



|주|트|리|니|티|소|프|트 www.trinitysoft.co.kr
 경기 안양시 동안구 학의로282 금강펜테리움IT타워 A동 902호
 TEL 1644-3055 FAX 031)463-3055



- 중소기업청 벤처기업확인 (연구개발기업:기술보증기금)
- 중소기업청 기술혁신형 중소기업(INNO-BIZ) 확인
- 중소기업청 성능인증 확인
- 기업부설연구소 인정 (한국산업기술진흥협회)
- 특허청 웹 보안 핵심기술 보유
 - 웹 서버의 보안장치
 - 웹 보안방법 및 그 장치
 - 네트워크 기반의 게시물 검증방법 및 그 장치
 - 웹 서버 업로드 파일의 검증방법 및 그 장치
 - 웹방화벽에서의 White-URL 수집방법 및 White-URL수집기능이 구비된 웹방화벽
 - 역추적을 이용한 소스코드 취약점 분석방법 및 장치
 - 검색엔진을 이용한 웹서버 취약점 점검 시스템 및 방법
 - 웹 응용프로그램의 취약점 분석 장치 및 방법
 - 프락시 서버에서의 악성 자바 애플릿 탐지 방법
 - 방화벽을 이용한 악성코드 유포사이트 관리 방법,장치 및 시스템
- 중소기업청 '벤처코리아' 벤처기업 부문 대상 수상
- 정보통신부 '대한민국SW대상' 장관상 수상
- 지식경제부 '신기술실용화 촉진대회' 장관상 수상
- 미래창조과학부 '정보보호 산업발전' 장관상 수상
- 중소기업청 '벤처활성화' 중소기업청장상 수상
- 행정자치부 '정보보호 유공' 국무총리 표창
- 미래창조과학부 'K-Globa300' 시큐어코딩 교육과정 콘텐츠 개발 및 운영사업 부문 선정기업



교육·컨설팅

Education & Consulting



회사 소개

Introduction of Trinitysoft

(주)트리니티소프트는 웹 애플리케이션 계층의 해킹 시도로부터 기업의 전산시스템을 안전하게 보호하고자, 다음의 솔루션을 개발하였습니다.

▶ **Webs-Ray™** 웹 애플리케이션 방화벽 'Webs-Ray (웹스레이)' 는 실시간으로 웹 해킹을 탐지하고 정보유출 차단기능을 제공합니다.

▶ **CODE-RAY XG** 웹 소스코드 보안약점 분석솔루션 'CODE-RAY XG (코드레이 엑스지)' 는 개발된 웹 소스가 배포되기 전 단계에서부터 해킹에 취약할 수 있는 부분을 탐지합니다. 본서에는 이 제품을 위주로 한 교육 컨설팅 내용이 소개되어 있습니다.

- 개발단계(SDLC)에서부터 소스코드의 허점, 오류, 에러가 없는 건강한 소프트웨어를 구현하는데 도움을 주는 시큐어코딩 솔루션입니다. 소프트웨어 분석 및 설계, 개발구현, 테스트, 운영 등 각 단계에서 발생할 수 있는 보안약점을 관리하기 위해 단계별로 *소스코드 통합보안관리 기능을 제공합니다.
*소스코드 배포관리 / 리비전 관리 / 소스코드 백업 및 복구 / 소스코드 취약점 분석 / 소스코드 변조탐지 및 복구 / 개발자 업무통제 / 형상관리
- OWASP TOP10, CWE/SANS TOP25, 행정자치부 47개 보안약점, 국정원 홈페이지 8대취약점, 전자금융감독규정 등에서 정의한 가이드라인을 기초로 보안약점을 분석/관리합니다.
- IT보안인증사무국으로부터 [취약성 점검도구]부문과 [소스코드 보안약점 분석도구]부문에서 각각 CC(국내공통평가기준) 인증을 획득하였습니다. 또한 TTA 한국통신기술협회로부터 GS품질 인증을, 특허청으로부터 2종의 기술특허를 획득하였습니다.
- 미래창조과학부로부터 시큐어코딩 과정 교육콘텐츠 개발 및 운영사업 부문에서 K-Global 300기업으로 선정되었습니다.
- KISA(한국인터넷진흥원)의 시큐어코딩 과정 교육콘텐츠 개발 및 운영사업 공급자로 선정, 1년간 성공리에 완료하였습니다.

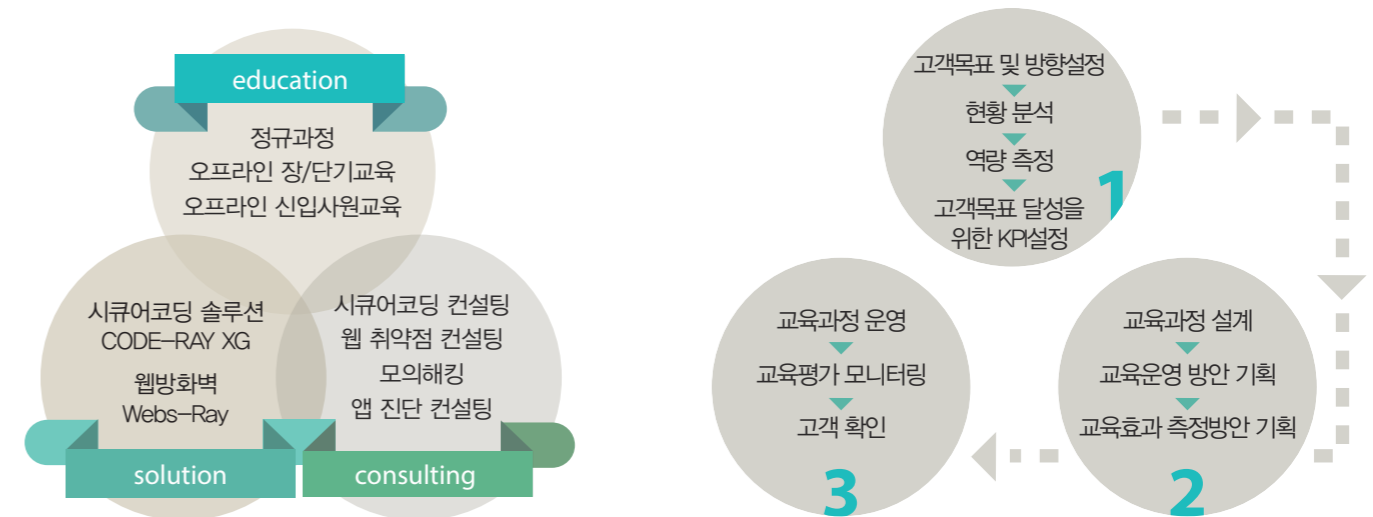


교육 소개

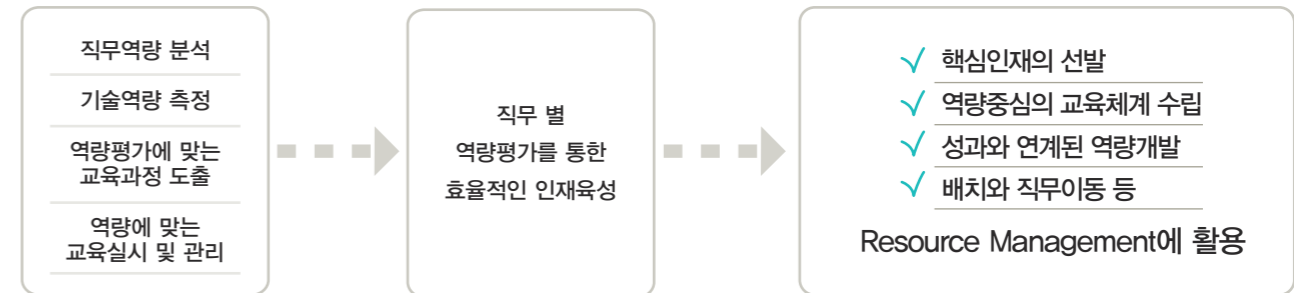
Introduction of EDU

▶ 특징점

- 자사의 솔루션을 활용한 컨설팅과 연계되어 있습니다. 축적되어 온 개발경험과 현장 노하우를 통하여 사전지식만을 전달하는 단순교육을 탈피, 실무 맞춤형 교육서비스를 지향합니다.
- 교육분석설계 - 교육개발 - 교육관리 에 이르는 3단계 운영프로세스를 바탕으로, 전문강사진이 직접 강의합니다.



▶ 목적

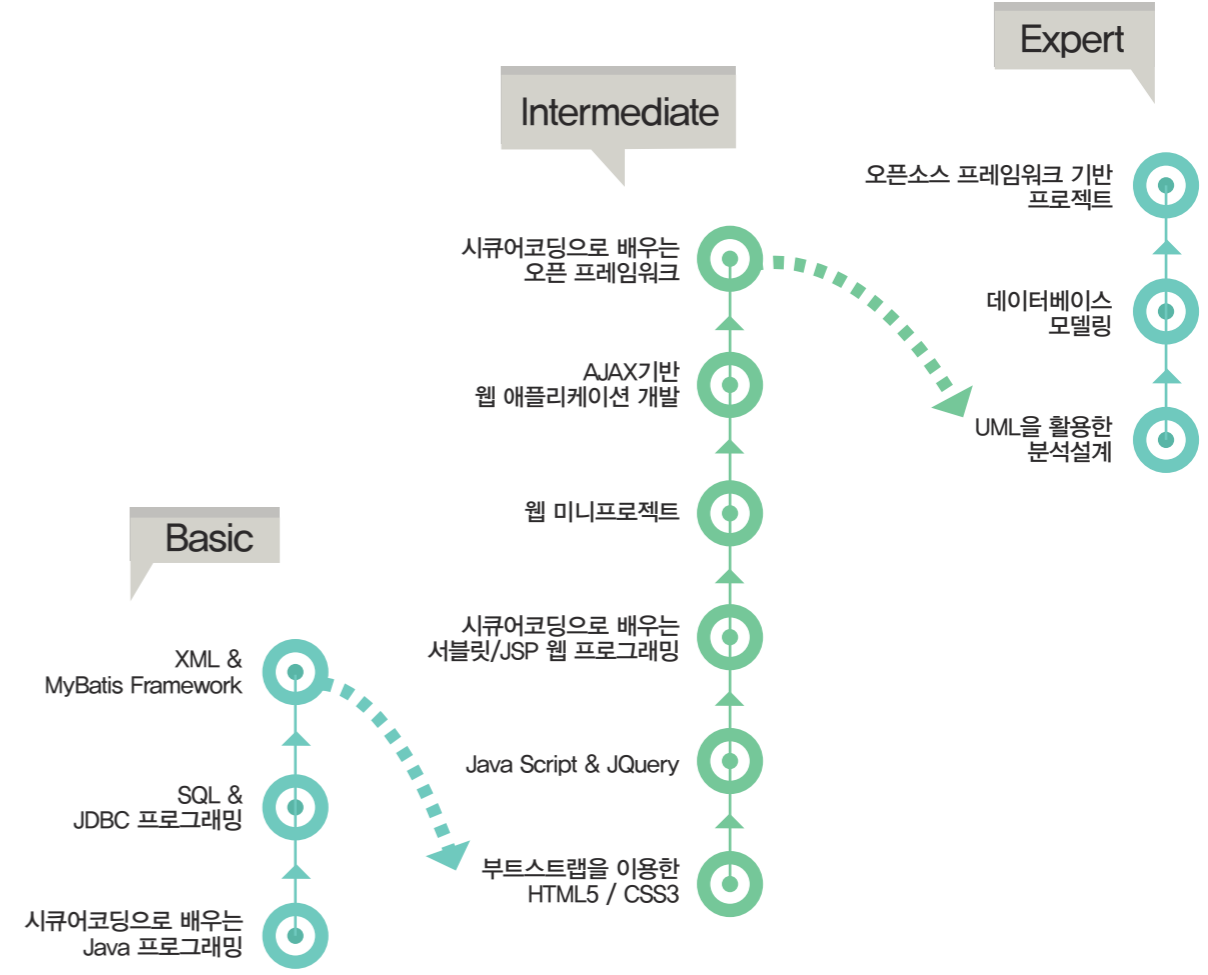


교육_오프라인 프로그램

• 단기교육 목록

	Mobile	Web UI	Web Application	Architect/PM	보안
Expert	안드로이드 앱 성능향상 안드로이드 앱 보안	웹 기획	웹 서비스 JavaEE Refactoring JavaEE Clean Code	EA(Enterprise Architecture) 소프트웨어 아키텍처 PMP	보안컨설팅 ISMS / PIMS 금융보안
Intermediate	모바일 앱 아키텍처 오픈API를 활용한 매쉬업 하이브리드앱 개발	AJAX 활용 Angular JS	자바디자인 패턴 프로그래밍 자바 시큐어코딩 기법 UML을 활용한 객체지향 분석설계	Agile 방법론 CBD 방법론 객체 모델링	웹 모의해킹 C 시큐어코딩 Java 시큐어코딩 네트워크 보안 시스템 보안 안드로이드 앱 취약점 분석
	JQuery Mobile Sencha Touch 안드로이드 앱 프로그래밍 iOS 앱 프로그래밍	HTML5/CSS3 BootStrap jQuery Framework	전자정부 표준 Framework Spring Framework 활용 MyBatis Framework Java Script/jQuery HTML5/CSS3	자바디자인 패턴 UML을 활용한 객체지향 분석설계 시큐어코딩 설계	보안윤리 정보보안 기초 네트워크 개론 정보보안기사
Basic		HTML5/CSS3 Java Script		개발방법론 기술문서 작성기법	
공 통 과 목					
	운영체제 Window Server Linux 자격증: LPIC	프로그래밍 기초 JAVA 프로그래밍 JDBC 프로그래밍 서블릿/JSP 프로그래밍 자격증: OCJP, OCWCD	C 프로그래밍 C++ 프로그래밍 C# 프로그래밍 자료구조 Python 자격증: 정보처리기사	데이터베이스 SQL Oracle DB MySQL DB CUBRID DB 자격증: SQLD, OCP	개발환경 IDE-이클립스 활용 빌드 배포(maven) 형상관리(Subversion, Git) 단위테스트 기초(jUnit) CI (Hudson)

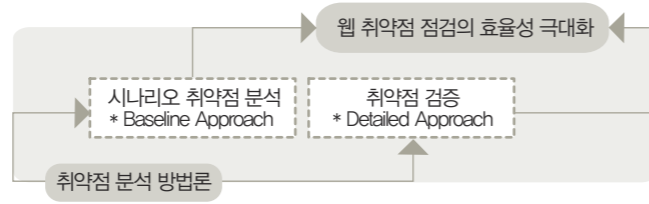
• 신입사원교육 및 장기교육 목록



▶ 특징점

- 고객사의 내부규정과 관련법률의 준수를 목적으로 하는 정보보안 인프라에 적합하도록, 보안약점 점검/분석에서부터 모의해킹까지 고객맞춤형 컨설팅을 제공하고 있습니다.
- 자사의 소스코드 보안약점 분석솔루션 및 기술력을 검증받은 제품을 이용하여, 보안 전문컨설턴트에 의해 진행됩니다.
- 보안약점 분석 산출물의 품질을 높이기 위해 ISO/IEC 1335 TR (GMITS)에서 권고하는 Combine Approach 방법론을 적용하고 있습니다.

- * Baseline Approach
기본 시나리오 수립 및 시나리오 조합을 통한 웹 취약점 분석
- * Detailed Approach
시나리오에서 확인된 취약점을 검증하여 파급효과를 분석



소스코드 보안약점 점검/분석 < 시큐어코딩 컨설팅

시큐어코딩 점검 툴을 이용하여 웹 애플리케이션 소스코드 상에서 발생가능한 보안약점을 확인하고 시작/경로/탐지 라인을 제공하고 있으며, 행정자치부 시큐어코딩 47개 기준 및 OWASP TOP10을 점검기준으로 삼고 있습니다.

웹 취약점 컨설팅 > 툴 진단점검

홈페이지 변조, 악성코드 삽입, 피싱사이트 악용 등 인터넷 침해사고 피해를 웹 취약점 분석 툴을 이용하여 사전에 예방하는 서비스이며, OWASP TOP10을 점검기준으로 삼고 있습니다.

툴 진단점검 및 분석 불가능한 부분의 수동점검 < 모의해킹

웹 보안약점 점검, 소스코드 점검, 컨설턴트에 의한 모의검증의 3단계 점검과정을 거쳐 취약부분에 대한 검증작업을 수행합니다. 내/외부자 관점에서 침투테스트를 시도하여 이로 인해 발생가능한 해킹위험을 예방 및 차단하는 대응책을 제시합니다.

앱 진단 컨설팅 > 모바일 앱 분석 및 보안약점 점검

취약한 앱 보안약점을 전문컨설턴트가 수동으로 메뉴를 접근, 상세하게 수행하는 컨설팅입니다.