침해사고 대응 업무의 이해

침해사고 대응의 과정

준비, 대응, 개선

침해사고 대응 준비

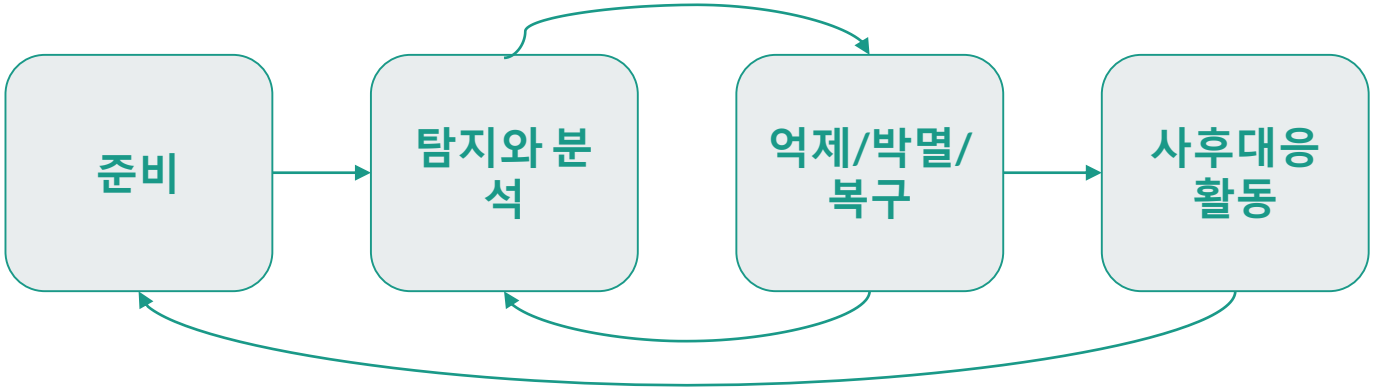
프로세스 준비

- **사이버 복원력 : 사이버 리소스를 포괄하는 시스템에서 불리한 상황이나 스트레스, 공격, 침해를 예상하고 견디며 복구하고 적응하는 능력**

프로세스 유형

예방 - 탐지 - 대응은 사이버 환경을 방어하기 위한 가장 기본적인 프로세스이다.

침해사고 대응 프로세스(NIST 모델)



인력 준비

1. 기술적으로 훈련이 되어야한다.
2. 사고 대응 정책과 절차를 교육받아야한다.
3. 구성원들이 서로 의견을 나누고 협력해야 한다.
4. 각 부서 및 이해 당사자와 의견을 주고받아야 한다.
5. 정보관리 시스템을 잘 활용해야한다.

기술 준비

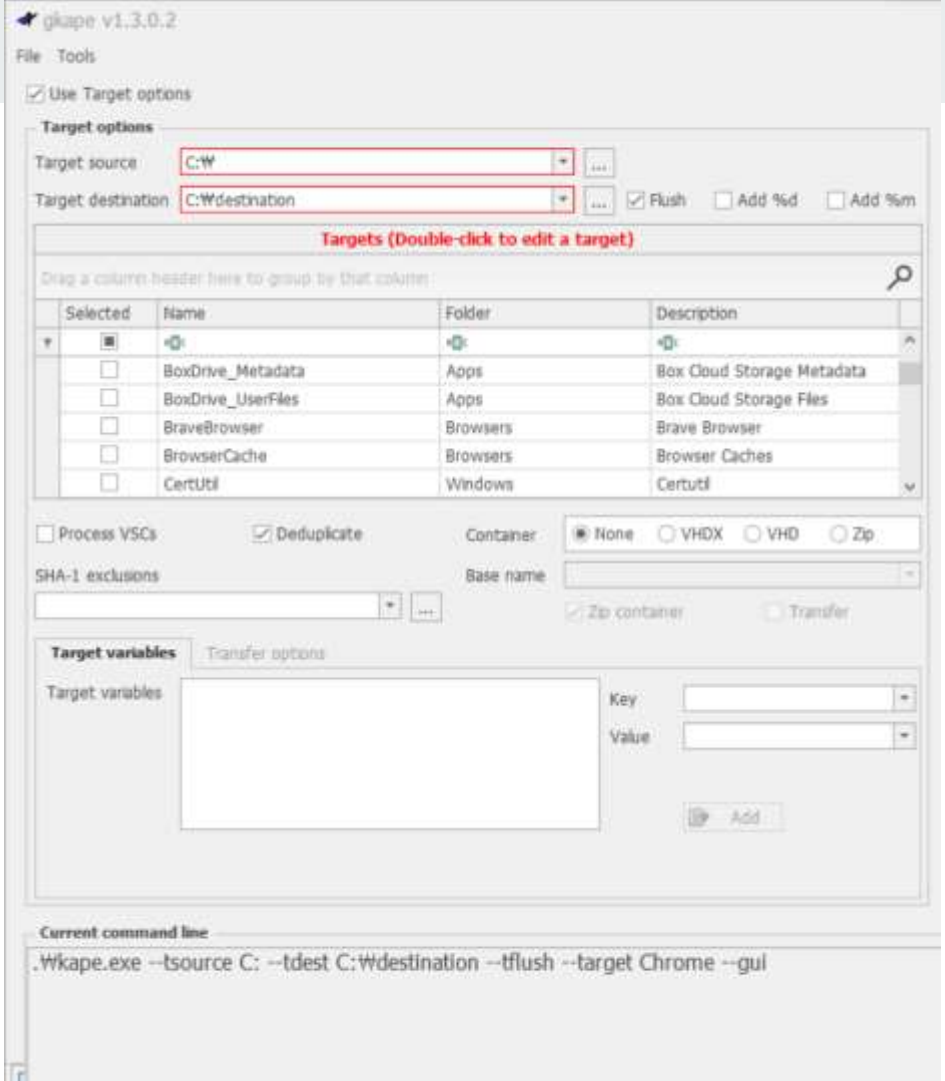
1. 로그 및 네트워크 패킷 등 네트워크에서 발생한 이벤트 수집
2. 프로세스, 서비스, 포트를 이해하기 위해 주요 시스템 문서화
3. 취약점 점검 및 침투테스트(퍼플팀 구성)
4. 물리적 장비 및 소프트웨어 환경 준비

대응 기법

- 원격 선별 진단
- 메모리 수집
- 디스크 이미징
- 네트워크 모니터링
- 자료 분석

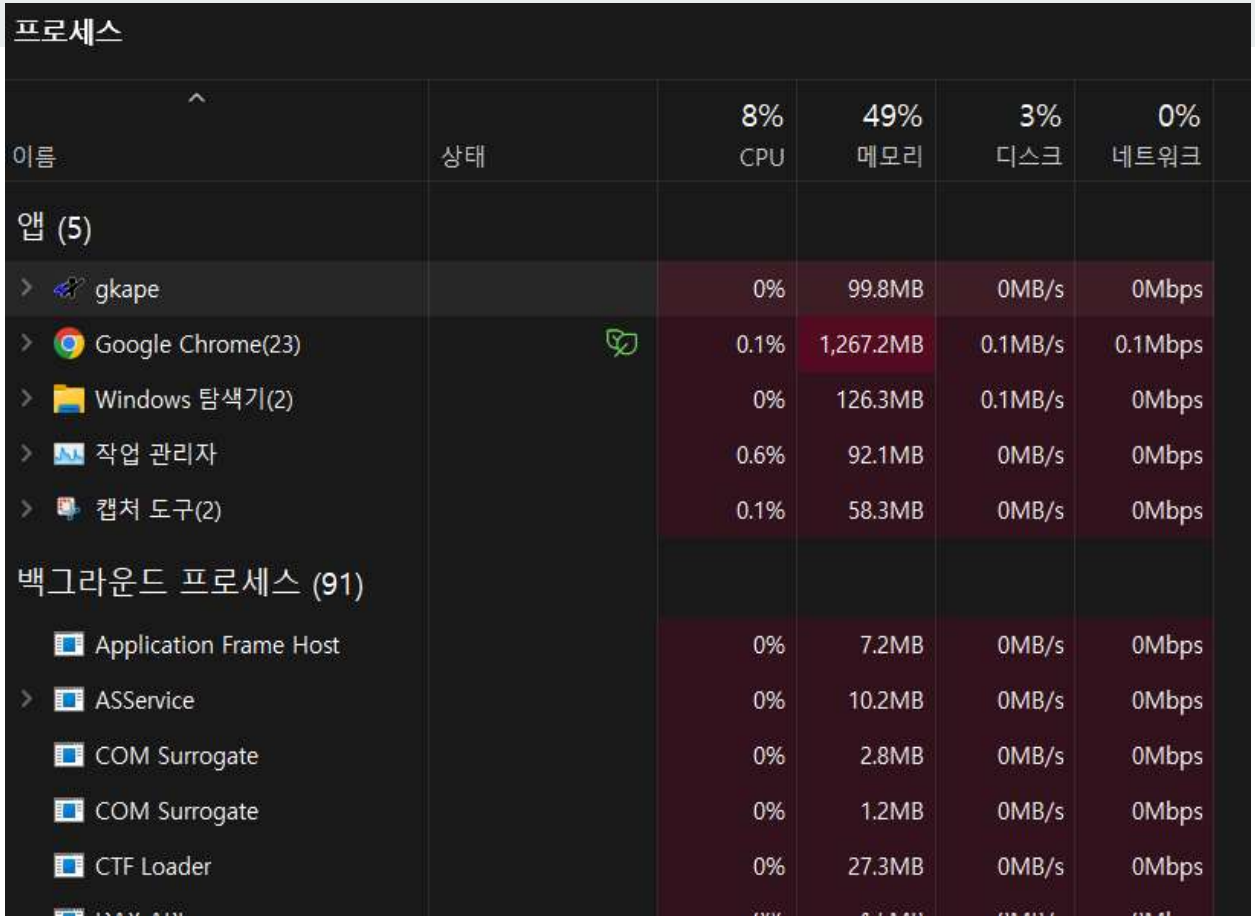
선별 수집 및 분석 실습

KAPE 원격 선별 수집 도구



메모리 덤프

+ 물리적인 방법



AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- C:₩
  - NONAME [NTFS]
    - [orphan]
    - [root]
    - [unallocated space]

File List

Name	Size	Type	Date Modified
$BadClus	0	Regular File	2022-01-01 오전 8:...
$Bitmap	7,015	Regular File	2022-01-01 오전 8:...
$Boot	8	Regular File	2022-01-01 오전 8:...
$I30	8	NTFS Index...	2023-09-12 오전 5:...
$LogFile	65,536	Regular File	2022-01-01 오전 8:...
$MFT	210,944	Regular File	2022-01-01 오전 8:...
$MFTMirr	4	Regular File	2022-01-01 오전 8:...
$Secure	1	Regular File	2022-01-01 오전 8:...
$TXF_DATA	1	NTFS Logg...	2023-09-12 오전 5:...
$UpCase	128	Regular File	2022-01-01 오전 8:...

Custom Content Sources

Evidence:File System|Path|File | Options

New Edit Remove Remove All Create Image

Properties | Hex Value I... | Custom Co...

```
00 | 30 00 00 00 01 00 00 00-00 10 00 00 01 00 00 00 | 0···············
10 | 10 00 00 00 A0 00 00 00-A0 00 00 00 01 00 00 00 | ···· ··· ·····
20 | 3F ED 00 00 00 00 02 00-78 00 5A 00 01 00 00 00 | ?í·····x·Z·····
30 | 05 00 00 00 00 00 05 00-63 32 A0 62 56 66 D9 01 | ·····c2 bVfÙ·
40 | B0 95 16 E2 95 E3 D9 01-B0 95 16 E2 95 E3 D9 01 | °··â·ãÙ·°··â·ãÙ·
50 | B0 95 16 E2 95 E3 D9 01-00 30 00 00 00 00 00 00 | °··â·ãÙ··0·····
60 | 00 30 00 00 00 00 00 00-26 00 00 00 00 00 00 00 | ·0·····&·····
70 | 0C 02 44 00 55 00 4D 00-50 00 53 00 54 00 7E 00 | ··D·U·M·P·S·T·~·
80 | 31 00 2E 00 54 00 4D 00-50 00 5A 00 00 00 00 00 | 1·.·T·M·P·Z·····
90 | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 | ················
a0 | 18 00 00 00 03 00 00 00-01 00 00 00 00 00 00 00 | ················
```

Cursor pos = 0

isted: 33Selected: 0C:₩/NONAME [NTFS]/[root]

NUM

지속적 개선

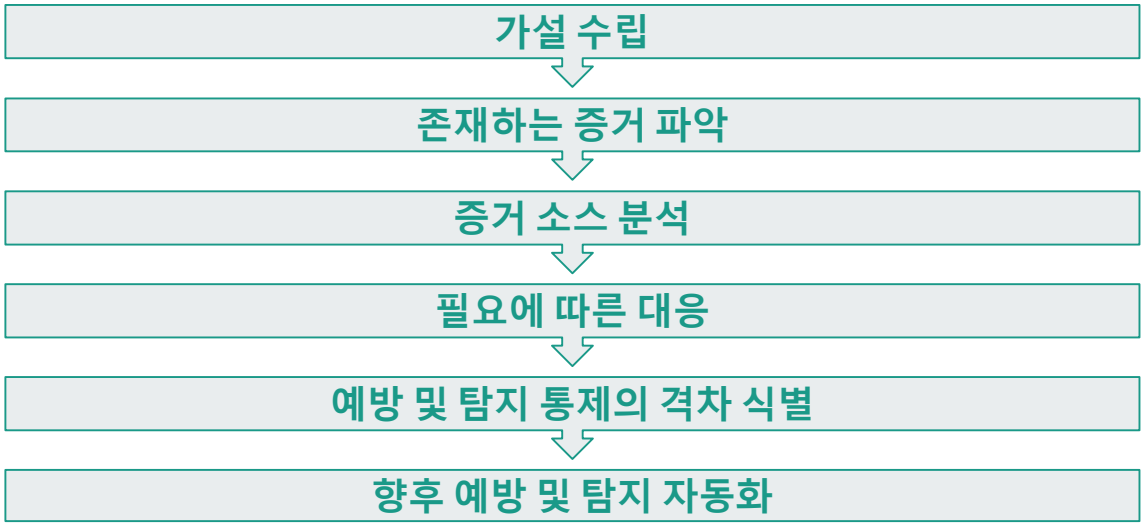
1. 침해사고 대응자는 사고 처리에 대한 보고서를 작성해야한다.
2. 사용한 도구 및 대응 방안에 대한 평가를 내리고 프로세스를 개선한다.
3. 계정들에 대한 적절한 통제, 세분화 및 격리로 예방활동을 해야한다.

예방 활동

예방- 탐지- 대응 순환

- 위협 헌팅 프로세스
- 공격자 모방

위협 헌팅 프로세스



공격자 모방

기본적으로 레드팀과 블루팀 훈련이 있음

- **Atomic Red Team**
- **Caldera**

ATOMIC RED TEAM 살펴보기 더 알아보기 원자학 뉴스 레터 SLACK에 가입하세요

Atomic Red Team 살펴보기

이 사이트는 MITRE ATT&CK® 프레임워크 및 지원하는 플랫폼 에 매핑되어 있는 Atomic Red Team™ 테스트 라이브러리를 탐색하고 탐색하는 데 도움을 주기 위해 설계되었습니다 .

caldera.readthedocs.io/en/latest/

CALDERA

최신

문서 검색

이용안내
칼데라 설치
시작하기

문서 » CALDERA 문서에 오신 것을 환영합니다! GitHub에서 편집

CALDERA 문서에 오신 것을 환영합니다!

CALDERA™는 자율적인 위반 및 시뮬레이션 훈련을 쉽게 실행하도록 설계된 사이버 보안 프레임워크입니다. 수동 레드팀 참여 또는 자동화된 사고 대응을 실행하는 데에도 사용할 수 있습니다. CALDERA는 MITRE ATT&CK™ 프레임워크를 기반으로 구축되었으며 MITRE에서 활발히 진행되는 연구 프로젝트입니다.

프레임워크는 두 가지 구성 요소로 구성됩니다.

1. **핵심 시스템** . 이는 REST API 및 웹 인터페이스를 갖춘 비동기 명령 및 제어(C2) 서버를 포함하는 프레임워크 코드입니다.