

기업의 보안 수준 강화를 위한 최적의 서비스, 파수 마인드셋 (Mind-SAT) 올인원 패키지

과학기술정보통신부 지정 정보보호 전문 서비스 기업 '파수'가
다년간의 경험을 기반으로 기업의 보안 수준을 끌어올릴 올인원 서비스를 제공합니다.

사내에 중요한 자료들은 많은데, 보안 위협은 증가한다고 하고, 내부에 보안 전문 인력은 따로 없고...
지금까지 참 막막하셨죠?

그러나 막상 보안 담당자를 채용하더라도 취약점 진단, 훈련, 교육을 모두
자체적으로 진행하기에는 역부족인 것 또한 현실입니다.

파수 마인드셋 (Mind-SAT) 올인원 패키지는 별도의 구축 비용 없이 서비스 이용료만 지불하는
합리적인 가격정책 아래 고객 니즈에 따라 선택할 수 있는 맞춤형 보안 서비스, 검증된 기술력
그리고 전문적인 노하우로 기업 여러분들의 오랜 고민을 바로 해결해 드립니다.

아래와 같은 고민이 1개라도 있다면, 지금 바로 연락주세요!

- 보안 담당자가 따로 없어 현재 보안 수준을 체크하기가 어렵다.
- 임직원들의 보안 의식 수준을 높이고 싶다.
- 원청사에서 보안 수준 체크가 지속적으로 일어나고 있다.
- 보안인증을 별도로 진행하기에는 제반 비용이 너무 부담스럽다.



• 인프라 진단
• 모의해킹

• 악성메일 모의훈련
• 신고센터 운영
• 결과 보고서

• 보안강화 교육
• 특화 교육

기업의 보안 수준 강화를 위한 최적의 서비스, 파수 마인드셋 (Mind-SAT) 올인원 패키지



취약점 진단 PACK

인프라 진단

과학기술정보통신부 지정 정보보호 전문 서비스 기업으로서 서버, WEB / WAS 취약점 진단, DBMS 취약점 진단, 네트워크 · 정보보호시스템 취약점 진단에 대해 자체 보유 진단 프로그램과 인터뷰 및 실사점검 결과를 종합해 기술적 보안 수준을 진단하고, 취약점의 원인 분석

모의해킹

사전에 인가받은 장소와 장비를 통해 주요 정보통신기반시설 웹 취약점 분석 평가 28개 항목으로 취약점을 진단하며, 크로스사이트 스크립팅, SQL 인젝션 등 실제 악의적인 해커에 의한 침입 가능성을 점검

정보보호 대책 제시

자산별 취약점에 대한 위험평가를 실시해 위험도에 따른 보호 대책 제시

- 위험 수용 취약점 관리 방안 제시
- 위험 통제 취약점 조치 방안 제시

모의 훈련 PACK

악성메일 모의훈련

파수는 사회공학적 기법을 근간으로 시나리오 기반의 악성 의심 메일을 생성하고 직원에게 발송해 신고를 유도, 신고율과 참여율을 통계화 하고 전체적인 보안 수준을 점검

신고센터 운영

수신한 메일 중 의심스러운 메일은 열기, 첨부파일 실행, 링크 클릭 등을 하지 않고 악성메일 여부를 먼저 확인할 수 있도록 신고센터를 운영하며, 검증 과정을 거쳐 신고자에게 악성메일 유무 판단 결과 전달

결과 보고서

- 훈련 상세 보고서 제공 (훈련 결과에 대한 통계값 및 RAW 데이터)
- 훈련 결과보고서 제공 (훈련의 개요, 수행 절차, 훈련 결과 등)

정보보안교육

보안강화 교육

- 임직원들의 보안 인식 강화 및 발생 가능성이 있는 위협을 먼저 제시하고 대응 방안 제공
- 교육의 수준은 전반적인 보안 인식에 대한 교육이 필요한 상황과 악성 메일 훈련 결과를 토대로 심층적 교육이 필요한 상황을 구분해 보안 교육 서비스 제공

특화 교육

- 대상을 특정한 표적 공격에 대응하는 전문적인 보안교육은 물론 특정 인원 혹은 직무자들만을 위한 심층적인 보안교육 필요
- 나날이 발전하는 공격의 다양성에 대응하는 맞춤형 보안교육과 더불어 심도 있는 교육이 필요한 곳에 전문적인 보안교육 제공

체크리스트

구분	세부내용	단위	수량	비고
인프라 진단	서버(UNIX)	EA		
	서버(Windows)	EA		
	네트워크 (스위치, 라우터)	EA		
	정보보호시스템 (방화벽 등)	EA		
	Database	EA		
	WEB/WAS	EA		
모의해킹	내부 URL	URL		
	외부 URL	URL		
모의훈련	악성메일 모의훈련	사용자		
		횟수		
	신고센터	사용자		
	보고서	종류		
교육	보안강화 교육	횟수		
	특화 교육	횟수		