알약 개방형OS 1.1

-도움말-

ESTsecurity

목차

1. About 알약 개방형OS 1.1

기술/고객 지원 안내

우편번호 06711

주소 서울시 서초구 반포대로 3 이스트빌딩

홈페이지 http://www.estsecurity.com/

전화 1544-9744

구매/라이선스 문의

전화 1544-8209

홈페이지 http://www.estsecurity.com/buy/products

2. 알약 개방형OS 소개

2.1 제품 개요

점점 심각해지고 있는 운영체제의 라이선스 비용과 지원 종료 이슈로 많은 기업들이 개방형 OS 를 업무용 PC 의 운영체제로 선택하고 있습니다. 개방형 OS 와 같은 리눅스 기반 악성코드가 계속해서 증가하는 추세이지만, 개방형 OS 환경은 윈도우 PC 에 비해 상대적으로 보안솔루션이 잘 갖춰져 있지 않은 상황입니다.

2.2 제품 특장점

- 듀얼 엔진 탑재, 검증된 탐지력

듀얼 엔진으로 구성된 강력한 탐지율은 국제 보안 인증을 통해 세계적으로 인정받았습니다. 전세계에서 광범위하게 수집되는 해외 위협요소 DB 와 국내 최대 사용자를 기반으로 구축된 국내 위협요소 DB 를 바탕으로 전방위적인 악성코드 탐지, 치료가 가능합니다.

- 오탐지 최소화

오진의 위험을 최소화하기 위해 사용자에게 업데이트 되기 전 OS 및 주요 보안 프로그램, 범용프로그램들의 오진 여부를 확인하는 프로세스를 거쳐 업데이트를 진행하는 검증 시스템을 바탕으로 안전하고 검증된 DB 를 제공합니다.

- CUI, GUI 환경 모두 지원, 사용자 편의성 극대화

사용자 편의를 위해 터미널 명령 기반의 CUI 외에 GUI 기반의 웹 관리 인터페이스를 제공합니다. GUI 웹 관리 인터페이스를 통해 관리자 개인 PC 를 통해서 쉽고 빠른 사용이 가능합니다.

- 간편하고 쉬운 설치

install 형태로 제공되는 셋업은 초보자 CUI · GUI 상에서 손쉽게 설치할 수 있습니다.

- 검사 성능 조정 기능으로 시스템 리소스 최소화

검사 성능 조정 기능을 통해 개방형 OS 시스템의 리소스를 최적으로 활용하며,
저사양 PC 에서도 제품 사용이 가능합니다.

- 실시간 감시 기능을 통한 빈틈없는 방어 체계 구축

실시간으로 감시하여 바이러스 및 악성코드 등에 노출되는 위협을 사전에 차단/처리합니다.

2.3 설치 환경

알약 개방형 OS 1.1 사용을 위한 시스템 권장 사양은 다음과 같습니다.

구분		지원 범위
OS		HamoniKR 4.0, 5.0, 6.0, 7.0 구름O OS – 2.0, 3.0, 4.0 한컴구름 – 3.0 Tmax구름 - 21
CPU	최소	500 Mhz 이상
	권장	2.0 Ghz 이상
RAM	최소	512MB 이상
	권장	1GB 이상
HDD	최소	1.2GB 이상
	권장	2GB 이상

※ OS별 상세 지원 버전은 별도의 상담을 통해 확인하실 수 있습니다.

3. 설치 및 사용

3.1 설치/실행/제거

1) 설치

- 설치 파일을 설치할 PC 에 복사 후, root 권한으로 다음 명령어를 실행합니다.

```
# ./alyac-1.1.00.00000-x86_64.install
```

- 설치파일의 실행 권한이 없을 경우, root 권한으로 chmod 명령어 실행하여 권한을 수정합니다.

```
# chmod 755 alyac-1.1.00.00000-x86_64.install
```

- 추가 패키지 설치를 위해 y/n 을 물어볼 시에는 모두 y 로 진행합니다.
- 단독형 (OLD) 버전의 경우 설치 시 옵션을 설정하면 부팅 시 자동 실행 기능을 끌 수 있습니다.

```
.# /alyac-1.1.00.00000-x86_64.install -- -r off
```

※알약이 사용자의 홈 디렉터리(/home 하위 디렉터리)에 설치될 경우, OS 보안 설정에 따라 기능이 제한될 수 있으므로, 홈 디렉터리 설치를 권장하지 않습니다.

2) 실행/종료/재시작

- 다음 명령으로 알약 서비스를 실행/종료/재시작 합니다

.

① 서비스 실행

```
# service alyac start
```

② 서비스 종료

```
# service alyac stop
```

③ 서비스 재시작

```
# service alyac restart
```

3) 삭제

- 알약이 설치된 디렉터리에서 다음 명령어를 실행하여 알약을 삭제합니다.

```
# ./uninstall.sh
```

- 디폴트로 설치되는 디렉터리의 위치는 /usr/local/ALYac 입니다.

3.2 사용

1) 웹 UI 를 이용한 알약 사용

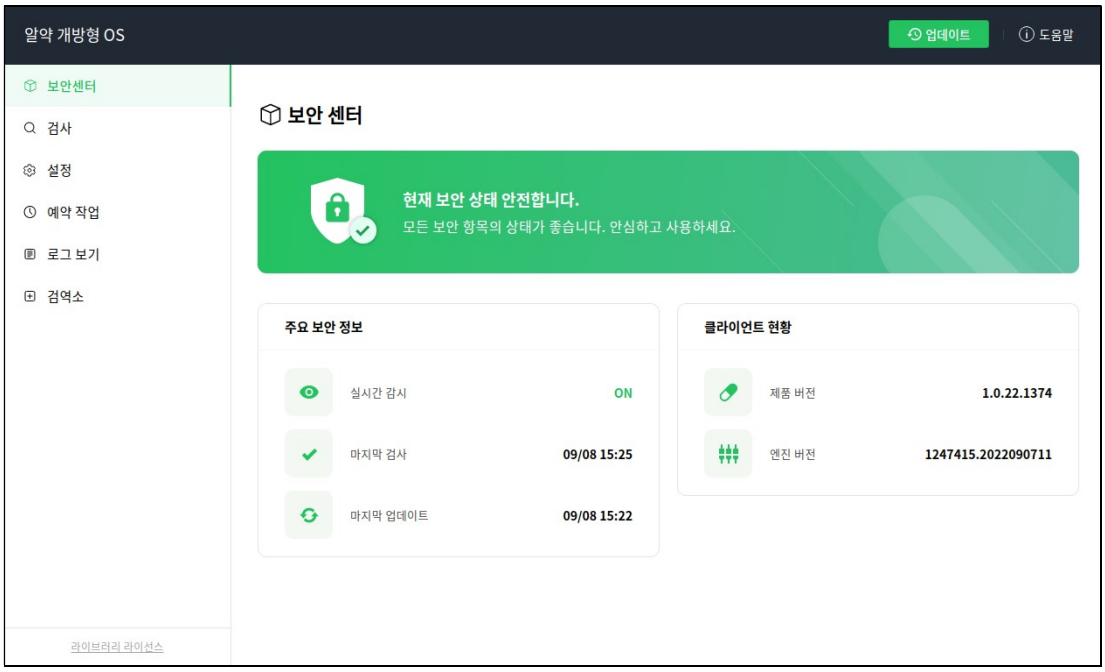
- 시작 메뉴, 트레이 아이콘을 이용해 알약을 실행하거나, 웹 브라우저에서 접속 URL 을 입력하면 웹 UI 를 사용할 수 있습니다.

[접속 URL]

http://127.0.0.1:24237/

2) 알약 웹 UI

- 알약 개방형 OS 의 웹 UI 는 아래와 같이 구성되어 있습니다.



[웹 UI 기능 요약]

- **보안 센터** : PC 의 안전 상태, 주요 보안 상태 정보와 클라이언트 현황을 확인할 수 있습니다.
- **검사** : PC 의 원하는 영역이나 파일에 대해, 검사를 실행할 수 있습니다.
- **설정** : 실시간 감시, 검사 등 알약 동작에 대한 상세 옵션을 설정할 수 있습니다.
- **예약 작업** : 검사나 업데이트의 예약을 설정할 수 있습니다.
- **로그 보기** : 알약에서 발생하는 로그들을 확인할 수 있습니다.
- **검역소** : 격리된 악성 파일들을 확인하고 관리할 수 있습니다.

• **업데이트** : 알약에 대한 수동 업데이트를 진행할 수 있습니다.
• **도움말** : 알약 사용법에 대한 가이드를 확인할 수 있습니다.

[보안 센터 상세]

• 웹 UI 에서는 알약의 보안 상태와 클라이언트 현황에 대한 정보를 제공합니다.
• 보안 센터 기능

[보안 센터 정보]
• 안전 상태 표시 배너
• 주요 보안 정보
• 클라이언트 현황

[안전 상태 종류 및 기준]
• 안전 상태 종류 : 안전/위험
• 안전 상태 위험 기준
  ○ 실시간 감시 off
  ○ 마지막 검사 15 일 경과
  ○ 마지막 업데이트 7 일 경과

[설정 상세]

• 웹 UI [설정] 탭에서는 업데이트/실시간 감시/검사/저장소/탐지 제외에 대한 옵션을 설정할 수 있습니다.
• 원하는 옵션을 설정 후, 우측 하단의 [저장] 버튼을 클릭하여, 제품에 옵션을 적용할 수 있습니다.
• [기본값으로 재설정] 버튼을 클릭 시, 모든 [설정] 탭 내 옵션을 제품 기본값으로 되돌릴 수 있습니다.

4. 서버 연동 및 라이선스 등록

4.1 서버 연동(연동형 제품)

1) 서버 연동

① root 권한으로 다음 명령어를 이용하여 서버 설정을 진행합니다.

```
# ALYac license -s
```

② 변경할지 여부를 묻는 질문에서, 'Y'를 입력하여 서버 정보 변경을 진행합니다.

③ 관리 서버 정보를 입력하고 설정을 마칩니다.

2) 사용자 정보 연동

① 다음 명령어로 사용자 정보 설정을 진행합니다.

```
# ALYac license -u
```

② 변경할지 여부를 묻는 질문에서, 'Y'를 입력하여 서버 정보 변경을 진행합니다.

③ 사용자 정보와 부서 정보를 입력하고 설정을 마칩니다.

4.2 라이선스 등록(단독형 제품)

1) 라이선스 등록

① 다음 명령어로 라이선스 등록을 진행합니다.

```
# ALYac license -r
```

② 'Y'를 입력 후 라이선스 등록을 진행합니다.

5. 검사/치료

5.1 검사/치료

1) 터미널 환경

※명령 실행 전 터미널 크기를 확인해주시기 바랍니다. 최소 터미널 크기보다 작을 경우, 검사 창이 깨져 보일 수 있습니다.

최소 터미널 크기: 70(열) x 24(행)
권장 터미널 크기: 80(열) x 24(행) 이상

- 다음 명령어로 검사 환경을 살펴봅니다.

```
# ALYac scan
```

[검사 옵션]

- **옵션 없음** : 악성 파일 탐지 시 치료 여부 (y/n)으로 나타냅니다.
- **-so** : 스캔만 하며 파일이 악성으로 탐지되면 보여주기만 합니다.
- **-ac** : 스캔 후 파일이 악성으로 탐지되면 자동 치료 합니다.
- **-meta** : 터미널 UI 없이 스캔 한 파일의 절대경로와 악성 여부를 나타냅니다.
- **-config** : 검사 시 옵션을 설정합니다.
- **-meta-do** : meta 옵션에서 악성으로 탐지된 파일만 나타냅니다.

[실행 예시]

- 악성 파일 탐지 시 치료 여부 확인.

```
# ALYac scan /home
```

- 스캔만 진행(치료 하지 않음)

```
# ALYac scan -so /home
```

- 악성 파일 탐지 시 자동 치료

```
# ALYac scan -ac /home
```

2) 웹 UI 환경

- [검사] 탭을 선택합니다.
- 목록에서 검사 대상을 선택한 후, [검사 시작] 버튼을 클릭하여 검사를 진행할 수 있습니다.
- 검사를 시작하면 검사 창이 발생하며, 진행 상황과 탐지된 악성코드를 확인할 수 있습니다.
- 탐지된 악성코드는 검사 종료 후, [탐지 항목 치료] 버튼을 선택하여 치료 할 수 있습니다.

5.2 검사 및 저장소 설정

1) 터미널 환경

- 아래 명령어를 실행하여, 원하는 검사 설정을 진행합니다.

```
# ALYac scan -config
```

[검사 설정]

• Memory Usage : 메모리 사용 수준을 관리하는 옵션으로, 프로세스 전체 메모리를 관리하지는 않습니다.
메모리 사용 수준은 LOW/MEDIUM/HIGH 중 선택할 수 있습니다

• Scan Level : 검사 레벨

- SIMPLE : 검사 속도가 가장 빠른 검사 옵션입니다.
- NORMAL : Simple 검사에서 스크립트 스캐너를 추가한 옵션으로, 파일 패턴으로도 탐지합니다.
- DEEP : Normal 검사에서 휴리스틱 검사를 추가한 옵션입니다.

• Max Scan Size : 입력한 값을 초과하는 파일은 검사하지 않습니다.

• Use Tera Engine : 테라엔진 사용 여부를 설정합니다.
※테라 엔진(Tera Engine) : 자체 개발 엔진으로 알약에서 기본적으로 사용하는 엔진입니다.

• Use CPU QOS Level : 수동 검사 시 ALYac 프로세스의 CPU 점유율 정도를 선택할 수 있습니다.

• Use NFS Scan: 검사 시, NFS 영역의 검사 여부를 설정할 수 있습니다.

2) 웹 환경

- [설정] 탭을 선택합니다.
- [검사]와 [저장소] 하위의 옵션들 중 원하는 옵션을 설정합니다.

[검사 설정(공통)]

- **메모리 사용:** 메모리 사용수준을 관리하는 옵션으로, 프로세스 전체 메모리를 관리하지는 않습니다. 메모리 사용 수준은 LOW/MEDIUM/HIGH 중 선택할 수 있습니다.
- **검사 수준**
  - **빠른 검사 :** 검사 속도가 가장 빠른 검사 옵션입니다.
  - **기본 검사 :** 빠른 검사에서 스크립트 스캐너를 추가한 옵션으로, 파일 패턴으로도 탐지합니다.
  - **정밀 검사 :** 기본 검사에서 휴리스틱 검사를 추가한 옵션입니다.
- **테라 엔진 사용 :** 테라엔진 사용 여부를 설정

※ 테라엔진(Tera Engine) : 자체 개발 엔진으로 알약에서 기본적으로 사용하는 엔진입니다.

- **최대 검사 용량 :** 입력한 값을 초과하는 파일은 검사하지 않습니다.
- **CPU 사용** : 검사 시, CPU 사용 수준을 설정합니다.
- **NFS 검사** : NFS로 연결된 영역의 검사 여부를 설정할 수 있습니다.

[저장소 설정(단독형 제품)]

- **로그 저장 기간**: 로그 파일의 저장 기간을 설정합니다.
  - 1개월/3개월/6개월/12개월 선택 가능
  - 로그 저장소 위치 : /usr/local/ESTsoft/ALYac/log

- **검역소 저장 기간** : 검역소 파일의 저장 기간을 설정합니다.
  - 1개월/3개월/6개월/12개월 선택 가능
  - 검역소 파일(탐지파일) 저장소 위치 : /usr/local/ESTsoft/ALYac/data/quarantine/data
  - 검역소 파일에 대한 정보 위치 : /usr/local/ESTsoft/ALYac/data/quarantine/info

3) 추가 : 터미널 환경 파일 사이즈를 통한 검사 대상 제한

[기능 사용]

① ALYac scan -config 를 입력하면 검사 옵션을 제공합니다.
② 방향키로 Max Scan Size 메뉴를 선택합니다.
③ 방향키로 파일 크기 제한 값을 입력합니다.

- Unlimited : 제한 없이 모든 사이즈의 파일 검사
- 1B 이상 : 입력 값을 초과하는 파일 모두 검사 안 함

④ c 를 입력하면, 직접 값을 입력할 수 있습니다.

- Set Value (ex: 100kb, 100mb, Unlimited...)

⑤ Enter 를 입력해 값을 저장하면, 입력한 값이 최대 검사 크기 옵션에 적용됩니다.

6. 실시간 감시

6.1 실시간 감시

1) 터미널 환경

- 아래 명령어로 실시간 감시를 설정할 수 있습니다.

```
# ALYac realtime
```

[실시간 감시 설정 옵션]

- -c : 실시간 감시 기능 활성화 여부를 설정합니다.
- -ac : 실시간 감시 중 탐지 시 자동 치료 여부를 설정합니다.
- -d : 실시간 감시를 할 범위를 설정합니다.
- -e : 실시간 감시에서 제외할 대상을 설정합니다.
- -m : 실시간 감시 동작 모드를 설정합니다.
  ▶ Performance-focused: 서버 성능을 최우선으로 동작하며, I/O 가 많은 시스템에서 적합한 방식입니다.
  ▶ Balanced: 서버 성능과 보안의 균형을 맞춰 동작하며, 'Performance-focused' 옵션보다 리소스 사용량이 증가할 수 있습니다.
- -s : 실시간 감시 설정 상태를 확인합니다.
- -v: 실시간 감시 모듈의 버전을 확인합니다.
- -h : 실시간 감시 모듈의 도움말을 확인합니다.

[감시할 디렉터리 설정 상세]

- 아래 명령어를 통해 실시간으로 감시할 디렉터리 영역을 설정할 수 있습니다.

```
# ALYac realtime -d
```

- 명령어 실행 시, 순서에 따라 아래와 같은 선택 옵션으로 설정을 진행할 수 있습니다.

- [a] : 전체 디렉터리 감시
- [s] : 특정 디렉터리 감시 (권장)

  [s 옵션 선택 시 추가 옵션]

  ○ [ad] : 감시할 디렉터리 추가 (경로를 나타내는 /를 앞에 반드시 입력)
  ○ [rd] : 설정된 디렉터리 리스트에서 제거
  ○ [sd] : 디렉터리 리스트 보기
  ○ [q] : 저장 후 종료

[감시에서 제외할 디렉터리 설정 상세]

- 아래 명령어를 이용해, 실시간 감시에서 예외처리 할 디렉터리 영역을 설정할 수 있습니다.

```
# ALYac realtime -e
```

- 명령어 실행 시, 아래와 같은 옵션을 선택할 수 있습니다.

- [ad] : 예외 처리 할 디렉터리 추가 (경로를 나타내는 /를 앞에 반드시 입력)
- [rd] : 예외처리 된 디렉터리 리스트에서 제거
- [sd] : 예외처리 된 디렉터리 확인
- [q] : 저장 후 종료

2) 웹 환경

- [설정] 탭을 누른 후, 하위의 [실시간 감시] 항목에서 관련 기능들을 설정할 수 있습니다.
- 설정 후, 우측 하단의 저장 버튼을 클릭해 변경된 설정 값을 저장합니다.

[상세 옵션]

- **실시간 감시 설정**: 실시간 감시 옵션을 설정할 수 있습니다.
- **동작 방식**:: 실시간 감시 모듈의 동작 방식을 설정할 수 있습니다.
  ▶ **성능 우선**: 서버 성능을 최우선으로 동작하며, I/O 가 많은 시스템에서 적합한 방식입니다.
  ▶ **균형**: 서버 성능과 보안 수준의 균형을 맞춰 동작하며, '성능 우선' 옵션보다 리소스 사용량이 증가할 수 있습니다.
- **치료 설정**: 탐지된 항목의 자동 치료 여부를 설정할 수 있습니다.
- **검사 설정**: 감시할 영역을 설정하고 감시에서 제외된 항목을 확인 할 수 있습니다.
  ▶ **특정 디렉터리 추가**: /디렉터리명/ 을 입력 후, Add 버튼을 클릭하면 리스트에 추가됩니다.
  ▶ **특정 디렉터리 항목 삭제**: 디렉터리 항목 선택 후, Remove 버튼을 클릭해서 리스트에서 삭제합니다.

7. 검역소/예약

검역소 기능이란?

- 알약으로 치료했던 위험요소(바이러스/악성코드)를 항목별로 안전하게 격리하여 보관하는 곳입니다.

7.1 검역소

1) 터미널 환경에서 검역소 설정하기

- 다음 명령어로 검사하게 되면 검역소 기능을 실행할 수 있습니다.

```
# ALYac quarantine
```

[검역소 옵션]

- **옵션 없음** : -l 옵션과 동일한 기능을 제공합니다.
- yy-mm-dd : 특정 날짜의 항목이 나타납니다.
- **-l** : 저장된 날짜의 리스트가 나타납니다.
- **-da** : 모든 검역소 항목을 삭제합니다.
- **-d** *'ARG'*: 특정 검역소 항목을 삭제합니다.
- **-r** *'ARG'*: 특정 검역소 항목을 복구합니다.

2) 웹 환경에서 검역소 설정하기

① [검역소] 탭을 누르면 탐지 후 검역소에 보관된 항목을 확인할 수 있습니다.

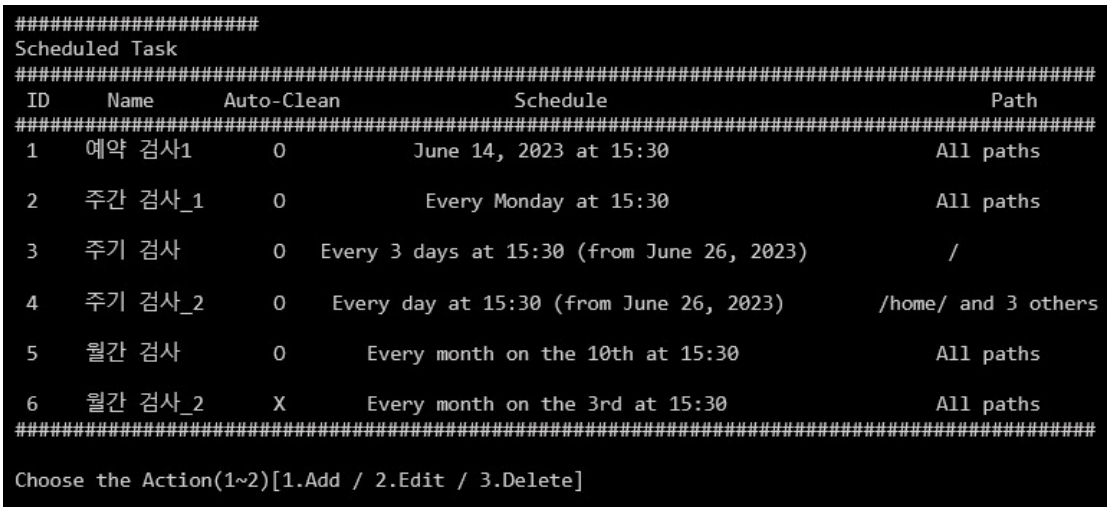
② [삭제] / [모든 항목 삭제] / [복구] 버튼
- [삭제] : 선택한 검역소 항목을 삭제합니다.
- [모든 항목 삭제] : 모든 검역소 항목을 삭제합니다.
- [복구] : 선택한 검역소 항목을 원래 위치로 복구합니다.

7.2 예약 작업

1) 터미널 환경(예약 검사만 지원)

① 다음 명령어로 예약 검사를 관리할 수 있습니다.

```
# ALYac scan -s
```



- ID : 작업의 ID 를 나타내며, 작업 생성 시 자동으로 등록됩니다.
- Name : 작업명을 나타내며, 입력하지 않을 시 공백으로 나타납니다.
- Auto-Clean : 스캔 후, 자동 치료 여부를 나타냅니다.
- Schedule : 검사 스케줄을 나타내며, 검사 진행 날짜 혹은 주기와 시간을 나타냅니다.
- Path : 예약 검사 대상 경로를 나타냅니다.

② 1 을 입력하면, 예약 검사를 아래 순서에 따라 등록할 수 있습니다.

[예약 검사 등록]

① Name
- 예약 작업의 작업명을 입력
- 사용하지 않을 시, 공백으로 진행

② Auto-Clean
- 검사 후 탐지된 악성코드 자동 치료 여부 선택 (y/n)

③ Schedule
- 반복 없음 및 주별, 월별, 특정 일자 간격으로 반복 검사를 설정

④ Path
- 검사 대상 경로 설정
- 여러 경로 설정 시 콤마(,)로 구분
- 빈 값으로 입력 시, 전체 경로 대상으로 검사 진행

⑤ NFS Scan
- NFS 영역의 검사 여부를 설정

③ 2 를 입력하면, 예약 검사 리스트의 ID 를 입력하고, 이미 설정된 속성을 선택하여 수정할 수 있습니다.

[예약 검사 변경]

① Name
- 예약 작업의 작업명을 수정

② Auto-Clean
- 검사 후 탐지된 악성코드 자동 치료 여부 변경

③ Schedule
- 반복 검사 스케줄을 변경

④ Path
- 검사 대상 경로 변경
- 여러 경로 설정 시 콤마(,)로 구분
- 빈 값으로 입력 시, 전체 경로 대상으로 검사 진행

⑤ NFS Scan
- NFS 영역의 검사 여부를 변경

④ 3 을 입력하면, 예약 검사 리스트의 ID 를 이용하여 예약 검사를 삭제할 수 있습니다.

2) 웹 환경

- [예약 작업] 탭을 선택하면 예약 검사와 예약 업데이트 기능을 이용할 수 있습니다.
- 예약 작업 캘린더에서는 등록된 예약 작업 일정을 달력 형태로 확인할 수 있습니다.
- 예약 작업 리스트에서는 예약 작업을 등록, 수정, 삭제할 수 있습니다.

[예약 작업 추가/수정]

- **작업명 :** 예약 작업의 작업명을 설정할 수 있습니다.
- **작업 종류** : 검사/검사 후 치료/업데이트 3 가지 작업 중 하나를 선택할 수 있습니다.
- **반복 설정/작업 설정** : 원하는 일정에 따라 작업이 진행 혹은 반복되도록 설정할 수 있습니다.
- **검사 경로** : 검사/검사 후 치료의 경우, 원하는 경로를 지정하여 검사를 진행할 수 있습니다.
- **NFS 검사 :** NFS 영역의 검사 여부를 설정할 수 있습니다.

8. 탐지제외/업데이트

8.1 탐지제외

- 탐지 제외된 항목은 위험요소(바이러스, 악성코드)를 포함하고 있어도 탐지하지 않습니다.

1) 터미널 환경

① 아래 명령어를 입력하여, 탐지제외 항목으로 진입합니다.

```
# ALYac exclude
```

② A(add)를 입력하면, 탐지제외 항목이 제공됩니다.

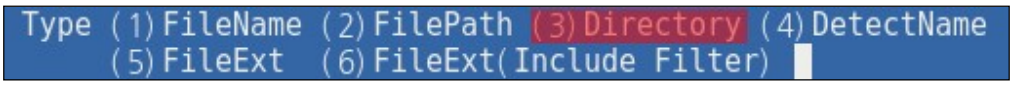
- FileName : 파일명에 지정한 내용이 포함되어 있으면 탐지 제외합니다.
- FilePath : 지정한 경로는 탐지 제외합니다.
- Directory* : 지정한 디렉터리는 탐지 제외합니다.
- DetectName : 지정한 탐지명은 탐지 제외합니다.
- FileExt* : 지정한 확장자의 탐지 제외합니다.
- FileExt(Include Filter)* : 지정한 확장자만 탐지합니다. (다른 파일은 모두 검사 안 함)

※ 별표(*)는 1.0.9.0 이상의 버전에서만 지원됩니다.

[항목별 사용법]

① Directory

- 탐지제외 유형에서 3번을 선택합니다.



- 선택 시, 탐지 제외할 디렉터리 입력 화면이 제공됩니다.

[설정 예시]

- 예외 대상으로 /data/verified* / 를 추가 시

  - /data/verified 로 시작되는 이름의 디렉터리 경로는 모두 검사하지 않습니다.
  - 예) /data/verifiedmail, /data/verifiedsetup 를 검사하지 않음

- 예외 대상으로 /sa?ple 를 추가 시

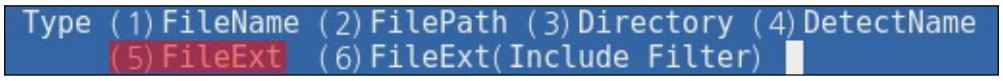
  - ?에 해당하는 한 글자는 달라도 앞뒤 키워드가 같다면 검사하지 않습니다.
  - 예) /sample, /sanple, /saaple 등을 모두 검사하지 않음

- 예외대상으로 /t+mp 를 추가 시

- +에 해당되는 한 개 이상의 글자가 달라도, 앞뒤 키워드가 같다면 검사하지 않습니다.
- 예) /temp, /tamp, /teeeemp, /tafwfwf23wngnmp 등을 모두 검사하지 않음

② FileExt

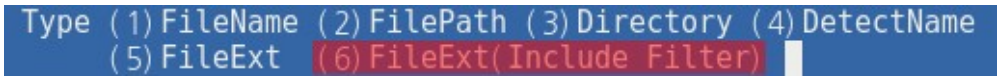
- 탐지제외 유형에서 5 번을 선택합니다.



- 선택 시, 탐지 제외할 확장자 입력 화면이 제공됩니다.
- 탐지 제외 확장자가 등록되면, 리스트에 추가됩니다.

③ FileExt(Include Filter)

- 탐지제외 유형에서 6 번을 선택합니다.



- 탐지 대상에 포함할 확장자 입력 화면이 제공됩니다.
- 탐지할 확장자가 등록되면, 리스트에 추가됩니다.

※주의 사항 : 탐지 제외 항목 혼합 사용 시

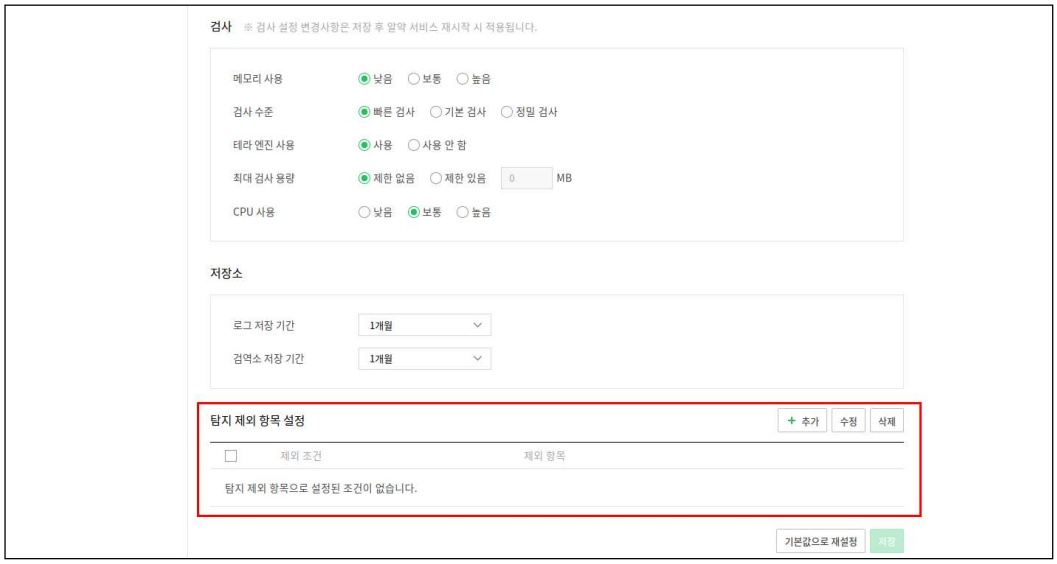
- FileExt 옵션과 FileExt(Include Filter) 옵션을 모두 설정하게 될 경우, 모든 파일을 검사하지 않게 되니, 주의해주시기 바랍니다.

[예외 처리 적용 우선 순위]
- 검사 시 FileExt(Include Filter)를 먼저 확인 후, FileExt 를 확인

[이슈 예시]
1) 확장자 exe 에 FileExt 와 FileExt(Include Filter) 모두 적용 시
2) 검사 중 exe 가 아닌 다른 확장자 파일을 만났을 경우 ⇒ FileExt(Include Filter) 옵션으로 인해 검사하지 않음.
3) 검사 중 exe 확장자 파일을 만났을 경우 ⇒ FileExt 옵션으로 인해 검사하지 않음.
▶ 결론적으로 모든 파일이 검사에서 제외

2) 웹 환경

- [설정] 탭을 누른 후, 하위의 [탐지 제외 항목 설정] 에서 탐지 제외를 설정할 수 있습니다.



- [추가] 버튼을 통해 제외 항목을 추가 할 수 있습니다.
- 필요 시, 생성된 항목을 선택 후, [수정]/[삭제] 버튼을 통해 항목을 수정하거나 삭제할 수 있습니다.

[제외 조건]

- **파일명 제외** : 파일명에 지정한 내용이 포함되어 있으면 탐지 제외합니다.
- **파일(전체 경로) 제외** : 지정한 경로는 탐지 제외합니다.
- **폴더(전체 경로) 제외** : 지정한 디렉터리는 탐지 제외합니다.
- **탐지명 제외** : 지정한 탐지명은 탐지 제외합니다.
- **파일 확장자 제외** : 지정한 확장자의 탐지 제외합니다.
- **파일 확장자 탐지** : 지정한 확장자만 탐지합니다. (다른 파일은 모두 검사 안 함)

8.2 업데이트

1) 터미널 환경

- 아래 명령어를 이용하여 업데이트를 진행할 수 있습니다.

```
# ALYac update
```

[상세 옵션]

- -u, --update : 업데이트를 실행합니다.
- -b, --verbose : 업데이트를 실행합니다. 업데이트의 진행 과정을 자세히 출력합니다.
- -f, --force : 강제 업데이트를 실행합니다. 알약 동작 여부와 관계없이 업데이트를 진행합니다.
- -h, --help : 도움말을 출력합니다.

- 업데이트를 실행 시, 업데이트할 제품을 확인하는 문구가 나오며, 각 제품의 번호를 통해 업데이트를 원하는 제품을 선택할 수 있습니다.

2) 웹 환경

- 웹 UI 우측 상단의 [업데이트] 버튼으로 업데이트를 진행 할 수 있습니다.

9. 로그/기타

9.1 로그

1) 터미널 환경에서 로그 조회하기

- 다음 명령으로 로그를 조회할 수 있습니다.

```
# ALYac log
```

[상세 옵션]

- yy-mm-dd : 원하는 날짜를 입력하여 로그를 조회합니다.
- -l, --list : 로그가 저장되어있는 날짜의 리스트를 확인합니다.
- --legacy ARG : 이전 버전의 로그들을 조회합니다.

2) 웹 환경에서 로그 조회하기

- [로그 보기] 탭을 눌러 기간별 로그를 조회할 수 있습니다.

- 이벤트 로그, 탐지 로그로 분류하여 볼 수 있으며, 검색을 원하는 기간을 설정하여
로그를 조회할 수 있습니다.

- 로그의 삭제를 원할 경우, 원하는 항목을 선택 후 [로그 삭제] 버튼을 클릭하여 제거할 수 있습니다.

9.2 미치료 항목

1) 터미널 환경에서 미치료 항목 관리하기

- 다음 명령으로 미치료 항목을 관리할 수 있습니다.

```
# ALYac log -u
```

[상세 옵션]

- No Action(default) : 항목만 확인하고 명령어를 종료합니다.
- Rescan : 재검사를 진행합니다.
- Exclude : 탐지 제외 처리를 진행합니다.

2) 웹 환경에서 미치료 항목 관리하기

- [로그 보기] - [미치료 항목]을 눌러 미치료 항목을 관리할 수 있습니다.

- 원하는 기간을 설정하여 미치료 항목을 조회할 수 있습니다.

- 재검사/치료 버튼을 통해, 미치료 항목에 대해 재검사 및 치료 여부를 결정할 수 있습니다.

- 탐지 제외 버튼을 통해, 미치료된 항목을 간편하게 탐지 제외에 등록할 수 있습니다.

- 삭제 버튼을 통해, 미치료 항목에 등록된 항목을 삭제할 수 있습니다.(GUI 만 제공)

10. 자주하는 질문

10.1 웹 서비스

Q. 어떤 웹 브라우저를 지원하나요?

A : 브라우저는 아래 명시된 버전을 지원합니다.

- Chrome 71 이상 / Firefox ESR 60 이상 / Fiefox 64 이상 / Edge 18 이상 / IE 10 이상

Q. 검사 도중, 치료 도중 웹 브라우저를 종료해버렸어요.

A : 검사 도중 웹 브라우저를 종료한 경우, 종료한 시점에서 검사가 중단됩니다.

- 단, 디렉터리를 검사 중이었을 경우 해당 디렉터리까지는 검사를 완료합니다.
  이 때 탐지된 파일들은 로그에서 확인할 수 있습니다.

- 치료 도중 웹 브라우저를 종료한 경우에는 치료가 계속 진행됩니다.