Samsung
Financial Networks

『이상징후모니터링(Splunk)솔루션 도입』

제안 요청서

2026年 8月

삼성자산운용㈜

목 차

제 목	내 용
사업 개요	추진배경 및 필요성, 추진일정, 기대효과, 사업 범위, 계약 관련 사항 등
시스템 운용 조건	인프라 표준 사양, 연동 대상 이기종 장비, 환경 구성, 보안 및 정책 가이드 등
제안 요청 내용	구축 범위, 기능 요구사항, 탐지 시나리오·AI위협 대응 요건, 성능·보안·품질 요건 등
제안서 작성 지침	제안서 목차, 세부 작성 요령 등
제안 고려사항	아래 참조
제안서 접수 및 유의사항	아래 참조

Ⅰ. 프로젝트 개요

1. 추진 배경 및 필요성

- 이기종 보안·인프라 로그의 폭증과 지능화된 사이버 위협(내부자 위협, 계정탈취, 랜섬웨어, APT 등)에 대응하기 위한 이상징후 모니터링 솔루션(Splunk) 도입 필요
- 장기간·대용량 로그의 실시간 수집·분석 기반 이상행위 탐지를 통한 보안관제 도입 必
- ChatGPT, Claude, Gemini 等 생성형 AI 서비스 확산에 따른 'Shadow AI' 정보유출 위협에 대한 탐지·모니터링 대응 체계 마련

2. 추진 일정

- 전체 일정: 계약 체결 후 약 4개월 이내
  - 분석/설계: 1개월
  - 구축 및 테스트: 2개월
  - 안정화: 1개월

※ 제안서 제출 時 상주/비상주 구분으로 견적서 반영

- 제안서 접수: 2026년 8월 20일(목) 17:00까지
- 결과 선정 및 통보: 2026년 8월 21일(금) 예정

※ 필요 時 제안평가 진행을 통해 결과 선정 일자는 변경 가능

3. 기대효과

- 이기종 보안 로그 통합 수집·분석을 통한 관제 사각지대 해소 및 사고대응(MTTR) 단축
- 이상행위 탐지로 오탐 감소 및 실제 위협 우선순위 식별
- 생성형 AI 오·남용 행위 조기 탐지를 통한 정보유출 사고 예방
- 샘플 대시보드·리포팅 체계 제공을 통한 보안관제 업무 효율성 제고

4. 제안 적용범위

본 제안요청서에 정의된 제안요청사항은 시스템 구축 시 충실히 반영되어야 하며, 본 문서에서 별도 제시하지 않은 사항은 국내/외 표준에 부합하도록 구축하여야 한다. 시스템 구축을 위한 업무 범위는 본 제안요청서, 제안 서류 일체, 계약관련 부속서류 일체에 준한다.

5. 계약 관련 사항

- 계약은 제안 평가 결과에 따라 우선협상대상자로 선정된 구축업체와 협상이 완료된 후 계약 체결
- 우선협상자로 선정된 제안업체가 정당한 사유 없이 계약체결을 이행하지 아니할 경우 업체 선정을 취소하고 차순위 업체와 협상을 실시하거나 필요시 재입찰을 수행할 수 있다.

- 목적물에 대한 소유권 및 지식재산권은 삼성자산운용에 귀속되며, 계약 업체는 본 계약을 통하여 당사에 제공되거나 이용된 지적재산권(특허, 저작권 등) 등이 제3자의 지적재산권을 침해하지 않을 것을 보증하여야 한다.
- 계약 업체의 귀책 사유 등으로 계약을 온전히 수행할 가능성이 없다고 판단되는 경우 계약을 해제, 해지할 수 있다.

Ⅱ. 시스템 운용 조건

1. 일반사항

- 개발 및 운영에 필요한 일체의 H/W 및 S/W 구매는 당사 규정 및 관련 지침에 따라 별도 경쟁입찰로 진행한다.
- H/W는 표준에 부합하는 제품으로 요구되는 사양의 최소/권장 사양을 제시하여야 한다.
  - CPU, Memory, Disk, Network의 최소/권장사양 및 용량 산정 근거를 명시할 것
  - 일 평균 로그 유입량(EPS) 및 저장 보관기간 기준 스토리지 산정 근거를 명시할 것
  - 이중화 및 DR 구성 시 권장 아키텍처를 명시할 것
- 초기 구축 후 아키텍처 변경 없이 HW 증설로 용량 및 성능을 확장할 수 있는 운영 구조를 제안하여야 한다.
- 제안업체가 제안한 제품 및 사양은 필요시 당사 기술검토에 따라 변경 및 가감이 가능하다.

2. 인프라 환경 구성

- 당사에서 제공한 H/W, S/W 및 기술지원을 이용하여 인프라 환경 구성은 제안업체에서 직접 수행한다.
- 설치, 구성 및 개발이 완료된 후 시스템에 대한 인수인계 및 운영계 이관은 당사의 기준과 절차에 준한다.

3. 데이터(로그) 이관

- 기존 로그 관리 체계에서 데이터 이관이 필요한 경우, 그에 대한 작업은 제안업체의 작업 범위이다.
- 연동 장비별 로그는 논리적으로 분리 저장하고 보관기간을 다르게 설정할 수 있어야 한다.

4. 업무연속성 계획(BCP) 수립

- 제안 사업이 BCP 대상 프로젝트인 경우, 업무연속성과 재해복구 계획을 수립하고 관련 산출물("DR 설치작업 결과서", "DR 업무체크리스트", "가동 절차서", "BCP 모의 테스트 결과서")을 필수로 작성해야 한다.
- 분석 서버 장애 시 예정된 스케줄 작업(Job)이 지체 없이 가용한 타 분석 서버에서 자동 전환되어 수행되어야 한다.

6. 보안 및 정책 가이드 준수

- 금융 관련 법규 및 당사 보안규정을 준수할 수 있어야 한다.
  - 전자금융거래법 및 동법 시행령
  - 전자금융감독규정 및 모범규준
  - 정보통신망 이용촉진 및 정보보호 등에 관한 법률
  - 개인정보보호법 및 동법 시행령·시행규칙·고시
  - 기타 금융 IT 관련 법규 및 당사 보안 규정
- 제안 방식이 개발이 아닌 패키지 소프트웨어인 경우, 소프트웨어의 보안수준을 검증할 수 있는 제3자를 통한 객관적인 보안 수준 평가 결과를 제시해야 한다.

Ⅲ. 제안요청 내용

1. 구축 범위 요약

- 이기종 보안·인프라 로그를 통합 수집·저장·분석하는 SIEM 플랫폼을 구축하는 건으로, 무중단 확장 가능한 운영환경을 구성한다.
- 머신러닝(MLTK) 기반 위협 탐지 시나리오(총 30건)를 구현하여 MITRE ATT&CK 프레임워크 기반의 실시간 상관분석 체계를 마련한다.
- 생성형 AI(ChatGPT, Claude, Gemini 等) 오·남용에 따른 정보유출 위협(Shadow AI, 총 12건 유형)을 탐지·대응할 수 있는 체계를 구성한다.

□ 프로젝트 구축 시스템 범위

항 목	내 용	비 고
연동 대상 로그	FW, IPS, WAF, NAC, 백신, URL통제, DLP, Web로그, 서버접근로그, DB접근로그, PC보안, DRM, 개인정보검출, 서버보안, 웹쉘탐지, 웹메일 등	이기종 통합수집
AI 연동	자체 AI Assistant 또는 외부 LLM(ChatGPT 등) 연동	자연어 검색질의 지원
대시보드	샘플 대시보드 기본 제공, 사용자 커스터마이징 가능	Top N, 2D/3D 차트 등
연동 방식	Network, DB, File, NoSQL DB, Hadoop 등	REST API, Python SDK 등

※ 개인정보(고유식별정보 등) 처리 시 암호화 필수

2. 업무 기능 요건

제안업체는 아래 기능 요구사항을 모두 충족하는 솔루션을 제안하여야 하며, 요구사항별 충족 여부 및 구현 방안을 제안서에 구체적으로 기술하여야 한다. (요구사항 총 65건)

(1) 보안로그 수입을 위한 운영환경 요구사항

▶ 1. 안정성 (보안로그수집 환경에 필요한 분산처리)

항목	주요기능	상세 요구사항
1-1	데이터 저장 안정성 보장	로그 저장 서버 및 매니저 시스템에 장애가 발생할 경우, 저장 데이터에 손실 없이 서비스가 중단되어서는 안되며, 데이터 증가에 따른 성능 저하는 최소화되야 되며 대량의 로그 발생시 로그가 유실되어서는 안된다. (예, 서버 Crash/다운, NW 인터페이스에러, SW 중단, 로그 대량유입 등)
1-2	분석 업무 무중단 보장	분석 업무와 관련되어 분석 서버 장애시에도 분석 중인 업무(검색, 리포팅 작업 등) 이 중단되어서는 안된다. 즉, 분석 서버 장애시, 예정된 schedule job이 지체 없이 가용한 타 분석 서버에서 자동으로 Job이 전환되어 수행되어야 한다.

▶ 2. 이상징후플랫폼 기반 운영환경

항목	주요기능	상세 요구사항
2-1	플랫폼위의 어플리케이션 확장 운영	빅데이터 플랫폼위에서 다양한 수집/분석 앱(예, SIEM App, Compliance App 등) 을 쉽게 추가하여 활용할 수 있는 앱 생태계를 제공해야 한다.
2-2	무중단 확장 및 업그레이드 지원	플랫폼의 기능, 구성, 어플리케이션 확장 및 버전 업그레이드 시 서비스 업무가 중단되어서는 안된다.
2-3	보안 장비별 대시보드 제공	상관 룰 수행 및 탐지 뿐만 아니라, 보유중인 각 보안 장비별 대시보드를 손쉽게 구성할 수 있어야 한다. 보안 장비별 기 구축된 대시보드를 공유하고 재 활용할 수 있는 체계를 제공하여야 한다. (예를 들어, FireEye를 연동시 처음부터 구축하는것이 아니라, 벤더 또는 앱스토어 등에서 제공되는 FireEye앱을 설치하여 기본적인 분석대시보드를 기본으로 제공받을 수 있어야 한다.)
2-4	검색/분석 검색 명령어 제공	플랫폼 위에 다양한 분석을 위하여 기본 제공하는 검색/분석 명령어가 다양해야 하며, 최근 1시간, 1일 등에 대한 통계처리(avg, sum, total 등)를 제공해야 되고 ML 분석관련된 명령어를 제공해야 한다. (예, 통계, 상관분석 등 명령어 제공)
2-5	사용자가 커스텀 명령어 추가 기능	기본 분석 명령어에서 제공되지 않는 추가 명령어를 만들수 있는 확장 기능을 제공하여야 한다. (예를 들어, IPS, 트래픽 페이로드변환을 위해 Base64 인코딩/디코딩 변환 명령어 등)
2-6	확장 가능성	초기 구축 후, 아키텍처 변경없이 HW 증설로 용량 및 성능을 확장할 수 있는 운영 구조여야 한다.

▶ 3. 운영지원

항목	주요기능	상세 요구사항
3-1	업무시스템과 연동	도입 시스템에서 데이터를 기타 관제 시스템으로 송/수신 하기 위해 다양한 방안(Network, DB, File, NoSQL DB, Hadoop 등) 으로 연동이 가능해야 한다.
3-2	다국어 지원	유입되는 로그에 다국어가 있는 경우 처리가능해야 하고, 검색 시에도 다국어 검색이 가능해야 한다. (지원하는 언어 표기)
3-3	시스템 모니터링	도입 시스템의 상세한 모니터링(리소스, SIEM 기능, 스케줄, 로그 수집 상태 등)이 가능해야 하며, CPU, Memory, Disk 주요 Process 등 자원사용량에 이상 발생 및 로그 수집이 일정시간 중단된 경우 시 알람 및 경고 메시지를 제공 해야 한다.
3-4	정규표현식 지원	정규표현식을 이용하여 파싱, 로그 필터, 식별규칙, 검색, 연관분석에 활용이 가능해야 한다. (예를들어, 수동 및 자동 파싱 기능을 제공해야한다)

(2) 로그 관리 요구사항

▶ 4. 로그 수집 및 저장

항목	주요기능	상세 요구사항
4-1	로그 수집	다양한 이기종 로그를 통합수집 지원(FW, IPS, WAF, NAC, 백신, URL통제, DLP, Web로그, 서버접근로그, DB접근로그, PC보안, DRM, 개인정보검출, 서버보안, 웹쉘탐지, 웹메일 등) 해야 한다.
4-2	로그 수동 입력	상시 연동하는 장비 로그 수집 이외에, 분석가가 임의의 샘플 로그를 제공된 UI에서 수동으로 업로드하여 파싱 및 분석을 수행할 수 있어야 한다.
4-3	파싱 규칙 설정 (쿼리 내 필드 파싱)	로그 내에 자동으로 파싱되지 않은 부분을, 쿼리 내에서 임의로 필드 정의하고 이용할 수 있어야 한다.
4-4	유연한 로그 연동	추가 개발없이 유연한 로그연동을 지원해야 하며, 신규 도입 장비의 로그 연동시 개발자(제조사) 지원없이도 사용자가 직접 또는 기술지원업체의 엔지니어만으로 로그연동이 가능해야 한다. (개발 불필요해야 함)
4-5	수집로그 정합성 및 무결성 보장	네트워크 및 인프라 등 장애시 연동된 시스템 로그와 수집된 로그의 정합성을 보장 하여야 한다.
4-6	연동 장비 별 보관기능	물리적으로 동일 서버(또는 Appliance)에 저장하더라도, 연동 장비(로그) 별로 논리적인 스토리지 그룹을 분리하여 저장하고, 보관기간을 다르게 설정 하여야 한다.

▶ 5. 로그 분석 및 조사

항목	주요기능	상세 요구사항
5-1	실시간 수집 및 과거 데이터 분석	장기간의 대용량 데이터를 실시간 수집 중인 데이터와 함께 통합 분석할 수 있는 기능을 제공해야 한다.
5-2	로그 분석에 필요한 다양한 검색명령어 및 함수 제공	수집한 로그를 분석할수 있는 다양한 검색 명령어 제공해야 한다. (160개 이상의 명령어 및 시계열, 통계 등의 함수 지원)
5-3	머신러닝을 활용한 데이터 분석	머신러닝 툴킷을 제공하여 위협 및 이상행위 탐지를 위한 머신러닝 모델 생성 과 검증 및 운영 기능을 제공해야 한다. (30개 이상의 머신러닝 알고리즘 제공)
5-4	머신러닝 커스텀 알고리즘 추가 확장 기능	사용자가 파이썬 머신러닝 라이브러리를 추가하여, 머신러닝 분석에 활용할수 있는 사용자 추가 기능 제공해야 한다.
5-5	머신러닝 지원 기능	위협 및 이상행위 탐지를 위한 머신러닝 모델 생성 및 검증/운영을 손쉽게 구현하기 위한 다양한 기능을 제공해야 한다.
5-6	AI 및 ChatGPT를 이용한 검색 활용	자체 제공되는 AI (AI Assistant) 기능 이용 및 ChatGPT 연동을 통해 자연어 형태의 질의 시 로그 분석을 위한 검색 구문 자동 생성 및 설명을 제공함으로써 검색에 대한 편의성을 제공해야 한다.

▶ 6. 로그 검색

항목	주요기능	상세 요구사항
6-1	대용량 로그 검색	도입 시스템이 저장 중인 모든 데이터는 저장기간에 상관없이 조건문으로 검색할수 있어야 한다.
6-2	외부 참조 데이터	외부에 존재하는 데이터(File, DB, Hadoop, Mongodb등)의 변경사항을 자동/주기적으로 갱신할 수 있어야 한다. (예. 자산정보, 인사정보)
6-3	파싱 로그의 필드 조합	로그의 파싱된 필드의 조합을 통해 신규 필드로 표현이 가능해야 한다.
6-4	로그 검색 함수 지원	로그 검색 지원 함수(문자열/수치연산/형변환,조건함수 등)를 이용해 검색 및 통계/요약이 가능해야 한다.
6-5	이벤트 태깅	수집된 원본 로그 이벤트에 제시된 조건을 기준으로 태깅을 할 수 있어야 한다. (예를 들어, src_ip 대역이 특정 범위에 해당하면, '업무망' 등으로 해당 원천 이벤트에 태그를 추가)
6-6	검색 결과를 조합한 신규 필드 생성	로그의 파싱된 필드를 조합하여, 신규 필드로 표현할 수 있는 기능 제공하여야 한다
6-7	검색 결과내 재검색	검색한 결과내에서 계속적인 재 검색 기능 등 다양하고 유연한 검색기능 제공 가능해야 한다. (조회 결과 내 재검색 기능)
6-8	검색언어(쿼리)의 사용 편리성	상대적으로 간결하고 복잡도가 적고, 자동완성 기능을 지원해야 한다.
6-9	Lookup 기능(외부 파일 참조 기능)	Lookup 기능을 통해 외부 파일을 참조할 수 있고, 자산 정보 및 참조 데이터(인사정보, 국가정보, 블랙/화이트리스트 등)를 주기적으로 수집하여, 이벤트 로그와 상관분석을 지원해야 한다.

▶ 7. 보안위협 분석룰

항목	주요기능	상세 요구사항
7-1	상관관계분석 룰 제공	고객사 환경에 적용이 가능한 시나리오기반의 실시간 상관관계분석 룰(Rule)을 솔루션 메뉴와 탐지 룰/시나리오 사이트를 기본 제공해야 한다
7-2	외부 DB연동 이상행위 룰 생성 지원	다양한 오픈소스 위협DB(Threat Intelligence Feeds) 및 국가기관의 위협DB 등과 연동할 경우, SIEM에서 수집된 로그와 자동 매핑하여 이상행위를 탐지하는 룰(정책)을 지원해야 한다
7-3	다중 분석룰 규칙	수집된 로그 혹은 단일/복수 룰을 사용하여 별도의 룰(정책) 생성 적용이 가능해야 한다.
7-4	상관분석룰 정기적 제공	다양한 보안로그를 활용하여 위협을 탐지할수 있는 상관분석룰을 정기적으로 제공하여야 한다. 예를 들어 분기마다 정기적으로 업데이트 제공
7-5	다양한 방식의 Alert 기능을 제공	메신저(텔레그램, Slack), SMS, E-mail 등을 통해 위험도 및 담당 부서에 Alert 기능을 제공 하여야 한다.

항목	주요기능	상세 요구사항
		(예 : 보안부서 시나리오의 경우 보안부서에 한하여 Alert 메일 등을 발송 위험도에 따라 메일, SMS, 메신저 Alert 을 유기적으로 발송 가능해야 함)

(3) 추이/연계 분석 요구사항

▶ 8. 분석

항목	주요기능	상세 요구사항
8-1	분석 화면 지원	분석 화면에서 필터(조건), Drill Down, 화면 탭, 화면 분할 등의 기능이 지원해야 한다.
8-2	분석 결과 도식화	분석 화면의 다양한 표현(표, 그래프, 추이선, 그룹핑, 분포도 등)이 가능해야 한다.
8-3	사용자 임시 필드 정의	연관관계 분석시 임시 데이터 저장을 위한 사용자 필드 지정이 가능해야 한다.
8-4	사용자 정의 필드(태그)	수집된 로그 및 식별 규칙에 분류 기준에 따른 사용자 정의 필드(태그)가 입력이 되어야 한다.

(4) 대시보드 요구사항

▶ 9. 대시보드

항목	주요기능	상세 요구사항
9-1	샘플 대시보드 제공	제공 솔루션은 제품에서 기본적으로 샘플 대시보드들을 제공하여야 한다
9-2	커스터마이징 지원 대시보드 위젯 기능	제공 솔루션은 개별 사용자가 필요로 하는 정보를 보여주기 위해 커스터마이징 가능한 대시보드 위젯을 제공하여야 한다.
9-3	현황 대시보드 제공	자체적으로 실시간 수집되는 로그 수집 상태 및 현황을 모니터링 할 수 있는 대시보드를 제공 해야 한다
9-4	다양한 형태의 대시보드	다양한 종류의 대시보드(Top N 등) 생성 기능 및 다양한 그래프를 이용하여 이벤트 발생 현황에 대한 통계 모니터링 기능을 지원하여야 한다
9-5	사용자 정의형 대시보드	추가적인 개발 작업 없이, 표, 차트, 버블차트, 지도, 2D/3D 차트 등 필요로 하는 대시보드를 쉽게 만들수 있어야 한다.
9-6	고급 대시보드 작성	추가 개발 과정없이, 대시보드 내에서 사용자의 다중 입력값을 처리하여 동작하는 dynamic 대시보드를 제공해야 한다. (예를 들어, 하나의 대시보드 내에서 검색 조건, ip 대역, 검색 시간 등을 손쉽게 입력하여 원하는 분석을 할 수 있는 기능)
9-7	대시보드 드릴다운 지원	대시보드에서 각 항목에 대한 드릴다운 방식을 통해 상세 내용을 확인할 수 있는 기능을 제공하여야 한다.

항목	주요기능	상세 요구사항
9-8	대시보드 신속성	제안 솔루션은 보안과 네트워크 정보를 빠르게 가시화 시킬 수 있는 대시보드를 제공하여야 한다.
9-9	대시보드 권한 설정	대시보드의 항목별 사용자 권한 설정이 가능해야 한다.

(5) 관리 요구사항

▶ 10. 사용자 권한

항목	주요기능	상세 요구사항
10-1	권한관리 기능	사용자, 사용자그룹, 롤 기반의 권한 관리 기능을 제공해야 한다.
10-2	권한별 데이터 접근제어	사용자 권한별 각 데이터에 대한 접근 제어가 가능해야 한다.
10-3	메뉴 접근 제어	사용자 권한별 리포트, 대시보드 및 화면 메뉴에 대한 접근 제어가 가능해야 한다.
10-4	이력 조회	계정발급 이력 조회 및 사용자 작업 이력 등에 대해 조회할 수 있어야 한다.

▶ 11. 감사/장애 로그

항목	주요기능	상세 요구사항
11-1	감사로그	감사로그 - 관리자, 운영자의 로그인/아웃, 등 모든 작업에 대해 구체적으로 기록이 가능해야 한다. (추적성확보)
11-2	오류/장애 로그 기록	오류 및 장애 발생에 대비한 오류/장애 로그 모두 기록 가능해야 한다. (오류일시, 내역 등 상세히)

(6) 확장성 요구사항

▶ 12. API 연동

항목	주요기능	상세 요구사항
12-1	API 연동방법	외부의 시스템에서 도입 시스템 내부의 데이터를 활용할 수 있도록 REST API 및 Python등의 다수의 개발 SDK를 제공해야 한다. (예시: API를 통하여 탐지한 사고상태값과 담당자를 변경할 수 있어야 함)

▶ 13. 머신러닝 적용

항목	주요기능	상세 요구사항
13-1	머신러닝 알고리즘 적용	3rd party 제품 연동 또는 별도의 개발 없이 머신러닝 기능 제공하여야 한다. - 플러그인 형태 또는 앱 형태의 서비스 제공

항목	주요기능	상세 요구사항
13-2	룰 머신러닝 적용 기능	단순 룰&복합상관관계 룰에 대한 머신러닝 모델 및 통계 명령어를 적용 가능해야 한다.
13-3	머신러닝을 위한 쇼케이스 기능	샘플 데이터를 바탕으로 여러 유스케이스와 알고리즘에 대해서 테스트 해 볼 수 있는 쇼케이스(showcase) 기능을 제공해야 한다
13-4	머신러닝을 위한 실험 기능	운영 데이터를 바탕으로 여러 알고리즘을 적용하여 테스트 해 볼 수 있는 실험(experiment) 기능을 제공해야 한다
13-5	커스텀 알고리즘적용 기능	커스텀 알고리즘을 3rd party 제품 연동이 가능해야 한다.
13-6	LLM 연동 기능	이상징후 분석을 위해 public LLM 연동이 가능해야 한다.
13-7	딥러닝 기능 제공	딥 러닝을 위한 기능을 제공해야 하며, Jupyter Lab Notebook으로 신속한 개발 환경을 지원해야 한다.

3. 보안위협 탐지 시나리오 요건

제안 솔루션은 머신러닝 툴킷(MLTK) 기반의 탐지 모델을 활용하여 아래 위협 탐지 시나리오(총 30건)를 구현할 수 있어야 하며, 각 시나리오는 MITRE ATT&CK Tactic/Technique과 매핑되어 관리되어야 한다.

ID	시나리오	데이터 소스	유형	탐지 목적 / MITRE 매핑
R005	백신 탐지 직후 보안 서비스 중지	AV, EDR, OS Event	복합	악성코드 탐지 후 AV/EDR 서비스 중지 이벤트가 따라오는 패턴을 분류한다. [MITRE] TA0112 Defense Impairment / Disable or Modify Tools
R009	DLP 파일 전송 크기 이상	DLP, Proxy	단일	사용자/부서별 전송 파일 크기, 건수, 목적지를 기반으로 유출 이상치를 찾는다. [MITRE] TA0010 Exfiltration / T1567 Exfiltration Over Web Service
R010	고위험 CVE 서버 대상 exploit 시도	Vulnerability Scanner, IPS, WAF	복합	자산 CVSS, exploitability, IPS hit, WAF 차단을 결합한다. [MITRE] TA0001 Initial Access / T1190 Exploit Public-Facing Application
R011	DRM 문서 열람 후 대량 압축	DRM, OS, EDR	복합	중요 문서 열람 이후 zip/7z 생성량과 파일 접근 수를 모델링한다. [MITRE] TA0009 Collection / T1560 Archive Collected Data
R012	퇴사 예정자 야간 접근 이상	HR, AD, VPN, DLP	복합	퇴사 예정자 계정의 시간대, 데이터 접근, 외부 전송을 기준선과 비교한다. [MITRE] TA0009 Collection / TA0010 Exfiltration / T1005 Data from Local System / T1041

ID	시나리오	데이터 소스	유형	탐지 목적 / MITRE 매핑
R013	관리자 그룹 변경 이상	AD, Windows Event, IAM	단일	그룹 변경 빈도, 변경자, 대상 계정 속성으로 권한 상승 가능성을 분류한다. [MITRE] TA0004 Privilege Escalation / T1098 Account Manipulation
R014	VPN 지리적 불가능 이동	VPN, GeoIP, HR	단일	로그인 위치, 시간 간격, 이동 속도를 군집화해 불가능 이동을 찾는다. [MITRE] TA0001 Initial Access / T1078 Valid Accounts
R015	EDR 난독화 명령 실행	EDR, OS	단일	명령행 길이, base64 패턴, LOLBin 여부를 기반으로 악성 실행을 분류한다. [MITRE] TA0005 Stealth / TA0002 Execution / T1027 Obfuscated Files or Information / T1059
R019	PowerShell 실행 빈도 이상	EDR, Windows Event	단일	호스트별 powershell 실행량과 인코딩/네트워크 옵션 사용률을 모델링한다. [MITRE] TA0002 Execution / T1059.001 PowerShell
R020	OS 이벤트 로그 삭제/급감	Windows Event, EDR	복합	로그 삭제 이벤트와 이벤트 발생량 급감, 보안 도구 상태를 함께 본다. [MITRE] TA0112 Defense Impairment / Clear Windows Event Logs
R021	동일 해시 악성코드 내부 확산	AV, EDR, NAC	복합	해시별 감염 호스트 수, 네트워크 세그먼트 수, 시간 확산 속도를 군집화한다. [MITRE] TA0008 Lateral Movement / T1021 Remote Services
R023	NAC 위치와 계정 로그인 위치 불일치	NAC, AD, VPN, HR	복합	단말 물리/네트워크 위치와 계정 로그인 위치의 불일치를 이상치로 탐지한다. [MITRE] TA0001 Initial Access / T1078 Valid Accounts
R024	DLP 위반 반복 사용자 군집	DLP, HR	복합	부서/직무별 DLP 위반 유형과 빈도를 군집화한다. [MITRE] TA0010 Exfiltration / T1020 Automated Exfiltration
R025	중요 문서 열람 후 USB 사용	DRM, OS, DLP	복합	중요 문서 열람, USB mount, 파일 복사량을 결합해 유출 가능성을 분류한다. [MITRE] TA0010 Exfiltration / T1052 Exfiltration Over Physical Medium
R028	LSASS 접근 이상	EDR, Windows Event	단일	프로세스별 LSASS handle open, dump 파일 생성, 권한 수준을 feature로 모델링한다. [MITRE] TA0006 Credential Access / T1003 OS Credential Dumping

ID	시나리오	데이터 소스	유형	탐지 목적 / MITRE 매핑
R029	AD 계정 잠금 패턴 이상	AD, OS	단일	사용자/출발지별 실패, 잠금, 성공 전환을 기준선화한다. [MITRE] TA0006 Credential Access / T1110 Brute Force
R030	휴직자/비활성 계정 사용	HR, AD, VPN	복합	HR 상태와 로그인 성공, MFA 실패, 접근 자산을 결합한다. [MITRE] TA0001 Initial Access / T1078 Valid Accounts
R031	Proxy 다운로드 확장자/크기 이상	Proxy, AV, APT	복합	다운로드 확장자, 크기, 평판, AV verdict를 결합한다. [MITRE] TA0002 Execution / T1204 User Execution
R032	신규 서비스 등록 이상	EDR, Windows Event	단일	서비스 생성 이벤트의 실행 경로, 서명, 사용자, 시간대를 feature화한다. [MITRE] TA0003 Persistence / T1543 Create or Modify System Process
R033	Linux sudo 사용 패턴 이상	Linux OS, PAM, HR	단일	사용자별 sudo 명령 빈도, 실패율, 명령 카테고리를 기준선화한다. [MITRE] TA0004 Privilege Escalation / T1548 Abuse Elevation Control Mechanism
R037	백신 업데이트 실패 단말의 악성 이벤트 증가	AV, EDR, NAC	복합	업데이트 상태와 악성 이벤트 수의 예측 오차를 본다. [MITRE] TA0112 Defense Impairment / Disable or Modify Tools
R041	EDR 프로세스 트리 희귀 패턴	EDR	단일	parent-child process, 서명, 경로, 명령행 길이 조합의 희귀도를 학습한다. [MITRE] TA0002 Execution / TA0005 Stealth / T1059 / T1027
R042	Proxy POST 바이트 급증	Proxy, DLP	단일	사용자별 POST bytes와 업로드 목적지 수를 기준선화한다. [MITRE] TA0010 Exfiltration / T1041 Exfiltration Over C2 Channel
R043	DRM 문서 열람 시간대 이상	DRM, HR	복합	사용자/부서별 문서 열람 시간대와 문서 민감도를 모델링한다. [MITRE] TA0009 Collection / T1005 Data from Local System
R044	NAC 격리 해제 직후 고위험 접속	NAC, Firewall, EDR	복합	격리 해제, EDR 상태, 외부 통신, 내부 접속 증가를 결합한다. [MITRE] TA0008 Lateral Movement / T1021 Remote Services

ID	시나리오	데이터 소스	유형	탐지 목적 / MITRE 매핑
R045	스팸 캠페인 수신자 로그인 이상군	Spam, AD, VPN	복합	캠페인 수신자들의 실패율, 국가, MFA 실패, 성공 여부를 군집화한다. [MITRE] TA0001 / TA0006 / T1566 / T1110
R046	예약 작업 생성 이상	Windows/Linux OS, EDR	단일	스케줄러 생성 이벤트의 실행 파일, 권한, 사용자, 시간대를 분류한다. [MITRE] TA0003 Persistence / T1053 Scheduled Task/Job
R048	APT/AV/EDR 판정 불일치 이상	APT, AV, EDR	복합	동일 해시에 대한 보안 솔루션별 verdict 불일치를 위험 feature로 사용한다. [MITRE] TA0005 Stealth / T1027 Obfuscated Files or Information
R049	직무 변경 후 권한 사용 패턴 이상	HR, AD, OS, DLP	복합	직무 변경 이후 이전 직무 권한 사용, 민감 자료 접근, 시스템 로그인 변화를 모델링한다. [MITRE] TA0004 Privilege Escalation / T1098 Account Manipulation
R050	복합 위험 점수: 취약 서버+피싱+EDR 실행+외부 업로드	Vulnerability Scanner, Spam, EDR, Proxy, DLP, HR	복합	여러 모델 점수와 룰 기반 위험을 결합해 공격 흐름 단위의 최종 위험도를 산정한다. [MITRE] TA0001/TA0002/TA0010 / T1190/T1059/T1567

- 시나리오별 상세 분석 절차, 오탐/정탐 판단 기준, 사고대응 절차 등 세부 내역은 [별첨1. 탐지룰-시나리오 상세표]를 참조한다.

4. 생성형 AI(Shadow AI) 보안위협 대응 요건

ChatGPT, Claude, Gemini, Deepseek 등 생성형 AI 서비스 사용 확산에 따른 정보유출 위험에 대응하기 위해, 제안 솔루션은 아래의 AI 사용 행위 패턴을 탐지·분석할 수 있는 방안을 제시하여야 한다.

No	대분류	탐지 행위	예시	의심 유형(위협)
1	정보유출	민감정보 입력 시도	1) 고객정보 2) 주민번호/여권번호 3) 계좌 및 신용카드 번호 4) 소스코드 5) 영업기밀	정보유출 의심
2	정보유출	대량문서 AI분석 요청	1) 300개 문서 2) 500개 이메일 3) 1000개 파일 업로드	퇴사(이직) 준비 정보수집 경쟁사 이직
3	정보유출	업무시간 외 AI 사용량 증가	기본: 09:00 ~ 18:00 최근: 02:00 ~ 05:00 (사용량 급증)	계정탈취 정보유출 비정상 데이터 수집

No	대분류	탐지 행위	예시	의심 유형(위협)
4	정보유출	평소 사용하지 않은 AI 서비스 사용	갑자기 타 서비스 사용 ChatGPT, Claude, Deepseek, Gemini 접속	우회사용 shadow AI 데이터 반출
5	정보유출	AI를 통한 코드 유출	개발자가 프로젝트 전체 소스코드를 AI에 입력 1) Git 저장소에 내용복사 2) 대량코드 붙여넣기 3) 코드파일 업로드	알고리즘 유출
6	정보유출	반복적인 정보추출 요청	1) 계약서 질의 2) 고객목록정리 3) 매출데이터 정리	체계적인 정보 수집
7	정보유출	권한범위를 벗어난 AI 검색	ChatGPT 사용자가 재무팀 자료 또는 인사평가 문서, 임원연봉 자료 질의	내부 탐색
8	정보유출	AI 응답결과 대량 다운로드	AI 가 생성한 결과를 PDF, 엑셀, csv 로 반복 저장	대량 데이터 수집/유출
9	정보유출	신규지역 AI 접속	한국사용자가 10분내 타 지역에서 로그인	계정탈취 VPN 우회
10	정보유출	다수의 AI 계정 생성	동일한 사용자가 ChatGPT, Claude, Gemini, Deepseek 계정 반복 생성	DLP 우회 규제회피
11	정보유출	생성형 AI 를 활용한 자동화 데이터 수집	Copilot Agent 또는 AI Agent 를 이용하여 1) 이메일 10,000건 분석 2) Share point 전체 분석 3) Team 파일 수집	내부 데이터 대량 수집
12	정보유출	퇴사자 전조증상	AI 사용자 로그 중 1) 고객목록 요약 2) 계약서 정리 3) 프로젝트 문서 요약 + USB 사용 증가, 클라우드 업로드 증가, AI 사용 증가	정보 수집

5. 성능 요건

요구사항 번호	요구사항 명	요구사항 내용
PER-1	로그 수집·색인 성능	1. 일 평균 로그 유입량 11GB/day, 최대 1,000EPS 기준 무손실 수집이 가능하여야 한다. (단, 향후 3년 로그소스 증설을 고려하여 30%이상의 여유용량 제시) 2. 대량 로그 유입 시에도 로그 유실이 발생하지 않아야 한다.
PER-2	검색 응답 성능	1. 최근 24시간 데이터 기준 일반 검색 응답시간은 60초 이내를 원칙으로 한다. 2. 장기 보관 데이터(1년 이상) 검색 시에도 조건문 기반 검색이 가능하여야 한다.
PER-3	탐지 처리 성능	1. 실시간 상관분석 룰은 이벤트 발생 후 5분 이내 탐지·알림이 가능하여야 한다. 2. 머신러닝 모델 적용(apply)은 최근 5분~1시간 데이터 기준으로 주기적 수행이 가능하여야 한다.
PER-4	동시 사용자	1. 동시 분석/조회 사용자 2~3명을 수용하여야 한다. 2. 분석 서버 장애 시에도 예정된 스케줄 작업이 지체 없이 전환 수행되어야 한다.

6. 보안 요건

요구사항 번호	요구사항 명	요구사항 내용
SER-1	보안관리 계획 수립	1. 프로젝트 수행사 보안 관리자 지정 및 실행·점검 가능한 보안관리 계획을 수립한다.
SER-2	자체 보안관리 상세 실행방안	1. 자료정보(문서, 데이터 등) 보안관리 방안을 수립하고 관리한다. 2. 물리적 환경(공간, 장비 등) 및 투입인력 보안관리 방안을 수립하고 관리한다. 3. 내/외부망 접근 필요 시 보안관리 방안을 계획하고 관리한다.
SER-3	보안규정 준수	1. 금융 관련 법규 및 당사 보안규정을 준수하여 시스템 구축을 수행해야 한다.
SER-4	개인정보·중요정보 암호화	1. 고유식별정보 등 중요정보 처리 시 암호화를 적용하여야 한다. 2. 감사로그를 통해 관리자·운영자의 모든 작업에 대한 추적성을 확보하여야 한다.

7. 품질 요건

요구사항 번호	요구사항 명	요구사항 내용
QUR-1	테스트	1. 요구사항별 적합/부적합을 판정할 수 있도록 체계적인 테스트를 수행한다. 2. 탐지 시나리오별 오탐/정탐 판단 기준에 따른 테스트를 실시하고 결과를 기록하여 제출한다. 3. 단위·통합·성능 테스트에 대한 테스트 방안을 수립하고 문서화하여 단계별 산출물로 제시하여야 한다.
QUR-2	품질관리 방안수립	1. 제공되는 분석 도구 및 구현방안, 품질 요건 테스트 방안, 개발 단계별 품질 관리 방안을 제시한다. 2. 품질관리를 위한 조직 및 투입인력을 제시한다.
QUR-3	결함관리	1. 프로젝트 과정 中 발견된 모든 결함은 당사 결함관리시스템에 등록하고 프로젝트 기간 中 제거함을 원칙으로 한다.

8. 프로젝트 관리 요건

- 제안업체는 제안 프로젝트의 관리 및 구축 방법론을 제시하여야 하며, 이는 당사 프로젝트 관리 요건 및 산출물 목록에 부합하여야 한다.
- 제안업체는 범위/일정관리, 의사소통관리, 이슈/위험 관리, 품질관리, 형상관리, 투입인력관리에 대한 방안을 제시하여야 한다.
- 프로젝트 수행 時 보안관리 상세 계획을 반드시 포함하여야 한다.
  - 수행사 보안관리자 지정 및 보안관리 계획 수립
  - 자료정보(문서, 데이터 等) 보안관리 방안
  - 물리적 환경(공간, 장비 等) 및 투입인력 보안관리 방안
  - 내/외부망 접근 시 보안관리 방안

9. 기타 주요 요건

- 라이선스 이슈, 비인가 S/W 설치 등으로 인해 발생되는 문제의 책임은 제안 업체에 있다.
- 기존 시스템(장비별 로그원)과의 원활한 연동 등은 본 프로젝트 제안업체의 업무범위에 속한다.
- 3rd Party 솔루션(Threat Intelligence, App 등) 연동 時, 최종 책임은 솔루션 공급사가 아닌 본 프로젝트 제안 업체에 귀속된다.
- 해당 시스템의 운영 안정화 및 운영부서 인수인계 완료는 본 프로젝트 제안 업체의 업무범위에 속한다.

Ⅳ. 제안서 작성 지침

1. 제안서 목차

목 차

2. 세부 작성 지침

- 앞에서 정의된 목차 및 프로젝트 특성을 검토하고, 변경된 사항에 대해 목차를 수정, 보완한다.
- 제안서는 한글 작성을 원칙으로 한다.

- 제안서 용지의 규격은 A4, MS Office PowerPoint 사용을 권고한다.
- 각 장마다 쉽게 참고할 수 있도록 각 장 별로 일련번호를 표기한다.
- 제안서 작성은 본 지침에 따라 각 부문에서 요구하는 내용을 구체적이고 상세하게 기술하여야 하며 "공급될 수 있다", "가능하다" 등의 모호한 표현은 가능한 사용하지 않아야 한다.

- 제안서에 포함된 정보는 제안업체의 입장에서 정확하고 완전한 것이어야 하며, 당사는 제안 내용에 포함된 정보에 대하여 입증할 자료를 제안업체에 요청할 수 있다.

- 필요시 제안업체는 제안서 이외의 보조자료 제출이 가능하다.

Ⅴ. 제안 고려사항

1. 상세 가격 제시

- 구독 서비스의 경우 1년, 5년 기준의 견적서 및 용역에 대한 견적을 구분해서 제출

- 솔루션을 포함하여 제안 時 솔루션 견적을 함께 포함하되 개발비 견적과 분리하여 제출해야 하며, 솔루션 포함 제안 사유를 제안서에 명시하여야 한다.

2. 구축 이후 유지보수에 대한 계획 및 상세 가격 제시

- 유지보수관련 업무別 상세내용 및 투입인력을 제시하여야 한다.

- 유지보수관련 가격은 구축 견적과 별도의 견적서로 같이 제출하여야 한다.

3. 제안업체는 당사 시스템과의 범용성 및 호환성 등을 고려하여 최적의 대안을 제시

- 패키지 기능, 성능, 당사 요구사항 만족도 등의 검토결과를 제출하여야 한다.

- 당사의 기존 이기종 로그원(FW, IPS, WAF, EDR, DLP 등) 연동 방법을 고려하여 제안하여야 한다.

- 제안업체의 제안서에 Out-of-Scope으로 명시되어 당사와 서면 동의되지 않은 부분은 제안업체의 책임으로 귀속된다.

4. 입찰에서 프로젝트 수행 종료 時까지 당사 보안사항 준수 필수

- 입찰참가자는 입찰에 관한 서류 또는 각종 자료 및 입찰과정에서 얻은 모든 정보를 당 입찰 외의 목적으로 사용하지 않는 비밀유지의 의무를 유지한다.

[참고] 중요정보

구분	세부내용
고유 식별정보	주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 ※ 개인정보보호법 제24조 및 동법 시행령 제19조
민감정보	사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 병력, 신체적·정신적 장애, 성적 취향, 유전자 검사정보, 범죄경력정보 등

구분	세부내용
	※ 개인정보보호법 제23조 및 동법 시행령 제18조
인증정보	비밀번호, 바이오정보(지문, 홍채, 정맥 등) ※ 개인정보의 안전성 확보조치 기준 고시 제2조
신용정보	신용정보, 신용카드번호, 계좌번호 등 ※ 신용정보의 이용 및 보호에 관한 법률 제2조, 제19조 등
개인식별정보	이름, 주소, 전화번호, 핸드폰번호, 생년월일, 이메일주소, 성별 등
기타개인정보	해당 사업의 특성에 따라 별도 정의

- 용역수행 중 부정당업자 등록 사유 발생 및 비밀유지 의무 위반 時 계약서에 의거한 계약해제, 해지, 해당인력변경, 손해배상청구 等을 받을 수 있음

VI. 제안서 접수 및 유의사항

1. 제출시기 및 방법(제안서, 견적서)

- 제출기한: 2026년 8월 20일(목) 17시까지
- 제출서류: 제안서, 청렴 서약서, 사업자등록증
- 제출방법: 제출기한까지 이메일 제출
- 제출처: asset.bid@samsug.com
- 제안서 크기 및 포맷: "제안서 작성지침" 참조

2. 작성 시 유의사항

- 제안서 작성과 관련하여 발생하는 모든 제반 소요비용은 정보제공 업체가 부담함을 원칙으로 한다.
- 제출되는 제안서의 기재 내용은 당사의 별도 요청이 없는 한 어떠한 사유로도 수정 또는 삭제할 수 없다.
- 제안서 작성 내용 중 모호한 표현은 불가능한 것으로 간주한다.
- 제안서 기재사항 누락과 기재내용이 상이함에 따라 생기는 불이익은 정보제공 업체가 감수해야 한다.
- 문서는 MS-WORD, 파워포인트, PDF 외에는 허용하지 않는다.
- 문서는 한글로 작성한다.

3. 견적서 작성 지침

- 조직별 상세 업무정의 및 상세 업무별 가격 제시를 병행한다.

- 제안가격 산출 근거를 포함하여 제출한다.

- 가격제안은 부가가치세를 포함한 가격으로 작성해야 한다.

- 패키지를 구성하는 각 구성품목의 가격과 패키지의 유지보수요율을 포함시켜야 한다.

(별첨 1)

표준산출물 리스트

단계	주요 산출물	내용	비고
계약	수행계획서	범위, 일정, 품질 등 프로젝트 수행을 위한 상세 계획 기술	최종 검수 時 최종본 제출
분석	AS-IS 분석서	이기종 로그원·기존 관제체계에 대한 현황 분석 등을 기술	각 단계 종료 후 2주 內 검수 및 제출
설계	To-Be 정의서	탐지 시나리오 설계서, 대시보드 정의서, 연동 인터페이스 정의서 等 포함	
개발	개발 소스 / 탐지룰	시스템 개발 소스 및 탐지 시나리오(룰) 구현 결과	
개발	보안성 검토서	수행사 자체 보안성검토 결과	
개발	테스트시나리오 및 결과서	단위, 통합, 인수, 성능테스트 계획과 시나리오, 결과 기술	
이행	사용자/운영 매뉴얼	사용자 가이드 및 시스템 운영 가이드 기술	
이행	요구사항추적표	업무요건(기능·탐지시나리오·AI위협 대응) 구현과정 기술	
종료	최종검수확인서	프로젝트 모든 검수 대상 산출물 等을 기술	최종 검수 時 첨부

※ 검수 시점 및 산출물 목록은 과제속성에 따라 협의 및 변경 가능

※ 탐지룰-시나리오 상세표(오탐/정탐 판단 기준, 사고대응 절차 등 포함) 및 생성형 AI 보안위협 시나리오 상세표는 원본 데이터 파일(엑셀)을 별첨한다.