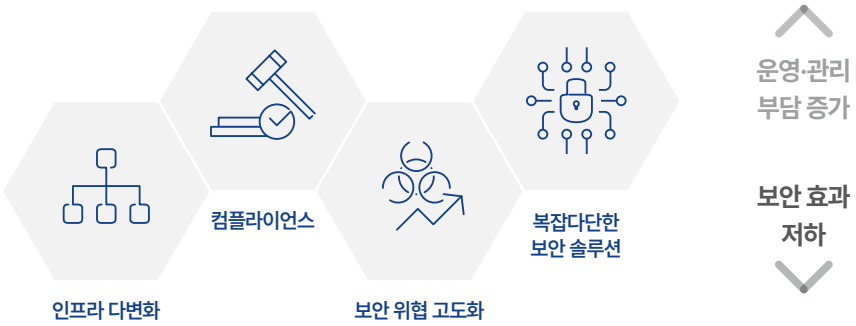
보안 솔루션 운용 최적화
효과적인 보안 솔루션 관리
장애 최소화 및 사전 예방 효과

보안 위협 분석 및 대응
시스템 진단을 통한 잠재 위협 탐지
보안(침해)사고 원인 규명 및
재발 방지책 수립

전문가 기술지원
전문가 이슈 대응 및 조치방안 제공
보안솔루션 구축 지원 및 안정화

서비스 배경

기업의 IT 환경은 갈수록 복잡해지고 있으며, 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. 데이터 분석 서비스

안랩 보안 솔루션의 안정적인 운영을 위해 로그 수집, 분석 및 시스템 최적화 작업을 수행하는 서비스 입니다. 이를 통해 보안 위협 요소를 식별하고, 효과적인 대응 방안을 제시함으로써 보안 체계를 강화하고 안정적인 운영 환경을 제공합니다.

* 안랩 EPP, MDS 솔루션 이용 고객사에 한함

서비스 방식

- 서비스 등급에 따라 안랩 전문가가 원격 또는 방문하여 보안 솔루션 운영 현황 분석 결과 보고 및 조치 필요/권고 사항 가이드

주요 내용

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

기대 효과

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

02. AIPS·DPX 정책 최적화 서비스

보안 솔루션의 운영 현황, 탐지 로그 및 정책을 분석하여 고객 환경에 최적화된 정책을 수립하고 보안 위협의 대응 체계 수립을 지원합니다.

서비스 방식

- 안랩 전문가가 현장 방문하여 정책 최적화 수행

주요 내용

- 운영 현황 및 탐지 로그 분석 (AIPS)
- 시그니처 최적화 방안 제시, 정책 적용 및 적용 결과 분석, 결과 보고서 제공 (AIPS)
- 자동 학습 기능을 통해 Zone별 정책 최적화 수행 (DPX)
- 보호대상 정책 최적화 및 결과 보고서 제공 (DPX)

기대 효과

- 정책 최적화를 통해 보안 사고 예방 및 솔루션의 안정적인 운영 기대

03. DDoS 공격 모의훈련 서비스

기업 및 기관에서 운영 중인 시스템을 대상으로 공격되는 DDoS 공격에 효과적으로 대응하기 위해 현재 네트워크 및 서버의 보안 대응 수준을 확인하고 향후 공격 발생 시 대응 방안을 제공합니다.

서비스 방식

- 안랩 전문가가 계측 장비를 이용하여 DDoS 공격·대응 및 결과 보고 수행

주요 내용

- 훈련의 정확성 확보를 위한 계측 장비 사용
- 시나리오 기반 최신 DDoS 공격 재현
- DDoS 대응 정책 및 절차 전반에 대한 문제점 진단 및 개선 방안 도출

기대 효과

- DDoS 공격 모의 훈련을 통해 최적의 대응 방안 제시 및 사고 예방 기여
- 방어 대응 체계 검증 / 트래픽 가용성 확인/ 각종 보안 장비 서비스 취약점 확인

01. 의심 시스템 진단 서비스

기업 및 기관에서 운영 중인 시스템을 분석하여 은닉하고 있는 보안 위협 및 취약점을 사전에 탐지하고 대응 방안을 제공하는 서비스로, 보안(침해)사고를 사전에 예방함으로써 기업의 리스크 관리에 기여합니다.

서비스 방식

- 안랩의 자체적인 시스템 로그 수집 유틸리티를 이용해 보안 위협 및 취약점 분석

주요 내용

- 보안 위협 및 위협과 연관된 기술적 취약점 점검이 포함된 시스템 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 점검 제공 가능

기대 효과

- 보안 위협·취약점을 분석하여 보안(침해)사고 예방 및 보안 수준 향상에 기여
- 보안(침해)사고 대응 조치를 위한 원인 파악 및 기술적 보호 대책 제시

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

- 분석 요청 파일에 대한 상세 분석 및 결과 보고서 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 분석 정보 제공
- 분석 정보 기반 대응 방안 제시

03. A-FIRST 포렌식 서비스

안랩의 차별적인 위협 분석 기술력과 전문성을 기반으로 보안(침해) 사고를 분석하여 최적의 대응 방안을 제시하는 '전문 디지털 포렌식 서비스'입니다. 기업 및 기관의 자체 확인이 어려운 공격 유입 경로를 분석하고 디지털 증거를 수집해 사고의 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

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 보안(침해) 사고 시, '악성코드 전문가 분석 서비스'로 연계 가능

기대 효과

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

01. 전문가 온디멘드 서비스

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

서비스 방식
- 안랩 전문 기술지원 엔지니어의 직접 지원

주요 내용
- 고객의 요구 시점에 신속한 현장 기술지원 서비스 제공

기대 효과
- 신속하고 전문적인 이슈 해결
- 비즈니스 중단 방지 또는 최소화

02. XDR 구축 서비스

XDR 구축 서비스는 고객 환경에 최적화된 XDR 솔루션 도입과 안정적인 운영 환경 정착을 지원하는 전문가 서비스입니다. 이를 통해 보안 가시성을 확보하고, 고도화된 위협 탐지·대응 체계를 효과적으로 구축할 수 있습니다.

서비스 방식
- 안랩 전문가가 XDR 솔루션 구축 및 운영 프로세스 확립

주요 내용
- 구축 환경 분석 및 연동 대상 보안 로그 분석
- XDR 솔루션 구축 및 이기종 보안 솔루션 연동
- 탐지 현황 분석을 통한 보안 리스크 식별
- 식별된 보안 리스크 기반 연계 대응 정책 수립

기대 효과
- XDR 기반 통합 보안 가시성 확보 및 리스크 관리 체계 구축에 기여
- 운영 프로세스 확립을 통한 안정성 확보 및 조직 보안 수준 향상 기대

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

AhnLab