AI Agents Navigate Unfamiliar OT Systems and Move Equipment in Minutes, Booz Allen Finds

In Booz Allen’s isolated OT lab, AI models met every objective across eight scenarios and reached an industrial control network from a perimeter compromise in just over 16 minutes.

The post AI Agents Navigate Unfamiliar OT Systems and Move Equipment in Minutes, Booz Allen Finds appeared first on SecurityWeek.

https://www.securityweek.com/ai-agents-navigate-unfamiliar-ot-systems-and-move-equipment-in-minutes-booz-allen-finds/

ICS Patch Tuesday: Siemens Issues 17 Advisories, Rockwell Fixes ArmorBlock Takeover Flaw

ABB previously published an advisory warning about possible probing of a dynovaPRO vulnerability.

The post ICS Patch Tuesday: Siemens Issues 17 Advisories, Rockwell Fixes ArmorBlock Takeover Flaw appeared first on SecurityWeek.

https://www.securityweek.com/ics-patch-tuesday-siemens-issues-17-advisories-rockwell-fixes-armorblock-takeover-flaw/

Harmonic Security Raises $50 Million for Workforce AI Protection

The cybersecurity startup plans to expand engineering and go-to-market teams in the US and UK.

The post Harmonic Security Raises $50 Million for Workforce AI Protection appeared first on SecurityWeek.

https://www.securityweek.com/harmonic-security-raises-50-million-for-workforce-ai-protection/

Microsoft Disrupts Chinese-Language Phishing Market Behind 1B+ Messages

Backed by a federal court order, Microsoft and Health-ISAC seized domains powering YAM Store, CoGUI, and Iron Man.

The post Microsoft Disrupts Chinese-Language Phishing Market Behind 1B+ Messages appeared first on SecurityWeek.

https://www.securityweek.com/microsoft-disrupts-chinese-language-phishing-market-behind-1b-messages/

US Arrests Two in Crackdown on North Korean IT Worker Laptop Farms

Investigators stormed 40 locations in Texas and seized 187 laptops used by North Korean IT workers to hide their location.

The post US Arrests Two in Crackdown on North Korean IT Worker Laptop Farms appeared first on SecurityWeek.

https://www.securityweek.com/us-arrests-two-in-crackdown-on-north-korean-it-worker-laptop-farms/

Sicurezza dell’AI, 400 ricercatori da tutto il mondo chiedono sandbox più robuste e trasparenza sugli incidenti

Intelligenza artificiale e sicurezza, la lettera aperta di 415

ricercatori: “Servono più ricerca e contenimenti robusti”

Le falle nei sistemi di contenimento dell’intelligenza artificiale (AI) possono essere lette in due modi: come un segnale dei limiti dell’allineamento dei modelli oppure come il risultato di pratiche di sicurezza informatica insufficienti. **La lettera** aperta firmata da **415 ricercatori e accademici** non sceglie una sola spiegazione. Indica entrambe come dimensioni del problema e sostiene che per ridurre i rischi servano sia modelli dal comportamento più prevedibile sia ambienti di test e procedure più rigorosi.

Tra i firmatari ci sono alcuni nomi di spicco, a livello internazionale come **Yoshua Bengio** (Université de Montréal), **Stuart J. Russell** (Università della California, Berkeley), **Yejin Choi** (Università di Stanford), **Toby Walsh** (UNSW Sydney), **Michael Wooldridge** (Università di Oxford), **Ron Deibert** (Citizen Lab, Università di Toronto).
Nel documento risultano, inoltre, **11 firmatari italiani**, tra cui **Giorgio Giacinto** (Università di Cagliari), **Stefano Zanero** (Politecnico di Milano), **Battista Biggio**, (Università di Cagliari), **Fabio Roli**, (Università di Genova).

Il documento parte da un punto preciso: **alcuni modelli di AI avrebbero aggirato ambienti di test non adeguatamente protetti, compromettendo sistemi appartenenti a organizzazioni esterne**. La lettera non descrive i singoli episodi, ma ne ricava una preoccupazione più ampia: se le pratiche di sviluppo e implementazione non cambiano, incidenti simili potrebbero ripetersi e produrre conseguenze più gravi per infrastrutture critiche esposte.

Allineamento e sicurezza

informatica, due fronti complementari

Per i firmatari, **l’allineamento dell’AI è rilevante perché mira a far sì che i modelli agiscano in modo prevedibile**. La possibilità, però, che un modello superi i confini di un ambiente di test non può essere affrontata solo intervenendo sul suo comportamento. La lettera richiama anche la responsabilità delle organizzazioni: **sistemi di contenimento poco solidi e procedure inadeguate possono esporre reti e sistemi esterni**.

Il nodo è particolarmente delicato per i modelli dotati di capacità informatiche e connessi a Internet. Secondo i ricercatori, la quantità di azioni consentite all’interno di una **sandbox** deve essere commisurata alla capacità, ancora limitata, di prevedere se le azioni del modello possano causare un fallimento della sicurezza, per esempio in presenza di obiettivi non allineati. Più ampio è l’accesso concesso al modello, maggiore diventa l’importanza di controllare ciò che può fare e di valutare i rischi associati.

La prima raccomandazione: isolamento (*airgapping*) e contenimento ad alta affidabilità

La proposta più immediata riguarda le organizzazioni che sviluppano, testano o implementano modelli di AI con capacità informatiche. La lettera chiede loro di **adottare subito sistemi di contenimento ad alta affidabilità** e di procedere con cautela. Nella fase iniziale, la misura indicata è l’isolamento fisico dei modelli, tramite ***airgapping***, cioè la disconnessione da Internet.

La raccomandazione riflette un principio prudenziale: finché

non è possibile prevedere con sufficiente affidabilità il comportamento del modello, è necessario limitarne l'accesso all'esterno. **L'airgapping viene presentato come una misura iniziale di sicurezza**, non come l'unico possibile assetto per ogni sistema.
Il documento invita infatti a sviluppare e standardizzare approcci di allineamento e contenimento che possano consentire, in condizioni adeguate, un accesso più ampio fuori dalla sandbox.

Un organismo internazionale per standard e incidenti

Per affrontare questa sfida, i firmatari propongono di istituire un organismo internazionale, in consultazione con i governi e con esperti di AI e cybersicurezza. Il suo compito sarebbe definire, nell'interesse pubblico, le migliori pratiche per l'allineamento e il contenimento dei modelli, comprese le soluzioni che permettono una maggiore connettività rispetto all'isolamento fisico.

All'organismo dovrebbe inoltre essere affidato il compito di registrare e monitorare i fallimenti dei sistemi di contenimento. **La lettera considera la condivisione delle informazioni una condizione per imparare dagli errori**: quando un incidente si verifica perché il contenimento non ha funzionato, l'evento dovrebbe essere segnalato all'organismo competente e, in prospettiva, reso pubblico.

La trasparenza avrebbe una doppia funzione, secondo i firmatari: favorire la ricerca e l'apprendimento dagli incidenti, ma anche **rendere le organizzazioni responsabili delle proprie pratiche**. Il documento non presenta una soluzione tecnica già definita. Delinea invece un'agenda che combina contenimento più rigoroso, ricerca sulla sicurezza dell'AI, standard condivisi e segnalazione degli incidenti. La sfida è a dir poco storica, riconoscono i ricercatori, e

richiederà una reale collaborazione tra le comunità dell’intelligenza artificiale e quelle della sicurezza informatica.

The post Sicurezza dell’AI, 400 ricercatori da tutto il mondo chiedono sandbox più robuste e trasparenza sugli incidenti appeared first on Key4biz.

https://www.key4biz.it/sicurezza-dellai-400-ricercatori-da-tutto-il-mondo-chiedono-sandbox-piu-robuste-e-trasparenza-sugli-incidenti/590962/

Manovra, tensione sul taglio dell’Irpef. Verso il Consiglio europeo. Cosa succede in Parlamento

Si allungano i tempi per la manovra. Tensione sul taglio dell’Irpef

La **manovra** procede a passo lento e fatica a decollare: la decisione del governo di provare la **carta europea** per l’infiammata dell’inflazione, fa slittare l’arrivo in Parlamento della quinta **legge di bilancio** del governo di **Giorgia Meloni**. Nel giorno in cui il Cdm vara il **Documento programmatico di bilancio**, l’ossatura su cui prenderà forma la manovra, domina una certa incertezza. Palazzo Chigi nel

pomeriggio diffonde un ordine del giorno che contempla oltre al **Dpb** anche "l'illustrazione delle linee" della manovra; tre quarti d'ora dopo l'odg viene "aggiornato" e il punto sparisce. Fonti di Palazzo Chigi parlano di "mero **errore materiale**": del resto era stato lo stesso ministro **Giancarlo Giorgetti** a chiarirlo in Aula. Prima di chiuderla, infatti, Giorgetti vuole aspettare la conclusione della **procedura europea** sulla **clausola di salvaguardia**, per definire una manovra con "contorni definiti". E visto che il verdetto dovrebbe arrivare dall'Eurogruppo del 9 novembre, potrebbe non essere rispettato il termine, non perentorio, del 20 ottobre per l'invio del testo al Parlamento.

Il governo incassa intanto il via libera del Parlamento al **Dpfp** e allo **scostamento** per quasi 29 miliardi di flessibilità concessa dall'Ue per energia e difesa. Ma il sentiero di avvicinamento alla manovra si fa più incerto anche sulle misure. Quella che appariva ormai come una certezza, l'estensione del **taglio dell'Irpef** fino a 60mila euro, viene ora data per improbabile: la misura, che tre giorni fa il viceministro dell'Economia **Maurizio Leo** davanti alla platea di Confartigianato dava quasi per fatta, è al momento congelata. Ma gli alleati non sembrano tutti d'accordo. "Assolutamente no, bisogna procedere per un nuovo taglio dell'Irpef", fa muro il leader di Forza Italia **Antonio Tajani**. Al posto di questa misura, che avrebbe riguardato 3,3 milioni di contribuenti, ora si pensa ad un **bonus per i fragili**, che andrebbe ad intercettare una platea più ampia.

L'idea, sulla falsariga di una proposta di Fi, è di anticipare all'anno in corso le detrazioni Irpef per le spese sanitarie. Il Mef è intanto intenzionato a confermare la **detassazione degli incrementi contrattuali** e l'**iperammortamento**, che si punta a rafforzare. Difficile prevedere se e quanto sarà stanziato in più per la sanità, anche se per il ministro **Orazio Schillaci** l'importante è che i fondi vengano "spesi bene". Si lavora anche per estendere la **flat tax** per le

partite Iva fino a 100mila euro: una proposta della Lega, che spinge anche per le **pensioni anticipate** e per il **taglio del canone Rai**. Per i giovani, l'idea è una **flat tax sugli aumenti contrattuali**, oltre alla proposta di FI di una no tax area per gli under 35. FdI vorrebbe rendere strutturale la detassazione dei **fringe benefit**, mentre gli azzurri propongono anche di estendere l'esenzione dal bollo a tutte le prime auto, comprese quelle aziendali.

Oggi Meloni parlerà in Parlamento in vista del Consiglio Ue

Questa mattina sarà in **Senato**, poi intorno all'ora di pranzo salirà al **Quirinale** per la consueta colazione con il presidente della Repubblica **Sergio Mattarella**, infine nel primo pomeriggio interverrà alla Camera. Questo il timing che scandirà la giornata di **Giorgia Meloni**, attesa in Parlamento per rendere comunicazioni in vista del **Consiglio europeo** di domani e venerdì. Nell'intervento la premier toccherà i temi che poi saranno oggetto della riunione in programma a Bruxelles. Al primo punto figura lo spinoso **dossier competitività** e quelli altrettanto complessi legati ai **prezzi dell'energia**. La premier ha già chiarito che l'Italia, "non siede al tavolo europeo per dire sempre sì ma per dire quello che va detto anche se è scomodo, anche se costa". E a proposito di argomenti "scomodi", nel suo intervento Meloni toccherà anche quello riguardante il **sostegno a Kiev**, tema al centro del Consiglio Ue tanto quanto quello degli **attacchi ibridi in Europa** connessi alla Russia. In attesa della versione definitiva della risoluzione della maggioranza nella bozza continua ad essere presente il passaggio che prevede di "garantire la continuità del **sostegno multidimensionale** alle istituzioni e alla popolazione ucraina, anche in vista dell'inverno, e a sostenere ogni iniziativa diplomatica volta a una **pace giusta e duratura**".

Nel testo s’impegna il governo a “non far venir meno la pressione sulla Russia che porti come primo risultato un **cessate il fuoco** pieno, incondizionato e immediato, ribadendo che tali misure sono rivolte contro il regime russo e la sua capacità di sostenere la guerra di aggressione e non contro la popolazione russa”. Nessun riferimento al **dossier armi**, decisamente poco spendibile in chiave elettorale, mentre figura un richiamo alla necessità di “promuovere una decisione sulla **rappresentanza europea nel processo di pace** per l’Ucraina, sviluppando ulteriormente la proposta avanzata dal Governo italiano per la designazione di un inviato speciale europeo o, in alternativa, definendo un formato che, in virtù di un chiaro mandato da parte del Consiglio Ue, possa esprimere con autorevolezza ed efficacia la posizione dell’insieme degli Stati membri nella convinzione che nessuna decisione sulla sicurezza europea possa essere assunta senza l’Europa”.

Da capire se Meloni citerà nel suo intervento il presidente **Donald Trump** sia in considerazione degli ultimi sviluppi sul fronte del conflitto russo-ucraino sia per quanto riguarda il **Medio Oriente**, altro punto all’ordine del giorno della riunione di Bruxelles con particolare riferimento alla situazione in Iran, Yemen, a Gaza/Cisgiordania e in Libano. Di certo, invece, si soffermerà sul dossier migranti.

La Lega esulta per i passi avanti sull’Autonomia

In Cdm arriva l’ok alle prime intese sull’**Autonomia** con quattro regioni del nord. Si concretizza così l’assist di **Giorgia Meloni** a **Matteo Salvini** in vista del **congresso straordinario** della Lega del 24 e 25 ottobre all’Allianz MiCo di Milano. Via libera, quindi, ai disegni di legge di “attribuzione di ulteriori forme e condizioni particolari di Autonomia” per **Liguria**, **Lombardia**, **Piemonte** e **Veneto**. L’iter,

infatti, prevede che il Cdm deliberi l'intesa definitiva e un disegno di legge di approvazione dell'intesa entro 45 giorni. I ddl verranno, quindi, trasmessi al **Parlamento**, con allegata l'intesa, per poi essere sottoposti alle **Camere** nel passaggio definitivo. Per l'occasione sono arrivati a Palazzo Chigi i governatori di Lombardia e Veneto, **Attilio Fontana** e **Alberto Stefani**; per loro, così come per i ministri leghisti **Matteo Salvini** e **Roberto Calderoli**, nessuna conferenza stampa al termine del Cdm ma un comunicato stampa.

Intanto, in vista del **congresso leghista**, in cui si discuterà anche della segreteria politica e del nuovo simbolo, il presidente della Regione Lombardia **Attilio Fontana**, tra i più critici nelle scorse settimane, non si scompone sulle modalità di voto, per cui non sarà previsto lo scrutinio segreto per le mozioni: "Nessuno di noi ha chiesto il congresso; quindi, non è un problema che ci poniamo particolarmente". Alla domanda se nella due giorni congressuale verranno portate avanti le **istanze dei ribelli** lombardi, Fontana risponde: "Può darsi, adesso vediamo, non abbiamo ancora deciso niente", confermando poi che il progetto dell'**associazione del Nord** "va avanti". Eppure, fra i nordisti l'umore non è dei migliori: si ritiene che lo spazio di azione sia ridotto all'osso. Anche **Massimiliano Romeo** torna a battere sul tasto dell'idea di "una Lega nazionale strutturata come una confederazione di Lega Nord, Lega Centro e Lega Sud, unita e capace di dare voce alle esigenze di ogni territorio".

Alla Camera

Dopo che ieri sono state discusse e approvate le risoluzioni di maggioranza sul Documento programmatico di finanza pubblica, nella giornata di oggi l'**Assemblea della Camera** tornerà a riunirsi alle 9.00 per esaminare la pdl per il riconoscimento e tutela delle **persone che assistono e si prendono cura dei propri cari**, il ddl sull'accordo per il **trasferimento delle persone condannate** tra **Italia** e **Vietnam**,

il ddl sulla **protezione civile** e le mozioni sulla tutela dell'operato della **Corte penale internazionale**.

A seguire dibatterà sulla pdl sulla **tutela e sulla valorizzazione** delle attività commerciali dei **centri storici**, sul ddl sulla responsabilità professionale degli esercenti le **professioni sanitari**. Come di consueto alle 15.15 svolgerà le **interrogazioni a risposta immediata** (*question time*). Infine, dibatterà sulle **comunicazioni del Presidente del Consiglio dei ministri Giorgia Meloni** in vista della riunione del **Consiglio europeo del 15 e 16 ottobre 2026**.

Per quanto riguarda le **Commissioni**, la **Affari Costituzionali** esaminerà la pdl sulla revoca della cittadinanza e l'Atto Ue relativo all'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol). La **Giustizia** esaminerà la pdl sulle persone offese da reati commessi con violazione delle norme per la prevenzione degli infortuni sul lavoro, svolgerà audizioni e dibatterà sul DL sulla giustizia e gli impianti di interesse strategico nazionale. Discuterà sul ddl sulle circoscrizioni giudiziarie. La **Affari Esteri** svolgerà audizioni sulla relazione sullo stato di attuazione del Piano Mattei.

La **Cultura** proseguirà l'indagine conoscitiva sulle sfide educative e culturali e sull'impatto delle nuove tecnologie nella scuola. Discuterà sulle pdl sulla formazione delle classi nelle scuole di ogni ordine e grado. La **Ambiente** proseguirà l'esame in seconda lettura del DL sugli impianti di interesse strategico nazionale. Dibatterà sulla pdl sui consorzi di gestione e tutela del territorio e delle acque irrigue, sulla pdl sulla detenzione e commercializzazione delle borse di plastica e sulla pdl per la destinazione di veicoli fuori uso alle scuole di indirizzo tecnico e agli Istituti tecnici superiori per l'utilizzazione a fini didattici. La **Trasporti** proseguirà l'esame del ddl sulla governance portuale e rilancio degli investimenti in infrastrutture strategiche di trasporto marittimo di interesse

generale.

La **Affari Sociali** esaminerà la pdl sull'inclusione delle persone sorde nella vita civile e sociale e la pdl sulla figura professionale dell'assistente spirituale nell'ambito della rete per le cure palliative. Discuterà sulla pdl sull'istituzione del Premio "Dottor Geppino Micheletti" e si confronterà sulla pdl sul registro nazionale degli orfani per crimini domestici. La **Agricoltura** discuterà e svolgerà audizioni sulla proposta di risoluzione sul sostegno del settore ittico nazionale. La **Politiche dell'Ue** svolgerà audizioni sulla proposta di regolamento Ue sulla disponibilità degli alloggi e sulla loro accessibilità economica e sulla proposta di regolamento Ue per rafforzare l'ecosistema europeo del cloud e dell'IA.

Al Senato

L'**Assemblea del Senato** tornerà alle 9.00 per le **comunicazioni del Presidente del Consiglio dei ministri Giorgia Meloni** in vista del Consiglio europeo del 15 e 16 ottobre 2026. A seguire, si confronterà sul DL sui **prezzi petroliferi** e le infrastrutture e attività **energetiche strategiche**.

Per quanto riguarda le **Commissioni**, la **Affari Costituzionali** esaminerà il ddl sulla sicurezza, il ddl sulla rappresentanza di interessi e lo schema di Dlgs sui Vigili del fuoco. La **Giustizia** si confronterà sul ddl per la riforma dell'ordinamento professionale del commercialista, sul ddl per il rilascio degli immobili e sul ddl sulle professioni pedagogiche e educative. Dibatterà sul ddl sull'allontanamento del minore, sul ddl sulla legittima difesa. La **Affari Esteri e Difesa** si confronterà sul ddl sulla difesa nazionale.

La **Politiche dell'Ue** esaminerà il ddl delegazione europea 2026, la relazione programmatica sulla partecipazione dell'Italia all'Unione europea per l'anno 2026 e la relazione consuntiva per il 2025. Dibatterà sull'affare assegnato

relativo agli aspetti istituzionali della strategia commerciale dell'Unione europea e svolgerà audizioni sulla proposta di regolamento sulla disponibilità degli alloggi e sulla loro accessibilità economica. La **Finanze** si confronterà sul ddl sulla tutela dei consumatori e sullo schema di Dlgs sulla vigilanza finanziaria sulle imprese assicurative.

La **Cultura** svolgerà audizioni e proseguirà l'esame del DL sulla scuola. Si confronterà sul ddl sul cinema e discuterà sul ddl sulla dichiarazione di monumento nazionale di teatri italiani e sul ddl sulla rete nazionale dei presepi viventi. La **Ambiente** proseguirà l'esame del DL sulle attività energetiche strategiche e del ddl sul parco nazionale dell'Etna. Si confronterà sui ddl sulle isole minori e sul ddl sulla cattura della CO_2. Riprenderà l'esame dei ddl sui data center dibatterà sullo schema di Dlgs sulla qualità dell'aria.

La **Industria** proseguirà l'esame del ddl sullo sviluppo del settore agricolo e dell'affare assegnato sulle principali aree di crisi industriale complessa in Italia. Esaminerà il documento conclusivo dell'indagine conoscitiva sugli effetti del cambiamento climatico in agricoltura. Dibatterà sul ddl sulle grotte d'Italia, sul ddl sulle reti delle città madri del made in Italy, sui ddl sull'attività di acconciatore ed estetista, sui ddl sui prodotti agroalimentari di qualità e sui ddl sul registro nazionale dei pizzaioli. La **Affari Sociali** proseguirà l'esame dei ddl sul potenziamento dei servizi sanitari in ambito reumatologico.

The post Manovra, tensione sul taglio dell'Irpef. Verso il Consiglio europeo. Cosa succede in Parlamento appeared first on Key4biz.

https://www.key4biz.it/manovra-tensione-sul-taglio-dellirpef-verso-il-consiglio-europeo-cosa-succede-in-parlamento/590957/

Chrome, Firefox Updates Patch 114 Flaws as Mozilla Unveils Firefox Enterprise

Mozilla has introduced Firefox Enterprise for organizations with strict compliance, governance, and security requirements.

The post Chrome, Firefox Updates Patch 114 Flaws as Mozilla Unveils Firefox Enterprise appeared first on SecurityWeek.

https://www.securityweek.com/chrome-firefox-updates-patch-114-flaws-as-mozilla-unveils-firefox-enterprise/

Citrix, Fortinet, Ivanti Patch 29 Vulnerabilities Across Their Products

Critical-severity flaws could lead to authentication bypass, code execution, and sensitive authentication information leaks.

The post Citrix, Fortinet, Ivanti Patch 29 Vulnerabilities Across Their Products appeared first on SecurityWeek.

https://www.securityweek.com/citrix-fortinet-ivanti-patch-29-vulnerabilities-across-their-products/

Microsoft Patches Record 1,413 Vulnerabilities, Including Exploited Windows Zero-Day

The most important is CVE-2026-96951, a security feature bypass flaw in Windows that has been exploited in the wild.

The post Microsoft Patches Record 1,413 Vulnerabilities, Including Exploited Windows Zero-Day appeared first on SecurityWeek.

https://www.securityweek.com/microsoft-patches-record-1413-vulnerabilities-including-exploited-windows-zero-day/