www.infokairali.in വില 30 രൂപ 2025 ജൂൺ

ഇൻഫോ-കൈരളി

കമ്പ്യൂട്ടർ മാഗസിൻ

facebook.com/infokairali 9447124390

ഗിമ്പ് 3.0: ഓപൺ സോഴ്സ്
ഇമേജ് എഡിറ്റിംഗിന്റെ പുതിയ മാറ്റങ്ങൾ

എഡ്ജ് എഐ - എഡ്ജ് കമ്പ്യൂട്ടിങ്ങിന്റെയും
എഐയുടെയും സംയോജനം

സൈബർ കോട്ടയുടെ രഹസ്യായുധം: ഡിജിറ്റൽ പ്രതിരോധത്തിന്റെ കഥ

വീട്ടിലൊരു തീയേറ്റർ നിങ്ങളുടെ സ്വപ്നമാണോ?

Aries DM Pvt Ltd അവതരിപ്പിക്കുന്നു ലോകത്തിലെ ആദ്യത്തെ റെഡിമെയ്ഡ് ഹോം തീയേറ്റർ

വീടിന്റെ ടെറസിന്റെ അനുയോജ്യമായ ഭാഗത്ത് കുറഞ്ഞ സമയം കൊണ്ട് ഇത് നിർമ്മിക്കാം. വീടിന്റെ പുറത്ത് ഔട്ട്ഹൗസ് പോലെയും നിർമ്മിക്കാം

8 അടി വീതിയും 12 അടി നീളവുമുള്ള 4 സീറ്റർ, 8 അടി വീതിയും 16 അടി നീളവുമുള്ള 7 സീറ്റർ,കൂടാതെ കസ്റ്റമൈസ്ഡ് സൈസുകളിലും റെഡിമെയ്ഡ് തീയേറ്റർ ലഭ്യമാണ്.

റെഡിമെയ്ഡ് ഹോം തീയേറ്റർ നേരിട്ട് കണ്ടു മനസ്സിലാക്കുന്നതിനായി 9539000522 അല്ലെങ്കിൽ 9446090206 നമ്പറിലേക്ക് വാട്സ്ആപ്പ് ചെയ്യൂ... കൂടുതലറിയാൻ www.ariesdm.com സന്ദർശിക്കുക.

ARIES DM
DIGITAL MAGICS

Aries Digital Magics Pvt Ltd
Door No: 11/335
Pullappallil Buildings
Manjoor P0, Kuruppanthara
Kottayam, Kerala, India - 686603
www.ariesdm.com

നമ്മുടെ ICM | കേരളത്തിൽ മുൻനിരയിൽ !

PSC നിയമനങ്ങൾക്ക് യോഗ്യമായ ഗവ. അംഗീകൃത കമ്പ്യൂട്ടർ കോഴ്സുകളിലേക്ക് പ്രവേശനം നേടാം

കേന്ദ്ര ഗവൺമെന്റ്
ഭാരതത്തിലൊട്ടാകെ NCVT യുടെ
12313 അംഗീകൃത തൊഴിൽ
അധിഷ്ഠിത സ്ഥാപനങ്ങളിൽ
നടത്തിയ ഫെയ്സ് ടു ട്രേഡിങ്ങിൽ
കേരളത്തിൽ മാത്രമല്ല തമിഴ്നാട്,
പോണ്ടിച്ചേരി ഉൾപ്പെടെ ഒന്നാം സ്ഥാനം
നേടിയ നമ്മുടെ ICM സംസ്ഥാന
സർക്കാർ ഈ വർഷം നടത്തിയ
ഗ്രേഡിങ്ങിൽ മുൻനിരയിൽ

icm

COMPUTER PVT ITI

THALAYOLAPARAMBU

Call : +91 980 928 6999

COURSES

PGDCA, DCA,
Data Entry, PDCFA,
2D/ 3D Animation,
Graphic Designing
& DTP, Tally Certification
from Tally Accademy,
Special coaching
for SAP

അവധിക്കാല കമ്പ്യൂട്ടർ
സ്പോക്കൺ ഇംഗ്ലീഷ്
ഫാഷൻ ഡിസൈനിങ്
അബാക്കസ് ക്ലാസ്സുകൾ

40-ലധികം വ്യത്യസ്തങ്ങളായ
അവധിക്കാല കോഴ്സുകൾ
PSC നിയമനത്തിന് യോഗ്യമായ
ഗവ. അംഗീകൃത കമ്പ്യൂട്ടർ കോഴ്സുകളും
50% വരെ ഫീസ് ഇളവും

INFO-KAIRALI

VOL.26 NO.8 JUNE 2025

Kuruppanthara
Kottayam - 686 603
Whatsapp: 9447124390
Website: www.infokairali.com
E-Mail: kairali.info@gmail.com
facebook.com/infokairali

Managing Editor & Editor in Charge
SOJAN JOSE

Editorial Support
NANDAKUMAR E.

Sub Editors
MARY MATHEWS
OJITHA K S

Digital Marketing Consultant
ANAND SOJAN

Circulation
SHAJI MANIMALA

Marketing
LINO MOHAN

Advisory Board Chairman
DR. ACHUTH SANKAR S. NAIR
Retd. Director, Quality Assurance, Professor, Dept of Computational Biology and Bioinformatics, University of Kerala

Advisory Board
PROF. JYOTHY JOHN
Retd. Principal, College of Engineering Chengannur

Er. M.P. LOKNATH
General Secretary, Internet Society of India

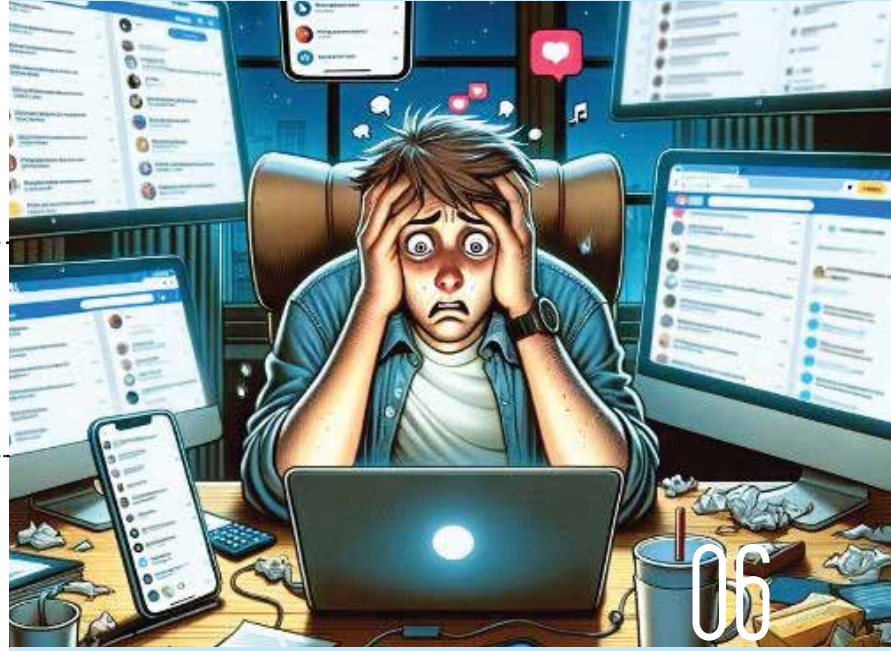
DR. SABU M. THAMPI
Associate Professor, IIITM-K Trivandrum

DR. UMESH P.
HOD, Department of Applied Science, College of Engineering, Aranmula

MR. ROBIN TOMMY
Innovation Lead, TCS, Trivandrum

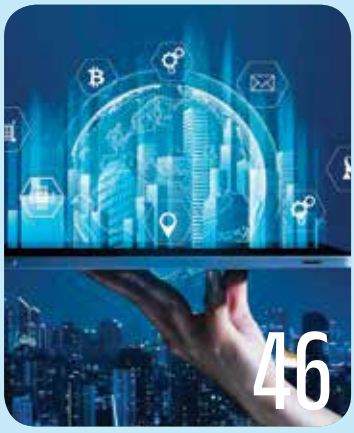
MR. GOKUL ALEX
Senior Manager, UST Global, Infinity Labs Trivandrum,

Lay-Out & Design
SANTHOSH



സൈബർ കോട്ടയുടെ രഹസ്യായുധം: ഡിജിറ്റൽ പ്രതിരോധത്തിന്റെ കഥ

ഗിമ്പ് 3.0: ഓപ്പൺ സോഴ്സ് ഇമേജ് എഡിറ്റിംഗിന്റെ പുതിയ മാറ്റങ്ങൾ



എഡ്ജ് എഐ - എഡ്ജ് കംപ്യൂട്ടിങ്ങിന്റെയും എഐയുടെയും സംയോജനം

ഇൻഫോ എഡിറ്റ്

റിമോട്ട് വർക്ക്: ജീവനക്കാരെ തിരികെ വിളിക്കുമ്പോൾ

ഈയിടെ വാഷിംഗ്ടണിൽ പ്രസിദ്ധമായ ഒരു പോഡ്കാസ്റ്റിൽ റിമോട്ട് വർക്കിനെപ്പറ്റിയൊരു ചർച്ച നടക്കുകയുണ്ടായി. കമ്പനികൾ റിമോട്ട് വർക്ക് വേണ്ടെന്നു തീരുമാനിക്കുന്നതാണ് വിഷയം. ഓഫീസിൽ എല്ലാ ജോലിക്കാരും ഒന്നിച്ചുണ്ടാവുന്നതാണ് നല്ലതെന്നാണ് കമ്പനികളുടെ തീരുമാനമത്രെ.

എന്നാൽ ഈ വിഷയത്തെപ്പറ്റി ഭിന്നാഭിപ്രായങ്ങളാണുള്ളത്. കോർപ്പറേറ്റ് കമ്പനികൾ ഏതുവിധേനയും ചിലവുകുറക്കാനുള്ള പദ്ധതിയിലാണ്. ജീവനക്കാരെ പറഞ്ഞുവിടുന്നത് അതിന്റെ പ്രധാന ചവിട്ടുപടിയായി മാറിക്കഴിഞ്ഞു.

2020 ൽ കോവിഡ് വന്നത്തോടെയാണ് റിമോട്ട് വർക്ക് സർവസാധാരണമായത്. അതിനോട് പൊരുത്തപ്പെട്ട് ജീവനക്കാർ മികച്ച പ്രകടനങ്ങൾ കാഴ്ചവെച്ചു മുന്നേറിയിരുന്നു. 2025 ൽ കമ്പനികൾ ജീവനക്കാരെ തിരികെ വിളിക്കുമ്പോൾ ചില പൊരുത്തക്കേടുകളുണ്ടായിവരുന്നു. ഏറെക്കാലമായി റിമോട്ട് വർക്ക് ചെയ്തുവരുന്ന ജീവനക്കാരെ കമ്പനിയിൽ വരാനാവശ്യപ്പെടുമ്പോൾ അവർ സ്വയം ജോലി വിടുന്നതായി കണ്ടുവരുന്നു. അങ്ങനെയാവുമ്പോൾ കമ്പനിക്ക് പ്രത്യേകിച്ചൊന്നും ചെയ്യേണ്ടി വരുന്നില്ലായെന്നതാണ് തന്ത്രം.

പുതിയ തീരുമാനം ബാധിക്കുന്നത് കമ്പനിയിൽ തിളങ്ങി നിൽക്കുന്ന പ്രതിഭകളെയാണെന്നതാണ് മറ്റൊരു തമാശ. ഇവർ കമ്പനിക്കൊരു മുതൽക്കൂട്ടാണെങ്കിലും ഓഫീസിൽ തിരികെ പോകുന്നതിനോട് യോജിപ്പില്ലെങ്കിൽ അവർ വിട്ടു പോകാനുള്ള സാധ്യതയാണുള്ളത്. കമ്പനിയിലെ മുൻനിരക്കാർക്ക് പുതിയ അവസരങ്ങൾ ലഭിക്കാൻ പ്രയാസമുണ്ടാവില്ല.

കമ്പനികളിൽ പുതിയ ജീവനക്കാരുടെ നിയമനം ഈയിടെ വളരെ കുറവാണ്. നിലവിലുള്ള ജോലിക്കാർ കമ്പനിയിലുണ്ടായാൽ സമയം നന്നായി പ്രയോജനപ്പെടുത്താൻ കഴിയുമെന്ന ചിന്ത കമ്പനികൾക്കുമുണ്ട്.

ജോലി എവിടെയിരുന്നു ചെയ്താലും ശരിയായ രീതിയിൽ വേണ്ട സമയത്ത് കൊടുക്കുന്നതാണ് പ്രധാനം. കമ്പനിയിൽ ജോലി ചെയ്യുമ്പോൾ അനവധി തടസങ്ങൾ വന്നേക്കാം. ജോലി ചെയ്യുന്ന സമയം കുറവായിരിക്കും. റിമോട്ട് വർക്കാവുമ്പോൾ അധികം തടസങ്ങളൊന്നും വരാനുള്ള സാധ്യതയില്ല. അഥവാ വന്നാൽത്തന്നെ സ്വയം പരിഹരിക്കാൻ എളുപ്പമായിരിക്കും. ജോലിയെ ബാധിക്കുകയുമില്ല.

എഡിറ്റോറിയൽ ടീം

സൈബർ കോട്ടയുടെ രഹസ്യായുധം: ഡിജിറ്റൽ പ്രതിരോധത്തിന്റെ കഥ

© ഷാഹിദ് നീർമുണ്ട

ഇന്നത്തെ നമ്മുടെ ലോകം ഡിജിറ്റൽ ടെക്നോളജിയുടെ ഒരു കുത്തൊഴുക്കിലാണെന്ന് പ്രത്യേകം പറയേണ്ടതില്ലല്ലോ! സത്യം പറഞ്ഞാൽ, നമ്മുടെ കൈയ്യിലുള്ള സ്മാർട്ട്ഫോൺ തൊട്ട് ആകാശത്തോളം ഉയരത്തിലുള്ള ക്ലൗഡ് കംപ്യൂട്ടിങ് സിസ്റ്റങ്ങൾ വരെ, എല്ലാം നമ്മുടെ ജീവിതത്തിന്റെ ഭാഗമായില്ലേ? ഒന്ന് ആലോചിച്ച് നോക്കിയേ, നമ്മുടെയൊരു ദിവസം എങ്ങനെയാ തുടങ്ങുന്നതെന്ന്? രാവിലെ കണ്ണുതുറക്കുമ്പോൾ നമ്മളെ വിളിച്ചുണർത്തുന്നത് നമ്മുടെ സ്മാർട്ട്ഫോണിന്റെ അലാറം. ഒരു കപ്പ് കാപ്പിയുമായിട്ട്, രാത്രി എന്തൊക്കെ ഇൻസ്റ്റാഗ്രാം പോസ്റ്റുകൾ വന്നെന്ന് സ്ക്രോൾ ചെയ്യും. പിന്നെ ജോലിക്ക് പോകുമ്പോൾ, ട്രാഫിക്കിൽ വഴി തെറ്റാതെ നമ്മളെ നയിക്കുന്നത് ആരാ? നമ്മുടെ GPS തന്നെ!.ജോലി എല്ലാം കഴിഞ്ഞു വൈകുന്നേരമാകുമ്പോൾ നെറ്റ്ഫ്ലിക്സിൽ പുതിയ സീരീസ് ഇറങ്ങിയോ എന്ന് നോക്കും, അല്ലെങ്കിൽ യൂട്യൂബിൽ തകർപ്പൻ വൈറൽ വീഡിയോ കണ്ട് നമ്മളൊന്ന് റിലാക്സ് ചെയ്യും, അല്ലേ? ഇതിനിടയിൽ വാട്സ്ആപ്പിലെ ഗ്രൂപ്പ് ചാറ്റുകൾ, ഇഷ്ടമുള്ളതൊക്കെ ഓൺലൈനായി ഓർഡർ ചെയ്യുന്നത്, അറിയാത്ത കാര്യങ്ങൾ ഗൂഗിളിൽ തപ്പി നോക്കുന്നതും ഒക്കെ നമ്മുടെ ദിനചര്യയുടെ ഭാഗമായി. ആകെമൊത്തം പറഞ്ഞാൽ, ഈ ഡിജിറ്റൽ ലോകമില്ലാതെ നമുക്കൊരു ജീവിതമുണ്ടോ എന്ന് ചോദിച്ചു

നിങ്ങൾ റാൻസംവെയർ ആക്രമണങ്ങൾ എന്ന് കേട്ടിട്ടുണ്ടോ? ശരിക്കും ഇതൊരു സൈബർ ലോകത്തെ പിടിച്ചുപറിക്കാരനാണ്!. നമ്മുടെ കംപ്യൂട്ടറിനെയോ നെറ്റ്‌വർക്കിനെയോ ഇവൻ ഒറ്റയടിക്ക് 'ഹൈജാക്ക്' ചെയ്യും.

പോവും, അത്രയ്ക്കങ്ങോട്ട് നമ്മളതിനോട് ഇഴുകിച്ചേർന്നു കഴിഞ്ഞു.

അതുപോലെ തന്നെ, നിലവിൽ ബിസിനസ്സുകാരെല്ലാം ഡേറ്റയെ ആശ്രയിച്ചാണ് തീരുമാനമെടുക്കുന്നത്. നമ്മളെപ്പോലുള്ള സാധാരണക്കാർ സോഷ്യൽ മീഡിയ വഴി ലോകത്തിന്റെ ഏത് കോണിലുള്ളവരുമായിട്ടും ബന്ധപ്പെടുന്നു. സർക്കാർ കാര്യങ്ങളാകട്ടെ, ഇ-ഗവേണൻസ് സംവിധാനങ്ങൾ വഴി വളരെ കാര്യക്ഷമമായി മുന്നോട്ട് പോകുന്നു.പക്ഷേ, ഈ ഡിജിറ്റൽ വിപ്ലവം ഒരുപാട് അവസരങ്ങൾ തുറന്നുതരുമ്പോൾ തന്നെ, ചില വലിയ അപകടങ്ങളും ഒളിഞ്ഞിരിപ്പുണ്ട് കേട്ടോ! റാൻസംവെയർ ആക്രമണങ്ങൾ, ഡേറ്റാ ചോർത്തലുകൾ, ഫിഷിംഗ് തട്ടിപ്പുകൾ, സോഷ്യൽ എൻജിനീയറിങ് തന്ത്രങ്ങൾ ഇതൊക്കെ നമ്മുടെ ഈ ഡിജിറ്റൽ ലോകത്തിന്റെ സുരക്ഷയ്ക്ക് എന്നും ഒരു വെല്ലുവിളിയാണ്.

ഏപ്രിൽ 2025-ൽ, എഫ്ബിഐ ഒരു ഞെട്ടിപ്പിക്കുന്ന റിപ്പോർട്ട് പുറത്തുവിട്ടു. അവരുടെ ഇന്റർനെറ്റ് ക്രൈം കംപ്ലയിന്റ് സെന്റർ (IC3) വഴി കിട്ടിയ എല്ലാ പരാതികളും വിലയിരുത്തിയാണ് ഈ വാർഷിക റിപ്പോർട്ട് ഉണ്ടാക്കിയിരിക്കുന്നത്. ഈ റിപ്പോർട്ട് അനുസരിച്ച്, 2024-ൽ സൈബർ കുറ്റകൃത്യങ്ങൾ വഴി ആളുകൾക്ക് നഷ്ടമായത് എത്രയാണെന്നോ? 16.6 ബില്യൺ ഡോളർ! അതായത്, ഏകദേശം 1,38,000 കോടി രൂപയോളം വരും! ഇത് 2023-നെ അപേക്ഷിച്ച് 4.1 ബില്യൺ ഡോളറിന്റെ വലിയ വർദ്ധനവാണ്. മാത്രമല്ല, 2019-ൽ രേഖപ്പെടുത്തിയ തുകയുടെ അഞ്ചിരട്ടിയിലധികമാണിത്! സൈബർ ലോകത്ത് നമ്മൾ എത്രത്തോളം ശ്രദ്ധിക്കണം എന്നതിന്റെ ഒരു ഉദാഹരണമാണിത്.

ഡിജിറ്റൽ ലോകം നമുക്ക് ഒരുപാട് വാതിലുകൾ തുറന്നു തരുന്നുണ്ടെങ്കിലും, സൈബർ ഭീഷണികൾ എന്നൊക്കെ പറയുന്നത് നമ്മുടെ കൂടെപ്പിറപ്പായി മാറിയിട്ടുണ്ട്. മുകളിൽ നമ്മൾ കണ്ട ഓരോ ഭീഷണികളെയും കുറിച്ചും അവ നമ്മുടെ ഡിജിറ്റൽ ലോകത്തെ എങ്ങനെയാണ് വെല്ലുവിളിക്കുന്നതെന്നും ഒന്നുകൂടി നോക്കിയാലോ?

റാൻസംവെയർ ആക്രമണങ്ങൾ (Ransomware Attacks)

നിങ്ങൾ റാൻസംവെയർ ആക്രമണങ്ങൾ എന്ന് കേട്ടിട്ടുണ്ടോ? ശരിക്കും ഇതൊരു സൈബർ ലോകത്തെ പിടിച്ചുപറിക്കാരനാണ്!. നമ്മുടെ കംപ്യൂട്ടറിനെയോ നെറ്റ്‌വർക്കിനെയോ ഇവൻ ഒറ്റയടിക്ക് 'ഹൈജാക്ക്' ചെയ്യും. എന്നിട്ട് അവിടെയുള്ള ഫയലുകൾ, ഫോട്ടോകൾ, വീഡിയോകൾ – അങ്ങനെ നിങ്ങളുടെ എല്ലാ ഡേറ്റയും – ഒരു വ്യക്തിക്കും തുറക്കാൻ പറ്റാത്ത രീതിയിൽ പൂട്ടിയിടും; അതായത്, ആർക്കും മനസ്സിലാകാത്ത കോഡാക്കി മാറ്റും (എൻക്രിപ്റ്റ് ചെയ്യുക). ആ ഡേറ്റ തിരിച്ചു കിട്ടണമെങ്കിൽ തനിക്ക് ഒരു നിശ്ചിത തുക പണം തരണമെന്ന് ഹാക്കർമാർ ആവശ്യപ്പെടും. ഈ പണത്തിനാണ് റാൻസം എന്ന് പറയുന്നത്. കൊടുത്തില്ലെങ്കിലോ? "നിങ്ങളുടെ ഡേറ്റ ഒന്നുകിൽ പൂർണ്ണമായി ഡിലീറ്റ് ചെയ്യും, അല്ലെങ്കിൽ പൊതുജനങ്ങൾക്ക് മുന്നിൽ പരസ്യപ്പെടുത്തും!" എന്നൊക്കെ പറഞ്ഞ് ഭീഷണിപ്പെടുത്തും. ഒരു തരം ഡിജിറ്റൽ ബ്ലാക്ക്മെയിലിംഗ് എന്ന് പറയാം. ചെറിയ കട നടത്തുന്ന ആളായാലും, വൻകിട കോർപ്പറേഷനുകൾക്കും സർക്കാർ സ്ഥാപനങ്ങൾക്കും വരെ ഇത് വലിയ തലവേദനയും, ചിലപ്പോൾ ലക്ഷക്കണക്കിന് രൂപയുടെ സാമ്പത്തിക നഷ്ടവും ഉണ്ടാക്കും. നമ്മുടെ ദൈനംദിന ജീവിതം പോലും താളം തെറ്റിക്കാൻ ഇവന്മാർക്ക് ഒരൊറ്റ ക്ലിക്ക് മതി.

ഡേറ്റാ ചോർച്ച (Data Breaches)

ഒരാളുടെയോ ഒരു സ്ഥാപനത്തിന്റെയോ രഹസ്യ വിവരങ്ങൾ നമ്മളറിയാതെ ചോർന്നുപോവുകയോ ഹാക്കർമാർ കൈക്കലാക്കുകയോ ചെയ്യുന്ന അവസ്ഥയാണിത്. നമ്മുടെ പേര്, വിലാസം, ജനനത്തീയതി തുടങ്ങി ബാങ്ക് അക്കൗണ്ട് വിവരങ്ങൾ, ക്രെഡിറ്റ് കാർഡ് നമ്പറുകൾ, ആരോഗ്യപരമായ വിവരങ്ങൾ, ഒരു കമ്പനിയുടെ ബിസിനസ് രഹസ്യങ്ങൾ എന്തും ഇതുപോലെ ചോർത്തപ്പെടാം.ഇത് നമ്മുടെ സ്വകാര്യതയിലേക്കുള്ള ഒരു കടന്നുകയറ്റമാണ്. ഐഡന്റിറ്റി മോഷണം (നമ്മുടെ വിവരങ്ങൾ ഉപയോഗിച്ച് മറ്റൊരാൾ ചമയുന്നത്), സാമ്പത്തിക തട്ടിപ്പുകൾ, വ്യക്തിപരമായ ഉപദ്രവങ്ങൾ എന്നിവയിലേക്കൊക്കെ ഇത്

ചുരുക്കിപ്പറഞ്ഞാൽ, ഡിജിറ്റൽ ലോകം ഇങ്ങനെ കുതിച്ചു പായുമ്പോൾ, ഈ സൈബർ ഭീഷണികൾ വ്യക്തികൾക്കും സ്ഥാപനങ്ങൾക്കും, എന്തിന് രാജ്യങ്ങൾക്ക് പോലും വലിയ തലവേദനയാണ്.

വഴിതുറക്കും. സ്ഥാപനങ്ങളെ സംബന്ധിച്ചിടത്തോളം ജനങ്ങളുടെ വിശ്വാസം നഷ്ടപ്പെടാനും വലിയ സാമ്പത്തിക പിഴകൾ നൽകേണ്ടി വരാനും നിയമനടപടികൾ നേരിടാനും സാധ്യതയുണ്ട്.

ഫിഷിംഗ് തട്ടിപ്പുകൾ (Phishing Scams)

ഇമെയിൽ വഴിയോ എസ്എംഎസ് വഴിയോ വ്യാജ വെബ്സൈറ്റുകൾ വഴിയോ ആളുകളെ പറ്റിച്ചു അവരുടെ രഹസ്യ വിവരങ്ങൾ (യൂസർ നെയിം, പാസ്വേഡ്, ബാങ്ക് വിവരങ്ങൾ, ഒടിപി ഒക്കെ) തട്ടിയെടുക്കുന്ന വിദ്യയാണിത്. ബാങ്കിൽ നിന്നോ, സർക്കാരിൽ നിന്നോ, അല്ലെങ്കിൽ നമുക്ക് വിശ്വാസമുള്ള ഏതെങ്കിലും സ്ഥാപനത്തിൽ നിന്നോ ഉള്ള സന്ദേശമാണെന്ന് തെറ്റിദ്ധരിപ്പിച്ചാണ് ഇത്തരം തട്ടിപ്പുകൾ നടക്കുന്നത്. ഇങ്ങനെയുള്ള സൈബർ ആക്രമണങ്ങളിലേക്ക് ആളുകളെ കുടുക്കാനുള്ള ഒരു പ്രധാന കവാടമായാണ് ഫിഷിംഗ് പ്രവർത്തിക്കുന്നത്. ഇതിലൂടെ കിട്ടുന്ന വിവരങ്ങൾ ഉപയോഗിച്ച് പിന്നെ വലിയ തട്ടിപ്പുകൾ നടത്താൻ ഹാക്കർമാർക്ക് എളുപ്പമാണ്. ഒരു ലിങ്കിൽ ക്ലിക്ക് ചെയ്യുന്നതോടെ ചിലപ്പോൾ എല്ലാം പോയെന്ന് വരും!

സോഷ്യൽ എൻജിനീയറിംഗ് തന്ത്രങ്ങൾ (Social Engineering Tactics)

ഇവിടെ ഹാക്കർമാർ ടെക്നോളജിയെ അത്രയധികം ആശ്രയിക്കുന്നില്ല. പകരം, മനുഷ്യന്റെ മനശാസ്ത്രപരമായ ദൗർബല്യങ്ങളെ മുതലെടുത്ത് വിവരങ്ങൾ ചോർത്തുകയോ സുരക്ഷാ സംവിധാനങ്ങളെ മറികടക്കുകയോ ചെയ്യുന്ന തന്ത്രമാണിത്. സഹായിക്കാനുള്ള നമ്മുടെ മനസ്സ്, ഒരാളിലുള്ള വിശ്വാസം, ഭയം, ആകാംഷ ഇതൊക്കെയാണ് ഹാക്കർമാർ ചൂഷണം ചെയ്യുന്നത്. ഉദാഹരണത്തിന്, ഒരു കമ്പനിയിലെ ജീവനക്കാരനെ വിളിച്ച് ഐടി ഡിപ്പാർട്ട്മെന്റിൽ നിന്നാണെന്ന് പറഞ്ഞ് പാസ്വേർഡ് ചോദിച്ചറിയുക. അല്ലെങ്കിൽ, വളരെ പ്രധാനപ്പെട്ട ഒരു ഫയലാണെന്ന് പറഞ്ഞ് ഒരു മാൽവെയർ അടങ്ങിയ അറ്റാച്ച്മെന്റ് തുറപ്പിക്കുക. ഇതൊക്കെ സോഷ്യൽ എഞ്ചിനീയറിംഗിന്റെ ഭാഗമാണ്. നമ്മുടെ ശ്രദ്ധയില്ലായ്മയോ അമിത വിശ്വാസമോ ആണ് ഇവർക്ക് തുണയാകുന്നത്.

ഈ ഭീഷണികളെല്ലാം നമ്മുടെ ഡിജിറ്റൽ ജീവിതത്തിന് ഒരു വെല്ലുവിളിയായി നിൽക്കുമ്പോൾ, നമ്മൾ ഓരോരുത്തരും കുറച്ചുകൂടി ശ്രദ്ധാലുക്കളായിരിക്കണം, അല്ലേ? ചുരുക്കിപ്പറഞ്ഞാൽ, ഡിജിറ്റൽ ലോകം ഇങ്ങനെ കുതിച്ചു പായുമ്പോൾ, ഈ സൈബർ ഭീഷണികൾ വ്യക്തികൾക്കും സ്ഥാപനങ്ങൾക്കും, എന്തിന് രാജ്യങ്ങൾക്ക് പോലും വലിയ തലവേദനയാണ്. ഈയൊരു സാഹചര്യത്തിലാണ് 'ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം' (Digital Immune System) എന്നൊരു കിടിലൻ ആശയം രക്ഷകനായി വരുന്നത്!

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം: ഒരു രക്ഷകൻ!

നമ്മുടെ ശരീരത്തിലെ പ്രതിരോധ ശേഷി അഥവാ ഇമ്മ്യൂൺ സിസ്റ്റം അസുഖങ്ങളുണ്ടാക്കുന്ന സൂക്ഷ്മാണുക്കളെ തിരിച്ചറിഞ്ഞ് നശിപ്പിക്കുന്നത് പോലെ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം സൈബർ ഭീഷണികളെ കണ്ടുപിടിച്ച് തടയുകയും, എന്തെങ്കിലും പ്രശ്നം വന്നാൽ വേഗം തിരിച്ചുവരാൻ സഹായിക്കുകയും ചെയ്യുന്നു. ഒന്ന് ആലോചിച്ചു നോക്കിയേ, നമ്മുടെ ശരീരത്തിലെ വെളുത്ത രക്താണുക്കൾ ഒരു വൈറസിനെതിരെ പോരാടുന്നത് പോലെ, ഫയർവാളുകൾ അനധികൃതമായ കടന്നുകയറ്റങ്ങളെ തടയുന്നു! ഭാവിയിലെ ആക്രമണങ്ങളെ തടയാൻ ഓർമ്മ സെല്ലുകൾ സഹായിക്കുന്നത് പോലെ, മെഷീൻ ലേണിംഗ് അൽഗോരിതങ്ങൾ പുതിയ ഭീഷണികളെ മനസ്സിലാക്കി അതിനനുസരിച്ച് പ്രതികരിക്കുന്നു. അതുകൊണ്ട് തന്നെ, നമ്മുടെ ഡിജിറ്റൽ ലോകത്തിന്റെ ആരോഗ്യം നിലനിർത്താൻ ഈ സംവിധാനം അത്യാവശ്യമാണെന്ന് പറയാം.ഒരു ബിസിനസ് സ്ഥാപനത്തിന്റെ പ്രധാനപ്പെട്ട ഡേറ്റ ചോർന്നുപോയാൽ എന്താ സംഭവിക്കുക? ഉപഭോക്താക്കൾക്ക് അവരോടുള്ള വിശ്വാസം പോകും, സാമ്പത്തിക നഷ്ടം വരും, നിയമപരമായ പ്രശ്നങ്ങളും ഉണ്ടാകും. അതുപോലെ, നമ്മളുടെ സ്വകാര്യ വിവരങ്ങൾ ദുരുപയോഗം ചെയ്യപ്പെട്ടാൽ അത് നമ്മു

സൈബർ ലോകത്തിന്റെ ഈ 'പ്രതിരോധ സംവിധാനം' നമ്മുടെ സ്വന്തം ശരീരത്തിൽ നിന്ന് പല കാര്യങ്ങളും കടമെടുത്തിട്ടുണ്ട് എന്ന് പറഞ്ഞാൽ വിശ്വസിക്കുമോ? ശരിക്കും നമ്മുടെ ശരീരത്തിന്റെ പ്രതിരോധ ശേഷി പോലെ തന്നെയാണിത്!

ടെ സ്വകാര്യതയ്ക്ക് വലിയ ഭീഷണിയാണ്. പക്ഷേ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഈ ഭീഷണികളെ മുൻകൂട്ടി തടയാനും, അഥവാ എന്തെങ്കിലും ആക്രമണം ഉണ്ടായാൽ പെട്ടെന്ന് തിരിച്ച് വരാനും നമ്മളെ സഹായിക്കും. ഈ 'ഡിജിറ്റൽ ഇമ്മ്യൂൺ സിസ്റ്റം' വരുന്നതോടെ സൈബർ ലോകം കൂടുതൽ സുരക്ഷിതമാകുമല്ലോ, അല്ലേ? എന്താണ് നിങ്ങളുടെ അഭിപ്രായം?

ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഒരു വൺമാൻ ഷോ ആണെന്ന് ധരിക്കരുതേ? ഇത് ശരിക്കും ഒരു കൂട്ടായ പ്രവത്തനമാണ്. സോഫ്റ്റ്വെയറുകൾ, ഹാർഡ്വെയറുകൾ, ചില നിയമങ്ങൾ, പിന്നെ കൃത്യമായ നടപടികൾ ഇതെല്ലാം ഒത്തുചേരുമ്പോഴാണ് ഈ സംവിധാനം രൂപം കൊള്ളുന്നത്. നമ്മുടെ ഡിജിറ്റൽ ലോകത്തെ സൈബർ ആക്രമണങ്ങളിൽ നിന്ന് സുരക്ഷിതമാക്കുക എന്നതാണ് ഇതിന്റെ പ്രധാന ജോലി. സ്വയം കാര്യങ്ങൾ നിരീക്ഷിച്ചും, ഭീഷണികളെ വേഗം കണ്ടെത്തിയും, അതിനോട് കൃത്യമായി പ്രതികരിച്ചും, എന്തെങ്കിലും തകരാർ വന്നാൽ പഴയ സ്ഥിതിയിലേക്ക് തിരിച്ചെത്തിച്ചുമൊക്കെയാണ് ഇത് പ്രവർത്തിക്കുന്നത്.

മനുഷ്യ ശരീരത്തോട് സാമ്യമുള്ള ഡിജിറ്റൽ പ്രതിരോധം

സൈബർ ലോകത്തിന്റെ ഈ 'പ്രതിരോധ സംവിധാനം' നമ്മുടെ സ്വന്തം ശരീരത്തിൽ നിന്ന് പല കാര്യങ്ങളും കടമെടുത്തിട്ടുണ്ട് എന്ന് പറഞ്ഞാൽ വിശ്വസിക്കുമോ? ശരിക്കും നമ്മുടെ ശരീരത്തിന്റെ പ്രതിരോധ ശേഷി പോലെ തന്നെയാണിത്! അതുകൊണ്ടാണ് ഈ ഡിജിറ്റൽ സിസ്റ്റങ്ങൾക്ക് ഇത്ര കാര്യക്ഷമവും സ്വയംപര്യാപ്തവുമായി പ്രവർത്തിക്കാൻ കഴിയുന്നത്. പ്രധാനപ്പെട്ട സാമ്യങ്ങൾ എന്തൊക്കെയാണെന്ന് നോക്കിയാലോ?

• സംരക്ഷണം (Protection): ആദ്യത്തെ കാര്യം സംരക്ഷണം തന്നെ! ഇത് ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഏറ്റവും പ്രധാനപ്പെട്ട ലക്ഷ്യമാണ്. നമ്മുടെ ശരീരം വൈറസ്, ബാക്ടീരിയ പോലുള്ള രോഗാണുക്കളിൽ നിന്നും മറ്റ് പ്രശ്നങ്ങളിൽ നിന്നുമൊക്കെ സ്വയം രക്ഷിക്കുന്നത് പോലെ, ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം സൈബർ ലോകത്തെ നമ്മുടെ പ്രധാനപ്പെട്ട ഡേറ്റയെയും സിസ്റ്റങ്ങളെയും മാൽവെയർ, വൈറസ്, റാൻസംവെയർ, ഫിഷിംഗ് ആക്രമണം, സിസ്റ്റം തകരാറുകൾ തുടങ്ങിയവയിൽ നിന്നെല്ലാം സംരക്ഷിക്കുന്നു. നമ്മുടെ ശരീരത്തിന് രോഗാണുക്കളിൽ നിന്ന് സംരക്ഷണം വേണ്ടത് പോലെ തന്നെ ഡിജിറ്റൽ ലോകത്തിനും അത് അത്യാവശ്യമാണ്.

• തിരിച്ചറിയൽ (Identification/Detection): ഇത് ശരിക്കും ഒരു ഡിറ്റക്ടീവിന്റെ പണിയാണ്! നമ്മുടെ ശരീരത്തിലെ പ്രതിരോധ സംവിധാനം പുറത്തുനിന്ന് വരുന്ന രോഗാണുക്കളെയും, ശരീരത്തിന് ദോഷകരമായ വസ്തുക്കളെയും കൃത്യമായി തിരിച്ചറിയുന്ന പോലെയാണിത്. ഒരു ഭീഷണിയെ കണ്ടുപിടിച്ചാൽ മാത്രമേ അതിനെതിരെ പ്രതിരോധം തീർക്കാനും സിസ്റ്റത്തെ രക്ഷിക്കാനും പറ്റൂ, അല്ലേ? മനുഷ്യശരീരം അതിന്റേതല്ലാത്ത എന്തിനെയും അസ്വാഭാവികമായ കോശങ്ങളെയും തിരിച്ചറിയുന്നത് പോലെ, ഡിജിറ്റൽ സിസ്റ്റം നമ്മുടെ കംപ്യൂട്ടറുകളിലെ അസ്വാഭാവിക പ്രവർത്തനങ്ങൾ, മാൽവെയറുകൾ, സുരക്ഷാ പിഴവുകൾ എന്നിവയെല്ലാം നിരീക്ഷണം വഴിയും AI/ML പോലുള്ള പുതിയ ടെക്നോളജികൾ വഴിയും കണ്ടെത്തുന്നു.

• പ്രതികരണം (Response): ഒരു പ്രശ്നം കണ്ടുപിടിച്ചാൽ പിന്നെ വെറുതെ ഇരിക്കില്ല! നമ്മുടെ ശരീരം അസുഖം വന്നാൽ ആന്റിബോഡികൾ ഉണ്ടാക്കിയും രോഗാണുക്കളെ നശിപ്പിച്ചുമൊക്കെ പ്രതികരിക്കുന്നത് പോലെ, ഡിജിറ്റൽ സിസ്റ്റം കണ്ടെത്തിയ ഭീഷണികളെ ബ്ലോക്ക് ചെയ്യും, മാൽവെയറുകളെ 'കാറന്റൈനിൽ' ആക്കും, സുരക്ഷാ പ്രശ്നങ്ങൾ പരിഹരിക്കും, സിസ്റ്റം പഴയപടിയാക്കാൻ വേണ്ട കാര്യങ്ങൾ ചെയ്യും. ഇതൊക്കെ സ്വയമേവ നടക്കുന്ന കാര്യങ്ങളാണ്.

• സ്വയം രോഗശാന്തിയും പുനഃസ്ഥാപിക്കലും (Self-Healing and Recovery): നമുക്കൊരു മുറിവുണ്ടാ

നമ്മുടെ ശരീരത്തിലെ പ്രതിരോധശേഷി അഥവാ ഇമ്മ്യൂൺ സിസ്റ്റം അസുഖങ്ങളുണ്ടാക്കുന്ന സൂക്ഷ്മാണുക്കളെ തിരിച്ചറിഞ്ഞ് നശിപ്പിക്കുന്നത് പോലെ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം സൈബർ ഭീഷണികളെ കണ്ടുപിടിച്ച് തടയുകയും, എന്തെങ്കിലും പ്രശ്നം വന്നാൽ വേഗം തിരിച്ചുവരാൻ സഹായിക്കുകയും ചെയ്യുന്നു.

യാൽ ശരീരം തന്നെ അത് ഉണക്കും, കേടായ കോശങ്ങളെ നന്നാക്കും. അതുപോലെ തന്നെയാണ് ഡിജിറ്റൽ ലോകത്തും. തകരാറിലായ സോഫ്റ്റ്വെയറുകളെ സ്വയം റീസ്റ്റാർട്ട് ചെയ്യുക, ബാക്കപ്പിൽ നിന്ന് ഡേറ്റ തിരിച്ചെടുക്കുക, ഒരു സിസ്റ്റം പോയാൽ വേറൊന്നിലേക്ക് മാറുക എന്നിങ്ങനെയൊക്കെ ചെയ്ത് ഈ സംവിധാനം വേഗത്തിൽ പഴയ അവസ്ഥയിലേക്ക് തിരിച്ചെത്താൻ സഹായിക്കും.

• ഓർമ്മയും പഠനവും (Memory and Learning): ഇത് ശരിക്കും രസകരമാണ്! നമുക്കൊരു അസുഖം വന്നാൽ, ആ രോഗാണുവിനെ ശരീരം ഓർത്തുവെക്കും. അടുത്ത തവണ അവൻ വന്നാൽ, അതിശക്തമായി, വേഗത്തിൽ അവനെ തടയാൻ ശരീരത്തിന് പറ്റും. വാക്സിനേഷൻ ഒക്കെ ഇങ്ങനെയാണല്ലോ പ്രവർത്തിക്കുന്നത്. അതുപോലെ, ഡിജിറ്റൽ സിസ്റ്റവും മുൻപുണ്ടായ സൈബർ ആക്രമണങ്ങളെയും പ്രശ്നങ്ങളെയും കുറിച്ചുള്ള വിവരങ്ങൾ ശേഖരിച്ച് പഠിക്കും (ഇവിടെ AI/ML പോലുള്ള ടെക്നോളജികളാണ് സഹായിക്കുന്നത്). ഈ പഠനം വഴി ഭാവിയിൽ സമാനമായ ഭീഷണികളെ മുൻകൂട്ടി കാണാനും തടയാനും, പിന്നെ പെട്ടെന്ന് പ്രതികരിക്കാനുള്ള കഴിവ് കൂട്ടാനും ഈ സംവിധാനത്തിന് കഴിയും.

• ഒന്നിലധികം ലെയറുകളുള്ള പ്രതിരോധം (Multiple Layers of Defense): ഇത് വളരെ പ്രധാനപ്പെട്ട ഒരു കാര്യമാണ്! മനുഷ്യ ശരീരത്തിന് ഒരുപാട് പ്രതിരോധ ലെയറുകൾ ഉണ്ട്. തൊലിയും, കണ്ണുനീരും, ഉമിനീരും ഒക്കെ രോഗാണുക്കളെ ഉള്ളിൽ കടക്കാതെ തടയുന്നു. ഇനി അഥവാ കടന്നാൽ, വെളുത്ത രക്താണുക്കളും പനിയും വീക്കവുമൊക്കെ വരും. ഒരു രോഗാണുവിന് വേണ്ടി മാത്രമല്ല, പൊതുവായ ഒരു പ്രതിരോധമാണിത്. അതുപോലെ, ഡിജിറ്റൽ സിസ്റ്റത്തിലും ഒരു ഭീഷണിയെ തടയാൻ ഒരൊറ്റ സുരക്ഷാ സംവിധാനം മാത്രം പോരാ. അതുകൊണ്ട്, ഫയർവാളുകൾ, ആന്റിവൈറസ് സോഫ്റ്റ്വെയറുകൾ, ഇൻട്രൂഷൻ ഡിറ്റക്ഷൻ സിസ്റ്റങ്ങൾ, എൻക്രിപ്ഷൻ, സുരക്ഷാ പാച്ചുകൾ, ആക്സസ് കൺട്രോളുകൾ തുടങ്ങി പല തലങ്ങളിലുള്ള പ്രതിരോധ സംവിധാനങ്ങളാണ് ഇവിടെ ഉപയോഗിക്കുന്നത്.

അപ്പോൾ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം എന്ന് പറയുന്നത് വെറും കുറച്ച് സുരക്ഷാ സോഫ്റ്റ്വെയറുകൾ ഇൻസ്റ്റാൾ ചെയ്യുന്നതിനും അപ്പുറമുള്ള ഒരു വലിയ കാര്യമാണ് മനസിലായില്ലേ? നമ്മുടെ സ്വന്തം ശരീരത്തിന്റെ രോഗപ്രതിരോധ ശേഷി പോലെ തന്നെ, ഇത് ചലനാത്മകവും (Dynamic), സ്വയം കാര്യങ്ങൾ തിരിച്ചറിഞ്ഞ് (Self-Aware) പ്രതികരിക്കാൻ കഴിവുള്ളതും, ഓരോ പ്രശ്നങ്ങളിൽ നിന്നും പഠിച്ച് (Learning) മുന്നോട്ട് പോകുന്നതും, ഏത് പ്രതിസന്ധിയിലും അതിജീവിക്കാൻ (Resilient) ശേഷിയുള്ളതുമായ ഒരു കൂട്ടായ സംവിധാനമാണിത്. ഇങ്ങനെയുള്ള കഴിവുകളാണ് ഇന്നത്തെയും ഭാവിയുടെയും സങ്കീർണ്ണവും ഭീഷണി നിറഞ്ഞതുമായ നമ്മുടെ ഡിജിറ്റൽ ലോകത്തിന് അതിജീവിക്കാനും സുരക്ഷിതമായി മുന്നോട്ട് പോകാനും ഇത് അത്യാവശ്യമാക്കി മാറ്റുന്നത്. വെറുതെ ആക്രമണങ്ങളെ തടയുക എന്നതിനപ്പുറം, പ്രശ്നങ്ങളെ സ്വയം പരിഹരിക്കാനും, തകരാറുകളിൽ നിന്ന് വേഗത്തിൽ കരകയറാനും, ഓരോ ആക്രമണങ്ങളിൽ നിന്നും പാഠം ഉൾക്കൊണ്ട് കൂടുതൽ മികച്ചതാവാനും ഇതിന് സാധിക്കണം. ഇത്രയും ശക്തമായ ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം എങ്ങനെയാണ് ശരിക്കും പ്രവർത്തിക്കുന്നത്? ഏതൊക്കെ ഘടകങ്ങളാണ് ഇതിനെ ഇത്രയും കാര്യക്ഷമമാക്കുന്നത്? അടുത്ത ലേഖനത്തിൽ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ പ്രധാന ഘടകങ്ങളെക്കുറിച്ച് നമുക്ക് വിശദമായി ചർച്ച ചെയ്യാം.

●

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഘടകങ്ങൾ

സൈബർ ആക്രമണങ്ങളും സാങ്കേതിക തകരാറുകളും ഒക്കെ കൂടി വരുന്ന ഈ കാലത്ത്, നമ്മുടെ ഡിജിറ്റൽ ലോകത്തെ സുരക്ഷിതമായി നിർത്താനും കാര്യങ്ങൾ തടസ്സമില്ലാതെ മുന്നോട്ട് കൊണ്ടുപോകാനും ഒരു പുതിയ തരം പ്രതിരോധം അത്യാവശ്യമാണ്, അല്ലേ? അവിടെയാണ് ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം എന്ന ആശയം കടന്നുവരുന്നത്. നമ്മുടെ സ്വന്തം ശരീരത്തിന്റെ രോഗപ്രതിരോധ ശക്തിയെപ്പോലെ തന്നെ, ഡിജിറ്റൽ ഭീഷണികളെ സ്വയം തിരിച്ചറിഞ്ഞ് തടയാനും, എന്തെങ്കിലും കുഴപ്പങ്ങൾ വന്നാൽ അതിൽ നിന്ന് വേഗത്തിൽ കരകയറാനും കഴിവുള്ള സിസ്റ്റങ്ങൾ ഉണ്ടാക്കുക എന്നതാണ് ഇതിന്റെ പ്രധാന ലക്ഷ്യം. ശരിക്കും ഈ സംവിധാനം ഒരുപാട് സാങ്കേതികവിദ്യകളും പ്രോസസ്സുകളും ഒരുമിച്ച് പ്രവർത്തിക്കുമ്പോഴാണ് രൂപപ്പെടുന്നത്. നമ്മുടെ ഡിജിറ്റൽ പരിസ്ഥിതിയുടെ സുരക്ഷയും കരുത്തും ഉറപ്പാക്കുന്ന ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ പ്രധാന ഘടകങ്ങൾ എന്തൊക്കെയാണെന്ന് താഴെ നോക്കാം.

കോട്ടയിലെ കാവൽക്കാരൻ: ഡിജിറ്റൽ ഫയർവാൾ (Firewall)

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ ഒരു പ്രധാന താരമാണ് നമ്മുടെ ഫയർവാൾ. പഴയ കോട്ടയുടെ ഗേറ്റ് കണ്ടിട്ടില്ലേ? അതേപോലെയാണ് ഫയർവാളിന്റെയും പണി. നമ്മുടെ ഡിജിറ്റൽ നെറ്റ്വർക്കിലേക്ക് ആരും അനുവാദമില്ലാതെ കടന്നുപോകാതെയും സൈബർ ഭീഷണികൾ അകത്ത് കയറാതെയും സംരക്ഷിക്കുന്നത് ഇവനാണ്. ശരിക്കും പറഞ്ഞാൽ, ഒരു ഡിജിറ്റൽ ഫിൽട്ടർ പോലെയാണ് ഇവൻ പ്രവർത്തിക്കുന്നത്. ഡേറ്റയുടെ ഒഴുക്കിനെ എപ്പോഴും നിരീക്ഷിച്ചുകൊണ്ട്, അപകടകാരികളായ എല്ലാ പ്രവർത്തനങ്ങളെയും ഇവൻ തടയും. നമ്മുടെ സ്വന്തം നെറ്റ്വർക്കിനും പൊതുവായ ഇന്റർനെറ്റിനും ഇടയിൽ ഒരു മതിൽ പോലെ നിൽക്കുന്ന ഒരു നെറ്റ്വർക്ക് സുരക്ഷാ ഉപകരണമോ സോഫ്റ്റ്വെയറോ ആണ് ഈ ഫയർ വാൾ. ചില

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ ഒരു പ്രധാന താരമാണ് നമ്മുടെ ഫയർവാൾ. പഴയ കോട്ടയുടെ ഗേറ്റ് കണ്ടിട്ടില്ലേ? അതേപോലെയാണ് ഫയർവാളിന്റെയും പണി.

നിയമങ്ങൾ (റൂൾസ്) മുൻകൂട്ടി സെറ്റ് ചെയ്തിട്ടുണ്ടാകും. അതിന്റെ അടിസ്ഥാനത്തിൽ, ഓരോ ഡേറ്റാ പാക്കറ്റിനെയും ഇവ വിശദമായി പരിശോധിക്കും. നല്ല പാക്കറ്റുകളെ മാത്രം അകത്തേക്ക് വിടും, അപകടമുള്ളവരെ ഉടൻ തടയും. ഇത് ഹാർഡ്‌വെയർ രൂപത്തിലോ സോഫ്റ്റ്‌വെയർ രൂപത്തിലോ അല്ലെങ്കിൽ രണ്ടും ചേർന്ന രൂപത്തിലോ ആകാം. ഒരു ഗേറ്റ്കീപ്പർ ചെയ്യുന്ന എല്ലാ കാര്യങ്ങളും ഇവനും ചെയ്യും, അതായത്:

• നെറ്റ്‌വർക്കിലൂടെ വരുന്ന എല്ലാ ഡേറ്റാ ട്രാഫിക്കും എവിടെനിന്ന് വരുന്നു, എവിടേക്ക് പോകുന്നു, എന്താണ് അതിന്റെ ഉള്ളടക്കം എന്നൊക്കെ ഇവൻ സൂക്ഷ്മമായി നിരീക്ഷിക്കും.

• IP അഡ്രസ്, പോർട്ട് നമ്പർ, പ്രോട്ടോക്കോൾ എന്നിവയുടെയൊക്കെ അടിസ്ഥാനത്തിൽ ചില നിയമങ്ങൾ പ്രയോഗിച്ച്, ട്രാഫിക്കിനെ അകത്തേക്ക് വിടണോ വേണ്ടയോ എന്ന് തീരുമാനിക്കും.

• ഹാക്കർമാർ, മാൽവെയറുകൾ, മറ്റ് ഭീഷണികൾ എന്നിവരിൽ നിന്നൊക്കെ നമ്മുടെ നെറ്റ്‌വർക്കിനെ സംരക്ഷിക്കുന്നത് ഇവന്റെ പ്രധാന ജോലിയാണ്.

• പിന്നെ, എന്തെങ്കിലും സുരക്ഷാ പ്രശ്നങ്ങൾ ഉണ്ടായാൽ അതെല്ലാം രേഖപ്പെടുത്തി വെയ്ക്കുകയും, പിന്നീട് സിസ്റ്റം അഡ്മിനിസ്ട്രേറ്റർമാർക്ക് അത് പഠിക്കാൻ സഹായിക്കുകയും ചെയ്യും.

എന്തായാലും, സൈബർ ലോകത്ത് ഫയർവാൾ ഒരു വലിയ സഹായം തന്നെയാണല്ലേ? ഫയർവാൾ ഒരു വലിയ കാവൽക്കാരനാണെന്ന് നമ്മൾ കണ്ടു. പക്ഷേ, ഈ ഫയർവാളുകൾ പലതരം ഉണ്ടെന്ന് അറിയാമോ? ഓരോന്നിനും ഓരോ തരം സുരക്ഷാ ആവശ്യങ്ങൾ നിറവേറ്റാൻ കഴിയും. പ്രധാനപ്പെട്ട തരങ്ങൾ നമുക്ക് നോക്കാം:

• പാക്കറ്റ് ഫിൽട്ടറിംഗ് ഫയർവാൾ (Packet Filtering Firewall): ഇവനാണ് കൂട്ടത്തിൽ ഏറ്റവും ബേസിക്. ഡേറ്റാ പാക്കറ്റുകളുടെ തലപ്പത്തുള്ള വിവരങ്ങൾ (IP അഡ്രസ്സും പോർട്ട് നമ്പറുമൊക്കെ) നോക്കി ഫിൽട്ടർ ചെയ്യും. ഇവന് നല്ല വേഗതയുണ്ടെങ്കിലും, കാര്യമായ ആഴത്തിലുള്ള പരിശോധനയൊന്നും ഇവന് ചെയ്യാനാവില്ല.

• സ്റ്റേറ്റ്ഫുൾ ഇൻസ്പെക്ഷൻ ഫയർവാൾ (Stateful Inspection Firewall): ഇവൻ കുറച്ചുകൂടി സ്മാർട്ടാണ്! ഒരു പാക്കറ്റ് എവിടെ നിന്ന് വന്നു, എങ്ങോട്ട് പോകുന്നു, അതിന് മുൻപുള്ള കണക്ഷന്റെ ചരിത്രം എന്താണ് എന്നൊക്കെ ഇവൻ ഓർത്തുവെക്കും. അതുകൊണ്ട് തന്നെ ഇത് കൂടുതൽ സുരക്ഷിതവും ആധുനികവുമാണ്.

• പ്രോക്സി ഫയർവാൾ (Proxy Firewall): ഇവനെ നമുക്കൊരു ഇടനിലക്കാരൻ എന്ന് വിളിക്കാം. നമ്മൾ ഒരു വെബ്സൈറ്റ് തുറക്കുമ്പോൾ, നമ്മളും വെബ്സൈറ്റ് സെർവറും തമ്മിൽ നേരിട്ട് ബന്ധം സ്ഥാപിക്കാൻ ഇവൻ സമ്മതിക്കില്ല. പകരം, ഇവൻ ഒരു 'പ്രോക്സി' ആയി നിന്ന് ഡേറ്റയുടെ ഉള്ളടക്കം വരെ കൃത്യമായി വിശകലനം ചെയ്ത ഉയർന്ന സുരക്ഷ ഉറപ്പാക്കുന്നു.

• നെക്സ്റ്റ്-ജനറേഷൻ ഫയർവാൾ (Next-Generation Firewall - NGFW): ഇവനാണ് പുതിയ കാലത്തെ സൂപ്പർ താരം! വെറും പാക്കറ്റ് പരിശോധന മാത്രമല്ല, ഡേറ്റയുടെ ഉള്ളിലേക്ക് ഇറങ്ങിച്ചെന്ന് (ഡീപ് പാക്കറ്റ് ഇൻസ്പെക്ഷൻ) പരിശോധിക്കും. നുഴഞ്ഞുകയറ്റങ്ങളെ തടയാനും ആപ്ലിക്കേഷനുകളുടെ തലത്തിൽ വരെ ഫിൽട്ടറിംഗ് ചെയ്യാനും ഇവന് കഴിയും. ഇന്നത്തെ സങ്കീർണ്ണമായ ഭീഷണികളിൽ നിന്ന് വിപുലമായ സംരക്ഷണം നൽകുന്നത് ഇവനാണ്.

• ക്ലൗഡ് ഫയർവാൾ (Cloud Firewall): ക്ലൗഡ് കംപ്യൂട്ടിംഗ് വന്നപ്പോൾ അതിനുവേണ്ടി പ്രത്യേകം ഉണ്ടാക്കിയ ഫയർവാളാണിത്. വെർച്വൽ നെറ്റ്‌വർക്കുകളെയും ക്ലൗഡ് ആപ്ലിക്കേഷനുകളെയും സംരക്ഷിക്കാൻ ഇവൻ മിടുക്കനാണ്.

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ മറ്റൊരു സൂപ്പർ സ്റ്റാറാണ് ഇൻട്രൂഷൻ ഡിറ്റക്ഷൻ ആൻഡ് പ്രിവൻഷൻ സിസ്റ്റം (IDPS). നമ്മുടെ ഡിജിറ്റൽ നെറ്റ്‌വർക്കുകൾക്കും സിസ്റ്റങ്ങൾക്കും തത്സമയം (Real-time) കാവലിരിക്കുകയും ഭീഷണികളെ തടയുകയും ചെയ്യുന്ന ഒരു മിടുക്കനാണിത്.

സൈബർ ഭീഷണികളുടെ രൂപവും ഭാവവും ഓരോ ദിവസവും മാറിക്കൊണ്ടിരിക്കുകയാണല്ലോ. അതുകൊണ്ട്, ഫയർവാളുകളും ആധുനിക സാങ്കേതികവിദ്യകളുമായി ചേർന്ന് വികസിച്ചുകൊണ്ടിരിക്കുന്നുണ്ട്. ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഈ നിർണായക ഘടകമായ ഫയർവാളുകൾ, പുതിയ തലമുറ ആക്രമണങ്ങളെ തടയാൻ കഴിവ് വർദ്ധിപ്പിച്ചുകൊണ്ട് രൂപം മാറിക്കൊണ്ടിരിക്കുകയാണ്.AI (നിർമ്മിത ബുദ്ധി), ക്ലൗഡ്, സീറോ ട്രസ്റ്റ് (ഒന്നിനെയും കണ്ണുമടച്ച് വിശ്വസിക്കാതിരിക്കുക), ഓട്ടോമേഷൻ എന്നിവയുടെയെല്ലാം കൂട്ടുകെട്ട് ഫയർവാളുകളെ കൂടുതൽ ബുദ്ധിപരവും സാഹചര്യങ്ങൾക്കനുസരിച്ച് മാറാൻ കഴിവുള്ളതുമാക്കി മാറ്റുന്നു. സാധാരണക്കാർ മുതൽ വലിയ സ്ഥാപനങ്ങൾ വരെ, ഈ പുതിയ ട്രെൻഡുകൾ നമ്മുടെ ഡിജിറ്റൽ ലോകം സുരക്ഷിതവും കരുത്തുറ്റതുമാക്കാൻ സഹായിക്കുന്നു.അതുകൊണ്ട്, ഒരു ഫയർവാൾ നമ്മുടെ ഡിജിറ്റൽ ലോകത്തിന്റെ കാവൽക്കാരനാണെന്ന് ചുരുക്കത്തിൽ പറയാം, നിങ്ങൾക്ക് എന്ത് തോന്നുന്നു?

ഡിജിറ്റൽ ലോകത്തെ 'ആന്റിബോഡികൾ': ആന്റി വൈറസ്/ആന്റി-മാൽവെയർ സോഫ്റ്റ്‌വെയർ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ മറ്റൊരു പ്രധാനപ്പെട്ട പോരാളിയാണ് നമ്മുടെ ആന്റിവൈറസ്/ആന്റി-മാൽവെയർ സോഫ്റ്റ്‌വെയറുകൾ. മനുഷ്യശരീരത്തിലെ രോഗാണുക്കളെ തുരത്തുന്ന ആന്റിബോഡികളെ ഓർമ്മയില്ലേ? അതേപോലെയാണ് ഈ സോഫ്റ്റ്‌വെയറുകളുടെയും ജോലി. നമ്മുടെ കംപ്യൂട്ടറുകൾ, ലാപ്‌ടോപ്പുകൾ, സെർവറുകൾ തുടങ്ങിയ ഡിജിറ്റൽ ഉപകരണങ്ങളെ വൈറസുകൾ, വേമുകൾ, ട്രോജനുകൾ, റാൻസംവെയർ, സ്പൈവെയർ എന്നിങ്ങനെ ദോഷകരമായ സോഫ്റ്റ്‌വെയറുകളിൽ (ഇവരെയൊക്കെ നമ്മൾ മൊത്തത്തിൽ മാൽവെയറുകൾ എന്ന് വിളിക്കും) നിന്ന് സംരക്ഷിക്കുന്നത് ഇവരാണ്.ഈ സോഫ്റ്റ്‌വെയറുകൾ എപ്പോഴും ഭീഷണികളെ തിരിച്ചറിയുകയും, അവയെ നിർവീര്യമാക്കുകയും, നമ്മുടെ ഡിജിറ്റൽ ലോകത്തെ സുരക്ഷിതമാക്കുകയും ചെയ്യും. ഇവ എങ്ങനെയാണ് പ്രവർത്തിക്കുന്നതെന്നോ? സിസ്റ്റത്തിലെ ഫയലുകളെയും പ്രോഗ്രാമുകളെയും സ്കാൻ ചെയ്ത്, അറിയപ്പെടുന്ന മാൽവെയറുകളുടെ 'സിഗ്നേച്ചറുകളുമായി' (അതായത്, അവരുടെ പ്രത്യേക അടയാളങ്ങളുമായി) താരതമ്യം ചെയ്യും. സിഗ്നേച്ചർ നോക്കി മാത്രമല്ല, അസ്വാഭാവികമായ സിസ്റ്റം പ്രവർത്തനങ്ങളെ നിരന്തരം നിരീക്ഷിച്ചുകൊണ്ട് പുതിയതും ഇതുവരെ കണ്ടുപിടിക്കാത്തതുമായ മാൽവെയറുകളെ കണ്ടെത്താനുള്ള ഹ്യൂറിസ്റ്റിക് (Heuristic) രീതികളും ഇവർക്കുണ്ട്.

നമ്മൾ ഒരു ഫയൽ തുറക്കുമ്പോഴോ അല്ലെങ്കിൽ

ഡൗൺലോഡ് ചെയ്യുമ്പോഴോ ഒക്കെ ഈ ആന്റിവൈറസ് സോഫ്റ്റ്‌വെയർ റിയൽ-ടൈം സ്കാനിംഗ് വഴി നമുക്ക് സംരക്ഷണം തരും. ഇവയുടെ കാര്യക്ഷമത നിലനിർത്താൻ, വൈറസ് ഡെഫനിഷനുകൾ നമ്മൾ എപ്പോഴും അപ്‌ഡേറ്റ് ചെയ്യേണ്ടത് അത്യാവശ്യമാണ് എന്ന് പറയേണ്ടതില്ലല്ലോ?. എൻഡ്പോയിന്റ് ഉപകരണങ്ങളെ (നമ്മുടെ സ്വന്തം കംപ്യൂട്ടറുകളും ഫോണുകളുമൊക്കെ) സാധാരണ മാൽവെയർ ഭീഷണികളിൽ നിന്ന് രക്ഷിക്കുന്നത് ഇവരാണ്. വ്യക്തികൾക്കും വലിയ സ്ഥാപനങ്ങൾക്കും ഇത് ഒരുപോലെ പ്രധാനപ്പെട്ട സുരക്ഷാ സംവിധാനമാണ്. ചുരുക്കിപ്പറഞ്ഞാൽ, ആന്റിവൈറസ്/ആന്റി-മാൽവെയർ സോഫ്റ്റ്‌വെയറുകൾ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഒരു അവിഭാജ്യ ഘടകമാണ്. റിയൽ-ടൈം സ്കാനിംഗ്, ഹ്യൂറിസ്റ്റിക് വിശകലനം, AI-അധിഷ്ഠിത സാങ്കേതികവിദ്യകൾ എന്നിവയിലൂടെ, ഈ സോഫ്റ്റ്‌വെയറുകൾ ആധുനിക സൈബർ ആക്രമണങ്ങളെ ചെറുക്കാൻ നമ്മളെ സഹായിക്കുന്നു.

സൈബർ ലോകത്തെ സൂപ്പർ കാവൽക്കാരൻ: IDPS

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ മറ്റൊരു സൂപ്പർ സ്റ്റാറാണ് ഇൻട്രൂഷൻ ഡിറ്റക്ഷൻ ആൻഡ് പ്രിവൻഷൻ സിസ്റ്റം (IDPS). നമ്മുടെ ഡിജിറ്റൽ നെറ്റ്‌വർക്കുകൾക്കും സിസ്റ്റങ്ങൾക്കും തത്സമയം (Real-time) കാവലിരിക്കുകയും ഭീഷണികളെ തടയുകയും ചെയ്യുന്ന ഒരു മിടുക്കനാണിത്. എപ്പോഴും ജാഗ്രതയോടെ കാര്യങ്ങൾ നിരീക്ഷിക്കുന്ന ഒരു കാവൽക്കാരനെപ്പോലെ, അനധികൃതമായി കടന്നുപോകാൻ ശ്രമിക്കുന്നവരെയും, മാൽവെയറുകളെയും, നെറ്റ്‌വർക്ക് ആക്രമണങ്ങളെയും IDPS തിരിച്ചറിയുകയും, അവയെ തടയുകയോ അതിനോട് പ്രതികരിക്കുകയോ ചെയ്യുന്നു.ഈ സംവിധാനം നെറ്റ്‌വർക്കിലൂടെയുള്ള ഡേറ്റാ ട്രാഫിക്കിനെയും സിസ്റ്റത്തിന്റെ ഓരോ പ്രവർ

എൻക്രിപ്ഷൻ എന്നാൽ, ഒരു അൽഗോരിതം (Encryption Algorithm) ഉപയോഗിച്ച് ഡേറ്റയെ വായിക്കാൻ പറ്റാത്ത രീതിയിലേക്ക് മാറ്റുന്ന പരിപാടിയാണ്. ഈ മാറ്റത്തിന് ഒരു എൻക്രിപ്ഷൻ കീ (Key) ആവശ്യമാണ്.

ത്തനങ്ങളെയും നിരന്തരം നിരീക്ഷിക്കും. സംശയകരമായ എന്തെങ്കിലും നുഴഞ്ഞുകയറ്റ ശ്രമങ്ങൾ (Intrusions) കണ്ടെത്തിയാൽ, അത് സ്വയം നടപടികൾ എടുത്ത് തടയും, അല്ലെങ്കിൽ സിസ്റ്റം അഡ്മിനിസ്ട്രേറ്റർമാർക്ക് മുന്നറിയിപ്പ് നൽകും. IDPS-നെ നമുക്ക് ഹാർഡ്‌വെയർ ആയോ സോഫ്റ്റ്‌വെയർ ആയോ അല്ലെങ്കിൽ ഇവ രണ്ടും ചേർത്തോ ഉപയോഗിക്കാം.

നെറ്റ്‌വർക്ക് ട്രാഫിക് വിശകലനം ചെയ്യുക, സിസ്റ്റം ലോഗുകൾ പരിശോധിക്കുക, അറിയപ്പെടുന്ന ആക്രമണ രീതികളുമായി താരതമ്യം ചെയ്യുക, അല്ലെങ്കിൽ അസാധാരണമായ പെരുമാറ്റങ്ങളെ നിരീക്ഷിക്കുക എന്നിവയിലൂടെയാണ് ഇവൻ ഭീഷണികളെ കണ്ടെത്തുന്നത്. ഒരു ഭീഷണി കണ്ടെത്തിയാൽ, IDPS ഉടൻ തന്നെ അലാറം മുഴക്കുകയോ, ആ ദോഷകരമായ ട്രാഫിക് ബ്ലോക്ക് ചെയ്യുകയോ, കണക്ഷൻ വിച്ഛേദിക്കുകയോ, അല്ലെങ്കിൽ ഭീഷണിയുടെ ഉറവിടം തടയുകയോ പോലുള്ള നടപടികൾ സ്വീകരിക്കുന്നു. ഫയർവാളുകൾക്ക് പോലും കണ്ടെത്താൻ കഴിയാത്തതോ, അവയെ മറികടന്ന് വരുന്നതോ ആയ സങ്കീർണ്ണമായ ആക്രമണങ്ങളെ (പ്രത്യേകിച്ച് നെറ്റ്‌വർക്കിനുള്ളിൽ നടക്കുന്നവ) കണ്ടെത്താനും തടയാനും IDPS സഹായിക്കും. തത്സമയം ഭീഷണികളെ പ്രതിരോധിക്കാൻ ഇത് അത്യാധുനിക സംരക്ഷണം നൽകുന്നുണ്ട്. ശരിക്കും നമ്മുടെ ഡിജിറ്റൽ ലോകത്തിന് ഒരു അദൃശ്യ കവചം പോലെയാണ് IDPS പ്രവർത്തിക്കുന്നത്.

ഡേറ്റയുടെ രഹസ്യ കോഡ്: എൻക്രിപ്ഷൻ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഒരു അടിസ്ഥാന ഘടകമാണ് നമ്മുടെ എൻക്രിപ്ഷൻ. ഇതിനെ നമുക്കൊരു രഹസ്യ കോഡ് എന്ന് വിളിക്കാം! നമ്മുടെ ഡേറ്റയെ ആരും അനുവാദമില്ലാതെ വായിക്കുന്നത് തടയുകയാണ് എൻക്രിപ്ഷന്റെ പ്രധാന പണി. ഇവൻ ഡേറ്റയെ നമുക്ക് വായിക്കാൻ പറ്റാത്ത ഒരു രൂപത്തിലേക്ക് (ഇതിനെ നമ്മൾ സിഫർടെക്സ്റ്റ് എന്ന് പറയും) മാറ്റിയെഴുതും. ശരിയായ ഒരു താക്കോൽ (കീ) ഉപയോഗിച്ച് മാത്രമേ ഈ കോഡാക്കിയ ഡേറ്റയെ വീണ്ടും വായിക്കാവുന്ന സാധാരണ രൂപത്തിലേക്ക് (പ്ലെയിൻടെക്സ്റ്റ്) മാറ്റിയെടുക്കാൻ പറ്റൂ. ഡേറ്റയുടെ രഹസ്യസ്വഭാവം, കൃത്യത, ആധികാരികത എന്നിവയെല്ലാം ഉറപ്പാക്കുന്നത് ഈ ടെക്നോളജിയാണ്.

എൻക്രിപ്ഷൻ എന്നാൽ, ഒരു അൽഗോരിതം (Encryption Algorithm) ഉപയോഗിച്ച് ഡേറ്റയെ വായിക്കാൻ പറ്റാത്ത രീതിയിലേക്ക് മാറ്റുന്ന പരിപാടിയാണ്. ഈ മാറ്റത്തിന് ഒരു എൻക്രിപ്ഷൻ കീ (Key) ആവശ്യമാണ്. ഈ കീ ഉണ്ടെങ്കിൽ മാത്രമേ ഡേറ്റ സുരക്ഷിതമാക്കാനും, പിന്നീട് അത് തിരിച്ച് ഡീക്രിപ്റ്റ് ചെയ്യാനും പറ്റൂ. ഡേറ്റ കൈമാറ്റം ചെയ്യുമ്പോഴും (data in transit), കംപ്യൂട്ടറുകളിൽ സൂക്ഷിക്കുമ്പോഴും (data at rest), ആപ്ലിക്കേഷൻ ഉപയോഗിക്കുമ്പോഴും ഒക്കെ ഈ എൻക്രിപ്ഷൻ വ്യാപകമായി ഉപയോഗിക്കാറുണ്ട്. ഉദാഹരണത്തിന്, നമ്മൾ വെബ്സൈറ്റുകൾ സന്ദർശിക്കുമ്പോൾ വെബ് അഡ്രസ്സിന്റെ മുന്നിൽ കാണുന്ന https കണ്ടിട്ടില്ലേ? അവിടെ SSL/TLS സർട്ടിഫിക്കറ്റുകൾ നമ്മുടെ ഡേറ്റാ കൈമാറ്റത്തെ എൻക്രിപ്റ്റ് ചെയ്യുന്നുണ്ട്. അതുപോലെ, വെർച്വൽ പ്രൈവറ്റ് നെറ്റ്‌വർക്കുകൾ (VPN) ഉപയോഗിക്കുമ്പോൾ ഡേറ്റ എൻക്രിപ്റ്റ് ചെയ്യപ്പെടും. അതുപോലെ, ഹാർഡ് ഡ്രൈവുകൾ എൻക്രിപ്റ്റ് ചെയ്യുന്നത്, നമ്മുടെ ഡേറ്റ ചോർന്നുപോയാൽ പോലും വിവരങ്ങൾ ദുരുപയോഗം ചെയ്യുന്നത് തടയാൻ സഹായിക്കും. ഇതുപോലുള്ള എൻക്രിപ്ഷൻ ഡേറ്റയുടെ രഹസ്യസ്വഭാവം (Confidentiality) ഉറപ്പാക്കുന്നു. അതുകൊണ്ട്, നമ്മുടെ ഡേറ്റ ചോർത്തപ്പെട്ടാൽ പോലും, അത് എൻക്രിപ്റ്റ് ചെയ്തിരിക്കുന്നതുകൊണ്ട് അനധികൃതമായി ആർക്കും അത് വായിക്കാനോ ദുരുപയോഗം ചെയ്യാനോ കഴിയില്ല. ഇത് ഡേറ്റാ ചോർച്ച മൂലമുണ്ടാകുന്ന നഷ്ടങ്ങളുടെ വ്യാപ്തി ഒരുപാട് കുറയ്ക്കാൻ സഹായിക്കും. അതുകൊണ്ട്, നമ്മുടെ ഡിജിറ്റൽ ജീവിതത്തിൽ എൻക്രിപ്ഷന് വലിയ പ്രാധാന്യമുണ്ട്, അല്ലേ?

സൈബർ സുരക്ഷയിൽ ഏറ്റവും എളുപ്പത്തിൽ വീഴുന്ന കണ്ണി പലപ്പോഴും മനുഷ്യരാണ്. അറിവില്ലായ്മ കാരണം നമ്മൾ വരുത്തുന്ന പിഴവുകൾ വലിയ സൈബർ ആക്രമണങ്ങൾക്ക് കാരണമായേക്കാം.

ഡിജിറ്റൽ ലോകത്ത് ആര്, എപ്പോൾ, എവിടേക്ക്? IAM പറഞ്ഞുതരും

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ മറ്റൊരു അവിഭാജ്യ ഘടകമാണ് നമ്മുടെ ഐഡന്റിറ്റി ആൻഡ് ആക്സസ് മാനേജ്മെന്റ് (IAM). 'ആരാണ് ശരിയായ ആൾ? ഏത് സമയത്താണ് അവർക്ക് പ്രവേശനം വേണ്ടത്? എവിടെയാണ് അവർക്ക് പോകേണ്ടത്?' എന്നൊക്കെ കൃത്യമായി തീരുമാനിക്കുന്ന ഒരു ഗേറ്റ് കീപ്പർ ഇവനാണ്. ആളുകളുടെ വിവരങ്ങൾ പരിശോധിച്ച്, അവർക്ക് അനുവാദമുള്ള സ്ഥലങ്ങളിലേക്ക് മാത്രം കയറ്റിവിട്ട്, അനധികൃതമായി ആരും കടന്നുപോകാതെ തടയുന്ന പണിയാണ് IAM-ന്.ഈ IAM ഉള്ളതുകൊണ്ട് നമ്മുടെ സുരക്ഷ കൂടും, കാര്യങ്ങൾ വേഗത്തിൽ നടക്കും, പിന്നെ നിയമപരമായ കാര്യങ്ങളൊക്കെ കൃത്യമായി പാലിക്കുകയും ചെയ്യാം. ഒരു സ്ഥാപനത്തിലെ ഡിജിറ്റൽ കാര്യങ്ങളിലേക്ക് ആർക്കൊക്കെ കയറാം എന്ന് തീരുമാനിക്കുന്ന നയങ്ങളെയും ടൂളുകളെയും ഒരുമിച്ച് നിർത്തുന്ന ഒരു വലിയ സംവിധാനമാണിത്. ജീവനക്കാർ, ഉപഭോക്താക്കൾ, പങ്കാളികൾ ഇവരെല്ലാം ആരാണെന്ന് തിരിച്ചറിഞ്ഞ്, അവരുടെ ഐഡന്റിറ്റി ഉറപ്പിച്ച ശേഷം, വേണ്ടത്ര അനുമതി നൽകുകയോ തടയുകയോ ചെയ്യും.

IAM സിസ്റ്റങ്ങൾ എന്തൊക്കെയാ ചെയ്യുന്നത് എന്നറിയാമോ? ആൾ ആരാണെന്ന് ഉറപ്പുവരുത്തുക (ഓതന്റിക്കേഷൻ), അവർക്ക് എന്ത് ചെയ്യാനുള്ള അനുമതിയുണ്ടെന്ന് തീരുമാനിക്കുക (ഓതറൈസേഷൻ), പിന്നെ ഈ ഐഡന്റിറ്റി സംബന്ധിച്ച കാര്യങ്ങൾ മൊത്തത്തിൽ കൈകാര്യം ചെയ്യുക എന്നിവയെല്ലാം ഇതിൽപ്പെടും. ഒന്നിലധികം രീതികളിൽ ആളുകളെ തിരിച്ചറിയുന്ന മൾട്ടി-ഫാക്ടർ ഓതന്റിക്കേഷൻ (MFA), ഒരു തവണ ലോഗിൻ ചെയ്താൽ എല്ലാ സിസ്റ്റങ്ങളിലേക്കും കയറാൻ പറ്റുന്ന സിംഗിൾ സൈൻ-ഓൺ (SSO), പാസ്വേഡുകൾ കൈകാര്യം ചെയ്യുന്ന സിസ്റ്റങ്ങൾ, ഓരോ സ്ഥാനത്തിനനുസരിച്ച് പ്രവേശനം നൽകുന്ന റോൾ-ബേസ്ഡ് ആക്സസ് കൺട്രോൾ (RBAC) ഇതൊക്കെ IAM-ന്റെ ഭാഗമാണ്.ഡിജിറ്റൽ കാര്യങ്ങളിലേക്ക് ആര് കയറുന്നു, അവർക്ക് എന്തൊക്കെ ചെയ്യാനുള്ള അധികാരമുണ്ട് എന്നൊക്കെ കൃത്യമായി നിയന്ത്രിക്കുന്നതുകൊണ്ട് അനധികൃത പ്രവേശനം, ഡേറ്റാ ചോർച്ച, ദുരുപയോഗം എന്നിവ യെല്ലാം തടയാൻ സാധിക്കും. അതുകൊണ്ട്, സുരക്ഷാ നിയമങ്ങൾ കൃത്യമായി നടപ്പിലാക്കാനും IAM വലിയൊരു സഹായമാണ്.

സൈബർ ലോകത്തെ 'രക്ഷാകവചം': സുരക്ഷാ അവബോധ പരിശീലനം

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഏറ്റവും അത്യാവശ്യമായ ഒരു ഘടകമാണ് സുരക്ഷാ അവബോധ പരിശീലനം (Security Awareness Training). സൈബർ ഭീഷണികളെക്കുറിച്ച് നമ്മളെയെല്ലാം ബോധവാന്മാരാക്കുകയും, ഡിജിറ്റൽ ലോകത്ത് എങ്ങനെ സുരക്ഷിതമായി പെരുമാറണമെന്ന് പഠിപ്പിക്കുകയും ചെയ്യുന്ന ഒന്നാണിത്.ഒരു സ്ഥാപനത്തിന്റെ സുരക്ഷയിൽ ഏറ്റവും ദുർബലമായ കണ്ണിയാകാൻ സാധ്യതയുള്ളത് മനുഷ്യരാണ്. അതുകൊണ്ട്, നമ്മളോരോരുത്തരെയും ശക്തിപ്പെടുത്താൻ ഈ പരിശീലനം നിർണായകമാണ്. ഫിഷിംഗ്, മാൽവെയർ, സോഷ്യൽ എഞ്ചിനീയറിംഗ് പോലുള്ള ആക്രമണങ്ങളെ തിരിച്ചറിയാനും അവയെ പ്രതിരോധിക്കാനും ഈ പരിശീലനം നമ്മളെ (ജീവനക്കാരെയും ഉപഭോക്താക്കളെയും) പ്രാപ്തരാക്കുന്നു.ഈ പരിശീലനം വഴി എന്തൊക്കെയാണ് പഠിപ്പിക്കുന്നതെന്നോ? ഫിഷിംഗ് ഇമെയിലുകൾ എങ്ങനെ തിരിച്ചറിയാം, സോഷ്യൽ എഞ്ചിനീയറിംഗ് തന്ത്രങ്ങളിൽ കുടുങ്ങാതെ എങ്ങനെ ശ്രദ്ധിക്കാം, ശക്തമായ പാസ്വേഡുകൾ എങ്ങനെ ഉണ്ടാക്കാം, സുരക്ഷിതമല്ലാത്ത വെബ്സൈറ്റുകൾ എങ്ങനെ ഒഴിവാക്കാം എന്നിങ്ങനെ പല കാര്യങ്ങളും ഇതിൽ ഉൾപ്പെടും. ചിലപ്പോൾ, യഥാർത്ഥ സാഹചര്യങ്ങൾ പോലെ തോന്നിക്കുന്ന സിമുലേഷൻ പരിശീലനങ്ങളും ഇതിൽ ഉണ്ടാവാറുണ്ട്.

സൈബർ സുരക്ഷയിൽ ഏറ്റവും എളുപ്പത്തിൽ വീഴുന്ന കണ്ണി പലപ്പോഴും മനുഷ്യരാണ്. അറിവില്ലായ്മ കാരണം നമ്മൾ വരുത്തുന്ന പിഴവുകൾ വലിയ സൈബർ ആക്രമണങ്ങൾക്ക് കാരണമായേക്കാം. അതുകൊണ്ട്, ഫിഷിംഗ്, സോഷ്യൽ എഞ്ചിനീയറിംഗ് പോലുള്ള ആക്രമണങ്ങളെ തടയാൻ ഉപയോക്താക്കൾക്ക് ശരിയായ അവബോധം നൽകുന്നതാണ് ഏറ്റവും ഫലപ്രദമായ മാർഗ്ഗങ്ങളിലൊന്ന്.ഫിഷിംഗ് സിമുലേഷനുകൾ, രസകരമായ ഗെയിമിഫിക്കേഷൻ രീതികൾ, AI ഉപയോഗിച്ചുള്ള പഠന മൊഡ്യൂളുകൾ എന്നിവയിലൂടെയൊക്കെയാണ് ഈ പരിശീലനം നൽകുന്നത്. ഇത് നമ്മളെ സുരക്ഷിതമായ ഡിജിറ്റൽ ശീലങ്ങൾ വളർത്തിയെടുക്കാൻ സഹായിക്കും. നമ്മുടെ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിൽ ഏറ്റവും പ്രധാനപ്പെട്ട ഒരു ആയുധം ഈ 'അവബോധം' തന്നെയാണെന്ന് പറയാം.

ഡേറ്റയുടെ 'ഇൻഷുറൻസ്': ബാക്കപ്പ് ആൻഡ് റിക്കവറി സിസ്റ്റം

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ ഒരു ജീവൻ രക്ഷാ കവചമാണ് ബാക്കപ്പ് ആൻഡ് റിക്കവറി സിസ്റ്റം. സൈബർ ആക്രമണങ്ങൾ വന്നാലോ, ഹാർഡ്വെയർ തകരാറിലായാലോ, നമ്മൾ അറിയാതെ വല്ല തെറ്റും പറ്റിയാലോ, അല്ലെങ്കിൽ പ്രകൃതി ദുരന്തങ്ങൾ ഉണ്ടായാലോ ഒക്കെ നമ്മുടെ ഡേറ്റയെ രക്ഷിക്കുകയും, ആവശ്യമുള്ളപ്പോൾ പഴയപടിയാക്കുകയും ചെയ്യുന്നത് ഇവനാണ്. ഒരു ജീവനുള്ള ശരീരത്തിലെ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ മറ്റൊരു സൂപ്പർ സ്റ്റാറാണ് സെക്യൂരിറ്റി ഇൻഫർമേഷൻ ആൻഡ് ഇവന്റ് മാനേജ്മെന്റ് (SIEM). ഒരു വലിയ നിരീക്ഷണ കേന്ദ്രം പോലെയാണ് ഇവൻ പ്രവർത്തിക്കുന്നത്.

രോഗപ്രതിരോധ സംവിധാനം പോലെ, ഈ സിസ്റ്റം നമ്മുടെ ഡേറ്റ എപ്പോഴും ലഭ്യമാണെന്നും കേടുപാടില്ലാതെ ഇരിപ്പുണ്ടെന്നും ഉറപ്പുവരുത്തും. ബിസിനസ് കാര്യങ്ങൾ തടസ്സമില്ലാതെ മുന്നോട്ട് കൊണ്ടുപോകാനും (Business Continuity) ഇവൻ സഹായിക്കും. ബാക്കപ്പ് ആൻഡ് റിക്കവറി സിസ്റ്റം ചെയ്യുന്നത് എന്താണെന്നോ? നമ്മുടെ ഡേറ്റയുടെ പകർപ്പുകൾ (ബാക്കപ്പുകൾ) ഉണ്ടാക്കുകയും, ഡേറ്റ നഷ്ടപ്പെടുകയോ കേടുപാടുകൾ സംഭവിക്കുകയോ ചെയ്യുമ്പോൾ ആ പകർപ്പുകൾ ഉപയോഗിച്ച് എല്ലാം പഴയപടിയാക്കുകയും (Recovery) ചെയ്യുന്ന ഒരു വലിയ പ്രക്രിയയാണിത്. ഡേറ്റ സുരക്ഷിതമായി സൂക്ഷിക്കാനും, നമ്മുടെ ബിസിനസ് പ്രവർത്തനങ്ങൾ തടസ്സമില്ലാതെ തുടരാനും ഇവൻ സഹായിക്കും. ഈ ബാക്കപ്പുകൾ നമ്മുടെ കംപ്യൂട്ടറിൽ തന്നെയോ, ക്ലൗഡിലോ, അല്ലെങ്കിൽ രണ്ടും ചേർന്ന ഹൈബ്രിഡ് രീതിയിലോ ഒക്കെ സൂക്ഷിക്കാം.

കൃത്യമായ ഇടവേളകളിൽ നമ്മുടെ ഡേറ്റയുടെയും സിസ്റ്റം ഫയലുകളുടെയും പകർപ്പുകൾ എടുത്ത് മറ്റൊരു സ്ഥലത്ത് (ക്ലൗഡിലോ, എക്സ്റ്റേണൽ ഹാർഡ് ഡ്രൈവിലോ, ടേപ്പുകളിലോ ഒക്കെ) സൂക്ഷിക്കും. റാൻസംവെയർ പോലുള്ള ആക്രമണങ്ങൾ വന്നാൽ, പണം കൊടുക്കാതെ, അവസാനമായി എടുത്ത സുരക്ഷിതമായ ബാക്കപ്പിൽ നിന്ന് നമ്മുടെ ഡേറ്റയും സിസ്റ്റവും വീണ്ടെടുക്കാൻ (recover) ഇവൻ സഹായിക്കും. വലിയ ദുരന്തങ്ങൾ ഉണ്ടായാൽ പോലും ബിസിനസ് പ്രവർത്തനങ്ങൾ നിർത്താതെ മുന്നോട്ട് പോകുന്നു എന്ന് ഉറപ്പാക്കാൻ ഡിസാസ്റ്റർ റിക്കവറി പ്ലാനുകളും (DRP) ഇവന്റെ ഭാഗമായിട്ടുണ്ട്.സൈബർ ആക്രമണങ്ങൾ, പ്രകൃതിദുരന്തങ്ങൾ, മനുഷ്യ പിഴവുകൾ, ഹാർഡ്വെയർ തകരാറുകൾ എന്നിവ കാരണം ഡേറ്റ നഷ്ടപ്പെട്ടാൽ അതിൽ നിന്ന് കരകയറാനുള്ള ഒരു നിർണായക വഴിയാണ് ഈ സിസ്റ്റം. ബിസിനസ് തടസ്സമില്ലാതെ മുന്നോട്ട് പോകാൻ ഇത് വലിയ പങ്കുവഹിക്കുന്നു. സാധാരണ കംപ്യൂട്ടറുകൾക്കും ക്ലൗഡ് സംവിധാനങ്ങൾക്കും യോജിച്ച പലതരം പരിഹാരങ്ങൾ ഇന്നുണ്ട്. അതുകൂടാതെ, AI ഉപയോഗിച്ചുള്ള സംവിധാനങ്ങൾ, DRaaS (Disaster Recovery as a Service) പോലുള്ള പുതിയ ടെക്നോളജികൾ എന്നിവയെല്ലാം ഇന്നത്തെ സൈബർ ഭീഷണികളെ ചെറുക്കാൻ സഹായിക്കുന്നുണ്ട്.അതുകൊണ്ട്, നമ്മുടെ ഡിജിറ്റൽ വിവരങ്ങൾക്ക് ഒരു 'ഇൻഷുറൻസ്' പോലെയാണ് ബാക്കപ്പ് ആൻഡ് റിക്കവറി സിസ്റ്റം പ്രവർത്തിക്കുന്നത്.

ഡിജിറ്റൽ ലോകത്തെ 'നിരീക്ഷണ ക്യാമറ': SIEM

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ മറ്റൊരു സൂപ്പർ സ്റ്റാറാണ് സെക്യൂരിറ്റി ഇൻഫർമേഷൻ ആൻഡ് ഇവന്റ് മാനേജ്മെന്റ് (SIEM). ഒരു വലിയ നിരീക്ഷണ കേന്ദ്രം പോലെയാണ് ഇവൻ പ്രവർത്തിക്കുന്നത്. ഒരു സ്ഥാപനത്തിന്റെ മുഴുവൻ കംപ്യൂട്ടർ സംവിധാനങ്ങളിൽ നിന്നും വരുന്ന സുരക്ഷാ വിവരങ്ങൾ ഇവൻ ശേഖരിച്ച്, വിശകലനം ചെയ്യും. എന്നിട്ട്, എന്തെങ്കിലും ഭീഷണി കണ്ടാൽ ഉടൻ തന്നെ തിരിച്ചറിഞ്ഞ് അതിനോട് പ്രതികരിക്കും. സൈബർ ആക്രമണങ്ങൾ, അകത്ത് നിന്നുള്ള പ്രശ്നങ്ങൾ, നയങ്ങൾ തെറ്റിക്കുന്നത് ഇതൊക്കെ കണ്ടെത്താൻ SIEM സഹായിക്കും, നമ്മുടെ സ്ഥാപനങ്ങളെ സുരക്ഷിതമായി നിർത്തുകയും ചെയ്യും. SIEM എന്ന് പറയുന്നത് ഒരുതരം സോഫ്റ്റ്വെയറോ സേവനമോ ആണ്. ഒരു സ്ഥാപനത്തിന്റെ നെറ്റ്വർക്കുകൾ, സെർവറുകൾ, ആപ്ലിക്കേഷനുകൾ എന്നിങ്ങനെയുള്ള എല്ലാ IT സംവിധാനങ്ങളിൽ നിന്നും വരുന്ന ലോഗുകളും ഓരോ സംഭവങ്ങളെയും (ഇവന്റുകൾ) ഇവൻ ശേഖരിക്കും. എന്നിട്ട്, തത്സമയം അതായത് ലൈവായി വിശകലനം ചെയ്ത് സുരക്ഷാ ഭീഷണികൾ കണ്ടെത്തുകയും, ഓഡിറ്റിംഗിനും നിയമപരമായ ആവശ്യങ്ങൾക്കും വേണ്ടി റിപ്പോർട്ടുകൾ ഉണ്ടാക്കുകയും ചെയ്യും.

എന്തൊക്കെയാണ് SIEM സിസ്റ്റം ചെയ്യുന്നതെന്നോ? എല്ലാ ലോഗ് ഡേറ്റയും ശേഖരിക്കും, അതിനെ സാധാരണ നിലയുമായി താരതമ്യം ചെയ്ത് അസ്വാഭാവികമായ പ്രവർത്തനങ്ങൾ കണ്ടെത്തുകയും, സുരക്ഷാ ഭീഷണികളെ തിരിച്ചറിയുകയും ചെയ്യും. എന്നിട്ട് സുരക്ഷാ മുന്നറിയിപ്പുകൾ (അലേർട്ടുകൾ) നൽകുകയും, സംഭവങ്ങളെക്കുറിച്ച് റിപ്പോർട്ടുകൾ തയ്യാറാക്കുകയും ചെയ്യും. പല സുരക്ഷാ സംവിധാനങ്ങളിൽ നിന്നുള്ള വിവരങ്ങൾ ഒരുമിച്ച് വിശകലനം ചെയ്യുന്നതുകൊണ്ട്, സങ്കീർണ്ണമായ ആക്രമണങ്ങളെയും ഭീഷണികളെയും ഇവന് വേഗത്തിൽ കണ്ടെത്താൻ കഴിയും. സുരക്ഷാ പ്രശ്നങ്ങളെക്കുറിച്ച് SIEM നമുക്ക് കൃത്യമായ ഒരു ചിത്രം തരും. ഭീഷണികളെ വേഗത്തിൽ കണ്ടുപിടിക്കാനും അവയ്ക്ക് പ്രതിവിധി കണ്ടെത്താനും ഇത് സഹായിക്കും. അതുകൊണ്ട് തന്നെ സുരക്ഷാ നിരീക്ഷണം, ഭീഷണി കണ്ടെത്തൽ, സുരക്ഷാ സംഭവങ്ങളെക്കുറിച്ചുള്ള അന്വേഷണം എന്നിവയ്ക്കെല്ലാം ഇത് അത്യാവശ്യമാണ്. ഫിഷിംഗ്, മാൽവെയർ, DDoS ആക്രമണങ്ങൾ എന്നിവയെല്ലാം ഇവന് വേഗത്തിൽ തിരിച്ചറിയാൻ കഴിയും. പക്ഷേ, ഒരു കാര്യം ശ്രദ്ധിക്കണം; SIEM ഇൻസ്റ്റാൾ ചെയ്യാനും കൈകാര്യം ചെയ്യാനും നല്ല സാങ്കേതിക അറിവ് വേണം. ലൈസൻസിംഗ്, വേണ്ടുന്ന സംവിധാനങ്ങൾ, പരിപാലനം എന്നിവയൊക്കെ കുറച്ച് ചെലവേറിയതാണ്. AI (നിർമ്മിത ബുദ്ധി), ക്ലൗഡ്, SOAR (Security Orchestration, Automation and Response) പോലുള്ള പുതിയ ട്രെൻഡുകൾ SIEM-ന്റെ കഴിവുകൾ ഒരുപാട് കൂട്ടുന്നുണ്ട്. എങ്കിലും, ഇത് കൃത്യമായി

ബിസിഐ വഴി യാത്രികർക്ക് റോബോട്ടിക് സഹായികളെ നിയന്ത്രിച്ച് ഭക്ഷണം തയ്യാറാക്കാനും കഴിയും. റോബോട്ടിനെ മനസ്സ് കൊണ്ട് നിയന്ത്രിച്ച് ഒരു ബഹിരാകാശ കോളനി നിർമിക്കാം.

നടപ്പിലാക്കാൻ നല്ല വൈദഗ്ധ്യവും വിഭവങ്ങളും ആവശ്യമാണ്.

സോഫ്റ്റ്വെയറുകൾക്ക് 'പരിരക്ഷ': പാച്ച് മാനേജ്മെന്റ്

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ ഒരു പ്രധാനപ്പെട്ട ഘടകമാണ് പാച്ച് മാനേജ്മെന്റ്. സോഫ്റ്റ്വെയറുകൾ, ഓപ്പറേറ്റിംഗ് സിസ്റ്റങ്ങൾ, ആപ്ലിക്കേഷനുകൾ, ഫേംവെയറുകൾ എന്നിവയിലൊക്കെയുള്ള സുരക്ഷാ പ്രശ്നങ്ങൾ (വൾനറബിലിറ്റികൾ) പരിഹരിക്കാൻ സോഫ്റ്റ്വെയർ അപ്ഡേറ്റുകൾ അഥവാ പാച്ചുകൾ കണ്ടെത്തുകയും, പരിശോധിക്കുകയും, ഇൻസ്റ്റാൾ ചെയ്യുകയും ചെയ്യുന്ന പരിപാടിയാണിത്. നമ്മുടെ ശരീരത്തിന്റെ പ്രതിരോധ സംവിധാനം പോലെ, ഈ പാച്ച് മാനേജ്മെന്റ് സൈബർ ആക്രമണങ്ങളിൽ നിന്ന് സിസ്റ്റങ്ങളെ സംരക്ഷിക്കുകയും, ഡേറ്റാ ചോർച്ച, മാൽവെയർ, റാൻസംവെയർ എന്നിവയെ തടയുകയും ചെയ്യും. പാച്ച് മാനേജ്മെന്റ് ചെയ്യുന്നത് എന്താണെന്നോ? ഒരു സ്ഥാപനത്തിലെ കംപ്യൂട്ടറുകളിലെയും, സോഫ്റ്റ്വെയറുകളിലെയും, മറ്റ് ഉപകരണങ്ങളിലെയും പാച്ചുകൾ (അതായത്, സുരക്ഷാ അപ്ഡേറ്റുകൾ, ബഗ്ഗുകൾ തീർക്കാനുള്ള പരിഹാരങ്ങൾ, പുതിയ ഫീച്ചറുകൾ) കൃത്യമായി ഇൻസ്റ്റാൾ ചെയ്യുന്ന ഒരു പ്രക്രിയയാണിത്. Microsoft, Adobe, Cisco പോലുള്ള സോഫ്റ്റ്വെയർ കമ്പനികളാണ് ഈ പാച്ചുകൾ പുറത്തിറക്കുന്നത്. ഇവ സുരക്ഷാ പ്രശ്നങ്ങൾ പരിഹരിക്കാനും കാര്യങ്ങൾ കൂടുതൽ മെച്ചപ്പെടുത്താനും സഹായിക്കും. സുരക്ഷാ പിഴവുകളെക്കുറിച്ച് എപ്പോഴും നിരീക്ഷിക്കുക, പുതിയ പാച്ചുകൾ വന്നാൽ അത് കണ്ടുപിടിക്കുക, ഏതൊക്കെ സിസ്റ്റങ്ങൾക്ക് ഈ പാച്ചുകൾ ആവശ്യമുണ്ടെന്ന് സ്കാൻ ചെയ്ത് കണ്ടെത്തുക, അവ ഡൗൺലോഡ് ചെയ്ത് ഇൻസ്റ്റാൾ ചെയ്യുക, ഇൻസ്റ്റാൾ ചെയ്തത് വിജയകരമാണെന്ന് ഉറപ്പുവരുത്തുക ഇതൊക്കെയാണ് ഇതിൽ ഉൾപ്പെടുന്നത്. സൈബർ ആക്രമണങ്ങൾ പലപ്പോഴും സോഫ്റ്റ്വെയറുകളിലെ അറിയപ്പെടുന്ന സുരക്ഷാ പിഴവുകൾ മുതലെടുത്താണ് നടക്കാറുള്ളത്. പാച്ചുകൾ കൃത്യസമയത്ത് ഇൻസ്റ്റാൾ ചെയ്യുന്നത് ഈ പിഴവുകൾ അടയ്ക്കുകയും ആക്രമണത്തിനുള്ള സാധ്യത കുറയ്ക്കുകയും ചെയ്യും. ഇത് സിസ്റ്റങ്ങളുടെ സുരക്ഷയും കാര്യക്ഷമതയും നിലനിർത്താൻ അത്യാവശ്യമാണ്.

എന്നാൽ, വലിയ നെറ്റ്വർക്കുകളിൽ ഒരുപാട് കംപ്യൂട്ടറുകളിലും സോഫ്റ്റ്വെയറുകളിലും പാച്ച് ചെയ്യുന്നത് അല്പം വെല്ലുവിളിയാണ്. കൂടാതെ, ഓരോ പാച്ചും ടെസ്റ്റ് ചെയ്യാനും ഇൻസ്റ്റാൾ ചെയ്യാനും നിരീക്ഷിക്കാനുമൊക്കെ സമയവും നല്ല അറിവും ആവശ്യമാണ്. ചിലപ്പോൾ, പാച്ചുകൾ പുറത്തിറങ്ങുന്നതിന് മുമ്പു തന്നെ ആക്രമണങ്ങൾ സംഭവിക്കാനും സാധ്യതയുണ്ട്. ഓട്ടോമേറ്റഡ് ടൂളുകൾ, ക്ലൗഡ് വഴിയുള്ള പരിഹാരങ്ങൾ, ഭീഷണികളെക്കുറിച്ചുള്ള വിവരങ്ങൾ നൽകുന്ന ത്രെറ്റ് ഇന്റലിജൻസ് എന്നിവയെല്ലാം ഈ പ്രക്രിയയെ കൂടുതൽ എളുപ്പത്തിലാക്കുന്നുണ്ട്. പക്ഷേ, ഇത് വിജയകരമായി നടപ്പിലാക്കാൻ സാങ്കേതികപരമായ അറിവും ശ്രദ്ധയും അത്യാവശ്യം തന്നെയാണ്.

ഡിജിറ്റൽ ലോകത്തെ 'അതിർത്തികൾ': നെറ്റ്വർക്ക് സെഗ്മെന്റേഷൻ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ ഒരു പ്രധാന ഘടകമാണ് നെറ്റ്വർക്ക് സെഗ്മെന്റേഷൻ. ഇതൊരു ഓർഗനൈസേഷന്റെ വലിയ നെറ്റ്വർക്കിനെ ചെറിയ, വേർതിരിച്ച, സുരക്ഷിതമായ ഭാഗങ്ങളായി (അതായത്, സെഗ്മെന്റുകളായി) വിഭജിക്കുന്ന പരിപാടിയാണ്. നമ്മുടെ ശരീരത്തിലെ കോശങ്ങൾ കൃത്യമായി വേർതിരിക്കപ്പെട്ടിരിക്കുന്നത് പോലെയാണിത്. സൈബർ ആക്രമണങ്ങൾ ഒരു ഭാഗത്ത് നടന്നാൽ അത് മറ്റുള്ളവിടങ്ങളിലേക്ക് പടരുന്നത് തടയാനും, ഡേറ്റയുടെ സുരക്ഷ കൂട്ടാനും, നമ്മുടെ IT ലോകത്ത് എന്താണ് നടക്കുന്നത് എന്ന് കൂടുതൽ വ്യക്തമായി മനസ്സിലാക്കാനും നെറ്റ്വർക്ക് സെഗ്മെന്റേഷൻ സഹായിക്കും. ഒരു വലിയ നെറ്റ്വർക്കിനെ ചെറിയ ചെറിയ ഉപ-നെറ്റ്വർക്കുകളായി (സബ്നെറ്റുകളായി) അല്ലെങ്കിൽ സോണുകളായി തിരിക്കുന്ന പ്രക്രിയയാണിത്. ഓരോ ഭാഗത്തിനും അതിന്റേതായ സുരക്ഷാ നിയമങ്ങളും പ്രവേശന നിയന്ത്രണങ്ങളും ഉണ്ടാകും. ഫയർവാളുകൾ, VLAN-കൾ (Virtual Local Area Networks), SDN (Software-Defined Networking) അല്ലെങ്കിൽ മറ്റ് സാങ്കേതികവിദ്യകൾ എന്നിവ ഉപയോഗിച്ചാണ് ഈ വേർതിരിവ് ചെയ്യുന്നത്. അകത്തുനിന്നുള്ളതോ പുറത്തുനിന്നുള്ളതോ ആയ ഭീഷണികളെ നിയന്ത്രിക്കാനും, ഡേറ്റാ ചോർച്ച, റാൻസംവെയർ, മാൽവെയർ

ഒരു ശരീരത്തിലെ പ്രതിരോധ സംവിധാനത്തിന്റെ മുൻനിരയിലുള്ള കോശങ്ങൾ പോലെയാണ് എൻഡ്പോയിന്റ് പ്രൊട്ടക്ഷൻ പ്രവർത്തിക്കുന്നത്. മാൽവെയർ, റാൻസംവെയർ, ഫിഷിംഗ്, അകത്തുനിന്നുള്ള ഭീഷണികൾ എന്നിവയെ തടയുകയും, ഡേറ്റയുടെ സുരക്ഷയും നെറ്റ്വർക്കിന്റെ കൃത്യതയും ഉറപ്പാക്കുകയും ചെയ്യുന്നത് ഇവയാണ്.

എന്നിവ പടരുന്നത് തടയാനും ഇത് സഹായിക്കും.

ഫയർവാളുകൾ, VLAN-കൾ, ആക്സസ് കൺട്രോൾ ലിസ്റ്റുകൾ (ACLs) എന്നിവ ഉപയോഗിച്ച് നെറ്റ്വർക്കിന്റെ വിവിധ ഭാഗങ്ങൾ തമ്മിലുള്ള ആശയവിനിമയം IAM നിയന്ത്രിക്കും. ഉദാഹരണത്തിന്, ജീവനക്കാർ ഉപയോഗിക്കുന്ന നെറ്റ്വർക്ക്, സെർവറുകൾ ഉള്ള നെറ്റ്വർക്ക്, അതിഥികൾക്ക് ഉപയോഗിക്കാനുള്ള നെറ്റ്വർക്ക് എന്നിവയെയെല്ലാം വേർതിരിക്കാം. ഒരു നെറ്റ്വർക്ക് ഭാഗത്ത് ആക്രമണം നടന്നാൽ, അത് മറ്റ് ഭാഗങ്ങളിലേക്ക് അതിവേഗം പടരുന്നത് തടയാൻ സെഗ്മെന്റേഷൻ സഹായിക്കുന്നു. ഇത് ആക്രമണത്തിന്റെ വ്യാപ്തി കുറയ്ക്കുകയും നാശനഷ്ടങ്ങൾ പരിമിതപ്പെടുത്തുകയും ചെയ്യും. കൂടുതൽ പ്രധാനപ്പെട്ട ഡേറ്റയും സിസ്റ്റങ്ങളും ഉള്ള ഭാഗങ്ങൾക്ക് അധിക സുരക്ഷ നൽകാനും ഇത് ഉപയോഗിക്കാം. എങ്കിലും, ഹാർഡ്വെയർ, ഫയർവാളുകൾ, SDN ടൂളുകൾ, നിരീക്ഷണ സംവിധാനങ്ങൾ എന്നിവയെല്ലാം ഇതിന് ആവശ്യമായതുകൊണ്ട് കുറച്ച് ചെലവേറിയതാണ് ഈ പരിപാടി എങ്കിലും, നെറ്റ്വർക്ക് സെഗ്മെന്റേഷൻ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഒരു അവിഭാജ്യ ഘടകം തന്നെയാണ്. ഇത് ഭീഷണികളുടെ വ്യാപനം കുറയ്ക്കുകയും, ഡേറ്റാ സുരക്ഷ കൂട്ടുകയും, നെറ്റ്വർക്ക് ദൃശ്യപരത മെച്ചപ്പെടുത്തുകയും ചെയ്യുന്നു. മൈക്രോ സെഗ്മെന്റേഷൻ, സീറോ ട്രസ്റ്റ്, SDN പോലുള്ള പുതിയ ട്രെൻഡുകൾ ഈ പ്രക്രിയയെ കൂടുതൽ കാര്യക്ഷമമാക്കുന്നുണ്ട്. പക്ഷേ, ഇത് ശരിയായി നടപ്പിലാക്കാൻ നല്ല സാങ്കേതിക അറിവും ശ്രദ്ധയും ആവശ്യമാണ്.

ഡിജിറ്റൽ അതിർത്തിയിലെ 'സേന': എൻഡ്പോയിന്റ് പ്രൊട്ടക്ഷൻ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഏറ്റവും അത്യാവശ്യമുള്ള ഒരു ഘടകമാണ് എൻഡ്പോയിന്റ് പ്രൊട്ടക്ഷൻ. ഇത് എന്താണെന്ന് വെച്ചാൽ, ഒരു സ്ഥാപനത്തിന്റെ നെറ്റ്വർക്കിലുള്ള ലാപ്ടോപ്പുകൾ, ഡെസ്ക്ടോപ്പുകൾ, മൊബൈൽ ഫോണുകൾ, സെർവറുകൾ, എന്തിന് IoT ഉപകരണങ്ങൾ (സ്മാർട്ട് ഗാഡ്ജറ്റുകൾ) വരെ സൈബർ ഭീഷണികളിൽ നിന്ന് സംരക്ഷിക്കുന്ന പരിപാടിയാണിത്. ഒരു ശരീരത്തിലെ പ്രതിരോധ സംവിധാനത്തിന്റെ മുൻനിരയിലുള്ള കോശങ്ങൾ പോലെയാണ് എൻഡ്പോയിന്റ് പ്രൊട്ടക്ഷൻ പ്രവർത്തിക്കുന്നത്. മാൽവെയർ, റാൻസംവെയർ, ഫിഷിംഗ്, അകത്തുനിന്നുള്ള ഭീഷണികൾ എന്നിവയെ തടയുകയും, ഡേറ്റയുടെ സുരക്ഷയും നെറ്റ്വർക്കിന്റെ കൃത്യതയും ഉറപ്പാക്കുകയും ചെയ്യുന്നത് ഇവയാണ്. എൻഡ്പോയിന്റ് പ്രൊട്ടക്ഷൻ എന്നാൽ, ഈ ഉപകരണങ്ങളെ സുരക്ഷിതമാക്കാൻ രൂപകൽപ്പന ചെയ്ത സോഫ്റ്റ്വെയറുകൾ, ഹാർഡ്വെയറുകൾ, നയങ്ങൾ എന്നിവയുടെ ഒരു വലിയ കൂട്ടായ്മയാണ്. സാധാരണ ആന്റിവൈറസിനെക്കാൾ ഒരു പടികൂടി കടന്ന്, മാൽവെയറുകളെ തടയുക, ഭീഷണികളെ കണ്ടെത്തുക, അതിനോട് പ്രതികരിക്കുക, സൈബർ കുറ്റകൃത്യങ്ങളെക്കുറിച്ച് അന്വേഷിക്കുക (ഫോറൻസിക് വിശകലനം) എന്നിങ്ങനെ സമഗ്രമായ സുരക്ഷാ പരിഹാരങ്ങളാണ് ഇത് നൽകുന്നത്. എൻഡ്പോയിന്റ് പ്രൊട്ടക്ഷൻ പ്ലാറ്റ്ഫോമുകൾ (EPP), എൻഡ്പോയിന്റ് ഡിറ്റക്ഷൻ ആൻഡ് റെസ്പോൺസ് (EDR), മൊബൈൽ ഡിവൈസ് മാനേജ്മെന്റ് (MDM) എന്നിവയെല്ലാം ഇതിന്റെ പ്രധാന ഭാഗങ്ങളാണ്.

ആന്റിവൈറസ്/ആന്റി-മാൽവെയർ, എൻഡ്പോയിന്റ് ഡിറ്റക്ഷൻ ആൻഡ് റെസ്പോൺസ് (EDR), ഡേറ്റ എൻക്രിപ്ഷൻ, ഫയർവാൾ, ആപ്ലിക്കേഷൻ കൺട്രോൾ, ഡിവൈസ് കൺട്രോൾ, ഉപയോക്താക്കളുടെ പെരുമാറ്റം നിരീക്ഷിക്കൽ എന്നിവയെല്ലാം എൻഡ്പോയിന്റ് ഉപകരണങ്ങളിൽ നടപ്പിലാക്കും. പ്രത്യേകിച്ച്, EDR സിസ്റ്റങ്ങൾ ഓരോ ഉപകരണത്തിലെയും പ്രവർത്തനങ്ങളെ സസൂക്ഷ്മം നിരീക്ഷിച്ച് ഭീഷണികളെ കണ്ടെത്തുകയും അതിനനുസരിച്ച് പ്രതികരിക്കുകയും ചെയ്യും. സൈബർ ആക്രമണങ്ങൾ പലപ്പോഴും എൻഡ്പോയിന്റ് ഉപകരണങ്ങളിലൂടെയാണ് തുടങ്ങുന്നത്. അതുകൊണ്ട്, ഇവയെ കൃത്യമായി സംരക്ഷിക്കുന്നത് നമ്മുടെ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന് വളരെ നിർണായകമാണ്. റിമോട്ട് വർക്കിംഗ് (ദൂരെയുള്ള സ്ഥലങ്ങളിൽ നിന്ന് ജോലി ചെയ്യുന്നത്) കൂടിയതോടെ എൻഡ്പോയിന്റ് സുരക്ഷയുടെ പ്രാധാന്യം ഒരുപാട് വർദ്ധിച്ചിട്ടുണ്ട്. എന്നാൽ, ഒരുപാട് എൻഡ്പോയിന്റ് ഉപകരണങ്ങളെ ഒരുമിച്ച് കൈകാര്യം ചെയ്യുന്നത് ചിലപ്പോൾ അല്പം വെല്ലുവിളിയാണ്. എങ്കിലും, എൻഡ്പോയിന്റ് പ്രൊട്ടക്ഷൻ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ മുൻനിര പ്രതിരോധമാണ്. AI, EDR, XDR (Extended Detection

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ ഒരു പ്രധാന ഘടകമാണ് ഭീഷണി ഇന്റലിജൻസ് (Threat Intelligence). സൈബർ ഭീഷണികളെക്കുറിച്ചുള്ള വിവരങ്ങൾ ശേഖരിക്കുകയും, അവയെ വിശകലനം ചെയ്ത്, ഒരു സ്ഥാപനത്തെ മുൻകൂട്ടി സംരക്ഷിക്കാൻ സഹായിക്കുകയും ചെയ്യുന്ന ഒരു 'ചാരക്കണ്ണ്' ആണിത്.

and Response), സീറോ ട്രസ്റ്റ് പോലുള്ള പുതിയ ട്രെൻഡുകൾ ഈ സുരക്ഷാ പരിഹാരങ്ങളെ കൂടുതൽ ശക്തമാക്കുന്നുണ്ട്.

സൈബർ ലോകത്തെ 'ചാരക്കണ്ണ്': ത്രെഡ് ഇന്റലിജൻസ്

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ ഒരു പ്രധാന ഘടകമാണ് ഭീഷണി ഇന്റലിജൻസ് (Threat Intelligence). സൈബർ ഭീഷണികളെക്കുറിച്ചുള്ള വിവരങ്ങൾ ശേഖരിക്കുകയും, അവയെ വിശകലനം ചെയ്ത്, ഒരു സ്ഥാപനത്തെ മുൻകൂട്ടി സംരക്ഷിക്കാൻ സഹായിക്കുകയും ചെയ്യുന്ന ഒരു 'ചാരക്കണ്ണ്' ആണിത്. നമ്മുടെ ശരീരത്തിന്റെ പ്രതിരോധ സംവിധാനത്തിന്റെ ബുദ്ധിശക്തിയെപ്പോലെ, ഭീഷണി ഇന്റലിജൻസ് മാൽവെയർ, ഫിഷിംഗ്, റാൻസംവെയർ, APT-കൾ (Advanced Persistent Threats) തുടങ്ങിയ ഭീഷണികളെ മുൻകൂട്ടി തിരിച്ചറിയുകയും, അവയെ നേരിടാനുള്ള തന്ത്രങ്ങൾ മെനയുകയും ചെയ്യുന്നു. സൈബർ ഭീഷണികളെക്കുറിച്ചുള്ള വിവരങ്ങൾ ശേഖരിച്ച്, അതിനെ പ്രയോജനപ്പെടുത്താൻ കഴിയുന്ന 'വിവരങ്ങളാക്കി' മാറ്റുന്ന പ്രക്രിയയാണിത്. ഭീഷണി എവിടെ നിന്ന് വരുന്നു, ആക്രമണത്തിന്റെ രീതികൾ (അതായത്, Tactics, Techniques, and Procedures - TTPs), എന്തൊക്കെയാണ് ദുർബലതകൾ (Vulnerabilities), ആക്രമണകാരികളുടെ ലക്ഷ്യങ്ങൾ എന്നിവയെക്കുറിച്ചുള്ള വിശദാംശങ്ങൾ ഈ വിവരങ്ങളിൽ ഉണ്ടാകും. SIEM, EDR, ഫയർവാളുകൾ എന്നിവയുമായി ചേർന്ന് പ്രവർത്തിക്കുമ്പോൾ, ഭീഷണി ഇന്റലിജൻസ് സ്ഥാപനങ്ങളെ മുൻകരുതൽ നടപടികൾ എടുക്കാനും, ആക്രമണങ്ങൾ ഉണ്ടായാൽ ഉടൻ പ്രതികരിക്കാനും സഹായിക്കും.

സുരക്ഷാ ഫീഡുകൾ, ഗവേഷണ റിപ്പോർട്ടുകൾ, ഡാർക്ക് വെബ് നിരീക്ഷണം, മറ്റ് സുരക്ഷാ കൂട്ടായ്മകൾ എന്നിങ്ങനെ പലയിടങ്ങളിൽ നിന്നും ഭീഷണി സംബന്ധിച്ച വിവരങ്ങൾ ശേഖരിച്ച് ഇവയെ ഉപയോഗയോഗ്യമായ അറിവുകളാക്കി മാറ്റും. ഈ വിവരങ്ങൾ സുരക്ഷാ ടീമുകൾക്ക് പുതിയ ഭീഷണികളെക്കുറിച്ച് മനസ്സിലാക്കാനും, അവയെ പ്രതിരോധിക്കാനുള്ള തന്ത്രങ്ങൾ ഉണ്ടാക്കാനും, നിലവിലുള്ള സുരക്ഷാ സംവിധാനങ്ങൾ മെച്ചപ്പെടുത്താനും സഹായിക്കും. സൈബർ ഭീഷണികൾ ഓരോ നിമിഷവും മാറിക്കൊണ്ടിരിക്കുന്ന ഈ കാലത്ത്, പുതിയ ഭീഷണികളെക്കുറിച്ച് മുൻകൂട്ടി അറിയുന്നത് പ്രതിരോധ നടപടികൾ തയ്യാറാക്കാൻ വലിയ സഹായമാണ്. ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന് ഓരോ ആക്രമണത്തിൽ നിന്നും പഠിക്കാനും, സ്വയം അപ്ഡേറ്റ് ചെയ്യാനും, ഏറ്റവും പുതിയ ഭീഷണികളെ ചെറുക്കാനും ആവശ്യമായ വിവരങ്ങൾ നൽകുന്നത് ഈ ത്രെഡ് ഇന്റലിജൻസാണ്. AI (നിർമ്മിത ബുദ്ധി), SOAR (Security Orchestration, Automation and Response), UEBA (User

ഘടകങ്ങളും (ഫയർവാൾ, ആന്റിവൈറസ്, IDPS, എൻക്രിപ്ഷൻ, IAM, സുരക്ഷാ അവബോധ പരിശീലനം, ബാക്കപ്പ്, ത്രെഡ് ഇന്റലിജൻസ്, നെറ്റ്വർക്ക് സെഗ്മെന്റേഷൻ എന്നിവ) എങ്ങനെയാണ് പ്രവർത്തിക്കുന്നതെന്നും വിശദമായി കണ്ടു. ഒറ്റയ്ക്ക് നിൽക്കുമ്പോൾ ഓരോന്നും ഓരോ സുരക്ഷാ കവചങ്ങളാണെങ്കിൽ പോലും, ഈ ഘടകങ്ങളെല്ലാം ഒരുമിച്ച്, അതായത് ഒരു ടീമായി പ്രവർത്തിക്കുമ്പോഴാണ് നമ്മുടെ ഡിജിറ്റൽ ലോകത്തിന് അതിശക്തമായ ഒരു യഥാർത്ഥ 'പ്രതിരോധശക്തി' ലഭിക്കുന്നത്. ഒരു സൈബർ ആക്രമണം വരുമ്പോൾ, ഇവ ഓരോന്നും അവരവരുടെ പണി കൃത്യമായി ചെയ്യും, അഥവാ ഒന്നിനെ മറികടന്ന് വന്നാൽ അടുത്തവൻ തടയും. അതായത്, അങ്ങനെ ഒരു ബഹുമുഖ പ്രതിരോധം!

നമ്മുടെ ശരീരത്തിലെ രോഗപ്രതിരോധ സംവിധാനം പോലെ തന്നെ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനവും വെറും പ്രതിരോധത്തിൽ ഒതുങ്ങുന്നില്ല. ഭീഷണികളെ മുൻകൂട്ടി തിരിച്ചറിയാനും, അതിനോട് വേഗത്തിൽ പ്രതികരിക്കാനും, ഓരോ ആക്രമണത്തിൽ നിന്നും പാഠം ഉൾക്കൊണ്ട് സ്വയം പഠിക്കാനും, അതിജീവിച്ച് കൂടുതൽ കരുത്തുറ്റതാകാനും ഇതിന് കഴിയും. ഇന്നത്തെ ലോകത്ത് സൈബർ ഭീഷണികൾ അനുദിനം സങ്കീർണ്ണമായിക്കൊണ്ടിരിക്കുമ്പോൾ, വ്യക്തികളുടെ സ്വകാര്യതയും, സ്ഥാപനങ്ങളുടെ പ്രവർത്തനവും, രാജ്യങ്ങളുടെ സുരക്ഷയും ഉറപ്പാക്കാൻ ഇങ്ങനെയൊരു സമഗ്രവും ചലനാത്മകവുമായ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം തീർത്തും അനിവാര്യമാണ്. അപ്പോൾ, ഈയൊരു അത്യാധുനിക ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം നമ്മുടെ ഡിജിറ്റൽ ജീവിതത്തിന് എന്തൊക്കെ തരത്തിലുള്ള പ്രയോജനങ്ങളാണ് നൽകുന്നത്? സൈബർ ലോകത്ത് ഇത് നമുക്ക് നൽകുന്ന ആഴത്തിലുള്ള സുരക്ഷയും മറ്റ് നേട്ടങ്ങളും എന്തൊക്കെയാണെന്ന് അടുത്ത ലേഖനത്തിൽ നമുക്ക് വിശദമായി പരിശോധിക്കാം.

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ പ്രയോജനങ്ങൾ

ഇന്ന് നമ്മുടെ ജീവിതം ഡിജിറ്റൽ ലോകവുമായി അത്രയേറെ അടുത്തുപോയി, അല്ലേ? വിരൽത്തുമ്പിൽ ലോകം നമ്മുടെ മുന്നിൽ നിൽക്കുമ്പോൾ, ഈ ഡിജിറ്റൽ ലോകത്തിന്റെ മറുവശത്ത് ഒളിഞ്ഞിരിക്കുന്ന നിരന്തരമായ ഭീഷണികളെ നമ്മൾ പലപ്പോഴും ശ്രദ്ധിക്കാറില്ല. സൈബർ ആക്രമണങ്ങൾ വ്യക്തികളുടെ സ്വകാര്യതയെ തകർക്കാൻ കഴിയും, ചിലപ്പോൾ വലിയ സ്ഥാപനങ്ങളുടെ അടിത്തറ പോലും ഇളക്കാം. ഈ ഡിജിറ്റൽ യുദ്ധക്കളത്തിൽ നമ്മുടെ സൈബർ ആസ്തികളെ നമ്മൾ എങ്ങനെ സംരക്ഷിക്കും? ഇവിടെയാണ് വളരെ പ്രസക്തിയേറുന്ന ഒരു ആശയം കടന്നുവരുന്നത് – അത് മറ്റൊന്നുമല്ല, നമ്മുടെ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം (Digital Immune System). മനുഷ്യ ശരീരം രോഗങ്ങളെയും അണുക്കളെയും തിരിച്ചറിഞ്ഞ് പോരാടുന്നത് പോലെ, ഡിജിറ്റൽ ലോകത്തെ വൈറസുകളെയും ആക്രമണങ്ങളെയും ചെറുക്കാൻ കഴിവുള്ള ഒരു ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തെക്കുറിച്ചാണ് നമ്മൾ സംസാരിക്കുന്നത്. ഡിജിറ്റൽ ലോകം ഓരോ ദിവസം കഴിയുന്തോറും കൂടുതൽ സങ്കീർണ്ണമായിക്കൊണ്ടിരിക്കുമ്പോൾ, അതിന്റെ സുരക്ഷ ഉറപ്പാക്കാൻ ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഒരു അനിവാര്യതയായി മാറുന്നത് എങ്ങനെയാണെന്നും, അതിന്റെ പ്രധാന പ്രയോജനങ്ങൾ എന്തൊക്കെയാണെന്നും ഉദാഹരണങ്ങൾ സഹിതം നമുക്ക് വിശദമായി ചർച്ച ചെയ്യാം.

1) നേരത്തെയുള്ള ഭീഷണി കണ്ടെത്തൽ: ഒരു 'ഡിറ്റക്ടീവ്' പോലെ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ ഏറ്റവും വലിയ ഗുണങ്ങളിൽ ഒന്നാണ് നേരത്തെയുള്ള ഭീഷണി കണ്ടെത്തൽ. നമ്മളൊക്കെ അറിയാതെ നമ്മുടെ കംപ്യൂട്ടറുകളിലും നെറ്റ്‌വർക്കുകളിലുമൊക്കെ ഒളിഞ്ഞിരിക്കുന്ന സൈബർ ഭീഷണികളെ, നിർമിത ബുദ്ധിയും (AI) മെഷീൻ ലേണിംഗുമൊക്കെ (Machine Learning) ഉപയോഗിച്ച് ഈ സംവിധാനം മുൻകൂട്ടി കണ്ടെത്തും. അതായത്, ഹാക്കിംഗ്, മാൽവെയർ, ഫിഷിംഗ് പോലുള്ള ആക്രമണങ്ങൾ വരുന്നതിന് മുൻപേ ഇവയെ തടഞ്ഞ് നമ്മുടെ പ്രതിരോധം ശക്തിപ്പെടുത്തും. 2020-ൽ ഒരു വലിയ ബാങ്കിംഗ് സ്ഥാപനം, അവരുടെ AI അധിഷ്ഠിത ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഉപയോ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ മറ്റൊരു വലിയ പ്രത്യേകതയാണ് തത്സമയ പ്രതികരണവും ഓട്ടോമേറ്റഡ് പരിഹാരവും. അതായത്, ഒരു ഭീഷണി കണ്ടെത്തിയാൽ, മനുഷ്യന്റെ സഹായം ഒന്നുമില്ലാതെ തന്നെ ഇവൻ ലൈവായി പ്രതികരിക്കുകയും പരിഹാരം നടപ്പിലാക്കുകയും ചെയ്യും.

ഗിച്ച് ഒരു വലിയ ഫിഷിംഗ് ആക്രമണം തടഞ്ഞു. ഉപഭോക്താക്കളുടെ ലോഗിൻ വിവരങ്ങൾ മോഷ്ടിക്കാൻ ശ്രമിച്ച ഒരു വ്യാജ ഇ-മെയിൽ ആക്രമണമായിരുന്നു അത്. പക്ഷേ, ഈ സംവിധാനം അത് തത്സമയം തിരിച്ചറിഞ്ഞ് ബ്ലോക്ക് ചെയ്തു കളഞ്ഞു. ലക്ഷക്കണക്കിന് ആളുകളുടെ ഡേറ്റയാണ് അന്ന് സുരക്ഷിതമായത്. HSBC, JPMorgan Chase, Bank of America പോലുള്ള ലോകോത്തര ബാങ്കുകൾ AI ഉപയോഗിച്ചുള്ള സുരക്ഷാ സംവിധാനങ്ങൾ കൊണ്ടുവന്നത് ഇതുകൊണ്ടൊക്കെയാണ്. ഉദാഹരണത്തിന്, HSBC 2020-ൽ AI അടിസ്ഥാനമാക്കിയുള്ള തട്ടിപ്പ് കണ്ടെത്തൽ സിസ്റ്റങ്ങൾ ഉപയോഗിച്ച് ഫിഷിംഗ്, മാൽവെയർ ആക്രമണങ്ങളിൽ നിന്ന് വലിയൊരു രക്ഷനേടിയതായി റിപ്പോർട്ടുകളുണ്ട്.

2) തത്സമയ പ്രതികരണവും ഓട്ടോമേറ്റഡ് പരിഹാരവും: ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ മറ്റൊരു വലിയ പ്രത്യേകതയാണ് തത്സമയ പ്രതികരണവും ഓട്ടോമേറ്റഡ് പരിഹാരവും. അതായത്, ഒരു ഭീഷണി കണ്ടെത്തിയാൽ, മനുഷ്യന്റെ സഹായം ഒന്നുമില്ലാതെ തന്നെ ഇവൻ ലൈവായി പ്രതികരിക്കുകയും പരിഹാരം നടപ്പിലാക്കുകയും ചെയ്യും. ഇത് നമുക്ക് ഒരുപാട് സമയം ലാഭിച്ചുതരും, കാര്യക്ഷമതയും കൂട്ടും. 2021-ൽ, ആക്സഞ്ചർ (Accenture) എന്ന വലിയൊരു ടെക് കമ്പനിയുടെ ക്ലൗഡ് സേവനത്തിനെതിരെ ഒരു റാൻസംവെയർ ആക്രമണം ഉണ്ടായി. പക്ഷേ, അവരുടെ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ആക്രമണത്തെ ഉടൻ തിരിച്ചറിഞ്ഞ്, ബാധിച്ച സെർവറുകളെ സ്വയമേവ മാറ്റിനിർത്തുകയും, ബാക്കപ്പിൽ നിന്ന് ഡേറ്റ തിരികെ കൊണ്ടുവരുകയും ചെയ്തു. ഇങ്ങനെ ബിസിനസ് കാര്യങ്ങൾ തടസ്സമില്ലാതെ മുന്നോട്ട് കൊണ്ടുപോകാൻ അവർക്ക് കഴിഞ്ഞു.

3) ഡേറ്റ സുരക്ഷയും സ്വകാര്യതയും: നമ്മുടെ ഡേറ്റയുടെ സുരക്ഷയും സ്വകാര്യതയും ഉറപ്പാക്കുക എന്നത് ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ മറ്റൊരു പ്രധാന പ്രയോജനമാണ്. ഡേറ്റ ആരും മോഷ്ടിക്കാതെയും, അനുവാദമില്ലാതെ ആരും ഉപയോഗിക്കാതെയും ഇത് ശക്തമായ സംരക്ഷണം നൽകുന്നു. ഇത് ഉപഭോക്താക്കൾക്ക് സ്ഥാപനങ്ങളോടുള്ള വിശ്വാസം കൂട്ടുകയും ചെയ്യും. നമ്മുടെ ഇന്ത്യയിലെ തന്നെ 'ഡിജിറ്റൽ ഇന്ത്യ' പദ്ധതിയുടെ ഭാഗമായി, ആധാർ ഡേറ്റാബേസിന്റെ സുരക്ഷ ഉറപ്പാക്കാൻ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനങ്ങൾ ഉപയോഗിക്കുന്നുണ്ട്. എൻക്രിപ്ഷനും തത്സമയ നിരീക്ഷണവുമൊക്കെ ഉപയോഗിച്ച്, നൂറ് കോടിയിലധികം ആളുകളുടെ വ്യക്തിഗത വിവരങ്ങൾ സുരക്ഷിതമായി സൂക്ഷിക്കാൻ ഇതിന് കഴിയുന്നു.

4) വ്യാജ വാർത്തകളും തെറ്റായ വിവരങ്ങളും തടയൽ: നമ്മുടെ സാമൂഹിക ജീവിതത്തിൽ വലിയ പ്രശ്നങ്ങളുണ്ടാക്കുന്ന ഒന്നാണല്ലോ വ്യാജ വാർത്ത

കളും തെറ്റായ വിവരങ്ങളും. AI അധിഷ്ഠിത ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനങ്ങൾ സോഷ്യൽ മീഡിയയിലെ വ്യാജ വാർത്തകളെയും, AI ഉണ്ടാക്കുന്ന വ്യാജ വീഡിയോകളെയും (ഡീപ്ഫേക്കുകൾ) തിരിച്ചറിഞ്ഞ് തടയും. ഇത് സമൂഹത്തിൽ തെറ്റിദ്ധാരണകൾ പടരുന്നത് ഒഴിവാക്കാൻ സഹായിക്കും. ഇന്ത്യ-പാകിസ്താൻ സംഘർഷം നടന്ന സമയത്ത്, AI ഉപയോഗിച്ച് ഉണ്ടാക്കിയ വ്യാജ വീഡിയോകൾ സോഷ്യൽ മീഡിയയിൽ ഒരുപാട് പ്രചരിച്ചിരുന്നു. പക്ഷേ, ചില സോഷ്യൽ മീഡിയ പ്ലാറ്റ്ഫോമുകളുടെ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ആ വീഡിയോകളിലെ അസാധാരണമായ മുഖഭാവങ്ങളും ഓഡിയോയിലെ പ്രശ്നങ്ങളുമൊക്കെ കണ്ടുപിടിച്ച് അവ ബ്ലോക്ക് ചെയ്തു. ഇത് പൊതുജനങ്ങളിൽ വലിയ ആശയക്കുഴപ്പം ഒഴിവാക്കാൻ സഹായിച്ചു.

5) ചെലവ് കുറയ്ക്കലും കാര്യക്ഷമത വർധിപ്പിക്കലും: ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം വെറും സുരക്ഷ മാത്രമല്ല, ചെലവ് കുറയ്ക്കാനും കാര്യക്ഷമത വർധിപ്പിക്കാനും സഹായിക്കും. ഓട്ടോമാറ്റിക് ആയി കാര്യങ്ങൾ ചെയ്യുന്നതുകൊണ്ട് അധികം ആളുകളെ ഈ ആവശ്യങ്ങൾക്ക് നിയോഗിക്കേണ്ടി വരില്ല, സുരക്ഷാ ചെലവുകൾ കുറയ്ക്കാനും ഇത് സഹായിക്കും. സൈബർ ആക്രമണങ്ങൾ തടയുന്നതിലൂടെയും, എന്തെങ്കിലും തകരാർ വന്നാൽ സിസ്റ്റം പ്രവർത്തനരഹിതം ആയിരിക്കുന്ന സമയം (downtime) കുറയ്ക്കുന്നതിലൂടെയും ഈ സംവിധാനം സാമ്പത്തികമായി വലി

സൈബർ ഭീഷണികൾ കൂടുതൽ സങ്കീർണ്ണവും കണ്ടെത്താൻ പ്രയാസമുള്ളതുമായി മാറിക്കൊണ്ടിരിക്കുന്ന ഈ സാഹചര്യത്തിൽ, ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഒരു നിർണായക പങ്ക് വഹിക്കും.

യ നേട്ടങ്ങൾ നൽകും. വലിയ സുരക്ഷാ പ്രശ്നങ്ങൾ ഉണ്ടാകുമ്പോഴുണ്ടാകുന്ന ഭീമമായ നഷ്ടങ്ങളെ ഇത് ഒഴിവാക്കുകയും ചെയ്യും. 'നഷ്ടം വരുന്നത് തടയുന്നതാണ് ഏറ്റവും വലിയ ലാഭം' എന്ന് പറയുന്നത് പോലെ.

6) സിസ്റ്റം വിശ്വാസ്യത വർദ്ധിപ്പിക്കുന്നു: ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം നമ്മുടെ ഡിജിറ്റൽ സിസ്റ്റങ്ങളുടെയും ആപ്ലിക്കേഷനുകളുടെയും വിശ്വാസ്യതയും സ്ഥിരതയും കൂട്ടും. അതായത്, എപ്പോഴും പ്രവർത്തനക്ഷമമായിരിക്കും. ഇത് ഉപയോഗിക്കുന്നവർക്ക് ഒരു നല്ല അനുഭവം നൽകുകയും ചെയ്യും.

7) വേഗത്തിലുള്ള വീണ്ടെടുക്കൽ: ഏതെങ്കിലും സിസ്റ്റത്തിന് തകരാറ് സംഭവിച്ചാൽ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം വേഗത്തിൽ വീണ്ടെടുക്കൽ പ്രവർത്തനങ്ങൾ തുടങ്ങും. അതായത്, പ്രശ്നത്തിന്റെ വ്യാപ്തി കുറയ്ക്കാനും, എല്ലാ സേവനങ്ങളും ഉടൻ തന്നെ സാധാരണ നിലയിലാക്കാനും ഇത് സഹായിക്കും.

8) ബിസിനസ് തുടർച്ച ഉറപ്പാക്കുന്നു: സൈബർ ആക്രമണങ്ങളോ സിസ്റ്റം തകരാറുകളോ ഉണ്ടാകുമ്പോൾ ബിസിനസ് കാര്യങ്ങൾ തടസ്സപ്പെടാനുള്ള സാധ്യത വളരെ വലുതാണ്. പക്ഷേ, ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം തകരാറുകൾ വേഗത്തിൽ കണ്ടെത്തി പരിഹരിക്കുകയും, ബാക്കപ്പുകളിൽ നിന്ന് ഡേറ്റ തിരികെ കൊണ്ടുവന്ന് പ്രവർത്തനങ്ങൾ സാധാരണ നിലയിലാക്കുകയും ചെയ്യുന്നതുകൊണ്ട്, ബിസിനസ് തുടർച്ച ഉറപ്പാക്കാൻ ഇതിന് കഴിയും. ഒരു ബിസിനസ് സ്ഥാപനത്തിന് ഇതിലും വലിയൊരു ആശ്വാസം വേറെയില്ല.

നമ്മൾ മുൻപ് കണ്ടില്ലേ, ഫയർവാൾ, ആന്റിവൈറസ്, IDPS, എൻക്രിപ്ഷൻ, IAM, സുരക്ഷാ അവബോധ പരിശീലനം, ബാക്കപ്പ്, ത്രെഡ് ഇന്റലിജൻസ്, നെറ്റ്വർക്ക് സെഗ്മെന്റേഷൻ എന്നിങ്ങനെ പല പല ഘടകങ്ങളെക്കുറിച്ച്? ഈ ഓരോ ഭാഗങ്ങളും തനിച്ച് നിന്നാൽ വലിയ ശക്തിയില്ലായിരിക്കാം. പക്ഷേ, ഇവയെല്ലാം ഒരുമിച്ച്, ഒരു ഓർക്കസ്ട്രയിലെ ഉപകരണങ്ങളെപ്പോലെ കൃത്യമായ താളത്തിൽ പ്രവർത്തിക്കുമ്പോഴാണ് ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം അതിന്റെ പൂർണ്ണ ശക്തിയിൽ എത്തുന്നത്.ഫയർവാൾ ഒരു കവചമായി നിൽക്കുമ്പോൾ, ആന്റിവൈറസ് അകത്തുള്ള രോഗാണുക്കളെ കൊല്ലുന്നു, IDPS സംശയാസ്പദമായ നീക്കങ്ങളെ നിരീക്ഷിക്കുന്നു, എൻക്രിപ്ഷൻ വിവരങ്ങളെ സുരക്ഷിതമാക്കുന്നു, IAM ശരിയായ ആൾക്കാരെ മാത്രം അകത്തേക്ക് വിടുന്നു, ത്രെഡ് ഇന്റലിജൻസ് പുതിയ ഭീഷണികളെക്കുറിച്ച് മുന്നറിയിപ്പ് നൽകുന്നു, ബാക്കപ്പ് സിസ്റ്റങ്ങൾ ഡേറ്റ നഷ്ടപ്പെടാതെ കാക്കുന്നു. ഇങ്ങനെ ഓരോ ഘടകവും അതിന്റേതായ പങ്ക് കൃത്യമായി നിർവഹിക്കുന്നു. ഈ കൂട്ടായ പ്രവർത്തനം സൈബർ ആക്രമണങ്ങൾ ഉണ്ടാകുമ്പോൾ അവയെ പല തലങ്ങളിൽ വെച്ച് നേരിടാൻ സഹായിക്കും. ഒരു ഭീഷണി ഒരു പ്രതിരോധം മറികടന്നാൽ, അടുത്തത് അതിനെ കാത്തിരിപ്പുണ്ടാകും. അങ്ങനെ, ഡിജിറ്റൽ ലോകത്തിന് ഒരു അദൃശ്യവും എന്നാൽ അതിശക്തവുമായ ഒരു പ്രതിരോധ വലയം ഈ സംവിധാനം ഒരുക്കുന്നു.

ചുരുക്കത്തിൽ, ഡിജിറ്റൽ യുഗത്തിന്റെ വെല്ലുവിളികൾ നാൾക്കുനാൾ വർദ്ധിച്ചു വരികയാണ്. സൈബർ ഭീഷണികൾ കൂടുതൽ സങ്കീർണ്ണവും കണ്ടെത്താൻ പ്രയാസമുള്ളതുമായി മാറിക്കൊണ്ടിരിക്കുന്ന ഈ സാഹചര്യത്തിൽ, ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഒരു നിർണായക പങ്ക് വഹിക്കും. ഇത് കേവലം ഒരു സുരക്ഷാ ഉപകരണം എന്നതിലുപരി, ഡിജിറ്റൽ ലോകത്തിലെ അതിജീവനത്തിനുള്ള ഒരു തന്ത്രമാണ്. ഭീഷണികളെ മുൻകൂട്ടി അറിയാനും അവയെ ചെറുക്കാനും തകർച്ചകളിൽ നിന്ന് വേഗത്തിൽ കരകയറാനുമുള്ള ഇതിന്റെ കഴിവ്, വ്യക്തികൾക്കും സ്ഥാപനങ്ങൾക്കും ഒരുപോലെ ആശ്രയമാണ്.ഡിജിറ്റൽ ലോകം പുരോഗമിക്കുമ്പോൾ, അതിനൊപ്പം ശക്തിപ്പെടുന്ന ഒരു ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം കെട്ടിപ്പടുക്കേണ്ടത് സുരക്ഷിതമായ ഒരു ഭാവിക്കായി അനിവാര്യമാണ്. നമ്മുടെ ഡേറ്റയും സേവനങ്ങളും സംരക്ഷിച്ച്, ബിസിനസ് തടസ്സമില്ലാതെ മുന്നോട്ട് കൊണ്ടുപോയി, ഡിജിറ്റൽ ലോകത്ത് സുരക്ഷിതമായി മുന്നോട്ട് പോകാൻ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം നിർണായക പങ്ക് വഹിക്കുന്നു. ഡിജിറ്റൽ ലോകം സുരക്ഷിതമാകുമ്പോൾ മാത്രമാണ് അതിന്റെ പൂർണ്ണമായ സാധ്യതകൾ നമുക്ക് പ്രയോജനപ്പെടുത്താൻ സാധിക്കുകയുള്ളൂ. സൈബർ സുരക്ഷാ തന്ത്രങ്ങളുടെ ഭാവി ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനങ്ങളിലായിരിക്കുമെന്ന് നിസ്സംശയം പറയാം.

മികച്ച ആനുകൂല്യങ്ങളോടെ ഇൻഫോകൈരളി വരിക്കാരാകാം !

ഇൻഫോ കൈരളി ഒരു ലക്കം 30 രൂപ. വാർഷിക വരിക്കാർ ആകുന്നവർക്ക് പ്രത്യേക ഡിസ്കൗണ്ട്

വരിക്കാരാകുവാൻ 9447124390
എന്ന നമ്പറിൽ വാട്സ്ആപ്പ് മെസ്സേജ് ചെയ്യുകയോ വിളിക്കുകയോ ചെയ്യുക

കാലാവധി – 1 വർഷം
മുഖവില : 360/-
അയയ്ക്കേണ്ട തുക : 340/-

കാലാവധി – 3 വർഷം
മുഖവില : 1080/-
അയയ്ക്കേണ്ട തുക : 980/-

കാലാവധി – 2 വർഷം
മുഖവില : 720/-
അയയ്ക്കേണ്ട തുക : 660/-

കാലാവധി – 5 വർഷം
മുഖവില : 1800/-
അയയ്ക്കേണ്ട തുക : 1450/-

ഇൻഫോകൈരളിയുടെ ഡിജിറ്റൽ കോപ്പിയും ലഭ്യമാണ്

ഇൻഫോകൈരളി വരിസംഖ്യ നേരിട്ട് ബാങ്കിൽ അടയ്ക്കാം

Name : INFOKAIRALI A/c No- 67003574237,Branch- Kuruppanthara, Bank- State Bank of India,
Ac Type- Current account IFSC code- SBIN0070136

ഗൂഗിൾ പേ നമ്പർ: 9447124391

പേയ്മെന്റ് അടച്ചശേഷം വാട്സ്ആപ്പ് (9447124390)/ മെയിൽ (kairali.info@gmail.com) മുഖാന്തരം നിങ്ങളുടെ പേര്, മൊബൈൽ നമ്പർ, വിലാസം എന്നീ വിവരങ്ങൾ ഇൻഫോകൈരളിയെ അറിയിക്കുമല്ലോ

ഡിജിറ്റൽ പ്രതിരോധത്തിൽ എഐയുടെയും ഓട്ടോമേഷന്റെയും പങ്ക്

ഇന്ന് നമ്മുടെ ലോകം ഒരു ഡിജിറ്റൽ കൊടുങ്കാറ്റിലൂടെയാണ് കടന്നുപോകുന്നത്, അല്ലേ? ഓരോ നിമിഷവും സൈബർ ഭീഷണികൾ പുതിയ മുഖങ്ങളുമായിട്ടാണ് വരുന്നത്. ചിലപ്പോൾ നമ്മൾ അറിയാതെ തന്നെ നമ്മുടെ സിസ്റ്റങ്ങളിലേക്ക് കടന്നു കയറാൻ കഴിയുന്നത്ര സങ്കീർണ്ണമാണ് കാര്യങ്ങൾ. ഇങ്ങനെ നമ്മുടെ ഡിജിറ്റൽ വിവരങ്ങളെയും സ്ഥാപനങ്ങളുടെ പ്രവർത്തനങ്ങളെയും എങ്ങനെയാണ് സുരക്ഷിതമാക്കുക എന്ന ചോദ്യം പലരുടെയും മനസ്സിലുണ്ടാകും. ഇതിനൊരു കിടിലൻ ഉത്തരമാണ് ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം (Digital Immune System). രോഗാണുക്കളെയും വൈറസുകളെയും തിരിച്ചറിഞ്ഞ്, അവരെ ചെറുത്ത് തോൽപ്പിച്ച്, ഭാവിയിൽ അതേ രോഗം വരാതെ നമ്മളെ സംരക്ഷിക്കാൻ ശരീരം സ്വയം പഠിച്ച് കരുത്താർജ്ജിക്കുന്നില്ലേ? അതേ മാതൃകയിൽ, ഒരു സ്ഥാപനത്തിന്റെ നെറ്റ്‌വർക്കുകളെയും, വിലപ്പെട്ട ഡേറ്റയെയും, ഉപയോഗിക്കുന്ന ആപ്ലിക്കേഷനുകളെയുമൊക്കെ തുടർച്ചയായ സൈബർ ആക്രമണങ്ങളിൽ നിന്ന് കാത്തു രക്ഷിക്കാനാണ് ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം രൂപകൽപ്പന ചെയ്തിരിക്കുന്നത്.

ഇതൊരു വെറും സുരക്ഷാ സോഫ്റ്റ്‌വെയറുകളുടെ കൂട്ടമല്ല കേട്ടോ! ഈ സംവിധാനം ശരിക്കും ഒരു സജീവമായ സംരക്ഷകനാണ്. സൈബർ ഭീഷണികളെ മുൻകൂട്ടി കണ്ടെത്താനും, സ്വയമേവ അതിനോട് പ്രതികരിക്കാനും, നടന്ന ആക്രമണങ്ങളിൽ നിന്ന് പാഠം ഉൾക്കൊണ്ട് സ്വന്തം പ്രതിരോധ ശേഷി കാലക്രമേണ കൂട്ടാനും ഇതിന് കഴിവുണ്ട്. അതായത്, ഇന്നലെ കണ്ട ഒരു സൈബർ ആക്രമണത്തിന്റെ രീതി പഠിച്ച്, നാളെ വരാനിരിക്കുന്ന സമാനമായ ഭീഷണികളെ കൂടുതൽ വേഗത്തിലും കൃത്യതയോടെയും തടയാൻ ഇവന് സാധിക്കും. ഈ വിസ്മയകരമായ പ്രവർത്തനത്തിന് പിന്നിൽ നിർണായക പങ്ക് വഹിക്കുന്ന രണ്ട് സൂപ്പർ ടെക്നോളജികളാണ് കൃത്രിമ ബുദ്ധിയും (AI - Artificial Intelligence) ഓട്ടോമേഷനും.AI-യുടെ ബുദ്ധിയും ഓട്ടോമേഷന്റെ വേഗതയും ഒരുമിക്കുമ്പോൾ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം മനുഷ്യന്റെ ഇടപെടൽ കാര്യമായി കുറച്ച് തന്നെ, സൈബർ ലോകത്ത് ഒരു നിതാന്ത ജാഗ്രത പുലർത്തും. ഇത് നമ്മുടെ ഡിജിറ്റൽ ജീവിതത്തെ കൂടുതൽ സുരക്ഷിതവും, വിശ്വസനീയവുമാക്കുകയും ചെയ്യും.

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ യഥാർത്ഥ 'ബുദ്ധികേന്ദ്രം' എന്ന് പറയുന്നത് നമ്മുടെ കൃത്രിമ ബുദ്ധി (AI) തന്നെയാണ്. ശരിക്കും ഇവനാണ് എല്ലാ കാര്യങ്ങളും തലച്ചോറ് പോലെ വിശകലനം ചെയ്യുന്നത്.

സൈബർ ലോകത്തെ 'ബുദ്ധികേന്ദ്രം': കൃത്രിമ ബുദ്ധിയുടെ (AI) പങ്ക്

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ യഥാർത്ഥ 'ബുദ്ധികേന്ദ്രം' എന്ന് പറയുന്നത് നമ്മുടെ കൃത്രിമ ബുദ്ധി (AI) തന്നെയാണ്. ശരിക്കും ഇവനാണ് എല്ലാ കാര്യങ്ങളും തലച്ചോറ് പോലെ വിശകലനം ചെയ്യുന്നത്. വലിയ അളവിലുള്ള ഡേറ്റയെ (കംപ്യൂട്ടർ ലോഗുകൾ, നെറ്റ്‌വർക്കിലൂടെ പോകുന്ന വിവരങ്ങൾ, സിസ്റ്റത്തിന്റെ ഓരോ ചലനങ്ങളും ഒക്കെ) അതിവേഗം പരിശോധിച്ച്, അതിലെ ചെറിയ സൂചനകളും അസാധാരണമായ കാര്യങ്ങളുമൊക്കെ കണ്ടെത്താൻ AI അൽഗോരിതങ്ങൾക്ക് പ്രത്യേക കഴിവുണ്ട്. അറിയപ്പെടുന്നതും ഇതുവരെ കണ്ടിട്ടില്ലാത്തതുമായ സൈബർ ആക്രമണങ്ങൾ, മാൽവെയറുകൾ, ഫിഷിംഗ് തട്ടിപ്പുകൾ എന്നിങ്ങനെ എല്ലാ പ്രശ്നങ്ങളെയും വളരെ കൃത്യതയോടെ കണ്ടുപിടിക്കാൻ AI സഹായിക്കും. പെരുമാറ്റ വിശകലനം (Behavioral Analytics) പോലുള്ള AI സാങ്കേതികവിദ്യകൾ ഓരോ ഉപയോക്താവിന്റെയും സിസ്റ്റത്തിന്റെയും സാധാരണ പ്രവർത്തന രീതിയെക്കുറിച്ച് പഠിക്കും. എന്നിട്ട്, അതിൽ നിന്ന് ചെറിയ വ്യതിയാനങ്ങൾ വന്നാൽ പോലും ഇവൻ സൂക്ഷ്മമായി നിരീക്ഷിക്കും. ഒരു അസ്വാഭാവിക പ്രവർത്തനം കണ്ടെത്തിയാൽ, അത് ഒരു സാധ്യതയുള്ള ഭീഷണിയായി കണക്കാക്കുകയും, ഉടൻ തന്നെ പ്രതിരോധ നടപടികൾ സ്വീകരിക്കാൻ ഈ സംവിധാനത്തിന് നിർദ്ദേശം നൽകുകയും ചെയ്യും. അതുപോലെ, ഒരു പുതിയ മാൽവെയർ വന്നാൽ, AI അതിനെ വിശകലനം ചെയ്യുകയും, അതിന്റെ ദോഷകരമായ സ്വഭാവം മനസ്സിലാക്കുകയും, അതിനനുസരിച്ച് പ്രതിരോധതന്ത്രങ്ങൾ വികസിപ്പിക്കുകയും ചെയ്യും.

ഭീഷണി കണ്ടെത്തുന്നതിൽ AI-യുടെ മാന്ത്രികത

സൈബർ സുരക്ഷയിൽ AI-യുടെ ഏറ്റവും പ്രധാനപ്പെട്ട പങ്ക് ഭീഷണികളെ തിരിച്ചറിയുന്നതിലാണ്. സാധാരണ സുരക്ഷാ സംവിധാനങ്ങൾ മുൻകൂട്ടി സെറ്റ് ചെയ്ത നിയമങ്ങളെയും 'സിഗ്നേച്ചറുകളെയും' (അടയാളങ്ങളെയും) ആശ്രയിച്ച് പ്രവർത്തിക്കുമ്പോൾ, AI-ക്ക് വലിയ അളവിലുള്ള ഡേറ്റയെ (നെറ്റ്‌വർക്ക് ട്രാഫിക്, ഉപയോക്താക്കളുടെ പ്രവർത്തനങ്ങൾ, സിസ്റ്റം ലോഗുകൾ പോലുള്ളവ) തത്സമയം വിശകലനം ചെയ്യാനും, സാധാരണ നിലയിൽ നിന്നുള്ള മാറ്റങ്ങളെ (anomalies) കണ്ടെത്താനും കഴിയും. മെഷീൻ ലേണിംഗ് അൽഗോരിതങ്ങൾ ഉപയോഗിച്ച്, AI സിസ്റ്റങ്ങൾക്ക് ദോഷകരമായ പ്രവർത്തനങ്ങളുടെ സൂചന നൽകുന്ന പാറ്റേണുകളും മാതൃകകളും പഠിക്കാൻ കഴിയും. ഒരു സംശയാസ്പദമായ പ്രവർത്തനം കണ്ടെത്തിയാൽ, AI ഉടൻ തന്നെ സുരക്ഷാ വിദഗ്ധർക്ക് മുന്നറിയിപ്പ് നൽകുകയും, പ്രതിരോധ നടപടികൾ സ്വീകരിക്കാൻ സഹായിക്കുകയും ചെയ്യും. ഈ കഴിവ്, അറിയപ്പെടുന്നതും അറിയപ്പെടാത്തതുമായ പുതിയ സൈബർ ആക്രമണങ്ങളെ ഫലപ്രദമായി പ്രതിരോധിക്കാൻ സ്ഥാപനങ്ങളെ സഹായിക്കുന്നു.

ഭാവിയെ അറിയുന്ന AI

AI പ്രവചനാത്മക സുരക്ഷയുടെ കാര്യത്തിലും ഒരു നിർണായക പങ്ക് വഹിക്കുന്നുണ്ട്. മെഷീൻ ലേണിംഗ് മോഡലുകൾ ഉപയോഗിച്ച്, AI-ക്ക് മുൻപ് നടന്ന ആക്രമണങ്ങളുടെ ഡേറ്റയും ഇപ്പോഴത്തെ സാഹചര്യങ്ങളും വിശകലനം ചെയ്ത് ഭാവിയിൽ ഉണ്ടാകാൻ സാധ്യതയുള്ള ആക്രമണങ്ങളെക്കുറിച്ച് ഒരു സൂചന നൽകാൻ കഴിയും. ഉദാഹരണത്തിന്, ഒരു സ്ഥാപനത്തിലെ ജീവനക്കാരുടെ പെരുമാറ്റത്തിൽ വരുന്ന അസാധാരണമായ മാറ്റങ്ങൾ (ലോഗിൻ ചെയ്യുന്ന സമയം, അവർ തുറന്നു നോക്കുന്ന ഫയലുകൾ തുടങ്ങിയവ) AI തിരിച്ചറിയുകയും, ഇത് ഒരു 'ഇൻസൈഡർ ത്രെഡ്' (അകത്ത് നിന്നുള്ള ഭീഷണി) ആകാനുള്ള സാധ്യതയെക്കുറിച്ച് മുന്നറിയിപ്പ് നൽകുകയും ചെയ്യും. അതുപോലെ, ഇമെയിലുകളിലും മറ്റ് മെസ്സേജുകളിലുമൊക്കെ സംശയാസ്പദമായ എന്തെങ്കിലും കണ്ടാൽ (സംസാര ഭാഷ, ലിങ്കുകൾ, അറ്റാച്ച്മെന്റുകൾ) AI അതിനെ വിശകലനം ചെയ്ത് ഫിഷിംഗ് ശ്രമങ്ങളെ മുൻകൂട്ടി കണ്ടെത്താനും തടയാനും കഴിയും. ആക്രമണങ്ങൾ സംഭവിക്കുന്നതിന് മുൻപുതന്നെ പ്രതിരോധ നടപടികൾ എടുക്കാൻ ഈ 'പ്രവചനാത്മകമായ' കഴിവ് സ്ഥാപനങ്ങളെ സഹായിക്കുന്നു.

AI സിസ്റ്റങ്ങൾക്ക് പുതിയ ഡേറ്റയിൽ നിന്ന് സ്വയം പഠിക്കാനും, പുതിയ ഭീഷണികളെ വേഗത്തിൽ തിരിച്ചറിയാനും, നിലവിലുള്ള പ്രതിരോധ തന്ത്രങ്ങളെ കൂടുതൽ മികച്ചതാക്കാനും കഴിയും.

സ്വയം പഠിച്ച് മെച്ചപ്പെടുന്ന AI

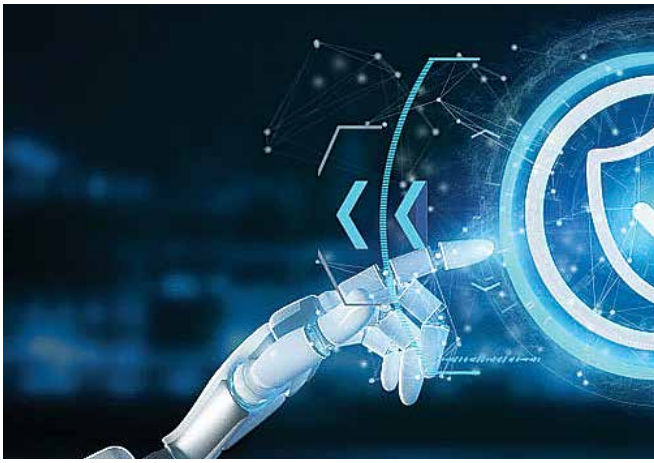
AI-യുടെ സ്വയം പഠന ശേഷി സൈബർ സുരക്ഷയുടെ ഒരു വലിയ മുന്നേറ്റമാണ്. സൈബർ ഭീഷണികൾ നിരന്തരം മാറിക്കൊണ്ടിരിക്കുന്ന ഒരു സാഹചര്യത്തിൽ, സുരക്ഷാ സംവിധാനങ്ങളും കാലത്തിനനുസരിച്ച് സ്വയം നവീകരിക്കേണ്ടത് അത്യാവശ്യമാണ്. AI സിസ്റ്റങ്ങൾക്ക് പുതിയ ഡേറ്റയിൽ നിന്ന് സ്വയം പഠിക്കാനും, പുതിയ ഭീഷണികളെ വേഗത്തിൽ തിരിച്ചറിയാനും, നിലവിലുള്ള പ്രതിരോധ തന്ത്രങ്ങളെ കൂടുതൽ മികച്ചതാക്കാനും കഴിയും. ഒരു പുതിയതരം മാൽവെയർ ആക്രമണം കണ്ടെത്തിയാൽ, AI അതിന്റെ സ്വഭാവം വിശദമായി വിശകലനം ചെയ്യുകയും, ഭാവിയിൽ സമാനമായ ആക്രമണങ്ങളെ പ്രതിരോധിക്കാൻ ആവശ്യമായ അറിവ് നേടുകയും ചെയ്യുന്നു. ഈ 'അഡാപ്റ്റീവ് ലേണിംഗ്' കഴിവ്, AI-യെ സൈബർ സുരക്ഷയുടെ ഒരു ഒഴിച്ചുകൂടാനാവാത്ത ഘടകമാക്കി മാറ്റുന്നു. കാരണം, മാറിക്കൊണ്ടിരിക്കുന്ന ഭീഷണികൾക്കെതിരെ ഇത് നിരന്തരമായ പ്രതിരോധം ഉറപ്പാക്കും. ചുരുക്കത്തിൽ, കൃത്രിമ ബുദ്ധി സൈബർ സുരക്ഷയുടെ വിവിധ തലങ്ങളിൽ വിപ്ലവം സൃഷ്ടിക്കുകയും, സ്ഥാപനങ്ങൾക്ക് അവരുടെ ഡിജിറ്റൽ ആസ്തികളെ കൂടുതൽ ഫലപ്രദമായി സംരക്ഷിക്കാൻ സഹായിക്കുകയും ചെയ്യുന്നു.

സൈബർ ലോകത്തെ 'അതിവേഗ സഹായി': ഓട്ടോമേഷന്റെ പങ്ക്

സൈബർ സുരക്ഷാ രംഗത്ത് ഓരോ ദിവസവും ഭീഷണികളുടെ വേഗതയും സങ്കീർണ്ണതയും കൂടിവരികയാണ്. മനുഷ്യന്റെ ഇടപെടൽ മാത്രം കൊണ്ട് ഫലപ്രദമായി നേരിടാൻ പറ്റാത്ത ഒരു അവസ്ഥയിലേക്ക് കാര്യങ്ങൾ എത്തിയിരിക്കുന്നു, അല്ലേ? ഈ സാഹചര്യത്തിൽ, ഓട്ടോമേഷൻ നമ്മുടെ ഡിജിറ്റൽ സുരക്ഷയുടെ ഒരു അവിഭാജ്യ ഘടകമായി മാറിയിട്ടുണ്ട്. സുരക്ഷാ പ്രശ്നങ്ങൾ ഉണ്ടാകുമ്പോൾ തത്സമയം പ്രതികരിക്കാനും, പല സുരക്ഷാ സംവിധാനങ്ങളെയും ഒരുമിച്ച് പ്രവർത്തിപ്പിക്കാനും, ആവർത്തന സ്വഭാവമുള്ള ജോലികൾ ഒഴിവാക്കാനുമൊക്കെ ഓട്ടോമേഷൻ സൈബർ സുരക്ഷാ ടീമുകളെ സഹായിക്കും. അങ്ങനെ നമ്മുടെ പ്രതിരോധ ശേഷി ഒരുപാട് കൂട്ടുകയും ചെയ്യും.

തത്സമയ പ്രതികരണം: സൈബർ സുരക്ഷയിൽ ഓട്ടോമേഷന്റെ ഏറ്റവും പ്രധാനപ്പെട്ട പങ്ക് തത്സമയ പ്രതികരണമാണ്. ഒരു സൈബർ ഭീഷണി തിരിച്ചറിഞ്ഞാൽ, മനുഷ്യന്റെ സഹായത്തിനായി കാത്തുനിൽക്കാതെ തന്നെ ഓട്ടോമേറ്റഡ് സംവിധാനങ്ങൾക്ക് ഉടൻ പ്രതികരിക്കാൻ കഴിയും. ഉദാഹരണത്തിന്, ഒരു സംശയാസ്പദമായ ലോഗിൻ ശ്രമം പലതവണ ആവർത്തിക്കുകയാണെങ്കിൽ, ഓട്ടോമാറ്റിക് ആയി ആ അക്കൗണ്ട് താൽക്കാലികമായി തടയാനും, കൂടുതൽ നാശനഷ്ടങ്ങൾ വരുന്നത് ഒഴിവാക്കാനും ഓട്ടോമേഷന് കഴിയും. അതുപോലെ, ഒരു അപകടകരമായ ഫയൽ നെറ്റ്വർക്കിൽ പടരാൻ ശ്രമിക്കുകയാണെങ്കിൽ, ഓട്ടോമേറ്റഡ് പ്രതിരോധ സംവിധാനങ്ങൾക്ക് ആ ഫയലിനെ 'കാറന്റൈൻ' ചെയ്യാനും, ബാധിക്കപ്പെട്ട സിസ്റ്റങ്ങളെ നെറ്റ്വർക്കിൽ നിന്ന് ഒറ്റപ്പെടുത്താനും, ഫയർവാൾ നിയമങ്ങൾ നിമിഷങ്ങൾക്കുള്ളിൽ മാറ്റാനുമൊക്കെ സാധിക്കും. ആക്രമണങ്ങൾ മൂലമുണ്ടാകുന്ന പ്രശ്നങ്ങൾ ഒരുപാട് കുറയ്ക്കാനും, സുരക്ഷാ ടീമുകൾക്ക് കൂടുതൽ ഗുരുതരമായ ഭീഷണികളിൽ ശ്രദ്ധ കൊടുക്കാൻ സമയം നൽകാനും ഈ തത്സമയ പ്രതികരണ ശേഷി സഹായിക്കുന്നു.

സുരക്ഷാ സംയോജനം: ഓട്ടോമേഷൻ പലതരം സുരക്ഷാ സംവിധാനങ്ങളെയും ഒരുമിപ്പിച്ച് പ്രവർത്തിപ്പിക്കാൻ സഹായിക്കുന്ന സുരക്ഷാ സംയോജനത്തിൽ (Security Orchestration) ഒരു പ്രധാന പങ്ക് വഹിക്കുന്നു. സാധാരണയായി ഒരു സ്ഥാപനത്തിന്റെ സൈബർ സുരക്ഷാ ലോകത്ത് SIEM, EDR, IDS/IPS പോലുള്ള പലതരം സുരക്ഷാ ഉപകരണങ്ങളുണ്ടാകും. ഒരു ഭീഷണി കണ്ടെത്തിയാൽ, ഈ വ്യത്യസ്ത സംവിധാനങ്ങൾ തമ്മിൽ വിവരങ്ങൾ കൈമാറുകയും, ഒരുമിച്ച് പ്രതിരോധ നടപടികൾ സ്വീകരിക്കുകയും ചെയ്യുന്നത് ഓട്ടോമേഷൻ സാധ്യമാക്കുന്നു. ഉദാഹരണത്തിന്, SIEM ഒരു സംശയാസ്പദമായ പ്രവർത്തനം കണ്ടെത്തിയാൽ, അത് ഉടൻ തന്നെ EDR-ന് വിവരം കൈമാറും. EDR ആ ഉപകരണത്തിൽ കൂടുതൽ പരിശോധന നടത്തുകയും, ആവശ്യമെങ്കിൽ പ്രതിരോധ നടപടികൾ സ്വീകരിക്കുകയും ചെയ്യും. ഇങ്ങനെ എല്ലാവരും ഏകോപിച്ച് പ്രവർത്തിക്കുന്നത്, ഓരോന്നും ഒറ്റയ്ക്ക് പ്രതികരിക്കുന്നതിനേക്കാൾ വളരെ ഫലപ്രദമായ ഒരു സുരക്ഷാ കവചം ഉണ്ടാക്കുന്നു.



AI-യും ഓട്ടോമേഷനും ചേർന്നുള്ള പ്രവർത്തനം സുരക്ഷാ സംഭവങ്ങളോടുള്ള പ്രതികരണസമയം ഗണ്യമായി കുറയ്ക്കുന്നു. ഒരു ഭീഷണി തിരിച്ചറിയപ്പെട്ടാൽ, ഓട്ടോമേറ്റഡ് വർക്ക്ഫ്ലോകൾക്ക് തൽക്ഷണം പ്രതിരോധ നടപടികൾ സ്വീകരിക്കാൻ കഴിയും.

മാനുവൽ ജോലികൾക്ക് വിട: സൈബർ സുരക്ഷയിലെ ആവർത്തന സ്വഭാവമുള്ള മാനുവൽ ജോലികൾ ഓട്ടോമേറ്റ് ചെയ്യുന്നതിലൂടെ സുരക്ഷാ ടീമുകൾക്ക് അവരുടെ വിലയേറിയ സമയം ലാഭിക്കാനും, കൂടുതൽ തന്ത്രപരമായ കാര്യങ്ങളിൽ ശ്രദ്ധ കേന്ദ്രീകരിക്കാനും സാധിക്കും. ലോഗുകൾ വിശകലനം ചെയ്യുക, സുരക്ഷാ മുന്നറിയിപ്പുകൾ തരംതിരിക്കുക (അലേർട്ട് ട്രിയാഷ്), സുരക്ഷാ പിഴവുകൾ സ്കാൻ ചെയ്യുക, റിപ്പോർട്ടുകൾ ഉണ്ടാക്കുക തുടങ്ങിയ ജോലികൾ ഓട്ടോമേറ്റ് ചെയ്യുന്നതിലൂടെ മനുഷ്യന്റെ ഇടപെടൽ കുറയ്ക്കുകയും, പിഴവുകൾ ഒഴിവാക്കുകയും ചെയ്യാം. ഇത് സുരക്ഷാ ടീമിന്റെ മൊത്തത്തിലുള്ള കാര്യക്ഷമത വർദ്ധിപ്പിക്കുകയും, അവർക്ക് പുതിയ ഭീഷണികളെക്കുറിച്ച് പഠിക്കാനും, കൂടുതൽ ശക്തമായ സുരക്ഷാ തന്ത്രങ്ങൾ വികസിപ്പിക്കാനും സമയം കണ്ടെത്താനും സഹായിക്കുന്നു. ചുരുക്കത്തിൽ, ഓട്ടോമേഷൻ സൈബർ സുരക്ഷയുടെ ഒരു നിർണായക ഘടകമാണ്. ഇത് തത്സമയ പ്രതികരണം സാധ്യമാക്കുകയും, സുരക്ഷാ സംവിധാനങ്ങളുടെ ഏകോപനം ഉറപ്പാക്കുകയും, സുരക്ഷാ ടീമുകളുടെ പ്രവർത്തനഭാരം കുറയ്ക്കുകയും ചെയ്യുന്നു. ഈ ഗുണങ്ങൾ ഓട്ടോമേഷനെ ഏതൊരു ശക്തമായ ഡിജിറ്റൽ സുരക്ഷാ തന്ത്രത്തിന്റെയും അവിഭാജ്യ ഘടകമാക്കി മാറ്റുന്നു.

കൂടാതെ, AI-യും ഓട്ടോമേഷനും ചേർന്നുള്ള പ്രവർത്തനം സുരക്ഷാ സംഭവങ്ങളോടുള്ള പ്രതികരണ സമയം ഗണ്യമായി കുറയ്ക്കുന്നു. ഒരു ഭീഷണി തിരിച്ചറിയപ്പെട്ടാൽ, ഓട്ടോമേറ്റഡ് വർക്ക്ഫ്ലോകൾക്ക് തൽക്ഷണം പ്രതിരോധ നടപടികൾ സ്വീകരിക്കാൻ കഴിയും. ഇത്, മനുഷ്യന്റെ ഇടപെടലിനായി കാത്തുനിൽക്കുന്ന കാലതാമസം ഒഴിവാക്കുകയും, ആക്രമണത്തിന്റെ വ്യാപ്തി പരിമിതപ്പെടുത്തുകയും ചെയ്യുന്നു. അക്കൗണ്ടുകൾ താൽക്കാലികമായി തടയുക, നെറ്റ്വർക്ക് സെഗ്മെന്റുകൾ ഒറ്റപ്പെടുത്തുക, ഫയർവാൾ നിയമങ്ങൾ മാറ്റുക തുടങ്ങിയ അടിയന്തിര പ്രതികരണങ്ങൾ ഓട്ടോമേഷനിലൂടെ വളരെ വേഗത്തിലും കൃത്യതയോടെയും നടപ്പിലാക്കാൻ സാധിക്കുന്നു. മാനുവൽ സുരക്ഷാ പ്രക്രിയകളിൽ സംഭവിക്കാവുന്ന പിഴവുകൾ ഒഴിവാക്കാൻ AI-യും ഓട്ടോമേഷനും സഹായിക്കുന്നു എന്നത് മറ്റൊരു പ്രധാന നേട്ടമാണ്. ലോഗ് വിശകലനം, അലേർട്ട് ട്രയാജ്, ദുർബലതാ സ്കാനിംഗ് തുടങ്ങിയ ആവർത്തന സ്വഭാവമുള്ള ജോലികൾ ഓട്ടോമേറ്റ് ചെയ്യുന്നതിലൂടെ, മനുഷ്യന്റെ ശ്രദ്ധക്കുറവ് മൂലമുണ്ടാകാവുന്ന സുരക്ഷാ വീഴ്ചകൾ ഇല്ലാതാക്കാം. ഇത് സുരക്ഷാ പ്രവർത്തനങ്ങളുടെ കൃത്യതയും കാര്യക്ഷമതയും വർദ്ധിപ്പിക്കുകയും, സുരക്ഷാ ടീമുകൾക്ക് കൂടുതൽ തന്ത്രപരമായ കാര്യങ്ങളിൽ ശ്രദ്ധ കേന്ദ്രീകരിക്കാൻ അവസരം നൽകുകയും ചെയ്യുന്നു.

ഡേറ്റാ അനലിറ്റിക്സ്: ഭാവിയെ പ്രവചിച്ച് സുരക്ഷിതമാക്കാം

ഡേറ്റാ അനലിറ്റിക്സ് ഭാവിയിലെ ഡിജിറ്റൽ പ്രതിരോധത്തിന്റെ മറ്റൊരു നിർണായക ഘടകമാണ്. വലിയ അളവിലുള്ള സുരക്ഷാ ഡേറ്റയെ വിശകലനം ചെയ്യുന്നതിലൂടെ, മറഞ്ഞിരിക്കുന്ന ഭീഷണികളെയും, സുരക്ഷാ വീഴ്ചകളെയും, സിസ്റ്റങ്ങളിലെ ദുർബലതകളെയും കണ്ടെത്താൻ സാധിക്കും. ബിഗ് ഡേറ്റാ ടെക്നോളജികളും നൂതന അനലിറ്റിക്കൽ ടൂളുകളും ഉപയോഗിച്ച്, സുരക്ഷാ വിദഗ്ധർക്ക് ആക്രമണങ്ങളുടെ രീതികളും, ലക്ഷ്യങ്ങളും, ഉറവിടങ്ങളും മനസ്സിലാക്കാൻ കഴിയും. ഈ വിവരങ്ങൾ ഭാവിയിലെ പ്രതിരോധ തന്ത്രങ്ങൾ മെച്ചപ്പെടുത്താനും, സുരക്ഷാ നയങ്ങൾ കൂടുതൽ ശക്തമാക്കാനും സഹായിക്കും. പ്രവചനാത്മക അനലിറ്റിക്സ് ഉപയോഗിച്ച്, ഭാവിയിൽ ഉണ്ടാകാൻ സാധ്യതയുള്ള സുരക്ഷാ പ്രശ്നങ്ങളെ മുൻകൂട്ടി തിരിച്ചറിയാനും, പ്രതിരോധ നടപടികൾ സ്വീകരിക്കാനും സാധിക്കും.

അതുപോലെ, AI-യും ഓട്ടോമേഷനും സംയോജിപ്പിച്ച ഒരു സജീവ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം സ്ഥാപനങ്ങളുടെ ഡിജിറ്റൽ സുരക്ഷ ഉറപ്പാക്കുന്നതിൽ ഒരു നിർണായക പങ്ക് വഹിക്കുന്നു. വർധിച്ചു വരുന്ന സൈബർ ഭീഷണികളുടെ സങ്കീർണ്ണതയെയും വേഗതയെയും ഫലപ്രദമായി നേരിടാൻ ഈ സാങ്കേതിക വിദ്യകൾ സ്ഥാപനങ്ങളെ സജ്ജമാക്കുന്നു. “ഭാവിയുടെ സൈബർ സുരക്ഷ, മനുഷ്യരുടെ കൃത്യതയും മെഷീനുകളുടെ വേഗതയും ചേർന്ന് നിർമിക്കുന്ന ബുദ്ധിമുട്ടുള്ള പ്രതിരോധ ശൃംഖല ആകും” എന്ന കാഴ്ചപ്പാട് സൂചിപ്പിക്കുന്നത് പോലെ, AI-യുടെ ബുദ്ധിയും ഓട്ടോമേഷന്റെ കാര്യക്ഷമതയും ഒരുമിച്ച് ചേർന്ന് ഒരുക്കുന്ന ഈ പ്രതിരോധം, ഡിജിറ്റൽ ലോകത്തെ സുരക്ഷിതമാക്കുന്നതിൽ ഒരു പ്രധാന മുന്നേറ്റമായിരിക്കും.

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം: വെല്ലുവിളികളും പരിഹാരമാർഗ്ഗങ്ങളും

സ്ഥാപനങ്ങളുടെ ഡിജിറ്റൽ ലോകത്തെ സുരക്ഷിതമാക്കാൻ ലക്ഷ്യമിട്ടുള്ള ഒരു അത്യാധുനിക സംവിധാനമാണ് ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം (Digital Immune System) എന്ന് നമ്മൾ കണ്ടു. സൈബർ സുരക്ഷ എന്ന് പറയുമ്പോൾ പലപ്പോഴും നമ്മുടെ മനസ്സിലേക്ക് വരുന്നത് ഫയർവാളുകളും ആന്റിവൈറസുമൊക്കെയാണ്. അവ പ്രധാനപ്പെട്ടവയാണെന്നതിൽ സംശയമില്ല. എന്നാൽ, ഇന്നത്തെ കാലത്ത് അതൊന്നും മാത്രം മതിയാകില്ല. ഹാക്കർമാർ ഓരോ ദിവസവും പുതിയ തന്ത്രങ്ങളും, ഇതുവരെ കണ്ടിട്ടില്ലാത്ത ആക്രമണ രീതികളുമായാണ് വരുന്നത്. നമ്മൾ ഒരു വാതിൽ അടയ്ക്കുമ്പോൾ അവർ മറ്റൊരു ജനലിലൂടെ കയറാൻ ശ്രമിക്കുന്നു. ഈ സാഹചര്യത്തിൽ, കേവലം പ്രതിരോധം എന്നതിനപ്പുറം, കൂടുതൽ സ്മാർട്ടായ ഒരു സമീപനം ആവശ്യമാണ്. അവിടെയാണ് ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം അതിന്റെ പ്രാധാന്യം തെളിയിക്കുന്നത്. കൃത്രിമ ബുദ്ധിയുടെയും (AI) ഓട്ടോമേഷന്റെയും ശക്തി ഒരുമിച്ച് ചേരുമ്പോൾ, സൈബർ ഭീഷണികളെ മുൻകൂട്ടി കണ്ടെത്താനും അവയെ ഫലപ്രദമായി പ്രതിരോധിക്കാനും കഴിവുള്ള ഈ സമഗ്രമായ സമീപനം ഒരുപാട് സാധ്യതകൾ വാഗ്ദാനം ചെയ്യുന്നുണ്ട്. പക്ഷേ, ഏതൊരു നൂതന സാങ്കേതികവിദ്യയെയും പോലെ, ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന് മുന്നിലും ചില വെല്ലുവിളികളുണ്ട്. ഈ വെല്ലുവിളികളെ കൃത്യമായി തിരിച്ചറിയുകയും, അവയ്ക്ക് ഫലപ്രദമായ പരിഹാരമാർഗ്ഗങ്ങൾ കണ്ടെത്തുകയും ചെയ്യുന്നത് ഈ സംവിധാനത്തിന്റെ വിജയകരമായ നടത്തിപ്പിന് അത്യാവശ്യമാണ്.

പ്രധാന വെല്ലുവിളികൾ (Major Challenges)

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം എന്നത് നമ്മുടെ ഡിജിറ്റൽ ലോകത്തിന് ഒരു വലിയ രക്ഷാകവചമാണെന്ന് നമ്മൾ കണ്ടു. പക്ഷേ, ഏതൊരു നൂതനസാങ്കേതികവിദ്യയെയും പോലെ, ഈ സംവിധാനത്തിനും അതിന്റേതായ ചില വെല്ലുവിളികളുണ്ട്. അവയെന്തൊക്കെയാണെന്നും എങ്ങനെയാണ് ഇവയെ നേരിടേണ്ടതെന്നും നമുക്ക് നോക്കാം:

സങ്കീർണ്ണത (Complexity): ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ പ്രധാന വെല്ലുവിളികളിലൊന്നാണ് അതിന്റെ സങ്കീർണ്ണത. ഒരു സ്ഥാപനത്തിന്റെ ഡിജിറ്റൽ അന്തരീക്ഷത്തിൽ പലതരം ഉപകരണങ്ങൾ, പ്ലാറ്റ്ഫോമുകൾ, നെറ്റ്വർക്കുകൾ എന്നിങ്ങനെ ഒരുപാട് കാര്യങ്ങൾ ഒരുമിച്ച് പ്രവർത്തിക്കുന്നുണ്ട്. സുരക്ഷാ ടൂളുകളും വിവരങ്ങൾ വരുന്ന വഴികളും പലപ്പോഴും ഒരുമിച്ചു നിൽക്കാതെ ചിതറിക്കിടക്കും. അങ്ങനെയൊരു സാഹചര്യത്തിൽ, ഒരു സൈബർ ആക്രമണം വന്നാൽ അതിന്റെ ഉറവിടം കണ്ടെത്താനും, ആക്രമണം എത്രത്തോളം പടർന്നു എന്ന് മനസ്സിലാക്കാനും, കൃത്യമായ പ്രതിരോധം നൽകാനും ഈ പലതരം സിസ്റ്റങ്ങളെ ഒരുമിപ്പിച്ച് വിശകലനം ചെയ്യേണ്ടി വരും. ഈ സങ്കീർണ്ണമായ ഘടന, സംവിധാനത്തിന്റെ നടത്തിപ്പും പരിപാലനവും കൂടുതൽ ബുദ്ധിമുട്ടുള്ളതാക്കും.

ഡേറ്റയുടെ അളവും ഗുണനിലവാരവും (Data Volume & Quality): ഡിജിറ്റൽ പ്രതിരോധ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിലെ AI മോഡലുകൾക്ക് നന്നായി പ്രവർത്തിക്കാൻ വലിയ അളവിലുള്ള ഡേറ്റ വേണം. പക്ഷേ, നമ്മൾ ശേഖരിക്കുന്ന ഡേറ്റയുടെ ഗുണനിലവാരം കുറവാണെങ്കിൽ, അത് സുരക്ഷാ മോഡലുകൾ തെറ്റായ തീരുമാനങ്ങളെടുക്കാൻ കാരണമാകും.

സംവിധാനത്തിലെ AI മോഡലുകൾക്ക് നന്നായി പ്രവർത്തിക്കാൻ വലിയ അളവിലുള്ള ഡേറ്റ വേണം. പക്ഷേ, നമ്മൾ ശേഖരിക്കുന്ന ഡേറ്റയുടെ ഗുണനിലവാരം കുറവാണെങ്കിൽ, അത് സുരക്ഷാ മോഡലുകൾ തെറ്റായ തീരുമാനങ്ങളെടുക്കാൻ കാരണമാകും. അനാവശ്യമായ മുന്നറിയിപ്പുകൾ (false positives) ഉണ്ടാകാനും, ശരിക്കും ഉള്ള ഭീഷണികളെ കണ്ടില്ലെന്ന് നടിക്കാനും (false negatives) ഇത് വഴിവെച്ചേക്കാം. അതുകൊണ്ട്, ഡേറ്റയുടെ കൃത്യതയും വിശ്വാസ്യതയും ഉറപ്പാക്കേണ്ടത് വളരെ പ്രധാനമാണ്.

നൈപുണ്യമുള്ള തൊഴിലാളികളുടെ കുറവ് (Lack of Skilled Workforce): ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം രൂപകൽപ്പന ചെയ്യാനും, നടപ്പിലാക്കാനും, പരിപാലിക്കാനുമൊക്കെ AI, സൈബർ സുരക്ഷ, ഡേറ്റാ അനലിറ്റിക്സ് പോലുള്ള മേഖലകളിൽ നല്ല അറിവുള്ള ആളുകളെ ആവശ്യമാണ്. പക്ഷേ, ഈ സാങ്കേതികവിദ്യകളിൽ പ്രാവീണ്യമുള്ള ജീവനക്കാർക്ക് വിപണിയിൽ വലിയ ക്ഷാമമുണ്ട്. അതുകൊണ്ട്, സാങ്കേതികമായി മികച്ച ഒരു സംവിധാനം ഉണ്ടാക്കാൻ സ്ഥാപനങ്ങൾക്ക് ഇത് വലിയൊരു വെല്ലുവിളിയാകും.

സ്വകാര്യതയും നിയമപരമായ വെല്ലുവിളികളും (Privacy & Regulatory Challenges): നമ്മുടെ ഡേറ്റയെ AI ഉപയോഗിച്ച് വിശകലനം ചെയ്യുമ്പോൾ, വ്യക്തികളുടെ സ്വകാര്യതയ്ക്ക് ഭീഷണി വരാനുള്ള സാധ്യതയുണ്ട്. കൂടാതെ, GDPR, HIPAA പോലുള്ള വിവിധ രാജ്യങ്ങളിലെയും പ്രാദേശിക തലത്തിലെയും നിയമങ്ങളും ചട്ടങ്ങളും പാലിക്കുക എന്നത് ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന് മുന്നിലുള്ള മറ്റ് പ്രധാന വെല്ലുവിളികളാണ്. ഡേറ്റ ശേഖരിക്കുന്നതും, സൂക്ഷിക്കുന്നതും, ഉപയോഗിക്കുന്നതുമായി ബന്ധപ്പെട്ട എല്ലാ നിയമങ്ങളും കൃത്യമായി പാലിക്കുന്നുണ്ടെന്ന് ഉറപ്പാക്കേണ്ടത് അത്യാവശ്യമാണ്.

ഈ വെല്ലുവിളികളെല്ലാം ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ വിജയത്തിന് തടസ്സമാകാതിരിക്കാൻ നമ്മൾ അവയെ എങ്ങനെ നേരിടാമെന്ന് നോക്കാം.

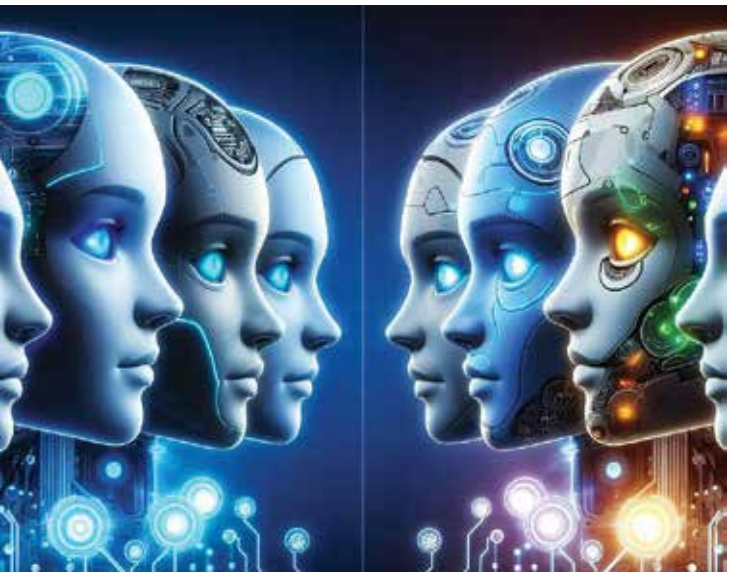
ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം: വിജയത്തിലേക്കുള്ള വഴികൾ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഒരു സ്ഥാപനത്തിന്റെ സൈബർ സുരക്ഷാ കവചത്തെ അടിമുടി ശക്തിപ്പെടുത്തുന്ന ഒരു നിർണായക മുന്നേറ്റമാണെന്ന് നമ്മൾ കണ്ടു. പക്ഷേ, ഇതൊരു നല്ല ആശയം ആണെന്ന് പറഞ്ഞാൽ മാത്രം പോരാ. ഇത് വിജയകരമായി നടപ്പിലാക്കണമെങ്കിൽ പല കാര്യങ്ങളും ഒരുമിച്ച് കൊണ്ടുപോകേണ്ടതുണ്ട്. സാങ്കേതികവിദ്യ, ആളുകളുടെ അറിവും കഴിവും കൂട്ടിയെടുക്കൽ, സ്ഥാപനത്തിന്റെ നയങ്ങൾ, നിയമപരമായ കാര്യങ്ങൾ, ഓട്ടോമേഷൻ രീതികൾ, പിന്നെ എല്ലാവരുമായുള്ള സഹകരണം

ഇവയെല്ലാം ഈ ലക്ഷ്യം നേടുന്നതിൽ ഒരുപോലെ പ്രധാനപ്പെട്ട പങ്കുവഹിക്കുന്നു. ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം വിജയകരമായി നടപ്പിലാക്കാൻ സഹായിക്കുന്ന ചില പ്രധാന വഴികൾ നമുക്ക് പരിശോധിച്ചാലോ?

സാങ്കേതികപരമായ സംയോജനം: സാങ്കേതികപരമായ സംയോജനം ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനത്തിന്റെ അടിത്തറയാണ്. പലപ്പോഴും ഒറ്റപ്പെട്ട രീതിയിൽ പ്രവർത്തിക്കുന്ന വിവിധ സുരക്ഷാ ഉപകരണങ്ങളെയും സംവിധാനങ്ങളെയും ഒരുമിപ്പിക്കേണ്ടത് അത്യാവശ്യമാണ്. ഇതിനായി SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response), EDR (Endpoint Detection & Response) പോലുള്ള പ്ലാറ്റ്ഫോമുകളെ ഒരുമിപ്പിക്കണം. വ്യത്യസ്ത സുരക്ഷാ ടൂളുകൾക്കിടയിൽ API (Application Programming Interface) ഉപയോഗിച്ച് വിവരങ്ങൾ കൈമാറാൻ കഴിഞ്ഞാൽ, എല്ലാം തടസ്സമില്ലാതെ ഒഴുകിനീങ്ങും. ഇത് കൃത്യമായ വിശകലനത്തിനും, ഓട്ടോമാറ്റിക് ആയി പ്രതിരോധം തീർക്കാനും സഹായിക്കും. കൂടാതെ, ക്ലൗഡിലും നമ്മളുടെ സ്വന്തം സിസ്റ്റത്തിലും ഉള്ള സൗകര്യങ്ങൾ ഒരുമിപ്പിച്ച് (ഹൈബ്രിഡ് മോഡൽ) ഉപയോഗിക്കുന്നത് എല്ലാ ഡിജിറ്റൽ ആസ്തികൾക്കും കൃത്യമായ സുരക്ഷാ

ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഫലപ്രദമായി പ്രവർത്തിപ്പിക്കാൻ നല്ല അറിവുള്ള ജീവനക്കാർ അത്യാവശ്യമാണ്. AI, സൈബർ സുരക്ഷ, ഡേറ്റാ സയൻസ് പോലുള്ള മേഖലകളിൽ കഴിവുള്ള ആളുകളുടെ കുറവ് വലിയൊരു വെല്ലുവിളിയാണ്.



തന്ത്രങ്ങൾ ഉണ്ടാക്കാൻ സഹായിക്കും.

ശക്തമായ ഡേറ്റാ ഗവേണൻസ്: AI മോഡലുകൾക്ക് നന്നായി പ്രവർത്തിക്കാൻ ഗുണമേന്മയുള്ള ഡേറ്റ വേണം. അപ്പോൾ മാത്രമാണ് അവർക്ക് ഭീഷണികളെ ശരിയായി തിരിച്ചറിയാനും പ്രവചിക്കാനും കഴിയൂ. അതുകൊണ്ട്, നമ്മൾ ശേഖരിക്കുന്ന ഡേറ്റ വൃത്തിയാക്കാനും, കൃത്യമായി രേഖപ്പെടുത്താനും (ലേബലിംഗ്), നിലവാരമനുസരിച്ച് ക്രമീകരിക്കാനും (സ്റ്റാൻഡേർഡൈസേഷൻ) പോലുള്ള കാര്യങ്ങൾ കൃത്യമായി നടപ്പിലാക്കണം. യൂറോപ്യൻ യൂണിയന്റെ GDPR പോലുള്ള സ്വകാര്യതാ നിയമങ്ങൾ പാലിച്ചുകൊണ്ട് വേണം ഡേറ്റ കൈകാര്യം ചെയ്യാൻ. വ്യക്തിഗത വിവരങ്ങൾ സുരക്ഷിതമാക്കാൻ ഡേറ്റാ അനാനിമൈസേഷൻ പോലുള്ള ടെക്നിക്കുകൾ ഉപയോഗിക്കുകയും വേണം.

AI മോഡലുകളുടെ മെച്ചപ്പെടുത്തൽ: AI മോഡലുകളുടെ പ്രകടനം എപ്പോഴും മെച്ചപ്പെടുത്തിക്കൊണ്ടിരിക്കണം. തെറ്റായ മുന്നറിയിപ്പുകൾ (false positives) കുറയ്ക്കുകയും, ശരിക്കും ഉള്ള ഭീഷണികളെ കണ്ടില്ലെന്ന് നടിക്കുന്നത് (false negatives) ഇല്ലാതാക്കുകയും ചെയ്യേണ്ടത് പ്രധാനമാണ്. ഇതിനായി AI മോഡലുകൾക്ക് കൂടുതൽ തരം ഡേറ്റകൾ നൽകി പരിശീലനം കൊടുക്കണം. മനുഷ്യ വിദഗ്ധർ AI കണ്ടെത്തുന്ന കാര്യങ്ങൾ വിലയിരുത്തി ആവശ്യമെങ്കിൽ തിരുത്തലുകൾ വരുത്തുന്ന Human-in-the-loop എന്ന സമീപനം മോഡലുകളുടെ കൃത്യത വർദ്ധിപ്പിക്കാൻ സഹായിക്കും. കൂടാതെ, Continuous learning mechanism ഉപയോഗിച്ച് പുതിയ ഭീഷണികളെ തിരിച്ചറിയാനും പ്രതിരോധിക്കാനുമുള്ള AI-യുടെ കഴിവ് കാലക്രമേണ കൂട്ടിയെടുക്കണം.

ജീവനക്കാർക്ക് സ്ഥിരമായ പരിശീലനം: ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം ഫലപ്രദമായി പ്രവർത്തിപ്പിക്കാൻ നല്ല അറിവുള്ള ജീവനക്കാർ അത്യാവശ്യമാണ്. AI, സൈബർ സുരക്ഷ, ഡേറ്റാ സയൻസ് പോലുള്ള മേഖലകളിൽ കഴിവുള്ള ആളുകളുടെ കുറവ് വലിയൊരു വെല്ലുവിളിയാണ്. ഇത് മറികടക്കാൻ സ്ഥാപനങ്ങൾ സ്വന്തമായി പരിശീലന പരിപാടികൾ സംഘടിപ്പിക്കുകയും, L&D (Learning & Development) പ്ലാറ്റ്ഫോമുകൾ ഉണ്ടാക്കുകയും വേണം. Coursera, Udemy, BitDegree പോലുള്ള ഓൺലൈൻ കോഴ്സുകൾ ഉപയോഗിച്ച് ജീവനക്കാരുടെ കഴിവ് വർദ്ധിപ്പിക്കാനും സാധിക്കും.

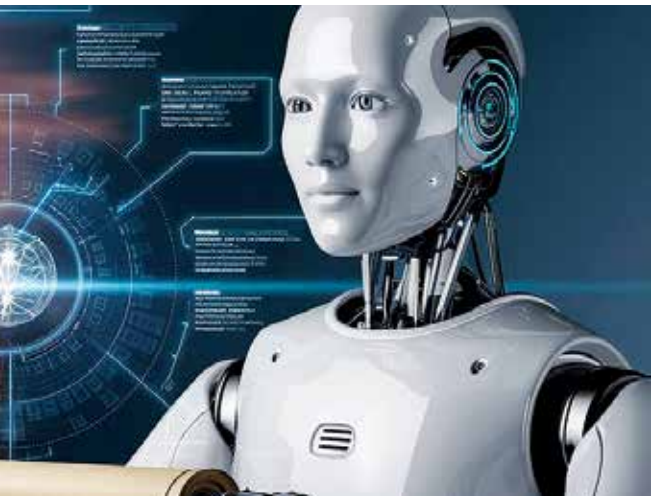
വ്യക്തമായ സുരക്ഷാ നയങ്ങൾ രൂപീകരിക്കുക: എല്ലാം വ്യക്തമായി നിർവചിക്കുന്ന തന്ത്രപരമായ ഉത്തരവാദിത്തങ്ങളും നടപടിക്രമങ്ങളും ഉണ്ടാകണം. നിയമപരമായ പ്രശ്നങ്ങളും, സുരക്ഷാ കാര്യങ്ങളിലെ ശ്രദ്ധയില്ലായ്മയും ഒഴിവാക്കാൻ വ്യക്തമായ സുരക്ഷാ നയങ്ങൾ രൂപീകരിക്കണം. സൈബർ ആക്രമണങ്ങൾ ഉണ്ടായാൽ എന്ത് ചെയ്യണം എന്ന് വിശദീകരിക്കുന്ന ഒരു Incident Response Plan (IRP) തയ്യാറാക്കുകയും, ബിസിനസ്സ് തടസ്സമില്ലാതെ മുന്നോട്ട് കൊണ്ടുപോകാനുള്ള Business Continuity Plan (BCP) ഉണ്ടാക്കുകയും വേണം. കൂടാതെ, നിയമങ്ങൾക്കനുസരിച്ച് സുരക്ഷാ ഓഡിറ്റുകൾ പതിവായി നടത്തുകയും വേണം.

ഓട്ടോമേഷൻ പ്രയോജനപ്പെടുത്തുക: ഓട്ടോമേഷന്റെ സാധ്യതകൾ പൂർണ്ണമായി ഉപയോഗിക്കണം. സുരക്ഷാരംഗത്തെ പതിവായുള്ള ജോലികൾ (അലേർട്ട് ട്രയാജ്, വൈറസ് സ്കാനുകൾ പോലുള്ളവ) ഓട്ടോമേറ്റ് ചെയ്യുന്നതിലൂടെ സുരക്ഷാ ടീമിന്റെ സമയം

സുരക്ഷാരംഗത്തെ പതിവായുള്ള ജോലികൾ (അലേർട്ട് ട്രയാജ്, വൈറസ് സ്കാനുകൾ പോലുള്ളവ) ഓട്ടോമേറ്റ് ചെയ്യുന്നതിലൂടെ സുരക്ഷാ ടീമിന്റെ സമയം ലാഭിക്കാനും, മനുഷ്യന്റെ പിഴവുകൾ ഒഴിവാക്കാനും കഴിയും.

ലാഭിക്കാനും, മനുഷ്യന്റെ പിഴവുകൾ ഒഴിവാക്കാനും കഴിയും. RPA (Robotic Process Automation) ഉപയോഗിച്ച് ആവർത്തന സ്വഭാവമുള്ള പ്രവർത്തനങ്ങൾ കാര്യക്ഷമമായി കൈകാര്യം ചെയ്യാം. അപകടകരമായ സാഹചര്യങ്ങളിൽ സ്വയം പ്രതികരിക്കുന്ന Auto-remediation workflows (ഉദാഹരണത്തിന്, ഹാക്ക് ചെയ്യപ്പെട്ട അക്കൗണ്ട് താൽക്കാലികമായി പ്രവർത്തനരഹിതമാക്കൽ) സ്ഥാപിക്കുന്നത് സുരക്ഷാ പ്രതികരണത്തിന്റെ വേഗത വർദ്ധിപ്പിക്കും.

സൈബർ ലോകത്തെ കൂട്ടായ സഹകരണം: സൈബർ ഭീഷണികളെ ഒറ്റയ്ക്ക് നേരിടുന്നത് അത്ര എളുപ്പമുള്ള കാര്യമല്ല, അല്ലേ? പ്രത്യേകിച്ച്, ഓരോ ദിവസവും പുതിയ രൂപത്തിലും ഭാവത്തിലുമൊക്കെയാണ് ആക്രമണങ്ങൾ വരുന്നത്. അതുകൊണ്ട്, മറ്റ് സ്ഥാപനങ്ങളുമായും സുരക്ഷാ രംഗത്തെ കൂട്ടായ്മകളുമായും സഹകരിക്കുന്നത് വളരെ പ്രയോജനകരമാണ്. ഒരുമിച്ച് നിന്നാൽ ഏത് വലിയ വെല്ലുവിളിയെയും നേരിടാൻ നമുക്ക് കഴിയും. ISACs (Information Sharing and Analysis Centers) പോലുള്ള കൂട്ടായ്മകൾ ഈ സഹകരണത്തിന് വലിയൊരു പ്ലാറ്റ്ഫോമാണ്. ഇവിടെ പുതിയ ഭീഷണികളെക്കുറിച്ചുള്ള വിവരങ്ങൾ പങ്കുവെക്കാനും, എല്ലാവർക്കും ഒരുപോലെ പ്രയോജനപ്പെടുന്ന പ്രതിരോധ തന്ത്രങ്ങൾ ഒരുമിച്ച് വികസിപ്പിക്കാനും കഴിയും. ത്രെട്ട് ഇന്റലിജൻസ് ഫീഡുകൾ (reat intelligence feeds) ഉപയോഗിക്കുന്നത് ഇന്നുള്ളതും ഭാവിയിലുണ്ടാകാൻ സാധ്യതയുള്ളതുമായ ഭീഷണികളെക്കുറിച്ച് നമുക്ക് മുൻകൂട്ടി മുന്നറിയിപ്പ് നൽകും. ഇത് നമ്മളെ കൂടുതൽ ഒരുങ്ങിയിരിക്കാൻ സഹായിക്കും. ചിലപ്പോൾ, എല്ലാ സുരക്ഷാ കാര്യങ്ങൾക്കും സ്വന്തമായി വിദഗ്ധരെ വെക്കാൻ ഒരു സ്ഥാപനത്തിന് കഴിഞ്ഞെന്ന് വരില്ല. അങ്ങനെയുള്ളപ്പോൾ, പ്രത്യേക അറിവുള്ള



മൂന്നാം കക്ഷി സുരക്ഷാ സേവനങ്ങൾ നൽകുന്നവരുമായി (MSSP - Managed Security Service Providers) കൈകോർക്കുന്നത് വിപുലമായ സുരക്ഷാ പരിഹാരങ്ങൾ ലഭ്യമാക്കാനും സഹായിക്കും. ചുരുക്കത്തിൽ, സൈബർ ലോകത്ത് ഒറ്റയാൾ പോരാട്ടം എന്നത് പ്രായോഗികമല്ല, കൂട്ടായ പ്രവർത്തനം തന്നെയാണ് ഏറ്റവും വലിയ ശക്തി.

ഈ പ്രായോഗിക പരിഹാര മാർഗ്ഗങ്ങളെല്ലാം നമ്മൾ ഒരുമിപ്പിച്ച് നടപ്പിലാക്കുകയാണെങ്കിൽ, ഒരു സ്ഥാപനത്തിന് അവരുടെ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം കൂടുതൽ ശക്തിപ്പെടുത്താനും, ഒപ്പം കൂടുതൽ കാര്യക്ഷമമാക്കാനും സാധിക്കും. സാങ്കേതിക വിദ്യകൾ, നമ്മുടെ മനുഷ്യ വിഭവശേഷി, വ്യക്തമായ നയങ്ങൾ, നിയമപരമായ കാര്യങ്ങൾ, ഓട്ടോമേഷൻ രീതികൾ, പിന്നെ എല്ലാവരുമായുള്ള സഹകരണം ഇവയെല്ലാം ശരിയായ രീതിയിൽ ചേർത്തുവെക്കുമ്പോൾ, വർധിച്ചുവരുന്ന സൈബർ ഭീഷണികളെ ഫലപ്രദമായി നേരിടാനും, നമ്മുടെ ഡിജിറ്റൽ സുരക്ഷ ഉറപ്പാക്കാനും നമുക്ക് കഴിയും. ശരിക്കും പറഞ്ഞാൽ, ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം എന്ന് പറയുന്നത് വെറും കുറച്ച് സൈബർ സുരക്ഷാ ഉപകരണങ്ങൾ വാങ്ങി വെക്കുന്നതിനപ്പുറമാണ്. ഇതൊരു സ്ഥാപനത്തിന്റെ ഡിജിറ്റൽ ജീവമണ്ഡലത്തെത്തന്നെ സംരക്ഷിക്കുന്ന, എപ്പോഴും ഉണർന്നിരിക്കുന്ന, നിരന്തരമായി പ്രവർത്തിക്കുന്ന ഒരു പ്രക്രിയയാണ്. ജൈവ ലോകത്തിലെ പ്രതിരോധ സംവിധാനം പോലെ, സൈബർ ഭീഷണികളെ തിരിച്ചറിയാനും, പ്രതിരോധിക്കാനും, അവയിൽ നിന്ന് പഠിച്ച് കൂടുതൽ കരുത്തോടെ മുന്നോട്ട് പോകാനും ഇത് സ്ഥാപനങ്ങളെ പ്രാപ്തരാക്കുന്നു. കൃത്രിമ ബുദ്ധിയുടെ (AI) ബുദ്ധിയും, ഓട്ടോമേഷന്റെ വേഗതയും കൃത്യതയും, ഡേറ്റാ അനലിറ്റിക്സിന്റെ ആഴത്തിലുള്ള ഉൾക്കാഴ്ചയും ഒരുമിച്ചു ചേരുമ്പോൾ, നാളത്തെ സൈബർ ലോകത്തെ വെല്ലുവിളികളെ അതിജീവിക്കാൻ ശേഷിയുള്ള ഒരു ശക്തമായ ഡിജിറ്റൽ രക്ഷാകവചം നമുക്ക് സൃഷ്ടിക്കാൻ കഴിയും. ഈ സാങ്കേതികവിദ്യകളെ ബുദ്ധിപരമായി ഉപയോഗിക്കുന്നതിലൂടെ, സ്ഥാപനങ്ങൾക്ക് അവരുടെ ഡിജിറ്റൽ ഭാവിയെ സുരക്ഷിതമാക്കുകയും, ഒപ്പം തടസ്സങ്ങളില്ലാതെ വളർച്ച നേടുകയും ചെയ്യാം. അതുകൊണ്ട്, ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനം എന്നത് വെറുമൊരു സാങ്കേതിക പരിഹാരമല്ല, മറിച്ച് ഡിജിറ്റൽ യുഗത്തിലെ അതിജീവനത്തിനുള്ള ഒരു തന്ത്രപരമായ നിക്ഷേപം കൂടിയാണ്. ഡിജിറ്റൽ ലോകം സുരക്ഷിതമാകുമ്പോൾ മാത്രമാണ് അതിന്റെ പൂർണ്ണമായ സാധ്യതകൾ നമുക്ക് പ്രയോജനപ്പെടുത്താൻ സാധിക്കുകയുള്ളൂ. സൈബർ സുരക്ഷാ തന്ത്രങ്ങളുടെ ഭാവി ഈ ഡിജിറ്റൽ പ്രതിരോധ സംവിധാനങ്ങളിലായിരിക്കും എന്നതിൽ ഒരു സംശയവുമില്ല. ഒരു സുരക്ഷിതമായ ഡിജിറ്റൽ ഭാവിക്കായി നമുക്ക് കൈകോർക്കാം.

കമ്പ്യൂട്ടർ പുസ്തകങ്ങൾ മലയാള ഭാഷയിൽ

ഇൻഫോകൈരളിയിൽ നിന്നും പ്രസിദ്ധീകരിച്ച 36 വ്യത്യസ്ത കമ്പ്യൂട്ടർ പുസ്തകങ്ങൾ

1.	കംപ്യൂട്ടർ ഗുരുകുലം– ടാലി GST	:	വില–200/
2.	കംപ്യൂട്ടർ ഗുരുകുലം– JAVA	:	വില–200/
3.	കംപ്യൂട്ടർ ഗുരുകുലം– വിഷ്വൽ ബേസിക്	:	വില– 200/
4.	കംപ്യൂട്ടർ ഗുരുകുലം– ഓക്കിൾ	:	വില– 200/
5.	ഹാർഡ് വെയർ	:	വില– 200/
6.	അഡോബി ഇല്യുസ്ട്രേറ്റർ	:	വില–200/
7.	നിങ്ങൾക്കും തുടങ്ങാം സ്വന്തം വെബ്സൈറ്റ്	:	വില–200/
8.	ഫോട്ടോഷോപ്പ് പഠിക്കാം	:	വില–200/
9.	മാസ്റ്ററിംഗ് ഓട്ടോ കാർഡ്	:	വില–275/
10.	ഫ്ലാഷ് ദി 2ഡി ആനിമേറ്റർ	:	വില–250/
11.	ഇൻറർനെറ്റ്– അറിഞ്ഞതും അതിനപ്പുറവും	:	വില–250/
12.	ആനിമേഷൻ അടിസ്ഥാനതത്വങ്ങളും എളുപ്പവഴികളും	:	വില–150/
13.	LCD മോണിറ്റർ റിപ്പയറിംഗ്	:	വില–90/
14.	വിൻഡോസ് 7 ടിപ്സ് & ട്രിക്സ്	:	വില–90/
15.	ഓഫീസ് ടിപ്സ് & ട്രിക്സ്	:	വില–90/
16.	ലിനക്സ്	:	വില–90/
17.	HTML	:	വില–90/
18.	ഇലക്ട്രോണിക്സ്	:	വില–90/
19.	ഗ്നു /ലിനക്സ്	:	വില–90/
20.	ടെക് ഡിക്ഷ്ണറി	:	വില–75/
21.	മൊബൈൽ ഫോൺ റിപ്പയറിംഗ്	:	വില–120/
22.	ഇൻറർനെറ്റിലൂടെ സമ്പാദിക്കാം	:	വില–120/
23.	ഇൻറർനെറ്റ് ടിപ്സ് & ട്രിക്സ്	:	വില–100/
24.	മലയാളം കംപ്യൂട്ടിംഗ്	:	വില–100/
25.	ഇൻറർനെറ്റ് സുരക്ഷാ	:	വില–50/

ഇൻഫോകൈരളി അക്കാദമിക് സീരീസ് ബുക്കുകൾ

1.	Basics of Computer	:	Rs. 75/
2.	Computer Hardware & Basic Networking	:	Rs. 90/-
3.	Tally	:	Rs. 90/-
4.	C programming	:	Rs. 90/-
5.	C++	:	Rs. 90/-
6.	DTP	:	Rs. 120/-
7.	Mobile Phone Repairing & Servicing	:	Rs. 150/-
8.	SQL & VB.NET	:	Rs. 200/-

മുഖവിലയിൽ നിന്ന് 10% വില കുറവിൽ പുസ്തകങ്ങൾ ലഭ്യമാണ്. പുസ്തകങ്ങൾ സ്വന്തമാക്കാനായി വിളിക്കുക 9447124390
എല്ലാ പ്രമുഖ ബുക്ക് സ്റ്റാളുകളിലും ഈ പുസ്തകങ്ങൾ ലഭ്യമാണ്.

ഇൻഫോകൈരളി പുസ്തകങ്ങളുടെ വില നേരിട്ട് ബാങ്കിൽ അയയ്ക്കാം
Name : INFOKAIRALI A/c No- 67003574237,Branch- Kuruppanthara, Bank- State Bank of India,
Ac Type- Current account IFSC code- SBIN0070136
ഗൂഗിൾ പേ നമ്പർ: 9447124391

പേയ്മെന്റ് അടച്ചശേഷം വാട്സ്ആപ്പ് (9447124390)/ മെയിൽ (kairali.info@gmail.com) മുഖാന്തരം നിങ്ങളുടെ പേര്, മൊബൈൽ നമ്പർ, വിലാസം എന്നീ വിവരങ്ങൾ ഇൻഫോകൈരളിയെ അറിയിക്കുമല്ലോ

ഗിമ്പ് 3.0: ഓപ്പൺ സോഴ്സ് ഇമേജ് എഡിറ്റിംഗിന്റെ പുതിയ മാറ്റങ്ങൾ

റിൻസി ജോൺ

ഗിമ്പ് (GNU ഇമേജ് മാനിപുലേഷൻ പ്രോഗ്രാം) ഒരു സൗജന്യ, ഓപ്പൺ സോഴ്സ് ഇമേജ് എഡിറ്റിംഗ് സോഫ്റ്റ്വെയറാണ്. ഫോട്ടോ എഡിറ്റിംഗ്, ഗ്രാഫിക് ഡിസൈൻ, ഡിജിറ്റൽ ആർട്ട് എന്നിവയ്ക്കായി ലോകമെമ്പാടുമുള്ള ഉപയോക്താക്കൾ ഗിമ്പ് ഉപയോഗിക്കുന്നു. അഡോബ് ഫോട്ടോഷോപ്പിന്റെ ശക്തമായ ഒരു പകരക്കാരനായി ഗിമ്പ് വർഷങ്ങളായി പ്രശസ്തമാണ്. ഗിമ്പ് 3 റിലീസായ വാർത്ത അറിഞ്ഞിരിക്കുമല്ലോ. ഗിമ്പ് 3 മാറ്റങ്ങൾ അറിഞ്ഞിരിക്കാം.

ഗിമ്പ് 3 റിലീസിന്റെ പ്രാധാന്യം

കാത്തിരിപ്പുകൾക്ക് വിരാമമിട്ടുകൊണ്ട് ഗിമ്പ് 3.0 2025 മാർച്ച് 23-ന് പുറത്തിറങ്ങിയിരിക്കുന്നു. നോൺ-ഡിസ്ട്രക്റ്റീവ് എഡിറ്റിംഗ്, മോഡേൺ യൂസർ ഇന്റർഫേസ്, മെച്ചപ്പെട്ട ഫീച്ചറുകൾ എന്നിവയിലൂടെ ഗിമ്പ് 3.0 ഓപ്പൺ സോഴ്സ് സോഫ്റ്റ്വെയറിന് ഒരു മുതൽക്കൂട്ടാവുകയാണ്. ഗിമ്പ് 3 യുടെ പുതിയ സവിശേഷതകൾ മനസ്സിലാക്കാം.

ഗിമ്പ് 3: പുതിയ സവിശേഷതകൾ

നോൺ-ഡിസ്ട്രക്റ്റീവ് എഡിറ്റിംഗ്

ചിത്രത്തിന്റെ ഒറിജിനൽ ഡേറ്റയെ ബാധിക്കാതെ എഡിറ്റിംഗ് നടത്താം. ഫിൽട്ടറുകൾ, അഡ്ജസ്റ്റ്മെന്റുകൾ എന്നിവ ലെയറുകളായി ചെയ്യാം.

ഫിൽട്ടറുകൾ ഓൺ/ഓഫ് ചെയ്യാം, പരാമീറ്ററുകൾ എപ്പോൾ വേണമെങ്കിലും മാറ്റാം. ഉദാഹരണത്തിന്, ബ്രൈറ്റ്നസ് അഡ്ജസ്റ്റ് ചെയ്ത ശേഷം, പിന്നീട് അത് റിവേഴ്സ് ചെയ്യാം.(പിൻവലിക്കാം/ അൺഡു)

ജിടികെ 3 അടിസ്ഥാനമാക്കിയ പുതിയ യൂസർ ഇന്റർഫേസ്

HiDPI സ്ക്രീനുകൾ: ഹൈ-റെസല്യൂഷൻ ഡിസ്പ്ലേകളിൽ ഐക്കണുകളും ടെക്സ്റ്റും ഷാർപ്പ് ആയിരിക്കും.

വെയ്ലാൻഡ് സപ്പോർട്ട്: ലിനക്സിൽ വെയ്ലാൻഡ് പ്രോട്ടോക്കോളിന് നേറ്റീവ് സപ്പോർട്ട് (പ്ലഗ്ഇൻ ആവശ്യമില്ല. ബിൽറ്റ് ഇൻ സപ്പോർട്ട്). ഇതുവരെ ഗിമ്പ് പ്രധാനമായും X11 എന്ന പഴയ ലിനക്സ് ഗ്രാഫിക്കൽ സിസ്റ്റം ഉപയോഗിച്ച് പ്രവർത്തിച്ചിരുന്നതാണ്. വെയ്ലാൻഡ് സുരക്ഷിതമാണ്.

തീം കസ്റ്റമൈസേഷൻ: CSS ഉപയോഗിച്ച് ഇന്റർഫേസിന്റെ തീമുകൾ മാറ്റാം, ഉപയോക്താക്കൾക്ക് താല്പര്യമുള്ള വിധം ക്രമീകരിക്കാം.

മൾട്ടി-ലെയർ സെലക്ഷൻ

ഒന്നിലധികം ലെയറുകൾ: ഒരേസമയം ഒന്നിലധികം ലെയറുകൾ തിരഞ്ഞെടുത്ത് എഡിറ്റ് ചെയ്യാം.

ബാച്ച് ഓപ്പറേഷനുകൾ: ഒന്നിലധികം ലെയറുകളിൽ ഒരേ മാറ്റങ്ങൾ (ഉദാ: റീസൈസ്, ഫിൽട്ടർ)

ഫോട്ടോ എഡിറ്റിംഗ്, ഗ്രാഫിക് ഡിസൈൻ, ഡിജിറ്റൽ ആർട്ട് എന്നിവയ്ക്കായി ലോകമെമ്പാടുമുള്ള ഉപയോക്താക്കൾ ഗിമ്പ് ഉപയോഗിക്കുന്നു. അഡോബ് ഫോട്ടോഷോപ്പിന്റെ ശക്തമായ ഒരു പകരക്കാരനായി ഗിമ്പ് വർഷങ്ങളായി പ്രശസ്തമാണ്.

പെയിന്റ് സെലക്ട് ടൂൾ

സങ്കീർണ്ണമായ ഒബ്ജക്ടുകളെ എളുപ്പത്തിൽ സെലക്ട് ചെയ്യാൻ സഹായിക്കുന്ന AI-അധിഷ്ഠിത പെയിന്റ് സെലക്ട് ടൂൾ. പെയിന്റ് ബ്രഷ് പോലെ ഒബ്ജക്ടിന്റെ മുകളിൽ വരയ്ക്കുക, ടൂൾ സ്വയം അതിന്റെ എഡ്ജുകൾ കണ്ടെത്തും.

വെൽക്കം ഡയലോഗ്

ഗിമ്പ് തുറക്കുമ്പോൾ ഒരു വെൽക്കം ഡയലോഗ് കാണാം, അവിടെ നിന്ന് പുതിയ ചിത്രം, ടെംപ്ലേറ്റുകൾ, അല്ലെങ്കിൽ ഫയലുകൾ തുറക്കാം. തുടക്കക്കാർക്ക് എളുപ്പമായിരിക്കും.

ഗിമ്പ് 3: മറ്റ് ഫീച്ചറുകൾ

കളർ മാനേജ്മെന്റ്

അഡോബ് RGB: പ്രൊഫഷണൽ ഫോട്ടോഗ്രാഫർമാർക്കായി RGB കളർ സ്പേസ് സപ്പോർട്ട്

CMYK, LAB: CMYK, LAB കളർ മോഡുകൾക്കുള്ള തയ്യാറെടുപ്പ്, പ്രിന്റിംഗിന് ഉപയോഗപ്രദമാകും.

ഫയൽ ഫോർമാറ്റ് സപ്പോർട്ട്

PSD സപ്പോർട്ട്: അഡോബ് ഫോട്ടോഷോപ്പിന്റെ PSD ഫയലുകൾ മെച്ചപ്പെട്ട രീതിയിൽ തുറക്കാനും എഡിറ്റ് ചെയ്യാനും കഴിയും.

പുതിയ ഫോർമാറ്റുകൾ: JPEG XL, QOI, AVIF, WebP എന്നിവയ്ക്ക് സപ്പോർട്ട്.

പെർഫോമൻസ് ഫീച്ചറുകൾ

റെൻഡർ കാഷിംഗ്: ഫിൽട്ടറുകളും എഡിറ്റിംഗും വേഗത്തിലാക്കാൻ കാഷിംഗ്.

മൾട്ടി-ത്രെഡിംഗ്: മൾട്ടി-കോർ CPU-കളെ പൂർണമായി ഉപയോഗിക്കുന്നു, വേഗത വർധിപ്പിക്കുന്നു.

പ്ലഗിൻ, സ്ക്രിപ്റ്റ് മാറ്റങ്ങൾ

പുതിയ API: പ്ലഗിനുകൾക്കായി Python 3, JavaScript API-കൾ.

പോരായ്മകൾ: ഗിമ്പ് 2.10-ന്റെ ചില പഴയ പ്ലഗിനുകൾ ജിമ്പ് 3 യിൽ പ്രവർത്തിക്കില്ല.

ജനപ്രിയ പ്ലഗിനുകൾ: G'MIC, Resynthesizer എന്നിവയ്ക്ക് അപ്ഡേറ്റുകൾ ലഭ്യമാണ്, പക്ഷേ എല്ലാ പ്ലഗിനുകളും ഇതുവരെ പൊരുത്തപ്പെട്ടിട്ടില്ല.

ഗിമ്പ് 3: ചവിട്ടുപടികൾ

7 വർഷത്തെ കഠിനാധ്വാനത്തിന്റെ ഫലമാണ് ഗിമ്പ് 3.0. സങ്കീർണ്ണമായ കോഡ് മാറ്റങ്ങളും ബഗ് ഫിക്സിംഗും കാരണം റിലീസ് വൈകി.

സിസ്റ്റം സപ്പോർട്ട്

പ്ലാറ്റ്ഫോമുകൾ: വിൻഡോസ്, macOS, ലിനക്സ് (Wayland, X11).

ഹാർഡ്വെയർ: കുറഞ്ഞത് 4GB RAM, 1GB സ്റ്റോറേജ്; GPU ആക്സിലറേഷനുള്ള മോഡേൺ ഹാർഡ്വെയർ.

ഗിമ്പ് 3 എങ്ങനെ ഡൗൺലോഡ് ചെയ്യാം?

വെബ്സൈറ്റ്: www.gimp.org-ൽ നിന്ന് ഡൗൺലോഡ് ചെയ്യാം.

ഇൻസ്റ്റാളേഷൻ

ഔദ്യോഗിക സൈറ്റിൽ നിന്ന് OS-ന് അനുയോജ്യമായ പതിപ്പ് തിരഞ്ഞെടുക്കുക.

ഡൗൺലോഡ് ചെയ്ത ഫയൽ റൺ ചെയ്യുക.

ഇൻസ്റ്റാളർ നിർദ്ദേശങ്ങൾ പാലിക്കുക.

ഗിമ്പ്: ഫോട്ടോ എഡിറ്റിങ് vs ഡിജിറ്റൽ പെയിന്റിങ്

ഫോട്ടോ എഡിറ്റിംഗ്: ഗിമ്പ് ഫോട്ടോ റീട്ടച്ചിംഗ്, കളർ കറക്ഷൻ, കോമ്പോസിഷൻ എന്നിവയിൽ മികച്ചതാണ്.

ഡിജിറ്റൽ പെയിന്റിങ്: ഗിമ്പിന് പെയിന്റിങ് ടൂളുകളുണ്ടെങ്കിലും, കൃത (Krita) പോലുള്ള സോഫ്റ്റ്വെയറുകൾ ഇതിന് കൂടുതൽ അനുയോജ്യമാണ്.

പകരക്കാർ: ഫോട്ടോഷോപ്പ് (പണമടച്ച്), Photopea (ഓൺലൈൻ), Paint.NET (ലളിതമായ എഡിറ്റിംഗ്).

ഗിമ്പ് vs അഡോബ്

ഗിമ്പ്: സൗജന്യം, ഓപ്പൺ സോഴ്സ്, കമ്മ്യൂണിറ്റി സപ്പോർട്ട്.

അഡോബ്: പ്രൊഫഷണൽ-ഗ്രേഡ്, വില കൂടുതൽ, സബ്സ്ക്രിപ്ഷൻ മോഡൽ.

ഭാവി പദ്ധതികൾ

ഗിമ്പ് 3.2: ബഗ് ഫിക്സുകൾ, UI മെച്ചപ്പെടുത്തലുകൾ, പുതിയ ഫിൽട്ടറുകൾ.

നാൾവഴികൾ: മെച്ചപ്പെട്ട CMYK സപ്പോർട്ട്, AI-അധിഷ്ഠിത ടൂളുകൾ, വേഗത.

ഫോട്ടോ ഫ്രെയിം ക്യാമ്പെയിനുകൾക്ക് സുസ്ഥിര ഡിജിറ്റൽ പരിഹാരം

സൽമാൻ ഷാ ടി. എൻ.

ഡിജിറ്റൽ ലോകം അതിവേഗം മുന്നേറുന്ന കാലത്താണ് വ്യക്തിഗത അഭിപ്രായങ്ങളും സമൂഹപരമായ സന്ദേശങ്ങളും സോഷ്യൽ മീഡിയയിലൂടെ വ്യാപകമായി പ്രചരിക്കുന്നത്. ഈ പശ്ചാത്തലത്തിലാണ് ഫോട്ടോ ഫ്രെയിം ക്യാമ്പെയിൻ വെബ്സൈറ്റ് എന്ന ആശയം ജനപ്രീതി നേടുന്നത്. വ്യക്തികൾക്ക് തങ്ങളുടെ പ്രൊഫൈൽ ചിത്രങ്ങൾ പ്രതിപാദ്യമായ സന്ദേശങ്ങൾ ഉൾക്കൊള്ളുന്ന ഫ്രെയിമുകളിൽ ആക്കുന്നതിനുള്ള അവസരമാണ് ഇത്തരം വെബ്സൈറ്റുകൾ നൽകുന്നത്. രാഷ്ട്രീയ ക്യാമ്പയിനുകൾ സെമിനാറുകൾ, ക്യാമ്പയിനുകൾ, വിദ്യാഭ്യാസ സ്ഥാപനങ്ങൾക്കായുള്ള ക്യാമ്പയിനുകൾ പവലിധ വാർഷികാഘോഷങ്ങൾ എന്നിവയ്ക്കായി ഫോട്ടോ ഫ്രെയിം ക്യാമ്പെയിനുകൾ നടത്തപ്പെടുന്നു.

ഉദ്ദേശ്യവും പ്രാധാന്യവും

ഫോട്ടോ ഫ്രെയിം ക്യാമ്പെയിൻ വെബ്സൈറ്റിന്റെ പ്രധാന ലക്ഷ്യം വ്യക്തിഗത (Personalized) സാമൂഹിക അവബോധം പ്രകടമാക്കു

ഫോട്ടോ ഫ്രെയിം ക്യാമ്പെയിൻ വെബ്സൈറ്റിന്റെ പ്രധാന ലക്ഷ്യം വ്യക്തിഗത (Personalized) സാമൂഹിക അവബോധം പ്രകടമാക്കുന്നതിനുള്ള സംവിധാനമായി പ്രവർത്തിക്കുക എന്നതാണ്.

ന്നതിനുള്ള സംവിധാനമായി പ്രവർത്തിക്കുക എന്നതാണ്. പരിസ്ഥിതി സംരക്ഷണം, ആരോഗ്യ ബോധവത്കരണം വിദ്യാഭ്യാസ സ്ഥാപനങ്ങൾക്കായുള്ള ക്യാമ്പയിനുകൾ, തിരഞ്ഞെടുപ്പ് ക്യാമ്പയിനുകൾ തുടങ്ങിയ വിഷയങ്ങളിലായി വിവിധ ഫ്രെയിമുകൾ ഇവിടെ ലഭ്യമാകുന്നു. അതിന് പുറമെ മുൻപ് വിദ്യാഭ്യാസ പരിപാടികളിലും സാമൂഹിക ക്യാമ്പയിനുകളിലും വ്യാപകമായി ഉപയോഗിച്ചിരുന്നത് പ്ലാസ്റ്റിക് ഫ്രെയിമുകളാണ്—പ്രത്യേകിച്ച് ഫോട്ടോ എടുക്കുന്നതിനായി ഒരുക്കുന്ന "photo booth" ഡിസൈൻ ചെയ്ത സ്റ്റാൻഡുകൾ, ബോർഡുകൾ എന്നിവ പ്രേക്ഷകരെ ആകർഷിക്കുന്നതിനുള്ള ആശയങ്ങൾ പങ്കുവെക്കാനുള്ള മാർഗമായിരുന്നുവെങ്കിലും, പിന്നീട് ഇവ പ്ലാസ്റ്റിക് മാലിന്യത്തിൽ കണപ്പെടുകയും ഒട്ടനവധി പരിസ്ഥിതിക്ക് ഹാനികരമായ അവസ്ഥകൾ സൃഷ്ടിക്കുകയും ചെയ്തു.

ഇത്തരം സാഹചര്യത്തിൽ FrameWaves.com പോലുള്ള വെബ്സൈറ്റുകൾ പരിസ്ഥിതിയുടെയും സാങ്കേതികതയുടെയും ചേർച്ചയിലൂടെ മികച്ച പരിഹാരമായി മാറുന്നു. വിദ്യാലയങ്ങൾ, കോളേജുകൾ, രാഷ്ട്രീയ കക്ഷികൾ തുടങ്ങിയ സംഘടനകൾക്ക് അവരുടെ സന്ദേശങ്ങൾ ഡിജിറ്റൽ ഫ്രെയിമുകൾ വഴി പ്രചരിപ്പിക്കാൻ ഇതൊരു അനുയോജ്യമായ മാർഗമാണ്.

FrameWaves.com എന്താണ്?

FrameWaves ഒരു ഓൺലൈൻ ഫോട്ടോ ഫ്രെയിം ക്യാമ്പെയിൻ പ്ലാറ്റ്ഫോമാണ്, നിങ്ങളുടെ പ്രോഗ്രാം, ക്യാമ്പെയിൻ, ഫെസ്റ്റിവൽ, കോളേജ് യൂത്ത് ഫെസ്റ്റ് മുതലായവക്ക് വ്യക്തിഗതമായി ബ്രാൻഡുചെയ്ത ഫ്രെയിമുകൾ സൃഷ്ടിക്കാനും പങ്കുവെക്കാനും സഹായിക്കുന്നു.

സവിശേഷതകൾ

നിങ്ങളുടെ ഇൻസ്റ്റിറ്റ്യൂഷൻ/സംഘടനയുടെ ലോഗോ, പ്രതിപാദ്യ സന്ദേശം, ആഗ്രഹിക്കുന്ന രൂപകൽപ്പന ഉൾപ്പെടുത്തി ഫ്രെയിം സൃഷ്ടിക്കാം

പങ്കാളികൾക്ക് അവരുടെ പ്രൊഫൈൽ ചിത്രത്തിൽ ആ ഫ്രെയിം ചേർക്കാൻ ലളിതമായ സംവിധാനം

No app download – വെബ്സൈറ്റ് വഴി നേരിട്ട്

Eco-friendly: പ്ലാസ്റ്റിക് ഫ്രെയിമുകൾ ഒഴിവാക്കുന്നു, മാലിന്യം ഇല്ല

സൗജന്യ/താണ നിരക്കുകൾ: ചെലവേറിയ പ്രിന്റിങ് ഒഴിവാക്കാം

സമൂഹമാധ്യമങ്ങളിലൂടെ വേഗത്തിൽ പ്രചരിപ്പിക്കാം

വിദ്യാർത്ഥികൾക്കും പങ്കാളികൾക്കും വീട്ടിൽ നിന്നോ മൊബൈലിലൂടെയോ പങ്കെടുത്ത് ഫ്രെയിം ഉപയോഗിക്കാം

ഉദാഹരണം:

മുമ്പ്, "Science Fest 2023" എന്ന പരിപാടിയിൽ വലിയ പ്ലാസ്റ്റിക് ഫ്രെയിം തയ്യാറാക്കിയിരുന്നു. അതിന്റെ ഉപയോഗശേഷം അതിനെ എങ്ങനെയെങ്കിലും ഒഴിവാക്കേണ്ടി വന്നു.

എന്നാൽ 2024-ൽ, അതേ പരിപാടിക്ക് FrameWaves.com വഴി ഡിജിറ്റൽ ഫ്രെയിം സൃഷ്ടിച്ചു, മുഴുവൻ വിദ്യാർത്ഥികളും അവരുടെ പ്രൊഫൈൽ ചിത്രങ്ങളിൽ അതുപയോഗിച്ചു, നിരവധി ആളുകൾക്ക് അത് ഷെയർ ചെയ്യാനും റീച്ച് ചെയ്യാനും സാധിച്ചു.

പ്രവർത്തന രീതി

ഫോട്ടോ ഫ്രെയിം ക്യാമ്പെയിൻ വെബ്സൈറ്റ് ഉപയോഗിക്കുന്നത് വളരെ ലളിതമാണ്:

ഉപയോക്താവ് തന്റെ ചിത്രം വെബ്സൈറ്റിലേക്ക് അപ്ലോഡ് ചെയ്യുന്നു

ഇഷ്ടപ്പെട്ട ഫ്രെയിം തിരഞ്ഞെടുക്കുന്നു

ചുവടെ ഒരു പ്രിവ്യൂ ലഭിക്കുന്നു

ആ ചിത്രം ഡൗൺലോഡ് ചെയ്ത് പ്രൊഫൈൽ

Twibbonize എന്നത് ഒരു സൗജന്യ പ്ലാറ്റ്ഫോമാണ്.ഇത് ഉപയോഗിച്ച് നിങ്ങൾക്ക് നിങ്ങളുടെ പ്രൊഫൈൽ ഫോട്ടോകൾക്ക് (Facebook, Instagram, Whatsapp മുതലായവ) പ്രത്യേകമായ ഒരു ഫ്രെയിം ചേർത്ത് ഒരേ സമയത്ത് ഒരുപാട് ആളുകളെ ക്യാമ്പെയിൻ പ്രചരിപ്പിക്കാം.

ചിത്രമായി ഉപയോഗിക്കാം

വിലകൊടുത്ത റെഡിമേഡ് ആപ്പ് അല്ലാതെ, ഓരോ വ്യക്തിക്കും ഉദ്ദേശിച്ച സന്ദേശം അടങ്ങിയ ഫ്രെയിം തിരഞ്ഞെടുക്കാനും അതിന്റെ അടിസ്ഥാനത്തിൽ സ്വന്തം വ്യക്തിത്വം പ്രകടിപ്പിക്കാനും അവസരമൊരുക്കുന്ന ഒരു ജനാധിപത്യ പ്ലാറ്റ്ഫോമാണ് ഇത്.

സാമൂഹിക വിപ്ലവത്തിനുള്ള സംഭാവന

വിവിധ പൊതുപ്രശ്നങ്ങൾക്കും പ്രതിപാദ്യങ്ങൾക്കും പിന്തുണയറിയിക്കാൻ, സമൂഹമാധ്യമങ്ങൾ ഉപയോഗിക്കുന്ന നൂതന മാർഗമാണ് ഈ ക്യാമ്പെയിൻ. പൊതുജനങ്ങൾക്കിടയിൽ ബോധവത്കരണ പ്രവർത്തനങ്ങൾ ശക്തമാക്കുന്നതിനും ഒറ്റ ചിത്രത്തിലൂടെ വലിയ സന്ദേശങ്ങൾ പ്രചരിപ്പിക്കുന്നതിനും ഇത് ഉപകരിക്കുന്നു.

ഭാവി സാധ്യതകൾ

ഭാവിയിൽ കൂടുതൽ ഭാഷാസഹായം, പ്രത്യേക ഇനങ്ങൾക്കായി ഡൈനാമിക് ഫ്രെയിമുകൾ, ഫ്രെയിം സൃഷ്ടിക്കാൻ ഉപയോക്താക്കൾക്ക് അവസരം എന്നിങ്ങനെയുള്ള ആധുനിക ഘടകങ്ങൾ ഉൾപ്പെടുത്തി ഈ പ്ലാറ്റ്ഫോം വികസിപ്പിക്കാൻ സാധ്യതയുണ്ട്. രാഷ്ട്രീയ ക്യാമ്പെയിനുകൾ മുതൽ സാമൂഹിക പ്രവർത്തനങ്ങൾ വരെ, ഫോട്ടോ ഫ്രെയിം ക്യാമ്പെയിൻ വെബ്സൈറ്റ് ഒരു കരുത്തുറ്റ മീഡിയ ഉപാധിയായി

മാറുകയാണ്.

Twibbonize എന്താണ്?

Twibbonize എന്നത് ഒരു സൗജന്യ പ്ലാറ്റ്ഫോമാണ്.

ഇത് ഉപയോഗിച്ച് നിങ്ങൾക്ക് നിങ്ങളുടെ പ്രൊഫൈൽ ഫോട്ടോകൾക്ക് (Facebook, Instagram, Whats App മുതലായവ) പ്രത്യേകമായ ഒരു ഫ്രെയിം ചേർത്ത് ഒരേ സമയത്ത് ഒരുപാട് ആളുകളെ ക്യാമ്പെയിൻ പ്രചരിപ്പിക്കാം.

1. Twibbonize വെബ്സൈറ്റ് തുറക്കുക

twibbonize.com എന്ന സൈറ്റിൽ പോകുക.

2. ലോഗിൻ ചെയ്യുക അല്ലെങ്കിൽ ക്യാമ്പെയിൻ തിരയുക

പുതിയ ക്യാമ്പെയിനുകൾ തിരയാം (ഉദാ: കേരള അവകാശദിനം, വിദ്യാഭ്യാസ ബോധവൽക്കരണം തുടങ്ങിയവ)

അല്ലെങ്കിൽ നിങ്ങളുടെ അക്കൗണ്ട് ഉണ്ടാക്കി പുതിയ ക്യാമ്പെയിൻ തുടങ്ങാം.

3. Frame തെരഞ്ഞെടുക്കുക

നിങ്ങൾക്ക് ഇഷ്ടമുള്ള ഫ്രെയിം/ക്യാമ്പെയിൻ തെരഞ്ഞെടുക്കുക.

4. നിങ്ങളുടെ ഫോട്ടോ അപ്ലോഡ് ചെയ്യുക

നിങ്ങളുടെ പ്രൊഫൈൽ ഫോട്ടോ അപ്ലോഡ് ചെയ്ത് ഫ്രെയിമിന്റെ കൂടെ ചേർക്കുക.

5. ഡൗൺലോഡ് ചെയ്ത് ഷെയർ ചെയ്യുക

റെഡിയായ ചിത്രം ഡൗൺലോഡ് ചെയ്ത് നിങ്ങളുടെ സോഷ്യൽ മീഡിയയിൽ പോസ്റ്റ് ചെയ്യാം.

കംപ്യൂട്ടർ ഓപ്പറേറ്റർ ആന്റ് പ്രോഗ്രാമിങ് അസിസ്റ്റന്റ്; തൊഴിൽ നേടുവാൻ മികച്ച കംപ്യൂട്ടർ കോഴ്സ്

വിജയകുമാർ റ്റി.ഡി
പ്രൈവറ്റ് ഐടിഐ മാനേജ്മെന്റ് അസോസിയേഷൻ

മികച്ച ജോലി ലക്ഷ്യംവയ്ക്കുന്ന പ്ലസ് ടു, ഡിഗ്രി കഴിഞ്ഞവർക്ക് ഏറ്റവും അനുയോജ്യമായ കോഴ്സാണ് കേന്ദ്ര ഗവൺമെന്റ് NCVT യുടെ അംഗീകാരത്തോടെയും പൂർണ്ണ നിയന്ത്രണത്തിലും നടത്തപ്പെടുന്ന കംപ്യൂട്ടർ ഓപ്പറേറ്റർ ആൻഡ് പ്രോഗ്രാമിങ് അസിസ്റ്റന്റ്(CO&PA). ഇന്ത്യയിലെ ഏറ്റവും മികച്ച അംഗീകൃത ഒരുവർഷ കംപ്യൂട്ടർ കോഴ്സായി ഈ കോഴ്സ് അറിയപ്പെടുന്നു.

CO&PA കോഴ്സിന്റെ പ്രസക്തി

ഭാരത സർക്കാരിന്റെ നാഷണൽ കൗൺസിൽ ഫോർ വൊക്കേഷണൽ ട്രെയിനിംഗിന്റെ (NCVT) നിയന്ത്രണത്തിൽ അഖിലേന്ത്യാ അടിസ്ഥാനത്തിൽ തയ്യാറാക്കിയിട്ടുള്ള ക്രാഫ്റ്റ്സ്മാൻ ട്രെയിനിങ് സ്കീം അനുസരിച്ചുള്ള കോഴ്സാണ് CO&PA. ഈ കോഴ്സ് വിവിധ സംസ്ഥാനങ്ങളിൽ സർക്കാർ/സ്വകാര്യ ഐ.ടി.ഐ.കൾ മുഖേന നടത്തിവരുന്നു. കേന്ദ്ര/സംസ്ഥാന ഗവൺമെന്റിന്റെ എല്ലാ ഡിപ്പാർട്ട്മെന്റുകളും അംഗീകരിച്ചതാണ് ഈ കോഴ്സ്. വിദേശ രാജ്യങ്ങളിൽ പോലും ഈ കോഴ്സിന് അംഗീകാരമുണ്ട്. എസ്.എസ്.എൽ.സി/ പ്ലസ് ടു/ ഡിഗ്രി യോഗ്യതയുള്ളവർക്ക് ഈ കോഴ്സിൽ ചേർന്നു പഠിക്കാവുന്നതാണ്. റെഗുലർ/ ഫുൾടൈം രീതിയിലാണ് പാഠ്യപദ്ധതി.

നാഷണൽ സ്കിൽ ക്വാളിഫിക്കേഷൻ ഫ്രെയിംവർക്ക് (NSQF) എന്ന ഭാരതസർക്കാർ പദ്ധതിയിൽ ഉൾപ്പെടുത്തിയിരിക്കുന്നതിനാൽ ഈ കോഴ്സിന് ഒരു അന്താരാഷ്ട്ര നിലവാരം ലഭിക്കുന്നു.

തൊഴിൽ സാധ്യത

സർക്കാർ/സ്വകാര്യ മേഖലയിൽ ലഭ്യമായ നിരവധി തസ്തികകളിലേക്ക് ഏറ്റവും അനുയോജ്യമായ കോഴ്സാണ് CO&PA. PSC/UPSC അംഗീകരിച്ച കോഴ്സ് ആയതിനാൽ തൊഴിൽ ലഭിക്കുവാൻ സാധ്യത വളരെ കൂടുതലാണ്. കംപ്യൂട്ടർ അധിഷ്ഠിതമായ വിവിധ തസ്തികകളിലേക്ക് അപേക്ഷിക്കുന്നതിനുള്ള അടിസ്ഥാന യോഗ്യതയായി CO&PA ഉൾപ്പെടുത്തിയിരിക്കുന്നതിനാൽ അവസരങ്ങൾ ഏറെയാണ്.

എല്ലാ ദിവസവും രണ്ടുമണിക്കൂർ തിയറിയും അഞ്ചുമണിക്കൂർ പ്രാക്ടിക്കലും ഉൾപ്പെടുത്തിയിരിക്കുന്നതിനാൽ പ്രായോഗിക പരിജ്ഞാനം കൂടുതലുണ്ടാകും. കൂടാതെ വിജയികളാകുന്ന കുട്ടികൾക്ക് ഉടൻതന്നെ അപ്രന്റീസ്ഷിപ്പ് ലഭിക്കുന്നു. (അപ്രന്റീസ് എന്നാൽ സർക്കാർ/പൊതുമേഖലാ സ്ഥാപനങ്ങളിൽ 7000 -15000 വരെ സ്റ്റൈപ്പന്റോടുകൂടി ജോലി ചെയ്യുവാൻ ലഭിക്കുന്ന അവസരം).

COPA കോഴ്സ് വിജയകരമായി പൂർത്തിയാക്കുന്നവർക്ക് സോഫ്റ്റ്വെയർ മേഖലകളിൽ അസിസ്റ്റന്റ് പ്രോഗ്രാമേഴ്സ്, കമ്പ്യൂട്ടർ ഇൻസ്ട്രിക്ടർ, ലാബ് അസിസ്റ്റന്റ്, അസിസ്റ്റന്റ് ടു സർവീസ് എൻജിനീയർസ്,

കമ്പ്യൂട്ടർ ഓപ്പറേറ്റർ, ഹാർഡ്‌വെയർ ആൻഡ് സോഫ്റ്റ്‌വെയർ സെയിൽസ് പേഴ്സൺ, DTP ഓപ്പറേറ്റർ, ജൂനിയർ ഇൻസ്ട്രക്ടർ ഇൻ ഐടിഐ, ലാബ് അസിസ്റ്റന്റ് ഇൻ പോളിടെക്നിക് കോളേജ്/ എൻജിനീയറിങ് കോളേജ്, ടെക്നീഷ്യൻ എ ഗ്രേഡ് ഇൻ ഡിഫൻസ് (DRDO), സൈബർ സെൽ ഇൻ പോലീസ് ഡിപ്പാർട്ട്മെന്റ് എന്നിങ്ങനെ നിരവധി തൊഴിൽ സാധ്യതകളാണുള്ളത്.

CO&PA കോഴ്സ് സിലബസ്

കംപ്യൂട്ടർ മേഖലയിൽ തൊഴിൽ ലഭിക്കുന്നതിനുള്ള 7-ൽ പരം കോഴ്സുകൾക്ക് അനുയോജ്യമായ എംഎസ് ഓഫീസ്, അഡ്വാൻസ്ഡ് എക്സൽ, മൈ എസ്ക്യു എൽ, പൈത്തൺ, ജാവ സ്ക്രിപ്റ്റ്, എച്ച് ടി എം എൽ & സി എസ് എസ്, കംപ്യൂട്ടർ ഹാർഡ്വെയർ, ബേസിക്സ് ഓഫ് കംപ്യൂട്ടർ, സൈബർ സെക്യൂരിറ്റി, ഇ-കോമേഴ്സ്, ക്ലൗഡ് കംപ്യൂട്ടിങ്, ആപ്ലിക്കേഷൻ ഡെവലപ്മെന്റ് ലൈഫ്സൈക്കിൾ എന്നിവ ഉൾപ്പെടുത്തിയിരിക്കുന്നു.

പരിശീലന രീതിയും സർട്ടിഫിക്കറ്റും

അഖിലേന്ത്യാതലത്തിൽ നടത്തുന്ന ഓൾ ഇന്ത്യാ ട്രേഡ് ടെസ്റ്റിൽ വിജയികളാകുന്നവർക്ക് NCVT

നൽകുന്ന സർട്ടിഫിക്കറ്റ് ലോകരാഷ്ട്രങ്ങൾ അംഗീകരിച്ചതും സർക്കാർ / സ്വകാര്യ മേഖലയിൽ ജോലിക്കായി മുന്തിയ പരിഗണന ലഭിക്കുന്നതുമാണ്. മെയ്/ ജൂൺ/ ജൂലൈ മാസങ്ങളിലായിരിക്കും പ്രവേശനം ആരംഭിക്കുക.

പഠനകേന്ദ്രങ്ങൾ

NCVT-യുടെ നിലവാരവും നിയന്ത്രണത്തിലും പ്രവർത്തിക്കുന്നതിനാൽ കേരളത്തിൽ സ്വകാര്യമേഖലയിൽ കുറച്ച് സ്ഥാപനങ്ങൾക്ക് മാത്രമേ ഈ കോഴ്സ് നടത്തുവാൻ അംഗീകാരമുള്ളൂ. സ്വകാര്യ മേഖലയിൽ CO&PA കോഴ്സ് നടത്തുന്ന പ്രമുഖ സ്ഥാപനങ്ങൾ ഇവയാണ്.

തിരുവനന്തപുരം ജില്ല : **നാലഞ്ചിറ**,ജയമാത ITI, PH:9656847413, 04712531055,**നെടുമങ്ങാട്**, നെറ്റ് ITI, PH:7559983031,**ആറ്റിങ്ങൽ**, യൂ ടെക് ITI, PH:9072991069, **നെയ്യാറ്റിൻകര**, കമ്പ്യൂട്ടർ പാർക്ക് ITI, PH:9495220402.

കൊല്ലം ജില്ല: **ശാസ്താംകോട്ട**, സെൻട്രൽ ITI, PH:9400853522 **അഞ്ചൽ**, F.C.M ITI, PH:9846756609, **പുനലൂർ**, ഡേറ്റാടെക് കംപ്യൂട്ടർ ITI

പത്തനംതിട്ട ജില്ല: **കടമ്പനാട്**, ഗേറ്റ് വേ കംപ്യൂട്ടർ എഡ്യൂക്കേഷൻ ITI, PH: 9400934455, 04734284455 **പന്തളം**, മൈക്രോ കോളേജ് ഓഫ് എഞ്ചിനിയറിംഗ് & കമ്പ്യൂട്ടർ ടെക് ITI, PH:9446438028

ആലപ്പുഴ ജില്ല: **കായംകുളം**, വിൻടെക് കംപ്യൂട്ടർ ITI, PH: 9656799660/9947239660 **മാവേലിക്കര**, ഡേറ്റാടെക് കംപ്യൂട്ടർ ITI, PH. 9446492407

കോട്ടയം ജില്ല: **കോട്ടയം**, NICT കംപ്യൂട്ടേഴ്സ്, PH:9447464308, **ഏറ്റുമാനൂർ**, P.Tech ITI, PH:9447758661, **പാല**, മന്നം ഇൻസ്റ്റിറ്റ്യൂട്ട് ഓഫ് കംപ്യൂട്ടർ ITI, PH: 9447121369, **തലയോലപ്പറമ്പ്**, ICM കംപ്യൂട്ടേഴ്സ് ITI, PH:9809286999

എറണാകുളം ജില്ല: **ലിസ്സി ജംഗ്ഷൻ**, സ്കിൽ ടെക് ഐടിഐ PH: 9061083083, 04842402527

പാലക്കാട് ജില്ല: **മണ്ണാർക്കാട്**, മണ്ണാർക്കാട് ഐടിഐ PH: 9605062525

കാസർഗോഡ് ജില്ല: **കാഞ്ഞങ്ങാട്**, ഓർഫനേജ് ITI, PH: 04672203931, 9846743127

മാർക്കറ്റർമാർക്കും സാധാരണക്കാർക്കും കരുത്ത് പകരുന്ന AI ടൂളുകൾ

© ജെസ്‌ലി എ എൽ M.Tech, ഗൂഗിൾ സർട്ടിഫൈഡ് ഡിജിറ്റൽ മാർക്കറ്റർ

ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസ് (AI) എന്നത് ഭാവിയുടെ ഒരു സങ്കൽപ്പമല്ല; അത് നമ്മുടെ വർത്തമാന കാലത്തിന്റെ അവിഭാജ്യഘടകമാണ്. വ്യവസായങ്ങളെയും ദൈനംദിന ജീവിതത്തെയും ഇത് അതിവേഗം മാറ്റിമറിച്ചുകൊണ്ടിരിക്കുന്നു. ഈ ലേഖനം, പരിചയസമ്പന്നരായ മാർക്കറ്റർമാരെയും സാധാരണക്കാരെയും ശാക്തീകരിക്കുന്ന ഏറ്റവും പുതിയ AI ടൂളുകളെ വിശദീകരിക്കുന്നു.

മാർക്കറ്റർമാർക്കുള്ള AI

AI മാർക്കറ്റിംഗ് രംഗത്ത് വലിയ മാറ്റങ്ങൾ വരുത്തിക്കൊണ്ടിരിക്കുന്നു, കാര്യക്ഷമത, വ്യക്തിഗതമാക്കൽ, ഉപഭോക്താവിനെക്കുറിച്ചുള്ള ആഴത്തിലുള്ള ധാരണ എന്നിവയ്ക്കായി AI വലിയ അവസരങ്ങൾ നൽകുന്നു. ഏറ്റവും പുതിയ ട്രെൻഡുകളും ടൂളുകളും താഴെ പറയുന്നവയാണ്:

1. Content സൃഷ്ടിക്കുന്നതിനും മെച്ചപ്പെടുത്തുന്നതിനും:

മാർക്കറ്റർമാർ എങ്ങനെ Content നിർമ്മിക്കുന്നു എന്നതിനെ AI വിപ്ലവകരമായി മാറ്റുന്നു.

• Generative AI (ഉദാ: Jasper AI, Copy.ai, Writesonic, Claude): ബ്ലോഗ് പോസ്റ്റുകൾ, സോഷ്യൽ മീഡിയ ക്യാപ്ഷനുകൾ, പരസ്യ കോപ്പികൾ, കൂടാതെ വീഡിയോ സ്ക്രിപ്റ്റുകൾ എന്നിവയുൾപ്പെടെയുള്ള വിവിധതരം ഉള്ളടക്കങ്ങൾ ഈ ടൂളുകൾക്ക് സൃഷ്ടിക്കാൻ കഴിയും, ഇത് ഉള്ളടക്കം നിർമ്മിക്കുന്നതിനുള്ള സമയം ഗണ്യമായി കുറയ്ക്കുന്നു. ഒരു ബ്രാൻഡിന്റെ പ്രത്യേക ശൈലിക്കും ശബ്ദത്തിനും അനുസരിച്ച് ഉള്ളടക്കം നിർമ്മിക്കാനും ഇവ സഹായിക്കും.
Jasper AI: https://www.jasper.ai/
Copy.ai: https://www.copy.ai/
Writesonic: https://writesonic.com/
Claude: https://claude.ai/

• വീഡിയോ നിർമ്മാണം (ഉദാ: Synthesia, Descript, InVideo AI): വീഡിയോകൾക്കായി യാഥാർത്ഥ്യബോധമുള്ള AI അവതാറുകൾ സൃഷ്ടിക്കാനും, ഓഡിയോയും വീഡിയോയും എഡിറ്റ് ചെയ്യാനും, വാചകങ്ങളിൽ നിന്ന് മുഴുവൻ വീഡിയോകളും സൃഷ്ടിക്കാനും AI-ക്ക് കഴിയും. ഇത് വീഡിയോ ഉള്ളടക്കം കൂടുതൽ എളുപ്പത്തിൽ ലഭ്യമാക്കുന്നു.
Synthesia: https://www.synthesia.io/
Descript: https://www.descript.com/
InVideo AI: https://invideo.io/ai/

2 . ഉപഭോക്തൃ ഇടപഴകലും സേവനവും:

ഉപഭോക്തൃ ഇടപെടലുകൾ മെച്ചപ്പെടുത്തുന്നതിനും, അവ കൂടുതൽ കാര്യക്ഷമവും വ്യക്തിഗതവുമാക്കുന്നതിനും AI സഹായിക്കുന്നു.

• AI ചാറ്റ്ബോട്ടുകൾ (ഉദാ: Drift, HubSpot, Zendesk, Ada): ഈ ബുദ്ധിപരമായ ചാറ്റ്ബോട്ടുകൾ തൽക്ഷണ ഉപഭോക്തൃ പിന്തുണ നൽകുന്നു, പതിവ് ചോദ്യങ്ങൾക്ക് ഉത്തരം നൽകുന്നു, ലീഡുകൾക്ക് യോഗ്യത നൽകുന്നു, മീറ്റിംഗുകൾ ഷെഡ്യൂൾ ചെയ്യുന്നു. 24/7 സഹായം നൽകുകയും ഉപഭോക്തൃ സംതൃപ്തി മെച്ചപ്പെടുത്തുകയും ചെയ്യുന്നു.
Drift: https://www.drift.com/
HubSpot Chatbot Builder: https://www.hubspot.com/products/ai/chatbots
Zendesk Chatbot: https://www.zendesk.com/service/ai/chatbot/
Ada: https://www.ada.cx/

4. മാർക്കറ്റിംഗ് ഓട്ടോമേഷനും വർക്ക്ഫ്ലോ ഒപ്റ്റിമൈസേഷനും (ഉദാ: Zapier AI, Airtable AI):

ആവർത്തിച്ചുള്ള മാർക്കറ്റിംഗ് ജോലികൾ ഓട്ടോമേറ്റ് ചെയ്യാനും ബുദ്ധിപരമായ വർക്ക്ഫ്ലോകൾ സൃഷ്ടിക്കാനും AI-ക്ക് കഴിയും.

• Zapier AI: https://zapier.com/ai
• Airtable AI: https://www.airtable.com/product/ai

സാധാരണക്കാർക്കുള്ള AI

പ്രൊഫഷണൽ മേഖലകൾക്കപ്പുറം, AI നമ്മുടെ ദൈനംദിന ജീവിതത്തിൽ കൂടുതൽ ഉപയോഗിക്കപ്പെടുന്നു. നമ്മൾ അറിയാതെ പോലും ഇത് നമ്മുടെ ജീവിതത്തിന്റെ ഭാഗമായിക്കൊണ്ടിരിക്കുന്നു. ഉൽപ്പാദനക്ഷമത വർദ്ധിപ്പിക്കുന്നതിനും, സൗകര്യങ്ങൾ മെച്ചപ്പെടുത്തുന്നതിനും, വ്യക്തിഗതമാക്കിയ അനുഭവങ്ങൾ നൽകുന്നതിനും ഈ ടൂളുകൾ രൂപകൽപ്പന ചെയ്തിട്ടുള്ളതാണ്.

1. വ്യക്തിഗത ഉൽപ്പാദനക്ഷമതയും സഹായവും

• AI ചാറ്റ്ബോട്ടുകളും അസിസ്റ്റന്റുമാരും (ഉദാ: ChatGPT, Google Gemini, Microsoft Copilot, Claude): ചോദ്യങ്ങൾക്ക് ഉത്തരം നൽകാനും, ക്രിയാത്മകമായ എഴുത്തുകൾ (ഇമെയിലുകൾ, സംഗ്രഹങ്ങൾ, രൂപരേഖകൾ) സൃഷ്ടിക്കാനും, ആശയങ്ങൾ കണ്ടെത്താനും, കോഡിംഗിൽ സഹായിക്കാനും ഈ ടൂളുകൾക്ക് കഴിയും.
ChatGPT: https://chat.openai.com/
Google Gemini: https://gemini.google.com/
Microsoft Copilot: https://copilot.microsoft.com/

• എഴുത്ത് സഹായികൾ (ഉദാ: Grammarly, HyperWrite): വ്യാകരണത്തെറ്റുകൾ കണ്ടെത്താനും, ശൈലി മെച്ചപ്പെടുത്താനും, എഴുത്ത് തുടങ്ങാനുള്ള ബുദ്ധിമുട്ടുകൾ ഇല്ലാതാക്കാനും ഈ ടൂളുകൾ സഹായിക്കുന്നു.
Grammarly: https://www.grammarly.com/
HyperWrite: https://hyperwriteai.com/

2. ഉള്ളടക്കം കാണുന്നതിനും സൃഷ്ടിക്കുന്നതിനും:

• വ്യക്തിഗതമാക്കിയ ശുപാർശകൾ: സ്ട്രീമിംഗ് സേവനങ്ങൾ (സംഗീതം, വീഡിയോ), ഇ-കൊമേഴ്സ് പ്ലാറ്റ്ഫോമുകൾ, സോഷ്യൽ മീഡിയ എന്നിവയിലെ ശുപാർശകൾക്ക് പിന്നിൽ AI അൽഗോരിതങ്ങളാണ് പ്രവർത്തിക്കുന്നത്. ഇത് ഓരോ വ്യക്തിയുടെയും താൽപ്പര്യങ്ങൾക്കനുസരിച്ച് ഉള്ളടക്കങ്ങളും ഉൽപ്പന്നങ്ങളും നിർദ്ദേശിക്കുന്നു.

• ചിത്രം നിർമ്മിക്കുന്ന ടൂളുകൾ (ഉദാ: DALL-E 3, Midjourney, Ideogram): വാചക വിവരണങ്ങളിൽ നിന്ന് അതുല്യമായ ചിത്രങ്ങൾ സൃഷ്ടിക്കാൻ ഈ AI ടൂളുകൾക്ക് കഴിയും. ഇത് വ്യക്തിഗതമായ സർഗ്ഗാത്മകതയ്ക്കും ദൃശ്യ ആശയവിനിമയത്തിനും പുതിയ വഴികൾ തുറക്കുന്നു.
DALL-E 3 (ChatGPT-യിൽ ലഭ്യമാണ്): https://chat.openai.com/
Midjourney: https://www.midjourney.com/
Ideogram: https://ideogram.ai/

●

ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസും ഡിജിറ്റൽ മാർക്കറ്റിംഗും സൗജന്യമായി പരിശീലിക്കാം

കേരളത്തിനകത്തും പുറത്തും വിവിധ കമ്പനികൾക്കും ബിസിനസ് ഉടമകൾക്കും ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസ് / ഡിജിറ്റൽ മാർക്കറ്റിങ് തുടങ്ങിയവ പരിശീലിക്കാൻ ആഗ്രഹിക്കുന്നവർക്കും പരിശീലനം നൽകുന്ന ഡിജിറ്റൽ മാഗ്നെറ്റ് ട്രെയിനിങ് സെന്റർ എല്ലാ ഞായറാഴ്ചകളിലും സംഘടിപ്പിക്കുന്ന ട്രെയിനിങ് പ്രോഗ്രാമിൽ പങ്കെടുക്കുന്നതിലൂടെ ഈ മേഖലയിലെ വിശാലമായ ലോകത്തെ നിങ്ങൾക്കും അടുത്തറിയാം. പങ്കെടുക്കുവാൻ താഴെ കൊടുത്തിരിക്കുന്ന ഫോൺ നമ്പറിൽ വിളിക്കാം അല്ലെങ്കിൽ വാട്സാപ്പ് ചെയ്യാം Ph: +91 6235080604.

വാട്സ്ആപ്പ് ഗ്രൂപ്പിൽ ജോയിൻ ചെയ്യാൻ ഈ ലിങ്ക് തുറക്കാം. rebrand.ly/DMJESLEY

1.5 മണിക്കൂർ സൗജന്യ ഡിജിറ്റൽ മാർക്കറ്റിംഗ് ട്രെയ്നിനിങ്

DIGITAL MAGNET
INSTITUTE OF DIGITAL MARKETING
www.digitalmagnetonline.com

ONLINE TRAINING

TOPICS

- facebook മാർക്കറ്റിംഗ്
- Google പരസ്യങ്ങൾ
- amazon സെല്ലർ അക്കൗണ്ട്
- വെബ്സൈറ്റ് നിർമ്മാണം
- ഇ–കൊമേഴ്സ്
- ഗ്രാഫിക് ഡിസൈൻ
- ഓൺലൈൻ മണി മേക്കിങ്

Trainer: Jesley A L (M.Tech)
Google Certified Digital Marketer

ക്ലാസിൽ പങ്കെടുക്കുവാൻ ഈ വാട്സ്ആപ്പ് ഗ്രൂപ്പിൽ ജോയിൻ ചെയ്യാം

> REGISTER NOW
Free

EVERY SUNDAY

To Attend Free Training

CALL or WHATSAPP
+91 7012041882

SCAN QR CODE

ഇൻഫോ സൈറ്റ്

Info Site

ആര്യ എസ് നായർ

മൗസ് ആകെ മാറി

കാലം മാറി എന്നാലും പിസി ആണെങ്കിലും ലാപ്ടോപ്പ് ആണെങ്കിലും, സിസ്റ്റത്തിന് ഒരു 'മൗസ്' അത് നിർബന്ധമാണ് നമുക്ക്. പോർട്രോണിക്സിന്റെ റ്റൊആഡ് എർഗോ 3 (Portronics Toad Ergo3) മൗസിന്റെ പരമ്പരാഗത രൂപഘടനയെ മാറ്റിമറിക്കുന്ന ഡിസൈനാണ്. കൈകൾക്ക് കൂടുതൽ ഗ്രിപ്പ് നൽകുന്ന വിധത്തിൽ, കൂടുതൽ

ഈസിയായി വർക്ക് ചെയ്യാവുന്ന തരത്തിലുമാണ് ഈ മൗസിന്റെ ഡിസൈൻ. ഒരേ സമയം ഈ മൗസ് ഒന്നിലധികം ഡിവൈസുകളുമായി കണക്ട് ചെയ്യാം. അതുകൊണ്ടുതന്നെ നിങ്ങളുടെ ലാപ്ടോപ്പിലും മൊബൈൽ ഫോണിലും ഒക്കെ ഈ മൗസ് കണക്ട് ചെയ്ത് ഉപയോഗിക്കാം. വയർലെസ്സായ ഈ മൗസ് യുഎസ്ബി ഉപയോഗിച്ച് ചാർജ് ചെയ്യാം. ഫോർവേഡ്, ബാക്ക് വേർഡ്, ഡി പി ഐ തുടങ്ങി ആറോളം നാവിഗേഷൻ ബട്ടനുകളാണ് ഇതിൽ ഉള്ളത്. കൈക്ക് കൂടുതൽ ആയാസം ഉണ്ടാകാത്ത വിധം ഉയർന്നതാണ് ഇതിന്റെ ഡിസൈൻ. കൂടാതെ ആർജിബി ലൈറ്റ് നൽകി കൂടുതൽ സ്റ്റൈലിഷ് ആക്കിയിരിക്കുന്നു. 148 ഗ്രാമാണ് ഭാരം. 1,149 രൂപയ്ക്ക് ഓഫർ പ്രൈസിൽ വിപണിയിൽ ലഭിക്കും.

ഇനി ടേബിൾ വെറുമൊരു ടേബിൾ അല്ല

വീട്ടിൽ ഒരിടത്ത് ചടഞ്ഞു കൂടിയിരിക്കുമ്പോൾ ഒരു ടേബിൾ വലിച്ചിട്ട് ടിവിക്ക് മുന്നിൽ ഇരുന്ന് അതിൽ നമ്മൾ സ്നാക്സും ഫോണും ഒക്കെ നിരത്താറുണ്ട് അല്ലേ? സാധനങ്ങൾ നിരത്തി പലതും താഴെ വീണു പോകാറുമുണ്ട്. ഈ ടേബിളിൽ കപ്പ് ഹോൾഡറും ബ്ലൂടൂത്ത് സ്പീക്കറും വയർലെസ് ചാർജറും ഒക്കെ ഉണ്ടെങ്കിലോ? ഫീസ്റ്റോ കോച്ച് (Fiisto Coucha) എന്ന കമ്പനിയാണ് ഈ അത്ഭുത ടേബിൾ വിപണിയിൽ എത്തിക്കുന്നത്. ഇതിൽ ബ്ലൂടൂത്ത് സ്പീക്കർ, വയർലെസ് ചാർജർ, ലാപ്ടോപ്പ് സ്റ്റാൻഡ്, കപ്പ്, സ്നാക്ക് ഹോൾഡറുകൾ, ഫാൻ തുടങ്ങിയ സൗകര്യങ്ങളെല്ലാം ഉണ്ട്. നിങ്ങൾക്ക് എഴുന്നേറ്റ് നടക്കാതെ തന്നെ കയ്യെത്തും ദൂരത്ത് ആവശ്യമുള്ളതെല്ലാം വയ്ക്കാം. വ്യത്യസ്തങ്ങളായ നിറങ്ങളിൽ ഈ ടേബിൾ ലഭ്യമാണ്.

ഇതിന്റെ ബേസ് ഒരു സെമി സർക്കുലർ ഷേപ്പിലാണ്. ഇത് ടേബിളിനെ സ്റ്റൈലിഷാക്കുന്നു. 180 ഡിഗ്രി വരെ റൊട്ടേറ്റബിൾ ആണ് ഈ ടേബിൾ. അഡ്ജസ്റ്റ് ചെയ്യാവുന്ന ഈ ടേബിളിന്റെ പരമാവധി ഉയരം 25.6 ആണ്. 12000 രൂപയിൽ താഴെയാണ് വില.

വീട് സ്മാർട്ട് ആക്കും റോബോട്ട്

സ്വിച്ചുകൾ ഇല്ലാത്ത സ്മാർട്ട് യുഗത്തിൽ നിങ്ങളുടെ വീട് സ്മാർട്ട് അല്ലല്ലോ എന്നോർത്ത് വിഷമിച്ചിരിക്കുകയാണോ? സ്വിച്ച് ബോട്ട് (SwitchBot) എന്ന റോബോട്ട്

നിങ്ങളുടെ സ്വിച്ചുകളെ ഇനി സ്മാർട്ട് ആക്കും. സ്ഥിരമായി ഉപയോഗിക്കുന്ന അടുത്ത് ഈ കുഞ്ഞൻ റോബോട്ട് ഘടിപ്പിക്കുകയേ വേണ്ടൂ. നിങ്ങളുടെ കമാൻഡ് കിട്ടിയാൽ ആ സ്വിച്ച് കുഞ്ഞൻ റോബോർട്ട് ഓൺ ചെയ്യുകയും ഓഫ് ചെയ്യുകയും ചെയ്യും. സ്ഥിരമായി ഒരു സമയത്ത് ചായ കുടിക്കുന്ന ശീലം ഉണ്ടെങ്കിൽ ആ സമയം കോഫി മേക്കർ ഓൺ ചെയ്യാൻ റോബോട്ടിനെ സെറ്റ് ചെയ്യുവയ്ക്കാം. ബെഡിൽ കിടന്നുള്ള വായനക്ക് ശേഷം ഉറങ്ങാൻ ഉള്ള സമയത്ത് ലൈറ്റ് ഓഫ് ചെയ്യാനും ഈ റോബോട്ടിനെ സെറ്റ് ചെയ്യാം. 3995 രൂപയാണ് വില.

ഇൻഫോ സൈറ്റ് Info Site

മീറ്റിങ്ങുകളിൽ ലൈഫ് മിസ്സ് ആക്കണ്ട

ഓഫീസ് ഓൺലൈൻ ആയപ്പോൾ മീറ്റിംഗ് ഒക്കെ സമയവും കാലവും ഇല്ല. രാത്രിയിലോ യാത്രകൾക്കിടയിലെ ഒക്കെ മീറ്റിംഗ് അറ്റൻഡ് ചെയ്യേണ്ടി വരുമ്പോൾ, പറയുന്ന പല കാര്യങ്ങളും നിങ്ങൾക്ക് മിസ്സ് ആകാറു

ണ്ടോ? എങ്കിൽ നിങ്ങൾക്കുള്ളതാണ് ഹൈ ഡോക് (Hi Dock) ന്റെ P1 & P1 mini ഐ വോയിസ് റെക്കോർഡർ. ഇയർഫോൺ ഉപയോഗിച്ചാൽ പോലും, ഈ ഡിവൈസ് ഉപയോഗിച്ച് മീറ്റിങ്ങുകൾ ആദ്യം മുതൽ അവസാനം വരെ റെക്കോർഡ് ചെയ്യാം. കൂടാതെ പറയുന്ന കാര്യങ്ങൾ ട്രാൻസ്ക്രൈബ് ചെയ്യാനും വോയിസ് കോളുകൾ ചുരുക്കി ടെക്സ്റ്റ് മെസ്സേജ് ആക്കി മാറ്റാനും ഈ ഡിവൈസിന് സാധിക്കും. ഹൈ ഡോക്ക് P1 ന് 64 GB ഇൻബിൽഡ് സ്റ്റോറേജും, 600 mAh ബാറ്ററി കപ്പാസിറ്റിയും എട്ടു മണിക്കൂർ വരെ റെക്കോർഡിങ്ങും 1000 മണിക്കൂർ വരെ ബാറ്ററി ബാക്കപ്പും ലഭിക്കും. ഹൈ സെൻസിറ്റീവ് ഈ സി എം മൈക്രോഫോൺ ആണ് ഇതിൽ ഉള്ളത്. ബൈ ഡയറക്ഷണൽ നോയിസ് ക്യാൻസലൈസേഷനും ഇതിൽ ഉണ്ട്. 15,000 രൂപയിൽ താഴെയാണ് വില.

കംപ്ലീറ്റ് സെൻസർ

ആപ്പിൾ, ഗൂഗിൾ, അലക്സ തുടങ്ങി വിവിധ ഡിവൈസുകൾ കൊണ്ട് വീട് നിറയുമ്പോൾ ഒരു ഡിവൈസിന്റെ സിഗ്നൽ മറ്റൊന്നിന് മനസ്സിലാകാത്ത വന്നാൽ എന്ത് ചെയ്യും? എല്ലാ ഡിവൈസുകളുടെയും സിഗ്നലുകളെ കണക്ട് ചെയ്യുന്ന ഒരു സ്മാർട്ട് ഡിവൈസ് അവതരിപ്പിച്ചിരിക്കുകയാണ് അക്വേറ (Aqura) വീട്ടിലെ എല്ലാ ഡിവൈസുകളെയും ബന്ധിപ്പിക്കുന്ന ഒരു ഹബ്ബായാണ് അക്വാറ പ്രവർത്തിക്കുന്നത്. ഓരോ ഡിവൈസിൽ നിന്നും ഉണ്ടാകുന്ന സിഗ്നലിനെ കളക്ട് ചെയ്യാൻ ഓരോ ഡിവൈസുകൾക്കും വ്യത്യസ്ത ഡിവൈസുകളുടെ ആവശ്യം വരുന്നില്ല. എല്ലാ ഡിവൈസുകളെയും പരസ്പരം കണക്ട് ചെയ്യാൻ അക്വാറ മതി.

സ്മാർട്ട് ആയി ഇരുത്താം

സ്ക്രീൻ ടൈം കൂടുമ്പോൾ അറിയാതെ നടുവിളഞ്ഞു പോകുന്നത് നിങ്ങൾ ശ്രദ്ധിക്കാറുണ്ടോ? ഇല്ലെങ്കിലും വിഷമിക്കേണ്ട, അപ്പ് റൈറ്റ്(upright) ശ്രദ്ധിച്ചു കൊള്ളും. അപ്പ്റൈയ്റ്റ് എന്ന കമ്പനി വിപണിയിൽ എത്തിക്കുന്ന പോസ്റ്റർ കറക്റ്റ് ആണ് ഗോ2 (Go 2) ജോലി ചെയ്യുമ്പോഴും നടക്കുമ്പോഴും എല്ലാം ഈ ഉപകരണം നിങ്ങൾക്ക് ധരിക്കാം. നിങ്ങളുടെ നട്ടെല്ലിന്റെ മുകൾ ഭാഗത്ത് ധരിക്കാവുന്ന ചെറിയൊരു സെൻസറാണിത്. ഒരു പാച്ച് ഉപയോഗിച്ച് ഇത് ശരീരത്തിൽ നേരിട്ട്

ഘടിപ്പിക്കുകയോ, നെക്കിളി പോലെ സെൻസർ പുറകിലേക്ക് വരുന്ന രീതിയിൽ ധരിക്കുകയോ ചെയ്യാം. പുറം താഴ്ന്നു വരുമ്പോൾ സെൻസർ വൈബ്രേറ്റ് ചെയ്തു പോസ്റ്റർ കറക്ഷന് ഇന്റിമേഷൻ നൽകും. കൂടാതെ നിങ്ങളുടെ ഫോണിലേക്ക് 'പോസ്റ്ററിന്റെ' ഫീഡ്ബാക്കുകൾ അയയ്ക്കും. രണ്ട് സെൻസറുകളാണ് ഈ ഡിവൈസിലുള്ളത്. 48 മില്ലിമീറ്റർ മാത്രമാണ് വലിപ്പം. 6000 രൂപയിൽ താഴെയാണ് വില.

വെബ്സൈറ്റ് റിവ്യു
WEBSITE REVIEW

എന്തിനും ഏതിനും ഇന്റർനെറ്റിൽ ഉത്തരം തിരയുന്നവരാണ് നമ്മൾ. ചിലപ്പോഴെല്ലാം ഒരു ഉത്തരത്തിന് പലയിടത്തുമായി തിരയേണ്ടി വരും. പക്ഷെ നാം തിരയുന്ന ചോദ്യങ്ങൾക്ക് മറുപടി ഒരു വെബ്സൈറ്റ് തരുന്നുണ്ടെങ്കിലോ? എന്തും ഏറ്റവും എളുപ്പമായി ചെയ്ത് തീർക്കാൻ ഒരു വെബ്സൈറ്റ് നിങ്ങളെ സഹായിക്കുമെങ്കിലോ? അതല്ലേ ഏറ്റവും സഹായം. അത്തരത്തിൽ ചെറുതും വലുതുമായ നിരവധി വെബ്സൈറ്റുകൾ ഇന്റർനെറ്റിലുണ്ട്. ഗവൺമെന്റ് വെബ്സൈറ്റുകളും അല്ലാത്ത വെബ്സൈറ്റുകളും നിരവധിയാണ്. അതിൽ ചിലതാണ് ഇത്.

◐ ആതിര ശിശുപാലൻ

പാഠപുസ്തകം ഡൗൺലോഡ് ചെയ്യാം (scert.kerala.gov.in/)

സ്കൂൾ തുറന്നതോടെ കുട്ടികൾ തിരികെ പുസ്തകങ്ങളുടെ ലോകത്തേക്ക് എത്തിയിരിക്കുകയാണ്. വർണ്ണങ്ങൾ നിറഞ്ഞ പഠനത്തിന്റെ ലോകത്ത് നിന്നു പല വിഷയങ്ങളിലും വിജ്ഞാനം നേടാൻ അവരെ കാത്തിരിക്കുന്ന പുസ്തകങ്ങളുണ്ട്. ഗവൺമെന്റ് സ്കൂളുകളിൽ പരിഷ്കരിച്ച പുതിയ പുസ്തകങ്ങൾ ആണ് ഇക്കുറി പല ക്ലാസ്സുകളിലും എത്തിയിരിക്കുന്നത്. എന്നാൽ ഇതെല്ലാം കാണാനും ഡൗൺലോഡ് ചെയ്യാനുമുള്ള സൗകര്യവും വിദ്യാഭ്യാസ വകുപ്പ് ഒരുക്കിയിട്ടുണ്ട്. https://scert.kerala.gov.in/ എന്ന വെബ്സൈറ്റിൽ നേരത്തെ തന്നെ ഈ സൗകര്യം നിലവിൽ വന്നു കഴിഞ്ഞു.

പുതിയ അദ്ധ്യാന വർഷത്തിൽ വേണ്ടുന്ന പാഠപുസ്തകങ്ങളും പ്രവർത്തി പുസ്തകങ്ങളും ഏതെല്ലാമാണെന്ന് ഇതിൽ കാണാം. മാത്രമല്ല ഡൗൺലോഡ് ചെയ്തെടുക്കാനും സാധിക്കും. ഒന്ന് മുതൽ പത്താം ക്ലാസ്സ് വരെയുള്ള പാഠപുസ്തകങ്ങൾ ഇവിടെ ലഭ്യമാണ്. പുസ്തകങ്ങൾ വെബ്സൈറ്റ് ലോഗിൻ ചെയ്ത ശേഷം ഹോം പേജിൽ തന്നെ കാണാനുള്ള സൗകര്യം ഉണ്ട്. മാത്രമല്ല ടീച്ചർമാർക്ക് വേണ്ടിയുള്ള ടെക്സ്റ്റും ഈ വെബ്സൈറ്റിൽ തന്നെ ഉണ്ട്. ഇവയെല്ലാം ഡൗൺലോഡ് ചെയ്യാനുള്ള സൗകര്യവും ഇവിടെ ഒരുക്കിയിട്ടുണ്ട്.

കറന്റ് ബിൽ അറിയണോ? (old.kseb.in/billview)

പലരും കറന്റ് ബിൽ എത്രയെന്ന് മറന്നു പോകുകയോ അല്ലെങ്കിൽ ബിൽ കളഞ്ഞു പോകുകയോ ചെയ്യാറുള്ളത് പതിവാണ്. എന്നാൽ ബില്ലിന് വേണ്ടി

കഷ്ടപ്പെടേണ്ട. ഇതാ നിങ്ങളുടെ കറന്റ് ബില്ലോ, നിങ്ങളുടെ അയൽപക്കത്തെ വ്യക്തിയുടെ ബില്ലോ, സുഹൃത്തിന്റെ ബില്ലോ അറിയാൻ ഇനി എളുപ്പമാർഗം ഉണ്ട്. അതിനായി old.kseb.in/billview എന്ന വെബ്സൈറ്റ്

ഓപ്പൺ ചെയ്യുക. അതിൽ നിങ്ങളുടെ കൺസ്യൂമർ ഐഡി കൊടുക്കുക. ശേഷം കെഎസ്ഇബിയുമായി ലിങ്ക് ചെയ്തിരിക്കുന്ന മൊബൈൽ നമ്പർ കൊടുക്കുക. പിന്നീട് വരുന്ന പേജ് നിങ്ങളുടെ അവസാനം ലഭിച്ച കറന്റ് ബില്ലിന്റെ ഡീറ്റെയ്ൽസ് ആയിരിക്കും.

വളരെ ചെറിയ ഒരു പേപ്പറിൽ നിങ്ങൾക്ക് ലഭിക്കുന്ന ബില്ലിന്റെ അതേ വിശദാംശങ്ങൾ ഇവിടെ വ്യക്തമായി കാണിക്കുന്നു. മുതിർന്നവർക്ക് ഇത്തരത്തിൽ ബിൽ വ്യക്തമായി കാണാനും മനസ്സിലാക്കാനും സാധിക്കും. അധികം ബുദ്ധിമുട്ടില്ലാതെ വളരെ പെട്ടന്ന് തന്നെ ബിൽ ഡീറ്റെയ്ൽസ് കാണാൻ പെട്ടെന്ന് സാധിക്കും.

വിദ്യാർത്ഥികൾക്ക് പഠനത്തിന് സഹായി (https://www.wolframalpha.com)

സ്കൂൾ തുറന്നു. ഇനി പഠനത്തിന്റെ തിരക്കുകളിലേക്ക് വിദ്യാർത്ഥികൾ കടക്കുകയാണ്. കുട്ടികൾക്ക് പഠിക്കാനുള്ള മികച്ച സഹായി ആണ് wolframalpha. ഇതിനെ "കംപ്യൂട്ടേഷണൽ നോളജ് എഞ്ചിൻ" എന്നാണ് വിശേഷിപ്പിക്കുന്നത്. എന്നു പറഞ്ഞാൽ കംപ്യൂട്ടർ അധിഷ്ഠിത നോളജ് മെഷീൻ. കുട്ടികൾക്ക് പഠിക്കാൻ ആവശ്യമായ എല്ലാ കാര്യങ്ങളും ഇതിൽ ഉണ്ട്. പ്രധാനമായും കണക്കിലെ എല്ലാ ഉത്തരങ്ങളും കണ്ടെത്താൻ ഇത് സഹായിക്കുന്നു. മാത്രമല്ല ഹിസ്റ്ററി, എഞ്ചിനീയറിങ്, ആർട്സ് ആന്റ് മീഡിയ, കെമിസ്ട്രി, ഫിസിക്സ് തുടങ്ങി നിരവധി വിഷയങ്ങൾ ഈ ഒരൊറ്റ വെബ്സൈറ്റ് കൈകാര്യം ചെയ്യുന്നു. കണക്കിലെ ചോദ്യങ്ങൾക്ക് ഉത്തരം കിട്ടും എന്ന് മാത്രമല്ല അതെല്ലാം സ്റ്റെപ്പ് അനുസരിച്ച് ലഭിക്കുകയും ചെയ്യും. കുട്ടികൾക്ക് ധൈര്യമായി പഠനസഹായി

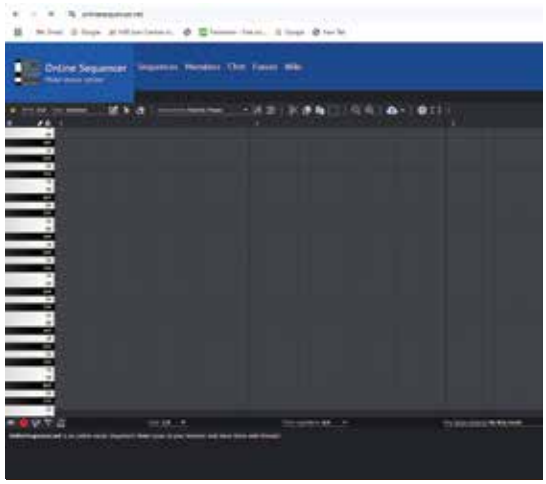
ആയി കൊണ്ടു നടക്കാവുന്ന ഒരു വെബ്സൈറ്റ് ആണിതെന്ന കാര്യത്തിൽ സംശയം ഇല്ല.

ഇംഗ്ലീഷ് ഇനി എളുപ്പം കൈകാര്യം ചെയ്യാം (https://onelook.com)

ഇംഗ്ലീഷ് പലരും കൈകാര്യം ചെയ്യാൻ ഏറെ ഇഷ്ടപ്പെടാൻ ആഗ്രഹിക്കുന്ന ഭാഷയാണ്. എന്നാൽ ഇംഗ്ലീഷ് എഴുതാൻ അറിയുന്നവർക്ക് പോലും നന്നായി സംസാരിക്കാൻ സാധിക്കണമെന്നില്ല. എന്നാൽ ഇനി ഒട്ടും പേടിക്കാതെ onelook.comന്റെ സഹായത്തോടെ തന്നെ ഇംഗ്ലീഷ് അതിവേഗം കൈകാര്യം ചെയ്യാം. ഈ വെബ്സൈറ്റ് ഇംഗ്ലീഷ് ഇഷ്ടപ്പെടുന്നവർക്ക് വേണ്ടിയുള്ളതാണ്. കാരണം നാം പലപ്പോഴും ഇംഗ്ലീഷിൽ

ഉപയോഗിക്കുന്ന നീണ്ട വാചകങ്ങൾക്ക് പകരമായി ഇണങ്ങുന്ന ഒറ്റ വാക്കിന് വേണ്ടി തിരയാറുണ്ട്. ഇനി അതെല്ലാം ഈ വെബ്സൈറ്റിൽ തന്നെ തിരഞ്ഞ് അതിവേഗം കണ്ടെത്താം. നിങ്ങളുടെ പറയാൻ അല്ലെങ്കിൽ എഴുതാൻ ഉദ്ദേശിക്കുന്ന വാചകത്തിന് പകരം മറ്റൊരു വാക്ക് ഇവിടെ നിന്നും ലഭിക്കും. വെബ്സൈറ്റ് തുറക്കുമ്പോൾ തന്നെ അവിടെ നിങ്ങളുടെ വാചകം ടൈപ് ചെയ്ത് കൊടുത്ത ശേഷം അടുത്ത് കാണുന്ന 'Thesaurus' ബട്ടൺ ക്ലിക്ക് ചെയ്ത് കൊടുക്കണം. അപ്പോൾ ആ വചകത്തിന് പകരമായുള്ള നിരവധി വാക്കുകൾ വരുന്നതാണ്.

സംഗീതം ഇഷ്ടപ്പെടുന്നവർക്ക് (onlinesequencer.net)



സ്വന്തമായി ഈണമുണ്ടാക്കി സ്വയം ആസ്വദിക്കാൻ നിങ്ങൾക്ക് ഇഷ്ടമാണോ? അത്തരക്കാർക്ക് വേണ്ടിയുള്ളതാണ് onlinesequencer.net എന്ന വെബ്സൈറ്റ്. ഈ വെബ്സൈറ്റിൽ ഒരു ഇലട്രിക്ക് പിയാനോ ആണ് ഉള്ളത്. അതിൽ പിയാനോ കീയിൽ ഉള്ളത് പോലെയുള്ള കീ നോട്സുകളും ഉണ്ട്. ഇതിൽ ക്ലിക്ക് ചെയ്ത് കൊടുത്ത് മുകളിലെ പ്ലേ ബട്ടണിൽ ക്ലിക്ക് ചെയ്താൽ പിയാനോ ശബ്ദത്തിലുള്ള മ്യൂസിക്ക് കേൾക്കാവുന്നതാണ്. ●

എഡ്ജ് എഐ - എഡ്ജ് കംപ്യൂട്ടിങ്ങിന്റെയും എഐയുടെയും സംയോജനം

കെ.എൻ. നായർ

എഡ്ജ് കംപ്യൂട്ടിങ്ങ് സാങ്കേതികവിദ്യയുമായി നിർമ്മിത ബുദ്ധി അഥവാ എഐ സംയോജിപ്പിക്കുന്നതോടെ ക്യാമറ, സെൻസർ, സ്മാർട്ട്ഫോൺ തുടങ്ങിയ ഉപകരണങ്ങൾക്ക് അവ സംഭരിച്ച ഡേറ്റ ക്ലൗഡിലേക്കോ അല്ലെങ്കിൽ ദൂരെ സ്ഥിതി ചെയ്യുന്ന ഒരു ഡേറ്റ സെന്ററിലേക്കോ അയക്കാതെ ഡേറ്റയുടെ ഉത്ഭവ സ്ഥാനത്തു തന്നെ പ്രോസസ്സ് ചെയ്യാനും അതുവഴി ഈ ഉപകരണങ്ങളെ സ്വയം ചിന്തിക്കാനും തീരുമാനങ്ങൾ എടുക്കാനും പ്രാപ്തമാക്കുന്നു. ഡേറ്റ ശേഖരിച്ച സ്ഥലത്തു തന്നെ വിശകലനം ചെയ്യുക എന്നതാണ് എഡ്ജ് കംപ്യൂട്ടിങ്ങിന്റെ മുഖമുദ്ര. ഇതിൽ എഐ സംയോജിപ്പിക്കുന്നതോടെ ഡേറ്റ അവിടെ വെച്ച് അപ്പോൾ തന്നെ വിശകലനം ചെയ്യാനും അനുയോജ്യമായ രീതിയിൽ പ്രതികരിക്കാനും സാധിക്കുന്നു.

ഉദാഹരണമായി സ്വയം ഓടിക്കുന്ന ഒരു വാഹനത്തിന്റെ കാര്യം തന്നെയെടുക്കാം. ഇതിലുള്ള സെൻസറുകൾ, ക്യാമറകൾ തുടങ്ങിയവയിലൂടെ റോഡിലെ മറ്റു വാഹനങ്ങൾ, കാൽനടയാത്രക്കാർ, ട്രാഫിക് ലൈറ്റുകൾ, തുടങ്ങിയവയെപ്പറ്റിയുള്ള വിവരങ്ങൾ തുടർച്ചയായി ശേഖരിക്കുന്നു. ഈ ഡേറ്റയെല്ലാം പ്രോസസ്സിങ്ങിനായി ക്ലൗഡിലേക്കോ, ഡേറ്റ സെന്ററിലേക്കോ അയക്കേണ്ടി വരികയാണെങ്കിൽ അതിൽ കാല താമസം ഉണ്ടാവുകയും ഒരു പക്ഷെ അപകടത്തിലേക്ക് നയിക്കുകയും ചെയ്തേക്കാം. എഐ സംയോജിത ക്ലൗഡ് കംപ്യൂട്ടിങ്ങിന്റെ അഥവാ എഡ്ജ് എഐയുടെ സഹായത്തോടെ ഈ ഡേറ്റ തൽക്ഷണം വാഹനത്തിനുള്ളിൽ വെച്ച് തന്നെ വിശകലനം ചെയ്യാനും, വേണ്ട രീതിയിൽ പ്രതികരിക്കാനും സാധിക്കുന്നു.

എഡ്ജ് എഐ ആപ്ലിക്കേഷനുകൾ വിവിധ ഡിവൈസുകളിൽ ഡേറ്റ വിശകലനം ചെയ്യാനും മെഷീൻ ലേണിംഗ് (എംഎൽ), ഡീപ് ലേണിംഗ് (ഡിഎൽ) അൽഗോരിതങ്ങൾ പ്രവർത്തിപ്പിക്കാനും സഹായിക്കുന്നു. ഇതുമൂലം ക്ലൗഡിൽ ചെയ്യുന്നതിലും വളരെയധികം വേഗത്തിൽ ഡേറ്റ പ്രോസസ്സ് ചെയ്യാൻ സാധിക്കുന്നു. കൂടാതെ എഡ്ജ് ഡിവൈസുകളിൽ എഐ ആപ്ലിക്കേഷനുകൾ നേരിട്ട് വിന്യസിക്കുന്നതിനാൽ ഉപയോക്താവിന്റെ സമീപത്തു വെച്ചു തന്നെ തൽസമയ ഡേറ്റ

തിരക്കേറിയ റോഡുകളിലൂടെ സ്വയം ഡ്രൈവ് ചെയ്യുന്ന വാഹനങ്ങൾ മുതൽ രോഗലക്ഷണങ്ങൾ തിരിച്ചറിയാൻ ലാബറട്ടറിയിലെ സാങ്കേതികവിദഗ്ധരെ സഹായിക്കുന്ന തുവരെയുള്ള പല വ്യത്യസ്ത രംഗങ്ങളിലും ഇന്ന് ഈ ടെക്നോളജി ഉപയോഗിക്കുന്നു.

പ്രോസസ്സിങ്ങ് സാധ്യമാക്കുന്നു. പ്രവർത്തനങ്ങൾ കൂടുതൽ കാര്യക്ഷമമാക്കുന്നതിലും കൂടുതൽ വേഗത്തിൽ ഉൾക്കാഴ്ചകൾ കണ്ടെത്തുന്നതിലും ഇത് സഹായിക്കുന്നു.

എഡ്ജ് എഐയുടെ പരിണാമം

ഐഎ രംഗത്ത് സമീപകാലത്തുണ്ടായ വൻ മുന്നേറ്റങ്ങൾ, ഐഒടി രംഗത്തെ വളർച്ച, എഡ്ജ് കംപ്യൂട്ടിങ്ങിലെ വികസനങ്ങൾ ഇവയെല്ലാം എഡ്ജ് എഐയുടെ വിന്യാസത്തിന്റെ വേഗത വർദ്ധിപ്പിച്ചു. തിരക്കേറിയ റോഡുകളിലൂടെ സ്വയം ഡ്രൈവ് ചെയ്യുന്ന വാഹനങ്ങൾ മുതൽ രോഗലക്ഷണങ്ങൾ തിരിച്ചറിയാൻ ലാബറട്ടറിയിലെ സാങ്കേതികവിദഗ്ധരെ സഹായിക്കുന്നതുവരെയുള്ള പല വ്യത്യസ്ത രംഗങ്ങളിലും ഇന്ന് ഈ ടെക്നോളജി ഉപയോഗിക്കുന്നു.

മിക്കവാറും എല്ലാ മേഖലയിലുള്ള സംരംഭങ്ങളും അവരുടെ ബിസിനസ് പ്രക്രിയകൾ, കാര്യക്ഷമത, സുരക്ഷ തുടങ്ങിയവ മെച്ചപ്പെടുത്താനായി ഓട്ടോമേഷനെ ആശ്രയിക്കുന്നു. ഇതിനായി ഉപയോഗിക്കുന്ന കംപ്യൂട്ടർ പ്രോഗ്രാമുകൾ പാറ്റേണുകൾ തിരിച്ചറിയാനും ആവർത്തിച്ചുള്ളതും സുരക്ഷിതവുമായ രീതിയിൽ ജോലികൾ നടപ്പിലാക്കാൻ കഴിവുള്ളവയുമായിരിക്കണം. ഈ ജോലികൾ ഉൾക്കൊള്ളുന്ന വ്യത്യസ്ത സാഹചര്യങ്ങളെയെല്ലാം ഈ പ്രോഗ്രാമുകളിൽ പൂർണ്ണമായി വിവരിക്കുകയെന്നത് അസാധ്യമാണ്. എഡ്ജ് എഐ ഡിവൈസുകളെ മനുഷ്യബുദ്ധിക്കു സമാനമായ രീതിയിൽ പ്രവർത്തിക്കാനും, സമാനമായ ജോലികൾ വ്യത്യസ്തമായ സാഹചര്യങ്ങളിലും ചെയ്യാനും പ്രാപ്തമാക്കുന്നു.

പ്രധാന സാങ്കേതികവിദ്യകൾ

സമീപ കാലത്തുണ്ടായ ചില നവീകരണങ്ങളിലൂടെയാണ് എഡ്ജ് കംപ്യൂട്ടിങ്ങിൽ എഐ വിന്യസിക്കുന്നതു കൊണ്ടുണ്ടാകുന്ന ഫലപ്രാപ്തിയെപ്പറ്റി ശാസ്ത്രലോകം കൂടുതലായി മനസ്സിലാക്കിയത്. ന്യൂറൽ നെറ്റ്വർക്കുകളിലും അനുബന്ധ സാങ്കേതികവിദ്യകളിലും ഉണ്ടായ വികസനങ്ങൾ ഇവയിലെ മെഷീൻ ലേർണിംഗ് പ്രക്രിയകൾ കൂടുതൽ സുഗമമാക്കി. ഇതോടെ എഐ മോഡലുകളെ പരിശീലിപ്പിക്കാനും, എഡ്ജ് കംപ്യൂട്ടിങ്ങ് സാങ്കേതികവിദ്യയുമായി ഇവയെ സംയോജിപ്പിക്കാനും അനായാസേന സാധിച്ചു.

എഡ്ജ് എഐ മോഡലുകളുടെ വിന്യാസം വിപുലീകരിക്കുന്നതിൽ കംപ്യൂട്ടിങ്ങ് രംഗത്തെ അടിസ്ഥാന സൗകര്യങ്ങളിലുള്ള വളർച്ചയും ഒരു പ്രധാന പങ്കു വഹിച്ചിട്ടുണ്ട്. എഡ്ജ് എഐ വിജയകരമായി നടപ്പാക്കാൻ ഉയർന്ന കംപ്യൂട്ടിങ്ങ് പവർ ആവശ്യമാണ്. ഒന്നിലധികം ജിപിയുകൾ സമാന്തരമായി ഉപയോഗിക്കുന്ന രീതികൾ ന്യൂറൽ നെറ്റ്വർക്കിന്റെ ഉപയോഗം മെച്ചപ്പെടുത്തുന്നതിൽ സഹായകരമായിട്ടുണ്ട്.

ഐഒടിയുടെ വർദ്ധിച്ചുവരുന്ന വ്യാപനം ബിഗ് ഡേറ്റയുടെ ക്രമാതീത വളർച്ചയ്ക്ക് കാരണമായി. സെൻസറുകൾ, സ്മാർട്ട് ക്യാമറകൾ, റോബോട്ടുകൾ തുടങ്ങിയവയുടെ ഉപയോഗത്തിലൂടെ ഒരു ബിസിനസിന്റെ വിവിധ വശങ്ങളിൽ നിന്നുമുള്ള ഡേറ്റ അനായാസം ശേഖരിക്കാനാകും. ബൃഹത്തായ ഈ ഡേറ്റ വിശകലനം ചെയ്യാനായി എഐ പോലെയുള്ള സാങ്കേതികവിദ്യ എഡ്ജിൽ ആവശ്യമായി വരുന്നു.

യന്ത്രങ്ങൾക്ക് കാണുക, വസ്തുക്കളെ തിരിച്ചറിയുക, സംസാരം മനസ്സിലാക്കുക, തുടങ്ങിയ മനുഷ്യസഹജ രീതികളിൽ പ്രവർത്തിക്കാൻ മനുഷ്യന്റെ കഴിവുകളെ അനുകരിക്കേണ്ടതുണ്ട്. ഡീപ് ന്യൂറൽ നെറ്റ്വർക്ക് എന്ന ഡേറ്റ ഘടനയാണ് ഇതിനായി ഉപയോഗിക്കുന്നത്.

ആധുനിക വയർലെസ് സാങ്കേതികവിദ്യകളായ 5G, വൈഫൈ-6 എന്നിവ എഡ്ജ് എഐയുടെ സുഗമമായ പ്രവർത്തനത്തിൽ ഒരു പ്രധാന പങ്കു വഹിക്കുന്നു. ഈ സാങ്കേതികവിദ്യകൾ ഉയർന്ന വേഗത, കുറഞ്ഞ ലേറ്റൻസി, ഉയർന്ന കണക്റ്റിവിറ്റി തുടങ്ങിയവ നൽകുന്നു.

സമാനമായ ചോദ്യങ്ങളും അവയുടെ ഉത്തരങ്ങളും ഉപയോഗിച്ച് പരിശീലനം ലഭിച്ച നെറ്റ്വർക്കുകളാണ് ഇവ.

ആധുനിക വയർലെസ് സാങ്കേതികവിദ്യകളായ 5G, വൈഫൈ-6 എന്നിവ എഡ്ജ് എഐയുടെ സുഗമമായ പ്രവർത്തനത്തിൽ ഒരു പ്രധാന പങ്കു വഹിക്കുന്നു. ഈ സാങ്കേതികവിദ്യകൾ ഉയർന്ന വേഗത, കുറഞ്ഞ ലേറ്റൻസി, ഉയർന്ന കണക്റ്റിവിറ്റി തുടങ്ങിയവ നൽകുന്നു. ഇവ കാര്യക്ഷമത മെച്ചപ്പെടുത്തുകയും വലിയ അളവിലുള്ള ഡേറ്റ തത്സമയം വിശകലനം ചെയ്യാൻ സഹായിക്കുകയും ചെയ്യുന്നു.

പ്രധാന നേട്ടങ്ങൾ

എഡ്ജ് എഐയുടെ പ്രധാന നേട്ടങ്ങളിലൊന്ന് വളരെ കുറഞ്ഞ ലേറ്റൻസിയാണ്. ഡേറ്റയുടെ പ്രോസസ്സിങ്ങ് പൂർണ്ണമായി ഡിവൈസുകളിൽ തന്നെ നടക്കുന്നതുകൊണ്ട് വിവരങ്ങൾ ദൂരെയുള്ള ഒരു സെർവറിലേക്കും തിരിച്ചും യാത്ര ചെയ്യേണ്ടി വരുന്നില്ല. ഇതുമൂലം ഉപയോക്താക്കൾക്ക് പ്രതികരണങ്ങൾ വളരെ എളുപ്പം ലഭ്യമാകുന്നു.

ഡേറ്റ പ്രാദേശികമായി പ്രോസസ്സ് ചെയ്യുന്നതു മൂലം ഇന്റർനെറ്റിലൂടെ അയക്കുന്ന ഡേറ്റയുടെ അളവ് കുറവാണ്. ഇതുമൂലം ഇന്റർനെറ്റ് ബാൻഡ്വിഡ്ത്തിന്റെ ഉപയോഗവും കുറയുന്നു. ഡേറ്റ കണക്ഷന് ഒരേസമയം കൂടുതൽ അളവിൽ ഡേറ്റ കൈമാറ്റം ചെയ്യാനും സ്വീകരിക്കാനും ഇത് സഹായിക്കുന്നു.

സിസ്റ്റം കണക്റ്റിവിറ്റിയും സംയോജനവും ആവശ്യമില്ലാതെ തന്നെ ഉപയോക്താക്കൾക്ക് തത്സമയം ഡേറ്റ പ്രോസസ്സ് ചെയ്യാൻ എഡ്ജ് എഐ അനുവദിക്കുന്നു. മറ്റു ലൊക്കേഷനുകളുമായി ആശയവിനിമയം നടത്താതെ തന്നെ ഡേറ്റ ഏകീകരിക്കാൻ സാധിക്കുന്നതു കൊണ്ട് ഈ പ്രക്രിയകളിൽ വളരെയധികം സമയം ലാഭിക്കാൻ സാധിക്കും.

മറ്റു നെറ്റ്വർക്കുകളിലൂടെ ഡേറ്റ അയയ്ക്കേണ്ട ആവശ്യകത കുറയുന്നതുമൂലം ഡേറ്റയുടെ സ്വകാര്യതയും, സുരക്ഷയും വർദ്ധിക്കുന്നു. ഇത് സൈബർ ആക്രമണങ്ങളിൽ നിന്നും ഒരു പരിധി വരെ സംരക്ഷണം നൽകുന്നു. തന്നെയുമല്ല ഡേറ്റയുടെ വിശകലനം പ്രാദേശികമായി നടത്തുന്നതിനാൽ ഡേറ്റ ദുരുപയോഗം ചെയ്യപ്പെടാനുള്ള സാധ്യതയും കുറയുന്നു.

ക്ലൗഡിൽ സ്ഥിതി ചെയ്യുന്ന എഐ മോഡലുകളുടെ ഉപയോഗം ചെലവേറിയതായിരിക്കും. തത്സമയ തുടർവിശകലനത്തിനായി ആവശ്യമായ ഡേറ്റ സൂക്ഷിക്കാൻ വേണ്ടി മാത്രം ക്ലൗഡ് സ്റ്റോറേജ് സംവിധാനങ്ങൾ ഉപയോഗിക്കുന്നത് ക്ലൗഡിലെ കംപ്യൂട്ടറുകളുടെയും നെറ്റ്വർക്കുകളുടെയും ജോലിഭാരം കുറയ്ക്കുകയും, ചെലവുകൾ കുറയ്ക്കാൻ സഹായിക്കുകയും ചെയ്യുന്നു.

ക്ലൗഡ് കംപ്യൂട്ടിംഗ് സേവനങ്ങളെ പൂർണ്ണമായി ആശ്രയിക്കുന്ന ഒരു സംരംഭത്തിലെ കേന്ദ്രീകൃത സംവിധാനങ്ങളുടെ ജോലിഭാരം വളരെയധികം വർദ്ധിക്കുന്നു. എഡ്ജ് എഐയുടെ ഉപയോഗത്തിലൂടെ ഡേറ്റ ഉത്ഭവസ്ഥാനത്തു നിന്നും കേന്ദ്രീകൃത സെർവറുകളിലേക്ക് അയക്കുകയും, പ്രോസസ്സ് ചെയ്ത ഡേറ്റ തിരിച്ചും അയക്കേണ്ടി വരുന്ന സാഹചര്യം ഒഴിവാക്കാനാകും. ഇത് നെറ്റ്വർക്കുകൾ, സെർവറുകൾ തുടങ്ങിയ ഹാർഡ്വെയറുകളുടെ മേലുള്ള സമ്മർദ്ദം ഗണ്യമായി കുറയ്ക്കുന്നു.

എഡ്ജ് എഐയുടെ ഉപയോഗം ഇതുപോലെ നിരവധി സൗകര്യങ്ങൾ നൽകുന്നു. ഡേറ്റയുടെ ഉറവിടത്തിനടുത്തു തന്നെയുള്ള ഡിവൈസുകളിൽ ഡേറ്റ പ്രോസസ്സ് ചെയ്യുന്നതു കാരണം എഡ്ജ് എഐ ഉപകരണങ്ങൾക്ക് ക്ലൗഡ് സംവിധാനങ്ങളോടുള്ള കണക്റ്റിവിറ്റി ഇല്ലാതെ തന്നെ സുഗമമായി പ്രവർത്തിക്കുവാൻ സാധിക്കുന്നു. ഇത് ഓട്ടോണോമസ് വാഹനങ്ങൾ, ഓട്ടോമാറ്റിക് ഡ്രോണുകൾ തുടങ്ങിയ പല ആശയങ്ങളും പ്രാവർത്തികമാക്കാൻ സഹായിച്ചിട്ടുണ്ട്.

ഓട്ടോണോമസ് വാഹനങ്ങളിലെ ക്യാമറ മുമ്പിലുള്ള വസ്തുക്കൾ, റോഡിലെ ട്രാഫിക്, ട്രാഫിക് ലൈറ്റുകൾ തുടങ്ങിയവയെപ്പറ്റിയുള്ള വിവരങ്ങളും, പുറകിലുള്ള അൾട്രാസോണിക് സെൻസറുകൾ വാഹനത്തിന്റെ ചലനം, മറ്റു വാഹനങ്ങളുമായുള്ള ആപേക്ഷിക വേഗത തുടങ്ങിയ വിവരങ്ങളും ശേഖരിക്കുന്നു.

പ്രായോഗിക തലങ്ങളിൽ

ഐഒടി സെൻസറുകൾ, സ്മാർട്ട് ക്യാമറകൾ, ഓട്ടോണോമസ് സംവിധാനങ്ങൾ തുടങ്ങിയവയുടെ വ്യാപനം വർദ്ധിക്കുന്നതോടെ എഐ ആപ്ലിക്കേഷനുകളുടെ കൂടുതൽ കാര്യക്ഷമവും, സുരക്ഷിതവുമായ, പ്രവർത്തനങ്ങൾക്ക് എഡ്ജ് എഐയുടെ സാന്നിധ്യം നിർണായകമായിക്കൊണ്ടിരിക്കുന്നു.

എഡ്ജ് എഐയുടെ യഥാർത്ഥലോക ഉപയോഗത്തിന്റെ ഏറ്റവും ദൃശ്യമായ ഉദാഹരണങ്ങളിൽ ഓട്ടോണോമസ് വാഹനങ്ങൾ, ഓട്ടോമാറ്റിക് ഡ്രോണുകൾ മുതലായവ ഉൾപ്പെടുന്നു. ഗൂഗിൾ, ഊബർ, ടെസ്ല തുടങ്ങിയ കമ്പനികൾ സ്വയംഭരണ ഡ്രൈവിംഗിനായുള്ള വിവിധ സാങ്കേതികവിദ്യകൾ വികസിപ്പിച്ചെടുത്തിട്ടുണ്ട്

ഓട്ടോണോമസ് വാഹനങ്ങളിലെ ക്യാമറ മുമ്പിലുള്ള വസ്തുക്കൾ, റോഡിലെ ട്രാഫിക്, ട്രാഫിക് ലൈറ്റുകൾ തുടങ്ങിയവയെപ്പറ്റിയുള്ള വിവരങ്ങളും, പുറകിലുള്ള അൾട്രാസോണിക് സെൻസറുകൾ വാഹനത്തിന്റെ ചലനം, മറ്റു വാഹനങ്ങളുമായുള്ള ആപേക്ഷിക വേഗത തുടങ്ങിയ വിവരങ്ങളും ശേഖരിക്കുന്നു. കൂടാതെ ലിഡാർ എന്ന സാങ്കേതികവിദ്യയുടെ (Light Detection and Ranging) സഹായത്തോടെ യാത്ര ചെയ്യേണ്ട വഴിയുടെയും, റോഡുകളുടെയും മറ്റുമുള്ള മാപ്പ് തയ്യാറാക്കുന്നു. ഈ ഡേറ്റയെല്ലാം എഐ സാങ്കേതികവിദ്യയുടെ സഹായത്തോടെ പ്രോസസ്സ് ചെയ്ത് വാഹനം മുമ്പോട്ട് പോകാനുള്ള നിർദേശങ്ങൾ നൽകുന്നു.

തത്സമയം ഡേറ്റ വിശകലനം ചെയ്യാനും വേഗത്തിൽ തീരുമാനമെടുക്കാനുമുള്ള എഡ്ജ് എഐയുടെ കഴിവ് ഇതിനെ സ്മാർട്ട് സിറ്റിയുടെ പ്രവർത്തനങ്ങളിലെ ഒരു പ്രധാന ഘടകമാക്കുന്നു. വിവിധ സെൻസറുകളിൽ നിന്നും ലഭിക്കുന്ന ഡേറ്റ തൽക്ഷണം പ്രോസസ്സ് ചെയ്ത് ഗതാഗത കുരുക്കുകൾ, സുരക്ഷാ ഭീഷണികൾ, വൈദ്യുതി വിതരണത്തിലെ അപാകതകൾ മുതലായവയോട് ഉടനടി പ്രതികരിക്കാനും, പരിഹാരം കാണുവാനും സാധിക്കുന്നതുകൊണ്ട് പൊതുസുരക്ഷ മെച്ചപ്പെടുത്താൻ ഇത് സഹായിക്കും.

ആരോഗ്യ പരിപാലന രംഗത്ത് എഡ്ജ് എഐ ഇന്ന് വ്യാപകമായി ഉപയോഗിച്ചു വരുന്നു. കുറഞ്ഞ പ്രതികരണ സമയം, മെച്ചപ്പെട്ട ഡേറ്റ സുരക്ഷ തുടങ്ങി വിവിധ ഗുണങ്ങൾ ഇത് നൽകുന്നു. ധരിക്കാവുന്ന ഉപകരണങ്ങൾ (wearable devices) ഉപയോഗിച്ച് എഡ്ജ് എഐയുടെ സഹായത്തോടെ രോഗിയുടെ രക്ത സമ്മർദ്ദം, ഹൃദയമിടിപ്പ്, തുടങ്ങിയവ തുടർച്ചയായി നിരീക്ഷിക്കാനും. ഇവയിലെ വ്യതിയാനങ്ങൾ ഉടനെ തന്നെ ആരോഗ്യ സേവനദാതാക്കളെ അറിയിക്കാനും സാധിക്കും. അതുപോലെ ഈ സാങ്കേതികവിദ്യ ഉപയോഗിച്ച് എക്സ്റേ, സിടി സ്കാൻ തുടങ്ങിയവ തത്സമയം വിശകലനം ചെയ്യാൻ സാധിക്കും. ഫ്രാക്ച്ചർ, ട്യൂമർ തുടങ്ങിയ അപാകതകളെ വേഗത്തിലും കൃത്യമായും കണ്ടെത്താൻ ഇത് സഹായിക്കും. ഇതുകൂടാതെ മെഡിക്കൽ ഡേറ്റയുടെ സ്വകാര്യത സംരക്ഷിക്കുക, ആരോഗ്യപരിപാലന രംഗത്തെ ചെലവുകൾ കുറയ്ക്കുക തുടങ്ങിയ പല രംഗങ്ങളിലും എഡ്ജ് എഐക്ക് വലിയ സംഭാവനകൾ നൽകാനാകും.

ഉൽപ്പാദന രംഗത്ത് സെൻസർ ഡേറ്റ വിശകലനം ചെയ്ത് പ്രശ്നങ്ങൾ നേരത്തെ കണ്ടുപിടിച്ച് പ്രവചനാത്മക പരിപാലനം പ്രാവർത്തികമാക്കാൻ എഡ്ജ് എഐ സഹായിക്കുന്നു. റീട്ടെയിൽ രംഗത്ത് ടെക്സ്റ്റ് അധിഷ്ഠിത തിരയലുകൾക്ക് പകരം വോയ്സ് കമാൻഡുകളിലൂടെ ഓർഡർ ചെയ്യാൻ എഡ്ജ് എഐ ഉപഭോ

ക്താക്കളെ സഹായിക്കുന്നു. എഡ്ജ് എഐയുടെ ഉപയോഗം ഇതുപോലെ പല മേഖലകളിലും ഗുണ പരമായ മാറ്റങ്ങൾ കൊണ്ടുവരും.

നൂതന പ്രവണതകൾ

എഡ്ജ് എഐ, ന്യൂറൽ നെറ്റ്വർക്ക്, ഐഒടി, 5G തുടങ്ങിയ സാങ്കേതിക വിദ്യയിലുണ്ടായ വികസനങ്ങൾ സാധാരണമായ യന്ത്രപഠനത്തിന്റെ (generalised machine learning) അടിസ്ഥാന സൗകര്യങ്ങളിലെ വർദ്ധനയ്ക്കു കാരണമായി. ഇത് എഡ്ജ് എഐ സാങ്കേതികവിദ്യയെ തങ്ങളുടെ ബിസിനസുകളിലേക്ക് കൊണ്ടുവരാനും തത്സമയ പ്രതികരണങ്ങൾക്കനുസരിച്ച് പ്രവർത്തിക്കാനും സംരംഭങ്ങളെ പ്രാപ്തമാക്കുന്നു.

എഡ്ജ് എഐയിലെ ഭാവി പ്രവണതകളിൽ ചിലത് ഇവയാണ്:

• മൈക്രോ എഐ: സ്മാർട്ട് വാച്ചുകൾ, ഐഒടി സെൻസറുകൾ, ഡ്രോണുകൾ തുടങ്ങിയ ഉപകരണങ്ങളിൽ നേരിട്ട് ഉപയോഗിക്കാൻ കഴിയുന്ന ഭാരം കുറഞ്ഞ, ഉയർന്ന ഊർജ്ജക്ഷമതയുള്ള എഐ മോഡലുകൾ ഉപയോഗിക്കുന്ന രീതിയാണ് ഇത്.

• എഡ്ജ് എഐ ഡിവൈസുകളിൽ ഏറ്റവും നൂതനമായ 5G സാങ്കേതികവിദ്യയുടെ ഉപയോഗം ഈ ഉപകരണങ്ങൾക്കാവശ്യമായ ഉയർന്ന വേഗതയും, കുറഞ്ഞ ലേറ്റൻസിയും ഉറപ്പുവരുത്തുന്നു.

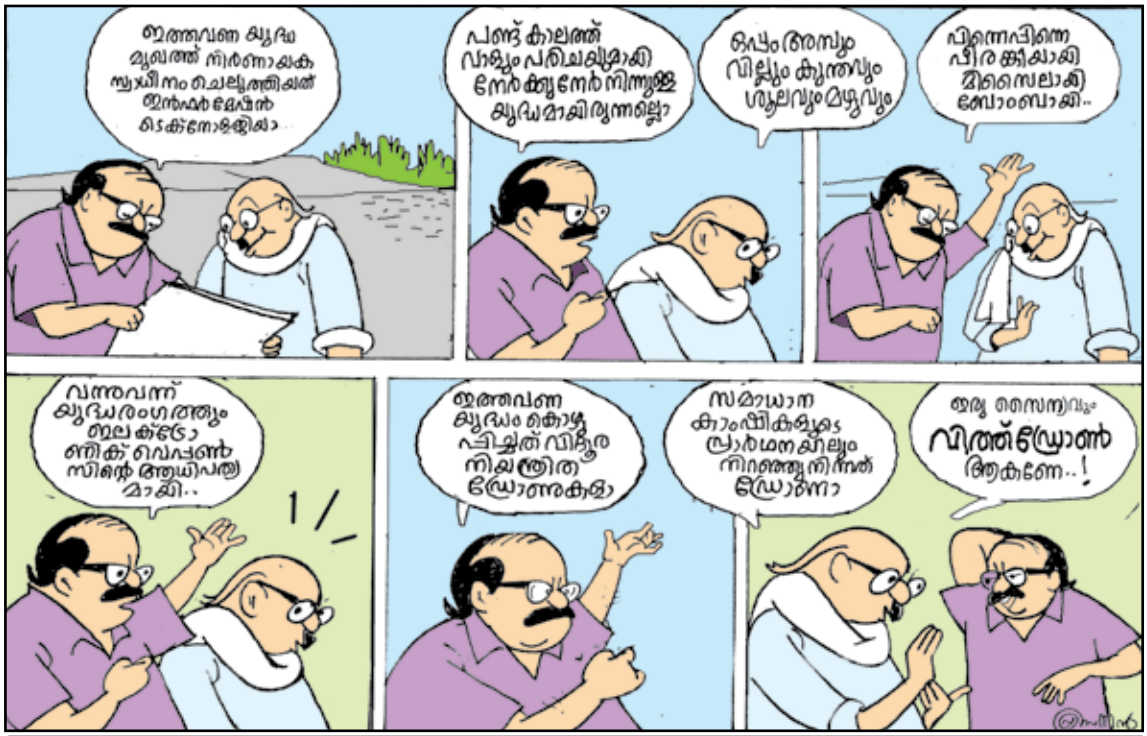
• ജനറേറ്റീവ് എഐ മോഡലുകൾ: വരും ദിനങ്ങളിൽ എഡ്ജ് ഡിവൈസുകളിൽ ജനറേറ്റീവ് എഐ മോഡലുകൾ കൂടുതലായി സംയോജിപ്പിക്കുമെന്ന് കരുതുന്നു. ഇത് തത്സമയ ഉൾക്കാഴ്ചകളും, വ്യക്തിഗത അനുഭവങ്ങളും നൽകാൻ സഹായിക്കും.

• വ്യവസായരംഗത്തെ പരിവർത്തനം: എഡ്ജ് എഐയുടെ വ്യാപനം വർദ്ധിക്കുന്നതോടെ ഗതാഗതം, കൃഷി, ആരോഗ്യ പരിപാലനം, ഉത്പാദനം തുടങ്ങിയ മേഖലകളിൽ വലിയ മാറ്റങ്ങൾ കൊണ്ടുവരും എന്നു പ്രതീക്ഷിക്കുന്നു.

• എഡ്ജ് എഐയുടെ വിന്യാസം വർദ്ധിക്കുന്നതോടെ ഫെഡറേറ്റഡ് ലേർണിങ്ങ് (Federated learning) അഥവാ സഹകരിച്ചുള്ള പഠനം (Collaborative learning) കൂടുതൽ വ്യാപകമാകുമെന്ന് കരുതുന്നു. വിവിധ ഉപയോക്താക്കൾ സംയുക്തമായി ഒരു എഐ മോഡലിനെ പരിശീലിപ്പിക്കുന്ന രീതിയാണിത്. ഇതിൽ വിവിധ പങ്കാളികൾ തങ്ങളുടെ ഡേറ്റ സ്വയം സൂക്ഷിക്കുന്നതുകൊണ്ട് ഡേറ്റ സ്വകാര്യത സംരക്ഷിക്കപ്പെടുന്നു. സ്വകാര്യ ഡേറ്റയുടെ മാനേജ്മെന്റിനും സംഭരണത്തിനുമായുള്ള മാനദണ്ഡങ്ങളും, നിയമങ്ങളും പാലിക്കപ്പെടുന്നതുകൊണ്ട് ഫെഡറേറ്റഡ് ലേർണിംഗ് വലിയ സ്വീകാര്യത കൈവരിച്ചിട്ടുണ്ട്.

ഡേറ്റ പ്രോസസ്സിങ്ങ് സംവിധാനങ്ങളെ ഡേറ്റയുടെ ഉറവിടത്തിനടുത്ത് കൊണ്ടുവന്ന് എഡ്ജ് എഐ ഡേറ്റ പ്രോസസ്സിങ്ങ് രംഗത്ത് വൻ മാറ്റങ്ങൾ കൊണ്ടുവരുന്നു എന്ന് കാണാം. വിവരസാങ്കേതിക വിദ്യയുടെ വളർച്ചയിൽ എഐ സംയോജിത എഡ്ജ് കംപ്യൂട്ടിങ്ങ് ഭാവിയിൽ വലിയ സംഭാവനകൾ നൽകും എന്നതിൽ സംശയമില്ല. ●

വിറ്റിമൗസ് — പ്രസന്നൻ



Info-Kairali Computer Magazine, Owned, Edited & Printed by Sojan Jose, Pullappallil, Manjoor P.O., Kuruppanthara, Kottayam.
Printed at Print Park, Kottayam and Published by Kairali Publications, Kuruppanthara, Kottayam. Editor- Sojan Jose

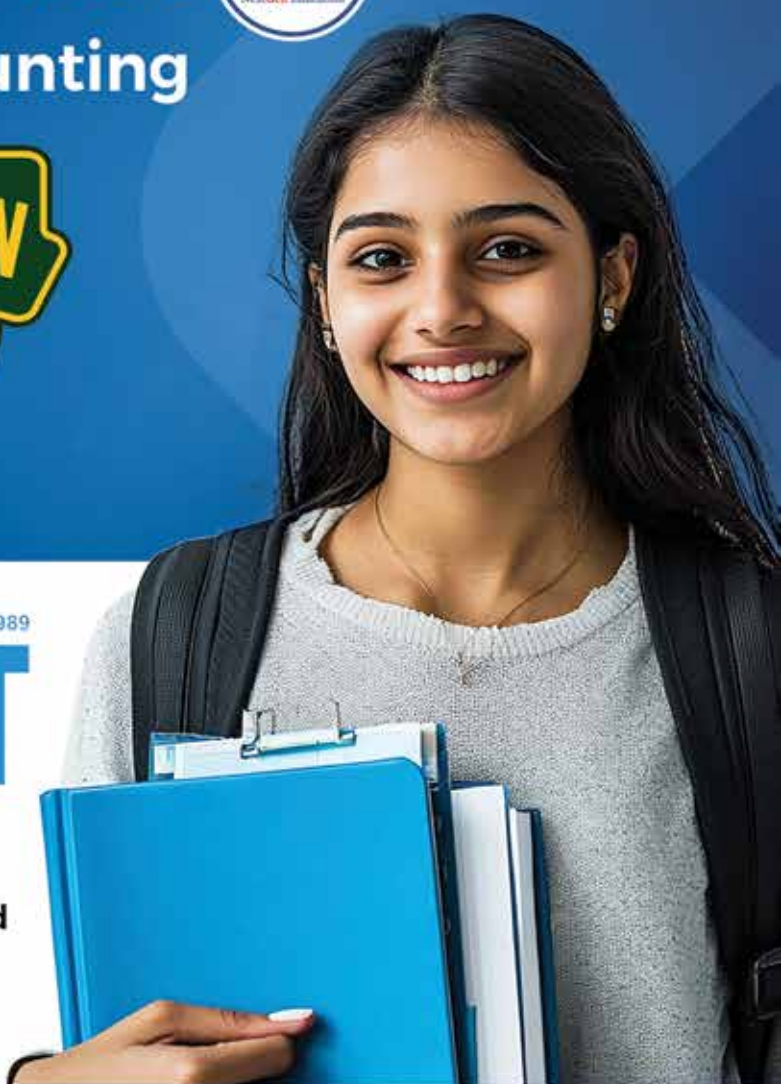
+2/DEGREE കഴിഞ്ഞവർക്ക്

സുവർണ്ണാവസരം

SAP S/4 HANA

Financial Accounting

ADMISSION OPEN



Since 1989

NICT

3rd Floor
Triveni Complex
Tourist Banglow Road
KOTTAYAM
Ph: 9447464308

PUSH YOUR SAP SKILLS TO A NEXT LEVELS
BE A NEXT GENERATION LEARNER

Info-Kairali 300 **JUNE 2025**
Published on 29 MAY 2025
Price Rs.30
RNI-KERMAL/1998/1064 Regd. No. H6-42564/98

Registered-Regn No.KL/KTM/42/2024-26
Licence No.