

4 EU, 사이버보안 역량 강화에 9,600만 유로 신규 공모 개시

➔ EU, 사이버보안 기술 개발·배포와 대응 역량 구축을 함께 지원

- ECCC, AI 방어 등 7개 분야를 지원하는 사이버보안 신규 공모 개시
 - 유럽사이버보안역량센터(ECCC)가 디지털유럽프로그램(DEP) 산하 총 9,600만 유로 규모의 사이버보안 지원사업 공모를 개시 ('26.9.1), 기술 개발·배포와 현장 대응역량 구축 지원을 병행
 - 공모는 △공공용 AI 보안 도구 △중소기업용 AI 보안 솔루션 △준비태세 테스트 △지역 케이블 허브 △NCC 네트워크 강화 △규제 이행 지원 △민·군 이중용도 기술의 7개 세부 사업으로 구성
 - 사업별 예산은 500만~2,000만 유로로 차등 배분되며, AI 기반 보안 관련 재원에 전체의 3분의 1이 넘는 3,500만 유로가 몰려 이번 공모에서 가장 큰 기술 투자 축을 형성
- 다년도 작업프로그램과 EU 보안 요건이 공모 운영의 기반으로 작용
 - 이번 공모는 ECCC 운영이사회가 승인하는 DEP 2025~2027 사이버보안 작업프로그램에 근거하며, 사이버보안은 DEP의 '특정목표 3'으로 지정되어 ECCC가 이행을 전담하는 구조
 - 재원은 EU 다년도재정프레임워크('21~'27)에서 조달되며, 공모는 단발성 지원이 아니라 승인된 다년도 계획에 따라 사이버보안 투자를 이어가는 관리 체계로 운영
 - 모든 세부 사업의 참여 주체에 DEP 규정 제12조 5항의 EU 보안 요건이 적용되어, 신뢰할 수 있는 주체 중심으로 참여를 거르는 안전장치가 병행되는 점도 특징

➔ AI 기반 사이버 방어부터 핵심 인프라·규제 대응까지 지원 확대

1. 공공과 중소기업으로 나눠 지원하는 AI 사이버보안 투자 설계

- (공공부문) 국가당국부터 국경 간 허브까지 방어 전 주기에 AI 투입
 - AI 기반 방어 사업 중 하나인 공공용 사업에 1,500만 유로를 배정, 국가 당국·CSIRT·NIS2 대상 기관 등에 생성형 AI를 포함한 AI 기반 보안 시스템·도구·서비스의 개발과 배포를 지원
 - 지원 기능은 △위협 탐지 △취약점 탐지 △위협 완화 △사고 복구 △데이터 분석·공유까지 방어 전 주기를 포괄하며, AI 솔루션 자체의 보안·견고성·신뢰성 확보도 요건으로 병행
 - 개별 기관을 넘어 국경 간 허브까지 대상에 포함해 유럽 공동 방어망 전체의 지능화를 겨냥하는 동시에 방어 도구인 AI가 새로운 공격 표면이 되는 위험까지 함께 관리하는 설계로 해석



● (중소기업) 단일 사업 최대 규모 투입, 보안 격차 해소에 초점

- 중소기업(SME) 사업에는 단일 사업 최대 규모인 2,000만 유로를 배정해 △리스크 관리 △위협 탐지 △사고 대응·통지 기능을 갖춘 사용자 친화적 AI 보안 도구의 개발·배포를 지원
- 탐지에서 사고 통지까지 대응 절차 전반을 도구화해, 보안 전담 조직이 없는 SME도 도구에 기대어 방어를 수행할 수 있도록 도입 문턱을 낮춘 구성이 특징
- 공공부문 사업이 방어망의 지능화를 노린다면 SME 사업은 보급 확대에 초점, 역내 전체 방어 수준이 가장 약한 고리에서 결정된다는 인식이 최대 자원 배정으로 이어진 것으로 분석

2. 중요 인프라와 해저케이블까지 보호 범위 확대

● (준비태세 테스트) 사이버연대법의 비상대응 체계를 재정으로 가동

- 앞의 AI 사업이 방어 도구의 확보를 겨냥한다면, 준비태세 테스트 부문은 확보한 도구가 실제 위기에서 작동하는지 확인하는 대응 태세의 점검에 해당
- 고위험·핵심 부문 기관을 위한 준비태세 테스트 부문에는 1,500만 유로를 투입해, 사이버연대법상 ‘사이버보안 비상 메커니즘’ 산하 2개 조치에 해당하는 대응 태세 점검을 지원
- 지원 활동은 △침투테스트 △위협 평가 △취약점·리스크 모니터링 △조율된 취약점 공개 △훈련·교육으로 구성되어, 사고 발생 전 약점을 찾아 보완하는 검증형 활동이 중심
- 개별 기관의 자율 점검이 아닌 EU 전역에서 조율된 방식이라는 점이 핵심으로, 입법으로 설계된 비상대응 체계가 공모 재정을 통해 실행 단계로 옮겨가는 과정으로 해석

● (케이블 허브) 해역 단위 감시 거점으로 물리 인프라까지 보호

- 지역 케이블 허브 사업에는 500만 유로를 배정, EU 해역(sea basin)별 1개씩 허브를 점진 구축해 해저케이블 인프라의 복원력 제고와 보안 강화를 지원
- 허브는 △신흥 위협 탐지·분석 △준실시간 상황인식 △사고 보고 △국가당국 간 정보공유의 기능을 갖추며, 여러 나라의 관할 해역을 지나는 케이블 특성에 맞춘 해역 단위 관리가 특징
- 배정 예산은 7개 사업 중 가장 작지만 소프트웨어 중심의 보안 투자가 물리 인프라로 확장된 대목으로, 해저케이블 위협 대응이 개별 회원국 소관에서 EU 공동 관리로 옮겨가는 변화로 분석

3. 생태계 육성과 규제 이행 지원으로 완성하는 투자 설계

- (생태계·규제 이행) 커뮤니티 육성과 법제 이행 지원으로 방어 저변 확충
 - 도구와 인프라가 방어의 물적 기반이라면, 나머지 3개 사업은 이를 운용할 인력·기업 저변과 제도 이행을 뒷받침하는 역할로, 기술 투자가 실제 방어력으로 이어지기 위한 연결 고리에 해당
 - 국가조정센터(NCC) 네트워크 강화 부문에는 1,100만 유로를 투입해 △첨단 보안 솔루션 보급 △보안 인식 제고 △스킬 육성 △스타트업·SME 성장 지원 등 커뮤니티 지원 기능을 확대
 - 규제 이행 지원 부문에는 2,000만 유로를 배정해 CRA·NIS2·GDPR·AI법 등 EU 법제로 새로 생긴 의무와 책임에 직면한 이해관계자에게 재정적·조직적 지원을 제공
 - 규제로 의무를 부과하는 동시에 이행 비용을 재정으로 뒷받침하고 인력·기업 저변까지 함께 키우는 구조로, 준수 부담이 큰 중소 주체의 이탈 없이 제도를 안착시키려는 설계로 해석
- (이중용도) 민간과 국방의 경계를 잇는 보안 기술 개발 지원
 - 민·군 이중용도 기술 부문에는 1,000만 유로를 투입해 민간과 국방 양쪽에서 쓰이는 보안 기술의 △작동 프로토타입 △출시 가능한 제품 △운영 인프라 개발을 지원
 - 산출물로 시제품 수준을 넘어 ‘출시 가능한(ready-to-market)’ 제품까지 명시해, 연구 결과가 실제 조달·활용으로 이어지는 단계까지 사업 범위에 포함
 - 민간 보안 기술이 국방 수요로 이어지는 통로를 공적 지원으로 마련하는 시도로, 민·군 간 운영 협력 강화라는 목표를 기술 개발 지원이라는 실행 수단으로 구현한 사례로 분석

출처 : IEU Monitoring 외(2026.9.)

<https://ieu-monitoring.com/editorial/eccc-opens-e96m-digital-europe-cybersecurity-calls-covering-ai-cable-hubs-and-dual-use/1248637>

<https://cadeproject.org/updates/eu-cybersecurity-centre-opens-e96-million-funding-call/>

https://cybersecurity-centre.europa.eu/news/new-eccc-call-proposals-under-digital-europe-programme-open-applications-2026-09-01_en