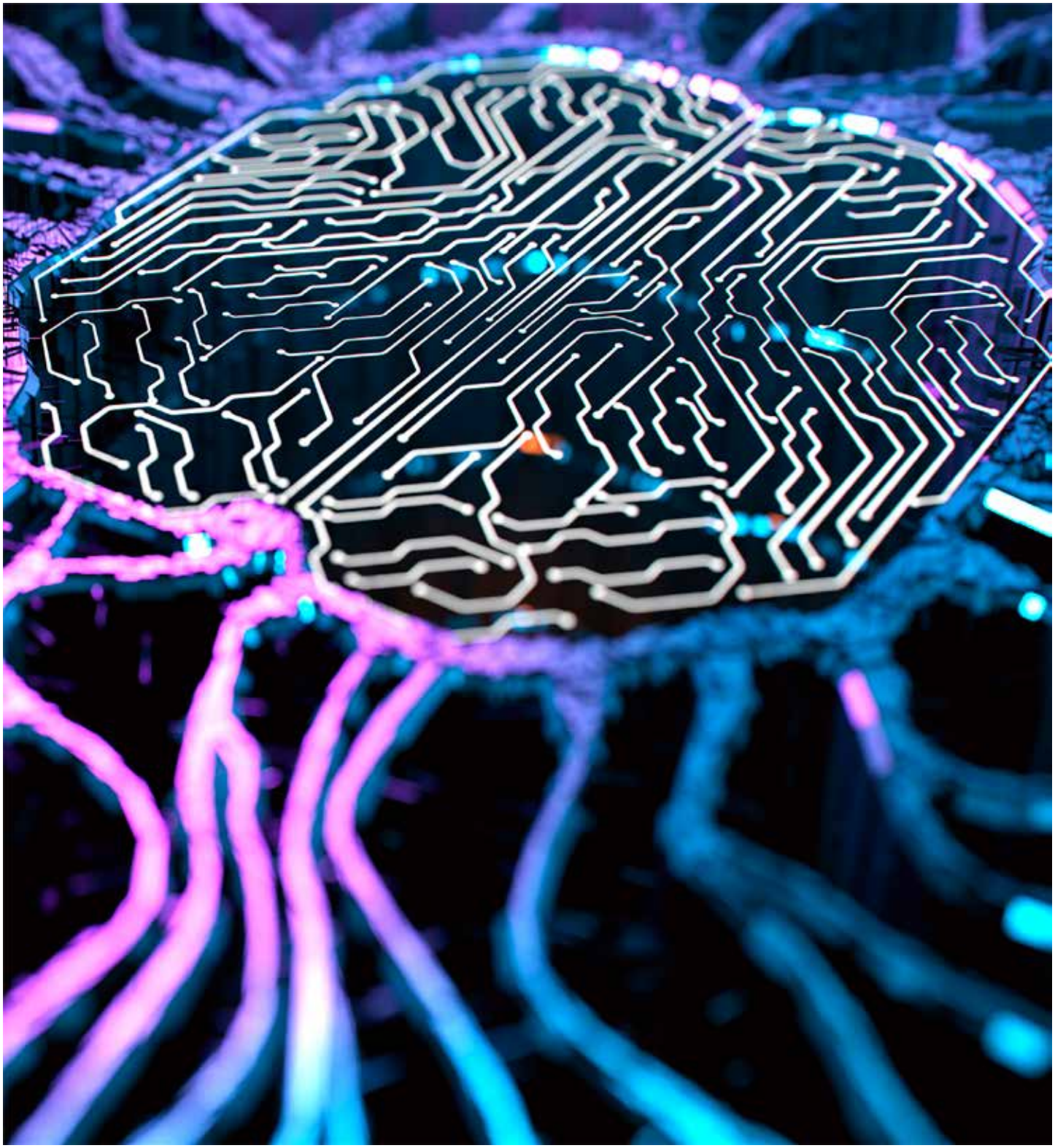
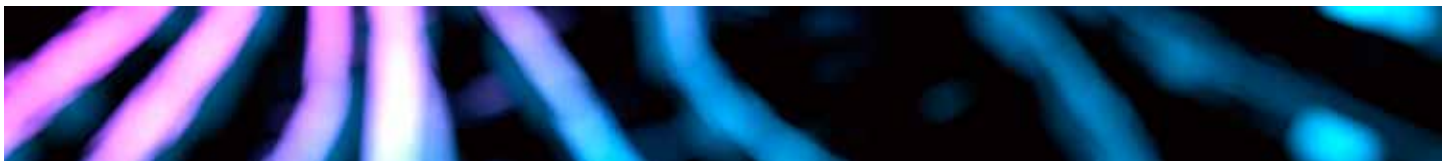
လုံခြုံသော AI (ဉာဏ်ရည်တု) စနစ် ဖွံ့ဖြိုးတိုးတက်ရေးဆိုင်ရာ လမ်းညွှန်ချက်များ





National Cyber Security Centre
a part of GCHQ

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

National Cyber and Information Security Agency

Republic of Estonia
Information System Authority

Department of Justice
Federal Bureau of Investigation

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

INCD
Israel National Cyber Directorate

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

NISC
内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

National Cyber Security Centre

NITDA

NSM
NORWEGIAN NATIONAL CYBER SECURITY CENTRE

National Security Agency
United States of America

NASK

국가정보원
National Intelligence Service

Ministerstwo Cyfryzacji

CSA SINGAPORE
Cyber Security Agency of Singapore

ဤစာတမ်းအကြောင်း

ဤစာတမ်းကို UK အမျိုးသားဆိုက်ဘာလုံခြုံရေး စင်တာ (NCSC)၊ US ဆိုက်ဘာလုံခြုံရေးနှင့် အခြေခံအဆောက်အအုံ လုံခြုံရေးအေဂျင်စီ (CISA) နှင့် အောက်ပါ နိုင်ငံတကာမိတ်ဖက်အဖွဲ့အစည်းများမှ ထုတ်ဝေထားသည်။

- အမျိုးသား လုံခြုံရေးအေဂျင်စီ (NSA)
- အမေရိကန် ဗဟိုထောက်လှမ်းရေး ဗျူရို (FBI)
- ဩစတြေးလျလုံခြုံရေးအချက်ပြ ညွှန်ကြားရေးမှူးရုံး၏ ဩစတြေးလျ ဆိုက်ဘာလုံခြုံရေးစင်တာ (ACSC)
- ကနေဒါ ဆိုက်ဘာလုံခြုံရေးစင်တာ (CCCS)
- နယူးဇီလန် အမျိုးသားဆိုက်ဘာလုံခြုံရေးစင်တာ (NCSC-NZ)
- ချီလီအစိုးရ ကွန်ပျူတာလုံခြုံရေးဆိုင်ရာ အပြစ်အပျက် တုံ့ပြန်ရေးအဖွဲ့ (CSIRT)
- ချက်နိုင်ငံ အမျိုးသားဆိုက်ဘာနှင့် သတင်းအချက်အလက် လုံခြုံရေး အေဂျင်စီ (NUKIB)
- အက်စတိုနီးယားနိုင်ငံ သတင်းအချက်အလက် လုံခြုံရေး အာဏာပိုင် (RIA) နှင့် အက်စတိုနီးယားနိုင်ငံ အမျိုးသားဆိုက်ဘာလုံခြုံရေးစင်တာ (NCSC-EE)
- ပြင်သစ်နိုင်ငံ ဆိုက်ဘာလုံခြုံရေး အေဂျင်စီ (ANSSI)
- ဂျာမနီနိုင်ငံ သတင်းအချက်အလက် လုံခြုံရေးဆိုင်ရာ ဖက်ဒရယ်ရုံး (BSI)
- အစ္စရေးနိုင်ငံ အမျိုးသားဆိုက်ဘာ ညွှန်ကြားရေးမှူးရုံး (INCD)
- အီတလီနိုင်ငံ အမျိုးသားဆိုက်ဘာလုံခြုံရေး အေဂျင်စီ (ACN)
- ဂျပန်နိုင်ငံ ဆိုက်ဘာလုံခြုံရေးဖြစ်ရပ်ဆိုင်ရာ အသင့်ဖြစ်မှုနှင့် နည်းဗျူဟာဆိုင်ရာ အမျိုးသားစင်တာ (NISC)
- ဂျပန်နိုင်ငံ သိပ္ပံ၊ နည်းပညာနှင့် ဆန်းသစ်တီထွင်မှု မူဝါဒ အတွင်းဝန်ရုံး၊ အစိုးရအဖွဲ့ရုံး
- နိုင်ဂျီးရီးယားနိုင်ငံ အမျိုးသားသတင်းအချက်အလက် နည်းပညာ ဖွံ့ဖြိုးတိုးတက်ရေး အေဂျင်စီ (NITDA)
- နော်ဝေနိုင်ငံ အမျိုးသားဆိုက်ဘာလုံခြုံရေး စင်တာ (NCSC-NO)
- ပိုလန်နိုင်ငံ ဒီဂျစ်တယ်ရေးရာ ဝန်ကြီးဌာန
- ပိုလန်နိုင်ငံ NASK အမျိုးသားသုတေသနအသင်း (NASK)
- ကိုးရီးယားသမ္မတနိုင်ငံ အမျိုးသားထောက်လှမ်းရေးဌာန (NIS)
- စင်ကာပူနိုင်ငံ ဆိုက်ဘာလုံခြုံရေး အေဂျင်စီ (CSA)

အသိအမှတ်ပြုမှုများ

အောက်ပါအဖွဲ့အစည်းများမှ ဤလမ်းညွှန်ချက်များ ဖွံ့ဖြိုးတိုးတက်ရေးကို ပံ့ပိုးပေးသည် -

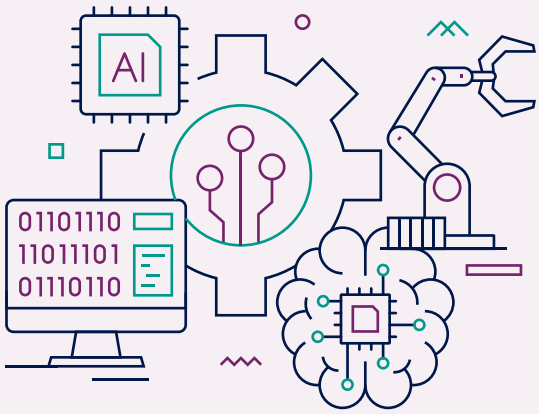
- Alan Turing အသင်း
- Anthropic
- Databricks
- ဂျော့ဂျ်တောင်းတက္ကသိုလ် လုံခြုံရေးနှင့် နည်းပညာပေါ်ထွန်းရေး စင်တာ
- Google
- Google DeepMind
- IBM
- ImBue
- Microsoft
- OpenAI
- Palantir
- RAND
- Scale AI
- Carnegie Mellon တက္ကသိုလ်မှ ဆော့ဖ်ဝဲလ်အင်ဂျင်နီယာ အသင်း
- AI လုံခြုံရေးအတွက် စတန်းဖော့ဒ်စင်တာ
- ပထဝီနိုင်ငံရေး၊ နည်းပညာနှင့် အုပ်ချုပ်ရေးဆိုင်ရာ စတန်းဖော့ဒ် အစီအစဉ်

မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤစာတမ်းပါ အချက်အလက်များကို NCSC နှင့် ထုတ်ဝေရေးအဖွဲ့အစည်းများမှ" အရှိအတိုင်း "တင်ဆက်ပေးထားပြီး ဥပဒေအရလိုအပ်ခြင်းမှအပ ၎င်းအားသုံးစွဲ၍ ဖြစ်ပေါ်လာသော ဆုံးရှုံးမှု၊ ထိခိုက်မှု သို့မဟုတ် ပျက်စီးမှုတစ်စုံတစ်ရာအတွက် ၎င်းတို့တွင် တာဝန်မရှိပါ။ ဤစာတမ်းပါ အချက်အလက်များသည် NCSC နှင့် ထုတ်ဝေရေးအဖွဲ့အစည်းများ၏ မည်သည့် ကြားခံပါတီအဖွဲ့အစည်း၊ ထုတ်ကုန် သို့မဟုတ် ဝန်ဆောင်မှုကိုမှ အားပေးခြင်း သို့မဟုတ် ထောက်ခံခြင်းမဟုတ်ပါ။ ဝက်ဘ်ဆိုက်များ၏ လင့်ခ်များနှင့် ကိုးကားချက်များအပြင် ကြားခံအဖွဲ့အစည်းအချက်အလက်များကို အချက်အလက် အနေဖြင့်သာ ဖော်ပြပေးထားခြင်းဖြစ်ပြီး ထိုရင်းမြစ်များကို အခြားသူများအား ထောက်ခံပေးခြင်း သို့မဟုတ် အားပေးခြင်းမဟုတ်ပါ။

ဤစာတမ်းကို မီးအချက်ပြလုပ်ထုံးလုပ်နည်း -အကန့်အသတ်မရှိ ပုံစံဖြင့် (TLP:CLEAR basis) (https://www.first.org/tlp/) တွင် ရရှိနိုင်ပါသည်။

အကြောင်းအရာများ



အဓိကအကြောင်းအရာ အကျဉ်းချုပ်

ဤစာတမ်းသည် ဉာဏ်ရည်တု (AI) ကို အသုံးပြုသည့်စနစ် တစ်ခုခုပံ့ပိုးပေးသူများအတွက် ရည်ရွယ်ပြီး အဆိုပါစနစ်များကို အစမှ ဖန်တီးထားခြင်းဖြစ်စေ သို့မဟုတ် အခြားသူများပံ့ပိုးထားသည့် ကိရိယာများနှင့် ဝန်ဆောင်မှုများအပေါ်မှာ တည်ဆောက်ထားခြင်းဖြစ်စေ ဤလမ်းညွှန်ချက်သည် အကျုံးဝင်ပါသည်။ ဤလမ်းညွှန်ချက်များကို အကောင်အထည်ဖော်ဆောင်ခြင်း သည် ပံ့ပိုးပေးသူများ ရည်ရွယ်ထားသလိုလည်ပတ်သည့်၊ လိုအပ်သည့်အခါ ရရှိနိုင်သည့် AI စနစ်များ တည်ဆောက်ရန် ကူညီပေးမည်ဖြစ်ပြီး ထိရှလွယ်သောအချက်အလက်များကို အခွင့်အာဏာမရှိသော အဖွဲ့အစည်းများထံသို့ မပေါက်ကြားအောင် လုပ်ဆောင်ရာတွင် အထောက်အကူပြုစေနိုင်ပါသည်။

ဤစာတမ်းကို အဓိကအားဖြင့် အဖွဲ့အစည်းတစ်ခုမှ ပံ့ပိုးပေးထားသော မိုဒယ်များကို အသုံးပြုနေသော သို့မဟုတ် ပြင်ပအပ်ပလီကေးရှင်း ပရိုဂရမ်မင်း ကြားခံဆက်သွယ်ရေးစနစ် (APIs) ကို အသုံးပြုနေသော AI ပံ့ပိုးပေးသူများအတွက် ရည်ရွယ်ထားပါသည်။ (ဒေတာသိပ္ပံပညာရှင်များ၊ ဒဗလိုပါများ၊ မန်နေဂျာများ၊ ဆုံးဖြတ်ချက်ချသူများနှင့် အန္တရာယ်လျှော့ချသူများ အပါအဝင်) သက်ဆိုင်ရာ အဖွဲ့အစည်းများ**အားလုံး**အနေဖြင့် ၎င်းတို့၏ AI စနစ်များ၏ **ဒီဇိုင်း၊ ဖွံ့ဖြိုးတိုးတက်မှု၊ ဖြန့်ကြက်မှု**အပြင် **လည်ပတ်မှု**တို့နှင့်ပတ်သက်၍ ဆုံးဖြတ်ချက်များ ချမှတ်ရာတွင် အထောက်အကူဖြစ်စေရန်အတွက် ဤလမ်းညွှန်ချက်များကို ဖတ်ရှုရန် ကျွန်ုပ်တို့ တိုက်တွန်းလိုက်ပါသည်။

လမ်းညွှန်ချက်များအကြောင်း

AI စနစ်များတွင် လူ့ဘောင်အဖွဲ့အစည်းကို အကျိုးအများအပြား ဖြစ်စေသည့် အလားအလာရှိပါသည်။ သို့သော် AI ၏ အခွင့်အလမ်းများ အပြည့်အဝ ဖြစ်ပေါ်လာရန် ယင်းကို ဖွံ့ဖြိုးတိုးတက်အောင် လုပ်ဆောင်ရမည်၊ ဖြန့်ကြက်ရမည်၊ လုံခြုံပြီး တာဝန်ယူတာဝန်ခံသည့်ပုံစံဖြင့် ဆောင်ရွက်ရပါမည်။

AI စနစ်များသည် သာမန် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်မှုများနှင့်အတူ ထည့်သွင်းစဉ်းစားရန် လိုအပ်သည့် လုံခြုံရေးအားနည်းချက်အသစ်များ ကျရောက်နိုင်သည်။ ဖွံ့ဖြိုးတိုးတက်မှုအရှိန်အဟုန် မြင့်မားလာသည့်အခါ - AI ဖြစ်ရပ်မှာကဲ့သို့ - လုံခြုံရေးမှာ အများအားဖြင့် ဒုတိယဦးစားပေး ဖြစ်လာနိုင်သည်။ လုံခြုံရေးသည် ဖွံ့ဖြိုးတိုးတက်ရေးအဆင့်အတွက်သာမက စနစ်ဖြစ်စဉ်တစ်လျှောက်လုံးအတွက်ပါ အဓိကလိုအပ်ချက်တစ်ခု ဖြစ်ရမည်။

ဤအကြောင်းကြောင့် လမ်းညွှန်ချက်များကို AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်အတွင်း- **လုံခြုံသောဒီဇိုင်း၊ လုံခြုံသောဖွံ့ဖြိုးတိုးတက်မှု၊ လုံခြုံသောဖြန့်ကြက်မှု**နှင့် **လုံခြုံသောလည်ပတ်မှုနှင့် ပြုပြုပြင်ထိန်းသိမ်းမှု**ဟူ၍ အဓိကကဏ္ဍလေးပိုင်း ပိုင်းခြားထားသည်။ ကဏ္ဍတစ်ခုစီအတွက် အဖွဲ့အစည်းဆိုင်ရာ AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှု လုပ်ငန်းစဉ်အပေါ် ဖြစ်စေနိုင်သောအန္တရာယ်ကို လျှော့ချပေးမည့် ထည့်သွင်းစဉ်းစားမှုများနှင့် အန္တရာယ်လျှော့ပေါ့ပေးမှုများကို ကျွန်ုပ်တို့ အကြံပြုထားပါသည်။

1. လုံခြုံသောဒီဇိုင်း

ဤကဏ္ဍတွင် AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်၏ ဒီဇိုင်းအဆင့်နှင့်ဆိုင်သော လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။ ယင်းတွင် စနစ်နှင့် မော်ဒယ်ဒီဇိုင်းကို ထည့်သွင်းစဉ်းစားရန် သီးခြားအကြောင်းအရာများနှင့် အပေးအယူလုပ်ခြင်းများအပြင် အန္တရာယ်များကို နားလည်ခြင်းနှင့် ခြိမ်းခြောက်မှုဖော်ထုတ်ခြင်းတို့ ပါဝင်သည်။

2. လုံခြုံသောဖွံ့ဖြိုးတိုးတက်မှု

ဤကဏ္ဍတွင် ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက် လုံခြုံရေး၊ အထောက်အထားစာရွက်စာတမ်းအပြင် ပိုင်ဆိုင်မှုနှင့် နည်းပညာဆိုင်ရာ အကြွေး စီမံခန့်ခွဲမှုအပါအဝင် AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်၏ ဖွံ့ဖြိုးတိုးတက်မှုအဆင့်နှင့်ဆိုင်သော လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။

3. လုံခြုံသောဖြန့်ကြက်မှု

ဤကဏ္ဍတွင် အခြေခံအဆောက်အအုံနှင့် မော်ဒယ်များကို ချိုးဖောက်ခြင်း၊ ခြိမ်းခြောက်ခြင်း သို့မဟုတ် ဆုံးရှုံးမှုမှ ကာကွယ်ခြင်း၊ အဖြစ်အပျက်စီမံခန့်ခွဲရေး လုပ်ငန်းစဉ်များ ဆောင်ရွက်ခြင်းနှင့် တာဝန်ယူထုတ်ပေးခြင်းများအပါအဝင် AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်၏ ဖြန့်ကြက်မှုအဆင့်နှင့်ဆိုင်သော လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။

4. လုံခြုံသောလည်ပတ်မှုနှင့် ပြုပြုပြင်ထိန်းသိမ်းမှု

ဤကဏ္ဍတွင် AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်၏ လုံခြုံသောလည်ပတ်မှုနှင့် ပြုပြုပြင်ထိန်းသိမ်းမှုအဆင့်နှင့်ဆိုင်သော လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။ ယင်းမှာ မှတ်တမ်းတင်ခြင်းနှင့် စောင့်ကြည့်ခြင်း၊ မွမ်းမံမှု စီမံဆောင်ရွက်ရေးနှင့် အချက်အလက် မျှဝေခြင်းအပါအဝင် စနစ်တစ်ခု ဖြန့်ကြက်ခြင်းနှင့် အထူးသက်ဆိုင်သော လုပ်ဆောင်မှုများဆိုင်ရာ လမ်းညွှန်ချက်များကို ပေးပါသည်။

လမ်းညွှန်ချက်များသည်' နဂိုမူလအားဖြင့် လုံခြုံသော 'ချဉ်းကပ်နည်းကို လိုက်နာပြီး CISA မှ ထုတ်ဝေသော NCSC ၏လုံခြုံသောဖွံ့ဖြိုးတိုးတက်မှုနှင့် ဖြန့်ကြက်မှု လမ်းညွှန်ချက်၊ NIST ၏ လုံခြုံသောဆော့ဖ်ဝဲလ် ဖွံ့ဖြိုးတိုးတက်မှု မူဘောင်နှင့်' ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း စည်းမျဉ်းများ၊ NCSC နှင့် နိုင်ငံတကာဆိုက်ဘာ အေဂျင်စီများမှ သတ်မှတ်ဖော်ပြထားသော အခြေခံသဘောတရားများနှင့် အနီးစပ်ဆုံး ချိန်ညှိထားပါသည်။ ၎င်းတို့မှ ဦးစားပေးသတ်မှတ်သည်မှာ -

- ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးရလဒ်များအတွက် တာဝန်ယူခြင်း
- အလုံးစုံ ပွင့်လင်းမြင်သာမှုနှင့် တာဝန်ခံမှုကို လက်ခံခြင်း
- အဖွဲ့အစည်းတည်ဆောက်ပုံနှင့် ခေါင်းဆောင်မှုကို ဒီဇိုင်းဖြင့် လုံခြုံအောင် တည်ဆောက်ခြင်းသည် ထိပ်တန်းဦးစားပေးကိစ္စ ဖြစ်သည်။

နိဒါန်း

ဉာဏ်ရည်တု (AI) စနစ်များတွင် လူ့ဘောင်အဖွဲ့အစည်းကို အကျိုးအများအပြား ဖြစ်စေသည့် အလားအလာရှိပါသည်။ သို့သော် AI ၏ အခွင့်အလမ်းများ အပြည့်အဝ ဖြစ်ပေါ်လာရန် ယင်းကို ဖွံ့ဖြိုးတိုးတက်အောင် လုပ်ဆောင်ရမည်၊ ဖြန့်ကြက်ရမည်၊ လုံခြုံပြီး တာဝန်ယူတာဝန်ခံသည့်ပုံစံဖြင့် ဆောင်ရွက်ရပါမည်။ ဆိုက်ဘာလုံခြုံရေးသည် AI စနစ်များ၏ ဘေးကင်းမှု၊ ခံနိုင်ရည်ရှိမှု၊ အတွင်းရေး၊ တရားမျှတမှု၊ အကျိုးသက်ရောက်မှုနှင့် ယုံကြည်စိတ်ချရမှုတို့အတွက် မရှိမဖြစ်လိုအပ်သော လိုအပ်ချက်တစ်ခုဖြစ်သည်။

သို့သော် AI စနစ်များသည် သာမန်ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်မှုများနှင့်အတူ ထည့်သွင်းစဉ်းစားရန် လိုအပ်သည့် လုံခြုံရေးအားနည်းချက်အသစ်များ ကျရောက်နိုင်သည်။ ဖွံ့ဖြိုးတိုးတက်မှုအရှိန်အဟုန် မြင့်မားလာသည့်အခါ -AI ဖြစ်ရပ်မှာကဲ့သို့ -လုံခြုံရေးမှာ အများအားဖြင့် ဒုတိယဦးစားပေး ဖြစ်လာနိုင်သည်။ လုံခြုံရေးသည် ဖွံ့ဖြိုးတိုးတက်ရေးအဆင့်အတွက်သာမက စနစ်ဖြစ်စဉ်တစ်လျှောက်လုံးအတွက် အဓိကလိုအပ်ချက်တစ်ခု ဖြစ်ရမည်။

ဤစာတမ်းသည် ဉာဏ်ရည်တု (AI) ကို အသုံးပြုသည့်စနစ် တစ်ခုခုပုံပိုးပေးသူများ[1]အတွက် ရည်ရွယ်ပြီး အဆိုပါစနစ်များကို မှာ အစမှ ဖန်တီးထားခြင်းဖြစ်စေ သို့မဟုတ် အခြားသူများပုံပိုးထားသည့် ကိရိယာများနှင့် ဝန်ဆောင်မှုများအပေါ်မှာ တည်ဆောက်ထားခြင်းဖြစ်စေ ဤလမ်းညွှန်ချက်သည် အကျုံးဝင်ပါသည်။ ဤလမ်းညွှန်ချက်များကို အကောင်အထည်ဖော်ဆောင်ခြင်း သည် ပုံပိုးပေးသူများ ရည်ရွယ်ထားသလိုလည်ပတ်သည့်၊ လိုအပ်သည့်အခါ ရရှိနိုင်သည့် AI စနစ်များ တည်ဆောက်ရန် ကူညီပေးမည်ဖြစ်ပြီး ထိရှလွယ်သောအချက်အလက်များကို အခွင့်အာဏာမရှိသော အဖွဲ့အစည်းများထံသို့ မပေါက်ကြားအောင် လုပ်ဆောင်ရာတွင် အထောက်အကူ ပြုစေနိုင်ပါသည်။

ဤလမ်းညွှန်ချက်များကို သတ်မှတ်ထားသော ဆိုက်ဘာလုံခြုံရေး၊ အန္တရာယ်စီမံခန့်ခွဲမှု၊ နှင့် အဖြစ်အပျက်တုံ့ပြန်ရေးဆိုင်ရာ အကောင်းဆုံးအလေ့အကျင့်နှင့်အတူ ထည့်သွင်းစဉ်းစားသင့်သည်။ အထူးသဖြင့် ကျွန်ုပ်တို့မှ ပံ့ပိုးသူများအား US ဆိုက်ဘာလုံခြုံရေးနှင့် အခြေခံအဆောက်အအုံ လုံခြုံရေးအေဂျင်စီ (CISA)၊ UK အမျိုးသား ဆိုက်ဘာလုံခြုံရေး စင်တာ (NCSC) နှင့် ကျွန်ုပ်တို့၏ နိုင်ငံတကာမိတ်ဖက်အဖွဲ့အစည်းများမှ ရေးဆွဲထားသော' ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း' [2]စည်းမျဉ်းများကို လိုက်နာရန် တိုက်တွန်းထားပါသည်။ ၎င်းတို့မှ ဦးစားပေးသတ်မှတ်သည်မှာ -

- ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးရလဒ်များအတွက် တာဝန်ယူခြင်း
- အလုံးစုံ ပွင့်လင်းမြင်သာမှုနှင့် တာဝန်ခံမှုကို လက်ခံခြင်း
- အဖွဲ့အစည်းတည်ဆောက်ပုံနှင့် ခေါင်းဆောင်မှုကို ဒီဇိုင်းဖြင့် လုံခြုံအောင် တည်ဆောက်ခြင်းသည် ထိပ်တန်းဦးစားပေးကိစ္စ ဖြစ်သည်။

'ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း 'စည်းမျဉ်းများကို လိုက်နာရာတွင် စနစ်ဖြစ်စဉ်တစ်လျောက်လုံး၌ အရေးပါသောအရင်းအမြစ်များ လိုအပ်ပါသည်။ ဆိုလိုသည်မှာ ထုတ်လုပ်သူများဒဗလိုပါများအနေဖြင့် စနစ်ဒီဇိုင်းအလွှာတိုင်းနှင့် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်အဆင့်များတွင် ဝယ်ယူသုံးစွဲသူများကို ကာကွယ်ပေးသော ကိရိယာများ၏ **အင်္ဂါရုပ်များ၊ စက်ယန္တရားများ**နှင့် **အကောင်အထည်ဖော်ဆောင်မှု**တို့ကို ဦးစားပေးလုပ်ဆောင်ရပါမည်။ ဤသို့လုပ်ဆောင်ခြင်းမှ ဝယ်ယူသုံးစွဲသူ များနှင့် ၎င်းတို့၏ အချက်အလက်များကို မဝေးတော့သည့်ကာလတွင် ကာကွယ်ပေးသည့်အပြင် နောက်ပိုင်းတွင် အကုန်အကျများသည့် ပြန်လည်ဒီဇိုင်းရေးဆွဲခြင်းများကိုလည်း ကာကွယ်ပေးမည် ဖြစ်သည်။

AI လုံခြုံရေး အဘယ်ကြောင့် ကွဲပြားကြသနည်း။

ဤစာတမ်းတွင် စက်ကိရိယာဖြင့်သင်ကြားရေး (ML) အပ်ပလီကေးရှင်းများ[3]ကို အထူးရည်ညွှန်းရန် 'AI' ဟူသော ဝေါဟာရကို ကျွန်ုပ်တို့ အသုံးပြုပါသည်။ ML အမျိုးအစားအားလုံးကို ထည့်သွင်းစဉ်းစားထားပါသည်။ ML အပ်ပလီကေးရှင်းများကို အောက်ပါတို့ပါဝင်သည့် အပ်ပလီကေးရှင်းများအဖြစ် သတ်မှတ်ပါသည် -

- လူသားတစ်ဦးမှ အထူးတလည်စီမံထားသည့် စည်းမျဉ်းများ မလိုအပ်ဘဲ ကွန်ပျူတာများကို မှတ်မိစေပြီး အကြောင်းအရာကို အချက်အလက်ပုံစံများဖြင့် ဆောင်ကြဉ်းပေးနိုင်အောင် ခွင့်ပြုသည့် ဆော့ဖ်ဝဲလ်အစိတ်အပိုင်းများ (မော်ဒယ်များ) ပါဝင်သည့် အပ်ပလီကေးရှင်းများ
- ကိန်းဂဏန်းဆိုင်ရာကျိုးကြောင်းဆင်ခြင်မှုအပေါ် အခြေခံ၍ ကြိုတင်ခန့်မှန်းချက်များ၊ ထောက်ခံအကြံပြုချက်များ သို့မဟုတ် ဆုံးဖြတ်ချက်များလုပ်ဆောင်သည့် အပ်ပလီကေးရှင်းများ

ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ခြိမ်းခြောက်မှုများ ရှိသည့်အပြင် AI စနစ်များသည် အားနည်းချက်အသစ်များ ရှိနိုင်သည်။ 'ပဋိပက္ခဖြစ်စေသော စက်ကိရိယာဖြင့် သင်ကြားရေး' (AML) ဟူသော စကားရပ်ကို ဟာ့ဒ်ဝဲလ်၊ အလုပ်စီးဆင်းမှုများနှင့် ပစ္စည်းဖြည့်သွင်းရေး ကွင်းဆက်များအပါအဝင် ML အစိတ်အပိုင်းများထဲရှိ အခြေခံအားနည်းချက်များအပေါ် ခေါင်းပုံဖြတ်ခြင်းကို ဖော်ပြရန် အသုံးပြုသည်။ AML သည် တိုက်ခိုက်သူများအား ML စနစ်များထဲတွင် မရည်ရွယ်ထားသော အပြုအမူများ လုပ်စေနိုင်သည်၊ ယင်းတွင် အောက်ပါတို့ပါဝင်နိုင်သည် -

- မော်ဒယ်၏ အမျိုးအစားခွဲခြင်း သို့မဟုတ် လုပ်ဆောင်မှုစွမ်းရည် ဆုတ်ယုတ်ခြင်းအပေါ် သက်ရောက်ခြင်း
- အသုံးပြုသူများအား ခွင့်ပြုချက်မရှိသည့် လုပ်ဆောင်မှုများကို ဆောင်ရွက်နိုင်ခြင်း
- ထိရှလွယ်သော မော်ဒယ်အချက်အလက်များကို ထုတ်ယူခြင်း

ဤသက်ရောက်မှုများကို ရရှိရန် ကြီးမားကျယ်ပြန့်သော ဘာသာစကားမော်ဒယ် (LLM) ဒိုမိန်းအတွင်း ထိုးနှက်တိုက်ခိုက်မှုများ လုပ်ဆောင်ခြင်း သို့မဟုတ် လေ့ကျင့်ရေးဒေတာ သို့မဟုတ် အသုံးပြုသူတုံ့ပြန်ချက်ကို ရည်ရွယ်ချက်ရှိရှိ ပြင်ဆင်ခြင်း ('ဒေတာအဆိပ်ခတ်ခြင်း' အဖြစ်လည်း သိရှိသည်) ကဲ့သို့ နည်းလမ်းများစွာ ရှိပါသည်။

ဤစာတမ်းကို မည်သူတို့ ဖတ်ရှုသင့်သနည်း။

ဤစာတမ်းကို အဓိကအားဖြင့် အဖွဲ့အစည်းတစ်ခုမှ ပံ့ပိုးပေးထားသော မိုဒယ်များကို အသုံးပြုနေသော သို့မဟုတ် ပြင်ပအပ်ပလီကေးရှင်း ပရိုဂရမ်မင်း ကြားခံဆက်သွယ်ရေးစနစ် (APIs) ကို အသုံးပြုနေသော AI ပံ့ပိုးပေးသူများအတွက် ရည်ရွယ်ထားပါသည်။ သို့သော် (ဒေတာသိပ္ပံပညာရှင်များ၊ ဒဗလိုပါများ၊ မန်နေဂျာများ၊ ဆုံးဖြတ်ချက်ချသူများနှင့် အန္တရာယ်လျှော့ချသူများ အပါအဝင်) အဖွဲ့အစည်းများ**အားလုံး**အနေဖြင့် ၎င်းတို့၏ စက်ကိရိယာဖြင့် သင်ကြားရေး AI စနစ်များ၏ **ဒီဇိုင်း၊ ဖြန့်ကြက်မှု**နှင့် **လည်ပတ်မှု**တို့နှင့်ပတ်သက်၍ ဆုံးဖြတ်ချက်များ ချမှတ်ရာတွင် အထောက်အကူဖြစ်စေရန်အတွက် ဤလမ်းညွှန်ချက်များကို ဖတ်ရှုရန် ကျွန်ုပ်တို့ တိုက်တွန်းလိုက်ပါသည်။

ဆိုလိုသည်မှာ ဤလမ်းညွှန်ချက်အားလုံးသည် အဖွဲ့အစည်းအားလုံးအတွက် တိုက်ရိုက်သက်ဆိုင်မည်မဟုတ်ပါ။ တိုက်ခိုက်မှု၏ ရှုပ်ထွေးမှုအဆင့်နှင့် နည်းလမ်းများမှာ AI စနစ်ကို ဖျက်လိုဖျက်စီးပြုလုပ်လိုသည့် အပေါ်တွင် မူတည်သည့်အတွက် ဤလမ်းညွှန်ချက်များကို သင့်အဖွဲ့အစည်း၏ အသုံးပြုသောဖြစ်ရပ်များနှင့် ခြိမ်းခြောက်မှုနှင့်အတူ ထည့်သွင်းစဉ်းစားသင့်သည်။

လုံခြုံသော AI စနစ် ဖော်ဆောင်ရန် မည်သူမှာ တာဝန်ရှိသနည်း။

ခေတ်သစ် AI ဖြည့်သွင်းရေးကွင်းဆက်များတွင် အများအားဖြင့် ဆောင်ရွက်သူအများအပြားရှိပါသည်။ ရိုးရှင်းသောနည်းလမ်းတစ်ခုက အခြင်းအရာနှစ်ခုကို ယူဆထားသည် -

- ဒေတာပြင်ဆင်ခြင်း၊ အယ်လ်ဂိုရစ်သမ် ဖွံ့ဖြိုးတိုးတက်မှု၊ ဒီဇိုင်း၊ ဖြန့်ကြက်မှုနှင့် ပြုပြင်ထိန်းသိမ်းမှုတို့အတွက် တာဝန်ရှိသော' ပံ့ပိုးပေးသူ'
- အချက်အလက်ဖြည့်သွင်းပြီး လိုအပ်သောအချက်အလက် ရရှိသော' အသုံးပြုသူ'

အပ်ပလီကေးရှင်းအများအပြားတွင် ဤပံ့ပိုးသူ-အသုံးပြုသူ ချဉ်းကပ်နည်းကို အသုံးပြုထားသော်လည်း ကြားခံအဖွဲ့အစည်းများမှ ပံ့ပိုးပေးထားသည့် ဆော့ဖ်ဝဲလ်၊ ဒေတာ၊ မော်ဒယ်များနှင့်/သို့မဟုတ် အဝေးသုံး ဝန်ဆောင်မှုများကို ပံ့ပိုးသူများမှ ၎င်းတို့၏ကိုယ်ပိုင်စနစ်များတွင် ထည့်သွင်းရန် ရှုရှုလှသောကြောင့် ၎င်းအသုံးပြုမှုမှာ သိသိသာသာရှားပါးလာသည်[4]။ ဤရှုပ်ထွေးသောဖြည့်သွင်းရေး ကွင်းဆက်များက နောက်ဆုံးအသုံးပြုသူများအား AI စနစ် လုံခြုံရေးဆိုင်ရာ တာဝန်ကို နားလည်ရန် ခက်ခဲစေပါသည်။

အသုံးပြုသူများ (ပြင်ပ AI အစိတ်အပိုင်းတစ်ခုကို ပေါင်းစပ်နေသော' နောက်ဆုံးအသုံးပြုသူများ 'သို့မဟုတ်' ပံ့ပိုးသူများဖြစ်ဖြစ်[5]) သည် ၎င်းတို့အသုံးပြုနေသော စနစ်များနှင့်ပတ်သက်သော အန္တရာယ်များကို အပြည့်အဝနားလည်ရန်၊ အကဲဖြတ်ရန် သို့မဟုတ် ဖြေရှင်းရန် လုံလောက်သောအသိအမြင်နှင့်/သို့မဟုတ် ကျွမ်းကျင်မှု မရှိပါ။ သို့ဖြစ်၍ ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း 'စည်းမျဉ်းများနှင့်အညီ **AI အစိတ်အပိုင်းများ ပံ့ပိုးသူများအနေဖြင့် ဖြည့်သွင်းရေးကွင်းဆက်အထိ သက်ရောက်သော အသုံးပြုသူများ၏ လုံခြုံရေးဆိုင်ရာရလဒ်များအတွက် တာဝန်ယူသင့်ပါသည်။**

ပံ့ပိုးသူများအနေဖြင့် ၎င်းတို့၏မော်ဒယ်များ၊ ပိုက်လိုင်းများနှင့်/သို့မဟုတ် စနစ်များတွင် ဖြစ်နိုင်ပါက လုံခြုံရေးထိန်းချုပ်မှုများနှင့် အန္တရာယ်လျှော့ချမှုများကို အကောင်အထည်ဖော်ဆောင်သင့်ပြီး ဆက်တင်များအသုံးပြုသည့်နေရာများတွင် အလုံခြုံဆုံးရွေးချယ်နည်းကို မူလပုံစံ (default) အဖြစ် အကောင်အထည်ဖော်ဆောင်သင့်သည်။ အန္တရာယ်များကို လျော့ချ၍မရသည့်နေရာများမှာ ပံ့ပိုးသူအနေဖြင့် အောက်ပါတို့ကို တာဝန်ယူသင့်သည် -

- အသုံးပြုသူများအား ၎င်းတို့နှင့် (သက်ဆိုင်ပါက) ၎င်းတို့၏ကိုယ်ပိုင် အသုံးပြုသူများ လက်ခံထားသော ဖြည့်သွင်းရေးကွင်းဆက်အထိ သက်ရောက်သည့် အန္တရာယ်များကို အသိပေးခြင်း
- ၎င်းတို့အား အစိတ်အပိုင်းကို လုံခြုံစွာမည်သို့သုံးစွဲရမည်ကို အကြံပေးခြင်း

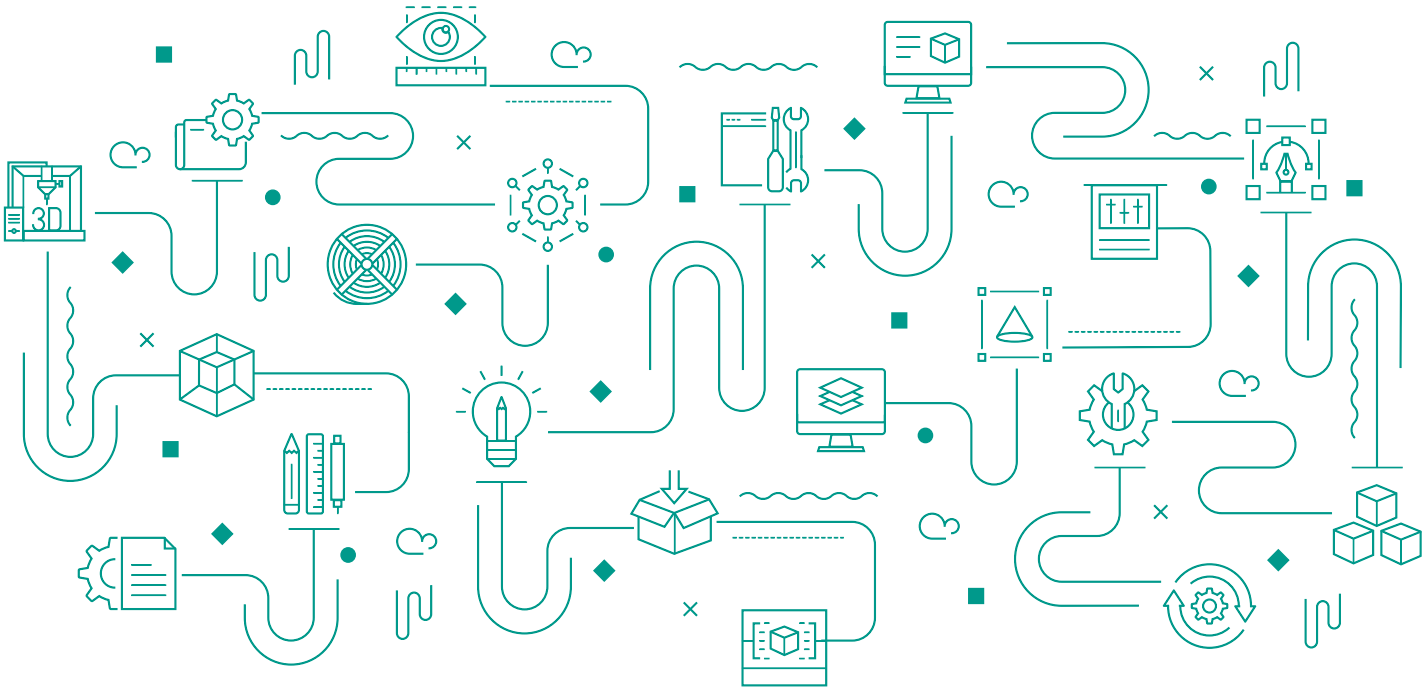
စနစ်ချိုးဖောက်ခံရမှုက ကိုင်တွယ်ထိတွေ့၍ရသော သို့မဟုတ် ကြီးမားသော ရုပ်ပိုင်းဆိုင်ရာ သို့မဟုတ် ဂုဏ်သိက္ခာပိုင်းဆိုင်ရာ ထိခိုက်မှု၊ လုပ်ငန်းလည်ပတ်မှုများ သိသိသာသာ ဆုံးရှုံးမှု၊ ထိရှလွယ်သော သို့မဟုတ် အတွင်းရေး အချက်အလက်များ ပေါက်ကြားခြင်းနှင့်/သို့မဟုတ် ဥပဒေကြောင်းအရ သက်ရောက်မှုများ ဖြစ်ပေါ်နိုင်ပါက AI ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အန္တရာယ်များကို **အရေးတကြီး** ကိုင်တွယ်ဖြေရှင်းသင့်သည်။

လုံခြုံသော AI (ဉာဏ်ရည်တု) စနစ် ဖွံ့ဖြိုးတိုးတက်ရေးဆိုင်ရာ လမ်းညွှန်ချက်များ

လမ်းညွှန်ချက်များကို AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်အတွင်း - **လုံခြုံသောဒီဇိုင်း၊ လုံခြုံသောဖွံ့ဖြိုးတိုးတက်မှု၊ လုံခြုံသောဖြန့်ကြက်မှုနှင့် လုံခြုံသော လည်ပတ်မှုနှင့် ပြုပြုပြင်ထိန်းသိမ်းမှု**ဟူ၍ အဓိကကဏ္ဍလေးပိုင်း ပိုင်းခြားထားသည်။ ကဏ္ဍတစ်ခုစီအတွက် အဖွဲ့အစည်းဆိုင်ရာ AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှု လုပ်ငန်းစဉ်အပေါ် ဖြစ်စေနိုင်သောအန္တရာယ်ကို လျှော့ချပေးမည့် ထည့်သွင်းစဉ်းစားမှုများနှင့် အန္တရာယ်လျှော့ပေါ့ပေးမှုများကို ကျွန်ုပ်တို့ အကြံပြုထားပါသည်။

ဤစာတမ်းတွင် သတ်မှတ်ထားသော လမ်းညွှန်ချက်များကို အောက်တွင်ဖော်ပြထားသည့် ဆော့ဖ်ဝဲလ်ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ် အလေ့အကျင့်များနှင့် အနီးစပ်ဆုံး ချိန်ညှိထားပါသည်။

- NCSC ၏လုံခြုံသောဖွံ့ဖြိုးတိုးတက်မှုနှင့် ဖြန့်ကြက်မှုလမ်းညွှန်ချက်
- အမျိုးသား စံချိန်စံညွှန်းများနှင့် နည်းပညာတက္ကသိုလ် (NIST) လုံခြုံသောဆော့ဖ်ဝဲလ် ဖွံ့ဖြိုးတိုးတက်မှု မူဘောင် (SSDF)[6]



1. လုံခြုံသောဒီဇိုင်း

ဤကဏ္ဍတွင် AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်၏ **ဒီဇိုင်း**အဆင့်နှင့်ဆိုင်သော လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။ ယင်းတွင် စနစ်နှင့် မော်ဒယ်ဒီဇိုင်းကို ထည့်သွင်းစဉ်းစားရန် သီခြားအကြောင်းအရာများနှင့် အပေးအယူလုပ်ခြင်းများအပြင် အန္တရာယ်များကို နားလည်ခြင်းနှင့် ခြိမ်းခြောက်မှုဖော်ထုတ်ခြင်းတို့ ပါဝင်သည်။

ဝန်ထမ်းများကို ခြိမ်းခြောက်မှုနှင့် အန္တရာယ်များအား နားလည်ရန် နိုးဆော်ပါ

စနစ်ပိုင်ရှင်များနှင့် အကြီးတန်းခေါင်းဆောင်များသည် AI လုံခြုံမှုအပေါ် ခြိမ်းခြောက်မှုများနှင့် ၎င်းတို့လျော့ပါးရေး နည်းလမ်းများကို နားလည်ပါသည်။ သင်၏ ဒေတာသိပ္ပံပညာရှင်များနှင့် ဒဗလိုပါများ (ဆော့ဖ်ဝဲရေးသားသူများ) သည် သက်ဆိုင်ရာ လုံခြုံရေးခြိမ်းခြောက်မှုများနှင့် ချို့ယွင်းမှုများကို သတိပြမိကြပြီး သိရှိပြီးသော ဆုံးဖြတ်ချက်များ ချနိုင်ရန် အန္တရာယ်လျှော့ချသူများအား ကူညီပေးပါသည်။ သင်သည် အသုံးပြုသူများအား AI စနစ်များ ရင်ဆိုင်နေရသော ထူးခြားသောလုံခြုံရေး အန္တရာယ်များနှင့် ပတ်သက်၍ (ဥပမာ၊ စံသတ်မှတ်ထားသော InfoSec လေ့ကျင့်မှု တစ်စိတ်တစ်ပိုင်းအဖြစ်) လမ်းညွှန်ပေးသည့်အပြင် ဒဗလိုပါများအား လုံခြုံသောကုဒ်ရေးနည်းများနှင့် လုံခြုံပြီး တာဝန်သိသော AI အလေ့အကျင့်များ ပြုလုပ်ရန် လေ့ကျင့်ပေးပါသည်။

သင့်စနစ်အပေါ်ကျရောက်စေနိုင်သော ခြိမ်းခြောက်မှုများကို ပုံဖော်ပါ

သင်၏ အန္တရာယ်စီမံခန့်ခွဲမှုလုပ်ငန်းစဉ် တစ်စိတ်တစ်ပိုင်းအနေဖြင့် သင့်စနစ်အပေါ်ကျရောက်နိုင်သော ခြိမ်းခြောက်မှုများကို အကဲဖြတ်ရန် အလုံးစုံသောလုပ်ငန်းစဉ်ကို သင် အသုံးပြုသင့်သည်၊ ၎င်းတွင် AI အစိတ်အပိုင်းတစ်ခု ချိုးဖောက်ခံရပါက သို့မဟုတ် မျှော်လင့်မထားသည့်ပုံစံဖြင့် ပြုမူလာပါက စနစ်၊ အသုံးပြုသူများ၊ အဖွဲ့အစည်းများနှင့် ပိုမိုကျယ်ပြန့်သောလူဘောင်အဖွဲ့အစည်းအပေါ် ကျရောက်နိုင်သော သက်ရောက်မှုများကို နားလည်ထားခြင်းပါဝင်သည် [7]။ ဤလုပ်ငန်းစဉ်တွင် AI နှင့်သက်ဆိုင်သော ခြိမ်းခြောက်မှုများ၏ အကျိုးသက်ရောက်မှုကို အကဲဖြတ်ခြင်း [8] နှင့် သင်၏ဆုံးဖြတ်ချက်ချခြင်းကို မှတ်တမ်းတင်ခြင်းတို့ ပါဝင်သည်။

သင့်စနစ်တွင် အသုံးပြုသည့် အာရုံခံနိုင်စွမ်းနှင့် ဒေတာအမျိုးအစားများသည် တိုက်ခိုက်သူ ပစ်မှတ်ထားသည့် တန်ဖိုးဖြစ်နိုင်ကြောင်း သင်နားလည်ထားသည်။ သင့်အကဲဖြတ်ချက်တွင် AI စနစ်များကို တန်ဖိုးမြင့်ပစ်မှတ်များအဖြစ် ပို၍ရှုမြင်လာနိုင်သည့်အပြင် AI ကိုယ်၌က အလိုအလျောက် တိုက်ခိုက်မှုနည်းလမ်းသစ်များ ဖြစ်ပေါ်စေနိုင်သောကြောင့် အချို့သောခြိမ်းခြောက်မှုများ ကြီးထွားလာနိုင်ကြောင်း ထည့်သွင်းသုံးသပ်သင့်သည်။

သင့်စနစ်ကို လုံခြုံရေးအပြင် လည်ပတ်နိုင်မှုနှင့် စွမ်းဆောင်ရည်အတွက် ဒီဇိုင်းထုတ်ပါ။

လက်တကမ်းတွင်ရှိသော အလုပ်တာဝန်တစ်ခုကို AI အသုံးပြု၍ အသင့်လျော်ဆုံးဖြေရှင်းနိုင်ကြောင်း သင်ယုံကြည်ပါသည်။ ၎င်းကို ဆုံးဖြတ်ပြီးနောက် သင်၏ AI နှင့် သက်ဆိုင်သော ဒီဇိုင်းရွေးချယ်မှုများ၏ သင့်လျော်မှုကို အကဲဖြတ်ပါသည်။ သင်၏ ခြိမ်းခြောက်မှုပုံစံနှင့် လည်ပတ်မှု၊ အသုံးပြုသူ အတွေ့အကြုံ၊ ဖြန့်ကြက်မှုပတ်ဝန်းကျင်၊ စွမ်းဆောင်ရည်၊ အာမခံချက်၊ ကြီးကြပ်မှု၊ ကျင့်ဝတ်နှင့် ဥပဒေဆိုင်ရာ လိုအပ်ချက်များအပါအဝင် အခြားထည့်သွင်းစဉ်းစားမှုများ နှင့်အတူ ဆက်စပ်လုံခြုံရေးဆိုင်ရာ လျော့ချမှုများကို ထည့်သွင်းစဉ်းစားပါသည်။ ဥပမာ -

- အတွင်း ဖွံ့ဖြိုးတိုးတက်မှုလုပ်မည်လား သို့မဟုတ် ပြင်ပအစိတ်အပိုင်းများကို အသုံးပြုမည်လားကို ရွေးချယ်သည့်အခါ ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက်လုံခြုံရေးကို ထည့်သွင်းစဉ်းစားသည်၊ ဥပမာ -
  - မော်ဒယ်အသစ်ကို လေ့ကျင့်ခြင်း၊ ရှိပြီးသား မော်ဒယ်ကို (ချိန်ညှိခြင်းဖြင့် သို့မဟုတ် ချိန်ညှိခြင်းမရှိဘဲ) အသုံးပြုခြင်း သို့မဟုတ် ပြင်ပ API မှ တစ်ဆင့် မော်ဒယ်တစ်ခုကို ဝင်ရောက်အသုံးပြုခြင်းဆိုင်ရာ သင်၏ရွေးချယ်မှုသည် သင့်လိုအပ်ချက်များနှင့် သင့်လျော်ပါသည်။
  - ပြင်ပမော်ဒယ်ဝန်ဆောင်မှုပေးသူတစ်ဦးနှင့် အလုပ်လုပ်ရန် သင့်ရွေးချယ်မှုတွင် အဆိုပါဝန်ဆောင်မှုပေးသူ၏ ကိုယ်ပိုင်လုံခြုံရေးရပ်တည်ချက်ကို ထိုက်သင့်သောအကဲဖြတ်ခြင်းတစ်ခု ပါဝင်သည်။
  - ပြင်ပစာကြည့်တိုက်ကို အသုံးပြုပါက သင်သည် ထိုက်သင့်သောအကဲဖြတ်မှုတစ်ခု ပြီးဆုံးအောင်ဆောင်ရွက်ရမည် (ဥပမာ၊ (ဆော့ဖ်ဝဲထုတ်လုပ်ရာတွင် အသုံးပြုသည့် ကွန်ပြူတာ) စာကြည့်တိုက်တွင် အငြင်းဖြစ်စေသောကုဒ်စီမံဆောင်ရွက်မှု ချက်ချင်းမဖြစ်ပေါ်စေဘဲ မယုံကြည်ရသော မော်ဒယ်များတင်သည့်စနစ်ကို ကာကွယ်တားဆီးသည့် ထိန်းချုပ်မှုများရှိအောင် ဆောင်ရွက်ရန်ဖြစ်သည် [9])
  - ကြားခံအဖွဲ့မော်ဒယ်များ သို့မဟုတ် နံပါတ်စဉ်တပ်ထားသော အလေးချိန်များကို အဝေးမှ ကုဒ်စီမံဆောင်ရွက်မှု လုပ်နိုင်သဖြင့် မယုံကြည်ရသော ကြားခံအဖွဲ့ကုဒ်အဖြစ် မှတ်ယူသင့်သဖြင့် ၎င်းတို့ကို တင်သွင်းသည့်အခါ စကင်ဖတ်ခြင်းနှင့် သီခြားခွဲထားခြင်း /သီးသန့်ထားခြင်းများ သင်လုပ်ဆောင်သည်

- ပြင်ပ API တစ်ခုကို အသုံးပြုပါက အသုံးပြုသူများအား အကောင့်ဝင်ရန်နှင့် ဖြစ်နိုင်ခြေရှိသော ထိလွယ်ရှလွယ်သည့်အချက်အလက်များကို မပေးပို့မီ အတည်ပြုရန် လိုအပ်ခြင်းကဲ့သို့ သင့်အဖွဲ့အစည်း၏ ထိန်းချုပ်မှုပြင်ပ၌ရှိသော ဝန်ဆောင်မှုများသို့ ပေးပို့နိုင်သည့် ဒေတာများအတွက် သင့်လျော်သော ထိန်းချုပ်မှုများ အသုံးပြုသင့်သည်။
- ဒေတာနှင့် ထည့်သွင်းထားသောအချက်အလက်များကို သင့်လျော်သော စစ်ဆေးမှုများနှင့် သန့်စင်ခြင်းတို့ ပြုလုပ်သင့်သည်။ ၎င်းတွင် အသုံးပြုသူ တုံ့ပြန်ချက် သို့မဟုတ် စဉ်ဆက်မပြတ် လေ့လာသင်ယူမှုဒေတာကို သင့်မော်ဒယ်ထဲသို့ ထည့်သွင်းသည့်အခါ လေ့ကျင့်ရေးဒေတာမှ စနစ်အပြုအမူကို ဖော်ထုတ်ပေးကြောင်း အသိအမှတ်ပြုခြင်း ပါဝင်သည်။

- သင်သည် AI ဆော့ဖ်ဝဲလ်စနစ် ဖွံ့ဖြိုးတိုးတက်ရေးကို လက်ရှိလုံခြုံသော ဖွံ့ဖြိုးတိုးတက်မှုနှင့် လည်ပတ်မှုဆိုင်ရာ အကောင်းဆုံး အလေ့အကျင့်များတွင် ပေါင်းစပ်ထားသည်။ AI စနစ်၏ အစိတ်အပိုင်းအားလုံးကို သိရှိထားသောအားနည်းချက်အမျိုးအစားများကို လျှော့ချ သို့မဟုတ် ရှင်းလင်းပေးသည့် ကုဒ်လုပ်နည်းများနှင့် ဘာသာစကားများကို အသုံးပြု၍ သင့်လျော်သောပတ်ဝန်းကျင်များတွင် ရေးသားထားပါသည်

- AI အစိတ်အပိုင်းများသည် ဥပမာ ဖိုင်များကို ပြင်ဆင်ခြင်း သို့မဟုတ် ပြင်ပစနစ်များသို့ အချက်အလက်များကို ညွှန်ပြခြင်းကဲ့သို့ လုပ်ဆောင်ချက်များကို အစပျိုးရန် လိုအပ်ပါက သင့်အနေဖြင့် ဖြစ်နိုင်ချေရှိသော လုပ်ဆောင်ချက်များအတွက် သင့်လျော်သော ကန့်သတ်ချက်များကို အသုံးပြုသင့်သည် (၎င်းတွင် လိုအပ်ပါက ပြင်ပ AI နှင့် AI နှင့်မဆိုင်သော လုံခြုံရေးပျက်ကွက်မှုများ ပါဝင်သည်)

- အသုံးပြုသူ အပြန်အလှန်ဆက်သွယ်မှုဆိုင်ရာ ဆုံးဖြတ်ချက်များကို AI နှင့်သက်ဆိုင်သော အန္တရာယ်များမှ အသိပေးပါသည်၊ ဥပမာ-
  - သင့်စနစ်သည် ဖြစ်နိုင်ချေရှိသော တိုက်ခိုက်သူအား မလိုအပ်သော အသေးစိတ်အချက်အလက်များမဖော်ပြဘဲ အသုံးပြုသူများကို အသုံးပြုနိုင်သော အချက်အလက်များ ပေးပါသည်
  - လိုအပ်ပါက သင့်စနစ်သည် မော်ဒယ်အချက်အလက်များကို ထိရောက်သောကာကွယ်မှုများ ပေးပါသည်
  - API တစ်ခုကို ပြင်ပဖောက်သည်များ သို့မဟုတ် ပူးပေါင်းဆောင်ရွက်သူများအား ပေးပါက သင်သည် API မှတစ်ဆင့် AI စနစ်အပေါ်တိုက်ခိုက်သည့် တိုက်ခိုက်မှုများကို လျော့ချပေးသည့် သင့်လျော်သော ထိန်းချုပ်မှုများ အသုံးပြုသင့်သည်
  - သင်သည် စနစ်ထဲတွင် အလုံခြုံဆုံးဆက်တင်များကို နဂိုမူရင်းအတိုင်း ပေါင်းစပ်ထားသည်
  - စနစ်တစ်ခု၏ လည်ပတ်မှုကို ကန့်သတ်ရရှိရန် သင်သည် အနည်းဆုံး အထူးစဉ်းမျဉ်းများ အသုံးပြုသင့်သည်
  - သင်သည် သုံးစွဲသူများအား အန္တရာယ်ရှိသော လုပ်ဆောင်မှုစွမ်းရည်များကို ရှင်းပြသင့်ပြီး ၎င်းတို့ကို အသုံးပြုရန် အသုံးပြုသူများ ရွေးချယ်ရန် လိုအပ်ပါသည်၊ တားမြစ်ထားသည့် အသုံးပြုမှုကိစ္စများကို ဆက်သွယ်ပြောဆိုသင့်ပြီး ဖြစ်နိုင်ပါက အသုံးပြုသူများအား အခြားဖြေရှင်းနည်းများကို အသိပေးပါ

သင်၏ AI မော်ဒယ်ကို ရွေးချယ်သည့်အခါ လုံခြုံရေးဆိုင်ရာ အကျိုးကျေးဇူးများနှင့် အပေးအယူလုပ်ခြင်းများကို ထည့်သွင်းစဉ်းစားပါ

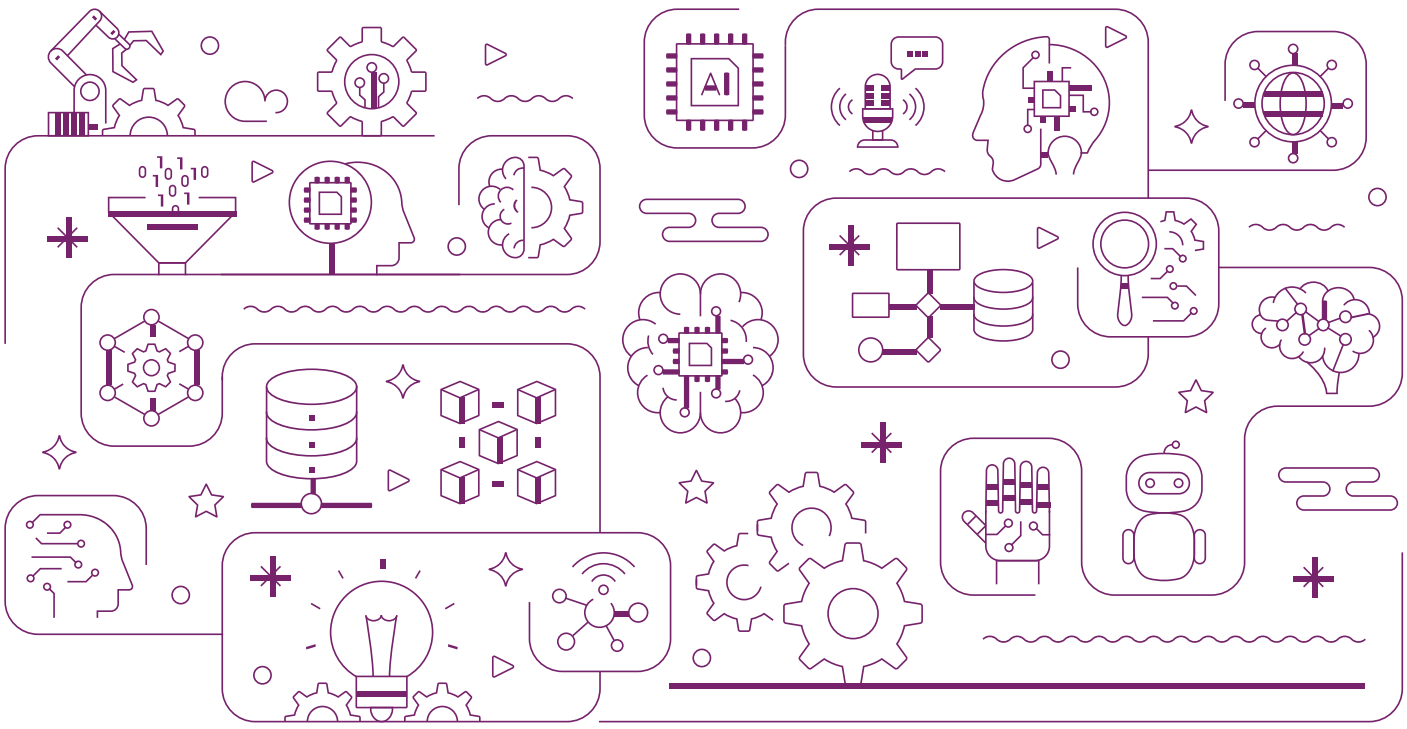
သင်၏ AI မော်ဒယ်ရွေးချယ်မှုတွင် လိုအပ်ချက်များစွာကို ချိန်ခွင်လျှာညီပေးခြင်းတို့ ပါဝင်မည်ဖြစ်သည်။ ၎င်းတွင် မော်ဒယ်ဗိသုကာဒီဇိုင်း ရွေးချယ်မှု၊ ဖွဲ့စည်းပုံစနစ်၊ လေ့ကျင့်ရေးဒေတာ၊ လေ့ကျင့်ရေး အယ်လ်ဂိုရီသမ်နှင့် ဟိုက်ပါပါရာမီတာများ ပါဝင်သည်။ သင်၏ဆုံးဖြတ်ချက်များကို သင်၏ခြိမ်းခြောက်မှုပုံစံဖြင့် အသိပေးပြီး AI လုံခြုံရေးသုတေသန တိုးတက်မှုနှင့် ခြိမ်းခြောက်မှုအပေါ် နားလည်သဘောပေါက်မှုများ ဖွံ့ဖြိုးလာသောကြောင့် ပုံမှန်ပြန်လည်အကဲဖြတ်ပါသည်။

AI မော်ဒယ်ကို ရွေးချယ်သည့်အခါ သင်၏ထည့်သွင်းစဉ်းစားမှုများတွင် အောက်ပါတို့အပြင် တခြားအရာများ ပါဝင်နိုင်သည် -

- သင်အသုံးပြုနေသော မော်ဒယ်၏ ရှုပ်ထွေးမှု၊ ဆိုလိုသည်မှာ ရွေးချယ်ထားသော ဗိသုကာဒီဇိုင်းနှင့် ကန့်သတ်ချက်ဘောင် အရေအတွက်ကို ဆိုလိုသည်၊ သင့်မော်ဒယ်၏ ရွေးချယ်ထားသော ဗိသုကာဒီဇိုင်းနှင့် ကန့်သတ်ချက်ဘောင် အရေအတွက်သည် အခြားအချက်များကြားတွင် လေ့ကျင့်ရေးဒေတာ မည်မျှလိုအပ်သည်နှင့် အသုံးပြုသည့်အခါ ထည့်သွင်းထားသောဒေတာပြောင်းလဲမှုအတွက် မည်မျှခံနိုင်ရည်ရှိမှုအပေါ် အကျိုးသက်ရောက်စေမည်ဖြစ်သည်

- သင်အသုံးပြုလိုသည့်ကိစ္စအတွက် မော်ဒယ်၏ သင့်လျော်မှုနှင့်/သို့မဟုတ် ၎င်းကို သင်၏ သီးခြားလိုအပ်ချက်နှင့် လိုက်လျောညီထွေဖြစ်အောင် ပြုပြင်မွမ်းမံနိုင်ခြေ (ဥပမာ -ချိန်ညှိခြင်းဖြင့်)
- သင့်မော်ဒယ်၏ အချက်အလက်များကို ချိန်ညှိခြင်း၊ အဓိပ္ပာယ်ဖွင့်ဆိုခြင်းနှင့် ရှင်းပြနိုင်မှု (ဥပမာ အပြစ်ရှာဖွေခြင်း၊ စာရင်းစစ် သို့မဟုတ် စည်းကမ်းလိုက်နာမှုအတွက်)၊ အဓိပ္ပာယ်ဖွင့်ဆိုရန် ပို၍ခက်ခဲသော ကြီးမားပြီး ရှုပ်ထွေးသည့် မော်ဒယ်များထက် ပိုမိုရိုးရှင်းသော၊ ပိုမိုပွင့်လင်းသော မော်ဒယ်များကို အသုံးပြုရာတွင် အကျိုးကျေးဇူးများ ရှိနိုင်ပါသည်။
- အရွယ်အစား၊ ခိုင်မာမှု၊ အရည်အသွေး၊ အာရုံခံနိုင်စွမ်း၊ အသက်၊ ဆက်စပ်မှုနှင့် ကွဲပြားမှုအပါအဝင် လေ့ကျင့်ရေးဒေတာအတွဲ(များ)၏ ဝိသေသလက္ခဏာများ
- မော်ဒယ်ခိုင်မာအောင် ပြုလုပ်ခြင်း (ဥပမာ ပဋိပက္ခဖြစ်စေသော လေ့ကျင့်ရေး)၊ စနစ်ပုံမှန်ပြောင်းလဲခြင်းနှင့်/သို့မဟုတ် အတွင်းရေးကို ကာကွယ်ပေးသည့် နည်းပညာများ အသုံးပြုခြင်း၏ တန်ဖိုး
- မော်ဒယ် သို့မဟုတ် ဖောင်ဒေးရှင်းမော်ဒယ်၊ လေ့ကျင့်ရေးဒေတာနှင့် ဆက်စပ်ကိရိယာများအပါအဝင် အစိတ်အပိုင်းများ၏ ရင်းမြစ်နှင့် ပစ္စည်းဖြည့်သွင်းရေး ကွင်းဆက်များ

ဤအချက်များအနက် မည်မျှက လုံခြုံရေးရလဒ်များအပေါ် သက်ရောက်မှုဖြစ်စေသည်နှင့်ပတ်သက်၍ အချက်အလက် ပိုမိုသိရှိလိုပါက NCSC ၏ 'စက်ကိရိယာဖြင့် သင်ကြားရေးဆိုင်ရာ အခြေခံစဉ်းမျဉ်းများ'၊ အထူးသဖြင့် လုံခြုံရေးအတွက် ဒီဇိုင်း (မော်ဒယ်ဗိသုကာဒီဇိုင်း) ကို ကိုးကားပါ။



2. လုံခြုံသောဖွံ့ဖြိုးတိုးတက်မှု

ဤကဏ္ဍတွင် ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက် လုံခြုံရေး၊ အထောက်အထားစာရွက်စာတမ်းအပြင် ပိုင်ဆိုင်မှုနှင့် နည်းပညာဆိုင်ရာ အကြွေး စီမံခန့်ခွဲမှု အပါအဝင် AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်၏ **ဖွံ့ဖြိုးတိုးတက်မှု**အဆင့်နှင့်ဆိုင်သော လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။

သင်၏ပစ္စည်းဖြည့်သွင်းရေး ကွင်းဆက်ကို လုံခြုံအောင်လုပ်ပါ

သင်သည် စနစ်ဖြစ်စဉ်တစ်လျှောက်လုံးရှိ သင်၏ AI ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက်များ၏ လုံခြုံရေးကို အကဲဖြတ်ပြီး စောင့်ကြည့်စစ်ဆေးကာ ပစ္စည်းပေးသွင်းသူများအား သင့်အဖွဲ့အစည်း၏ အခြားဆော့ဖ်ဝဲလ်များနှင့် သက်ဆိုင်သည့် အလားတူစံနှုန်းများကို လိုက်နာရန် လိုအပ်ပါသည်။ ပစ္စည်းပေးသွင်းသူများသည် သင့်အဖွဲ့အစည်း၏ စံနှုန်းများကို မလိုက်နာပါက သင်သည် သင်၏လက်ရှိ အန္တရာယ်စီမံခန့်ခွဲမှုဆိုင်ရာမူဝါဒများနှင့်အညီ လုပ်ဆောင်သည်။

အဖွဲ့အစည်းအတွင်း၌ မထုတ်လုပ်ပါက သင့်အနေဖြင့် သင့်စနစ်များတွင် ခိုင်မာသောလုံခြုံရေးကို သေချာစေရန် ကောင်းစွာလုံခြုံပြီး မှတ်တမ်းတင်ထားသော ဟာ့ဒ်ဝဲနှင့် ဆော့ဖ်ဝဲလ် အစိတ်အပိုင်းများ (ဥပမာ၊ မော်ဒယ်များ၊ ဒေတာ၊ ဆော့ဖ်ဝဲစာကြည့်တိုက်များ၊ မော်ဂျူးများ၊ ပေါင်းကူးချိတ်ဆက်ပေးသည့် ဆော့ဖ်ဝဲလ် (middleware)၊ မူဘောင်များနှင့် ပြင်ပ API များ) ကို စီးပွားဖြစ်၊ အများသုံးရင်းမြစ်နှင့် အခြားကြားခံအဖွဲ့ဒပလိုပါများမှ ရယူပြီး ထိန်းသိမ်းနိုင်သည်။

လုံခြုံရေးစံနှုန်းများနှင့် မကိုက်ညီပါက ရည်မှန်းချက်အောင်မြင်ရေးစနစ်များအတွက် အစားထိုးဖြေရှင်းနည်းများသို့ ပြောင်းရန် အဆင်သင့်ဖြစ်ပါသည်။ သင်သည် ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက်နှင့် ဆော့ဖ်ဝဲဖွံ့ဖြိုးတိုးတက်မှု ဖြစ်စဉ်များ၏ အထောက်အထားများကို ခြေရာခံရန်အတွက် NCSC ၏ ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက် လမ်းညွှန်ကဲ့သို့ ရင်းမြစ်များနှင့် ဆော့ဖ်ဝဲလ်အချက်အလက်များအတွက် ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက်အဆင့်များ (SLSA)[10] ကဲ့သို့သော မူဘောင်များကို အသုံးပြုပါသည်။

သင့်ပိုင်ဆိုင်မှုများကို ဖော်ထုတ်ပါ၊ ခြေရာခံပါ၊ ကာကွယ်ပါ။

သင်သည် မော်ဒယ်များ၊ ဒေတာ (အသုံးပြုသူတို့ပြန်ချက်အပါအဝင်)၊ အချက်ပြသင်္ကေတများ၊ ဆော့ဖ်ဝဲလ်၊ စာရွက်စာတမ်းများ၊ မှတ်တမ်းများနှင့် အကဲဖြတ်ချက်များ (မလုံခြုံနိုင်သည့် အလားအလာရှိသော စွမ်းရည်များနှင့် ချို့ယွင်းမှုများအကြောင်း အချက်အလက်များအပါအဝင်) အပါအဝင် သင့်အဖွဲ့အစည်း၏ AI နှင့်သက်ဆိုင်သော ပိုင်ဆိုင်မှုများ၏ တန်ဖိုးကို သင်နားလည်သဘောပေါက်ပါသည်။ ၎င်းတို့က မည်သည့်နေရာတွင် ကြီးမားသော ရင်းနှီးမြှုပ်နှံမှုကို ကိုယ်စားပြုသည်နှင့် မည်သည့်နေရာတွင် ၎င်းတို့ကို တိုက်ခိုက်သူမှ ဝင်ရောက်အသုံးပြုနိုင်သည်ကို နားလည်ထားရန် အရေးကြီးသည်။ သင်သည် မှတ်တမ်းများကို ထိရှလွယ်သော ဒေတာအဖြစ် သတ်မှတ်ပြီး ၎င်းတို့၏ လျှို့ဝှက်မှု၊ ခိုင်မာမှုနှင့် ရရှိနိုင်မှုကို ကာကွယ်ရန် ထိန်းချုပ်မှုများကို အကောင်အထည်ဖော်ဆောင်ပါ။

သင့်ပိုင်ဆိုင်မှုများ မည်သည့်နေရာတွင် ရှိသည်ကို သင်သိပြီး အကဲဖြတ်ကာ ဆက်စပ်အန္တရာယ်များကို လက်ခံထားသည်။ သင့်တွင် ခြေရာခံရန်၊ စစ်မှန်ကြောင်းသက်သေပြရန်၊ ဗားရှင်းထိန်းချုပ်ရန်နှင့် သင့်ပိုင်ဆိုင်မှုများကို လုံခြုံအောင်ပြုလုပ်ရန် လုပ်ငန်းစဉ်များနှင့် ကိရိယာများရှိပြီး ချို့ဖောက်ခံရသည့် ဖြစ်စဉ်တွင် ၎င်းတို့ကို စိတ်ချရသည့် အခြေအနေတစ်ခုတွင် ပြန်လည်သိမ်းထားနိုင်သည်။

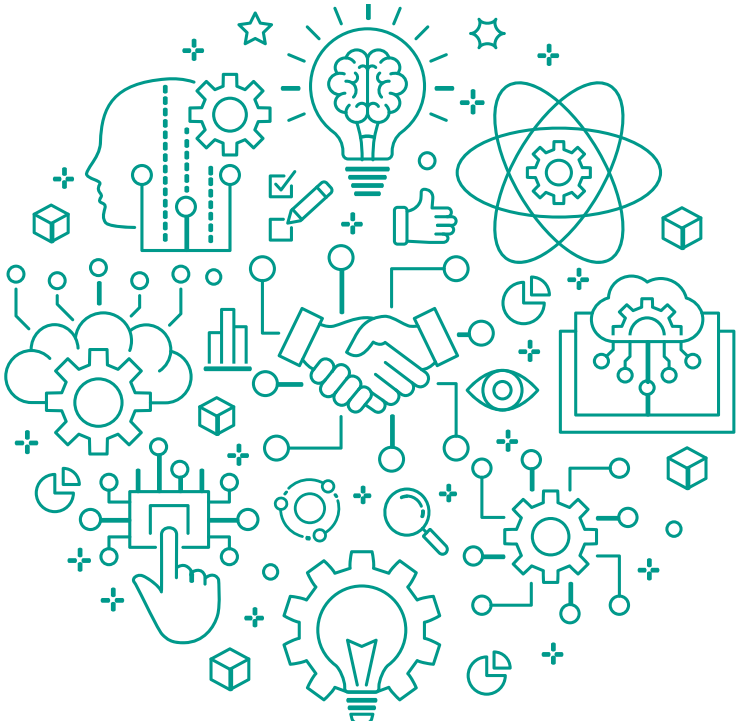
သင့်တွင် AI စနစ်များ ဝင်ရောက်နိုင်သည့် ဒေတာများကို စီမံရန်နှင့် AI မှ ၎င်း၏ အာရုံခံစားမှု (နှင့် အကြောင်းအရာထုတ်ပေးရန် ထည့်သွင်းရသည့် အချက်အလက်များ၏ အာရုံခံစားမှု) အရ ထုတ်လုပ်သည့် အကြောင်းအရာများကို စီမံရန် လုပ်ငန်းစဉ်များနှင့် ထိန်းချုပ်မှုများ လက်ဝယ်ရှိပါသည်။

သင်၏ဒေတာ၊ မော်ဒယ်များနှင့် အချက်ပြသင်္ကေတများကို မှတ်တမ်းတင်ပါ

သင်သည် မော်ဒယ်များ၊ ဒေတာအတွဲများနှင့် ညွှန်ကြားချက်-သို့မဟုတ် စနစ်-အချက်ပြသင်္ကေတများ၏ ဖန်တီးမှု၊ လည်ပတ်မှုနှင့် ဖြစ်စဉ်စီမံခန့်ခွဲမှုတို့ကို မှတ်တမ်းတင်ထားသည်။ သင့်စာရွက်စာတမ်းတွင် (ပြင်ဆင်ချိန်ညှိထားသော ဒေတာနှင့် လူသား သို့မဟုတ် အခြားလုပ်ငန်းလည်ပတ်မှုဆိုင်ရာ တုံ့ပြန်ချက်အပါအဝင်) လေ့ကျင့်ရေးဒေတာရင်းမြစ်များ၊ ရည်ရွယ်ထားသော အတိုင်းအတာနှင့် ကန့်သတ်ချက်များ၊ ကာကွယ်ပေးမှုများ၊ လျှို့ဝှက်သင်္ကေတများ သို့မဟုတ် လက်မှတ်များ၊ ထိန်းသိမ်းချိန်၊ အကြံပြုထားသည့် ပြန်လည်သုံးသပ်မှုအကြိမ်ရေနှင့် ပျက်ကွက်နိုင်ခြေရှိသော မုဒ်များကဲ့သို့သော လုံခြုံရေးဆိုင်ရာ အချက်အလက်များ ပါဝင်သည်။ ၎င်းကိုလုပ်ဆောင်ရန် ကူညီပေးသည့် အသုံးဝင်သောဖွဲ့စည်းပုံများတွင် မော်ဒယ်ကတ်များ၊ ဒေတာကတ်များနှင့် ဆော့ဖ်ဝဲကုန်ကြမ်းစာရင်းများ (SBOMs) ပါဝင်သည်။ ပြည့်စုံသောစာရွက်စာတမ်းများ ထုတ်လုပ်ခြင်းမှ ပွင့်လင်းမြင်သာမှုနှင့် တာဝန်ခံမှုကို ထောက်ခံပေးသည်[11]။

သင်၏နည်းပညာအကြွေးကို စီမံခန့်ခွဲပါ

ဆော့ဖ်ဝဲလ်စနစ်တစ်ခုခုနှင့် AI စနစ်ဖြစ်စဉ်တစ်လျှောက်ရှိ သင်၏' နည်းပညာအကြွေး 'ကို ဖော်ထုတ်ပြီး ခြေရာခံကာ စီမံခန့်ခွဲသင့်သည် (ရေရှည်အကျိုးကျေးဇူးများအတွက် အကောင်းဆုံးကျင့်သုံးမှုများကို မျက်ကွယ်ပြုပြီး အင်ဂျင်နီယာဆိုင်ရာ ဆုံးဖြတ်ချက်များကို ရေတိုရလဒ်များ ရရှိစေရန် ဦးစားပေးသည့်အခါ နည်းပညာအကြွေး ဖြစ်ပေါ်သည်)။ ငွေကြေးအကြွေးများကဲ့သို့ နည်းပညာဆိုင်ရာအကြွေးသည် ပင်ကိုယ်အားဖြင့် မဆိုးသော်လည်း အစောဆုံး ဖွံ့ဖြိုးတိုးတက်မှုအဆင့်များမှစ၍ စီမံခန့်ခွဲသင့်သည်[12]။ ထိုသို့လုပ်ဆောင်ခြင်းသည် စံဆော့ဖ်ဝဲထက် AI ကဏ္ဍတွင် ပိုမိုခက်ခဲနိုင်ကြောင်းနှင့် လျင်မြန်သောဖွံ့ဖြိုးတိုးတက်မှုနှင့် ကောင်းမွန်စွာတည်ဆောက်ထားသော ပရိုတိုကောများနှင့် အင်တာဖေ့စ်များမရှိခြင်းကြောင့် သင်၏နည်းပညာအကြွေး ပမာဏများ မြင့်မားဖွယ်ရှိကြောင်း သင် အသိအမှတ်ပြုသည်။ (AI စနစ်များကို ဖျက်သိမ်းရန် လုပ်ငန်းစဉ်များအပါအဝင်) သင်၏ဖြစ်စဉ်အစီအစဉ်များမှ အနာဂတ်၌ အလားတူစနစ်များအပေါ် ကျရောက်နိုင်သော အန္တရာယ်များကို အကဲဖြတ်ခြင်း၊ အသိအမှတ်ပြုခြင်းနှင့် လျော့ပါးသက်သာစေရန် သေချာဆောင်ရွက်ပါ။



3. လုံခြုံသောဖြန့်ကြက်မှု

ဤကဏ္ဍတွင် အခြေခံအဆောက်အအုံနှင့် မော်ဒယ်များကို ချိုးဖောက်ခြင်း၊ ခြိမ်းခြောက်ခြင်း သို့မဟုတ် ဆုံးရှုံးမှုမှ ကာကွယ်ခြင်း၊ အဖြစ်အပျက်စီမံခန့်ခွဲရေး လုပ်ငန်းစဉ်များ ဆောင်ရွက်ခြင်းနှင့် တာဝန်ယူထုတ်ပေးခြင်းများအပါအဝင် AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်၏ **ဖြန့်ကြက်မှု**အဆင့်နှင့်ဆိုင်သော လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။

သင်၏အခြေခံအဆောက်အအုံကို လုံခြုံအောင်ထားပါ

သင်သည် သင့်စနစ်ဖြစ်စဉ်၏ အစိတ်အပိုင်းတိုင်းတွင် အသုံးပြုသည့် အခြေခံအဆောက်အအုံအတွက် ကောင်းမွန်သော အခြေခံအဆောက်အအုံ လုံခြုံရေးဆိုင်ရာ စည်းမျဉ်းများကို ကျင့်သုံးပါသည်။ သင်သည် သင်၏ API များ၊ မော်ဒယ်များနှင့် ဒေတာများ၊ ၎င်းတို့၏ လေ့ကျင့်ရေးနှင့် စီမံဆောင်ရွက်ရေးလိုင်းများ၊ သုတေသနနှင့် ဖွံ့ဖြိုးတိုးတက်မှုအပြင် ဖြန့်ကျက်ခြင်းတွင် သင့်လျော်သော အသုံးပြုခွင့်ဆိုင်ရာထိန်းချုပ်မှုများကို သင် အသုံးပြုပါသည်။ ၎င်းတွင် ထိရှလွယ်သော ကုဒ် သို့မဟုတ် ဒေတာပါဝင်သည့် ပတ်ဝန်းကျင်များကို သင့်လျော်စွာခွဲခြားထားပါသည်။ ၎င်းမှ မော်ဒယ်ကို ခိုးယူရန် သို့မဟုတ် ၎င်း၏ စွမ်းဆောင်ရည်ကို ထိခိုက်စေရန် ရည်ရွယ်သည့် စံဆိုက်ဘာလုံခြုံရေးတိုက်ခိုက်မှုများကို လျော့ပါးစေရန်လည်း ကူညီပေးပါမည်။

သင်၏မော်ဒယ်ကို စဉ်ဆက်မပြတ်ကာကွယ်ပါ

တိုက်ခိုက်သူများသည် မော်ဒယ်ကို တိုက်ရိုက်ဝင်ရောက်ခြင်းဖြင့် (မော်ဒယ်အလေးချိန်များ ရယူခြင်းဖြင့်) သို့မဟုတ် သွယ်ဝိုက်သောနည်းဖြင့် (အပလီကေးရှင်း သို့မဟုတ် ဝန်ဆောင်မှုမှတစ်ဆင့် မော်ဒယ်ကို မေးမြန်းခြင်းဖြင့်) မော်ဒယ်တစ်ခု၏ လည်ပတ်မှု [13]သို့မဟုတ် လေ့ကျင့်ထားသည့်ဒေတာ [14]ကို ပြန်လည်တည်ဆောက်နိုင်သည်။ တိုက်ခိုက်သူများသည် လေ့ကျင့်မှုအတွင်း သို့မဟုတ် ပြီးနောက် မော်ဒယ်များ၊ ဒေတာ သို့မဟုတ် အချက်ပြ သင်္ကေတများကို ခြယ်လှယ်နိုင်ပြီး အချက်အလက်များကို မယုံနိုင်စရာဖြစ်စေနိုင်သည်။

သင်သည် မော်ဒယ်နှင့် ဒေတာကို တိုက်ရိုက်နှင့် သွယ်ဝိုက်ဝင်ရောက်ခြင်းအား ဤသို့ ကာကွယ်နိုင်သည် -

- စံဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အကောင်းဆုံး အလေ့အကျင့်များကို အကောင်အထည်ဖော်ခြင်း
- လျှို့ဝှက်အချက်အလက်များကို ရယူရန်၊ ပြင်ဆင်ရန်နှင့် ထုတ်ယူရန် ကြိုးပမ်းမှုများကို ရှာဖွေပြီး တားဆီးရန်အတွက် စုံစမ်းမေးမြန်းရေးအင်တာဖေ့စ် (query interface) ပေါ်ရှိ ထိန်းချုပ်မှုများကို အကောင်အထည်ဖော်ခြင်း

အသုံးပြုစနစ်များမှ မော်ဒယ်များမှာ မှန်ကန်အကြောင်း ဆောင်ရွက်ရန် မော်ဒယ်ကို လေ့ကျင့်ထားသည်နှင့်ချက်ချင်း သင်သည် လျှို့ဝှက်သင်္ကေတများ (cryptographic hashes) နှင့်/သို့မဟုတ် မော်ဒယ်ဖိုင်များ၏ လက်မှတ်များ (ဥပမာ၊ မော်ဒယ်အလေးချိန်များ) နှင့် ဒေတာအတွဲများ (စစ်ဆေးရေးဂိတ်များအပါအဝင်) ကို တွက်ချက်ပြီး မျှဝေပါ အချက်အလက်အား ဝှက်စာဖြင့်ထိန်းသိမ်းခြင်းနှင့်ပတ်သက်လျှင် ကောင်းမွန်သော အဓိကစီမံခန့်ခွဲမှုမှာ မရှိမဖြစ်အရေးကြီးသည်[15]။

အတွင်းရေးလျှို့ဝှက်ချက်အန္တရာယ် လျော့ချရေးဆိုင်ရာ သင်၏ချဉ်းကပ်မှုသည် အသုံးပြုလိုသည့်ကိစ္စနှင့် ခြိမ်းခြောက်မှုပုံစံပေါ်တွင် များစွာမူတည်ပါသည်။ အချို့သော အပလီကေးရှင်းများ၊ ဥပမာအားဖြင့် အလွန်ထိရှလွယ်သောဒေတာများပါဝင်သည့် အပလီကေးရှင်းများသည် အကောင်အထည်ဖော်ဆောင်ရန် ခက်ခဲသော သို့မဟုတ် အကုန်အကျများနိုင်သော သီအိုရီဆိုင်ရာအာမခံချက်များ လိုအပ်နိုင်သည်။ သင့်လျော်ပါက မော်ဒယ်များနှင့် အချက်အလက်များအား ရရှိနေသည့် သုံးစွဲသူများ၊ အသုံးပြုသူများ၊ တိုက်ခိုက်သူများနှင့် ဆက်နယ်နေသော အန္တရာယ်အဆင့်များကို စူးစမ်းရန် သို့မဟုတ် အာမခံရန် အတွင်းရေးလျှို့ဝှက်ချက် မြင့်တင်မှုနည်းပညာများ (ဥပမာ ကွဲပြားခြားနားသော အတွင်းရေးလျှို့ဝှက်ချက် သို့မဟုတ် အမျိုးအစားတူသော ကုဒ်ဝှက်ခြင်းကဲ့သို့) ကို အသုံးပြုနိုင်ပါသည်။

ဖြစ်ရပ်စီမံခန့်ခွဲမှုလုပ်ထုံးလုပ်နည်းများ ဖော်ဆောင်ပါ

သင်၏ AI စနစ်များကို ထိခိုက်စေသော လုံခြုံရေးဆိုင်ရာ ဖြစ်ရပ်များ မလွဲမသွေဖြစ်ပွားမှုသည် သင်၏ ဖြစ်ရပ်တုံ့ပြန်မှု၊ တိုးမြင့်ရေးနှင့် ပြန်လည်ပြင်ဆင်ရေး အစီအစဉ်များတွင် ထင်ဟပ်နေသည်။ သင့်အစီအစဉ်များသည် မတူညီသောအခြေအနေများကို ထင်ဟပ်စေပြီး စနစ်နှင့် ကျယ်ပြန့်သော သုတေသနများ ပြောင်းလဲလာသည်နှင့်အမျှ ပုံမှန်ပြန်လည်အကဲဖြတ်ပါသည်။ သင်သည် အရေးပါသော ကုမ္ပဏီဒစ်ဂျစ်တယ်ရင်းမြစ်များကို အော့ဖ်လိုင်း အရန်သိမ်းဆည်းစနစ်များတွင် သိမ်းဆည်းထားသည်။ တုံ့ပြန်သူများကို AI နှင့်ပတ်သက်သည့် ဖြစ်ရပ်များကို အကဲဖြတ်ပြီး ဖြေရှင်းရန် လေ့ကျင့်သင်ကြားထားပါသည်။ သင်သည် သုံးစွဲသူများနှင့် သုံးစွဲသူများအား အပိုင်ငြေကြေး မကုန်ကျစေဘဲ ၎င်းတို့၏ဖြစ်ရပ်တုံ့ပြန်ရေးလုပ်ငန်းစဉ်များကို ပိုမိုဆောင်ရွက်နိုင်ရန် အရည်အသွေးမြင့် စာရင်းစစ်မှတ်တမ်းများနှင့် အခြားလုံခြုံရေးအင်္ဂါရပ်များ သို့မဟုတ် အချက်အလက်များကို ပေးပါသည်။

AI ကို တာဝန်သိစွာ ဖြန့်ချိပါ

မော်ဒယ်များ၊ အပ်ပလီကေးရှင်းများ သို့မဟုတ် စနစ်များ မဖြန့်ချိမီ ၎င်းတို့ကို စံညွှန်းသတ်မှတ်ခြင်းနှင့် ကျွမ်းကျင်ပညာရှင်အသင်းဖွဲ့၍ ဆိုက်ဘာလုံခြုံရေးစမ်းသပ်ခြင်း (ထို့အပြင် ဤလမ်းညွှန်ချက်များ၌ မပါသော အခြားစစ်ဆေးမှုများ၊ ဥပမာ - ဘေးကင်းလုံခြုံရေး သို့မဟုတ် တရားမျှတရေး) ကဲ့သို့ သင့်လျော်ပြီး ထိရောက်သော လုံခြုံရေးအကဲဖြတ်မှု ဆောင်ရွက်ပြီးမှသာ ဖြန့်ချိပါ၊ ထို့အပြင် အသုံးပြုသူများအား ကန့်သတ်မှုများ သို့မဟုတ် ပျက်ကွက်နိုင်ခြေရှိသော မုဒ်များအကြောင်းကို ရှင်းလင်းစွာပြောဆိုပါ။ ဤစာတမ်း၏ အဆုံးဌာနရှိသော ထပ်လောင်းဖတ်မှတ်စရာ ကဏ္ဍ တွင် လူတိုင်း အသုံးပြုနိုင်သော လုံခြုံရေးစစ်ဆေးရေး စာကြည့်တိုက်များ၏ အသေးစိတ်အချက်အလက်များကို ဖော်ပြထားသည်။

အသုံးပြုသူများအတွက် မှန်ကန်သောအရာများကို ပြုလုပ်ရန် လွယ်ကူအောင်ဆောင်ရွက်ပါ

ဆက်တင်အသစ် သို့မဟုတ် ဖွဲ့စည်းပုံစနစ်ဆိုင်ရာ ရွေးချယ်မှုတစ်ခုစီကို ၎င်းကရရှိလာသော လုပ်ငန်းအကျိုးအမြတ်များနှင့် ၎င်းမိတ်ဆက်ပေးသည့် လုံခြုံရေးအန္တရာယ်များနှင့်အတူ အကဲဖြတ်ရန်လိုအပ်ကြောင်း သင်အသိအမှတ်ပြုပါသည်။ အကောင်းဆုံးအနေဖြင့် အလုံခြုံဆုံးဆက်တင်တစ်ခုကို တစ်ခုတည်းသောရွေးချယ်မှုအဖြစ် စနစ်ထဲတွင် ပေါင်းပေးသွားမည်ဖြစ်သည်။ ဖွဲ့စည်းပုံစနစ်ပြင်ဆင်ရာတွင် မူလရွေးချယ်မှုသည် သာမန်ခြိမ်းခြောက်မှုများကို ကျယ်ကျယ်ပြန့်ပြန့် ကာကွယ်သင့်သည် (ဆိုလိုသည်မှာ နဂိုမူလအားဖြင့် ကာကွယ်ခြင်းဖြစ်သည်)။ သင်သည် သင့်စနစ်အား အန္တရာယ်ရှိသော နည်းလမ်းများဖြင့် အသုံးပြုခြင်း သို့မဟုတ် ဖြန့်ကျက်ခြင်းအား တားဆီးရန် ထိန်းချုပ်မှုများကို ကျင့်သုံးသည်။

သင်သည် ကန့်သတ်ချက်များကို မီးမောင်းထိုးပြခြင်းနှင့် ပျက်ကွက်နိုင်ခြေရှိသော မုဒ်များပါဝင်သော သင့်မော်ဒယ် သို့မဟုတ် စနစ်ကို သင့်လျော်စွာအသုံးပြုရန်အတွက် အသုံးပြုသူများအား လမ်းညွှန်ချက်ပေးပါသည်။ သင်သည် အသုံးပြုသူများအား ၎င်းတို့တာဝန်ရှိသည့် လုံခြုံရေးကဏ္ဍများကို ရှင်းလင်းစွာဖော်ပြပြီး ၎င်းတို့၏ဒေတာများကို မည်သည့်နေရာ (နှင့် မည်သို့) အသုံးပြုမည်၊ ဝင်ရောက်ကြည့်ရှုနိုင် သို့မဟုတ် သိမ်းဆည်းမည်နှင့် ပတ်သက်၍ ပွင့်လင်းမြင်သာမှုရှိရမည် (ဥပမာ၊ ၎င်းကို မော်ဒယ်ပြန်လည်လေ့ကျင့်ရေးအတွက် အသုံးပြုပါက သို့မဟုတ် ဝန်ထမ်းများ သို့မဟုတ် လုပ်ဖော်ကိုင်ဖက်များက ပြန်လည်သုံးသပ်ပါက)။

4. လုံခြုံသောလည်ပတ်မှုနှင့် ပြုပြုပြင်ထိန်းသိမ်းမှု

ဤကဏ္ဍတွင် AI စနစ် ဖွံ့ဖြိုးတိုးတက်မှုဖြစ်စဉ်၏ **လုံခြုံသောလည်ပတ်မှုနှင့် ပြုပြုပြင်ထိန်းသိမ်းမှု**အဆင့်နှင့်ဆိုင်သော လမ်းညွှန်ချက်များ ပါဝင်ပါသည်။ ယင်းမှ မှတ်တမ်းတင်ခြင်းနှင့် စောင့်ကြည့်ခြင်း၊ မွမ်းမံမှု စီမံဆောင်ရွက်ရေးနှင့် အချက်အလက် မျှဝေခြင်းအပါအဝင် စနစ်တစ်ခု ဖြန့်ကြက်ခြင်းနှင့် အထူးသက်ဆိုင်သော လုပ်ဆောင်မှုများဆိုင်ရာ လမ်းညွှန်ချက်များကို ပေးပါသည်။

သင့်စနစ်၏ အပြုအမူကို စောင့်ကြည့်ပါ

သင့်အနေဖြင့် လုံခြုံရေးကို ထိခိုက်စေသော အမူအကျင့်များ ရုတ်တရက်နှင့် တဖြည်းဖြည်းချင်း ပြောင်းလဲမှုများကို သတိပြုနိုင်သည်အထိ သင့်မော်ဒယ်နှင့် စနစ်၏ ရလဒ်များနှင့် စွမ်းဆောင်ရည်ကို တိုင်းတာပါသည်။ သင့်အနေဖြင့် သဘာဝအလျောက် ဒေတာစီးဆင်းမှုအပြင် ဖြစ်နိုင်ခြေရှိသော ကျူးကျော်ဝင်ရောက်မှုများနှင့် ချိုးဖောက်မှုများကို ဖော်ထုတ်နိုင်ပါသည်။

သင့်စနစ်၏ ထည့်သွင်းအချက်အလက်များကို စောင့်ကြည့်ပါ

အတွင်းရေးလျှို့ဝှက်ချက်နှင့် ဒေတာကာကွယ်ရေး ပြဋ္ဌာန်းချက်များနှင့်အညီ စနစ်ချိုးဖောက်ခံရသည့် သို့မဟုတ် တလွဲအသုံးပြုသည့်ကိစ္စတွင် သင်သည် ကျင့်ဝတ်လိုက်နာမှု တာဝန်ဝတ္တရားများ၊ စာရင်းစစ်၊ စုံစမ်းစစ်ဆေးခြင်းနှင့် ပြန်လည်ပြင်ဆင်ခြင်းတို့ လုပ်ဆောင်ရန်အတွက် သင့်စနစ်ထဲတွင် ထည့်သွင်းထားသော အချက်အလက်များ (ရည်ညွှန်းချက် တောင်းဆိုမှုများ၊ မေးမြန်းမှုများ သို့မဟုတ် အချက်ပေးသင်္ကေတများကဲ့သို့သော) ကို စောင့်ကြည့်ပြီး မှတ်တမ်းတင်ပါသည်။ ၎င်းတွင် (ပုံများကို ဖြတ်တောက်ခြင်းနှင့် အရွယ်အစား ချိန်ညှိခြင်းကဲ့သို့) ဒေတာပြင်ဆင်မှုအဆင့်များကို တလွဲအသုံးပြုရန် ရည်ရွယ်ထားသောအရာများအပါအဝင် ဖြန့်ဝေခြင်းပြင်ပနှင့်/သို့မဟုတ် ပဋိပက္ခဖြစ်နိုင်သော ထည့်သွင်းအချက်အလက်များကို ပြတ်သားစွာ ထောက်လှမ်းခြင်းတို့ ပါဝင်နိုင်သည်။

အပ်ဒိတ်များပြုလုပ်ရာတွင် ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း နည်းလမ်းကို ကျင့်သုံးပါ

သင်သည် ထုတ်ကုန်တိုင်း အလိုအလျောက်အပ်ဒိတ်များကို မူရင်းပုံစံဖြင့် ထည့်သွင်းပြီး ၎င်းတို့ကို ဖြန့်ဝေရန်အတွက် လုံခြုံသော၊ စံနှုန်းကိုက်ညီအောင် ပြုလုပ်ထားသော အပ်ဒိတ်လုပ်ထုံးလုပ်နည်းများကို အသုံးပြုပါ။ သင်၏ အပ်ဒိတ်လုပ်ငန်းစဉ်များ (စစ်ဆေးခြင်းနှင့် အကဲဖြတ်ခြင်းစနစ်များအပါအဝင်) က ဒေတာ၊ မော်ဒယ်များ သို့မဟုတ် အချက်ပြသင်္ကေတများ ပြောင်းလဲမှုများသည် စနစ်အမူအကျင့်ပြောင်းလဲမှုများ (ဥပမာ၊ သင်သည် ကြီးမားသောအပ်ဒိတ်ဖြစ်ခြင်းကို ဗားရှင်းအသစ်များကဲ့သို့ သဘောထားသည်) သို့ ဦးတည်သွားနိုင်သည့် အချက်ကို ထင်ဟပ်စေသည်။ သင်သည် မော်ဒယ်ပြောင်းလဲမှုများကို အကဲဖြတ်ရန်နှင့် တုံ့ပြန်ရန် (ဥပမာ၊ အစမ်းကြည့်ရှုခွင့်နှင့် ဗားရှင်းကွဲသော API များ ပံ့ပိုးပေးခြင်းဖြင့်) အသုံးပြုသူများအား ပံ့ပိုးပေးပါသည်။

သင်ယူခဲ့သော သင်ခန်းစာများကို စုဆောင်းပြီး မျှဝေပါ

သင်သည် အကောင်းဆုံးအလေ့အကျင့်ကို သင့်လျော်သလိုမျှဝေရန် ကမ္ဘာ့ဂေဟစနစ်လုပ်ငန်း၊ ပညာရေးရပ်ဝန်း၊ အစိုးရအဖွဲ့အစည်းများနှင့် ပူးပေါင်း၍ သတင်းအချက်အလက်မျှဝေရေး အသိုက်အဝန်းတွင် ပါဝင်နေပါသည်။ သင်သည် လုံခြုံရေးသုတေသီများအား အားနည်းချက်များကို သုတေသနပြုပြီး သတင်းပို့နိုင်ရန် ခွင့်ပြုချက်ပေးခြင်းအပါအဝင် စနစ်လုံခြုံရေးနှင့်ပတ်သက်သည့် တုံ့ပြန်ချက်အတွက် သင့်အဖွဲ့အစည်းအတွင်းနှင့်အပြင် နှစ်ရပ်လုံး၌ ပွင့်ပွင့်လင်းလင်း ဆက်သွယ်ခြင်းကို ထိန်းသိမ်းထားသည်။ လိုအပ်သည့်အခါ သင်သည် ကြီးမားကျယ်ပြန့်သော အသိုင်းအဝိုင်းသို့ ဥပမာ ပြီးပြည့်စုံပြီး တွေ့ရများသည့် အားနည်းချက်စာရင်းကောက်ယူခြင်းအပါအဝင် အားနည်းချက်ရှိသော ထုတ်ဖော်ချက်များအပေါ် တုံ့ပြန်သည့် သတင်းလွှာများ ထုတ်ဝေပေးခြင်းဖြင့် ပြဿနာများကို မြှင့်တင်ဖော်ပြပါသည်။ သင်သည် ပြဿနာများကို လျင်မြန်စွာနှင့် သင့်လျော်စွာ လျော့ပါးသက်သာစေရန်နှင့် ပြေလည်စေရန် လုပ်ဆောင်ပါသည်။

ထပ်လောင်းဖတ်မှတ်စရာ

AI ဖွံ့ဖြိုးတိုးတက်မှု

စက်ကိရိယာဖြင့် သင်ကြားလေ့လာမှု လုံခြုံရေးဆိုင်ရာ စည်းမျဉ်းများ
ML အစိတ်အပိုင်းတစ်ခုပါသည့် စနစ်တစ်ခု ဖွံ့ဖြိုးတိုးတက်အောင် ဆောင်ရွက်ခြင်း၊ ဖြန့်ကြက်ခြင်း သို့မဟုတ် လည်ပတ်ခြင်းဆိုင်ရာ NCSC ၏ အသေးစိတ် လမ်းညွှန်ချက်။

ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း - ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အန္တရာယ်ဟန်ချက်ကို ပြောင်းလဲခြင်း - ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း ဆော့ဖ်ဝဲလ်ဆိုင်ရာ စဉ်းမျဉ်းများနှင့် ချဉ်းကပ်နည်းများ
CISA ၊ NCSC နှင့် အခြား အေဂျင်စီများမှ ပူးတွဲရေးသားထားသည့် ဤလမ်းညွှန်ချက်တွင် AI အပါအဝင် ဆော့ဖ်ဝဲလ်စနစ်များ ထုတ်လုပ်သူများအနေဖြင့် ထုတ်ကုန်ဖွံ့ဖြိုးတိုးတက်ရေး၏ ဒီဇိုင်းအဆင့်တွင် လုံခြုံရေးကို ပေါင်းစပ်ထည့်သွင်းရန်နှင့် ထုတ်ကုန်များကို လုံခြုံစွာ တင်ပို့နိုင်ရန် ထည့်သွင်းစဉ်းစားသင့်ကြောင်း ဖော်ပြထားသည်။

AI လုံခြုံရေးဆိုင်ရာ စိုးရိမ်ဖွယ်ရာများ အကျဉ်းချုပ်
ဂျာမန် သတင်းအချက်အလက် လုံခြုံရေးဆိုင်ရာ ဖက်ဒရယ်ရုံး (BSI) မှ ထုတ်ဝေထားသည့် ဤစာတမ်းတွင် စက်ကိရိယာဖြင့် သင်ကြားရေးစနစ်များအပေါ် ဖြစ်ပေါ်နိုင်သည့် တိုက်ခိုက်မှုများနှင့် အဆိုပါတိုက်ခိုက်မှုများအပေါ် ခုခံကာကွယ်မှုများအကြောင်း မိတ်ဆက်ထားပါသည်။

အဆင့်မြင့် AI စနစ်များ ဖော်ဆောင်နေသည့် အဖွဲ့အစည်းများအတွက် ဟီရိုရှိမားလုပ်ငန်းစဉ်ဆိုင်ရာ နိုင်ငံတကာလမ်းညွှန်မှုများ နှင့် အဆင့်မြင့် AI စနစ်များ ဖော်ဆောင်နေသည့် အဖွဲ့အစည်းများအတွက် ဟီရိုရှိမားလုပ်ငန်းစဉ်ဆိုင်ရာ နိုင်ငံတကာကျင့်ဝတ်စည်းကမ်း
G7 ဟီရိုရှိမား AI လုပ်ငန်းစဉ်၏ တစိတ်တပိုင်းအဖြစ် ထုတ်ဝေထားသည့် ဤစာတမ်းများသည် အဆင့်အမြင့်ဆုံး အခြေခံမော်ဒယ်များနှင့် ထုတ်လုပ်နိုင်သော AI စနစ်များ အပါအဝင် အဆင့်မြင့်ဆုံး AI စနစ်များကို ဘေးကင်းလုံခြုံရေး၊ လုံခြုံရေးနှင့် ကမ္ဘာတစ်ဝှန်းလုံးတွင် ယုံကြည်စိတ်ချရသော AI ဖြစ်လာစေရန် ရည်ရွယ်ချက်ဖြင့် ဖော်ဆောင်နေသော အဖွဲ့အစည်းများအတွက် လမ်းညွှန်ချက်ပေးပါသည်။

AI အတည်ပြုချက်
စံသတ်မှတ်ထားသော စစ်ဆေးမှုများမှတစ်ဆင့် နိုင်ငံတကာအသိအမှတ်ပြု အခြေခံမှုများအစုကို ဆန့်ကျင်၍ AI စနစ်များ၏ စွမ်းဆောင်ရည်ကို အတည်ပြုသော စင်ကာပူနိုင်ငံ၏ AI အုပ်ချုပ်ရေးဆိုင်ရာ စစ်ဆေးရေးမူဘောင်နှင့် ဆော့ဖ်ဝဲလ်ကိရိယာ။

AI ဆိုက်ဘာလုံခြုံရေးကျင့်သုံးမှုများဆိုင်ရာ အလွှာအထပ်ထပ်မူဘောင် — ENISA (europa.eu)
အမျိုးသားစည်းကမ်းထိန်းသိမ်းရေး အာဏာပိုင်များနှင့် AI အဖွဲ့အစည်းများအား ၎င်းတို့၏ AI စနစ်များ၊ လည်ပတ်မှုများနှင့် လုပ်ငန်းစဉ်များ လုံခြုံရေးအတွက် လိုက်နာရမည့် အဆင့်များကို ညွှန်ကြားပေးသည့် မူဘောင်။

ISO 5338: AI စနစ်ဖြစ်စဉ်ဆိုင်ရာ လုပ်ငန်းစဉ်များ (သုံးသပ်ဆဲ)
စက်ကိရိယာဖြင့် သင်ကြားခြင်းနှင့် ဆရာမဲ့လေ့လာသင်ကြားနည်းစနစ်များကို အခြေခံသော AI စနစ်များ၏ ဖြစ်စဉ်များကို ဖော်ပြသည့် လုပ်ငန်းစဉ်များအစုနှင့် ဆက်စပ်သဘောတရားများ။

AI ကလောက်ဒ်ဝန်ဆောင်မှုလိုက်နာရေး စံနှုန်းများဆိုင်ရာ စာရင်း (AIC4)
BSI ၏ AI ကလောက်ဒ်ဝန်ဆောင်မှုလိုက်နာရေး စံနှုန်းများဆိုင်ရာ စာရင်းမှ AI ဖြစ်စဉ်တစ်လျောက်လုံးရှိ ၎င်း၏ဝန်ဆောင်မှုဆိုင်ရာ လုံခြုံရေးကို အကဲဖြတ်နိုင်သည့် AI စံနှုန်းများကို ဖော်ပြထားပါသည်။

NIST IR 8269 (မူကြမ်း (ပဋိပက္ခဖြစ်စေသော စက်ကိရိယာဖြင့် သင်ကြားရေး၏ မျိုးခွဲပညာနှင့် ဝေါဟာရအသုံးအနှုန်း
စက်ကိရိယာဖြင့် သင်ကြားခြင်းနှင့် ဆရာမဲ့လေ့လာသင်ကြားနည်းစနစ်များကို အခြေခံသော AI စနစ်များ၏ ဖြစ်စဉ်များကို ဖော်ပြသည့် လုပ်ငန်းစဉ်များအစုနှင့် ဆက်စပ်သဘောတရားများ။

MITRE ATLAS
MITER ATT&CK မူဘောင်နှင့်အညီ တည်ဆောက်ထားသော စက်ကိရိယာဖြင့် သင်ကြားရေး (ML) စနစ်များအတွက် ပဋိပက္ခဖြစ်စေသော နည်းဗျူဟာများ၊ နည်းပညာများနှင့် ပြဿနာလေ့လာချက်များဆိုင်ရာ အသိပညာ။

ကြီးမားသော AIအန္တရာယ်များ သုံးသပ်ချက် (2023)
AI ဘေးကင်းလုံခြုံရေးစင်တာမှ ထုတ်ဝေသည့် ဤစာတမ်းတွင် AI ကြောင့်ဖြစ်ပေါ်လာသော အန္တရာယ်နယ်ပယ်များကို ဖော်ပြထားသည်။

ကြီးမားကျယ်ပြန့်သော ဘာသာစကားမော်ဒယ်များ- စက်မှုလုပ်ငန်းနှင့် အာဏာပိုင်များအတွက် အခွင့်အလမ်းများနှင့် အန္တရာယ်များ
LLM များ ဖန်တီးခြင်း၊ ဖြန့်ကြက်ခြင်းနှင့်/သို့မဟုတ် အသုံးပြုခြင်းဆိုင်ရာ အခွင့်အလမ်းများနှင့် အန္တရာယ်များအကြောင်း ပိုမိုသင်ယူလေ့လာလိုသော ကုမ္ပဏီများ၊ အာဏာပိုင်များနှင့် ဒဗလပ်ပါများအတွက် BSI မှ ထုတ်ဝေထားသည့် စာတမ်း။

AI မော်ဒယ်များ၏ လုံခြုံရေးစစ်ဆေးရာတွင် သုံးစွဲသူများကို ကူညီပေးသော လူတိုင်းအသုံးပြုနိုင်သည့် စီမံကိန်းများမှာ-

- Adversarial Robustness Toolbox (IBM)
- CleverHans (တိုရန်တိုတက္ကသိုလ်)
- TextAttack (ဗာဂျီးနီးယားတက္ကသိုလ်)
- Prompt Bench (မိုက်ခရိုဆော့ဖ်)
- Counterfit(မိုက်ခရိုဆော့ဖ်)
- AI Verify (Infocomm မီဒီယာ ဖွံ့ဖြိုးတိုးတက်ရေးအာဏာပိုင်၊ စင်ကာပူ)

ဆိုက်ဘာလုံခြုံရေး

CISA ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စွမ်းဆောင်မှု ရည်မှန်းချက်များ
သိရှိထားသော အန္တရာယ်များနှင့် ပဋိပက္ခဖြစ်စေသော နည်းပညာများ၏ ဖြစ်နိုင်ခြေနှင့် သက်ရောက်မှုကို အဓိပ္ပါယ်ရှိစွာလျှော့ချရန်အတွက် အရေးကြီးသော အခြေခံ အဆောက်အအုံဆိုင်ရာ အဖွဲ့အစည်းများအားလုံး အကောင်အထည်ဖော်ဆောင်ထားသင့်သည့် ကာကွယ်မှုအစု။

NCSC CAF မူဘောင်
ဆိုက်ဘာ အကဲဖြတ်ရေးမူဘောင် (CAF) မှ အထူးအရေးကြီးသော ဝန်ဆောင်မှုများနှင့် လုပ်ဆောင်မှုများအတွက် တာဝန်ရှိသော အဖွဲ့အစည်းများအတွက် လမ်းညွှန်ချက် ပေးပါသည်။

MITRE ၏ ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက်ဆိုင်ရာ လုံခြုံရေးမူဘောင်
ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက်အတွင်း ပစ္စည်းဖြည့်သွင်းသူများနှင့် ဝန်ဆောင်မှုပံ့ပိုးသူများကို အကဲဖြတ်စစ်ဆေးရေး မူဘောင်။

အန္တရာယ် စီမံခန့်ခွဲမှု

NIST AI အန္တရာယ် စီမံခန့်ခွဲမှုဆိုင်ရာ မူဘောင် (AI RMF)
AI RMF တွင် AI နှင့် သီးသန့်ဆက်စပ်နေသည့် လူတစ်ဦးချင်း၊ အဖွဲ့အစည်းများနှင့် လူ့ဘောင်အဖွဲ့အစည်းအတွက် လူမှုနည်းပညာဆိုင်ရာ အန္တရာယ်များကို မည်ကဲ့သို့ စီမံခန့်ခွဲရမည်ကို ဖော်ပြထားပါသည်။

ISO 27001: အချက်အလက်လုံခြုံရေး၊ ဆိုက်ဘာလုံခြုံရေးနှင့် အတွင်းရေးကာကွယ်မှု
ဤစံနှုန်းသည် အဖွဲ့အစည်းများအား အချက်အလက်လုံခြုံရေးဆိုင်ရာ စီမံခန့်ခွဲမှုစနစ်တစ်ခု တည်ဆောက်ခြင်း၊ အကောင်အထည်ဖော်ဆောင်ခြင်းနှင့် ပြုပြင်ထိန်းသိမ်းခြင်းနှင့်ပတ်သက်၍ လမ်းညွှန်ချက်ပေးပါသည်။

ISO 31000: အန္တရာယ် စီမံခန့်ခွဲမှု
အဖွဲ့အစည်းများအား အဖွဲ့အစည်းများအတွင်း အန္တရာယ် စီမံခန့်ခွဲမှုဆိုင်ရာ လမ်းညွှန်ချက်များနှင့် အခြေခံမူများကို ပံ့ပိုးပေးသည့် နိုင်ငံတကာစံနှုန်းတစ်ခု။

NCSC အန္တရာယ် စီမံခန့်ခွဲမှုဆိုင်ရာ လမ်းညွှန်ချက်
ဤလမ်းညွှန်ချက်မှ ဆိုက်ဘာလုံခြုံရေးအန္တရာယ်ဆိုင်ရာ ကျွမ်းကျင်သူများအား ၎င်းတို့၏ အဖွဲ့အစည်းများအပေါ် သက်ရောက်မှုရှိသော ဆိုက်ဘာလုံခြုံရေးအန္တရာယ်များကို ပိုမိုကောင်းမွန်စွာ နားလည်ပြီး စီမံခန့်ခွဲနိုင်ရန် ကူညီပေးပါသည်။

မှတ်ချက်

1. AI စနစ်တစ်ခုတည်ဆောက် (သို့မဟုတ် AI စနစ်တစ်ခု တည်ဆောက်ထား) ပြီး ထိုစနစ်ကို ဈေးကွက်ထဲမှာ မိတ်ဆက်ထားသော သို့မဟုတ် ကိုယ်ပိုင်အမည် သို့မဟုတ် ကုန်အမှတ်တံဆိပ်ဖြင့် ၎င်းကို အသုံးပြုထားသော ပုဂ္ဂိုလ်၊ လူထုအာဏာပိုင်၊ အေဂျင်စီ သို့မဟုတ် အခြားအဖွဲ့အစည်းအဖြစ် ဖော်ပြထားသည်
2. ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်းနှင့်ပတ်သက်၍ အချက်အလက်ပိုမိုသိရှိလိုပါက CISA ၏ ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း ဝက်ဘ်စာမျက်နှာနှင့် လမ်းညွှန်ချက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ အန္တရာယ်ဟန်ချက်ကို ပြောင်းလဲခြင်း- ဒီဇိုင်းဖြင့် လုံခြုံစေခြင်း ဆော့ဖ်ဝဲလ်ဆိုင်ရာ စဉ်းမျဉ်းများနှင့် ချဉ်းကပ်နည်းများ ကို ကြည့်ရှုပါ
3. စည်းမျဉ်းအခြေခံစနစ်များကဲ့သို့ ML မဟုတ်သော AI ချဉ်းကပ်နည်းများကို ဆန့်ကျင်လျက်
4. CEPS မှ ၎င်းတို့၏ထုတ်ဝေမှုဖြစ်သည့် 'AI တန်ဖိုးကွင်းဆက်ကို EU ၏ ဉာဏ်ရည်တုအက်ဥပဒေနှင့် ပြန်လည်ညှိနှိုင်းခြင်း 'တွင် AI ဖွံ့ဖြိုးတိုးတက်ရေး အပြန်အလှန်တုံ့ပြန်မှု ခုနစ်မျိုးကို ဖော်ပြထားသည်
5. ISO/IEC 22989:2022(en) သည် ဤအချက်ကို 'AI စနစ်တစ်ခု တည်ဆောက်ပေးသည့် လုပ်ဆောင်ချက်အစိတ်အပိုင်းတစ်ခု 'အဖြစ် သတ်မှတ်သည်
6. NIST သည် ဘေးကင်းလုံခြုံပြီး ယုံကြည်စိတ်ချရသော ဉာဏ်ရည်တု (AI) ဖွံ့ဖြိုးတိုးတက်ရေးနှင့် အသုံးပြုမှု တိုးတက်လာစေရန်အတွက် လမ်းညွှန်ချက်များ ထုတ်လုပ်ခြင်း (နှင့် အခြားလုပ်ဆောင်မှုများ) ကို ဆောင်ရွက်ရန် တာဝန်ယူထားပါသည်။ 2023ခုနှစ် အောက်တိုဘာလ 30 ရက် ညွှန်ကြားရေးအမိန့်တွင် ဖော်ပြထားသည့် NIST ၏ တာဝန်များကို ကြည့်ရှုပါ
7. ခြိမ်းခြောက်မှုဖော်ထုတ်ခြင်းနှင့်ပတ်သက်သည့် အချက်အလက်များကို OWASP ဖောင်ဒေးရှင်းမှ ရရှိနိုင်သည်
8. MITRE ATLAS ပဋိပက္ခဖြစ်စေသော စက်ကိရိယာဖြင့် သင်ကြားရေး101 ကို ကြည့်ရှုပါ
9. GitHub: အန္တရာယ်ရှိသော Lambda အလွှာကို အသုံးပြု၍ အများသုံး စက်ကိရိယာဖြင် သင်ကြားရေးစာကြည့်တိုက် (Tensorflow) ဆိုင်ရာ RCE PoC
10. SLSA: 'ဆော့ဖ်ဝဲလ် ပစ္စည်းဖြည့်သွင်းရေးကွင်းဆက်ရှိ အချက်အလက် တည်တံ့ခိုင်မြဲမှုကို ကာကွယ်ခြင်း'
11. METI (ဂျပန်နိုင်ငံ စီးပွားရေး၊ ကုန်သွယ်ရေးနှင့် စက်မှုလုပ်ငန်း ဝန်ကြီးဌာန၊ 2023)၊ 'ဆော့ဖ်ဝဲလ် စီမံခန့်ခွဲမှုအတွက် ဆော့ဖ်ဝဲလ် အစိတ်အပိုင်းများစာရင်း မိတ်ဆက်လမ်းညွှန်'
12. Google သုတေသန- စက်ကိရိယာဖြင့် သင်ကြားရေး နည်းပညာအကြွေးဆိုင်ရာ ကြီးမားသောအတိုးနှုန်း ခရက်ဒစ်ကတ်
13. Tramèr et al 2016, API များ ကြိုတင်ခန့်မှန်းမှုမှတစ်ဆင့် စက်ကိရိယာဖြင့် သင်ကြားရေးမော်ဒယ်များ ခိုးယူခြင်း
14. Boenisch, 2020, စက်ကိရိယာဖြင့် သင်ကြားရေးအတွင်းရေးကို တိုက်ခိုက်ခြင်းများ (အပိုင်း1): IBM-ART မူဘောင်နှင့် ဖော်ဒယ်ပြောင်းလဲမှုဆိုင်ရာ တိုက်ခိုက်ခြင်းများ
15. အမျိုးသားဆိုက်ဘာလုံခြုံရေး စင်တာ၊ 2020၊ သီးသန့်စီမံထားသော အများပြည်သူဆိုင်ရာ အဓိကအခြေခံအဆောက်အအုံတစ်ခု ဒီဇိုင်းရေးဆွဲပြီး တည်ဆောက်ခြင်း