Oasis Grace
Engineering Projects Pvt Ltd.
Build Your Future With Us
RTN.DR.R.SATHYANARAYANAN,
Director - Business Development
+91 9360136897 /
+91 8148231942
No.15, North Mada Street, Srinagar
Colony, Saidapet, Chennai-600015
www.oasisgrace.in
mail2rsathya@gmail.com

தமிழ் குரல் மக்கள்
தினசரி காலை நாளிதழ்
tamilmakkalkuralll@gmail.com
RN No. TNBIL/2021/81709
உள்ளது உள்ளபடி

காலை 10 மணி முதல் மதியம் 2 மணி வரை முதல் முறை இந்த ஜோட்டலை கொண்டுவருபவர்களுக்கு சிறப்பு சலுகை
MM கிளினிக்
காசு மற்றும் மருத்துவ காப்பீடு
8668018731
அடையார் தலை பெண்கள் சாலை, அடையார், சென்னை-20

கடந்த ஓராண்டில், இந்தியாவின் 92% நிறுவனங்கள் செயற்கை நுண்ணறிவு முகவர் தொடர்பான பாதுகாப்புச் சம்பவங்களை எதிர்கொண்டுள்ளன; அவற்றில் 36% நிறுவனங்கள் மட்டுமே இச்சம்பவங்களை 24 மணி நேரத்திற்குள் கட்டுக்குள் கொண்டு வந்தன.

சென்னை – 19 நவம்பர், 2026 500 பாதுகாப்புத் தலைவர்களிடம் நடத்தப்பட்ட 'செயல்படுத்தப்பட்டது ஆனால் கட்டுப்பாடற்றது: இந்தியாவில் முகவர் பாதுகாப்பின் நிலை' என்ற சர்வீஸ்நோவின் புதிய ஆய்வின்படி, கடந்த ஆண்டில் 92 சதவீத இந்திய நிறுவனங்கள் முகவர் பாதுகாப்புச் சம்பவத்தை எதிர்கொண்டுள்ளன, ஆனாலும் அவற்றுள் 36 சதவீத நிறுவனங்கள் மட்டுமே 24 மணி நேரத்திற்குள் அச்சம்பவத்தைக் கட்டுப்படுத்தியுள்ளன.

"இந்திய நிறுவனங்களின் செயல்பாட்டில் AI ஏஜெண்டுகள் தற்போது ஒரு அங்கமாகிவிட்டன, ஆனால் பாதுகாப்பு ஏற்பாடுகள் அதற்கு ஈடுகொடுக்கும் வகையில் வளரவில்லை. உங்களால் பார்க்க முடியாத ஒன்றைப் பாதுகாக்கவும் கட்டுப்படுத்தவும் முடியாது. ஒவ்வொரு ஏஜெண்டும் ஒரே இடத்தில் பதிவு செய்யப்பட்டு, பொறுப்புடைமைக்கு உட்படுத்தப்பட்டு, வெளிப்படையாகத் தெரிய வேண்டும். மேலும், கட்டுப்பாடுகள் தானியங்கி முறையில் செயல்படுத்தப்பட வேண்டும் மற்றும் இயந்திர வேகத்தில் எதிர்வினைகள் நிகழ வேண்டும். அப்போதுதான், பாதுகாப்பு குழுக்களால் சிக்கல்களை முன்கூட்டியே கண்டறிந்து, சரியான நேரத்தில் அவற்றைக் கட்டுப்படுத்த முடியும்" என்று சர்வீஸ்நவ் நிறுவனத்தின் இந்தியா மற்றும் சார்க் பிராந்தியத்திற்கான ஜிவிபி மற்றும் நிர்வாக இயக்குநர் குல்மீத் பாவா தெரிவித்தார்.

பாதுகாப்பு குறித்த நம்பிக்கை, கட்டுப்பாட்டை விட முன்னிலையில் உள்ளது.

இந்தியாவின் பாதுகாப்புத் தலைவர்களில் பாதியினர், தங்கள் நிறுவனத்தின் பாதுகாப்புச் செயல்பாடுகள் நன்கு நிலைபெற்றுவிட்டதாகக் குறிப்பிடுகின்றனர்; இருப்பினும், அதன் அடித்தளங்கள் சீரற்ற நிலையிலேயே இருப்பதாக ஆய்வு காட்டுகிறது:

ஏஜெண்டிக் ஏஐ பாதுகாப்பு நிர்வாகத்திற்குப் பொறுப்பான ஒரு குறிப்பிட்ட நபர் நியமிக்கப்பட்டிருப்பது 19% நிறுவனங்களில் மட்டுமே காணப்படுகிறது.

18% பேர் மட்டுமே தங்கள் முகவர்கள் குறித்த ஒருங்கிணைந்த, ஒற்றை இடைமுகத்திலான பார்வையைப் பெற்றுள்ளனர்

30% நிறுவனங்கள் மட்டுமே, பாதுகாப்புச் சோதனைகளில் தேர்ச்சி பெறும் வரை ஏஜெண்டுகளைத் தடுக்கும் தானியங்கி வரிசைப்படுத்தல் நுழைவாயிலை நடைமுறைப்படுத்துகின்றன.

47% நிறுவனங்களால் மட்டுமே தேவைப்படும்போது முழுமையான ஆதாரத் தொகுப்பை வழங்க முடிகிறது

கண்டறிதல் தானியங்கி முறையில் நடைபெறுகிறது, ஆனால் எதிர்வினை இன்னும் மனித முயற்சியைச் சார்ந்தே உள்ளது.

மனித மேற்பார்வை ஒரு முக்கியமான பாதுகாப்பாகத் தொடர்ந்தாலும், செயற்கை நுண்ணறிவு முகவர்கள் தொடர்ச்சியாகவும் இயந்திர வேகத்திலும் செயல்படும் இடங்களில் அது மட்டுமே ஒரே பாதுகாப்பு அரணாக இருக்க முடியாது. இந்திய நிறுவனங்களில் ஏறக்குறைய பாதி (51%), செயற்கை நுண்ணறிவு முகவரின் இயல்புக்கு மாறான நடத்தையை நிகழ்நேரத்தில் தானியங்குபடுத்துகின்றன. இருப்பினும், 67% நிறுவனங்களால் ஒரு முகவர் இயல்புக்கு மாறாகச் செயல்படும்போது தானாக நடவடிக்கை எடுக்க முடிவதில்லை. இது, ஒரு அச்சுறுத்தலைக் கண்டறிவதற்கும் அதற்குப் பதிலளிப்பதற்கும் இடையிலான இடைவெளியை எடுத்துக்காட்டுகிறது.

வெறும் 46% மட்டுமே ஏஜெண்ட் உருவாக்கம் தொடங்குவதற்கு முன்பு பாதுகாப்பைக் கொண்டுவருகின்றன, எனவே பாதுகாப்பு அவற்றைச் சுற்றியுள்ள கட்டுப்பாடுகளை வடிவமைப்பதற்கு முன்பே பல ஏஜெண்ட்கள் வடிவமைக்கப்பட்டு உருவாக்கப்படுகின்றன. இந்த பாதிப்பு தகவல் தொழில்நுட்பத் துறையையும் தாண்டிச் செல்கிறது: 83% நிறுவனங்கள், செயல்பாட்டுத் தொழில்நுட்பம் (OT) அல்லது பௌதீகச் சூழல்களில் AI ஏஜெண்ட்களை இயக்குகின்றன அல்லது அவற்றுடன் ஊடாடுகின்றன, மேலும் 29% மட்டுமே அவற்றுக்கென ஒரு தனி நிர்வாகக் கட்டமைப்பை வடிவமைத்துள்ளன.

"நிழல் ஏஜ" சிக்கல்

கடந்த 12 மாதங்களில், 37% நிறுவனங்கள், பாதுகாப்பு குழுக்களுக்கு ஒருபோதும் தெரியப்படுத்தப்படாத அல்லது பதிவு செய்யப்படாத AI ஏஜெண்ட்கள் செயல்பாட்டில் இருப்பதைக் கண்டறிந்துள்ளன. பதிவு செய்யப்படாத இந்த ஏஜெண்ட்கள் ஒரு முக்கியமான பார்வைக் குறைபாடாக உள்ளன: நிறுவனங்களால் பார்க்க முடியாத ஒன்றை அவர்களால் நிர்வகிக்க முடியாது.

CERT-In (இந்திய கணினி அவசரக்கால பதிலளிப்புக் குழு) அக்டோபர் 2026-ல் வெளியிட்ட AI ஏஜெண்டுகள் குறித்த ஆலோசனையானது (CIAD-2026-0049), இந்திய நிறுவனங்களின் முன்னுரிமைப் பட்டியலில் 'ஏஜெண்டுகளின் தெரிவுநிலை மற்றும் கட்டுப்பாடு' குறித்த விஷயத்தைக் கொண்டு வந்துள்ளது. ServiceNow ஆய்வு, நிறுவனங்கள் தங்கள் வசம் உள்ள ஏஜெண்டுகளை எந்த அளவுக்குக் கண்காணிக்கவும், நிர்வகிக்கவும் முடிகிறது என்பதை ஆராய்கிறது. மேலும், CERT-In-ன் 2022-ஆம் ஆண்டு வழிகாட்டுதல்களின்படி, இந்திய நிறுவனங்கள் ஏதேனும் சைபர் சம்பவங்கள் குறித்து அறிந்த ஆறு மணி நேரத்திற்குள் அது குறித்துத் தெரிவிக்க வேண்டியது கட்டாயமாகும்.

ஒருங்கிணைந்த தளத்தில் 'ஏஜெண்டிக் செக்யூரிட்டி' முறையைச் செயல்படுத்தும் நிறுவனங்கள் ஆய்வில் பங்கேற்றவர்களில் 43%, அவ்வாறு செய்யாத நிறுவனங்களை விடச் சிறப்பாகச் செயல்படுகின்றன: இவர்களில் 62% நிறுவனங்கள், ஏஜெண்ட்களின் அசாதாரண நடத்தைகளைக் கண்டறிந்து தானியங்கி முறையில் நிகழ்நேர எச்சரிக்கைகளை வழங்குகின்றன (மற்ற நிறுவனங்களில் இது 43% மட்டுமே). மேலும், 45% நிறுவனங்கள் ஏஜெண்ட் கொள்கை மீறல்களைத் தானாகவே சரிசெய்கின்றன (மற்ற நிறுவனங்களில் இது 24% மட்டுமே), மற்றும் 51% நிறுவனங்கள் தொடர்ந்து ஆதாரங்களைச் சேகரிக்கின்றன (மற்ற நிறுவனங்களில் இது 43% மட்டுமே).

என்ன இயங்குகிறது என்பதை அறிவதில் இருந்தே இடைவெளியைக் குறைப்பது தொடங்குகிறது. நிறுவனங்களுக்குத் தங்களின் AI ஏஜெண்ட்கள் குறித்த முழுமையான பதிவேடு, ஏஜெண்ட்கள் மற்றும் அடையாளங்கள் முழுவதற்குமான ஒரே பார்வை, மற்றும் அவற்றை நிர்வகிக்கப் பொறுப்பான ஒரு நியமிக்கப்பட்ட தலைவர் ஆகியோர் தேவை. அறிக்கையின் முழுமையான கண்டுபிடிப்புகளை ஆராய, இங்கே கிளிக் செய்யவும் - செயல்படுத்தப்பட்டும் நிர்வகிக்கப்படாதவை: இந்தியாவில் ஏஜெண்ட் பாதுகாப்பின் நிலை.