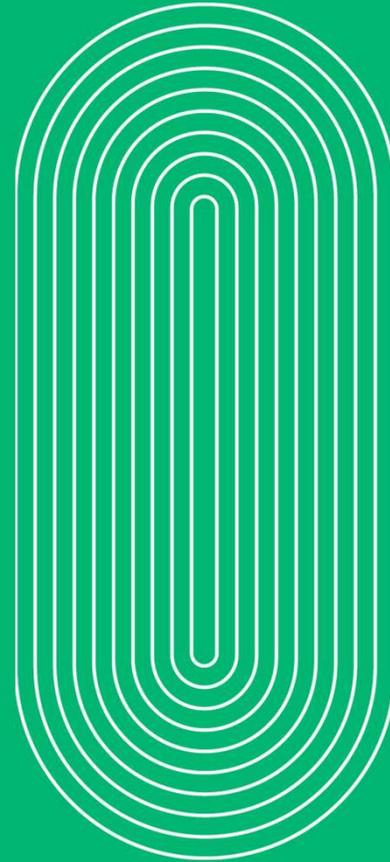


스마트한 취약점 관리 솔루션
알약 내PC 지키미(MPI)



알약 내PC지키미

INDEX

안전하고 효율적인
패치관리 솔루션

01 제안배경

-제안 배경

02 제품소개

-알약 내PC 지키미

-도입 효과

-주요 점검 항목

-주요 기능

-상세 UI

03 고객지원

-이스트시큐리티 대응 센터

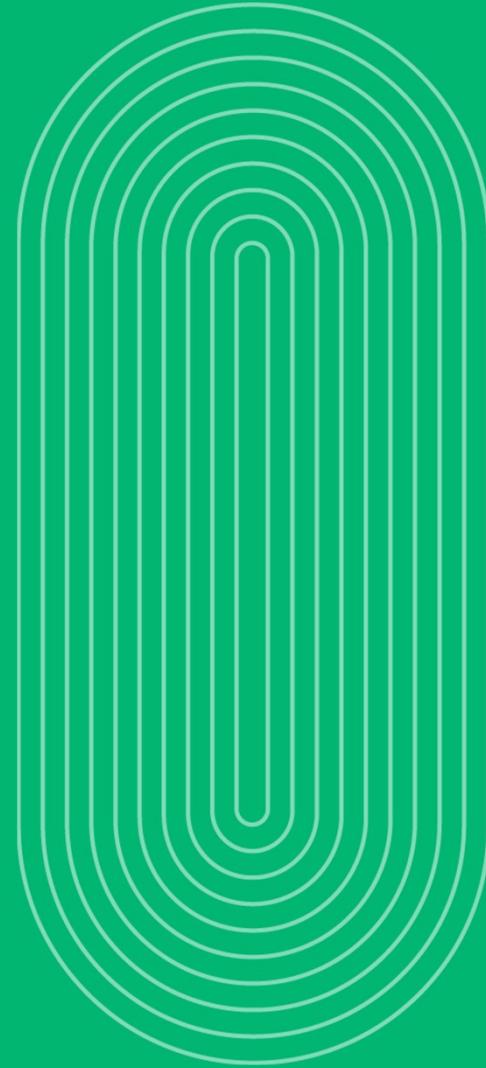
-고객지원 서비스

-구성 및 운용

01

제안 배경

-제안 배경



보안 위협의 많은 비중이 취약점 공격

고도화되는 취약점 공격

- 기업의 업무용 PC에 발생하는 악성코드 공격이 증가, 공격의 대부분은 시스템 및 애플리케이션의 취약점 이용
- 급증하는 엔드포인트 보안 공격에 적절한 대응을 취하지 못하는 기업은 정보유출, 금전적 피해, 시스템 파괴 등의 위협에 그대로 노출

2019년 3분기 사이버 공격 분석



- A사 보안관제서비스 탐지 110만여 건 중 앱취약점 공격 **31%**

- 시스템 취약점 공격 **7%**

■ 웹공격 ■ 앱취약점 공격 ■ 시스템 취약점 공격 ■ 기타

취약점 조치만으로 **사전에 많은 보안 위협을 줄일 수 있습니다**

조치가 필요한 취약점



점검이 필요한 수많은 항목들

사이버 보안 진단의날
ISMS 인증 관련 점검 항목



지속적으로 발표되는 신규 패치

MS 보안 패치
한글, PDF 패치



시간은 부족하고 조치해야 할 항목과 업무용 PC들은 많음

보안 관리자들의 부담

내부 직원들



또 뭘해야해? 귀찮아

일일이 직원들에게 요청하기 너무 힘들어
뭐 할 때마다 사용자들의 문의가 너무 많아



협조가 잘 안되는 직원들

경영진(감사직원)



00월 31일까지 보고 완료

누락된 점검 결과는 없을까?
정해진 시점까지 보안 상태를 안전하게 만들 수 있을까?



기한이 다가오면서 느끼는 불안감

바쁜 관리자들을 위한 솔루션

답답함

불안감

조치가 필요한 수많은 점검 항목들
협조가 잘 안되는 직원들
기한이 다가오면서 느끼는 불안감



여유로움

안정감

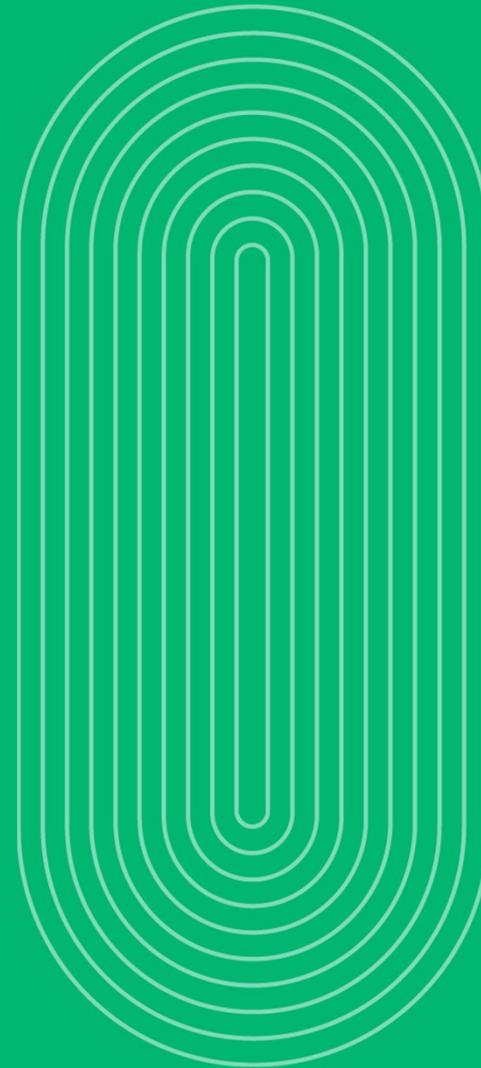
한 번 설정으로 간편하게 자동조치
자동화된 조치 유도과 명확한 안내를 통한
확실한 조치누락없는 점검 결과

바쁜 관리자들이 **자동화된 조치**를 통해
여유롭고 안정적으로 점검이 필요한 취약점을 관리할 수 있습니다

02

제품 소개

- 알약 내PC 지키미
- 도입 효과
- 주요 점검 항목
- 주요 기능
- 상세 UI



알약 내PC 지키미(MyPCInspector)

바쁜 관리자들이 자동화된 조치를 통해 여유롭고 안정적으로 점검이 필요한 취약점을 관리할 수 있습니다



- 자동조치 정책으로 사용자가 조치하지 않아도 자동으로 점검과 조치를 한 번에 진행
- 자동 조치가 불가능한 항목에 대해서는 사용자의 네트워크를 차단하여 조치 유도
- 일괄조치 및 상세한 수동 조치 안내를 통해 관리자에게 문의하지 않아도 스스로 PC 관리 가능



- 누락 점검결과 방지를 통해서 안정적인 점검 환경 제공
- 한눈에 파악 가능한 취약점 현황과 점검 결과를 통해 사용자 관리 가능
- 점검 결과에 따른 보안 점수와 PC상태 확인
- 사이버 보안 진단의 날, ISMS 인증 등 다양한 컴플라이언스 점검 항목 지원



- 알약 제품군 도입 시 별도 서버 구축 없이 라이선스 구매만으로 사용 가능한 시스템 구축 편의성 제공
- 통합 관리 솔루션 ASM5 연동을 통해 백신, 자산, 취약점 등 보안 기능 통합 관리
- 취약점 현황에 대해 빠른 파악이 가능한 시각화된 대시보드 및 보고서 제공

도입 효과

정책 한 번 설정으로 취약 항목 자동조치

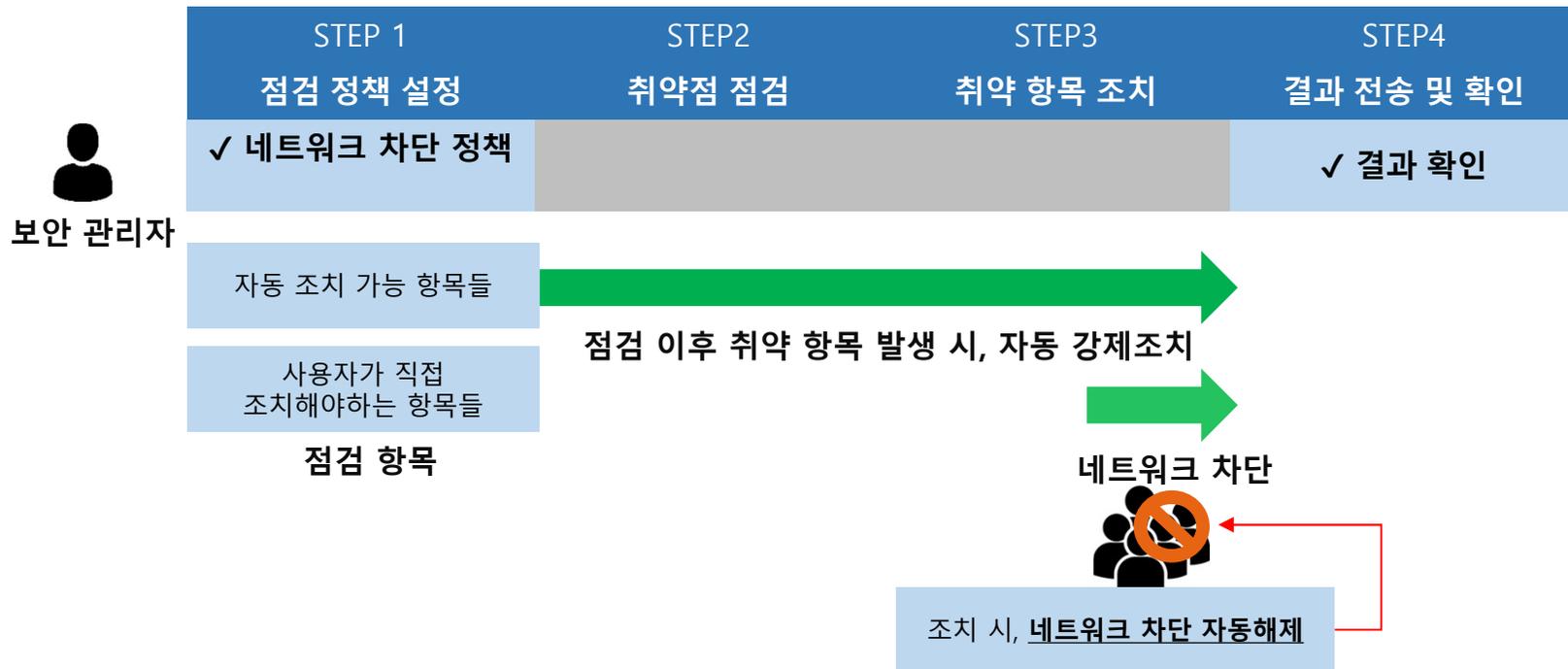
[자동 강제조치] 정책 설정만으로 점검 시 자동조치를 진행하여 사용자가 조치하지 않아도 자동조치 가능하며, 취약점 점검 결과를 항상 최신화하고 취약 항목만 조치하여 불필요한 리소스를 최소화함.



도입 효과

자동화된 조치 유도과 명확한 안내를 통한 확실한 조치

- 일부 점검 항목의 경우 사용자가 직접 조치(로그인 암호 설정, 비인가 프로그램 삭제 등)해야하며, 자동조치가 불가능한 점검 항목은 사용자가 조치하도록 네트워크를 차단하여 조치 유도합니다.
- 네트워크 차단 시, 조치해야하는 취약 항목 및 조치 방법을 명확하게 안내해서 문의없이 사용자 스스로 조치할 수 있게하고, 사용자가 네트워크 차단해제 기준을 달성하는 경우 차단 자동해제



도입 효과

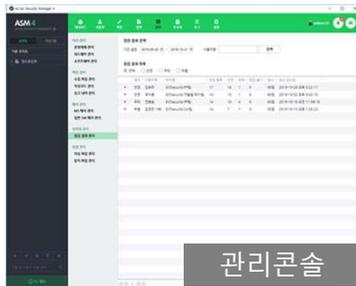
누락없는 점검결과

사용자 점검 결과가 누락되는 경우없이 전송 실패한 점검 결과는 동기화되어 누락방지를 예방합니다.

사용자 점검 결과 누락 발생



누락없는 점검 결과



관리콘솔



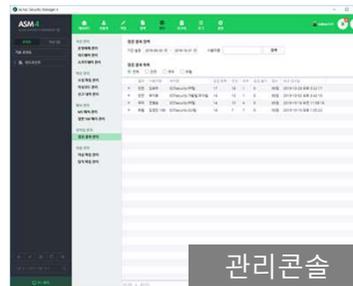
점검 결과 전송 실패



클라이언트

트래픽 부하, 네트워크 연결 문제로 누락된 점검 결과가 있을 수 있음

내부직원들의 불만 발생



관리콘솔



전송 실패한 점검 결과 동기화



클라이언트

점검 결과가 전송 실패하는 경우 동기화되어 자동으로 점검결과 반영

도입 효과

취약점 완벽 대응

알약 내PC지키미 도입 시 안정적이고 효율적인 PC 취약점 관리를 통해 고도화되는 위협을 사전 예방할 수 있으며, 최소화된 운영 리소스와 비용으로 알약 및 다양한 솔루션과 연계된 통합 보안 시스템을 구축하여 기업의 보안 수준을 향상시킬 수 있습니다.

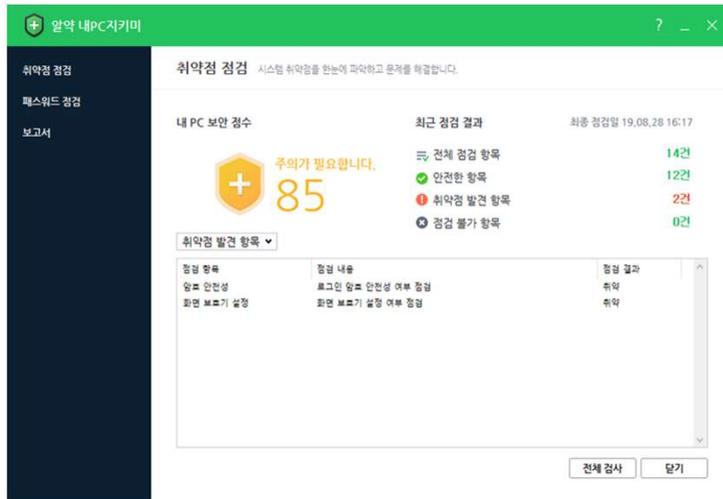
	안전한 보안 환경 구축	<ul style="list-style-type: none">• 취약 항목 자동 조치로 안전한 기업보안 상태 유지• 실시간 모니터링을 통한 신속 대응 가능
	TCO 절감	<ul style="list-style-type: none">• ASM 연동을 통한 시스템 구축 및 관리 비용 최소화• 보안 사고 방지를 통한 기업 손실 감소 및 업무 연속성 유지
	효율적인 보안 솔루션 통합 관리	<ul style="list-style-type: none">• 통합 에이전트와 서버를 통해 다양한 보안 기능 사용• 일관된 보안 정책 유지 가능

도입 효과

통합 운영 및 관리

알약 내PC지키미는 다양한 점검 항목과 점검 설정 등 세부 정책을 통해 사용자 PC상태와 보안 수준을 효율적으로 관리할 수 있습니다. 특히 알약 패치관리(PMS)와 함께 도입 시, 알약 패치관리(PMS)와 연동되어 기업 내 PC의 윈도우 업데이트나 주요 소프트웨어의 패치 설치 현황을 실시간으로 확인하고, 신속하게 패치 파일을 배포하여 관리할 수 있습니다.

알약 내PC지키미



알약 패치관리(PMS)



주요 점검 항목

기본 점검 16가지

보안 업데이트	<ul style="list-style-type: none"> - 바이러스 백신 설치 및 실행 여부 점검 - 바이러스 백신의 최신 보안 패치 여부 점검 - 운영체제, MS Office의 최신 보안 패치 설치 여부 점검 - 한글 프로그램의 최신 보안 패치 설치 여부 점검
암호 안전성	<ul style="list-style-type: none"> - 로그인 암호 안전성 여부 점검 - 로그인 암호의 분기 1회 이상 변경 여부 점검
화면 보호기 설정	<ul style="list-style-type: none"> - 화면 보호기 설정 여부 점검
공유 폴더 설정	<ul style="list-style-type: none"> - 사용자 공유 폴더 설정 여부 점검
보안 프로그램 설치	<ul style="list-style-type: none"> - USB 자동 실행 여부 점검 - 미사용(3개월) ActiveX 프로그램 존재 여부 점검
설치 프로그램 관리	<ul style="list-style-type: none"> - 편집 프로그램 설치 여부 점검 - 무선 랜카드 설치 여부 점검 - 보안USB 설치 여부 점검 - PDF 프로그램의 최신 보안 패치 설치 여부 점검 - 비인가 프로그램 설치 여부 점검

주요 점검 항목

정밀 점검 9가지

계정 관리

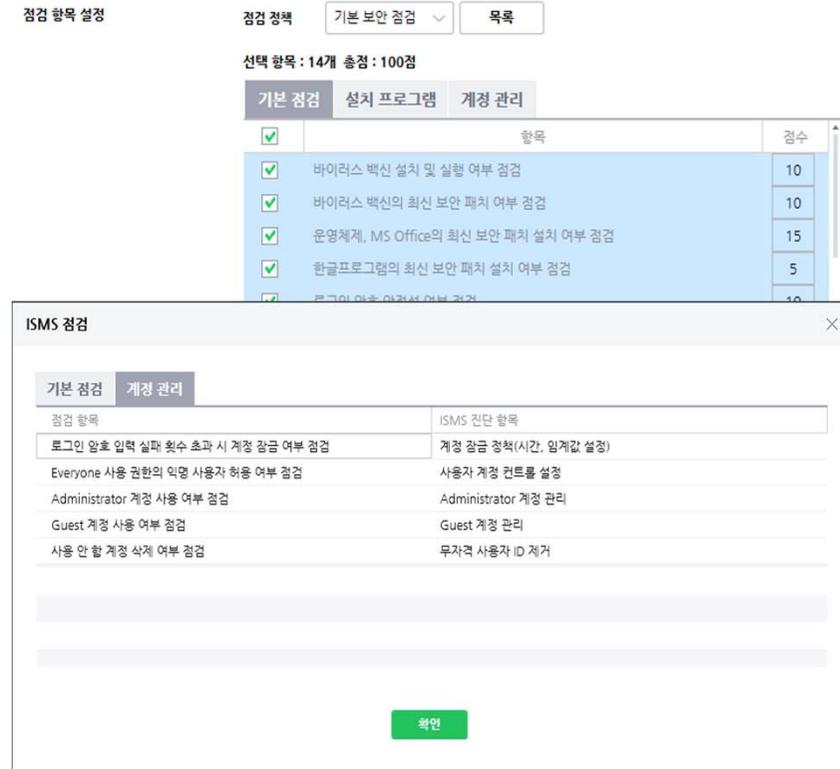
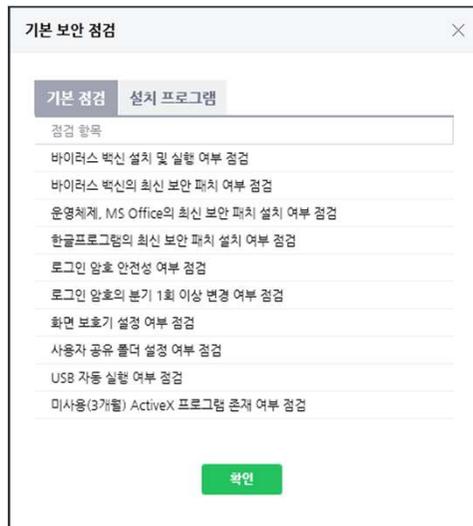
- 로그인 암호 입력 실패 횟수 초과 시 계정 잠금 여부 점검
- Everyone 사용 권한의 익명 사용자 허용 여부 점검
- Administrator 계정 사용 여부 점검
- Guest 계정 사용 여부 점검
- 사용 안 함 계정 사용 여부 점검
- **(2.0 점검항목)** 로그인 암호 최대/최소 사용기간 설정 점검
- **(2.0 점검항목)** 최근 사용한 로그인 암호 설정 점검
- **(2.0 점검항목)** Windows 자동 로그인 점검

주요 기능

취약점 점검

- 사용자/그룹에게 긴급 패치 및 패치 셋에 포함되지 않은 개별 파일의 배포가 가능합니다.

- 사내 PC 취약점 현황 및 점검 결과 관리
- 사이버 보안 진단의 날, ISMS 인증 관련 점검 항목 지원
- PC환경별 맞춤 취약점 점검 항목과 진단 기준 설정
- 취약점 점검 항목, 예외 항목 등 그룹별 맞춤 정책 설정 가능
- PMS와 연동되어 빠르고 안정적인 패치관리

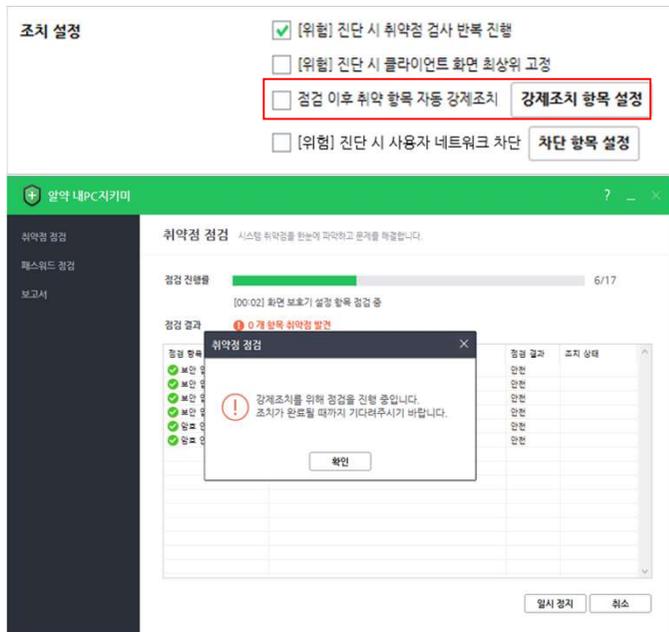


주요 기능

취약점 조치

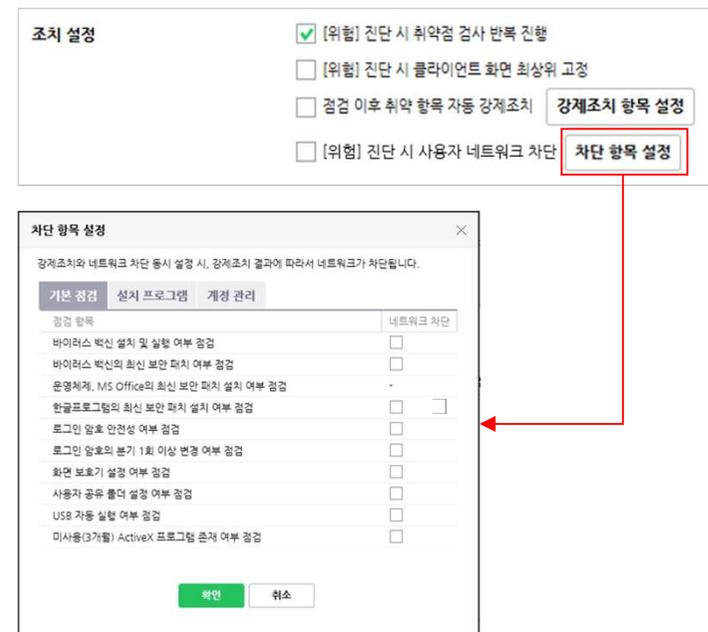
- 사용자/그룹에게 긴급 패치 및 패치 셋에 포함되지 않은 개별 파일의 배포가 가능합니다.
- 자동 조치 정책으로 사용자가 조치하지 않아도 자동으로 점검과 조치를 한 번에 진행
- 일정 점수 이하이거나 설정한 점검 항목이 취약한 경우, 사용자 PC의 '네트워크를 차단'하여 사용자 조치 유도
- 다수의 취약 항목을 사용자가 원클릭으로 간편하게 조치 가능

[자동조치 정책]



*사용자 화면

[네트워크 차단]



주요 기능

모니터링 & 리포팅

- 사용자/그룹에게 긴급 패치 및 패치 셋에 포함되지 않은 개별 파일의 배포가 가능합니다.
- 대시보드를 통한 취약점 점검 및 진단 현황 확인
- 취약점 항목별 점검 현황 및 그룹별 진단 점수 실시간 모니터링
- 취약점 종류, 에이전트 별, 기간별, 부서별 진단 통계 제공
- 보고서 표지, 목차, 보고서 요약 정보 등 보고서 생성부터 보고까지 한 번에 할 수 있도록 양식 제공



상세 UI 및 활용

관리콘솔 > 사용자

ALYac Security Manager 4

ASM 4 ALYAC SECURITY MANAGER

조직도 | 가상그룹

기본 조직도

> Estsoft

공통 관리

사용자 현황

패치 관리

패치 현황

취약점 관리

취약점 현황

사용자 목록 43명

전체 | 점검 | 15 일 이내 미점검 | 결과 | 안전

<input type="checkbox"/>	사용자 명	부서명	점검 여부	보안 점수	결과	점검 일시	IP
<input type="checkbox"/>	강소라	보안사업본부:알약M개발팀:	점검	80	주의	2016-09-20 오전 9:46:58	192.168.197.157
<input type="checkbox"/>	곽승권	보안사업본부:알약M개발팀:	점검	40	위험	2016-09-01 오전 10:12:56	192.168.197.160
<input type="checkbox"/>	구기석	보안사업본부:코어개발팀:	미점검	0	-	-	192.168.190.10
<input type="checkbox"/>	금서미	보안사업본부:알약개발부문:ASM개발팀:	점검	80	주의	2016-10-04 오후 4:55:17	192.168.231.8
<input type="checkbox"/>	김동원1234	보안사업본부:알약개발부문:ASM개발팀:	미점검	0	-	-	192.168.231.11
<input type="checkbox"/>	김보라	보안사업본부:보안대응부문:이슈대응팀:	점검	90	안전	2016-09-07 오전 9:54:52	192.168.190.70
<input type="checkbox"/>	김송진	보안사업본부:알약개발부문:Endpoint개발팀:	미점검	0	-	-	192.168.190.73
<input type="checkbox"/>	김정민	보안사업본부:알약개발부문:Endpoint개발팀:	점검	88	주의	2016-09-21 오후 4:34:07	192.168.190.197
<input type="checkbox"/>	김종우	보안사업본부:알약개발부문:SecureCloud개발팀:	미점검	0	-	-	192.168.190.82
<input type="checkbox"/>	김준섭	보안사업본부:	미점검	0	-	-	192.168.231.4
<input type="checkbox"/>	김태진	보안사업본부:알약개발부문:Endpoint개발팀:	미점검	0	-	-	192.168.231.16
<input type="checkbox"/>	김현승	보안사업본부:알약개발부문:Endpoint개발팀:	미점검	0	-	-	192.168.190.8
<input type="checkbox"/>	김희선(업무용)	보안사업본부:알약개발부문:Endpoint개발팀:	미점검	0	-	-	192.168.190.217
<input type="checkbox"/>	박귀남	보안사업본부:알약M개발팀:	미점검	0	-	-	192.168.197.141
<input type="checkbox"/>	박유정	보안사업본부:알약개발부문:Endpoint개발팀:	점검	64	주의	2016-10-06 오후 6:48:22	192.168.231.67
<input type="checkbox"/>	박재만	보안사업본부:알약개발부문:ASM개발팀:	미점검	0	-	-	192.168.231.3
<input type="checkbox"/>	박종혁	보안사업본부:알약M개발팀:	미점검	0	-	-	192.168.197.148
<input type="checkbox"/>	서광현	보안사업본부:코어개발팀:	미점검	0	-	-	192.168.190.17
<input type="checkbox"/>	성환혁	보안사업본부:코어개발팀:	미점검	0	-	-	192.168.231.70
<input type="checkbox"/>	신승훈	보안사업본부:알약개발부문:ASM개발팀:	점검	56	위험	2016-09-30 오후 6:36:55	192.168.231.2
<input type="checkbox"/>	신승혁	보안사업본부:코어개발팀:	미점검	0	-	-	192.168.190.11
<input type="checkbox"/>	안수연	보안사업본부:알약개발부문:Endpoint개발팀:	점검	50	위험	2016-09-19 오후 5:12:31	192.168.230.239
<input type="checkbox"/>	안지민	보안사업본부:알약M개발팀:	점검	50	위험	2016-09-01 오후 3:14:26	192.168.197.158
<input type="checkbox"/>	오지호	보안사업본부:알약개발부문:Endpoint개발팀:	미점검	0	-	-	192.168.231.9

Page 1 / 1

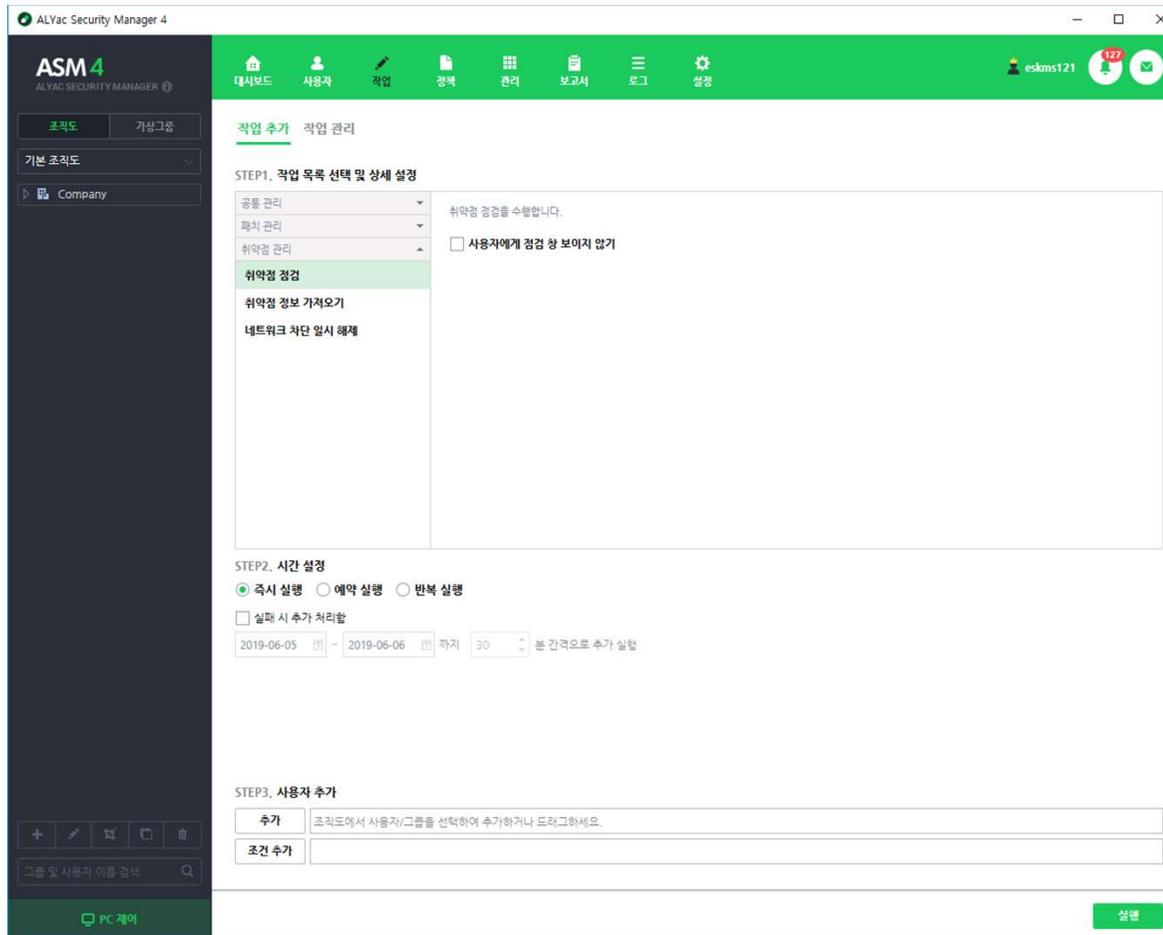
작업 목록 | 실행 | 수정 | 삭제 | 내보내기

취약점 현황

전체 사용자의 기본 정보 및 취약점 점검 현황 확인

상세 UI 및 활용

관리콘솔 > 작업

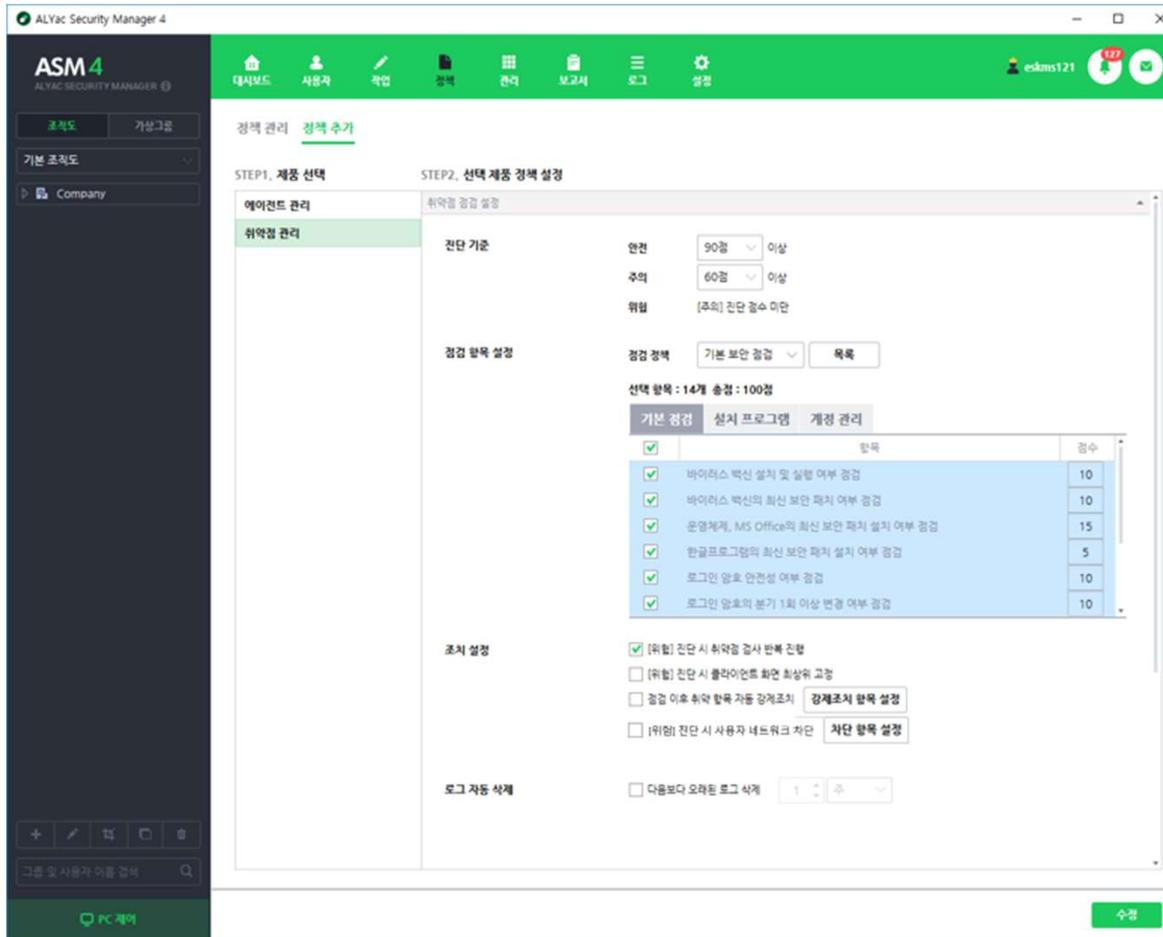


취약점 관리

선택한 사용자나 그룹에게
취약점 관리 작업 명령 가능

상세 UI 및 활용

관리콘솔 > 정책



취약점 관리

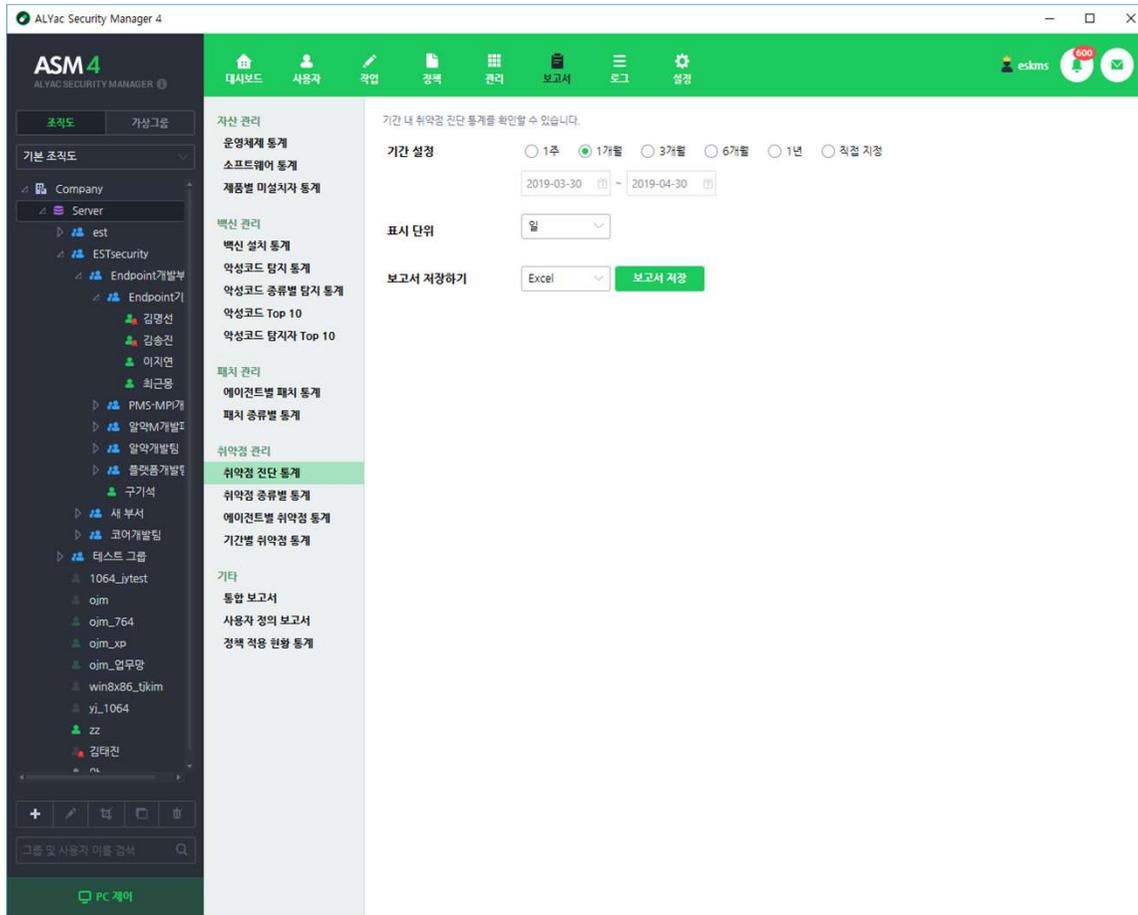
정책 설정 후 선택한 사용자나 그룹에게 정책 적용 가능

취약점 점검 항목 및 점수 설정

- 사이버 진단의 날, ISMS 점검 정책 설정
- 기본 점검 항목
- 설치 프로그램 점검
- 계정 관리 점검
- 네트워크 환경 점검
- (※ 정밀 점검 항목 지속적으로 추가 예정)
- 조치 유도 및 자동 강제 조치 정책 설정
- 강제조치/네트워크 차단/최상위 고정

상세 UI 및 활용

관리콘솔 > 보고서



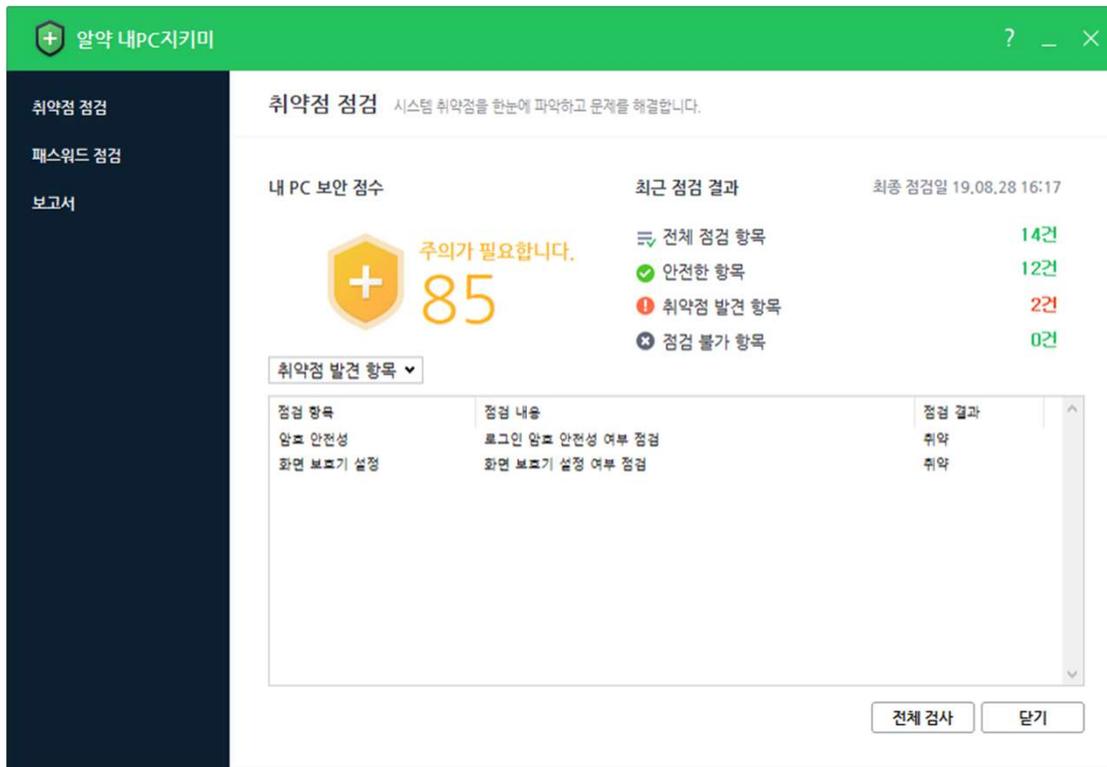
취약점 보고서

취약점 진단, 취약점 종류별, 에이전트별 취약점, 기간별 통계 보고서

보고서 생성부터 보고까지 한번에 진행할 수 있도록 통합 보고서 양식 제공
(표지, 목차, 취약점 요약)

상세 UI 및 활용

클라이언트 > 취약점 점검



취약점 점검

취약점 항목 점검

- 내PC지키미 기본 점검 항목
- 직관적으로 취약 항목 확인
- 취약한 항목 자동/수동 조치

상세 UI 및 활용

클라이언트 > 패스워드 점검



패스워드 점검

패스워드의 안전성 점검 및 결과 제공

상세 UI 및 활용

클라이언트 > 보고서

+ 알약 내PC지키미
? _ ×

취약점 점검

패스워드 점검

보고서

보고서 취약점 점검 내역 별 보고서를 확인할 수 있습니다.

시스템 정보

운영체제: Windows 10 Enterprise

안티 바이러스 S/V: 알약 내PC지키미

안티 스파이웨어 S/V: 알약 내PC지키미

개인 방화벽 S/W: 알약 내PC지키미

점검 내역

점검 일시: 2019-09-18 16:16

2019-09-18 13:39

2019-09-18 12:53

2019-09-11 16:47

2019-09-09 13:17

2019-09-09 11:08

2019-09-09 11:01

2019-09-09 10:17

2019-09-06 16:15

2019-09-05 17:19

2019-09-05 17:09

2019-09-05 16:58

NO.	점검 항목	점검 결과	점검 자동 조치 결과
1	바이러스 백신 설치 및 실행 여부 점검	안전	-
2	바이러스 백신의 최신 보안 패치 여부 점검	안전	-
3	운영체제, MS Office의 최신 보안 패치 설치 여부 점검	안전	-
4	한글프로그램의 최신 보안 패치 설치 여부 점검	안전	-
5	로그인 암호 안전성 여부 점검	안전	-
6	로그인 암호의 분기 1회 이상 변경 여부 점검	안전	-
7	화면 보호기 설정 여부 점검	안전	-
8	사용자 공유 폴더 설정 여부 점검	안전	-
9	USB 자동 실행 여부 점검	안전	-
12	무선 랜카드 설치 여부 점검	안전	-
13	보안USB 설치 여부 점검	안전	-
14	PDF 프로그램의 최신 보안 패치 설치 여부 점검	안전	-
15	비인가 프로그램 설치 여부 점검	안전	-
17	Everyone 사용 권한의 익명 사용자 허용 여부 점검	안전	-

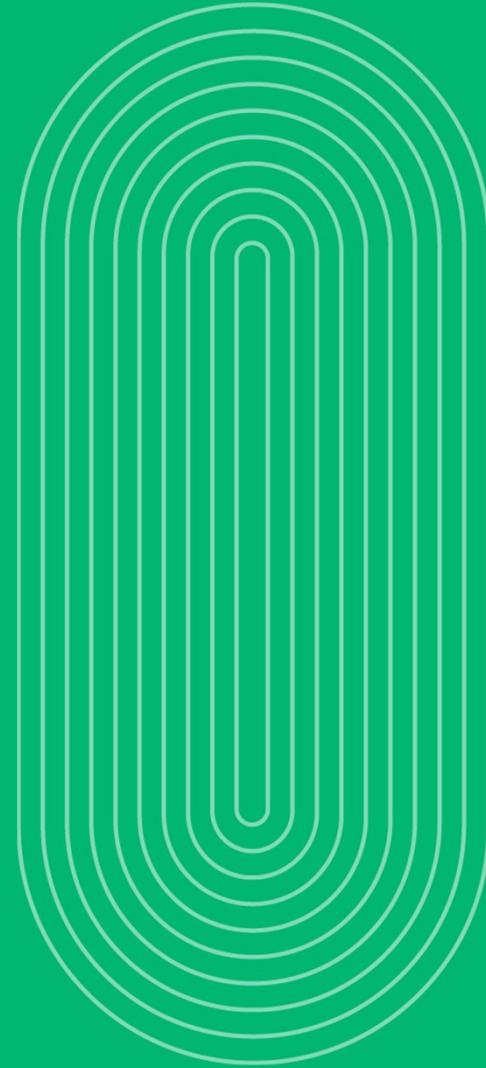
보고서

취약점 점검 내역 별 보고서 확인

03

고객 지원

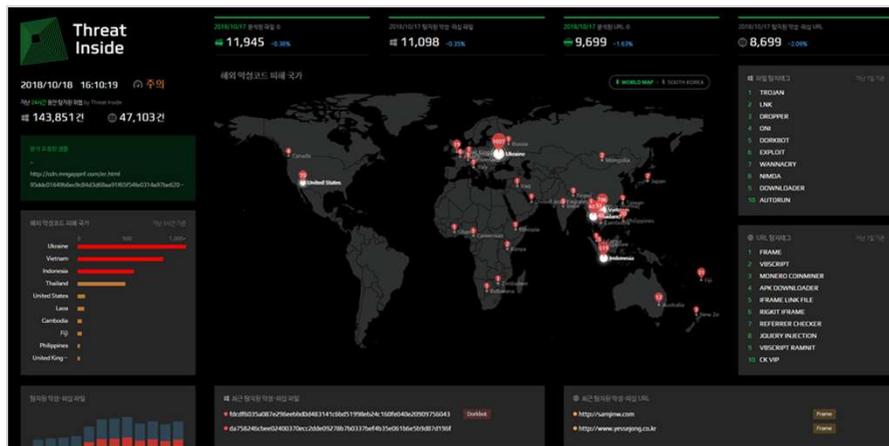
- 이스트시큐리티 대응 센터
- 고객지원 서비스
- 구성 및 운용



ESRC

이스트시큐리티 대응센터 ESRC

국내 보안 사고는 주로 국내 사정을 잘 알고 있는 집단이 조직적이고 계획적으로 진행하여 이뤄졌습니다.
 국내 최고 전문가들로 구성된 이스트시큐리티 대응센터(ESRC)는 정부 주요 기관들과 연계한 **상시 대응 체계**를 유지하여,
국내에 특화된 APT 공격과 랜섬웨어 등 각종 위협에 **가장 빠르게 대응**하고 있습니다.



고객지원 서비스

지원 센터

시큐리티 대응센터

실시간 모니터링 체계를 구축하여 국가기관과 연계한 상시 대응 체계를 유지하고 있습니다. DDos, 해킹, 랜섬웨어 등 긴급상황 발생 시 고객사를 포함한 민간의 피해를 최소화하고자 하며, 전용 백신 개발 및 배포를 통해 위기 상황에 신속하게 대응하고 있습니다.

기술 지원 센터

기업 고객들을 위한 전문 기술 지원 센터를 운영하고 있습니다. 기술지원 요청 시, 원격 지원은 물론 방문 지원 서비스 등 특화된 지원 서비스를 기업 고객들께 제공하며, 기술지원 핫라인을 24시간 운영하여 빈틈없는 보안 서비스를 제공하고 있습니다.

지원 시스템

오류 보고 시스템

알약과 ASM은 오류 발생 시 이를 자동으로 신고하여 가장 빠르게 조치 받을 수 있는 시스템을 지원합니다. 오류 보고 시스템을 통해 관리자는 장애 상황 발생 시 신속한 선조치 및 긴급 복구 서비스를 제공받게 됩니다.

장애 모니터링 시스템

전문 보안 기술 인력들이 기업용 모니터링 시스템을 통해 고객사의 알약 및 ASM 동작 상태를 24시간 체크합니다. 모니터링 시스템을 통해 관리자가 인지하기 전에 장애 조치를 제공받고 조치 결과를 안내 받을 수 있습니다.

고객지원 서비스

전문 기술 인력이 체계적이고 신속한 고객 지원 서비스를 제공합니다.

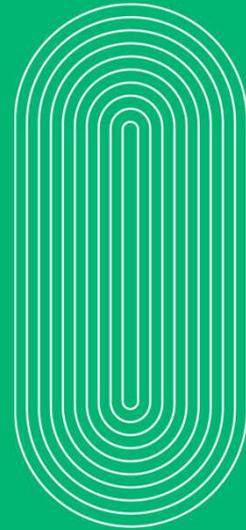
 신고하기/ e-mail 상담 (2시간 이내 회신)	 전문 기술 인력의 전화 상담	 야간 및 공휴일, 주간 핫라인 운영
 PC 원격지원 서비스	 대규모 사이트 전담 인력 배정 및 정기 방문 점검 서비스 제공	 제품 교육 서비스 제공

- 구매문의 : 02-3470-2970
- 고객센터 : 1544-9744
- 홈페이지 : <https://www.estsecurity.com/enterprise/product/alyac-enterprise>

구성 및 운영

시스템 구성





알약 내PC 지키미

ESTSECURITY

문의처 TEL : 02-583-4616 홈페이지 : www.estsecurity.com