안전한 어플리케이션 보안을 위한 Consulting

02-861-6373 / bc@boancloud.co.kr

정보보호컨설팅전문기업 보안클라우드

보안클라우드
(08503) 서울특별시 금천구 가산디지털1로 181, 1508호(가산동, 가산W센터)
181, GasanDigital 1-ro, GumCheon-gu, Seoul, Republic of Korea
https://www.boancloud.co.kr

회사 소개

㈜보안클라우드는 정보보호 분야에서 최고의 전문성을 갖춘 인재들로 구성되어 있으며, 고객의 다양한 보안 요구에 맞춘 최상의 서비스를 제공합니다.
당사는 정보 보안 컨설팅, 시큐어 코딩 컨설팅 및 보안 취약점 진단을 핵심 사업으로 삼고 있으며, 최신 보안 위협에 대응하는 전문적인 솔루션을 제공합니다.

회사개요

- 회 사 명 : ㈜보안클라우드(BOANCLOUD Inc.)
- 대표이사 : 고 공 석
- 설립일자 : 2015년 3월 25일
- 사업분야 : 정보호호컨설팅, SW개발, 보안솔루션 공급, 정보보호 교육
- 주 소 : 서울특별시 금천구 가산디지털1로 181, 1508호(가산동, 가산더블유센터)
- 연 락 처 : TEL : 02)861-6373, FAX : 070)4275-5163
- 홈페이지 : https://boancloud.co.kr

Consulting 사업 분야

1. 소스코드 보안약점 진단 : 안전한 소프트웨어 개발보안

산업 소프트웨어 공학에서 안전한 코딩 지침의 중요성은 소프트웨어 개발자가 코드의 약점을 인식하고 회피하며, 이를 지원하는 조직적 체계와 연결됩니다.
정보보안은 현대 기업의 핵심 과제로, 소스코드 보안약점 진단 서비스를 통해 안전한 디지털 환경을 제공합니다. 이 서비스는 공공기관 지침에 따라 보안약점을 진단하고 실행 가능한 개선방안을 제시합니다.

2. 모의해킹 컨설팅: 디지털 보안을 강화하는 전략적 접근

디지털 전환은 기업에 기회를 제공하지만 사이버 위협도 증가시킵니다.
당사의 모의해킹 컨설팅은 해커의 공격 기법을 모방해 IT 시스템을 진단하고 보안 취약점을 해결할 구체적인 조치를 제공합니다.

3. 웹 취약점 진단 컨설팅: 자동화 도구를 활용한 분석

웹 취약점 진단은 보안의 첫 단계로, 자동화 도구를 통해 다양한 취약점을 신속히 탐지하고 효율적으로 대응할 수 있습니다.
DAST와 같은 고급 보안 도구를 활용해 조직의 보안을 강화하고 복잡한 문제 해결을 위한 실행 가능한 정보를 제공합니다.

4. 해킹 메일 모의훈련 : 실전 감각을 키우는 사이버 보안 훈련

최근 사이버 공격의 주요 수단 중 하나로 자리 잡은 해킹 이메일은 기업 정보 유출 및 시스템 마비를 초래하는 주요 위협 요소입니다.
이를 사전에 예방하고 임직원들의 보안 대응 역량을 강화하기 위하여 의심스러운 이메일을 식별하고 적절히 대응할 수 있는 능력을 배양하는 데 지원합니다.

1. 소스코드 보안약점 진단 : 안전한 소프트웨어 개발보안

산업 소프트웨어 공학에서 안전한 코딩 지침의 중요성은 소프트웨어 개발자가 코드의 약점을 인식하고 회피하며, 이를 지원하는 조직적 체계와 연결됩니다. 정보보안은 현대 기업의 핵심 과제로, 소스코드 보안약점 진단 서비스를 통해 안전한 디지털 환경을 제공합니다. 이 서비스는 공공기관 지침에 따라 보안약점을 진단하고 실행 가능한 개선방안을 제시합니다.

서비스 소개 : 시큐어코딩 진단

단순히 보안 취약점을 식별하는 것을 넘어 현실적으로 실행 가능한 수준의 개선방안을 제공합니다

1 보안약점 진단도구 : CODE-RAY XG V6.0 R2

CODE-RAY XG V6.0 R2는 고급 분석 기능을 통해 소스코드 보안 취약점을 정밀 탐지·분석합니다. 이 도구는 감리법인이 사용하는 최고 수준의 기술로, 소프트웨어 개발 및 유지보수 과정의 보안 위험을 최소화합니다.

2 진단인력 : 소프트웨어 보안약점 진단원

소프트웨어 보안약점 진단원은 전문성과 최신 보안 지식을 바탕으로 소스코드를 분석하고, 프로젝트 특성에 맞춘 진단과 개선 작업을 수행합니다.

3 보안약점 기준 진단

신규 또는 유지보수로 변경된 소스코드는 행정안전부에서 제시한 49개의 보안약점 기준에 따라 철저히 진단됩니다. 이를 통해 귀하의 시스템이 최신 보안 기준에 부합하도록 보장하며, 잠재적인 보안 취약점을 사전에 예방하여 안정적인 운영 환경을 제공합니다.

소스코드 보안약점 진단 절차

Step1. 사전환경조사
- 점검 기준 및 분석 대상 협의
- 진단 시스템 환경 파악

Step2. 취약점 진단 및 조치
- 점검 기준에 따른 소스코드 분석 후 결과 진단
- 취약점 통계 자료 및 보고서 제공

Step3. 취약점 이행 점검
- 동일한 기준에 따라 소스코드 2차 분석 이후 결과 진단
- 수정 가이드 제공

Step4. 잔여취약점 보완
- 최종 진단 결과 리뷰 및 잔여 취약점 보완 조치

소스코드 보안약점 진단 서비스의 차별성

1 전문성

소프트웨어보안약점 진단원을 활용하여 보안약점 진단 분야에서 수 년간의 경험과 전문 지식을 토대로 컨설팅을 진행합니다

2 신뢰성

CC인증 보안약점 진단도구 및 국내외 Compliance를 준수하여 컨설팅 서비스의 신뢰성을 보장합니다.

3 맞춤형 해결책

각 고객의 독특한 필요와 요구사항에 맞춘 맞춤형 보안 솔루션을 제공합니다.

2. 모의해킹 컨설팅: 디지털 보안을 강화하는 전략적 접근

서비스 소개 : 모의해킹 컨설팅

디지털 전환은 기업에 기회를 제공하지만 사이버 위협도 증가시킵니다. 당사의 모의해킹 컨설팅은 해커의 공격 기법을 모방해 IT 시스템을 진단하고 보안 취약점을 해결할 구체적인 조치를 제공합니다.

실제 해킹 시나리오 시뮬레이션

전문 해커가 사용하는 다양한 공격 기법을 활용하여, 실제와 같은 해킹 시도를 모의합니다. 이를 통해 기업은 자신들의 보안 시스템이 실제 공격에 어떻게 대응할 수 있는지를 평가할 수 있습니다.

종합적인 취약점 분석

자동화된 도구만으로는 발견하기 어려운 복잡하고 창의적인 보안 취약점까지 식별합니다. 이 과정은 OWASP TOP 10과 같은 잘 알려진 컴플라이언스 기준에 기반하여 수행됩니다.

맞춤형 보안 솔루션

발견된 취약점에 기반하여, 귀사의 IT 환경과 비즈니스 요구에 맞춤화된 보안 강화 방안을 제공합니다.

모의해킹 진행 절차

Step1. 사전환경조사	Step2. 점검사항논의	Step3. 서버 침투 테스트	Step4. 취약점 결과 분석	Step5. 대응방안 수립
• 고객과의 긴밀한 협의를 통해 IT 환경 파악 • 정보 수집 및 위협 모델링	• 점검 방법, 대상, 기간 등에 대한 상세한 계획 수립	• 해커가 진행하는 방식과 동일하게 모의해킹 수행	• 모의 공격을 통해 발견된 취약점 분석 • 침투 결과 증적 확보 • 검출결과 리뷰 및 가이드 제공	• 취약점을 해결하기 위한 맞춤형 대응 방안 마련 • 결과 보고서 제공 및 후속 기술 지원

모의해킹 서비스의 차별성

단순한 보안 점검을 넘어서 귀사의 사이버 보안 체계를 종합적으로 강화하고, 지속 가능한 발전을 위한 신뢰할 수 있는 파트너임의 보장합니다.

1 웹 어플리케이션 심층 분석 및 가이드 제공

모의해킹 결과에 대한 정확한 분석을 위해 소스코드 보안약점 진단원을 활용하여 귀사의 소프트웨어 소스코드 내 잠재적인 보안 취약점을 식별합니다. 이를 통해 발견된 보안 이슈에 대해 정확하고 실행 가능한 가이드를 제공함으로써, 사이트에 최적화된 이행 조치 방안을 제시합니다.

2 풍부한 실무 경험

당사는 10여 년간 공공, 금융 등 다양한 사업 분야에서 모의해킹 사업을 수행해 온 깊은 경험을 보유하고 있습니다. 이러한 경험은 다양한 산업군의 특성과 요구사항을 이해하고, 맞춤형 보안 솔루션을 제공하는 데 핵심적인 역할을 합니다.

3 신뢰성 있는 컴플라이언스 준수

당사는 자체 시나리오 기반의 모의해킹뿐만 아니라, 주요 통신 기반시설의 기술적 취약점 분석 및 평가 기준, 그리고 OWASP TOP 10 등 국내외에서 인정하는 알려진 컴플라이언스를 준수합니다.
이는 당사의 서비스가 최고의 보안 표준과 법적 요구사항을 충족시키며, 고객에게 최상의 보안 환경을 제공한다는 것을 의미합니다.

3. 웹 취약점 진단 컨설팅: 자동화 도구를 활용한 취약점 분석

웹 취약점 진단은 보안의 첫 단계로, 자동화 도구를 통해 다양한 취약점을 신속히 탐지하고 효율적으로 대응할 수 있습니다. DAST와 같은 고급 보안 도구를 활용해 조직의 보안을 강화하고 복잡한 문제 해결을 위한 실행 가능한 정보를 제공합니다.

DAST를 활용한 첨단 웹 애플리케이션 보안 분석

DAST

- 웹 애플리케이션의 URL을 자동 수집하고 실행 중인 애플리케이션의 취약점을 분석하는 실시간 보안 검사 기법

보안 취약점

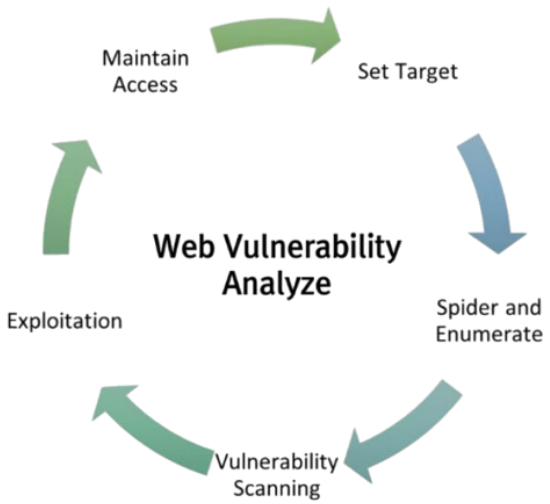
- 공격 방식을 모방해 실제 시나리오에서 발생할 수 있는 취약점을 식별하고 수정하도록 지원

위협 탐지

- SQL 인젝션, XSS, 인증 취약점 등 다양한 보안 이슈를 탐지

기대효과

- DAST는 보안을 강화하고 개발 주기를 단축하며 보안 위험을 최소화하는 데 필수



심층적 보안 분석 및 맞춤형 해결책

우리는 DAST와 같은 도구를 활용하여 심층적인 보안 분석을 제공합니다. 이를 통해 고객의 특정 요구사항, 기술 스택, 그리고 위협 환경을 깊이 이해하고, 맞춤형 보안 해결책을 제공함으로써 각 조직이 사이버 위협에 효과적으로 대응할 수 있도록 지원합니다.

Step1. 사전환경조사

- 점검 대상 선정 및 사전 협의
- 정보 수집 및 위협 모델링
- 수집 정보 분석 및 사전 진단

Step2. 진단 실시

- 자동 진단 도구를 이용한 취약점 진단 수행
- 취약점을 이용한 시스템 침투

Step3. 취약점 진단 결과 리뷰

- 취약점 결과 분석 및 가이드
- 취약점 결과 증적 확보
- 검출 결과 리뷰 및 가이드

Step4. 결과 보고

- 최종 보고서 작성 및 기술 지원
- 결과 보고서 제공 및 후속 기술 지원

지속적인 교육과 지원

지속적인 교/육

- 최신 보안 동향, 도구, 기법에 대한 교육 제공.
- 보안 사고 사례 공유 및 분석.
- 사이버 위협 탐지 및 대응 훈련.

지속적인 지/원

- 고객이 자신의 보안 프로토콜을 지속적으로 강화할 수 있도록 지원.
- 취약점 진단 자동화 도구와 맞춤형 컨설팅을 통해 조직의 보안 요구 충족.

4. 해킹 메일 훈련 : 실전 감각을 키우는 사이버 보안 훈련

서비스 소개

최근 사이버 공격의 주요 수단 중 하나로 자리 잡은 해킹 이메일은 기업 정보 유출 및 시스템 마비를 초래하는 주요 위협 요소입니다. 이를 사전에 예방하고 임직원들의 보안 대응 역량을 강화하기 위하여 의심스러운 이메일을 식별하고 적절히 대응할 수 있는 능력을 배양하는 데 지원합니다.

해킹 메일 훈련의 기대효과

사고 예방 01
- 해킹메일로 인한 데이터 유출, 랜섬웨어 감염 등 주요 보안 사고를 사전 차단
- 임직원들의 실수를 줄여 보안 사고 발생률 감소

조직 문화 강화 02
- 임직원 개개인의 해킹메일 식별 능력이 향상되어 사이버 보안에 대한 실질적인 대응 역량 향상
- 보안 위협 상황에서 효과적으로 대처 가능

신뢰성 03
- 보안 수준이 강화됨에 따라 고객 및 파트너와의 신뢰도를 높이고, 조직의 평판을 유지

비용 절감 04
- 보안 사고로 인한 복구 비용과 운영 중단으로 발생하는 손실을 예방하여 장기적으로 비용 효율적인 보안 환경 구축

해킹 메일 훈련 서비스 절차

Step1. 사전환경조사	Step2. 해킹 메일 훈련	Step3. 반응 모니터링	Step4. 결과 분석 및 보고	Step5. 교육 및 피드백
• 고객과의 긴밀한 협의를 통해 IT 환경 파악 및 요구사항 파악 • 시나리오 설계 및 훈련 범위 파악	• 설계된 시나리오에 따라 해킹 이메일 발송 • 시나리오별, 부서별, 인원별 사전 협의된 방식으로 메일 발송	• 임직원들의 반응 모니터링 • 이메일 열람, 링크 클릭, 첨부파일 다운로드 등 추적	• 훈련 결과 분석 및 결과 보고서 제공 • 취약 부서 및 인원 분석 • 훈련 결과 데이터 수집 후 보고서 제공	• 분석 결과를 바탕으로 교육 및 피드백 제공 • 분석 결과 맞춤형 교육 • 보안 인식 개선 교육 실시

서비스의 차별성

단순한 교육을 넘어서, 해킹 메일 모의훈련을 통해 귀사의 사이버 보안 대응 역량을 종합적으로 강화하고, 지속 가능한 보안 체계 구축을 위한 신뢰할 수 있는 파트너임을 보장합니다.

1 맞춤형 해킹 시나리오 설계

최신 해킹 트렌드를 분석하여 기업 환경에 적합한 시나리오를 제공합니다. 스피어피싱, 악성 첨부파일, 의심스러운 링크 등 다양한 유형의 해킹 이메일을 시뮬레이션하여 실제 상황과 유사한 환경에서 훈련이 이루어집니다.

2 실시간 모니터링 및 상세 분석

모의훈련 중 임직원들의 모든 행동은 실시간으로 세밀하게 모니터링됩니다. 이메일 열람, 링크 클릭, 첨부파일 실행 등 사용자의 반응을 즉각적으로 추적하여 정확한 데이터를 수집합니다. 이렇게 수집된 데이터를 바탕으로 조직의 보안 취약점을 심층적으로 분석하며, 개인별 및 부서별로 상세한 보고서를 제공합니다.

3 보안 인식 강화 교육 연계

모의훈련이 끝난 후에는 각 상황에 따른 올바른 대응 방법에 대한 맞춤형 교육을 제공합니다. 단순히 위험을 인지하는 것에 그치지 않고, 실제 해킹 시도에 대해 어떻게 대처해야 하는지 구체적 가이드라인 제공합니다.

5. CSAP SaaS 보안인증 컨설팅 : 클라우드 보안인증 대비

클라우드 컴퓨팅 시대에 보안 인증의 중요성은 서비스 제공자가 데이터 보호와 시스템 안전성을 보장하며, 이를 지원하는 체계적 접근과 밀접하게 연결됩니다. 정보보안은 현대 기업과 공공기관의 필수 과제로, CSAP SaaS 보안인증 컨설팅은 안전하고 신뢰할 수 있는 클라우드 서비스를 구축하도록 지원합니다.

공공기관 서비스 제공을 위한 CSAP 인증

복잡한 인증 절차를 효율적으로 지원

- 전문가의 경험과 노하우
- 인증 획득 시간 단축
- 정부 규제 및 법적 요건 준수

맞춤형 보안 정책 설계 및 문서화 지원

- 고객사의 환경에 맞는 보안 정책과 절차를 설계하고, CSAP 인증 요건을 충족하는 문서를 작성
- 주요 정책 및 지침, 취약점 점검 보고서 등 필수 문서 작성
- 공공기관 표준 문서 양식에 대한 검토 및 피드백 제공

실무 중심의 취약점 점검 및 개선 지원

- 인증 평가에 필요한 CCE, CVE 기반 취약점 점검, 소스코드 분석, 모의침투 테스트를 수행.
- 취약점 발견 시, 이를 해결하기 위한 기술적 개선 방안을 제시하고 실행 과정을 지원
- 인증 평가에서 요구되는 이행 여부 점검 및 검증

CSAP SaaS 컨설팅 서비스 절차

사전환경 파악	인증 문서 작성 지원	취약점 진단	평가 결과 지원
• 보안 정책, 네트워크 구성, 데이터 보호 체계 등 주요 요소를 평가하여 개선 방향을 제시	• CSAP 인증 요건에 맞는 정책, 절차, 보고서 등 필수 문서를 작성	• CCE 및 CVE 기반 취약점 점검, 소스코드 분석, 모의침투 테스트 등을 수행	• 인증 평가 과정에서 발생하는 보완 요구사항에 대해 신속히 대응할 수 있도록 지원

CSAP SaaS 컨설팅 상세 제공 내역

1 CSAP 제도 안내 및 인증 문서 작성 지원

클라우드 보안 인증 제도(CSAP)에 대한 명확한 이해를 제공하며, 인증 프로세스에서 요구되는 다양한 문서를 체계적으로 작성하도록 지원합니다. 이를 통해 고객이 인증 절차를 원활하게 진행할 수 있도록 도움을 드립니다.

2 CCE, CVE, 소스코드 진단 등 사전 취약점 점검 지원

국제적으로 공인된 취약점 데이터베이스(CCE, CVE)를 기반으로 시스템의 보안 취약점을 철저히 점검합니다. 또한 소스코드의 안전성을 진단하고 모의침투 테스트를 통해 실질적인 보안 강화를 돕습니다.

3 CSAP SaaS 보안인증 문의 응대

인증 준비 과정에서 발생하는 모든 문의 사항에 대해 전문가의 조언을 제공하며, 인증 성공률을 높이기 위한 최적의 가이드를 제시합니다.

정책 수립부터 기술적 솔루션까지 종합적인 지원을 제공하여 고객의 CSAP 인증 획득 시간을 단축시킬 수 있습니다.

㈜보안클라우드는 중앙행정기관 및 공사/공단과 사기업 등 기타 다양한 기관을 대상으로 보안 기술 지원을 제공하며, 소스코드 보안약점 진단, 모의해킹, 유지보수 등 다양한 서비스를 통해 신뢰받는 파트너로 자리 잡고 있습니다. 특히, 소스코드 보안약점 진단도구(CODE-RAY XG)를 활용한 진단과 맞춤형 기술 지원을 통해 고객의 보안 수준을 효과적으로 강화하고 있습니다.

대표 고객사

KRA 한국마사회
BMW Financial Services
검찰 PROSECUTION SERVICE
경기도
인천교통공사
ksure 한국무역보험공사
건강보험심사평가원
삼성SDS
한전KPS
한국고용정보원 Korea Employment Information Service
행정안전부 국가정보자원관리원
KEIT 한국산업기술기획평가원
KSPO 국민체육진흥공단
SK magic
국가인권위원회
INU 인천대학교
KISA 한국인터넷진흥원
경기도환경교육센터
kotra 대한무역투자진흥공사
성균관대학교
국토교통부 항공교통본부
KAC 한국공항공사
부천대학교 BUCHEON UNIVERSITY
한국행정연구원 Korea Institute of Public Administration
경찰청
서울특별시 SEOUL METROPOLITAN GOVERNMENT