[별지 제3호] 물품공급 또는 기술지원협약서

○ 사 업 명 : 노후 보안관제시스템 현행화 사업
○ 발주기관 : 공정거래위원회
○ 제조사 또는 공급사 : ㈜시큐레이어

제1조(목적) 이 협약은 SOAR솔루션 등 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 **(175,000,000 원 VAT포함)**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 03월 수일

발주기관 : 공정거래위원회 (인)

제조사 또는 공급사 : ㈜시큐레이어

# 규 격 서(시방서)

2024년 3월

공정거래위원회

○ 프로젝트명 : 노후 보안관제시스템 현행화 사업

○ 금　　액 : 175,000,000원(VAT 포함)

○ 목　　적 : 각종 장비에서 정보(로그 등)을 수집하여 인공지능 등 최신 기술 기반의 보안관제시스템 구축

○ 특정제품필요성 : 공정거래위원회에 도입된 기존 통합자료분석시스템과 호환을 위해 시큐레이어의 SOAR 도입 필요

○ 대상시스템 :

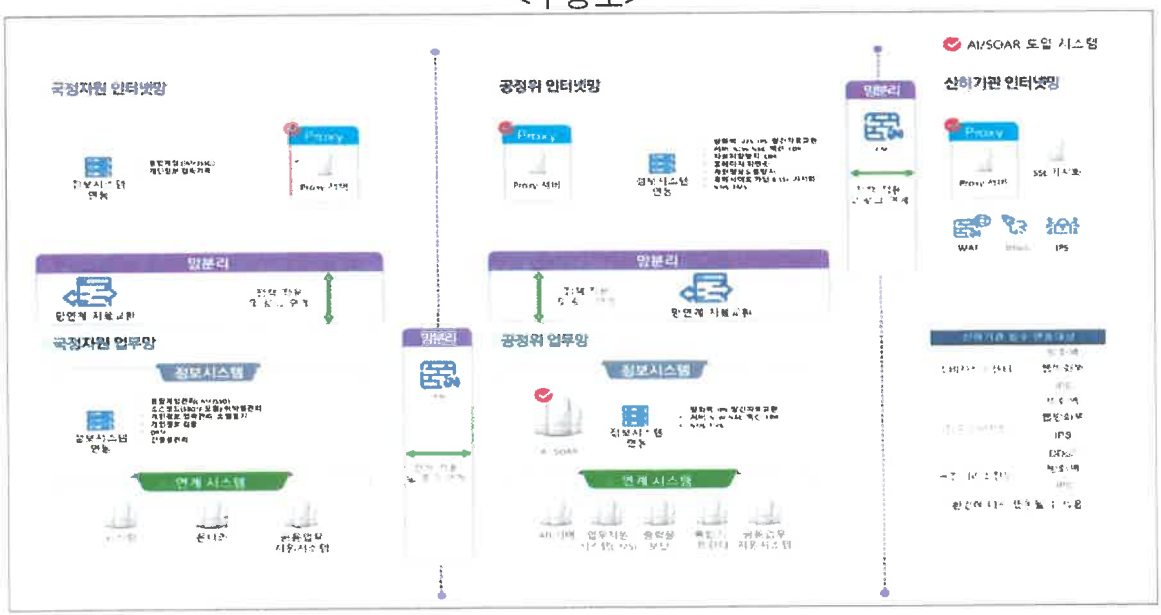
- 보안관제시스템
  - eyeCloudXOAR v4.0 Manager 1EA(통합)
  - eyeCloudXOAR v4.0 Collector 200GB/Day(통합)
  - eyeCloudXOAR v4.0 Proxy 4EA(통합)
  - eyeCloudAI v3.0 Manager 1EA(조달)
  - 보안관제 자동화 대응 서버(통합)
  - 데이터수집 및 저장 서버(통합)
  - 데이터 중계 및 분배 서버(통합)
  - 인공지능분석 솔루션 서버(통합)

○ 도입시기 : 협의 후 결정

○ 기술지원내용 :



<구성도>



- 로그 취합 및 관리, 분석은 업무망에 구현
- Proxy를 통해 다른 망*의 로그 취합, 정책배포

  * 공정위 인터넷망, 한국소비자원망, 한국공정거래조정원망, 상담센터망
- 망간 연계는 망연계 방식을 준수하여야 함

· 연계 원칙은 단방향 통신, 파일전송 방식임
- IAM과 연계하여 사용자 및 권한 관리되어야 함
- 보안장비 외 각종 장비*의 로그 수집하여야 함

  * (보안장비)방화벽, IPS, VPN, TMS, 백신, EDR, 통합계정권한관리, 통합계정인증, 시스템계정관리, 접근제어, 보안USB, 네트워크접근제어, 자료교환, 자료저장방지, 유해사이트차단 등
  * (통신장비)NMS, FMS, 포트스캔 등
  * (개인정보보호)개인정보검출, 개인정보접속기록관리, 개인정보등록차단, IAM 등
  * (기타)AD, DRM, 출력물관리(프린터, 복합기) 등
  * (타기관)한국소비자원, 공정거래조정원에서 제공하는 로그
- 사용자에게 필요한 정보에 대해 알림 기능을 제공하여야 함
- 보안인증사무국으로부터 발급된 CC인증(통합보안관리, EAL2) 획득 제품
- IPv4, IPv6 네트워크 데이터 수집, 운영 기능 제공(공인 인증기관의 증빙자료 제출)
- 고객사에서 요청하는 모든 종류의 수집 대상 장비들에 대하여 제한 없는 로그 수집 기능을 제공
- LogFile(Directory), SYSLOG, SNMP, DB연동, API 등 다양한 방식에 의한 실시간 수집 기능 제공
- 저장데이터 무결성 검증 기능
- 데이터 전송 암호화 TLS v1.3 지원
- TCP 암호화 압축 전송 기능 제공
- Microsoft Office365 Management API 연계 데이터 수집 기능 제공
- 수집된 로그의 장비/로그 유형별 실시간 모니터링 기능 제공
- 3D 기반 네트워크 구성도를 생성하여 각종 이벤트 발생 여부와 자산 및 그룹의 시스템 상태를 도식화 하여 모니터링 하는 기능 제공
- 종합적인 현황(사이버 위기경보 단계, 이벤트 발생현황, 로그수집현황 등) 모니터링이 가능한 종합대시보드 기능 제공
- 다양한 이벤트 탐지옵션 제공(최초 발생시, 두번째부터 발생시마다, 발생시마다, 최초임계치 초과시, 두번째부터 임계치 초과시마다, 임계치초과시 마다, 스케줄 시간내 임계치 초과시, 스케줄 시간내 미 발생시)
- 실시간/스케줄 방식 다단계 이벤트 기능 제공
- GUI 설정에 의한 검색 조건에 해당하는 로그를 File/DB/Syslog로 추출/전송

하는 기능 제공
- GUI 설정에 의한 사용자 계정 정보 및 자산 정보 자동 연동 기능 제공
- 탐지 위협 대응 상태별(대기/분석/대응/종료) 종합 현황 및 위협 통계 정보 가시화 기능 제공
- 탐지 위협별 Playbook 적용 및 자동(수동) Playbook 수행 기능 제공
- 탐지 위협 정보 대상 IoC Feature 추출 자동화 및 온톨로지 기반 분석 기능 제공
- 위협별 자동 위협 분석, 대응(차단) 등 보안관제 프로세스 기반의 시나리오 관리 기능 제공
- 위협이벤트 대상 분석 보고서 자동생성 기능 제공
- 보안장비 연계 관리를 통한 차단/정책 적용을 위한 연계 정보 관리화
- 사용자의 요청에 따라 검색질의 수행하여 빅데이터 기반의 데이터를 고속 검색 할 수 있는 기능
- 기계학습을 위해 추출된 학습 데이터를 Random Sampling, Over Sampling, Under Sampling의 기본으로 한 데이터 표본 추출 기능
- AI 모델 기본 설정 정보 로드 또는 알고리즘, 샘플데이터 및 스케쥴 정보를 기반 새로운 모델 정보 생성 기능
- 이상행위 AI 모델을 사용하여 실시간 수집 데이터를 대상으로 실시간 AI 탐지 결과를 모니터링 할 수 있는 기능
- 공정위에 기존 제품과 호환을 위해 특정제품 도입 필요