TLP:CLEAR

Senisim Wei bilong Cybersecurity Birua: Pasin na Rot bilong Security-by-Design na -Default

Publication: April 13, 2023

Cybersecurity and Infrastructure Security Agency

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

Table of Contents

BIKPELA TINGTING: MEKIM SAMTING EM NO STRONG

Technology em stap long olgeta hap long laif bilong yumi long olgeta dei. Ol bikpela system save stap long Internet em ken senisim economy, sindaun bilong yumi na helt bilong yumi tu, kain olsem long personal identity management na go inap long medical care. Wanpela kain samting olsem, em taim ol cyber breaches mekim ol hausik stopim ol surgery na salim wok bilong lukautim ol sik manmeri go long narapela ples. Taim ol technology na ol bikpela system ino strong, bai ol cyber birua ken kamap na bringim bagarap na ol safety[1] wari.

Long dispela taim nau moa long bipo, ol technology manufacturer mas mekim samting wantaim ol tingting na pasin bilong Secure-By-Design na Secure-By-Default na mas mekim dispela nambawan tru. Sampela vendor em go pas tru long mekim ol dispela senis tasol sampela em kam bihain yet. Ol authoring agency o ogenaisesin mekim dispela toksave toktok strong long olgeta technology manufacturer long mekim ol product bilong ol long wei we customer bai no nid long wokim monitoring, mekim ol update na stretim samting long ol system long stopim cyber birua. Ol manufacturer mas lukim wok bilong strongim security bilong customer bilong ol olsem bikpela samting. Long taim bipo, ol technology manufacturer save lusim wok bilong strongim security bilong ol product long han bilong customer taim samting bagarap. Taim ol yusim pasin bilong Secure-By-Design, em nau bai stopim wei bilong traim stretim samting bihain long em bagarap pinis.

Long kamapim dispela high standard bilong software security, ol ogenaisesin mekim dispela toksave toktok strong long ol manufacturer long mekim product security olsem bikpela samting taim ol mekim ol niupela feature na salim ol product hariap tasol go long market. Taim dispela kain tingting stap, ol engineering team bai kamapim niupela wei bilong wok we security em pas tru long wok bilong ol na bai kamap isi long mekim. Wankain long dispela, European Union toktok strong long product security long Cyber-Resilience-Act we ol manufacturer mas putim security long olgeta hap bilong life-cycle bilong ol product na stopim ol product we nogat strongpela security.

Long mekim peles bihain taim we technology na ol wankain product em gat strongpela security long

[1] Ol authoring agency o ogenaisesin wokim dispela toksave em luksave olsem tok “safety” gat planti mining taim yu yusim. Long dispela toksave o guide, “safety” em toktok long wei bilong strongim ol technology security standard long lukautim ol customer long hevi bilong ol cyber birua

lukautim ol customer, ol ogenaisesin mekim dispela toksave toktok strong long ol manufacturer long senisim ol design na development program na larim ol Secure-By-Design na -Default product tasol long go long ol customer. Ol Secure-By-Design product em ol product we security bilong customer em bikpela samting na no technical feature tasol. Ol Secure-By-Design product em gat security olsem bigpela tingting bipo long ol stat mekim samting. Ol Secure-By-Default product em ol product we yu ken stat yusim stret na noken wari long senisim configuration o baim sampela moa security feature. Dispela tupela samting wantaim em senisim hevi bilong strongim security go long ol manufacturer na rausim sampela wei bilong security birua painim ol customer taim igat misconfiguration, sapos patching no kamap hariap na ol kain birua olsem.

Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI) na ol dispela international partners[2] givim ol strongpela toktok insait long dispela guide olsem rot bilong ol technology manufacturer long bihainim long strongim security bilong product ol mekim:

- Australian Cyber Security Centre (ACSC)
- Canadian Centre for Cyber Security (CCCS)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- Germany's Federal Office for Information Security (BSI)
- Netherlands' National Cyber Security Centre (NCSC-NL)
- Computer Emergency Response Team New Zealand (CERT NZ) na New Zealand's National Cyber Security Centre (NCSC-NZ).

Ol ogenaisesin mekim dispela toksave luksave long halvim bilong planti private sector partners long mekim go het security-by-design na security-by-default. Tingting bilong dispela product em long statim toktok namel long ol kantri long makim ol bikpela priority, investment na rot bilong bihainim long kamap long peles we technology em gat strongpela security na ken kam bek hariap taim samting bagarap wantaim design na default. Long kamapim dispela samting, ol ogenaisesin mekim dispela toksave laik kisim feedback o tingting bilong ol interested parties na laik bung wantaim long

[2] Bihain long dispela em ol kolim "authoring agencies" o "ol ogenaisesin mekim dispela toksave"

harim gut dispela ol tingting na strongim ol wok na mekim go het moa.

Sapos yu laikim sampela moa infomesin o toksave long product safety, lukim dispela pepa bilong CISA, The Cost of Unsafe Technology and What We Can Do About It.

Secure-by-Design

"Secure-by-Design" em min olsem ol mekim technology product wantaim strongpela banis long stopim ol cyber birua long lukim o kalap go insait long ol device, data na ol masin o infrastructure em pas wantaim. Ol software manufacturer ken mekim risk assessment long painim na makim ol cyber threat em ken bagarapim ol bikpela system na putim ol wei bilong traim stopim ol cyber threat taim kamap.

Ol strongpela information technology (IT) development pasin na wei bilong putim planti kain defense o banis bilong bilong lukautim samting – ol kolim defense-in-depth – em gutpela long bihainim dispela long stopim ol birua o bagarap kamap long ol system na long data bilong yumi. Dispela ol authoring agencies toktok strong olsem ol manufacturer mas yusim wanpela tailed threat model taim ol mekim samting long stopim olgeta kain threats long system na lo strongim rot bilong salim system go long ol customer.

Ol ogenaisesin mekim dispela toksave toktok strong long ol manufacturers mas lukluk na tingting bikpela long security taim ol mekim ol product na platform bilong ol. Taim ol mekim samting Secure-by-Design, dispela mas gat bikpela investment bilong ol resources kam long ol software manufacturers long olgeta hap bilong product design na development process na no inap samting ol putim bihain taim.

Em nogat wanpela wei tasol bilong stopim ol birua o bagarap em ol cyber actor ken bringim taim ol yusim ol technology vulnerability, na ol product we em "Secure-by-Design" bai painim yet ol vulnerability o dua we security em no strong; tasol planti bilong ol dispela kain dua o vulnerability em kam long samting we gat liklik namba tasol. Ol manufacturer mas makim rot bilong ol product bilong ol long stap wantaim Secure-by-Design pasin na senisim dispela sapos igat gutpela tingting tasol.

Ol authoring agency o ogenaisesin mekim dispela toksave luksave olsem taim ol manufacturer karim hevi bilong security bilong ol customer, em bai mas putim moa moni go long development.

Tasol, taim ol putim dispela investment long “Secure-by-Design” tingting long wok bilong mekim ol niupela technology product na lukautim ol product stap yet nau, dispela em ken strongim tru security bilong ol customer na rausim ol sampela rot we customer save painim birua. Secure-by-Design tingting em save strongim security bilong customer na strongim nem bilong manufacturer na tu em bai daunim ol maintenance na patching cost bilong ol.

Dispela Recommendation bilong ol Software Manufacturer hap em kam bihain liklik long dispela document bai givim ol sampela product development practice na policy we ol manufacturer ken lukim na traim bihainim.

Secure-by-Default

“Secure-by-Default” em min olsem product em gat strong long pasim ol birua bai kamap taim customer opim na yusim stret na noken baim sampela samting moa. Dispela ol product ken banisim gut ol end-user na bai ol no inap wokim ol arapela samting long strongim security bilong ol. Ol Secure-by-Default product em ol mekim customer luksave olsem taim ol lusim ol safe default, em bai gat moa sans olsem ol bai painim birua sapos ol no putim ol sampela kain banis.

- Secure configuration em mas samting bai kamap olgeta taim. Ol Secure-by-Default product em bai gat strongpela security olgeta taim long lukautim ol ogenaisesin long ol cyber birua na tu bai givim wei bilong strongim dispela security banis tasol no inap askim long yu baim sampela moa moni.
- Customer mas noken wari long traim save gut long wei bilong security configuration. Ol IT wok manmeri save karim hevi bilong planti security na operational wok, na dispela save katim sot taim bilong ol dispela wok manmeri long save gut na lainim ol niupela wei na pasin bilong strongim security long ogenaisesin. Taim ol strongim security bilong product configuration – strongim “default path” – ol manufacturer ken halvim na strongim security bilong ol customer bilong ol wantaim product we ol mekim, salim na yusim wantaim tingting na wei bilong “Secure-by-Default”.

Ol manufacturer bilong ol product we em “Secure-by-Default” bai no inap askim customer long baim sampela moa moni long strongim security. Ol bai gat dispela security long base product wankain olsem seatbelt stap long olgeta niupela kar. Security em no samting bai yu mas baim

wantaim bikpela moni tru, em mas kamap olsem samting we ol customer ken kisim tasol olgeta taim.

RECOMMENDATION BILONG OL SOFTWARE MANUFACTURER

Dispela guide em bungim ol tingting na toktok strong long ol manufacturer long makim rot bilong bihainim na strongim IT security. Ol authoring agencies toktok strong long ol manufacturer long yusim ol tingting em ol raitim tamblo taim ol mekim ol product long strongim security na lukautim gut ol customer bilong ol wantain Secure-by-Design na -Default tingting.

Tingting bilong Software Product Security

Ol technology manufacturer mas senis na strongim tingting long software security. Ol authoring agency mekim tripela strongpela tingting long halvim ol software manufacturer long putim software security insait long ol design process bilong ol bipo long mekim na salim product go long ol customer bilong ol.

1. Hevi bilong security em mas noken stap long customer tasol. Ol software manufacturer mas kisim hevi bilong security wari bilong customer husait baim product bilong ol na strongim security bilong product.
2. Holim strong pasin bilong tok tru na wokabaut stret. Ol software manufacturer mas soim olsem ol save mekim na salim ol safe na secure product, na tu ol toksave olsem ol narakain long ol arapela manufacturer taim ol mekim ol safe na secure product. Dispela em kain olsem ol ken toksave long samting ol lainim long ol customer olsem hamas customer yusim strongpela authentication mechanism long product bilong ol. Dispela em kain samting olsem ol gat strongpela tingting long bihainim ol vulnerability advisories na na wokim gut ol common vulnerability na exposure (CVE) record. Luksave tu, olsem ol CVEs em no samting nogut. Ol dispela namba em soim olsem igat gutpela code analysis na strongpela testing community.
3. Strongim bun na ol lida bilong ogenaisesin long wokim dispela samting. Ol technical subject matter expertise o save manmeri em bikpela samting long mekim product security strong, ol senior lida o executives bai mekim ol bikpela decision long kamapim senis long ogenaisesin. Strongpela tingting bilong ol lida bilong ol software manufacturer long

makim security olsem bikpela samting long product development na dispela nidim gutpela bung tingting o partnership wantaim ol customer bilong ogenaisesin long save gut long:

a. Wei bilong wokim product deployment wantaim tailored threat model
b. Tingting long wei bilong putim ol security control long bihainim tingting bilong Secure-by-Default
c. Wei bilong skelim ol resource long mak bilong kampani na save bilong sensim ol olpela wei bilong wok wantaim ol Secure-by-Design tingting
d. Nid long oltaim kisim na harim tingting bilong ol wokman na customer long ol security issue. Software security mas bikpela samting long ol toktok o bung insait long ogenaisesin (all-hands o brown bags) na tu ol product marketing na toktok o bung wantaim ol customer
e. Makim strong bilong ol customer deployment. Ol senior lida bai laik save wanem hap ol investment long security by design na default woklong halvim ol customer long ol kain samting olsem nogat planti security patches, liklik configuration error na stopim sampela wei bilong kamapim birua.

Long kamapim dispela tripela tingting, ol manufacturer mas tingim ol operational tactic o rot bilong mekim development process kamap gutpela moa.

Kirapim bung wantaim ol senior lida bilong kampani long toktok strong long pasin bilong Secure-by-Design na Secure-by-Default insait long kampani. Ol policies na procedures mas stap long makim tru ol production team husait save mekim ol product na bihainim ol dispela tingting, na tu dispela em ken givim luksave long ol gutpela software security wok o givim wei bilong kisim ol bikpela position moa.

Wokim wok olsem software security em bikpela samting long kamapim gutpela business. Kain olsem, traim putim wanpela “software security lida” o “software security team” wantaim wok bilong strongim business na IT tingting na bungim ol software security standard wantaim manufacturer accountability. Ol manufacturer mas gat gutpela wei bilong makim sapos product security em gutpela o nogat.

Yusim wanpela tailored threat model long taim bilong development long strongim ol product

gat bikpela impact. Ol threat model save lukluk long wei bilong yusim product na kamap wantaim wei bilong strongim security bilong dispela product. Long pinis, ol senior lida mas mekim klia olsem ol team karim hevi bilong strongim security long ol product na dispela bai soim olsem product em gutpela tru.

Secure-by-Design Tactics

Secure Software Development Framework (SSDF), na tu ol kolim National Institute of Standards and Technology (NIST) SP 800-218, em ol secure software development tingting em ken kamap long olgeta hap bilong software development lifecycle (SDLC). Taim ol bihainim ol dispela tingting, em ol software producer ken kamap strongpela moa na ken painim na rausim ol birua stap long released software, stopim wei bilong yusim ol dispela kain birua na rausim tru ol samting em ken kamapim ol birua long bihain taim.

Ol authoring agency toktok strong long yusim ol Secure-by-Design tactics, kain olsem ol tingting kam long SSDF. Ol software manufacturer mas kamapim wantaim rot bilong putim moa Secure-by-Design software development tingting long ol product bilong ol. Dispela em sampela rot bilong bihainim long yusim ol dispela tingting:

- Memory safe programming languages (SSDF PW.6.1): Pastaim tru, yusim memory safe language sapos yu inap. Ol authoring agency luksave olsem ol arapela wei bilong strongim memory em stap, olsem address space layout randomisation (ASLR), control-flow integrity (CFI), na fuzzing em ken halvim wantaim ol olpela codebase, tasol ol no inap sapos yumi lukluk wantain secure-by-design na dispela em olsem ol no strong inap long stopim ol birua. Sampela bilong ol niupela memory safe language em C#, Rust, Ruby, Java, Go, na Swift. Ridim infomesin o toksave pepa bilong NSA sapos yu laik save sampela moa.
- Secure Hardware Foundation: Putim ol architectural feature em bai strongim na lukautim memory, kain olsem dispela ol toktok long em long Capability Hardware Enhanced RISC Instructions (CHERI) we em ken mekim ol hardware Instruction-Set Architectures (ISAs) longpela moa. Sapos yu laikim sampela moa infomesin o toksave, go na lukim CHERI webpage bilong University bilong Cambridge.
- Secure Software Components (SSDF PW.4.1: Kisim na lukautim gut ol strongpela software

components (e.g., software libraries, modules, middleware, frameworks) kam long verified commercial, open source, na ol third-party developer long strongim security long ol consumer software product.

- Web template frameworks (SSDF PW.5.1): Yusim ol web template framework we bai gat automatic escaping bilong ol user input long pasim ol web birua kain olsem cross-site scripting.
- Parameterised queries (SSDF PW.5.1): Yusim parameterised queries na noken kisim user input long ol query, to stopim ol SQL injection attack.
- Static na dynamic application security testing (SAST/DAST) (SSDF PW.7.2, PW.8.2): Yusim ol dispela tool long sekim product source code na wei application wok, long painim we ol samting ken bagarap o bruk. Dispela ol tool bai karamapim ol issue kain olsem nogat gutpela memory management go nap long error prone database query construction (e.g., unescaped user input bai kamapim SQL injection). Ol SAST na DAST tool bai inap long go insait long development process na ron em yet olsem wanpela hap bilong software development. SAST na DAST mas go wantaim ol arapela kain testing, kain olsem unit testing na integration testing, long mekim ol product stap wantaim ol strongpela security requirement. Taim ol issue kamap, ol manufacturer ken wokim root-cause analysis long painim na stretim ol vulnerability o birua.
- Code review (SSDF PW.71., PW.7.2): Traim hat long mekim code we go insait long ol product mas go long peer review wantaim ol arapela developer long strongim quality bilong em.
- Software Bill of Materials (SBOM) (SSDF PS.3.2, PW.4.1): Karim wok bilong mekim SBOM[3] long givim luksave long ol hap bilong software go insait long ol product.
- Vulnerability disclosure programs (SSDF RV.1.3): Kirapim ol vulnerability disclosure program long givim ol security researcher wei bilong ripotim ol vulnerability na kisim legal safe harbour taim ol wokim dispela. Hap bilong dispela, em ol supplier mas gat process bilong painim root cause bilong ol vulnerability o birua. Dispela kain ol process bai mas gat wei bilong kisim ol Secure-by-Design tingting insait long dispela pepa (o long ol wankain

[3] Sampela authoring agency wok long painim ol niupela wei bilong kisim security assurance long software supply chain.

tingting) we bai stopim dispela birua long kam insait.

- CVE completeness: Makim gut ol published CVEs na em mas gat root cause o common weakness enumeration (CWE) long givim sans long lain long industry long wokim software security root causes analysis. Wok bilong stretim olgeta CVE em ken kisim sampela moa taim, dispela em givim sans long ol orgenaisesin long painim ol rot bilong industry we em bai halvim olgeta manufacturer na customer. Long painim moa infomesin o toksave long lukautim ol vulnerability, go na lukim CISA's Stakeholder-specific SVCC guidance.
- Defense-in-Depth: Mekim samting wantaim tingting olsem sapos ol bagarapim wanpela security control bai no nap bringim bagarap o birua long olgeta system. Kain olsem, strongim wei bilong givim user privilege we mas gat liklik access pastaim na ol yusim ol access control list na dispela ken daunim tru bagarap long ol account. Na tu, ol software sandboxing technique ken rausim ol birua o vulnerability na ken stopim bagarap long kamap long olgeta applications.
- Bungim ol Cyber Performance Goals (CPGs): Mekim product we em bungim ol basic security tingting. Cybersecurity Performance Goals bilong CISA em givim ol bikpela cybersecurity mak ol ogenaisesin mas mekim. Na tu, sapos yu laikim sampela moa wei bilong strongim ogenaisesin bilong yu, lukim Cyber Assessment Framework bilong UK, we wankain long ol CPG bilong CISA. Sapos wanpela manufacturer no bungim ol CPG – kain olsem ol nogat phising-resistant multi-factor authentication bilong olgeta wok manmeri – em bai ol luksave olsem ol no mekim ol Secure-by-Design product.

Ol authoring agency luksave olsem dispela ol senis em bikpela samting long ol ogenaisesin. Olsem na, wok bilong kirapim dispela wok mas gat mak we ol lukluk long criticality, complexity, na impact long business. Dispela ol tingting em nap long kamap long ol niupela software na ol ken mekim bikpela isi tasol long bungim ol niupela use case na product. Sampela taim, criticality na risk long wanpela product bai gat accelerated schedule long kisim ol dispela tingting. Sampela taim, ol dispela tingting ken kamap long ol olpela codebase na ol ken stretim isi isi.

Secure-by-Default Tactics

Wantaim ol tingting stap long Secure-by-Design development, ol authoring agency toktok strong tu long ol software manufacturers long strongim Secure-by-Default configuration long ol product bilong ol. Dispela ol ogenaisesin mas wok hat long mekim update long ol product long stap wantaim ol dispela tingting taim ol wok long strongim na senisim.

- Rausim ol default password: Ol product mas noken kam wantaim default password we olgeta save. Long rausim default password, ol authoring agency toktok strong long ol product mas gat strongpela password em ol administrator mekim taim ol wokim installation na configuration.
    - Ol privileged user mas yusim Multifactor Authentication (MFA): Yumi lukim olsem planti enterprise deployment em gat ol administrator we ol no strongim account bilong ol wantaim MFA. Taim ol luksave olsem ol administrator em bikpela target, ol product mas mekim MFA opt-out na noken opt-in. Na tu, system mas olgeta taim toksave long administrator long yusim MFA long account bilong ol inap ol bihainim toksave na mekim. NCSC bilong Netherlands gat ol rot em wankain olsem CISA, bai yu ken go lukim Mature Authentication Factsheet bilong ol long painim sampela moa infomesin o toksave.
- Single sign-on (SSO): Ol IT application mas yusim single sign on technology wantaim ol niupela open standards. Kain olsem Security Assertion Markup Language (SAML) o OpenID Connect (OIDC). Dispela samting mas stap taim customer em yusim pastaim tru na mas noken baim moa.
- Secure Logging: Givim ol gutpela quality audit log long ol customer nating. Ol audit log em bikpela samting long painim na stopim ol security incident. Em bikpela samting tu taim gat investigation long ol suspected o klia security incident. Tingting long ol best practice kain olsem givim isipela integration wantaim security infomesin o toksave na event management (SIEM) system na wantaim application programming interface (API) access we em yusim coordinated universal time (UTC), standard time zone formatting, na gutpela wei bilong wokim ol documentation.

- Software Authorisation Profile: Ol software supplier mas givim tok strong bilong ol long ol authorised profile role na tingting bilong ol long yusim ol dispela role. Ol manufacturer mas gat ol klia toksave long ol customer long soim bagarap ol nap painim sapos ol no bihainim ol recommended profile authorisation. Kain olsem: Ol medical doctor inap lukim olgeta patient record, na wanpela medical scheduler em ken lukim liklik hap tasol long halvim long mekim wok bilong ol.
- Forward-looking security over backwards compatibility: Planti taim, ol backwards-compatible legacy feature save kam wantaim ol product, na planti taim dispela em ol tanim on, tasol dispela em ken bringim birua o bagarapim product security. Mekim security bikpela samting moa long backwards compatibility, na givim strong long ol security team long rausim ol feature em no strong maski sapos em bai bringim sampela senis na pen.
- Bihainim na daunim namba bilong ol “hardening guide”: Daunim namba bilong ol “hardening guide” we ol mekim bilong ol product na traim long lukluk long ol niupela software update na halvim long bringim namba go daun wantaim ol update.
- Tingting long user experience taim ol yusim ol security settings: Olgeta niupela security setting save mekim hat liklik long ol end user long lainim na tu ol mas lukluk long dispela na skelim wantaim ol gutpela samting dispela bai givim long business. Em gutpela moa sapos strongpela setting bilong product em stap insait taim customer kisim. Taim configuration mas kamap, dispela default option em ken sanap strong long stopim ol common threat.

Ol authoring agency luksave olsem dispela senis bai gat operational effect long wei ol bai yusim software. Olsem na tingting bilong customer em bikpela samting tru long karim gut operational na security wari. Ol authoring agency tingting strong olsem nambawan samting long bringim senis go long secure software development practices, em sapos igat klia rot bilong bihainim na sapot bilong ol executive lida long bihainim dispela rot. Tingting bilong ol customer em bikpela samting tasol ol authoring agency lukim ol bikpela case we customer em no laik long bihainim ol strongpela standard, planti taim ol network protocol. Em bikpela samting tru taim ol manufacturer kamap wantaim gutpela wei long halvim ol customer long strongim security product bilong ol na no lusim

ol stap nating na ken painim birua.

HARDENING GUIDE NA LOOSENING GUIDE

Hardening guide em save kamap taim nogat inap product security control stap insait long architecture bilong product long taim mekim pastaim tru. Dispela em mekim ol hardening guide kamap olsem rot bilong ol manmeri nogut long painim na yusim ol feature we nogat strongpela security. Planti ogenaisesin no save olsem ol hardening guide stap na dispela em min olsem ol device configuration settings bilong ol em no strong. Narapela model stap ol kolim ol loosening guide mas senisim ol hardening guide na toksave gut long ol user long ol senis ol mas wokim na toksave gut tu long ol security risk bai stap.

Ol authorising agency toktok strong long ol software manufacturer long senis go long wei bilong yusim Secure-by-Default na givim ol loosening guide na noken mekim ol hardening guide we em toksave tasol long ol wei bilong strongim product. Ol loosening guide save toksave gut na toktok klia long ol business risk na bringim gutpela save long ol birua em ken kamap wantaim ol cyber intrusion. Ol senior executive bilong ol customer ken tingting gut na skelim security risk wantaim ol business requirement.

RECOMMENDATION BILONG OL CUSTOMER

Ol authoring agencies toktok strong olsem ol ogenaisesin mas holim ol supplying technology manufacturer bilong ol accountable long security bilong product bilong ol. Na tu, ol authoring agency toktok strong olsem ol executive lida bilong ogenaisesin mas baim ol Secure-by-Design na Secure-by-Default product na mekim dispela olsem bikpela samting. Dispela em kain samting olsem ol policy we IT department mas lukluk gut long security bilong manufacturer bipo long ol baim, na tu, ol givim strong na pawa long ol IT department long tok nogat sapos ol gat wari long security bilong ol product. Ol IT department mas gat pawa long mekim ol purchasing criteria we Secure-by-Design na Secure-by-Default practice em bikpela samting (ol practice o tingting stap long dispela document na ol arapela we ogenaisesin mekim). Na tu, ol IT department mas kisim sapot bilong ol executive management taim ol gat wari wantaim ol purchasing decision. Ol decision bilong ogenaisesin long karim risk bilong ol wanwan technology product mas gat formal documentation na mas kisim tok orait long wanpela senior business executive, na tu, mas givim dispela infomesin o

toksave long ol Board of Directors.

Ol bikpela enterprise IT service save sapotim security bilong ogenaisesin, kain olsem enterprise network, enterprise identity and access management, na security operations and response capabilities, mas gat luksave olsem ol bikpela business function na mas kisim moni long soim olsem dispela em bikpela samting long wok bilong ogenaisesin. Ol ogenaisesin mas wokim plan long strongim ol dispela hap o capability bilong ogenaisesin wantaim ol manufacturer husait gat gutpela Secure-by-Design na Secure-by-Default practices.

Sapos em inap kamap, ol ogenaisesin mas wok hat long kamapim strategic partnership relationship wantaim ol bikpela IT supplier. Ol dispela kain relationship mas wok gut long olgeta hap bilong ogenaisesin na mas gat wei bilong stretim ol wari na wok bung wantaim. Security em mas bikpela samting tru namel long dispela relationship na ol ogenaisesin mas wok hat long strongim ol Secure-by-Design na Secure-by-Default practice long ol formal (e.g., contract na vendor agreement) na informal hap bilong relationship. Ol ogenaisesin mas lukluk gut na tok klia wantaim ol technology supplier long strong bilong internal control bilong ol.

Long go wantaim tingting bilong mekim Secure-by-Default bikpela samting long ol ogenaisesin, ol IT lida mas toktok gut wantaim ol industry peer bilong ol long luksave long ol product na service we bai wok strong wantaim design tingting na pasin bilong ogenaisesin. Dispela ol lida mas wok wantaim long halvim ol manufacturer long mekim klia ol security initiative em woklong kamap. Taim ol wok wantaim, ol customer ken givim gutpela tingting long ol manufacturer na kamapim rot bilong ol long strongim security bilong ol.

Taim yu yusim ol cloud system, ogenaisesin mas save gut long shared responsibility model wantaim technology supplier bilong ol. Dispela em olsem, ol ogenaisesin mas gat gutpela save long security responsibility bilong supplier bilong ol na ino responsibility bilong customer tasol. Ol ogenaisesin mas mekim bikpela samting long ol cloud provider long tok klia long security posture, internal controls na strong bilong ol long karim wok aninit long shared responsibility model.

TOK KLIA

Ol infomesin insait long dispela report em ol givim “as is” na em bilong toksave tasol. CISA na ol authoring agencies no inap long toktok strong o tokim ol manmeri long yusim wanpela kain product o service. Wanem kain company o product o process o service em ol toktok long em long dispela

report em no soim olsem CISA o ol authoring agency laikim ol manmeri long yusim, em bilong toksave tasol. Dispela document em wok bung bilong CISA na ino regulatory document o document bilong lo.

OL RESOURCE

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
- The Cost of Unsafe Technology and What We Can Do About It | CISA
- Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (foreignaffairs.com)
- CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance
- CISA's Phishing Resistant MFA Fact Sheets
- Cyber Guidance for Small Businesses | 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
- The Cyber Threat - Response and Reporting
- FBI's Cyber Strategy

National Institute bilong Standards na Technology (NIST)

- NIST's Digital Identity Guidelines
- NIST's Cyber Security Framework
- NIST's Secure Software Development Framework (SSDF)

Cyber Security Centre bilong Australia (ACSC)

- ACSC's IoT Code of Practice Guidance for Manufacturers

National Cyber Security Centre bilong United Kingdom (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
- University of Cambridge's CHERI
- So long and thanks for all the bits - NCSC.GOV.UK

Cyber Security Center bilong Canada (CCS)

- CCCS's Guidance on Protecting Against Software Supply Chain Attacks
- Cyber supply chain: An approach to assessing risks
- Canadian Centre for Cyber Security's CONTI ransomware guidance

Federal Office bilong Information Security long Germany (BSI)

- The BSI Grundschutz compendium (module CON.8)
- The international standard IEC 62443, part 4-1
- State of IT-security in Germany report, 2022
- BSI practices of web application security

National Cyber Security Centre bilong Netherlands

- NCSC-NL's Mature Authentication Factsheet

Arapela

- How Complex Systems Fail
- The New Look in complex system failure