TLP:CLEAR

SIKIUA TRU LONG DISAEN

SEFTEM BALENS BLONG SAEBASIKIURITI RISK:

OL PRINSIPOL MO OL APROJ BLONG STAP SIKIUA TRU LONG DISAEN SOFWEA

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Ol Topik

OVAVIU:
VALNEREBOL TRU LONG DISAEN

Teknoloji hem i stap insaed long klosap evri eria blong deili laef. Ol sistem we man i aksesem tru long intanet oli konek i ko long ol impoten sistem we oli afektem long wan daerek wei ikonomik prosperiti, laef, mo iven helt blong yumi, mo hemia i inkludim pesenal aedentiti manejmen kasem medikol kea. Wan eksampol blong rabis saed blong ol kaen sevis olsem hem i ol saeba atak we i hapen raon long wol we i mekem se ol hospital oli kanselem ol sejeri mo daevetem kea blong ol peisen. Taem teknoloji i no sikiua mo ol impoten sistem oli isi blong atakem, hemia i save invaetem ol rabis saeba atak, we maet i save mekem se i stap kat ol siries sefti[1] risk.

Olsem wan risal blong hemia, hem i impoten blong ol teknoloji manufakjera oli mekem sikiua tru long disaen mo sikiua tru long difolt ol mein poen blong prodak disaen mo ol divelopmen proses. Sam venda oli bin tekem ol bigfala step blong draevem indastri ia i ko fowod long sofwea asurens, be ol narafala wan oli bihaen. Ol ejensi we oli raetem dokumen ia oli stap enkarejem long wan strong wei evri teknoloji manufakjera blong bildim ol prodak blong olketa long wan wei we i mekem se ol kastoma oltaem oli no nid blong mekem monita, ol rutin apdeit, mo damej kontrol long ol sistem blong olketa blong mekem se ol saeba atak oli no hapen tumas. Mifala i stap askem strong tu long ol sofwea manufakjera blong bildim ol prodak blong olketa long wan wei we i mekem i isi blong otomeitem konfikureisen, monitoring, mo ol rutin apdeit. Oli stap enkarejem ol manufakjera blong oli tekem onasip blong impruvum ol sikiuriti aotkam blong ol kastoma blong olketa. Folem histri, ol teknoloji manufakjera oli bin stap dipen long fasin blong fiksim ol ples we i isi blong oli atakem we oli faenem afta we ol kastoma oli instolem ol prodak, mo hem i nidim ol kastoma blong oli yusum mani blong olketa wan blong fiksim ol eria ia. Sipos nomo we yumi yusum ol sikiua tru long disaen praktis bambae yumi brekem ol rabis saekol blong krietem mo aplaem ol ansa mo aplaem olketa. **Ol Not:** Toktok ia “sikiua tru long disaen” hem i kavremap tuketa sikiua tru long disaen mo sikiua tru long difolt.

Blong kasem hae standed blong sofwea sikiuriti ia, ol ejensi we oli raetem dokumen ia oli stap enkarejem ol manufakjera blong putum olsem praeoriti intekreisen blong prodak sikiuriti olsem wan impoten pririkwisit long ol fija mo spid from maket. Ova taem, ol tim blong ol enjinia bambae oli save putum wan niu peis we i stap semak oltaem we sikiuriti hem i rili disaen insaed mo i tekem les wok blong mentenem.

Yuropian Yunion hem i riflektem tingting ia, taem hem i riinfosem impotens blong prodak sikiuriti long Saeba Risiliens Akt, we i emfasaesem se ol manufakjera oli mas implementem sikiuriti truaot long laef saekol blong wan prodak blong stopem ol manufakjera blong oli no introdusum ol prodak i ko long maket we maet oli isi blong atakem.

[1] Ol ejensi we oli raetem dokumen ia oli luksave se wod ia “sefti” hem i kat fulap mining we i folem konteks we man i yusum long hem. Folem pepes blong gaed ia, “sefti” bambae hem i rifea long fasin blong leftemap ol standed blong teknoloji sikiuriti blong protektem ol kastoma long ol rabis saeba aktiviti.

Blong krietem wan fiuja we teknoloji mo ol prodak we oli yusum teknoloji oli sef blong ol kastoma, ol ejensi we oli raetem dokumen ia oli askem ol manufakjera blong oli jenjem disaen blong olketa mo divelopem ol prokram blong oli alaoem sikiua tru long disaen mo ol difolt prodak blong oli shipim i ko long ol kastoma. Longtaem bifo manufakjera i divelopem ol prodak, manufakjera i lukluk long sikiuriti blong ol kastoma blong ol prodak we oli sikiua tru long disaen olsem wan mein bisnis gol, i no se hem i jes wan teknikol fija. Ol prodak we oli sikiua tru long disaen oli stat wetem gol ia bifo divelopmen i stat. Ol prodak we oli stap finis oli save jenj i ko long wan steit we oli sikiua tru long disaen taem oli ripitim blong jenjem olketa. Ol prodak we oli sikiua tru long difolt oli olketa we oli sikiua blong yusum 'aotsaed long boks' wetem smol o nokat konfikureisen jenj we i neseseri mo oli kat ol sikiuriti fija we i nokat adisenal kost blong hem. Tuketa, tufala prinsipol ia oli muvum bigfala pat blong beden blong stap sikiua i ko long ol manufakjera mo i katem daon ol janis se ol kastoma bae oli kam viktim blong ol sikiuriti insiden we i hapen from ol miskonfikureisen, kwik ripea wok we i no naf, o fulap narafala isiu we i komon.

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI) mo olketa intanasonal patna ia[2] oli stap kivim ol rekomendeisen insaed long gaed ia olsem wan rodmap blong teknoloji manufakjera blong mekem sua se i kat sikiuriti blong ol prodak blong olketa:

- 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 okanaeseisen we oli raetem dokumen ia oli luksave ol kontribusen blong fulap praevet sekta patna blong mekem sikiuriti tru long disaen mo sikiuriti tru long difolt hem i muv fowod. Eim blong prodak ia hem i blong muvum wan intanasonal konveseisen abaot ol mein praeoriti, ol invesmen, mo ol disisen blong ajivim wan fiuja we teknoloji hem i sef, sikiua, mo risilien tru long disaen mo difolt. Blong kasem eim ia, ol okanaeseisen we oli raetem dokumen ia oli askem ol pati we oli intres blong kivim fidbak long prodak ia mo oli wantem kat wan siris blong ol sesen we bae oli lisen blong jenjem moa, spesifaem moa mo advansem moa gaedans blong yumi blong ajivim ol gol we yumi sherem.

Blong kasem moa infomeisen abaot impotens blong prodak sefti, lukluk atikol blong CISA, The Cost of Unsafe Technology and What We Can Do About It.

[2] Afta long ples ia oli singaotem se "ol okannaeseisen we oli raetem dokumen ia."

WANEM HEM I NIU

Fesfala pablikeisen blong ripot ia i bin jenereitem bigfala storian insaed long sofwea indastri. Nius we i stap kamaot evridei abaot ol okanaeseisen mo wanwan man we sikiuriti blong olketa i stap long denja hem i haelaetem nid blong kat fulap moa storian abaot hao blong adresem ol problem long ol sofwea prodak we oli stap kontinu oltaem mo we oli sistematik.

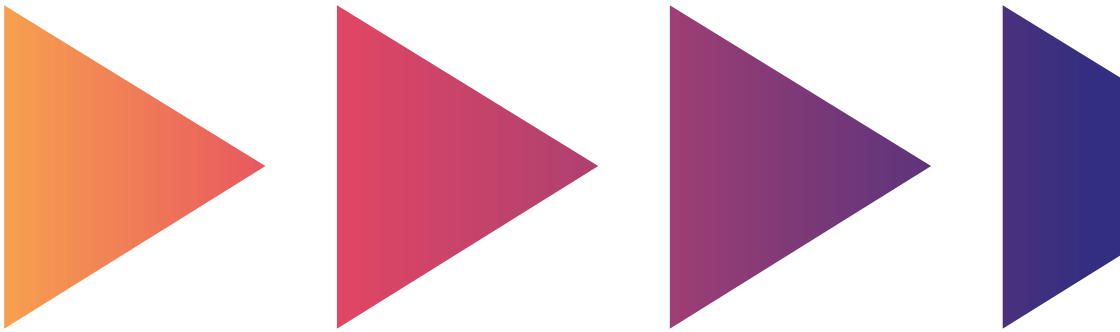
Afta long rilis long Eprel 2023, ol okanaeseisen we oli raetem dokumen ia (afta long ples ia oli singaotem olsem “mifala” mo “blong mifala”) oli bin kasem fidbak we i kam long plante plante man, kampani mo ol tred asosieisen. Mos komon rikwes long fidbak hem i blong kivim moa ditel abaot ol trifala prinsipol from se oli aplae long tuketa ol sofwea manufakjera mo ol kastoma blong olketa. Long dokumen ia, mifala i ekspandem orijinel ripot mo taj long ol narafala topik olsem manufakjera mo kastoma saes, kastoma majuriti, mo skop blong ol prinsipol.

Sofwea i stap long evriples mo i nokat wan singol ripot we bae i save kamaot blong i kavremap gud evri topik abaotem ol sofwea sistem, divelopmen blong ol sofwea prodak, kastoma diploemen mo mentenens, mo intekreisen wetem ol narafala sistem. Blong gaedens we i stap andanit ia we i no stret gud long wan kaen envaeromen, mifala i luk fowod blong harem ol komuniti oli talem olsem wanem ol praktis we i stap insaed long pepa ia oli lid i ko long ol kaen sikiuriti impruvmen.

Ripot ia hem i aplae long ol atifisol intelijens (AI) sofwea sistem mo ol model tu. Nomata maet bae oli difren long ol tradisonal fom blong sofwea, ol mein sikiuriti praktis oli stil aplae long ol AI sistem mo ol model. Sam sikiua tru long disaen praktis maet oli nidim modifikeisen blong eksplenem ol AI-spesifik konsidereisen, be ol trifala mein prinsipol blong sikiua tru long disaen oli aplae long evri AI sistem.

Mifala i luksave se blong jenjem wan sofwea divelopmen laefsaekol (SDLS) blong i stret wetem olketa sikiua tru long disaen prinsipol, hem i no wan simpol wok mo i save tekem taem. Mo tu, ol sofwea manufakjera we oli smol moa maet oli save strakel blong implementem fulap long ol tingting we i stap ia. Mifala i biliv se sofwea indastri i nid blong mekem ol tul mo ol prosija we oli mekem se ol prodak oli moa sef, i avelebol long fulap man. Taem moa man mo ol okanaeseisen oli fokasem atensen blong olketa long ol impruvmen blong sofwea sikiuriti, mifala i biliv se i kat rum blong ol inoveisen we bambae oli mekem speis we i stap bitwin ol bigfala sofwea maufakjera mo olketa we oli moa smol bambae i kam moa smol blong benefitim evri kastoma.

Hemia hem i apdeit blong orijinel sikiua tru long disaen ripot hem i pat blong komitmen blong mifala blong bildim ol patnaship wetem plante stekholda komuniti we oli konkonek blong sapotem teknolojikol ekosistem blong yumi. Hem i risal blong fulap fidbak we i kam long plante pat blong ekosistem ia, mo bambae mifala i kontinu blong lisen mo lan long ol tingting. Nomata we i kat fulap jalenj i stap long fored, mifala i kat bigfala strong mo positif tingting taem mifala i lanem moa abaot ol man mo ol okanaeseisen we oli aoptem finis wan sikiua tru long disaen prinsipol, fulap taem wetem sakses.



OLSEM WANEM BLONG YUSUM DOKUMEN IA

Mifala i askem strong long ol sofwea manufakjera blong folem ol prinsipol we oli stap insaed long dokumen ia. Ol sofwea manufakjera oli save demonstretem komitmen blong olketa taem oli dokumentem long wan pablik wei, ol aksen we oli bin tekem, folem ol step we oli stap long lis andanit ia. Mifala i enkarejem ol sofwea manufakjera blong faenem ol taktik blong mitim spirit blong prinsipol ia mo blong krietem ol atifak we bambae oli kivim wan strong mesej long iven ol man o okanaeseisen tete we oli no bilivim we oli save kam olsem ol kastoma se oli stap ekspresem sikiua tru long disaen prinsipol.

Mo tu wetem ol aksen we ol sofwea manufakjera oli mas tekem, ol kastoma oli save influensem dokumen ia. Ol kampani we oli stap pem sofwea oli mas askem ol had kwesten long ol venda blong olketa, mo bae oli lukluk long ol eksampol blong folem ol prinsipol we oli listim long dokumen ia blong i inspaerem olketa. Taem oli mekem olsem, ol kastoma oli save help blong seftem maket i ko long ol prodak we oli moa sikiua tru long disaen. Wan eksampol blong ol kwesten we ol kastoma oli save askem long ol venda hem i stap insaed long CISA's Guidance for K-12 Technology Acquisitions.

Mifala i enkarejem ol entapraes kastoma blong inkoporeitem ol praktis ia i ko insaed long ol prokiuamen proses, ol venda diu dilijens asesmen, ol entapraes risk akseptens disisen, mo ol narafala step we oli tekem blong skelem ol venda. Ol kastoma oli mas pushum tu ol venda blong olketa blong dokumentem long wan pablik wei ol sikiua tru long disaen aksen we wanwan venda i tekem. Sipos oli wok tuketa olsem wan krup, hemia i save krietem wan strong diman siknel blong sikiuriti, we i save enkarejem mo eneblem ol sofwea manufakjera blong tekem ol step i ko from sikiuriti we i moa bigwan. Blong talem long narafala wei, semak olsem we mifala i lukaotem blong krietem wan yunivesel sikiua tru long disaen prinsipol insaed long ol sofwea manufakjera, mifala i nid blong krietem wan "sikiua tru long diman" kalja wetem ol kastoma blong olketa.

Sikiua tru long Disaen

"Sikiua tru long disaen" hem i minim se oli bildim ol teknoloji prodak long wan wei we hem i stopem long wan risinabol wei ol rabis saeba akta blong oli kat sakses taem oli aksesem ol divaes, data, mo infrastrakja we i konek. Ol sofwea manufakjera oli mas mekem wan risk asesmen blong aedentifaem mo nambarem ol saeba tret we oli stap ko raon long ol mein sistem, mo afta inkludim ol proteksen long ol prodak bluprint we i eksplenem saeba tret landskep we i stap jenj.

Mifala i rekomendem tu ol divelopmen praktis blong sikiua infomeisen teknoloji (IT) mo ol maltipol leia difens— we oli kolem dip-difens—blong stopem aktiviti blong ol ataka blong i ko putum ol sistem long denja o blong oli aksesem sensitif infomeisen we oli no sapos blong aksesem. Ol ejensi we oli raetem dokumen ia oli rekomendem tu se ol manufakjera oli yusum wan stret model long stej blong prodak divelopmen blong adresem evri tret we i save tek ples long wan sistem mo eksplenem diploemen proses blong wanwan sistem.

Ol ejensi we oli raetem dokumen ia oli askem ol manufakjera blong tekem wan ful sikiuriti aproj blong ol prodak mo platfom blong olketa. Sikiua tru long disaen divelopmen hem i nidim stratejik invesmen blong ol risos we ol sofwea manufakjera oli dedikeitem long wanwan leia blong prodak disaen mo divelopmen proses we bae oli no "jes putum i ko" afta. Hem i nidim se ol top bisnis eksekiutif blong manufakjera oli kat strong lidaship blong mekem se sikiuriti hem i wan bisnis praeoriti, mo i no jes wan teknikel fija. Kolaboreisen ia bitwin ol bisnis lida mo ol teknikel tim i eksten long ol prliminieri stej blong disaen mo divelopmen, tru long kastoma diploemen mo mentenens. Oli enkarejem ol manufakjera blong mekem ol had tredof mo ol investem, we i inkludim olketa we bambae oli "invisibol" long ol kastoma (eksampol, yusum ol prokraming langwij we i stopem ol valnerabiliti we oli komon.) Oli mas praeoritaesem ol fija, ol mekanisim, mo implimenteisen blong ol tul we oli protektem ol kastoma be i no ol prodak fija we maet bae i luk gud be i mekem atak sefes i ko bigwan.

I nokat wan singol ansa blong endem tret we i stap oltaem blong ol rabis saeba akta we oli tek advantej long ol wiknes insaed long teknoloji, mo ol prodak we oli "sikiua tru long disaen" bambae oli kontinu blong safa long ol wiknes ia; be, wan bigfala set blong ol wiknes hem i from wan smol sabset blong ol rut kos. Ol manufakjera oli mas divelopem ol rodmap we oli raetem blong alaenem ol prodak potfolio blong olketa we oli stap naoia wetem moa sikiua tru long disaen praktis, mo mekem sua se oli folem wan difren rod taem nomo we i kat ol ekstraodineri situeisen.

Ol ejensi we oli raetem dokumen ia oli andastanem se fasin blong tekem onasip abaot ol sikiuriti aotkam blong ol kastoma mo blong mekem sua se level blong kastoma sikiuriti ia maet bae save inkrisim ol divelopmen kost. Be, sipos ol manufakjera oli inves long ol sikiua tru long disaen praktis taem oli stap divelopem ol niufala teknoloji prodak mo mentenem olketa we oli stap finis, hemia hem i save impruvum bigwan sikiuriti blong ol kastoma mo katem daon janis blong ol ataka oli atak. Ol prinsipol blong sikiua tru long disaen oli no mekem sikiuriti blong ol kastoma i strong mo oli no mekem reputeisen blong brand hem i strong nomo be hem i katem daon mentenens mo pajing kos blong ol manufakjera long longtem.

Ol Rekomendeisen blong ol Sofwea Manufakjera seksen we oli listim i stap andanit ia hem i kivim wan list blong ol praktis mo polisi blong ol prodak divelopmen we oli rekomendem blong ol manufakjera oli tingbaot.

Sikiua tru long Difolt

"Sikiua tru long difolt" hem i minim se ol prodak oli resilien akensem ol eksploiteisen teknik aotsaed long boks mo i no nidim adisenal kost. Ol prodak ia oli protek akensem ol tret mo ol wiknes we oli stap hapen oltaem mo ol en yusa oli no nid blong tekem ol ekstra step blong sikiurem olketa. Ol sikiua tru long difolt prodak oli disaenem blong mekem ol kastoma oli save gud se taem we oli ko aot long ol sef difolt, oli stap inkrisim ol janis blong oli stap long denja be sipos nomo we oli implementem ol ekstra kontrol we oli kompensetem wok ia. Sikiua tru long difolt hem i wan kaen sikiua tru long disaen.

- Wan sef konfikureisen hem i shud stap olsem difolt beislaen. Ol prodak we oli sikiua tru long difolt oli tanem on ol sikiuriti kontrol long wan otomatik wei we prodak i nidim blong protektem ol entapraes akensem ol rabis saeba akta, mo tu blong saplaem abiliti blong yusum mo konfikarem moa ol sikiuriti kontrol we i nokat adisenal kost blong hem.
- Kompleksiti blong sikiuriti konfikureisen hem i no sapos blong stap olsem wan kastoma problem. Ol IT staf blong ol okanaeseisen sam taem oli ova lod wetem ol sikiuriti mo opereisenal risponsibiliti, mekem se oli nokat inaf taem blong andastanem mo implementem ol sikiuriti implikeisen mo mitikeisen we oli nidim blong kat wan strong saeba sikiuriti. Ol manufakjera oli save helpem ol kastoma blong olketa impruvum sikiua prodak konfikureisen—sikiurem "difolt rod" —blong mekem se oli manufakjarem, distributum, mo yusum ol prodak blong olketa long wan sikiua wei folem ol "sikiua tru long difolt" standed.

Ol manufakjera blong ol prodak we oli "sikiua tru long difolt" oli no jajem wan ekstra kos blong implimentem ol ekstra sikiuriti konfikureisen. Be, oli inkludim olketa insaed long beis prodak olsem ol sitbel we oli inkludim insaed long evri niu trak.

Sikiuriti hem i no sapos blong stap olsem wan lakseri opsen, be oli mas lukluk se hem i wan raet we ol kastoma oli risivim we oli no mas nikosiet from o pem moa from.

OL REKOMENDEISEN BLONG OL SOFWEA MANUFAKJERA

Joen gaed ia hem i kivim ol rekomendeisen i ko long ol manufakjera blong divelopem wan rodmap we oli raetem blong implementem mo mekem sua se i kat IT sikiuriti. Ol ejensi we oli raetem dokumen ia oli rekomendem se ol sofwea manufakjera oli implementem ol strateji mo aotlaenem long ol seksen andanit ia blong tekem onasip blong ol sikiuriti aotkam blong ol kastoma blong olketa tru long ol prinsipol blong sikiua tru long disaen mo difolt.

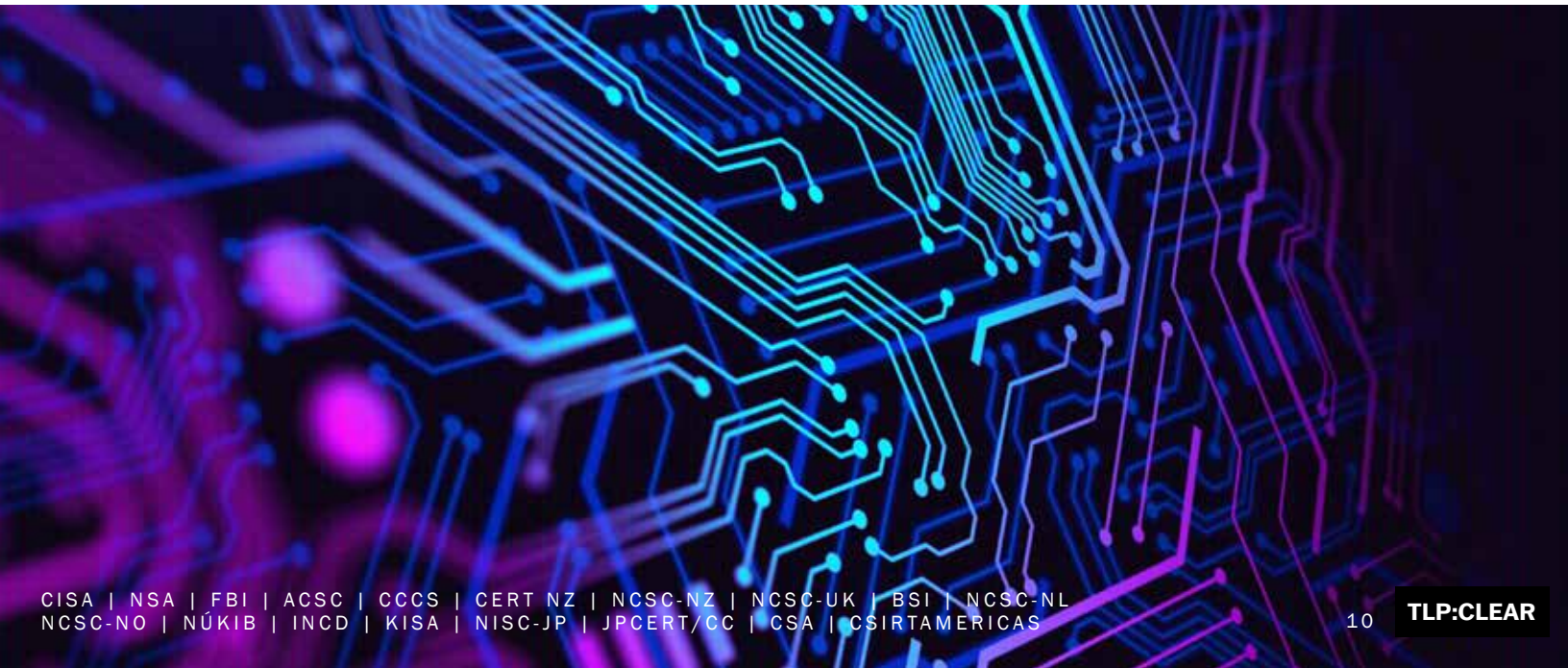
OL PRINSIPOL BLONG SOFWEA PRODAK SIKIURITI

Mifala i stap enkarejem ol teknoloji manufakjera blong adoptem wan stratejik fokas we i praeoritaesem sofwea sikiuriti. Ol ejensi we oli raetem dokumen ia oli divelopem ol trifala impoten prinsipol ia andanit ia blong gaedem ol sofwea manufakjera blong bildim sofwea sikiuriti i ko insaed long ol disaen proses blong olketa bifo oli divelopem, konfikurem mo shipim ol prodak blong olketa.

1 **Tekem onaship blong ol kastoma sikiuriti aotkam** mo jenjem ol prodak folem. Beden blong sikiuriti i no mas foldaon fulwan long kastoma.

2 **Holem radikol transparensi mo akaontebiliti.**
Ol sofwea manufakjera oli shud leftemap olketa wan blong dilivarem ol sef mo sikiua prodak, mo tu blong difrensietem olketa wan aot long evri narafala wan insaed long manufakjera komuniti folem abiliti blong olketa wan blong mekem hemia. Hemia hem i inkludim fasin blong serem infomeisen we oli lanem long ol kastoma diploemen blong olketa, olsem oli apruvum ol strong otentikeisen mekanisim tru long difolt. Hem i inkludim tu wan strong komitmen blong mekem sua se ol rikod blong ol advaes abaot ol risk mo ol komon risk mo eksposa (CRE) oli komplit mo stret. Be, lukaot long temteisen blong kaontem ol CRE olsem wan neketif metrik, from se ol kaen namba olsem oli wan saen tu blong wan helti kod analisis mo testing komuniti.

3 **Bildim okanaeseisenal strakja mo lidaship blong ajivim ol gol ia.**
No mata we ol sabjek mata ekspetis hem i impoten long prodak sikiuriti, ol sinia eksekiutif oli ol praemeri disisen meka blong implementem jenj long wan okanaeseisen. Ol eksikiutif oli nid blong praeoritaesem sikiuriti olsem wan kritikol elemen blong prodak divelopmen akros long okanaeseisen, mo i nid blong patna wetem ol kastoma.



Blong mekem olketa trifala prinsipol ia, ol manufakjera oli shud tingbaot sam opereisenal taktik blong jenjem ol divelopmen proses blong olketa.

Holem ol rutin miting wetem kampani eksekiutif lidaship blong draevem impotens blong sikiua tru long disaen mo sikiua tru long difolt insaed long okanaeseisen. Oli mas establishim ol polisi mo ol prosija blong riwodem ol prodaksen tim we oli stap divelopem ol prodak blong folem ol prinsipol ia, we i save inkludim ol awod blong implementem aotstanding sofwea sikiuriti praktis o ol insentif blong wok lada mo promosen kraeteria.

Opereit raon long impotens blong sofwea sikiuriti long bisnis sakses. Eksampol, tingting blong putum wan "sofwea sikiuriti lida" o wan "sofwea sikiuriti tim" we i holem ol bisnis mo IT praktis blong i joenem ol sikiuriti standed mo manufakjera akaontebiliti. Ol manufakjera oli mas mekem sua se oli kat wan strong, indipenden prodak sikiuriti asesmen mo ol ivalueisen prokram blong ol prodak blong olketa.

Yusum wan stret tret model we oli mekem long taem blong divelopmen blong praeoritaesem ol prodak we oli mos impoten mo oli kat hae impak. Ol tret model oli tingbaot wan speifik yus-keis blong wan prodak mo mekem sua se ol divelopmen tim oli sikiurem ol prodak. Las wan, sinia lidaship i shud holem ol tim oli akaontebol blong dilivarem ol sikiua prodak olsem wan mein elemen blong prodak ekselens mo kwaliti.

Olsem pat blong Oktoba 2023 apdeit long gaedens ia, i kat moa infomeisen abaot ol trifala prinsipol ia tru long olketa ekspleneisen, demonstreisen, mo evidens ia.

PRINSIPOL 1: Tekem Onaship blong ol Kastoma Sikiuriti Aotkam

EKSPLENEISEN

Ol moden bes praktis oli dikteitem se ol sofwea manufakjera oli mas invest long ol prodak sikiuriti efot we i inkludim **aplikeisen hadening, ol fija blong aplikeisen** mo ol aplikeisen **ol difolt seting.**

Ol sofwea manufakjera oli nid blong implimentem **aplikeisen hadening** mo hemia oli mekem taem oli yusum ol proses mo ol teknoloji we i leftemap kost blong wan rabis akata we i wantem kompromaesem ol aplikeisen. Ol aplikeisen hadening protokol mo ol prosija oli help blong resistim ol atak we ol intelijen rabis akta oli mekem. Ol toktok olsem hadening, prodak sikiuriti, mo resiliens oli rilet klosap long prodak kwaliti. Mein samting hem i sikiuriti hem i mas "stap finis insaed olsem wan mein pat blong prodak" mo i "no wan samting blong adem afta." [1] Taem sofwea manufakjera hem i putum sikiuriti finis insaed long prodak, hemia oli no save inkrisim sikiuriti blong ol kastoma blong olketa nomo be oli save inkrisim tu kwaliti blong ol prodak blong olketa. Eksampol blong ol taktik hem i inkludim wok blong mekem sua se ol yusa input oli validet mo sanitaes, mo oli no entarem daerek i ko long kod (hemia i minim se oli yusum ol paramitaraes kwiri), yusum wan memori sef prokraming langwij, strong sofwea divelopmen laef saekol (SDLS) manejmen, mo yusum kriptokrafik ki manejmen we hadwea i bakemap.

Ol aplikeisen oli nid blong sapotem **ol aplikeisen fija** we oli rilet long saebasikiuriti. Samtaem oli singaotem se "ol kapabiliti" ol fija ia oli ekstendem fanksenaliti blong wan prodak o sevis long ol wei we oli help blong mentenem o inkrisim sikiuriti posja blong wan kastoma. Ol eksampol blong ol fija we oli rilet long sikiuriti oli inkludim sapoting transpot leia sikiuriti (TLS) blong evri netwok koneksen, singol saen on (SSO) sapot, malti-fakta otentikeisen (MFO) sapot, sikiuriti ivent odit lokin, rol-bes akses kontrol (RBAK), mo atribiut-bes akses kontrol (ABAK).

Sam long ol prodak fija ia oli save konfikarem olketa blong letem ol kastoma oli intekreitem prodak ia long wei we i moa isi long ol envaeromen o ol wokflo blong olketa we oli stap finis. Ol konfikureisen ia oli minim se ol aplikeisen oli mas kat **ol difolt seting** oli setemap i stap kasem taem we ol kastoma oli konfikarem olketa. Ol difolt seting ia oli nid blong setem olketa long sikiua wei "aotsaed long boks" blong mekem se ol kastoma oli spendem smol namba blong ol risos blong mekem stak blong ol teknoloji prodak blong olketa oli moa sikiua.

Wanwan long ol elemen ia – aplikeisen blong hadening, aplikeisen blong ol sikiuriti fija, mo aplikeisen blong ol difolt seting – hem i plei wan rol long sikiuriti blong aplikeisen, mo sikiuriti stan blong kastoma long en. Ol sofwea manufakjera oli mas tingbaot wanwan long ol elemen ia mo hao oli rilet long wanwan long olketa. Ol manufakjera oli mas tingbaot moa samting mo i no jes ol invesmen blong olketa blong inkoporetem jenj long ril-wol sikiuriti stan blong ol kastoma blong olketa. Ol manufakjera oli mas tekem wan step i ko moa mo tingbaot olsem wanem ol elemen ia oli jenjem ril-wol sikiuriti stan blong ol kastoma blong olketa, nomata se ol risal bambae hem i gud o nogud.

Ol manufakjera oli mas tekem onaship blong ol sikiuriti aotkam blong ol kastoma blong olketa mo no mesarem olketawan fulwan nomo long ol efot mo ol invesmen blong olketa. Risponsibiliti i shud stap long olketa antap, wetem ol manufakjera, long ples we i kat bigfala janis se bae katem daon ol namba blong taem we bae save kat kompromaes.

Be yumi rikret se hemia i no keis tete. Tumas manufakjera oli putum beden blong sikiuriti long kastoma mo oli no inves long komprihensif **aplikeisen hadening.** Eksampol, taem manufakjera hem i pajem wan valnerabiliti, samtaem bae yumi luk ol semak valnerabiliti ia oli kamaot long klia ples from se oli bin adresem simtom mo i no rut kos blong difek ia. Prodak ia maet i implimentem ol difren mitikeisen long ol difdifren pat blong kod beis blong semak klas blong valnerabiliti. Olsem wan keis long poen, afta we manufakjera hem i fiksim wan imput sanitaeseisen valnerabiliti, ol riseja mo ol ataka oli faenem ol kod pat we oli no kasem eni benefit aot long input sanitaeseisen we i impruv ia. Manufakjera hem i aplaem ol fiks wanwan long wan taem be i no se bae yunifaem kodbes blong elimineitem klas blong valnerabiliti ia akros long ful aplikeisen.

Ol aplikeisen fija oli save krietem tuketa ol benefit mo risk blong ol kastoma. Ol fija we oli alaoem ol intekreisen poen wetem fulap ekstenel sistem mo ol vesen oli save inkrisim bigwan valiu blong wan prodak. Mo yes ol sapoting fija we oli nokat wan ritaemen plan, olsem wan netwoking protokol, oli save leko ol kastoma oli valnerabol sipos oli nokat wan andastanding blong ol implikeisen blong ol yus blong fija ia we bae kontinu oltaem. Eksampol, sam prodak ia oli kontinu blong yusum ol netwoking protokol we oli kat ol orijin blong olketa long ol yia long 1990 o 2000 mo naoia ol man oli save se oli nomo sef. I kat plante fakta we oli save sloem spid we ol kastoma oli apgred long hem mo diploem ol moden sikiuriti mesa. Maet oli save yusum ol prodak we oli intekret wetem res blong netwok blong okanaeseisen, be oli nokat ol moden sikiuriti mesa, we oli priventem IT tim blong oli no modenaesem. Yet, ol sofwea manufakjera oli save faktorem ol paten ia i ko insaed long ol planing proses blong olketa blong enkarejem ol kastoma blong stap ap tudeit.

Aplikeisen blong ol difolt seting oli wan eria we oli adem blong potensel risk blong ol kastoma. Ol manufakjera samtaem oli jusum sam kaen difolt seting, we i mekem i moa isi blong ol kastoma oli yusum ol aplikeisen fija we oli wantem. Nogud saed hem i praktis ia i inkrisim atak sefes blong ol kastoma we maet oli nidim sam kaen fija o ol protokol we difolt i enablem olketa. Mo tu, fulap sikiuriti kontrol oli tokel of long difolt o nidim ol kastoma blong tekem taem blong konfikurem ol seting blong olketa blong inkrisim sikiuriti. Eksplisit tret modeling hem i wan taktik we maet i save help blong infomem disisen we ol fija oli shud stap on tru long difolt o wijwan seting nao i nid blong i sikiua tru long difolt. Wan narafala taktik hem i blong investikeitem ol wei blong mekem se administreta hem i save faenem ol fija.

Sam manufakjera oli stap shipim ol prodak we oli kat ol difolt we oli save krietem risk blong sam o evri kastoma blong olketa. Insted blong setem ol difolt we oli moa sef, samtaem oli jus blong produsum wan **hadening gaed** we ol kastoma oli mas implimentem wetem mani blong olketa wan. Ol hadening gaed oli kat sam komon problem. I had blong faenem sam hadening gaed mo oli no sapotem gud olketa. Ol narafala wan oli had blong implimentem, samtaem oli nidim sofwea divelopmen blong raetem wan ekstensen modyul. Be yet, sam narafala wan oli tingting se man we i stap ridim gaed ia hem i kat bigfala saebasikiuriti eksperiens blong andastandem ol wei we ol difdifren seting oli stap jenjem sefes atak. Ol praktisena we oli nokat wan ful andstanding blong ol wei we ol ataka oli wok maet oli feil blong implimentem ol hadening gaed instraksen long stret wei, espeseli sipos ol instraksen ia oli no mekem ol tredof oli klia. Mo tu, i no se evri hadening gaed, ol enjinia we oli save gud abaotem ol ataka taktik mo ikonomiks oli raetem, mekem se i had blong krietem ol hadening gaed we oli no ifektif iven sipos oli implementem long feitful wei. Milien kastoma oli stap tekem risponsibiliti blong hadenem ol maltipol instens blong sofwea o ol sistem, samtaem long ol envaeromen we i nokat inaf risos. Fasin blong dipen long ol hadening gaed hem i no rilaeabol.

Oli mas stap ivalueitem ol seting blong wan aplikeisen oltaem nomata sipos ol seting ia oli difolt wan o kastoma i setemap, akensem andastanding we manufakjera i kat naoia abaot tret landskep. Oli mas mekem ol aplikeisen wetem ol klia indiketa abaot ol potensel risk we maet i save hapen aot long ol seting ia mo oli mas mekem ol man oli save ol indiketa ia. Semak olsem we wan moden trak i kat wan indiketa abaot ol sitbelt mo i ekspresem indiketa ia taem i mekem wan alet i singaot, sipos yu traem blong draev be yu no bakelemap sofwea ia, hem i mas ekspresem ol indiketa abaot stret blong sikiuriti blong wan sistem. Sipos oli konfikarem wan aplikeisen blong hem i no nidim MFP blong ol administreta akaon, hemia i mas mekem ol administreta oli awea oltaem se olekta mo ful okanaeseisen blong olketa oli stap long denja sipos oli no konfikarem MFO. Mo tu, sipos oli konfikarem wan aplikeisen blong sapotem ol protocol we oli moa olfala we naoia oli save se oli implimentem wik kriptokrafi, oli mas mekem i klia oltaem long ol administrea se okanaeseisen ia hem i stap long denja mo provaedem ol risos blong risolvem situeisen. Mifala i askem strong long ol manufakjera blong implimentem ol rutin prod we oli bildim i ko insaed long prodak mo no dipen long ol administreta blong kat taem, ekspetis, mo aweanes blong intepretem ol hadening gaed. Ol opotuniti oli stap long klia we blong inoveisen blong balensem sikiuriti mo ol yusabiliti konsidereisen.

Wanwan long ol elemen antap ia hem i krietem wan situeisen we hem i wik we ol kastoma oli nid blong risejem, fandem, pem, provaedem staf, mo monitarem moa **sikiuriti prodak** blong katem daon janis blong kompromaes. Ol smol mo midiem saes okanaeseisen (ol SMO) long jenerol wei oli no save fasiliteitem ol opsen ia. Oli nokat ekspetis, fanding, mo taem we hem i taksem bandwit mo fanksen, we i fosem sikiuriti i ko long wan praeoriti we i moa lo, mo, long totol, i mekem kolektif risk i ko moa wos. Long narafala saed, sikiuriti invesmen we smol manufakjera nomo oli mekem bambae hem i gud. Wan komon toktok we i samaraesem problem ia hem i se sofwea indastri hem i nidim moa sikiua prodak, i no moa sikiuriti prodak. Ol sofwea manufakjera oli mas lidim transfomeisen ia.

> ***Sofwea indastri hem i nidim moa sikiua prodak, i no moa sikiuriti prodak. Ol sofwea manufakjera oli mas lidim transfomeisen ia.***

Tete, samtaem yumi ridim ol komen we i kamaot long ol manufakjera blong eksplenem se wan kastoma hem i kompromaes from se hem i no eneblem wan kaen sikiuriti fija o folem wan kaen hadening gaedens. Be, afta wan kompromaes, ol manufakjera oli mas eksplenem sipos wan kaen sikiuriti fija o wan kaen hadening gaedens we sipos i bin stap bamabe i priventem kompromaes ia mo tingting blong mekem i wan difolt mo kastoma i no nid blong pem. Long ol keis ia we prodak hemwan hem i no haden inaf long ol disaen mo ol implimenteisen feis, manufakjera i mas eksplenem olsem wanem oli stap wok blong elimineitem klas blong valnerabiliti ia aot long ol prodak laen blong olketa.

Ol sofwea manufakjera oli kat wan risponsibiliti blong mekem sua se oli disaenem mo divelopem ol prodak blong olketa wetem sikiuriti olsem wan top praeoriti. Blong pepes ia, oli shud **mesarem ol risal long objektif wei** blong ol efot blong olketa long fil. Mifala i askem ol manufakjera blong ko jes fokas long ol intenel efot blong olketa, be blong mesarem long objectif wei mo ripotem oltaem ol risal mo ifektifnes blong ol sikiuriti efot mo konfikureisen blong wan prodak, mo blong bildim wan fidbak lup we i krietem ol jenj insaed long SDLS we i lid i ko long ol impruvmen we oli save mesarem insaed long kastoma sefti mo moa sikiua prodak. Ripoting i mas inkludim data we i nokat aedentiti we akademik mo sikiuriti risej komuniti oli save yusum blong trakem ol hae-level trend mo mesarem prokres long ful ikosistem.

DEMONSTREITEM PRINSIPOL IA

Ol Sofwea manufakjera mo ol onlaen sevis oli mas faenem ol wei blong demonstreitem ol sakses taem oli implimentem prinsipol ia. Oli mas traem blong kivim evidens long fom blong ol atifakt blong ol aotsaeda oli eksamaenem. I nokat wan singol atifakt we hemwan bambae i pruvum se wan manufakjera hem i stap implementem wan strong sikiua tru long disaen prokram, be taem oli provaedem ol difdifren atifakt bambae oli bildim wan keis blong komitmen we manufakjera i kat blong divelopem ol sikiua prodak. Aproj ia hem i stap long spirit blong "soem, insted blong talem."

Blong demonstreitem prinsipol ia, ol sofwea manufakjera oli mas tingbaot ol step olsem olketa ia we oli stap long list we i stap andanit ia. Ol ejensi we oli raetem dokumen ia oli luksave se smol sofwea manufakjera bambae oli save implimentem ol praktis ia stretawe mo produsum ol koresponding atifakt long stat blong sikiua tru long disaen wokbaot blong olketa. Mo tu, ol sofwea manufakjera bambae oli nid blong praeoritaesem list ia folem hao ol kastoma oli diploem prodak long fil blong ajivim ol bigfala sikiuriti benefit.

OL PRAKTIS BLONG SIKIUA TRU LONG DIFOLT

1. **Elimineitem ol difolt paswod.** Oli kontinu blong poentem finga long ol difolt paswod olsem kos blong fulap atak evri yia. Taem ol sofwea maneja oli mekem komitmen blong elimineitem siries problem ia bambae hem i dinaem isi akses long ol ataka. Mo tu, ol manufakjera oli mas lukluk long ol wanem paswod praktis we oli mas implimentem, olsem mimimam paswod lengt mo no alaoem ol paswod brij we ol ataka oli save.

2. **Kondaktem ol fil test.** Taem we teknoloji i kontinu blong jenj mo kam moa kompleks, hem i stap kam moa impoten blong ol sofwea manufakjera oli kondaktem sikiuriti-sentrik yusa testing blong andastandem sikiuriti stand blong ol prodak blong olketa long fil. Semak olsem hao ol yusa risej hem i infomem ol rikwaemen blong sofwea divelopmen, ol sofwea manufakjera oli mas kondaktem tu sikiuriti-fokas yusa risej blong andastandem weaples sikiuriti yusa eksperiens (UX) i no kasem yet. Taem oli luk olsem wanem ol kastoma oli diploem mo yusum ol prodak blong olketa long ol ril-wol envaeromen, ol sofwea manufakjera oli save kasem ol impoten insaet abaot usability mo ifektifnes blong ol sikiuriti fija blong olketa mo ol kontrol. Ol insaet ia oli save help blong aedentiafem ol eria blong impruvmen mo rifaenem ol prodak blong olketa blong oli mitim long wei we i moa gud ol sikiuriti nid blong ol kastoma. Eksampol, ol fil test maet oli save sajestem ol jenj long UX flo, ol difolt, aleting, mo monitaring. Ol fil test maet oli soem tu weaples ol pas impruvmen long disaen blong prodak i katem daon velositi blong ol sikiuriti paj, ridiusum ol konfikureisen mistek, mo minimaesem atak sefes.

Ol manufakjera oli mas tingbaot olketa samting ia:

- Ol kastoma oli stap implimentem hadening gaed long stret wei?
- Ol sikiuriti fija blong prodak we i stap naoia oli stap wok olsem we man i ekspektem long fil?
- Ol fija ia oli risistim ol ril-wol atak?
- Wijwan fija bambae oli ridiusum janis blong kompromaes i moa gud?

  Not: Blong kasem moa tingting about ol elemen ia, maet ol sofwea patna bae oli wantem patna wetem ol kastoma blong kondaktem ol red tim eksasaes blong luk olsem wanem prodak hem i risistim ol atak. Maet ol fil test ia oli save tek ples long fisikol ples blong kastoma, onlaen, o tru long telemetri long aplikeisen long wan wei we i proteksem praevesi.

3. **Katem daon hadening gaed saes.** Ol manufakjera oli save impruvum ol standing blong sikiuriti blong ol kastoma sipos oli strimlaen o iven elimineitem ol prodak hadening gaed mo fokas long ol mos kritikol sikiuriti mesa we ol kastoma oli mas praeoritaesem taem oli diploem ol prodak blong olketa. Insted blong kilim ol kastoma wetem wan longfala lis blong ol sikiuriti mesa, i gud blong ol manufakjera oli aedentifaem ol top sikiuriti risk we oli save afektem ol prodak blong olketa mo kivim klia mo stret gaedens abaot hao blong katem daon ol risk ia. Mo tu, i gud blong ol manufakjera oli kivim ol kastoma blong olketa ol tul mo otomeisen we i simplifaem proses blong implimentem ol sikiuriti kontrol, olsem ol script we i isi blong diploem long envaeromen blong olketa. Ol tul ia tu oli mas save verifaem mo soem klia ol jenj we oli mekem long orijinel beislaen. Taem ol manufakjera oli strimlaenem ol hadening gaed mo kivim ol kastoma ol tul we oli isi blong yusum mo otomeisen, ol manufakjera oli save katem daon beden long ol kastoma blong olketa mo help blong mekem sua se ol prodak blong olketa oli diploem long wan sikiua wei. Wan taktik hem i blong tingting blong implimentem Pareto prinsipol blong katem daon namba blong ol step blong ol komon yus keis (80%), mo afta kivim gaedens blong konteks mo tuling blong ol sinario we oli no komon tumas (20%). Long wei ia, ol sofwea manufakjera

bambae oli mekem ol simpol samting oli simpol, mo ol had samting oli posibol. Fil testing bambae hem i wan paoaful tul blong mesarem hao long hem i tekem ol kastoma blong diskaverem, andastandem, mo implimentem ol hadening gaed. I gud blong ol manufakjera oli tingbaot olsem wanem prodak i save stikim ol administreita blong tekem aksen insaed long prodak hemwan mo no dipen long olketa blong implimentem ol wok aot long wan hadening gaed.

4. **Diskarejem long wan aktif wei yus blong ol lekasi fija we oli no sef.** Praeoritaesem sikiuriti tru long ol klia apgred rod ova long bakwod kompatibiliti. Pablishim ol blok post we oli soem adopsen blong ol fija we oli moa sef mo ol protokol, mo kritisaesem ol fija we oli no sef tru long anaonsmen, maet stat long insaed blong prodak hemwan. Wan bigfala namba blong ol kastoma oli demonstreitem se bambae oli no kipim ol sistem blong olketa i stap wetem moden netwok, aedentiti, mo ol narafala sikiuriti fija. Long sam keis, ol kastoma oli fraet long fanksenaliti we oli stap naoia se bae i brok wetem wan apgred. Taem manufakjera i mekem ol apgred oli simpol olsem we i posibol, bambae i kat janis se ol kastoma bambae oli apgredem mo mekem ol sikiuriti fiks plante taem mo moa kwik. Ol sofwea manufakjera oli mas stikim strong ol kastoma blong folem ol apgred rod we oli ridiusum kastoma risk.

5. **Implimentem ol alet we oli pulum atensen.** Semak long ol sitbelt woning saon long ol trak we oli kontinu blong mekem nois taem pasenja i no fasem sitbelt, i gud blong ol manufakjera oli implimentem ol laet we oli on long stret taem mo we oli ripit taem we ol yusa o ol admin oli stap long ol steit we oli rili no sef, blong wonem ol administreta se oli stap yusum ol protokol we oli no apruvum long ol envaeromen blong olketa mo sajestem ol apgred rod. Implimentem ol alet we oli on long stret taem mo oli ripit taem we ol yusa o ol admin, o aplikeisen konfikureisen, oli stap long wan steit we i no sef. Mekem mod blong no stap sef i klia long ol administreita long wan rekula besis. Wan narafala fija i save nidim wan supa administreita blong aknolejem se MFO long akaon blong olketa evri taem hem i lokin, o iven disebelem sam mein fija kasem taem we oli enebelem MFO. I kat speis blong inoveit blong ajivim ol gol ia mo long semak taem no mekem ol alet we man bae i les blong harem.

6. **Krietem ol sikiua konfikureisen templet.** Ol templet ia oli save prisetem sam kondisen i ko long ol seting we oli sef long wan risk apetaet blong wan okanaeseisen. Maet bae hem i ova simpol blong kat ol/lo/midiem/hae sikiuriti templet, be eksampol ia hem i soem olsem wanem plante seting oli save apdeitem blong manejem risk blong okanaeseisen. Ol hadening gaed oli save sapotem ol templet long saed blong ol risk we manufakjera i bin aedentifaem.

OL SIKIUA PRODAK DIVELOPMEN PRAKTIS

1. **Dokumentem konfomens long wan sikiua SDLS fremwok.** Ol sikiua SDLS fremwok oli kivim ol objektif mo ol eksampol long ol man, ol proses, mo ol teknoloji. Tingting blong pablishim wan ditel diskripsen abaot wijwan sikiua SDLS fremwok kontrol oli bin implimentem finis mo diskraebem eni narafala kontrol we oli bin yusum finis. Insaed long US, tingting blong yusum NIST Sikiua Sofwea Divelopmen Fremwok (SSDF). Nomata we hem i no wan jeklis, SSDF "i diskraebem wan set blong fandamentel, saon praktis blong sikiuriti sofwea divelopmen."

2. **Dokumentem ol Saebasikiuriti Pefomens Gol (CPG) o ekwivalen konfomens.** Taem wan okanaeseisen hem i konfemem se oli konfom long NIST SSDF standed, oli stap talem se SDLS blong olketa hem i infom tru long ol bes praktis we oli andastandem gud. Be, hem i no inaf se oli kat wan strong SDLS nomo. Olketa tu oli nid blong protektem entapraes blong olketa wan mo ol divelopmen envaeromen akensen ol rabis akta we bae oli lukaot blong manipuleitem ol sikiuriti propeti blong prodak ia taem we oli stap divelopem yet. Hemia hem i no wan klas blong atak we i hapen long tingting blong man nomo, be hem i wan we oli bin mekem finis mo i kat rabis ifek long ol kastoma, mo i eksten tu i ko long nasonal sikiuriti. Ol okanaeseisen oli mas tingting blong pablishim ol ditel abaot konfomens blong okanaeseisen long ol CISA CPG, NIST Saebasikiuriti Fremwok (SCF), o ol narafala saebasikiuriti prokram fremwok.

3. **Valnerabiliti manejmen.** Sam manufakjera oli kat wan valnerebol manejmen prokram we i fokas blong pajem ol valnerabiliti insaed mo aotsaed, mo smol moa. Ol prokram we oli moa majua oli inkoporetem ekstensif analisis we data i draevem abaot ol valerabiliti mo ol rut kos blong olketa, tekem ol step blong elimineitem long wan sistematik wei ful klas blong valnerabiliti[3]. Oli implimentem ol fomol prokram raon long seting kwaliti planing, kwaliti kontrol, kwaliti impruvmen, mo kwaliti mesamen. Oli lukluk difekt manejmen olsem wan bisnis isiu, i no jes wan sikiuriti isiu. Ol prokram ia oli no difren long sam wei long kwaliti mo sefti prokram long ol narafala indastri.

4. **Yusum open sos sofwea long wan risponsibol wei.** Taem wan i yusum wan open sos sofwea, hem i mas akt risponsibol mo vetem ol open sos pakej, fostarem ol kod kontribusen i ko bak long ol dipendensi mo help sastenem divelopmen mo mentenens blong ol kritikol komponen. Blong refrens, Ministri blong Ekonomi, Tred, mo Indastri (METI) blong Japan hem i pablishim " Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security."

5. **Provaedem ol sikiua difolt blong ol divelopa.** Mekem difolt rut long sofwea divelopmen i sikiua taem man i provaedem ol sef bilding blok blong ol divelopa. Eksampol, from se SQL injeksen valnerabiliti i fulap we i mekem ril-wol damej, mekem sua se ol divelopa oli yusum wan laebri we oli mentenem gud blong proventem klas blong valnerabiliti. Oli save olketa tu olsem ol "rod we oli pevem" o "ol rod we oli kat gud laet," praktis ia i mekem sua se spid mo sikiuriti tuketa i kat, mo i katem daon mistek blong human.

6. **Fostarem wan sofwea divelopmen wokfos we i andastandem sikiuriti.** Mekem sua se ol sofwea divelopa blong yu oli andastandem sikiuriti tru long trening we yu kivim long olketa abaot ol bes praktis blong sikiurem koding. Mo tu, help blong jenjem bigfala wokfos taem yu apdeitem ol praktis blong haerem man blong ivaluetem sikiuriti nolej mo wok wetem ol yunivesiti, ol komuniti kolej, ol butkam, mo ol eduketa blong wivim sikiuriti i ko insaed long komputa saens mo ol sofwea divelopmen kerikulum.

[3] NIST SSDF, PO 1.2, Eksampol 2: "Difaenem ol polisi we oli spesifaem ol sikiuriti rikwaemen blong sofwea blong okanaeseisen, mo verifaem komplaeans long ol ki poen insaed long SDLS (eksampol, ol klas blong ol sofwea wiknes we ol geit oli verifaem, ol ansa long ol valnerabiliti we oli diskaverem long sofwea we i rilis)."

7. **Test sikiuriti insiden ivent manejmen (SIEM) mo sikiuriti okestreisen, otomeisen, mo rispons (SOAR) intekreisen.** Anda long wok blong kondaktem ol fil tes, wok tuketa wetem popula SIIM mo ol SOAR provaeda wetem ol kastoma we yu selektem blong andastanem olsem wanem ol rispons tim oli yusum ol lok blong investikeitem ol sikiuriti insiden we oli saspektem o we oli ril. Smol sofwea divelopa oli kat eksperiens we oli ansa long wan insiden mo oli save krietem ol lok entri we oli no helpem ol risponda semak olsem we oli ekspektem. Taem divelopmen tim i wok tuketa wetem ol SIIM mo SOAR teknoloji mo ol ril insiden rispons profesenal, tim i save krietem ol lok we oli talem korek mo ful stori, sevem taem mo katem daon daot long wan insiden.

8. **Alaen wetem Zero Trust Architecture (ZTA).** Alaenem ol prodak diploemen gaed wetem mifala, eksampol, ol NIST ZTA model mo CISA Zero Trust Maturity Model. Enkarejem ol kastoma blong inkoporetem ol prinsipol ia insaed long ol envaeromen blong olketa.

OL PRO-SIKIURITI BISNIS PRAKTIS

1. **Povaedem lokin we i no nidim ekstra fi.** Ol klaod sevis oli mas komit blong jenereitem mo storem ol lok we oli rilet long sikiuriti we i no nidim ekstа fri. Ol prodak we oli hostem on-saet oli mas mekem semak samting blong jenereitem ol lok we oli rilet long sikiuriti we i no nidim ekstra fi. Mo tu, i gud blong prodak i lokem ol sikiuriti iven tru long difolt from se fulap kastoma maet oli no andastandem valiu blong olketa kasem afta we wan insiden i hapen. Maet ol taktik ia oli nidim wan gudfala riviu abaot ol wanem sikiuriti iven we i gud blong oli lokem blong kivim saebasikiuriti steit aweanes, olsem wanem wan kastoma i save konfikarem loking, blong wanem taem piried ol lok ia oli holem i stap, olsem wanem oli protektem lok intekriti mo storej, mo olsem wanem ol lok ia oli save analaesem olketa. Long sam keis, riviu ia maet bae i sajestem nid blong oli rifaktarem akitekja blong aplikeisen lok manejmen blong help mekem se oli wok mo long wan kost we manufakjera i save pem. Taem man i wok wetem ol insiden rispons (IR) ekspet hemia i save inkrisim ol janis se ol lok ia bambae oli yusful long ol investiketa long fil. Lukluk seksen blong ol SIIM.

2. **Elimineitem ol taks we oli haed.** Pablishim wan komitmen blong neva jajem ol sikiuriti o praevesi fija o ol intekreisen. Eksampol, insaed long bigfala eria blong aedentiti mo akses manejmen (AAM), i kat ol sevis we oli singaotem ol singol saen-on (SSO) sevis. Sam manufakjera oli jajem moa blong konektem sistem blong olketa i ko long wan SSO sevis (samtaem oli rifea long hem olsem wan aedentiti provaeda). “SSO taks” ia hem i minim se fulap SMO oli no save kasem gudfala aentiti mo akses manejmen, mekem se i stopem olketa blong oli no kasem wan strong sikiuriti stand. Sam sevis oli jajem moa blong eneblem MFO blong ol yusa. **Oli no mas jajem sikiuriti olsem wan laskeri gud be oli mas tekem olsem wan kastoma raet.** Sam manufakjera oli komplen se smol kastoma oli askem ol fija ia, mo oli kostem moa blong menetenem. Ol komplen ia oli iknorem fakt ia se smol kastoma bambae oli kol blong komplen o baken, i no evri kastoma oli rili andastandem wanem hem i ol benefit blong ol fija ia, mo se evri fija oli kost wan samting blong mentenem. Yet yumi no luk plante manufakjera oli jajem ekstra blong avelebiliti o data intekriti. Ol kost ia oli sapotem ol ki atribyut ia we oli bildim i ko insaed long praes we evri kastoma oli pem, semak olsem ol kost blong inkludim ol sitbelt, ol kolapsibol stiaring kolom, mo ol eabak we oli sevem ol laef long ol aksiden.

3. **Embreisem ol open standed.** Implimentem ol open standed, espeseli araon long komon netwok mo ol aedentiti protokol. Avoedem ol propaetari protocol taem we ol open standed oli avelebol.

4. **Provaedem apgred tuling.** Fulap kastoma oli no wiling blong adoptem letes vesen blong prodak, inkludim wok blong instolem ol fija we oli moa niu mo sikiua olsem ol sikiua netwok koneksen. Ol sofwea manufakjera oli save inkrisim kastoma adopsen blong ol niu apgred taem oli provaedem ol tuling blong help katem daon daot mo risk. Ofarem ol fri laesens blong ol kastoma blong testem ol apgred mo ol paj long wan test envaeromen olsem wan wei blong motiveitem ol kastoma.

PRINSIPOL 2: Embreisem Radikol Transparensi mo Akaontebiliti

EKSPLENEISEN

Ol sofwea manufakjera oli mas tekem praed long olketawan blong dilivarem ol prodak we oli sef mo sikiua, mo tu blong difrensieitem olketawan long ol narafala memba blong manufakjera komunitu folem abiliti blong olketa blong mekem hemia.

Yumi adresem wan komon konsen abaot transparensi. Taem we ol praktisena oli diskasem radikol transparensi, i kat wan tendensi blong konveseisen i ko fasfas long wan konsen se oli stap provaedem wan “rodmap blong ol ataka”. Be, bigfala evidens hem i se ol ataka oli stap mekem gudfala wok nomo nomata we i nokat ol rodmap ia, mo ol kaen konsen olsem oli mas tekem wan bak sit long transparensi we i benefitim ol daerek kastoma, ol indaerek kastoma, ol saplae jen, mo ful sofwea indastri.

Transparensi hem i helpem indastri blong establishim ol konvensen—long narafala toktok, “gud” i luk olsem wanem. Hem i helpem ol konvensen ia oli jenj ova long taem blong ansa long ol kastoma nid, ol jenj long ol tret akta taktik o ikonomi, o teknoloji evolusen. Transparensi hem i helpem ol manufakjera wetem ol risos we oli smol moa blong lan long olketa we oli moa majua mo olketa we oli kat ol risos we oli moa kapebol. Ol storian abaot wok blong sherem infomeisen hem i gud blong ekspan i ko biyon ol ril-taem tret indiketa, blong inkludim ol elemen andanit ia.

Transparensi i fosem ol disisen raon long sikiuriti blong oli mekem eli long divelopmen proses, mo blong oli wan aktiviti blong ol bisnis lida we i kontinu mo tu ol

enjinia mo ol sikiuriti profesenal. Transparensi hem i bildim akaontebiliti i ko insaed long wan prodak.

Wan not long jois blong adjektif ia “radikol” long fored blong “transparensi”. Tete, hem i no komon blong ol sofwea manufakjera oli pablishim ful infomeisen abaot hao oli divelopem mo mentenem sofwea mo hao oli majurem ol prokram blong olketa tru long data ova long taem. Long sofwea indastri, smol manufakjera oli ofarem ol tua we oli gaed i eksplenem olsem wanem oli disaenem sofwea blong olketa. I kat smol opotuniti blong ol sofwea manufakjera oli luk olsem wanem ol pia okanaeseisen oli strakjarem ol SDLC prokram blong olketa, mo olsem wanem ol prokram ia oli holdap long ol kastoma envaeromen akensem ol ril ataka. Kolektif indastri bambae i benefit moa aot long wok blong sherem infomeisen abaot ol topic olsem ol strateji blong mesarem ol sikiuriti kost difek mo blong elimineitem ol klas blong valnerabiliti. Olsem wan risal blong ol komon praktis ia, evri sofwea manufakjera oli mas lanem olsem wanem blong dil wetem prodak sikiuriti olketa wan. Maet bae i no tru long wok blong jajem wan lakseri taks long ol sikiuriti fija, i mekem se sefti mo sikiuriti hem i kam wan kost senta be i no wan profit senta, mo ol kampani bambae oli benefit tru kolaboreisen mo transparensi we bae i mekem lod i laet.

Mifala i wantem fokas long ol taktik we bambae oli spidim bigwan evolusen blong sofwea indastri. Yumi nomo save afodem blong mekem ol opotunistik, inkrimental impruvmen. Sipos yumi olsem wan krup yumi ovakamem ol tret we ol intelijen mo ol adaptif enemi oli mekem, yumi mas embreisem ol level blong transparensi we bambae i no fil kamfotebol tete, be bae i draevem indastri i ko fowod. I kat ol manufakjera tete we bambae oli embodiem sam long ol sikiua tru long disaen prinsipol. Olsem William Gibson i talem, “fiuja i stap ia finis, be hem i distribut long wan iven wei.” **Radikol transparensi bambae i help blong distributum infomeisen ia mo benefitim ol difenda moa bitim ol adveseri blong yumi.**

Transparensi i save mekem moa blong helpem ol pia okanaeseisen oli majurem ol SDLC blong olketa. Ol prospektif kastoma mo ol investa oli save lan moa abaot ol investmen mo ol tredof we ol manufakjera oli mekem, mo sikiuriti stand we ol invesmen ia oli krietem blong ol kastoma. Ol manufakjera we oli embreisem radikol transparensi bambae oli kivim ol kastoma infomeisen blong helpem olketa mekem ol disisen blong pem samting i no folem nomo praes mo ol fija, be folem sikiuriti tu.

Nomata we ol okanaeseisen oli wok had blong sikiurem saplae jen mo SDLC blong olketa, ol kampani oli bin kat ol bild proses blong olketa i kompromaes i no long taem i pas. Wok blong embreisem radikol transparensi i shud lid i ko long pablik disklosa blong atak mo tu blong ol impruvmen we kampani i bin mekem blong priventem mo ditektem ol fiuja atak. Kaen wok blong sherem infomeisen ia bambae i helpem ol narafala okanaeseisen oli lan mo no nid blong ko tru semak problem.

DEMONSTREITEM PRINSIPOL IA

Blong demonstreitem prinsipol ia, ol sofwea manufakjera oli shud tekem olketa step ia:

OL SIKIUA TRU LONG DIFOLT PRAKTIS

1. **Pablishim ol akreket sikiuriti releven statistik mo ol tren.** Ol eksampol topik oli inkludim ol kastoma mo ol administreta oli adoptem MFO mo yusum ol lekasi protokol we oli no sef.
2. **Pablishim ol pajing statistik.** Ditelem wanem pesen blong ol kastoma oli stap long letes vesen blong prodak, mo wanem yu stap mekem blong mekem se ol apdeit oli moa isi mo moa rilaeabol.
3. **Pablishim data abaot ol privilej we oli no yusum.** Pablishim ful infomeisen abaot ol eksesif pemisen long evri kastoma mo tu ol prod mo ol narafala jenj long prodak we yu stap mekem blong ridiusum ol atak sefes blong ol kastoma. Ol privilej we oli no yusum oli posibol se oli ol gudfala kandidet blong ol administreta alet, olsem ol sitbelt saon.

OL SIKIUA PRODAK DIVELOPMEN PRAKTIS

1. **Establishim ol intenal sikiuriti kontrol.** Fulap kampani oli bin luk ol benefit blong muvum data blong olketa i ko long ol klaod provaeda. Naoia ol klaod provaeda ia oli kam taket blong ol ataka. Ol Sofwea olsem wan Sevis (SoaS) provaeda oli mas pablishim ol statistic blong ol intenal kontrol blong olketa. Eksampol, ol SoaS provaeda oli mas pablishim ol statistic abaot intenal diploemen blong olketa blong fishing-resisten MFO, olsem Fas Aedentiti Onlaen (FADO) otentikeisen. Bae hem i gud sipos oli save talem se i nokat stap i save aksesem kastoma o narafala sensitif data sipos hem i no otentikeitem tru long fishing-resisten MFO.

2. **Pablishim ol hae-level tret model.** Sikiurem tru long ol disaen prodak oli stat wetem ol tret model we oli raetem we i diskraebem wanem we ol krieta oli stap traem blong protektem mo long hu. Ol ifektif tret model oli kasem infomeisen taem we ol intrusen oli hapen we oli no kasem olketa yet, mo oli shud kavremap tuketa ol entapraes mo ol divelopmen envaeromen, mo tu wei we ol sofwea manufakjera oli wantem se bae oli yusum long ol kastoma envaeromen.

3. **Pablishim ful infomeisen abaot ol sikiua SDLC self-atesteisen.** Ol manufakjera we oli stap folem NIST SSDF, o ol narafala fremwok we oli semak, oli stap wok long wan aktif wei tuwod wan majua sofwea divelopmen laefsaekol. Taem man i pablishim wan self-atesteisen abaot wijwan kontrol we ol manufakjera oli enaktem, mo blong ol wijwan prodak, hemia bae i demonstreitem wan komitmen blong folem ol bes praktis ia mo provaedem wan inkris level blong konfidens long ol kastoma blong olketa. Ol narafala setifikeisen skim oli inkludim Israel Cyber Supply Chain Methodology, olsem eksampol.

4. **Embreisem valnerabiliti transparensi.** Pablishim wan komitmen we bambae i mekem sua se ol prodak valnerabiliti we oli aedentifaem bambae oli pablishim olsem ol CVE entri we oli stret mo komplit. Hemia hem i espeseli tru blong Komon wiknes enumereisen fil we i aedentifaem rut kos blong ol valnerabiliti. Taem CVE databes hem i holem korek mo komplit infomeisen, indastri hem i kat moa janis blong trakem olsem wanem ol prodak oli stap kam moa sikiua, mo wanem klas blong ol valnerabiliti oli privalen. Be lukaot long temteisen blong kaontem ol CVE olsem wan neketif metric, from se ol kaen namba olsem tu oli wan saen blong wan helti kod analisis mo testing komuniti. Taem ol manufakjera oli implimentem wan sikiua tru long disaen filosofi, hem i posibol se festaem ro CVE kaont blong olketa bambae i ko antap from diskaveri i moa komprihensif mo remedieisen blong ol valnerabiliti long kod we i stap. Ol manufakjera oli mas pablishim analisis blong ol pas valnerabiliti, inkludim eni paten mo mesa we oli bin tekem blong adresem ful klas blong ol valnerabiliti. Eksampol, sipos wan bigfala pesentej blong ol CVE blong wan kampani oli rilet long kros-saeting script (XSS), wok blong dokumentem rut kos analisis, rispons (olsem muv i ko long ol web templet fremwok we i priventem XSS), mo ol risal bambae i siknal long kastoma se bambae oli no kam victim blong wan klas blong valnerabiliti we ol mitikeisen blong hem oli bin andastandem ova ten yia i pas finis.

5. **Pablishim ol Sofwea Bil blong Material (Ol SBBM).** Ol manufakjera oli mas kat wan koman blong ol saplae jen blong olketa. Ol okanaeseisen oli mas bildimap mo mentenem ol SBbM [2] blong wanwan prodak, rikwestem data long ol saplaea blong olketa, mo mekem ol SBbM oli avelebol blong ol daonstrim kastoma mo ol yusa. Hemia bambae i helpem blong demonstreitem dilijens blong olketa blong andastandem ol komponen we oli yusum long krieisen blong ol prodak blong olketa, abiliti blong olketa blong rispon long ol niu risk we oli aedentifaem, mo i save helpem ol kastoma blong andastandem olsem wanem blong respond sipos wan long ol modyul long saplae jen i kat wan niu valnerabiliti we oli jes faenem.

Blong referens, Japan's Ministry of Economy, Trade, and Industry (METI) i bin pablishim "Guide of Introduction of Software Bill of Materials (SBOM) for Software Management." Transparensi i shud ekstend i ko long femwea long ol divaes we oli embed finis mo data mo ol model we oli yusum long AI/mashin lening (ML). Biyon wok blong help long ol pejesing disisen mo ol opereisenal kapabiliti, ol SBbM oli ple wan impoten rol long infrasktrakja blong ditektem mo rispon long ol rabis saplae jen atak.

6. **Pablishim wan valnerabiliti disklosa polisi.** Pablishim wan valnerabiliti disklosa polisi we (1) i otoraesem testing akensem evri prodak we manufakjera i ofarem mo ol kondisen blong ol test ia, (2) provaedem likol sef haba blong ol aksen we oli mekem i konsisten wetem polisi, mo (3) alaoem pablik disklosa blong ol valnerabiliti afta wan set taemlaen. Ol manufakjera oli mas mekem rut-kos analisis blong wan valerabiliti we oli diskaverem mo, kasem poen we oli save, tekem ol aksen blong elimineitem evri valnerabiliti klas. Lukluk Vulnerability Disclosure Policy Template blong CISA blong referens langwij.

OL PRO-SIKIURITI BISNIS PRAKTIS

1. **Nemem long pablik wan sikiua tru long disaen sinia eksekiutif sponsa.** Long fulap okanaeseisen, sikiuriti (olsem kwaliti) oli deleketem i ko long ol teknikel tim we oli kat abiliti blong mekem ol strakjeral jenj blong impruvum bigwan sikiuriti blong ol prodak. Taem oli nemem long pablik wan top bisnis eksekiutif blong lukluk ova long sikiua tru long disaen prokram, hemia bae i transfomem sikiuriti blong ol prodak i ko insaed long wan top-level bisnis konsen.

2. **Pablishim wan sikiua tru long disaen rodmap.** Ol manufakjera oli mas dokumentem ol jenj we oli mekem long ol SDLC blong impruvum kastoma sikiuriti, inkludim ol ditel abaot ol fil-test ripot, ol aksen we oli tekem blong elimineitem ful klas blong valnerabiliti, mo ol narafala aetem we oli listim insaed long ol narafala prinsipol. Semak olsem long keis blong kwaliti impruvmen efot, ol sikiuriti impruvmen prokram oli kat ol klia stej blong planing, kontrol, mo impruvmen. Long spirit blong soem insted blong talem, taem man i pablishim rodmap mo ol ditel bihaen long ol stej ia hemia bae i bildimap konfidens se ol prodak ia oli sikiua tru long disaen. Afta we manufakjera i ajivim prokres we i kat mining, oli save ditelem olketa long ol transparensi ripot. Taem manufakjera i mekem hemia hem i no soem nomo komitmen blong sikiua tru long disaen be i save inspaerem ol narafala wan blong adoptem ol semak kaen prokram from hem i soem wan eksistens pruf.

3. **Pablishim wan memori-sefti rodmap.** Ol manufakjera oli save tekem ol step blong elimineitem wan long ol bigfala klas blong valnerabiliti taem oli maekretem ol prodak we oli stap mo bildim ol niu prodak tru long ol memori sef langwij. Maet hemia bae i no posibol long evri keis, ol manufakjera oli save konsidarem blong divelopem ol aplikeisen rapa long ol memori sef langwij insted blong oli raetemaot evri aplikeisen bakegen. Hemia i save inkludim olsem wanem ol manufakjera oli stap apdeitem haering, trening, kod riviu, mo ol narafala intenal proses, mo tu ol wei we oli stap helpem open sos komuniti blong mekem semak samting.

4. **Pablishim ol risal.** Taem oli stap apdeitem SDLC blong olketa blong i ripresentem sikiua tru long disaen filosofi, ol okanaeseisen bambae oli faenem ol kwik win, moa risos intensif win, mo sam setbak we oli no ekspektem. Taem okanaeseisen i presentem ol intenal sakses mo ol rodblok blong olketa, ful indastri bambae i save lan long ol risal.

PRINSIPOL 3: Lid stat long Top

EKSPLENEISEN

Nomata we ovarol filosofi oli singotem se "sikiua tru long disaen," ol insentif blong kastoma sefti oli stat long taem bifo stej blong prodak disaen. Oli stat wetem ol bisnis gol mo ol implisit mo eksplisit obejktif mo ol aotkam we oli disaerem. Taem nomo we ol sinia lida oli mekem sikiuriti wan bisnis praeoriti, taem oli krietem ol intenal insentif, mo fostarem wan kalja we i aplae long evriwan blong mekem sikiuriti wan disaen rikwaemen, bambae oli ajivim ol bes risal.

Nomata we teknikel sabjek mata ekspetis hem i impoten long prodak sikiutiti, hem i no wan mata we oli save leko fulwan long teknikel staf. Hem i wan bisnis praeoriti we i mas stat long top.

Sam man oli bin tingting sipos wan sofwea manufakjera hem i embreisem tufala fes prinsipol mo produsum ol miningful atifakt, namba tri prinsipol i neseseri? Olsem wanem wan kampani i establishim visen blong hem, misen, ol valiu, mo kalja bambae i afektem prodak, mo olketa elemen ia oli kat wan hevi komponen long top. Yumi luk hemia long ol narafala indastri we oli bin mekem ol bigbigfala impruvmen long sefti mo kwaliti. Kwaliti ekspet J.M. Juran we i wan profesenal hem i bin raetem:

> ***Blong kasem kwaliti lidaship hem i nidim ol top maneja blong pesenali tek jaj blong manejem kwaliti. Long ol kampani we oli bin kasem kwaliti lidaship, ol top maneja oli bin pesenali gaedem inisietif ia. Mi bin no bin awea abaot eni eksepsen. [3]***

Yumi biliv se sikiuriti hem i wan sab-katikori blong prodak kwaliti. Taem we sikiuriti mo kwaliti hem i kam ol bisnis imperatif mo i no ol teknikel fanksen we oli leko fulwan long teknikel staf, ol okanaeseisen bambae oli save ansa long ol sikiuriti nid blong ol kastoma blong olketa moa kwik mo moa ifisien. Andap long hemia, taem ol okanaeseisen oli investem ol neseseri risos blong mekem sua se sofwea sikiuriti hem i mein bisnis praeoriti stat long bikining, hemia bambae i katem daon ol long-tem kost blong adresem ol sofwea difek-mo hemia bae i mekem se bae i lowarem ol nasonal risk.

Long semak wei we ol lidaship tim oli bin implimentem ol koporet sosol risponsibiliti (KSR) prokram, i kat wan aweanes we i stap kro se ol koporet bod, inkludim olketa blong ol sofwea manufakjera, oli shud tekem wan moa aktif rol blong gaedem ol saebasikiuriti prokram. Toktok ia koporet saeba risponsibiliti (KSR) samtaem oli yusum blong diskraebem tingting ia we i jes kamaot.

DEMONSTREITEM PRINSIPOL IA

Blong demonstreitem prinsipol ia, ol sofwea manufakjera oli mas tekem ol step blong inkludim olketa samting ia:

1. **Inkludim ol ditel blong wan sikiua tru long disaen prokram long ol koporet faenansol ripot.** Sipos manufakjera hem i wan pablik tred kampani, adem wan seksen long wanwan anuel ripot i ko long topik blong ol efot blong sikiua tru long disaen. Hem i komon blong ol otomobil anual faenansol ripot blong inkludim ol seksen abaot draeva mo pasenja sefti, inkludim infomeisen abaot ol sentralaes mo kwaliti mo sefti komiti we i distribut. Taem okanaeseisen i ditelem sikiua tru long disaen prokram long wan faenansol ripot, hemia bambae i demonstreitem se okanaeseisen hem i linkim kastoma sikiuriti mo ol koporet faenansol aotkam mo i no jes adoptem nomo wan toktok long ol maketing materiel from se hem i popula.

2. **Provaedem ol rekula ripot i ko long ol bod blong daerekta blong yu.** Nomoli ol Jif infomeisen sikiuriti ofisa (JISO) ripot we oli mekem i ko long ol koporet bod, oli inkludim infomeisen abaot ol karen mo ol plan sikiuriti prokram, ol tret, ol sikiuriti insiden we oli saspektem mo we oli konfemem, mo ol narafala apdeit we oli bes long sikiuriti stand mo helt blong kampani. Andap long wok blong risivim infomeisen abaot sikiuriti stand blong entapraes, ol bos oli mas rikwestem infomeisen abaot prodak sikiuriti mo ifek we i kat long kastoma sikiuriti. Ol bos oli no mas lukluk fulwan nomo long JISO, be oli mas lukluk bigwan long ol narafala memba blong kampani manejmen blong draevem kastoma risk i ko daon.

3. **Empaoarem sikiua tru long disaen eksekiutif.** I kat wan bigfala difrens bitwin wan okanaeseisen we ol teknikel tim oli kat “eksekiutif bae-in,” mo olketa we ol bisnis lida oli pesenali manejem kastoma sikiuriti impruvmen proses mo oli yusum ol standed bisnis proses. Toktok ia “eksekiutif bae-in” hem i minim se wan man i mas salem tingting blong wan kastoma sefti prokram be i no se hem i wan top-level bisnis gol. Eksekiutif i mas kasem paoa blong influensem ol prodak investmen blong ajivim ol kastoma sikiuriti aotkam.

4. **Krietem ol miningful intenal insentif.** Wael yu tingbaot blo no krietem ol rabis insentif, alaenem ol riwod sistem blong impruvum kastoma sikiuriti blong majem ol narafala biheivia mo aotkam we oli kat valiu. Stat long sikiua tru long disaen eksekiutif kasem prodak manejmen, sofwea divelopmen, sapot, ol sel, likol, mo ol narafala okanaeseisen, wivim ol kastoma sikiuriti insentif i ko long wok blong haea, ol promosen, ol salari, ol bonas, ol stok opsen, mo ol narafala komon proses long raning blong bisnis. Eksampol, taem we oli establishim kraeteria blong promotem ol sofwea divelopa, inkludim ol konsidereisen blong impruvum sikiuriti blong prodak wetem narafala kraeteria olsem aptaem, pefomens, mo ol fija impruvmen.

5. **Krietem wan sikiua tru long disaen kaonsel.** Long sam indastri, hem i komon blong ol okanaeseisen oli krietem wan sentrol kwaliti kaonsel, mo blong embedem ol kwaliti ripresentetif insaed long ol mein divisen o bisnis yunit. Taem okanaeseisen i inkludim tuketa ol sentralaes mo distribut memba, ol krup ia oli wok blong impruvum kwaliti akensem ol top level gol be lo sem taem oli risivim telemetri we i kamaot dip insaed long okanaeseisen. Mo tu, wan sikiua tru long disaen kaonsel bambae i impruvum sikiuriti akensem ol sikiua tru long disaen gol truaot long okanaeseisen.

6. **Krietem mo ivolvem ol kastoma kaonsel.** Fulap sofwea manufakjera oli kat ol kastoma kaonsel we ol kastoma blong ol difdifren rijin, indastri, mo ol saes oli mekemap. Ol kaonsel ia oli save provaedem wan bigfala infomeisen abaot ol kastoma sakses mo ol jalenj taem oli diploem ol prodak blong kampani. Strakjarem kaonsel ajenda wetem ol topik we i fokas blong adresem kastoma sefti, iven sipos hem i no stap long top blong maen naoia blong ol patisipen. Konsidarem weaples kastoma kaonsel i stap ripot i ko long hem mo olsem wanem blong askem ol patisipen blong ol insaet abaot sikiuriti blong prodak olsem we oli diploem. Eksampol, kaonsel i kat wan baeas tuwod maketing mo ol sel pepes, o prodak manejmen? Sikiua tru long disaen eksekiutif i mas help blong stiarem ol kastoma inta aksem ia mo i shud linkim olketa wetem ol narafala elemen insaed long pepa ia, olsem ol fil stadi.

OL SIKIUA TRU LONG DISAEN TAKTIK

Sikiua Sofwea Divelopmen Fremwok (SSDF), we narafala nem blong hem hem i Nasonal Instiut blong ol Standed mo Teknoloji (NIST) SP 800-218, hem i wan mein set blong hae-level sikiua divelopmen sofwea praktis we oli save intekretem i ko insaed long wanwan stej blong sofwea divelopmen laefsaekol (SDLC). Taem okanaeseisen i folem ol praktis ia hem i save helpem ol sofwea produsa blong oli mo ifektif blong faenem mo karemaot ol valerabiliti long sofwea we oli rilisim, mitikeitem potensel impak blong eksploetem ol valnerabiliti, mo adresem ol rut kos blong ol valnerabiliti blong priventem blong oli no hapen bakegen long fiuja.

Ol okanaeseisen we oli raetem dokumen ia oli enkarejem yus blong ol taktik blong sikiua tru long disaen, inkludim ol prinsipol we oli referensem ol SSDF praktis. Ol sofwea manufakjera oli mas divelopem wan rodmap we oli raetem blong adoptem moa sikiua tru long disaen sofwea divelopmen praktis long ful potfolio blong olketa. Lis ia hem i wan lis we i no komplit we i soem ol bes praktis rodmap:

- **Ol memori sef prokraming langwij (SSDF PW.6.1).** Praeoritaesem yus blong ol memori sef langwij long ples we i posibol. Ol okanaeseisen we oli raetem dokumen ia oli aknolejem se ol memori spesifik mitikeisen oli save helpem ol taktik we oli blong taem we i moa shot blong ol lakasi kodbes. Ol eksampol oli inkludim ol C/C++ langwij impruvmen, ol hadwea mitikeisen, adres speis leiaot randomaeseisen (ASLR), kontrol-flo intekriti (KFI), mo fasing. Be, i kat wan akrimen we i stap kasem fulap sapot se adopsen blong ol memori sef langwij hem i save elimineitem klas blong difekt ia, mo ol sofwea manufakjera oli shud eksplorem ol wei blong adoptem olketa. Sam eksampol blong ol moden memori sef langwij hem i inkludim C#, Rust, Ruby, Java, Go, mo Swift. Ridim memori sefti information sheet moa infomeisen blong NSA.
- **Sikiua Hadwea Faondeisen.** Inkoporetem ol akitekjeral fija we i eneblem faen-gren memori proteksen, olsem olketa we Capability Hardware Enhanced RISC Instructions (CHERI) i bin diskraebem we i save ekstendem konvensenal hadwea Instruction-Set Architectures (ISAs), mo ol narafala fija olsem ol Trusted Platform Modules and Hardware Security Module. Blong moa infomeisen visitim CHERI webpej blong Yunivesiti blong Kambrij.
- **Sikiurem ol Sofwea Komponen (SSDF PW 4.1).** Akwaerem mo mentenem ol komponen blong sofwea we oli sikiua gud (eksampol, ol sofwea laebri, ol modul, midelwea, ol fremwok) long ol komesel, open sos, mo ol narafala ted pati divelopa we oli verifaem olketa blong mekem sua se sikiuriti insaed long ol konsuma sofwea prodak oli strong.
- **Web templet fremwok (SSDF PW.5.1).** Yusum ol web templet fremwok we oli implimentem otomatik eskeping blong yusa input blong avoedem ol web atak olsem kros-saet skripting.
- **Ol paramitaraes kwiri (SSDF PW 5.1).** Yusum ol paramitaraes kwiri insaed blong inkludim ol yusa input kwiri, blong avoedem ol SQL injeksen atak.
- **Statik mo daenamik aplikeisen sikiuriti testing (SAST/DAST)** (SSDF PW.7.2, PW.8.2). Yusum ol tul ia blong analaesem prodak sos kod mo aplikeisen biheivia blong ditektem ol praktis we i save kat mistek long olketa. Ol tul ia oli kavremap ol isiu stat long nogud manejmen blong memori kasem era pron databes kwiri konstraksen (eksampol, ol yusa input we oli no ronwe we oli lid i ko long SQL injeksen). Ol SAST mo DAST tul oli save inkoporetem olketa i ko insaed long ol divelopmen proses mo ranem olketa otomatikli olsem pat blong sofwea divelopmen. SAST mo DAST i mas komplimentem ol narafala kaen testing, olsem yunit testing mo intekreisen testing, blong mekem sua se ol prodak ia oli komplae wetem ol sikiuriti rikwaemen we oli ekspektem. Taem oli aedentifaem ol isiu ia, ol manufakjera oli mas mekem rut-kos analisis blong adresem ol valnerabiliti long wan sistematik wei.

- **Kod Riviu** (SSDF PW.7.1, PW.7.2). Traem blong mekem sua se kod we yu sabmitim i ko long ol prodak oli ko tru long ol kwaliti kontrol teknik olsem pia riviu we ol narafala divelopa oli mekem o "era siding."
- **Sofwea Bil blong ol Materiel (SBBM)** (SSDF PS.3.2, PW.4.1). Inkoporetem krieisen blong SBBM[4] blong provaedem visibiliti i ko insaed long set blong sofwea we i ko insaed long ol prodak.
- **Ol valnerabiliti disklosa prokram** (SSDF RV.1.3). Establishim ol valnerabiliti disklosa prokram we oli alaoaem ol sikiuriti riseja blong ripotem ol valnerabiliti mo risivim likol sef haba taem oli mekem hemia. Olsem pat blong hemia, ol saplaea oli shud establishim ol proses blong wokemaot ol rut kos blong ol valnerabilti we oli diskaverem. Ol kaen proses ia oli shud inkludim wok blong wokemaot sipos oli adoptem eni sikiua tru long disaen praktis insaed long dokumen ia (o ol narafala praktis we oli semak) bambae i priventem introdaksen blong valnerabiliti.
- **CRE komplitnes.** Mekem sua se ol CRE we oli pablishim oli inkludim rut kos o komon wiknes enumereisen (KWE) blong mekem se i kat indastri-waed analisis blong ol wiknes blong sofwea sikiuriti disaen. Wael wok blong mekem sua se evri CRE oli stret mo komplit hem i save tekem ekstra taem, hem i alaoem ol disparet entiti blong spotem ol indastri jenj we i benefitim evri manufakjera mo ol kastoma. Blong moa infomeisen abaot wok blong manejem ol valnerabiliti, lukluk Stakeholder-Specific Vulnerability Categorization (SSVC) guidance blong CISA.
- **Dip-Difens.** Disaenem infrakstrakja long wei we sipos wan singol sikiuriti kontrol i kompromaes bambae hem i no kompromaesem ful sistem. Eksampol, taem okanaeseisen i mekem sua se oli no kivimaot tumas yusa privilej, mo oli yusum ol akses kontrol lis, hemia i save katem daon impak blong wan akaon we i kompromaes. Mo tu, ol sofwea sanboksing teknik oli save kwarantimin wan valnerabiliti blong limitim kompromaes blong wan ful aplikeisen.
- **Satisfaem Ol Saebasikiuriti Pefomens Gol (SPGs).** Disaenem ol prodak we oli mitim ol besik sikiuriti praktis. Ol Saebasikiuriti Pefomens Gol blong CISA oli aotlaenem ol impoten, beslaen saebasikiuriti mesa we ol okanaeseisen oli shud implementem. Mo tu, blong moa wei blong mekem stand blong okanaeseisen blong yu i strong, lukluk Saeba Asesmen Fremwok blong Inglan we i serem semak samting wetem ol SPG blong CISA. Sipos wan manufakjera hem i no mitim ol SPG—olsem hem i no mekem se i mas kat fishing-resisten MFO blong evri employi—bambae oli no save luk olketa se oli stap dilivarem ol prodak we oli sikiua tru long disaen.

Ol okanaeseisen we oli raetem dokumen ia oli luksave se ol jenj ia oli ol bigfala jenj insaed long weaples okanaeseisen i stap long hem. From hemia, oli mas praeoritaesem introdaksen blong olketa folem ol stret tret modeling, kritikaliti, kompleksiti mo bisnis impak. Oli save introdusum ol praktis ia blong niufala sofwea mo ekspandem long ol rekula stej blo kavremap ol keis mo ol prodak we oli ekstra. Long sam keis, kritikaliti mo risk ples blong wan seten prodak i save minim wan taemlaen we i hariap blong adoptem ol praktis ia. Long ol narafala keis, ol divelopa oli save introdusum ol praktis ia i ko insaed long wan lekasi kodbes mo risolvem bakegen ova long taem.

[4] Sam long ol okanaeseisen we oli raetem dokumen ia oli stap eksplorem ol narafala aproj blong kasem ol sikiuriti asurens raon long sofwea saplae jen.

OL SIKIUA TRU LONG DIFOLT TAKTIK

Antap long wok blong adoptem ol sikiua tru long disaen divelopmen praktis, ol okanaeseisen we oli raetem dokumen ia oli rekomendem se ol sofwea manufakjera oli praeoritaesem ol skiua tru long difolt konfikureisen long ol prodak blong olketa. Oli mas trae had blong apdeitem ol prodak blong oli konfom wetem ol praktis ia taem we oli rifreshem olketa. Olsem eksampol,

- **Eliminetem ol difolt paswod.** Ol prodak oli no mas kam wetem ol difolt paswod we oli semsemak long evri prodak. Blong elimineitem ol difolt paswod, ol okanaeseisen we oli raetem dokumen ia oli rekomendem se ol prodak oli mas kam wetem rikwaemen se ol administreta oli setemap wan strong paswod long taem blong instoleisen mo konfikureisen o blong prodak i shipim wan yunik, strong paswod blong wanwan divaes.

- **Mandetem maltifakta otentikeisen (MFO) blong ol privilej yusa.** Yumi obsevem se ol administreta oli manejem oli fulap entapraes diploemen we oli no protektem ol akaon blong olketa wetem MFO. From se ol administreta oli ol hae valiu taket, ol prodak oli mas mekem MFO opt-aot insted blong opt-in. Mo tu, sistem i mas promptem administreta oltaem blong enrol long MFO kasem taem we oli saksaesfuli eneblem i ko long akaon blong olketa. NCSC blong Netaland hem i kat gaedens we i semak long hemia blong CISA, visitim Majua Otentikeisen Fakstshit blong olketa blong kasem moa infomeisen.

- **Singol saen-on (SSO).** Ol IT aplikeisen oli mas implimentem singol saen on sapot tru long ol moden open standed. Ol eksampol oli inkludim Sikiuriti Asesen Makap Langwij (SAML) o OpenID Konek (OIDK.) Kapabiliti ia oli mas mekem i avelebol tru long difolt mo bae i nokat ekstra jaj.

- **Sikiua Lokin.** Provaedem ol hae-kwaliti odit lok i ko long ol kastoma mo no jajem ekstra o mekem ol ekstra konfikureisen. Ol odit lok oli impoten blong ditektem mo eskaletem ol potensel sikiuriti insiden. Oli impoten tu long taem blong wan investikeisen blong wan sikiuriti insiden we oli saspektem o we i konfem. Konsidarem ol bes praktis olsem provaedem isi intekreisen wetem sikiuriti infomeisen mo ol iven manejmen sistem wetem aplikeisen prokraming intafeis (API) akses we i yusum kodinet yunivesel taem (UTC), standed taem son fomating, mo ol strong dokumenteisen teknik.

- **Sofwea Otoraeseisen Profael.** Ol sofwea saplaea oli mas provaedem ol rekomendeisen abaot ol profael rol we oli otoraesem mo ol desiknetem yus keis blong olketa. Ol manufakjera oli mas inkludim wan visibol woning we i notifaem ol kastoma blong wan risk we i stap ko bigwan sipos oli stap ko aot long profael otoraeseisen we oli rekomendem. Eksampol, ol medikol dokta oli save luk evri peisen rikod, be wan medikol skejula hem i kat smol akses long sam infomeisen we man i nidim blong skejulem ol apoemen.

- **Fowod-luking sikiuriti ova bakwod kompatibiliti.** Plante taem tumas, ol bakwod-kompatibol lekasi fija oli inklud insaed, mo samtaem oli eneblem olketa insaed long ol prodak nomata we oli kosem ol risk long prodak sikiuriti. Praeoritaesem sikiuriti ova ol bakwod kompatibiliti, empaoarem ol sikiuriti tim blong karemaot ol fija we oli no sikiua iven sipos hem i minim se blong kosem ol niu jenj.

- **Trakem mo katem daon "hadening gaed" saes.** Katem daon saes blong ol "hadening gaed" we oli inkludim wetem ol prodak mo traem blong mekem sua se saes i ko daon

ova taem olsem ol niu vesen blong sofwea we oli rilisim. Intekretem ol komponen blong "hadening gaed" olsem difolt konfikureisen blong prodak. Ol okanaeseisen we oli raetem dokumen ia Luksave se ol shot hadening gaed oli risal blong wan patnaship we i stap ko hed wetem ol eksisting kastoma mo inkludim ol efot we fulap prodak tim oli mekem, inkludim yusa eksperiens (UX).

- **Tingbaot ol konsikwens blong yusa eksperiens blong ol sikiuriti seting.** Wanwan niu seting oli inkrisim koknitif beden long ol en yusa mo oli mas asesem wetem bisnis benefit we hem i mekem. Hem i moa gud sipos wan seting i no mas stap; insted, mos sikiua seting oli sapos blong oli intekretem i ko insaed long prodak tru long difolt. Taem we konfikureisen hem i neseseri, difolt opsen hem i mas sikiua long wan jenerol wei akensem ol komon tret.

Ol okanaeseisen we oli raetem dokumen ia oli aknolejem se ol jenj ia maet oli save kat ol operesenal ifek long hao man i emploem sofwea ia. So, kastoma input hem i impoten blong balensem operesenal mo ol sikiuriti konsidereisen. Yumi biliv se blong divelopem ol rodmap we oli raetem mo eksikiutif sapot we i praeoritaesem ol tingting ia i ko insaed long ol mos impoten prodak blong wan okanaeseisen hem i fes step tuwod ol sikiua sofwea divelopmen praktis. Taem we kastoma input hem i impoten, yumi mas obsevem ol impoten keis we ol kastoma oli no bin wiling o no save adoptem ol standed we oli impruvum, samtaem ol netwok protokol. Hem i impoten blong ol manufakjera oli krietem ol minigful insentif blong ol kastoma oli stap long present mo no alaoem olketa blong oli stap valnerebol foeva.

OL HADENING VS LUSENING GAED

Ol hadening gaed oli save kam olsem wan risal blong wok blong nokat ol prodak sikiuriti kontrol we oli embedem i ko insaed long akitekja blong wan prodak long stat blong divelopmen. Olsem wanem risal, ol hadening gaed oli save stap tu olsem wan rodmap blong ol enemi oli pinpoenemaot mo eksploetem ol fija we oli no sikiua. Hem i komon blong fulap okanaeseisen blong oli no awea long ol hadening gaed, mekem se oli leko divaes konfikureisen seting blong olketa i stap long wan poen we i no sikiua. Wan inveted model we oli save se hem i olsem wan lusening gaed hem i mas riplesem ol kaen hadening gaed olsem mo eksplenem ol jenj we ol yusa oli shud mekem taem oli listim tu ol sikiuriti risk we i ol risal blong hem. Ol sikiuriti praktisenal oli shud raetem ol gaed ia, olketa we oli save ekspelenem ol tredof long klia langwij blong inkrisim ol janj blong yusa i aplaem long stret wei.

Insted blong divelopem ol hadening gaed we oli listim ol wei blong sikiurem ol prodak, ol okanaeseisen we oli raetem dokumen ia oli rekomendem ol sofwea manufakjera blong seftem olketa i ko long wan sikiua tru long difolt aproj mo provaedem ol "lusening gaed." Ol gaed ia oli eksplenem bisnis risk blong ol didisen long simpol, langwij we man i save andastandem, mo i save reisemap okanaeseisenal aweanes blong ol risk long ol rabis saeba intrusen. Ol sinia eksekiutif blong ol kastoma oli mas wokemaot ol sikiuriti tredof, blong balensem sikiuriti wetem ol narafala bisnis rikwaemen.

OL REKOMENDEISEN BLONG OL KASTOMA

Ol okanaeseisen we oli raetem dokumen ia oli rekomendem se ol okanaeseisen oli holem ol sofwea manufakjera we oli saplaea oli akaontebol blong ol sikiuriti aotkam blong ol prodak blong olketa. Olsem pat blong hemia, ol okanaeseisen we oli raetem dokumen ia oli rekomendem se ol eksekiutif oli praeoritaesem impotens blong pem ol sikiua tru long disaen mo sikiua tru long difolt prodak. Hemia i save kamaot tru long ol polisi we oli establishim we i rikwaerem se ol IT dipatmen oli asesem sikiuriti blong sofwea bifo oli pem, mo tu blong empaoarem ol IT dipatmen blong push i ko bak sipos i neseseri. Ol okanaeseisen oli mas empaoarem ol IT dipatmen blong divelopem kraeteria blong pejesem samting we i emfasaesem impotens blong ol sikiua tru long difolt praktis (tuketa we oli aotlaenem insaed long dokumen ia mo ol narafala wan we okanaeseisen oli divelopem). Mo tu, eksikiutif manejmen i mas sapotem ol IT dipatmen taem oli enfosem ol kraeteria ia long ol pejesing disisen. Ol okanaeseisen oli mas fomoli dokumentem ol okanaeseisenal disisen blong akseptem ol risk we oli asosiet wetem ol spesifik teknoloji prodak, wan sinia bisnis eksekiutif i mas apruvum hemia, mo presentem long wan rekula wei i ko long bod blong ol daerekta.

Ol mein entapraes IT sevis we oli sapotem sikiuriti stand blong okanaeseisen olsem entapraes netwok, entapraes aedentiti mo akses manejmen, mo ol sikiuriti opereisen mo ol rispons kapabiliti, oli mas luk olketa olsem ol impoten bisnis fanksen we oli fandem blong alaenem wetem impotens blong olketa i lukluk long sakses blong oknaeseisen misen. Ol okanaeseisen oli mas divelopem wan plan blong apgredem ol kapabiliti ia blong leverejem ol manufakjera we oli embreisem ol praktis blong sikiua tru long disaen mo sikiua tru long difolt.

Long ples we i posibol, ol okanaeseisen oli mas trae had blong fojem ol stratejik rileisenship wetem ol mein IT saplaea blong olketa. Ol kaen rileisensip ia i inkludim trast long maltipol level blong okanaeseisen mo provaedem ol wei blong risolvem ol isiu mo aedentifaem ol praeoriti we oli sherem. Sikiuriti hem i mas wan mein elemen blong ol kaen rileisenship ia mo ol okanaeseisen oli mas trae had blong riinfosem impotens blong ol praktis blong sikiua tru long disaen mo sikiua tru long difolt long tuketa fomol (eksampol, ol kontrak mo venda akrimen) mo infomol daemensen blong rileisensip. Ol okanaeseisen oli mas ekspektem transparensi long ol teknoloji saplaea blong olketa abaot intenel kontrol stand blong olketa mo tu ol rodmap blong olketa tuwods adopsen blong ol praktis blong sikiua tru long disaen mo sikiua tru long difolt.

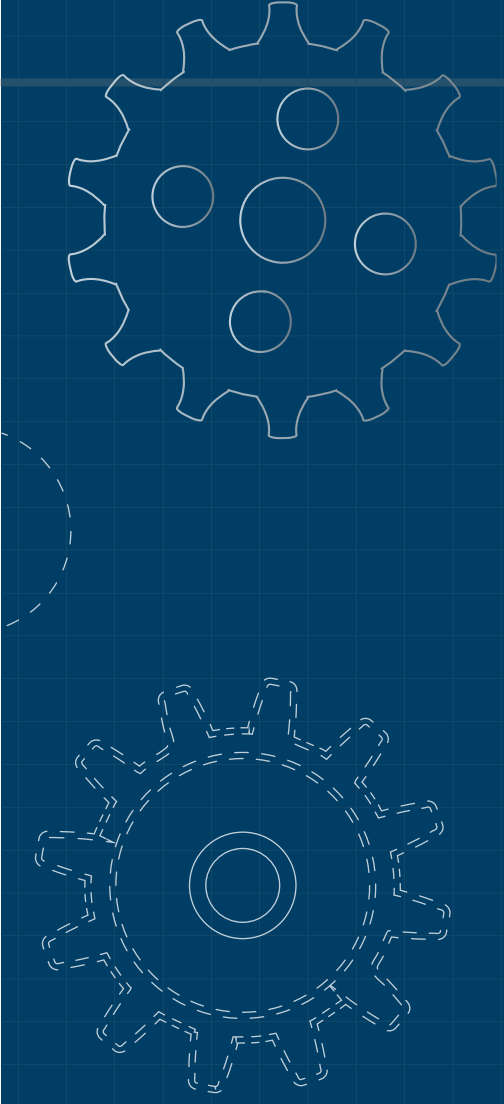
Andap long wok blong mekem sikua tru long difolt wan praeoriti insaed long wan okanaeseisen, ol IT lida oli mas kolaboret wetem ol indastri pia blong olketa blong andastandem ol wijwan prodak mo ol sevis we oli embodim ol disaen prinsipol ia long bes wei. Ol lida ia oli mas kodinetem ol rikwes blong olketa blong helpem ol manufakjera oli praeoritaesem ol apkaming sikiuriti inisietif blong olketa. Taem oli wok tuketa, ol kastoma oli save help kivim miningful input long ol manufakjera mo krietem ol insentif blong olketa blong praeoritaesem sikiuriti.

Taem oli leverejem ol klaod sistem, ol okanaeseisen oli mas mekem sua se oli andastandem risponsibiliti model we oli sherem wetem teknoloji saplaea blong olketa. Hemia i minim se, ol okanaeseisen oli mas kat klariti abaot ol sikiuriti risponsibiliti blong saplaea insted blong jes kat ol kastoma risponsibiliti.

Ol okanaeseisen oli mas praeoritaesem ol klaod provaeda we oli transparent abaotem sikiuriti stand blong olketa, ol intenel kontrol, mo abiliti blong liv ap long ol oblikeisen blong olketa anda long risponsibiliti model we oli sherem.

DISKLEMA

Infomeisen insaed long ripot ia mifala i kivim “olsem we i stap” blong infomeisenal pepes nomo. CISA, mo ol okanaeseisen we oli raetem dokumen ia oli no endosem eni komesel prodak o sevis, inkludim eni sabjek blong analisis. Eni refrens long ol spesifik komesel entiti o ol komesel prodak, ol proses, o ol sevis tru long sevis mak, tredmak, manufakjera, o hemia we oli no rifea long hem, hem i no minim se CISA mo ol okanaeseisen we oli raetem dokumen ia oli stap endosem, rekomendem o fevoretem. Dokumen ia hem i wan joen inisietif we CISA i mekem we hem i no otomatikali kam olsem wan rekulatori dokumen.



Ol Risos

CISA

- CISA's SBOM Guidance (SBOM Gaedans blong CISA)
- CISA's Cross-Sector Cybersecurity Performance Goals (Ol Kros-Sekta Pefomens Gol blong CISA)
- Guidelines on Technology Interoperability (Ol Gaedlaen abaot Teknoloji Intaoperabiliti)
- CISA and NIST's Defending Against Software Supply Chain Attacks (Difens blong CISA mo NIST Akensem Ol Sofwea Saplae JenAtak)
- The Cost of Unsafe Technology and What We Can Do About It | CISA (Kost blong Teknoloji we i no Sef mo Wanem Yumi Save Mekem Abaotem)
- Stop Passing the Buck on Cybersecurity: (Stop pasem wok long saebasikiuriti) Why Companies Must Build Safety Into Tech Products (foreignaffairs.com) (Stop pasem wok blong Saebasikiuriti: From wanem ol Kampani oli Mas Bildim Sefti i ko Insaed long ol Teknoloji Prodak)
- CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance (Gaedans blong Stekholda-Spesifik Valnerabiliti Katigoraeseisen blong CISA)
- CISA's Phishing Resistant MFA Fact Sheets (Ol MFO Fishing Resisten Fakt Shit)
- Cyber Guidance for Small Businesses | CISA (Saeba Gaedans blong ol Smol Bisnis | CISA)

NSA

- NSA's Cybersecurity Information Sheet on Memory Safety (Saebasikiuriti Infomeisen Shit long Memori Sefti blong NSA)
- NSA's ESF Securing the Software Supply Chain: (ESF blong NSA abaot wok blong sikiurim Sofwea Jein Saplae) Best Practices for Suppliers (Ol Bes Praktis blong ol Saplaea)

FBI

- Understanding and Responding to the SolarWinds Supply Chain Attack: (Andastanem mo Ansa long ol SolaWin Saplae Jein Atak:) The Federal Perspective (Federel Tingting)
- The Cyber Threat - Response and Reporting (Saeba Tret – Ansa mo Ripoting)
- FBI's Cyber Strategy (Saeba Strateji blong FBI)

National Institute of Standards and Technology (NIST) (Nasonal Istityut blong ol Standed mo Teknoloji (NIST))

- NIST's Digital Identity Guidelines (Ol Gaedlaen blong Dijitel Aedentiti blong NIST)
- NIST's Cyber Security Framework (Saeba Sikiuriti Fremwok blong NIST)
- NIST's Secure Software Development Framework (SSDF) (Sikiua Sofwea Divelopmen Fremwok blong NIST)

Australian Cyber Security Centre (ACSC) (Saeba Sikiuriti Senta blong Ostrelia (ACSC)

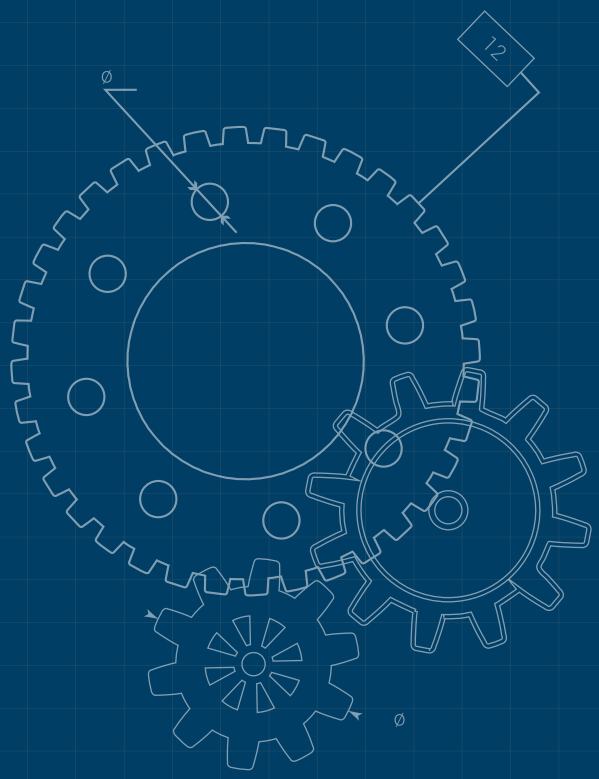
- ACSC's IoT Code of Practice Guidance for Manufacturers (IoT Kod blong Praktis Gaedans we ACSC i mekem blong ol Manufakjera)

The United Kingdom's National Cyber Security Centre (UK) (Nasonal Saeba Sikiuriti Senta blong Yunaeted Kingdom (UK))

- The UK's Cyber Assessment Framework (Saeba Asesmen Fremwok blong UK)
- The UK NCSC's Secure Development and Deployment guidance (Sikiua Divelopmen mo Diploemen gaedens blong UK)
- The UK NCSC's Vulnerability Management guidance (Valnerabiliti Manejmen gaedans blong NCSC blong UK)
- The UK NCSC's Vulnerability Disclosure Toolkit (Valnerbiliti Disklosa Tulkit blong NCSC blong UK)
- University of Cambridge's CHERI (CHERI blong Yunivesiti blong Kambrij)
- So long and thanks for all the bits - NCSC.GOV.UK (Long taem mo tankio from evri bit - NCSC.GOV.UK)

Canadian Centre for Cyber Security (CCCS)

- CCCS's Guidance on Protecting Against Software Supply Chain Attacks (Gaedans blong CCCS abaot Proteksen Akensem ol Sofwea Saplae Jen Atak)
- Cyber supply chain: An approach to assessing risks (Saeba Saplae Jen: Wan aproj blong asesem ol risk)
- Canadian Centre for Cyber Security's CONTI ransomware guidance (Kanada Senta blong Saeba Sikiuriti blong gaedans blong ransomwea CONTI)



Germany's Federal Office for Information Security (BSI) (Federel Ofis blong Infomeisen Sikiuriti blong Jemeni BSI)

- The BSI Grundschutz compendium (module CON.8) (BSI Grundschuts kompendium) (module CON.8)
- The international standard IEC 62443, part 4-1 (Intanasonal standed IEC 62443, pat 4-1)
- State of IT-security in Germany report, 2022 (Steit blong IT-sikiuriti long Jenemi ripot, 2022)
- BSI practices of web application security (OI BSI praktis blong web aplikeisen sikiuriti)

Netherland's National Cyber Security Centre (Nasonal Saeba Sikiuriti Senta blong Netalands)

- NCSC-NL's Mature Authentication Factsheet (Majua Otentifikeisen Fakt Shit blong NCSC-NL)

Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) Nasonal Senta blong Insiden Redines mo Strateji blong Saebasikiuriti blong Japan)

- Japan's National Cybersecurity Strategy (Nasonal Saebasikiuriti Strateji blong Japan)

Japan's Ministry of Economy, Trade and Industry (METI) (Ministri blong Ikonomi, Tred mo Indastri (METI)

- Guide of Introduction of Software Bill of Materials (SBOM) for Software Management (Gaed blong Introdaksen blong Sofwea Bill blong ol Material (SBBM) blong Sofwea Manejmen)
- Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security (Koleksen blong Yus Keis Eksampol Abaot ol Manejmen Metod blong Yusum OSS mo Ensurum Sikiuriti Blong Hem)

Cyber Security Agency of Singapore (Saeba Sikiuriti Ejensi blong Sinkapo)

- Technical Advisory on Secure API Development (Teknikol Advaeseri abaot Sikiua API Divelopmen)
- CSA SingCERT Vulnerability Disclosure Policy (SingCERT valenerabiliti Disklosa Polisi blong CSA)
- CSA SingCERT Incident Response Checklist (SingCERT Insiden Rispons Jeklis blong CSA)
- CSA SingCERT Incident Response Playbooks (OI SingCERT Insiden Rispons pleibuk blong CSA)
- CSA Security by Design Framework (Sikiuriti tru long Disaen Fremwok blong CSA)
- CSA Security by Design Framework Checklist (Sikiuriti tru long Disaen Fremwok Jeklis blong CSA)
- CSA Guide to Cyber Threat Modelling (Gaed blong Saeba Tret Modeling blong CSA)
- CSA Cybersecurity Labelling Scheme (Saebasikiuriti Lebeling Skim blong CSA)

Narafala

- How Complex Systems Fail (Olsem wanem ol Kompleks Sistem Oli Feil)
- The New Look in complex system failure (Niu Luk long kompleks sistem feilia)

OL REFERENS

[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.