AKDAN HALL
Pre-Excution Detect Security Solutions

AKDAN HALL PED V1.0_제품설명서 V1.3

목차



1 | 개요

악단홀이란?
악단홀은 무엇을 막는가?
제품특징
주요기능
설치환경
실행소프트웨어 구성

2 | 트리피타카 엔진

Forward Engineering(포워드 엔지니어링)
Exploitation Detecting Trap(취약점 공격 탐지 트랩)
Four-Layer Structure(4계층 구조)

3 | 악단홀 PED

PED Solutions (사전 실행 탐지)
Unknown Malware Detection (알려지지 않은 악성코드 탐지)

4 | 화면정보

제품화면
라이선스 발급 및 관리
다양한 테마

5 | 기능 설명

신분증
파일
PED 메뉴
격리소
감사로그

6 | 비고

악단홀이란?

신개념 개인용 보안 솔루션

가볍고 빠르게 사용자 pc에서 문서형 악성코드를 전문으로 탐지하는
PED(사전실행탐지) 보안 솔루션입니다.

악단홀은 무엇을 막는가?

① HWP, PDF, DOC, XLS, PPT와 같은 '문서형 악성코드'
악성코드에 감염된 문서 파일 하나가 당신의 PC를 무용지물로 만들 수 있습니다.

문서형 악성코드의 공격 패턴은 세 가지입니다.

1) 어플리케이션의 취약점을 공략하는 방법
2) 문서 안의 매크로를 이용하는 방법
3) 원격 템플릿을 이용한 방법

어떤 방식이라도 여러분이 클릭하는 순간 실행파일처럼 구동합니다.
문서 파일이라고 안전할거라 생각하는 것은 금물입니다.



악단홀은 무엇을 막는가?

② VBS, JS, HTML과 같은 '스크립트형 악성코드'

보안 기술이 진화하면서 여러분의 PC는 다양한 공격에 대비하고 있습니다.
하지만 vbs 파일은 그렇지 못합니다.
지금 PC에 test.vbs라는 파일을 만들어 다음 문구를 저장해보십시오.

MsgBox "Hello?"

놀랍게도 최신 윈도우인 11에서도 쉽게 실행됩니다.
VBS 인터프리터인 wscript.exe와 cscript.exe는 윈도우에 기본으로 포함되어 있습니다.

VBS는 MS에서 1980년대에 개발한 스크립트 언어입니다.
오래된 만큼 허술하고 위험한 문법이 많지만 널리 쓰입니다..

③ JPG, AVI, MOV와 같은 기타 취약점을 노리는 '비실행형 컨텐츠'

그림 파일이나 동영상, 토렌트 파일 등 상용 어플리케이션을 사용하는 모든 컨텐츠는 취약점 공격으로 활용될 수 있습니다.



1 | 개요



제품특징

- ▶ 최신 유형의 스크립트와 문서 악성코드를 탐지
- ▶ 쾌속 샌드박스 기술로 분석 소요 시간은 평균 1초
- ▶ 드라이버 사용을 최소화하여 시스템 최적화

주요기능

- ▶ **비실행형 악성코드 탐지** | 문서, 스크립트 등 실행파일이 아닌 악성코드 탐지
- ▶ **UNKNOWN 악성코드 탐지** | 백신이 탐지하지 못하는 최신 악성코드 탐지
- ▶ **사전실행탐지** | 모든 문서파일을 실행 전 분석하여 안전하게 실행가능
- ▶ **악단 분석보고서** | 악성코드 파일의 분석 내용을 확인하여 보다 전문적으로 컴퓨터를 보호
- ▶ **트리피타카 엔진** | 자체개발한 악성코드 탐지 엔진으로 포워드엔지니어링 기술을 통해 악성코드 탐지
- ▶ **포워드엔지니어링** | OS / APP 에뮬레이터를 통해 악성코드를 빠르게 분석



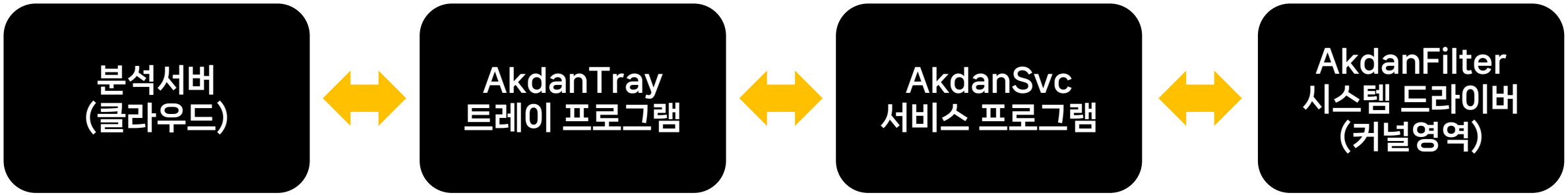
설치 환경

악단홀은 최소사항에서도 동작되게 설계되었지만, 빠르고 원활한 사용을 위해 권장사항 이상의 PC를 이용해 주시기 바랍니다.

항목	최소사항	권장사항
CPU	Quad Core 2.5GHz	Quad Core 3.0GHz
RAM	4GB이상	8GB이상
HDD	NTFS 파일시스템 100MB이상	NTFS 파일시스템 500MB이상
OS	윈도우10이상	윈도우10이상

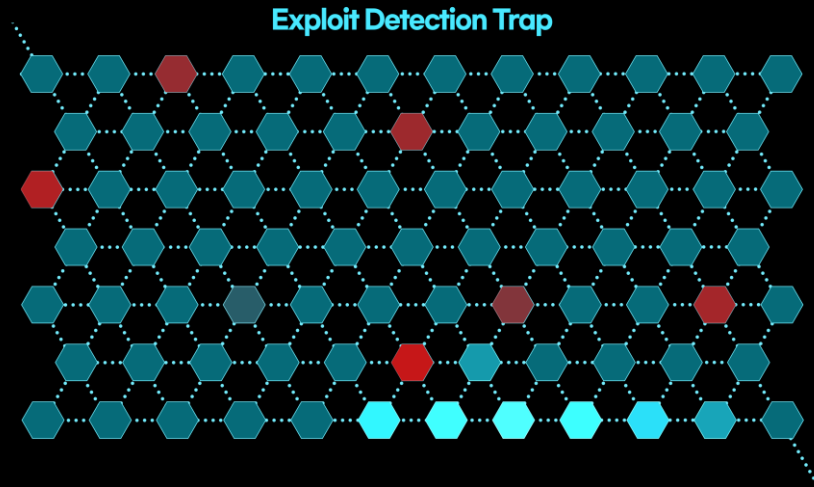
악단홀은 GUI 기반 사용자 환경을 제공합니다.

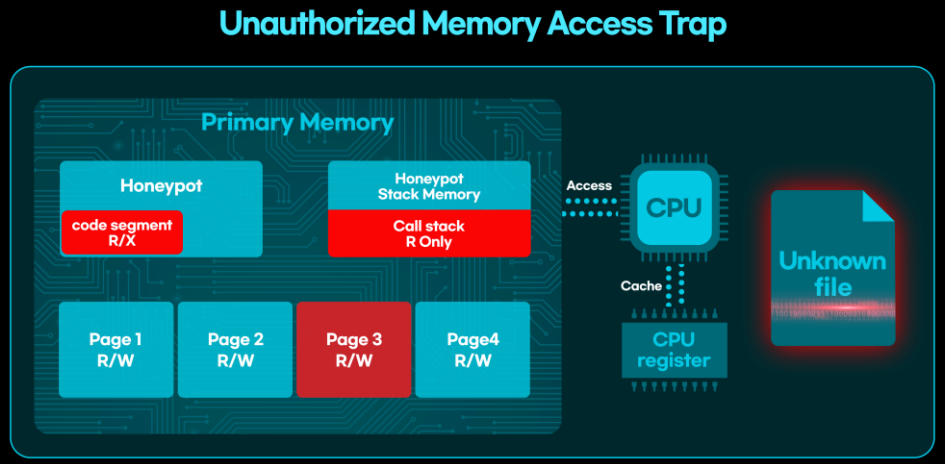
실행 소프트웨어 구성


분석서버
(클라우드)
AkdanTray
트레이 프로그램
AkdanSvc
서비스 프로그램
AkdanFilter
시스템 드라이버
(커널영역)

Forward Engineering(포워드 엔지니어링)

01





1초 이내로 분석을 마치는 쾌속 샌드박스

트리피타카 엔진은 뇌 신경의 뉴런처럼 순식간에 분석을 마칩니다.
포워드 엔지니어링이 적용된 쾌속 샌드박스가 행위를 분석해 내기까지 1초면 충분합니다.

시스템 API와 메모리 모니터링으로 정밀분석

난독화가 심하고 행위 변동의 폭이 큰 스크립트류 악성코드는 시스템 API를 감시해야 합니다.
한편 취약점 공격류 악성코드는 메모리의 오동작을 감시해야 합니다.
포워드 엔지니어링으로 최적화된 샌드박스는 불필요한 동작은 제외하고 악성코드 탐지에
필요한 부분은 포함시켜 정밀한 분석이 가능합니다.

저탄소 시대에 적합한 기술

기존대비 샌드박스 연산량을 1/100로 줄여 가볍고 빠르게 탐지할 수 있습니다.
고성능의 서버가 필요하지 않아 저탄소 시대에 적합한 기술입니다.

Exploitation Detecting Trap(취약점 공격 탐지 트랩)

02

메모리 오동작 탐지 트랩

악단의 CPU 에뮬레이터는 실행 중 메모리 오동작을 추적하여 제로데이 공격도 탐지 할 수 있습니다. 특히 콜스텍 영역의 탐지 기술은 메모리 가드가 없으면 OS에서 지원하지 못하는 기술로 현재 특허 출원 중입니다.

파편화 문제를 초월

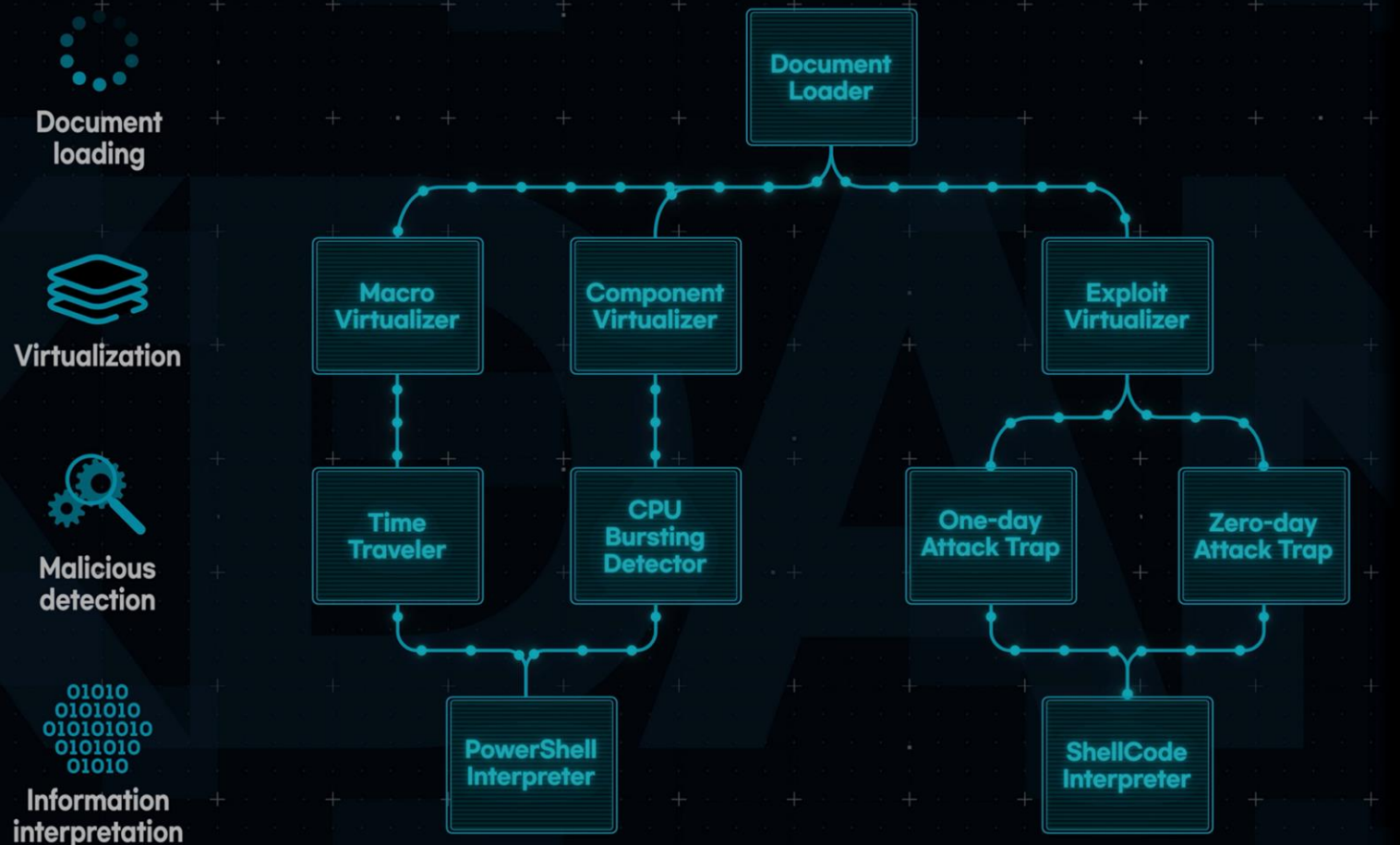
특정 프로그램 버전의 취약점을 악용하는 류의 악성코드는 프로그램 버전이 달라지면 동작하지 않아 탐지할 수 없습니다.
이것을 파편화 문제라고 합니다.

이러한 매복상태의 악성코드를 잡아내고자 한 번이라도 발견된 취약한 버전의 프로그램들을 모아서 탐지 트랩을 만들었습니다.
약 100여개의 탐지 트랩으로 알려진 취약점을 이용하는 원데이 공격류 악성코드를 원천적으로 잡아낼 수 있습니다.



Four-Layer Structure(4계층 구조)

03



문서적재, 가상화, 악성탐지, 정보해석
(무한 확장 구조)

트리피타카 엔진은 문서적재, 가상화, 악성탐지, 정보해석 총 4가지 계층으로 이루어졌습니다.

각 계층에는 여러 엔진들이 배치되었으며 확장 가능하게 설계되었습니다.

PED Solutions (사전 실행 탐지)

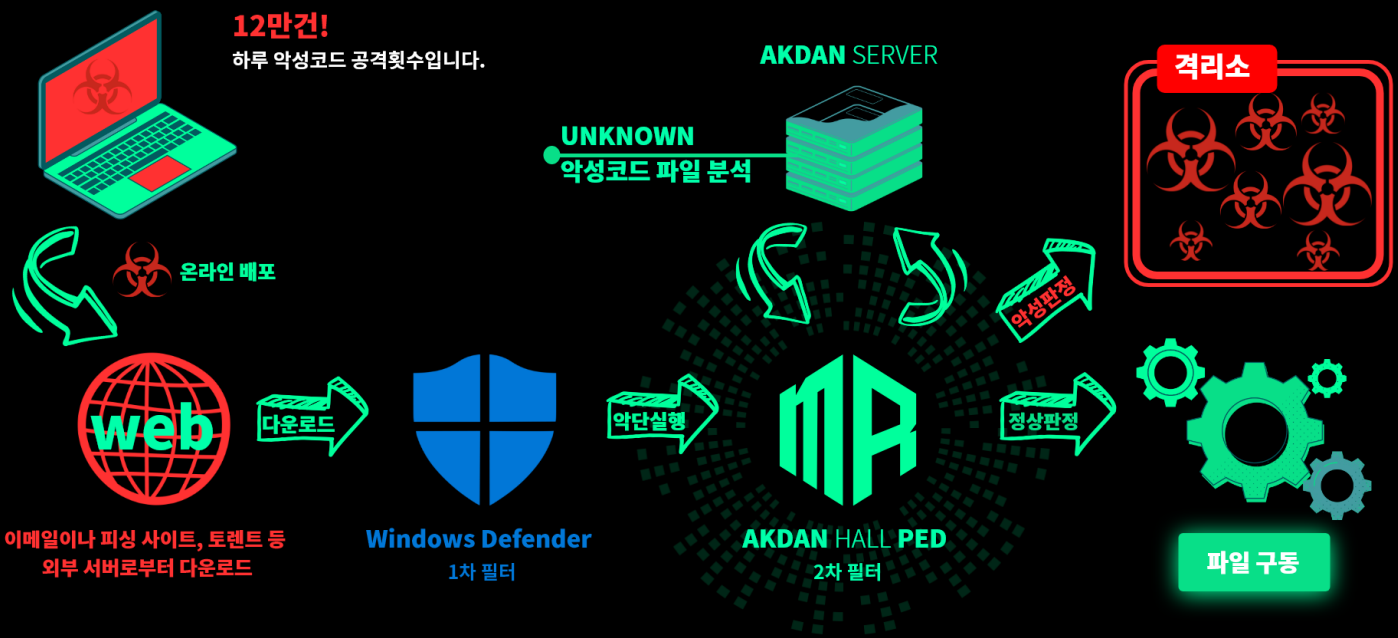
01

실행 직전 동작하여 백신과 상호보완

백신이 1차적으로 필터링한 파일을 대상으로
2차 검사를 수행합니다.

내 PC에 존재하는 파일들은 이미 백신이 걸러 낸 파일입니다.
시그니처에 등록된 파일은 다운로드 직후에 바로 격리시키기 때문입니다.

이 파일들을 대상으로 실행하기 직전, 2차검사를 수행합니다.
기존의 백신과 PED 솔루션이 내 PC의 보안 수준을 함께 높이는 것입니다.



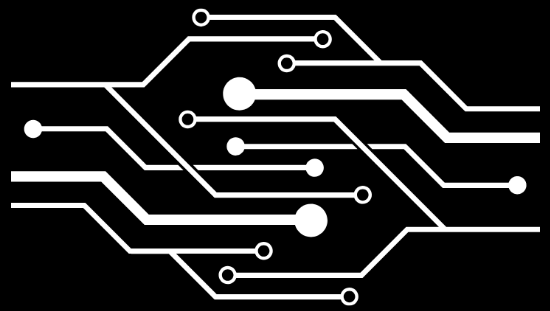
Unknown Malware Detection (알려지지 않은 악성코드 탐지)

02

악단홀의 트리피타카 엔진은 변종까지 탐지할 수 있습니다.

백신은 아직 시그니처에 등록되지 않은 악성코드는 걸러내지 못합니다.
최초의 악성코드는 전통적으로 샌드박스에서 직접 실행해 악성여부를 판단합니다.
하지만 시간도 오래 걸리고(약 1분) CPU 소모량도 높아서 고성능의 서버가 필요합니다.

트리피타카 엔진은 쾌속 샌드박스 분석 기술을 탑재한 악단의 핵심 기술입니다.



악성코드 분석에 최적화된 자체 샌드박스로 평균 분석시간이 1초 내외입니다.
CPU 사용량도 적어서 저사양의 서버에서 구동될 수 있습니다.
빠르고 적은 유지비용 덕분에 개인용 샌드박스 분석기술을 제공할 수 있게 되었습니다.



3 | 화면정보

MODE 변경

유·무료의 간편/전문가 모드를 제공하며,
필요에 따라 모드를 변경할 수 있습니다.

라이선스 관리

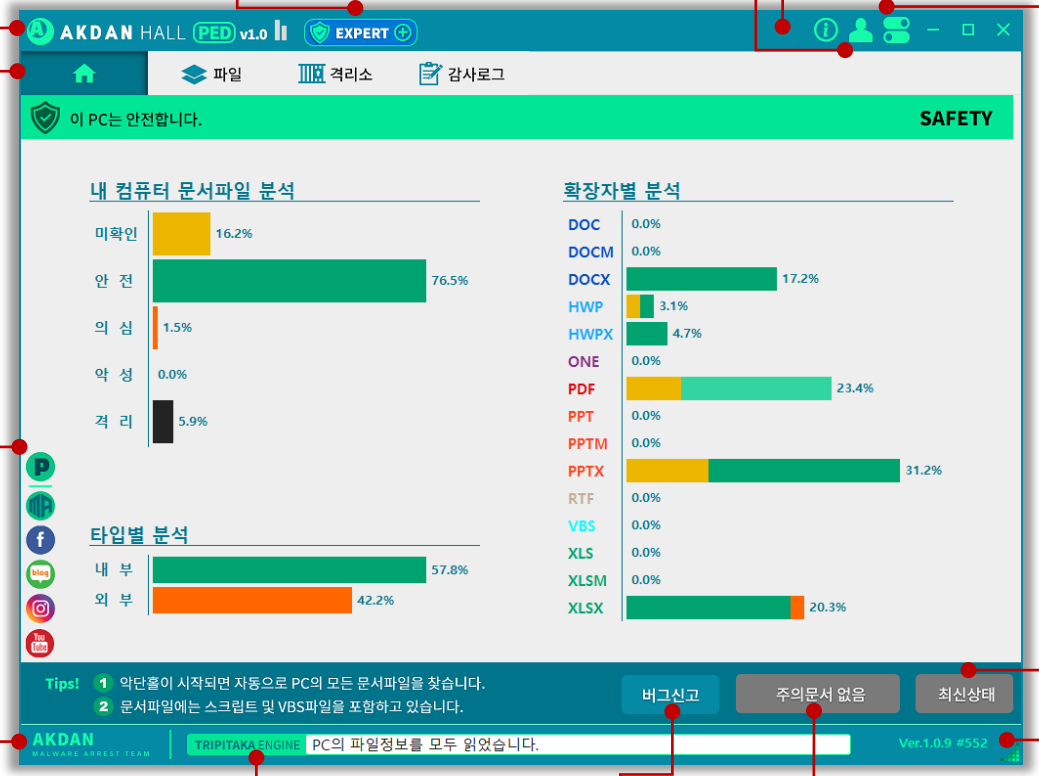
라이선스 발급 및 검증(로그인)을 할 수 있으며,
로그인 시 제품 구매 및 기술 상담이 가능합니다.

시스템 버튼

튜토리얼 가이드 / 라이선스관리 / 옵션설정 / 최소화 / 최대화 / 닫기
기능을 가진 버튼입니다.
옵션설정은 사용자 취향대로 조정이 가능합니다.

제품명 및 드래그 바

제품명이 표시됩니다. 또한 해당 바를 클릭한 상태로 움직이면 창을 움직일 수 있습니다.
*드래그 바 : 상단을 누른 채로 이동이 가능한 바

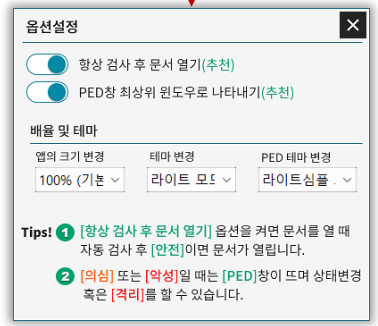


홈/분석/격리/감사로그

▶ **홈** | 악단홀이 실행되면 기본으로 보여집니다.
▶ **파일** | 파일을 분류 / 검사 / 격리 / 삭제 등 파일관련 기능을 수행합니다.

▶ **격리소** | 분석에서 격리된 파일이 모이는 곳이며 격리된 파일을 복원, 삭제 할 수 있습니다.

▶ **감사로그** | 악단홀의 시스템로그를 볼 수 있는 곳입니다.



메인화면

현재 내 PC의 문서파일을 종류별로 분석하여 보여주며,
각종 악성코드검거단 관련 페이지 바로가기가 가능합니다.

- **패치노트** | 악단홀의 업데이트 및 개선사항을 열람할 수 있습니다.
- **홈페이지** | 악성코드검거단 홈페이지 바로가기 버튼입니다.
- **페이스북** | 악성코드검거단 페이스북 바로가기 버튼입니다.
- **블로그** | 악성코드검거단 블로그 바로가기 버튼입니다.
- **인스타그램** | 악성코드검거단 인스타그램 바로가기 버튼입니다.
- **유튜브** | 악성코드검거단 유튜브 바로가기 버튼입니다.

업데이트 버튼

버전 및 업데이트 날짜를 확인 할 수 있습니다.

버전 및 업데이트 날짜

버튼이 활성화 되면 클릭하여 제품을 업데이트 할 수 있습니다.

회사로고

악단홀 제작사 악성코드검거단 로고가 표시됩니다.

알림창

현재 악단홀이 수행 중이거나 수행 완료된 작업에 대하여 알려줍니다.

버그신고 버튼

사용자가 제품 사용 중 겪은 장애나 불편사항을 작성하여 보낼 수 있습니다.

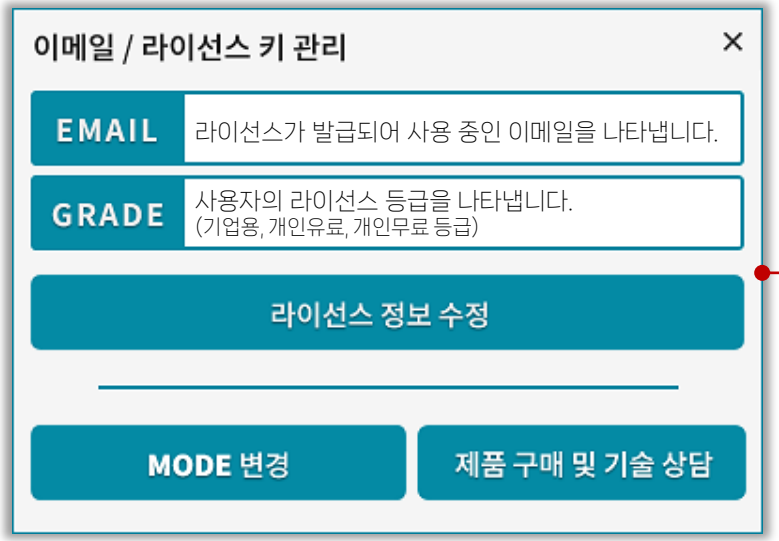
주의문서 버튼

PC 내 주의문서의 여부를 알 수 있습니다.
주의문서 확인 시 클릭하면 파일 탭 내의 주의문서 탭으로 이동 합니다.

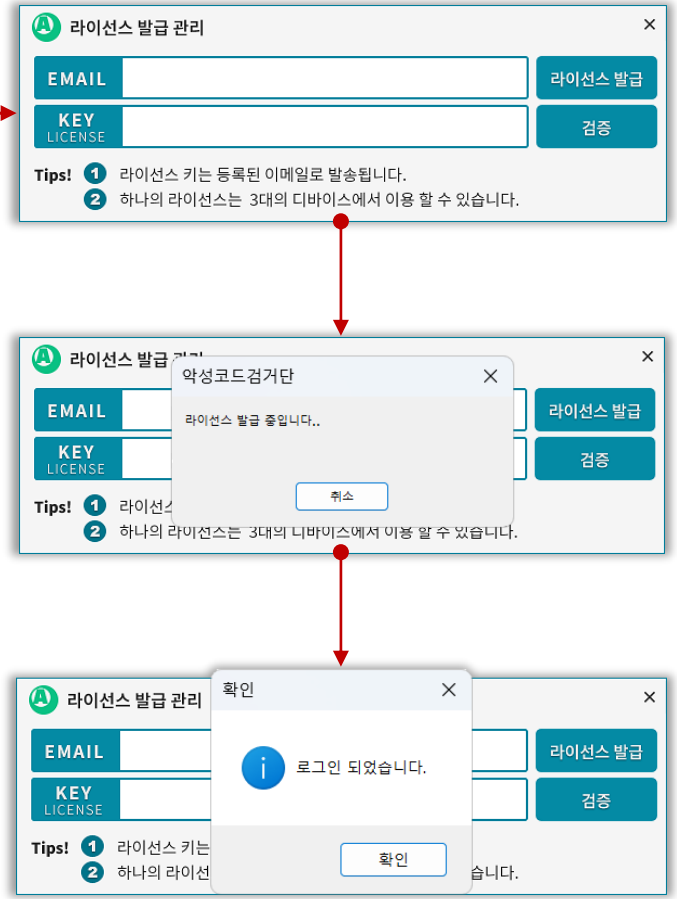
3 | 화면정보

이메일/라이선스 발급 및 관리

를 누를 시 아래와 같은 창이 뜹니다.



악단홀 최초 실행 및 라이선스 정보 수정을 누를 시 뜨는 창입니다.



'라이선스 키'를 발급받고자 하는 이메일을 입력합니다.

라이선스 발급을 누르고 잠시 기다립니다.

이메일로 발송된 '라이선스 키'를 입력 후
검증을 누르면 로그인이 완료됩니다.

MODE 변경

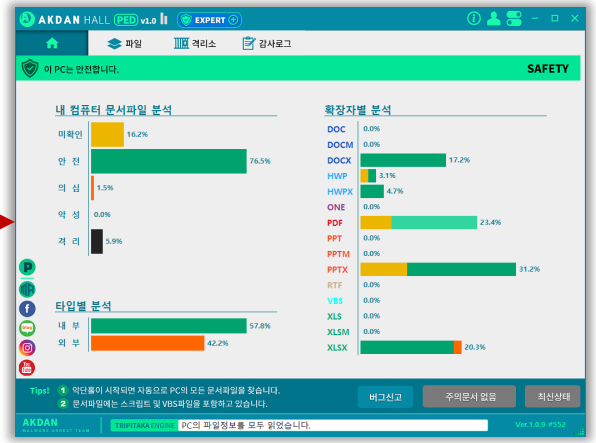
제품명 상단에 위치한 방패모양을 누를 시 아래와 같은 창이 뜹니다.
사용자가 필요에 따라 모드를 변경할 수 있습니다.





간편 모드

실행 시 윈도우 우측 상단에 표시되며, 최소한의 주요기능을 제공하여 보다 간편하고 빠르게 악단홀을 활용할 수 있습니다.



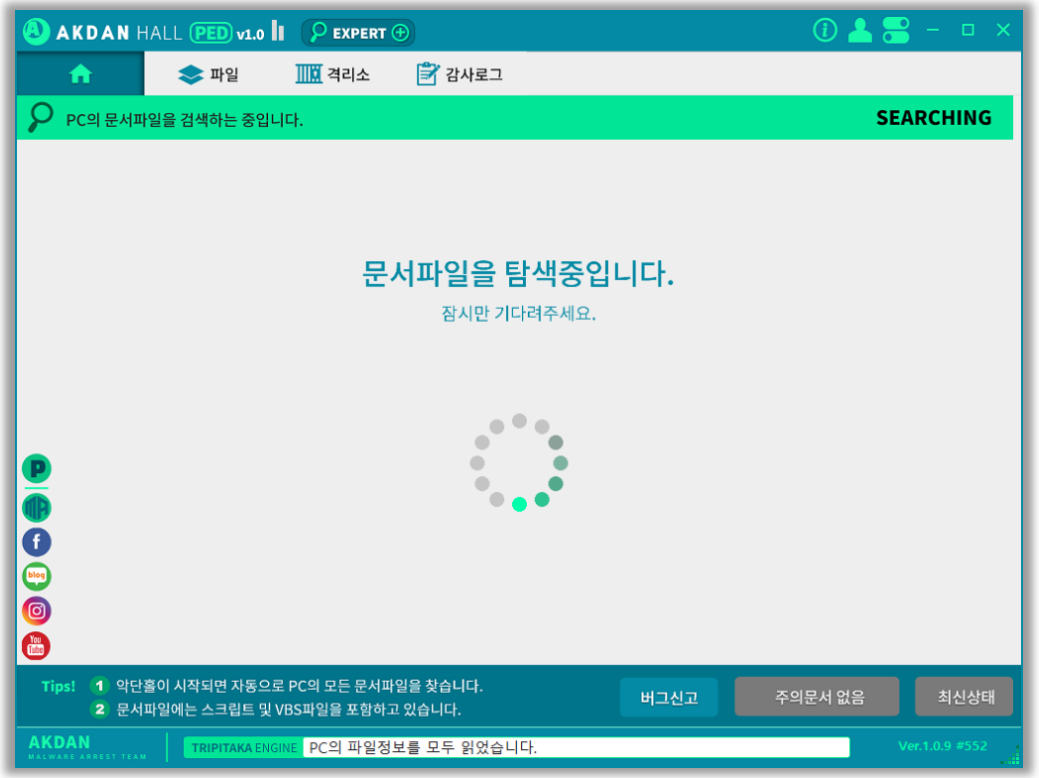
전문가 모드

간편 모드에서 제공하는 기능 포함 다양한 기능을 사용하실 수 있습니다. 이를 통해 더 효율적으로 파일을 관리하고 보호할 수 있습니다.

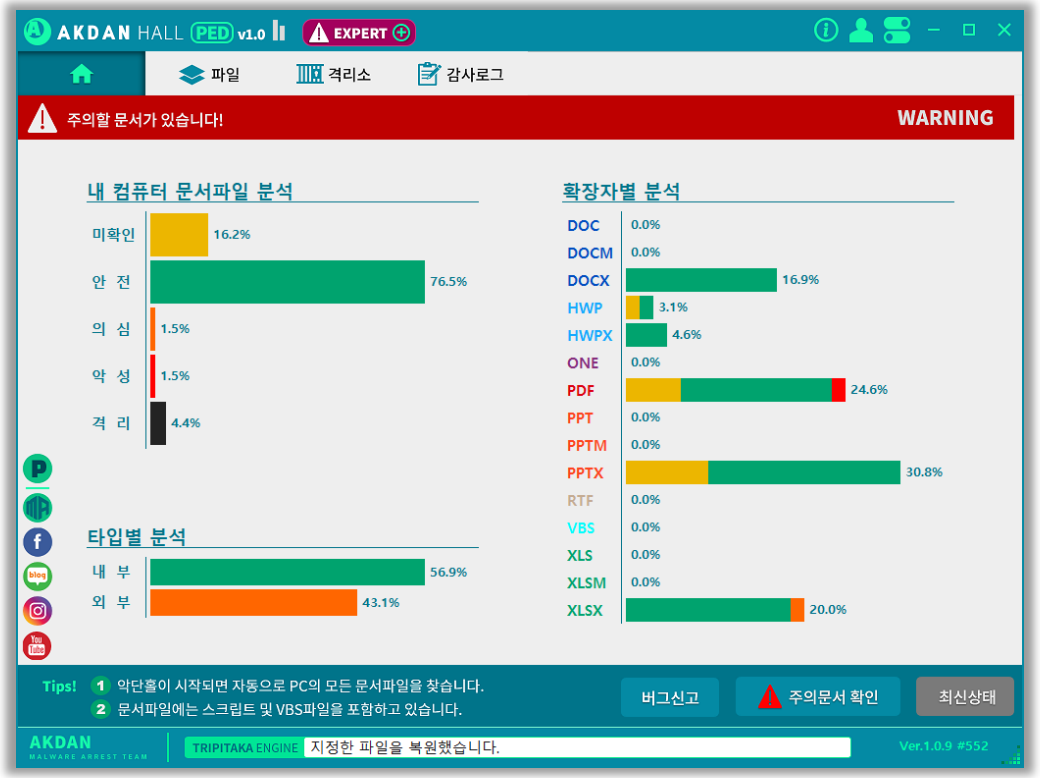
※ 이미지는 플러스(유료)모드 기준입니다.

3 | 화면정보

처음 실행 시 PC내 문서 탐색 중일 때의 화면

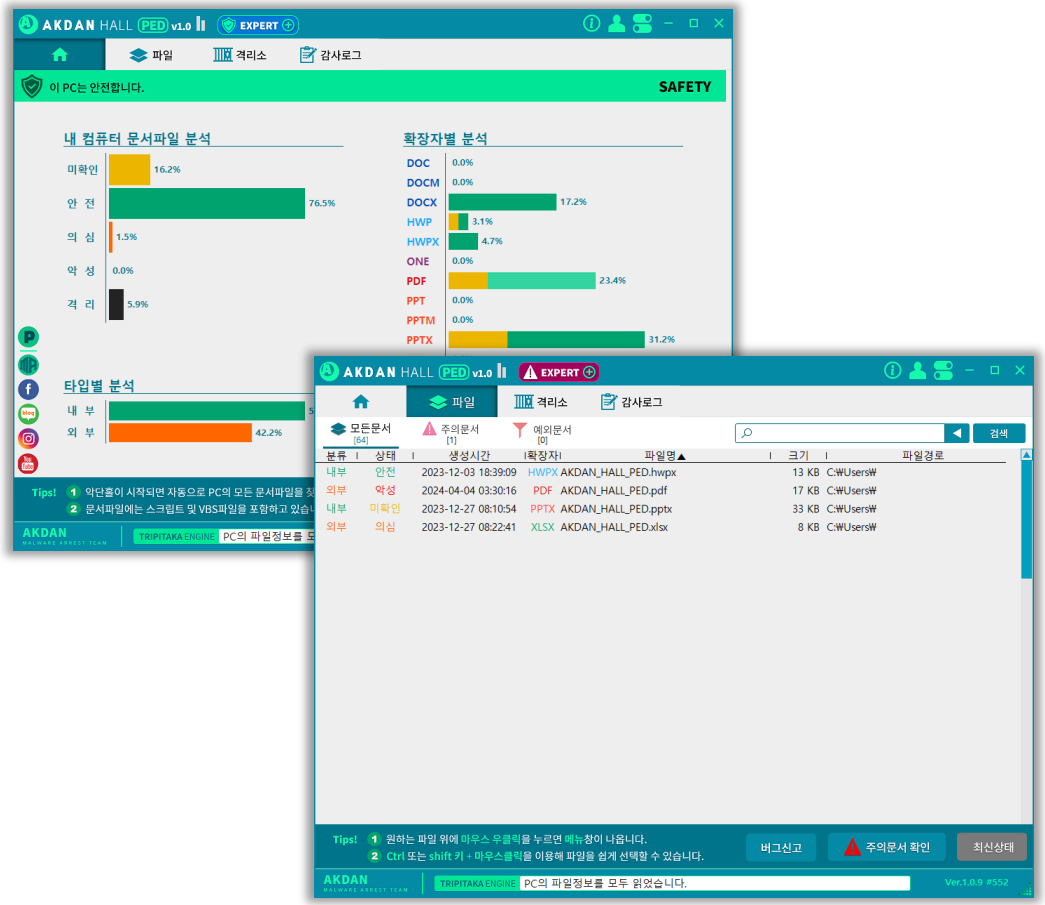


악성문서파일이 감지되었을 때의 화면



3 | 화면정보

테마 - 라이트모드



테마 - 다크모드



4 | 기능설명 [신분증]

신분증이란?

신분증 시스템은 분석된 파일을 이미지화 함으로써 유저가 쉽게 정보를 확인 할 수 있도록 기획되었다.
[AHPED 분석] 을 마친 모든 파일은 [AHPED 신분증] 이 부여된다. (*AHPED : AkdanHall PED로 실행 전 검사를 뜻합니다.)
해당 신분증 분류 및 정보는 다음과 같으며 신분증은 윈도우 및 분석 콘텍스트 메뉴에 표시된다.

안전파일



악성파일



AHPED 파일 콘텍스트 메뉴 표시



의심파일



미확인파일

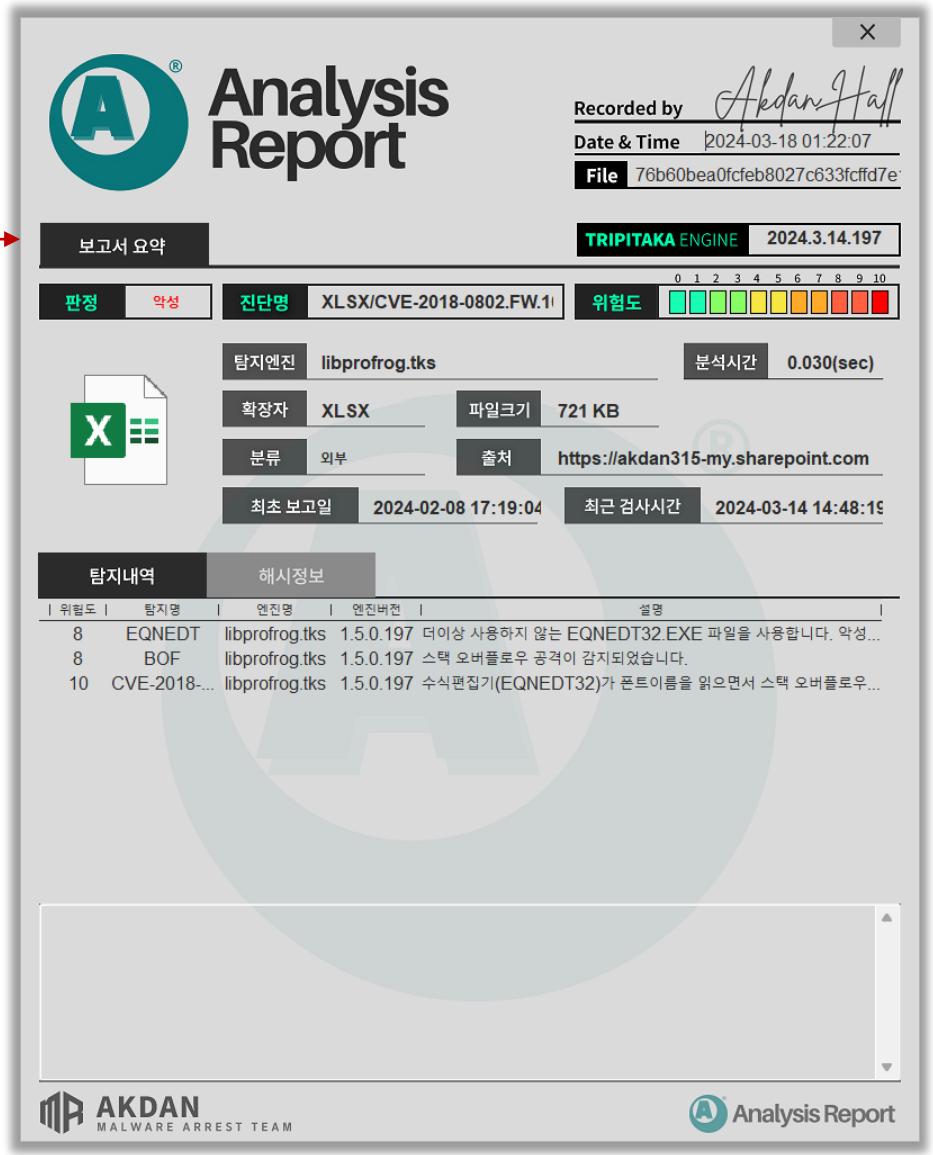


4 | 기능설명 [신분증]

분석 보고서

신분증 내에 분석 보기 버튼 클릭 시 상세 분석 리포트 창이 출력됩니다.





4 | 기능설명 [파일]

BTN **파일**

PC에서 불러온 문서파일을 검사 / 격리 / 삭제할 수 있습니다.

파일 분류

파일은 모든 문서, 주의 문서, 예외 문서로 분류됩니다.

BTN **모든 문서** PC에서 불러온 모든 문서파일을 볼 수 있습니다.

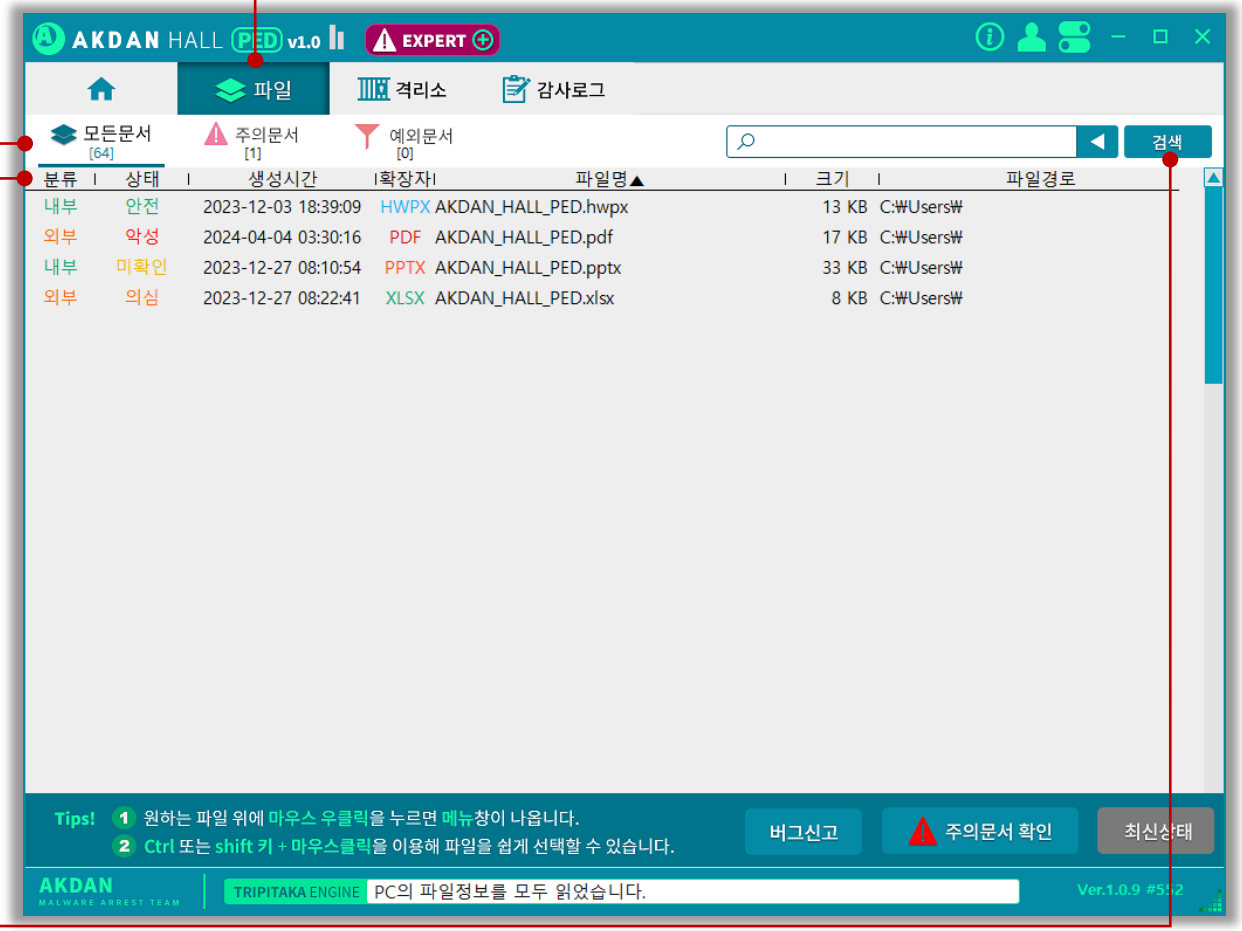
BTN **주의 문서** PC에서 탐지된 "외부 미확인 파일 or 의심 및 악성파일"을 볼 수 있습니다.

문서 속성

▶ **분류** | 파일이 외부에서 온 파일인지 직접 제작된 내부파일인지를 분류합니다.
▶ **상태** | 분석결과 및 검사여부에 따라 미확인/정상/의심/악성/에러로 분류됩니다.
▶ **생성시간** | 파일이 수정된 날짜 및 시간을 말합니다.
▶ **확장자** | 파일의 확장자명을 말합니다.
▶ **파일명** | 파일 이름을 말합니다.
▶ **크기** | 파일의 용량을 말합니다.
▶ **파일경로** | 파일이 위치한 경로를 말합니다.

검색어 기능

▶ **검색** | 파일명을 입력 후 검색버튼 클릭 시 입력한 파일이 출력됩니다.



파일 분류와 상태 설명

파일분류	외부	다른 사람이나 외부 조직으로부터 받은 파일 전자메일을 통해 수신한 첨부 파일, 공동 작업을 위해 공유 받은 문서, 다른 조직에서 제공한 자료 등이 해당될 수 있습니다.
	내부	본인 또는 해당 조직 내에서 직접 생성하거나 소유한 파일 개인 작업물, 회사 내 문서, 프로젝트 파일 등이 해당될 수 있습니다.
파일상태	악성	컴퓨터 시스템에 해를 가하는 목적으로 설계된 파일로, 악의적인 코드나 프로그램을 포함하고 있습니다. 즉시 격리 및 삭제 조치를 권장합니다.
	안전	악성 코드나 위협을 가지고 있지 않아 안전하게 사용 가능한 파일입니다.
	의심	악성성 여부가 명확하지 않지만, 일부 이상 징후를 보이는 파일입니다. 보안 소프트웨어가 경고를 발생시키거나 이상한 동작을 보일 때 해당 파일을 의심해야 합니다.
	미확인	아직 검사되지 않았거나 출처가 명확하지 않은 파일을 의미합니다. 보안을 위해 이러한 파일을 실행하거나 열기 전 검사를 권장합니다.
	에러	분석엔진에서 예측하지 못한 데이터를 가진 경우입니다. 오진신고를 통해 당사에 개선을 요청할 수 있습니다.

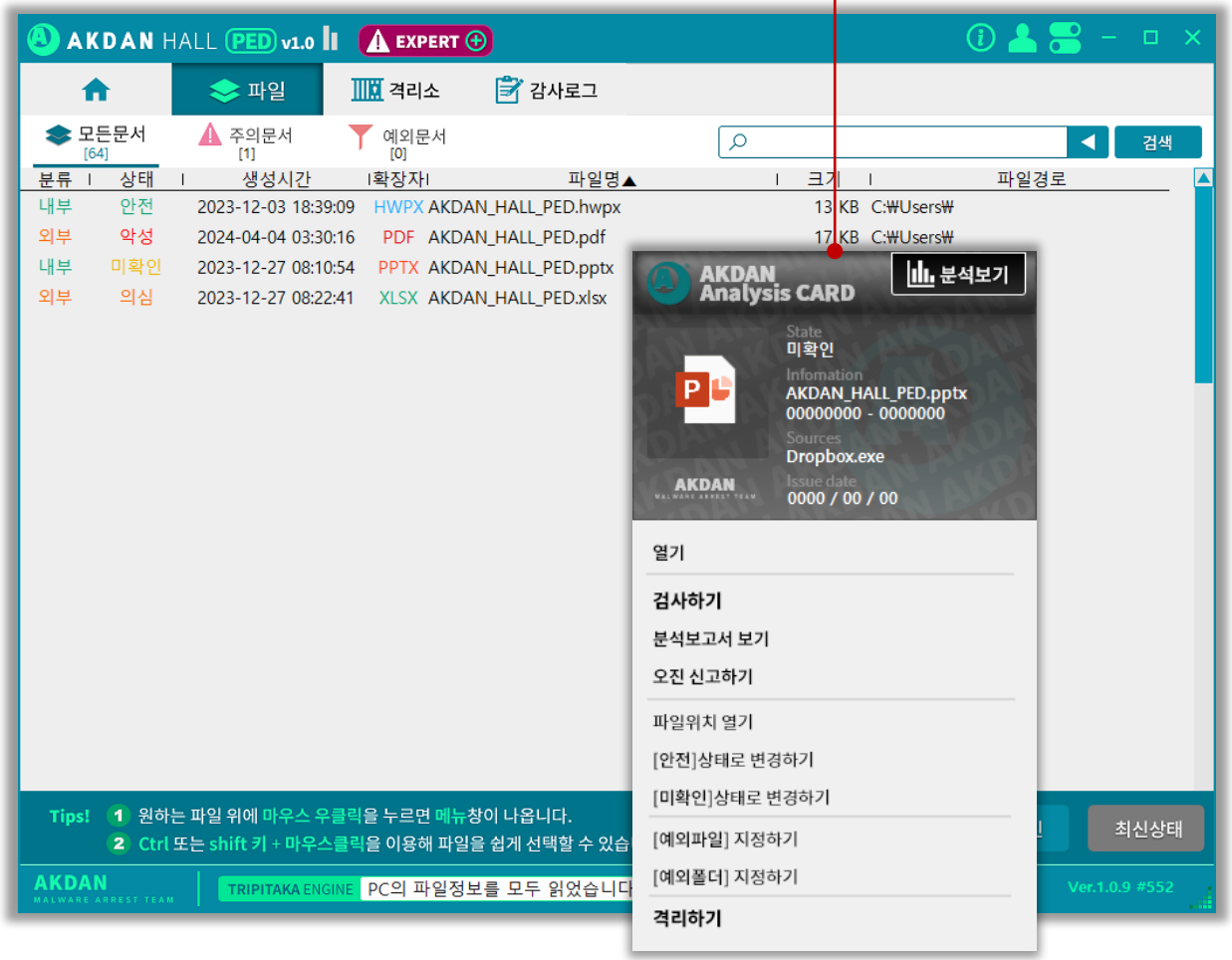
4 | 기능설명 [파일]

파일 콘텍스트 메뉴

선택된 파일에서 마우스 우클릭을 통해 메뉴창을 열 수 있습니다.
메뉴창에는 파일 분석검사 및 격리, 악성코드 조회의 기능을 이용 할 수 있습니다.

메뉴 구성

- ▶ **열기** | 파일을 실행합니다.
- ▶ **검사하기** | 파일의 악성여부를 실시간으로 검사합니다.
- ▶ **분석보기/분석보고서 보기** | 파일의 상세 분석 리포트 창이 출력됩니다.
- ▶ **오진 신고하기** | 파일정보가 포함된 데이터를 전송하여 오진을 신고할 수 있습니다.
- ▶ **파일위치 열기** | 파일이 저장된 장소를 엽니다.
- ▶ **[안전] 상태로 변경하기** | 파일을 안전파일로 변경합니다.
- ▶ **[미확인] 상태로 변경하기** | 파일을 미확인 상태로 복원합니다.
- ▶ **[예외파일] 지정하기** | 해당 파일을 검사 예외 파일로 지정합니다.
- ▶ **[예외폴더] 지정하기** | 해당 파일이 저장된 경로를 검사 예외 폴더로 지정합니다.
- ▶ **격리하기** | 파일을 격리에 분리시킵니다.



4 | 기능설명 [파일]

BTN **예외 문서** 사용자가 검사 예외 지정한 문서 파일 및 폴더를 볼 수 있으며, 경로 열기/예외 경로 추가/해제가 가능합니다.

문서 속성

▶ **등록시간** | 파일이나 폴더가 예외 지정된 시간을 말합니다.

▶ **구분** | 예외 지정된 형태를 말하며, 예외 파일은 확장자명, 예외 폴더는 디렉토리로 구분됩니다.

▶ **파일명** | 예외 지정된 파일 이름을 말합니다.

▶ **파일경로** | 예외 지정된 파일이 위치한 경로를 말합니다.

예외 문서 콘텍스트 메뉴

선택된 파일에서 마우스 우클릭을 통해 메뉴창을 열 수 있습니다.
메뉴창에는 경로 열기, 예외경로 해제하기, 예외경로 추가하기를 할 수 있습니다.
또한, 보드 위에서 우클릭 시 "예외경로 추가하기" 단일 기능 이용이 가능합니다.

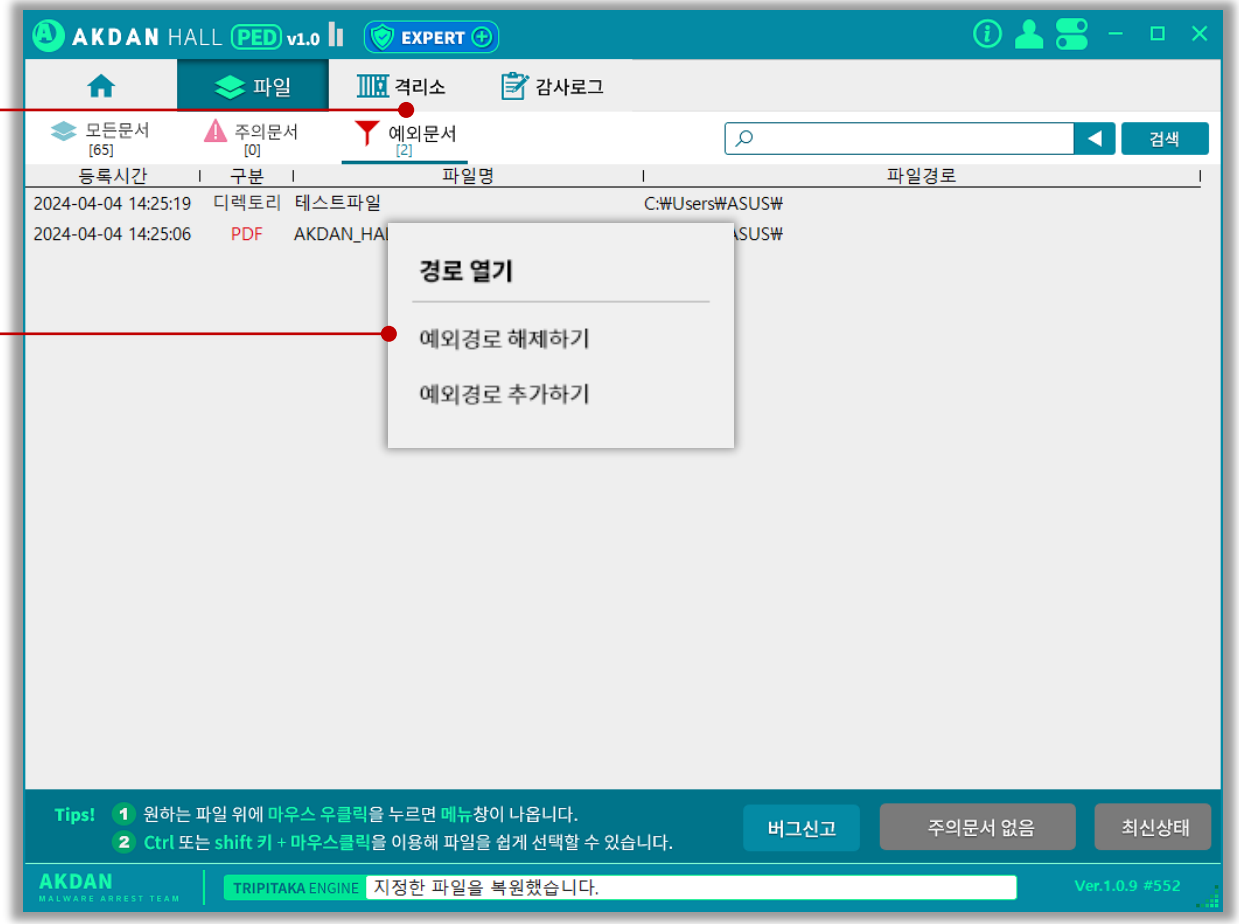
메뉴 속성

▶ **경로열기** | 예외 폴더나 예외 파일이 저장된 장소를 엽니다.

▶ **예외경로 해제하기** | 파일의 예외 경로를 해제합니다.
해제 시 예외경로에 해당되었던 문서파일은 분석결과값에 따라 "모든문서/주의문서" 탭으로 복원됩니다.

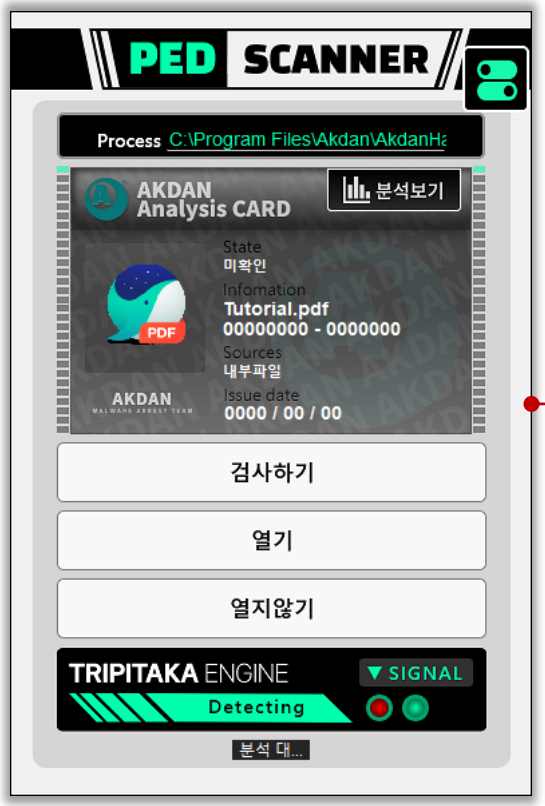
▶ **예외경로 추가하기** | 검사 예외 시키고자 하는 경로를 추가합니다.
예외 지정된 파일과 폴더는 "모든문서/주의문서"탭에서 사라집니다.

* 예외 파일 지정을 하여도 "모든문서/주의문서"탭에서만 사라질 뿐, 파일의 분석결과값은 사라지지 않습니다.



PED 메뉴

미확인 상태의 파일을 마우스 더블 클릭 시 PED 메뉴가 열립니다.
메뉴창에는 파일 상태에 따라 PED 메뉴 버튼이 변경되며, 검사하기, 열기, 분석보기, 격리하기 등이 가능합니다.



미확인 파일 PED 메뉴 구성

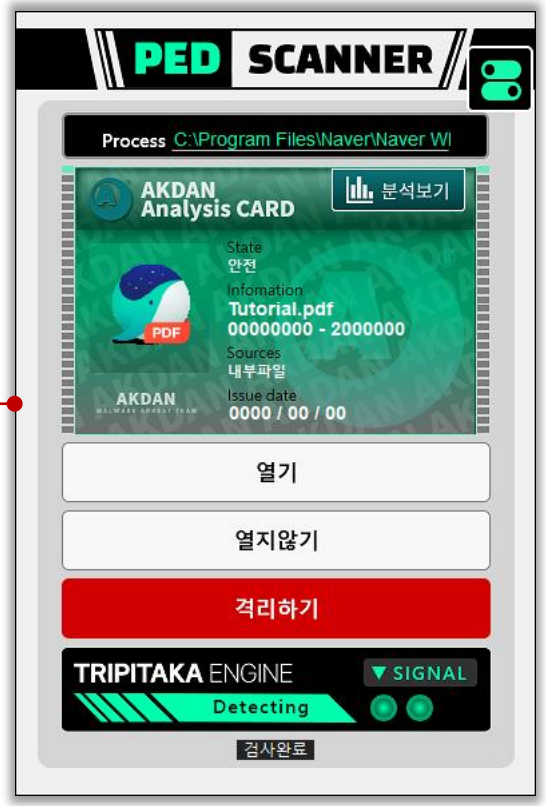
- ▶ **검사하기** | 파일의 악성여부를 실시간으로 검사합니다.
- ▶ **열기** | 파일을 실행합니다.
- ▶ **열지않기** | 파일을 실행시키지 않습니다.

안전 파일 PED 메뉴 구성

- ▶ **열기** | 파일을 실행합니다.
- ▶ **열지않기** | 파일을 실행시키지 않습니다.
- ▶ **격리하기** | 파일을 격리에 분리시킵니다.

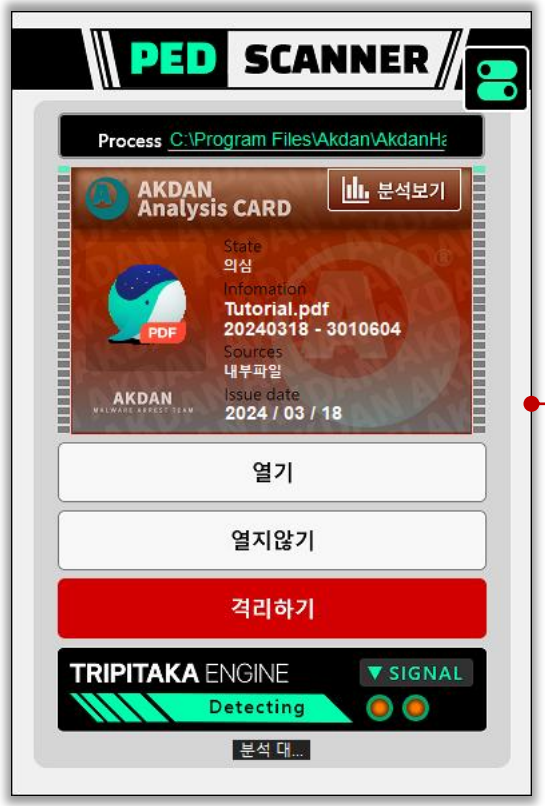
공 통 PED 메뉴 구성

- ▶ **분석보기** | 검사를 마친 해당 안전 파일에 대한 상세 분석 리포트 창이 출력됩니다.
- ▶ **항상 검사 후 열기** | 파일 실행 시 자동으로 PED 검사 후 실행하는 옵션입니다.
- ▶ **최상위 윈도우로 나타내기** | PED 창을 항상 위로 상단 고정하는 옵션입니다.



PED 메뉴

미확인 상태의 파일을 마우스 더블 클릭 시 PED 메뉴가 열립니다.
메뉴창에는 파일 상태에 따라 PED 메뉴 버튼이 변경되며, 검사하기, 열기, 분석보기, 격리하기 등이 가능합니다.

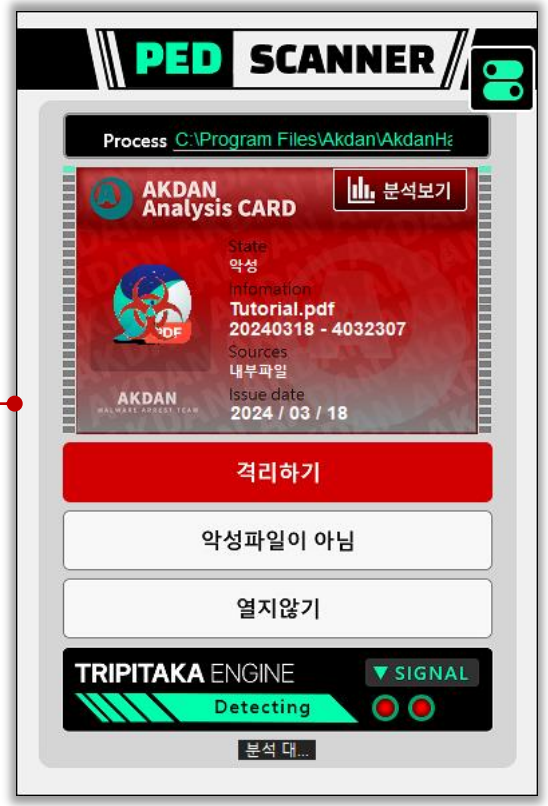


의심 파일 PED 메뉴 구성

- ▶ **열기** | 파일을 실행합니다.
- ▶ **열지않기** | 파일을 실행시키지 않습니다.
- ▶ **격리하기** | 파일을 격리에 분리시킵니다.

악성 파일 PED 메뉴 구성

- ▶ **격리하기** | 파일을 격리에 분리시킵니다.
- ▶ **악성파일이 아님** | 안전파일로 변경하며 오진 신고할 수 있는 창이 뜹니다.
- ▶ **열지않기** | 파일을 실행시키지 않습니다.



4 | 기능설명 [파일]

PED 메뉴

미확인 상태의 파일을 마우스 더블 클릭 시 PED 메뉴가 열립니다.
메뉴창에는 파일 상태에 따라 PED 메뉴 버튼이 변경되며, PED 검사 후 열기, 검사하기, 파일 상태 변경, 격리하기 등이 가능합니다.



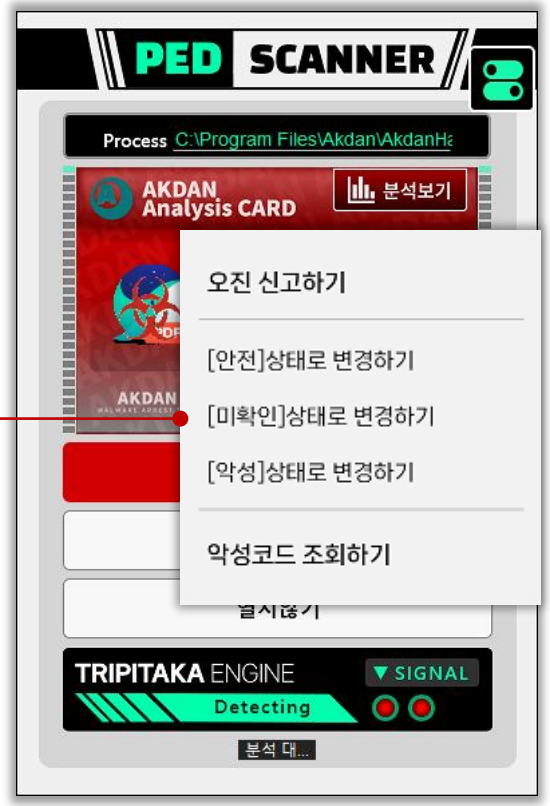
검사 중 화면

PED 검사하기를 누를 시 뜨는 화면으로, 적색램프와 청색램프가 번갈아 깜박입니다.

기 타 PED 콘텍스트 메뉴 구성

선택된 파일의 신분증을 마우스 우클릭 시 메뉴창을 열 수 있습니다.

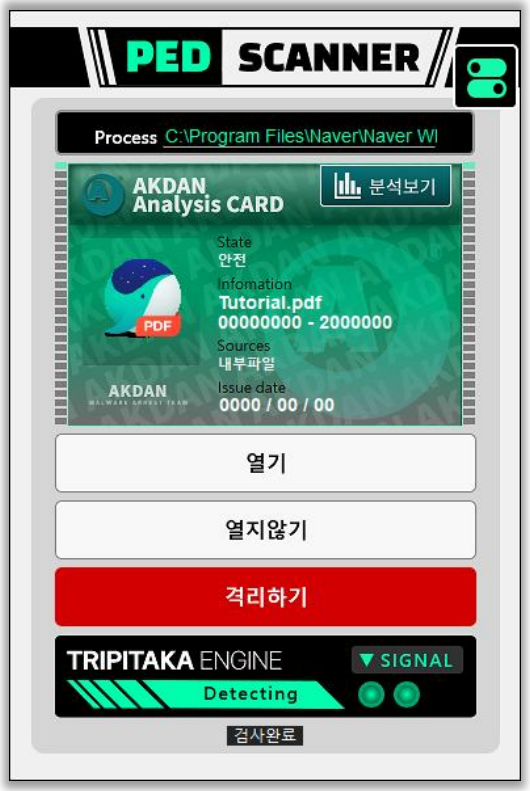
- ▶ **오진 신고하기** | 파일정보가 포함된 데이터를 전송하여 오진을 신고할 수 있습니다.
- ▶ **[안전] 상태로 변경하기** | 해당 파일을 안전파일로 변경합니다.
- ▶ **[미확인] 상태로 변경하기** | 해당 파일을 미확인 상태로 변경합니다.
- ▶ **[악성] 상태로 변경하기** | 해당 파일을 악성파일로 변경하며, 위험파일 탭에 분류됩니다.
- ▶ **악성코드 조회하기** | 파일의 악성코드 여부를 바이러스토탈 사이트를 통해 조회합니다.



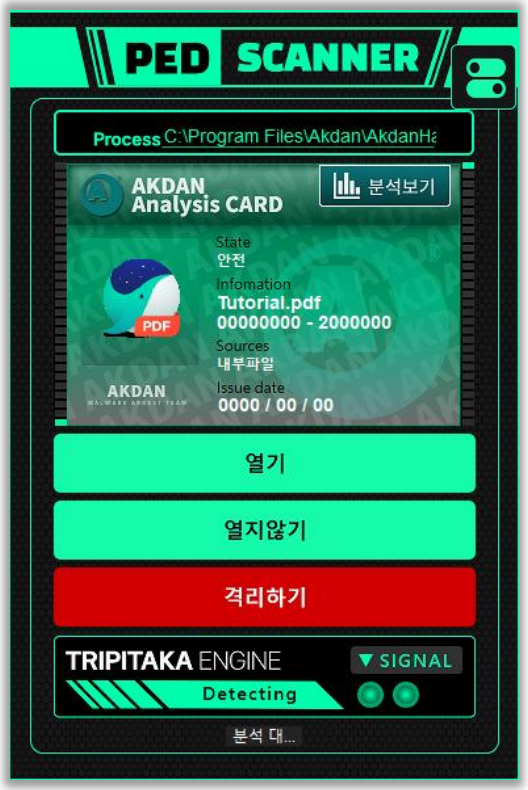
기 타 PED 점멸 표시등

			
안전파일	악성파일	의심파일	미확인/에러 파일 검사 중인 파일

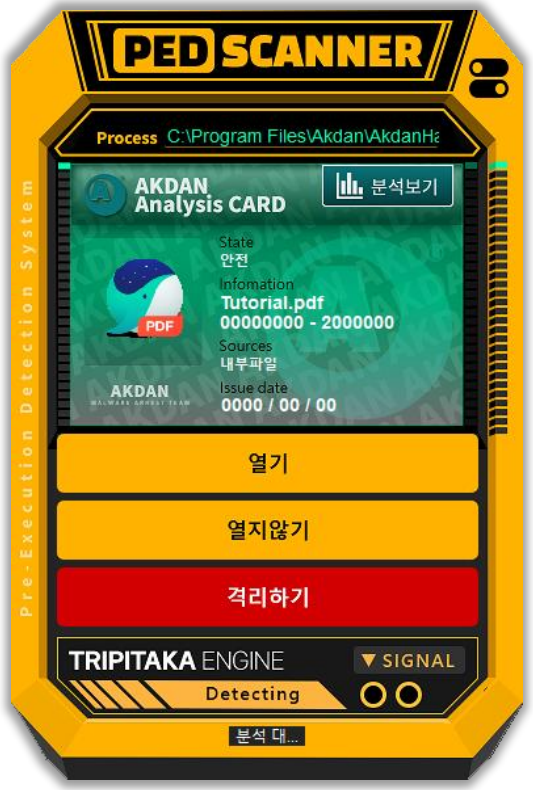
PED테마



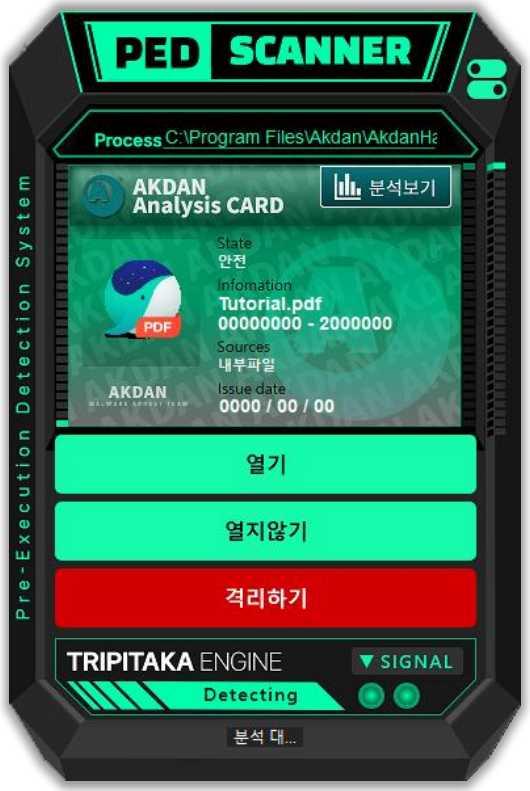
라이트심플 모드



다크심플 모드



옐로우 모드



다크 모드

BTN **격리소**

[검사 콘텍스트] 메뉴 중 [격리 시키기]를 눌러 격리 할 수 있습니다.
해당 화면도 [리스트박스]로 구성되어 있어 [검사]화면과 동일하게 파일선택 기능을 사용 할 수 있습니다.

격리소 속성

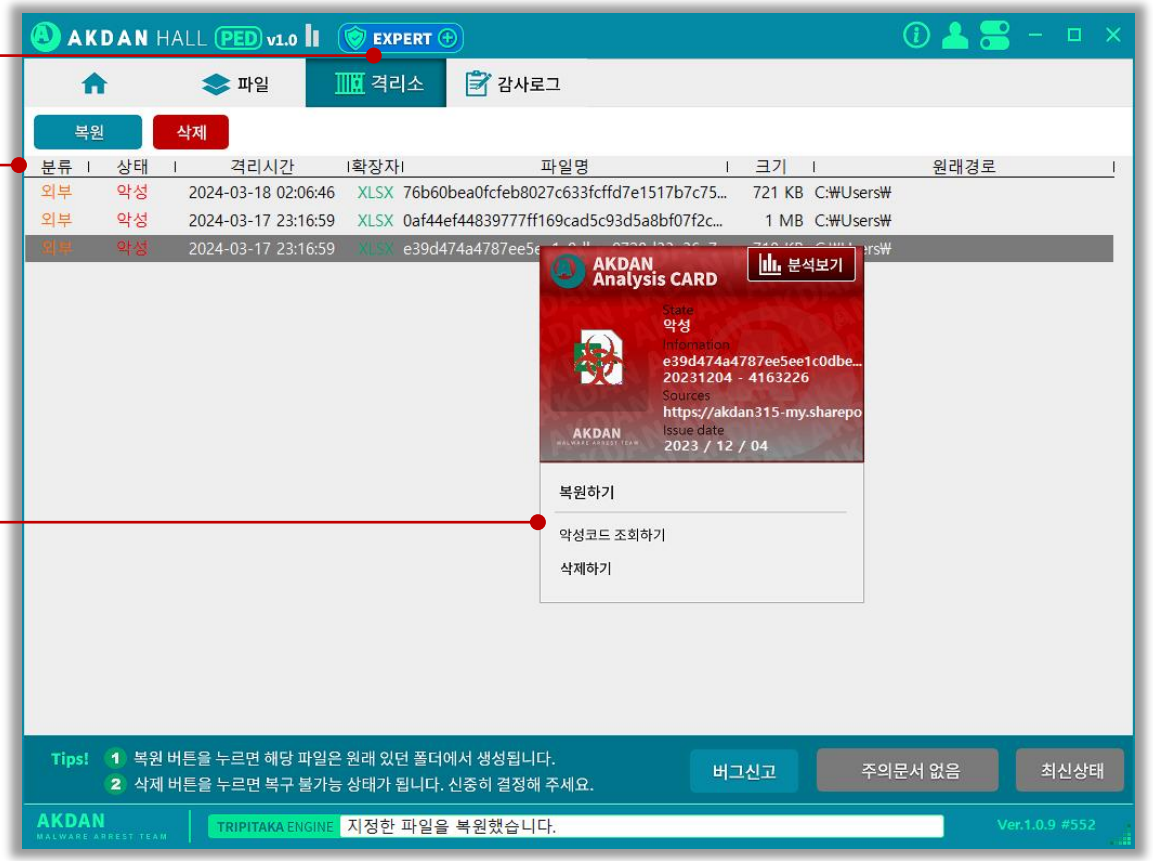
- ▶ **분류** | 파일이 외부에서 온 파일인지 직접 제작된 내부파일인지를 분류합니다.
- ▶ **상태** | 분석결과 및 검사여부에 따라 미확인/정상/의심/악성/에러로 분류됩니다.
- ▶ **격리시간** | 파일이 격리된 날짜 및 시간을 말합니다.
- ▶ **확장자** | 파일의 확장자명을 말합니다.
- ▶ **파일명** | 파일 이름을 말합니다.
- ▶ **크기** | 파일의 용량을 말합니다.
- ▶ **원래경로** | 파일이 본래 위치했던 경로를 말합니다.

격리소 콘텍스트 메뉴

격리된 파일을 처리하는 메뉴입니다.
격리관련 버튼기능을 보다 쉽게 처리 하도록 [콘텍스트 메뉴]로도 사용 할 수 있습니다.

메뉴 구성

- ▶ **분석보기** | 분석 보고서 버튼 클릭 시 상세 분석 리포트 창이 출력됩니다.
- ▶ **복원하기** | 선택된 파일을 [미확인] 파일로 복구시킵니다. 오진 혹은 실수로 격리된 파일을 복구할 수 있습니다.
- ▶ **악성코드 조회하기** | 파일의 악성코드 여부를 바이러스토탈 사이트를 통해 조회합니다.
- ▶ **삭제하기** | 선택된 파일을 AHPED, 윈도우에서 삭제합니다.



4 | 기능설명 [감사로그]

BTN **감사로그**

악단홀 시스템의 중요 내용들이 날짜 시간별로 등록됩니다.
원하는 날짜를 지정하여 로그 리스트 기간조회를 할 수 있습니다.

로그 분류

악단홀 중요 내용은 시스템 로그와 검사 로그로 분류됩니다.

BTN **시스템 로그** 악단홀에서 이루어지는 모든 작업 내용이 기록됩니다.

BTN **검사 로그** 검사 요청, 악성 및 의심 파일 탐지 기록을 볼 수 있습니다.

감사로그 구성

▶ **기록시간** | 검사나 격리 및 복원 등의 이벤트가 발생한 시간을 말합니다.

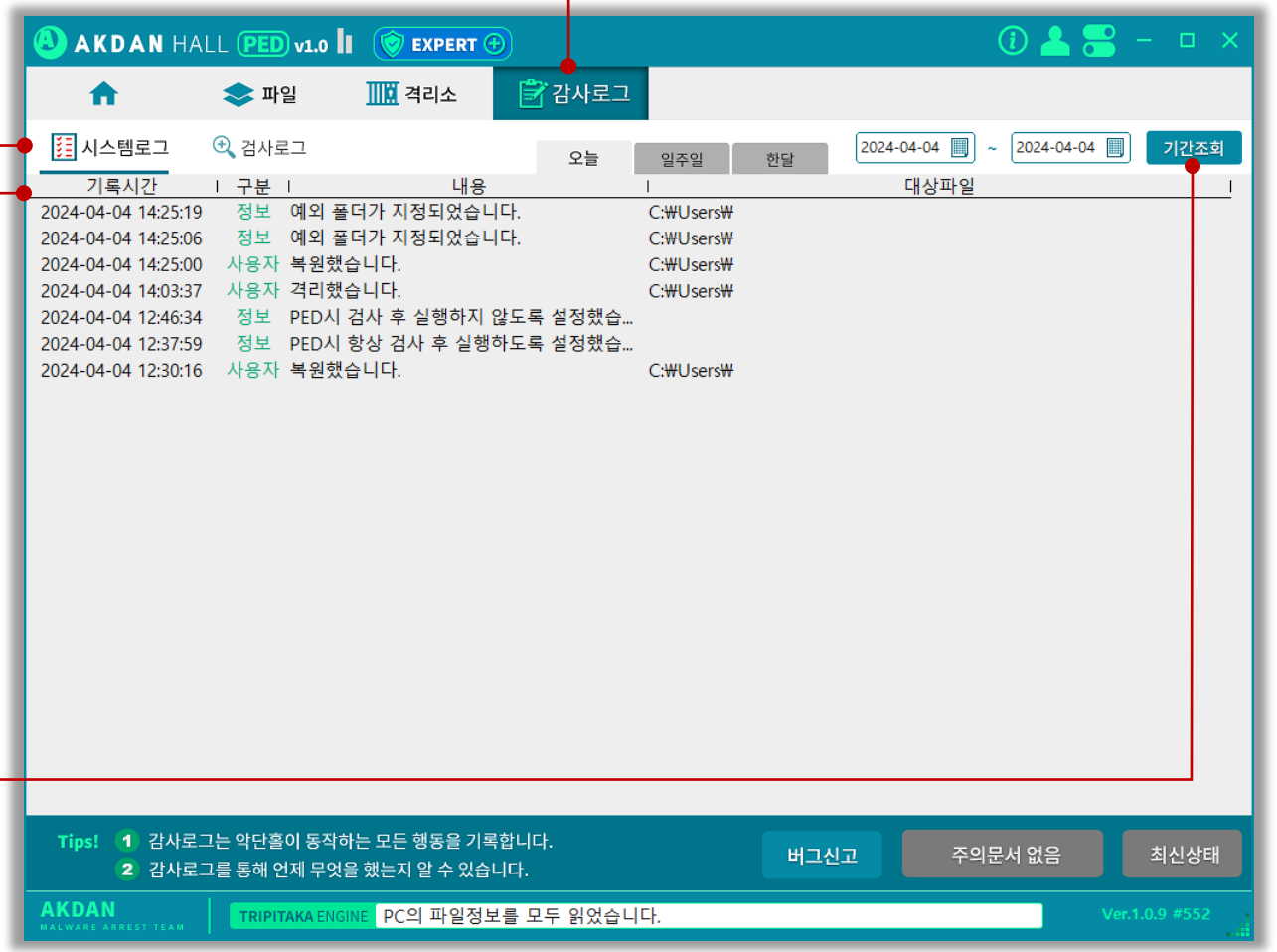
▶ **구분** | 해당 기록의 세부 분류를 말합니다.

▶ **내용** | 어떠한 이벤트가 수행되었는지 상세한 내용을 보여줍니다.

▶ **대상파일** | 대상 파일이 위치한 경로를 말합니다.

기간조회 기능

▶ **기간조회** | 접속 날을 기준으로 오늘, 일주일, 한 달 단위 또는 원하는 날짜를 지정하여 감사로그 리스트를 불러올 수 있습니다.



THE END

악성코드검거단 ㈜ https://www.akdan.co.kr/
연락처 : 031-698-4155 [상담시간] 평일 | 10:00 ~ 17:00 (점심시간 | 12:00 ~ 13:00, 토요일/공휴일 제외)
주소 : 13558 경기도 성남시 분당구 성남대로331번길 8 (정자동) 킨스타워 19층

도입문의: contact@akdan.co.kr
기술지원: support@akdan.co.kr