TLP:CLEAR


# လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း

## ဆိုက်ဘာလုံခြုံရေး

## အန္တရာယ်ဆိုင်ရာ ဟန်ချက် ပြောင်းလဲခြင်း -

လုံခြုံမှုရှိအောင် စီမံလုပ်ဆောင်သည့် ဆော့ဖ်ဝဲ၏
အခြေခံသဘောတရားနှင့် ကိုင်တွယ်ဖြေရှင်းနည်းများ

TLP:CLEAR







Communications Security Establishment

**Canadian Centre for Cyber Security**

Centre de la sécurité des télécommunications

**Centre canadien pour la cybersécurité**











# အကြောင်းအရာများ

# အကျဉ်းချုံး - လုံခြုံမှုအားနည်းသော ပြင်ဆင်မှု

စက်မှုနည်းပညာသည် နေ့စဉ်နိစ္စဓုဝဘဝ၏ ဘက်ပေါင်းစုံတွင် ပါဝင်ပေါင်းစပ်မှုရှိနေပါသည်။ အင်တာနက်ကို အခြေခံသည့်စနစ်များသည် ကျွန်ုပ်တို့၏ စီးပွားရေးဖွံ့ဖြိုးမှု၊ ရှင်သန်နေထိုင်မှုများနှင့် ကျန်းမာရေးအပြင် ကိုယ်ရေးအချက်အလက် စီမံခန့်ခွဲရေးမှစ၍ ကျန်းမာရေးစောင့်ရှောက်မှုအထိ တိုက်ရိုက်သက်ရောက်မှုရှိသော အရေးကြီးသည့် စနစ်များနှင့် ချိတ်ဆက်မှုရှိနေပါသည်။ ဤကဲ့သို့ အဆင်ပြေတိုးတက်မှုများ၏ အားနည်းချက်တစ်ခုကို ဥပမာတစ်ခု ပြရမည်ဆိုလျင် - ကမ္ဘာတခွင် ဆိုက်ဘာလုံခြုံရေးများ ချိုးဖောက်ခံရသောကြောင့် ဆေးရုံများတွင် ခွဲစိတ်မှုများကို ဖျက်သိမ်းလိုက်ရခြင်းများနှင့် လူနာစောင့်ရှောက်ရေးတွင် အပြောင်းအလဲများ ဖြစ်စေပါသည်။ နည်းပညာ လုံခြုံမှုအားနည်းခြင်းနှင့် အရေးကြီးသည့် အချက်အလက်သိုလှောင်ရေးစနစ်များတွင် အားနည်းချက်များ ရှိခြင်းသည် မသမာသည့် ဆိုက်ဘာကျူးကျော်တိုက်ခိုက်မှုများ ဖြစ်စေရန် ဖိတ်ခေါ်သလို ဖြစ်စေနိုင်ပြီး ထိုမှတဆင့် ဆိုးဝါးသည့် လုံခြုံရေးဆိုင်ရာ[1] အန္တရာယ်များ ကျရောက်စေနိုင်ပါသည်။

ထို့အတွက်ကြောင့် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအတွက် မိမိ၏ ထုတ်ကုန်များထုတ်လုပ်သည့်အခါတွင် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံလုပ်ဆောင်ခြင်း (Secure-by-Design) နှင့် အလိုအလျောက် လုံခြုံမှုရှိနေခြင်းများ (Secure-by-Default) ကို အဓိကထားပြီး လုံခြုံစွာရှိအောင် မွမ်းမံထားသည့် ပစ္စည်းများကို ထုတ်လုပ်ရန် အင်မတန်မှ အရေးကြီးပါသည်။ တချို့ထုတ်လုပ်သူများသည် ဆော့ဖ်ဝဲလုံခြုံမှုရှိအောင် တိုးတက်သောခြေလှမ်းများနှင့် လုပ်ဆောင်နေပြီး တချို့ထုတ်လုပ်သူများမှာ နောက်ကျကျန်နေတာမျိုး ဖြစ်နေပါသည်။ အာဏာပိုင် အဖွဲ့အစည်းများအနေဖြင့် စက်မှုကုန်ထုတ်လုပ်သူတိုင်းအား အကြံပြုလိုသည်မှာ မိမိ၏ ထုတ်ကုန်ပစ္စည်းများကို ထုတ်လုပ်ရာတွင် ဝယ်ယူသုံးစွဲသူများအတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဝန်ထုတ်မှုများလျော့ပါးအောင် လုပ်ဆောင်ပေးဖို့ လိုအပ်ပြီး အဲဒီအထဲမှာ ဆိုက်ဘာကျူးကျော်တိုက်ခိုက်မှုမှ ကာကွယ်ရန်အတွက် သုံးစွဲသူများမှ တချိန်လုံး စောင့်ကြပ်မှုလုပ်ရခြင်း၊ မကြာခဏ အသစ်မွမ်းမံရခြင်း၊ ပြင်ဆင်ရခြင်းမျိုး ပြုလုပ်စရာမလိုအောင် ဆောင်ရွက်ကြရန် အကြံပြုလိုပါသည်။ ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများ အနေဖြင့် ၎င်းတို့၏ ပစ္စည်းများ တည်ဆောက်ရာတွင် အလိုအလျောက် configuration လုပ်ခြင်းများ၊ monitoring နှင့် ပုံမှန် updates များလုပ်အောင် စီမံလုပ်ဆောင်ဖို့ ထပ်မံတိုက်တွန်းလိုပါသည်။ သုံးစွဲသူများအတွက် လုံခြုံမှုပိုကောင်းမွန်စေရေးအတွက် ကုန်ထုတ်လုပ်သူဖက်မှ တာဝန်ယူလုပ်ဆောင်ပေးရန် အကြံပြုလိုပါသည်။ ယခင်ကဆိုလျင် သုံးစွဲသူများမှ ပစ္စည်းကို ဝယ်ယူသုံးစွဲပြီးမှ တွေ့ရှိသည့် အားနည်းချက်များကို ကုန်ထုတ်လုပ်သူများက ပြင်ဆင်ပေးခြင်းဖြစ်ပြီး ကုန်ထုတ်လုပ်သူများက အမှားကိုပြင်ဆင်သည့်အခါတွင်လည်း သုံးစွဲသူများမှ အဖိုးအခများထပ်မံ အကုန်အကျခံခဲ့ရသည့် အနေအထားရှိခဲ့ပါသည်။ ကုန်မထုတ်လုပ်မီအချိန်မှစ၍ လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်းနည်းဖြင့် ထုတ်လုပ်မှသာလျင် တီထွင်လိုက် ပြင်ဆင်လိုက်၊ ပြန်တီထွင်လိုက်စသည့် သံသရာမှ ကင်းလွတ်နိုင်မည် ဖြစ်ပါသည်။ **မှတ်ချက် -** "လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း" ဟုဆိုရာတွင် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်းနှင့် အလိုအလျောက် လုံခြုံမှုရှိနေခြင်းနှစ်မျိုးစလုံးကို ဆိုလိုပါသည်။

အဆင့်မြင့်သည့် ဆော့ဖ်ဝဲလုံခြုံရေး ရရှိရန်အတွက် ကုန်ထုတ်လုပ်သူများအနေဖြင့် ဈေးကွက်တွင် မရောင်းချမီ လုံခြုံရေးကို ရှေးရှုပေါင်းစပ်ထားသည့် ကုန်ပစ္စည်းများကို လုပ်ဆောင်ရန်လိုအပ်သည်ဟု နှလုံးသွင်းပြီး ဦးစားပေးလုပ်ဆောင်ပေးရန် အာဏာပိုင်အေဂျင်စီများအနေဖြင့် အကြံပြုလိုပါသည်။ အချိန်ကြာလာသည်နှင့်အမျှ အင်ဂျင်နီယာအဖွဲ့များသည် လုံခြုံမှုရှိသည့် ကုန်ပစ္စည်းများအားအားသွန်ခွန်စိုက်ထုတ်လုပ်စရာမလိုပဲ အလိုအလျောက် ပုံမှန်အနေအထားအတိုင်း စည်းဝါးတကျ လုပ်ဆောင်လာနိုင်ကြမည်ဖြစ်ပြီး မွမ်းမံထိန်းသိမ်းမှု လုပ်ရခြင်းများလည်း အားသွန်ခွန်စိုက်လုပ်ရန်မလိုအပ်သော အနေအထား ဖြစ်လာနိုင်ပါသည်။

ထိုအချက်ကို ရှေးရှုဒ၍ ဥရောပသမဂ္ဂသည် လုံခြုံမှုရှိသည့် ကုန်ပစ္စည်းများထုတ်လုပ်ရန် အရေးကြီးကြောင်းကို တွန်းအားပေးသည့်အနေဖြင့် ဆိုက်ဘာတိုက်ခိုက်ခြင်းကို ခုခံနိုင်ရေးအက်ဥပဒေ (Cyber Resilience Act) ကို ရေးဆွဲခဲ့ပါသည်။ ထိုဆိုက်ဘာအက်ဥပဒေသည် လုံခြုံမှုအားနည်းချက်ရှိနေသည့် ကုန်ပစ္စည်းများစျေးကွက်တွင် မရှိစေရန်အတွက် ကုန်ထုတ်လုပ်သူများအနေဖြင့် ကုန်ပစ္စည်းတစ်ခု၏ သက်တမ်းတလျှောက်တွင် လုံခြုံမှုရှိနေရန် တီထွင်လုပ်ဆောင် ထည့်သွင်းရမည်ဟု သတ်မှတ်ထားပါသည်။

1 အာဏာပိုင်အဖွဲ့အစည်းများအနေဖြင့် "လုံခြုံရေး"ဆိုသည့် အသုံးအနှုန်းတွင် အသုံးပြုမှု အပေါ်မူတည်၍ အဓိပ္ပာယ် အမျိုးမျိုး သက်ရောက်မှု ရှိသည်ကို နားလည်ပါသည်။ ဤလမ်းညွှန်မှု ရည်ရွယ်ချက်အရ "လုံခြုံရေး" ဟု သုံးရာတွင် ဝယ်ယူသုံးစွဲသူများကို မသမာသည့် ဆိုက်ဘာ လှုပ်ရှားမှု များမှ ကာကွယ်နိုင်ရန်အတွက် စက်မှု ပိုင်းဆိုင်ရာ လုံခြုံရေး စံနှုန်းများမြင့်တင်ရေးကို ဆိုလိုပါသည်။

အနာဂတ်တွင် သုံးစွဲသူများအတွက် လုံခြုံမှုရှိသည့် စက်မှုကုန်ပစ္စည်းနှင့် ဆက်စပ်ကုန်ပစ္စည်းများ တီထွင်နိုင်ရန်အတွက် အာဏာပိုင်အေဂျင်စီများမှ ကုန်ပစ္စည်းထုတ်လုပ်ရောင်းချသူများအား ၎င်းတို့၏ ကုန်ပစ္စည်းများကို ပြန်လည်မွမ်းမံပြီး ပစ္စည်းထုတ်လုပ်ရာတွင် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံထားသည့် ကုန်ပစ္စည်းများ (Secure-by-Design) နှင့် အလိုအလျောက် လုံခြုံမှုရှိနေသည့် ကုန်ပစ္စည်းများ (Secure-by-Default) ကိုသာ ထုတ်လုပ်ရန်ခွင့်ပြုဖို့ တိုက်တွန်းထားပြီး ထို့မှတဆင့် သုံးစွဲမည့်သူများထံ ရောင်းချရန် တိုက်တွန်းလိုပါသည်။ လုံခြုံမှုအတွက်ပြင်ဆင်စီမံထားသော ကုန်ပစ္စည်းများဆိုသည်မှာ စက်မှုပိုင်းဆိုင်ရာ တစ်ခုတည်းသာမက သုံးစွဲသူများ၏ လုံခြုံဘေးကင်းမှုကိုပါ ပဓာနထားသည့် စီးပွားလုပ်ငန်းမျိုးဖြစ်ပါသည်။ လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံထားသော ကုန်ပစ္စည်းထုတ်လုပ်မှု မစတင်မီကပင် ထို့အတွက် ရည်ရွယ်ချက်ထားရှိပြီး လုပ်ဆောင်ရမည်ဖြစ်ပါသည်။ ထပ်ခါထပ်ခါ လုပ်ဆောင်ခြင်းအားဖြင့် လက်ရှိ ကုန်ပစ္စည်းများသည် လုံခြုံမှုရှိသော ကုန်ပစ္စည်းအဖြစ် ဆင့်ကဲ ပြောင်းလဲမှု ဖြစ်လာနိုင်ပါသည်။ အလိုအလျောက်လုံခြုံမှုရှိနေသည့် ကုန်ပစ္စည်းများဆိုသည်မှာ "အထုတ်မှ ထုတ်လိုက်သည်နှင့်" ပြုပြင်မွမ်းမံမှု ထပ်လုပ်ရန်နှင့် ထပ်မံကုန်ကျခံစရာမလိုအပ်ပဲ လုံခြုံရေးအလိုအလျောက်ပါရှိသော ကုန်ပစ္စည်းများ ဖြစ်ပါသည်။ ၎င်းအခြေခံမှုများ ပေါင်းစည်းလိုက်သည့် အခါတွင် ကုန်ထုတ်လုပ်သူများအတွက် လုံခြုံရေးဆိုင်ရာ ဝန်ထုတ်ဝန်ပိုးများ လျော့ကျစေသလို သုံးစွဲသူများအား သာကောင်အဖြစ်မှ ရှောင်ရှားစေနိုင်ပြီး ၎င်းတို့ကို ကုန်ပစ္စည်းသုံးစွဲရာတွင် လွဲမှားစွာ ဖွဲ့စည်းထုတ်လုပ်ထားသောပစ္စည်း၊ အလွယ်နည်းဖြင့် ပြုလုပ်ထားသောပစ္စည်းနှင့် အခြားပြဿနာများရှိသောကုန်ပစ္စည်းများ ဝယ်ယူသုံးစွဲမိရာမှ မိမိ၏ လုံခြုံရေး ထိခိုက်နစ်နာမှုများ မဖြစ်အောင် လျှော့ချပေးရာ ရောက်နိုင်ပါသည်။

ဆိုက်ဘာလုံခြုံရေးနှင့် အခြေခံအဆောက်အဦးလုံခြုံရေးဆိုင်ရာ အေဂျင်စီ(CISA)၊ နိုင်ငံတော် လုံခြုံရေးဆိုင်ရာ အေဂျင်စီ (NSA)၊ ဗဟို ထောက်လှမ်းရေးဌာန(FBI) နှင့် အောက်ပါ နိုင်ငံတကာ မိတ်ဖက်အဖွဲ့များ[2]သည် ကုန်ထုတ်လုပ်သူများအနေဖြင့် ၎င်းတို့၏ ကုန်ပစ္စည်းများကို လုံခြုံမှုရှိစွာ ထုတ်လုပ်နိုင်ရန်အတွက် ဤလမ်းညွှန်ပါ အကြံပြုချက်များကို လမ်းပြမြေပုံသဖွယ် အသုံးပြုရန် ဝေဉ်ပေးလျက်ရှိပါသည်။ မိတ်ဖက်အဖွဲ့များမှာ -

- သြစတြေးလျနိုင်ငံ ဆိုက်ဘာလုံခြုံရေးစင်တာ (ACSC)
- ကနေဒါ ဆိုက်ဘာလုံခြုံရေးစင်တာ (Canadian Centre for Cyber Security (CCCS))
- ယူကေနိုင်ငံ အမျိုးသားဆိုက်ဘာလုံခြုံရေးစင်တာ (United Kingdom's National Cyber Security Centre (NCSC-UK))
- ဂျာမနီနိုင်ငံသတင်းအချက်အလက် လုံခြုံရေးဆိုင်ရာ ဖယ်ဒရယ်ရုံး(Germany's Federal Office for Information Security (BSI))
- နယ်သာလန်နိုင်ငံ အမျိုးသားဆိုက်ဘာလုံခြုံရေးစင်တာ (Netherlands' National Cyber Security Centre (NCSC-NL))
- နော်ဝေးနိုင်ငံ အမျိုးသားဆိုက်ဘာလုံခြုံရေးစင်တာ (NCSC-NO)
- နယူးဇီလန်နိုင်ငံ ကွန်ပျူတာဆိုင်ရာ အရေးပေါ်နှင့် တုံ့ပြန်ရေးဆိုင်ရာအသင်း (Computer Emergency Response Team New Zealand (CERT NZ)) နှင့် နယူးဇီလန်နိုင်ငံ အမျိုးသားဆိုက်ဘာလုံခြုံရေးစင်တာ (New Zealand's National Cyber Security Centre (NCSC-NZ))
- ကိုရီးယားနိုင်ငံ အင်တာနက်နှင့် လုံခြုံရေးဆိုင်ရာ အေဂျင်စီ(KISA)
- အစ္စရေးနိုင်ငံ အမျိုးသားဆိုက်ဘာ ညွှန်ကြားရေးမှူးရုံး (INCD)
- ဂျပန်နိုင်ငံ ဆိုက်ဘာလုံခြုံရေးဖြစ်ရပ်ဆိုင်ရာ အသင့်ဖြစ်မှုနှင့် နည်းဗျူဟာဆိုင်ရာ အမျိုးသားစင်တာ (NISC) နှင့် ဂျပန်နိုင်ငံ ကွန်ပျူတာဆိုင်ရာ အရေးပေါ်တုံ့ပြန်ရေးအဖွဲ့ ညှိနှိုင်းဆောင်ရွက်ရေးစင်တာ(JPCERT/CC)
- အမေရိကားနိုင်ငံ အစိုးရဆိုက်ဘာ ဖြစ်ရပ်တုံ့ပြန်ရေးအဖွဲ့၏ OAS/CICTE ကွန်ရက် (CSIRT)
- စင်ကာပူနိုင်ငံ ဆိုက်ဘာလုံခြုံရေး အေဂျင်စီ(CSA)
- ချက်ပြည်သူ့သမ္မတနိုင်ငံ အမျိုးသားဆိုက်ဘာနှင့် အချက်အလက် လုံခြုံရေးဆိုင်ရာ အေဂျင်စီ (NÚKIB) တို့ ဖြစ်ပါသည်။

ပုဂ္ဂလိကကဏ္ဍမှ မိတ်ဖက်အဖွဲ့အစည်းများသည် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံထားခြင်းနဲ့ အလိုအလျောက် လုံခြုံမှုရှိသော ကုန်ပစ္စည်းများ ထုတ်လုပ်ရာတွင် တိုးတက်မှုရှိအောင် လုပ်ဆောင်ရာတွင် ပါဝင်ကူညီနေသည်ကို အာဏာပိုင် အဖွဲ့အစည်းများမှ အသိအမှတ်ပြုပါသည်။ ၎င်းကုန်ပစ္စည်းသည် နိုင်ငံတကာ ပြောဆိုဆွေးနွေးပွဲများအတွက် ဦးစားပေးဆွေးနွေးစရာများအတွက် ရည်ရွယ်ပြီး ရင်းနှီးမြှုပ်နှံရေးနှင့် အနာဂတ်တွင် လုံခြုံပြီး၊ ဘေးကင်းသည့်အပြင် ခံနိုင်ရည်ရှိစွာ ပြင်ဆင်စီမံထားသည့် ပစ္စည်းနှင့် အလိုအလျောက်လုံခြုံမှုရှိသော ပစ္စည်းများ ထုတ်လုပ်ရာတွင် ဆုံးဖြတ်ချက်ချနိုင်ရန် ဖြစ်သည်။ အဆုံးတွင် အာဏာပိုင် အဖွဲ့အစည်းများမှ ဤကုန်ပစ္စည်းနှင့်ပတ်သက်၍ သက်ဆိုင်ရာ အဖွဲ့များထံမှ ဝေဖန်အကြံပြုချက်များ ရယူပြီး ဘုံရည်မှန်းချက်များအောင်မြင်ရေးအတွက် ထပ်မံမွမ်းမံနိုင်ရန်၊ သတ်မှတ်ပြဋ္ဌာန်းမှုများလုပ်ရန်နှင့် ကျွန်ုပ်တို့၏ လမ်းညွှန်ချက်များကိုလည်း ထပ်ဆင့်တိုးတက်လာစေရန်အတွက် ရည်ရွယ်ပါသည်။

ကုန်ပစ္စည်းလုံခြုံရေးနှင့် ပတ်သက်သည့် အရေးကြီး အသေးစိတ်အချက်အလက်များ ထပ်မံသိရှိလိုပါက CISA ၏ လုံခြုံမှုမရှိတဲ့ နည်းပညာကို အသုံးပြုခြင်းအတွက် ကုန်ကျစရိတ်များနဲ့ အဲဒီအတွက် ဘာတွေလုပ်ဆောင်သင့်သလဲ ဆိုသည့် ဆောင်းပါးတွင် ဖတ်ရှုနိုင်ပါသည်။

[2] ယခုမှစ၍ "အာဏာပိုင် အဖွဲ့အစည်းများ" ဟု သုံးနှုန်းပါမည်။

# အသစ်အဆန်းများ

ဤစာစောင်ကို စတင်ထုတ်ဝေချိန်မှစ၍ ဆော့ဖ်ဝဲကဏ္ဍတွင် ပြောဆိုဆွေးနွေးမှု များစွာ ထွက်ပေါ်လာခဲ့ပါသည်။ အဖွဲ့အစည်းများနှင့် လူတစ်ဦးတစ်ယောက်ခြင်းစီတို့၏ ဆိုက်ဘာလုံခြုံရေး တိုက်ခိုက်ခံရသည့် နေ့စဉ်သတင်းများကြောင့် ပြောဆိုဆွေးနွေးမှုများ ပြုလုပ်ရန် ပိုမို လိုအပ်သည်ကို ဖော်ပြနေပြီး ဆော့ဖ်ဝဲကုန်ပစ္စည်းများ၏ ရေရှည်ပြဿနာနှင့် စနစ်များကို မည်ကဲ့သို့ လုပ်ဆောင်သင့်သနည်း ဆိုသည့် ဆွေးနွေးမှုများ ပိုလုပ်ရန် လိုအပ်သည်ကို ပြသနေပါသည်။

ဤစာစောင်ကို 2023 ခုနှစ်၊ ဧပြီလတွင် ထုတ်ဝေပြီးနောက်ပိုင်း အာဏာပိုင် အဖွဲ့အစည်းများ (ယခုမှစ၍ “ကျွန်ုပ်တို့” နှင့် “ကျွန်ုပ်တို့၏” အဖြစ် ညွှန်းဆိုသွားမည်) အနေဖြင့် တစ်ဦးတစ်ယောက်ခြင်းထံမှဖြစ်စေ၊ ကုမ္ပဏီများနှင့် ကုန်သွယ်ရေးအသင်းအဖွဲ့များထံမှ ဝေဖန်အကြံပြုချက်ကောင်းများ ရာနဲ့ချီကို ရရှိခဲ့ပါသည်။ ဝေဖန်အကြံပြုချက်များထဲမှ အများဆုံးတောင်းဆိုကြသည်မှာ အခြေခံသဘောတရား ၃ ရပ်ကို အသေးစိတ် ရှင်းပြရန် တောင်းဆိုကြပြီး ၎င်းအခြေခံသဘောတရားများသည် ဆော့ဖ်ဝဲ ထုတ်လုပ်သူများနှင့် ၎င်းတို့၏ ပစ္စည်းကို ဝယ်ယူသုံးစွဲသူများအတွက်လည်း အကျိုးဝင်သည့်အတွက် ဖြစ်ပါသည်။ ဤစာစောင်သည် နဂိုမူလ အစီရင်ခံစာကို ချဲ့ကားထားပြီး အခြားသော အကြောင်းအရာဖြစ်သည့် ကုန်ထုတ်လုပ်သူများ၊ ဝယ်ယူသုံးစွဲသူများ အရွယ်အစား၊ ဝယ်ယူသုံးစွဲသူများ၏ သဘောပေါက် နားလည်နိုင်စွမ်းအား နှင့် အခြေခံသဘောတရား၏ အနေအထားများအကြောင်းပါ ထည့်သွင်းထားပါသည်။

ဆော့ဖ်ဝဲသည် နေရာတကာတွင်ရှိပြီး ဆော့ဖ်ဝဲ စနစ်တစ်ခုလုံးအကြောင်း၊ ဆော့ဖ်ဝဲပစ္စည်း ထုတ်လုပ်မှုအကြောင်း၊ ဝယ်ယူသုံးစွဲသူများ၏ အသုံးပြုမှုအကြောင်း၊ ထိန်းသိမ်းမွမ်းမံမှုနှင့် တခြားသော စနစ်များနှင့် သဟဇာတဖြစ်စေမှုအကြောင်းများကို အစီရင်ခံစာတစ်ခုတည်းတွင် လုံလောက်စွာ တင်ပြနိုင်မည်မဟုတ်ပေ။ အောက်ပါ လမ်းညွှန်ချက်အတွက် သေခြာစွာ ပုံဖော်ရှင်းလင်းခြင်းမရှိသေးပဲ ဤစာစောင်မှ မည်သည့် လုံခြုံရေး တိုးတက်မှုမျိုး ဖြစ်စေသည့်အကြောင်း ဖော်ပြပြောဆိုတာမျိုး ကြားရရန်လည်း မျှော်လင့်ပါသည်။

ဤစာစောင်သည် artificial intelligence (AI) ဟုခေါ်သည့် ဉာဏ်ရည်တု ဆော့ဖ်ဝဲစနစ်နှင့် ဆော့ဖ်ဝဲပုံစံ ထုတ်လုပ်သူများအတွက်ပါ ရည်ရွယ်ပါသည်။ AI စနစ်နှင့် ပုံစံသည် သာမာန် ဆော့ဖ်ဝဲ နှင့် ကွဲပြားမှုရှိနိုင်သော်လည်း အခြေခံကြသည့် လုံခြုံရေးဆိုင်ရာ အလေ့အထကို ဆက်လက် ကျင့်သုံးရန် အကျိုးဝင်ပါသည်။ အေအိုင်အတွက် အထူး ထုတ်လုပ်ရသည့်အခါတွင် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံပြင်ဆင်ခြင်းနည်းလမ်းများကို ပိုသင့်တော်မှုရှိအောင် ပြုပြင်ရတာမျိုးရှိနိုင်သော်လည်း လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်းဆိုင်ရာ အခြေခံသဘောတရား ၃ ချက်သည် အေအိုင် စနစ်အားလုံးအတွက်ပါ အကျိုးဝင်ပါသည်။

ဆော့ဖ်ဝဲထုတ်လုပ်မှု သက်တမ်း software development lifecycle (SDLC) ကို လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ခြင်းမှုနှင့် ကိုက်ညီရန် ပြောင်းလဲမှုလုပ်ရာတွင် ရိုးရှင်းလွယ်ကူမှုမရှိပဲ အချိန်ယူရမည်ဆိုသည်ကို ကျွန်ုပ်တို့အနေဖြင့် နားလည်ပါသည်။ ထို့အပြင် အသေးစား ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် ဤအကြံပြုချက်အများအပြားကို လိုက်နာလုပ်ဆောင်ရန် အခက်အခဲများ ရှိနိုင်သည်ကိုလည်း နားလည်ပါသည်။ ဆော့ဖ်ဝဲထုတ်လုပ်ရေးကဏ္ဍတွင် ကုန်ပစ္စည်းများကို ပိုမိုလုံခြုံမှု ရှိစေရန် အသုံးပြုသည့် ပစ္စည်းများနှင့် လုပ်ထုံးလုပ်နည်းများ လွယ်လွယ်ကူကူ ရရှိအောင် လုပ်ဆောင်ပေးရန် လိုအပ်သည်ဟု ကျွန်ုပ်တို့အနေဖြင့် ယုံကြည်ပါသည်။ လူပုဂ္ဂိုလ်များနှင့် အဖွဲ့အစည်းများက ဆော့ဖ်ဝဲလုံခြုံမှု ပိုရှိလာစေရေးအတွက် အာရုံစိုက်လာသည်နှင့်အမျှ တီထွင်ကြဆမှုအခွင့်အလမ်းများ ပိုများလာနိုင်သည်ဟု ကျွန်ုပ်တို့အနေဖြင့် ယုံကြည်ပြီး ထိုအခြေအနေမျိုးတွင် အသေးစားနှင့် အကြီးစား ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများ အကြားရှိသည့် ကွာဟမှုများကို စေ့စပ်ပေးနိုင်သကဲ့သို့ ဝယ်ယူသုံးစွဲသူများအားလည်း အကျိုးအမြတ် ရရှိစေနိုင်ပါသည်။

ဤလုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ခြင်းဆိုင်ရာ အစီရင်ခံစာအသစ်သည် အခြားသော ဆက်စပ်အဖွဲ့အစည်းများနှင့် ဆက်ဆံရေးတည်ဆောက်ခြင်းနှင့် စက်မှုပိုင်းဆိုင်ရာတွင် သဟဇာတစနစ် ရှိစေရန် ရည်ရွယ်သည့် ကျွန်ုပ်တို့၏ လုပ်ဆောင်ချက် တစိတ်တပိုင်း ဖြစ်ပါသည်။ သဟဇာတစနစ်၏ အစိတ်အပိုင်းများစွာ၏ ဝေဖန်အကြံပြုချက်မှ ဤအစာများ ဖြစ်ပေါ်လာခြင်းဖြစ်ပြီး အမြင်အမျိုးမျိုးကို ကျွန်ုပ်တို့ ဆက်လက် နားဆင်လေ့လာသွားမည် ဖြစ်ပါသည်။ ရှေ့တွင် စိန်ခေါ်မှု များစွာရှိနေသော်လည်း လူအများအပြားနှင့် အဖွဲ့အစည်းအများအပြားသည် လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ခြင်း နည်းလမ်းကို အများအားဖြင့် အောင်မြင်စွာ အသုံးပြုနေကြသည်ကို သိရသောကြောင့် ကျွန်ုပ်တို့အနေဖြင့် အကောင်းဖက်ကို ရှေးရှုထားပါသည်။

# ဤစာစောင်ကို မည်သို့ အသုံးပြုနိုင်သနည်း

ဤစာစောင်ပါ အခြေခံသဘောတရားများကို လိုက်နာကျင့်သုံးရန် ကျွန်ုပ်တို့အနေဖြင့် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအား တိုက်တွန်းလိုပါသည်။ ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် အောက်ပါခြေလှမ်းများအတိုင်း လိုက်နာ လုပ်ဆောင်နေသည့် အကြောင်းကို မှတ်တမ်းများဖြင့် မှတ်သားပြီး အများသိရှိအောင် လုပ်နိုင်ပါသည်။ ဆောဖ်ဝဲကုန်ထုတ်လုပ်သူများအနေဖြင့် ဤအခြေခံ သဘောတရား၏ အနှစ်သာရအတိုင်း လုပ်ဆောင်ရာတွင် နည်းဗျူဟာများ အသုံးပြုရန် ကျွန်ုပ်တို့အနေဖြင့် တိုက်တွန်းလိုပါသည်။ သံသယစိတ်နဲ့ ကြည့်နေသည့် ဝယ်ယူသုံးစွဲသူများနှင့် ဝယ်ယူဖို့ အလားအလာရှိသူများကို ဆွဲဆောင်စေနိုင်မည့် လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ထားသော ပစ္စည်းများကို တီထွင်ဖန်တီးပြီး စိတ်ဝင်စားဖွယ် ဖြစ်အောင် စွဲဆောင်ရန် တိုက်တွန်းလိုပါသည်။

ဆောဖ်ဝဲကုန်ထုတ်လုပ်သူများမှ ဤစာစောင်ပါ အချက်များကို လိုက်နာသင့်သကဲ့သို့ ဝယ်ယူသုံးစွဲသူများသည်လည်း ဤစာစောင်ကို အသုံးချ၍ အကျိုးအမြတ်ရအောင် စွမ်းဆောင်နိုင်ပါသည်။ ဆော့ဖ်ဝဲ ဝယ်ယူသည့် ကုမ္ပဏီများအနေဖြင့် ကုန်ထုတ်လူသူများကို အကြပ်ရိုက်စေမည့် မေးခွန်းများ မေးသင့်ပါသည်၊ ဥပမာ ဤစာစောင်တွင် ရေးသားထားသည့် အခြေခံ သဘောတရားပါ အချက်များကို လိုက်နာခြင်း ရှိမရှိကို မေးမြန်းနိုင်ပါသည်။ ထိုကဲ့သို့ လုပ်ဆောင်ခြင်းအားဖြင့် ဝယ်ယူသုံးစွဲသူများသည် ပိုမို လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံသည့် ကုန်ပစ္စည်းများ ဈေးကွက်တွင် ပေါ်လာစေရန် တွန်းအားပေးမှု ဖြစ်စေနိုင်ပါသည်။ ဝယ်ယူသူများအနေဖြင့် ကုန်ထုတ်လုပ်သူများအား မေးမြန်းနိုင်တဲ့ မေးခွန်း ဥပမာများကို ဆိုက်ဘာလုံခြုံရေးနှင့် အခြေခံအဆောက်အဦး လုံခြုံရေးအေဂျင်စီ CISA ၏ K-12 Technology Acquisitionsလမ်းညွှန်ချက်တွင် ဖော်ပြထားပါသည်။

ဝယ်ယူသူ ကုမ္ပဏီများကို ဤအခြေခံ သဘောတရားများအား အခြေခံသည့် လုပ်ဆောင်ချက်များကို ထည့်သွင်းအသုံးပြုပြီး ထိုကဲ့သို့ အချက်ကို လိုက်နာမှု ရှိမရှိ ကုန်ထုတ်လုပ်သူများကို စောင့်ကြည့်ခြင်း၊ ကုန်ပစ္စည်း လက်ခံသည့် ဆုံးဖြတ်ချက်ကို ဝယ်ယူသူ ကုမ္ပဏီမှ ဆုတ်ကိုင်ပြီး ကုန်ပစ္စည်း ထုတ်လုပ်သူများကို စောင့်ကြည့်လေ့လာရာတွင် တခြားသော ခြေလှမ်းများကိုပါ အသုံးပြုခြင်းမျိုး လုပ်ရန် တိုက်တွန်းလိုပါသည်။ ကုန်ထုတ်လုပ်သူများသည် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံမှု လုပ်ငန်းများလုပ်ဆောင်ထားသည်ကို လူအများသိစေရန် မှတ်တမ်းများဖြင့် မှတ်တမ်းတင်ခြင်းများ ပြုလုပ်ရန် ဝယ်ယူသုံးစွဲသူများမှ ကုန်ထုတ်လုပ်သူများကို တိုက်တွန်းတောင်းဆိုနိုင်ပါသည်။ ထိုကဲ့သို့ အတူတကွ လုပ်ဆောင်ပါက လုံခြုံမှုရှိသော ကုန်ပစ္စည်းများကို ဝယ်လိုအားကောင်းကြောင်း ပြသရာရောက်သည့်အတွက် ဆော့ဖ်ဝဲကုန်ထုတ်လူသူများက ပိုမို လုံခြုံသော ကုန်ပစ္စည်းများကို ထုတ်လုပ်သည့် ခြေလှမ်းများ လှမ်းရန် နှိုးဆော်မှု ဖြစ်စေနိုင်ပါသည်။ တနည်းအားဖြင့် ဆိုသော် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများထံမှ ပိုမို လုံခြုံစွာ ပြင်ဆင်စီမံသော ပစ္စည်းများကို ထုတ်လုပ်ရန် လိုလားသကဲ့သို့ တဖက်တွင်လည်း ကျွန်ုပ်တို့မှ ထိုပစ္စည်းများကို "ဝယ်ယူလိုအားခိုင်မာကြောင်း" ပြသရန်လည်း လိုအပ်ပါသည်။

# လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း

"လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း" (Secure-by-Design) ဆိုသည်မှာ မသမာသည့် ဆိုက်ဘာတိုက်ခိုက်မှုများမှ မိမိ၏ စက်ပစ္စည်း၊ အချက်အလက်များနှင့် ဆက်သွယ်ရေးစနစ်ကို ဝင်ရောက်ကြည့်၍မရစေရန် အတော်အတန် ကာကွယ်မှုရှိအောင် လုပ်ဆောင်ပေးထားသော စက်မှုကုန်ထုတ် ပစ္စည်း ဖြစ်ပါသည်။ ဆော့ဖ်ဝဲပစ္စည်း ထုတ်လုပ်သူများအနေဖြင့် အရေးကြီးသည့်စနစ်များအား ဆိုက်ဘာတိုက်ခိုက်ခံရနိုင်ခြေရှိမှုကို ဆန်းစစ်ဖော်ထုတ်ခြင်းနှင့် မှတ်တမ်းယူခြင်းများ ပြုလုပ်ပြီး ထိုအထဲတွင် ခေတ်အလိုက်ပြောင်းလဲဖြစ်ပေါ်နေသော ဆိုက်ဘာလုံခြုံရေး တိုက်ခိုက်မှုများအတွက် ခံရနိုင်ခြေရှိသော ကာကွယ်မှုများ ထည့်တွက်ထားသည့် ကုန်ပစ္စည်း၏ ပုံစံပြာ (blueprint) များကို ထည့်သွင်းသင့်ပါသည်။

အိုင်တီ (IT) နည်းပညာ၏ ဖွံ့ဖြိုးတိုးတက်မှု လုပ်ထုံးလုပ်နည်းနှင့် အလွှာအဆင့်ဆင့်ဖြင့် နက်ရှိုင်းစွာ ကာကွယ်ထားခြင်းဟု ခေါ်သည့် တဆင့်ခံကာကွယ်မှုအလွှာများကို လုံခြုံဘေးကင်းမှုရှိအောင် လုပ်ဆောင်ရမည်ဖြစ်သည်- ထိုကဲ့သို့ လုပ်ဆောင်မှုသည် စနစ်များကို တိုက်ခိုက်ခံရမှုမှ ကာကွယ်နိုင်ခြင်း သို့မဟုတ် ထိလွယ်ရှလွယ်သော အချက်အလက်များကို တရားမဝင်နည်းဖြင့် ရယူရန် ခက်ခဲစေနိုင်ပါသည်။ အာဏာပိုင်အဖွဲ့အစည်းများအနေဖြင့် ကုန်ထုတ်လုပ်သူများအား အကြံပြုလိုသည်မှာ မိမိထုတ်လုပ်သည့် ကုန်ပစ္စည်းများ ကြုံရနိုင်သည့် တိုက်ခိုက်မှုများကို စမ်းသပ်ရာတွင်လည်း စနစ်တစ်ခုချင်းစီအတွက် ကိုက်ညီသော စမ်းသပ်မှုပုံစံ tailored threat model ကို အသုံးပြုပြီး ဖြစ်နိုင်ခြေရှိသည့် တိုက်ခိုက်မှုများအတွက် ကာကွယ်လုပ်ဆောင်ရန် အကြံပြုလိုပါသည်။

အာဏာပိုင်အဖွဲ့အစည်းများအနေဖြင့် ကုန်ထုတ်လုပ်သူများကို ၎င်းတို့၏ ကုန်ပစ္စည်းများနှင့် ပလက်ဖောင်းများအတွက် လုံးဝလုံခြုံမှုရှိစေမည့် နည်းလမ်းကို အသုံးပြုရွေးချယ်လုပ်ဆောင်ကြရန် တိုက်တွန်းလိုပါသည်။ လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း (secure-by-design) ထုတ်လုပ်မှုတွင် ကုန်ထုတ်လုပ်မှုဒီဇိုင်းအလွှာတစ်ခုခြင်းစီအတွက် ဆော့ဖ်ဝဲထုတ်လုပ်ရေးအတွက် ကြီးမားသော အရင်းအမြစ်များလိုအပ်ပြီး ထုတ်လုပ်မှု ဖြစ်စဉ်အတွင်းတွင်လည်း "ထပ်မံ ဖြည့်စွက်ရန်" ဆိုတာမျိုး မဖြစ်စေရန်အတွက် အရင်းအမြစ်များ လိုအပ်ပါသည်။ လုပ်ငန်းတစ်ခုအတွက် လုံခြုံရေးကို ဦးစားပေးနေရာ ထားရှိလုပ်ဆောင်ခြင်းကို ထိပ်ဆုံးပိုင်းမှ ကုန်ထုတ်လုပ်သူများ၏ ခိုင်မာသည့် ခေါင်းဆောင်မှု လိုအပ်ပြီး နည်းပညာကဏ္ဍတစ်ခုတည်းမှ လုပ်ဆောင်နိုင်သည့်အရာ မဟုတ်ပါ။ ထိပ်ပိုင်းမှ စီးပွားရေးအရာရှိများနှင့် နည်းပညာအသင်းများ ပူးပေါင်းဆောင်ရွက်မှုသည် သုံးစွဲသူများ၏ အသုံးချမှုမတိုင်မီနှင့် ထိန်းသိမ်းမှုမှတဆင့် ဒီဇိုင်းရေးဆွဲခြင်းနှင့် ဖွံ့ဖြိုးရေးစတင်သည့် အစောပိုင်းကာလကတည်းက စတင်ဖြစ်ပေါ်နေရန် လိုအပ်ပါသည်။ ကုန်ထုတ်လုပ်သူများအနေဖြင့် သုံးစွဲသူများ "မမြင်နိုင်သည့်အရာများ" ဖြစ်သည့် အားနည်းချက်များပြီး ခုခံနိုင်မှုနည်းပါးသောဆော့ဖ်ဝဲများ ပပျောက်စေရန်အတွက် (ဥပမာ- ကျယ်ကျယ်ပြန့်ပြန့်ရှိနေသည့် အားနည်းချက်များကို ပရိုဂရမ်မင်း programming ဘာသာရပ်များဆီ ပြောင်းလဲထည့်သွင်းအသုံးပြုခြင်း) အတိုးအလျှော့ အပေးအယူများလုပ်ရန်နှင့် ရင်းနှီးမြှုပ်နှံမှုများ လုပ်ကြရန် တိုက်တွန်းလိုပါသည်။ ၎င်းတို့အနေဖြင့် ဆွဲဆောင်မှုရှိသော်လည်း တိုက်ခိုက်မှု မျက်နှာပြင်ဖြစ်စေနိုင်သည့် ကုန်ပစ္စည်း၏ သွင်ပြင်အင်္ဂါကို ဦးစားပေးမည့်အစား သုံးစွဲသူများကို ကာကွယ်ပေးမည့် အရာများကို အသုံးပြုမည့် စက်ယန္တရားများကို ဦးစားပေးသင့်ပါသည်။

အားနည်းချက်ရှိနေသည့် စက်မှုကို မသမာသည့် ဆိုက်ဘာတိုက်ခိုင်မှုများ ရပ်တန့်အောင် လုပ်ဆောင်ရာတွင် ဖြေရှင်းချက်တစ်ခုတည်း မရှိပါ၊ လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံထားသည့် (secure-by-design) ကုန်ပစ္စည်းများသည် အားနည်းချက်အပေါ်မူတည်ပြီး ဆက်လက် တိုက်ခိုက်ခံရမည် ဖြစ်သော်လည်း ထိုအားနည်းချက် အများစုသည် သေးငယ်သော ပြဿနာအရင်းအမြစ်မှ ဖြစ်ပေါ်လာခြင်း ဖြစ်ပါသည်။ ကုန်ထုတ်လုပ်သူများအနေဖြင့် လက်ရှိကုန်ပစ္စည်းများကို လုံခြုံစွာပြင်ဆင်စီမံခြင်း နည်းလမ်းများနှင့် ချိန်ညှိရန် ရေးသားထားသောလမ်းပြမြေပုံများကို ဖော်ဆောင်ပေးသင့်ပြီး ထူးခြားသည့် အခြေအနေများတွင်သာ သွေဖီသွားရန်ဆောင်ရွက်သင့်သည်။

သုံးစွဲသူများအတွက် လုံခြုံရေးရလဒ်နှင့် အဆင့်မြင့် လုံခြုံရေးအတွက် လုပ်ဆောင်ရာတွင် ကုန်ထုတ်လုပ်မှု စရိတ် ပို များပြားလာနိုင်သည်ကို အာဏာပိုင် အဖွဲ့အစည်းများအနေဖြင့် နားလည်ပါသည်။ သို့သော်လည်း လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံထားသည့် စက်မှုများကို ထုတ်လုပ်ရန်အတွက် ရင်းနှီးမြှုပ်နှံပြီး တဖက်တွင်လည်း ကုန်အသစ်များ ထုတ်လုပ်နေရင်းလက်ရှိ ကုန်များကိုလည်း ရေရှည်ထိန်းသိမ်းနိုင်မှုလုပ်နိုင်ခြင်းသည် သုံးစွဲသူများအတွက် လုံခြုံရေးနှင့် အချက်အလက်အခိုးခံရမှုမျိုးမဖြစ်အောင် ပိုမိုကာကွယ်ပေးရာ ရောက်နိုင်ပါသည်။ လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း အခြေခံသဘောတရားသည် သုံးစွဲသူများအတွက် လုံခြုံမှုပေးပြီး ကုန်ထုတ်လုပ်သူ၏ အမှတ်တံဆိပ်ဂုဏ်သတင်းကို ကျော်စောစေရုံသာမက ရေရှည်တွင် ကုန်ထုတ်လုပ်သူတွေအတွက် ပြုပြင်ထိန်းသိမ်းမှုနှင့် ဖာထေးမှုအတွက် ကုန်ကျစရိတ်ကိုလည်း လျော့နည်းစေနိုင်ပါသည်။

အောက်ပါအချက်အလက်များသည် ဆော့ဖ်ဝဲထုတ်လုပ်သူများအတွက် အကြံပြုချက်များ၏ စာရင်းဖြစ်ပြီး ကုန်ထုတ်လုပ်ရာတွင် ထည့်သွင်းစဉ်းစား အသုံးပြုနိုင်သည့် လုပ်ထုံးလုပ်နည်းများနှင့် မူဝါဒများကို အကြံပြုထားခြင်း ဖြစ်ပါသည်။

# အလိုအလျောက် လုံခြုံမှုရှိနေခြင်း

"Secure-by-Default" အလိုအလျောက် လုံခြုံမှုရှိနေခြင်းဆိုသည်မှာ ငွေကြေးထပ်မံ ကုန်ကျခံစရာမလိုဘဲ တိုက်ခိုက်ခံရမှုနည်းလမ်းများကို ခံနိုင်ရည်ရှိရန်အတွက် တည်ဆောက်ထားသည့် ကုန်ပစ္စည်းများကို ဆိုလိုပါသည်။ ထိုပစ္စည်းများသည် ကျယ်ကျယ်ပြန့်ပြန့်ဖြစ်ပေါ်နေသော ခြိမ်းခြောက်မှုများနှင့် အားနည်းချက်များကို ကာကွယ်ပေးခြင်းဖြစ်ပြီး ထိုကဲ့သို့ အကာအကွယ်ရရှိရန်အတွက် ဝယ်ယူသုံးစွဲသူများမှ ပိုမိုကုန်ကျခံစရာမလိုခြင်းမျိုး ဖြစ်ပါသည်။ Secure-by-default အလိုအလျောက် လုံခြုံမှုရှိနေသည့် ကုန်ပစ္စည်းကို သုံးစွဲသူများအသုံးပြုသည့်အခါ အလိုအလျောက် လုံခြုံနေခြင်းရှိသည့်နည်းလမ်းမှ သွေဖီသည့်အခါတွင် အချက်အလက်ချိုးဖောက် ခံရနိုင်ခြေများကြောင်း သေချာသိနားလည်အောင် လုပ်ဆောင်ထားရန်လိုအပ်ပြီး တခြားနည်းလမ်းဖြင့် ကာကွယ်ပေးမည့် နောက်ထပ်ထိန်းချုပ်မှုများ ထပ်မံရယူမှသာ ရနိုင်မည့်အကြောင်းပါ သိထားအောင် လုပ်ရန်လိုအပ်ပါသည်။ အလိုအလျောက် လုံခြုံမှုရှိခြင်းသည် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း ပုံစံတစ်မျိုး ဖြစ်ပါသည်။

» လုံခြုံမှုရှိသည့် ဖွဲ့စည်းပုံစနစ်သည် အခြေခံဖြစ်သင့်ပါသည်။ အလိုအလျောက် လုံခြုံနေသော ပစ္စည်း (Secure-by-Default products) သည် မသမာသော ဆိုက်ဘာတိုက်ခိုက်မှုများကို အကာအကွယ်ပေးနိုင်ရန်အတွက် လိုအပ်သော ထိန်းချုပ်မှုများကို အလိုအလျောက်ပေးထားသည့်အပြင် ထပ်မံကုန်ကျရန် မလိုအပ်ဘဲ လုံခြုံရေးဆိုင်ရာ အစိတ်အပိုင်းကို အသုံးပြုခွင့် ပေးထားပါသည်။

» လုံခြုံရေးဆိုင်ရာ တည်ဆောက်ပုံ၏ ရှုပ်ထွေးမှုသည် သုံးစွဲသူများအတွက် ပြဿနာမဖြစ်သင့်ပေ။ အိုင်တီအဖွဲ့အစည်းမှ အမှုထမ်းများအနေနှင့် လုံခြုံရေးဆိုင်ရာနှင့် လုပ်ငန်းလည်ပတ်ခြင်းဆိုင်ရာ တာဝန်များဖြင့် ဝန်ပိနေလေ့ရှိသည်။ ထိုကြောင့် လုံခြုံရေးပြဿနာနှင့် ခိုင်ခံ့ပြည့်စုံသော လုံခြုံရေးစနစ်ရရှိခြင်းကို နားလည်သဘောပေါက်အောင် လုပ်ဆောင်ရာတွင် အကန့်အသတ်ရှိနိုင်ပါသည်။ လုံခြုံရေးဆိုင်ရာ တည်ဆောက်ပုံအားတိုးမြင့်လုပ်ဆောင်ခြင်းအားဖြင့် - အလိုအလျောက်လမ်းကြောင်းများ ပွင့်စေခြင်းအားဖြင့် - ကုန်ထုတ်လုပ်သူများသည် ၎င်းတို့၏ ဝယ်ယူသုံးစွဲသူများလိုအပ်သည့် ပစ္စည်းများ ထုတ်လုပ်နိုင်ရေး၊ ဖြန့်ဖြူးရေးလုပ်ဆောင်ရာတွင် အလိုအလျောက် လုံခြုံနေသာ အဆင့်သတ်မှတ်ချက်နှင့်အညီ လုပ်ဆောင်ထားပေးနိုင်ပါသည်။

"အလိုအလျောက် လုံခြုံမှုရှိသော ကုန်ပစ္စည်း" များကို ထုတ်လုပ်ပြီး ထိုလုံခြုံရေးဆိုင်ရာ လုပ်ဆောင်မှုအတွက် ပိုမိုတောင်းခံမှုများ မလုပ်သင့်ပါ။ ၎င်းအစား ကားအသစ်တွင် ကားထိုင်ခုံခါးပတ် (seatbelt) လို အခြေခံကုန်အနေဖြင့် အလိုအလျောက် ပါလာပြီးသားဖြစ်အောင် ထည့်သွင်းလိုက်တာမျိုး ဖြစ်ပါသည်။

***လုံခြုံရေးသည် ဇိမ်ခံရန် မဟုတ်သည့်အတွက် ထိုလုံခြုံရေးအတွက် သုံးစွဲသူများမှ အပေးအယူလုပ်စရာမလိုအောင် သို့မဟုတ် အဖိုးအခ ထပ်မံပေးစရာမလိုဘဲ လူတိုင်းရသင့်သည့် အနေအထားဖြစ်အောင် လုပ်ဆောင်ရမည်ဖြစ်ပါသည်။***

## ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအတွက် အကြံပြုချက်များ

ဤအာဏာပိုင်အေဂျင်စီများ၏ ပူးတွဲအကြံပေးချက်များသည် ကုန်ထုတ်လုပ်သူများအနေဖြင့် အိုင်တီလုံခြုံရေးရှိစေရန်နှင့် လုံခြုံရေးအစီအစဉ်များ အကောင်အထည်ဖော်ရာတွင် လမ်းညွှန်ချက်ရေးဆွဲရန်အတွက် အကြံပြုချက်များ ဖြစ်ပါသည်။ အာဏာပိုင် အဖွဲ့အစည်းများအနေဖြင့် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအား အောက်ပါ ဗျူဟာအတိုင်း အကောင်အထည်ဖော်ကြရန် အကြံပြုလိုပြီး လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံထားခြင်းနှင့် အလိုအလျောက်လုံခြုံမှုရှိနေခြင်း အခြေခံမူမှတဆင့် ၎င်းတို့၏ သုံးစွဲသူများ လုံခြုံရေးရလာဒ် ရရှိစေရန် ဦးဆောင်ဦးရွက်ပြုရန် အကြံပြုပါသည်။

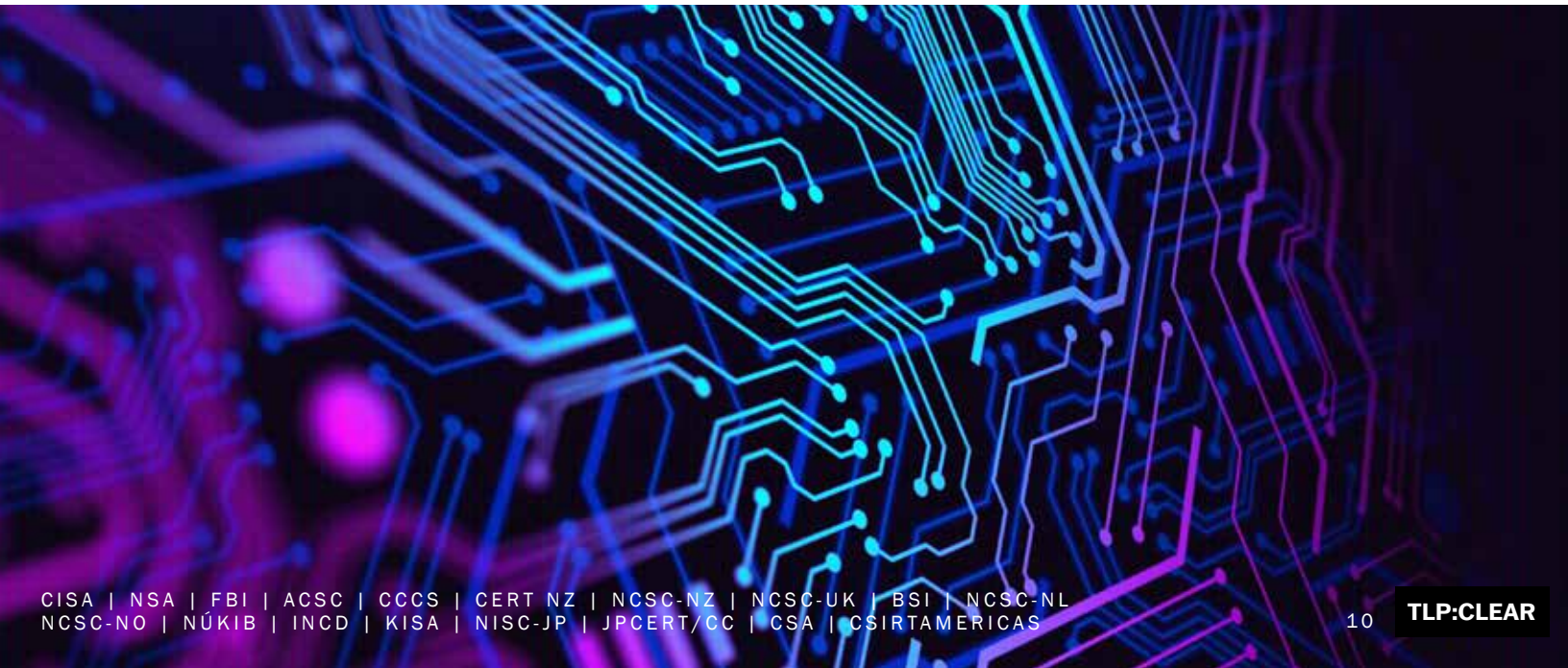
# ဆော့ဖ်ဝဲကုန်ပစ္စည်းများအတွက် လုံခြုံရေးဆိုင်ရာ အခြေခံမူများ

စက်မှုကုန်ပစ္စည်းထုတ်လုပ်သူများအနေဖြင့် ဆော့ဖ်ဝဲလုံခြုံရေးကို ဦးစားပေး အာရုံစိုက်ထားသည့် ဗျူဟာအား လက်စွဲအနေဖြင့် အသုံးပြုရန် တိုက်တွန်းလိုပါသည်။ အာဏာပိုင်အဖွဲ့အစည်းများသည် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနေဖြင့် ၎င်းတို့၏ ဆော့ဖ်ဝဲကို မထုတ်လုပ်မီ၊ အခြားပစ္စည်းနှင့် တွဲဖက်သုံးစွဲမှုမပြုခင်နှင့် ကုန်ပစ္စည်း တင်ပို့မှုမလုပ်မီ ဆော့ဖ်ဝဲဒီဇိုင်းရေးဆွဲနေသည့်အဆင့်တွင် အောက်ပါ အဓိက အခြေခံမူ ၃ ချက်ကို လမ်းညွှန်အဖြစ် အသုံးပြုနိုင်ရန်အတွက် ရေးဆွဲပေးထားပါသည်။

1 **ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးတာဝန်ယူပေးရမည်** ဖြစ်ပြီး ခေတ်နှင့်အညီ မိမိ၏ ကုန်ပစ္စည်းကို လိုက်လံပြောင်းလဲရမည် ဖြစ်သည်။ လုံခြုံရေးဝန်ကို သုံးစွဲသူများအပေါ်သာ ကျခံစေတာမျိုးမဖြစ်သင့်ပါ။

2 **ကြီးမားသိသာသည့် ပွင့်လင်းမြင်သာမှုရှိခြင်းနှင့် တာဝန်ခံမှုများကို လက်ခံကျင့်သုံးပါ။**
ဆော့ဖ်ဝဲထုတ်လုပ်သူများအနေဖြင့် လုံခြုံပြီး ဘေးကင်းသည့် ကုန်ပစ္စည်းများ ထုတ်လုပ်နိုင်မှုအပေါ် ဂုဏ်ယူဝင့်ကြွားသင့်သည့်အပြင် ကုန်ထုတ်လုပ်သူ အသိုင်းအဝိုင်းအတွင်း အခြားသူများနှင့်မတူအောင် လုပ်ဆောင်ပေးနိုင်သည့်အတွက် တမူထူးခြားမည်ဖြစ်ပါသည်။ ထိုအထဲမှာ ခိုင်မာစစ်မှန်သည့် နည်းပညာယန္တရား သုံးစွဲမှု အလိုအလျောက်များလာခြင်း စသည့် သုံးစွဲသူများ၏ ထိရောက်စွာ အသုံးချနိုင်မှုမျိုးကို သိရှိရသည့်အခါ ထိုအချက်အလက်များကို မျှဝေခြင်းမျိုး ဖြစ်ပါသည်။ အားနည်းချက်များကို ဖော်ပြခြင်း (vulnerability advisories) နှင့် ပူးတွဲဖြစ်တတ်သည့် အားနည်းချက်များနှင့် ဖော်ထုတ်သည့် (common vulnerability and exposure (CVE)) မှတ်တမ်းများကို ဖြည့်စွက်ပြီး မှန်ကန်စွာ လုပ်ထားခြင်းသည်လည်း အရေးကြီးသည့်လုပ်ဆောင်ချက် ဖြစ်ပါသည်။ သို့သော် ထို CVE မှတ်တမ်းအချက်အလက်ထုတ်ဖော်မှုအား အဆိုးဖက်ဆောင်သည့် အနေအထားအဖြစ် မြင်နိုင်ခြင်းကို သတိထားသင့်ပါသည်၊ ထိုအချက်အလက်များသည် ကုန်ပစ္စည်း၏ အရည်အသွေးကို ရှာဖွေ ဆန်းစစ်စမ်းသပ်မှု (healthy code analysis) နှင့် ဆော့ဖ်ဝဲများကို စမ်းသပ်ပေးသည့် အသိုင်းအဝိုင်း (testing community) ရှိခြင်း၏ လက္ခဏာကောင်းများ ဖြစ်သည်ကို ရည်ညွှန်းပေးသော မှတ်တမ်းဖြစ်ပါသည်။

3 **ထိုရည်မှန်းချက်များ အောင်မြင်ရန်အတွက် ဖွဲ့စည်းပုံရေးဆွဲတည်ထောင်ခြင်းနှင့် ခေါင်းဆောင်ပိုင်းဆိုင်ရာ ဦးဆောင်မှုများ ရှိအောင် တည်ဆောက်ရပါမည်။**
စက်မှုကုန်ပစ္စည်းများ ထုတ်လုပ်ရာတွင် စက်မှုကျွမ်းကျင်မှုများရှိရန် အရေးကြီးသကဲ့သို့ အဖွဲ့အစည်းအတွင်း ဖြစ်ပေါ်သည့် အပြောင်းအလဲများကို အကောင်အထည်ဖော်ဆောင်ရာတွင် အဓိက ဆုံးဖြတ်ချက်ပေးသူများမှာ ထိပ်ပိုင်းမှ အရာရှိများ ဖြစ်ကြပါသည်။ ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်ငန်းတွင် လုံခြုံဘေးကင်းရေးကို ဦးစားပေးလုပ်ရမည်ဟု ထိပ်သီး အလုပ်အမှုဆောင်အဆင့်မှ သတ်မှတ်ထားလျင် ထိုအချက်ကို သုံးစွဲသူများ၏ နားလည်မှုရရှိရန် လိုအပ်ပါသည်။



ထိုအခြေခံသဘောတရား ၃ ချက်ကို အသုံးပြုနိုင်ရန်အတွက် ကုန်ထုတ်လုပ်သူများအနေဖြင့် ၎င်းတို့၏ ကုန်ထုတ်လုပ်မှု လုပ်ငန်းစဉ်တွင် လည်ပတ်ခြင်းဆိုင်ရာ ဗျူဟာတချို့ကို ထည့်သွင်းစဉ်းစားသင့်ပါသည်။

အဖွဲ့အစည်းအတွင်း လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံထားခြင်းနှင့် အလိုအလျောက် လုံခြုံမှုရှိနေခြင်းနည်းလမ်းများ အရေးပါမှုကို ဖော်ဆောင်ရန် အတွက် ကုမ္ပဏီထိပ်သီးခေါင်းဆောင်များနှင့် ပုံမှန်အစည်းအဝေးများ ကျင်းပရန်အရေးကြီးပါသည်။ အခြေခံမူများအတိုင်း လိုက်နာထုတ်လုပ်သည့် အသင်းများကို ဂုဏ်ပြုသင့်ပြီး ထိုအထဲတွင် ဆော့ဖ်ဝဲလုံခြုံမှုရှိအောင် ထူးခြားစွာ စွမ်းဆောင်အကောင်အထည်ဖော်နိုင်မှုအတွက် ဆုချီးမြှင့်ခြင်း သို့မဟုတ် ရာထူးတိုးမြှင့်ပေးခြင်းများ လုပ်ဆောင်နိုင်ရန်အတွက် မူဝါဒနှင့် လုပ်ထုံးလုပ်နည်းများ ချမှတ်ထားရန်လည်း လိုအပ်ပါသည်။

ဆော့ဖ်ဝဲလုံခြုံမှုအား အရေးထားခြင်းသည် လုပ်ငန်းအောင်မြင်ခြင်းဟူသည့် ဆောင်ပုဒ်ဖြင့် လုပ်ငန်းကို လည်ပတ်သင့်ပါသည်။ ဥပမာ "ဆော့ဖ်ဝဲလုံခြုံရေး ခေါင်းဆောင်" တစ်ဦး သို့မဟုတ် "ဆော့ဖ်ဝဲလုံခြုံရေးအဖွဲ့" တစ်ဖွဲ့ကို စီးပွားရေးလုပ်ငန်းနှင့် အိုင်တီလုပ်ထုံးလုပ်နည်းများကို ဆော့ဖ်ဝဲလုံခြုံရေးစံနှုန်းများနှင့် တာဝန်ခံယူမှုရှိသော ကုန်ထုတ်လုပ်မှုနှင့် တိုက်ရိုက်ချိတ်ဆက်ရန် ခန့်အပ်ခြင်းကို စဉ်းစားပါ။ ကုန်ထုတ်လုပ်သူများ အနေဖြင့် ၎င်းတို့တွင် ခိုင်ခံ့ လွတ်လပ်သည့် လုံခြုံရေးဆန်းစစ်မှုရှိခြင်းနှင့် ၎င်းတို့၏ ထုတ်ကုန်များကို ပြန်လည်ဆန်းစစ်ပေးသည့် အစီအစဉ်များ ချထားရန် လိုအပ်ပါသည်။

ကုန်ထုတ်လုပ်သည့်ကာလတွင် အရေးအကြီးဆုံးနှင့် သက်ရောက်မှုအများဆုံးဖြစ်သော ကုန်များကို ဦးစားပေးထုတ်လုပ်နိုင်ရန်အတွက် ကုန်ပစ္စည်း၏ လုံခြုံရေးဆိုင်ရာ တိုက်ခိုက်နိုင်ခြေရှိမှုများအား စမ်းသပ်ရာတွင်လည်း တစ်ခုခြင်းစီအတွက် ကိုက်ညီသော စမ်းသပ်မှုပုံစံအတိုင်း လုပ်ဆောင်သင့်ပါသည်။ တိုက်ခိုက်နိုင်ခြေရှိမှုများအား စမ်းသပ်ခြင်းသည် ကုန်ပစ္စည်း၏ အဓိက အသုံးပြုမှုကို ထည့်သွင်းစဉ်းစားမှုဖြစ်စေသည့်အပြင် ကုန်ထုတ်လုပ်သည့်အသင်းသားများအားလည်း ကုန်ပစ္စည်းကို ပိုကောင်းမွန်စေရန် အားဖြည့်လုပ်ဆောင်စေနိုင်ပါသည်။ နောက်ဆုံးတွင် ထိပ်သီးခေါင်းဆောင်များအနေဖြင့် လုံခြုံမှုရှိသည့်ကုန်ပစ္စည်းများကို အကောင်းဆုံးနှင့် အရည်အသွေးအမြင့်ဆုံး ထုတ်လုပ်ရန်အတွက် ကုန်ပစ္စည်း ထုတ်လုပ်သည့် အသင်းများကို တာဝန်ယူမှု တာဝန်ခံမှုရှိအောင် လုပ်ထားသင့်ပါသည်။

၂၀၂၃ ခုနှစ် အောက်တိုဘာလတွင် ထုတ်ဝေသည့် ဤလမ်းညွှန်ချက်၏ အစိတ်အပိုင်းအဖြစ် ဤအခြေခံသဘောတရား သုံး ရပ်သည် ရှင်းပြချက်၊ လက်တွေ့လုပ်ဆောင်ချက်နှင့် သက်သေဟူသော အချက်သုံးချက်ဖြင့် တိုးချဲ့ထားပါသည်။

# အခြေခံ သဘောတရား ၁ - ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးကို တာဝန်ယူခြင်း

## ရှင်းပြချက်

ခေတ်သစ် လုပ်ထုံးလုပ်နည်းများအရ ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများသည် လုံခြုံဘေးကင်းသည့် ကုန်ပစ္စည်းများ ထုတ်လုပ်နိုင်ဖို့ ရင်းနှီးမြှုပ်နှံရမည်ဟု ပြဋ္ဌာန်းထားပြီး ထိုအထဲ**တွင် application hardening အက်ပလီကေးရှင်း တင်းကြပ်ခြင်း၊ application features** နှင့် အက်ပလီကေးရှင်း **default settingsများ ပါဝင်ပါသည်။**

ဆော့ဖ်ဝဲကုန်ထုတ်လူသူများအနေဖြင့် မသာမာသည့်နည်းလမ်းဖြင့် အချက်အလက်များရယူရန် ကြိုးစားမည့်သူများအား ကုန်ကျစေမည့် နည်းပညာနှင့် လုပ်ငန်းစဉ်များကို အသုံးချသည့် **application hardening (အက်ပလီကေးရှင်း တင်းကြပ်ခြင်း)** နည်းကို ကျင့်သုံးသင့်ပါသည်။ Application hardening ၏ လုပ်ထုံးလုပ်နည်းနှင့် ကျင့်ဝတ်များသည် ကုန်ပစ္စည်းများအား မသာမာသည့် အချက်အလက်ခိုးယူတိုက်ခိုက်မှုဒဏ်ကို ခံနိုင်မှု ရှိစေပါသည်။ တင်းကြပ်ခြင်း၊ ပစ္စည်းလုံခြုံမှုနှင့် ခံနိုင်ရည်ရှိမှု စသည့် စကားစုများသည် ပစ္စည်း၏ အရည်အသွေးနှင့်လည်း ဆက်စပ်လေ့ရှိပါသည်။ အဓိက ဆိုလိုသည်မှာ လုံခြုံရေးသည် "တပါတည်း ပူးတွဲပါဝင်" ရမည်ဖြစ်ပြီး "ထပ်မံဖြည့်စွက်ရန်" မဖြစ်သင့်ပါ။ [1] လုံခြုံရေးကို တပါတည်း ပူးတွဲပါဝင်စေခြင်းဖြင့် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးအား တိုးမြင့်ပေးရုံသာမက ၎င်းတို့၏ ကုန်ပစ္စည်းအရည်အသွေးကိုလည်း တိုးမြင့်ရာ ရောက်စေပါသည်။ ရိုးရှင်းသော ဗျူဟာထဲတွင် အသုံးပြုသူအတွက် ခိုင်လုံမှုနှင့် သန့်စင်မှုတို့ ပါဝင်ထားပြီး ကုဒ်ထဲကို ဝင်ရောက်ခြင်းမဟုတ်ပဲ (ဥပမာ - parameterized queries ကို အစားထိုးသုံးရန်)၊ လုံခြုံရေးအတွက် ကောင်းမွန်သော ပရိုဂရမ်းမင်းဘာသာရပ် memory safe programming language ကို အသုံးပြုသည့်အပြင် လုံခြုံရေးအဆင့်မြင့်သော ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်မှု၏ လုပ်ထုံးလုပ်နည်းသက်တမ်း rigorous software development life cycle (SDLC) စီမံခြင်းနှင့် hardware-backed cryptographic key managementကို အသုံးပြုခြင်း ဖြစ်ပါသည်။

Applications များသည် ဆိုက်ဘာ လုံခြုံရေးနှင့်ဆက်စပ်သော **application features** များကို အထောက်အကူပြုဖို့ လိုအပ်ပါသည်။ ထို features များကို တခါတရံ "capabilities" ဟု ခေါ်ပြီး ထိုအရာများသည် ပစ္စည်း သို့ ဝန်ဆောင်မှု၏ လုပ်ဆောင်ချက်များကို သက်တမ်းတိုးမှုဖြစ်စေပြီး ၎င်းတို့သည် ဝယ်လူသုံးစွဲသူ၏ လုံခြုံရေးကို ထိန်းသိမ်းရန် သို့မဟုတ် လုံခြုံရေး အနေအထားကို တိုးမြင့်မှု ဖြစ်စေနိုင်ပါသည်။

လုံခြုံရေးဆိုင်ရာ features နမူနာထဲတွင် ကွန်ယက်အားလုံးအတွက် transport layer security (TLS) ဆက်သွယ်မှု၊ တစ်ကြိမ်လော့အင်ဝင်ခြင်း single sing on (SSO) ပံ့ပိုးမှု၊ အသုံးပြုသူများအတွက် အချက်အလက်အမျိုးမျိုး မှန်ကန်ကြောင်း အထောက်အထားပြပြီးမှ ဝင်နိုင်သည့် multi-factor authentication (MFA) ပံ့ပိုးမှု၊ security event audit logging၊ role-based access control (RBAC)နှင့် attribute-based access control (ABAC) တို့ ဖြစ်ပါသည်။

တချို့သော ပစ္စည်းများ၏ ရုပ်ပြင်လက္ခဏာများသည် ပြောင်းလဲမှုလုပ်နိုင်ပြီး ဝယ်ယူသုံးစွဲသူများအား လက်ရှိ ရှိနေသော ပတ်ဝန်းကျင်အနေအထားနဲ့ အလုပ်စီးဆင်းမှုကို အခြားသော ပစ္စည်းများနှင့် ပေါင်းစည်းလျင်လည်းသဟဇာတမှု ဖြစ်စေနိုင်ပါသည်။ ထိုပြောင်းလဲချက်များ လုပ်ဆောင်ခြင်းဟု ဆိုရာတွင် ဝယ်ယူသုံးစွဲသူဖက်မှ အပြောင်းအလဲမလုပ်မခြင်းapplications များတွင် **default settings** ရှိရမည်ဖြစ်သည်။ ထို default settings များကို "ပြင်ပနေရာတွင်" လုံခြုံစွာ ထားရှိရမည်ဖြစ်ပြီး ထိုမှသာလျင် ဝယ်ယူသုံးစွဲသူများအနေဖြင့် ၎င်းတို့၏ စက်မှုပစ္စည်းများကို ပိုမိုလုံခြုံစွာ လုပ်ဆောင်ရာတွင် အရင်းအမြစ်များကို အနည်းငယ်သာ သုံးစွဲရတာမျိုး ဖြစ်စေနိုင်ပါသည်။

၎င်း အခြေခံသဘောတရားများဖြစ်ကြသော application hardening, application security features နှင့် application default settings တို့သည် အက်ပလီကေးရှင်းများ၏ လုံခြုံရေးအတွက် အရေးကြီးသော အခန်းကဏ္ဍတွင် ပါဝင်သကဲ့သို့ ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေး အနေအထားအတွက်လည်း အရေးပါပါသည်။ ဆော့ဖ်ဝဲ ထုတ်လုပ်သူများအနေဖြင့် ၎င်းအခြေခံ သဘောတရား တစ်ခုခြင်းစီအတွက် ထည့်သွင်းစဉ်းစားမှုလုပ်ပြီး တစ်ခုနှင့်တစ်ခု ဆက်စပ်မှုကိုလည်း နှလုံးသွင်းသင့်ပါသည်။ ထုတ်လုပ်သူများအနေဖြင့် ထိုအခြေခံ သဘောတရားများကို ၎င်းတို့ ထုတ်လုပ်မည့် ကုန်ပစ္စည်းများထဲတွင် ထည့်သွင်းဖို့အတွက် ရင်းနှီးမြုပ်နှံရန်အတွက်ထက်မက စဉ်းစားမှု လုပ်သင့်ပါသည်။ ထုတ်လုပ်သူများအနေဖြင့် ခြေလှမ်းတစ်လှမ်းဆုတ်ပြီး ထိုအခြေခံ သဘောတရားများအားဖြင့် လက်တွေ့ဘဝတွင် ဝယ်ယူသုံးစွဲသူများ ကြုံတွေ့နေရသည့် လုံခြုံရေးအနေအထား အဆိုးအကောင်းများကို ထည့်တွက်ပြီး သေခြာ ဆန်းစစ်တွေးတောမှု လုပ်သင့်ပါသည်။

ထုတ်လုပ်သူများသည် ၎င်းတို့၏ အားသွန်ခွန်စိုက်မှုနှင့် ရင်းနှီးမြုပ်နှံမှုကို တိုင်းတာခြင်းထက် ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးကို တာဝန်ယူသင့်ပါသည်။ ကုန်ထုတ်လုပ်ရာတွင် လုံခြုံရေးတိုက်ခိုက်ခံရမှု ဖြစ်နိုင်ခြေနည်းပါးအောင် လုပ်ဆောင်ရာတွင် အောက်ခြေမှ အထက်ဆီသို့ ဦးတည်သောနည်းဖြင့် တာဝန်ယူမှု ရှိသင့်ပါသည်။

သို့သော်လည်း လက်ရှိအနေအထားမှာ ထိုကဲ့သို့ တာဝန်ယူခြင်း မရှိသေးပါ။ ကုန်ထုတ်လုပ်သူအများအပြားသည် ကောင်းမွန်ပြည့်စုံသော **application hardening တွင် ရင်းနှီးမြုပ်နှံမည့်အစား လုံခြုံရေး၏ ဝန်ထုတ်ဝန်ပိုးများကို ဝယ်ယူသုံးစွဲသူများအား ထမ်းပိုးခိုင်းလျက်ရှိပါသည်။** ဥပမာ - လုံခြုံရေး အားနည်းချက်တစ်ခုအား ထုတ်လုပ်သူမှ ဖာထေးရန် လုပ်ဆောင်ချိန်တွင် ဆင်တူသော အားနည်းချက်တစ်ခု ဖြစ်ပေါ်လေ့ရှိပြီး အကြောင်းရင်းမှာ ပြဿနာအရင်းအမြစ်အား ဖြေရှင်းမည့်အစား ဖြစ်ပေါ်လာသည့် အပေါ်ယံ လက္ခဏာကိုသာ ကုစားသည့်အတွက် ဖြစ်ပါသည်။ တူညီသော အားနည်းချက်ရှိသည့် ပစ္စည်းကို မတူညီသည့် ကုဒ်ကို အခြေခံသည့် အစိတ်အပိုင်းများ ထည့်သွင်းအသုံးပြုနိုင်ပါသည်။ ဥပမာ - အားနည်းချက် တစ်ခုအား ထုတ်လုပ်သူဖက်မှ ပြုပြင်လိုက်သည့်အခါတွင် သုသေသနပြုသူ သို့မဟုတ် တိုက်ခိုက်သူဖက်က ပစ္စည်းသန့်စင်မှု မဖြစ်စေသည့် ကုဒ်၏ လမ်းကြောင်းကို ရှာဖွေတွေ့ရှိနိုင်ပါသည်။ ပစ္စည်းထုတ်လုပ်သူမှ ပြဿနာအရင်းအမြစ်ဖြစ်သော အားနည်းချက်များကို စုပေါင်းမပြုပြင်ပဲ ပေါ်လာသည့် ပြဿနာ တစ်ခုပြီးမှ တစ်ခုပြုပြင်ခြင်းမျိုး လုပ်သည့်အတွက် ဖြစ်ပါသည်။

**Application features** သည် ဝယ်ယူသုံးစွဲသူများအတွက် အကျိုးကျေးဇူးရစေနိုင်သကဲ့သို့ အန္တရာယ်လည်း ဖြစ်စေနိုင်ပါသည်။ တခြားသော ပြင်ပစနစ်အပြင် အခြားသောပုံစံများနှင့် ပူးပေါင်းရန် သဟဇာတဖြစ်စေသည့် features များသည် ကုန်ပစ္စည်း၏ တန်ဖိုးကို များစွာ တိုးမြင့်စေပါသည်။ သို့သော် ကန့်သတ်ချက်မရှိသည့် features များ - ဥပမာ ကွန်ယက်ပရိုတိုကော လိုအရာများကို သုံးစွဲသူဖက်မှ သေခြာ နားလည်သဘောပေါက်မှု မရှိပဲ ထို feature ကို ဆက်လက် အသုံးပြုပါက တိုက်ခိုက်ခံရရန် အားနည်းချက် ဖြစ်စေနိုင်ပါသည်။ ဥပမာ - အချို့သော ကုန်ပစ္စည်းများသည် ၁၉၉၀ ပြည့်နှစ် သို့မဟုတ် ၂၀၀၀ ပြည့်နှစ် ဝန်းကျင်တွင် စတင်သည့် ကွန်ယက်ဆိုင်ရာ ပရိုတိုကောများကို ဆက်လက် အသုံးပြုနေပြီး ထိုပရိုတိုကောများသည် လုံခြုံဘေးကင်းမှု မရှိကြောင်း သိရပါသည်။ သုံးစွဲသူများ လျင်မြန်စွာ upgrade လုပ်ရန်နှင့် ခေတ်သစ် လုံခြုံရေး အနေအထားကို အသုံးပြုပြီး လုပ်ခြုံရေးမော်ဒန်ကို အသုံးပြုပြီး မည်ကဲ့သို့ သေခြာ ဆန်းစစ်အချိန်ယူပြီးမှ လုပ်ဆောင်သင့်သည်ဆိုသည့် အခြေခံ အကြောင်းအရာများ ရှိပါသည်။ ၎င်းသည် ပစ္စည်းများအား အဖွဲ့အစည်း၏ အခြားသော ကွန်ယက်များနှင့် သဟဇာတဖြစ်ရန် လုပ်ဆောင်နိုင်သော်လည်း ခေတ်သစ် လုံခြုံရေးနည်းပညာ အသုံးပြုမှုနည်းပါးသည့်အတွက် အိုင်တီအသင်းသားများအား ခေတ်နှင့်အညီ မဆောင်ရွက်နိုင်ရန် ဟန့်တားမှု ဖြစ်စေနိုင်သည်။ ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် ၎င်း အခြေခံအကြောင်းအရာများကို ၎င်းတို့၏ အစီအစဉ်လုပ်ငန်းစဉ်တွင် ထည့်သွင်းပြီး ဝယ်ယူသုံးစွဲသူများလည်း သိနားလည်ရန် တိုက်တွန်းမှု ပြုလုပ်နိုင်ပါသည်။

**Application default settings** ဆိုသည်မှာ သုံးစွဲသူများအတွက် ဖြစ်နိုင်ခြေရှိသည့် အန္တရာယ်များကို ထပ်မံဖြည့်စွက်စေသည့်အရာ ဖြစ်ပါသည်။ ထုတ်လုပ်သူများသည် ဝယ်ယူသုံးစွဲသူများ လိုချင်သည့် features များကို အသုံးပြုရ လွယ်ကူရန် တချို့သော default settings များကို ရွေးချယ်ထားရှိပေးပါသည်။ ဤကဲ့သို့ လုပ်ဆောင်ခြင်း၏ အားနည်းချက်မှာ ထို အလိုအလျောက်ပါရှိသည့် default features နှင့် protocol များကို မလိုအပ်သည့် ဝယ်ယူသုံးစွဲသူများအား တိုက်ခိုက်ခံရနိုင်ခြေ ပိုများစေခြင်း ဖြစ်ပါသည်။ ထို့အပြင် လုံခြုံရေးထိန်းချုပ်သည့်အရာသည် default ၏ ကန့်သတ်ချုပ်နှောင်မှုဖြစ်ခြင်း သို့မဟုတ် ဝယ်ယူသုံးစွဲသူများသည် လုံခြုံရေး တိုးမြင့်ရန်အတွက် အချိန်ယူလေ့လာပြီးမှ လိုအပ်သည်များကို ရရှိရန် setting တွင် အပြောင်းအလဲ လုပ်ရလေ့ရှိပါသည်။ Explicit treat modeling ဆိုသည်မှာ မည်သည့် feature အတွက် အလိုအလျောက် လုံခြုံနေခြင်း by default ကို သုံးမလား သို့မဟုတ် လုံခြုံမှုရှိအောင် စီမံလုပ်ဆောင်ခြင်း secure by default ကို သုံးမလား ဟူသည့် ဆုံးဖြတ်ချက်ချရာတွင် အသုံးပြုသည့် နည်းဗျူဟာ ဖြစ်ပါသည်။ တခြားသော နည်းဗျူဟာမှာ စီမံခန့်ခွဲသူများအား feature များကို ပိုမို ရှာဖွေရ လွယ်ကူအောင် လုပ်ဆောင်ခြင်း ဖြစ်ပါသည်။

တချို့သော ထုတ်လုပ်သူများသည် ဝယ်ယူသုံးစွဲသူတချို့ သို့မဟုတ် ဝယ်ယူသူအားလုံး၏ လုံခြုံရေးကို အလိုအလျောက် ထိခိုက်စေနိုင်သည့် ပစ္စည်းများအား တင်ပို့ရောင်းချမှုမျိုး ရှိပါသည်။ ပိုမိုလုံခြုံသည့် default များအစား **hardening guide တင်းကြပ်ခြင်းလမ်းညွှန်** ကို အသုံးပြုပြီး ထိုနည်းမှာ ဝယ်ယူသုံးစွဲသူများဖက်မှ လုံခြုံရေးအတွက် အကုန်ကျခံပြီး အသုံးပြုနိုင်ခြင်း ဖြစ်ပါသည်။ ထိုတင်းကြပ်ခြင်းလမ်းညွှန်သည် ဖြစ်လေ့ဖြစ်ထရှိသော ပြဿနာများကို ကြိုရလေ့ရှိပါသည်။ တချို့သော တင်းကြပ်ခြင်း လမ်းညွှန်များသည် ရှာဖွေရခက်ခဲပြီး ကောင်းမွန်စွာ ပံ့ပိုးမှု လုပ်ထားခြင်းလည်း မရှိပါ။ တချို့သော တင်းကြပ်ခြင်းလမ်းညွှန်မှာ အသုံးပြုရန် ရှုတ်ထွေပြီး တခါတရံ ဆော့ဖ်ဝဲ ထုတ်လုပ်သူအား module ကို သက်တမ်းတိုးပေးဖို့ လုပ်ဆောင်ခိုင်းတာမျိုး ဖြစ်စေပါသည်။ တချို့သူများက ဖတ်ရှုသူသည် ဆိုက်ဘာလုံခြုံရေးနှင့် ပတ်သက်လာလျင် အတွေ့အကြုံရှိ၍ မတူညီသော တိုက်ခိုက်နိုင်ခြေများကို နားလည်းသဘောပေါက်သူဟု ယူဆကြပါသည်။ ဆိုက်ဘာ တိုက်ခိုက်ရေးသမားများ၏ လှုပ်ရှားမှု နည်းလမ်းများကို ကောင်းမွန်စွာ နားမလည်သည့် ကွန်ပြူတာသမားများသည် တင်းကြပ်ခြင်းလမ်းညွှန်hardening guide ကို ကောင်းမွန်စွာ အသုံးပြုမှု မလုပ်တာမျိုး ဖြစ်စေနိုင်ပြီး အထူးသဖြင့် အကြိုပြုသတ်မှတ်ချက်အတိုင်း မလုပ်ဆောင်ပါက တိုက်ခိုက်ခံရနိုင်ခြေများသည် စသည့် သတိပေးချက်ဖြင့် ညွှန်ကြားချက်အား ရှင်းလင်းစွာ မဖော်ပြထားခြင်းမျိုး ဖြစ်ပါသည်။ ထို့အပြင် တင်းကြပ်ခြင်းလမ်းညွှန်ချက် အားလုံးကို လုံခြုံရေးတိုက်ခိုက်သူများ၏ နည်းဗျူဟာနှင့် ၎င်းတို့၏ စီးပွားရေးများနှင့် သက်ရောက်မှုများကို ရင်းနှီးသည့်အင်ဂျင်နီယာများက ရေးသားခြင်းမဟုတ်သောကြောင့် တင်းကြပ်ခြင်းလမ်းညွှန်ချက်များအတိုင်း လိုက်နာလုပ်ဆောင်သည့်တိုင် ထိရောက်မှု မရှိတာမျိုး ဖြစ်နိုင်ပါသည်။ သန်းနှင့်ချီသော ဝယ်ယူသုံးစွဲသူများသည် ဆော့ဖ်ဝဲလုံခြုံရေး သို့မဟုတ် စနစ်လုံခြုံရေးအတွက် တစ်ခုတည်းမကသော အရာများအတွက် တာဝန်ယူနေရပြီး အများအားဖြင့် အရင်းအမြစ် လုံလောက်စွာ မရှိသည့် ပတ်ဝန်းကျင်အနေအထားတွင် လုပ်ဆောင်ရပါသည်။ တင်းကြပ်ခြင်း လမ်းညွှန်မှုအပေါ် မှီခိုခြင်းမျိုး မလုပ်သင့်ပါ။

Application ၏ setting ကို အမြဲတမ်း ဆန်းစစ်မှုလုပ်သင့်ပြီး ကုန်ထုတ်လုပ်သူများသည်လည်း လက်ရှိကြုံတွေ့နေရသည့် ခြိမ်းခြောက်မှုအနေအထားကိုကြည့်၍ setting ကို default ထားလို့ဖြစ်သလား သို့မဟုတ် ကုန်ထုတ်လုပ်သူ၏ လုံခြုံရေးအကြိုပြုချက်ကို မလိုက်နာပဲ ဝယ်ယူသုံးစွဲသူများက setting ပြောင်းလိုက်သလား ဆိုတာကို ဆန်းစစ်မှုလုပ်သင့်ပါသည်။ Application ပါ setting များကြောင့် ဖြစ်ပေါ်လာနိုင်သည့် အန္တရာယ်ညွှန်းကိန်း အချက်ပြစနစ်indicator ကိုလည်း ရှင်းလင်းစွာ ထားရှိသင့်ပြီး ထိုအချက်ပြညွှန်းကိန်းများကိုလည်း လူအများသိနိုင်စေရန် လုပ်ဆောင်သင့်ပါသည်။ ခေတ်မှီကားတွင် ကားထိုင်ခုံခါးပတ်နှင့်ဆိုင်သည့် အချက်ပြညွှန်းကိန်းကို ဖော်ပြပြီး ခါးပတ်မပတ်ထားပါက သတိပေးသံ ထွက်ပေါ်လာအောင် လုပ်ဆောင်ထားသကဲ့သို့ ဆော့ဖ်ဝဲ ထုတ်လုပ်ရာတွင်လည်း လုံခြုံရေးစနစ်၏ အချက်ပြညွှန်းကိန်းကိုပါ ထည့်သွင်းသင့်ပါသည်။ Application ၏ ပြောင်းလဲမှုတွင် တာဝန်ရှိသူအကောင့်အတွက် MFA ရှိရန်မလိုအပ်ပါက ထိုကဲ့သို့ MFA စနစ် မရှိခြင်းကြောင့် တာဝန်ရှိသူနှင့် ၎င်းတို့၏ အဖွဲ့အစည်း တစ်ခုလုံးအတွက် လုံခြုံရေးအန္တရာယ် ရှိနိုင်ကြောင်း သတိပေးချက်မျိုးလည်း ထားရှိသင့်ပါသည်။ ထို့အပြင် အကယ်၍ application ၏ ပြောင်းလဲမှုတွင် လျို့ဝှက်မှု အားနည်းသည့် ပရိုတိုကော အဟောင်းများနှင့် တွဲ၍ အသုံးပြုနိုင်ပါက အန္တရာယ်ရှိကြောင်း တာဝန်ရှိသူများနှင့် အဖွဲ့အစည်းကို သတိပေး၍ ထိုအန္တရာယ်များကို ကာကွယ်နိုင်မည့် နည်းလမ်းများ အချက်အလက်များကို သိအောင် လုပ်သင့်ပါသည်။ ထုတ်လုပ်သူများအား တိုက်တွန်းလိုသည်မှာ တာဝန်ရှိသူ၏ အချိန်ရှိမှုနှင့် ကျွမ်းကျင်မှုအပြင် တင်းကြပ်ခြင်းလမ်းညွှန်ချက်များအပေါ် မှီခိုခြင်းထက် မိမိ၏ ပစ္စည်းများအား ပုံမှန် စမ်းသပ်ပြုပြင်မှုများ ပြုလုပ်သင့်ပြီး တပါတည်း အလိုအလျောက် လုံခြုံရေးထည့်သွင်းသည့်နည်းကို အသုံးပြုရန် တိုက်တွန်းပါသည်။ လုံခြုံရေးနှင့် အသုံးပြုခြင်းဆိုင်ရာ ဟန်ချက်ညီရေးတွင် တီထွင်ကြံဆမှုအတွက် အခွင့်အလမ်းများရှိသည်မှာ ထင်ရှားလှပါသည်။

အပေါ်တွင် ဖော်ပြသည့် အခြေခံသဘောတရား တစ်ခုစီတိုင်းတွင် ခုခံကာကွယ်ခြင်းဌာ မစွမ်းသည့် အနေအထားများ ဖြစ်စေနိုင်ပြီး ဝယ်ယူသုံးစွဲသူများမှ လေ့လာမှုလုပ်ရန် လိုအပ်ခြင်း၊ ကုန်ကျခံရခြင်း၊ ဝယ်ယူရခြင်းနှင့် အလုပ်သမားများ ခန့်အပ်ခြင်း၊ အသုံးပြုရန် ရောင်းချပို့ဆောင်ခြင်းနှင့် **လုံခြုံရေးပစ္စည်းများ (security product)** အား စောင့်ကြပ်မှုမျိုးလုပ်ရန် လိုအပ်ပြီး ထိုမှသာလျင် လုံခြုံရေးချိုးဖောက်ခံရမှုကို လျော့ချနိုင်မည် ဖြစ်ပါသည်။ အထွေထွေအားဖြင့် အသေးစားနှင့် အလတ်စား အဖွဲ့အစည်းများ(SMOs)သည် ထိုရွေးချယ်မှုများကို အကောင်အထည်ဖော်လုပ်ဆောင်နိုင်စွမ်းမရှိပါ။ ၎င်းတို့အနေဖြင့် ကျွမ်းကျင်သူ ရှားပါးမှု၊ ရံပုံငွေ မလုံလောက်မှုနှင့် အချက်အလက်သယ်ယူပို့ဆောင်နိုင်စွမ်းအား bandwidth နှင့် ၎င်း၏ ဆောင်ရွက်နိုင်မှုအတွက် အချိန်ပေး လုပ်ဆောင်နိုင်စွမ်း မရှိခြင်းတို့ကြောင့် လုံခြုံရေးကို ဦးစားမပေးနိုင်သည့် အနေအထား ရောက်စေပြီး အန္တရယ်ကို စုပေါင်းခံရနိုင်ခြေ များစေပါသည်။ တခြားတဖက်တွင် လုံခြုံရေးအပေါ် ရင်းနှီးမြှုပ်နှံသည့် တချို့သော ကုန်ထုတ်လုပ်သူများကြောင့် စကေးညီမျှ စေနိုင်ပါသည်။ ပြဿနာအား အတိုချုပ်ရမည်ဆိုလျင် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်ရာတွင် ပိုမို လုံခြုံဘေးကင်းသည့် ပစ္စည်းများ ထုတ်လုပ်ရန် လိုအပ်ပြီး လုံခြုံရေးရရှိရန်အတွက် ထုတ်လုပ်သောပစ္စည်းများ မလိုအပ်ပါ။ ပြုပြင်ပြောင်းလဲရေးကို ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများက ဦးဆောင်ဦးရွက်မှု ပြုသင့်ပါသည်။

> ***ဆော့ဖ်ဝဲလုပ်ငန်းအနေဖြင့် ပိုမိုလုံခြုံဘေးကင်းသည့် ကုန်ပစ္စည်းများ ထုတ်လုပ်ရန်လိုအပ်ပြီး လုံခြုံရေးရရှိရန်အတွက် ထုတ်လုပ်သော ပစ္စည်းများ မလိုအပ်ပါ။ ပြုပြင်ပြောင်းလဲရေးတွင် ဆော့ဖ်ဝဲကုန် ထုတ်လုပ်သူများက ဦးဆောင်ဦးရွက်မှု ပြုသင့်ပါသည်။***

ယနေ့တွင် တခါတရံ ကျွန်ုပ်တို့အနေဖြင့် ကုန်ထုတ်လုပ်သူများထံမှ မှတ်ချက်များ ဖတ်ရပြီး ၎င်းတို့၏ ရှင်းပြချက်အရ ဝယ်ယူသူသည် လုံခြုံရေးဆိုင်ရာ feature တခုခု သို့မဟုတ် hardening guidance တစ်ခုကို မလိုက်နာခဲ့သည့်အတွက် လုံခြုံရေးဆိုင်ရာနှင့်ပတ်သက်ပြီး အပေးအယူလုပ်ရသည့် အနေအထားရောက်သွားရသည်ဟု အကြောင်းပြ ပြောဆိုတတ်ကြပါသည်။ ထိုကဲ့သို့ အကြောင်းပြမည့်အစား အချက်အလက်များ ခိုးယူတိုက်ခိုက်ခံရပြီးသည့်နောက်ပိုင်းတွင် ကုန်ထုတ်လုပ်သူဖက်မှ မည်ကဲ့သို့ လုပ်ဆောင်ပါက ထိုလုံခြုံရေးဆိုင်ရာ feature သို့မဟုတ် ထို hardening guidance အား တိုက်ခိုက်ခံရမည့် အနေအထား မရောက်ရှိအောင် ကာကွယ်နိုင်မည့်အကြောင်း ရှင်းပြောဆိုသင့်ပြီး ဝယ်ယူသုံးစွဲသူဖက်မှ ကုန်ကျခံစရာမလိုပဲ အလိုအလျောက် လုံခြုံမှုရှိအောင် လုပ်ဆောင်ပေးသင့်ပါသည်။ ထိုကိစ္စများတွင် ကုန်ပစ္စည်းများသည် ဒီဇိုင်းဆွဲစဉ်နှင့် အကောင်အထည်ဖော်စဉ်တွင် လုံခြုံရေးတင်းကြပ်မှုကို လုံလောက်စွာ ထည့်သွင်းခြင်းမရှိခြင်းကြောင့် ဖြစ်ရသည့်အတွက် ကုန်ထုတ်လုပ်သူများအနေဖြင့် ထိုကဲ့သို့ လုံခြုံရေး အားနည်းချက်များ မဖြစ်စေရန် မည်ကဲ့သို့ ပြောင်းလဲလုပ်ဆောင်နေသည့်အကြောင်း ရှင်းပြပြောဆိုသင့်ပါသည်။

ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနေဖြင့် ၎င်းတို့၏ ကုန်ပစ္စည်းများသည် ဒီဇိုင်းရေးဆွဲချိန်နှင့် ထုတ်လုပ်ချိန်တွင် လုံခြုံရေးကို ထိပ်ဆုံးမှ ဦးစားပေးထားသည် ဆိုသည့် အနေအထားဖြင့် ထုတ်လုပ်ရန် တာဝန်ရှိပါသည်. အဆုံးတွင် ၎င်းတို့အနေဖြင့် ၎င်းတို့၏ကုန်ပစ္စည်းသည် ဆော့ဖ်ဝဲကဏ္ဍတွင် **objectively measure the results မည်သည့်အနေအထားရှိသည်ဆိုသည်ကို အရှိကို အရှိအတိုင်း သေခြာသိရှိရန်တိုင်းတာထားသည့် ရလဒ်များ ရရှိရန် လုပ်ဆောင်သင့်ပါသည်။** ကျွန်ုပ်တို့အနေဖြင့် ကုန်ထုတ်လုပ်သူများအား တိုက်တွန်းလိုသည်မှာ ၎င်းတို့၏ အတွင်းရေးကြိုးစားမှုအပေါ်သာ အာရုံစိုက်ထားခြင်း မပြုလုပ်ပဲ အရှိကို အရှိအတိုင်း သေခြာတိုင်းတာမှုလုပ်ပြီး ရရှိသည့် ရလဒ်အား ပုံမှန်အစီရင်ခံသည့်အပြင် ပစ္စည်း၏ လုံခြုံရေးထိရောက်မှု၊ ပြုပြင်ပြောင်းလဲမှု၊ အစိတ်အပိုင်းများ၏ ဖွဲ့စည်းပုံထိရောက်မှု ရလဒ်ကို တိုင်းတာခြင်းနှင့် SDLC တွင် ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးနှင့် ပိုမိုလုံခြုံသည့် ကုန်ပစ္စည်းများအား ထုတ်လုပ်နိုင်သည်အထိ အဖန်ဖန် ပြန်ကျော့စေသည့် feedback loop များ ထားရှိလုပ်ဆောင်သင့်ပါသည်။ ပညာရှင် နှင့်လုံခြုံရေးဆိုင်ရာ သုတေသနပြုသည့် အသိုင်းအဝိုင်းများ အသုံးပြုနိုင်ပြီး ပုဂ္ဂလိကဆိုင်ရာ အချက်အလက်များအား မထိခိုက်စေသည့်နည်းဖြင့် သုံးစွဲသူ အနေအထားကို တိုင်းတာသည့် ဒေတာအချက်အလက်များ အစီရင်ခံစာတွင်ပါဝင်သင့်ပါသည်။


## ဤအခြေခံ သဘောတရားများအား လက်တွေ့အကောင်အထည်ဖော်ခြင်း

ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူနှင့် အွန်လိုင်းဝန်ဆောင်မှုများသည် ထိုအခြေခံ သဘောတရားများအား အောင်မြင်စွာ လက်တွေ့အကောင်အထည်ဖော်ရန်အတွက် လုပ်ကိုင်နိုင်သည့် နည်းလမ်းများရှာဖွေသင့်ပါသည်။ ပြင်ပလူများ လေ့လာဆန်းစစ်မှုလုပ်နိုင်မည့် ပစ္စည်းများဖြင့် သက်သေပြနိုင်သင့်ပါသည်။ ကုန်ထုတ်လုပ်သူသည် ကောင်းမွန်ပြည့်စုံသည့် လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ထားသော ပစ္စည်းများ ထုတ်လုပ်နေသည်ဆိုသည့် အကြောင်းကို ပစ္စည်းတစ်ခုတည်းကသာလျင် သက်သေပြနိုင်မည်မဟုတ်သော်လည်း မတူညီသော ပစ္စည်းများဖြင့် သက်သေပြနိုင်ပါက လုံခြုံမှုရှိသော ကုန်ပစ္စည်းများကို ထုတ်လုပ်သူဖြစ်ကြောင်း ကုန်ထုတ်လုပ်သူကို မြင်သွားတာမျိုး ဖြစ်စေနိုင်ပါသည်။ ဤကဲ့သို့သော ချဉ်းကပ်နည်းသည် “အပြောနှင့်ပြောမည့်အစား လက်တွေ့နှင့်ပြသခြင်း” ဆိုသည့် အနှစ်သာရကို ဖော်ဆောင်ခြင်း ဖြစ်ပါသည်။

ထိုအခြေခံ သဘောတရားများကို အကောင်အထည်ဖော်ရန်အတွက် ကုန်ထုတ်လုပ်သူများအနေဖြင့် အောက်ပါနည်းလမ်းများကို ထည့်သွင်းစဉ်းစားသင့်ပါသည်။ အာဏာပိုင်အဖွဲ့အစည်းများအနေဖြင့် အနည်းငယ်သော ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများသည် ထိုလုပ်ထုံးလုပ်နည်းများကို ချက်ခြင်း ထည့်သွင်းအကောင်အထည်ဖော်နိုင်သည့် အနေအထားရှိပြီး ၎င်းတို့၏ လုံခြုံမှုရှိအောင် စီမံပြုလုပ်ထားသည့် ပစ္စည်းများထုတ်လုပ်ခြင်းဆိုသည့် ခရီးစဉ်အတွင်းတွင် ထိုကဲ့သို့ ထုတ်လုပ်သောကုန်ပစ္စည်းများဖြင့် စတင် လက်တွေ့ပြသနိုင်စွမ်းရှိမည်ကို သိနားလည်ထားပါသည်။ ထို့အပြင် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများသည် ဝယ်ယူသုံးစွဲသူများ၏ အသုံးပြုမှု အနေအထားအားကြည့်၍ လုံခြုံမှု အများဆုံးရရှိစေနိုင်မည့်ရလဒ်ကို ရရှိရန် ဦးစားပေးမှုများ လုပ်ကိုင်ရန် လိုအပ်ပါသည်။

# အလိုအလျောက် လုံခြုံမှုရှိသော အလေ့အကျင့်များ

1. **အလိုအလျောက် Password ထားရှိပေးချခြင်းကို မလုပ်ရန်**
အလိုအလျောက် password ထားရှိပေးခြင်းကြောင့် တိုက်ခိုက်ခံရမှုများ နှစ်စဉ် ဆက်လက်ဖြစ်ပေါ် လေ့ရှိပါသည်။ ဤရေရှည်ပြဿနာကို ဖြေရှင်းရန်အတွက် ကြိုးစားခြင်းသည် တိုက်ခိုက်မည့်သူများအား အချက်အလက်ခိုးယူမှု မလုပ်နိုင်အောင် လုပ်ဆောင်ခြင်းဖြစ်ပါသည်။ အလားတူစွာ ကုန်ထုတ်လုပ်သူများအနေဖြင့် မည်သည့် password လုပ်ထုံးလုပ်နည်းကို ထည့်သွင်းသင့်သည်ဆိုသည်ကို စဉ်းစားသင့်ပါသည်။ ဥပမာ password ၏ အနည်းဆုံး အလုံးရေ၏ အရည်အတွက် မည်မျှရှိသင့်ဆိုသည့် သတ်မှတ်ချက် ထားရှိခြင်းနှင့် တိုက်ခိုက်မှုများတွင် အသုံးပြုလေ့ရှိသည့် password များအား အသုံးပြုခွင့်မပေးခြင်းမျိုး လုပ်ရန် စဉ်းစားသင့်ပါသည်။

2. **ထိန်းချုပ်သည့် အနေအထားမဟုတ်ပဲ တကယ့်ပြင်ပ အနေအထား အပေါ် အခြေခံပြီး စမ်းသပ်ဆန်းစစ်မှုများ လုပ်ရန်** စက်မှုနည်းပညာ ထွန်းကားလာသည်နှင့်အမျှ ပိုပြီး ရှုတ်ထွေးမှုလည်း ဖြစ်လာသည့်အတွက် ဆောဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် ဝယ်ယူသူများ၏ လုံခြုံရေးနဲ့ပတ်သက်၍ သုံးစွဲမှုပုံစံကို အခြေခံသည့် စမ်းသပ်မှုမျိုးလုပ်ရန် အရေးကြီးပြီး ထိုကဲ့သို့ လုပ်ဆောင်ခြင်းမှာ ၎င်းတို့ပစ္စည်း၏ လုံခြုံရေးအနေအထားသည် ပြင်ပတွင် မည်သည့်အနေအထားရှိသည်ကို သိစေနိုင်ပါသည်။ အလားတူစွာ သုံးစွဲသူများအပေါ် ပြုလုပ်သည့် သုတေသနသည် ဆော့ဖ်ဝဲထုတ်လုပ်ရာတွင် လိုအပ်သည့်အရာများကို သိစေနိုင်သည့်အတွက် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနေဖြင့် user experience (UX) လုံခြုံရေးဆိုင်ရာ အသုံးပြုမှုအတွေ့အကြုံများအားနည်းသည့်အခါ လုံခြုံရေးကို ဦးတည်ထားသည့် အသုံးပြုမှုသုတေသနကို လုပ်သင့်ပါသည်။ ဝယ်ယူသုံးစွဲသူများအနေဖြင့် တကယ့်ပြင်ပတွင် ပစ္စည်းများကို မည်ကဲ့သို့ အသုံးပြုနေသည်ကို စောင့်ကြည့်ခြင်းအားဖြင့် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် ၎င်းတို့ပစ္စည်း၏ လုံခြုံရေးအနေအထားထိရောက်မှုနှင့် ထိန်းချုပ်နိုင်မှုများကို သိစေနိုင်သည့်အတွက် အရေးပါသော ထဲထဲဝင်ဝင် ဖြစ်သော အချက်အလက်များကို ရရှိစေနိုင်ပါသည်။ ထိုကဲ့သို့ အချက်အလက်များမှတဆင့် မည်သည့်နေရာတွင် တိုးတက်မှုလုပ်သင့်သနည်း သို့မဟုတ် ပြုပြင်မွမ်းမံမှု လုပ်သင့်သနည်းဆိုသည်ကို သိစေနိုင်ပြီး ဝယ်ယူသုံးစွဲသူများ လိုအပ်သည့် လုံခြုံမှုရှိသော ကုန်ပစ္စည်းများကို ထုတ်လုပ်နိုင်မည်ဖြစ်သည်။ ဥပမာ - ပြင်ပကမ္ဘာအနေအထားကို လက်တွေ့လေ့လာဆန်းစစ်မှုမှတဆင့် UX ၏ အနေအထားကို ပြောင်းလဲရန်၊ defaults ၊ သတိပေးချက်နှင့် စောင့်ကြည့်နိုင်မှုအနေအထားများကို ပြောင်းလဲမှုလုပ်ရန် လိုအပ်ကြောင်း တွေ့ရှိနိုင်ပါသည်။ ပြင်ပကမ္ဘာအနေအထားကို လက်တွေ့လေ့လာဆန်းစစ်မှုမှတဆင့် ပစ္စည်းဒီဇိုင်း၏ လုံခြုံရေးဆိုင်ရာ ဖာထေးမှု အလျင်နှုန်းအား တိုးတက်မှုလုပ်ရန်၊ ပြုပြင်ပြောင်းလဲရေးတွင် အမှားနည်းအောင် လုပ်ဆောင်ရန်နှင့် တိုက်ခိုက်မှုဖြစ်စေနိုင်မှု မျက်နှာပြင်ကို လျော့ချခြင်း စသည့် တိုးတက်မှုများလည်း ဆောင်ရွက်နိုင်ပါသည်။

## ကုန်ထုတ်လုပ်သူများအနေဖြင့် အောက်ပါအချက်များကို စဉ်းစားသင့်ပါသည်။

- ဝယ်ယူသုံးစွဲသူများသည် hardening guide တင်းကြပ်ခြင်း လမ်းညွှန်များကို မှန်ကန်စွာ လိုက်နာကျင့်သုံးခြင်း ရှိပါသလား။
- လက်တွေ့တွင် ကုန်ပစ္စည်း၏ လုံခြုံရေး အစိတ်အပိုင်းများက မျှော်လင့်ထားသကဲ့သို့ ဆောင်ရွက်မှု ရှိပါသလား။
- လုံခြုံရေး အစိတ်အပိုင်းများက ပြင်ပ၏ တိုက်ခိုက်မှုများကို ခုခံနိုင်စွမ်းရှိပါသလား။
- အချက်အလက်များ ခိုးယူထိန်းချုပ်ခံရမှုများ မဖြစ်စေရန် မည်သည့် အစိတ်အပိုင်းက ဆောင်ရွက်ပေးနိုင်သနည်း စသည့် အချက်များ စဉ်းစားသင့်ပါသည်။

*သတိပြုရန် - ဤအခြေခံသဘောတရားများကို ကောင်းမွန်စွာ နားလည်သိရှိရန်အတွက် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနေဖြင့် ဝယ်ယူသုံးစွဲသူများနှင့် ပါတနာဖွဲ့၍ တိုက်ခိုက်မှုကို ခံနိုင်ရည်ရှိမရှိ သိနိုင်ရန် red team exercise ဟု ခေါ်သည့် ထုတ်လုပ်သူများမှ တိုက်ခိုက်သူများလို ဟန်ဆောင်ပြီး လုံခြုံရေးကို စမ်းသပ်ခြင်းနည်းများ လုပ်နိုင်ပါသည်။ ထိုကဲ့သို့ လက်တွေ့စမ်းသပ်မှုများသည် ဝယ်ယူသုံးစွဲသူများ၏ နေရာတွင် ပြုလုပ်နိုင်သကဲ့သို့ အွန်လိုင်းမှတဆင့် ပြုလုပ်နိုင်သည့်အပြင် ကိုယ်ရေးအချက်အလက်ကို အကာကွယ်ပေးထားသည့် အက်ပလီကေးရှင်းမှတဆင့်အချက်အလက် ထုတ်လွှင့်ချက်များအား မှတ်တမ်းယူသည့် telemetry နည်းအား အသုံးပြု၍ စမ်းသပ်နိုင်ပါသည်။*

3. **တင်းကြပ်မှုအရွယ်အစားအား ဖြေလျှော့ခြင်း** ကုန်ထုတ်လုပ်သူများအနေဖြင့် ဝယ်ယူသုံးစွဲသူ၏ လုံခြုံရေး ပိုမို ခိုင်လုံစေရန်အတွက် streamlining ပြုလုပ်ခြင်း သို့မဟုတ် ပစ္စည်း၏ hardening guide များကို ဖယ်ရှားခြင်းများ ပြုလုပ်နိုင်သည့်အပြင် ကုန်ပစ္စည်းများ ပို့ဆောင်ရောင်းချမှုမလုပ်ခင်အရေးအကြီးဆုံးသော လုံခြုံရေးဆိုင်ရာ လုပ်ဆောင်ချက်များအပေါ် အာရုံစိုက်လုပ်ဆောင်နိုင်ပါသည်။ ဝယ်ယူသုံးစွဲသူများအား လုံခြုံသည့် အနေအထားရောက်ရှိရန်အတွက် လုပ်စရာ တစ်ခုပြီးတစ်ခု လုပ်ဆောင်ခိုင်းပြီး စိတ်ကသိကအောက် ဖြစ်စေမယ့်အစား၊ ကုန်ထုတ်လုပ်သူများအနေဖြင့် ထိပ်ဆုံးမှ လုံခြုံရေး ခြိမ်းခြောက်မှု အန္တရာယ်အား သိအောင်လုပ်ပြီး ထိုအန္တရာယ်များကို ရှောင်ရှားရန်အတွက် မည်ကဲ့သို့ လုပ်ဆောင်နိုင်သည် ဆိုသည့် လမ်းညွှန်ချက်များကို ထားရှိပေးသင့်ပါသည်။ ထို့အပြင် ကုန်ထုတ်လုပ်သူများအနေဖြင့် ဝယ်ယူစားသုံးသူများအား လုံခြုံရေးထိန်းချုပ်မှုအတွက် လိုအပ်သည့် ပစ္စည်းများ ထားရှိပေးခြင်းမျိုးလုပ်သင့်သလို ထိုလုံခြုံရေးထိန်းချုပ်မှုများအား ထည့်သွင်းအသုံးပြုရာတွင် လွယ်ကူရှင်းလင်းမှုရှိအောင် အလိုအလျောက် လုပ်ဆောင်ပေးခြင်းမျိုးလည်း လုပ်ဆောင်ပေးသင့်ပါသည်။ ဥပမာ ဝယ်ယူသုံးစွဲသူများ၏ အနေအထားတွင် လွယ်ကူစွာ ထည့်သွင်းအသုံးပြုနိုင်ရန်အတွက် အညွှန်းများကို လွယ်ကူစွာ ရေးသားထားခြင်းမျိုး ဖြစ်ပါသည်။ ထို အရာများက မူလထုတ်ဝေခြင်းမှ သွေဖြီပြီး အပြောင်းအလဲများ လုပ်ခြင်းကို မှတ်မိပြီး အတည်ပြုပေးတာမျိုးကို လုပ်ဆောင်ပေးသင့်ပါသည်။ Hardening guides များကို ထိရောက်စွာ လုပ်ဆောင်ကာ ဝယ်ယူသုံးစွဲသူများအား အသုံးပြုရလွယ်ကူပြီး အော်တိုစနစ်ဖြစ်အောင်လုပ်ဆောင်ပေးခြင်းအားဖြင့် ကုန်ထုတ်လုပ်သူများသည် ဝယ်ယူသုံးစွဲသူများအတွက် ဝန်ထုတ်ဝန်ပိုးကို လျော့ပါးစေနိုင်ပြီး ၎င်းတို့၏ ထုတ်ကုန်များကိုလည်း လုံခြုံသည့်နည်းလမ်းဖြင့် တင်ပို့ရောင်းချနိုင်စေမည် ဖြစ်ပါသည်။ အသုံးပြုနိုင်သော နည်းဗျူဟာတစ်ခုမှာ ၈၀ – ၂၀ နိယာမဟု လူသိများတဲ့ Pareto principle ဖြစ်ပြီး ဖြစ်လေ့ဖြစ်ထရှိသည့် အရာများအတွက် (၈၀%) လျော့ချပြီး သိပ်ဖြစ်လေ့မရှိသည့် အစိတ်အပိုင်းများကို (၂၀%) လျော့ချကြည့်တာမျိုး လုပ်နိုင်ပါသည်။ ထိုနည်းလမ်းက ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအား ရိုးရှင်းသော အရာများကို ရိုး

ရှင်းစွာ ထုတ်လုပ်မှုဖြစ်စေသကဲ့သို့ ခက်ခဲသောအရာကိုလည်း ဖြစ်နိုင်ခြေ ရှိစေနိုင်ပါသည်။ Field testing (လက်တွေ့စမ်းသပ်မှု)သည် ဝယ်ယူသုံးစွဲသူများအနေဖြင့် hardening guide များကို သိရှိရန်၊ နားလည်ရန် သို့မဟုတ် အသုံးပြုရန် မည်မျှကြာမြင့်သနည်းဆိုသည်ကို တိုင်းတာရာတွင် အရေးကြီးသည့် စမ်းသပ်မှု ဖြစ်ပါသည်။ ကုန်ထုတ်လုပ်သူများ အနေဖြင့် လုပ်ပိုင်ခွင့်ရှိသူများအား hardening guide ထည့်သွင်းမှုလုပ်ရန်ကို အားကိုးနေမည့်အစား ကုန်ပစ္စည်းများက လုပ်ပိုင်ခွင့်ရှိသူများအား ထုတ်ထားသည့်ပစ္စည်းကို ပြန်လည်ဆန်းစစ်မှု ဖြစ်စေရန် တွန်းအားပေးသည့် အရာမျိုးကို ထည့်သွင်းစဉ်းစားသင့်ပါသည်။

4. **လုံခြုံမှုနောက်ခံမရှိသည့် features များကို အသုံးမပြုရန် ပြင်းထန်စွာ တိုက်တွန်းခြင်း** လုံခြုံရေးကို ဦးစားပေးရာတွင် ခေတ်သစ် feature များကိုပါ တွဲ၍အသုံးပြုခွင့်ပေးသည့် ခေတ်ဟောင်းမှ အရာများအစား ရှင်းလင်းသည့် upgrade လမ်းကြောင်းကို ရွေးချယ်ပါ။ ပိုမိုလုံခြုံသော feature နှင့် protocols များကို အသုံးပြုထားသည့်အရာများကို ဖော်ပြထားသည့် ဘလော့များတွင် ပြသထားခြင်းနှင့် လုံခြုံမှုမရှိသည့် feature များအား ဝေဖန်မှုများ လုပ်နိုင်ပြီး ဖြစ်နိုင်ပါက ထိုကုန်ပစ္စည်းအတွင်း လုံခြုံမှု အားနည်းနေသည့်အပိုင်းကို မီးမောင်းထိုးနိုင်ပါသည်။ ဝယ်ယူသုံးစွဲသူ အများအပြားက သူတို့၏ စနစ်ကို လက်ရှိမော်ဒန် ကွန်ယက်၊ identity နှင့် အခြားသော အရေးကြီးသည့် လုံခြုံရေး feature များနှင့် ကိုက်ညီအောင် လုပ်ဆောင်ထားခြင်း မရှိဘူးဆိုသည်ကို ပြသနေပါသည်။ တချို့ကိစ္စတွင် ဝယ်ယူသုံးစွဲသူများက သူတို့၏ စနစ်ကို upgrade လုပ်လိုက်ပါက လက်ရှိအသုံးပြုနေသည့်အရာများ ကောင်းမွန်စွာ အလုပ်မလုပ်မည်ကို စိုးရိမ်ကြပါသည်။ Upgrade များကို တတ်နိုင်သမျှ လွယ်ကူရှင်းလင်းစွာ လုပ်ဆောင်ထားခြင်းအားဖြင့် ဝယ်ယူသုံးစွဲသူများက upgrade လုပ်နိုင်သည့်အလားအလာ ပိုများလာနိုင်ပြီး၊ လုံခြုံရေးဆိုင်ရာများကို ပြင်ဆင်မွမ်းမံမှုပိုလုပ်ပြီး၊ ပို၍ လျင်မြန်စွာ လုပ်ဆောင်တာမျိုး ဖြစ်စေနိုင်ပါသည်။ ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများ အနေဖြင့် ဝယ်ယူသုံးစွဲသူများကို အန္တရာယ်ကို လျော့ချသည့်အနေဖြင့် upgrade များလုပ်ကြရန် တတ်အားသ၍ တိုက်တွန်းမှု ပြုသင့်ပါသည်။

5. **တပ်လှန့်မှုပြုသည့် စနစ်ကို ထည့်သွင်းခြင်း** ကားပေါ်တွင် လိုက်ပါသူမှ ခါးပတ် မတတ်ထားလျင် သတိပေးချက်ပေါ်လာသကဲ့သို့ ကုန်ထုတ်လုပ်သူများသည်လည်း သုံးစွဲသူများ၏ ပစ္စည်းများ အမှန်တကယ်လုံခြုံမှု မရှိသည့် အခြေအနေတွင် အချိန်မီနှင့် ထပ်ခါထပ်ခါ သတိပေးသည့် စနစ်များကို ထည့်သွင်းသင့်ပါသည်။ သုံးစွဲသူများသည် မလုံခြုံသော လုပ်ထုံးလုပ်နည်းများကို အသုံးပြုနေသည့်အကြောင်း ထိုအတွက်ကြောင့် upgrade လုပ်ရန် လိုအပ်ကြောင်း သတိပေးခြင်းမျိုး လုပ်ဆောင်နိုင်ပါသည်။ သုံးစွဲသူများ သို့မဟုတ် တာဝန်ရှိသူများသို့မဟုတ် အက်ပလီကေးရှင်း ပြုပြင်မွမ်းမံမှုအတွင်း လုံခြုံဘေးကင်းမှု မရှိသည့်အချိန်တွင် အချိန်မီ အကောင်အထည်ဖော်ခြင်း နှင့် ထပ်ခါသတိပေးချက်များ လုပ်ဆောင်ပါ။ လုံခြုံမှုမရှိခြင်းကို တာဝန်ရှိသူများအား ရှင်းလင်းစွာ ပုံမှန် သတိပေးပါ။ အကောင့်ထဲ ဝင်သည့်အခါတိုင်း MFA မရှိကြောင်း သတိပေးသည့် အပို feature ကို ထည့်ခြင်း သို့မဟုတ် MFA မလုပ်ပါက တချို့သော အဓိက feature များကို အလုပ်မလုပ်စေခြင်းမျိုး လုပ်နိုင်ပါသည်။ ထိုရည်မှန်းချက်များ အောင်မြင်ရန်အတွက် တီထွင်ကြံဆနိုင်ရန် အခွင့်အလမ်းများရှိပြီး သတိပေးချက်များကို လျစ်လျူရှုသည့်အနေအထားအဖြစ် ဦးဝွေ့သွားတာမျိုး မဖြစ်အောင်လည်း သတိဖြင့် ဆောင်ရွက်ရန် လိုအပ်ပါသည်။

6. **လုံခြုံသော အစီတ်အပိုင်းများဖန်တီးနိုင်ရန်အတွက် ဖောင်ပုံစံ ထားရှိခြင်း** ထိုဖောင်ပုံစံများတွင် အဖွဲ့အစည်း၏ လုံခြုံရေး setting အစီတ်အပိုင်းများကို ကြိုတင်ထည့်သွင်းခြင်းမျိုး လုပ်နိုင်ပါသည်။ လုံခြုံရေးပုံစံတွင် လုံခြုံရေး အဆင့်နိမ့်ခြင်း၊ အလည်အလတ်ရှိခြင်း၊ အဆင့်မြင့်ခြင်း စသည်ဖြင့် အင်မတန် ရိုးရှင်းစွာ ထားရှိနိုင်ပြီး ထိုဥပမာများသည် အဖွဲ့အစည်းအတွက် ဖြစ်နိုင်ခြေ အန္တရာယ်များအား စီမံရာတွင် setting မည်မျှလောက်ကို update လုပ်ရန် လိုအပ်ကြောင်း ဖော်ပြပေးပါသည်။ ကုန်ထုတ်လုပ်သူများဖက်မှ သိထားသည့် ဖြစ်နိုင်ခြေ အန္တရာယ်များကို ဖော်ပြသည့် hardening guide များဖြင့် ဖောင်ပုံစံကို ပံ့ပိုးမှု လုပ်နိုင်ပါသည်။

# လုံခြုံသော ကုန်ပစ္စည်းများ ထုတ်လုပ်ခြင်း ဆိုင်ရာ လုပ်ထုံးလုပ်နည်းများ

1. **ရည်ရွယ်သည့်အတိုင်း လုပ်ဆောင်နိုင်သည့် အရာများကို လုံခြုံဘေးကင်းသော SDLC မူဘောင်များတွင် မှတ်တမ်းတင်ထားပါ။** လုံခြုံဘေးကင်းသော SDLC မူဘောင်သည် အရှိကို အရှိအတိုင်း ပြသပြီး လူများ၏ ဥပမာများ၊ လုပ်ငန်းစဉ်များနှင့် စက်မှုနည်းပညာများကို လည်း ဖော်ပြထားပါသည်။ မည်သည့် SDLC ထိန်းချုပ်ရေးမူဘောင်ကို အသုံးပြုနေသည့်အကြောင်းကို အသေးစိတ် ရေးသားဖော်ပြပြီး အများသိရှိနိုင်အောင် ထုတ်ဝေသည့်အပြင် တခြားသော ထိန်းချုပ်မှုများ အသုံးပြုလျင်လည်း ဖော်ပြပါ။ အမေရိကန်နိုင်ငံတွင် NIST Secure Software Development Framework (SSDF). အား အသုံးပြုရန် စဉ်းစားပါ။ လုံခြုံသော ဆော့ဖ်ဝဲထုတ်လုပ်ရေးမူဘောင် SSDF သည် checklist မဟုတ်သော်လည်း ၎င်းသည် " အခြေခံကြပြီး လက်တွေ့ဆန်သည့် ဆော့ဖ်ဝဲထုတ်လုပ်မှုကို ဖော်ပြထားပါသည်။"

2. **Document Cybersecurity Performance Goals (CPG) သို့မဟုတ် equivalent conformance များကို မှတ်တမ်းတင်ပါ။** အဖွဲ့အစည်းတစ်ခုအနေဖြင့် NIST SSDF စံချိန်စံနှုန်းနှင့် ပြည့်မှီကြောင်း ပြောဆိုသည့်အခါတွင် ၎င်း၏ SDLC မှာ အကောင်းဆုံး လုပ်ထုံးလုပ်နည်းဖြင့်ကောင်းမွန်စွာနားလည် သဘောပေါက်မှု ရှိကြောင်းကို ပြသရာ ရောက်ပါသည်။ သို့သော်လည်း ၎င်းတို့အတွက် ကောင်းမွန်သည့် SDLC ရှိရုံနှင့် မလုံလောက်ပါ။ သူတို့၏ လုပ်ငန်းကို ကာကွယ်ရန်လိုအပ်သကဲ့သို့ ပစ္စည်းကို ထုတ်လုပ်နေသည့်အချိန် အတောအတွင်း လုံခြုံရေးဆိုင်ရာများအား ကြိုးကိုင်ခြယ်လှယ်နိုင်ရန် ကြိုးစားသည့် မသမာသူများ၏ တိုက်ခိုက်နိုင်မှု အနေအထားမှ ကာကွယ်မှုရှိအောင် လုပ်ဆောင်ထားရမည် ဖြစ်ပါသည်။ ၎င်းလုပ်ရပ်သည် သဘောတရားအရ တိုက်ခိုက်မှုများ မဟုတ်သော်လည်း ထိုကဲ့သို့ လုပ်ဆောင်မှုများ ရှိခဲ့ဖူးပြီး ထိုကဲ့သို့ ဖြစ်လျင် ဝယ်ယူသုံးစွဲသူများအပေါ် ဆိုးသွမ်းသော သက်ရောက်မှုဖြစ်စေသကဲ့သို့ နိုင်ငံတော် လုံခြုံရေးအထိပါ သက်ရောက်မှု ဖြစ်စေနိုင်ပါသည်။ အဖွဲ့အစည်းများအနေဖြင့် အဖွဲ့၏ CISA CPGs၊ NIST Cyber security Framework (CSF) သို့မဟုတ် တခြားသော ဆိုက်ဘာ လုံခြုံရေး အစီအစဉ်ဆိုင်ရာ မူဘောင်များ တည်ဆောက်ပုံကို ထုတ်ဝေမှုလုပ်ရန် စဉ်းစားသင့်ပါသည်။

3. **အားနည်းချက်များကို စီမံခန့်ခွဲခြင်း (Vulnerability management)။** တချို့သော ကုန်ထုတ်လုပ်သူများတွင် အားနည်းချက်များကို စီမံခန့်ခွဲသည့် အစီအစဉ်များ ထားရှိပြီး ၎င်းသည် ကုမ္ပဏီအတွင်း ရှိသည့် အားနည်းချက် သို့မဟုတ် ပြင်ပမှ တွေ့ရှိသည့် ပျော့ကွက်ဟာကွက်နှင့် တခြားအနည်းငယ်သော အရာများအား ဖာထေးရန်သာ အာရုံစိုက်ထားပါသည်။ ပိုမို အတည်တကျဖြစ်သော အစီအစဉ်များသည် အားနည်းချက်၏ ဒေတာအချက်အလက်များနှင့် ၎င်းတို့၏ ပြဿနာ အရင်းအမြစ်များအား အခြေခံထားသည့် ဒေတာအချက်အလက်များအပေါ် ကျယ်ကျယ်ပြန့်ပြန့် ပါဝင်လုပ်ဆောင်ထားခြင်းဖြစ်ပြီး အားနည်းချက် ဖြစ်စေသည့် အရာအားလုံးကို ဖယ်ရှားလိုက်ခြင်း ဖြစ်ပါသည်[3]။ ၎င်းတို့သည် setting ၏ အရည်အသွေးအတွက် ပြင်ဆင်ရေး၊ အရည်အသွေးထိန်းချုပ်ရေး၊ အရည်အသွေး မြင့်တင်ရေးနှင့် အရည်အသွေးတိုင်းတာခြင်းများအတွက် အတည်တကျ သတ်မှတ်ထားသည့် အစီအစဉ်များ ဖြစ်ပါသည်။ စံမံခန့်ခွဲမှု၏ မပြည့်စုံမှုကို စီးပွားရေးကိစ္စအဖြစ်သာ ရှုမြင်ပြီး လုံခြုံရေးကိစ္စအဖြစ် ရှုမြင်လေ့ မရှိပေ။ ထိုအစီအစဉ်များသည် တခြားသော ကဏ္ဍများ၏ အရည်အသွေးနှင့် လုံခြုံရေး အစီအစဉ်များနှင့် ကွာခြားမှု မရှိလှပါ။

4. **လူတိုင်းထည့်ဝင်နိုင်သော Open source software များကို တာဝန်ရှိစွာ အသုံးပြုပါ။** Open source software များကို အသုံးပြုသည့်အခါတွင် open source package များအား ဆန်းစစ်မှုလုပ်ပြီး တာဝန်ယူမှုရှိရန်၊ ကုဒ်မျဉ်းမှုများအား အသုံးပြုရာတွင် ၎င်းတို့၏ မှီငြမ်းမှုများကို လေ့လာရန်၊ ရေရှည်တည်တံ့ ဖွံ့ဖြိုးမှု ဖြစ်အောင် ပံ့ပိုးရန်နှင့် အရေးကြီးသည့် အချက်အလက်များအား ထိန်းသိမ်းမွန်းမံမှု လုပ်သင့်ပါသည်။ ဖတ်ရှုလိုပါက ဂျပန်နိုင်ငံ၏ စီးပွားရေးရာ၊ ကုန်သွယ်ရေးနှင့် စက်မှုရေးရာ ဝန်ကြီးဌာန(METI) မှ " OSS အသုံးပြုခြင်းနှင့် ၎င်း၏လုံခြုံရေးကို အခိုင်အမာတည်ဆောက်ခြင်းဆိုင်ရာ စီမံခန့်ခွဲမှုနည်းလမ်းများနှင့်ပတ်သက်သည့် အသုံးပြုမှုဖြစ်ရပ် နမူနာများ စုစည်းမှု" ဆိုသည့် ခေါင်းစဉ်ဖြင့် ထုတ်ဝေမှု လုပ်ထားပါသည်။

5. **တည်ဆောက်သူများအတွက် အလိုအလျောက် လုံခြုံမှုရှိခြင်းကို လုပ်ဆောင်ပေးခြင်း** ဆောဖ်ဝဲကို တည်ဆောက်နေစဉ်အတွင်း တည်ဆောက်သူများအတွက် လုံခြုံမှုရှိသော အခြေခံအုတ်မြစ်လမ်းကြောင်းကို အလိုအလျောက် ပါဝင်အောင်တည်ဆောက်ပေးတာမျိုး လုပ်ဆောင်ပေးပါ။ ဥပမာ - SQL injection ၏ ပျော့ကွက်ဟာကွက် ပျံ့နှံ့မှု အနေအထားကြောင့် လက်တွေ့တွင် ထိခိုက်နစ်နာမှုများ ဖြစ်စေပြီး ထိုပျော့ကွက်ဟာကွက်များကို ကာကွယ်နိုင်ရန် အတွက် တည်ဆောက်သူများအနေဖြင့် ကောင်းမွန်စွာ ထိန်းသိမ်းထားသည့် ကွန်ပြူတာ library ရှိရန် အရေးကြီးပါသည်။ "Paved roads (ခင်းထားသော လမ်း)" သို့မဟုတ် "well-lit paths (အလင်းရောင် ရသောလမ်း)" ဟု သိကြတဲ့ လုပ်ထုံးလုပ်နည်းသည် လျင်မြန်မှုနှင့် လုံခြုံရေးအပြင် လူကြောင့် အမှားဖြစ်ရသည့် ကိစ္စမျိုး နည်းပါးအောင် လုပ်ဆောင်ပေးပါသည်။

6. **လုံခြုံရေးကို နားလည်သည့် ဆော့ဖ်ဝဲ တည်ဆောက်ရေး လုပ်သားထုကို မွေးထုတ်ရန်** သင်၏ ဆော့ဖ်ဝဲ တည်ဆောက်သူသည် လုံခြုံရေး နားလည်ကြောင်း သေခြာစွာ လုပ်ဆောင်ထားရမည်ဖြစ်ပြီး ၎င်းတို့အား အကောင်းဆုံးသော secure coding ဆိုင်ရာ လုပ်ထုံးလုပ်နည်းများ တတ်ကျွမ်းအောင် သင်တန်းပို့ချတာမျိုး လုပ်ပေးသင့်ပါသည်။ ထို့အပြင် တက္ကသိုလ်များ၊ ကွန်မြူနီတီ ကောလိပ်၊ bootcampsနှင့် တခြားသော ပညာရှင်များနှင့် ပူးပေါင်း၍ လုပ်သားထု တစ်ခုလုံးအား အပြောင်းအလဲလုပ်ရန်အတွက် လုံခြုံရေး ဗဟုသုတကို ဆန်းစစ်ပြီး လုပ်သားခန့်အပ်ရေး လုပ်ထုံးလုပ်နည်းများကို update လုပ်ရာတွင် ပါဝင်ပံ့ပိုးနိုင်ပါသည်။

[3] NIS SSDF၊ PO 1.2 ဥပမာ ၂ - "အဖွဲ့အစည်း၏ ဆော့ဖ်ဝဲ လိုအပ်ချက် ဆိုင်ရာ မူဝါဒများကို အဓိပ္ပာယ် ဖွင့်ဆိုခြင်းလုပ်ပြီး SDLC တွင် အဓိကကြသည့် အရာတွင် လုံးဝလိုက်နာမှု ရှိကြောင်း အတည်ပြုရပါမည်။ (ဥပမာ - gates များဖြင့် ဆော့ဖ်ဝဲ၏ ပျော့ကွက်ဟာကွက်များကို အတည်ပြုနိုင်ပြီး ထုတ်ဝေပြီးသား ဆော့ဖ်ဝဲများ၏ ပျော့ကွက်ဟာကွက် တွေ့ ရှိသူ အပေါ် တုန့်ပြန်မှု လုပ်ရပါမည်။)"

7. **လုံခြုံရေးအချက်အလက်များနှင့် ဖြစ်ရပ်စီမံခန့်ခွဲမှု (Security incident event management (SIEM)) ကို စမ်းသပ်ရန်နှင့် security orchestration, automation, and response (SOAR) ပူးပေါင်းထည့်တွင်းရန်။** လက်တွေ့စမ်းသပ်မှုအပြင် ပေါ်ပြူလာဖြစ်သည့် SIEM နှင့် SOAR ထုတ်လုပ်သူတို့အပြင် တချို့သော ဝယ်ယူသုံးစွဲသူများနှင့် ပူးပေါင်းလုပ်ကိုင်၍ incident response team အနေဖြင့် လုံခြုံရေးဆိုင်ရာ အားနည်းမှုရှိနိုင်သည့် သံသယဖြစ်မှု သို့မဟုတ် ရှိနေသည့် လုံခြုံရေး အားနည်းမှုအား စုံစမ်းဆန်းစစ်ရန် log စာရင်းမှတ်တမ်းများကို မည်ကဲ့သို့ အသုံးပြုသနည်း ဆိုသည်ကို နားလည်အောင် လေ့လာမှု လုပ်နိုင်ပါသည်။ အနည်းငယ်သော ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများသည် ပေါ်ပေါက်လာသည့် ပြဿနာ incident များကို တုန့်ပြန်ဖူးသည့် အတွေ့အကြုံရှိကြပြီး ၎င်းတို့ လိုလားသည့် အတိုင်းအတာလောက် ကူညီမှု မလုပ်နိုင်သည်များကို log စာရင်းတွင် မှတ်သားထားနိုင်ပါသည်။ SIEM နှင့် SOAR နည်းပညာများ၊ တကယ့် ပြဿနာကို တုန့်ပြန်သည့် ပရော်ဖက်ရှင်နာ သမားများနှင့် အလုပ်လုပ်ခြင်းဖြင့် တည်ဆောက်ရေးအသင်းအနေဖြင့် မှန်ကန်ပြီး ပြည့်စုံသည့်အပြင် အချိန်ကုန် သက်သာပြီး ပြဿနာ ဖြစ်စဉ်တွင် မသေခြာမှုကို လျော့ကျစေသည့် အနေအထားများကို log စာရင်းတွင် မှတ်တမ်းတင်ထားနိုင်ပါသည်။

8. **Zero Trust Architecture (ZTA) နှင့် ချိန်ညှိယူပါ။** NIST ZTA model နှင့် CISA Zero Trust Maturity Model လို အရာများကဲ့သို့သော ထုတ်လုပ်ဖြန့်ချီမှုတွင် ပစ္စည်းထုတ်လုပ်ဖြန့်ချီရေးဆိုင်ရာလမ်းညွှန်ချက်ဖြင့် ချိန်ညှိယူပါ။ ဝယ်ယူသုံးစွဲသူများအား ၎င်းအခြေခံ သဘောတရားများကို လိုက်နာလုပ်ဆောင်ရန် တိုက်တွန်းပါ။

# အဆင့်မြင့်လုံခြုံရေးကို အလေးထားသော လုပ်ငန်းကျင့်သုံးမှုများ

1. **ငွေကြေးထပ်မံ တောင်းခံမှု မလုပ်ပဲ logging ဝင်ရောက်ခွင့် ပေးပါ။** Cloud ဝန်ဆောင်မှုသည် ထပ်မံကုန်ကျမှု မလိုပဲ လုံခြုံရေးနှင့် ဆက်စပ်သည့် log မှတ်တမ်း ထားရှိပေးသင့်ပါသည်။ ကုမ္ပဏီ၏ စက်ပစ္စည်းများကို အခြေခံပြီး လည်ပတ်သည့် on-premises ပစ္စည်းများသည်လည်း အဖိုးအခ ထပ်ပေးစရာမလိုပဲ လုံခြုံရေးနှင့် သက်ဆိုင်သည့် log မှတ်တမ်း ထားရှိသင့်ပါသည်။ ထို့အပြင် ကုန်ပစ္စည်းအနေဖြင့် လုံခြုံရေးဆိုင်ရာ ဖြစ်ရပ်များအား အလိုအလျောက် log မှတ်တမ်းယူသင့်ပြီး အကြောင်းရင်းမှာ ဝယ်ယူသုံးစွဲသူ အများအပြားသည် ထိုမှတ်တမ်း၏ အရေးပါမှုကို လုံခြုံရေးဆိုင်ရာ ပြဿနာဖြစ်ပြီးနောက်ပိုင်းမှ နားလည် သဘောပေါက်နိုင်သည့်အတွက် ဖြစ်ပါသည်။ ထိုကဲ့သို့ နည်းဗျူဟာသည် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ သိနားလည်မှု ရရှိရန်အတွက် မည်သို့သော လုံခြုံရေးဆိုင်ရာ ဖြစ်ရပ်များကို log မှတ်တမ်း ယူထားသင့်သည်ဆိုသည်ကို သိနားလည်ရန်အတွက် သေခြာစေ့စပ်သည့် ဆန်းစစ်မှု လုပ်ရန် လိုအပ်နိုင်ပါသည်။ ဝယ်ယူသုံးစွဲသူများအနေဖြင့် logging မှတ်တမ်းကို မည်သို့ ပုံဖော်မည်နည်း၊ မည်သည့်အချိန်ကာလ အထိ log ကို ထိန်းသိမ်းရန်လိုအပ်သနည်း၊ log အား မည်သည့် အချိန်အထိ သိုလှောင်ထားမည်နည်းအပြင် log အား မည်ကဲ့သို့ ဆန်းစစ်မှု လုပ်နိုင်သနည်း စသည်များကို ထည့်တွက်ပြီး ဆန်းစစ်မှု လုပ်သင့်ပါသည်။ တချို့သော ကိစ္စရပ်များတွင် ဆန်းစစ်မှုများက application ၏ log management architecture တစ်ခုလုံးကို အစမှပြန်လည်လုပ်ဆောင်ဖို့ လိုအပ်တာမျိုးဖြစ်နိုင်ပြီး ထိုကဲ့သို့ ဖြစ်ရခြင်းမှာ ကုန်ထုတ်လူများအတွက် ဥပဒေနှင့် မလွတ်ကင်းမှု ဖြစ်စေပြီး ကုန်ကျစရိတ်ခံရန်အတွက် ဖြစ်ပါသည်။ Incident response (IR) ကျွမ်းကျင်သူများနှင့် ပူးပေါင်းအလုပ်လုပ်ကိုင်ခြင်းအားဖြင့် log မှတ်တမ်း များသည် လက်တွေ့စမ်းသပ်မှုလုပ်သည့်အခါတွင် စုံစမ်းစစ်ဆေးမှုအတွက် လွယ်ကူစေနိုင်သည့် အခွင့်အလမ်းများ ဖြစ်စေနိုင်ပါသည်။ SIEM ဆိုသည့် ကဏ္ဍတွင် ကြည့်ရန်။

2. **လျှို့ဝှက် အခွန်များအား ဖယ်ရှားပစ်ရန်** လုံခြုံရေးအတွက် သို့မဟုတ် ကိုယ်ရေးကိုယ်တာဆိုင်ရာ feature များအတွက် သို့မဟုတ် စနစ်မတူသည့်အရာများနှင့် ပေါင်းစပ်မှုများအတွက် မည်သည့်အခါမျှ ငွေကြေးတောင်းခံမည်မဟုတ်ကြောင်း အာမခံချက်ကို ထုတ်ပြန်ရပါမည်။ ဥပမာ - identity and access management (IAM) အတွင်းတွင် တစ်ကြိမ်သာ လော့အင်ဝင်ခြင်း single sign-on (SSO) ဟု ခေါ်သည့် ဝန်ဆောင်မှု ရှိပါသည်။ တချို့သော ကုန်ထုတ်လုပ် သူများသည် SSO ဝန်ဆောင်မှု (တခါတရံ identity provider ဟုလည်း ခေါ်ဆို) ကို ဆက်သွယ်ရန်အတွက် ငွေကြေး ထပ်မံတောင်းခံခြင်း လုပ်ပါသည်။ ထို “SSO tax အခွန်” ဆိုသည်မှာ ပစ္စည်း၏ SMO အများအပြားအတွက် good identity and access management ကို မတတ်နိုင်မှုဖြစ်စေသည့်အတွက် လုံခြုံရေးခိုင်မာသော အနေအထားရရှိဖို့အတွက် လုပ်ဆောင်ရာတွင် အဟန့်အတား ဖြစ်စေနိုင်ပါသည်။ တချို့သော ဝန်ဆောင်မှုသည် MFA ကို အသုံးပြုနိုင်ရန်အတွက် ငွေကြေးပိုမို တောင်းခံခြင်းလုပ်လေ့ရှိပါသည်။ **လုံခြုံရေးကို ဇိမ်ခံပစ္စည်းသဖွယ် ဈေးနှုန်းသတ်မှတ်ခြင်းမျိုး မလုပ်သင့်ပဲ ဝယ်ယူသုံးစွဲသူများ၏ အခွင့်အရေးတစ်ရပ်အဖြစ် မှတ်ယူသင့်ပါသည်။** တချို့သော ကုန်ထုတ်လုပ်သူများသည် ၎င်း feature များကို လိုအပ်သည်ဟု တောင်းဆိုသည့် ဝယ်ယူသုံးစွဲသူများ နည်းပါးပြီး မွမ်းမံထိန်းသိမ်းရန်အတွက် ငွေကုန်ကြေးကျများသည်ဟု စောဒကတက်ကြပါသည်။ ထိုကဲ့သို့ စောဒက တက်မှုသည် ဝယ်ယူသုံးစွဲသူ အနည်းစုကသာ မကျေမနပ်ဖြစ်ကြောင်း ဆက်သွယ်မှုလုပ်ခြင်း သို့မဟုတ် အပေးအယူလုပ်တာဖြစ်ပြီး ဝယ်ယူသုံးစွဲသူတိုင်းသည် ထို feature များ၏ လှုပ်ရှားမှု အကျိုးရလဒ်အားလုံးကို နားမလည်သကဲ့သို့ ထို feature များကို ထိန်းသိမ်းမွမ်းမံရန်အတွက် ငွေကုန်ကြေးကျ ခံရသည်ကို နားမလည်ကြသည့်အချက်ကို လစ်လျူရှုရာ ရောက်ပါသည်။ ကုန်ထုတ်လုပ်သူအများအပြားသည် ရယူအသုံးပြုမှုအတွက်နှင့် ဒေတာကို တခြားစနစ်တစ်ခုနှင့် ပူးပေါင်းခြင်းများအတွက် ငွေကြေး ပိုမိုတောင်းခံခြင်းမျိုး ပြုလုပ်လျက်ရှိပါသည်။ Key attribute များကို တည်ဆောက်ရန်အတွက် လိုအပ်သည့် ငွေကြေးများကို ဝယ်ယူသုံးစွဲသူများအားလုံးကို ကုန်ကျစေမည့် နည်းဖြင့် တည်ဆောက်ထားပြီး ဥပမာ ကားပေါ်က ခါးပတ်များ၊ collapsible steering columns ဟုခေါ်သည့် ကားမတော်တဆမှု ဖြစ်ချိန်တွင် ကားစတီယာမှ မောင်းသူကို ဝင်ထိုးတာမျိုးမဖြစ်စေအောင် လုပ်ဆောင်ပေးခြင်းနှင့် airbag စသည့် ကားမတော်တဆ ဖြစ်ချိန်တွင် လူ့အသက်ကို ကယ်နိုင်သည့် ပစ္စည်းများအတွက် ကုန်ကျစရိတ်အား ထည့်တွက်ခြင်း ဖြစ်ပါသည်။

3. **Open standards များကို လက်ခံပါ။** Open standard ကို အကောင်အထည်ဖော် လက်ခံကျင့်သုံးပါ အထူးသဖြင့် common network identity protocol များအတွက် ဖြစ်ပါသည်။ Open standard များ ကျင့်သုံးသည့်အခါတွင် မူပိုင်လုပ်လိုက်သည့် ပရိုတိုကောကို ရှောင်ရှားပါ။

4. **Upgrade tooling များ လုပ်နိုင်အောင် လုပ်ဆောင်ပေးပါ။** ဝယ်ယူသုံးစွဲသူ အများအပြားသည် ကုန်ပစ္စည်း၏ နောက်ဆုံးပေါ် ဗားရှင်းကို အသုံးပြုရန် တွန့်ဆုတ်နေခြင်းမျိုး ဖြစ်တတ်ပြီး ထိုအထဲတွင် secure network connection ကဲ့သို့ ပိုမို သစ်လွင်ပြီး လုံခြုံသော feature များကို အသုံးပြုရန် မဝံ့မရဲဖြစ်ခြင်းတို့ ပါဝင်ပါသည်။ ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် မသေခြာ မရေရာမှုများကို လျှော့ချစေပြီး အန္တရာယ်ဖြစ်နိုင်ခြေ လျှော့ချပေးသည့် ကိရိယာများဖြင့် ဝယ်ယူသုံးစွဲသူများကို upgrade အသစ်များကို အသုံးပြုနိုင်အောင် လုပ်ဆောင်ပေးနိုင်ပါသည်။ ဝယ်ယူသုံးစွဲသူများကို တိုက်တွန်းသည့်အနေဖြင့် upgrade နှင့် patches များကို စမ်းသပ်သုံးကြည့်နိုင်ရန်အတွက် လိုင်စင်များကို အခမဲ့ ချပေးခြင်းမျိုးလည်း လုပ်ဆောင်နိုင်ပါသည်။

# အခြေခံ သဘောတရား ၂ - ကြီးမားသိသာသော ပွင့်လင်းမြင်သာမှုရှိခြင်းနှင့် တာဝန်ယူမှုရှိသည့်နည်းကို လိုက်နာကျင့်သုံးခြင်း

## ရှင်းပြချက်

ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် လုံခြုံဘေးကင်းမှုရှိသော ပစ္စည်းများကို ထုတ်လုပ်နိုင်သည့်အတွက် မိမိကိုယ်ကို ဂုဏ်ယူသင့်သည့်အပြင် ထိုကဲ့သို့ ဆောင်ရွက်နိုင်ခြင်းအားဖြင့် ၎င်းတို့ကို တခြားကုန်ထုတ်လုပ်မှု အသိုင်းအဝိုင်းထက် တမူထူးခြားမှု ဖြစ်စေပါသည်။

ပွင့်လင်းမြင်သာမှုနှင့် ဆက်စပ်၍ အဖြစ်များသော စိုးရိမ်မကင်းမှုကို ဆန်းစစ်ကြပါစို့။ ကြီးမားသိသာသည့် ပွင့်လင်းမြင်သာမှုအကြောင်းကို လက်ရှိလုပ်ကိုင်နေသူများ ဆွေးနွေးသည့်အခါတွင် စကားဝိုင်းမှာ စိုးရိမ်မကင်းမှုဖြစ်စရာ အကြောင်းဖက်ကို ဦးတည်သွားလေ့ရှိပြီး ၎င်းတို့က “မသမာနည်းနဲ့ တိုက်ခိုက်သူများအတွက် လမ်းပြမြေပုံ” ချပေးရာ ရောက်သွားနိုင်သည်ဟု စိုးရိမ်မကင်း ဖြစ်ကြပါသည်။ သို့သော်လည်း သက်သေအထောက်အထားများအရ ထိုလမ်းပြမြေပုံ မရှိသည့်အချိန်တွင်လည်း မသမာသူများက တိုက်ခိုက်မှုများကို လုပ်ကိုင်နိုင်စွမ်း ရှိနေသည့်အတွက် ထိုကဲ့သို့သော စိုးရိမ်မှုကို နောက်ဖယ်ထားပြီး တိုက်ရိုက် ဝယ်ယူသုံးစွဲသူများ၊ သွယ်ဝိုက်နည်းဖြင့် ဝယ်ယူသုံးစွဲသူများ၊ ထောက်ပံ့မှုကွင်းဆက် supply chainများနှင့် ဆော့ဖ်ဝဲလုပ်ငန်းကဏ္ဍ တစ်ခုလုံးအား အကျိုးရှိစေရန်အတွက် ပွင့်လင်းမြင်သာမှုရှိအောင် ဆောင်ရွက်သင့်ပါသည်။

ပွင့်လင်းမြင်သာခြင်းသည် ကဏ္ဍတစ်ခုလုံးအတွက် အစဉ်အလာ တည်ထောင်ပေးရာရောက်ပြီး တနည်းဆိုရသော် “ ကောင်းမွန်ခြင်း” နှင့် တူပါသည်။ ထိုအစဉ်အလာကောင်းများသည် အချို့နိုင်ကြောလာသည်နှင့်အမျှ ဝယ်ယူသုံးစွဲသူများ၏ လိုအပ်ချက်အရ အပြောင်းအလဲ ဖြစ်လာနိုင်ပြီး ခြိမ်းခြောက်မှု ဗျူဟာ ပြောင်းလဲခြင်း သို့မဟုတ် စီးပွားရေးအနေအထား သို့မဟုတ် နည်းပညာထွန်းကားသည့်ဖြစ်စဉ် များကြောင့် အပြောင်းအလဲ ဖြစ်နိုင်ပါသည်။ ပွင့်လင်းမြင်သာမှုသည် အရင်းအမြစ် နည်းပါးသည့် ကုန်ထုတ်လုပ်သူများအတွက် အရင်းအမြစ်များပြီး အတည်တကျဖြစ်သည့် ကုန်ထုတ်လုပ်သူများထံမှ သင်ခန်းစာများကို လေ့လာခွင့် ရရှိစေနိုင်ပါသည်။ အချက်အလက်မျှဝေခြင်းဆိုင်ရာ ပြောဆိုဆွေးနွေးမှုသည် လက်ရှိကြုံတွေ့ရသည့် ခြိမ်းခြောက်မှု ညွှန်းကိန်းထက် ကျော်လွန်သင့်ပြီး အောက်ပါ အခြေခံ သဘောတရားများ ပါဝင်ပါသည်။

ပွင့်လင်းမြင်သာမှုသည် ပစ္စည်းထုတ်လုပ်မှု အစောပိုင်းမှစ၍ လုံခြုံရေးဆိုင်ရာ ဆုံးဖြတ်ချက်များကို ချမှတ်စေနိုင်သကဲ့သို့ စီးပွားရေး ခေါင်းဆောင်များအတွက် ဆက်လက်လှုပ်ရှားမှုဖြစ်စေသည့်အပြင် အင်ဂျင်နီယာနှင့် လုံခြုံရေးဆိုင်ရာ ပရော်ဖက်ရှင်နာများအတွက် လည်း လှုပ်ရှားမှု ဖြစ်စေပါသည်။ ပွင့်လင်းမြင်သာမှုမှတဆင့် တာဝန်ယူမှုလည်း တည်ထောင်မှု ဖြစ်စေပါသည်။

"ပွင့်လင်းမြင်သာမှု" ၏ ရှေ့တွင် "ကြီးမားသိသာသော" ဟူသည့် နာမဝိသေသန ပါဝင်နေသည်ကို သတိပြုပါ။ ယနေ့တွင် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် ဆော့ဖ်ဝဲများအား မည်ကဲ့သို့ တည်ဆောက်ပြီး မည်ကဲ့သို့ ထိန်းသိမ်းမွမ်းမံမှုလုပ်သည်၊ ဒေတာ အချက်အလက်ကို အသုံးပြုသည့် အစီအစဉ်သည်လည်း မည်သည့်အဆင့်အထိ အတည်တကျမှု ဖြစ်လာပြီ ဆိုသည့် အချက်အလက် များကို ထုတ်ပြန်ခြင်းမျိုး လုပ်လေ့ရှိကြပါသည်။ ဆော့ဖ်ဝဲကဏ္ဍတွင် ထုတ်လုပ်သူ အနည်းအကျဉ်းကသာ ၎င်းတို့၏ ဆော့ဖ်ဝဲကို မည် ကဲ့သို့ ဒီဇိုင်းရေးဆွဲထားကြောင်း ရှင်းလင်းပြသမှု လုပ်ပါသည်။ ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအတွက် တခြားသော အလားတူ အဖွဲ့ အစည်းများက ၎င်းတို့၏ SDLC ပရိုဂမ်များအား မည်ကဲ့သို့ လုပ်ဆောင်ထားသနည်း၊ တိုက်ခိုက်သူများ၏ အန္တရာယ်မှ ခုခံကာကွယ် နိုင်ရန် ဝယ်ယူသုံးစွဲသူများအတွက် မည်ကဲ့သို့ ပရိုဂမ် ရေးဆွဲထားသည့်အကြောင်းများ လေ့လာရန် အခွင့်အလမ်းတချို့ ရှိပါသည်။ ကဏ္ဍအလိုက်စုစည်းခြင်းသည် လုံခြုံရေးအားနည်းချက်များ ပြုပြင်ရန်အတွက် ကုန်ကျစရိတ်ကို တိုင်းတာသည့် နည်းဗျူဟာများ ဆွေးနွေးချက်နှင့် အားနည်းချက်များအား ဖယ်ရှားခြင်း စသည့် အချက်အလက်များကို မျှဝေခြင်းမျိုးဖြစ်စေပြီး အကျိုးရှိစေနိုင် ပါသည်။ ထိုဘုံ လုပ်ထုံးလုပ်နည်းများ၏ ရလဒ်အနေဖြင့် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူတိုင်း ကုန်ပစ္စည်း၏လုံခြုံရေးဆိုင်ရာတွင် မိမိတို့ ကိုယ်တိုင် လုပ်ဆောင်နိုင်ရန် လေ့လာရမည် ဖြစ်ပါသည်။ လုံခြုံရေး features များ အပေါ်ဇီမ်ခံပစ္စည်းများလို အဖိုးအခ ကောက်ယူ ခြင်းမလုပ်ပဲ လုံခြုံရေးနှင့် ဘေးကင်းရေးသည် အမြတ်စားမည့်အရာမဟုတ်ပဲ ကုန်ကျခံရမည့် အရာ ဖြစ်လာမည် ဖြစ်ပါသည်။ ပူးပေါင်းလုပ်ဆောင်ခြင်းနှင့် ပွင့်လင်းမြင်သာစွာ လုပ်ဆောင်ခြင်းမှတဆင့် ကုမ္ပဏီများသည် လမ်းတလျှောက် မီးအလင်းရောင်များ ရရှိသည့် အကျိုးကျေးဇူးများ ခံစားရမည်ဖြစ်သည်။

ဆော့ဖ်ဝဲ လုပ်ငန်း တစ်ခုလုံး ဆင့်ကဲ တိုးတက်ပြောင်းလဲမှု ဖြစ်ပေါ်လာစေမည့် နည်းဗျူဟာမျိုးကို ကျွန်ုပ်တို့ အနေဖြင့် အာရုံစိုက်မှု လုပ်လိုပါသည်။ အခွင့်အလမ်းအရ တိုးတက်မှုနှင့် နှစ်တိုး တိုးတက်မှုလောက်ဖြင့် ကျေနပ်ဖို့ မသင့်တော့ပါ။ ပညာသားပါသည့် ခြိမ်းခြောက်မှုနှင့် လက်ရှိရှိနေသည့် ရန်သူများ၏ ခြိမ်းခြောက်မှုကို ကျော်လွှားနိုင်ရန်အတွက် ကျွန်ုပ်တို့ အတူတကွ ပူးပေါင်း ကျော်လွှားရမည်ဖြစ်ပြီး ယခုအချိန်အတွက် သက်တောင့်သက်သာမှု မရှိသည့် ပွင့်လင်းမြင်သာမှု အဆင့်ဆင့်ကို လက်ခံခြင်းမျိုး လုပ် ရမည်ဖြစ်သော်လည်း ထိုလုပ်ဆောင်ချက်သည် ကဏ္ဍတစ်ခုလုံးကို ရှေ့သို့ချီစေမည် ဖြစ်ပါသည်။ ယခုလောလောဆယ် ဤလုံခြုံမှု ရှိအောင် စီမံပြင်ဆင်ခြင်း အခြေခံသဘောတရားများနှင့် လုပ်ကိုင်နေသည့် ကုန်ထုတ်လုပ်သူ တချို့ ရှိပါသည်။ "အနာဂတ်က အခု လက်ရှိမှာ ရောက်နေပေမယ့် တန်းတူညီမျှစွာ မျှဝေမှုတော့ မရှိဘူး"ဟု William Gibson ဆိုသည့်အတိုင်း ဖြစ်ပါသည်။ **ကြီးမားသိသာသော ပွင့်လင်းမြင်သာမှုသည် အချက်အလက်များကို ဖြန့်ဝေရာတွင် အထောက်အကူပြုနိုင်သလို ရန်သူ၏ ရန်မှ ကာကွယ်ရေးတွင်လည်း အကျိုးကျေးဇူး ရရှိစေမည် ဖြစ်ပါသည်။**

ပွင့်လင်းမြင်သာမှုသည် တခြားသော လုပ်ငန်းတူ အဖွဲ့အစည်းများအား ၎င်းတို့၏ SDLCs များကို ပိုမို အတည်တကျဖြစ်အောင် လုပ်ဆောင်နိုင်မှုလည်း ပိုမို ဖြစ်စေနိုင်ပါသည်။ ဝယ်ယူသုံးစွဲသူများဖြစ်လာနိုင်သည့်ပုဂ္ဂိုလ်များနှင့် ရင်းနှီးမြှုပ်နှံသူများသည် ကုန် ထုတ်လုပ်သူများအနေဖြင့် သုံးစွဲသူများအတွက် လုံခြုံသည့်အနေအထား ရောက်ရှိဖို့ ကုန်ထုတ်လုပ်သူဖက်မှ ရင်းနှီးမြှုပ်နှံမှု လုပ်ရ ခြင်းနှင့် ပေးဆပ်လိုက်ရသည့် အရာများအကြောင်းကို လေ့လာနိုင်ပါသည်။ ကြီးမားသိသာသော ပွင့်လင်းမြင်သာမှုကို လက်ခံ ကျင့် သုံးသည့် ကုန်ထုတ်လုပ်သူသည် ၎င်းတို့၏ ဝယ်ယူသုံးစွဲသူများအား စျေးနှုန်းနှင့် features များ ဝယ်ယူရေးအတွက် ဆုံးဖြတ်ချက် ချ နိုင်ရန်အတွက် အချက်အလက် ပေးရုံသာမက လုံခြုံရေးအတွက်ပါ ဆုံးဖြတ်ချက် ချနိုင်မှု ဖြစ်စေနိုင်ပါသည်။

အဖွဲ့အစည်းများအနေဖြင့် ထောက်ပံ့ပို့ဆောင်မှု ကွင်းဆက် supply chain နှင့် ၎င်းတို့၏ SDLC များ လုံခြုံရေးအတွက် ကြိုးစား လုပ်ဆောင်ရင်း ၎င်းတို့၏ လုပ်ငန်းစဉ်များ တိုက်ခိုက်ခံရမှုမျိုးကို ကုမ္ပဏီတချို့ ခံခဲ့ရဖူးပါသည်။ ကြီးမားသိသာသော ပွင့်လင်း မြင်သာမှုကို လက်စွဲထားပါက ထိုကဲ့သို့ တိုက်ခိုက်မှုကို လူသိရှင်ကြား ဖြစ်စေသလို ကုမ္ပဏီဖက်က တိုက်ခိုက်မှုမှ ကာကွယ်ရန် လုပ်ဆောင်သည့် တိုးတက်မှုနှင့် နောက်နောင် မဖြစ်အောင် လုပ်ဆောင်သည့် အရာများကိုလည်း လူအများကို သိစေနိုင်ပါသည်။ ထို ကဲ့သို့သော အချက်အလက်များကို မျှဝေခြင်းသည် တခြားသော အဖွဲ့အစည်းများကိုလည်း အလားတူ ပြဿနာမျိုး မကြုံရအောင် သင်ခန်းစာ ပေးနိုင်ပါသည်။

## အခြေခံ သဘောတရားကို လက်တွေ့အသုံးချခြင်း

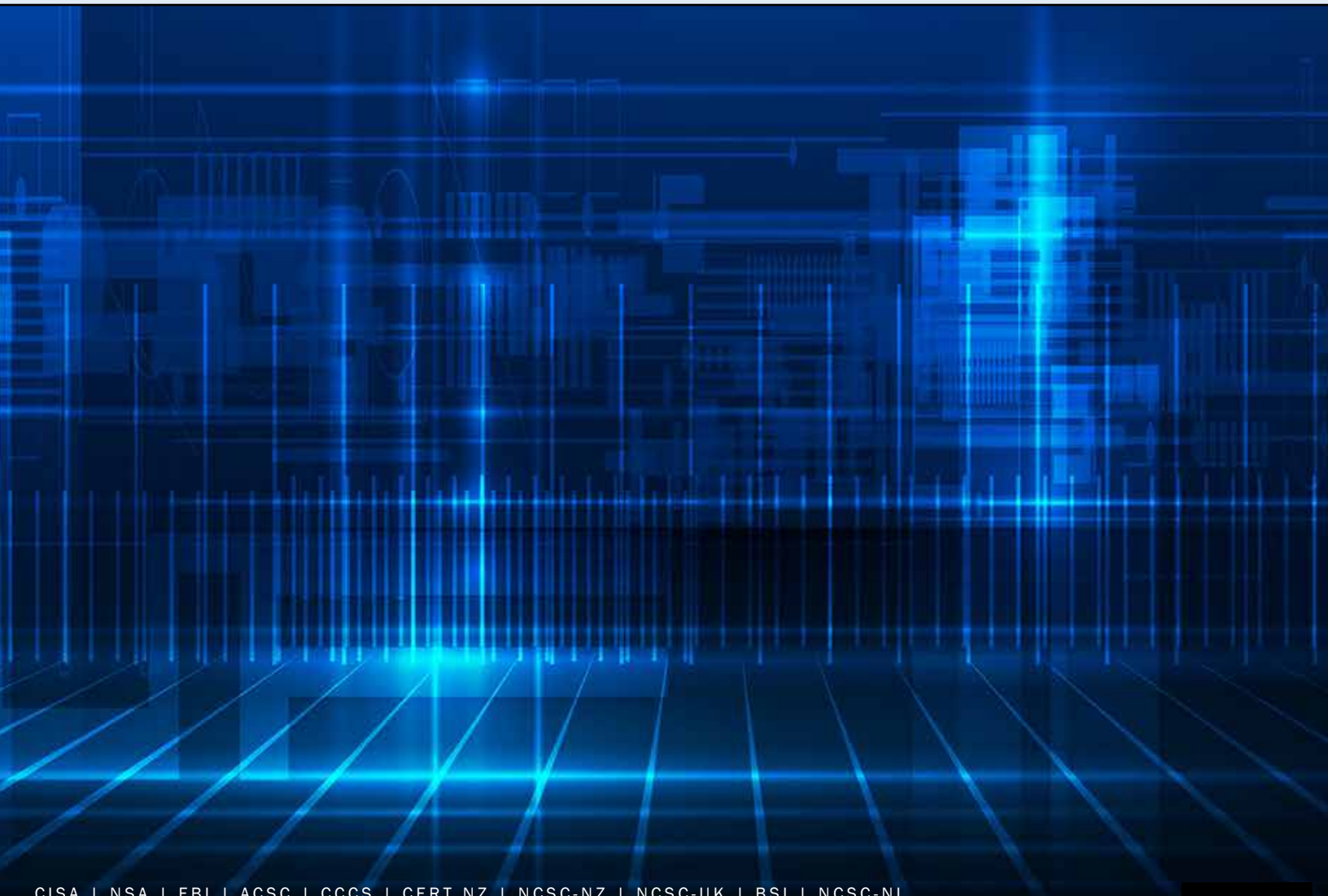
ထိုအခြေခံ သဘောတရားကို လက်တွေ့ကျင့်သုံးရန်အတွက် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအနေဖြင့် အောက်ပါ ခြေလှမ်းများဖြင့် လုပ်ဆောင်သင့်ပါသည် -

# အလိုအလျောက် လုံခြုံနေခြင်း နည်းလမ်းများ

1. **လုံခြုံရေးဆိုင်ရာ စာရင်းကိုန်းဂဏန်းများနှင့် သင့်တော်သည့် ဦးတည်ရာအလားအလာများကို စုပေါင်း ထုတ်ဝေပါ။** ဥပမာ ခေါင်းစဉ်ထဲတွင် ဝယ်ယူသုံးစွဲသူနှင့် တာဝန်ရှိသူအပြင် လုံခြုံဘေးကင်းမှု မရှိသည့် ပရိုတိုကောဟောင်းများမှ MFA ကို ထည့်သွင်းအသုံးပြုရေး ပါဝင်ပါသည်။

2. **လုံခြုံရေးဆိုင်ရာ ဖာထေးမှု စာရင်းကိုန်းဂဏန်းများကို ထုတ်ဝေပါ။** ဝယ်ယူသုံးစွဲသူများသည် မည်မျှ ရာခိုင်နှုန်းလောက်မှ ပစ္စည်း၏ နောက်ဆုံးပေါ် ဗားရှင်းကို အသုံးပြုထားသည့်အကြောင်း အသေးစိတ်ဖော်ပြပြီးupdate များကို ပိုမို လွယ်ကူစွာ လုပ်နိုင်ရန်နှင့် ပိုမို ယုံကြည်စိတ်ချမှု ရှိရန် မည်ကဲ့သို့ လုပ်ဆောင်ပေးသည် ဆိုသည့်အကြောင်းများကို အသေးစိတ် ဖော်ပြပါ။

3. **Unused privileges နှင့် ဆက်စပ်သည့် ဒေတာ အချက်အလက်များ ထုတ်ဝေပါ။** တိုက်တွန်းနှိုးဆော်မှု အပါအဝင်ဝယ်ယူသုံးစွဲသူအပေါ် အခြေခံသည့် လွန်ကဲသော ခွင့်ပြုချက်များဆိုင်ရာ အချက်အလက်နှင့် ဝယ်ယူသုံးစွဲသူများ၏ တိုက်ခိုက်ခံရနိုင်မှု မျက်နှာပြင်ကို လျှော့ချဖို့ မိမိအနေဖြင့် အခြားလုပ်ဆောင်ချက်များကို စုပေါင်း ထုတ်ဝေပါ။ ၎င်း unused privileges များသည် ကားခါးပတ်ကဲ့သို့ အုပ်ချုပ်သူအတွက် သတိပေးတပ်လှန့်မှု ကောင်းတစ်ရပ် ဖြစ်စေနိုင်ပါသည်။



# ကုန်ပစ္စည်း ထုတ်လုပ်မှု လုပ်ထုံးလုပ်နည်းကို လုံခြုံမှုရှိအောင် လုပ်ဆောင်ခြင်း

1. **လုပ်ငန်းအတွင်း လုံခြုံရေးထိန်းချုပ်မှုကို ထားရှိခြင်း** ကုမ္ပဏီ အများအပြားသည် ၎င်းတို့၏ အချက်အလက်များကို cloud ဝန်ဆောင်မှု ပေးသူများထံ ပြောင်းလဲခြင်းမှ အကျိုးရလဒ် ခံစားရမှုများ ရှိပါသည်။ ယခုအခါတွင်မူ မသမာသည့် တိုက်ခိုက်သူများမှ ထို cloud ဝန်ဆောင်မှုကို ပစ်မှတ်ထား တိုက်ခိုက်မှုများ ရှိလာပါသည်။ Software as a Service (SaaS) ဝန်ဆောင်မှု ပေးသူများအနေဖြင့် ၎င်းတို့ အဖွဲ့အတွင်း၏ ထိန်းချုပ်မှု စာရင်းကိန်းဂဏန်းများကို ဖော်ပြထုတ်ဝေသင့်ပါသည်။ ဥပမာ - SaaS ဝန်ဆောင်မှု ပေးသူများအနေဖြင့် ၎င်းအဖွဲ့အစည်းအတွင်း၏ Fast Identity Online (FIDO) authentication ကဲ့သို့သော phishing-resistant MFA ဆိုင်ရာ စာရင်းကိန်းဂဏန်းများကို ဖော်ပြသင့်ပါသည်။ အကောင်းဆုံးလုပ်ဆောင်နည်းမှာ phishing-resistant MFA မှတဆင့် authenticating မလုပ်ထားသည့် ဝယ်ယူသုံးစွဲသူ၏ အချက်အလက်နှင့် တခြားသော ထိလွယ်ရှလွယ်သော အချက်အလက်များအား မည်သည့် ဝန်ထမ်းမှ ဝင်ရောက်ကြည့်ရှုခွင့် မရအောင် ပြောဆိုလုပ်ဆောင်ထားသင့်ပါသည်။

2. **High-level threat models များကို ဖော်ပြထုတ်ဝေပါ။** လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်သည့် ပစ္စည်းများသည် တီထွင်ဖန်တီးသူများမှ မည်သည့်အရာကို မည်သူ့ရန်မှ ကာကွယ်ရန် လုပ်ဆောင်ထားသည်ဟု ဖော်ပြထားသည့် treat models ရေးသားခြင်းဖြင့် စတင်လေ့ရှိပါသည်။ ထိရောက်ကောင်းမွန်သော treat models သည် အထိန်းအကွပ်မဲ့သည့်အနေအထားတွင် ကျူးကျော်ဝင်လာသည့်နည်းလမ်းကို သိရှိစေပြီး ထိုအရာသည် စီးပွားရေးလုပ်ငန်းအတွက်နှင့် ဖွံ့ဖြိုးတည်ဆောက်ရေး အနေအထားအတွက်ပါ အကြီးဝင်မှု ရှိသင့်သကဲ့သို့ ဝယ်ယူသုံးစွဲသူများ၏ အနေအထားအတွက် အသုံးပြုရန် သင့်တော်သော ပစ္စည်းဖြစ်ဖို့ ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူဖက်မှ ရည်ရွယ်သည့်အတိုင်း ဖြစ်သင့်ပါသည်။

3. **Detailed secure SDLC self-attestations ကို ဖော်ပြထုတ်ဝေပါ။** NIST SSDF သို့မဟုတ် တခြား ဆင်တူသော မူဘောင်များကို အသုံးပြုသော ကုန်ထုတ်လုပ်သူများသည် အတည်တကျ ဖြစ်သည့် ဆော့ဖ်ဝဲ ဖွံ့ဖြိုးမှုသက်တမ်းအတွက် တက်ကြွစွာ လုပ်ကိုင်လျက် ရှိပါသည်။ ကုန်ထုတ်လုပ်သူမှ ထည့်သွင်းထားသည့် self-attestation controls ကို ဖော်ပြထုတ်ဝေခြင်းသည် အကောင်းဆုံး လုပ်ထုံးလုပ်နည်းအတိုင်း မည်သည့်ပစ္စည်းတွင် ထည့်သွင်းထားသည့်အကြောင်း သိစေရုံသာမက ဝယ်ယူသုံးစွဲသူများ၏ ယုံကြည်မှုကိုလည်း တိုးပွားရရှိစေနိုင်ပါသည်။ တခြားသော သက်ဆိုင်ရာ ဘာသာရပ်ကို အသိအမှတ်ပြုလက်မှတ်ထုတ်ဝေပေးသည့် certification schemes ထဲတွင် Israel Cyber Supply Chain Methodology အစ္စရေး၏ ဆိုက်ဘာ ထောက်ပံ့မှု ကွင်းဆက်ဆိုင်ရာ နည်းပညာဌာနလို အဖွဲ့မျိုး ရှိပါသည်။

4. **အားနည်းချက်၏ ပွင့်လင်းမြင်သာမှုရှိခြင်းကို လက်ခံကျင့်သုံးပါ။** ပစ္စည်း၏ အားနည်းများကို မှန်ကန်ပြီး ပြည့်စုံသည့် CVE entries များအနေဖြင့် ဖော်ပြသွားမည်ဟူသည့် ကတိကဝတ်များကို ဖော်ပြထုတ်ဝေပါ။ ထိုလုပ်ဆောင်ချက်သည် အားနည်းချက်များ၏ ပြဿနာအရင်းအမြစ်ကို ဖော်ထုတ်ရာတွင် Common weakness enumeration field အတွက် အထူးသင့်တော်ပါသည်။ CVE ဒေတာများ မှန်ကန် ပြည့်စုံမှု ပိုရှိလေလေ ပစ္စည်းများ၏ လုံခြုံမှုကို ပိုမို ခြေရာ ခံနိုင်လေလေ ဖြစ်စေနိုင်ပြီး ပျော့ကွက် ဟာကွက် ပျံ့နှံ့မှုများကိုလည်း ပိုသိနိုင်မည် ဖြစ်သည်။ သို့သော် CVE ၏ အချက်အလက်များကို အဆိုးဖက်ဆောင်သည့် အားနည်းချက်အဖြစ် ရှုမြင်နိုင်သည်ကို သတိထားရန်လိုအပ်ပါသည်။ အမှန်မှာ ထိုအချက်အလက်များသည် ကုန်ပစ္စည်း၏ အရည်အသွေးကို ရှာဖွေဆန်းစစ်စမ်းသပ်မှုhealthy code analysis နှင့် ဆော့ဖ်ဝဲများကို စမ်းသပ်ပေးသည့်အသိုင်းအဝိုင်းများ testing community ရှိသည့် လက္ခဏာကို ပြသခြင်း ဖြစ်ပါသည်။ ကုန်ထုတ်လုပ်သူများအနေဖြင့် လုံခြုံမှုရှိအောင် စီမံလုပ်ဆောင်ခြင်း နည်းလမ်းကို သုံးပြုချိန်တွင် ပထမ CVE အကြမ်း တွက်ချက်မှု တိုးလာတာမျိုး ဖြစ်နိုင်ပြီး ၎င်းမှာ ပိုမိုပြည့်စုံကျယ်ပြန့်သည့် ရှာဖွေမှုနှင့် လက်ရှိကုဒ်အတွင်း ရှိနေသည့် အားနည်းချက်ကို တိုးတက်အောင် ဆောင်ရွက်မှုကြောင့် ဖြစ်ပါသည်။ အတိတ်၏ အားနည်းချက်များကို ဖော်ပြသင့်ပြီး ထိုအထဲတွင် အားနည်းချက် တစ်ခုလုံးကို ကိုင်တွယ်သည့် patterns နှင့် measures များ ပါဝင်သင့်ပါသည်။ ဥပမာ - ကုမ္ပဏီ၏ CVEs ရာခိုင်နှုန်း အများစုမှာ cross-site scripting (XSS) နှင့် ဆက်စက်မှု ရှိလျင်၊ ပြဿနာအရင်းအမြစ်ကို မှတ်တမ်းတင်ခြင်းနှင့် တုန့်ပြန်မှု (ဥပမာ XSS ကို ဟန့်တားသည့် ဝဘ်ဆိုက်စာမျက်နှာပုံစံများဆိုင်ရာမူဘောင် web template frameworks ကို ပြောင်းလဲခြင်း) နှင့် ရလဒ်များက ဝယ်ယူသုံးစွဲသူများအား ၎င်းတို့သည် အားနည်းချက်များ၏ သားကောင်မဖြစ်နိုင်ကြောင်းကို အရိပ်လက္ခဏာ ပြနိုင်ပြီး ထိုအတွက် သက်သာမှုကို ဆယ်စုနှစ်ကြာ သိနားလည်ကြပြီ ဖြစ်သည်။

5. **Software Bills of Materials (SBOMs) ကို ဖော်ပြထုတ်ဝေပါ။** ကုန်ထုတ်လုပ်သူများအနေဖြင့် ၎င်းတို့၏ ထောက်ပံ့မှု ကွင်းဆက်ကို ကွပ်ကဲနိုင်မှု ရှိသင့်ပါသည်။ အဖွဲ့အစည်းများအနေဖြင့် ပစ္စည်းတစ်ခုခြင်းစီအတွက် SBOMs [2] ကို တည်ဆောက်၊ ထိန်းသိမ်းမွမ်းမံမှု ပြုလုပ်သင့်ပြီး ပစ္စည်းများ ဖြန့်ဖြူးသူထံမှာ အချက်အလက်တောင်းခံနိုင်သကဲ့သို့ SBOMs များကို အောက်ခြေက အသုံးပြုသူများ ရယူနိုင်စေရန်အတွက် လုပ်ဆောင်သင့်ပါသည်။ ထိုကဲ့သို့ လုပ်ဆောင်ခြင်းသည် လုံးလဝိရိယရှိမှုနှင့် ပစ္စည်းထုတ်လုပ်ရာတွင် ပါဝင်သည့် အစိတ်အပိုင်းများအား မိမိအနေဖြင့် နားလည်သိရှိကြောင်း ပြသရာရောက် သကဲ့သို့ ဖြစ်နိုင်ခြေ အန္တရာယ်အသစ်များကိုလည်း သိရှိနိုင်စွမ်းရှိပြီး ထောက်ပံ့မှုကွင်းဆက်၏ modules တစ်ခုတွင် အားနည်းချက်တွေ့ရှိပါက မည်ကဲ့သို့ တုန့်ပြန်ရမည်ကို ဝယ်ယူသုံးစွဲသူများအား နားလည်အောင် လုပ်ဆောင်ပေးနိုင်ပါသည်။

ဖတ်ရှုလိုပါက ဂျပန်နိုင်ငံ၏ စီးပွားရေးရာ၊ ကုန်သွယ်ရေးနှင့် စက်မှုရေးရာ ဝန်ကြီးဌာန(METI) မှ "Guide of Introduction of Software Bill of Materials (SBOM) for Software Management" ဆိုသည့် ခေါင်းစဉ်ဖြင့် ထုတ်ဝေမှု လုပ်ထားပါသည်။ ပွင့်လင်းမြင်သာခြင်းကို ပစ္စည်းထဲတွင်ထည့်သည့် firmware အတွက် အသုံးပြုနိုင်သည့်အပြင် အေအိုင် ဉာဏ်ရည်တု/ machine learning (ML) မှာ အသုံးပြုသည့် ဒေတာနှင့် models များအတွက်လည်း အသုံးပြုနိုင်ပါသည်။ ဝယ်ယူရေးဆုံးဖြတ်ချက်ချနိုင်ရန်အတွက် အထောက်အကူပြုမှုနှင့် operational capabilities များကို ကျော်လွန်၍ SBOMs သည် မသမာသည့် ထောက်ပံ့မှုကွင်းဆက် တိုက်ခိုက်ခံရသည့်အခါ သိအောင်လုပ်ပြီး တုန့်ပြန်နိုင်စွမ်းရှိအောင် လုပ်ဆောင်သည့် နေရာတွင် အရေးကြီးသည့် အခန်းကဏ္ဍတွင် ပါဝင်ပါသည်။

6. **အားနည်းချက်ထုတ်ဖော်ရေး မူဝါဒတစ်ခု Vulnerability disclosure မူဝါဒကို ဖော်ပြထုတ်ဝေပါ။** (1) ကုန်ထုတ်လုပ်သူမှပေးသည့် ပစ္စည်းများအားလုံးကို စစ်ဆေးခွင့်နှင့် အဆိုပါစစ်ဆေးမှုများအတွက် ဖန်တီးပေးသည့် (2) မူဝါဒနှင့်အညီဆောင်ရွက်သည့် လုပ်ရပ်များအတွက် တရားဝင်လုံခြုံမှုပေးသည့် (3) သတ်မှတ်ထားသော အချိန်ကာလတစ်ခုကုန်ဆုံးပြီးနောက် လူထုအား အားနည်းချက်များကို ထုတ်ဖော်မှုခွင့်ပေးသည့် အားနည်းချက်ထုတ်ဖော်ရေး မူဝါဒတစ်ခု ထုတ်ဝေပါ။ ကုန်ထုတ်လုပ်သူများအနေဖြင့် အားနည်းချက်များကို ရှာဖွေ တွေ့ရှိသည့်အခါမှာ ထိုကဲ့သို့ ဖြစ်ရသည့် အကြောင်းရင်းအား သိရအောင် အစွမ်းကုန် တတ်နိုင်သမျှ လုပ်ဆောင်ပြီး အားနည်းချက် အားလုံးကို ဖယ်ရှားမှုမျိုး ပြုလုပ်သင့်ပါသည်။ ဘာသာစကားအညွှန်းအတွက် CISA ၏ Vulnerability Disclosure Policy Template တွင် ကြည့်ပါ။

# လုံခြုံမှုကို ဦးစားပေးသည့် စီးပွားရေး လုပ်ငန်း၏ လုပ်ထုံးလုပ်နည်းများ

1. **Secure by design senior executive sponsor မည်သူ ဖြစ်ကြောင်း လူသိရှင်ကြား အသိပေးပါ။** အဖွဲ့အစည်းအများအပြားအတွင်း လုံခြုံရေးဆိုင်ရာကိစ္စတွင် (အရည်အသွေးဆိုင်ရာ ကဲ့သို့ပင်) ပစ္စည်း၏ လုံခြုံရေးနှင့် ပတ်သက်၍ သိသာသည့် တိုးတက်မှုကိုလုပ်ရန် အကန့်အသတ်ရှိသည့် ပညာရှင်အသင်းများကို လုပ်ပိုင်ခွင့်ပေးလေ့ရှိပါသည်။ လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်သည့် အစီအစဉ်အား ကြီးကြပ်သည့် အမှုဆောင်အရာရှိ မည်သူဖြစ်ကြောင်း လူသိရှင်ကြား အသိပေးခြင်းအားဖြင့် လုံခြုံရေးပစ္စည်း၏ လုံခြုံရေးကိစ္စသည် ဦးစားပေးခံရမည့် စီးပွားရေးလုပ်ရပ် တစ်ခုအဖြစ်သို့ ပြောင်းလဲစေနိုင်ပါသည်။

2. **လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း၏ လမ်းပြမြေပုံကို ဖော်ပြထုတ်ဝေပါ။** ကုန်ထုတ်လုပ်သူများအနေဖြင့် သုံးစွဲသူများ၏ လုံခြုံရေး တိုးတက်ရန်အတွက် SDLC ကို အပြောင်းအလဲလုပ်သည့်အခါတွင် မှတ်တမ်းတင်မှု လုပ်ထားသင့်ပြီး ထိုအထဲတွင် လက်တွေ့စမ်းသပ်မှု၏ အစီရင်ခံစာများ၊ အားနည်းချက်များကို ဖယ်ရှားရန်အတွက် လုပ်ဆောင်ချက်များနှင့် အခြေခံသဘောတရားတွင် ထည့်သွင်းထားသည့် တခြားအရာများ၏ စာရင်းတို့ ပါဝင်ပါသည်။ အရည်အသွေး တိုးတက်ရန်အတွက် ကြိုးစားသည့် ကိစ္စ၌ လုံခြုံရေးတိုးတက်မှုဆိုင်ရာ အစီအစဉ်တွင် တမူထူးသည့် စီစဉ်မှုအဆင့်များ၊ ထိန်းသိမ်းမှုနှင့် တိုးတက်ရေးဆိုင်ရာ အဆင့်များ ရှိပါသည်။ နှုတ်ဖြင့် ပြောမည့်အစား အလုပ်ဖြင့် သက်သေပြဆိုသည့် အနှစ်သာရအရ လမ်းပြမြေပုံနှင့် ၎င်းအဆင့်များကို လူသိအောင် ဖော်ပြထုတ်ဝေခြင်းအားဖြင့် ပစ္စည်းများသည် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံသော ပစ္စည်းဖြစ်ကြောင်း ယုံကြည်စိတ်ချမှု ပိုရစေနိုင်ပါသည်။ အဓိပ္ပာယ်ရှိသည့် တိုးတက်မှုကို ရရှိပြီးသည်နောက် ကုန်ထုတ်လုပ်သူများအနေဖြင့် ပွင့်လင်းမြင်သာမှုဆိုင်ရာ အစီရင်ခံစာတွင် အသေးစိတ်ဖော်ပြထုတ်ဝေမှု လုပ်နိုင်ပါသည်။ ထိုကဲ့သို့ လုပ်ဆောင်ခြင်းသည် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံမှုလုပ်သည် ဆိုသည်ကို ပြသရုံသာမက တခြားသူများလည်း ထိုကဲ့သို့ သက်သေအထောက်အထားကို ကြည့်ပြီး အလားတူ လုပ်ဆောင်လာနိုင်ပါသည်။

3. **Memory-safety လမ်းပြမြေပုံကို ဖော်ပြထုတ်ဝေပါ။** ကုန်ထုတ်လုပ်သူများသည် memory safe languages များကို အသုံးပြု၍ လက်ရှိရှိနေသည့် ပစ္စည်းကို တခြားစနစ်ဖြင့် ပူးပေါင်းစေခြင်းသို့မဟုတ် ပစ္စည်းအသစ်ကို တီထွင်ပြီး အကြီးမားဆုံးထဲတွင်ပါဝင်သော အားနည်းချက်များကို ဖယ်ရှားပစ်ရန် လုပ်ကိုင်နိုင်ပါသည်။ ကိစ္စရပ်တိုင်းအတွက် ထိုကဲ့သို့ လုပ်ဆောင်ရန် မဖြစ်နိုင်သော်လည်း ကုန်ထုတ်လုပ်သူများအနေဖြင့် အက်ပလီကေးရှင်း တစ်ခုလုံးကို ပြန်လည်ရေးတာမျိုး လုပ်ဆောင်မည့်အစား memory safe languages ထဲတွင် application wrappers ကို တီထွင်ပြီး အသုံးပြုသည့်နည်းကို စဉ်းစားသင့်ပါသည်။ ထို အထဲတွင် ကုန်ထုတ်လုပ်သူအနေဖြင့် အလုပ်သမား ခန့်အပ်မှုနှင့် ဆက်စပ်၍ မည်ကဲ့သို့ update လုပ်ထားသည့်အကြောင်း၊ မည်သည့် သင်တန်းများ တက်စေသည့်အကြောင်း၊ ကုဒ်ဆန်းစစ်မှုများ ပြုလုပ်သည့်အကြောင်းနှင့် အတွင်းရေး လုပ်ငန်းစဉ်များအပြင် open source community အားလည်း အလားတူ လုပ်လာစေရန် နည်းလမ်းများဖြင့် ပံ့ပိုးမှု လုပ်နေသည့်အကြောင်းများ ထည့်ဝင်နိုင်ပါသည်။

4. **ရလဒ်များအား ဖော်ပြ ထုတ်ဝေပါ။** လုံခြုံစွာ စီမံပြင်ဆင်ခြင်း အယူအဆအား အကောင်အထည်ဖော်ရန်အတွက် ၎င်းတို့၏ SDLC များကို update လုပ်သည့်အချိန်တွင် အဖွဲ့အစည်းများအနေဖြင့် လျင်မြန်သည့် အောင်မြင်မှု၊ ပိုမိုလွန်ကဲသော အရင်းအမြစ်များ ရရှိကြောင်း တွေ့ရမည်ဖြစ်သကဲ့သို့ မျှော်လင့်မထားသည့် အနှောင့်အယှက်များလည်း ကြုံရနိုင်သည်ကို တွေ့ရမည် ဖြစ်ပါသည်။ လုပ်ငန်းအတွင်း အောင်မြင်မှုနှင့် အဟန့်အတားများကို တင်ပြနိုင်မှုမှတဆင့် ကဏ္ဍတစ်ခုလုံးက ရရှိသည့် ရလဒ်ကနေ သင်ခန်းစာများ ရယူနိုင်ပါသည်။

# အခြေခံ သဘောတရား ၃ - ထိပ်ဆုံးမှ ဦးဆောင်ဦးရွက်မှု ပြုခြင်း

## ရှင်းပြချက်

ယေျဘုယျအားဖြင့် ဤအစီရင်ခံစာ၏ အနှစ်သာရမှာ "လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ခြင်း" ဟု ခေါ်ဆိုနိုင်ပြီး ကုန်ပစ္စည်းကို တီထွင်ဖို့ စီစဉ်သည့်အဆင့်မှ စတင်၍ ဝယ်ယူသုံးစွဲသူ၏ လုံခြုံရေးကို မက်လုံးအနေဖြင့် ထည့်သွင်းစဉ်းစားလုပ်ဆောင်ပေးသည့်နည်း ဖြစ်ပါသည်။ ထိုကဲ့သို့ လုပ်ဆောင်ရာတွင် စီးပွားရေး ရည်မှန်းချက်မှ စတင်ပြီး အကြွင်းမဲ့နှင့် တိကျရှင်းလင်းသည့် ရည်မှန်းချက်အပြင် လိုလားသည့် ရလဒ်များဖြင့် စတင်ပါသည်။ ခေါင်းဆောင်ပိုင်း ပုဂ္ဂိုလ်များမှ လုံခြုံရေးကို စီးပွားရေး၏ ဦးစားပေးအရာအဖြစ် လုပ်ဆောင်ခြင်း၊ လုပ်ငန်းခွင်အတွင်း မက်လုံးများဖန်တီးပေးခြင်းနှင့် လုံခြုံသည့် အနေအထားဖြစ်အောင် ဒီဇိုင်းဖန်တီးရမည်ဟု တစ်ယောက်မကျန် အားလုံးက လက်ခံမှသာလျင် အကောင်းဆုံးရလဒ်ကို ရရှိမည် ဖြစ်ပါသည်။

လုံခြုံသော ပစ္စည်းများ ထုတ်လုပ်ရေးတွင် နည်းပညာကျွမ်းကျင်မှုသည် အရေးပါသော်လည်း ထိုကိစ္စကို နည်းပညာဝန်ထမ်းများသာ လုံးဝ တာဝန်ယူ လုပ်ဆောင်ရမည့်အရာ မဟုတ်ပါ။ လုံခြုံရေးသည် စီးပွားလုပ်ငန်း၏ ဦးစားပေးရမည့် အရာ ဖြစ်သောကြောင့် ထိပ်သီးခေါင်းဆောင်များမှ ဦးဆောင်ဦးရွက်ပြု ရပါမည်။

အကယ်၍ ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများသည် ပထမ အခြေခံ သဘောထား ၂ ရပ်ကို အကောင်အထည်ဖော်ပြီး အဓိပ္ပာယ်ရှိသည့် ပစ္စည်းများ ထုတ်လုပ်နိုင်ပါက တတိယ အခြေခံ သဘောတရားကို အကောင်အထည်ဖော်ရန် လိုအပ်ပါသလားဟု တချို့သူများက တွေးတောမိမှာ ဖြစ်ပါသည်။ ကုမ္ပဏီက ၎င်း၏ အမြော်အမြင်စိတ်ကူး၊ ကုမ္ပဏီ၏ တန်ဖိုး၊ ရိုးရာများကို မည်ကဲ့သို့ တည်ထောင်ထားသည်ဆိုသည့်အချက်သည် ကုန်ပစ္စည်းအပေါ် သက်ရောက်မှုရှိပြီး ထိုအခြေခံသဘောတရားများတွင် ထိပ်ပိုင်းမှ heavy component ရှိပါသည်။ ဤကဲ့သို့ လုပ်ဆောင်ချက်မျိုးကို ကျင့်သုံးသည့် တခြားကဏ္ဍတွင် သိသာသည့် လုံခြုံရေးနှင့် အရည်အသွေး တိုးတက်မှုဖြစ်စေသည့်အကြောင်း ကျွန်ုပ်တို့အနေဖြင့် မြင်တွေ့ရပါသည်။ Noted quality ကျွမ်းကျင်သူ J.M. Juran ရေးသားထားသည်မှာ-

> ***ထိပ်တန်း အရည်အသွေး မြင့်မားမှုကို ထိန်းသိမ်းရန်အတွက် အထက်မန်နေဂျာများ၏ အရည်အသွေးပိုင်းဆိုင်ရာ တာဝန်ယူမှု လုပ်ရန် လိုအပ်ပါသည်။ ထိပ်တန်းအရည်အသွေး မြင့်မားမှုအတွက် ကြိုးစားသည့် ကုမ္ပဏီများတွင် မန်နေဂျာများမှ ဦးဆောင်ဦးရွက်မှု ပြုပြီး လမ်းညွှန်မှု လုပ်ပေးလေ့ ရှိပါသည်။ ချွင်းချက်များကို ကျွန်ုပ်တို့အနေဖြင့် သတိမထားမိပါ။ [3]***

**လုံခြုံရေးသည် ပစ္စည်းအရည်အသွေး၏ အစိတ်အပိုင်းဖြစ်သည်ဟု ယုံကြည်သည်ဟု ပါရှိပါသည်။** လုံခြုံရေးနှင့် အရည်အသွေးသည် စီးပွားရေးအတွက် အရေးကြီးသည့်အရာဖြစ်လာသည့်အခါတွင် ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးဆိုင်ရာကိစ္စကို ကိုင်တွယ်တုန့်ပြန်မှုလုပ်သည့်အခါ စက်မှုဝန်ထမ်းများလက်ထဲ ထိုးအပ်ပြီး ဆောင်ရွက်ခိုင်းမည့်အစား အဖွဲ့အစည်းအနေဖြင့် လုပ်ဆောင်လျင် ပိုမို ထိရောက် လျင်မြန်စွာ ဆောင်ရွက်ပေးနိုင်မည် ဖြစ်သည်။ ထို့အပြင် လိုအပ်သည့် အရင်းအမြစ်များတွင် ရင်းနှီးမြှုပ်နှံမှုလုပ်ထားပြီး ဆော့ဖ်ဝဲလုံခြုံရေးကို စီးပွားရေး၏ အဓိက ဦးစားမှုအဖြစ် အစကတည်းက ဆောင်ရွက်ပါက ရေရှည်တွင် ဆော့ဖ်ဝဲပျက်စီးမှုအတွက် ကုန်ကျစရိတ်ကို လျှော့ချနိုင်သကဲ့သို့ နိုင်ငံတော်၏ လုံခြုံရေးအတွက်လည်း ကောင်းမွန်မှု ဖြစ်စေနိုင်ပါသည်။

ခေါင်းဆောင်ပိုင်းမှ corporate social responsibility (CSR) အစီအစဉ်များကို အကောင်အထည်ဖော်သည့်အတိုင်း အလားတူစွာပင် ဆော့ဖ်ဝဲ ကုန်ထုတ်လုပ်သူများအပါအဝင် လုပ်ငန်း၏ ဘုတ်အဖွဲ့တွင် အကျွမ်းဝင်မှုဖြစ်စေပြီး ဆိုက်ဘာလုံခြုံရေး အစီအစဉ်တွင် ပိုပြီး တက်ကြွစွာ ပါဝင်လမ်းညွှန်မှုများ လုပ်ဆောင်နိုင်ပါသည်။ Corporate cyber responsibility (CCR) ဆိုသည့် အသုံးအနှုန်းကို အသစ်ထွက်ပေါ်လာသည့် အိုင်ဒီယာများအား ဖော်ပြရာတွင် တခါတရံ အသုံးပြုလေ့ရှိသည်။

# ဤအခြေခံ သဘောတရားကို အကောင်အထည်ဖော်ခြင်း

ဤ အခြေခံ သဘောတရားကို လက်တွေ့အကောင်အထည်ဖော်ရန်အတွက် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများမှ အောက်ပါ ခြေလှမ်းများဖြင့် လုပ်ဆောင်နိုင်ပါသည် -

1. **လုပ်ငန်း၏ ဒွေရေးကြေးရေး အစီရင်ခံစာတွင် လုံခြုံအောင် စီမံပြုပြင်ခြင်းဆိုင်ရာ အစီအစဉ် အသေးစိတ်ကို ထည့်သွင်း ဖော်ပြပါ။** အကယ်၍ ကုန်ထုတ်လုပ်ငန်းသည် လူသိရှင်ကြား လည်ပတ်သော ကုန်သွယ်ရေးကုမ္ပဏီဖြစ်ပါက နှစ်စဉ် အစီရင်ခံစာတွင် လုံခြုံမှုရှိအောင် စီမံလုပ်ဆောင်ခြင်း အကြောင်းကို အစီရင်ခံစာ၏ ကဏ္ဍတစ်ခုအတွင်း ထည့်သွင်းဖော်ပြပါ။ မော်တော်ယာဉ်များ၏ တစ်နှစ်တာ အစီရင်ခံစာထဲတွင် ဒါရိုက်ဘာနှင့် ခရီးသည်များ၏ လုံခြုံရေးနှင့် ပတ်သက်သည့် ကဏ္ဍကို ထည့်သွင်းဖော်ပြထားသည်ကို တွေ့ရလေ့ရှိပြီးအရည်အသွေးနှင့် လုံခြုံရေးကော်မတီ၏ ဗဟိုပြုမှုဆိုင်ရာ အချက်အလက်နှင့် ဖြန့်ဝေခြင်းဆိုင်ရာ အချက်အလက်များ ထည့်သွင်းဖော်ပြလေ့ရှိပါသည်။ ဒွေရေးကြေးရေးဆိုင်ရာ အစီရင်ခံစာထဲတွင် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း အစီအစဉ်ကို အသေးစိတ်ဖော်ပြထားခြင်းအားဖြင့် ထိုလုပ်ရပ်များအား ခေတ်စားနေ၍ မတ်ကတ်တင်းအရ မျက်နှာရအောင် လုပ်ခြင်းမျိုး မဟုတ်ပဲ ဤအဖွဲ့အစည်းသည် ဝယ်ယူသုံးစွဲသူ၏ လုံခြုံရေးနှင့် လုပ်ငန်း၏ ဒွေရေးကြေးရေး ရလဒ်များကို အလေးထားကြောင်း ပြသရာရောက်ပါသည်။

2. **သင့်၏ ဒါရိုက်တာ ဘုတ်အဖွဲ့ကို အစီရင်ခံစာများ ပုံမှန်ပေးပို့ပါ။** Chief information security officer (CISO) သည် အစီရင်ခံစာများကို လုပ်ငန်း၏ ဘုတ်အဖွဲ့ကို တင်ပြလေ့ရှိပြီး အစီရင်ခံစာထဲတွင် လက်ရှိလုံခြုံရေးအစီအစဉ်နှင့် အနာဂတ် လုံခြုံရေး အစီအစဉ် အကြောင်း၊ ခြိမ်းခြောက်မှု အန္တရာယ်များအကြောင်း၊ လုံခြုံရေးဆိုင်ရာ သံသယဖြစ်ဖွယ်ရာများနှင့် လုံခြုံရေးတိုက်ခိုက်ခံရမှုအပြင် လုံခြုံရေး အနေအထားနှင့် ကုမ္ပဏီ၏ ကောင်းမွန်စွာ ရှင်သန်ရပ်တည်နိုင်မှုပါဝင်သည့် တခြားသော updated centred အချက်များ ပါဝင်သင့်ပါသည်။ လုပ်ငန်း၏ လုံခြုံရေးအနေအထားဆိုင်ရာ အချက်အလက်ကို ရယူရုံသာမက ဘုတ်အဖွဲ့အနေဖြင့် ပစ္စည်း၏ လုံခြုံရေးဆိုင်ရာ အချက်အလက်နှင့် ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးအပေါ် သက်ရောက်နိုင်မှု အချက်အလက်များကိုပါ တောင်းခံသင့်ပါသည်။ ဘုတ်အဖွဲ့အနေဖြင့် CISO အပေါ်သာ အာရုံစိုက်ထားခြင်းမျိုးမလုပ်သင့်ပဲ တခြားသော ကုမ္ပဏီစီမံခန့်ခွဲရေး အဖွဲ့ဝင်ကို အဓိကထား၍ ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးအန္တရာယ် နည်းပါးအောင် လုပ်ဆောင်ပေးရမည် ဖြစ်ပါသည်။

3. **လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ခြင်းဆိုင်ရာ အရာရှိများအား လုပ်ကိုင်ခွင့် အာဏာပေးခြင်း** အဖွဲ့အစည်းအတွင်းတွင် နည်းပညာအသင်းမှ "ထိပ်သီးခေါင်းဆောင်လက်ခံလာအောင်လုပ်ဆောင်ရခြင်း executive buy-in" နှင့် ခေါင်းဆောင်များကိုယ်တိုင် လုပ်ငန်း၏ စံနှုန်းများကို အသုံးပြု၍ ဝယ်ယူသုံးစွဲသူ၏ လုံခြုံရေးလုပ်ငန်းစဉ်ကို ကိုယ်တိုင်ကိုယ်ကျ ကိုင်တွယ်ဖြေရှင်းရာတွင် သိသာသည့် ကွာခြားမှုများ ရှိပါသည်။ "Executive buy-in" ဆိုသည်မှာ တစ်ယောက်ယောက်က ဝယ်ယူသုံးစွဲသူများအတွက် လုံခြုံရေးဆိုင်ရာ အစီအစဉ်ကို လက်ခံလာအောင် ဖျောင်းဖျပြောဆိုမှု လုပ်ရခြင်းကို ဆိုလိုပြီး လုပ်ငန်း၏ ထိပ်သီးရည်ရွယ်ချက်အဖြစ် မထားရှိခြင်းကို ဆိုလိုပါသည်။ ဝယ်ယူသုံးစွဲသူများအတွက် လုံခြုံရေးရလဒ် ရရှိသည့် ပစ္စည်းထဲတွင် ရင်းနှီးမြှုပ်နှံရန်အတွက် ထိုခေါင်းဆောင်အား လုပ်ပိုင်ခွင့်အာဏာ ပေးရမည်ဖြစ်သည်။

4. **လုပ်ငန်းအတွင်း အဓိပ္ပာယ်ရှိပြီး ကောင်းမွန်သည့် မက်လုံးများကို ဖန်တီးခြင်း** သင့်တော်မှု မရှိသည့် မက်လုံးများ မပေးမိအောင် သတိထားဆောင်ရွက်ချိန်အတွင်း ဝယ်ယူသုံးစွဲသူများအတွက် လုံခြုံရေးစနစ်ကို တိုးတက်အောင် ဆောင်ရွက်နိုင်ခြင်းအပြင် အခြားသော အဖိုးတန် အပြုအမူနှင့် ရလဒ်များကို အသိအမှတ်ပြု ချီးမြှင့်မှုမျိုး လုပ်သင့်ပါသည်။ လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ခြင်း ထိပ်သီးခေါင်းဆောင်မှ ကုန်ထုတ်လုပ်မှု စီမံကြီးကြပ်ရေး၊ ဆော့ဖ်ဝဲထုတ်လုပ်ရေး၊ ပံ့ပိုးကူညီရေး၊ အရောင်းစာရေး၊ ဥပဒေပိုင်းဆိုင်ရာ ဝန်ထမ်းနှင့် အခြားအဖွဲ့အစည်းများအထိ အမှုထမ်းများကို ခန့်အပ်ရာတွင် ဝယ်ယူသုံးစွဲသူများ၏ လုံခြုံရေးကို ပဓာနထားသူကို မက်လုံးပေးသည့် အစီအစဉ်ကို ထည့်သွင်းမှုလုပ်ခြင်း ဥပမာ ရာထူးတိုးမြင့်ပေးခြင်းများ၊ လုပ်အားခ လစာ၊ အပိုဆုကြေးများ၊ စတော့ခ်တွင် ပါဝင်စေခြင်းနှင့် လုပ်ငန်းလည်ပတ်ရာတွင် ပါဝင်သည့် အခြားဘုံလုပ်ငန်းစဉ်တွင် ပါဝင်စေခြင်းစသည့် သင့်တော်သည့် မက်လုံးများ ပေးသင့်ပါသည်။ ဥပမာ - ဆော့ဖ်ဝဲတည်ဆောက်သူများအတွက် ရာထူးတိုးပေးခြင်းဆိုင်ရာ စံများ သတ်မှတ်ရာတွင် လုံခြုံရေးအတွက် တိုးတက်အောင် လုပ်ကိုင်ဆောင်ရွက်မှုအပြင် တခြားစံများဖြစ်သည့် လည်ပတ်နိုင်မှု၊ စွမ်းဆောင်နိုင်မှုနှင့် feature ကို တိုးတက်အောင် ဆောင်ရွက်နိုင်မှု စသည်တို့ကိုပါ ထည့်သွင်း စဉ်းစားသင့်ပါသည်။

5. **လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်သည့် ကောင်စီကို ဖွဲ့စည်းပါ။** တချို့သော ကဏ္ဍတွင် အဖွဲ့အစည်းများမှ အရည်အသွေးဆိုင်ရာ ဗဟိုကောင်စီကို ဖွဲ့စည်းမှု ပြုလုပ်လေ့ရှိပြီး အရည်အသွေးဆိုင်ရာ ကိုယ်စားလှယ်အား အရေးကြီးသည့် လုပ်ငန်းအစိတ်အပိုင်း သို့မဟုတ် ဌာနတွင် ထည့်သွင်းထားလေ့ရှိပါသည်။ ဗဟိုဆိုင်ရာနှင့် ဖြန့်ဖြူးခြင်းဆိုင်ရာ အဖွဲ့ဝင်များကို ပါဝင်စေခြင်းဖြင့် ထိုအဖွဲ့များသည် အဖွဲ့အစည်း၏ အချက်အခြာကျသည့်နေရာမှ telemetry များကို လက်ခံပြီး ထိပ်သီးရည်မှန်းချက် ရရှိဖို့အတွက် အရည်အသွေးများ တိုးတက်မှုရှိအောင် ဆောင်ရွက်မှု လုပ်ကြပါသည်။ အလားတူစွာ လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ခြင်း ကောင်စီသည်လည်း အဖွဲ့အစည်းတစ်ခုလုံးတွင် လုံခြုံမှုရှိအောင် စီမံပြင်ဆင်ခြင်းဆိုင်ရာ ရည်မှန်းချက် တိုးတက်မှုရှိအောင် ဆောင်ရွက်မည်ဖြစ်သည်။

6. **ဝယ်ယူစားသုံးသူများဆိုင်ရာ ကောင်စီကို ဖွဲ့စည်းပြီး ဆင့်ကဲ့ပြောင်းလဲပါ။** ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်ငန်းများတွင် ဝယ်ယူစားသုံးသူများဆိုင်ရာ ကောင်စီကို ထားရှိပြီး ထိုအဖွဲ့ကို ဒေသစုံ၊ ကဏ္ဍစုံနှင့် အရွယ်စုံသည့် ဝယ်ယူသုံးစွဲသူများဖြင့် ဖွဲ့စည်းလေ့ရှိပါသည်။ ထိုကောင်စီများသည် ကုမ္ပဏီ၏ ကုန်ပစ္စည်းနှင့် ပတ်သက်၍ ဝယ်ယူသုံးစွဲသူများ၏ ကြိုက်နှစ်သက်အဆင်ပြေမှုများ၊ စိန်ခေါ်မှုများနှင့် ဆက်စပ်၍ အချက်အလက်များစွာကို ဝေငှနိုင်ပါသည်။ ကောင်စီ၏ လုပ်ငန်းစဉ် agendaကို ရေးဆွဲရာတွင်လည်း ဆွေးနွေးမှုထဲတွင် ပါဝင်မည့်သူများအတွက် ဦးစားပေးအရာ မဟုတ်သည့်တိုင် ဝယ်ယူသုံးစွဲသူအတွက် လုံခြုံရေးဆိုင်ရာ ခေါင်းစဉ်များကို ဆွေးနွေးလုပ်ဆောင်ရမည့် အရာအဖြစ် ထည့်သွင်းသင့်ပါသည်။ ဝယ်ယူသုံးစွဲသူ ကောင်စီက မည်သည့်နေရာကို အစီရင်ခံသည်ကို ထည့်သွင်းစဉ်းစားသည့်အပြင် ကုန်ပစ္စည်းကို ဖြန့်ဖြူးပြီးသည့်နောက် ပစ္စည်း၏ လုံခြုံရေးနှင့် ဆက်စပ်ပြီး ပါဝင်သူများ၏ အမြင်သဘောထားများကို ရရှိအောင် မည်ကဲ့သို့ လုပ်ဆောင်မည့်အကြောင်းကိုပါ ထည့်သွင်းစဉ်းစားသင့်ပါသည်။ ဥပမာ - မတ်ကက်တင်းနှင့် ရောင်းချခြင်းရည်ရွယ်ချက် သို့မဟုတ် ပစ္စည်းစီမံခြင်းနှင့် ပတ်သက်၍ ကောင်စီတွင် ဘက်လိုက်မှု ရှိမရှိ ထည့်သွင်းစဉ်းစားပါ။ လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်းထိပ်သီးခေါင်းဆောင်အနေဖြင့် ဝယ်ယူသုံးစွဲသူများ၏ တုံ့ပြန်မှုရရှိအောင် လုပ်ဆောင်သင့်ပြီး ၎င်းတို့ကို ဤစာစောင်တွင် ပါဝင်သည့် တခြားသော အရာ ဥပမာ လက်တွေ့လေ့လာမှုလုပ်ခြင်းများတွင် ပါဝင်အောင် ပေါင်းကူးပေးတာမျိုး လုပ်ဆောင်နိုင်ပါသည်။

# လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်း၏ ဗျူဟာများ

လုံခြုံသောဆော့ဖ်ဝဲထုတ်လုပ်ရေးမူဘောင် (Secure Software Development Framework (SSDF)) သို့မဟုတ် စံနှုန်းများနှင့် နည်းပညာဆိုင်ရာ အမျိုးသားသိပ္ပံ (National Institute of Standards and Technology's (NIST)) SP 800-218 ဟုလည်း သိကြသည့်အရာသည် လုံခြုံရေးအဆင့်မြင့်သော ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်မှု၏ လုပ်ထုံးလုပ်နည်းအစုဖြစ်ပြီး ထိုအရာကို ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်မှု အဆင့်ဆင့်၏ သက်တမ်းတွင် (SDLC) ထည့်သွင်းအသုံးပြုနိုင်ပါသည်။ ထိုကဲ့သို့ လုပ်ထုံးလုပ်နည်းများကို လုပ်ခြင်းအားဖြင့် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအား ဆော့ဖ်ဝဲထုတ်လုပ်ရာတွင် အားနည်းချက်များကို ပိုမိုရှာဖွေတွေ့ရှိကာ ဖယ်ရှားနိုင်စေသကဲ့သို့ အားနည်းချက်များကြောင့် ဖြစ်ပေါ်လာတတ်သည့် ဆိုးကျိုးများကိုလည်း လျော့ပါးစေနိုင်သည့်အပြင် ထိုအားနည်းချက်များအား ဖြစ်စေသည့်အကြောင်းရင်းများကို သိရှိနိုင်ပြီး အနာဂတ်တွင် ထပ်မဖြစ်ရန် ကာကွယ်လုပ်ဆောင်စေနိုင်မည်ဖြစ်ပါသည်။

အာဏာပိုင်အဖွဲ့အစည်းများအနေဖြင့် လုံခြုံမှုရှိအောင် ပြင်ဆင်စီမံခြင်းဗျူဟာကို အသုံးပြုရန် တိုက်တွန်းလိုပြီး SSDF ကို အသုံးပြုသော အခြေခံသဘောတရားများကို ထည့်သွင်း အသုံးပြုသင့်ပါသည်။ ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနေဖြင့် ရေးဆွဲထားသော လမ်းပြမြေပုံကို တီထွင်သင့်ပြီး ၎င်းတို့၏ လုပ်ငန်းတွင့် လုံခြုံအောင် စီမံပြင်ဆင်ထားသည့် နည်းဖြင့် ဆော့ဖ်ဝဲများ ထုတ်လုပ်ရန်အတွက် ဖြစ်ပါသည်။ အောက်ပါစာရင်းသည် လမ်းပြမြေပုံအတွက် အကောင်းဆုံး လုပ်ထုံးလုပ်နည်း ဖြစ်ပါသည်။

- **လုံခြုံရေးအတွက် ကောင်းမွန်သော ကွန်ပြူတာပရိုဂမ် ဘာသာရပ် (SSDF PW.6.1)** အခွင့်သာတိုင်း memory လုံခြုံရေးအတွက် ကောင်းမွန်သော ဘာသာရပ်များကို (memory safe languages) ဦးစားပေးအသုံးပြုပါ။ အာဏာပိုင်အဖွဲ့အစည်းများအနေဖြင့် memory specific mitigations သည် shorter-term tacktiics for legacy codebases အတွက် အသုံးဝင်နိုင်ကြောင်းကို နားလည်ပါသည်။ ဥပမာ တချို့မှာ C/C++ ဘာသာရပ် ဖွံ့ဖြိုးမှုများ၊ hardware mitigations, address space layout rendomization (ASLR), control-flow integrity (CFI) နှင့် fuzzing တို့ ပါဝင်ပါသည်။ သို့သော်လည်း memory safe programming languages များကို အသုံးပြုခြင်းသည် ပျက်စီးမှုများကို ဖယ်ရှားပေးနိုင်သည်ဟု လူပြောများလာသည့်အတွက် ကုန်ထုတ်လုပ်သူများအနေဖြင့် ၎င်းကို အသုံးပြုနိုင်မည့် နည်းလမ်းကို ရှာဖွေသင့်ပါသည်။ ခေတ်သစ် memory safe languages ထဲတွင် C#, Rust, Ruby, Java, Go နှင့် Swift တို့ ပါဝင်ပါသည်။ NSA ၏ ကွန်ပြူတာ မှတ်ဉာဏ်လုံခြုံရေးဆိုင်ရာ အချက်အလက်များအကြောင်းဖတ်ပြီး ပိုမိုလေ့လာနိုင်ပါသည်။
- **လုံခြုံသော ဟဒ်ဝဲအခြေခံအုတ်မြစ် (Secure Hardware Foundation)** ဆော့ဖ်ဝဲရေးရာတွင် အသေးစိတ် memory ကာကွယ်ခြင်းနည်းကို ထည့်သွင်းအသုံးပြုပါ။ ဥပမာ Capability Hardware Enhance RISC Instructions (CHERI) ကနေ ဖော်ပြထားတာမျိုးဖြစ်ပြီး သမားရိုးကျ ဟဒ်ဝဲများကို ဆက်နွယ်အသုံးပြုနိုင်စေသည့် အရာများဖြစ်သည့် Instruction-Set Architectures (ISAs) နှင့် အခြားသော Trusted Platform Modules and Hardware Security Modulesတို့ ဖြစ်ပါသည်။ အချက်အလက်များ ပိုသိလိုပါက Cambridge တက္ကသိုလ်၏ CHERI ဝဘ်ဆိုက်စာမျက်နှာ တွင် လေ့လာနိုင်ပါသည်။
- **လုံခြုံမှုရှိသော ဆော့ဖ်ဝဲအစိတ်အပိုင်းများ (Secure Software Components) (SSDF PW 4.1)(SSDF PW 4.1)** စေ့စပ်သေခြာပြီး လုံခြုံမှုရှိသည့် ဆော့ဖ်ဝဲအစိတ်အပိုင်းများကို ဝယ်ယူသုံးစွဲပါ။ (ဥပမာ software libraries, modules, middleware, frameworks) ကို လိုင်စင်ရကုမ္ပဏီများ၊ လူတိုင်းထည့်ဝင်နိုင်သည့် open source နှင့် အခြား တတိယ ပါတီထုတ်လုပ်သူများထံမှ ရယူ ထိန်းသိမ်းပါ။
- **ဝဘ်ဆိုက်စာမျက်နှာ ပုံစံပြားဆိုင်ရာ မူဘောင်များ (Web template frameworks) (SSDF PW.5.1)(SSDF PW.5.1)** Cross-site scripting ကဲ့သို့သော user input တိုက်ခိုက်မှုကို အလိုအလျောက် ရှောင်ရှားနိုင်သည့် web template framework များကို အသုံးပြုပါ။
- **Parameterized queries (SSDF PW 5.1)** SQL injection တိုက်ခိုက်မှုကို ရှောင်ရှားရန်အတွက် queries ထဲတွင် user input ပါဝင်နေသည်ကို အသုံးပြုမည့်အစား parameterized queries ကို အသုံးပြုပါ။
- **ပုံသေနှင့် ပြောင်းလဲမှုရှိသောအပ်ပလီကေးရှင်း လုံခြုံရေး စမ်းသပ်မှု (Static and dynamic application security testing) (SAST/DAST)** (SSDF PW.7.2, PW.8.2) ထိုပစ္စည်းကို အသုံးပြု၍ ဆော့ဖ်ဝဲ၏ အရင်းအမြစ်ကုဒ်ကို ဆန်းစစ်ပြီး ဖြစ်တတ်သည့် အမှားများ၏ အမူအကျင့်များကို ဖော်ထုတ်နိုင်ရန် အသုံးပြုပါ။ ၎င်းတို့သည် ဆော့ဖ်ဝဲတွင် ဖြစ်တတ်သည့် memory ပြဿနာမှ သိုလှောင်ထားသည့် အချက်အလက်များရယူရာတွင် ဖြစ်တတ်သည့်အမှားများအတွက် အကျုံးဝင်စေသည် (ဥပမာ - SQL injection ကို မကာကွယ်သည့် အချက်အလက်ထည့်သွင်းမှု) တို့ ဖြစ်ပါသည်။ SAST နှင့် DAST တို့သည် အခြားသော စမ်းသပ်မှုများနှင့် လိုက်လျောညီတွေ့ ကိုက်ညီမှု ရှိပါသည်။ SAST နှင့် DAST သည် မျှော်မှန်းထားသည့် လုံခြုံရေးရရှိရန်အတွက် ထိုဆော့ဖ်ဝဲသည် တစ်ခုချင်းစီအတွက် စမ်းသပ်သည့် အခါတွင်ဖြစ်စေ ပေါင်းစပ်ထားသည့်အရာအတွက်ဖြစ်စေ ကိုက်ညီမှု ရှိသင့်ပါသည်။ ပြဿနာကို သိရသည့်အခါ ထုတ်လုပ်သူများအနေဖြင့် အားနည်းချက်ဖြစ်စေသည့် အရင်းအမြစ်ကို စနစ်တကျ ဖော်ထုတ်ဆန်းစစ်မှု လုပ်သင့်ပါသည်။

- **ကုဒ်သုံးသပ်ချက် (Code review)** (SSDF PW.7.1, PW.7.2) အရည်အသွေးမြင့်သော ဆော့ဖ်ဝဲဖြစ်ရန်အတွက် ထည့်သွင်းထားသည့် ကုဒ်များကို အခြား ဆော့ဖ်ဝဲရေးသူနှင့် လုပ်ဖော်ကိုင်ဖက်များ၏ ဆန်းစစ်မှု မှတ်ချက်များ သို့မဟုတ် "error seeding" ရယူရန် ကြိုးစားသင့်ပါသည်။
- **SSoftware Bill of Materials (SBOM) (SBOM) (SSDF PS.3.2, PW.4.1)** အခြားသော ဆော့ဖ်ဝဲများပါဝင်ပါက တီထွင်မှုတွင် SBOM[4] ကို ထင်သာမြင်သာမှုရှိရန် လုပ်ဆောင်ပြီးမှ ထည့်သွင်းအသုံးပြုသင့်ပါသည်။
- **အားနည်းချက်ဖော်ပြသည့် အစီအစဉ်များ (Vulnerability disclosure programs)** (SSDF RV.1.3) လုံခြုံရေး သုတေသီများ တွေ့ရှိသည့် အားနည်းချက်များကို ဖော်ပြစေနိုင်မည့် အစီအစဉ်များ ချမှတ်တည်ထောင်ထားသင့်ပြီး အားနည်းချက်များကို ထုတ်ဖော်ပြောဆိုသည့် အခါတွင်လည်း တရားရေးရာအရ ကာကွယ်မှုရှိအောင် လုပ်ဆောင်ပေးရပါမည်။ ဤအစီအပိုင်းတစ်ခုအဖြစ် ထုတ်လုပ်သူများသည် အားနည်းချက်များ၏ အရင်းအမြစ်ကို ရှာဖွေဖော်ထုတ်နိုင်မည့် လုပ်ငန်းစဉ်ကိုလည်း ချမှတ်ထားရှိသင့်ပါသည်။ ထိုလုပ်ငန်းစဉ်ထဲတွင် လုံခြုံအောင် ပြင်ဆင်စီမံခြင်း လုပ်ထုံးလုပ်နည်း (သို့မဟုတ် အခြား ဆင်တူမှုရှိသော လုပ်ထုံးလုပ်နည်းများ) ကို အသုံးပြုခြင်းသည် အားနည်းချက်ဖြစ်ပေါ်တတ်သည်ကို ကာကွယ်ပေးနိုင်ခြင်း ရှိမရှိဆိုသည့်အချက်ကိုပါ ထည့်သွင်းစဉ်းစားသင့်ပါသည်။
- **CVE ပြည့်စုံခြင်း (CVE completeness)** ဆော့ဖ်ဝဲထုတ်လုပ်မှု ကဏ္ဍတစ်ခုလုံးအတွက် လုံခြုံရေး အားနည်းချက်ဖြစ်စေသည့် ပြဿနာအရင်းအမြစ်ကို စိစစ်စီစဉ်ဖြာဆန်းစစ်မှု လုပ်ဆောင်ရာတွင် ထုတ်ဝေထားသည့် CVE မှတ်တမ်းများတွင် ပြဿနာဖြစ်စေသည့် အရင်းအမြစ်အချက်အလက်များ သို့မဟုတ် ဖြစ်တတ်သည့် အားနည်းချက်ဆိုင်ရာ မှတ်တမ်းများ (CWE) ပါဝင်အောင် လုပ်ထားသင့်ပါသည်။ CVE မှတ်တမ်းတိုင်း မှန်ကန် ပြည့်စုံမှုရှိမရှိ သေချာ ဆောင်ရွက်ရာတွင် အချိန်ကြာမြင့်နိုင်သော်လည်း ထိုလုပ်ရပ်သည် မတူညီသည့် လုပ်ငန်းများမှ ခေတ်ရေစီးကြောင်းကို ခန့်မှန်းသိစေနိုင်ပြီး ကုန်ထုတ်လုပ်သူများနှင့် ဝယ်ယူသုံးစွဲသူအတွက်ပါ အကျိုးရှိစေမည်ဖြစ်သည်။ CISA ၏ အာနည်းချက်ကို စီမံခြင်းဆိုင်ရာနှင့် ပတ်သက်၍ ပိုမိုသိလိုပါက CISA ၏ Stakeholder- specific SVCC guidance တွင် လေ့လာနိုင်ပါသည်။
- **အလွှာအဆင့်ဆင့်ဖြင့် နက်ရှိုင်းစွာ ကာကွယ်ထားခြင်း (Defense-in-Depth)** လုံခြုံရေး ထိန်းချုပ်မှုတစ်ခု တိုက်ခိုက်ခံရမှုမှအစ စနစ်တစ်ခုလုံး တိုက်ခိုက်ခံရမှု မဖြစ်စေရန်အတွက် အလွှာအဆင့်ဆင့်ဖြင့် နက်ရှိုင်းစွာ ကာကွယ်ထားသည့် ဒီဇိုင်းဖြင့် တည်ဆောက်ထားပါ။ ဥပမာ အသုံးပြုခွင့် ကန့်သတ်ခြင်းနှင့် အချက်အလက်ရယူနိုင်မည့်သူများကို ကန့်သတ်ခြင်းသည် အကောင့်တိုက်ခိုက်ခံရမှုများကို လျော့ကျစေနိုင်ပါသည်။ ထို့အပြင် ဆော့ဖ်ဝဲများအားတစ်ခုချင်းစီခွဲခြားရယူမှုလုပ်ထားခြင်းအားဖြင့် စနစ်တစ်ခုလုံး တိုက်ခိုက်မှုမဖြစ်စေရန် ကာကွယ်ပေးရာ ရောက်ပါသည်။
- **စိတ်ကျေနပ်ဖွယ်ရာကောင်းသော ဆိုက်ဘာစွမ်းဆောင်မှုဆိုင်ရာ ရည်မှန်းချက်များ (Satisfy Cyber Performance Goals (CPGs)** အခြေခံ လုံခြုံရေးဆိုင်ရာ လုပ်ထုံးလုပ်နည်းနှင့် ကိုက်ညီသည့် ဆော့ဖ်ဝဲကို တီထွင်ပါ။ CISA ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စွမ်းဆောင်မှု ရည်မှန်းချက်များ သည် အဖွဲ့အစည်းများမှ ထည့်သွင်းလုပ်ဆောင်သင့်သည့် အခြေခံ ဆိုက်ဘာကာကွယ်ရေး လုပ်ထုံးလုပ်နည်းများကို ဖော်ပြထားပါသည်။ ထို့အပြင် သင့်အဖွဲ့အစည်း၏ အနေအထားအား ပိုမိုခိုင်မာစေရန်အတွက် CSIA ၏ CPG နှင့် ဆင်တူသော UK ၏ ဆိုက်ဘာ ဆန်းစစ်အကဲဖြတ်မှုဆိုင်ရာ မူဘောင် (Cyber Assessment Framework) ကိုလည်း လေ့လာနိုင်ပါသည်။ CPGs MFA အကယ်၍ ကုန်ထုတ်လုပ်သူများမှ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ စွမ်းဆောင်မှု ရည်မှန်းချက်များ CPG နှင့်အညီ ဆောင်ရွက်မှုမရှိလျင် - ဥပမာ အမှုထမ်းအားလုံးအတွက် လှည့်စားဖြားယောင်းမှုကို ကာကွယ်ရန် တဆင့်ခံ စိစစ်မှုမျိုး မရှိခြင်းသည် - ထိုကုန်ပစ္စည်းများကို လုံခြုံအောင် ပြုပြင်စီမံထားသည့် ပစ္စည်းဟု မဆိုနိုင်ပါ။

အာဏာပိုင် အဖွဲ့အစည်းများ အနေဖြင့် ထိုအပြောင်းအလဲများသည် အဖွဲ့အစည်းများ၏ အနေအထားကို သိသာစွာ ပြောင်းလဲမှုဖြစ်စေသည်ကို သဘောပေါက်ပါသည်။ အရေးကြီးမှု၊ ခက်ခဲရှုတ်ထွေးမှုနှင့် စီးပွားရေးအပေါ် သက်ရောက်မှုကို အခြေခံပြီး ၎င်းတို့၏ လုံခြုံရေး အစီအစဉ်ကို အစောပိုင်းကတည်းက ဦးစားပေး လုပ်ရမည်ဖြစ်ပါသည်။ ထိုလုပ်ထုံးလုပ်နည်းများကို ဆော့ဖ်ဝဲအသစ်အတွက် အသုံးပြုနိုင်သည့်အပြင် သမားရိုးကျဆော့ဖ်ဝဲနှင့် ကုန်ပစ္စည်းအတွက်ပါ တိုးချဲ့အသုံးပြုမှုလည်း လုပ်နိုင်ပါသည်။ တချို့ ကိစ္စရပ်များတွင် ကုန်ပစ္စည်းတစ်ခု၏ အရေးကြီးမှုနှင့် ကြုံရနိုင်သည့် အခက်အခဲအနေအထားကြောင့် ထိုလုပ်ထုံးလုပ်နည်းများကို အလျင်အမြန် အသုံးပြုမှု ဖြစ်စေနိုင်ပါသည်။ တချို့အတွက် ထိုလုပ်ထုံးလုပ်နည်းများသည် တဆင့်ချင်း လုပ်ဆောင်ရမည် ဖြစ်ပါသည်။

[4] တချို့သော အာဏာပိုင်အဖွဲ့အစည်းများသည် ဆော့ဖ်ဝဲ၏ ထောက်ပံ့မှု ကွင်းဆက်တွင် လုံခြုံရေးအာမခံချက် ရရန်အတွက် နည်းလမ်းများ ရှာဖွေနေပါသည်။

# အလိုအလျောက် လုံခြုံစွာ ရှိနေခြင်း၏ ဗျူဟာများ

ဆော့ဖ်ဝဲများ ထုတ်လုပ်ရာတွင် ကုန်ထုတ်လုပ်သူများအနေဖြင့် လုံခြုံအောင် ပြင်ဆင်စီမံထားသည့် လုပ်ထုံးလုပ်နည်းများ (Secure-by-Design) ကို အသုံးပြုသည့်အပြင် အလိုအလျောက် လုံခြုံစွာ ရှိနေခြင်း (Secure-by-Default) နည်းကိုပါ ဦးစားပေးရန် အာဏာပိုင် အေဂျင်စီများ အကြံပြုလိုပါသည်။ ၎င်းသည် ဆော့ဖ်ဝဲများကို ခေတ်နှင့်အညီ ပြောင်းသည့်အခါတွင်လည်း ထိုလုပ်ထုံးလုပ်နည်းများနှင့် လိုက်လျောညီထွေမှု ဖြစ်စေနိုင်ပါသည်။ ဥပမာ -

- **Eliminate default passwords (အလိုအလျောက် password ထားရှိပေးခြင်းကို မလုပ်ရန်)** လူတိုင်းမျှဝေသုံးစွဲနိုင်သည့် password လျှို့ဝှက်နံပတ်များကို ကုန်ပစ္စည်းတွင် အလိုအလျောက် ထားရှိပေးခြင်းမျိုး မလုပ်သင့်ပါ။ အလိုအလျောက် password ထားရှိပေးခြင်း မလုပ်ရန် အတွက် အာဏာပိုင် အေဂျင်စီအနေဖြင့် အကြံပြုလိုသည်မှာ ဆော့ဖ်ဝဲ ထည့်သွင်းချိန်နှင့် ပုံဖော်ချိန်တွင် ဆော့ဖ်ဝဲအသုံးပြုမည့်သူများအား ခိုင်မာသည့် password များ ထားရှိပြီးမှ အသုံးပြုနိုင်အောင် ပြုလုပ်သင့်ကြောင်း အကြံပြုလိုပါသည်။

- **အထူးအသုံးပြုသူများအတွက် အချက်အလက်အမျိုးမျိုး မှန်ကန်ကြောင်း အထောက်အထား (Multifactor Authentication (MFA))ကို ပြဋ္ဌာန်းရမည်ဖြစ်သည်။** လုပ်ငန်းအများအပြားမှ တာဝန်ရှိသူများသည် ၎င်းတို့၏ အကောင့်များကို MFA နည်းဖြင့် ကာကွယ်မှု မလုပ်ထားကြကြောင်း ကျွန်ုပ်တို့အနေဖြင့် လေ့လာသိရှိရပါသည်။ တာဝန်ရှိသူများသည် ပစ်မှတ်ထားခံရနိုင်ခြေများသည့်အတွက် MFA တွင် ပါဝင်မည့်အစား ဖယ်ထားသင့်ပါသည်။ ထို့အပြင် တာဝန်ရှိသူအား MFA လုပ်ဆောင်ရန် ပုံမှန်စေခိုင်းသင့်ပြီး ၎င်းတို့၏ အကောင့်တွင် အောင်မြင်စွာ လုပ်ဆောင်နိုင်သည်အထိ လုပ်ခိုင်းသင့်ပါသည်။ နယ်သာလန်၏ NCSC လမ်းညွှန်မှုသည် CISA ၏ လမ်းညွှန်မှုနှင့် တူညီနေပြီး ၎င်းတို့၏ အချက်အလက်များပိုမိုသိလိုလျင် Mature Authentication Factsheet တွင် ကြည့်ရှုနိုင်ပါသည်။

- **တစ်ကြိမ်ဆိုင်းလော့အင်ဝင်ခြင်း (Single sign-on (SSO))** IT အိုင်တီများအနေဖြင့် ခေတ်မှီသော စံချိန်စံညွှန်းမှတဆင့် တစ်ကြိမ်လော့အင်ဝင်နိုင်သည့် နည်းပညာကို အသုံးပြုသင့်ပါသည်။ ဥပမာ Security Assertion Markup Language (SAML) နှင့် OpenID Connect (OIDC) တို့ ဖြစ်ပါသည်။ ထိုအရာကို ထပ်မံကုန်ကျခံစရာမလိုအောင် အလိုအလျောက် လုပ်ဆောင်ပေးသင့်ပါသည်။

- **လုံခြုံစွာလော့အင်ဝင်ထားခြင်း (Secure Logging)** သုံးစွဲသူများထံမှ အဖိုးအခ ထပ်တောင်းခံမှုမလုပ်ပဲ အရည်အသွေးမြင့်သော ဝဘ်ဆိုက်လှုပ်ရှားမှုမှတ်တမ်းကို လုပ်ဆောင်နိုင်ပါသည်။ ဝဘ်ဆိုက်လှုပ်ရှားမှု မှတ်တမ်းသည် လုံခြုံရေးချိုးဖောက်မှု ခံရနိုင်သည့်အရာကို သိရှိအောင် လုပ်ဆောင်ရာတွင် အင်မတန် အရေးပါသည်။ လုံခြုံရေး ချိုးဖောက်မှု ဖြစ်မဖြစ် သံသယဖြစ်နေသည့်အချိန် သို့မဟုတ် အတည်ပြုဖို့ စုံစမ်းနေချိန်အတွက်လည်း အရေးပါပါသည်။ လုံခြုံရေးအချက်အလက်များနှင့် ဖြစ်ရပ်စီမံခန့်ခွဲမှု စနစ်များကို ကမ္ဘာတလွှား၏ ကိုဩဒိနိတ်အချိန် (UTC)၊ စံသတ်မှတ်ထားသော နယ်မြေအချိန်ပုံစံနှင့် ခိုင်မာသောမှတ်တမ်းတင်ခြင်းနည်းလမ်းများကို အသုံးပြုသည့် application programming interface (API) နှင့် အလွယ်တကူပေါင်းစည်းအသုံးပြုခြင်းကဲ့သို့ အကောင်းဆုံး လုပ်ထုံးလုပ်နည်းများကို ထည့်သွင်းစဉ်းစားပါ။

- **ဆော့ဖ်ဝဲ ခွင့်ပြုချက်မှု (Software Authorization Profile)** ဆော့ဖ်ဝဲထုတ်လုပ်သူများအနေဖြင့် ခွင့်ပြုချက်ရရှိသည့်ပုဂ္ဂိုလ်များနှင့် ၎င်းအလုပ်အတွက် လိုအပ်သည့်အချက်များကိုသာ ယူခွင့်ရရန် လုပ်သင့်ပါသည်။ သတ်မှတ်ထားသည့် ခွင့်ပြုချက်မရှိပဲ ဝင်ရောက်ပါက အန္တရာယ်ရှိကြောင်း သိသာသည့် သတိပေးမှုများ လုပ်ဆောင်ပေးသင့်ပါသည်။ ဥပမာ - ဆရာဝန်သည် လူနာ၏ ကျန်းမာရေးဆိုင်ရာ မှတ်တမ်းများအားလုံးကို ကြည့်ရှုခွင့်ရှိသော်လည်း ကျန်းမာရေး အချိန်ဇယား ရေးဆွဲသူသည် ရက်ချိန်းအချိန်ဇယားရေးဆွဲရန်အတွက် အချက်အလက်မှ လွဲ၍ ကျန်အချက်များ ဝင်မကြည့်နိုင်ရင် လုပ်ဆောင်ခြင်းမျိုး ဖြစ်ပါသည်။

- **Forward-looking security over backwards compatibility.** ခေတ်ဟောင်း ဆော့ဖ်ဝဲများသည် လုံခြုံရေးဆိုင်ရာအတွက် အန္တရာယ်ရှိစေနိုင်သော်လည်း ၎င်းတို့ကို ဆက်လက်ထည့်သွင်း အသုံးပြုနိုင်ရန် လုပ်ဆောင်ထားလျက် ရှိပါသည်။ ဆော့ဖ်ဝဲဟောင်းများကို ခေတ်နှင့်အညီ ပြန်လည်သုံးစွဲနိုင်ရန် လုပ်ဆောင်ခြင်းထက် လုံခြုံရေးကို ဦးစားပေးရမည် ဖြစ်သကဲ့သို့ လုံခြုံရေးအသင်းသားများကိုလည်း လုံခြုံမှုမရှိသည့် အရာများကို ဖယ်ရှားခွင့်ပေးရမည်ဖြစ်ပြီး ထိုကဲ့သို့ ဖယ်ရှားမှုသည် လုပ်ငန်းအပြောင်းအလဲများ ဖြစ်စေသည့်တိုင်အောင် ဖယ်ရှားခွင့်ပေးသင့်ပါသည်။

- **တင်းကြပ်မှုအရွယ်အစားကို ခြေရာခံပြီး လျှော့ချခြင်း (Track and reduce "hardening guide" size)** တင်းကြပ်မှု အရွယ်အစားအား လျှော့ချပြီး ပုံစံသစ် ဆော့ဖ်ဝဲများ ထုတ်လုပ်သည့်အခါတွင် တင်းကြပ်မှုအရွယ်အစားကို တဖြေးဖြေးချည်းစီ လျှော့ချနိုင်ရန် လုပ်ဆောင်သင့်ပါသည်။ တင်းကြပ်ခြင်းကို ကုန်ပစ္စည်းထုတ်လုပ်ရေးအတွက် ပူးတွဲထည့်တွင်းရမည့်အရာအဖြစ် အသုံးပြုသင့်ပါသည်။ အာဏာပိုင် အဖွဲ့အစည်းများအနေဖြင့် ဝယ်ယူသုံးစွဲသူများနှင့် ထားရှိသည့် မိတ်ဆက်ဆက်ဆံရေး၊ ကုန်ထုတ်လုပ်သူအသင်းများ၏ ကြိုးစားဆောင်ရွက်မှုနှင့် ဝယ်ယူသုံးစွဲသူများ၏ အတွေ့အကြုံ (UX) သည် တင်းကြပ်မှုကို အချိန်တိုအတွင်း လျှော့ချမှုဖြစ်စေနိုင်သည်ကို သဘောပေါက်နားလည်ပါသည်။

- **သုံးစွဲသူအတွေ့အကြုံ အကျိုးသက်ရောက်မှုဆိုင်ရာ လုံခြုံရေးအနေအထားကိုလည်း ထည့်သွင်းစဉ်းစားရန် လိုအပ်ပါသည်။** လုံခြုံရေး setting တိုင်းသည် အသုံးပြုသူများအတွက် အပိုဝန်ထုတ်ဖြစ်စေနိုင်သည့်အတွက် ထိုအချက်ကို စီးပွားရေးအကျိုးအမြတ်နည်းစေနိုင်ခြင်းနှင့် တိုက်ဆိုင်၍ အကဲဖြတ်သင့်ပါသည်။ အကောင်းဆုံးအနေအထားအတွက် setting ရှိမနေသင့်ဘဲ ၎င်းအစား အကောင်းဆုံးလုံခြုံမှု setting ကို သာလျင် နဂိုကတည်းက အလိုအလျောက် ထည့်သွင်းထားတာမျိုး ဖြစ်သင့်ပါသည်။ ဖွဲ့စည်းပုံစနစ် မဖြစ်မနေလိုအပ်လာလျင် ဖြစ်ပေါ်လာနိုင်သည့် ခြိမ်းခြောက်မှုအန္တရာယ်ကို အလိုအလျောက် ကာကွယ်ပြီးသောနည်းကို အသုံးပြုသင့်ပါသည်။

အာဏာပိုင် အဖွဲ့အစည်းများအနေဖြင့် ထိုအပြောင်းအလဲများသည် ဆော့ဖ်ဝဲအသုံးပြုခြင်းဆိုင်ရာ လုပ်ငန်းလည်ပတ်ရေးအပေါ် သက်ရောက်မှုဖြစ်နိုင်သည်ကို နားလည်ပါသည်။ ထို့ကြောင့် သုံးစွဲသူ၏ အသုံးပြုမှု အတွေ့အကြုံသည် လုပ်ငန်းလည်ပတ်ရေးနှင့် လုံခြုံရေး ထိန်းညှိမှုအတွက် အလွန်အရေးကြီးပါသည်။ အာဏာပိုင် အဖွဲ့အစည်းများ၏ အမြင်အရ ဆော့ဖ်ဝဲလုံခြုံရေးရှိအောင် ဦးစားပေးလုပ်ကိုင်သည့် လုပ်ထုံးလုပ်နည်းသည် အဖွဲ့အစည်းအတွက် အရေးကြီးဆုံး လုပ်ဆောင်ရမည့် ပထမခြေလှမ်းဖြစ်ပြီး ထိုအိုင်ဒီယာများကို ဦးစားပေးသည့် အနေဖြင့် ထိပ်သီးခေါင်းဆောင်များသည် လမ်းပြမြေပုံ ရေးဆွဲပြီး လုပ်ဆောင်သင့်ပါသည်။ ဝယ်ယူသုံးစွဲသူများ၏ သုံးစွဲမှုအတွေ့အကြုံသည် အရေးကြီးသော်လည်း တခါတရံ အရည်အသွေးမြင့်တင်ရန်အတွက် လုပ်ဆောင်ရာတွင် ဝယ်ယူသုံးစွဲသူများမှ ဝင်ရောက်ပါဝင်ခြင်း မလုပ်လိုသည့် အနေအထားများ ရှိတတ်သည်ကိုလည်း အာဏာပိုင် အေဂျင်စီများအနေဖြင့် သတိပြုမိပါသည်။ ထို့ကြောင့် ဝယ်ယူသုံးစွဲသူများသည် အားနည်းချက်ရှိသူအဖြစ် တသက်လုံး မဖြစ်ရလေအောင် ခေတ်ရေစီးကြောင်းတွင် ပါဝင်လာစေရန်အတွက် ကုန်ထုတ်လုပ်သူများအနေဖြင့် အဓိပ္ပာယ်ရှိသည့် မက်လုံးများဖြင့် ဝယ်ယူသုံးစွဲသူများအား ဆွဲဆောင်နိုင်ရန် ပြုလုပ်သင့်ပါသည်။

# တင်းကြပ်မှု နှင့် ဖြေလျော့မှု လမ်းညွှန်ချက်များ
# (HARDENING VS LOOSENING GUIDES)

ဆော့ဖ်ဝဲထုတ်လုပ်ရန် စီစဉ်ရေးဆွဲချိန်မှစ၍ လုံခြုံဘေးကင်းသော ထိန်းချုပ်မှုကို ခိုင်ခံ့စွာ မလုပ်ဆောင်သည့်အတွက် တင်းကြပ်မှု လမ်းညွှန်ချက်များ (hardening guides) ကို လိုအပ်ခြင်း ဖြစ်စေနိုင်သည်။ တဖက်တွင်လည်း ထိုတင်းကြပ်မှုလမ်းညွှန်ချက်များသည် လုံခြုံမှုမရှိသောအရာများ၏ တိုက်ခိုက်ခံရနိုင်ခြေရှိမှုကို သိသာစေသည့် လမ်းပြမြေပုံလည်း ဖြစ်စေနိုင်ပါသည်။ အဖွဲ့အစည်းအများအပြားအနေဖြင့် တင်းကြပ်ရေးလမ်းညွှန်ချက်များကို နားမလည်သည့်အတွက် ၎င်းတို့၏ ကုန်ပစ္စည်းများကို မလုံခြုံသည့်အနေအထားဖြစ်စေနိုင်ပါသည်။ တဖက်တွင် ထိုတင်းကြပ်မှုလမ်းညွှန်ချက်များအစား ဖြေလျော့မှုလမ်းညွှန်ချက်ကို အသုံးပြုသင့်ပါသည်၊ မည်သည့်အရာကို ပြောင်းလဲသင့်ကြောင်း ရှင်းပြချက်သာမက ဖြစ်နိုင်ခြေရှိသည့် လုံခြုံရေးခြိမ်းခြောက်မှုကိုလည်း မှတ်တမ်းတင်ထားသင့်ပါသည်။ ထိုလမ်းညွှန်မှုများကို လုံခြုံရေးလုပ်ငန်း လုပ်ကိုင်နေသူများကို ရေးသားခိုင်းသင့်ပြီး ထိုအထဲတွင် ရေးထားသည့်အတိုင်း မလိုက်နာပါက အပေးအယူများ လုပ်ရနိုင်သည့်အကြောင်းကို ရှင်းလင်းစွာ ရေးသားဖော်ပြသင့်ပါသည်။

ကုန်ပစ္စည်းလုံခြုံရေးအတွက် တင်းကြပ်မှုလမ်းညွှန်ချက်များကို ဖန်တီးမည့်အစား အလိုအလျောက် လုံခြုံမှုရှိနေခြင်း နည်းလမ်းနှင့် "ဖြေလျော့ခြင်းနည်းလမ်း" ကို အသုံးပြုရန် အာဏာပိုင်အဖွဲ့အစည်းများအနေဖြင့် ကုန်ထုတ်လုပ်သူများအား အကြံပြုလိုပါသည်။ ထိုလမ်းညွှန်ချက်များသည် ဆိုက်ဘာတိုက်ခိုက်မှု၏ အန္တရာယ်အကြောင်းကို လုပ်ငန်းရှင်များ နားလည်သဘောပေါက်ရန် ရိုးရှင်းပြီး နားလည်လွယ်သော ဘာသာစကားများဖြင့် ရှင်းပြထားပါသည်။ လုံခြုံရေးဆိုင်ရာအချက်များကို အလျှော့အတင်း လုပ်မည်ဆိုပါက ဝယ်ယူသုံးစွဲသူများဆိုင်ရာ အကြီးအကဲများ၏ ဆုံးဖြတ်ချက်ရယူသင့်ပြီး အခြားသော စီးပွားလုံးဝန်း၏ လုံခြုံရေးနှင့် ထိန်းညှိလုပ်ဆောင်ရမည် ဖြစ်ပါသည်။

# ဝယ်ယူသုံးစွဲသူများအတွက် အကြံပြုချက်များ

အာဏာပိုင်အေဂျင်စီများအနေဖြင့် စက်မှုကုန်ထုတ်လုပ်သူများအား အကြံပြုလိုသည်မှာ ၎င်းတို့ ထုတ်လုပ်သည့် စက်မှုပစ္စည်းများ၏ လုံခြုံရေးနှင့် ပတ်သက်၍ တာဝန်ယူမှု တာဝန်ခံမှု ရှိသင့်ပါသည်။ ထိုသို့လုပ်ဆောင်ရန် အတွက် လုံခြုံအောင် ပြင်ဆင်စီမံထားသည့် ကုန်ပစ္စည်းနှင့် အလိုအလျောက် လုံခြုံမှုရှိနေသည့် ကုန်ပစ္စည်းများကို ဝယ်ယူအသုံးပြုရန် အရေးကြီးသည့်အကြောင်းကို အဖွဲ့အစည်း၏ ထိပ်သီးပုဂ္ဂိုလ်များမှ ဦးစားပေးလုပ်ဆောင်ရန် လိုအပ်ကြောင်း အကြံပြုလိုပါသည်။ လိုအပ်လျှင် ဝယ်ယူမှု မလုပ်မီအချိန်မှစ၍ အိုင်တီဌာနများအနေဖြင့် ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများ၏ ကုန်ပစ္စည်းလုံခြုံမှုကို ဆန်းစစ်မှုပြုလုပ်ခွင့်ပေးမည့် မူဝါဒများချမှတ်ပြီး လုပ်ဆောင်သင့်ပါသည်။ လုံခြုံအောင် ပြင်ဆင်စီမံထားသည့်ကုန်နှင့် အလိုအလျောက် လုံခြုံမှုရှိနေသာ ကုန်များတွင် (ဤစာစောင်တွင် ဖော်ပြထားသည့်အရာများအပြင် အခြားအဖွဲ့အစည်းများ၏ ဖော်ပြချက်များအပါအဝင် ဖြစ်ပါသည်) ရှိသင့်သည့် စံချိန်စံနှုန်းများကို သတ်မှတ်ဆုံးဖြတ်ရာတွင် အိုင်တီ ဌာနကို ဆုံးဖြတ်ခွင့်ပေးသင့်ပါသည်။ ထိုကဲ့သို့ ဝယ်ယူမှု ဆုံးဖြတ်ချက်များကို အိုင်တီဌာနမှ ချမှတ်အကြံပြုသည့်အခါတွင်လည်း ထိပ်သီးစီမံအုပ်ချုပ်သူ အရာရှိများ၏ ထောက်ခံအားပေးမှု လိုအပ်ပါသည်။ စက်မှုကုန်ပစ္စည်းများအတွက် လုံခြုံရေးဆိုင်ရာနှင့် ပတ်သက်၍ ကြုံရနိုင်သည့် အခက်အခဲများကိုလည်း မှတ်တမ်းတင်ထားသကဲ့သို့ အဖွဲ့အစည်း၏ ဆုံးဖြတ်ချက်အားလည်း မှတ်တမ်းတင်ထားသင့်ပါသည်၊ ထိုမှတ်တမ်းတင်မှုကိုလည်း အကြီးတန်းစီးပွားရေး အမှုဆောင်အရာရှိများ၏ သဘောတူညီချက်ရရှိမှု လိုအပ်ပြီး ထိုအရာများကိုလည်း ဒါရိုက်တာ ဘုတ်အဖွဲ့ကို ပုံမှန်တင်ပြမှု လုပ်သင့်ပါသည်။

ကုမ္ပဏီ၏ ဒေတာကွန်ရက်၊ အိုင်ဒီနှင့် အချက်အလက်ရယူခွင့်ဆိုင်ရာ စီမံမှု၊ လုံခြုံရေးဆိုင်ရာ၊ လုပ်ကိုင်နိုင်စွမ်းအပေါ် တုန့်ပြန်မှု စသည့် လုပ်ငန်း၏ လုံခြုံရေးဆိုင်ရာ အနေအထားကို ပံ့ပိုးပေးသည့် ကုမ္ပဏီ၏ အိုင်တီ ဝန်ဆောင်မှုကို အရေးကြီးသည့် လုပ်ငန်း၏ အစိတ်အပိုင်းအဖြစ် သတ်မှတ်ပြီး လုပ်ငန်း၏ ရည်မှန်းချက်အောင်မြင်မှုနဲ့ ကိုက်ညီစေမည့် ငွေကြေးများ ထားရှိသုံးစွဲမှု လုပ်နိုင်ရမည် ဖြစ်သည်။ လုံခြုံအောင် ပြင်ဆင်စီမံခြင်းနှင့် အလိုအလျောက် လုံခြုံမှုရှိနေသော ကုန်ပစ္စည်းများကို ကုန်ထုတ်လုပ်သူများ ထုတ်လုပ်နိုင်စွမ်းရှိရန်အတွက်လည်း အဖွဲ့အစည်းများမှ အစီအစဉ်များ ရေးဆွဲပြီး တိုးတက်မှုရှိအောင် ပံ့ပိုးပေးရမည် ဖြစ်သည်။

ဖြစ်နိုင်ပါက ကုမ္ပဏီများအနေဖြင့် ၎င်းတို့၏ အဓိက အိုင်တီပစ္စည်း ရောင်းချသူအဖွဲ့နှင့် ဗျူဟာကျကျ မိတ်ဖက်မှုရှိအောင် ကြိုးစားလုပ်ဆောင်သင့်ပါသည်။ ထိုမိတ်ဖက်ချိတ်ဆက်မှုများသည် အလွှာအသီးသီးရှိသည့် အဖွဲ့အစည်းများနှင့် ယုံကြည်မှုရယူခြင်းများပါဝင်ပြီး ပြဿနာ ကြုံရသည့်အချိန် သို့မဟုတ် ဘုံဦးစားပေးစရာများရှိသည့်အခါတွင် အပြန်အလှန်ဖေးဖေးမမ လုပ်ဆောင်နိုင်ကြမည် ဖြစ်ပါသည်။ ထိုကဲ့သို့ မိတ်ဖက်ဆက်ဆံမှုများတွင် လုံခြုံရေးကို အဓိကထားရမည်ဖြစ်ပြီး လုံခြုံအောင် ပြင်ဆင်စီမံခြင်းနှင့် အလိုအလျောက် လုံခြုံနေခြင်း၏ လုပ်ထုံးလုပ်နည်းများကို အလေးထားကျင့်သုံးနိုင်ရန်အတွက် ချိတ်ဆက်ထားရန်ဖြစ်ပြီး အတည်တကျ တရားဝင်နည်း (ဥပမာ စာချုပ်နှင့်တကွ သို့မဟုတ် ရောင်းဝယ်ရေးသဘောတူစာချုပ်) ဖြစ်စေ ရိုးရိုးနှုတ်အရ သဘောတူညီမှုဖြစ်စေ လုပ်ဆောင်ထားသင့်ပါသည်။ စက်မှုပစ္စည်းထုတ်လုပ်ရောင်းချသူများသည်လည်း ၎င်းတို့၏ လုံခြုံမှုထိန်းချုပ်ရေး အနေအထားနှင့် လုံခြုံအောင် ပြင်ဆင်စီမံထားခြင်းနှင့် အလိုအလျောက် လုံခြုံမှုရှိနေခြင်း လုပ်ထုံးလုပ်နည်းဆိုင်ရာ လမ်းပြမြေပုံနှင့် ဆက်စပ်ပြီး ကုမ္ပဏီများကို ပွင့်လင်းမြင်သာမှုရှိအောင် ချပြသင့်ပါသည်။

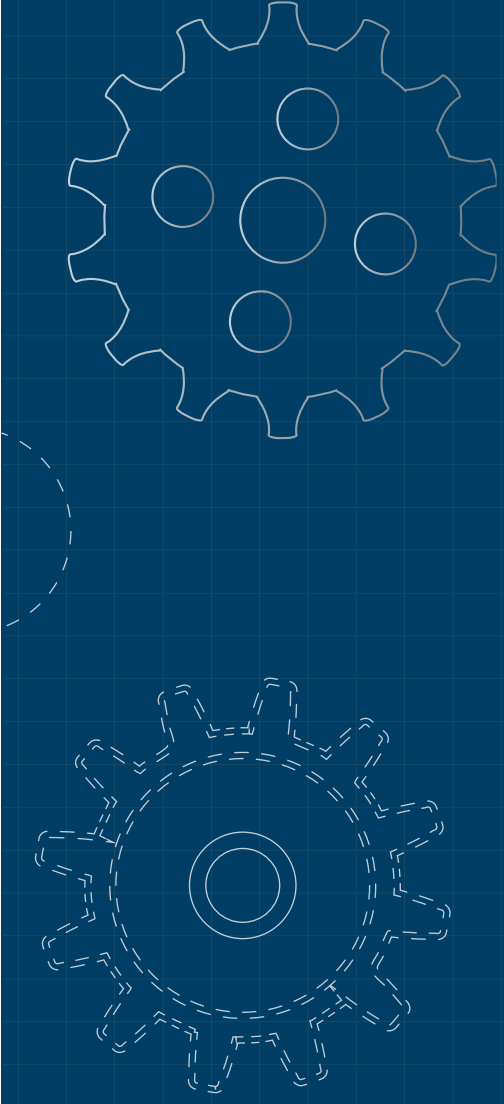
အဖွဲ့အစည်းအတွင်း အလိုအလျောက် လုံခြုံမှုရှိခြင်းကို ဦးစားပေးအရာအဖြစ် လုပ်ဆောင်သည့်အပြင် အိုင်တီ အကြီးအကဲများအနေဖြင့် ၎င်းတို့နှင့် လုပ်ငန်းတူ လုပ်ကိုင်သူများနှင့် ပူးပေါင်းမှု ရယူ၍ ထိုလုံခြုံရေးအခြေခံမူများ အကောင်အထည်ဖော်လုပ်ဆောင်ရန်အတွက် မည်သည့်ကုန်ပစ္စည်းနှင့် ဝန်ဆောင်မှုက အကောင်းဆုံးဖြစ်သည့်အကြောင်း နားလည်သဘောပေါက်ရန် ပူးပေါင်းမှုရယူသင့်ပါသည်။ ဆော့ဖ်ဝဲကုန်ထုတ်လုပ်သူများအနေဖြင့် နောက်နောင်ထုတ်လုပ်မည့်ကုန်များတွင် လုံခြုံရေးကို ဦးစားပေးနိုင်ရန်အတွက် ခေါင်းဆောင်များမှ ပူးပေါင်း၍ တင်ပြတောင်းဆိုမှုများ ပြုလုပ်သင့်ပါသည်။ အတူတူ ပူးပေါင်းလုပ်ကိုင်ဆောင်ရွက်ခြင်းအားဖြင့် သုံးစွဲသူများသည် ကုန်ထုတ်လုပ်သူများအတွက် အသုံးဝင်သည့် အကြံဉာဏ်များ ပေးနိုင်သည့်အပြင် ကုန်ထုတ်လုပ်သူများအား လုံခြုံရေးကို ဦးစားပေးအောင် လှုံ့ဆော်မှုများလည်း ဖြစ်စေနိုင်ပါသည်။

Cloud system ကို အသုံးပြုသည့်အချိန်တွင် အဖွဲ့အစည်းများသည် စက်မှုပစ္စည်းရောင်းချုံ့ပိုးသူများနှင့် တာဝန်ခွဲယူမှုရှိသင့်ကြောင်းကို နားလည်ရန် အရေးကြီးပါသည်။ လုံခြုံရေးဆိုင်ရာ တာဝန်ကို စက်မှုထုတ်လုပ်သူများမှ တာဝန်ယူရမည်ဖြစ်ပြီး သုံးစွဲသူ၏ တာဝန်သက်သက်မဟုတ်ကြောင်းကို အဖွဲ့အစည်းများမှ ရှင်းလင်းအောင် လုပ်ဆောင်ထားရမည်ဖြစ်သည်။ ထို့ကြောင့် ၎င်းတို့၏ လုံခြုံရေးအနေအထားကို ပွင့်လင်းမြင်သာမှုရှိအောင်လုပ်ဆောင်ထားသည့် ဆော့ဖ်ဝဲဝန်ဆောင်မှုပေးသူများ၊ ဌာနတွင်း လုံခြုံရေးထိန်းချုပ်မှု၊ ၎င်းတို့၏ ပူးတွဲတာဝန်ဝတ္တရားကို ထမ်းဆောင်မှုပေးနိုင်သည့် အဖွဲ့နှင့် ဦးစားပေး ပူးပေါင်းလုပ်ဆောင်ရန် အဖွဲ့အစည်းများကို အကြံပြုလိုပါသည်။

အဖွဲ့အစည်းများအနေဖြင့် cloud ဝန်ဆောင်မှုပေးသူများအား ၎င်းတို့၏ လုံခြုံရေးအနေအထားအကြောင်း၊ လုပ်ငန်းအတွင်း ထိန်းချုပ်မှုနှင့် တာဝန်မျှဝေခြင်းဆိုင်ရာ ပုံစံအရ ၎င်းတို့၏ တာဝန်ဝတ္တရားနှင့်အညီ လုပ်ကိုင်နိုင်စွမ်း ရှိမှုအကြောင်းတွေကို ပွင့်လင်းမြင်သာစွာ လုပ်ဆောင်သင့်ပါသည်။

# မသက်ဆိုင်ကြောင်း ရှင်းလင်းချက်

ဤအစီရင်ခံစာပါ အချက်အလက်များသည် "ဤကဲ့သို့" အချက်အလက်အသိပေးခြင်းရည်ရွယ်ချက်အနေဖြင့်သာ ဖော်ပြထားခြင်း ဖြစ်ပါသည်။ CISA နှင့် အာဏာပိုင် အဖွဲ့အစည်းများသည် မည်သည့် ထုတ်ကုန်၊ မည်သည့်ဝန်ဆောင်မှု၊ မည်သည့် လေ့လာဆန်းစစ်စိတ်ဖြာမှုကိုမှ ထောက်ခံမှု မလုပ်ထားပါ။ ကုမ္ပဏီ၏ နာမည် သို့မဟုတ် ပစ္စည်းတစ်ခု၏ နာမည်၊ သို့မဟုတ် လုပ်ငန်းစဉ် သို့မဟုတ် ဝန်ဆောင်မှု၊ ကုန်အမှတ်တံဆိပ်၏ နာမည်၊ ကုန်ထုတ်လုပ်သူ၏ နာမည်နှင့် အခြားနာမည်များကို ဖော်ပြခဲ့သည်ရှိသော် ၎င်းတို့ကို CISA နှင့် အာဏာပိုင်အေဂျင်စီမှ ထောက်ခံချက်ပေးခြင်း၊ သုံးစွဲရန် အကြံပြုခြင်း သို့မဟုတ် မျက်နှာသာပေးခြင်း မဟုတ်ကြောင်း အသိပေးလိုပါသည်။ ဤစာစောင်သည် CISA ၏ ဦးဆောင် ပူးပေါင်းဆောင်ရွက်မှု စာစောင်ဖြစ်ပြီး စည်းမျဉ်းစည်းကမ်းနှင့်တကွ လိုက်နာရမည့် စာစောင်မဟုတ်ကြောင်းကိုလည်း သတိပေးအပ်ပါသည်။



# ကျန်းမာရေးစောင့်ရှောက်မှု

## CISA

- CISA's SBOM Guidance
- CISA's Cross-Sector Cybersecurity Performance Goals
- Guidelines on Technology Interoperability
- CISA and NIST's Defending Against Software Supply Chain Attacks
- လုံခြုံမှုမရှိတဲ့ စက်မှုပစ္စည်းအသုံးပြုခြင်းအတွက် ကုန်ကျစရိတ်နဲ့ ဒါကို ဘယ်လိုဖြေရှင်းရမလဲ - CISA
- ဆိုက်ဘာလုံခြုံရေးအတွက် ကုန်ကျစရိတ်ကို တဆင့်ကျခံစေတာမျိုးကို ရပ်တန့်လိုက်ပါ - လုံခြုံစွာ တီထွင်ခြင်းနည်းကို ဘာကြောင့် စက်မှုထုတ်ကုန် ကုမ္ပဏီတွေ ကျင့်သုံးသင့်သလဲ (foreignaffairs.com)
- CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance
- CISA's Phishing Resistant MFA Fact Sheets
- အသေးစား စီးပွားရေးလုပ်ငန်းများအတွက် ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ လမ်းညွှန်ချက်များ Cyber | CISA

## NSA

- NSA's Cybersecurity Information Sheet on Memory Safety
- NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers

## FBI

- Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective
- ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ တိုက်ခိုက်မှု - တုန့်ပြန်ခြင်းနှင့် တိုင်တန်းခြင်း
- FBI ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ ဗျူဟာ

## စံနှုန်းများနှင့် နည်းပညာဆိုင်ရာ အမျိုးသားသိပ္ပံ (National Institute of Standards and Technology (NIST))

- NIST's Digital Identity Guidelines
- NIST ၏ ဆိုက်ဘာလုံခြုံရေးဆိုင်ရာ မူဘောင် NIST's Cyber Security Framework
- NIST ၏ လုံခြုံမှုရှိသော ဆော့ဖ်ဝဲထုတ်လုပ်ခြင်းဆိုင်ရာ မူဘောင် (SSDF)

## ဩစတြေးလျ၏ ဆိုက်ဘာလုံခြုံရေးစင်တာ (ACSC)

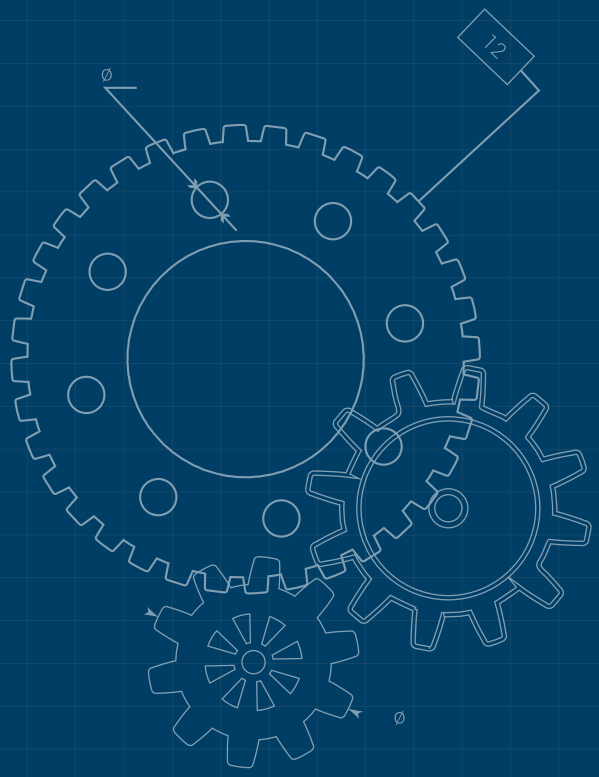
- ACSC's IoT Code of Practice Guidance for Manufacturers

## ယူကေနိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေးစင်တာ (UK)

- The UK's Cyber Assessment Framework
- The UK NCSC's Secure Development and Deployment guidance
- The UK NCSC's Vulnerability Management guidance
- The UK NCSC's Vulnerability Disclosure Toolkit
- Cambridge တက္ကသိုလ်၏ CHERI
- So long and thanks for all the bits - NCSC.GOV.UK

## ကနေဒါနိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေးစင်တာ (CCCS)

- CCCS's Guidance on Protecting Against Software Supply Chain Attacks
- ဆိုက်ဘာ၏ ထောက်ပံ့မှုကွင်းဆက် - ဖြစ်ပေါ်နိုင်သည့် အန္တရာယ်အား ဆန်းစစ်ခြင်း
- Canadian Centre for Cyber Security's CONTI ransomware guidance



## ဂျာမနီနိုင်ငံ အချက်အလက် လုံခြုံရေးဆိုင်ရာဌာန (Germany's Federal Office for Information Security (BSI))

- The BSI Grundschutz compendium (module CON.8)
- The international standard IEC 62443, part 4-1
- ဂျာမနီ၏ အိုင်တီ လုံခြုံရေးအနေအထား အစီရင်ခံစာ - ၂၀၂၂
- BSI practices of web application security

## နယ်သာလန်နိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေးစင်တာ NCSC

- NCSC-NL's Mature Authentication Factsheet

## Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

- ဂျပန်နိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေး ဗျူဟာ Japan's National Cybersecurity Strategy

## ဂျပန်နိုင်ငံ၏ စီးပွားရေး၊ ကုန်သွယ်ရေးနှင့် စက်မှုဆိုင်ရာ ဝန်ကြီးဌာန Japan's Ministry of Economy, Trade and Industry (METI)

- Guide of Introduction of Software Bill of Materials (SBOM) for Software Management
- Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security

## စင်ကာပူနိုင်ငံ၏ ဆိုက်ဘာလုံခြုံရေး အေဂျင်စီ

- Technical Advisory on Secure API Development
- CSA SingCERT Vulnerability Disclosure Policy
- CSA SingCERT Incident Response Checklist
- CSA SingCERT Incident Response Playbooks
- CSA Security by Design Framework
- CSA Security by Design Framework Checklist
- CSA Guide to Cyber Threat Modelling
- CSA Cybersecurity Labelling Scheme

## အခြား

- ရှုတ်ထွေးတဲ့ စနစ်တွေ ဘယ်လို ကျဆုံးကြရသလဲ
- ရှုတ်ထွေးတဲ့စနစ် ကျဆုံးခြင်း၏ ရှုထောင့်အသစ် The New Look in complex system failure

## ကျမ်းကိုးများ

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom and SBOMs references in TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] Juran on Quality by Design by J.M. Juran, 1992.