



# 랜섬크런처

RansomCruncher

## 관리자 매뉴얼

랜섬웨어 예방 및 데이터 관리 투트랙 보안백업 솔루션

1. 에이전트 설치
2. 매니저
3. 에이전트
4. 프로그램 정보

## 제 0 장. 랜섬크런처

### A. 프로그램 개요

랜섬크런처(RansomCruncher)는 소프트웨어 인증방식과 행위기반 차단방식을 도입하여 용자가 알 수 없거나 불필요한 소프트웨어가 중요 자료에 접근하는 것을 원천적으로 제어할 수 있는 강력한 보안 솔루션입니다. 중요자료 변조 행위뿐만 아니라 파일 이름/데이터 난독화 같은 우리가 예상하지 못하는 악성행위는 점차 증가하고 있는 가운데 기존의 평판기반, 시그니처 행위기반, 상황인식의 솔루션으로는 변종 악성 행위에 대응이 늦을 수밖에 없습니다. 이러한 문제점을 근본적으로 해결할 수 있는 EDR 기반 솔루션입니다.

### B. 구성

#### ① 클라우드 매니저 프로그램

\* 중앙에서 클라이언트를 관리하는 프로그램으로 모든 백업 설정이나 작업, 정책을 설정합니다.

#### ② 클라이언트 프로그램

\* 사용자측에서 설치되는 프로그램입니다.

### C. 매뉴얼 구성

챕터 번호 / 제목	내 용
제 1 장 에이전트 설치	에이전트 설치에 대해 설명합니다.
제 2 장 매니저	에이전트의 기능에 대해 설명합니다.
제 3 장 에이전트	백업된 데이터를 복원하는 기능에 대한 설명입니다.
제 4 장 프로그램 정보	리자드 클라우드 프로그램 정보 및 주의 사항에 대해 설명합니다.

## D. 목차

<b>제 1 장. 에이전트 설치</b> .....	<b>6</b>
A. 웹에서 설치.....	6
B. 배포용 셋업으로 설치.....	6
C. 로그인 설치.....	7
<b>제 2 장. 랜섬크런처 매니저</b> .....	<b>6</b>
A. 진입 화면.....	6
B. 인터페이스.....	7
C. 제품 등록 확인하기.....	8
D. 관리 메뉴.....	9
1. 사용자 관리.....	9
1-1. 사용자 생성.....	9
1-2. 사용자 편집.....	11
2. 그룹 관리.....	13
2-1. 그룹 생성.....	14
2-2. 그룹 편집.....	14
2-3. 조직도 그룹 메뉴.....	14
3. 시스템 로그.....	15
4. 보고서.....	16
5. Agent 업데이트.....	17
5-1. Agent 업데이트 편집.....	17
E. 정책 메뉴.....	18
1. 랜섬웨어 탐지정책 관리.....	18
1-1. 정책 생성.....	19
1-2. 정책 편집.....	19
2. 랜섬웨어 탐지 프로세스.....	20
2-1. 기본 프로세스.....	21
2-2. 공유 프로세스.....	21
2-3. 사용자 수집 프로세스.....	21
2-4. 프로세스 검출내역.....	22
<b>제 3 장. 에이전트</b> .....	<b>23</b>

A. 랜섬크런처 에이전트 .....	23
1. Home 화면 .....	23
1-1. 보안 등급 .....	23
1-2. 상단 메뉴 .....	24
1-3. 하단 메뉴 .....	24
2. 설정 화면 .....	25
2-1. 시작프로세스 관리 .....	25
2-2. 관리프로세스 목록 .....	25
2-3. 로그보기 .....	28
2-4. 프로그램 정보 .....	29
2-5. 격리소 대피소 보호 .....	29
2-6. 환경설정 .....	30

## **제 4 장. 프로그램 정보.....31**

A. 프로그램 정보 .....	31
B. 주의 사항 .....	31
C. 시스템 사양 .....	31
D. 연락처 .....	31

## 제 1 장. 에이전트 설치

▶ 에이전트(클라이언트 프로그램)는 백업할 대상 PC 에 설치하는 프로그램입니다. 에이전트 프로그램은 매니저 프로그램과 통신해서 필요한 백업정책을 내려 받고 이를 자동적으로 수행하게 됩니다.

### A. 웹에서 설치

※ 에이전트 설치시 반드시 매니저의 '기본 설정'이 모두 끝난 상태에서 설치해야 하며, 반드시 사용자의 ID/PW 를 가지고 웹 페이지에서 로그인 후 설치를 실행해야 합니다.

①  [설치] 버튼을 클릭합니다.

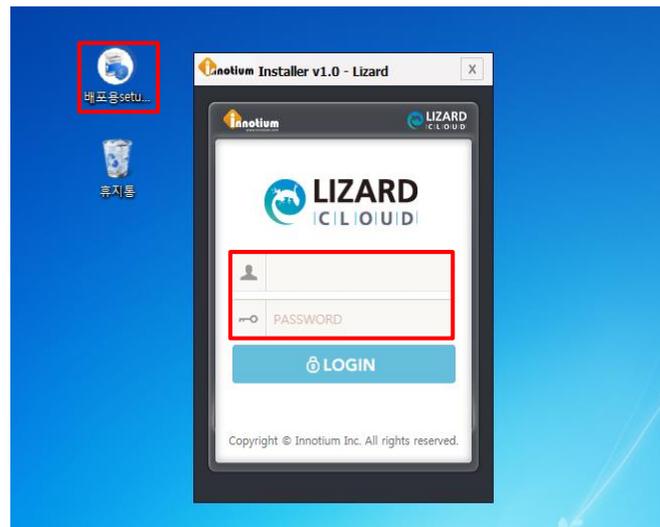
②  [Agent Setup] 버튼을 클릭하여 설치합니다.

※ 에이전트는 반드시 매니저에서 자신의 ID/PW 를 가지고 다운로드 받아서 설치해야 합니다. 다른 사람의 ID/PW 를 이용하여 에이전트를 설치할 경우 다른 사용자가 사용을 하지 못할 수 있습니다.

### B. 배포용 셋업으로 설치

- ① 관리자에게 받은 exe 파일을 다운받습니다.
- ② 다운받은 파일을 실행시켜 나온 로그인 창에 ID/PW 를 입력 후 로그인합니다.
- ③ 파일을 실행하면 1~2 분 이내에 프로그램이 설치됩니다.

※ 해당 프로그램은 1 회만 설치 가능하며, 프로그램을 다시 설치할 경우 관리자에게 요청하여 허가 받은 후 설치하시기 바랍니다.



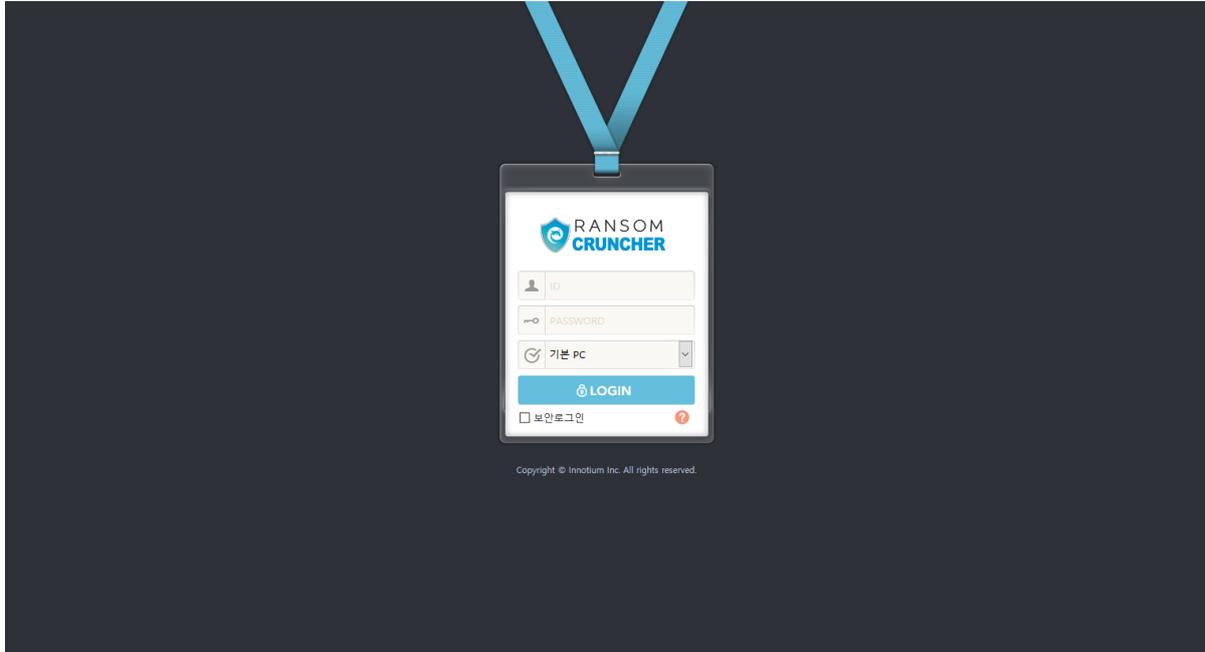
## C. 로그인 설치

- ① 관리자에게 받은 exe 파일을 다운받습니다.
- ② 실행 시 아래와 같은 로그인 페이지가 생성되며 아이디, 비밀번호 입력 시 해당 계정으로 등록됩니다.
- ③ 계정 등록은 최초 1 회만 진행되며 등록 후 재등록은 기능설정 > 매니저 설정에서 변경 가능합니다.

The screenshot shows a window titled "ID 등록 로그인" (ID Registration Login) with a close button (X) in the top right corner. On the left side, there is a blue vertical banner featuring a shield icon with a gear inside, and the text "RANSOM CRUNCHER" below it. The main content area contains two text input fields. The first field is labeled "아이디(사번)" (ID/Serial Number) and has a cursor in it. The second field is labeled "비밀번호를 입력하십시오." (Enter password). Below these fields are two buttons: "ID 등록" (ID Registration) and "취소" (Cancel).

## 제 2 장. 랜섬크런처 매니저

### A. 진입 화면



- ▶ 주소 창에 설정되어 있는 URL 혹은 IP 주소를 입력 후 관리자 혹은 사용자 ID와 패스워드를 입력하여 매니저에 접속합니다.
- ▶ 서버 PC 접속 : 기본적으로 "기본 PC"로 매니저에 접속하게 되며 서버계정을 사용하는 사용자의 경우에는 관리자가 지정한 서버계정 설정값을 리스트에서 클릭하여 서버계정으로 접속합니다. 서버계정을 접속하는 ID는 "기본 PC"로 접속하는 ID와 동일합니다.
- ▶ 보안로그인 : 아이오써티(ioCERTi)를 이용하여 보안 로그인 합니다.

## B. 인터페이스

▶ 매니저를 접속하면 아래와 같은 인터페이스가 나타납니다. 인터페이스는 사용자 권한에 따라 다르게 표시됩니다.

※ 매니저는 오직 관리자만 보도록 보안을 철저하게 유지하시기 바랍니다.



### [ 각 영역별 소개 ]

#### ① 상단메뉴(노란배경영역)

- 관리 : 사용자/그룹 생성, 삭제, 옵션 설정이 가능합니다.
- 정책 : 사용자/그룹에 할당할 정책, 옵션의 생성, 삭제, 수정이 가능합니다.
- 시스템 : 관리자가 모니터링 할 수 있도록 로그 및 보고서 등을 표시합니다.
- 설치 : 사용자 계정으로 접속 후 해당 메뉴로 에이전트 설치를 진행 할 수 있습니다.  
 ※ admin 계정은 에이전트 설치가 불가능합니다.
- 도움말 : 도움말 페이지로 이동합니다.

#### ② 조직도(파란배경영역)

- 생성된 그룹 및 사용자를 확인할 수 있습니다.
  - 초록색 사용자 : 에이전트와 매니저가 통신하는 상태
  - 주황색 사용자 : 에이전트와 매니저가 통신이 되지 않는 상태(에이전트 삭제, PC 종료 등)
  - 검정색 사용자 : 에이전트가 미설치 된 사용자
- Add user 버튼을 이용하여 사용자 생성이 가능하며 검색창에 사용자 ID, 이름으로 검색이 가능합니다.
- 사용자 ID 클릭 시 사용자 편집 화면으로 이동합니다.
- 그룹명 클릭 시 사용자 관리 메뉴를 이용하여 해당 그룹에 속한 사용자를 확인할 수 있으며, 그룹 편집 메뉴를 이용하여 그룹 편집 화면으로 이동합니다.

#### ③ 사용자 목록(분홍배경영역)

- 현재 등록된 사용자 목록을 보여주며, 사용자 클릭 시 해당 사용자에 대한 편집 화면으로 이동합니다.
- Agent 상태, 개수 보기, 사용자 ID 및 옵션명에 따른 사용자 정렬 및 검색이 가능합니다.

④ 쿼메뉴(주황배경영역)

- ※ 사용자 목록에서 선택된 사용자에게 편집 화면에서의 설정 없이 즉시 명령을 내릴 수 있습니다.
- 그룹 변경 : 사용자가 속한 그룹을 변경합니다.
- 정책 변경 : 사용자에게 적용된 정책을 변경합니다.
- 저장 : 사용자 목록을 엑셀파일(.xls)로 저장합니다.
- 삭제 : 선택한 사용자 계정을 삭제합니다.
- ID 생성 : 새 사용자를 생성합니다.
- 파일로 사용자 등록하기 : 텍스트 파일(.txt / UTF-8 형식)을 등록하여 다수의 사용자를 한 번에 생성할 수 있습니다.
- 비밀번호 초기화 : 사용자 ID의 비밀번호를 아이디/직접 입력을 통해 초기화 합니다.
- 업데이트 : 사용자의 에이전트를 최신 버전으로 업데이트 합니다.
- 제거 하기 : 에이전트를 제거하는 명령을 내립니다.
- 추가 설치 : 에이전트 재설치가 필요한 경우 사용합니다.

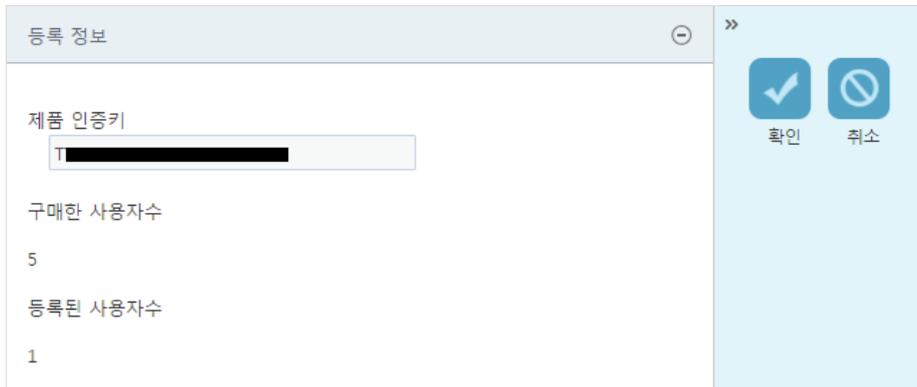
⑤ 로그인 정보(흰색배경영역)

- 현재 로그인 된 사용자의 정보 및 최근 매니저에 접속한 IP, 접속시간을 표시하며, Admin 계정으로 접속하면 매니저 설정이 변경 가능하며 그 외 ID로 로그인을 하게 되면 사용자 편집 화면으로 이동합니다.

## C. 제품 등록 확인하기

▶ 랜섬크런처를 구매하면, 본사로부터 라이선스가 발급됩니다. 실제 사용 가능 인원수가 표시됩니다. 이 라이선스와 실제 매니저에 등록된 라이선스가 일치하는지 반드시 확인하시기 바랍니다.

- ① [매니저의 접속 주소]/rc\_registry/registry.php 로 접속합니다.
- ② 제품 인증키 및 구매한 사용자수를 확인합니다.
- ③ 현재 구매한 사용자가 5명, 등록된 사용자가 1명임을 확인할 수 있습니다.



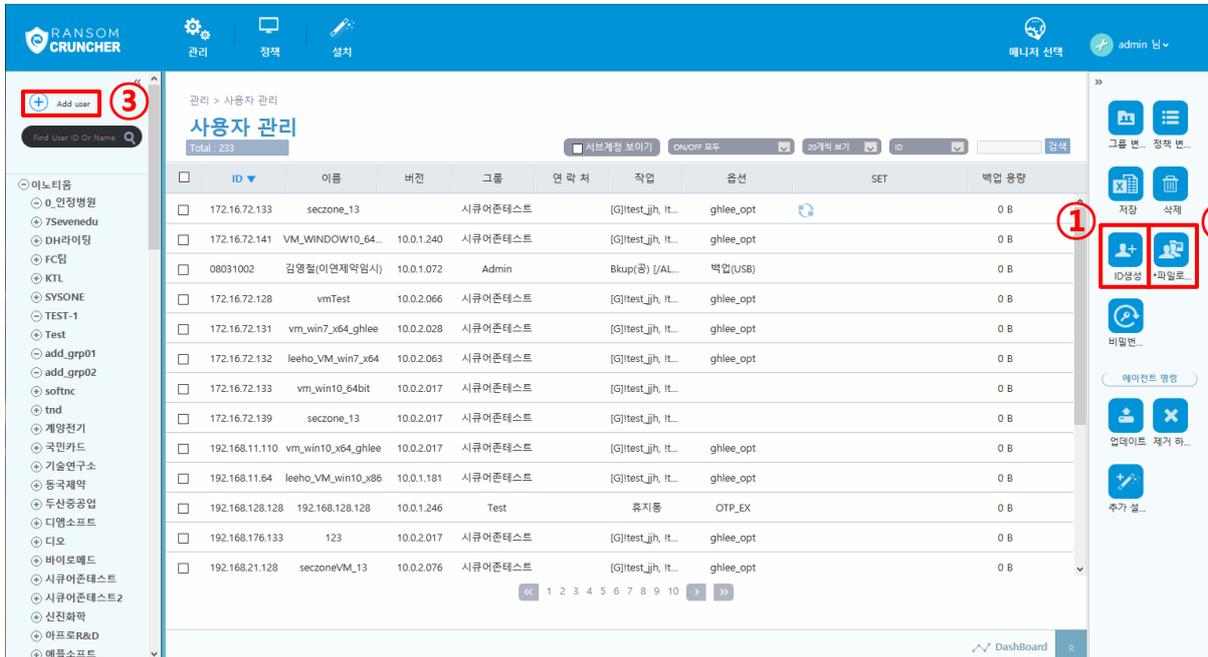
※ 라이선스에 문제가 있다면 구매처에 연락하여 지원받으시기 바랍니다.

## D. 관리 메뉴

### 1. 사용자 관리

▶ 처음 매니저를 접속하면, 사용자가 등록되어 있지 않습니다. 사용자를 수동으로 생성하는 방법은 3 가지가 있으며, 인사연동을 할 경우 사용자 생성은 별도로 하지 않습니다.

※ 접근경로 :  [관리]를 클릭하고  [사용자 관리]를 선택합니다.



### 1-1. 사용자 생성

▶ 매니저에서 사용자 생성은 3 가지 방법으로 생성할 수 있습니다.

#### 1-1-1. [ID 생성] 버튼으로 생성

①  ID생성 우측 즉시명령의 [ID 생성]을 클릭합니다.



② 아이디를 입력한 다음 [확인]을 클릭하여 사용자를 생성합니다.

### 1-1-2. [파일로 사용자 등록하기] 버튼으로 생성



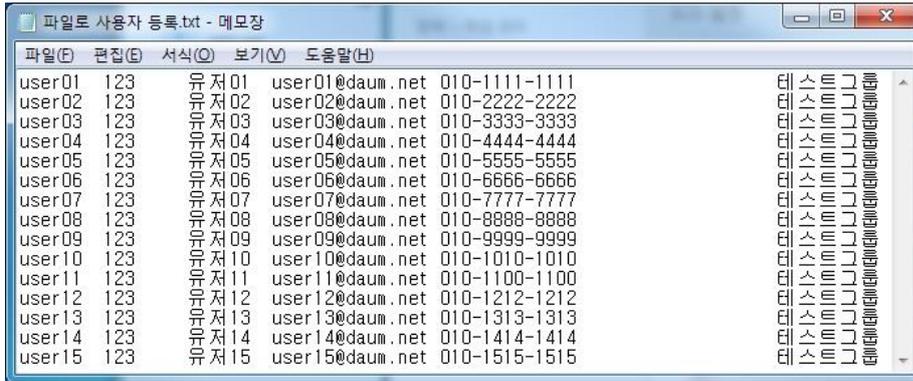
① 우측 즉시명령의 [파일로 사용자 등록하기]를 클릭합니다.



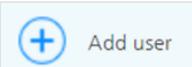
② [파일 선택]을 클릭합니다.

③ 아래와 같은 양식으로 txt 파일을 생성 후 등록을 해주면 사용자가 생성됩니다.

※ txt 파일의 인코딩 형식은 반드시 UTF-8 로 저장하시기 바랍니다.



### 1-1-3. [Add User] 버튼으로 생성



① 좌측 조직도 트리의 [Add User]를 클릭합니다.



② 아이디를 입력한 다음 [확인]을 클릭하여 사용자를 생성합니다.

## 1-2. 사용자 편집

### ▶ 사용자 관리

【 아이디 】 : 사용하고자 하는 사용자 ID 를 입력합니다. ID 는 생성할 때를 제외하고는 수정할 수 없습니다.

※ **사원번호로 ID 를 생성하는 것이 편리합니다.**

【 비밀번호 】 : ID 와 함께 사용할 비밀번호를 입력합니다.

【 사용자 이름 】 : 사용자의 이름을 입력합니다.

※ **직책과 간단한 부서명을 같이 기입하면 동명이인이 있을 경우 혼란하지 않을 수 있습니다.**

【 이메일 】 : 사용자의 이메일 정보를 입력합니다.

【 연락처 】 : 사용자의 연락처를 입력합니다.

【 비고 】 : 사용자에 대한 기타 정보를 입력합니다.

【 그룹 】 : 사용자가 속할 그룹을 설정합니다.

【 사용자 레벨 】 : 관리자, 그룹 관리자, 그룹 모니터, 일반 사용자로 나누어 집니다. 이 레벨에 의하여 부 관리자의 권한을 승계 받을 수 있습니다.

- 관리자 : 관리자 계정과 동일한 권한을 가지게 되며, 사용자/그룹 관리, 정책 생성/수정/삭제 등 모든 작업이 가능합니다.
- 그룹 관리자 : 본인이 속한 그룹에 한해서 사용자/그룹 관리, 정책 설정 등이 가능합니다.
- 그룹 모니터 : 본인이 속한 그룹의 사용자/그룹/정책 정보 등의 확인이 가능하며, 수정은 불가합니다.
- 일반 사용자 : 본인 계정의 정보 확인만 가능하며, 다른 작업은 불가합니다.

【 랜섬웨어 탐지정책 】 : 미리 생성한 탐지정책을 선택하여 설정합니다. 검색을 통해 생성된 탐지정책을 찾아서 적용할 수 있습니다.

※ 만약 그룹에 탐지정책을 설정했다면, 그룹에 부여한 탐지정책이 사용자에게 자동으로 부여되기 때문에 같은 탐지정책을 따로 설정하지 않아도 됩니다.

※ 사용자 편집 시 탐지정책을 선택하였다면, 우선 순위 적용으로 사용자에게 부여한 탐지정책이 설정되며 그룹에 적용한 탐지정책은 적용되지 않습니다.

(우선순위 : 사용자에게 설정된 정책 > 그룹에 설정된 정책)

【 업데이트 】 : 에이전트 프로그램의 버전을 체크하여 최신 버전의 프로그램으로 업데이트 합니다.

( 진행중인 작업 표시,  작업 완료 표시)

【 프로그램 제거 】 : 에이전트 프로그램 제거 시 사용됩니다.

※ 업데이트, 즉시 백업, 프로그램제거 상태 확인 → 관리자가 쉽게 상태를 확인하여 기존에 작업이 이루어졌는지 아닌지를 알 수 있습니다.

( 옵션이 설정되기 전 상태,  작업이 완료된 후 상태,  작업 선택 상태)

**【 프로그램 추가 설치 】** : 에이전트를 한번 설치한 사용자 계정으로 다른 PC 에 추가 설치 허용 대한 여부를 설정할 수 있습니다

(  프로그램 추가 설치 허용하기,  프로그램 추가 설치 완료)

▶ **사용자 로그** : 랜섬크런처 사용자 에이전트의 모든 동작 상태와 사용자에게 적용된 정책을 확인할 수 있습니다.

- Total 에 로그의 총 개수를 표시합니다.
- 검색 기능을 이용해 시간, 설명을 기준으로 로그를 검색할 수 있습니다.
- 표의 시간/설명을 클릭하면 오름차순, 내림차순으로 정렬할 수 있습니다.

▶ **랜섬웨어 탐지 프로세스** : 랜섬크런처 사용자 에이전트에서 수집하고 사용자가 직접 설정한 프로세스 리스트를 보여줍니다.

- Total 에 로그의 총 개수를 표시합니다.
- 검색 기능을 이용해 파일명, SHA2, 설명을 기준으로 로그를 검색할 수 있습니다.
- 우측 킷메뉴 [삭제] 버튼을 이용하여 리스트에서 해당 프로세스를 삭제할 수 있습니다.
- 우측 킷메뉴 [공유] 버튼을 이용하여 리스트에서 해당 프로세스를 다른 사용자와 공유할 수 있는 프로세스로 등록할 수 있습니다.

**【 허용할 프로세스 】** : 에이전트에서 허용한 프로세스와 사용자가 에이전트에서 허용할 프로세스로 설정한 프로세스 리스트를 표시합니다.

- [삭제]버튼을 클릭하여 등록된 프로세스를 삭제할 수 있습니다.
- [공유]버튼을 클릭하여 등록된 프로세스를 특정 그룹 또는 전체 사용자에게 허용/차단 프로세스로 공유할 수 있습니다.

**【 차단할 프로세스 】** : 에이전트에서 차단한 프로세스와 사용자가 에이전트에서 차단할 프로세스로 설정한 프로세스 리스트를 표시합니다.

- [삭제]버튼을 클릭하여 등록된 프로세스를 삭제할 수 있습니다.
- [공유]버튼을 클릭하여 등록된 프로세스를 특정 그룹 또는 전체 사용자에게 허용/차단 프로세스로 공유할 수 있습니다.

**【 예외처리 프로세스 】** : 사용자가 에이전트에서 예외처리 프로세스로 설정한 프로세스 리스트를 표시합니다.

- [삭제]버튼을 클릭하여 등록된 프로세스를 삭제할 수 있습니다.
- [공유]버튼을 클릭하여 등록된 프로세스를 특정 그룹 또는 전체 사용자에게 허용/차단 프로세스로 공유할 수 있습니다.

※ 공유 프로세스란?

특정 사용자 에이전트에서 수집된 프로세스를 같은 매니저상에 있는 사용자 에이전트에게 수집된 프로세스에 대하여 허용 또는 차단으로 등록하여 전체 또는 그룹사용자가 해당 프로세스를 공유할 수 있는 기능입니다. 공유 프로세스에서의 허용 프로세스는 사용자 프로세스에서는 예외 프로세스로 인식하여 사용되어 동작합니다.

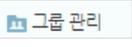
▶ **랜섬웨어 탐지 로그** : 랜섬크런처 사용자 에이전트에서 동작(차단, 복구등)하는 내역을 확인할 수 있습니다.

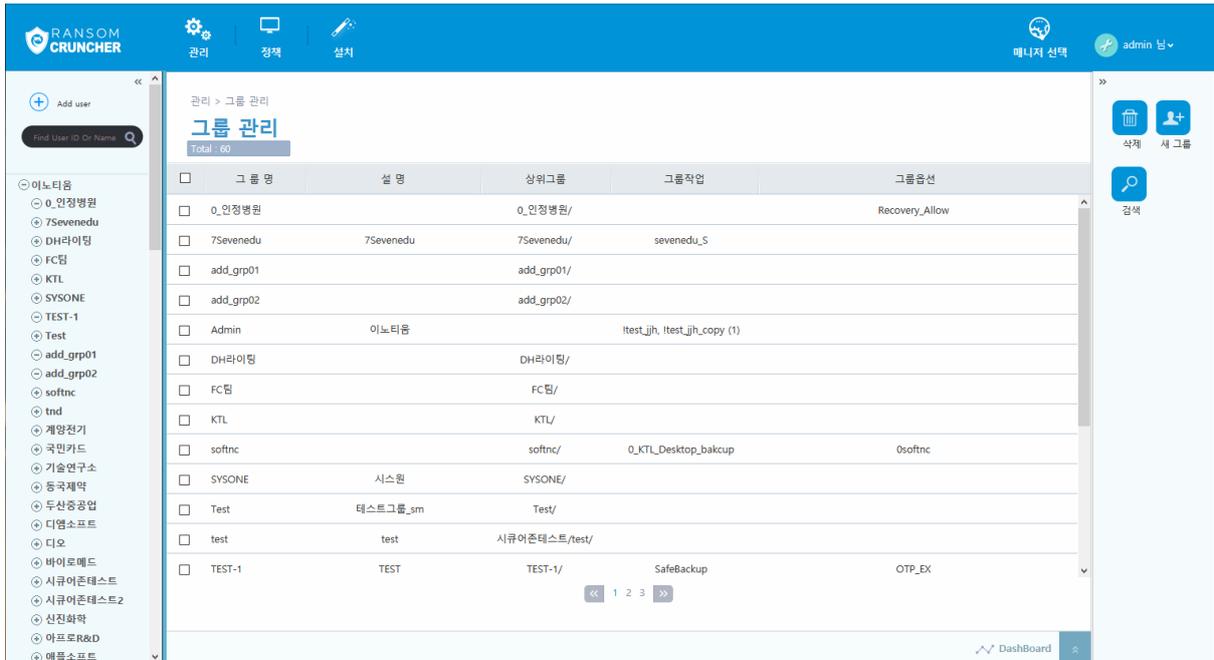
- Total 에 로그의 총 개수를 표시합니다.
- 검색 기능을 이용해 설명, 사용자, 시간을 기준으로 로그를 검색할 수 있습니다.
- 표의 시간/설명을 클릭하면 오름차순, 내림차순으로 정렬할 수 있습니다.

## 2. 그룹 관리

▶ 관리자가 그룹을 관리하기 위한 페이지로 그룹을 생성, 편집, 삭제를 할 수 있습니다. 처음 매니저를 실행하면 기본적으로 Admin 그룹이 생성되어 있습니다.

※ 그룹을 사용하면 부서별로 사용자를 분류하고 관리하기 편리합니다.

※ 접근경로 :  [관리]를 클릭하고  [그룹 관리]를 선택합니다.



### 2-1. 그룹 생성

①  [새 그룹]을 클릭합니다.

② 그룹명을 입력한 후 [확인]을 클릭합니다.

## 2-2. 그룹 편집

### ▶ 그룹 관리

【 그룹명 】 : 그룹명을 표시합니다.

※ 그룹명은 부서명으로 표기하면 관리가 용이합니다.

【 그룹설명 】 : 그룹에 대한 설명을 작성합니다.

【 그룹 】 : [그룹 설정] 버튼을 이용하여 그룹을 선택하고 해당 그룹을 원하는 그룹의 하위그룹으로 지정 할 수 있습니다.

【 랜섬웨어 탐지정책 】 : 미리 생성한 탐지정책을 선택하여 설정합니다. 검색을 통해 생성된 탐지정책을 찾아서 적용할 수 있습니다.

※ 사용자 편집 시 탐지정책을 선택하였다면, 우선 순위 적용으로 사용자에게 부여한 탐지정책이 설정되며 그룹에 적용한 탐지정책은 적용되지 않습니다.

(우선순위 : 사용자에게 설정된 정책 > 그룹에 설정된 정책)

## 2-3. 조직도 그룹 메뉴

▶ 조직도 그룹 클릭 메뉴 : 조직도에 표시된 그룹을 클릭하면 그룹을 모니터링 할 수 있는 메뉴가 표시됩니다.



【 사용자 관리 】 : 그룹에 속한 사용자들이 표시되는 사용자 관리 페이지로 이동합니다.

【 그룹 편집 】 : 그룹명, 그룹 정책등을 편집할 수 있는 편집화면으로 이동합니다.

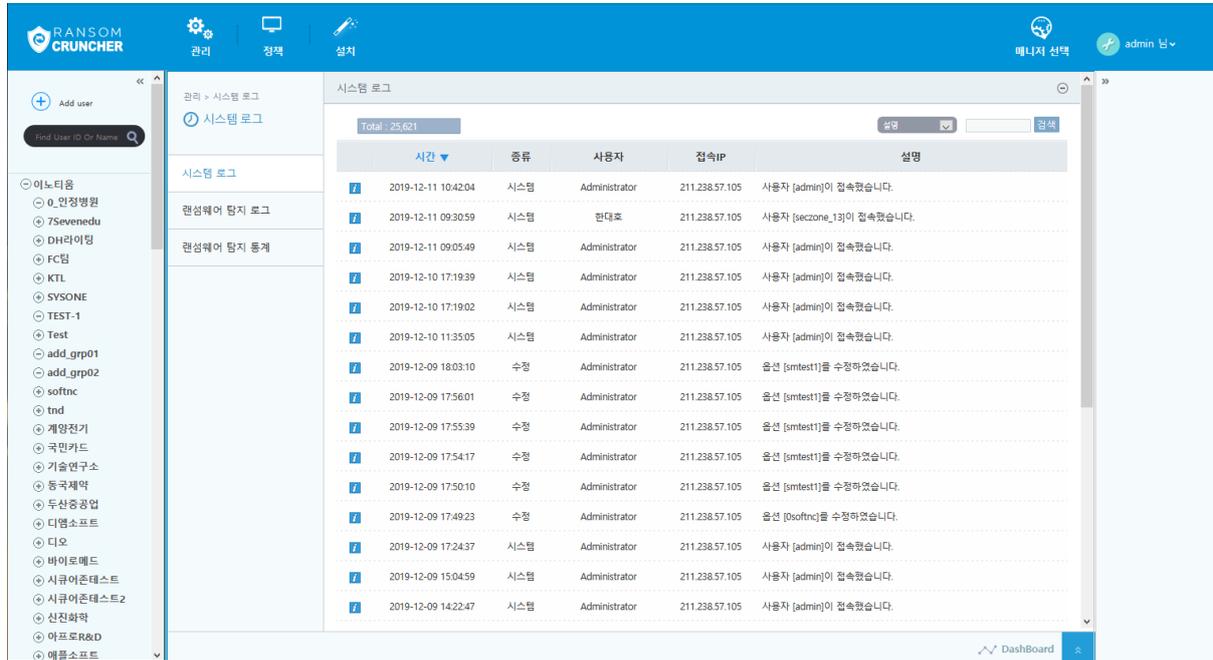
※ 편집화면의 내용은 2-2 의 그룹 편집과 동일합니다.

### 3. 시스템 로그

▶ 관리로그를 통하여 관리자가 특정 작업 수행 시 해당 작업 로그와 접속 IP 정보를 제공하여 어느 PC에서 명령을 수행하였는지 확인할 수 있습니다.



※ 접근경로 : [관리]를 클릭 후 [시스템 로그] [시스템 로그]를 클릭합니다.



▶ **시스템 로그** : 매니저에서 일어난 모든 이벤트를 확인할 수 있습니다.

- Total 에 로그의 총 개수를 표시합니다.
- 검색 기능을 이용해 설명, 사용자, 시간을 기준으로 로그를 검색할 수 있습니다.
- 표의 시간/사용자/접속 IP/설명을 클릭하면 오름차순, 내림차순으로 정렬할 수 있습니다.
- [저장]버튼을 클릭하여 xls 파일로 PC 에 저장할 수 있습니다.

▶ **랜섬웨어 탐지 로그** : 모든 사용자 에이전트에서 수집된 탐지 로그를 확인할 수 있습니다.

- Total 에 로그의 총 개수를 표시합니다.
- 검색 기능을 이용해 설명, 사용자, 시간을 기준으로 로그를 검색할 수 있습니다.
- 표의 시간/사용자/설명을 클릭하면 오름차순, 내림차순으로 정렬할 수 있습니다.
- [저장]버튼을 클릭하여 xls 파일로 PC 에 저장할 수 있습니다.

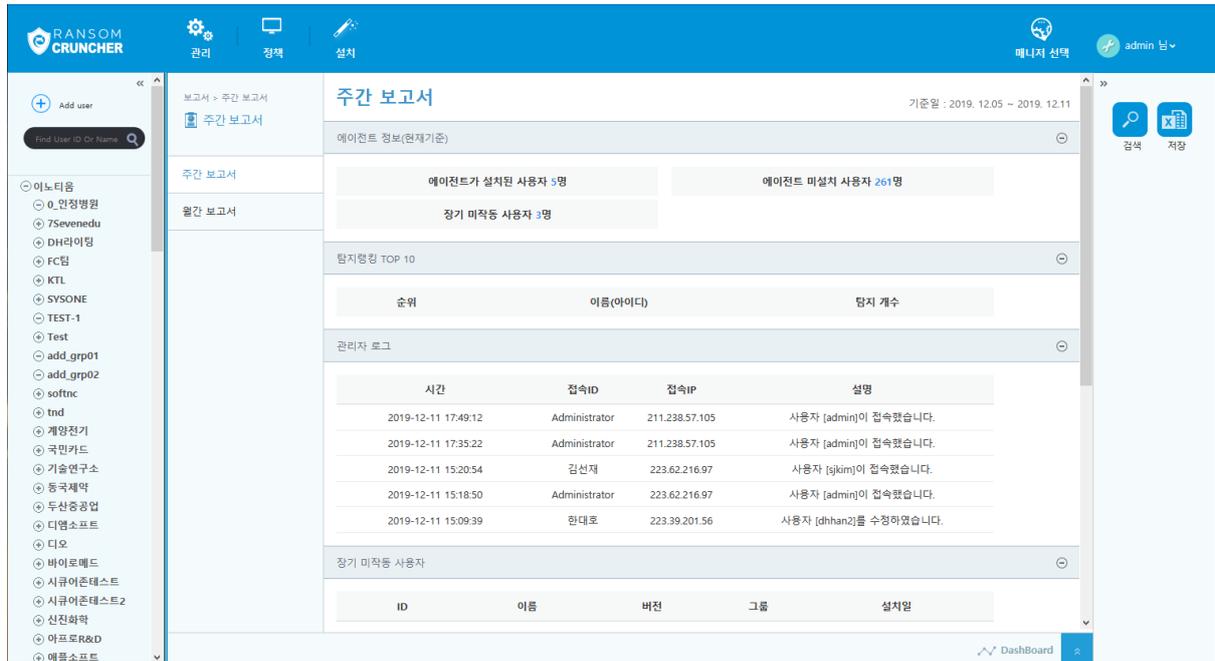
▶ **랜섬웨어 탐지 통계** : 기간을 설정하여 기간내 탐지된 프로세스를 그래프로 표출되어 사용자별, IP 별, 랜섬웨어 별로 확인할 수 있습니다.

※ 그래프로 표출되는 최대 개수는 10 개입니다.

## 4. 보고서

▶ 매니저에서 종합한 로그들을 주간/월간 보고서로 확인할 수 있습니다.

※ 접근경로 :  [관리]를 클릭 후  [보고서]를 클릭합니다.



화면 상단에는 'RANSOM CRUNCHER' 로고와 '관리', '정책', '설정' 메뉴가 있으며, 오른쪽에는 '매니저 선택'과 'admin 님' 사용자 정보가 표시되어 있습니다. 좌측에는 'Add user' 버튼과 'Find User ID Or Name' 검색창이 있습니다. 메인 영역에는 '주간 보고서' 탭이 선택되어 있으며, 기준일이 '2019. 12.05 ~ 2019. 12.11'로 설정되어 있습니다.

주요 데이터 요약:

- 에이전트가 설치된 사용자: 5명
- 에이전트 미설치 사용자: 261명
- 장기 미작동 사용자: 3명

참지랭킹 TOP 10 테이블:

순위	이름(아이디)	탐지 개수	
관리자 로그			
시간	접속ID	접속IP	설명
2019-12-11 17:49:12	Administrator	211.238.57.105	사용자 [admin]이 접속했습니다.
2019-12-11 17:35:22	Administrator	211.238.57.105	사용자 [admin]이 접속했습니다.
2019-12-11 15:20:54	김선재	223.62.216.97	사용자 [sjkim]이 접속했습니다.
2019-12-11 15:18:50	Administrator	223.62.216.97	사용자 [admin]이 접속했습니다.
2019-12-11 15:09:39	윈대로	223.39.201.56	사용자 [dhan2]를 수정하였습니다.

장기 미작동 사용자 테이블:

ID	이름	바전	그룹	설치일
[데이터 없음]				

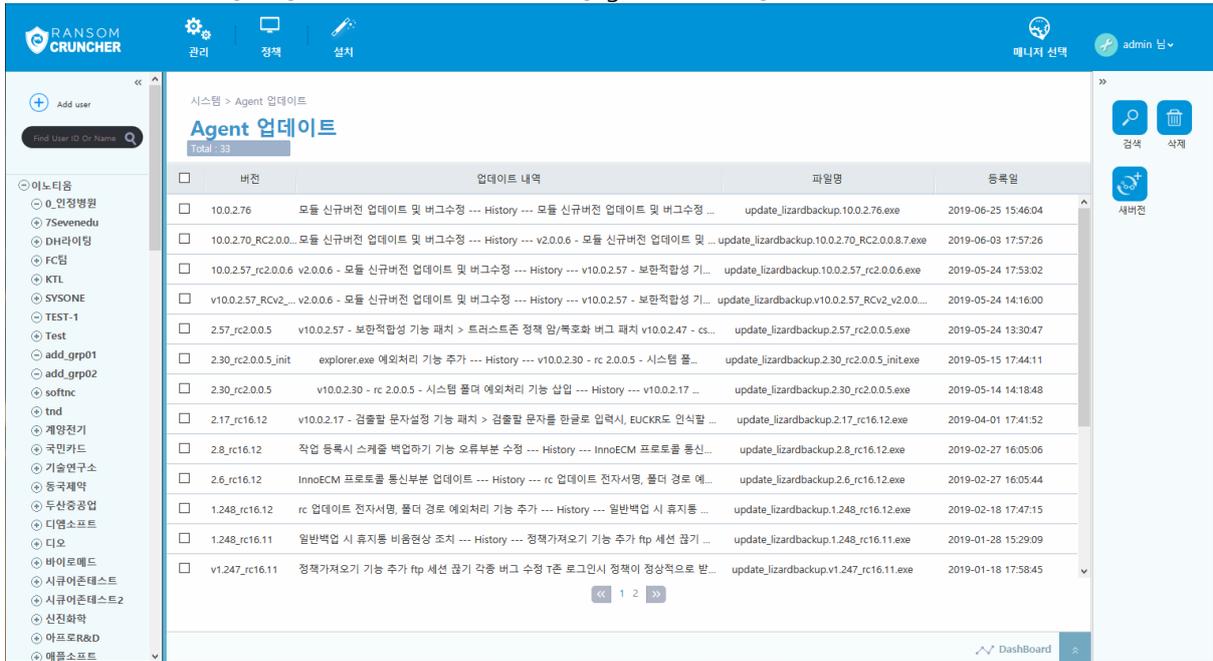
【 검색 】 : 버튼을 클릭하여 기준일/기준월을 선택할 수 있습니다.

【 저장 】 : 보고서를 xls 파일로 저장할 수 있습니다.

## 5. Agent 업데이트

▶ 사용자에게 에이전트 업데이트를 진행하기 전 업데이트 파일을 등록하는 페이지입니다.

※ 접근경로 :  [관리]을 클릭 후  [Agent 업데이트]을 클릭합니다.



화면 상단에는 'RANSOM CRUNCHER' 로고와 '관리', '정책', '설치' 메뉴가 있습니다. 오른쪽에는 'admin' 닉네임과 '새버전' 버튼이 있습니다. 메인 영역에는 'Agent 업데이트' 타이틀과 'Total: 33'이 표시되어 있습니다. 아래에는 업데이트 내역 테이블이 있습니다.

버전	업데이트 내역	파일명	등록일
10.0.2.76	모듈 신규버전 업데이트 및 버그수정 --- History --- 모듈 신규버전 업데이트 및 버그수정 ...	update_lizardbackup.10.0.2.76.exe	2019-06-25 15:46:04
10.0.2.70_RC2.0.0...	모듈 신규버전 업데이트 및 버그수정 --- History --- v2.0.0.6 - 모듈 신규버전 업데이트 및 ...	update_lizardbackup.10.0.2.70_RC2.0.0.8.7.exe	2019-06-03 17:57:26
10.0.2.57_rc2.0.0.6	v2.0.0.6 - 모듈 신규버전 업데이트 및 버그수정 --- History --- v10.0.2.57 - 보완적합성 기...	update_lizardbackup.10.0.2.57_rc2.0.0.6.exe	2019-05-24 17:53:02
v10.0.2.57_RCv2_...	v2.0.0.6 - 모듈 신규버전 업데이트 및 버그수정 --- History --- v10.0.2.57 - 보완적합성 기...	update_lizardbackup.v10.0.2.57_RCv2_v2.0.0...	2019-05-24 14:16:00
2.57_rc2.0.0.5	v10.0.2.57 - 보완적합성 가능 패치 > 트러스트론 정책 임/폭포화 버그 패치 v10.0.2.47 - cs...	update_lizardbackup.2.57_rc2.0.0.5.exe	2019-05-24 13:30:47
2.30_rc2.0.0.5_init	explorer.exe 예외처리 가능 추가 --- History --- v10.0.2.30 - rc 2.0.0.5 - 시스템 볼...	update_lizardbackup.2.30_rc2.0.0.5_init.exe	2019-05-15 17:44:11
2.30_rc2.0.0.5	v10.0.2.30 - rc 2.0.0.5 - 시스템 볼더 예외처리 가능 삽입 --- History --- v10.0.2.17 ...	update_lizardbackup.2.30_rc2.0.0.5.exe	2019-05-14 14:18:48
2.17_rc16.12	v10.0.2.17 - 검출할 문자설정 가능 패치 > 검출할 문자를 한글로 입력시, EUCKR도 인식할 ...	update_lizardbackup.2.17_rc16.12.exe	2019-04-01 17:41:52
2.8_rc16.12	작업 등록 시 스케줄 백업하기 가능 오류부분 수정 --- History --- InnoECM 프로토콜 통신...	update_lizardbackup.2.8_rc16.12.exe	2019-02-27 16:05:06
2.6_rc16.12	InnoECM 프로토콜 통신부분 업데이트 --- History --- rc 업데이트 전자서명, 볼더 경로 예...	update_lizardbackup.2.6_rc16.12.exe	2019-02-27 16:05:44
1.248_rc16.12	rc 업데이트 전자서명, 볼더 경로 예외처리 가능 추가 --- History --- 일반백업 시 휴지통 ...	update_lizardbackup.1.248_rc16.12.exe	2019-02-18 17:47:15
1.248_rc16.11	일반백업 시 휴지통 비움현상 조치 --- History --- 정책가져오기 가능 추가 ftp 세션 끊기 ...	update_lizardbackup.1.248_rc16.11.exe	2019-01-28 15:29:09
v1.247_rc16.11	정책가져오기 가능 추가 ftp 세션 끊기 각종 버그 수정 7종 로그인시 정책이 정상적으로 받...	update_lizardbackup.v1.247_rc16.11.exe	2019-01-18 17:58:45

### 5-1. Agent 업데이트 편집

#### ▶ Agent 업데이트

【 버전 】 : 업데이트 파일의 버전명을 기재합니다.

※ 버전명은 별도로 수정이 불가능하니 참고하여 등록하시기 바랍니다. 만약 버전명을 잘못 입력하였을 경우 해당 버전을 삭제하시고 다시 등록해야 합니다.

【 첨부파일 】 : [찾아보기] 버튼을 클릭하여 업데이트 파일을 등록합니다.

【 업데이트 내역 】 : 업데이트 파일을 등록할 때 해당 버전의 업데이트 내역을 기재할 수 있습니다.

※ 업데이트 내역은 새로운 버전을 등록할 때 이전 업데이트 내역을 가져오게 되며 해당 업데이트 파일의 업데이트 내역은 최상단에 작성하시기 바랍니다.

【 첨부파일 위치 】 : IP 대역을 지정하여 해당 IP 대역대를 가지고 있으면 지정한 파일 경로의 파일로 업데이트를 할 수 있도록 설정할 수 있습니다.

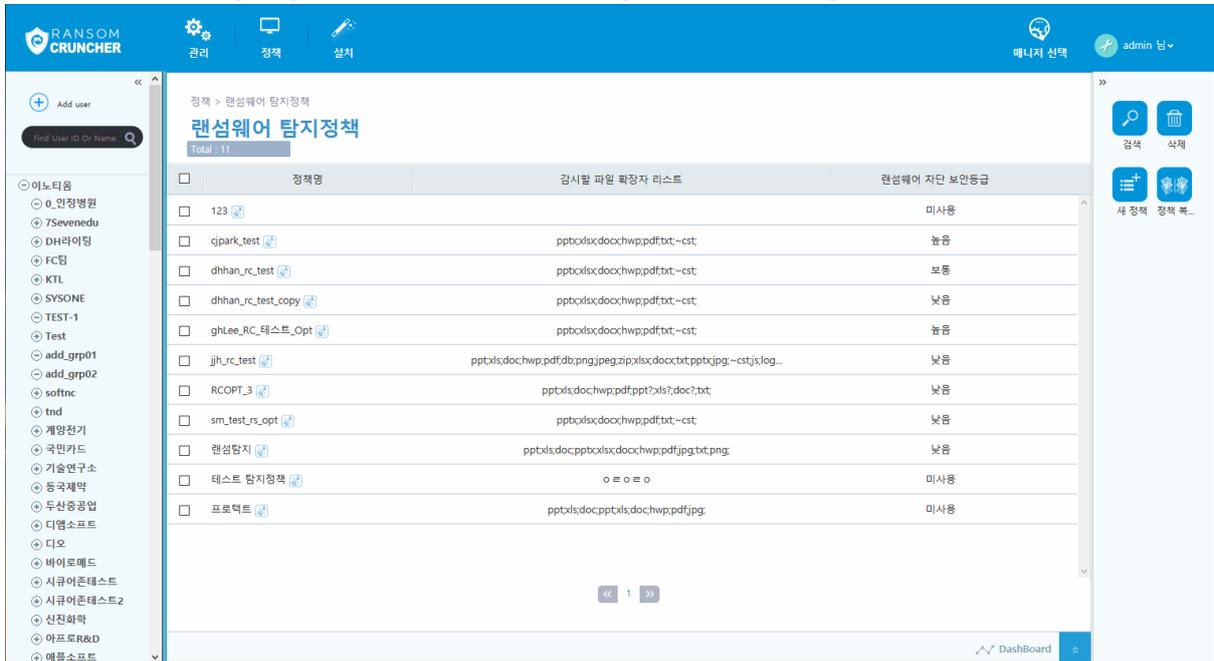
※ 반드시 필요한 부분은 아니며 본청 외에 지사가 있을 경우에 사용하시는 것을 권장해 드립니다.

## E. 정책 메뉴

### 1. 랜섬웨어 탐지정책 관리

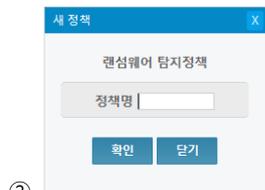
▶ 랜섬크런처 에이전트에서 동작하는 기능을 설정하는 페이지입니다.

※ 접근경로 :  [정책]을 클릭 후  [랜섬웨어 탐지정책] [랜섬웨어 탐지정책]를 클릭합니다.



#### 1-1. 정책 생성

①  오른쪽 메뉴에서 [새 정책]을 클릭합니다.



② 정책명을 입력한 후 [확인]을 클릭합니다.

## 1-2. 정책 편집

【 정책명 】 : 현재 정책명을 표시합니다.

【 작업 할당권한 】 : 특정 그룹에게만 부여할 수 있도록 권한을 설정합니다. 검색을 통해 그룹을 찾을 수 있습니다.

【 감시할 파일 확장자 】 : 랜섬웨어로부터 감시/보호할 파일을 확장자로 설정합니다. ";"을 이용하여 추가하고자 하는 확장자를 계속 추가할 수 있습니다.

【 프로세스 경로 예외처리 리스트 】 : 특정 폴더에서 동작하는 프로세스는 탐지에서 예외처리 하도록 설정합니다. ";"을 이용하여 추가하고자 하는 경로를 계속 추가할 수 있습니다.

※ 하위 폴더의 프로세스도 예외처리 되므로 주의해서 입력해야 합니다.

【 파일 경로 예외처리 리스트 】 : 특정 폴더의 파일 변조 행위를 탐지하지 않도록 예외처리 하도록 설정합니다. ";"을 이용하여 추가하고자 하는 경로를 계속 추가할 수 있습니다.

※ 하위 폴더의 파일도 예외처리 되므로 주의해서 입력해야 합니다.

【 전자서명 예외처리 리스트 】 : 특정 전자서명을 가진 프로세스는 탐지에서 예외처리 하도록 설정합니다. ";"을 이용하여 추가하고자 하는 전자서명을 계속 추가할 수 있습니다.

※ 여러 개의 전자서명을 등록 시 중복되는 전자서명이 있을 경우에는 중복된 전자서명부터는 등록이 안됩니다.

【 소프트웨어 인증 사용하기 】 : 소프트웨어 인증 기능을 사용하도록 합니다.

※ 전자서명이 없는 프로세스를 실행 차단하는 기능입니다.

【 사용자가 프로세스 예외처리 허용하기 】 : 사용자가 에이전트에서 수집된 프로세스를 직접 프로세스 예외처리 할 수 있도록 설정합니다.

【 랜섬웨어 차단 보안등급 】 : 설정한 보안등급에 따라 랜섬크런처에서 행위기반 탐지로 차단하는 기준을 설정할 수 있습니다.

- 미사용 : 행위기반 탐지를 사용하지 않습니다.
- 낮음 / 보통 : 파일 변경 및 삭제 행위를 임계치에 따라 탐지합니다.
- 높음 : 파일 변경 및 삭제 행위를 임계치에 따라 탐지하며 행위기반 탐지와 상황인식 기반 탐지기능을 사용합니다.

※ 각 등급별로 시간과 랜섬웨어가 감염시키는 파일의 개수에 따라 차단하는 등급이 정해집니다. 등급이 높을수록 차단 기준이 강화됩니다.

※ 행위기반 탐지 : 사용자가 PC의 파일을 일반적으로 변조 또는 수정하는 것이 아닌 악성코드나 랜섬웨어에 의해 수정되는 것을 탐지하는 기능입니다.

※ 상황인식기반 탐지 : 특정 프로세스가 좀비 프로세스와 같이 지속적으로 재시작 하는 상황을 탐지하여 프로세스의 재실행을 막는 기능입니다.

【 순간 롤백 사용여부 】 : 랜섬웨어에 피해를 입은 파일을 복구시키는 기능을 사용합니다.

- 순간 백업파일 최대 용량 : 설정 값 이하의 용량을 가진 파일들을 대상으로 순간 롤백합니다.
  - 차단 후 롤백 대기시간 : 차단 후 바로 롤백을 하지않고 설정한 시간이 지나면 롤백하도록 설정합니다.
- ※ 롤백기능 : 차단 후 데이터 변조가 일어난 파일들을 대상으로 복원시켜 주는 기능입니다.

【 랜섬웨어 차단시 프로세스 격리 】 : 랜섬크런처에 의해 차단된 프로세스 실행파일을 격리합니다.

※ 격리 기능은 오탐시에도 동작할 수 있으니 사용 시 유의하여 사용하시기 바랍니다.

【 예외 프로세스 수집 기간 】 : 일정주기동안 실행되는 프로세스를 수집하여 예외 프로세스로 등록합니다.

- 실행되는 프로세스는 예외 리스트로 등록하고, 실행된 전자서명을 수집하여 추후에도 예외합니다.
- 일정주기가 경과되면 탐지정책에 따라 동작합니다.

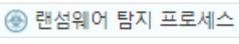
※ 수집 기간동안 탐지정책의 탐지/차단은 동작하지 않으며 기간 경과 후 정상 동작합니다.

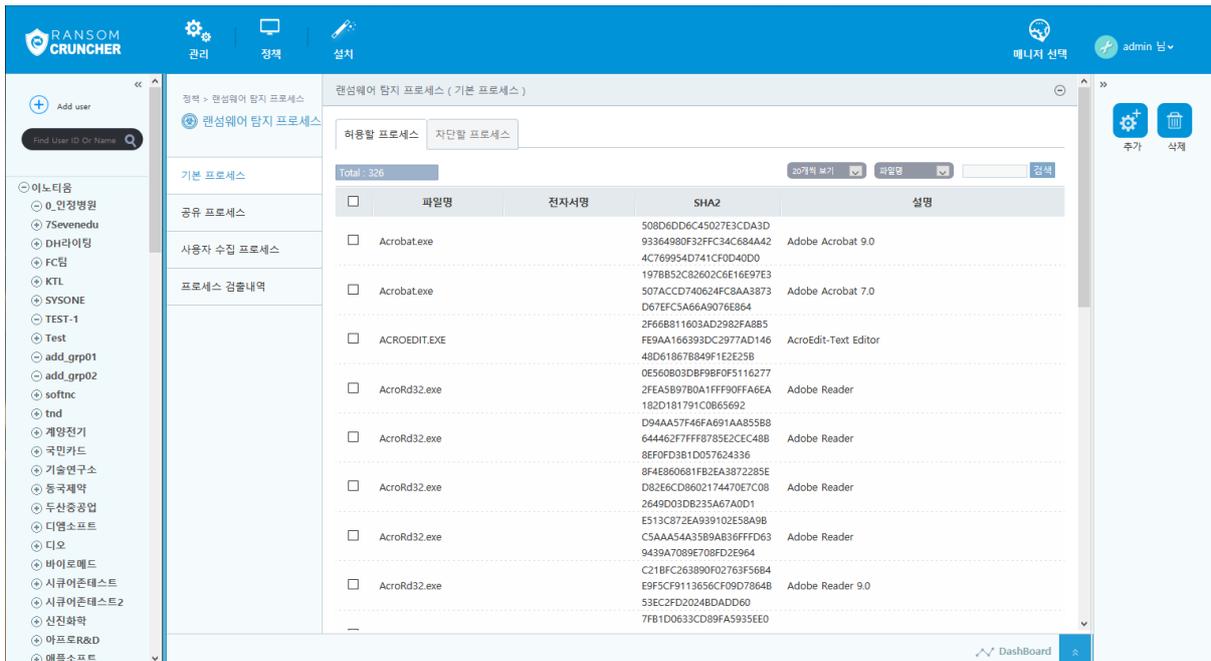
【 랜섬웨어 정책 주기설정 】 : 랜섬크런처에서 탐지정책을 받아오는 주기를 설정합니다.

【 트레이 아이콘 숨기기 】 : 우측 하단에 있는 트레이 아이콘 표시가 숨겨지도록 합니다.

## 2. 랜섬웨어 탐지 프로세스

▶ 이노티움에서 제공하는 기본 프로세스, 사용자 에이전트에서 수집된 사용자 수집 프로세스, 수집된 프로세스를 다른 사용자들과 프로세스를 공유하는 공유 프로세스, 프로세스 검출 내역을 일일/주간/월간별로 확인할 수 있는 프로세스 검출내역으로 프로그램 리스트를 관리하는 페이지입니다.

※ 접근경로 :  [정책]을 클릭 후  [랜섬웨어 탐지 프로세스]을 클릭합니다.



랜섬웨어 탐지 프로세스 ( 기본 프로세스 )

하중할 프로세스 | 차단할 프로세스

Total : 326

파일명	전자서명	SHA2	설명
<input type="checkbox"/> Acrobat.exe		508D6D6C45027E3CDA3D 93364980F32FFC34C684A42 4C769954D741CF0D40DD	Adobe Acrobat 9.0
<input type="checkbox"/> Acrobat.exe		1978B52C82602C6E16E97E3 507ACCD740624FC8AA3873 D67EFC5A66A9076E864	Adobe Acrobat 7.0
<input type="checkbox"/> ACROEDIT.EXE		2F66B811603AD2982FA8B5 FE9AA166393DC2977AD146 48D61867B849F1E2E258	AcroEdit-Text Editor
<input type="checkbox"/> AcroRd32.exe		0E560803DBF98F0F5116277 2FEA5897B0A1FFF90FFA6EA 182D181791C0665692	Adobe Reader
<input type="checkbox"/> AcroRd32.exe		D94AA27F46FA691AA85588 6444627FFF8785E2CEC48B 8EFOFD3B1D057624336	Adobe Reader
<input type="checkbox"/> AcroRd32.exe		8F4E860681FB2EA3872285E D82E6CD8602174470E7C08 2649D03DB235A67A0D1	Adobe Reader
<input type="checkbox"/> AcroRd32.exe		E513C872EA939102E58A98 C5AA4A3589A836FFFD63 9439A7089E708FD2E964	Adobe Reader
<input type="checkbox"/> AcroRd32.exe		C21BFC263890F02763F5684 E9F5CF9113656CF09D7864B 53EC2FD20248DADD60	Adobe Reader 9.0
<input type="checkbox"/> AcroRd32.exe		7FB1D0633CD89FA5935E00	

## 2-1. 기본 프로세스

▶ 기본적으로 제공하는 프로세스 리스트로써 사용자가 수정할 수 없고 소프트웨어 인증 및 행위기반 검사를 받지 않는 프로세스 리스트입니다. 관리자가 추가와 삭제 버튼을 이용하여 리스트를 수정할 수 있습니다.

【 허용할 프로세스 】 : 기본값으로 허용할 프로세스에 대한 리스트입니다. 허용할 프로세스로 등록되면 랜섬크런처에서 예외처리가 되어 소프트웨어 인증 및 행위기반 탐지를 하지 않습니다.

【 차단할 프로세스 】 : 기본값으로 차단할 프로세스에 대한 리스트입니다. 차단할 프로세스로 등록되면 프로세스가 실행이 되는 동시에 랜섬크런처에서 차단을 수행합니다.

- Total 에 프로세스의 총 개수를 표시합니다.
- 검색 기능을 이용해 파일명, SHA2, 전자서명, 설명을 기준으로 로그를 검색할 수 있습니다.

## 2-2. 공유 프로세스

▶ 수집된 프로세스 중 관리자가 모든 사용자들에게 적용해야 된다고 판단되어 다른 사용자에게 프로세스를 공유하는 항목이며 공유 프로세스도 기본 프로세스와 같이 소프트웨어 인증 및 행위기반 검사를 받지 않습니다.

【 허용할 프로세스 】 : 관리자가 추가한 허용할 프로세스에 대한 리스트입니다. 허용할 프로세스로 등록되면 랜섬크런처에서 예외처리가 되어 소프트웨어 인증 및 행위기반 탐지를 하지 않습니다.

【 차단할 프로세스 】 : 관리자가 추가한 차단할 프로세스에 대한 리스트입니다. 차단할 프로세스로 등록되면 프로세스가 실행이 되는 동시에 랜섬크런처에서 차단을 수행합니다.

- Total 에 프로세스의 총 개수를 표시합니다.
- 검색 기능을 이용해 파일명, SHA2, 전자서명, 설명을 기준으로 로그를 검색할 수 있습니다.

## 2-3. 사용자 수집 프로세스

▶ 사용자 수집 프로세스는 정책 > 랜섬웨어 탐지 프로세스와 사용자편집 > 랜섬웨어 탐지 프로세스 두가지 경로에서 확인이 가능합니다.

【 허용할 프로세스 】 : 관리자가 추가한 허용할 프로세스에 대한 리스트입니다. 허용할 프로세스로 등록되면 랜섬크런처에서 예외처리가 되어 소프트웨어 인증 및 행위기반 탐지를 하지 않습니다.

【 차단할 프로세스 】 : 관리자가 추가한 차단할 프로세스에 대한 리스트입니다. 차단할 프로세스로 등록되면 프로세스가 실행이 되는 동시에 랜섬크런처에서 차단을 수행합니다.

- Total 에 프로세스의 총 개수를 표시합니다.
- 검색 기능을 이용해 파일명, SHA2, 전자서명, 설명을 기준으로 로그를 검색할 수 있습니다.

### 2-3-1. 사용자 수집 프로세스(랜섬웨어 탐지 프로세스)

▶ 해당 목록은 사용자가 자신의 에이전트에서 프로세스에 대한 분류가 가능하기 때문에 유동적으로 변화할 수 있습니다. 사용자 수집 프로세스 리스트를 통해 관리자가 프로세스에 대한 관리 및 조치(프로세스 허용 또는 차단)가 가능합니다.

### 2-3-2. 사용자 수집 프로세스(각 사용자별)

▶ 각 사용자 별로 에이전트가 수집한 프로세스 리스트를 보여주며 사용자가 자신의 에이전트에서 프로세스를 분류한 리스트가 표시됩니다.

※ 허용, 차단, 예외처리 프로세스 항목은 사용자 수집 프로세스에서 공통으로 사용하는 항목입니다.

【 허용할 프로세스 】 : 사용자 에이전트에서 수집한 허용할 프로세스 리스트입니다.

※ 허용할 프로세스로 등록된 프로세스는 소프트웨어 인증을 거치지 않습니다.

【 차단할 프로세스 】 : 사용자 에이전트에서 수집한 차단할 프로세스 리스트입니다.

※ 행위기반 탐지를 통해 차단된 프로세스 리스트를 표시합니다.

【 예외처리 프로세스 】 : 사용자 에이전트에서 수집한 예외처리 프로세스 리스트입니다.

※ 예외처리 프로세스 리스트에 등록된 프로세스는 소프트웨어 인증 및 행위기반 탐지 대상에서 제외됩니다.

• Total 에 프로세스의 총 개수를 표시합니다.

• 검색 기능을 이용해 파일명, SHA2, 전자서명, 설명을 기준으로 로그를 검색할 수 있습니다.

### 2-4. 프로세스 검출내역

▶ 사용자 에이전트에서 수집된 프로세스를 바이러스 토탈을 통해 검사하여 결과를 표시해줍니다.

▶ **프로세스 검출내역** : 매니저와 통신하는 모든 사용자 에이전트에서 수집한 프로세스의 검사 결과를 표시합니다. 모든 프로세스 검출내역을 볼 수 있습니다.

※ 프로세스 검출내역의 검출결과는 다음과 같은 결과를 출력합니다.

• **검출** : 바이러스 토탈을 통해 랜섬웨어로 판명된 프로세스

• **미검출** : 바이러스 토탈을 통해 위험이 없는 프로세스 판명된 프로세스

• **조회 불가** : 바이러스 토탈을 통해 프로세스를 검사했지만 아직 프로세스에 대한 정보가 없다고 판명된 프로세스

• **검사 대기** : 아직 검사를 하지 않은 프로세스

• Total 에 프로세스의 총 개수를 표시합니다.

• 검색 기능을 이용해 파일명, SHA2, 검출내용을 기준으로 로그를 검색할 수 있습니다.

▶ **검출내역 - 일일** : 일일단위로 검사한 내역을 확인할 수 있습니다.

▶ **검출내역 - 주간** : 주간단위로 검사한 내역을 확인할 수 있습니다.

▶ **검출내역 - 월간** : 월간단위로 검사한 내역을 확인할 수 있습니다.

## 제 4 장. 에이전트

### A. 랜섬크런처 에이전트

#### 1. Home 화면

▶ 랜섬크런처의 기본 UI 화면입니다. 현재 보안상태와 적용된 보안 등급에 대한 상태를 알 수 있으며 다양한 기능을 아이콘을 클릭하여 상세하게 확인 가능합니다.

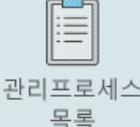


#### 1-1. 보안 등급



- 보안등급에 따라 미사용/낮음/보통/높음으로 출력됩니다.
- 등급에 따라 방패의 파란색이 점차 1/3 씩 채워지며 높음의 경우 방패가 파란색으로 가득 찹니다.

### 1-2. 상단 메뉴

- 
 시작프로세스 관리 : 시작프로세스를 확인하고 사용/미사용 설정이 가능합니다.
- 
 관리프로세스 목록 : 감시/인증/차단/예외 프로세스를 관리할 수 있습니다.
- 
 로그 : 사용자/랜섬웨어/모니터링 로그를 확인합니다.
- 
 : 랜섬크런처 UI 화면을 종료할 수 있습니다.

### 1-3. 하단 메뉴

- 
 프로그램 정보 : 프로그램 버전과 매니저 정보, 사용자 계정명을 출력합니다.
- 
 격리소/대피소 보호 : 격리소/대피소 보호 설정/해제 기능을 수행하며 추가적으로 설정 폴더도 보호 설정/해제합니다.
- 
 환경설정 : 매니저에서 할당된 정책을 확인 가능하며, SA 버전의 경우 정책을 설정할 수 있습니다. 추가적으로 매니저 주소 및 사용자 계정명을 변경 가능합니다.

## 2. 설정 화면

▶ 랜섬크런처의 세부 설정을 할 수 있는 화면입니다. 분류된 프로세스 리스트와 로그를 확인할 수 있으며 랜섬크런처가 관리하는 폴더를 확인 및 초기화 할 수 있습니다.

### 2-1. 시작프로세스 관리

▶ PC 부팅 시 시작되는 프로세스의 리스트를 나열합니다. 사용자는 해당 정보를 확인하고 사용/사용안함 설정하여 부팅 시점의 보안성을 향상 할 수 있습니다.

프로세스 경로	전자서명	상태	사용
C:/Program Files (x86)/iniLINE/CrossEX/crossex/CrossEXServ ...	iniLINE Co., Ltd.	사용	<input checked="" type="checkbox"/>
C:/Users/User13/AppData/Local/Microsoft/Teams/Update.exe - ...	서명없음	사용	<input checked="" type="checkbox"/>
C:/Program Files/Daou/Messenger/Daou/Messenger.exe	Daou Technology INC.	사용안함	<input type="checkbox"/>
C:/Program Files (x86)/Kakao/KakaoTalk/KakaoTalk.exe	Kakao corp.	사용	<input checked="" type="checkbox"/>
C:/WINDOWS/System32/DriverStore/FileRepository/realtekserv ...	Realtek Semiconductor Corp.	사용	<input checked="" type="checkbox"/>
C:/Program Files/CONEXANT/SAll/SACpl.exe	Conexant Systems, Inc.	사용	<input checked="" type="checkbox"/>
C:/Program Files/Conexant/cAudioFilterAgent/cAudioFilterAg ...	Conexant Systems LLC	사용	<input checked="" type="checkbox"/>
C:/Program Files/Everything/Everything.exe	David Carpenter	사용안함	<input type="checkbox"/>
C:/Program Files (x86)/Common Files/Adobe/AdobeGCCClient/AG ...	Adobe Inc.	사용	<input checked="" type="checkbox"/>
C:/Program Files (x86)/Common Files/Adobe/OOBE/PDApp/UWA/U ...	Adobe Systems Incorporated	사용	<input checked="" type="checkbox"/>
%ProgramFiles%/Elantech/ETDCtrl.exe	서명없음	사용안함	<input type="checkbox"/>
%windir%/system32/SecurityHealthSystray.exe	서명없음	사용안함	<input type="checkbox"/>
C:/Program Files (x86)/Epson Software/Event Manager/EEvent ...	서명없음	사용안함	<input type="checkbox"/>



**【 사용 】**: PC 부팅 시 해당 경로의 프로세스는 실행됩니다.

해당 버튼 클릭 시 사용안함 상태로 변경됩니다.



**【 사용안함 】**: PC 부팅 시 해당 경로의 프로세스는 실행되지 않습니다.

해당 버튼 클릭 시 사용 상태로 변경됩니다.

### 2-2. 관리프로세스 목록

▶ 랜섬크런처에서 수집한 프로세스 리스트를 출력합니다.

프로세스는 각각 감시/인증/차단/예외 프로세스로 나뉘며 아래와 같습니다.

**【 감시 】**: 소프트웨어 인증을 통과하지 못하여 차단된 프로세스 리스트입니다.

**【 인증 】**: 소프트웨어 인증을 통과하여 허용된 프로세스 리스트입니다.

해당 프로세스는 행위기반으로 감시하고, 랜섬웨어 행위 시 차단 프로세스 목록으로 이동 및 차단됩니다.

**【 차단 】**: 행위기반 탐지간 랜섬웨어 행위를 확인하여 차단된 프로세스 리스트입니다.

**【 예외 】**: 특정 프로세스를 소프트웨어 탐지/행위기반으로 탐지하지 않도록 설정한 예외 리스트입니다.

※ 인증 프로세스: 해당 프로세스는 행위기반으로 탐지되므로 랜섬웨어 행위 시 차단됨

※ 예외 프로세스: 해당 프로세스는 탐지하지 않으므로 랜섬웨어 행위 시 파일 감염됨

### 2-2-1. 감시 프로세스 목록

시간	이름	서명자	경로	HASH	차단	인증	삭제
2021-06-21 10:07:12	Everything.exe	David Carpenter	C:/Program Files ...	4e7f8 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- [차단]: 해당 프로그램을 악성프로그램으로 분류 하여 동작 시 즉시 차단하도록 등록 합니다.
- [인증]: 해당 프로그램을 정상프로그램으로 분류 하여 실행 가능하도록 인증 등록 합니다.  
인증한 프로그램은 지속적으로 이상행위를 탐지하여, 이상행위 발견 시 즉각 차단됨
- [삭제]: 해당 프로그램을 감시 목록 리스트상에서만 삭제합니다. 실제 파일을 삭제 하는 것이 아니며 대상 프로그램이 다시 실행 될 때 새로 검사를 진행 하여 분류 합니다.

### 2-2-2. 인증 프로세스 목록

시간	이름	서명자	경로	HASH	예외	삭제
2021-09-14 14:34:02	g2mupload.exe	LogMeIn, Inc.	C:/Users/User13/ ...	EBEAF ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2021-09-14 14:03:07	Calculator.exe	서명없음	C:/Program Files ...	D1017 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2021-09-14 09:03:32	EEventManage ...	서명없음	C:/Program Files ...	E2A36 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2021-09-14 09:03:22	CrossEXServ ...	iniLINE Co., Ltd.	C:/Program Files ...	B365C ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2021-09-14 09:03:17	RSSerCmd.exe	Advanced Micro Devices, Inc.	C:/Program Files ...	9B7B5 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2021-09-14 09:03:12	EPPCCMON.EXE	SEIKO EPSON CORPORATION	C:/Program Files ...	0CC13 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2021-09-13 11:52:33	EPECLINK.EXE	SEIKO EPSON Corporation	C:/Program Files ...	405F5 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2021-09-13 11:44:42	Setup.exe	SEIKO EPSON CORPORATION	C:/Users/User13/ ...	A44B5 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>

- [예외] : 해당 프로그램을 정상 프로그램으로 식별하여 프로그램 검사 없이 실행 되도록 등록
- [삭제] : 해당 프로그램을 감시 목록 리스트상에서만 삭제합니다. 실제 파일을 삭제 하는 것이 아니며 대상 프로그램이 다시 실행 될 때 새로 검사를 진행 하여 분류 합니다.

### 2-2-3. 차단 프로세스 목록

시간	이름	서명자	경로	HASH	예외	인증	삭제
2021-09-14 02:42:40	moc.exe	서명 없음	C:/Qt/5.5/msvc20 ...	b9a77 ...	<input checked="" type="checkbox"/>	<input type="radio"/>	<input type="checkbox"/>

- [예외] : 해당 프로그램을 정상 프로그램으로 식별하여 프로그램 검사 없이 실행 되도록 등록
- [인증] : 해당 프로그램을 정상프로그램으로 분류 하여 실행 가능하도록 인증 등록 합니다. 인증한 프로그램은 지속적으로 이상행위를 탐지하여, 이상행위 발견 시 즉각 차단됨
- [삭제] : 해당 프로그램을 감시 목록 리스트상에서만 삭제합니다. 실제 파일을 삭제 하는 것이 아니며 대상 프로그램이 다시 실행 될 때 새로 검사를 진행 하여 분류 합니다.

### 2-2-4. 예외 프로세스 목록

시간	이름	서명자	경로	HASH	차단	인증	삭제
2021-08-11 10:51:07	DaouMessage ...	Daou Technology INC.	C:/Program Files ...	3bcd4 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-08-11 09:43:23	devenv.exe	서명없음	C:/Program Files ...	b4c72 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-08-02 06:23:26	KakaoTalk.exe	Kakao corp.	C:/Program Files ...	a49b5 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-07-30 10:56:43	chrome.exe	Google LLC	C:/Program Files ...	a35c8 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-07-29 09:04:03	oCam.exe	OORT Inc.	C:/Program Files ...	635CD ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-07-29 04:27:54	node.exe	OpenJS Foundation	C:/Program Files ...	87c50 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-07-29 04:27:54	setup.exe	서명없음	C:/Program Files ...	9ddc3 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-07-07 08:57:53	dts_apo_task.exe	DTS, Inc.	C:/Program Files ...	ec76d ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-07-07 08:57:53	g2brun_insta ...	Public Procurement Service Republic of Korea	C:/Users/User13/ ...	c41d1 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2021-07-07 08:57:53	g2brun_insta ...	Public Procurement Service Republic of Korea	C:/Users/User13/ ...	51f40 ...	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

- [차단]: 해당 프로그램을 악성프로그램으로 분류 하여 동작 시 즉시 차단하도록 등록 합니다.
- [인증]: 해당 프로그램을 정상프로그램으로 분류 하여 실행 가능하도록 인증 등록 합니다.  
인증한 프로그램은 지속적으로 이상행위를 탐지하여, 이상행위 발견 시 즉각 차단됨
- [삭제]: 해당 프로그램을 감시 목록 리스트상에서만 삭제합니다. 실제 파일을 삭제 하는 것이 아니며 대상 프로그램이 다시 실행 될 때 새로 검사를 진행 하여 분류 합니다.

### 2-3. 로그보기

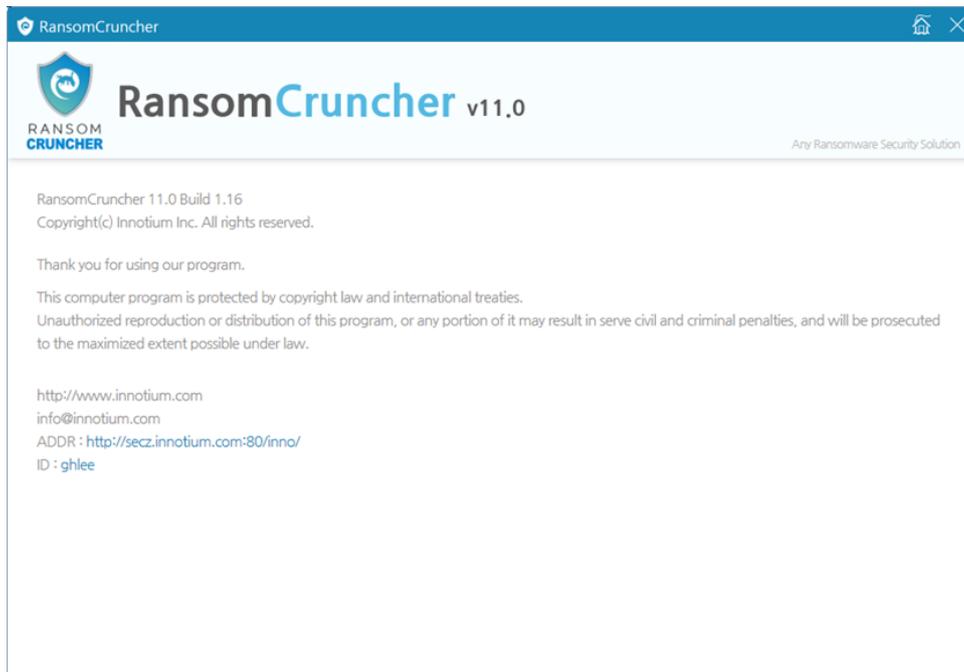
- ▶ 랜섬크런처에서 수집한 모든 로그가 표시되며 프로세스의 상세 내역을 확인할 수 있습니다.
- ※ 로그에 나타나는 프로세스의 수준은 다음과 같습니다.

시간	로그타입	프로세스/정책	작업내용/경로	결과
2021-09-14 14:49:22	<input checked="" type="checkbox"/> 기록	git.exe	C:/Program Files ...	소프트웨어인증 허용
2021-09-14 14:49:22	<input checked="" type="checkbox"/> 기록	git.exe	C:/Program Files ...	소프트웨어인증 허용
2021-09-14 14:48:02	<input checked="" type="checkbox"/> 기록	g2mupdate.exe	C:/Users/User13/ ...	소프트웨어인증 허용
2021-09-14 14:42:40	<input type="checkbox"/> 정보	기본동작	프로그램 시작[Ver 11.0 ...	동작정보 기록
2021-09-14 14:42:38	<input type="checkbox"/> 정보	기본동작	동일버전 업데이트 [11.0 ...	동작정보 기록
2021-09-14 14:42:27	<input type="checkbox"/> 정보	기본동작	프로그램 종료	동작정보 기록
2021-09-14 14:34:02	<input checked="" type="checkbox"/> 기록	g2mupload.exe	C:/Users/User13/ ...	소프트웨어인증 허용
2021-09-14 14:32:07	<input checked="" type="checkbox"/> 기록	git.exe	c:/program files ...	소프트웨어인증 허용
2021-09-14 14:29:22	<input checked="" type="checkbox"/> 기록	git.exe	C:/Program Files ...	소프트웨어인증 허용
2021-09-14 14:09:22	<input checked="" type="checkbox"/> 기록	git.exe	C:/Program Files ...	소프트웨어인증 허용

<p><b>정보</b></p>	<p>프로그램 시작/종료, 업데이트와 같은 사용자 동작에 따른 로그 리스트입니다.</p>
<p><b>탐지</b></p>	<p>소프트웨어 인증 및 행위기반 탐지로 인한 로그 리스트입니다. 블랙리스트 차단, 복원기록에 대한 내용도 함께 기록됩니다.</p>
<p><b>기록</b></p>	<p>프로그램 동작 내용을 기록하는 로그 리스트입니다. 프로세스의 실행 시기를 기록하므로 가장 많은 로그가 기록되며, 이슈 추적에 사용됩니다. 로그 데이터가 많이 저장되므로 로컬 DB 에만 기록되고 매니저에 기록되지 않는다는 특징을 가지고 있습니다.</p>

## 2-4. 프로그램 정보

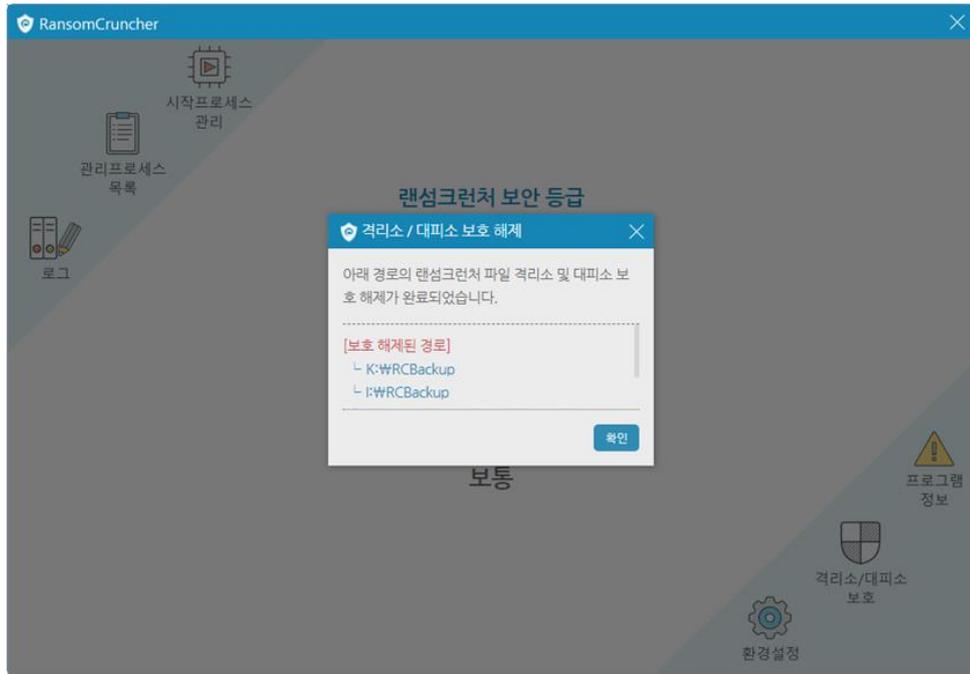
▶ 랜섬크런처 상세 빌드 정보와 매니저 주소, 사용자 계정명을 출력합니다.



## 2-5. 격리소 대피소 보호

▶ 랜섬크런처의 순간 복원 기능을 위한 대피소/격리소를 보호 설정/해제 기능을 지원합니다.

- ※ 대피소 : 프로세스가 보호하는 확장자의 파일을 변조할 때 임시로 대피소에 파일을 저장합니다.  
대피소의 최대 용량은 1GB 이며, 최대 용량 초과시 오래된 파일부터 삭제됩니다.
- ※ 격리소 : 랜섬웨어 행위를 차단하고 해당 프로세스가 변조 및 생성한 파일을 격리소로 이동합니다.



## 2-6. 환경설정

▶ 매니저에서 설정한 랜섬웨어 탐지 정책을 출력합니다.

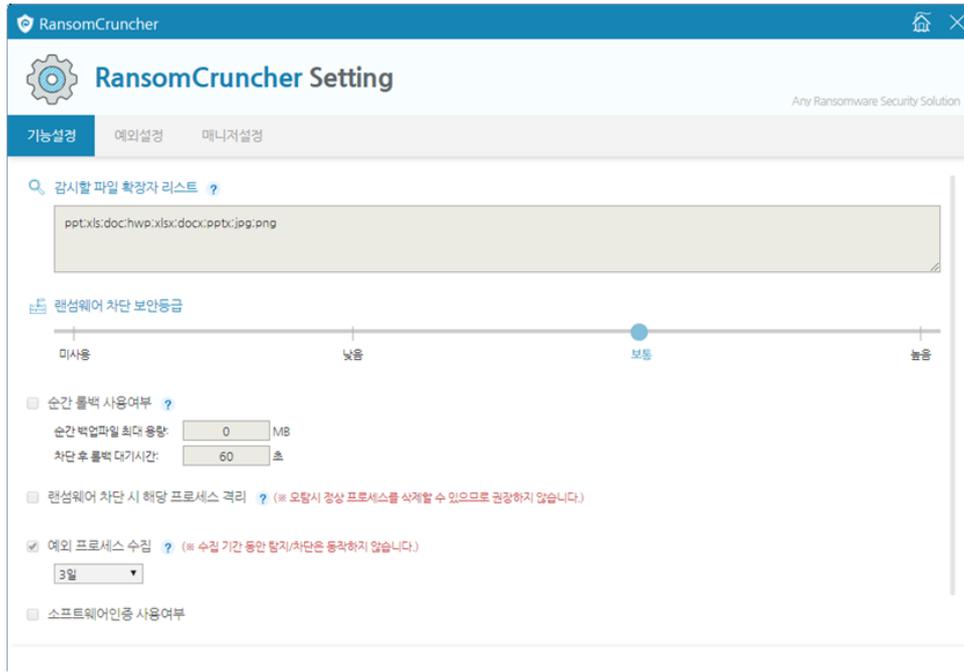
매니저 주소 및 사용자 계정 명을 변경할 수 있습니다.

SA 버전의 경우 랜섬웨어 탐지 정책을 설정하거나 매니저에 연결 할 수 있습니다.

### 2-6-1. 기능설정

▶ 랜섬웨어 정책 중 기능 관련 설정을 출력합니다.

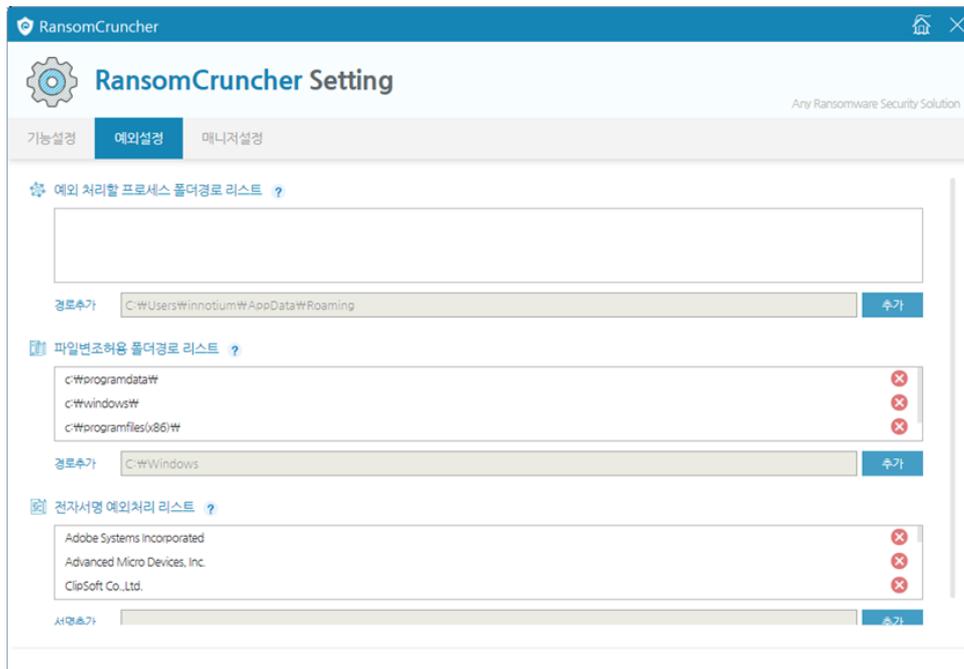
- 1) 감시할 파일 확장자 리스트  
: 입력된 파일 확장자의 파일을 보호하여 순간 롤백 기능을 지원하며, 해당 파일의 확장자 다량 변조하면 랜섬웨어로 판단됨.
- 2) 랜섬웨어 차단 보안 등급  
: 일정 시간 내에 특정 파일의 수를 변조하면 랜섬웨어로 판단하는 기준의 강도를 의미함.
- 3) 순간 롤백 사용여부  
: 프로세스가 감시할 파일 확장자의 파일을 변조 행위시 변조 이전 파일을 대피소에 저장한다.  
+ 순간 백업파일 최대 용량: 대피소에 저장할 파일의 최대 용량, 최대 용량보다 큰 파일은 저장하지 않는다. (단위 MB)  
+ 차단 후 롤백 대기시간: 차단 후 지정된 시간이 경과하고 나서 순간 롤백 기능이 동작한다. (단위: 초)
- 4) 랜섬웨어 차단 시 해당 프로세스 격리  
: 차단 후 해당 프로세스의 파일 명을 변조한다(ex. ransom.exe > ransom.exe\_tmp)
- 5) 예외 프로세스 수집  
: 제품 설치하고 일정 기간동안 동작하는 프로세스를 예외 리스트에 추가한다.  
동작한 프로세스의 전자서명도 수집한다. (단위: 일)  
수집일이 경과하면 지정된 정책에 따라 랜섬웨어를 탐지한다.
- 6) 소프트웨어인증 사용여부  
: 프로세스의 시그니처를 체크하여 차단(감시 목록)/허용(인증 목록)하는 기능을 의미함.  
허용된 프로세스는 행위기반으로 감시되며, 랜섬웨어 행위시 차단(차단 목록)된다.



### 2-6-2. 예외설정

▶ 랜섬웨어 정책 중 예외 관련 설정을 출력합니다.

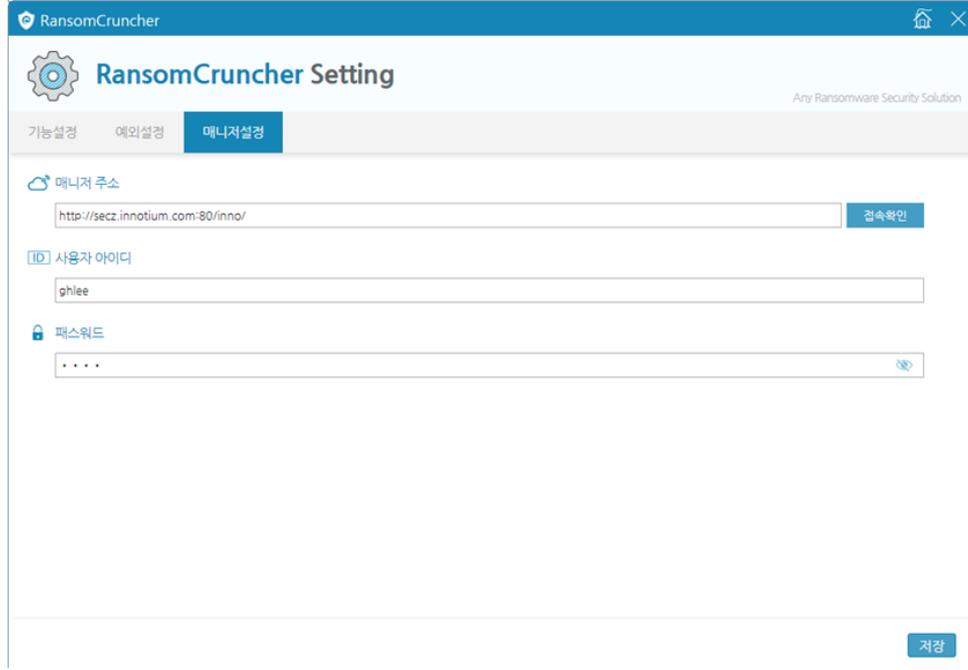
- 1) 예외 처리할 프로세스 폴더경로 리스트  
: 해당 경로에서 실행된 프로세스는 예외처리 함을 의미함. (하위 폴더 포함)
- 2) 파일변조허용 폴더경로 리스트  
: 해당 경로에서 변조된 파일은 예외처리 됨을 의미함. (하위 폴더 포함)
- 3) 전자서명 예외처리 리스트  
: 실행된 프로세스의 전자서명과 일치하면 예외처리 됨을 의미함.



### 2-6-3. 매니저설정

▶ 랜섬크런처와 연결된 매니저의 주소와 사용자 아이디를 변경 가능합니다.

- 1) 접속확인: 매니저 주소에 아이디와 비밀번호를 통한 로그인 확인.
- 2) 저장: 로그인을 통한 확인 후 계정정보를 저장함.



## 제 5 장. 프로그램 정보

### A. 프로그램 정보

랜섬크런처는 대한민국의 저작권법과 국제 저작권 조약으로 보호받습니다. (주)이노티움의 사전 서면 동의 없이 프로그램 또는 프로그램의 부속된 자료 파일이나 문서 내용을 수정하거나 변형, 복사, 배포할 수 없습니다.

프로그램 사용중에 어떤 문의 사항이 있으시면, 아래로 연락하여 주십시오.

### B. 주의 사항

- 설명서(매뉴얼)를 반드시 숙지하신 후 프로그램을 사용하십시오. 제품에 대한 최신 정보 및 제품 업그레이드 소식 등은 당사 홈페이지([www.innotium.com](http://www.innotium.com))를 통하여 제공됩니다.
- 랜섬크런처를 설치하기 전에 중요한 데이터는 반드시 미리 복사해 두시길 권장합니다. 설치 시 사용자의 부주의한 실수로 잃어버린 데이터에 대해 본사에서는 어떠한 책임도 지지 않습니다.
- 본 프로그램의 지속적인 업그레이드로 인해 일부 내용이 본 설명서와 다를 수 있습니다.

### C. 시스템 사양

항목	제품 최소 사양
CPU	Xeon 4Core 이상
RAM	16GB 이상
HDD 여유공간	250GB 이상 (SSD 권장)
파일시스템	-
운영체제	Linux(CentOS, redhat)
DBMS	MariaDB 10.X
NIC	1GB, 4Port

### D. 연락처

- 홈페이지 : <http://www.innotium.com>
- 이메일 : [help@innotium.com](mailto:help@innotium.com)
- 전화 : 02-3283-2021