SECURE BY DESIGN

SENISIM WEI BILONG CYBERSECURITY BIRUA:

PASIN NA ROT BILONG
SECURE BY DESIGN SOFTWARE

CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL
NCSC-NO | NÚKIB | INCD | KISA | NISC-JP | JPCERT/CC | CSA | CSIRTAMERICAS

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Federal Office
for Information Security

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

National Cyber Security Centre
Ministry of Justice and Security

National Cyber Security Centre
a part of GCHQ

CSIRTAmericas Network

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

CSA SINGAPORE

certnz

NSM
NORWEGIAN NATIONAL
CYBER SECURITY CENTRE

Israel National Cyber Directorate

National Cyber
and Information
Security Agency

KISA KOREA INTERNET & SECURITY AGENCY

JPCERT CC®

Contents

BIKPELA TINGTING: MEKIM SAMTING EM INO STRONG

Technology em stap long olgeta hap long laif bilong yumi long olgeta dei, na 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 global 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.

Bikos long dispela, ol software manufacturer mas mekim samting wantaim ol tingting na pasin bilong secure by design na secure by default na mas mekim dispela samting nambawan tru. Sampela vendor em go pas tru long mekim ol dispela senis tasol sampela em kam bihain yet. Ol authoring ogenaisesin tok strong long olgeta technology manufacturer long mekim ol product bilong ol long wei we customer bai ino nid long wokim monitoring, mekim ol update na stretim samting long ol system long stop cyber birua. Mipela tok strong tu long ol software manufacturer long mekim product bilong ol long wei we em gat automation long ol configuration, monitoring na ol update em save kamap olgeta taim. Ol manufacturer mas lukim wok bilong strongim security bilong customer bilong ol olsem bikpela samting. Long taim bipo, ol software manufacturer save lusim wok bilong strongim security bilong ol product long han bilong customer taim samting bagarap na ol customer mas putim moni long baim ol patch long stretim samting. Tasol taim ol yusim pasin bilong secure by design, em nau bai stopim wei bilong traim stretim samting bihain long em bagarap pinis. **Note:** Dispela samting “secure by design” em karamapim secure by design na secure by default wantaim.

Long kamapim dispela high standard bilong software security, ol authoring ogenaisesin tok 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 na lukautim.

Wankain long dispela, European Union tok 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 lukautim ol customer, ol authoring ogenaisesin toktok strong long ol manufacturer long

[1] Ol authoring ogenaisesin luksave olsem dispela tok “safety” em gat planti mining taim ol yusim ol arapela kain wei. Long bihainim tingting bilong dispela guide, “safety” em toktok long strongim ol technology security standard long lukautim ol customer long ol cyber birua.

senisim ol design na development program na larim ol secure by design na default product tasol go long ol customer. Bipo long ol mekim samting, ol secure by design product em ol product we security bilong customer em bikpela samting na ino technical feature tasol. Ol secure by design product em gat security olsem bikpela tingting bipo long ol stat mekim samting. Ol product em stap pinis ken senis long kamap secure by design taim ol senisim isi isi. 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 gat misconfiguration, sapos patching ino 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 software 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)
- Norway's National Cyber Security Center (NCSC-NO)
- Computer Emergency Response Team New Zealand (CERT NZ) and New Zealand's National Cyber Security Centre (NCSC-NZ)
- Korea Internet & Security Agency (KISA)
- Israel's National Cyber Directorate (INCD)
- Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
- OAS/CICTE Network of Government Cyber Incident Response Teams (CSIRT) Americas
- Cyber Security Agency of Singapore (CSA)
- Czech Republic's National Cyber and Information Security Agency (NÚKIB)

Ol authoring ogenaisesin 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. Long kamapim dispela samting, ol authoring ogenaisesin laik kisim feedback o tingting bilong ol interested parties na laik bung wantaim long 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 article long CISA, The Cost of Unsafe Technology and What We Can Do About It.

[2] Bihain long dispela yumi kolim ol "authoring ogenaisesin".

WANEM SAMTING NIUPELA

Nambawan publication bilong dispela report em kirapim planti toktok insait long software industry. News bilong olgeta dei tokaut long ol ogenaisesin na ol wanwan manmeri husait painim hevi na dispela soim olsem planti moa toktok mas kamap long rausim ol problem stap yet wantaim ol software product.

Bihain long release bilong April 2023, ol authoring ogenaisesin (long hia go bai yumi kolim “mipela” na “bilong mipela”) kisim ol feedback na tingting bilong planti ol manmeri, ol company na ol trade association. Long olgeta feedback em kambek, bikpela samting em ol laikim sampela moa infomesin long ol tripela tingting o pasin na wei o rot ol software manufacturer na ol customer bilong ol ken bihainim ol dispela tingting. Insait long dispela document, mipela bai opim ol tingting bilong dispela report ol mekim pastaim na lukluk long ol arapela samting olsem manufacturer na sais bilong customer, maturity bilong customer, na scope o banis em ol dispela tingting bai karamapim.

Software em stap long olgeta hap na nogat wanpela report bai inap long karamapim gut olgeta kain software system, development bilong ol software product, customer deployment na maintenance, na we ol system ken wok o integrate wantaim ol arapela system. Long kisim halvim o guidance long ol samting tamblo we em ino klia long ol sampela environment, mipela laik harim long community long we ol dispela pasin o tingting em stap long dispela paper bin halvim long bringim ol security improvement.

Dispela report em lukluk long halvim ol manufacturer bilong artificial intelligence (AI) software system na model tu. Em ol narakain long ol traditional software, ol wankain security practice o pasin em bai halvim ol AI system na model tu. Sampela secure by design pasin bai senis liklik long wok wantaim ol samting em AI-specific, tasol ol tripela bikpela secure by design tingting em karamapim olgeta AI system tu.

Mipela luksave olsem wok bilong senisim wanpela software development lifecycle (SDLC) long wok wantaim ol dispela secure by design tingting em ino isi na bai kisim sampela taim long kamap. Na tu, ol liklik software manufacturer bai painim hat long mekim na bihainim planti bilong ol dispela tingting. Yumi bilip olsem software industry bai mas mekim ol dispela tool na procedure isi long kisim na dispela bai mekim ol product strongpela na moa safe. Planti moa manmeri na ogenaisesin nau wok long lukluk gut long ol software security improvement, na yumi bilip olsem dispela em opim dua long mekim samting narakain na dispela bai halvim ol bikpela na ol liklik software manufacturer wankain na dispela bai halvim olgeta customer.

Ol senis o update em kamap long nambawan secure by design report em soim commitment bilong mipela long strongim partnership wantaim ol planti stakeholder community husait em ol hap bilong technological ecosystem bilong yumi. Dispela ol samting em kamap long toktok o feedback em kam long ol planti hap bilong dispela ecosystem, na mipela lukluk yet long harim na lainim samting long ol. Em gat planti ol challenge kam yet, tasol mipela pilim hamamas na lukluk go het yet long lainim sampela moa long ol pipol na ogenaisesin husait bihainim dispela secure by design tingting, na painim olsem em kamapim ol gutpela samting.

WEI BILONG YUSIM DISPELA DOCUMENT

Mipela tok strong long ol software manufacturer long bihainim ol tingting na pasin insait long dispela document. Ol software manufacturer ken soim commitment bilong ol taim ol soim rot ol bihainim long pablik, wantaim ol dispela step stap tamblo. Mipela tok strong long ol software manufacturer long painim ol wei long bungim bikpela tingting bilong ol dispela pasin o principle na long raitim ol dispela rot go daun na dispela bai halvim long senisim tingting bilong ol customer long bihainim dispela secure by design tingting.

Na tu wantaim ol dispela rot ol software manufacturer mas bihainim, ol customer ken yusim dispela document tu. Ol company wok long baim software mas askim ol strongpela question long ol vendor bilong ol, na ken kisim halvim long ol example ol soim insait long dispela document. Taim ol wokim olsem, ol customer ken halvim long senisim market go long ol product em bihainim secure by design tingting. Wanpela kain askim ol customer ken askim ol vendor em ol soim long CISA's Guidance for K-12 Technology Acquistions.

Mipela tok strong long ol enterprise customer long bringim ol dispela pasin go long ol procurement process, vendor due diligence assessment, enterprise risk acceptance decision, na ol arapela rot ol save bihainim long sekim ol vendor. Ol customer mas askim ol vendor bilong ol long raitim na mekim pablik ol rot ol bihainim long mekim ol secure by design senis. Olgeta wantaim, dispela ken kamapim strongpela tingting long wokim samting wantaim gutpela security, na dispela ken halvim na strongim ol software manufacturer long mekim ol senis long strongim security bilong ol. Long mekim toktok long narapela wei, kain olsem yumi traim long kamapim wanpela secure by design tingting wantaim ol software manufacturer, yumi mas kamapim wanpela "secure by design" culture o pasin wantaim ol customer bilong ol tu.

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 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 ogenaisesin tok strong olsem ol manufacturer mas yusim wanpela tailored threat model taim ol mekim samting long stopim olgeta kain threat long system na lo strongim rot bilong salim system go long ol customer.

Ol authoring ogenaisesin tok strong long ol manufacturers long lukluk na holim bikpela tingting long security taim ol mekim ol product na platform bilong ol. Taim ol mekim samting em 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 em ino inap samting ol putim bihain taim. Em mas gat ol strongpela lida namel long ol top business executive bilong ol manufacturer long mekim security kamap nambawan samting long ol business, na ino technical feature tasol. Dispela wok bung namel long ol business lida na ol technical team bai stat long ol stage we ol statim design na development, na go olgeta long taim bilong customer deployment na maintenance. Ol tok strong long ol manufacturer long mekim ol bikpela decision long senisim ol samting na mekim ol investment, kain olsem ol samting bai hait long ol customer (e.g. senis go long ol programming languages we ken rausim ol bikpela rot we ol birua ken yusim). Ol mas mekim nambawan samting em ol feature, mechanism, na implementation bilong ol tool we ken lukautim ol customer na ino ol product feature we luk nais tasol opim dua long birua.

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 ino strong; tasol planti bilong ol dispela kain dua o vulnerability em kam long samting we gat liklik namba tasol. Ol manufacturer mas raitim ol rot bilong bihainim long mekim ol product bilong ol bihainim ol secure by design tingting, na traim yusim ol dispela rot olgeta taim.

Ol authoring ogenaisesin 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. Ol 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 ol bai nogat nid long 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 ino putim ol sampela kain banis. Secure by default em wankain samting olsem secure by design.

- 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 ino inap askim yu long 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 ino 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 ino 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.

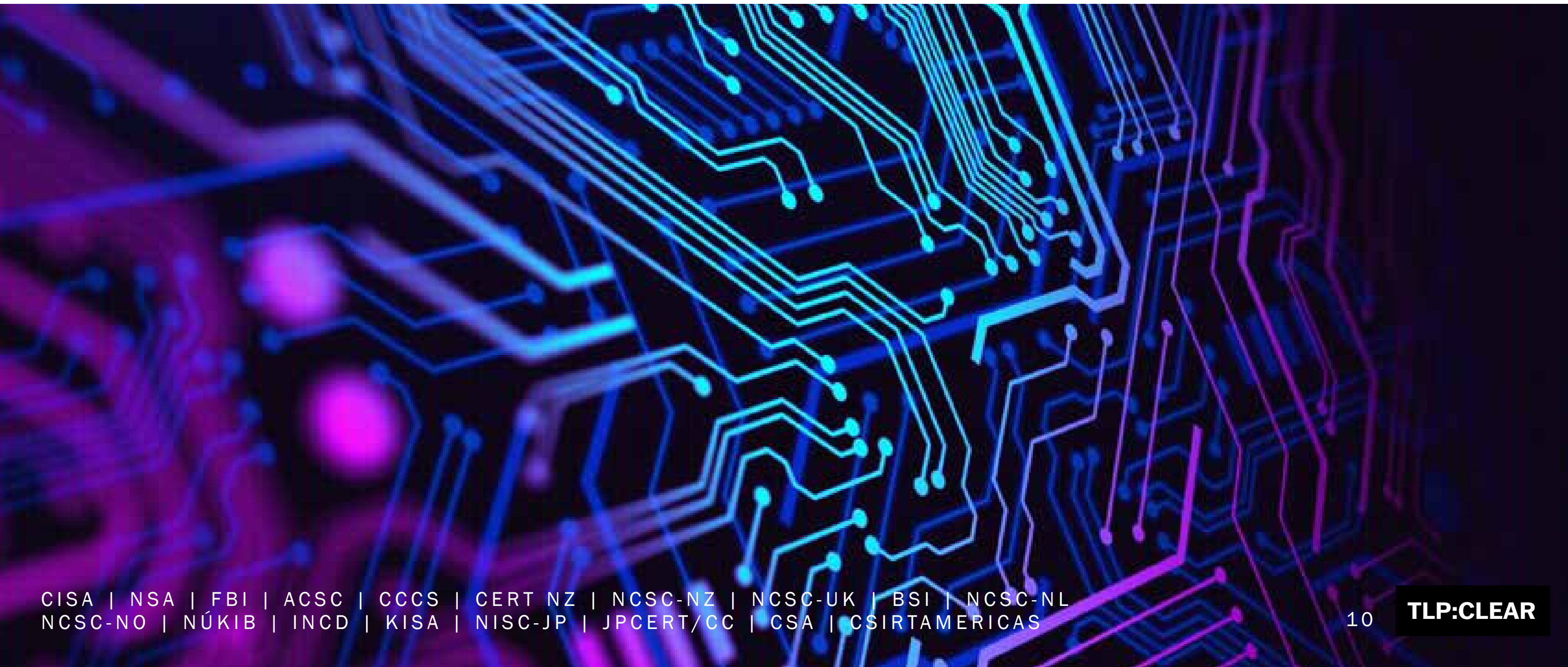
TINGTING O PASIN BILONG SOFTWARE PRODUCT SECURITY

Ol technology manufacturer mas senis na strongim tingting long software security. Ol authoring ogenaisesin 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 **Kisim hevi bilong security wari bilong customer husait baim product bilong ol** na strongim security bilong product. Hevi bilong security em mas noken stap long customer tasol.

2 **Holim strong pasin bilong tok tru na wokim samting klia.** Ol software manufacturer mas soim olsem ol save mekim na salim ol safe na secure product, na tu ol ken 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 advisory na wokim gut ol common vulnerability na exposure (CVE) record. Luksave tu, olsem ol CVEs em ino 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 executive lida long makim security olsem bikpela samting long product development na dispela nidim gutpela bung tingting o partnership wantaim ol customer bilong ogenaisesin.



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.

Insait long update em kamap long dispela guidance long October 2023, ol mekim dispela tripela tingting o pasin kamap klia moa wantaim ol explanation o tok klia, demonstration o wei bilong soim, na evidence.

PASIN 1: Go Pas Long Strongim Security Bilong Customer

TOK KLIA LONG DISPELA PASIN

Niupela best practice o wei bilong wokim samting tok olsem ol software manufacturer mas putim hatwok bilong ol go long product security long ol samting olsem **application hardening, application features,** na application **default settings.**

Ol software manufacturer mas wokim **application hardening** wantaim ol process na technology we em bai mekim ol malicious actor o birua wari o tingting planti taim ol laik traim bagarapim o kalap go insait long ol application. Ol application hardening protocol na procedure save halvim ol product long sanap strong taim ol birua o intelligent malicious actor kam. Ol samting olsem hardening, product security, na resilience em olgeta toktok long quality bilong ol product. Dispela tingting em olsem security em mas “stap insait taim ol mekim” na ino samting ol “putim go insait bihain”. [1] Taim security em stap insait taim ol mekim, ol software manufacturer ken strongim security bilong customer na tu strongim quality bilong product. Sampela rot ol ken bihainim em olsem ol mas sekim na lukautim wanem samting ol user putim go insait, na noken putim go stret long code (i.e., yusim ol parameterized query), yusim wanpela memory safe programming language, strongpela o rigorous software development lifecycle (SDLC) management, na yusim hardware-backed cryptographic key management.

Ol application mas sapotim ol **application feature** we em bilong cybersecurity. Sampela taim ol kolim “capabilities”, dispela ol features opim wei bilong yusim wanpela product o service long halvim long holim na strongim security bilong customer. Sampela ol security feature em kain olsem sapotim transport layer security (TLS) long olgeta network connection, sapotim single sign on (SSO), sapotim multi-factor authentication (MFA), security event audit logging, role-based access control (RBAC), na attribute-based access control (ABAC).

Sampela bilong ol dispela feature em configurable o customer ken senisim long mekim isi long putim go insait long peles na wei ol save wok nau. Ol dispela configuration min olsem ol application mas gat **default settings** em stap tasol ol customer ken senisim. Dispela ol default setting mas wok strong “out of the box” o taim customer kisim o baim na customer ken putim liklik hatwok o moni long strongim security bilong ol technology product bilong ol.

Olgeta bilong ol dispela samting – application hardening, ol application security feature, na ol application default setting – wok wantaim long strongim security bilong application, na tu long strongim na lukautim customer. Ol software manufacturer mas tingting gut long olgeta dispela samting na we ol ken wok wantaim. Ol manufacturer mas tingting bikpela moa na noken tingting tasol long we bilong putim ol dispela samting go insait long ol product bilong ol. Ol manufacturer mas go het moa na tingting long wei ol dispela samting ken senisim tru security pasin bilong ol customer, long mekim gutpela tru o long bringim birua long ol.

Ol manufacturer mas karim hevi bilong security bilong customer bilong ol na noken lukluk tasol long wei ol mekim samting o hamas moni ol putim. Hevi bilong dispela samting mas stap antap, wantaim ol manufacturer, we em gat bikpela moa sans long daunim o stopim birua long kamap bihain.

Tasol dispela samting em ino kamap tude. Planti ol manufacturer putim hevi bilong security long ol customer na ino save putim hatwok long wokim gut **application hardening.** Kain olsem, taim manufacturer putim patch long wanpela vulnerability o pasim wanpela rot bilong painim birua, planti taim yumi lukim ol wankain vulnerability kamap klia bikos ol lukluk long stopim samting kamap tasol na ino stretim samting em kamapim birua stret. Dispela product ken yusim ol kainkain rot insait long code base long stopim wankain ol vulnerability. Wanpela kain samting olsem, em taim manufacturer stretim wanpela input sanitization vulnerability, ol researcher o birua manmeri painim ol arapela code path we dispela samting em ino stretim gut. Ol manufacturer stretim wanwan hap tasol na ino tingting long lukluk long olgeta codebase na rausim dispela birua long olgeta hap bilong application.

Ol application feature ken bringim gutpela samting na tu ken bringim birua na hevi long ol customer. Ol feature we gat ol integration point wantaim ol planti external system na version ken bringim bikpela value tru long ol product. Na tu ol supporting feature we nogat retirement plan o rot bilong pinisim, kain olsem ol networking protocol, ken kamapim rot we ol customer ken painim birua sapos ol ino save gut long hevi bilong yusim ol olpela feature. Kain olsem, sampela product em yusim yet ol networking protocol em ol bin wokim long 1990s o 2000s na we yumi save nau olsem ol ino safe. Gat planti ol factor o samting we ken mekim hat taim ol customer laik mekim upgrade na putim ol niupela security measure hariap. Ol ken yusim ol product em save wok wantaim ol arapela hap bilong network bilong ogenaisesin, tasol nogat niupela ol security measure, na dispela bai mekim hat long IT team long putim ol niupela samting. Tasol, ol software manufacturer ken putim ol dispela kain samting long planning process bilong ol long toksave long ol customer long stap current.

Ol application default setting em wanpela hap we ol customer ken painim birua tu. Ol manufacturer save mekim ol default setting, dispela bai mekim isi long ol customer long yusim ol application feature ol laikim. Samting nogut long dispela pasin em olsem ol customer bai ino nidim sampela bilong ol dispela feature na protocol na em opim wei bilong birua long painim ol customer. Na tu, planti ol security protocol em ol save tanim off o nidim ol customer long mekim wok long senisim ol setting long strongim security. Explicit threat modelling em wanpela rot long halvim long mekim disisen long wanem ol feature bai ol mas tanim on wantaim ol default na wanem ol setting bai mas secure by default. Arapela rot em long lukluk gut na mekim wei bilong ol administrator long painim ol feature isi.

Sampela manufacturer save salim ol product wantaim ol default we ken kamapim birua long sampela o olgeta customer. We ol ken mekim ol default safe, planti taim ol save mekim wanpela **hardening guide** we ol customer ken mekim long ol product tasol em ol mas baim. Ol hardening guide gat sampela ol problem em ol kam wantaim. Sampela ol hardening guide em hat long painim na nogat gutpela sapot. Ol arapela em hat long mekim, na sampela taim ol nidim software development long raitim extension module. Ol arapela tu save tingting olsem husait ridim em gat gutpela save long cybersecurity long save long ol wei bilong senisim ol setting long stopim birua. Ol manmeri husait save wok wantaim ol dispela samting tasol nogat sampela save long we ol birua manmeri save wok ken painim hat long mekim ol toksave stap long hardening guide taim dispela toksave ino klia. Na tu, ino olgeta hardening guide em ol engineer raitim husait save long wei ol birua manmeri save tingting na wok, na dispela em min olsem ol hardening guide ol mekim em ino gutpela long halvim ol customer. Planti ol customer wok long karim hevi bilong strongim security long planti ol software o system, na planti taim em nogat planti moni o resource long halvim. Long wok wantaim ol hardening guide tasol em ino inap long halvim taim ol samting kamap bikpela.

Ol mas sekim ol setting bilong application oltaim, sapos ol default o customer mekim, wantaim save bilong manufacturer long ol birua em stap nau. Ol mas mekim ol application wantaim ol klia indicator o wei long lukim ol birua em ken kamap long ol dispela setting na mas toksave gut long ol customer long ol dispela indicator. Kain olsem ol niupela kar gat indicator bilong ol seat belt na bai mekim nois taim yu laik draiv wantaim nogat seat belt, ol software mas gat dispela kain indictator long soim security bilong system. Sapos wanpela application em nogat MFA long ol administrator account, em mas mekim wei long toksave long ol administrator olsem ol ken painim birua long account bilong ol na ogenaisesin bilong ol sapos ol ino stretim MFA. Na tu, sapos wanpela application em gat ol olpela protocol we gat ol cryptography em ino strong, em mas toksave long ol administrator olsem ogenaisesin ken painim birua na ol mas putim ol resource long stretim dispela wari. Mipela tok strong long ol manufacturer long putim ol toksave insait long product na noken traim putim dispela long ol administrator long mekim taim, gat save, na tingting long traim yusim ol hardening guide. Ol gutpela opotuniti stap long kamapim ol niupela wei bilong bringim gutpela security na usability wantaim.

Olgeta bilong ol dispela element antap em ken mekim ol situesen we ol customer mas traim long painim, putim moni, painim wok manmeri, na lukluk olgeta taim wantaim ol arapela **security product** long daunim sans bilong painim birua. Ol small na medium sais ogenaisesin (SMOs) em save painim hat long mekim ol dispela kain samting. Ol gat ol hevi bilong painim gutpela save manmeri, moni, na taim na dispela mekim hat long putim security olsem nambawan samting, na dispela em opim rot bilong painim birua. Na tu, ol investment long security ol sampela manufacturer mekim ken kamap bikpela samting. Wanpela toktok em ken mekim dispela problem klia em software industry em nidim ol strongpela o moa secure product, na ino planti moa ol product bilong security. Ol software manufacturer mas go het long bringim dispela senis.

> ***Software industry nidim ol strongpela secure product, na ino planti moa ol product bilong security. Ol software manufacturer mas go het long bringim dispela senis.***

Tude, yumi ken ridim ol toksave kam long ol manufacturer olsem wanpela customer em painim birua taim ol ino tanim on wanpela security feature o bihainim sampela hardening guidance. Arapela samting em, bihain long customer painim birua, ol manufacturer ken tok klia long wanem samting ken stopim dispela birua em wanpela security feature o hardening guidance na lukluk long mekim dispela samting olsem default wantaim nogat charge long customer. Long olgeta taim we dispela product em ino kisim gutpela hardening long design na implementation phase, ol manufacturer mas tok klia long rot ol wok long bihainim long rausim ol dispela kain birua long ol product bilong ol.

Ol software manufacturer mas karim hevi bilong mekim ol product wantaim security olsem nambawan samting. Long strongim dispela, ol mas lukluk gut long ol wok ol wokim na **skelim ol result stret**. Mipela toktok long ol manufacturer long noken lukluk tasol long ol wok bilong ol yet, tasol ol mas skelim gut na mekim report long ol result na strong bilong security bilong product bilong ol, na kirapim rot bilong kisim feedback long mekim senis long SDLC we ol ken strongim safety bilong ol customer na strongim ol secure product bilong ol. Reporting mas gat ol anonymized data we ol academic na security research community ken yusim long bihainim ol bikpela trend na skelim progress long olgeta hap long ecosystem.

WEI BILONG SOIM DISPELA PASIN

Ol software manufacturer na online service mas painim wei bilong soim ol gutpela samting em kamap taim ol bihainim dispela pasin o rot. Ol mas traim long painim ol evidence kain olsem ol artifact we ol lain autsait ken lukluk gut long em. Nogat wanpela artifact em yet bai inap long soim olsem wanpela manufacturer em gat gutpela secure by design program, tasol sapos ol givim sampela artifact em bai halvim long soim olsem dispela manufacturer em wok long traim long mekim ol secure product. Dispela rot em bihainim tingting bilong “soim em gutpela moa long toktok.”

Long soim dispela pasin o rot, ol software manufacturer mas traim ol step stap long dispela list. Ol authoring ogenaisesin luksave olsem nogat planti software manufacturer bai inap long mekim ol dispela samting hariap na kamapim ol artifact taim ol stat bihainim rot bilong secure by design. Na tu, ol software manufacturer bai mas mekim dispela list nambawan samting sapos ol customer yusim gut product o nogat long painim bikpela security benefit.

ROT BILONG SECURE BY DEFAULT

1. **Rausim ol default password.** Ol default password em kamap yet olsem rot we planti manmeri painim birua long olgeta yia. Taim yumi tingting strong long stopim dispela problem bai yumi ken mekim hat long ol birua long painim yumi. Na wankain samting tu, em ol manufacturer ken tingting gut long ol pasin bilong yusim password, kain olsem ol minimum password length na stopim ol manmeri long yusim ol password we ol painim birua wantaim bipo.
2. **Wokim ol field test.** Technology wok long senis na kamap bikpela, na dispela em bikpela samting long ol software manufacturer long mekim ol security-centric user testing long save gut long hau security bilong product bilong ol em wok insait long field o taim ol manmeri yusim. Wankain long wei ol user research save halvim ol software development requirement, ol software manufacturer mas mekim ol security-focused user research long save gut long we security user experience (UX) em ino wok gut. Taim ol lukluk long we ol customer yusim product bilong ol insait long peles bilong wok, ol software manufacturer ken kisim gutpela save long wei bilong strongim usability na effectiveness bilong ol security feature na control bilong product bilong ol. Dispela ol save ken halvim long luksave long ol hap we ol ken mekim product bilong ol gutpela moa na strongim security bilong ol customer. Kain olsem, ol field test ken soim olsem senis ken kamap long UX flow, ol default, alerting, na long monitoring. Ol field test ken soim wanem improvement ol bin wokim bipo long design bilong product na wei dispela senis em daunim namba bilong ol security patch, daunim ol configuration error, na stopim ol hap we birua ken kamap.

Ol manufacturer ken lukluk long ol dispela samting tu:

- Ol customer save bihainim gut ol toksave long hardening guide?
- Ol security feature bilong product nau wok long wok gut long field?
- Ol dispela feature save stopim tru ol birua?
- Wanem ol feature bai stopim gut ol birua?

Note: Long kisim gutpela save long ol dispela samting, ol software manufacturer ken wok olsem partner wantaim ol customer long mekim ol red team exercise long lukim sapos ol product ken stopim ol birua. Dispela ol field test ken kamap long peles bilong customer, virtually, o wantaim telemetry insait long application wantaim strongpela privacy.

3. **Mekim sais bilong hardening guide liklik moa.** Ol manufacturer ken strongim security posture bilong customer taim ol mekim gut o rausim ol product hardening guide na lukluk moa long ol critical security measure we ol customer mas mekim nambawan samting taim ol stat yusim product bilong ol. Ol noken mekim hat long ol customer wantaim bikpela list bilong ol security measure, em ol manufacturer ken toksave long ol bikpela security risk bilong product bilong ol na givim ol klia rot long bihainim long stopim ol dispela risk. Na tu, ol manufacturer ken givim ol customer ol tool na automation we em ken mekim wok bilong putim ol security control isi liklik, kain olsem ol script em ol ken putim long environment bilong ol. Dispela ol tool ken makim na soim ol senis bin kamap bihain long ol pastaim tru yusim dispela product. Taim ol mekim ol hardening guide isi liklik na givim ol customer ol tool na automation long yusim, ol manufacturer ken daunim hevi long ol customer and halvim long mekim ol product gutpela moa na isi long stat long yusim. Wanpela rot bilong bihainim em long yusim Parento principle long daunim namba bilong ol step long ol samting save kamap planti taim (em 80%), na givim gutpela toksave na tool bilong ol samting

ino save kamap planti taim (em 20%). Long dispela wei, software manufacturer bai mekim ol isi samting isi na ol hatpela samting ino hat tumas. Field testing em bai wanpela strongpela tool long lukim taim ol customer save kisim long painim, lainim, na bihainim ol hardening guide. Ol manufacturer ken tingting long wei product ken toksave long ol administrator long mekim samting insait long product yet na ino traim bihainim na mekim ol samting stap insait long hardening guide.

4. **Tok strong long stopim ol olpela feature em ino safe.**
   Mekim security olsem nambawan samting wantaim ol klia rot bilong mekim ol upgrade na ino traim long wokim backward compatibility. Mekim toksave long ol blog post long soim taim gat ol safer feature na protocol na rausim ol unsafe feature wantaim ol announcement, na dispela ken kam insait long product yet. Planti ol customer soim olsem ol ino inap long strongim ol system bilong ol wantaim ol niupela network, identity na ol arapela critical security feature. Sampela taim, ol customer save pret olsem ol functionality em stap bai bruk sapos ol wokim upgrade. Sapos ol mekim upgrade isi wantaim nogat problem, ol customer bai gat laik long mekim ol upgrade na kisim ol update bilong strongim security klostu na hariap. Ol software manufacturer mas tok strong long ol customer long bihainim ol rot bilong mekim upgrade na daunim customer risk.

5. **Putim ol strongpela alert.**
   Wankain long ol nois save kamap taim ol ino putim seat belt long kar, ol manufacturer mas putim ol gutpela alert taim ol user o admin ino stap long gutpela hap, na toksave long ol administrator olsem ol yusim ol olpela protocol long environment bilong ol na askim ol long bihainim rot bilong mekim upgrade. Putim ol gutpela alert taim ol user o admin, o application configuration, stap long unsafe state. Mekim dispela unsafe mode klia long ol administrator olgeta taim. Wanpela moa feature em long mekim olsem ol super administrator mas luksave taim nogat MFA long account bilong ol olgeta taim ol go long login screen, o stopim ol key feature inap ol tanim on MFA. Em gat sans long senis na kamap long ol dispela goal na ino kamapim alert fatigue.

6. **Mekim ol secure configuration template.**
   Dispela ol template ken mekim sampela ol configuration olsem ol safe setting long wok wantaim hamas risk ogenaisesin laik kisim. Em isi long traim mekim ol low/medium/high security template, tasol dispela em soim rot bilong yusim ol setting long lukautim risk bilong ol ogenaisesin. Ol template ken sapotim ol hardening guide long soim ol risk we manufacturer em painim.

ROT BILONG SECURE PRODUCT DEVELOPMENT

1. **Raitim go daun wei yu bihainim secure SDLC framework.** Ol secure SDLC framework em givim ol rot bilong bihainim wantaim ol pipol, process, na technology. Tingting long pablisim wanpela klia toksave long wanem secure SDLC framework control yu bihainim na toksave long wanem kain arapela control yu bin yusim bipo. Insait long US, tingting long yusim NIST Secure Software Development Framework (SSDF). Em ino checklist, tasol SSDF "toksave long ol gutpela pasin bilong secure software development."
2. **Raitim go daun ol Cybersecurity Performance Goals (CPG) o samting wankain yu bihainim.** Taim wanpela ogenaisesin tok olsem ol bihainim NIST SSDF standard, ol tok olsem SDLC bilong ol bihainim ol gutpela ol pasin o rot bilong em stap nau. Tasol, dispela strongpela SDLC tasol em ino inap. Ol mas lukautim enterprise na development environment bilong ol long ol birua husait laik traim long bagarapim ol security property bilong dispela product taim ol stap long development yet. Dispela kain birua em ino tingting tasol, wanpela em ol bin wokim na bringim bikpela hevi long ol customer, na tu long national security. Ol ogenaisesin mas tingting long raitim go daun na toksave long wei ogenaisesin em bihainim ol CISA CPGs, NIST Cybersecurity Framework (CSF), o ol arapela cybersecurity program frameworks.
3. **Management bilong ol vulnerability o dua bilong ol birua.** Sampela ol manufacturer gat vulnerability management program em save lukluk long stretim ol vulnerability ol painim insait o autsait, na dispela kain samting tasol. Sampela bikpela program em save kisim planti data-driven analysis bilong ol vulnerability na wanem samting em save kamapim ol, na save bihainim rot bilong rausim olgeta dispela kain vulnerability.[3] Ol save putim ol formal program long ol mekim ol samting olsem quality planning, quality control, quality improvement, na quality measurement. Ol save lukim defect management olsem bikpela samting bilong business, na ino samting bilong security tasol. Dispela ol program em wankain long sampela wei olsem ol quality na safety program stap long ol arapela industry.
4. **Yusim open source software wantaim gutpela tingting.** Taim yu yusim open source software, tingting gut na sekim ol open source package, mekim ol code contribution go long ol dependency, na halvim long lukautim development na maintenance bilong ol critical component. Long painim infomesin, Ministry of Economy, Trade and Industry (METI) bilong Japan em pablisim "Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security."
5. **Givim secure default long ol developer.** Mekim default rot bilong software development dispela secure rot wantaim ol safe building block bilong ol developer. Kain olsem, gat planti ol SQL injection vulnerability wok long bringim bikpela hevi, olsem na ol ken givim ol developer gutpela library long stopim ol dispela kain vulnerability o birua long kamap. Dispela em ol kolim ol "paved roads" o "well-lit paths", na dispela pasin o rot ken mekim samting kamap hariap na stap strong, na ken stopim ol manmeri long mekim samting krangi.
6. **Kamapim ol software developer wok manmeri husait save long security.** Strongim save bilong ol software developer bilong yu long security taim yu lainim ol long secure coding best practice. Na tu, halvim bikpela senis long kamap taim yu painim ol wok manmeri wantaim save long security na wok wantaim ol university, community college, bootcamp, na ol arapela educator long putim security go insait long ol computer science na software development curriculum.

[3] NIST SSDF, PO 1.2, Example 2: "Mekim ol policy em toktok long ol security requirement bilong software bilong ogenaisesin, na sekim olsem ol bihainim dispela long ol key point long SDLC (e.g., ol class bilong software birua ol sekim long ol gate, ol response taim ol painim ol vulnerability long software ol salim go aut.)"

7. **Testim security incident event management (SIEM) na security orchestration, automation na response (SOAR) wok wantaim.** Wantaim ol field test ol mekim, wok wantaim ol bikpela SIEM na SOAR provider na wantaim ol customer long kisim save long wei ol incident response team yusim ol log long lukluk long ol security incident ol ting olsem kamap na ol dispela em kamap tru. Sampela software developer tasol gat save long wei bilong wok wantaim ol incident na ken putim ol samting insait long ol log we em ino halvim ol responder long wok bilong ol. Taim ol wok wantaim ol SIEM na SOAR technology tu na wok wantaim ol incident response professional tru, ol development team ken putim ol infomesin long log we em givim klia stori, sotim taim na mekim samting klia long taim bilong incident.
8. **Go wantaim Zero Trust Architecture (ZTA).** Mekim ol product deployment guide go wantaim, samting olsem, ol NIST ZTA model na dispela CISA Zero Trust Maturity Model. Tok strong long ol customer long putim ol dispela pasin na tingting insait long ol environment bilong ol.

ROT BILONG PRO-SECURITY BUSINESS

1. **Givim logging na noken askim ol long baim moa.** Ol cloud service mas mekim na holim ol security-related log na noken askim long baim moa long dispela. Ol on-premises product mas bihainim dispela na mekim ol security-related log na noken askim long baim moa. Na tu, ol product mas mekim ol security event log olsem default bikos planti customer ino inap save long wei dispela ken halvim ol incident kamap pinis. Dispela ol rot bai nidim ol long lukluk gut o mekim review long wanem ol security event bai ol putim long log long soim cybersecurity state awareness, rot bilong customer long mekim ol log, wanem taim bai ol holim ol log, wanem wei bai ol lukautim integrity na storage bilong ol log, na wanem rot ol bai bihainim long wokim analysis long ol log. Sampela taim, dispela ol review ken toksave olsem bai mas gat senis o refactoring long log management architecture bilong application long halvim mekim ol wok stret na bai ol manufacturer hamamas long wok o moni bilong dispela wok tu. Ol mas wok wantaim ol incident response (IR) expert long givim bikpela moa sans long mekim ol log kamap gutpela long ol investigator husait yusim. Lukim section long ol SIEMs.
2. **Rausim ol tax em stap hait.** Pablisim toksave olsem bai yu ino inap askim long baim ol security o privacy feature o integration. Kain olsem, insait long bikpela piksa bilong identity na access management (IAM), gat ol service ol kolim single sign-on (SSO) service. Sampela ol manufacturer askim yu long baim moa long yusim ol SSO service (ol save kolim ol identity provider) wantaim system bilong ol. Dispela "SSO tax" em min olsem planti ol SMOs ino inap long yusim ol gutpela identity na access management, na dispela bai stopim ol long gat strongpela security. Sampela service save askim long baim moa long yusim MFA long ol user. **Security em ino karim bikpela prais olsem ol luxury good tasol yumi mas lukim olsem customer right.** Sampela manufacturer tok strong olsem nogat planti customer askim long ol dispela feature, na em hat moa long holim. Dispela ol toktok ino luksave olsem nogat planti customer bai ring long kros o traim senisim samting, na ino olgeta customer save long wanem kain gutpela samting ol dispela feature bai bringim, na olsem olgeta feature bai nidim moni long holim. Tasol yumi ino save lukim ol manufacturer askim long baim moa long ol samting olsem availability na data integrity. Ol cost long sapotim dispela ol bikpela samting em stap insait long prais olgeta customer baim, kain olsem cost bilong ol seatbelt, steering column yu ken senisim, na ol airbag we em ken lukautim yu taim accident kamap.
3. **Wok wantaim ol open standard.** Putim ol open standard long ol bikpela hap olsem network na identity procotol. Noken yusim ol propietary protocol taim yu ken yusim ol open standard.
4. **Givim ol tool bilong mekim upgrade.** Planti ol customer ino laik long yusim niupela kain version bilong ol product, na dispela em ol niupela na strongpela secure feature olsem secure network connection. Ol software manufacturer ken kisim planti moa customer long mekim ol niupela upgrade sapos ol givim ol tool long halvim mekim ol samting klia na daunim risk. Givim ol fri licence long ol customer long testim ol upgrade na patch long test environment olsem wei bilong kisim ol customer.

PASIN 2: Holim Strong Pasin Bilong Tok Tru Na Wokim Samting Klia

TOK KLIA LONG DISPELA PASIN

Ol software manufacturer mas wok hat long givim ol safe na secure product, na tu ol mas traim mekim ol yet narakain long ol arapela long manufacturer community long wei ol mekim dispela.

Yumi lukluk long wanpela wari em stap wantaim transparency. Taim ol wok manmeri long dispela samting toktok long pasin bilong tok tru, sampela taim ol save pas long wari olsem ol wok long givim "gutpela rot long ol birua." Tasol, bikpela evidence em tok olsem ol birua wok orait taim nogat ol dispela rot, na ol dispela wari ken stap baksait taim yumi toktok long pasin bilong tok tru long halvim ol direct customer, indirect customer, supply chain, na software industry olgeta.

Pasin bilong tok tru o transparency em halvim industry long sanapim ol gutpela wei bilong wok – long putim arapela wei, wanem samting em "gutpela" wei bilong wok. Em bai halvim ol dispela wei bilong wok long senis wantaim nid bilong ol customer, senis long pasin bilong ol birua, o senis wantaim technology. Pasin bilong tok klia halvim ol manufacturer wantaim liklik resource tasol long lainim samting long ol dispela wantaim bikpela resource. Ol toktok long bungim infomesin mas go bikpela moa long ol real-time threat indicator, na mas gat ol dispela element tamblo.

Pasin bilong tok klia bai halvim long mekim ol decision long security pastaim long development process, na dispela bai kamap olsem samting ol business leader na ol engineer na security professional bai wokim. Pasin bilong tok tru bai kamapim pasin bilong wok stret wantaim product.

Yumi lukluk long wei yumi strongim pasin bilong tok tru. Tude, em ino samting em save kamap we ol software manufacturer bai pablisim bikpela toksave long wei ol mekim na lukautim software na wei ol save strongim program bilong ol wantaim data o infomesin. Long software industry, nogat planti manufacturer save givim ol guided tour long wei ol mekim software bilong ol. Em nogat planti wei bilong ol software manufacturer long lukim wei ol arapela save sanapim SDLC program bilong ol, na wei ol dispela program save wok taim birua kamap long ol customer environment. Olgeta long industry wantaim bai painim halvim sapos planti moa rot bilong bungim infomesin kamap long ol samting olsem rot bilong luksave long hevi bilong ol security defect na long rausim sampela kain vulnerability. Wantaim ol dispela kain pasin, olgeta software manufacturer mas kamapim wei bilong lukautim security bilong product bilong ol yet. Sapos ol ino askim long baim moa long ol security feature, samting olsem safety na security bai kamap olsem cost center na ino profit center, na ol kampani ken painim gutpela samting taim olgeta wok wantaim na tok klia long wok bilong ol.

Yumi laik lukluk gut long ol rot we yumi ken strongim gut software industry. Em ino taim bilong yumi long traim mekim ol wanwan, liklik senis moa. Sapos yumi laik bung wantaim na rausim ol threat kam long ol birua wantaim gutpela save, yumi mas wok gut na tok klia na dispela bai hat tude, tasol em bai karim industry go het. Sampela ol manufacturer tude em ol karim ol dispela secure by design pasin. Olsem William Gibson tok, "future em kam stap pinis, tasol em ino stap wankain long olgeta." **Pasin bilong tok tru na tok klia bai salim aut dispela infomesin na halvim ol defender moa long ol birua.**

Pasin bilong tok tru ken halvim ol wankain ogenaisesin long strongim ol SDLC bilong ol. Ol customer na investor ken lainim sampela moa long ol investment na tradeoff ol manufacturer bin mekim, na wei dispela ol investment em strongim security bilong ol customer. Ol manufacturer husait holim pasin bilong tok tru na wokim samting klia bai givim ol customer infomesin long halvim ol mekim ol gutpela decision em ino kam long prais na feature tasol, em kam long security tu.

Ol ogenaisesin wok hat long lukautim ol supply chain na SDL bilong ol, tasol ol kampani painim hevi na birua kamap yet. Taim ol holim strong pasin bilong tok tru na wokim samting klia, dispela em min olsem ol mas tokaut long pablik long ol dispela birua na toksave long wanem senis ol mekim long stopim ol dispela kain birua long kamap gen. Dispela kain rot bilong bungim infomesin bai halvim ol arapela ogenaisesin long lainim ol dispela samting tasol na nogat nid long painim wankain hevi.

WEI BILONG SOIM DISPELA PASIN

Long soim dispela kain pasin, ol software manufacturer ken bihainim ol dispela step:

ROT BILONG SECURE BY DEFAULT

1. **Pablisim ol aggregate security statistic na trend.** Ol kain topic em olsem MFA adoption long ol customer na administrator na we ol yusim ol unsafe legacy protocol.
2. **Pablisim ol patching statistic.** Soim hamas percent bilong ol customer em stap long niupela version bilong product, na wanem samting yu wok long wokim long mekim ol update isi na kamap gut.
3. **Pablisim infomesin long ol unused privilege.** Pablisim infomesin long ol excessive permission long ol customer base na ol toksave na ol arapela senis long product yu mekim long daunim ol rot na dua we customer ken painim birua. Dispela ol unused privilege em gutpela samting long putim administrator alert long em, olsem ol seatbelt nois.

ROT BILONG SECURE PRODUCT DEVELOPMENT

1. **Sanapim ol internal security control.** Planti ol kampani lukim ol gutpela samting kam taim ol putim data bilong ol wantaim ol cloud provider. Ol dispela cloud provider kamap olsem taget bilong ol birua. Ol Software as a Service (SaaS) provider mas pablisim infomesin long ol internal control bilong ol. Kain olsem, ol SaaS provider mas pablisim infomesin long ol internal deployment bilong phishing-resistant MFA, olsem Fast Identity Online (FIDO) authentication. Em gutpela sapos ol ken tok olsem nogat wok manmeri ken lukim customer o ol arapela kain sensitive data sapos ol ino yusim authentication wantaim phishing-resistant MFA.
2. **Pablisim ol high-level threat model.** Ol secure by design product mas stat wantaim ol threat model em ol raitim na toksave gut long wanem samting ol laik mekim wok long traim long lukautim na long husait. Ol gutpela threat model bai kisim save long wei ol birua kamap, na bai karamapim ol enterprise na development environment wantaim, na tu bai toksave long wei ol software manufacturer laikim ol customer long yusim long environment bilong ol.
3. **Pablisim ol gutpela infomesion long ol secure SDLC self-attestation.** Ol manufacturer husait bihainim NIST SSDF, o ol arapela kain framework olsem em ol wok wantaim long kamapim gutpela software development lifecycle. Taim ol pablisim ol self-attestation long ol control dispela manufacturer em putim, na long wanem ol product, dispela bai soim wok bilong ol long bihainim ol dispela gutpela pasin na givim bikpela moa confidence long ol customer bilong ol. Ol arapela certification scheme em kain olsem Israel Cyber Supply Chain Methology.
4. **Holim strong pasin bilong tok klia long ol vulnerability.** Pablisim toksave olsem ol identified product vulnerability bai kamap olsem ol stret na klia CVE entry. Em tru long ol Common weakness enumeration field we em soim ol root cause bilong ol dispela vulnerability. Sapos pablik CVE database em stret na klia gut, em bai industry ken bihainim wei ol product wok long kamap secure moa, na wanem ol kain vulerability em save kamap moa. Tasol, lukaut gut long lukim namba bilong ol CVE olsem samting nogut, em ol dispela namba em soim olsem gat gutpela code analysis na testing community. Taim ol manufacturer putim dispela secure by design tingting, bai namba bilong ol CVE bai go antap taim ol mekim ol bikpela wok long painim na stretim ol vulnerability stap long code bilong ol. Ol manufacturer mas pablisim analysis bilong ol vulnerability ol painim bipo, wantaim ol pattern na measure ol yusim long stretim ol dispela kain vulnerability. Kain olsem, sapos bikpela percentage bilong ol CVE bilong wanpela kampani em kamap long ol cross-site scripting (XSS), sapos ol raitim root cause analysis, response (kain olsem senis go long ol web template framework long stopim XSS), na ol result bai soim ol customer olsem ol ino inap long painim hevi long ol dispela kain vulnerability we em gat wei bilong stopim em stap longpela taim pinis.
5. **Pablisim ol Software Bills of Materials (SBOMs).** Ol manufacturer mas gat gutpela save long supply chain bilong ol. Ol ogenaisesin mas mekim na lukautim SBOMs [2] bilong olgeta product bilong ol, askim long data long ol supplier bilong ol, na givim ol SBOMs long ol customer na user bilong ol. Dispela bai halvim long soim hatwok bilong ol long save gut long ol wanwan hap o component ol yusim long mekim product bilong ol, strong bilong ol long stretim ol niupela risk ol painim, na ken

halvim ol customer long rot bilong bihainim sapos ol painim niupela birua long sampela hap bilong supply chain bilong ol. Long painim sampela moa infomesin, Ministry of Economy, Trade, and Industry (METI) bilong Japan em pablisim ”Guide of Introduction of Software Bill of Materials (SBOM) for Software Management.” Pasin bilong tok klia na wok stret mas go tu long ol embedded device na data na ol model ol yusim insait long AI/machine learning (ML). Em halvim wantaim ol purchasing decision na operational capability, em ol SBOMs gat bikpela wok long infrastructure long painim na bekim ol birua stap long supply chain.

6. **Pablisim wanpela vulnerability disclosure policy.** Pablisim wanpela vulnerability disclosure policy we em (1) ken mekim ol wokim ol test long olgeta product em dispela manufacturer mekim na ol condition bilong ol test, (2) givim legal safe harbor long ol action kamap em stap wantaim dispela policy, na (3) mekim public disclosure bilong ol vulnerability long kamap bihain long sampela taim. Ol manufacturer mas mekim root-cause analysis long ol vulnerability ol painim na, long wanem wei em inap, mekim wok long rausim ol dispela kain vulnerability. Lukim Vulnerability Disclosure Policy Template bilong CISA long painim ol toktok long halvim wantaim dispela samting.

ROT BILONG PRO-SECURITY BUSINESS

1. **Givim nem bilong wanpela secure by design senior executive sponsor long pablik.** Long planti ogenaisesin, security (kain olsem quality) em stap wantaim ol technical team husait gat liklik pawa long mekim ol gutpela senis long strongim security bilong ol product. Givim nem bilong wanpela top business executive long lukautim dispela secure by design program bai senisim security bilong product long kamap wanpela nambawan samting long ogenaisesin.
2. **Pablisim wanpela secure by design roadmap.** Ol manufacturer mas raitim ol senis ol mekim long SDLC bilong ol long strongim customer security, wantaim ol field-test report, ol wok ol wokim long rausim ol wankain vulnerability, na ol samting em stap aninit long arapela pasin o tingting. Olsem long ol quality improvement wok, ol security improvement program gat ol wanwan hap o phase em planning, control na improvement. Long wei bilong soim na ino toktok tasol, taim ol pablisim roadmap na ol infomesin insait long ol dispela phase em bai strongim tingting na bilip olsem ol product em secure by design. Taim ol gat gutpela progress, ol manufacturer ken givim moa infomesin long ol transparency report. Taim ol mekim olsem bai ol soim hatwok bilong ol long bihainim ol secure by design tingting na ken givim strong long ol arapela kain program taim ol soim olsem dispela samting em kamap.
3. **Pablisim wanpela memory-safety roadmap.** Ol manufacturer ken bihainim rot long rausim wanpela bikpela kain vulnerability taim ol senisim ol product em stap nau na mekim ol niupela product wantaim ol memory safe language. Dispela em ino inap long kamap olgeta taim, tasol ol manufacturer ken tingting long mekim ol application wrapper wantaim ol memory safe language na noken traim long raitim olgeta application gen. Dispela em ken kamap taim ol manufacturer wok long mekim ol niupela hiring, training, code review, na ol arapela internal process, na tu wantaim ol wei ol wok long helpim ol open source community long wokim wankain samting.
4. **Pablisim ol result.** Taim ol mekim update long SDLC long putim dispela secure by design tingting, ogenaisesin bai painim ol gutpela samting hariap, ol gutpela samting wantaim ol resource, na sampela samting em ino kamap gut. Sapos ol soim ol dispela gutpela samting na ol samting ino kamap gut tumas, olgeta industry ken lainim sampela samting long ol dispela result.

PASIN 3: Lida Antap Mas Go Pas

TOK KLIA LONG DISPELA PASIN

Bikpela tingting em ol kolim “secure by design,” tasol ol incentive o gutpela samting long customer safety em bai kamap bipo long taim bilong product design. Ol stat wantaim ol business goal na ol implicit na explicit objective na ol desired outcome. Taim ol senior leader mekim security olsem wanpela bikpela samting long business, taim ol mekim ol internal incentive, na kamapim pasin bilong mekim security olsem wanpela design requirement bai ol kisim ol gutpela result.

Gutpela save long ol technical subject matter em bikpela samting long product security, tasol em ino samting bai ol lusim long ol technical staff. Em wanpela bikpela samting long business na em mas stat long antap.

Sampela manmeri askim sapos ol software manufacturer holim tupela tingting pastaim na kamapim ol gutpela artifact, em ol nid long bihainim namba tri pasin? Rot ol kampani bihainim long kamapim vision, mission, value, na culture bai senisim product, na ol dispela samting em save kam long top hap bilong ogenaisesin. Yumi lukim dispela long ol arapela industry husait mekim ol bikpela improvement long safety na quality. Expert bilong quality J.M. Juran raitim:

> ***Rot bilong painim quality leadership em min olsem ol manager long antap mas karim hevi bilong lukautim quality. Long ol kampani husait gat quality leadership, ol manager long antap em ol yet karim hevi bilong dispela wok. Mi ino save long ol arapela wei long painim dispela. [3]***

Mipela bilip olsem security em stap aninit long product quality. Taim security na quality kamap olsem bikpela samting long ol business na ino technical function tasol bilong ol technical staff long lukautim, ol ogenaisesin bai inap long stretim na bungim ol security wari bilong ol customer bilong ol gut na hariap tasol. Na tu, putim ol wok na ol resource long mekim software security kamap nambawan samting long business pastaim tru bai daunim hatwok bilong stretim ol software defect-na dispela bai daunim ol risk long national security.

Long wankain wei olsem ol leadership team karim ol corporate social responsibility (CSR) program, em nau gat planti moa tingting olsem ol corporate board, kain olsem ol dispela bilong ol software manufacturer, mas karim wok bilong lukautim ol cybersecurity program. Ol save yusim corporate cyber responsibility (CCR) long toktok long dispela niupela tingting.

WEI BILONG SOIM DISPELA PASIN

Long soim dispela pasin, ol software manufacturer mas bihainim ol samting olsem:

1. **Givim toksave long secure by design program long ol corporate financial report.** Sapos manufacturer em wanpela publicly traded kampani, putim wanpela section long ol annual report bilong ol secure by design wok. Ol kar o automobile kampani save gat ol section long annual financial report bilong ol long soim driver na passenger safety, wantaim ol infomesin long ol centralised na distributed quality na safety committee. Sapos ol soim ol secure by design program long ol financial report, em bai soim olsem ogenaisesin bungim customer safety wantaim ol corporate financial outcome na em ino bihainim ol marketing tingting tasol taim olgeta lain wok long toktok long em.
2. **Givim ol report long board of directors bilong yu.** Chief information security officer (CISO) em save givim report long ol corporate board na dispela save gat infomesin long ol current na planned security program, ol threat, suspected na confirmed security incident, na ol arapela update long security na health bilong kampani. Ol ino kisim infomesin long security bilong kampani tasol, ol board mas askim infomesin long product security na sapos em halvim security bilong ol customer o nogat. Ol board mas noken lukluk long CISO tasol, ol mas lukluk tu long ol arapela manager bilong kampani long daunim risk bilong ol customer.
3. **Strongim secure by design executive.** Em gat bikpela senis namel long ol ogenaisesin we ol technical team gat “executive buy-in,” na ol dispela we ol business leader lukautim ol customer security improvement process ol yet wantaim ol standard business process. Dispela tok “executive buy-in” em min olsem ol wok manmeri bin toktok strong long kisim sapot long customer safety program na em ino ol top-level bilong business kamap wantaim dispela tingting. Dispela executive mas gat pawa long bringim senis long ol product investment long strongim customer security.
4. **Mekim ol gutpela internal incentive.** Tingting gut long noken kamapim ol incentive em ino gutpela, na sanapim ol reward system long strongim customer security long kamap wankain olsem ol arapela gutpela behaviour na outcome. Long secure by design executive go long product management, software development, support, sales, legal na ol arapela ogenaisesin, putim ol customer security incentive go insait long hiring, promotion, ol salary, bonus, stock option, na ol arapela process em stap long wok bilong business. Kain olsem, taim ol kamapim ol criteria long promotion bilong ol software developer, tingting long ol samting em bai strongim security bilong product wantaim ol arapela criteria olsem uptime, performance, na feature improvement.
5. **Mekim wanpela secure by design council.** Long sampela ol industry, em save kamap olgeta taim we ol ogenaisesin bai mekim wanpela quality council, na long putim ol quality representative long ol bikpela division o business unit. Sapos ol gat ol centralised na distributed memba, dispela ol grup bai wok long strongim quality wantaim ol top level goal na bai kisim wok go insait tru long ogenaisesin. Na wankain samting, wanpela secure by design council bai strongim security na wok wantaim ol secure by design goal long ogenaisesin.
6. **Mekim na strongim ol customer council.** Planti ol software manufacturer gat ol customer council em gat ol customer kam long ol wanwan region, industry, na sais. Dispela ol council ken givim planti gutpela infomesin long ol gutpela samting ol customer painim na ol bel hevi ol painim wantaim ol product bilong kampani. Mekim agenda bilong council wantaim ol bikpela topic long lukluk long customer safety, maski sapos em ino bikpela samting yet long tingting bilong ol manmeri long council. Tingting long husait council bai givim report na rot bilong painim infomesin long ol manmeri bilong council long security bilong product. Kain olsem, council gat strongpela tingting go long marketing na sales, o long product management? Dispela secure by design executive mas halvim ol toktok wantaim ol customer na mas soim ol long ol arapela element long dispela pepa, kain olsem ol field study.

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 ogenaisesin toktok strong long yusim ol secure by design tactics, kain olsem ol tingting kam long SSDF. Ol software manufacturer mas kamapim wanpela 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 ogenaisesin luksave olsem ol arapela wei bilong strongim memory em stap, na em ken halvim wantaim ol olpela codebase. Dispela em kain olsem C/C++ language improvement, ol hardware mitigation, address space layout randomisation (ASLR), control-flow integrity (CFI), na fuzzing. Na tu, gat planti ol save manmeri gat wankain tingting olsem sapos ol yusim ol memory safe programming language em bai stopim ol dispela kain birua, na ol software manufacturer mas painim wei long yusim ol dispela samting. Sampela kain modern memory safe language em C#, Rust, Ruby, Java, Go, na Swift. Ridim memory safety information sheet bilong NSA long painim moa infomesin.
- **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, na tu ol arapela feature olsem Trusted Platform Modules na Hardware Security Modules. Sapos yu laikim sampela moa infomesin o toksave, go na lukim CHERI webpage bilong University of 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.
- **Parameterized queries (SSDF PW 5.1).** Yusim parameterised queries na noken kisim user input long ol query, long stopim ol SQL injection attack.
- **Static and 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 inap 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.7.1, 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, dispela ol kolim "error seeding."
- Software Bill of Materials (SBOM) (SSDF PS.3.2, PW.4.1). Karim wok bilong mekim SBOM[4] 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 tingting) we bai stopim dispela birua long kam insait.
- **CVE completeness.** Ol published CVE mas gat root cause o common weakness enumeration (CWE) long halvim ol lain long industry long lukluk gut long ol software security design flaw. 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 Stakeholder-Specific Vulnerability Categorization (SSVC) guidance. bilong CISA.
- **Defense-in-Depth.** Mekim samting wantaim tingting olsem sapos ol bagarapim wanpela security control bai ino inap 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 Cybersecurity Performance Goals (CPGs).** Mekim product we em bungim ol basic security tingting na rot. 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 ino bungim ol CPG – kain olsem ol nogat phishing-resistant MFA bilong olgeta wok manmeri – em bai ol luksave olsem ol ino mekim ol Secure by design product.

Ol authoring ogenaisesin 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 inap 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.

[4] Sampela bilong ol authoring ogenaisesin wok long lukluk long ol wei bilong kisim security assurance wantaim software supply chain.

SECURE BY DEFAULT TACTICS

Wantaim ol tingting stap long secure by design development, ol authoring ogenaisesin toktok strong tu long ol software manufacturer long strongim secure by default configuration long ol product bilong ol. Ol ogenaisesin mas wok hat long mekim update long ol product long stap wantaim ol dispela tingting taim ol wok long strongim na senisim. Kain olsem:

- **Rausim ol default passwords.** Ol product mas noken kam wantaim default password we olgeta save. Long rausim default password, ol authoring ogenaisesin 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 ino 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 na noken mekim ol baim moa o wokim sampela moa configuration. 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 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 Authorization 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 inap painim sapos ol ino 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 ino strong maski sapos em bai bringim sampela senis na pen.
- **Bihainim na daunim namba bilong “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 niupela release bilong software. Mekim ol hap bilong “hardening guide” kamap olsem default configuration bilong product. Ol authoring ogenaisesin

Luksave olsem ol sotpela hardening guide bai kamap taim gat ongoing partnership wantaim ol customer na gat hatwok bilong planti ol product team, kain olsem user experience (UX).

- **Tingting long user experience taim ol yusim ol security setting.** 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 ogenaisesin 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. Mipela bilip 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 ogenaisesin lukim ol bikpela case we customer em ino 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 ino 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 ino save olsem ol hardening guide stap na dispela em min olsem ol device configuration settings bilong ol em ino 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 security practitioner ken raitim ol dispela guide na ken mekim klia na isi long bihainim na yusim ol tingting stap insait long ol.

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 ogenaisesin toktok strong olsem ol ogenaisesin mas holim ol supplying software manufacturer bilong ol accountable long security bilong product bilong ol. Na tu, ol authoring ogenaisesin tok 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 software bipo long ol baim na tu ol givim strong na pawa long IT department long tok nogat sapos ol gat wari long security bilong software. Ol IT department mas gat pawa long mekim ol purchasing criteria we secure by design na secure by default rot em bikpela samting (ol practice o rot 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 ol gutpela secure by design na secure by default practice.

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.

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 wok long 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.

DISCLAIMER

Ol infomesin insait long dispela report em ol givim "as is" na em bilong toksave tasol. CISA na ol authorising ogenaisesin ino inap long toktok strong ol 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 ino soim olsem CISA o ol authorising ogenaisesin laikim ol manmeri long yusim, em bilong toksave tasol. Dispela document em work bung bilong CISA na ino regulatory document o document bilong lo.

OI 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 of Standards and Technology (NIST)

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

Australian Cyber Security Centre (ACSC)

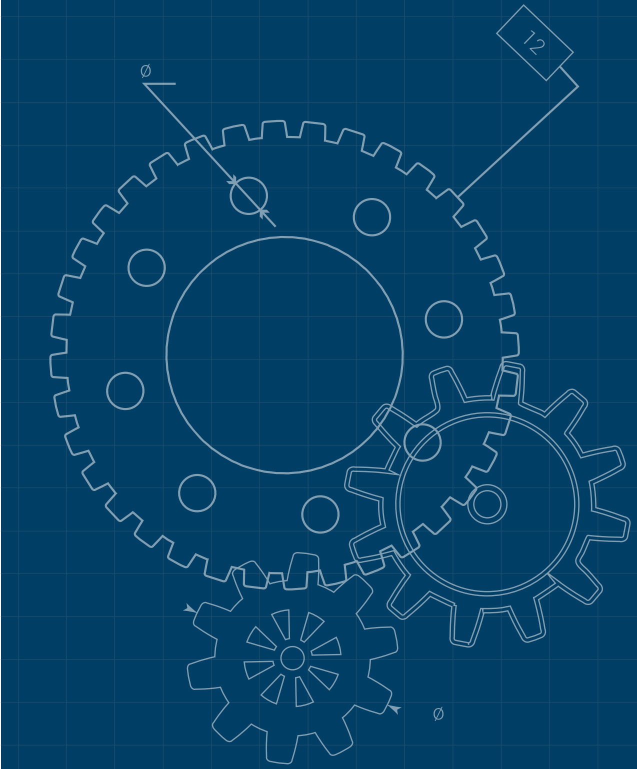
- ACSC's IoT Code of Practice Guidance for Manufacturers

The United Kingdom's National Cyber Security Centre (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

Canadian Centre for Cyber Security (CCCS)

- 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



Germany’s Federal Office for Information Security (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

Netherland’s National Cyber Security Centre

- NCSC-NL’s Mature Authentication Factsheet

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

- Japan’s National Cybersecurity Strategy

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

Cyber Security Agency of Singapore

- 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

Arapela

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

OL REFERENCE

[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.