KISA 정보보호 해외진출 전략거점(동남아 남부) 12월 주요동향

2025. 12. 30(화), 한국인터넷진흥원 보안산업단 [글로벌협력팀]

이슈	링크	주요내용 및 시사점
[인도네시아] (12월 1일) OJK·PPATK·BSSN이 금융 부문의 무결성과 보안을 강화하기로 합의했음.	https://katadata.co.id/berita/nasional/692c289edd824/ojk-ppatk-bssn-sepakati-penguatan-integritas-keamanan-sektor-jasa-keuangan	● 인도네시아 금융서비스청(Otoritas Jasa Keuangan, OJK), 금융거래보고분석센터(Indonesian Financial Transaction Reports and Analysis Center, PPATK), ● 국가사이버암호기관(Badan Siber dan Sandi Negara, BSSN)은 금융 서비스 부문의 보안 강화를 위해 업무협약(Collaboration Agreement, PKS)을 체결했음. ● 협약에는 자금세탁방지(Money Laundry Crime, TPPU), 테러자금조달방지(Terrorism Crime, TPPT), 대량살상무기 확산자금조달방지(Proliferation Financing of Weapons of Mass Destruction, PPSPM)가 포함됨. ● OJK–PPATK PKS는 2024년 5월 체결된 양해각서의 후속 조치이며, OJK–BSSN PKS는 금융, 혁신기술, 디지털 자산 및 크립토자산(cryptocurrency/크립토자산) 분야 사이버보안 강화를 목표로 함. ● 협약은 데이터 교환, 디지털 포렌식 지원, 사이버 사고 대응, 사이버 컨택 센터 구축 등 전 부문의 사이버보안 역량 강화를 포함함. ● 이번 협약은 자카르타에서 OJK, PPATK, BSSN 수장이 직접 참관하며 체결했음.

[인도네시아] (12월 1일) 멀티파이낸스 해킹이 화제가 되자 아스트라 리싱 대표가 입장을 밝혔음.	https://www.cnbcindonesia.com/market/20251201140630-17-690013/heboh-multifinance-kena-hack-bos-leasing-astra-bilang-gini	● PT 클리판 파이낸스 인도네시아(Clipan Finance Indonesia, CFIN) 해킹 의혹이 금융 리스 산업 전반의 데이터 보안 우려를 불러일으킴. ● 아스트라 크레딧 컴퍼니즈(Astra Credit Companies, ACC) CMSO는 사이버 보안 문제가 산업 내에서 반복적으로 발생해 온 사안이라고 설명함. ● ACC 내부 시스템은 정보기술(Information Technology, IT) 팀 관리 하에 안전하게 운영되고 있다고 강조함. ● 고객 데이터 보호를 위해 ACC는 엄격한 사이버 보안 기준과 최상위 디지털 방어 프로그램 및 장비를 적용하고 있음. ● ACC는 증가하는 사이버 위험에 대응하기 위해 상당한 보안 예산을 지속적으로 배정하고 있음.
[인도네시아] (12월 3일) 인도네시아는 핀테크 보안을 강화하기 위해 AI 윤리 규범을 개정했음.	https://opengovasia.com/indonesia-updated-ai-ethics-code-strengthens-fintech-security/?c=id	● 인도네시아 금융서비스청(Otoritas Jasa Keuangan, OJK)은 핀테크와 생성형 AI 관련 위험에 대응하기 위해 AI 윤리 강령을 업데이트함. ● OECD 지원으로 개정된 가이드라인은 소비자 보호, 데이터 신뢰성, 금융 포용성, 데이터 보안, 사이버 복원력 원칙을 강화함. ● 이번 개정에는 국가결제게이트웨이(National Payment Gateway, GPN) 등 국가 시스템과 유사하게 공정성 원칙도 포함됨. ● OJK는 AI가 효율성, 사기 탐지, 서비스 개인화는 높이지만 환각, 데이터 유출, 편향 알고리즘 등의 위험도 초래한다고 지적함. ● 2024년 11월~2025년 10월 중순 사이 약 30만 건의 사기 신고가 접수됐으며, OJK는 9만4천 개 이상 계정을 차단하고 '2L' 규칙 준수를 권고했음.

[인도네시아] (12월 4일) 인도네시아 지방정보통신부 협회가 한국과 협력해 사이버 보안 강화에 나섰음.	https://daerah.sindonews.com/read/1651289/174/asosiasi-dinas-kominfo-provinsi-seluruh-indonesia-gandeng-korsel-perkuat-keamanan-siber-1764753120	● 인도네시아 전국 지방정부 통신정보국 연합체(Asosiasi Kepala Dinas Komunikasi dan Informatika Provinsi Seluruh Indonesia, ASKOMPSI)는 한국 사이버보안 기업 LSWare Inc.와 지방정부 사이버보안 강화를 위한 양해각서(Memorandum of Understanding, MoU)를 체결함. ● 서명식은 서울 LSWare 본사에서 진행됐으며, 여러 주(Provinsi) 및 Diskominfo 대표들이 화상회의(Zoom)를 통해 참여함. ● 협력의 핵심은 지방정부 ICT 인력 역량 강화이며, LSWare는 기술 교육, 워크숍, 지속적 기술 지원을 제공하기로 했음. ● 이번 MoU는 지방 행정(Pemerintah Daerah, Pemda)의 안전한 디지털 전환과 사이버보안 기반 공공 서비스 구축을 목표로 함. ● ASKOMPSI와 LSWare는 2026년 Digital Leadership Government Awards (ADLGA) 프로그램까지 포함한 장기 협력을 통해 지속 가능한 체계를 구축하기로 했음.

[인도네시아] (12월 4일) 인도네시아는 글로벌 사이버보안 지수(GCI) 점수를 높여 사이버 방어를 강화함.	https://polkam.go.id/kemenko-polkam-perkuat-pertahanan-siber-melalui-skor-global-cybersecurity-index-indonesia/	● Kemenko Polkam(Coordinating Minister for Political and Security Affairs of Indonesia)은 인도네시아의 Global Cybersecurity Index(GCI) 점수 향상을 위한 권고안 마련을 목표로 조정회의를 개최했음. ● 정부는 GCI 개선이 단순한 순위 경쟁이 아니라 국가 사이버 공간의 안정성과 신뢰도를 보여주는 지표라고 강조했음. ● 마르스마 TNI 부디 에코 프라토모는 법적 기반, 기술적 역량, 조직적 체계, 역량 강화, 협력 등 GCI 다섯 핵심 영역을 통합적으로 강화해야 한다고 밝힘. ● 회의에는 부처기관(Ministry/Institution, K/L), 지방정부, 민간 부문, 이해관계자가 참여해 국가 사이버보안 역량과 BSSN(Badan Siber dan Sandi Negara) 역할을 논의했음. ● Kemenko Polkam은 규제 강화, 인력 양성, 국제 협력 확대를 포함한 실행 가능한 전략적 권고안으로 디지털 회복력 강화를 추진하기로 했음.
[인도네시아] (12월 5일) 텔콤은 동부 인도네시아의 디지털 주권을 강화하며 neuCentrIX 자야푸라를 공식 운영했음.	https://wartabalionline.com/2025/12/05/telkom-perkuat-kedaulatan-digital-di-timur-indonesia-neucentrix-jayapura-resmi-beroperasi/	● Telkom은 neuCentrIX Jayapura를 공식 개소하며 파푸아 지역에 첫 데이터 센터이자 28번째 edge 데이터 센터를 설치했음. ● 이 시설은 인도네시아 디지털 주권 강화를 목표로 동부 지역의 디지털 인프라 접근성을 확대함. ● neuCentrIX Jayapura는 공공서비스, 정부 데이터 처리, 지역 기업 지원 등 파푸아의 디지털 전환을 촉진함. ● 데이터 센터는 국제 표준 인프라를 갖추고 안전한 콜로케이션, 통합 연결성, 국가 인터넷 교환망(neuCentrIX) 접속을 제공함. ● 이번 개소는 TelkomGroup의 포용적 디지털 접근성 확보 의지를 보여주며, 지역 경제와 사회 서비스 향상에 기여했음.

[인도네시아] (12월 8일) 인도네시아는 아동의 디지털 이용을 공식적으로 규제하고 플랫폼 제재도 마련 중임.	https://www.merahputih.com/post/read/indonesia-resmi-atur-anak-di-ruang-digital-sanksi-bagi-platform-tengah-dirumuskan	● 인도네시아는 2025년 3월 아동 보호를 위한 전자시스템 운영 거버넌스를 규정한 정부령 PP 17/2025 (PP Tunas)를 공식화하고 시행 전 1년의 준비 기간을 설정했음. ● PP Tunas는 아동 연령과 위험 수준에 따라 소셜미디어 및 디지털 플랫폼 접근을 단계적으로 지연하도록 규정함. ● 규제는 소셜미디어뿐 아니라 낯선 사람과 상호작용 가능한 모든 전자시스템운영자(Penyelenggara Sistem Elektronik, PSE)에 적용됨. ● 통신디지털부(Kementerian Komunikasi dan Digital, Kemkomdigi)는 위험도 기반 플랫폼 분류체계와 제재 기준을 하위 규정에서 구체화하고 법률 격상도 검토 중임. ● 정부는 인도네시아가 호주와 함께 아동의 소셜미디어 접근을 구체적으로 규제한 선도 국가임을 강조하며 PP Tunas로 디지털 공간의 아동 보호를 강화했음.

[인도네시아] (12월 8일) 사이버대학교는 인도네시아 에마스 2045를 향한 IS-SMART 출범을 전폭 지원했음.	https://news.republika.co.id/berita/t6y27q472/cyber-university-dukung-penuh-peluncuran-issmart-menuju-indonesia-emas-2045	● 인도네시아는 Indonesia Society on Smart Technologies(IS-SMART)를 출범하며 지능형 기술 분야의 국가 협업 생태계를 공식 구축했음. ● 사이버 대학교(Cyber University)는 IS-SMART 설립에 참여하며 국가 디지털 전환 지원 의지를 표명함. ● 출범식은 "지능형 기술 교육을 통한 Indonesia Emas 2045"를 주제로 인적개발문화조정장관(Coordinating Minister for Human Development and Cultural Affairs, Menko PMK), DKI 자카르타 부지사, 교육부(Ministry of Education and Culture, Kemendikbud) 및 국가연구혁신청(National Research and Innovation Agency, BRIN) 관계자들이 참석했음. ● Cyber University는 MoU를 통해 스마트 기술 교육과 개발 분야에서 정부학계산업 커뮤니티 협력을 공식화했음. ● IS-SMART는 기술 주권과 자립적 기술 개발을 기반으로 Indonesia Emas 2045 실현을 추진한다고 밝힘.

[인도네시아] (12월 9일) 인도네시아 도박 산업에서 전국적인 사이버 연계 정황이 드러나고 있음.	https://gbhackers.com/indonesias-gambling/	● Malanta의 보안 연구진은 14년 이상 활동한 대규모 인도네시아어 기반 사이버 범죄 생태계를 발견했음. ● 이 조직은 32만8천 개 이상의 도메인을 통제하며 AWS(Amazon Web Service), Azure, Cloudflare 등 글로벌 클라우드를 광범위하게 활용함. ● 공격자는 취약한 워드프레스 PHP, 방치된 DNS, 만료 클라우드 자원을 악용해 합법적 HTTPS(Hypertext Transfer Protocol) 트래픽으로 위장한 C2(Command-and-Control)를 운영함. ● 모바일 악성코드 인프라는 7,700개 도메인을 통해 악성 APK 배포, 데이터 유출, FCM(Firebase Cloud Messaging) 원격 명령을 수행하며 인도네시아 IP전화번호은행 계좌 인증을 요구함. ● 연구진은 중앙집중화된 인프라와 높은 기술 완성도를 근거로 해당 작전을 국가 지원 APT(Advanced Persistent Threat) 수준으로 평가했음.
[인도네시아] (12월 10일) 클라우드플레어에 따르면 인도네시아가 전 세계 최대 DDoS 공격 발원지로 나타났음.	https://www.netralnews.com/indonesia-jadi-sumber-serangan-siber-ddos-terbesar-di-dunia-menurut-cloudflare/UEF3TGcxaG91OUZHODNUYkVXNVdxZz09	● 클라우드플레어(Cloudflare)는 2025년 3분기 보고서에서 인도네시아가 세계 최대 DDoS(Distributed Denial of Service) 공격 발원국이라고 발표했음. ● 인도네시아발 HTTP(Hypertext Transfer Protocol) 기반 공격은 최근 5년간 31,900% 증가했음. ● 태국, 베트남, 방글라데시, 인도, 싱가포르도 주요 발원지로 확인됐으며, 가장 많은 공격 피해 국가는 중국이었음. ● 보고서에 따르면 2025년 7~9월 동안 총 830만 건의 DDoS 공격이 탐지됐고, 아이수루(Aisuru) 봇넷이 핵심 위협으로 지목됨. ● 클라우드플레어는 시간당 평균 3,780건의 공격을 차단하며 대규모 DDoS 위협이 지속적으로 증가할 것으로 전망했음.

[인도네시아] (12월 10일) 인도네시아가 디지털 방향성 선언을 발표했음.	https://www.menpan.go.id/site/berita-foto/deklarasi-arah-indonesia-digital	● 인도네시아 국가행정개혁부(Minister of State Apparatus Utilization and Bureaucratic Reform, PANRB) 리니 위디안티니 장관은 'Arah Indonesia Digital' 선언 행사에 참석했음. ● 행사는 통신디지털부(Komdigi) 메우티아 하피드 장관이 개회했으며, '연결되고, 성장하고, 보호된다'는 주제로 진행됨. ● 정부는 선언을 통해 Indonesia Emas 2045와 연계된 국가 디지털 발전 전략 방향을 제시했음. ● 리니 장관은 디지털 정부와 관료제 개혁이 국가 디지털 전환 성공의 핵심임을 강조했음. ● PANRB는 BSSN 등 주요 기관과 함께 Komdigi로부터 국가 디지털 전환 전략 파트너로 인정받았음.
[인도네시아] (12월 11일) 호주와 인도네시아가 사이버 협력을 강화했음.	https://www.nationaltribune.com.au/australia-and-indonesia-deepen-cyber-ties-3/#google_vignette	● 호주와 인도네시아는 인도-태평양 인데버(Indo-Pacific Endeavour) 프로그램 일환으로 자카르타에서 사이버 세미나를 개최했음. ● 세미나에는 호주 국방군(Australian Defence Force, ADF)과 인도네시아 국가군(Indonesia Army, TNI) 사이버 전문가들이 참여했음. ● 양국은 사이버 위험 우선순위와 협력 필요성에 대해 공감대를 확인했음. ● 참가자들은 전 부대 사이버 인식 제고와 의심 활동 신속 보고, 비전문 인력 교육 방안을 논의했음. ● 이번 세미나는 회복력 있는 네트워크 구축과 향후 공동 교류 강화를 위한 기반을 마련했음.

[인도네시아] (12월 11일) 인도네시아는 미래를 위한 새로운 디지털 발전 방향을 제시했음.	https://manadopost.jawapos.com/lifestyle-teknologi/286942176/kemkominfo-ungkap-arah-baru-pembangunan-digital-indonesia-untuk-masa-depan	● 인도네시아 통신디지털부(Kemkominfo)는 국가 디지털 개발의 새로운 전략을 발표했음. ● 전략은 연결성, 디지털 역량, 데이터 생태계, 사이버 보안을 중심으로 디지털 전환을 추진함. ● 고속인터넷 보편화와 함께 AI, 클라우드, 사물인터넷(IoT) 등 핵심 기술 도입을 강조했음. ● 디지털 리터러시 강화와 데이터 거버넌스를 개선해 디지털 격차 해소와 사이버 회복력을 높이는 목표임. ● 민관 및 국제 협력을 통해 글로벌 디지털 경제 경쟁력과 미래 대응 역량을 강화하려고 함.
[인도네시아] (12월 15일) 인도네시아와 인도는 아시아의 디지털 강국 구축을 위해 협력했음.	https://rri.co.id/en/international/2042440/indonesia-india-partner-to-create-digital-powerhouse-in-asia	● 인도네시아와 인도는 아시아 디지털 경제 선도를 목표로 협력을 강화하고 있음. ● Komdigi는 양국 협력을 오랜 파트너십의 전략적 연장선으로 평가했음. ● 협력 핵심은 디지털 인프라, 인재 양성, 스타트업 생태계 분야에 있음. ● AI, 디지털 공공 인프라, 반도체전자 공급망, 사이버 보안, 데이터 거버넌스에서 협력을 확대할 계획임. ● 이번 협력은 아시아 디지털 경쟁력 강화와 전략적 연대 구축을 동시에 추진하는 행보임.

[인도네시아] (12월 16일) 텔콤셀과 ITB는 디지털 인재 육성을 위해 인도네시아 최초의 AI 혁신 허브를 출범했음.	https://industri.kontan.co.id/news/telkomselitb-resmikan-ai-innovation-hub-pertama-di-indonesia-dorong-talenta-digital	● 텔콤셀(Telkomsel)과 반둥 공과대학교(ITB)는 2025년 12월 16일 AI 혁신 허브(AI Innovation Hub)를 개소했음. ● 허브는 텔콤셀의 Hitakari 이니셔티브와 연계해 AI 인재 양성과 국가 디지털 전환 가속화를 목표로 함. ● 텔콤셀과 ITB가 공동 운영하며 AI 아카데미, AI 랩, 해커톤, 네트워킹 등 프로그램을 제공함. ● 초기에는 수백 명을 대상으로 AI 교육과 Komdigi 협력 인증 프로그램이 시행될 예정임. ● 이번 개소는 Indonesia Emas 2045 비전과 국가 AI 전략을 지원하기 위한 디지털 인재 역량 강화 조치였음.
[인도네시아] (12월 16일) BSSN과 인력부는 사이버 보안 협력을 추진했음.	https://infodigital.co.id/bssn-dan-kemnaker-kerja-sama-keamanan-siber/	● 인도네시아 국가사이버암호기관(BSSN)과 노동부(Ministry of Manpower, Kemnaker)는 2025년 12월 15일 사이버 보안 협력 MoU를 체결했음. ● MoU에는 데이터정보 공유, 사이버 및 암호 기술 역량 강화, 전자거래 보안 인증서 활용 등 6개 협력 분야가 포함됨. ● 노동부는 BSSN 지원이 Kemnaker 정보 시스템과 보안 강화에 기여해 왔다고 평가함. ● BSSN은 대통령 프라보워 수비안토로부터 국가 사이버 보안과 핵심 데이터 보호 임무를 부여받은 기관임. ● 이번 협력은 사이버 위협 대응과 데이터 보호 역량 강화로 국가 사이버 회복력을 높이기 위한 조치였음.

[인도네시아] (12월 17일) 인도네시아 디지털 투자 비즈니스 미팅 2025는 인도네시아와 UAE 간 블록체인 협력을 강화함.	https://jogja.antaranews.com/berita/789394/indonesia-digital-investment-business-meeting-2025-perkuat-kolaborasi-blockchain-indonesia-uae	● Indonesia Digital Investment Business Meeting 2025는 두바이 인터넷 시티에서 개최돼 디지털 투자와 블록체인 협력 강화에 초점을 맞춤. ● 행사는 Indonesia Blockchain Center(IBC)가 주최하고 Dubai Blockchain Center와 Sealbound가 지원함. ● UAE 주재 인도네시아 대사관과 총영사관 대표들이 양국 디지털 협력 증진 공로로 명예상을 받음. ● 포럼에서는 블록체인과 자산 토큰화가 산업 투명성, 거버넌스 강화, 글로벌 자금 접근성을 제공할 수 있음이 강조됨. ● 이번 회의는 인도네시아를 글로벌 디지털 경제 전략적 파트너로 자리매김하고 UAE와 지속 가능한 투자 협력을 확대하려는 의지를 보여줬음.
[인도네시아] (12월 18일) BGN은 6,000억 루피아 규모의 정보 시스템 구축을 위해 페루리를 직접 지정했음.	https://koranbumn.com/bgn-lakukan-penunjukan-langsung-peruri-untuk-membangun-sistem-informasi-senilai-rp600-miliar/	● 국가영양청(National Nutrition Agency, BGN)은 무료 영양 급식 프로그램(Nutritious Meals Program, MBG) 디지털화를 위해 6,000억 루피아 규모의 국가 영양 이행 정보시스템을 구축하고 있음. ● 해당 사업은 2025년 국가예산(State Budget, APBN)으로 편성되었고, 직접 지정 방식으로 조달이 진행됨. ● 정부조달정책기관(National Public Procurement Agency, LKPP)은 2025년 10월 22일 조달 계획(Rational Unified Process(RUP) 코드 60685000)을 수립했음. ● BGN은 대형 시스템 구축을 위해 국영기업 페루리(Peruri)를 수행 기관으로 직접 지정함. ● 디지털화를 통해 예산 유용 방지와 공동 감독을 강화하고 MBG 운영 효율성을 높이는 조치였음. ● 하루 4,900만 명에게 도달하는 성과를 뒷받침하려는 목적이었음.

[인도네시아] (12월 19일) 인도네시아 정부 기관들은 사이버 보안 강화를 위한 협약을 체결했음.	https://jatim.antaranews.com/berita/1015396/indonesia-agencies-seal-pact-to-strengthen-cyber-security	● 인도네시아 국가사이버암호청(Badan Siber dan Sandi Negara, BSSN)과 국가개발기획부(Ministry of National Development Planning, Kementerian PPN)는 국가 사이버 보안 강화를 위해 5년 협력 협약을 체결함. ● 협약에는 사이버 보안암호기술, 전자 인증, 개발 계획 지원, 데이터 공유 등 다양한 협력 분야가 포함됨. ● 양 기관은 사무총장 간 별도 협약을 통해 기술 협력과 프로그램 실행 기반도 마련함. ● 교육훈련, 역량 개발, 정보보안 문화 확산, 디지털 문해력 제고 활동 등도 협력 범위에 포함됨. ● 이번 협약은 프라보워 수비안토 대통령의 정책 기조에 따라 국가 사이버 회복력과 디지털 전환을 강화하려는 공동 의지를 확인한 조치였음.
[인도네시아] (12월 19일) 인도네시아는 아동의 온라인 보호를 위해 다각적인 조치를 시행했음.	https://opengovasia.com/indonesia-multi-faceted-measures-to-safeguard-children-online/?c=global	● 인도네시아 정부는 아동 보호를 위한 전자시스템 관리 정부령 제17호(2025년) 시행을 앞두고 부모 대상 홍보 강화를 촉구함. ● 통신디지털부는 규정 실효성을 위해 정보기술 자원봉사단과 지역사회 단체의 참여가 필요하다고 강조함. ● 정부령 내용이 복잡해 지역사회가 부모들에게 취지와 적용 방식을 설명하는 역할이 중요함. ● 해외 사례를 들어 제정 이후 사회적 적응에 시간이 걸리는 것은 자연스러운 과정임을 설명함. ● 이번 조치는 플랫폼 책임 강화와 공동 대응을 통해 아동 온라인 안전을 높이려는 정책적 노력임을 분명히 했음.

[인도네시아] (12월 23일) 얼굴 인식 기반 SIM 등록은 2026년부터 시행되며 관련 규정이 전면 공개됐음.	https://www.beritasatu.com/multimedia/2951863/registrasi-sim-pakai-wajah-berlaku-2026-ini-aturan-lengkapnya#goog_rewarded	● 인도네시아 정부는 고객 데이터 보호와 디지털 범죄 억제를 위해 얼굴 인식 기반 생체인식 SIM 카드 등록 제도를 도입할 계획임. ● 통신디지털부(Kemkominfo)는 제도가 2026년 초부터 단계적으로 시행될 예정이라고 밝힘. ● 얼굴 생체인식은 스캠, 피싱, 번호 오남용 방지와 가입자 신원 검증 강화를 목표로 함. ● 초기에는 자발적 참여 방식으로 운영되며 기존 NIK(National ID Number) 가족카드(KK) 기반 제도를 점진적으로 대체함. ● 이번 정책은 국가 디지털 보안 생태계 강화를 위한 핵심 조치로 평가되었음.
[인도네시아] (12월 29일) 공식적으로 오픈AI가 인도네시아의 디지털 세금 징수 주체로 지정됐음.	https://www.inews.id/news/nasional/resmi-openai-jadi-pemungut-pajak-digital-di-indonesia	● 인도네시아 국세청(Directorate General of Taxes, DJP)은 전자상거래 부가가치세(VAT/PPN) 징수를 위해 254개 기업을 전자상거래 과세 대상(Electronic Trading System Organizer, PMSE) 징수자로 지정함. ● 이번 지정에는 OpenAI와 International Bureau of Fiscal Documentation, Bespin Global, OpenAI OpCo, LLC 등 3개 신규 기업이 포함됨. ● 반면 Amazon Services Europe S.a.r.l.은 PMSE 징수자 지정이 철회됨. ● 2025년 11월 30일 기준 215개 PMSE 기업이 세금을 납부했으며, 누적 세수는 34.54조 루피아로 집계됨. ● 정부는 핀테크와 전자조달시스템(Case Tracking Information System, SIPP) 과세를 포함해 디지털 경제 세수 기반을 지속적으로 확대했음.

[인도네시아] (12월 29일) 사이버 보안 지침이 공식적으로 발표됐음.	https://rri.co.id/yogyakarta/iptek/2067935/pedoman-keamanan-siber-diluncurkan	● 인도네시아 핀테크 산업 협회(Indonesia Fintech Association, AFTECH)는 사이버 보안 가이드라인(Cyber Security Guidelines/Pedoman Keamanan Siber)을 공식 발표함. ● 가이드라인은 예방, 탐지, 대응, 내부 사고 처리 등 사이버 보안 전 주기를 기술적으로 규정함. ● AFTECH 사이버보안 부서는 국가사이버암호청(BSSN)과 CISSReC와 협력해 문서를 마련했음. ● 이번 조치는 AFTECH 통합 윤리강령 2025에서 사이버 보안을 핵심 원칙으로 채택한 후속 조치임. ● 이를 통해 핀테크 산업 전반의 사이버 회복력과 운영 표준을 체계적으로 강화했음.
[말레이시아] (12월 1일) 말레이시아는 사이버 방어를 강화하고 통신사들은 MyDigital ID 연동을 시작했음.	https://www.bernama.com/en/general/news.php?id=2497799	● 말레이시아 MCMC는 페낭 지역 미디어와 안전한 인터넷 캠페인(Safe Internet Campaign/Kempen Internet Selamat/KIS)을 강화함. ● 캠페인은 아동 온라인 안전과 증가하는 온라인 사기에 대한 인식 제고를 목표로 함. ● 페낭 전역 40여 명 미디어 종사자가 참여해 안전 메시지 확산 역할을 수행함. ● 행사는 JKPKK 등과 공동 기획돼 언론의 디지털 리터러시와 사이버 보안 역할을 강조함. ● 이번 캠페인은 언론 참여를 통해 소비자 보호와 사이버 보안 책임을 강화했음.

[말레이시아] (12월 2일) MCMC는 페낭 언론계와 함께 안전한 인터넷 캠페인을 강화했음.	https://bernama.com/en/news.php//world/crime_courts/news.php?id=2497232	● 말레이시아는 통신사에 MyDigital ID 신원 인증 시스템을 도입해 국가 사이버 방어를 강화함. ● National Cyber Security Agency(NACSA)와 Malaysian Communications and Multimedia Commission(MCMC)가 협력해 이 이니셔티브를 추진함. ● 시스템은 사기 전화, 신분 위조, 디지털 사기 차단을 목표로 함. ● 주요 조치는 선불 SIM 화이트리스트, 신규 SIM 등록 강화, 앱 로그인 시 인증된 신원 요구를 포함함. ● 이번 조치는 개인정보 보호와 국가 사이버보안 전략을 동시에 강화했음.
[말레이시아] (12월 3일) 카스퍼스키(Kaspersky)와 APU는 말레이시아의 사이버 보안 인재 육성 강화를 위해 협력했음.	https://www.businesstoday.com.my/2025/12/02/kaspersky-apu-partner-to-boost-malaysias-cybersecurity-talent/	● 카스퍼스키(Kaspersky)는 APU와 사이버 보안 인재 양성을 위한 MoU를 체결함. ● 협력 기간은 3년이며, 학문 프로그램 개선과 교수진 역량 강화가 포함됨. ● 학생들은 강연과 KIPS(Kaspersky Interactive Protection Simulation) 대회를 통해 실무형 사이버 대응 경험을 쌓음. ● 양측은 이번 협력이 말레이시아 디지털 성장과 사이버 회복력 강화에 기여할 것으로 평가함. ● 이번 MoU는 교육과 산업을 연결해 미래형 사이버 인재 생태계를 구축하려는 노력임.

[말레이시아] (12월 4일) 레오나르도는 지역 안보 지원을 위해 쿠알라룸푸르에 사이버 센터를 열었음.	https://www.crnasia.com/news/2025/cybersecurity/leonardo-opens-cyber-center-in-kuala-lumpur-to-support-regio	● 이탈리안 보안기업 레오나르도(Leonardo)가 쿠알라룸푸르에 지역 사이버 센터(Regional Cyber Centre)를 개소함. ● 센터는 글로벌 사이버보안 센터(Global CyberSec Center, GCC) 네트워크와 연계돼 운영됨. ● 말레이시아는 강력한 사이버 법체계와 중요 인프라 보호 경험을 바탕으로 신규 허브로 선정됨. ● 센터는 사이버, 물리, 핵심 통신을 통합해 하이브리드 위협 대응과 국가 안보를 지원함. ● 이번 개소는 말레이시아를 동남아 보안 허브로 공고히 하고 글로벌 네트워크 핵심 축으로 부상시키는 계기였음.
[말레이시아] (12월 5일) ZTE와 MMU는 말레이시아의 AI 사이버보안 디지털 인재 육성 강화를 위해 협력을 확대했음.	https://www.zte.com.cn/global/about/news/ZTE-and-MMU-expand-collaboration-to-advance-Malaysia-s-AI-cybersecurity-and-digital-talent-development.html	● 글로벌보안기업인 ZTE corporation와 멀티미디어대학교(Multimedia University, MMU)는 협력 확대를 위한 부속합의(addendum)를 체결함. ● 양측은 AI, 사이버 보안, 5G, 디지털 인재 양성 분야 협력을 강화하기로 합의함. ● MMU에는 ZTE의 AiCube 풀스택 AI 교육 플랫폼과 스마트 교실 인프라가 도입돼 몰입형 학습 환경이 마련됨. ● 해당 인프라는 MMU 학생뿐 아니라 공공서비스위원회(Public Service Department/Jabatan Perkhidmatan Awam/JPA) 프로그램 참가자에게도 개방됨. ● 이번 협력은 말레이시아의 디지털 전환과 혁신 생태계 지원을 위한 전략적 인재 양성 조치였음.

[말레이시아] (12월 8일) 말레이시아는 비트코인 채굴 절도 단속을 강화했음.	https://www.redhotcyber.com/en/post/malaysia-cracks-down-on-bitcoin-mining-thefts/	● 말레이시아는 약 1만 4천 개 불법 비트코인 채굴장을 추적 중임. ● 지난 5년간 약 11억 달러 규모의 전력 도난이 발생했음. ● 당국은 드론과 휴대용 센서를 활용해 이상 전력 사용을 감시하고 있음. ● 국영 전력회사 테나가 내셔널 베르하드(National Energy Limited/Tenaga Nasional Berhad/TNB)는 재정 손실과 전력 인프라 훼손 위험을 경고했음. ● 정부는 불법 채굴이 조직 범죄 수준의 국가 시스템 위협으로 확산됨에 따라 강력 대응에 나섰음.
[말레이시아] (12월 18일) 소셜미디어 대기업들은 2026년부터 말레이시아 법의 적용을 받게 됐음.	https://www.straitstimes.com/asia/se-asia/social-media-giants-subject-to-malaysian-laws-from-2026	● 말레이시아는 2026년 1월 1일부터 주요 소셜미디어를 자국 법률 적용 대상에 포함하기로 함. ● 이용자 800만 명 이상 사업자는 통신멀티미디어법(Communications and Multimedia Act/CMA)에 따른 라이선스를 적용받음. ● 대상 플랫폼에는 Instagram, Facebook, WhatsApp, TikTok, YouTube, Telegram이 포함됨. ● 말레이시아 통신멀티미디어위원회(MCMC)는 이번 조치가 플랫폼 책임과 이용자 안전을 명확히 하기 위한 것이라고 설명함. ● 말레이시아는 16세 미만 아동의 소셜미디어 이용을 제한해 온라인 아동 보호를 강화했음.

[말레이시아] (12월 22일) 2025년 말레이시아에서는 사이버 사고 신고가 5,700건 이상으로 급증했음.	https://thesun.my/news/malaysia-news/cyber-incidents-surge-in-malaysia-with-over-5700-reports-in-2025/?utm_source=Newswav&utm_medium=Website	● 말레이시아 사이버보안청(CyberSecurity Malaysia) 산하 사이버침해사고대응센터(Cyber999)는 올해 9월까지 5,735건의 사이버 사고 신고를 접수함. ● 디지털부 사무총장 파비안 비가르는 전년 대비 1,000건 이상 증가해 디지털 위협이 일상화됐다고 설명함. ● 말레이시아 왕립경찰(Royal Malaysia Police/Polis Diraja Malaysia/PDRM)에 따르면 11월까지 통신 사기를 중심으로 한 온라인 사기 피해액은 7억 링깃(RM700 million)을 초과함. ● 사고 유형은 사기, 데이터 유출, 악성코드 공격, 침입 시도 등이며 모든 인터넷 이용자가 잠재적 표적임이 강조됨. ● 정부는 디지털 인식 강화와 지역 디지털 회복력 제고를 통해 사이버 위협에 대응했음.
[말레이시아] (12월 26일) 말레이시아와 싱가포르는 증가하는 위협 속에서 해양 사이버보안 협력을 강화했음.	https://ipdefenseforum.com/2025/12/malaysia-singapore-strengthen-maritime-cybersecurity-ties-amid-rising-threats/	● 말레이시아와 싱가포르는 해저 케이블과 항만 물류 등 핵심 해상 인프라 보호를 위해 해양 사이버보안 협력을 확대하고 있음. ● 이번 협력은 글로벌 해운 산업의 사이버 취약성 심화에 대응하기 위한 조치임. ● 양국은 말라카 해협 순찰(Malacca Strait Patrols, MSP)을 기반으로 전통적 해상 안보 협력을 사이버 위협 대응과 실시간 정보 공유로 확장했음. ● 싱가포르 라자라트남 국제연구원(S. Rajaratnam School of International Studies, RSIS)과 Center for Strategic and International Studies (CSIS)는 해저 케이블과 해양 인프라의 전략적 중요성과 취약성을 강조함. ● 싱가포르 Maritime and Port Authority (MPA)와 말레이시아 MISC Berhad (Malaysia International Shipping Corporation Berhad)를 중심으로 AI 기반 대응과 데이터 공유를 강화해 아세안(ASEAN) 해양 디지털 회복력 기준을 제시했음.

[싱가포르] (12월 1일) 싱가포르 기업들은 AI와 데이터 활용에서는 앞서지만 여전히 사이버 보안 과제에 직면했음.	https://www.straitstimes.com/paid-press-releases/singapore-businesses-lead-in-ai-and-data-adoption-but-face-cybersecurity-challenges-20251201	● CPA 오스트레일리아 조사에 따르면 싱가포르 기업의 데이터 분석 도입률은 95%, 인공지능(AI) 도입률은 92%로 글로벌 평균을 크게 상회함. ● 많은 기업이 ChatGPT, Microsoft Copilot, Google Gemini 등을 제한적으로 활용하지만, 일부는 AI를 전사 전략에 깊이 통합함. ● CPA 오스트레일리아 싱가포르 지부 회장 그렉 언스워스는 AI의 실질적 가치를 위해 전략적 통합이 필요하다고 강조함. ● 사이버 보안 성숙도는 낮아 기업의 23%만이 보안을 경영 전략에 포함하고 있으며, 취약한 대응 중심 거버넌스 문제가 나타남. ● 이번 조사는 싱가포르의 경쟁력이 AI 활용 확대와 함께 사이버 회복력 및 책임 있는 혁신 문화 강화에 달려 있음을 보여줬음.
[싱가포르] (12월 3일) 유럽연합과 싱가포르는 AI와 사이버 보안 협력을 강화했음.	https://batamnewsasia.com/2025/12/03/eu-singapore-digital-cooperation-council-expands-ai-cybersecurity-and-semiconductor-focus/	● 유럽연합(EU)과 싱가포르는 AI 안전, 사이버 보안, 반도체, 신뢰 가능한 데이터 흐름 분야에서 협력을 강화함. ● 제2차 디지털 파트너십 이사회에서 혁신, 회복력, 경쟁력 강화를 목표로 한 공동 로드맵을 확정함. ● 양측은 AI 안전을 핵심 의제로 삼아 ALT-EDIC과 싱가포르 Sea-Lion 간 언어 모델 연구와 온라인 안전 강화 방안을 추진함. ● 국경 간 검증 가능한 자격 증명과 상호 운용 가능한 디지털 신원 및 신뢰 서비스 개발에도 합의함. ● 이번 협력은 사이버 보안 공동 대응과 반도체 양자 기술, 데이터 스페이스 협력을 통해 신뢰 가능한 유럽-아시아 디지털 생태계 구축을 진전시켰음.

[싱가포르] (12월 9일) 싱가포르는 국경 없는 온라인 위협에 맞춰 사이버 법규 최신화 과제에 직면했음.	https://www.scmp.com/week-asia/politics/article/3335660/can-singapores-cyber-laws-keep-pace-speed-borderless-online-threats?module=perpetual_scroll_0&pgtype=article	● 싱가포르는 주요 보험사가 설립한 인공지능 센터 오브 엑설런스(CoE)를 출범하며 국가 AI 전략을 발전시킴. ● 고한얀 국회 보좌관은 AI 도입 속도가 빠르며, 조직이 장기적 변화를 위해 실험과 새로운 사고방식을 수용해야 한다고 강조함. ● 센터는 인재 육성과 책임 있는 AI 활용을 핵심 목표로 삼고, 워크포스 전환과 조직 전체 AI 역량 향상에 주력함. ● 보험사는 Institute of Banking and Finance (IBF)와 Monetary Authority of Singapore (MAS)와 협력해 파일럿 프로그램과 직무 재설계를 통해 직원들의 고부가가치 역할 수행을 지원함. ● 이번 CoE 출범은 산업 전반에 AI가 인간 업무를 대체하는 것이 아닌 강화하는 방향으로 책임 있는 AI 문화를 확산시키는 사례였음.
[싱가포르] (12월 9일) 싱가포르는 새로운 'AI 우수센터(Artificial Intelligence Centre of Excellence (CoE))'를 통해 AI 역량 강화를 추진.	https://opengovasia.com/singapore-advancing-ai-fluency-with-new-centre-of-excellence/?c=global	● 싱가포르는 외국 간섭과 사이버 범죄를 억제하기 위해 다양한 법적 수단을 마련했음. ● 전문가들은 신속한 삭제 명령과 표적형 법률이 허위정보와 조직적 온라인 공격 대응에 도움을 준다고 평가함. ● 최근 OCHA(Online Criminal Harms Act) 근거로, 말레이계 무슬림 사회 대상 허위 적대적 콘텐츠를 게시한 줄피카르 모하맛 샤리프의 틱톡과 메타 계정을 싱가포르 이용자 대상으로 차단했음. ● FICA(Foreign Interference (Countermeasures) Act)는 해외 세력의 적대적 정보 개입 차단을 가능하게 함. ● 전문가들은 법률만으로는 급변하는 디지털 위협에 충분치 않으며, 지역 협력과 국민 디지털 역량 강화가 필요하다고 지적했음.

[싱가포르] (12월 11일) 공급망 위협이 커지는 가운데 싱가포르는 글로벌 제3자 사이버 위험 대응에서 선도적 위치를 차지했음.	https://www.techedt.com/singapore-leads-global-third-party-cyber-risk-maturity-as-supply-chain-threats-intensify	● 블루보이언트(BlueVoyant) 보고서에 따르면, 싱가포르는 공급망 서드파티 사이버 위험 관리 성숙도에서 세계 선두 수준을 유지하며, 조직의 60%가 강력한 서드파티 위험 관리 프로그램을 갖추고 있음. ● 이 수준은 미국 등 전통적 선진 시장을 능가하지만, 공급망 관련 사이버 사고는 여전히 빈번하며, 조직의 93%가 공급업체 관련 침해로 부정적 영향을 경험했음. ● 응답자의 거의 절반은 지난해 2~5건의 서드파티 침해를 겪었고, 3분의 1 이상은 최소 한 건의 침해를 경험함. ● 조직들은 경영진 감독 강화와 외부 전문 기관 아웃소싱 확대 등 투자를 늘리고 있으며, AI를 서드파티 위험 모니터링의 핵심 기술로 적극 도입할 계획임. ● 블루보이언트는 공급망 사이버 위험을 단순 준수 과제가 아니라 일상적 비즈니스 의사결정에 통합해야 한다고 강조함.

[싱가포르] (12월 15일) 싱가포르 경찰은 대규모 사기 단속에서 53만 9천 싱가포르달러를 압수하고 176개 은행 계좌를 동결했음.	https://the420.in/singapore-police-anti-scam-operation-investment-scams/	● 싱가포르 경찰청(Singapore Police Force/SPF)은 사이버 사기와 자금세탁 조직과 관련된 은행 계좌 176개를 동결하고 약 53만 9천 싱가포르달러를 압수했음. ● 이번 작전은 2025년 11월 17일부터 28일까지 반사기 사령부(Anti-Scam Command)와 경찰 육상부서 사기 전담팀이 공동으로 진행했음. ● 주요 단속 대상은 정부 기관 사칭 사기, 허위 투자 사기, 온라인 구인 사기 등 세 가지 유형이었음. ● 조사 결과 16세부터 85세까지의 피의자들이 범죄 조직에 계좌나 전자지갑을 제공해 자금세탁에 가담한 사실이 확인됐음. ● 이들은 범죄수익몰수법(Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act)과 컴퓨터 오남용법(Computer Misuse Act)에 따라 처벌받을 수 있음.
[싱가포르] (12월 15일) 싱가포르는 해양 산업을 위한 사이버 방어 훈련 센터를 공개했음.	https://maritimefairtrade.org/singapore-unveils-cyber-defense-training-center-for-maritime-industry/	● 싱가포르 기술디자인대학교(Singapore University of Technology and Design, SUTD)는 해양 산업 중심 실습형 사이버 보안 교육을 강화하고 있음. ● 이를 위해 실제 사이버 공격을 재현하는 마리오티(MariOT) 시설을 도입해 학생들이 실무 경험을 쌓도록 지원함. ● 싱가포르 해양항만청(Maritime and Port Authority of Singapore, MPA)은 IoT 등 디지털 기술 도입으로 해상 사이버 위협이 증가하고 있다고 강조함. ● SUTD와 MPA는 향후 3년간 선원, 항만 운영자, 사이버 보안 전문가 등 300명 이상을 대상으로 마리오티 훈련을 공동 개최할 예정임. ● 에이미 코 교통부 수석국무차관은 탈탄소화 디지털화 인력 개발이 해양 산업의 미래를 좌우한다고 언급하며, 싱가포르의 글로벌 해양 허브 경쟁력 유지에 기여할 것임.

[싱가포르] (12월 17일) 싱가포르와 중국은 기술 기반 경제 협력을 강화했음.	https://opengovasia.com/singapore-china-advance-tech-driven-economic-collaboration/?c=global	● 싱가포르와 중국은 충칭에서 열린 고위급 양자 회의를 통해 기술, 혁신, 디지털 경제 분야 협력 강화를 재확인했음. ● 이번 회의는 수교 35주년을 맞아 양국 관계에서 기술 기반 협력의 중요성을 강조했음. ● 양측은 디지털 연결성 강화, 규제 정합성 확보, 국경 간 데이터 거버넌스가 지속 가능한 성장과 역내 회복력에 필수적이라는 데 합의했음. ● 충칭 커넥티비티 이니셔티브(Chongqing Connectivity Initiative)와 신국제 육해무역회랑(New International Land–Sea Trade Corridor)을 중심으로 물리 디지털 인프라 연계가 추진됨. ● 디지털 금융, 연구 혁신 협력, e-CNY 시범 결제 등 실질적 프로젝트를 통해 양국은 디지털 경제 주도권 확보를 공동으로 모색하고 있음.
[싱가포르] (12월 26일) 싱가포르의 AI 및 기술 산업이 2025년 GDP 성장 모멘텀을 견인했음.	https://opengovasia.com/singapore-ai-and-tech-sectors-power-2025-gdp-momentum/?c=global	● 싱가포르 경제는 2025년 예상보다 높은 성과를 기록하며 Ministry of Trade and Industry (MTI)가 GDP 성장률 전망치를 약 4.0%로 상향 조정했음. ● 성장은 기술, 디지털 혁신, 인공지능(AI) 관련 산업이 제조 무역 서비스 전반에서 견인했음. ● 전자 제조 클러스터는 AI 반도체와 서버 수요 증가로 3분기 전년 대비 6.1% 성장했고, 인포컴 및 소비자 전자 부문은 67.6% 급성장했음. ● 바이오의약 제조, ICT, 금융 보험, 무역 전문 서비스 부문도 각각 첨단 제조 기술, 데이터 호스팅, 디지털 결제, AI 기반 수요 확대로 안정적 성장을 기록했음. ● 종합적으로 기술 AI 디지털 혁신이 싱가포르 경제의 핵심 성장 축으로 자리 잡고 국가 경쟁력과 회복력을 강화했음.

[브루나이] (12월 19일) 브루나이는 블록체인 혁신 보호를 위해 암호자산 지식재산권 제도를 구축했음.	https://www.mondaq.com/india/trademark/1720774/brunei-s-approach-to-crypto-ip-rights-coining-patents-for-blockchain-innovations	● 블록체인 기술은 스마트 계약과 암호화폐 등 다양한 분야에서 IP(Intellectual Property) 보호가 중요한 영역으로 성장하고 있음. ● 브루나이 다루살람은 보통법과 국제 IP 협약 참여를 바탕으로 블록체인 IP 보호에서 전략적 입지를 구축하고 있음. ● 특허 제도(Patents Order, 2011)는 기술 중립적으로 운영되어 블록체인 관련 발명도 보호 가능하며, 특허협력조약(Patent Cooperation Treaty, PCT)와 마드리드 프로토콜 가입으로 국제 보호도 지원됨. ● 상표법(Trademarks Act, 2017)은 블록체인 서비스 브랜드와 암호화폐 플랫폼 로고까지 보호하며, 중앙은행인 브루나이 통화청(Autoriti Monetari Brunei Darussalam, AMBD)는 암호자산에 대해 투자 위험 경고만 발령함. ● 결과적으로 브루나이는 암호화폐 규제에는 신중하나, 유연한 IP 체계를 통해 블록체인 혁신을 수용하며 조용하지만 의미 있는 암호 IP 국가로 자리매김했음.
[베트남] (12월 24일) 베트남에서는 금융 안보 확보를 위해 조기 탐지의 중요성이 강조됐음.	https://opengovasia.com/vietnam-early-detection-crucial-to-ensure-financial-security/?c=global	● 베트남 전문가들은 디지털 시대 국가 금융 안보를 위해 조기 탐지와 선제적 대응, 기관 간 긴밀한 협력이 필수적이라고 강조했음. ● 국가사이버보안협회(National Cybersecurity Association/NCA) 부위원장 응우옌 민 치인은 금융 시스템과 디지털 결제 인프라, 금융 데이터가 국가 안보와 직결된다고 설명했음. ● 베트남은 결의안 57호 68호, 디지털기술산업법 및 사이버보안법 2025 등을 통해 금융 디지털 안보의 제도적 기반을 마련했음. ● 국가은행(State Bank of Vietnam/SBV)는 은행권 디지털 전환을 선도하며 정보보안 역량을 강화하고, 공안부 사이버 하이테크범죄예방국(Department for Cybersecurity and High-Tech Crime Prevention/A05)는 국제 협력을 통해 대응 능력을 확대했음. ● 워크숍에서는 정부, 금융권, 보안기관의 통합적 대응이 디지털 경제 안정성과 회복력 확보에 핵심임을 재확인했음.

[인도] (12월 26일) 안드라 프라데시 경찰은 통신 사기에 연루된 국제 사이버범죄 조직을 적발했음.	https://www.siasat.com/andhra-police-busts-international-cybercrime-network-involved-in-telecom-fraud-3316886/	● 인도 안드라프라데시 범죄수사국(Andhra Pradesh Criminal Investigation Department, AP-CID)은 통신부(Department of Telecommunications, DoT)와 협력해 심박스(SIM Box) 운영과 통신 사기에 연루된 국제 범죄 조직원 14명을 체포했음. ● 피의자들은 외국인 2명을 포함하며, VoIP를 이용해 동남아에서 인도로 통화를 우회 전송해 약 20억 루피(Rs 20 crore) 피해를 발생시켰음. ● 범죄 조직은 텔레그램(Telegram)과 왓츠앱(WhatsApp)을 통해 국내 공범과 지시를 주고받고, 가짜 이름 임시 주소를 이용해 장비를 은밀히 반입하고 설치했음. ● 특별 수사팀은 비사카파트남, 하이데라바드, 루르켈라, 날란다, 아람볼, 콜카타 등에서 동시 단속을 실시해 운영자와 판매점(Point of Sale, POS) 관계자를 검거했음. ● 경찰은 심박스 14대, 다수의 통신 전산 장비, 약 1,500개의 SIM 카드를 압수하고, 자금 흐름과 추가 범죄 연계를 계속 추적하고 있음.
[필리핀] (12월 10일) DND는 IT 거버넌스와 사이버 보안을 위한 새로운 프레임워크를 발표했음.	https://www.pna.gov.ph/articles/1264691	● 필리핀 국방부(Department of National Defense, DND) 장관 길베르토 테오도로 주니어는 CYBERCON 2025에서 IT와 사이버보안 기준을 담은 국방부 훈령을 공식 발표했음. ● 이번 훈령은 국방 기관 전반의 정보 자산, 통신망, 임무 필수 플랫폼 보호와 사이버 회복력 강화를 목표로 통합 표준 체계를 마련했음. ● 국방부 산하 민간 부서와 군에 전달돼 전면 시행되며, 관련 정책 조정에 기여한 비상위원회 구성원은 Outstanding Achievement 훈장을 받았음. ● DND 사이버 훈련에서는 모의 사이버 위협 대응 능력을 평가해 우수 부대를 시상했음. ● CYBERCON은 국방부의 물리 디지털 영역 보호 임무에 맞춰 기관 간 협력과 사이버 대비태세 강화에 핵심적 역할을 하고 있음.

[필리핀] (12월 16일) 필리핀 상원은 블록체인 기반 예산 시스템을 승인했음.	https://opengovasia.com/the-philippines-senate-oks-blockchain-based-budget-system/?c=global	● 필리핀 상원은 CADENA 법(Citizen Access and Disclosure of Expenditures for National Accountability)을 최종 독회에서 만장일치로 통과시켰음. ● 법안은 모든 정부 기관이 예산과 조달 기록을 중앙 디지털 예산 플랫폼에 정기적으로 공개하도록 의무화함. ● 핵심 내용은 국가 예산 블록체인 시스템(National Budget Blockchain System)을 구축해 예산 배정, 집행, 조달 거래 기록을 위변조 없이 추적 가능하게 관리함. ● 플랫폼은 국민 누구나 예산 정보를 열람할 수 있도록 설계됐으며, 데이터는 공개 소스이자 독립 검증 가능함. ● CADENA 법은 공공 재정 관리 현대화와 시민의 정부 지출 감시 강화에 기여할 것으로 기대됨.
[태국] (12월 29일) 태국은 청소년의 AI 역량 강화를 위해 새로운 사이버보안 교육과정을 도입했음.	https://opengovasia.com/thailand-new-cybersecurity-curriculum-boosts-ai-skills-for-youth/?c=global	● 태국 Ministry of Higher Education, Science, Research and Innovation(MHESI)는 출라롱콘대학교와 AIS와 협력해 AI 사이버보안 역량 강화를 위한 신규 교육과정을 개발했음. ● 이번 MoU는 2025년 12월 26일 체결됐으며, AIS '안자이 사이버(Aunjai Cyber)' 콘텐츠를 고등교육에 편입했음. ● 교육과정은 2026년 2월부터 온라인으로 무료 제공되며, 학점 전환 가능한 크레딧 뱅크 제도를 통해 공식 인정됨. ● 총 10개 모듈은 딥페이크 식별, 안전한 AI 활용, 개인정보 보호 등 실무 중심 내용으로 구성됨. ● 출라롱콘대학교는 책임 있는 AI 활용과 정보 검증을 핵심 가치로 삼아 프로그램을 전국으로 확대할 계획임.

정보보호 해외진출 전략거점(중남미) 12월 주요동향

2025. 12. 31.(수), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[칠레] 국가 사이버 보안 프레임워크 법 제정 및 생태계 활성화	▸ **칠레, 포괄적인 '사이버 보안 프레임워크 법(Framework Law)' 시행을 통해 국가 보안 거버넌스 및 산업 생태계 강화(12월 1일)** ✓ 칠레 정부는 국가 사이버 보안 수준을 근본적으로 개선하기 위해 설계된 새로운 프레임워크 법률을 공식 시행함 ✓ 이 법안은 국가 사이버 보안국(ANCI)을 신설하여 범정부 차원의 보안 정책을 총괄하고 사고 대응을 지휘하게 함 ✓ 중요 인프라 운영자(OIV)에 대해 엄격한 보안 표준 준수와 사고 보고 의무를 부과하여 국가 마비 사태에 대비함 ✓ 새로운 법적 체계는 민간 보안 기업들에게 명확한 규제 가이드라인을 제공하여 관련 보안 솔루션 투자를 활성화하는 촉매제가 됨 ✓ 특히 사이버 보안을 국가적 우선순위로 설정함으로써 연구 개발(R&D) 지원과 인력 양성을 위한 제도적 기반을 마련함 ✓ 칠레가 라틴 아메리카 내에서 가장 안전한 디지털 허브로 도약하기 위한 전략적 토대를 구축한 것으로 평가받음 ✓ 글로벌 기업들이 안심하고 투자할 수 있는 안전한 비즈니스 환경을 조성하여 국가 경제 성장에 기여하고자 함 ✓ 이번 법 제정은 주변 국가들에게도 보안 입법의 모델로 작용하며 지역 내 보안 규제 강화를 선도할 것으로 보임 ✓ ttps://blog.investchile.gob.cl/cybersecurity-chile-new-framework-law
[브라질] 일본과 사이버 보안 분야 첫 공동 워킹 그룹 출범	▸ **브라질과 일본, 글로벌 사이버 위협 공동 대응 및 기술 협력을 위한 첫 번째 실무 회의 개최(12월 1일)** ✓ 브라질과 일본 정부는 사이버 보안 분야에서의 전략적 파트너십을 강화하기 위해 공동 워킹 그룹(Working Group)을 공식 출범시킴 ✓ 양국은 핵심 인프라 보호, AI 보안 기술, 그리고 5G 등 차세대 통신망 보안에 관한 지식과 경험을 공유하기로 함 ✓ 특히 일본의 앞선 보안 기술력과 브라질의 역동적인 디지털 시장을 결합하여 시너지를 창출하려는 목적을 가지고 있음 ✓ 이번 워킹그룹은 국제 사이버 규범 수립에 있어 협력을 강화하고, 국경을 초월한 사이버 범죄 수사 공조 체계를 다지는 계기가 됨 ✓ 민간 기업 간의 기술 교류와 비즈니스 매칭을 지원하여 양국의 보안 산업 동반 성장을 꾀하고 있음 ✓ 브라질은 일본의 사례를 통해 국가적 차원의 보안 거버넌스 체계를 고도화하고 인재 양성 프로그램을 벤치마킹할 예정임 ✓ 양국은 정기적인 회의를 통해 구체적인 협력 프로젝트를 발굴하고 실행 성과를 점검해 나갈 계획임 ✓ 이는 브라질이 전통적인 서방 국가 중심의 협력을 넘어 아시아 선진국과도 보안 파트너십을 확장하고 있음을 보여줌 ✓ https://www.agenzianova.com/en/news/giappone-brasile-avviato-il-primo-gruppo-di-lavoro-congiunto-sulla-cybersicurezza/
[멕시코] 국가 사이버 보안 계획 공식 발표	▸ **멕시코 정부, 국가 안보 및 디지털 주권 강화를 위한 '국가 사이버 보안 계획' 공개(12월 2일)** ✓ 멕시코 정부는 증가하는 사이버 위협에 대응하고 국가 핵심 인프라를 보호하기 위한 포괄적인 '국가 사이버 보안 계획'을 공식 발표함 ✓ 이 계획은 범정부 차원의 대응 체계를 구축하고, 공공기관 간의 위협 정보

이 슈	주 요 내 용 및 시 사 점
	공유 메커니즘을 표준화하는 데 중점을 두고 있음 ✓ 특히 사이버 범죄 수사 역량 강화와 디지털 환경에서의 시민 권리 보호를 핵심 전략 과제로 설정하여 법적 프레임워크를 정비함 ✓ 국가 사이버보안 위원회를 신설하여 민간 부문 및 학계와의 협력을 촉진하고, 국가적 차원의 사고 대응 역량을 한 단계 높이려는 의지를 보여줌 ✓ 급증하는 랜섬웨어 및 국가 배후 공격에 대비하기 위해 인프라 현대화와 전문 인력 양성을 위한 예산 배정을 공식화함 ✓ 이번 계획은 멕시코가 디지털 전환 과정에서 겪는 보안 공백을 메우고, 글로벌 보안 표준에 부합하는 방어 체계를 갖추는 전환점이 될 것으로 예상됨 ✓ 정부는 본 계획을 통해 대중의 디지털 신뢰도를 높이고 해외 투자 유치를 위한 안전한 사이버 생태계를 조성하는 것을 목표로 함 ✓ https://www.bnamericas.com/en/news/mexico-unveils-national-cybersecurity-plan
[멕시코] 가상자산 탈취 급증에 따른 제로 트러스트 의무화	▸ **멕시코, 34억 달러 규모의 가상자산 피해 발생에 대응하여 '제로 트러스트' 보안 원칙 도입 촉구(12월 4일)** ✓ 멕시코 내 가상자산 관련 범죄 피해액이 34억 달러(약 4조 5천억 원)에 달하며 경제 전반에 심각한 위협으로 부상함 ✓ 사이버 범죄자들이 피싱, 악성코드, 거래소 해킹 등 고도화된 수법을 동원하여 개인과 기업의 디지털 자산을 표적으로 삼고 있음 ✓ 이에 따라 보안 전문가들과 정책 입안자들은 기존 경계 보안의 한계를 인정하고 모든 접근을 의심하는 '제로 트러스트(Zero Trust)' 모델 도입을 강력히 권고함 ✓ 특히 금융 기관과 가상자산 거래소에 대해 다중 인증(MFA), 세밀한 접근 제어, 지속적인 모니터링 체계 구축을 의무화하려는 움직임이 나타남 ✓ 가상자산 탈취는 단순 금전 피해를 넘어 국가 금융 시스템의 신뢰도를 저하시키는 요인이 되며, 이를 방지하기 위한 기술적 규제 강화가 시급함 ✓ 멕시코 당국은 블록체인 보안 기술 도입을 장려하고, 범죄 자금의 흐름을 추적하기 위한 국제 공조 체계를 강화하고 있음 ✓ 제로 트러스트 아키텍처의 확산은 보안 솔루션 시장의 패러다임 변화를 야기하며, 관련 인증 및 가시성 확보 솔루션 수요를 급격히 증대시킬 것으로 보임 ✓ 기업들은 자산 보호를 위해 보안 투자를 비용이 아닌 필수적인 위험 관리 전략으로 인식해야 함을 강조함 ✓ https://mexicobusiness.news/cybersecurity/news/mexico-mandates-zero-trust-crypto-theft-hits-us34-billion
[엘살바도르] 미주개발은행(IDB), 엘살바도르의 사이버 보안 성과 높게 평가	▸ **IDB, 엘살바도르 정부의 사이버 보안 강화 조치와 제도적 발전을 긍정적인 국가 혁신 사례로 언급(12월 5일)** ✓ 미주개발은행(IDB)은 엘살바도르가 최근 시행한 사이버 보안 관련 법률 제정과 국가 CIRT(컴퓨터 침해사고 대응팀) 역량 강화를 높이 평가함 ✓ 엘살바도르는 디지털 자산 법제화와 함께 이를 뒷받침할 사이버 보안 인프라 구축에 국가적 역량을 집중해왔음 ✓ IDB 보고서는 엘살바도르가 공공 부문의 디지털 전환 과정에서 보안을 우선순위에 둔 점이 지역 내 다른 국가들에게 모범이 된다고 분석함 ✓ 특히 국제기구와의 협력을 통해 전문가를 양성하고, 국가적 차원의 사이버 위협 모니터링 체계를 구축한 성과를 강조함 ✓ 이러한 긍정적 평가는 엘살바도르가 향후 국제 금융 기구로부터 디지털 인프라 확충을 위한 추가적인 자금 지원을 받는 데 유리하게 작용할 전망임 ✓ 엘살바도르 정부는 이번 성과를 바탕으로 사이버 보안을 국가 경제의 핵심 경쟁력으로 키우겠다는 포부를 밝힘 ✓ 지역 내 보안 취약국에서 보안 혁신국으로 변모하려는 엘살바도르의 노력은 중남미 지역 전체의 보안 수준 상향 평준화에 기여할 것으로 보임

이 슈	주 요 내 용 및 시 사 점
	✓ 앞으로 민간 부문과의 협력을 확대하여 국가 전체의 사이버 회복 탄력성을 공고히 하는 과제가 남아 있음 ✓ https://dplnews.com/el-salvador-el-bid-destaca-medidas-importantes-en-ciberseguridad/
[브라질] 통신사 Vivo, 텔레포니카로부터 사이버 보안 사업부 재인수	▸ **브라질 최대 통신사 Vivo, 보안 역량 내재화 및 B2B 시장 경쟁력 강화를 위해 보안 사업 부문 통합 단행(12월 5일)** ✓ 브라질의 주요 통신 사업자인 Vivo는 모기업인 텔레포니카(Telefónica)로부터 사이버 보안 사업부를 다시 인수하여 독자적인 보안 서비스 역량을 강화함 ✓ 이번 인수는 급성장하는 브라질 내 기업(B2B) 보안 시장에서 주도권을 확보하고, 통신 서비스와 결합된 통합 보안 솔루션을 제공하기 위함임 ✓ Vivo는 자체 보안 관제 센터(SOC)와 전문 인력을 확보함으로써 고객들에게 더 신속하고 맞춤화된 보안 서비스를 제공할 수 있게 됨 ✓ 통신망 보안과 단말 보안을 통합 관리하는 서비스를 통해 디지털 전환을 추진하는 기업 고객들의 수요를 흡수하려는 전략임 ✓ 거대 통신사의 보안 시장 진출 강화는 브라질 보안 업계의 지형 변화를 야기하며 경쟁을 더욱 가속화할 전망임 ✓ Vivo는 이번 통합을 통해 클라우드 보안, IoT 보안 등 신성장 분야로 서비스 범위를 대폭 확장할 계획임 ✓ 데이터 보안과 프라이버시 보호가 중요해지는 시점에 통신사의 신뢰도를 기반으로 보안 시장에서의 입지를 공고히 하려는 움직임임 ✓ 보안 기술의 내재화는 통신사 스스로의 네트워크 안전성을 높이는 데도 기여할 것으로 기대됨 ✓ https://www.telcotitans.com/telefonicawatch/brazils-vivo-buys-back-cybersecurity-unit-from-telefonica/9993.article
[멕시코] 에스토니아와 사이버 보안 및 디지털화 협력 체결	▸ **멕시코와 에스토니아, 디지털 정부 구축 및 사이버 방어 역량 강화를 위한 전략적 파트너십 구축(12월 8일)** ✓ 세계적인 디지털 선진국인 에스토니아와 멕시코가 사이버 보안 및 공공 부문 디지털화를 위한 협력 방안을 논의함 ✓ 양국은 에스토니아의 성공 모델인 'X-Road'와 같은 안전한 데이터 교환 플랫폼 구축 노하우를 공유하기로 합의함 ✓ 멕시코는 에스토니아의 전자 시민권 및 디지털 ID 보안 기술을 벤치마킹하여 자국의 디지털 행정 서비스 안전성을 높이고자 함 ✓ 이번 협력은 단순 기술 이전을 넘어 사이버 보안 정책 수립, 사고 대응 팀(CERT) 운영 노하우 전수 등 포괄적인 지식 공유를 포함함 ✓ 특히 정부 기관 간의 상호 운용성을 확보하면서도 강력한 암호화 체계를 유지하는 보안 설계 원칙을 학습하는 데 집중함 ✓ 양국은 글로벌 사이버 위협에 공동 대응하기 위해 실시간 위협 인텔리전스 공유 채널을 구축하고 전문가 교류 프로그램을 운영할 예정임 ✓ 에스토니아의 앞선 사이버 방어 전략 도입은 멕시코가 라틴 아메리카 내 디지털 리더십을 확보하는 데 중요한 동력이 될 것으로 기대됨 ✓ 국제적인 협력을 통해 멕시코의 취약한 사이버 인프라를 보완하고, 선진화된 디지털 거버넌스를 구축하려는 노력을 보여줌 ✓ https://mexicobusiness.news/cybersecurity/news/mexico-estonia-collaborate-cybersecurity-digitalization
[멕시코] 연방 기관 대상 제로 트러스트 아키텍처 도입 의무화	▸ **멕시코 정부, 모든 연방 기관에 제로 트러스트 보안 모델 도입을 명령하여 국가 데이터 보호 강화(12월 10일)** ✓ 멕시코 연방 정부는 공공 부문의 데이터 유출 사고를 방지하기 위해 모든 연방 기관에 '제로 트러스트' 보안 원칙 준수를 의무화함 ✓ 이는 최근 발생한 대규모 정부 데이터 유출 사고에 대한 대응책으로, 내부망에 대한 무조건적인 신뢰를 폐기하고 엄격한 인증을 요구함

이 슈	주 요 내 용 및 시 사 점
	✓ 각 기관은 사용자 신원 확인, 기기 보안 상태 점검, 최소 권한 원칙 적용 등 제로 트러스트의 핵심 구성 요소를 이행해야 함 ✓ 특히 민감한 개인 정보를 취급하는 보건부, 재무부 등 주요 부처의 네트워크 가시성을 확보하고 비정상 행위 탐지 능력을 강화하는 데 주력함 ✓ 이번 조치는 파편화된 공공 보안 체계를 통합하고, 국가 차원의 일관된 보안 거버넌스를 구축하려는 전략적 움직임임 ✓ 연방 기관의 보안 인프라 현대화를 위해 기술 가이드라인을 배포하고, 정기적인 보안 심사를 통해 이행 수준을 점검할 계획임 ✓ 제로 트러스트 도입 의무화는 공공 조달 시장에서 해당 기술력을 보유한 보안 기업들에게 대규모 사업 기회를 제공할 것으로 전망됨 ✓ 정부는 본 조치를 통해 사이버 공격에 대한 회복 탄력성을 높이고, 국민들에게 안전한 디지털 행정 서비스를 제공하는 기반을 마련함 ✓ https://mexicobusiness.news/cybersecurity/news/mexico-mandates-zero-trust-across-federal-agencies
[브라질] 은행 대상 사이버 보안 요건 강화 및 규정 승인	▸ **브라질 중앙은행, 금융 시스템 안정성을 위해 은행권에 엄격한 보안 기준 적용 및 사고 보고 의무 강화(12월 10일)** ✓ 브라질 중앙은행(BCB)은 금융권의 사이버 사고가 잇따름에 따라 은행 및 금융 기관이 준수해야 할 새로운 사이버 보안 요건을 최종 승인함 ✓ 금융 기관은 사이버 보안 전략을 수립하고 이사회 차원의 승인을 받아야 하며, 전담 책임자(CISO) 임명이 의무화됨 ✓ 특히 즉시 결제 시스템인 Pix와 관련된 보안 사고를 방지하기 위해 실시간 사기 탐지 및 차단 시스템 구축이 강화됨 ✓ 제3자 서비스 제공업체(클라우드 등)에 대한 보안 관리 감독 책임을 은행에 부과하여 공급망 리스크를 엄격히 관리하게 함 ✓ 사고 발생 시 신속하게 중앙은행에 보고하고 고객에게 고지하는 절차를 표준화하여 투명성을 높임 ✓ 이번 규정은 브라질 금융 시스템의 신뢰도를 유지하고 대규모 금융 범죄로부터 국민의 자산을 보호하기 위한 필수적인 조치임 ✓ 금융 기관들은 규제 준수(Compliance)를 위해 보안 인프라 업그레이드와 관련 컨설팅에 대규모 투자를 단행할 것으로 예상됨 ✓ 강화된 보안 기준은 브라질 금융 보안 시장의 표준을 높이고 관련 솔루션의 수요를 촉진하는 역할을 할 것임
[베네수엘라] 석유 부문 사이버 공격 발생 및 배후 논란	▸ **베네수엘라 국영 석유 산업을 표적으로 한 대규모 사이버 공격 발생, 국가 기간 시설에 대한 보안 위협 심화(12월 10일)** ✓ 베네수엘라의 핵심 경제 동력인 석유 산업 인프라가 정교한 사이버 공격을 받아 운영에 차질을 빚는 사건이 발생함 ✓ 전문가들은 이번 공격이 단순히 금전적 목적을 넘어서 국가 기반 시설을 마비시키려는 정치적 의도가 다분한 '국가 배후 공격'의 특징을 보인다고 분석함 ✓ 특히 공격 방식이 과거 특정 국가가 수행했던 고도화된 작전 패턴과 유사하다는 주장이 제기되며 국제적인 논란이 일고 있음 ✓ 이번 사고로 인해 에너지 산업의 운영 기술(OT) 및 산업 제어 시스템(ICS) 보안의 취약성이 여실히 드러남 ✓ 베네수엘라 당국은 즉각적인 복구 작업에 착수하는 한편, 중요 인프라에 대한 보안 통제를 최고 수준으로 강화함 ✓ 물리적 피해로 이어질 수 있는 하이이브리드 위협에 대응하기 위해 사이버 방어 전략을 전면 재검토해야 한다는 목소리가 높음 ✓ **핵심 국가 자원을 보호하기 위한 폐쇄망 보안 기술과 외부 공격 차단 솔루션의** 중요성이 다시금 부각됨 ✓ 이번 사건은 지정학적 갈등이 사이버 공간으로 전이되어 국가 안보를 위협하는 현실을 보여주는 극명한 사례임

이 슈	주 요 내 용 및 시 사 점
	✓ https://caliber.az/en/post/politico-cyberattack-on-venezuela-s-oil-sector-bears-hallmarks-of-us-operation-experts-say
[페루] AI 기반 '디지털 방패' 구축으로 사이버 위협에 대응	▸ **페루, 급증하는 사이버 공격을 차단하기 위해 AI 및 머신러닝 기반의 국가적 보안 방어 체계 강화(12월 10일)** ✓ 페루는 라틴 아메리카 내 사이버 공격 빈도가 급격히 높아짐에 따라 AI 기술을 활용한 지능형 방어 시스템인 '디지털 방패' 구축에 박차를 가하고 있음 ✓ AI는 초 단위로 발생하는 수백만 건의 트래픽을 분석하여 기존 보안 시스템이 놓치기 쉬운 미세한 공격 징후를 탐지함 ✓ 특히 랜섬웨어와 피싱 공격이 정교해지는 상황에서 실시간 위협 차단 기능을 갖춘 AI 보안 솔루션이 핵심적인 역할을 수행 중임 ✓ 정부와 민간 기업들은 AI를 통해 사고 대응 속도를 높이고 수동적인 보안 운영의 한계를 극복하려 함 ✓ 페루 당국은 사이버 보안 강화를 위해 AI 전문 기술력을 보유한 해외 기업들과의 협력을 장려하고 있음 ✓ 지능형 위협에 대응하기 위해서는 데이터 기반의 자동화된 보안 관제(SOC) 환경 구축이 필수적임을 시사함 ✓ AI 기반 보안 인프라 확충은 페루의 디지털 경제 발전을 뒷받침하는 안전장치로서 기능할 것으로 기대됨 ✓ 교육 기관과 협력하여 AI 보안 전문가를 양성함으로써 기술적 자립도를 높이려는 시도도 병행되고 있음 ✓ https://www.itsitio.com/seguridad/el-nuevo-escudo-digital-en-peru-como-la-ia-hace-frente-al-auge-de-ciberataques/
[멕시코] 보안 투자 우선순위 설정을 둘러싼 리더십의 고민	▸ **멕시코 기업 및 기관 리더들, 제한된 예산 내에서 최적의 사이버 보안 투자 방향 설정에 어려움 토로(12월 12일)** ✓ 멕시코 내 많은 조직의 의사결정자들이 급격히 진화하는 사이버 위협에 비해 턱없이 부족한 보안 예산 배정 문제로 고심하고 있음 ✓ 랜섬웨어, AI 기반 공격 등 위협의 종류는 다양해지나, 어떤 분야에 우선적으로 투자해야 효과적인지 판단하기 위한 전문 지식이 부족한 실정임 ✓ 경영진은 사이버 보안을 단순 비용으로 인식하는 경향이 있어, 보안 담당자들이 투자 대비 효과(ROI)를 입증하는 데 큰 장벽을 느끼고 있음 ✓ 특히 중소기업(SMEs)은 전문 보안 인력 확보와 고가의 솔루션 도입 사이에서 전략적 선택의 기로에 서 있음 ✓ 전문가들은 리더십이 보안을 기술적 문제에서 비즈니스 연속성 및 리스크 관리의 핵심 영역으로 인식을 전환해야 한다고 강조함 ✓ 데이터의 중요도에 따른 차등적 보안 적용과 매니지드 보안 서비스(MSSP) 활용 등 현실적인 대안들이 논의되고 있음 ✓ 보안 투자 부족은 결국 사고 발생 시 더 큰 사회적, 경제적 손실로 이어지므로 국가 차원의 보안 투자 장려책이 필요함을 시사함 ✓ 리더들의 보안 인식 제고를 위한 교육과 컨설팅 수요가 증가하고 있으며, 이는 보안 시장의 체질 개선으로 이어질 수 있음 ✓ https://mexicobusiness.news/cybersecurity/news/mexican-leaders-struggle-prioritize-cybersecurity-investments
[칠레] 정부·금융·유통 분야에 사이버 공격 60% 이상 집중	▸ **칠레 내 전체 사이버 공격의 대다수가 민감한 데이터와 자금이 몰리는 특정 3대 핵심 산업 부문에 집중되고 있음(12월 15일)** ✓ 최근 통계에 따르면 칠레 내에서 발생하는 사이버 공격의 60% 이상이 정부 기관, 은행(금융), 소매(유통) 부문을 표적으로 함 ✓ 정부 부문은 정치적 목적이나 기밀 정보 탈취를 위해, 금융 및 유통 부문은 직접적인 금전적 이득을 노린 공격자들의 주요 표적이 됨 ✓ 특히 랜섬웨어 공격이 이들 산업의 비즈니스 연속성을 위협하며 막대한 복구 비용과 데이터 유출 피해를 야기하고 있음

이 슈	주 요 내 용 및 시 사 점
	✓ 공격자들은 피싱과 사회 공학 수법을 통해 내부 네트워크에 침투한 뒤 측면 이동을 통해 권한을 상급화하는 방식을 주로 사용함 ✓ 타겟 산업군에서는 보안 방어 체계 강화뿐만 아니라 공격을 당했을 때 빠르게 복구할 수 있는 '회복 탄력성(Resilience)' 확보가 최우선 과제가 됨 ✓ 특정 산업에 대한 공격 집중 현상은 해당 분야 기업들 간의 보안 정보 공유 커뮤니티(ISAC) 활성화 필요성을 제기함 ✓ 보안 기업들은 이러한 특정 산업별 맞춤형 보안 패키지와 사고 대응 서비스를 중심으로 시장 공략을 강화하고 있음 ✓ 국가 안보와 직결된 공공 서비스와 금융 인프라를 보호하기 위한 민관 합동 방어 체계 구축이 시급함을 시사함 ✓ https://portalinnova.cl/gobierno-banca-y-retail-concentran-mas-del-60-de-los-ciberataques-en-chile/
[멕시코] Llave MX 및 생체 인식 CURP 통합으로 디지털 신원 보안 강화	▸ **멕시코, 통합 인증 플랫폼 Llave MX와 생체 인식 CURP 연동을 통해 디지털 신원 도용 방지 체계 고도화(12월 15일)** ✓ 멕시코 정부는 디지털 행정 서비스의 관문인 'Llave MX' 플랫폼에 생체 인식 기반의 고유인구등록코드(CURP)를 전격 통합함 ✓ 이는 얼굴 인식, 지문 등 생체 정보를 활용하여 본인 확인 절차를 강화함으로써 명의 도용 및 사이버 사기를 원천 차단하기 위한 조치임 ✓ 시민들은 단일 디지털 신원을 통해 다양한 정부 서비스를 안전하게 이용할 수 있게 되며, 행정 절차의 편의성도 크게 향상됨 ✓ 데이터베이스의 중앙 집중화에 따른 보안 위험을 방지하기 위해 종단 간 암호화(E2EE)와 하드웨어 보안 모듈(HSM) 등 첨단 보안 기술이 적용됨 ✓ 멕시코 디지털 혁신청은 이번 통합이 민간 부문의 금융 거래 및 본인 인증 서비스와도 연계될 수 있도록 확장을 추진 중임 ✓ 생체 인식 데이터의 안전한 관리와 프라이버시 보호를 위한 법적 근거를 마련하고, 데이터 접근 권한을 엄격히 제한하고 있음 ✓ 이번 이니셔티브는 멕시코의 국가 디지털 신원 체계를 세계적 수준으로 격상시키고, 디지털 경제 활성화를 위한 '신뢰 인프라'를 구축하는 핵심 사업임 ✓ 대규모 생체 정보 처리 및 보호 기술에 대한 수요가 급증함에 따라 관련 보안 시장의 활성화가 기대됨 ✓ https://mexicobusiness.news/cybersecurity/news/mexico-boosts-digital-id-security-llave-mx-curp-integration
[베네수엘라] 사이버 보안, 비즈니스 성공의 전략적 기둥으로 부상	▸ **베네수엘라 기업 경영진, 디지털 전환 시대의 지속 가능한 성장을 위해 사이버 보안을 필수 경영 전략으로 채택(12월 15일)** ✓ 베네수엘라의 비즈니스 리더들 사이에서 사이버 보안이 단순한 기술적 보조 도구를 넘어 비즈니스 성공을 결정짓는 핵심 전략으로 인식되고 있음 ✓ 잦은 데이터 유출과 사이버 공격으로 인한 평판 손실이 기업 생존에 직결된다는 위기의식이 반영된 결과임 ✓ 성공적인 디지털 기업들은 초기 설계 단계부터 보안을 고려하는 '시큐리티 바이 디자인(Security by Design)' 원칙을 도입하고 있음 ✓ 경영진의 직접적인 관여와 보안 예산의 전략적 배정이 기업 경쟁력을 높이는 요소로 강조되고 있음 ✓ 특히 원격 근무와 클라우드 전환이 가속화됨에 따라 분산된 네트워크 환경을 보호하기 위한 신규 투자가 늘고 있음 ✓ 직원 대상의 정기적인 보안 인식 교육이 기술적 솔루션만큼이나 중요하다는 공감대가 형성됨 ✓ 사이버 보안은 이제 규제 준수를 위한 의무를 넘어, 고객에게 신뢰를 제공하는 마케팅 가치로 활용되고 있음 ✓ 베네수엘라 기업들은 보안 강화를 통해 글로벌 시장에서의 신뢰도를 회복하고 안정적인 비즈니스 생태계를 구축하려 노력함

이 슈	주 요 내 용 및 시 사 점
	✓ https://www.eluniversal.com/tecnologia/222113/la-ciberseguridad-eje-estrategico-del-exito-empresarial#google_vignette
[멕시코] 유통 및 서비스 업계, 보안 강화를 위한 AI 도입 가속화	▸ **멕시코의 소매 및 호텔·관광업계, 사기 탐지 및 고객 데이터 보호를 위해 인공지능(AI) 기반 보안 솔루션 채택 확대(12월 18일)** ✓ 멕시코의 주요 유통 및 서비스 기업들이 연말 성수기를 앞두고 급증하는 사이버 공격에 대비해 AI 기반 보안 시스템을 적극 도입하고 있음 ✓ AI는 대량의 결제 데이터를 실시간으로 분석하여 카드 도용 및 이상 거래(FDS)를 신속하게 탐지하는 데 탁월한 성능을 보임 ✓ 호텔 및 관광업계는 고객의 민감한 예약 정보와 결제 데이터를 보호하기 위해 머신러닝 기반의 침입 탐지 시스템을 강화하고 있음 ✓ 특히 챗봇 및 고객 응대 시스템을 통한 피싱 공격을 방지하기 위해 자연어 처리(NLP) 기술을 활용한 보안 필터링을 적용함 ✓ AI 도입을 통해 보안 운영의 자동화를 실현하고, 인력 부족 문제를 해결하면서도 보안 수준을 균일하게 유지하는 효과를 거두고 있음 ✓ 멕시코 기업들은 AI를 단순한 업무 도구가 아닌, 지능화된 사이버 범죄에 맞서기 위한 '디지털 방패'로 인식하기 시작함 ✓ 소매업계의 공급망 보안 강화를 위해 협력사와의 데이터 교환 과정에도 AI 기반의 위협 분석 기술이 도입되고 있음 ✓ 이러한 추세는 멕시코 내에서 실전 중심의 AI 보안 솔루션 시장 성장을 견인할 것으로 보임 ✓ https://mexicobusiness.news/cybersecurity/news/mexicos-retail-hospitality-sectors-adopt-ai-enhance-security
[페루] 연말연시 대목을 겨냥한 AI 기반 보안 모니터링의 중요성	▸ **크리스마스와 신년 휴가기간 동안 급증하는 사이버 사기를 막기 위해 AI 기반의 실시간 모니터링 기술이 핵심으로 부상(12월 24일)** ✓ 페루 당국과 금융업계는 연말 쇼핑 시즌과 휴가 기간을 틈탄 피싱 및 결제 사기에 대비해 보안 경계 태세를 강화함 ✓ 사이버 범죄자들이 가짜 할인 정보나 선물 이벤트로 위장하여 고객 정보를 탈취하는 사례가 빈발함에 따라 AI를 활용한 선제적 대응이 강조됨 ✓ AI 기반 모니터링 시스템은 사용자의 평소 거래 패턴에서 벗어난 의심스러운 활동을 즉각 감지하여 승인을 차단하는 등의 조치를 수행함 ✓ 유통업계는 온라인 쇼핑몰의 가용성을 유지하고 대규모 접속을 악용한 분산 서비스 거부(DDoS) 공격에 대비해 지능형 트래픽 관리 솔루션을 가동함 ✓ 소비자들에게는 연말 분위기에 편승한 의심스러운 링크 클릭 자제와 다중 인증 활성화 등 기본적인 보안 수칙 준수를 당부함 ✓ 이번 기간 동안의 AI 보안 운영 성과는 향후 페루 내 AI 보안 기술의 대중화와 신뢰 형성에 중요한 지표가 될 것임 ✓ 계절적 위협에 특화된 위협 인텔리전스 공유가 사고 예방에 결정적인 기여를 하고 있음 ✓ 보안 기업들은 시즌별 특화된 모니터링 서비스를 제공하며 시장 점유율 확대를 꾀하고 있음 ✓ https://www.apnoticias.pe/peru/andina/monitoreo-con-inteligencia-artificial-es-clave-para-ciberseguridad-en-navidad-y-ano-nuevo-1479446
	▸ **시사점 및 국내 보안 기업 진출 포인트** ✓ 중남미 권역의 사이버 보안 법제화 및 국가 거버넌스 체계 정립 가속화 - 칠레의 '사이버 보안 프레임워크 법' 시행과 멕시코의 '국가 사이버 보안 계획' 발표는 중남미 보안 시장이 체계적인 규제 환경으로 진입하고 있음을 의미 - 브라질의 은행권 보안 요건 강화 등 특정 산업별 규제가 구체화됨에 따라, 우리 기업은 현지 규제 준수를 결합한 통합 보안 컨설팅 및 솔루션 패키지로 시장

이 슈	주 요 내 용 및 시 사 점
	진입 전략을 수립해야 함 ✓ '제로 트러스트' 및 '디지털 신원(IAM)' 기반의 신뢰 인프라 수요 급증 - 멕시코의 연방 기관 대상 제로 트러스트 도입 의무화와 생체 인식 CURP 연동은 단순 경계 보안을 넘어선 지능형 접근 제어와 신원 확인 기술에 대한 시장을 창출하고 있음 - 가상자산 탈취 등 막대한 경제적 피해에 대응하기 위해 국내의 앞선 생체 인증, FDS, IAM 기술을 공공 행정 및 금융 신뢰 구축 프로젝트와 연계하여 최우선 투자 영역으로 공략할 필요가 있음 ✓ AI 기반의 지능형 위협 탐지 및 실시간 모니터링 시장 확대 - 페루의 '디지털 방패'와 멕시코 유통·서비스 업계의 AI 도입은 고도화된 공격에 대응하기 위한 AI/ML 기반 보안 솔루션이 시장의 필수 요구 사항이 되었음을 보여줌 - 특히 연말연시 등 특정 시즌의 위협 모니터링과 자동화된 사고 대응(SOAR) 기술을 통해 현지의 보안 운영 효율화 수요를 충족시키는 진출 포인트가 유망 ✓ 국가 핵심 인프라(OT/ICS) 보호를 위한 전략적 파트너십 기회 - 베네수엘라 석유 산업 공격 등 핵심 국가 자산에 대한 위협은 OT/ICS 보안의 중요성을 극대화시키고 있으며, 이는 멕시코와 칠레의 인프라 보호 계획과도 맞닿아 있음 - 한국의 강점인 물리 보안과 사이버 보안이 결합된 하이브리드 방어 기술을 국가 핵심 인프라 보호 프로젝트의 전략적 파트너로서 제안할 기회가 확대되고 있음 ✓ 인력 부족 해결을 위한 매니지드 보안 서비스(MSSP) 및 교육 수출 - 멕시코와 페루의 리더들이 공통적으로 지적하는 전문 인력 부족과 예산 한계 문제는 외부 전문 보안 관리 서비스(MSSP) 시장의 성장을 견인하고 있음 - 국내 보안 관제 운영 노하우를 바탕으로 한 원격 관제 서비스와 현지 전문가 양성을 위한 교육 프로그램을 연계하여 서비스형 보안(SaaS) 형태의 진출 모델 개발이 필요

KISA 정보보호 해외진출 전략거점(중동아프리카) 12월 주요동향

2025. 12. 31(수), 한국인터넷진흥원 보안산업단 글로벌협력팀

[해외 언론]

이 슈	주 요 내 용 및 시 사 점
[중동] 해킹공격 확대	▸ **MEA 해커 활동 증가 – 정부·금융·리테일 타깃** ✓ 사이버보안 매체 Dark Reading 분석에 따르면, 중동·아프리카(MEA) 지역에서의 해킹 공격은 정부기관, 금융기업, 소규모 리테일 업계로 확대되고 있다. 공격 유형은 랜섬웨어, 데이터 절취, 서비스 방해(DDoS) 등이며, 특히 공공 서비스와 금융 서비스에 대한 지속적 침해 시도 증가가 두드러진다. 이는 디지털 전환 속도가 빠르지만 보안 인프라가 따라가지 못하는 현실과 맞물려 발생한다는 평가다. ✓ MEA 지역의 사이버 위협은 단순한 해킹을 넘어서 금융·공공 서비스의 안정성에 직접 영향을 미칠 정도로 확대되고 있다. ✓ 출처: Dark Reading ✓ https://www.darkreading.com/cybersecurity-analytics/mea-hackers-govts-finance-smb-retailers
[사우디, UAE] 사이버보안 교육 확대	▸ **UAE·사우디 등 MEA 지역 INE Security 사이버보안 교육 확대** ✓ 글로벌 사이버보안 교육업체 INE Security가 2025년 중동 및 아시아 시장 확장 계획을 발표하면서, 사우디·UAE·이집트 시장을 중심으로 사이버보안 인력 역량 강화에 집중하고 있다고 밝혔다. 이 확장은 지역 디지털 전환, AI 도입 증가, 원격 근무의 확대로 인해 보안 인력 수요가 급증하기 때문이다. 회사는 구체적으로 사이버보안 핵심 기술 트레이닝, 실습형 과정, 취약점 분석 및 응답 준비 과정 등을 제공하며, 관계국의 대학·정부기관과 협업해 공인 자격증 취득 경로, 실전 대응 훈련 플랫폼을 지원할 계획이다. ✓ MEA 지역에서 보안 인력 부재는 지속적 문제였는데, 교육 확장은 국가 사이버 인프라 보강 + 취약점 대응 능력 강화를 위해 필수적인 전진이다. ✓ 출처: CyberNewsWire ✓ https://hackread.com/ine-security-expands-across-middle-east-and-asia-to-accelerate-cybersecurity-upskilling/
[사우디, UAE] 산업용 사이버보안 강화	▸ **KPMG·Dragos 파트너십 – 산업용 사이버보안 강화** ✓ KPMG가 산업 사이버보안 전문기업 Dragos와 공식 파트너십을 체결하면서, 중동 제조·에너지·인프라 산업에 특화된 보안 솔루션을 제공하기로 했다. 이는 특히 SCADA·OT 시스템 보호가 중요한 석유·가스 설비에서 방어 능력을 강화하기 위한 조치다. 양사는 위협 사전 탐지, 공격 시나리오 대응, 보안 운영센터(SOC) 운영 최적화 등 종합 보안 프레임워크를 구축할 예정이다. ✓ 산업 환경의 공격은 전통 IT 영역보다 피해 규모가 크기 때문에, 이러한 협력은 국가 중요 인프라 보호와 관련해 중요한 전환점으로 평가된다. ✓ 출처: Consultancy-ME ✓ https://www.consultancy-me.com/news/12388/kpmg-deepens-industrial-cybersecurity-capabilities-with-dragos-partnership
[사우디, UAE] 휴대폰 타깃 사이버 공격	▸ **글로벌 휴대폰 타깃 사이버 경고 – UAE·이집트 등 포함** ✓ 2025년 12월, Google 및 Apple은 전 세계 150여개국에서 사용자 휴대폰을 대상으로 한 심각한 사이버 공격 경고를 발령했다. 해당 캠페인은 스파이웨어·피싱 링크·악성 앱 설치를 유도하며, 사용자 계정 탈취, 금융 데이터 노출 위험을 내포한다. MEA에서 영향권에 있는 국가로 사우디·UAE·이집트 등이 명시됐다. 취약성

이 슈	주 요 내 용 및 시 사 점
	대응을 위해 OS 업데이트, 앱 설치 제한, 2단계 인증 사용 등이 권고되었다. ✓ 모바일 기기는 네트워크 경계 밖에서도 공격을 받기 때문에, 사용자 수준의 보안 지침 확산이 필수적임을 보여준다. ✓ 출처: Middle East Monitor ✓ https://www.middleeastmonitor.com/20251208-global-warning-over-cyber-attacks-targeting-users-phones-in-over-150-countries/
[사우디] Black Hat Mea 2025 개최	▸ **Black Hat MEA 2025 – 리야드 최대 사이버보안 행사** ✓ Black Hat Middle East & Africa 2025가 사우디 리야드에서 개최되며, 전 세계 보안 전문가·연구자·기업 리더들이 모였다. 행사에서는 AI 기반 공격 대응, 제로트러스트 네트워크, 클라우드 보안 보호 전략 등의 주제가 핵심으로 다뤄졌다. 특히 OT·산업용 보안, 사이버 인텔리전스 공유 프레임워크, 기술 혁신과 표준화가 강조됐다. 다양한 워크샵, 데모 세션이 병행되며 지역 보안 성숙도를 한 단계 끌어올리는 계기가 되었다. ✓ 지역 최대 보안 컨퍼런스로서, MEA 전체의 사이버 전략 논의 및 글로벌 협력 촉진 역할을 하고 있다. ✓ 출처: BusinessWire ✓ https://www.businesswire.com/news/home/20251204774207/en/Resecurity-Drives-Cybersecurity-Innovation-at-Black-Hat-MEA-2025-in-Riyadh-as-a-Gold-Sponsor
[사우디] AI 보안 도입 증가	▸ **사우디 기업의 AI 기반 보안 인식 및 도입 증가** ✓ 사우디 기업들의 사이버보안 인식 조사에서 60% 이상이 AI 기반 사이버 위협을 높은 수준으로 인식하고 있으며, 절반 이상은 AI 기술을 실제 보안 운영에 적용하고 있다는 결과가 나왔다. 조사에 따르면, AI 탐지·자동화 대응 시스템은 위협 식별과 복구 속도를 크게 향상시킨다. 또한 향후 91% 기업이 AI 에이전트 도입을 계획 중이며, 40%가 AI와 인간 전문가가 협업하는 보안 운영을 도입할 것이라고 응답했다. ✓ 사우디는 Vision 2030 전략의 일환으로 디지털 혁신 + AI 통합 보안에 집중하면서, 공격과 방어 양면에서 기술 주도권 확보를 모색하고 있다. ✓ 출처: Arab News ✓ https://www.arabnews.com/node/2623860/%7B%7B?utm_source=chatgpt.com
[UAE] 사이버보안 인재 내 민간 확대	▸ **UAE 사이버보안 인재 5,000명 민간 부문 확대** ✓ UAE는 사이버보안과 AI 분야에서 약 5,000명 Emirati 전문가가 민간 부문 보안 역할에 참여한다고 발표했다. 이는 국가 디지털 전략의 핵심 요소로, 매일 약 200,000건 사이버 공격을 분석·차단하는 현황에서 인력 확충의 필요성이 대두됐기 때문이다. 관련 교육 프로그램과 직무 전환 지원 등이 동시에 진행돼 국가 전체의 디지털 보안 탄력성 강화에 기여할 것으로 기대된다. ✓ 출처: Gulf News ✓ https://gulfnews.com/uae/uae-cybersecurity-boost-5000-emiratis-join-private-sector-to-combat-threats-1.500386069

이 슈	주 요 내 용 및 시 사 점
[UAE] 구글 클라우드 협력	▸ **UAE 사이버보안 센터 오브 엑설런스 및 Google 협력** ✓ UAE는 Google Cloud와 협력해 Cyber Security Centre of Excellence를 출범했다. 이 센터는 20,000개 이상의 사이버보안 직무 창출, 외국인 투자 유치, AI 기반 위협 대응 및 인재 양성을 목표로 한다. 또한 구글의 Cyber Security Academy를 통해 고급 기술 훈련과 최신 보안 솔루션 연구가 병행되어 UAE를 글로벌 보안 허브로 육성한다는 전략이다. ✓ 출처: The National News ✓ https://www.thenationalnews.com/news/uae/2025/04/09/uae-launches-cyber-security-centre-of-excellence-as-part-of-google-collaboration/
[카타르] 사이버 보안 역량 강화 선언	▸ **카타르, 국가 사이버보안 역량 고도화 및 국제 협력 강화** ✓ 카타르는 2025년 말 국제무대에서 사이버보안을 국가 디지털 경쟁력의 핵심 요소로 재확인했다. 외교부(MOFA)는 UN 및 다자 포럼에서 디지털 전환이 경제 성장과 혁신을 촉진하는 동시에 사이버 공격, 데이터 침해, 국가 간 디지털 격차라는 위험을 동반한다고 지적했다. 카타르는 국가 CERT 역량 강화, 공공·민간 협력 확대, 국제 정보 공유 체계 구축을 주요 전략으로 제시했다. 특히 개발도상국과의 협력 확대를 통해 사이버 역량 불균형이 글로벌 불안정 요인으로 작용하지 않도록 조정하겠다는 입장을 밝혔다. ✓ 출처: Qatar Ministry of Foreign Affairs ✓ https://mofa.gov.qa/en/qatar/latest-articles/latest-news/details/2025/10/28/qatar-stresses-importance-of-strengthening-cybersecurity--expanding-cooperation-between-developed-and-developing-countries
[카타르] 사이버보안 교육 체계 우수	▸ **카타르 사이버보안 교육 체계, 글로벌 모범 사례로 부상** ✓ 카타르는 2025년 사이버보안 교육 프로그램이 국제적으로 높은 평가를 받았다고 발표했다. 해당 커리큘럼은 초·중등부터 대학 및 전문 교육까지 전 주기를 포괄하며, 58만 명 이상이 참여했다. 실습 중심 교육, 사이버 위기 대응 시뮬레이션, 윤리적 해킹 교육 등이 포함되며, 국제 대회 수상으로 교육 품질을 입증했다. 이는 단기적 기술 인력 양성을 넘어 장기적 국가 사이버 회복탄력성(resilience) 구축을 목표로 한다. ✓ 출처: The Peninsula Qatar ✓ https://thepeninsulaqatar.com/article/17/07/2025/qatars-cybersecurity-curriculum-expands-earns-global-acclaim

[국내 언론]

이 슈	주 요 내 용 및 시 사 점
[사우디] 지니언스, 블랙햇 참가	▸ **지니언스, Black Hat MEA 2025 공식 부스 참가로 MEA 시장 진출 강화** ✓ 사이버보안 전문기업 지니언스(Genians)가 2025년 12월 2~4일 사우디 리야드에서 개최된 Black Hat MEA 2025에 공식 참가했다. 이 행사에서 지니언스는 NAC(네트워크 접근제어), 지니안 인사이트 E(EDR), ZTNA 등 3대 핵심 보안 솔루션을 선보였다. 부스에는 사우디 주요 시스템 통합(SI) 기업과 파키스탄 금융권 관계자 등 다수의 잠재 고객이 방문해 비즈니스 상담 약 30건을 진행했다. 이를 통해 지니언스는 중동?아프리카 시장에서 실질적 사업 확대의 기반을 마련했다. ✓ 지니언스는 한?중동 디지털 협력 전략(예: SHINE 이니셔티브) 및 사우디 비전 2030과 연계해 전시 활동을 전개했으며, 향후 현지 파트너 협력 강화, 주요 아프리카 국가 고객 확보 등을 목표로 하고 있다. ✓ 출처: 보안뉴스 ✓ https://m.boannews.com/html/detail.html?idx=140792
[UAE] 국가 사이버보안 전략 발표	▸ **UAE 국가 사이버보안 전략 2025-2031 발표** ✓ 2025년 12월 UAE가 국가 사이버보안 전략 2025?2031을 공식 발표했다. 이 전략은 UAE 정부가 디지털 경제를 보호하고 미래 위협에 대응하기 위해 마련한 것으로, 인공지능(AI) 기반 방어체계 구축, 데이터 프라이버시 보호, 사이버 인력 양성, 국제 정보 공유 체계 강화 등을 핵심 축으로 한다. 전략은 6년간 단계적 이행 계획을 포함하며, 공공·민간간 협력 강화, 클라우드 및 IoT 보안 표준 확립, 핵심 인프라 보호를 위한 기술·법제 개선 등을 강조한다. UAE는 이를 통해 금융, 에너지, 통신 등 주요 산업의 디지털 회복탄력성을 높이고, 국제적 사이버보안 협력 체계의 중심 역할을 수행할 계획이다. ✓ 출처: KOTRA UAE 사이버보안 전략 자료 ✓ https://www.kotra.or.kr/kodits/download/BASIC_ATTACH?storageNo=3998

[중점 키워드 및 시사점]

키워드	주요내용 및 시사점
MEA 해커 활동 증가	o Dark Reading 분석에 따르면, MEA 지역 해킹 공격이 정부기관, 금융기업, 소규모 리테일까지 확대되고 있으며, 랜섬웨어·데이터 절취·DDoS 공격이 빈번. 디지털 전환 속도가 빠른데 비해 보안 인프라가 부족하여 금융·공공 서비스 안정성에 직접 영향을 미침.
INE Security 교육 확대	o INE Security가 사우디·UAE·이집트 중심으로 사이버보안 인력 역량 강화를 위한 핵심 기술 트레이닝, 실습, 취약점 분석·응답 과정 제공. 보안 인력 부족 문제를 해소하고 국가 사이버 인프라 보강 및 취약점 대응 능력을 강화할 것으로 기대.
KPMG·Dragos 파트너십	o KPMG와 Dragos 파트너십으로 중동 제조·에너지·인프라 산업 SCADA·OT 시스템 보호 강화. 위협 탐지, 대응 시나리오, SOC 운영 최적화 등 종합 보안 프레임워크 구축. 산업 환경 공격 피해가 큰 만큼 국가 중요 인프라 보호의 전환점으로 평가.
글로벌 휴대폰 공격	o Google·Apple, 150개국 모바일 기기 대상 스파이웨어·피싱·악성 앱 공격 경고. OS 업데이트, 앱 설치 제한, 2단계 인증 권고. 모바일 기기는 네트워크 경계 밖에서도 공격 가능하므로 사용자 수준 보안 지침 확산이 필수.
Black Hat MEA 2025	o 리야드 개최 Black Hat MEA 2025에서 AI 공격 대응, 제로트러스트, 클라우드·OT 보안 전략 등 논의. 워크샵과 데모 세션을 통해 지역 보안 성숙도를 끌어올리고 글로벌 협력을 촉진하는 역할 수행.
사우디 AI 보안 도입	o 사우디 기업 60% 이상 AI 기반 사이버 위협 인식, 절반 이상 AI 기술 적용. 향후 91%가 AI 에이전트 도입, 40% AI-인간 협업 운영 계획. Vision 2030 전략과 연계해 디지털 혁신과 AI 기반 보안 기술 주도권 확보를 모색.
UAE 사이버보안 인재 확대	o UAE, 약 5,000명 Emirati 전문가 민간 부문 참여. 매일 20만 건 공격 분석·차단. 교육·직무 전환 지원 병행, 국가 디지털 전략 핵심 요소로 디지털 보안 탄력성 강화 및 전문 인력 확보에 기여.
UAE 센터 오브 엑셀런스	o UAE와 Google 협력 Cyber Security Centre of Excellence 출범. 20,000개 이상 직무 창출, AI 기반 위협 대응, 인재 양성. 민간·교육 연계 전문 인력 양성 기반 강화, UAE 글로벌 보안 허브 육성 전략.
카타르 사이버보안 역량	o 카타르, 국가 CERT 강화, 공공·민간 협력 확대, 국제 정보 공유 체계 구축. 개발도상국과 협력으로 글로벌 사이버 불균형 완화. 국가 디지털 경쟁력 확보 및 사이버 회복탄력성 향상.
카타르 사이버 교육	o 카타르 사이버보안 교육 프로그램, 초·중등~대학 전주기, 58만명 참여. 실습 중심, 위기 대응 시뮬레이션, 윤리적 해킹 포함. 단기 기술 인력 양성을 넘어 장기 국가 사이버 회복탄력성 구축 목표.