[별지 제3호] 물품공급 또는 기술지원협약서

ㅇ 사 업 명 : 노후 보안관제시스템 현행화 사업
ㅇ 발주기관 : 공정거래위원회
ㅇ 제조사 또는 공급사 : ㈜시큐레터

제1조(목적) 이 협약은 **망간 자료전송보안 솔루션** 1식 등에 대하여 발주기관은 발주자로서 제조사 또는 공급사는 특수한 능력·품질의 납품능력을 보유하거나 제조할 수 있는 제조사(또는 공급사)로서 위 사업의 낙찰자에게 물품공급 또는 기술지원을 원활히 제공토록 하는 것을 목적으로 한다.

제2조(사용 및 협약의 범위) ①이 협약은 위 사업의 물품공급 또는 기술지원에 한해 사용범위를 제한한다.

②위 물품 중 제조사 또는 공급사가 낙찰자에게 물품공급 또는 기술지원을 해야하는 범위는 규격서(시방서)에 반영된 특수한 능력·품질의 납품능력이 요구되는 부분으로 한다.

③제2항에 의한 특수한 능력·품질 등의 납품능력이 요구되는 범위에 대하여 이견이 있는 경우에는 발주기관의 해석 및 판단에 따른다.

제3조(협약금액) 제2조에 따른 제조사 또는 공급사의 물품공급 또는 기술지원 범위에 대한 협약금액은 특수능력·품질 부분의 비중 등을 고려하여 발주기관과 제조사 또는 공급사가 협의하는 금액 **(조달구매)**으로 한다.

제4조(물품공급 또는 기술지원확약서 발급) 위 사업의 낙찰자와 제조사 또는 공급사는 이 약정의 범위 및 공정한 거래질서 등에 반하지 아니하는 범위 내에서 물품공급 또는 기술지원을 하기로 협의하고, 제조사 또는 공급사는 물품공급 또는 기술지원확약서를 낙찰자에게 발급하여야 한다.

2024 년 3 월 6 일

발주기관 : 공정거래위원회 (인)

제조사 또는 공급사 : 시큐레터 (인)

규 격 서(시방서)

2024년 3월

공정거래위원회

o 프로젝트명 : 노후 보안관제시스템 현행화 사업

o 금　　액 : 조달구매

o 목　　적 : 망간 자료 전송시 문서에 포함된 고도화된 악성코드에 대해 사전 탐지 및 차단

o 특정제품필요성 : 공정거래위원회 도입된 기존 자료교환시스템과 호환을 위해 MARS V2제품 도입 필요

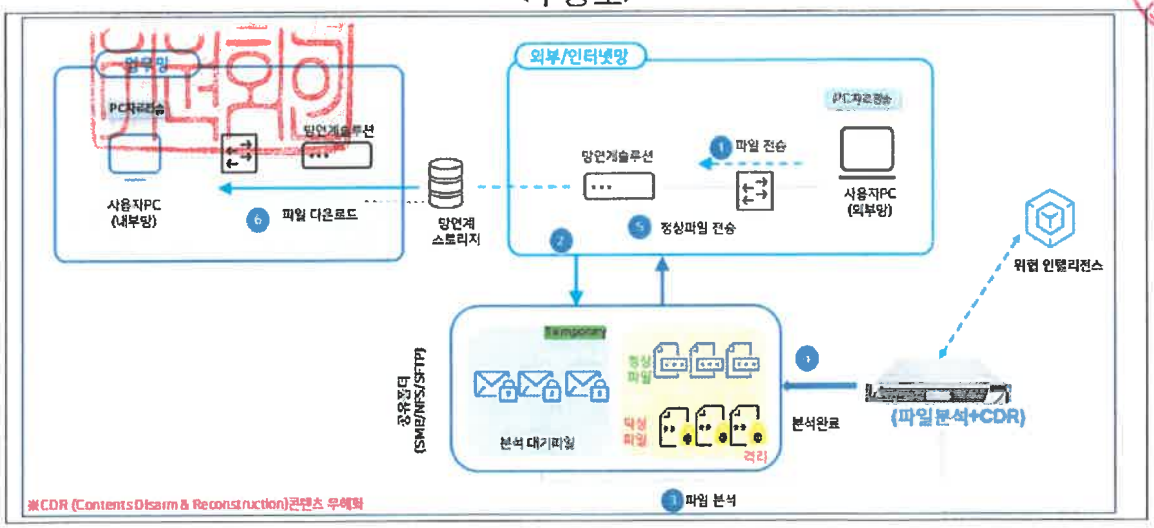
o 대상시스템 :

- 보안관제시스템
  · MARS V2 SLF450 Appliance with 1year MA Exp

o 도입시기 : 협의 후 결정

o 기술지원내용 :

<구성도>



- 로그 취합 및 관리, 분석은 업무망에 구현
- 망간 연계는 망연계 방식을 준수하여야 함
  · 연계 원칙은 단방향 통신, 파일전송 방식임
- 분석 결과에 대해 syslog형태로 SOAR에 제공하여야 함
- 위원회에서 운영 중인 자료교환시스템(에스큐브아이, Net-Protect)과 연계하여 자료교환에 요청된 문서자료에서 악성코드를 검사하는 기능 제공

<분석>
- 단일 장비에서 수동으로 문서파일에 대한 악성코드 검사 기능 제공
- 단일 장비(시스템)에서 관리, 분석 기능 제공
- 단일 파일의 용량 최대 1Tb까지 악성코드 탐지 지원
- 모든 Sandbox 동시 가동 지원
- YARA 정책 지원 가능
- White List, Black List 정책 지원
- 원본 파일과 분석 결과 파일에 대한 처리 및 경로 설정 제공

<위협대응>
- 악성코드 확정 파일에 대한 격리 기능
- 악성코드의 감염된 파일 추출 및 저장 기능 제공

<탐지>
- 어셈블리 레벨에서 악성코드 분석 기능 제공
- 리버스엔지니어링 기술을 이용한 분석 기능 제공
- 실행파일(PE)파일 변조된 확장자 차단 기능 제공
- 한글문서(HWP)에 대한 탐지 및 악성코드 차단기능 제공
- 알려지지 않은 신/변종 악성코드 탐지 및 차단
- Sleep(가상환경 회피기술) 모드 탐지 기능 지원
- 문서의 특정 페이지에 삽입된 악성코드 탐지/분석
- PDF, Office, HWP 파일의 URL을 추출 후 악성여부 검사 기능 제공
- 폐쇄환경(수동 업데이트)에서도 악성코드 탐지 및 분석 가능
- 시그니처 기반 탐지기능 지원
- 특정 OS, Application 영향도 없이 악성코드 탐지 가능
- 감염된 악성코드에 대한 차단 및 격리가 가능하며 격리된 파일 추출 가능

<관리>
- 관리화면 및 탐지 내역에 대한 설명에 한글/영문 언어 제공
- 악성코드의 기간별 탐지 내역 및 그래프 표시 지원
- 탐지된 취약점에 대한 CVE 코드 기반 표시 지원
- Sandbox의 실시간 상태 표시 및 가용 수량에 대한 표시 지원
- Sandbox에서 분석중인 파일 표시 지원
- https(암호화 프로토콜)을 사용하는 관리화면 제공
- 관리화면의 접속 Port 변경 지원
- 악성코드 탐지 현황에 대한 대시보드 표시 제공

- 서버 상태에 대한 정보(CPU, Memory, Disk, Sandbox) 표시 지원
- 관리화면을 통한 버전표시 및 패치, 업데이트 지원
- Syslog 전송기능 지원
- 관리화면에서 DB 백업 스케줄러 설정 지원
- 장애 상황 발생 시에 따른 서비스의 고객지원 도구(오류 수집) 기능 제공