

과업지시서

1. 사 업 명	이화여자대학교 원격 보안관제 용역																	
2. 사업기간	계약일로부터 24개월 (총 24개월)																	
3. 사업예산	총 65,000,000 원(부가세 포함)																	
4. 대금지급방법	<table><tr><td>용역</td><td>완료 후 전액 지급 【 】</td><td>선금지급 【 】 ※ 총 용역금액의: %</td></tr><tr><td>유지보수</td><td>월 1회 【 0 】</td><td>기타: 【 】</td></tr></table>			용역	완료 후 전액 지급 【 】	선금지급 【 】 ※ 총 용역금액의: %	유지보수	월 1회 【 0 】	기타: 【 】									
용역	완료 후 전액 지급 【 】	선금지급 【 】 ※ 총 용역금액의: %																
유지보수	월 1회 【 0 】	기타: 【 】																
5. 과업내용	1. 24시간X365일 연속 원격 보안관제 서비스를 제공 2. 대상 장비 리스트 <table><tr><th>관제 대상</th><th>제조사(모델명)</th><th>수량</th></tr><tr><td>인터넷 관문 방화벽(FW)</td><td>현장 설명회 참조</td><td>2</td></tr><tr><td>침입 차단 시스템(IPS)</td><td>현장 설명회 참조</td><td>1</td></tr><tr><td>웹 방화벽(WAF)</td><td>현장 설명회 참조</td><td>1</td></tr><tr><td colspan="2">합계</td><td>4</td></tr></table> 3. 계약일로부터 2주 이내 대상 장비에 대하여 보안관제 시작 4. SIEM 솔루션을 활용한 보안 장비(방화벽, IPS, WAF, VPN 등) 및 정보 보호시스템에서 발생하는 로그 수집·분석, 보안 이벤트 탐지 및 실시간 위협 대응 • 대상 장비를 이용한 상관관계 분석이 가능할 것 • 원격 보안관제 용역업체에서 자체 개발한 통합 보안관리 솔루션(SIEM,SOAR)이 있어야 함 • 대상 장비 간 관련성 분석을 통한 복합 공격에 대한 실시간 탐지 • 자동화된 탐지 룰 및 침해 징후 정교화, 최신 공격기법 반영 • 상세 분석을 통한 정탐 / 오탐 대응 및 조치 권고 5. 각종 보안 침해(악성코드 감염, 랜섬웨어, APT, 불법접근 등)에 대한 위협정보(CTI) 활용 및 인텔리전스 기반 선제적 탐지 6. 사고 조사 및 복구지원 • 침해사고 발생 시 원격접속, 현장출동 등 적극적인 사고 조사 수행 즉각적 탐지·분석·조치, 분석·대응 현황이 포함된 사고 리포트 및 원인 분석 보고서 제출(연 1회 이상 지원) 7. 상세 분석 보고서를 통한 대응 방안 제공 • 월간 관제 결과 리포트 제공 8. 위협 헌팅 및 침해 흔적 조사 서비스 등 • 침해사고 발생 시, 위협 분석 및 침해 흔적 조사 서비스 제공			관제 대상	제조사(모델명)	수량	인터넷 관문 방화벽(FW)	현장 설명회 참조	2	침입 차단 시스템(IPS)	현장 설명회 참조	1	웹 방화벽(WAF)	현장 설명회 참조	1	합계		4
관제 대상	제조사(모델명)	수량																
인터넷 관문 방화벽(FW)	현장 설명회 참조	2																
침입 차단 시스템(IPS)	현장 설명회 참조	1																
웹 방화벽(WAF)	현장 설명회 참조	1																
합계		4																

	9. 긴급 침해사고 발생 시 인시던트 대응 프로세스 이행 및 비상 연락망 확립, 현장 지원 10. 홈페이지 위변조 모니터링 서비스 지원 (WEBMON 이용) 11. 관제 운용에 필요한 정보보호 관련 법령 및 규정(정보통신망법, 개인정보보호법, ISMS 등) 준수. 12. 고객사 정보보호 및 보안 비밀유지 의무(관련 자료 외부 유출·누설 금지). 13. 비상 연락망 구축, 및 트렌드 리서치 보고서 격주 제공 14. 교육 훈련 계획 • 본 사업과 관련된 온라인 교육훈련 제공(20시간/연 10회) 15. 서비스 수준 계약(Service Level Agreement) • 보안관제 서비스 계약 후 보안관제서비스에 대한 품질보증을 위한 계획, 절차, 내용 등을 제시하여야 함 • 보안관제 서비스 계약 후 보안관제 서비스 수준 실적 평가를 위한 객관성 확보 방안 제시(서비스 수준 평가 항목 및 목표치) 하여야 함 • 보안관제 서비스 계약 후 보안관제 서비스 품질 향상을 위하여 매월 실적보고 등을 해야 하며, 미진할 경우 패널티 방안을 제시하여야 함
6. 과업수행결과물	• 월간 관제 결과 리포트
7. 참가자격	1. 현재 국가기관, 지방자치단체 또는 정부 투자기관의 부적합한 업체로 제재받고 있지 아니한 사업자 2. 「국가사이버안전관리규정」 및 「보안관제 전문기업 지정 등에 관한 공고」(과학기술정보통신부 공고, '16.11.16 시행)에 따라 입찰마감 전일까지 보안관제 전문업체로 지정되어 있는 업체로서 '보안관제 전문업체 지정서'를 보유한 사업자 3. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 정보보호 전문서비스 기업으로 지정된 업체로서 '정보보호 전문서비스 기업 지정서'를 보유한 사업자 4. 전문인직업 배상책임보험 가입 업체(전문인업무: 보안관제) 5. 금융기관 보안관제서비스 운영 사례 및 실적 보유 업체 6. 현장 설명회 참여 업체
8. 참가자격 관련 제출서류	1. 보안관제 전문업체 지정서 1부 2. 정보보호 전문서비스 기업 지정서 1부 3. 전문인직업 배상책임보험 가입 증서(전문인업무 : 보안관제) 1부 4. 금융기관 보안관제서비스 운영 관련 실적증명서 각 1부
9. 성범죄자 경력	

조 회	
10. 기타사항	1. 보안관제 시 필요한 원격 및 모니터링 등의 장비 일체는 보안관제 서비스 제공사에서 자체 구축(SIEM, SOAR, 로그관리, 등) 하여야 함 2. 본교 정보보호 담당자에게 필요시 보안관제 포탈화면 을 제공하여야 함 3. 계약 종료 시 수집된 로그는 복구 불가능하게 모두 파기 조치 및 파기 확인서 제출하여야 함 4. 본교의 데이터 송수신 등 원격구간 통신은 반드시 VPN 장비를 통해 전송하여야 함 5. 본교와의 VPN 구성에 필요한 장비는 보안관제 서비스 제공사가 구축(서비스 해지 시 회수) 하여야 함 6. 기존 보안관제 제공사가 구축한 환경 및 SOAR 스크립트 및 차단 정책 등을 모두 이전 받아야 함 (이전 받는 과정에서 발생하는 비용에 대해서는 제안사 측에서 부담)
11. 사업부서 및 연락처	정보인프라팀 (박준석, 02-3277-3073)