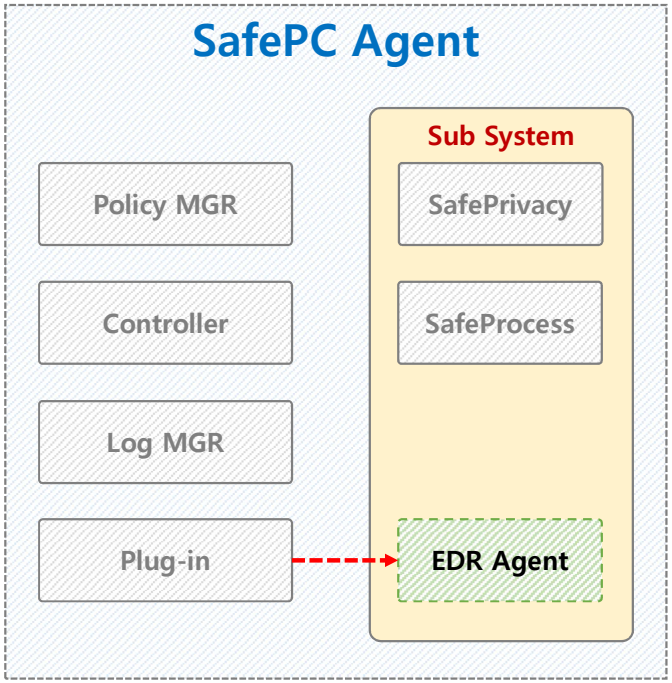
EDR 구현 시 SafePC 통합/연동 방안

작성자 : 장욱 (에이전트 1팀/기술연구소)
작성일 : 2017년 12월 1일

1. SafePC, EDR Agent 연동 방안 (Overview)



- 기존의 SafePC 는 Main Platform 으로 동작
- SafePrivacy, SafeProcess 등은 SafePC 의 Plug-in 방식으로 동작 (Sub System)
- EDR Agent 또한 SafePC 의 Sub System 으로 동작
  - 기존의 SafePC 의 기능을 활용 가능
  - SafePC 의 Plug-in 기능으로 고객사 별로 on/off
- EDR 의 기능중 다음은 최대한 Agent 의 기능을 활용
  - 대응/통제 : 기존 SafePC 의 매체 제어 기능을 통해 Isolate/Block 수행
  - 정책 및 로그 송수신 : NicsWS 프레임웍을 통해 송수신

2. SafePC, EDR Agent 연동 방안 Cont. (모듈 구성도 설명)

- EDR Agent 의 주요 모듈은 다음으로 구성
  - Log Generator : Monitor 모듈로 부터 전달받은 Raw Log 데이터를 취합, 1차 가공 후 저장
  - Policy Manager : NicsWs 를 통해 정책을 요청/수신 (서버 Response 에 대한 "즉시 정책 수신" 요청)
  - Controller : Isolate/Block 등의 요청 수신 시, 실제로 매체 및 네트워크 제어를 수행 (직접 또는 SafePC 모듈을 통해)
  - Monitor : 다음 각 sub system 요소에 대해 모니터링과 로깅을 수행
    - Process List Manager : 프로세스 LifeCycle 모니터링 및 Raw Log 생성 (Log Generator 로 전달)
    - File Monitor : 파일 모니터링 및 Raw Log 생성 (Log Generator 로 전달)
    - Registry Monitor : 레지스트리 접근 모니터링 및 Raw Log 생성 (Log Generator 로 전달)
    - Network Monitor : 네트워크 사용 모니터링 및 Raw Log 생성 (Log Generator 로 전달)
    - Abnormal Behavior Detector : 이상행위 (권한 상승, 민감한 API 호출 등) 모니터링 및 Raw Log 생성 (Log Generator 로 전달)
- EDR Agent 에서 SafePC 주요 연동부는 다음처럼 구성
  - **EDR 정책 전송 (NicsWS 사용 : WAS 기반 정책 송수신)**
  - **EDR 대응 기능 : SafePC 의 매체 제어 (Controller) 기능 활용**
  - **EDR 로그 수집 기능 :**

    Monitor 모듈에서 Raw Log 생성

    Log Generator 에서 Raw Log 1 차 가공후 NicsWs 를 통해 전송
  - **EDR 모니터링 : Monitor 모듈에서 자체 기능 또는 SafePC 가 제공하는 일부 기능을 통해 각 요소별 로 모니터링 및 로그 생성 수행**

3. SafePC, EDR Agent 연동 방안 Cont. (모듈 구성도 그림)