1. 보안동향

[신간] ‘AI 2025 활용 백과 with 샘 알트만’ 출간

[미리보기]

AI 기술이 사회 전반에 미치는 영향과 가능성에 대해 심도 있게 탐구 AI 기술의 윤리적 문제, 사회적 책임 논의 포괄해 AI 기술 혜택과 위험 분석[보안뉴스 김경애 기자] 한국 AI 교육협회 부회장 겸, 챗 GPT 인공지능지도사협회 수석부회장과 골프먼스리 발행인 조성수 대표가 ‘AI 2025 활용 백과 with 샘 알트만’을 12 일 출간했다. 이 책은 인공지능(A

바로가기

전 세계 표준으로 자리잡는 클라우드 네이티브 환경, 보안은 어떻게?

[미리보기]

공공부문, 시스템 100%를 클라우드 네이티브 환경으로 전환 목표로 이행중아스트론시큐리티, CSPM+CIEM+CWPP=CNAPP 로 공공 클라우드 보안 강화 약속[보안뉴스 원병철 기자] 클라우드 네이티브 환경이 전 세계 표준으로 자리 잡고 있다. 특히 공공부문에서 시스템의 100%를 클라우드 네이티브 환경으로 전환한다는 목표를 세우고 이행하고 있다. 문제는

바로가기

진화하는 RaaS 에 대한 대응은 스토리지 자체의 보안 강화

[미리보기]

스톤플라이, 진화하는 랜섬웨어 공격에 대한 대안으로 스토리지 보안 기능 강화 제안최성재 지사장, ISEC 2024 첫째날 강연에서 '서비스형 랜섬웨어와 방어기법' 강연[보안뉴스 원병철 기자] 최근 등장한 RaaS(Ransomware as a Service)는 자동화된 랜섬웨어 서비스로 고객지원과 업데이트를 지원하기 때문에 누구나 손쉽게 랜섬웨어 공격을 할

바로가기

2024 전국 공무원 정보보안 콘퍼런스, 성황리 개최

[미리보기]

3 개 세션으로 서울시 사이버 보안 및 AI 보안과 정책 등 소개전국 광역·기초자치단체의 보안책임자 협의회 구성 위한 논의도 진행[보안뉴스 조재호 기자] 대한민국 공무원의 사이버보안 역량 강화를 위한 행사가 지난 10 월 16 일부터 17 일까지 서울 강남구 코엑스에서 열린 'ISEC 2024'에서 동시개최 행사로 열렸다. '2024 전국 공무원 정보보안 콘퍼런스

바로가기

아시아 최대 규모 보안 콘퍼런스 ISEC 2024 'Future-proof' 주제로 성황리 개막!

[미리보기]

서울 코엑스 Hall D, 오디토리움에서 10 월 16~17 일 동시 개최보안이 우리의 미래를 담보한다는 의미의 'Future-proof' 주제로 열려총 198 개 기관 및 기업 참여, 18 개 트랙 92 개 세션, 145 개 전시부스 규모 제 11 회 CISO 역량강화 워크숍, 2024 년 제 3 차 CPO 워크숍 등 동시 개최[보안뉴스 엄호식 기자] 대한민국을 대표하는 사

바로가기

---

2. 보안권고문

美 CISA 발표 주요 Exploit 정보공유(Update. 2024-10-15)

[미리보기]

2024-11-05 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Microsoft Windows Kernel contains a time-of-check to time-of-use (TOCTOU) race condition vulnerability that could allow for privilege escalation. 2024-10-15 Microsoft Windows Kernel TOCTOU Race Condition Vulnerability Microsoft CVE-2024-30088 2024-11-05 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. Mozilla Firefox and Firefox ESR contain a use-after-free vulnerability in Animation timelines that allows for code execution in the content process. 2024-10-15 Mozilla Firefox Use-After-Free Vulnerability Mozilla CVE-2024-9680 2024-11-05 Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable. SolarWinds Web Help Desk contains a hardcoded credential vulnerability that could allow a remote, unauthenticated user to access internal functionality and modify data. 2024-10-15 SolarWinds Web Help Desk Hardcoded Credential Vulnerability SolarWinds CVE-2024-28987

바로가기

Eyeon Security
information security company

주소 | 서울특별시 서초구 서초대로 255 고덕빌딩 2 층(06595)
전화 | 02-2105-4400 (영업문의-1 번, 보안관제문의-2 번, 기술문의-3 번) 팩스 | 02-2105-4456
영업문의 | sales@eosec.co.kr 보안관제 및 기술 문의 | tech@eosec.co.kr