

웹 보안 및 취약점 관리를 위한 IBM 서비스형 보안 솔루션 소개

(IBM Application Security on Cloud)



최호식 차장 (hs_choi@kr.ibm.com)
IBM Korea Security Software

Agenda

1. 웹/모바일 애플리케이션 보안의 필요성
2. IBM Application Security on Cloud(ASOC) 소개
3. IBM ASOC 취약점 점검 방법
4. IBM ASOC 마켓플레이스 및 무료체험
5. IBM ASOC Summary

1. 웹/모바일 애플리케이션 보안의 필요성

파이낸셜뉴스

국제



정치 증권/금융 경제 사회 국제 오피니언 라이프 기획·이슈 연예·스포츠 해외토픽

영국항공, 해킹으로 고객 신용카드 결제 정보 유출

파이낸셜뉴스 | 입력 : 2018.09.07 10:53 | 수정 : 2018.09.07 10:53

영국항공(BA)의 홈페이지와 모바일 애플리케이션(앱)이 해킹 당해 신용카드 결제 38만건 관련 정보가 유출됐다고 6일(현지시간) CNBC가 보도했다.

지난달 21일부터 지난 5일까지 해킹됐으며 BA측은 여행 기록이나 여권 관련 정보는 피해가 없다고 밝혔다.

BA는 피해 고객에게 직접 연락을 하고 있으며 자신이 피해를 입었다고 의심될 경우 은행이나 신용카드 업체에 통보할 것을 제안했다.

앨릭스 크루즈 BA 최고경영자(CEO)는 이번 해킹 피해에 대해 깊은 사과를 밝히며 “고객들의 정보 보호를 심각하게 다루고 있다”고 말했다.

jjyoon@fnnews.com 윤재준 기자



(FILE) British Airways aircraft at Heathrow Airport in London, Britain 13 November 2009.EPA/ANDY RAIN <All rights reserved by Yonhap News Agency>

기사 원문: <http://www.fnnews.com/news/201809071049326790>

2. IBM Application Security on Cloud(ASOC) 소개

IBM ASOC는 최근 확산된 수십 개의 공개 보안 취약점을 발견하여 웹 또는 모바일 애플리케이션을 보호할 수 있습니다. 또한 애플리케이션이 프로덕션 환경으로 이동하여 배치되기 전에 애플리케이션의 취약점을 제거할 수 있습니다. 상세한 결과 보고를 통해 애플리케이션 보안 리스크를 효과적으로 해결할 수 있습니다.

1. 인공지능 컴퓨팅을 통해 분석시간을 획기적으로 줄이고, False Positive와 보안상 문제가 되지 않는 결과들을 제거하고, 중복된 취약점을 취합하여 수정 권고안 제시
2. 세계 각국 33개의 보안 연구소를 운영하며 빠른 취약점 업데이트
3. 클라우드 환경에서의 손쉬운 취약성 점검 수행 가능



취약점 식별

개발 라이프사이클의 적절한 단계에서 모바일 애플리케이션을 스캔합니다.



비즈니스 중요도에 따른 우선순위 설정
멀웨어와 기타 보안 위협에 대한 보안 리스크를 확인하여 기업에 중대한 영향을 미칠 문제부터 우선순위를 알려드립니다.



권장사항을 담은 보고서

요약 보고서, 발견된 이슈 리스트 및 이를 해결하기 위한 권장사항을 담은 상세 보고서를 제공합니다.

3. IBM ASOC 취약점 점검 방법 > 안내

애플리케이션 취약점 진단은 모의해킹과 비슷한 방식으로 진행하고 결과 리포트를 제공해 드리는 방식이므로 ,시스템에 영향을 줄 우려가 있습니다. 점검 전 아래 권고 사항을 숙지해주시기 바랍니다.

1

중요한 핵심 데이터베이스는 진단 전에 백업을 해주시기 바랍니다.

2

운영 중인 사이트라면 시스템에 영향을 줄일 수 있도록, 옵션으로 프로덕션 사이트를 선택 바랍니다.

3

진단 시간을 줄이거나 시스템 부하를 줄려면 테스트 범위를 한정해서 사용하시기 바랍니다. (포괄적 진단: O/S, 브라우저, DB 접근 등 모두 포함 옵션)

4

로그인이 필요한 사이트의 진단시, 테스트용 사용자 권한으로 로그인 될 수 있도록 설정 바랍니다.

5

스캔이 오래 걸릴 경우, 스캔을 완료하면 이메일을 통해 공지 받을 수 있도록 설정 바랍니다.

3. IBM ASOC 취약점 점검 방법 > Log-in

IBM ASOC는 IBM AppScan의 클라우드 버전입니다. IBM ASOC는 구매하신 IBM ID로 Log-in하여 취약점 점검을 수행할 수 있습니다.

시작합니다!

취약점 검색 및 위험성 관리
새 IBM Application Security on Cloud 사용

새로운 기능

- Easily identify which of your apps may be at risk due to the recent Apache Struts 2 vulnerability CVE-2018-11776 using either DAST or open source scanning.
- Static Analysis now supports applications written in Python or COBOL, [see full list here](#)
- New versions of our static analysis plug-ins for [Eclipse](#), [IntelliJ IDEA](#), and [Visual Studio](#) are available through their respective marketplaces.
- [Personal scans](#) empower developers to scan non-committed code directly from their IDE without breaking application compliance.
- Produce application regulatory and compliance [reports for GDPR, OWASP, PCI, SANS and HIPAA](#).

[모든 최근 업데이트 보기](#)

Application Security
on Cloud

로그인

새로 작성하시겠습니까? 무료 평가판

문서 포럼 지원 지원 문의 무료 평가판

©2018 IBM Corp. All rights reserved.

Let's talk
Security  

3. IBM ASOC 취약점 점검 방법 > Dashboard

앱 작성 버튼을 통해 스캔하고자 하는 대상의 이름을 부여하고 등록하면, 바로 해당 애플리케이션을 스캔하거나 스캔 완료한 결과 리포트를 다운로드해서 볼 수 있습니다.

Application Security on Cloud

문서 | 포럼 지원 | 지원 문의 | Hyun Chung (IBM KOREA INC.) | 사인아웃

내 애플리케이션

합계

1

테스트되지 않음

1

진행 중

0

완료됨

0

앱 작성

앱 가져오기

?

필터

검색

열 선택

삭제

위험 등급 ↓

이름

새로운 문제

비즈니스 단위

비즈니스 영향

마지막 주석

알 수 없음

Demo test

0

중간

스캔을 시작하시려면 눌러주세요.

First

Previous

1

Next

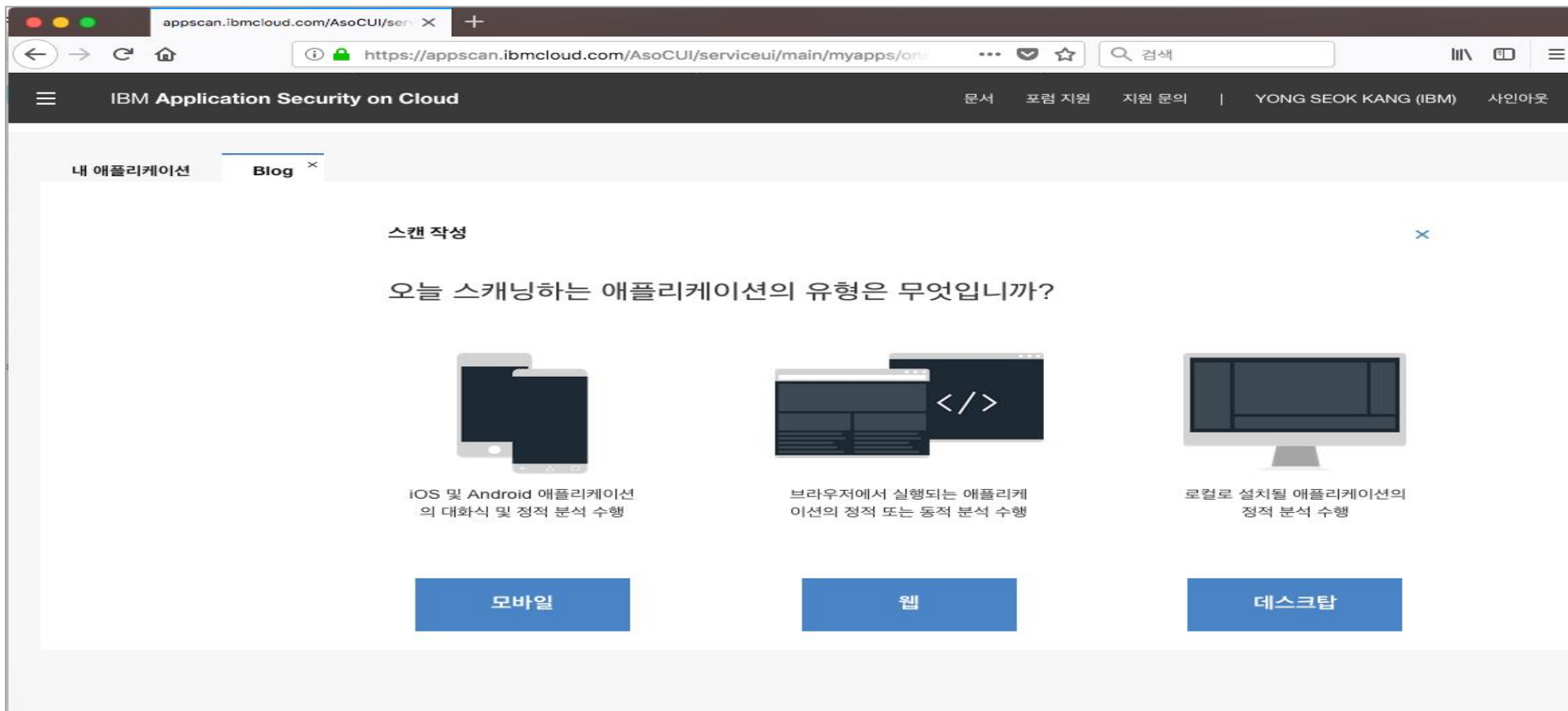
Last

1 중 1 - 1

페이지당 항목 수: 10 15 25 50

3. IBM ASOC 취약점 점검 방법 > Scan options

IBM Application Security on Cloud는 모바일 어플/앱 취약점 분석, 웹 애플리케이션 분석, 혹은 로컬 소스코드 분석 중 선택해서 점검을 할 수 있습니다.



3. IBM ASOC 취약점 점검 방법 > Mobile scan

스캔 대상 앱이 인터넷 공용네트워크망에 위치한 서버와 연결되어 있는지, 사설 네트워크(내부망, 인트라넷)를 사용하여 서버에 연결하여 스캔을 수행할 수 있습니다.

Application Security on Cloud

문서 | 포럼 지원 | 지원 문의 | Hyun Chung (IBM KOREA INC.) | [사인아웃](#)

내 애플리케이션

Demo test ×

스캔 작성

×

← 서버 위치는 어디입니까?



모바일 앱이 인터넷에서 서버와 상호작용합니다.

공용 네트워크



모바일 앱이 인터넷에서 액세스할 수 없는 서버와 상호작용합니다.

사설 네트워크

9

IBM Security



3. IBM ASOC 취약점 점검 방법 > Web scan(1/2)

애플리케이션에 대한 실시간 웹취약점 분석(동적분석)을 진행할지 프로그램 소스코드 분석(정적분석)을 수행할지에 대한 스캔 유형을 선택할 수 있습니다.



3. IBM ASOC 취약점 점검 방법 > Web scan(2/2)

웹 사이트에 대한 불법적인 진단을 방지하기 위해 스캔할 수 있는 권한이 부여되어 있는지 검증이 필요합니다. IBM에서 규정한 간단한 FILE(html 문서)을 해당 사이트의 루트 폴더에 추가함으로써 권한 부여를 인증하거나, Admin 권한을 가진 담당자에게 email을 보내서 담당자가 허가해 주는 방식으로 진단을 할 수 있는 권한인지 확인합니다.

Application Security on Cloud

문서 | 포럼 지원 | 지원 문의 | Hyun Chung (IBM KOREA INC.) | 사인아웃

플리케이션

Demo test

스캔 작성

스캔 유형: Dynamic Analyzer

URL 검증

스캔하기 전에 이 사이트를 스캔할 수 있는 권한이 부여되었는지 검증해야 합니다.

어떻게 검증하시겠습니까?

내 사이트의 루트 폴더에 검증 파일을 추가하겠습니다.

www.ibm.com

다운로드

또는

검증 링크가 있는 이메일 발송:

Admin @ www.ibm.com

이메일 발송

3. IBM ASOC 취약점 점검 방법 > Scanning

Application Security on Cloud

문서 포럼 지원 지원 문의 | Hyun Chung (IBM KOREA INC.) 사인아웃

내 애플리케이션

Demo test

세부사항

중간

위험 등급

118 새로운 문제

118 총 문제

118 규정 미준수 문제

스캔

2

0 완료됨

1 실행 중

0 실패

0 큐에 대기됨

규정 준수

해당 사항 없음

연관된 정책이 없음

애플리케이션 보고서

스캔 작성

보안 보고서

CWE/SANS Top 25 Most Dangerous Errors

EU General Data Protection Regulation

OWASP Top 10 2017

PCI Compliance

US Health Insurance Portability and Accountability Act

스캔 히스토리

문제 관리

정책

필터

검색

demo.testfire.net

이 스캔: 2018. 9. 21. 오전 10:39:31

스캔 진행 중... 실행 중

취소

https://demo.testfire.net?mode=demo

시작하려면 시작 단추를 클릭

3. IBM ASOC 취약점 점검 방법 > Summary(1/2)

스캔 완료시, 어떤 취약점이 있는지 상세 보고서를 통해서 확인 가능합니다.

Application Security on Cloud

문서 포럼 지원 지원 문의 | Hyun Chung (IBM KOREA INC.) 사인아웃

내 애플리케이션

Demo test

세부사항

중간

위험 등급

137

새로운 문제

137

총 문제

137

규정 미준수 문제

스캔

2

1 완료됨

0 실행 중

0 실패

0 큐에 대기됨

규정 준수

해당 사항 없음

연관된 정책이 없음

완료된 스캔결과를 원하는
보고서 형태로 받으세요

애플리케이션 보고서

스캔 작성

보안 보고서

CWE/SANS Top 25 Most Dangerous Errors

EU General Data Protection Regulation (GDPR)

OWASP Top 10 2017

PCI Compliance

US Health Insurance Portability and Accountability...

스캔 히스토리

문제 관리

정책

필터

검색

demo.testfire.net

이 스캔: 2018. 9. 21. 오전 10:39:31

총 문제

102

정보

재실행

다운로드

삭제

공유

또는 아래에서 완료된 스캔
결과를 다운로드 하세요

3. IBM ASOC 취약점 점검 방법 > Summary(2/2)

취약점 문제 관리 탭에서 개별 문제에 대한 상세 내용을 확인할 수 있습니다.

Application Security on Cloud

문서포럼 지원지원 문의 | Hyun Chung (IBM KOREA INC.)사인아웃

내 애플리케이션

Demo test

세부사항

137 새로운 문제
137 총 문제
137 규정 미준수 문제

중간
위험 등급

스캔

2

1 완료됨
0 실행 중
0 실패
0 큐에 대기됨

규정 준수

해당 사항 없음

연관된 정책이 없음

애플리케이션 보고서

스캔 작성

스캔 히스토리

문제 관리

정책

문제 가져오기

필터

검색

열 선택

새로 작성

열림

진행 중

해결됨

무시

패스됨

필터링된 보안 보고서

상태	위치	CVSS	문제 유형	심각도	스캔 이름	마지막 주석
새로 작성	https://demo.testfire.net/bank/login.aspx	9.7	SQL 인젝션	높음	demo.testfire.net	
새로 작성	https://demo.testfire.net/bank/login.aspx	7.5	XSS(Cross-Site Scripting)	높음	demo.testfire.net	
새로 작성	https://demo.testfire.net/bank/login.aspx	9.7	SQL 인젝션	높음	demo.testfire.net	
새로 작성	https://demo.testfire.net/bank/login.aspx	7.5	예측 가능한 로그인 실패	높음	demo.testfire.net	

3. IBM ASOC 취약점 점검 방법 > Presence

내부망에 위치한 애플리케이션을 스캔하기 위해서는 내부망 PC 중에서 인터넷에 접속 가능한 PC에 AppScan Presence 프로그램을 다운로드 받고 압축을 풀어서, startPresence.vbs 또는 startPresence.sh 파일을 실행하시면 스캔을 할 수 있는 환경 구성이 완료됩니다.

Application Security on Cloud

문서 | 포럼 지원 | 지원 문의 | Hyun Chung (IBM KOREA INC.)

내 애플리케이션

Demo test

개인용 사이트 스캐닝

Presence 활성화

✓ Presence 이름 지정

✓ Presence 다운로드

3 Presence 활성화

사이트 네트워크에 Presence 저장 및 스크립트 실행

사이트에서 **AppScan Presence**를 활성화하려면 다음을 수행하십시오.

1) AppScan Presence 파일을 압축 해제하여 사용 중인 사이트와 동일한 네트워크의 컴퓨터에 저장하십시오. 컴퓨터에는 해당 사이트와 인터넷에 대한 액세스 권한이 있어야 합니다.

2) Presence 폴더에서 startPresence.vbs 또는 startPresence.sh를 찾아 실행하십시오.

이전

완료

3. IBM ASOC 취약점 점검 방법 > Manual & Demo



IBM Application Security on Cloud 문서를 시작합니다. 여기서 이 서비스의 설치, 유지보수 및 사용법에 대한 정보를 찾을 수 있습니다.

목차

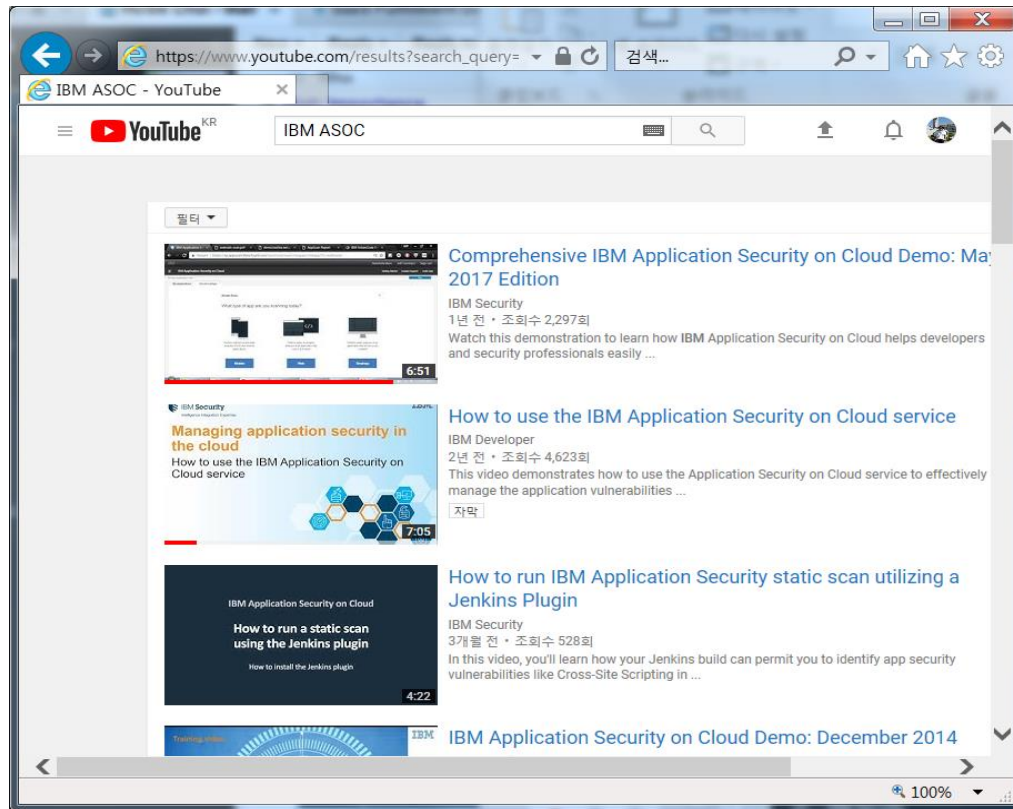
- 시작하기
- 사용자 관리
- 애플리케이션 인벤토리 작성
- 공식으로 위험성 판별
- 앱 취약점 스캔
- 스캔 결과에 대한 작업
- 진행상태 측정
- REST API로 서비스 기능 확장
- 문제점 해결
- 참조

개요

- 최신 업데이트
- 샘플 앱
- 시스템 요구사항 및 브라우저 지원
- REST API 사용
- FAQ
- 데모 비디오
- 자세한 정보

지원 자원

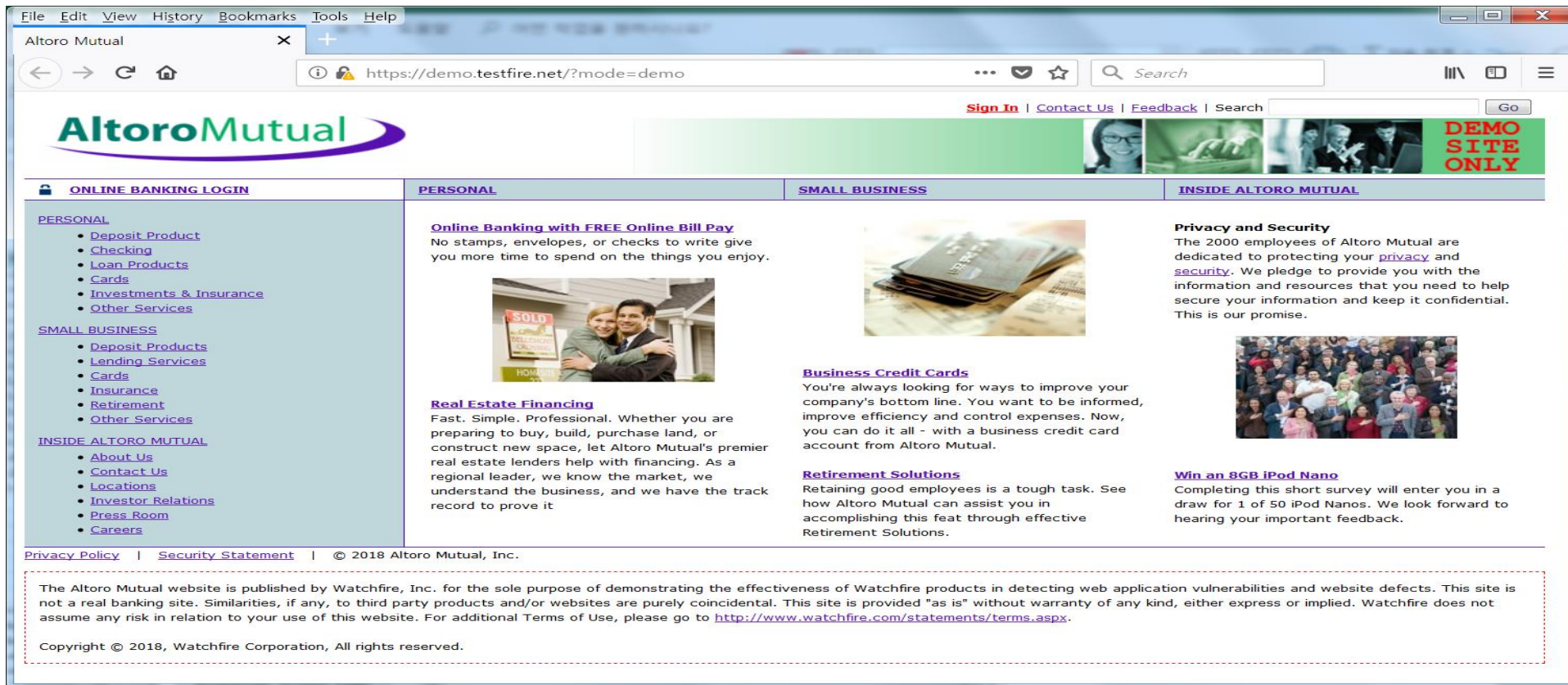
- 서비스 문제점 해결
- developerWorks에 대한 도움말 가져오기
- Mobile Analyzer 지원 포럼
- Dynamic Analyzer 지원 포럼
- Static Analyzer 지원 포럼
- IBM Software Support 홈페이지
- 무료 평가판



https://www.ibm.com/support/knowledgecenter/ko/SSYJJ_F_1.0.0/ApplicationSecurityonCloud/helpindex.html

3. IBM ASOC 취약점 점검 방법 > Demo website

IBM에서 제작한 무료 체험용도의 Demo website를 통해 모의 취약점 점검을 간편하게 테스트 하실 수 있는 ID/PW 포함한 환경을 제공합니다.



4. IBM ASOC 마켓플레이스 및 무료체험(1/3)

The screenshot shows a Google search results page for the query "ibm application security on cloud". The search bar is highlighted with a red rectangle. The results include a link to the IBM Appscan marketplace, a video titled "Managing application security in the cloud", and another video titled "IBM Application Security on Cloud Delegated User Administration".

Google
ibm application security on cloud

전체 이미지 뉴스 동영상 지도 더보기
설정 도구

검색결과 약 39,400,000개 (0.56초)

도움말: 한국어 검색결과만 검색합니다. 환경설정에서 검색 언어를 지정할 수 있습니다.

IBM Application Security on Cloud - 개요 - 대한민국
<https://www.ibm.com/kr-ko/marketplace/application-security-on-cloud>

IBM Appscan의 클라우드 버전으로, 클라우드에서 정적, 동적 및 모바일 ... IBM Application Security on Cloud은 IBM Appscan을 필요한 회수 또는 기간 동안 사용할 ...
이 페이지를 3번 방문했습니다. 최근 방문 날짜: 18. 11. 29

IBM Application Security on Cloud
<https://appscan.ibmcloud.com/>

"I've been absolutely blown away with the level of detail and the recommendations IBM Application Security on Cloud provides. The product has paid for itself ..."

동영상

Comprehensive
How to use the IBM
IBM Application

6:51 7:05 4:24

100%

4. IBM ASOC 마켓플레이스 및 무료체험(2/3)

https://www.ibm.com/kr-ko/marketplace/application-security-on-cloud

IBM Application Security on Cloud

마켓플레이스 ▼ IBM 마켓플레이스 검색

개요 상세 가격 자료

클라우드의 애플리케이션 보안

IBM Application Security on Cloud

IBM Appscan의 클라우드 버전으로, 클라우드에서 정적, 동적 및 모바일 애플리케이션 보안 테스트를 수행하여 앱이나 웹의 런치 전에 보안 취약점을 발견하고 수정할 수 있습니다.

무료 체험 시작하기

가격확인 및 구매하기

웹과 모바일의 보안 취약점, 어떻게 대응하고 계십니까?

IBM Application Security on Cloud은 IBM Appscan을 필요한 회수 또는 기간 동안 사용할 수

상담

100%

4. IBM ASOC 마켓플레이스 및 무료체험(3/3)

무료 체험 Application Security on Cloud를 무료로 이용해 보세요 무료 체험	표준 계획 예측 가능한 비용으로, 구매한 스캔을 세부 취약성 보고와 함께 실행할 수 있습니다. /스캔 (성공적으로 완료된 경우) ₩265,320* 부터 구매하기	전문가 플랜 예측 가능한 비용으로, 구매한 애플리케이션을 세부 취약성 보고와 병렬로 스캔할 수 있습니다. /연간 애플리케이션 단위 ₩6,508,800* 부터 구매하기
알려진 보안 취약성이 있는지 애플리케이션 스캔	알려진 보안 취약성이 있는지 애플리케이션 스캔	알려진 보안 취약성이 있는지 애플리케이션 스캔
30일 동안 체험판 사용 가능	구매한 스캔은 12개월 동안 사용 가능	자동 갱신되는 12개월 구독
스캔은 최대 총 4시간으로 제한됨	시간 제한이 없으며, 스캔이 완료될 때까지 실행됨	시간 제한이 없으며, 스캔이 완료될 때까지 실행됨
최대 5개의 무료 스캔	고객이 선택한 스캔 수	구독을 통해 동일한 앱을 무료로 무제한 스캔 가능
한 번에 최대 1개의 애플리케이션 스캔	병렬로 애플리케이션 스캔 - 구매한 애플리케이션 수로만 제한	병렬로 애플리케이션 스캔 - 구매한 애플리케이션 수로만 제한
수정 작업을 지원하는 요약 보고서	수정 작업을 용이화하는 세부 보고서	수정 작업을 용이화하는 세부 보고서

*표시된 가격은 모든 관련 세금을 제외한 금액입니다.

5. IBM ASOC Summary



전체 해킹 시도 중 70% 이상이
웹을 통해 이루어지고 있습니다

한국인터넷진흥원(KISA)



소스 코드부터 실행까지
클릭 한번에 해결가능한
보안 솔루션

이제 어플리케이션
보안취약점 테스트를
지금 바로 시작해보세요!

Application Security on Cloud

무료 체험판
신청하기

1. 인공지능 컴퓨팅을 통해 분석시간을 획기적으로 줄이고, False Positive와 보안상 문제가 되지 않는 결과들을 제거하고, **중복된 취약점을 취합하여 수정 권고안 제시**
2. 세계 각국 33개의 보안 연구소를 운영하며 **빠른 취약점 업데이트** 기반 취약점 대응 수행
3. 전문가가 아니더라도 **클라우드 환경에서의 손쉬운 취약성 점검** 수행 가능

감사합니다.

IBM Security 솔루션 영업 담당 : 최호식 차장(010-4995-8149, hs_choi@kr.ibm.com)