[별지 제3호] 물품공급 또는 기술지원협약서

○ 사 업 명 : 노후 보안관제시스템 현행화 사업
○ 발주기관 : 공정거래위원회
○ 제조사 또는 공급사 : 지니언스(주)

제1조(목적) 이 협약은 **EDR솔루션** 1식에 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.

2024년 3월 4일

발주기관 : 공정거래위원회 (인)

제조사 또는 공급사 : 지니언스(주) (인)

규 격 서(시방서)

2024년 3월

공정거래위원회

○ 프로젝트명 : 노후 보안관제시스템 현행화 사업

○ 금　　액 : 조달구매

○ 목　　적 : 사용자 단말(PC)에 대한 관제를 강화

○ 특정제품필요성 : 공정거래위원회에서 현재 운영중인 NAC 솔루션과 연계 및 Agent 통합을 위해 Genian EDR 솔루션 제품 도입 필요

○ 대상시스템 :

- 보안관제시스템
  · Genian Insights E v2.0 User License (조달)

○ 도입시기 : 협의 후 결정

○기술지원내용 :

<구성도>

- 로그 및 정책관리는 업무망에서 관리 및 접근
- 망간 연계는 망연계 방식을 준수하여야 함
  · 연계 원칙은 단방향 통신, 파일전송 방식임
- IAM과 연계하여 사용자 및 권한 관리되어야 함
- 모든 로그(위협 이벤트 포함)를 SOAR에 제공하여야 함
- SOAR에서 정책(IP, HASH, 네트워크 제어 정책 등)배포를 연계하여야 함

- 사용자에게 위협 탐지에 대한 알림 기능을 제공하여야 함
- 영구 사용 라이선스
- 솔루션을 운용하기 위한 H/W 및 S/W Platform 제공
- 임의의 에이전트 선택, 선택적 그룹 설정, 전체 그룹을 대상으로 탐지 및 차단 정책의 예외처리 기능 제공
- 관리 서버의 사용자 계정 차등 권한 관리(RoleBased) 기능 제공
- 관리자의 작업 이력에 대한 상세 감사로그를 보관 및 검색이 가능해야 하며 감사로그는 파일 내보내기 형태를 지원
- 관리 콘솔 접근 관리자 및 사용자에 대한 IP 접근 제어가 가능해야 하며 일체형 장비인 경우 콘솔에 대한 IP 접근 제어를 지원
- 보안 위협 이벤트 발생 시, 고객사 운영중인 1개 이상의 보안관제 시스템으로 상세 탐지로그 전송(Syslog)이 가능해야 하며, Syslog에 포함되는 로그 종류가 선택 가능해야 함
- Syslog 전송 형태는 UDP, TCP port 임의 설정 기능
- 관리 서버 시스템 상태를 확인하기 위해 SNMP 연동을 제공
- 타 솔루션과의 연동/개발을 위한 API, 플러그인 등을 제공
- 알려진 침해 위협 정보 TI(Threat Intelligence)의 DB를 업데이트하여 파일 기반의 알려진 위협 탐지를 지원해야 함
- AI, 머신러닝 등 유사 기능을 통해 파일 기반의 위협 의심파일 탐지를 지원해야 함
- Fileless 등 이상행위 기반 위협 탐지를 지원해야 함
- 행위 정보를 기반으로 사용자 정의 탐지 룰 생성 및 탐지가 가능해야 함
- 탐지된 악성코드+이상행위에 대한 종합적인 분석 화면을 제공
- 위협 이벤트 탐지 시, 연관성 관계를 도식화(시각화) 및 각 연관성에 대한 세부 정보를 확인 가능해야 함
- 탐지된 위협 의심 파일에 대한 참고 지표인 유사도 SSDEEP HASH(%), AI분석 지표를 제공
- 위협으로 탐지되는 파일을 수집하는 기능을 제공
- 탐지된 위협 파일이 외부에서 유입된 경우 유입경로 정보를 제공
- 사후 조사와 분석을 위한 단말의 다양한 이벤트 로그를 상시 수집 및 저장해야 함
- 침해 의심 단말의 추가 분석을 위한 아티팩트 수집 기능을 지원해야 함 (시스템 정보, 네트워크 정보, 브라우저 방문 기록, 윈도우 이벤트 로그,

Prefetch 파일, FileSystem 정보, 레지스트리 하이브 등)
- 문서/압축 파일 이동 현황(인터넷 업로드, 메신저, 공유폴더, 외장 저장 장치 등)에 대한 정보를 제공
- 단말이 서버와 통신 불가 시에도 이벤트 정보를 Local DB에 저장 후 서버와 통신 시 전송하는 기능을 지원
- 윈도우 이벤트 뷰어의 특정 윈도우 로그 실시간 수집 기능을 제공
- 탐지된 위협 파일에 대한 격리 또는 삭제 기능을 제공
- 실행중인 프로세스의 강제 종료 및 덤프 수집 기능을 제공
- 위협 탐지 단말의 네트워크 격리 기능을 제공
- 단말의 네트워크 차단 시에도 특정 IP로의 통신 허용 기능을 제공
- 동일한 위협 탐지 시 설정한 대응 정책에 따른 자동 대응 기능을 제공
- 탐지 정합성 향상을 위한 예외처리 기능을 제공