TLP:CLEAR

SECURE BY DESIGN

FETUUNAIGA O LE PALENI I LAMATIAGA MAI OSOFAIGA I LUGA O LE INITANETI:

MANATU FAAVAE MA AUALA E FAATINO AI POLOKALAME TAU KOMIPIUTA A LE SECURE BY DESIGN

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Mea o loo aofia ai

Aotelega Vulnerable by Design 4

Mea fou o loo iai 6

Faapefea ona Faaaoga lenei Pepa 7

Secure by Design 8

Secure by Default 9

Fautuaga mo Software Manufacturers (E fausia/gaosia polokalame tau komipiuta) . . . 9

Manatu Faavae o Tulaga tau Puipuiga o Polokalame tau Komipiuta 10

Manatu Faavae 1: Umia o le luga o tulaga tau Puipuiga o Tagata Faatau 11

Faamalamalamaaga 11

Faapupulaina o Lenei Manatu Faavae 14

Manatu Faavae 2: Opogi le faamaoni o le Faamalamalamaina o mea ma le Tali manino atu 20

Faamalamalamaaga 20

Faapupulaina o Lenei Manatu Faavae 21

Manatu Faavae 3: Taitai mai le pito i luga 26

Faamalamalamaaga 26

Faa ataina o Lenei Manatu Faavae 27

Metotia o le Secure by Design 28

Metotia o le Secure by Default 30

Taiala Faamalosi vs Taiala Lusi (Hardening vs Loosening Guides) 32

Fautuaga mo Tagata Faatau 33

Tautinoga Patino 34

Puna'oa 35

Mea o loo faauiga iai 36

AOTELEGA: VULNERABLE BY DESIGN

O le Tekonolosi ua toeitiiti aofia i soo se vaega o le soifuaga i aso taitasi, ma a'o faaauau ai pea ona faatupulaia le fesootaiga o tatou i faiga faigata e aafia sa'o ai le soifua manuia i tulaga tau tamaoaiga, soifua faatamāoaigaina, aemaise le soifua maloloina, e amata mai ile faasinomaga patino o lou tagata agai atu i le tausiga faafomai. O se tasi o itu lē lelei i tulaga faapea, o le solia ai lea o tulaga faavaomalo i luga o upega tafailagi ma o'o ai ina faalēaogaina e falemai taotoga ma le togafitiga o gasegase. O tulaga tau tekonolosi e lē malupuipuia ma e faigofie ona lamatia ai faiga taūa, e ono valaaulia ane ai ma ni osofaiga ōgaōga i luga o le initaneti, ma o'o ai i se tulaga e ono lamatia ai le saogalemu[1].

Ona o lea, e taūa tele ai ona faamautinoa e i latou e fausia polokalame o le komipiuta (software manufacturers) le faia o secure by design ma secure by default, o le vaega e taula'i iai le faatulagana o le oloa ma ona vaega eseese mo le faalauteleina. O nisi faioloa ua tulaga lelei a latou gaioiga ma unaia ai le auaunaga (industry) i le agai i luma i le vaega tau le faamautuina o software, ao isi o loo faatuai pea. O ofisa ua tuufaatasia lenei tusitusiga ua o latou unaia soo seisi e fausia tulaga tau tekonolosi (technology manufacturers) ina ia fausia a latou oloa e fua i le faaitiitia o le avega o le cybersecurity i ana paaga, e aofia ai ma le taofia o latou i le fai pea ma mataitu, o faafouga masani, ma le faatonutonuina o mea faaleagaina i a latou systems e faaitiitia ai osofaiga mai luga o le initaneti. Matou te unaia foi software manufacturers ia fausia a latou oloa i se auala e faaaoga ai le faaokometi o le toe faatulagana ma maitau ai isi mea e pei ona masani ai. O manufacturers o loo unaia ia latou umiaina le faaleleia o tulaga tau le puipuiga mo tagata faatau. Mai tausaga ua tuanai, sa faamoemoe ai software manufacturers ile faaleleia o tulaga maaleale e iloa ane ile ma'ea tuuina ane o oloa mai tagata faatau ma manaomia ai tagata faatau e faaaoga ia vaega o (patches) ae totogi i a latou lava tupe. Sei vagana ua tuu iai faiga e pei o le secure by design, ona faatoa mafai lea ona gausia le faataamilosaga lea o le fai lava ma toe fausia ma apalai iai nisi togafitiga. **Ia manatua:** O le faaupuga "secure by design" o loo aofia ai i totonu le secure by design ma le secure by default.

Ina ia ausia lea tulaga maualuga tau puipuiga i polokalame tau komipiuta, e faamalosia ai e ofisa o loo tuufaatasia lenei tusitusiga, manufacturers ina ia faamuamua le tuufaatasia o tulaga tau le puipuiga mo oloa, ia avea o se vaega e matuai muai manaomia mo mea o loo aofia ai faapea le vave i le maketi. A'o faasolo pea aso, o le a mafai e 'au o inisinia ona o latou faatuina se faiga fou e matua'i faatulaga ai ma faaitiitia ai nisi gaioiga manaomia e faamautuina ai.

Ina ia atagia lenei fuafuaga, e faamalosia ai e le Iuni a Europa le taua o le puipuiga o le oloa i le Cyber Resiliance Act, faamamafa ai e tatau i manufacturers ona faataunuu tulaga tau le puipuiga

[1] O ofisa o loo tuufaatasia lenei tusitusiga ua latou maitauina o le faaupuga "saogalemu" e tele ona uiga ae fua lava i le uiga o loo faaaogaina ai. Mo le faamoemoe o lenei taiala, "o le saogalemu" o le a faauigaina i le siitia o tulaga tau tekonolosi e puipuia ai tagata faatau mai osofaiga ogaoga i le initaneti.

mai lava ile faasologa mai o le olaga o le oloa, ina ia taofia ai manufacturers mai le faalauiloa o oloa o loo i ni tulaga maaleale i luga o le maketi.

Ina ia faia se lumanai e saogalemu ai tulaga tau tekonolosi ma oloa ua aofia ai ma saogalemu foi mo tagata faatau, ua unaia ai e ofisa o loo tuufaatasia lenei tusitusiga, manufacturers ina ia toe fetuunai a latou design poo le faatulagana o oloa ma polokalame toe faaleleia ina ia faataga ai nao le feaveaiina o oloa e secure by design and default. Ae lei oo mai le faalauteleina o mea, o oloa e secure by design ua faatulaga faatasi ma le puipuiga o tagata faatau, o se taulaiga autu faapisinisi lea ae ua le na'o se upu faatatau i tulaga o masini. O oloa a le secure by design e amata lava ile taulaiga lea a'o le'i amataina lona faalauteleina, O oloa o loo iai ile taimi nei e mafai ona faataamilo lava i le tulaga lea o le secure by design i ni taimi se tele. O oloa e secure by default o oloa ia o loo mautu lona faaaogina "out of the box" poo ua tatala ese mai le pusa, ae e itiiti lava pe leai foi ni suiga e manaomia ona toe faia i ai, ae o le a avanoa lava foi itu tau le puipuiga, ma o features o loo avanoa ane e aunoa ma se tau faaopoopo. A tuufaatasi, o nei filosofia e faagaioia esea le tele o le avega o le faatumauina o le mautu mo le 'augaosi (manufacturers) ma faaitiitia ai le avanoa e ono faaletonu ai tagata faatau i ni faaletonu e mafua mai i ni mea ua le o gatasi, lelava poo isi foi faaletonu masani e tele.

O le ofisa o le CISA poo le Cybersecurity and Infrastructure Security Agency, le National Security Agency (NSA), Federal Bureau of Investigation (FBI) ma isi paaga faavaomalo o loo taua i lalo[2] ua latou saunia fautuaga i lenei taiala e avea ma faafanua mo software manufacturers e faamautuina ai le saogalemu o a latou oloa:

- 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)

O ofisa o loo tuufaatasia lenei tusitusiga ua o latou maitauina le sao o nisi o ofisa ma paaga mai le vaega faigaluega tumaoti (private sector) e ala i le faalauteleina lea o le security by design ma le security by default. O lenei oloa ua fuafua e faasolo atu i talanoaga faavaomalo e faatatau i mea e ave i ai le faamuamua, inivesi ma faaiuga e tatau ona faia ina ia ausia ai se lumanai e saogalemu ai le tekonolosi ma mautu ma vave ona toe tulaga lelei mai ile faatulagana (design) ma le tulaga ua filifilia e faaaogaina (default). I lena la faaiuga ua sailia ai e ofisa o loo tuufaatasia lenei tusitusiga, ni finagalo faaalia i lenei oloa mai pati e fia faailoa ni taofi ma fuafua e talanoaina le mataupu lea ia atili faamalamalama ai ma faamautu ma faaleleia , ma ia faalautele a tatou taitaiga ia ausia ai moemitiga faasoaina.

Mo nisi faamatalaga e uiga i le taua o le saogalemu o le oloa, tagai i le tusitusiga i le CISA, The Cost of Unsafe Technology and What We Can Do About It.

[2] Lea ua faaigoa o le "authoring organisation."

O SE MEA FOU

O le uluai lomiga o lenei lipoti na afua ai se vaega tele o talanoaga i totonu o le auaunaga tau polokalame o le komipiuta (software industry). O tala fou i aso taitasi e faatatau i faalapotopotoga ma tagata taitoatasi o loo i se tulaga lamatia, ua atagia ai le manaoga mo le faia o nisi mau talanoaga pe faapefea ona talifaitau atu i faafitauli tumau ma faafitauli i polokalame o oloa tau komipiuta.

I le mae'a o lona faalauiloaina ia Aperila 2023, sa faailoa ai loa e ofisa o loo tuufaatasia lenei tusitusiga (lea tatou te ta'ua o "tatou" poo "matou"), ua o latou maua finagalo faaalia mai le faitau selau o tagata taitoatasi, kamupani ma nisi e galulue i fefaatauaiga. O le finagalo faaalia aupito taatele ina ia saunia nisi faamatalaga faaopoopo e uiga i manatu faavae e tolu pe a apalai e le gata i software manufacturers ae faapea foi i tagata faatau. I lenei la pepa, matou te faalautele ai le uluai lipoti ma pa'i i nisi o autu e pei o le tele o le manufacturer ma le tagata faatau, o le matua o le soifua o le tagata faatau ma le tulaga foi o manatu faavae.

O polokalame tau komipiuta o loo i soo se mea ma e le mafai e se lipoti se tasi ona faasoo lona kavaina o le lautele o software systems, lona faalauteleina o oloa tau polokalame, faasoasoaina o tagata faatau ma lona faatumauina aemaise le tuufaatasia ma isi systems. Mo se taiala i le pito i lalo e le o manino lona faatatauina i se siomaga patino, matou te nofo sauni I le lumanai e faalogo i le komiuniti pe na faapefea ona fesoasoani atu faiga o loo taua i lenei pepa i le faaleleia o le tulaga tau le puipuiga.

O lenei lipoti e apalai i manufacturers poo i latou e fausia malamalama ma polokalame tau masini komipiuta ma atamai faakomipiuta (artificial intelligence) (AI). E ui e ono ese i latou mai ituaiga polokalame ua masani ai, e ao pea ona apalai i ai faiga masani tau le puipuiga e le gata i systems a le AI ma fausaga. O nisi faiga i lalo o le secure by design e ono manaomia ona fetuuna'i ina ia faaofi ane ai tulaga o le AI, ae o manatu faavae uma e tolu o le secure by design e tatau ona apalai foi i systems uma a le AI.

Matou te maitau o le suia o le umi o le soifua o se polokalame tau komipiuta (Software development lifecycle) (SDLC) ina ia o gatasi ai ma manatu faavae ia o le secure by design e le o se galuega faigofie ma e ono umi se taimi e faia ai. Ae le gata i lea, e ono faigata i software manufacturers laiti ifo ona faatino le tele o nei mau manatu faaalia. Matou te talitonu e manaomia e le software industry poo i latou o loo galulue i le auaunaga tau polokalame komipiuta, ona faaavanoa meafaigaluega ma metotia e faasaogalemu atili ai oloa. A'o toatele ane tagata ma faalapotopotoga ua taula'i lo latou vaai i le faaleleia o le saogalemu o polokalame tau komipiuta, matou te talitonu o loo iai lava le avanoa mo nisi o mea fou e ono faaitiitia ai le va lea o software manufacturers tetele ma le vaega laiti, ina ia manuia uma ai tagata faatau.

O lenei faafouga mo le uluai lipoti o le secure by design o se vaega o la tatou mau ina ia fausia faiga faapaaga ma le toatele o komiuniti o loo faaaogaina a tatou tulaga tau tekonolosi. O le tali lea o finagalo faaalia mai le tele o vaega eseese o le ecosystem ma o le a faaauau pea ona faalogo iai ma a'oina mai nisi auala eseese. E ui ina tele le mau luitau i le lumanai, o loo matou matuai naunau e a'oa'oina mai nisi faamatalaga faatatau i tagata ma faalapotopotoga ua o latou muai faaaogaina le filisofia a le secure by design, e masani lava ina faamanuiaina.

FAAPEFEA ONA FAAAOGA LENEI PEPA

Matou te unaia software manufacturers ia usitaia manatu faavae o loo i totonu o lenei pepa. E mafai e software manufacturers ona faailoa lo latou maumaua'i i le tulaga lea e ala ile faapepaina faalauaitele o gaioiga ua faatino, ia o gatasi ma sitepu o loo lisi atu i lalo. Matou te unaia software manufacturers ia sailia nisi taumafaiga e fetaui ma le agaga o le manatu faavae ma ia fausia nisi oloa e iai ni o latou taua e saga faamautu ai le auaunaga i nisi o tagata faatau e masalosalo ma ia mautinoa o loo latou faaaogaina le filosofia a le secure by design.

Faaopoopo atu i gaioiga ia e tatau ona faatino e software manufacturers, e tatau foi ona faapea ona fai e tagata faatau i lenei pepa. O kamupani latou te faatauina polokalame tau komipiuta e tatau ona fesiligia fesili faigata mai tagata o loo faatau mai ai, faaaoga ai ma faataitaiga e pei ona lisiina atu i lenei pepa. I lona faatinoina, ia mafai ona fesoasoani tagata faatau e siitia le maketi agai i oloa o loo matele ina faamautuina e ala i lona faatulagana. O se faataitaiga o fesili e mafai ona fesili ai tagata faatau i e faatau maia oloa o loo tuuina atu i le CISA's Guidance for K-12 Technology Acquisitions.

Matou te unaia tagata faatau a kamupani tetele ia tuufaatasia le ituaiga faiga lea i a latou foi faiga faatau, iloiloga tau tagata faatau oloa, faiga faaiuga e faatatau i mea e ono lamatia ai, ma isi laasaga e faia ao iloiloina tagata faatau. E tatau foi i tagata faatau ona unai a latou faatauoloa (vendors) ina ia faamauina faalauaitele gaioiga a le secure by design o loo faatino e faatauoloa taitasi. I lona tuufaatasiga, e mafai e le faiga lea ona fausia mai ai se manaoga tele mo ni faailo tau le puipuiga, lea e mafai ona unaia ma mafai ai e software manufacturers ona faia ia laasaga agai i se tulaga lelei atu tau le puipuiga. I nisi faamatalaga, pei lava ona o tatou saili e fausia se filosofia a le secure by design e mautu ma iloa tele e software manufacturers, e manaomia ona o tatou fausia se aganuu o le "secure by demand" ma a latou tagata faatau.

Secure by design

O le uiga o le “Secure by design” o oloa tau tekonolosi ua fausia i se auala e malupuipuia ai mai osofaiga ogaoga i le initaneti a i latou o cyber actors, pe a maua lo latou avanoa i masini, faamaumauga ma siomaga o loo koneti atu i ai. O software manufacturers e tatau ona o latou faagaioi le risk assessment poo se iloiloga i tulaga lamatia ina ia iloa ai ma faanumera nisi o faamata‘u e mafai ona alofia, ona faaaofia ai lea o puipuiga i le faatulagana o lea oloa lea e faamatala ai le tulaga o faamata‘u e faia atu i upega tafailagi.

O le faalauteleina o faamatalaga mautu tau tekonolosi (IT) ma le tele o vaega tau le puipuiga- e faaigoa defense-in-depth poo le puipuiga i lona loloto- o loo manaomia foi e taofia ai tagata faafoliga mai le tuuina o systems i se tulaga lamatia pe maua foi le avanoa i ia faamatalaga maaleale e aunoa ma se faatagana. O loo fautuaina foi e ofisa ua tuufaatasia lenei tusitusiga, manufacturers ina ia faaaoga le tailored threat model i le taimi e faalautele ai oloa, ina ia tagofia ai nisi o faamata‘u e ono aliae ma ia faamautu le faasoasoaina o systems taitasi.

E unaia foi e ofisa o loo tuufaatasia lenei tusitusiga ia manufacturers ina ia silasila i mea nei e fesoota‘i uma puipuiga mo a latou oloa ma platforms. E manaomia ile faalauteleina o le secure by design le inivesi iai o meafaitino faatuatuaina e software manufacturers i vaega taitasi uma o le fausia o le faatulagana o le oloa ma lona faalauteleina e le mafai ona toe o ese ai mulimuliane. E manaomia ai taitaiga malosi mai sui pito i luga o le pisinisi ma le manufacturer ina ia o latou faamuamua le puipuiga o le pisinisi, ae le nao se tulaga e faaaoga ai masini. O lenei sootaga i le va o taitai faapisinisi ma technical teams e faasolo ane lava mai le vaega amata ole faatulagana ma le faalauteleina o le oloa seia oo lava ile taimi e faamatuu atu ai le oloa i tagata faatau ma lona faatumauina. Ua unaia manufacturers ina ia faatino fefaatauaiga faigata ma inivesi, e aofia ai nisi vaega e le mafai ona silasila i ai tagata faatau (faataitaiga, agai atu ile faapolokalameina o gagana e aveesea ai tulaga lamatia taatele). E tatau ona o latou faamuamua features poo mea o loo aofia ai, auala e faaaogaina ai, ma le faaaogaina o meafaigaluega e puipuia ai tagata faatau nai lo features e foliga e matagofie ae tele le avanoa e osofaia ai.

E leai se tali se tasi ile faamutaina o faamata‘u o osofaiga ogaoga i upega tafailagi mai ia i latou e faia lea tulaga e faaaoga ai vaega ogaoga o tulaga tau tekonolosi, ma o oloa o loo secure by design, o le a faaauau pea ona aafia i lamatiaga; peitai o se vaega tele o ia lamatiaga e mafua mai i sina sapuseti o mafuaaga autu. E tatau i manufacturers ona faalautele ni faafanua tusitusia ia o gatasi ai a latou oloa ile taimi nei ma faiga sili atu a le secure by design, faamautu ai e faatoa agai ese lava ona o ni itu tulaga ese.

E fia faailoa e ofisa o loo tuufaatasia lenei tusitusiga o le umia o le tali atu i tulaga tau le puipuiga mo tagata faatau ma le faamautuina o le maualuga o le puipuiga o iai mo se tagata faatau, e ono faaopoopo ai ma le tau e totogi mo le faalauteleina. Ae ui i lea, o le inivesi i faiga a le secure by design ao faatalitalia foi le faalauteleina o nisi o oloa tau tekonolosi ma le faamautuina o mafutaga o iai pea, e mafai ona faaleleia atili ai le itu tau le puipuiga o tagata faatau ma faaitiitia ai le avanoa e ono lamatia ai. O manatu faavae o le secure by design e le gata ina faamalosia ai le itu tau le puipuiga mo ana paaga aemaise le talaaga o le brand mo i latou e faalauteleina, ae o le faiga foi lea o le a faaitiitia ai ma tau mo le faamautuina ma le faaleleia mo manufacturers ile silasila mamao.

O Fautuaga mo Software Manufacturers ua saunia ai se lisi o oloa ma faiga e faalautele ai atoa ma faiga faavae e mafai ona silasila i ai le manufacturer.

Secure by Default

O le uiga o le ‘Secure by default” o oloa o loo i se tulaga lelei mai ni faiga e mafai ona alofia e ono faaaogaina ai ina ua tatala ese ma o latou pusa e aunoa ma se totogi faaopoopo. O nei oloa e puipuia mai ai mai faamata‘u ma tulaga ogaoga e aunoa ma le faatino e i latou e faaaogaina oloa o nisi laasaga faaopoopo mo le faamautuina o latou. O oloa a le Secure by default ua faatulaga ina ia silafia lelei ai e tagata faatau o le taimi latou te agai ese ai mai vaega saogalemu (safe defaults) o le a o latou faatuputeleina le avanoa e ono o‘o ai i se tulaga lamatia sei vagana ua faatulaga nisi o meafaatonutonu e pei o ni taui. O le Secure by default o se ituaiga o le secure by design.

- O se fetuunaiga mautu e tatau ona avea ma vaega e faamautu i ai (default baseline). O oloa a le Secure by default e otomeki lava ona faataga ai mea faatonutonu aupito i taua e manaomia mo le puipuia mai osofaiga ogaoga aemaise o le sapalaia o le malamalama e faaaoga ai ma soona faatulaga mea faatonutonu tau le puipuiga e aunoa ma se totogi faaopoopo.
- E le tatau ona avea le faigata o se fetuunaiga tau le puipuiga, o se faafitauli a se tagata faatau. O le aufaigaluega a le IT e masani lava ona tele a latou matafaioi tau le puipuiga ma le faataunuuina o mea, o le ala lea e le lava ai le taimi e malamalama ai ma faatino tulaga tau le puipuiga ma ni mea e manaomia e faamama ai se tulaga lamatia mai osofaiga i upega tafailagi. E mafai e manufacturers ona fesoasoani i tagata faatau e ala ile faalauteleina o faatulagana mautu o se oloa – faamautu ai le “default path”- faamautinoa o a latou oloa o loo gaosia, tufatufaina ma faaaogaina i se tulaga saogalemu fua i tulaga o le “secure by default”.

O manufacturers o oloa o loo ″secure by default” latou te le toe faaopoopo nisi totogi mo le faatinoina o fetuunaiga tau le puipuiga. Ae peitai, latou te faaaofia lea i le oloa faavae, e pei lava o le faaaofia o fusipa’u i soo se taavale fou.

E le tatau ona taugata le puipuiga, ae e tatau ona silasila i ai o se aia tatau a le tagata faatau e maua ai e aunoa ma ni feutanaiga pe faaopoopo foi se totogi.

FAUTUAGA MO SOFTWARE MANUFACTURERS

O lenei taiala faifaatasi ua saunia atu ai fautuaga mo manufacturers mo le faalauteleina o se faafanua tusitusia e faatino ma faamautu ai tulaga tau le puipuiga i faamatalaga tau le komipiuta. E fautuaina e ofisa o loo tuufaatasia lenei tusitusiga, ia faatino e software manufacturers fuafuaga o loo taua atu i lenei vaega ina ia umia ai ni tali e maua ane i tulaga tau le puipuiga mo a latou tagata faatau e tauala i manatu faavae o le secure by design and default.

MANATU FAAVAE TAU LE PUIPUIGA MO OLOA TAU POLOKALAME

Ua unaia software manufacturers ina ia unaia le faaaogaina o se taulaiga e faamuamua ai le puipuiga o polokalame o le komipiuta. Ua faalautele e ofisa o loo tuufaatasia lenei tusitusiga, manatu faavae autu e tolu e taitaia ai software manufacturers i le fausiaina o puipuiga mo polokalame o le komipiuta i totonu o a latou oloa ao lei faalauteleina, toe fetuunai ma lafoina.

1

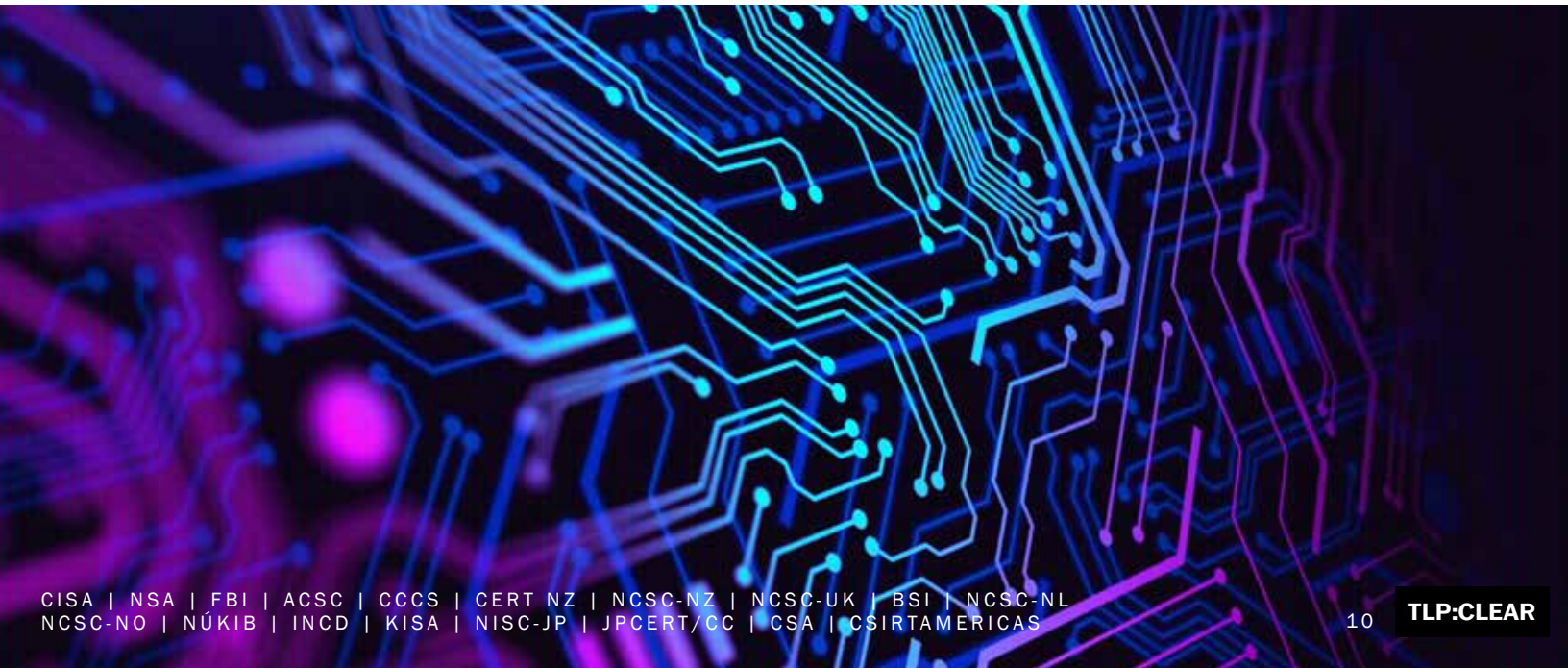
Ia umia le iuga o tulaga tau le puipuiga a tagata faatau ma fua iai le faatamiloga o oloa. O le avega o le tulaga tau le puipuiga e le tatau ona amo toatasi e le tagata faatau.

2

Opogi le faamaoni o le faamalamalamaina o mea ma le tali manino atu.
O software manufacturers e tatau ona o latou mitamita i lo latou kilivaina o ni oloa saogalemu ma mautu, aemaise o le tuuese mai o latou mai le tuuaofaiga o manufacturers ile komiuniti e fua i lo latou agavaa. E ono aofia ai i‘i le faasoaina o faamatalaga latou te maua mai tagata faatau, e pei o le faaaogaina o faiga e malosi mo le faamaoniaina o le tagata (authentication mechanism). E aofia ai foi ma se tautinoga malosi e faamautuina ai fautuaga tau tulaga lamatia ma faamaumauga, CVE poo common vulnerability and exposure (tulaga lamatia taatele ma le faailoaina o faamaumauga) o loo ua maē‘a ma sa‘o lelei. Ae ui i lea, ia silafia faaosoosoga e faitau CVE o se fua e le lelei, ona o ia ituaiga numera e mafai foi ona avea o se faailo o se iloiloga e maloloina (healthy code analysis) ma o loo tofotofo ai le komiuniti.

3

Fausia faatulagana o le faasologa ma le taitaiga ina ia ausia ai moemitiga nei.
E ui o le silafia faatatau i le galuega o loo faia e taua i le puipuiga o le oloa, o ofisa sinia o i latou lava o le ‘aufaifaaiuga mo le faatinoina o suiga i se faalapotopotoga. E manaomia ona faamuamua e ofisa sinia le tulaga tau le puipuiga o se elemeni taua i le faalauteleina o le oloa ile faalapotopotoga, ma o loo faapaaga ai ma tagata faatau.



Ina ia mafai ona faataga ia manatu faavae e tolu, e tatau ona silasila manufacturers i nisi o metotia e siomia ai le faiga o a latou galuega faalautele.

Fai fonotaga faaauau ma sui sinia o le kamupani ina ia unaia le taua o le secure by design ma le secure by default i totonu o le faalapotopotoga. O faiga faavae ma fuafuaga faataatitia e tatau ona faatuina ina ia faia ni taui mo ‘au o loo feagai ma le gaosiga ma le faalauteleina o oloa e fua agai i manatu faavae ia, e ono aofia ai ni faailoga (awards) mo le faataunuuina o le polokalame tau le puipuiga aupito sili pe fai foi apefai faalegaluega ma faalauiloa e siitia ai tulaga.

Gaioi faataamilo ile taua o le polokalame tau puipuiga i le manuia o se pisinisi. Mo se faataitaiga, silasila ile tuuina o se taitai o le polokalame tau le puipuiga poo se ‘au foi tau le puipuiga o le polokalame (software security team) latou te faatumauina pisinisi ma faamatalaga tau tekonolosi e iai sootaga ma nisi vaega tau le puipuiga ma le mafai ona tali manino mai o le manufacturer. E tatau i manufacturers ona faamautinoa o iai ni polokalame malosi mo le siakiina o le saogalemu ma le matauina o a latou oloa tutoatasi.

Faaaoga le tailored threat model (faataitaiga o ni faamata‘u fuafuaina lelei) ile taimi e faamatuu ai meafaitino ma le faalauteleina ina ia faamuamua mea faigata ma mea e tetele ona aafiaga. O threat models latou te silasila i mea e faaaogaina e le oloa ma faataga ai ‘au e faalauteleina oloa ina ia faateleina. Ma le vaega mulimuli, e tatau i ‘autaitai sinia ona tuu le matafaioi i luga o ‘au poo teams o loo feagai ma oloa ina ia avea o se elemeni autu lea o le tulaga lelei o oloa ma le ituaiga e iai.

O se vaega o le taiala ia Oketopa 2023, ua faafou ai lenei taiala, o manatu faavae ia e tolu ua faalauteleina e faaaoga ai nisi o faamatalaga nei, faataitaiga ma faamaoniga.

MANATU FAAVAE 1: Ia umia le luga o tulaga tau le Puipuiga a Tagata Faatau

FAAMALAMALAMAGA

O faiga aupito sili faaonaponei ua faatonutonu ai software manufacturers ma inivesi ai i puipuiga mo oloa ma taumafaiga, e aofia ai **talosaga faafaigata, mea o loo aofia ile talosaga,** ma talosaga **vaega ua faatulaga e agai i ai.**

E manaomia e software manufacturers ona faatino le **application hardening** e ala i le faaaogaina o fuafuaga ma le tekonolosi e siitia ai le tau mo se tagata osofai o loo fuafua e faaleaga pe tuuina talosaga i se tulaga lamatia. O mea ua faatulaga mo le application hardening ma lona faasologa e fesoasoani i le tetee atu i osofaiga a le aupopoto ile matafaioi lea. O faaupuga e pei o le hardening,poo le faamalosia o se oloa, puipuiga o se oloa ma lona sologa lelei e iai lona sootaga i le ituaiga e iai le oloa. O le manatu ina ia tatau lava ona “taulu” le puipuiga ma aua ne‘i “sola ese ai”. [1] O le taulu o le puipuiga, ona faatoa mafai lea ona faaopoopo e software manufacturers le puipuiga mo tagata faatau ma faaopoopo foi ma le aofai o a latou oloa. O nisi faataitaiga o ia metotia e aofia ai le faamautuina o loo faamaoniaina ma ia faamamaina le user input, ma aua ne‘i tuuina sa‘o i totonu o le code (faataitaiga e ala i le faaaoga o parameterized queries), faaaogaina o se gagana tau polokalame e saogalemu mo le mafaufau, le soifua o le polokalame tau le komipiuta, ma le faaaogaina o faiga faatonutonu o le hardware-backed cryptographic key management.

O talosaga e manaomia le lagolagoina o le **application features** e iai lona sootaga ile cybersecurity. E faaigoa i nisi taimi o “capabilities”, o nei features e faaumi ai le ola o se oloa poo se auaunaga i ni auala e fesoasoani e faamautu pe siitia ai foi le puipuiga ma le tulaga o

se tagata faatau. O nisi o faataitaiga o ia features e aofia ai le TLS poo le transport layer security mo fesootaiga uma tau initaneti, lagolago mo le single sign on (SSO), lagolago mo le multi-factor authentication (MFA), security event audit logging, role based access control (RBAC) ma le attribute-based access control (ABAC).

O nisi o features o nei oloa e mafai ona fetuunai ma mafai ai e tagata faatau ona tuufaatasia oloa i nisi o o latou siomaga ma faasologa o galuega. O nei fetuunaiga o lona uiga o talosaga e tatau ona iai le **default settings** ua faatulaga sei vagana ua toe fetuunai e tagata faatau. O ia faatulagana (default settings) e tatau ona faamautu lelei le faatulagaina i le tulaga ua aveesea ai mai le pusa ina ia faaitiitia le faaaoga e tagata faatau o meafaitino e faamautu ai a latou oloa tau tekonolosi.

O nei elemeni taitasi – faamalosia o le talosaga, mea o loo aofia ile talosaga, mea tau le puipuiga o loo aofia ai ile talosaga, ma le faatulagana o le setting, e taua tele lo latou sao i le puipuia o le talosaga, ma le iuga o le tulaga tau le puipuiga e tuuina atu ile tagata faatau. E tatau i software manufacturers ona mafaufau i mea taitasi nei o elemeni ma pe faapefea ona fesootai i isi. O manufacturers e tatau ona mafaufau ile tele o mea e le nao a latou inivesi i nisi o elemeni ia i a latou oloa. E tatau ona laasia le isi sitepu e manufacturers ma silasila pe faapefea ona suia e ia elemeni le tulaga moni o tagata faatau ile lalolagi, pe lelei pe leaga foi.

E tatau i manufacturers ona o latou umia le iuga o tulaga tau le puipuiga mo a latou tagata faatau ae le o le fua e latou ia i latou lava ma inivesi. E tatau ona amata faatuina mai le matafaioi lea mai le mata o le vai, e aofia ai manufacturers, lea e iai le avanoa aupito tele e ono faaitiitia ai ni tulaga lamatia.

Ae paga lea, e le o le tulaga lea ua iai i nei aso. Ua toatele manufacturers ua o latou tuuina le avega o tulaga tau le puipuiga i luga o tagata faatau ae le inivesi i faiga e faamalosia ai talosaga **application hardening.** Mo se faataitaiga, afai e faaleleia e le manufacturer se tulaga maaleale, e masani ona o tatou vaaia isi vaega maaleale tai faapea foi ua faailoa ane ona ua o latou tagofia auga nai lo le agai sa‘o i le faapogai o le faaletonu. E ono mafai e le oloa ona faatino nisi fesuiaiga i vaega eseese o le vaega autu (code base) mo le ituaiga tulaga maaleale lava lea e tasi. O se faataitaiga lelei lea o mea e pei ona taua, afai e maē‘a ona faaleleia e le manufacturer se vaega se tasi o maaleale, o le au suesue poo le ‘auosofai o le a o latou mauaina auala e lei faamanuiaina mai le vaega sa faaleleia. E faia e le manufacturer galuega faaleleia mai lea taimi i lea taimi nai lo le tuufaatasi uma o le codebase e aveese ai lea vasega o tulaga maaleale i le talosaga atoa.

Application features e mafai ona fausia uma ai penefiti ma lamatiaga mo tagata faatau. O mea o loo aofia ai (features) e faataga ai ni vaega e tuufaatasia ai (integration point) ae tele ona external systems ma ituaiga e mafai ona faateleina ai le taua o le oloa. I le ma lea, o supporting features poo mea o loo aofia e lagolago ai e aunoa ma se fuafuaga mo le litaea, aiaiga mo sootaga (networking protocols), e mafai ona tuuina ai le tagata faatau i se tulaga maaleale pe afai e le lava lo latou malamalama i aafiaga o le faaaogaina pea o lea feature. Mo se faataitaiga, o nisi o oloa o le a faaauau pea ona o latou faaaogaina aiaiga mo sootaga e iai o latou talaaga mai le vaitausaga o le 1990 poo le 2000 ma ua iloa nei e le saogalemu. E tele mafuaaga e mafai ona faalemu ai le vave e mafai ai e tagata faatau ona faafou pe faasoa faiga tau le puipuiga faaonaponei. E mafai ona o latou faaaoga oloa e mafai ona tuufaatasi ma isi vaega uma o le sootaga a le faalapotopotoga, ae le lava faiga tau le puipuiga faaonaponei, ma taofia ai le ‘au a le IT mai le faafouina o mea e pei ona iai i aso nei. Ae peitai, o software manufacturers e mafai ona o latou faaaofia nei faasologa i totonu o a latou fuafuaga faataatitita e unaia ai tagata faatau ina ia tumau pea.

Application default settings o se vaega faaopoopo e ono tulai ai ni lamatiaga mo tagata faatau. E masani ona filifili e manufacturers nisi vaega patino (default settings)ma faigofie ai mo tagata faatau ona faaaoga features o le talosaga latou te mananao ai. O le itu le lelei ona o lea ituaiga faiga e faatetele ai le avanoa mo ni osofaiga mo tagata faatau lea latou te le ono manaomia ni features patino ma ni aiaiga e mafai ona faataga e aunoa ma se tau faatonuina. Faaopoopo atu i lea, o le tele o tulaga faatonutonu mo puipuiga e mafai ona ki ma tape by default pe manaomia foi le tagata faatau ia faaalu lona taimi e faatulaga ai lona faatulagana ina ia faateleina ai lona puipuiga. O le Explicit threat modelling o se metotia e ono mafai ona fesoasoani e faailoa le faaiuga ua faia e tatau ai i features ona faaola by default pe manaomia nisi faatulagana e avea ai ma secure by default. O le isi metotia o le suesue lea o auala e mafai ai ona iloagofie features mo le tagata o loo faatonutonuina.

O nisi manufacturers latou te lafoina mai oloa e iai faaletonu e mafai ona maua ai ni lamatiaga mo nisi poo a latou tagata faatau uma foi. E ese mai le faatulaga o nisi o vaega saogalemu (safer defaults), e masani ona o latou filifili e fausia se taiala faamalosi **hardening guide** e tatau i tagata faatau ona faaaogaina ae totogi lava e latou. O taiala faamalosi (hardening guides) e tele faaletonu taatele e aafia ai. O nisi o nei taiala e faigata ona sailia ma e le lava foi le lagolagoina. O isi e faigata tele ona faatino, e fai lava ma manaomia le faalauteleina o polokalame tau komipiuta ina ia tusia ai se faataitaiga lautele. Ae ui i lea, e manatu nisi o le tagata o loo faitauina (reader) e iai lona tomai lautele tau cybersecurity e malamalama ai i auala e mafai ona suia ai e le mau faatulagana, le vaega e sao mai ai osofaiga. O i latou e faia lea matafaioi ae le lava lo latou malamalamaaga i auala e mafai ona galulue ane ai le ‘auosofai, e ono le mafai ona o latou faatinoina lelei le taiala faamalosi lea ma ona faatonuga, aemaise lava pe afai o faatonuga o loo aumai e le faamanino mai ai le tulaga o fefaatauaiga. E le gata i lea, e le o taiala faamalosi uma e tusia e inisinia o loo matuai masani i auala a le ‘auosofai ma tulaga tau tupe, e mafua ai ona o latou fausia taiala faamalosi e le tele ni o latou aoga tusa lava pe o loo faamaoni lona faatinoina. E faitau miliona tagata faatau o loo latou faatino le matafaioi e faamalosia ai vaega eseese o polokalame tau komipiuta ma systems, aemaise lava i siosiomaga e le o matuai lava ai mea faitino e faaaoga. O le faamoemoe i taiala faamalosi e le tuufaasolo.

O le faatulagana o se talosaga e tatau ona fai pea ma iloiloina pe o le faatulagana o se mea na muai faatulagaina (default) pe o se mea na faatulaga e le tagata faatau, e fua agai i le malamalama o le manufacturer o loo iai e faatatau i le faamata’u o loo feagai. O talosaga e tatau ona faatinoina ma ni faailo manino e faatatau i ni tulaga lamatia e ono aafia ai ma ono maua ane mai ia faatulagana ma e tatau lava ona faailoa ia faailo. Pei lava o se taavale faaonaponei, e iai lona faailo o fusipa‘u ma faailoa ane e le faailo lea e ala i le faa i‘i ane o se faamanatu pe afai e te taumafai e ave le taavale ae le faamauina lou fusipa‘u, e tatau foi i polokalame tau komipiuta ona faailo le tulaga o iai le itu tau le puipuiga o se system. Afai e faatulaga se talosaga ina ia aua ne‘i manaomia se MFA mo accounts a i latou o loo faatonutonuina le auaunaga (administrators), e tatau lava la ona faailoa i tagata ia o latou ma a latou faalapotopotoga o loo i se tulaga lamatia pe afai e le faatulagaina le MFA. Faaopoopo atu i lea, afai e faatulaga se talosaga e lagolago ai nisi o aiaiga ua leva lea o loo iloa nei e ono mafai ona maua ai se tulaga vaivai, e tatau ona fai ma faamanino i administrators o loo lamatia le faalapotopotoga ma ia saunia ni meafaitino e faaleleia ai lea tulaga. Matou te unaia manufacturers ina ia faatino siaki o loo tuuina i totonu o oloa ae le nao le faamoemoe i administrators e maua lo latou taimi, malamalaaga ma le silafia e faamalamalama ai taiala faamalosi. O avanoa o loo manino le iai mo ni tomai fou e faapaleni ai le puipuiga ma le faaaogaina.

O elemeni taitasi o loo taua i luga e mafai ona afua ai se tulaga e le mafai ona lagolagoina, e manaomia ai le faatino e tagata faatau o se suesuega, faatupe, faatau, aufaigaluega, faasoa, ma mataitu nisi oloa faaopoopo **security products** e faaitiitia ai le avanoa o se tulaga lamatia. O faalapotopotoga laiti pe feololo (SMOs) e masani lava ona le mafai ona o latou faatinoina nei vaega. Latou te feagai ma tulaga e le lava le malamalama, faatupega, ma le taimi lea e totogi ai lafoga mo le faaaogaina, ma faamalosia ai le puipuiga i se tulaga maualalo, ma a tuufaatasi, e afua ai ni lamatiaga. E ese mai lea, o inivesi tau le puipuiga e nisi o nai manufacturers e mafai ona faasolosolo pea. O se faaupuga taatele e masani ona ta aofai uma ai le faaletonu lea, o le manaomia lea e le auaunaga tau software o ni oloa malupuipuia ae le o le tele o oloa tau le puipuiga. O software manufacturers e tatau ona taitaia lea fesuiaiga.

> ***E manaomia e le auaunaga a le software nisi oloa mautu ae le o le tele o oloa tau puipuiga. O software manufacturers e tatau ona o latou taitaia lea fesuiaiga.***

O aso nei, e fai ma o tatou faitau faamatalaga mai manufacturers e faamalamalama ai o se tagata faatau ua i se tulaga lamatia ona o le le faatagaina o se feature patino tau le puipuiga pe taumulimuli foi i le taiala faamalosi. Peitai, afai e maēʻa ona i se tulaga lamatia, e tatau i manufacturers ona faamalamalama pe e ono mafai e se security feature poo se taiala faamalosi patino ona taofia le tulaga lamatia lea ma ia silasila i le faaaoga o le tulaga lea e fai ma default e aunoa ma se totogi. I tulaga faapea e lei lava ai ona faamalosia le tulaga o le oloa i vaega o le faatulagana ma le faatinoina, e tatau i le manufacturer ona faamalamalama pe faapefea ona o latou galulue e aveesea lea vasega o tulaga maaleale mai laina o a latou oloa.

O software manufacturers e iai a latou matafaioi e faamautu ai o a latou oloa o loo faatulaga ma faalautele ma le manatu e faamuamua lava le tulaga tau le puipuiga. I lea faaiuga, e tatau ai ona o latou fuaina le iuga **maioio lelei le fuaina o iuga** o a latou taumafaiga. Matou te valaau i manufacturers ina ia le gata le taulaʻi o le latou silasila i taumafaiga i totonu, ae ia fua foi ma fai ma lipoti le iuga ma le aoga o se oloa ma ona puipuiga ma faatulagana, ma ia fausia se fesootaiga o ni finagalo faaalia e faia ai ni suiga i le SDLC e afua ai nisi o mea faaleleia i le saogalemu o le tagata faatau ma ia sili ona malupuipuia oloa. O lipoti e tatau ona aofia ai ma faamatalaga faalilolilo e mafai ona faaaoga e le au aʻoaʻoina ma le au suesue tau puipuiga a le komiuniti, e mulimulitai ai i faiga aupito sili ma fua ai le sologa lelei o le ecosystem lautele.

FAAPUPULAINA O LENEI MANATU FAAVAE

O software manufacturers ma auaunaga i luga o upega tafailagi e tatau ona o latou sailia ni auala e mafai ona faapupula ai le manuia o le faatinoina o lea manatu faavae. E tatau ona o latou saili e saunia ni faamaoniga i ni artifacts mo tagata mai fafo e latou te asiasia. E le mafai e se artifact se tasi ona faamaonia o loo faataunuu ese manufacturer se polokalame mautu ma lelei, ae o le saunia ane o ni artifacts eseese e mafai ai ona fausia se finauga e uiga i le maumaua'i o le manufacturer i le faalauteleina o oloa mautu. O lenei faiga o loo i le agaga o le "faailoa ae le na'o le faamatala".

Ina ia faapupula lenei manatu faavae, e tatau i software manufacturers ona silasila i laasaga e pei ona faailoa atu i le lisi o loo i lalo. Ua maitauina e ofisa o loo tuufaatasia lenei tusitusiga, e iai ni nai software manufacturers o le a mafai ona vave lo latou faatinoina o nei faiga ma saunia ane ni artifacts talafeagai i le amataga o le latou faigamalaga ma le secure by design. I le ma le isi, o software manufacturers o le a manaomia lo latou faamuamua o lenei lisi e fuafua agai pe faapefea ona faasoasoa e le tagata faatau le oloa i le mea e faaaogaina ai ina ia ausia ai penefiti aupito tetele tau le puipuiga.

FAIGA O LE SECURE BY DEFAULT

1. **Aveese default passwords (‘uputatala mua‘ifili).** E faaauau pea ona avea upu tatala e agai muamua iai poo default passwords ma mafuaaga o le tele o le mau osofaiga i tausaga taitasi. O le faia o se tautinoga e aveesea lea ituaiga faafitauli o le a teena ai le faigofie ona ulufale o le ‘auosofai. E tai pei lava foi ona tatau ona silasila manufacturers i ituaiga faiga o passwords e ao ona faaaoga, e pei o le umi faatagaina mo se password ma le aua nei iloaina o isi passwords ua le toe faaaogaina.

2. **Faatino suesuega i siomaga.** A’o faaauau pea ona fesuiai faiga tau tekonolosi ma faasolo ina faigata, ua faateteleina le taua o le faia e software manufacturers o ni faataitaiga tau le puipuiga e faataitai ai poo malamalama i le tulaga tau le puipuiga o iai ana oloa. Tai pei lava ole logoina e le ‘ausuesue o mea e manaomia mo le faalauteleina o polokalame tau komipiuta, e tatau foi i software manufacturers ona faatino suesuega e patino i tagata o loo faaaogaina le suesuega ina ia malamalama ai i vaega o loo le lava ai le silafia o le tagata faaaoga (user). O le mataituina o le tagata faatau ma lona faasoaina ma le faaaogaina o a latou oloa i siomaga o le lalolagi, e mafai ai ona maua e software manufacturers le malamalamaaga i le faaaogaina ma le aoga o features o a latou oloa ma le faatonutonuina. O nei malamalamaaga o le a fesoasoani i le maitauina o vaega e manaomia ona faaleleia ma toe faafou ai a latou oloa ia sili ai ona ausia le tulaga tau le puipuiga o loo manaomia e tagata faatau. Mo se faataitaiga, o suesuega faataitai o loo faia i lea siomaga e ono faailoa ane ai nisi o suiga i le faagasologa o le UX, defaults, faamanatu ma le mataituina. O faataitaiga foi e faia i siomaga e ono faailoa ai poo fea tonu i le taimi ua sola ile faatulagana ma le faaleleia o le oloa, na faaitiitia ai le mamafa o tulaga faaleleia na faia i le puipuiga, faaitiitia mea sese i le faatulagana ma ia faaitiitia vaega e osofaia ane ai.

E tatau i manufacturers ona silasila i mea o loo taua i lalo:

- O sa’o le faatinoina e tagata faatau o le taiala faamalosi?
- O gaioi features o loo iai tau le puipuiga o le oloa ma le tulaga o loo faatalitalia ile siomaga?
- Pe moni e mafai e ia features ona tetee atu i osofaiga a le lalolagi?
- O a tonu features o le a sili atu ona faaitiitia ai le ono iai ise tulaga lamatia?

Faamaumauga: Ina ia maua se malamalamaaga loloto e faatatau i nei elemeni, e mafai e software manufacturers ona fai paaga ma tagata faatau ina ia faatino ni faiga e faataitai ai pe faapefea ona tetee le oloa i ni osofaiga. O ia faataitaiga e faia ile siomaga e ono mafai ona faatino i le nofoaga o le tagata faatau, pe faaaoga foi le telemetry mai le talosaga ise tulaga faalilolilo.

3. **Faaititia le tele o le taiala faamalosi.** O manufacturers e mafai ona o latou faaleleia tulaga tau le puipuiga o tagata faatau e ala ile faalautele poo le aveesea foi o tala faamalosi mo oloa ma taulai le silasila i le vaega aupito taua tau le puipuiga e mafai ai e tagata faatau ona ave i ai le faamuamua pe a faasoa a latou oloa. E ese mai le soona tuuina atu i tagata faatau o se lisi o mea manaomia tau le puipuiga, e tatau i manufacturers ona maitau le lamatiaga aupito maualuga o iai tau le puipuiga e mafai ona onosaia e ana oloa ina ia saunia ai se taiala e kilia ma sa‘o i auala e mafai ai ona agai ese ma ia lamatiaga. Faaopoopo atu i lea, o manufacturers e tatau ona o latou saunia ni meafaigaluega mo tagata faatau ma ia okometi ma faafaigofie ai le faatinoina o le faatonutonuina o tulaga tau le puipuiga, e pei o ni scripts e faigofie ai ona faasoa i o latou siomaga. O nei meafaigaluega e mafai ona faaopoopo atu i le mafai lea ona faamaonia ma faailoa manino suiga sa faia mai le amataga. O le faalauteleina o taiala faamalosi ma le saunia o meafaigaluega e faigofie ona faaaoga ma okometi mo tagata faatau, o le a mafai ai e manufacturers ona faaitiitia le avega i luga o tagata faatau ma fesoasoani ai i le faamautuina o loo faasoa a latou oloa i se tulaga mautu. O le isi metotia o le silasila lea i le faia o le Pareto principle

e faaitiitia ai le numera o laasaga mo le faaaogaina taatele (80%) ma le saunia o ni taiala ma nisi meafaigaluega e faaaoga mo nisi mataupu e le taatele tele(20%). O le auala lea o le a faafaigofie ai e software manufacturers ona faafaigofie mea faigofie, ma mafai ona ausia mea faigata. O le faia o faataitaiga i se siomaga, o se meafaigaluega taua lea mo le fuaina pe o le a le umi mo tagata faatau e iloa ai, malamalama ma faatino taiala faamalosi. E tatau i manufacturers ona silasila pe faapefea ona faaoso e le oloa le administrator ina ia faia se gaioiga i totonu lava ia o le oloa nai lo le faamoemoe ia i latou e faatino se gaioiga mai le taiala faamalosi.

4. **Ia vave ona aua le faamalosia le faaaoga o features e le saogalemu.**
Faamuamua le tulaga tau le puipuiga tauala atu i auala ua mae'a faaleleia nai lo le faaaoga o le backwards compatibility (o se isi polokalame tau komipiuta). Lomia tusitusiga i upega tafailagi o loo faailoa ai le faaaogaina o features saogalemu ma aiaiga, ma faailoa le lē fiafia i features e lē saogalemu e ala i le folafola atu, e lē taumate mai totonu lava o le oloa ia. O se vaega tele o tagata faatau ua o latou faailoa o le a o latou lē taofiofi i systems o loo iai i le taimi nei ma le sootaga faaonaponei, tulaga o o latou tagata, ma isi features aupito taua tau le puipuiga. I nisi mataupu, e fefefe tagata faatau i nisi o auaunaga o loo iai e ono amata lava i se upgrade, (faafouga). O le faia o ni faafouga e aunoa ma ni lavelave, o le a ono faafou ai e tagata faatau a latou oloa ma fai ma faaleleia tulaga tau le puipuiga ma vave foi. O software manufacturers e tatau ona o latou faaoso tagata faatau i auala mo le faafouina ina ia faaitiitia ai le lamatiaga ia i latou.

5. **Ia faatino ni faamanatu e vave ona faalogo ane ai le tagata.**
Tai pei lava foi o faailo o fusipa'u i taavale lea e masani ona pa'o ane pea pe afai e le faamauina fusipa'u, e tatau foi i manufacturers ona o latou faatino ma faaauau pea ona faamanatu i users poo admins pe afai ua iai i latou ini tulaga le saogalemu, lapatai administrators o loo ua o latou faaaogaina manatu faavae e le taliaina i o latou siomaga ma fautuaina iai le faia o ni upgrades (faafouga). Faatino pea ni faamanatu faaauau ma talafeagai pe afai o loo iai ise tulaga le saogalemu users ma admins, poo le faatulagana o le talosaga. Fai ma faamanino i administrators o loo lē saogalemu le tulaga o iai . O se isi feature faaopoopo e ono manaomia ai se super administrator e na te faamaonia le lava o le MFA i a latou accounts i taimi e log in ai pe faalēaoga foi nisi o features autū sei vagana ua o latou faataga le faaaogaina o le MFA. O loo iai le avanoa mo ni manatu fou e ausia ai nei moemitiga ae lē o faatino ai foi ma se faamanatu ua vaivai.

6. **Ia faia ni templates mo faatulagana mautū.**
O nei templates e mafai ona faa seti ai nisi o faatulagana i se tulaga saogalemu e fua i le tulaga o iai ni lamatiaga i se faalapotopotoga. E ui e ono foliga e matuai faigofie le iai o ni security templates e maualalo/feololo/maualuga tulaga tau le puipuiga, o lea faataitaiga ua faailoa ai le tele o le mau faatulagana e mafai ona faafou ina ia faatonutonu ai lamatiaga i le faalapotopotoga. O templates e mafai ona lagolago e taiala faamalosi i tulaga tau lamatiaga e maitauina e le manufacturer.

FAIGA MAUTŪ O LE FAALAUTELEINA O OLOA

1. **Faamauina le usitaia o aiaiga i se faavaa mautu a le SDLC.** O faavaa mo le Secure SDLC, e saunia ai ni mea e fia ausia ma ni faataitaiga i tagata, faagasologa o mea ma le tekonolosi. Silasila i le lomia o se faamatalaga auiliili o le faaaogaina o faavaa ia tau secure SDLC ma faamalamalama ai nisi tulaga tau le puipuiga sa faaaogaina. I totonu o Amerika, silasila i le faaaogaina o le NIST Secure Software Development Framework (SSDF). E ui e lē o se lisi e siaki agai i ai, o le SSDF e "faamalamalama ai se seti o faiga taua, ma mautū mo le saogalemu i le faalauteleina o software ".

2. **Faamauina Moemitiga a le Cybersecurity (CPG) pe o se isi tulaga tali tutusa.** Afai e faapea mai se faalapotopotoga o loo o gatasi i latou ma tulaga o le NIST SSDF, o loo latou faapea mai o le latou SDLC o loo logoina atu e ni faiga aupito lelei ma malamalama. 'Ae ui i lea, e le lava mo latou ina ia iai nao se latou SDLC malosi. E manaomia foi ona o latou puipui i la latou pisinisi ma le siomaga faalauteleina mai osofaiga a i latou o loo saili e taulamalama tulaga tau le puipuiga o le oloa ao iai pea i le vaega mo le faalauteleina. E le o se osofaiga lenei o se vasega o manatu, ae o se tulaga na faatinoina faatasi ma aafiaga mai tagata faatau, aemaise o le faaopoopoga o le puipuiga lautele. E tatau i faalapotopotoga ona o latou silasila i faamaumauga lomia ole faalapotopotoga ia o gatasi ma le CISA CPGs, ole NIST Cybersecurity Framework(CSF), pe o isi faavaa mo nisi polokalame tau cybersecurity.

3. **Faatonutonuina o tulaga maaleale.** O nisi manufacturers e iai a latou polokalame faatonutonu mo tulaga maaleale le vulnerability management program e taulai lava i le fonofonoina o tulaga maaleale e maua i totonu poo fafo foi, ma isi mea faaopoopo. O nisi polokalame sili atu ona lelei e tuuaofai ai ni iloiloga o tulaga maaaleale ma o latou mafuaaga, faia ma nisi laasaga e taumafai ai e aveesea se vaega tele o tulaga maaleale[3]. Latou te faatinoina ni polokalame aloaia e faatatau ile faatulagaina o fuafuaga aupito lelei, faatonutonuina o le ituaiga tulaga e iai, faaleleia ma le fuaina o le ituaiga tulaga o iai. Latou te silasila i pulega e le o lelei, o se mataupu tau pisinisi, ae le na'o se mataupu tau le puipuiga. O nei polokalame e ese mai i nisi auala mai polokalame tau ituaiga (quality)ma le saogalemu i nisi o matata.

4. **Ia faaaoga ma le mataala polokalame tau komipiuta o loo matala.** A faaaoga le open source software, ia mataala ile tatalaina o mea o loo aofia ane ai, tagai i le faaaogaina o codes ma le faatumauina o le faalauteleina ma le faatumauina o mea taua o loo aofia ai. Mo se faataitaiga, o le Matagaluega o le Tamaoaiga, Fefaatauaiga ma Fale gaosi oloa a Iapani (METI), ua o latou lomia "Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security."

5. **Ia saunia secure defaults mo developers.** Ia faaaoga le default route e fai ma vaega mautu pe a fai le faalauteleina ole software ina ia saunia ane ai ni poloka saogalemu mo le fausia o mea e developers poo i latou e feagai ma lea matafaioi. Mo se faataitaiga, ona ole taofia o le tuuina o le SQL injection vulnerabilities ua mafua ai mafatiaga i le lalolagi, faamautinoa e faaaoga e developers se potutusi e lelei ona faamautuina ina ia taofia ai lea vaega tele o tulaga maaleale. E faaigoa foi o paved roads poo le "well lit paths", o lenei faiga e faamautu ai le saosaoa ma le puipuiga ma faaitiitia ai mea sese e faia e le tagata.

6. **Faia se aufaigaluega o software developers e malamalama i le tulaga tau le puipuiga.** Faamautinoa e malamalama au software developers i le puipuiga e ala i le toleniina o i latou i faiga aupito lelei e faatatau ile secure coding. E le gata i lea, *ia fesoasoani e faaliliu le aufaigaluega lautele e ala ile faafou o faiga e faafaigaluega ai se tagata ma iloilo le malamalama tau le puipuiga ma le galulue faatasi ma iunivesite, kolisi a komiuniti, bootcamps ma isi faiaoga ina ia lalaga le tulaga tau le puipuiga i totonu o faiga faasaienisi tau komipiuta ma le software development curriculum.

[3] NIST SSDF, PO 1.2, Faataitaiga 2: "Faamalamalama faiga faavae o loo faamaape mai ai mea e manaomia mo le puipuiga o software a le faalapotopotoga, ma ia faamaonia o loo o gatasi ma ki autu ile SDLC(faataitaiga o vasega o faaletonu tau software ua faamaonia i pa, tali atu i tulaga maaleale o loo maua mai i le software sa faalauiloa)."

7. **Faataitai le security incident event management (SIEM) ma le security orchestration, automation and response (SOAR) integration.** Faaopoopo atu i le faia o suesuega i le siomaga (field test), galulue faatasi ma providers o le SIEM ma le SOAR, vaavaalua ai ma tagata faatau filifilia ua malamalama lelei ile faaaogaina e ‘au poo teams o logs e suesue ai nisi mea e masalomia pe oni faaletonu foi tau le puipuiga. O nisi software developers ua o latou oo ile tulaga lea o le tali atu ise faaletonu ma ono afua ai ni log entries poo ni faamaumauga tusitusia e le maua ai se fesoasoani mo reponders e pei ona o latou faatalitalia. A galulue faatasi ma le SIEM ma le SOAR ma a latou faiga tau tekonolosi ma i latou moni o polofesa i lea matata, o le a mafai ai loa e le development team ona faia ni logs e mafai ona faailoa ai pe sa’o pe moni foi ia tala, e sefe ai le taimi ma faaitiitia ai tulaga le mautinoa e faatatau i se mataupu.
8. **Ia o gatasi ma le Zero Trust Architecture (ZTA).** Ia o gatasi le faasoaina o taiala o oloa ma le faataitaiga, o models mai le NIST ZTA ma le CISA Zero Trust Maturity Model. Una’i tagata faatau ina ia tuufaatasi nei manatu faavae i o latou siomaga.

FAIGA E LAGOLAGO AI TULAGA TAU PUIPUIGA O PISINISI

1. **Ia faatino le faamauina o faamatalaga e aunoa ma se totogi faaopoopo.** O auaunaga ile Cloud e tatau ona o latou maumaua'i ile saunia o ni logs mo le teuina o faamatalaga faatatau ile puipuiga, e aunoa ma se totogi faaopoopo e manaomia. O oloa o loo i totonu o se nofoaga e tatau foi ona saunia ai ni logs tau le puipuiga e aunoa foi ma se isi totogi faaopoopo. E le gata i lea, o le oloa e tatau ona faamauina polokalame tau le puipuiga by default talu ai ona e ono le malamalama nisi o tagata faatau i lo latou taua sei vagana ua mae'a se faalavelave. O nei ituaiga metotia e ono manaomia ai le faia o se iloiloga auiliili poo a polokalame tau le puipuiga e tatau ona faia ina ia saunia ai se malamalamaaga tau cyber security, pe faapefea ona faatulaga e se tagata faatau le faia o logs, pe o le a foi le piliota e faamau ai ia logs, lona puipuia ma lona suesueina. I nisi mataupu, o le iloiloga e ono faailoa ane ai se manaoga mo le toe faia o le talosaga ile vaega lea o le log ia fesoasoani ai ia mafai ona faatinoina ma ise tau foi e talafeagai mo le manufacturer. O le galulue fa'atasi ma tagata tomai i fa'alavelave fa'afuase'i (incident response/ IR) e mafai ona fa'atuputeleina le avanoa e aoga ai logs i tagata su'esu'e i lea matata. Silasila ile vaega o loo i le SIEMs.
2. **Aveese lafoga o loo natia.** Lomia se tautinoga o le a leai lava se totogi e faia mo le puipuiga ma tulaga faalilolilo faapea le tuuaofaiga. Mo se faataitaiga, i totonu o le li'o tele lea o tulaga o mea ma le puleaina o le mafai ona ulufale ai(IAM), o loo iai auaunaga e faaigoa o le single sign-on (SSO). O nisi manufacturers e tetele atu a latou totogi i systems ia o le SSO (o nisi taimi e faaigoa o le identity provider). O le uiga o lenei "SSO tax" o se identity lelei ma ole faatonutonuina o le ulufale e le o iai se avanoa mo le tele o SMOs ma faasa ai i latou mai le ausia o se tulaga malosi tau le puipuiga. O nisi auaunaga e tetele atu a latou totogi mo le faatagaina o le MFA mo users. **O le tulaga tau le puipuiga e le tatau ona faia sona tau o se oloa taugata ae ia silasila iai o se aia tatau a le tagata faatau.** Ua finau mai nisi manufacturers o nisi tagata faatau e talosaga mo ia features, ae e taugata atu le tupe e faatumauina ai. O nei finauga e alofia ai le mea moni o ni nai tagata faatau o le a valaau mai e faailoa ni faitioga pe pakeni ae foi, e le o tagata faatau uma e malamalama i penefiti o nei features, ma o features uma ia e iai le tau e totogi e faatumauina ai. Ae e le toatele ni manufacturers tatou te vaai o o latou faia ni tau faaopoopo mo le faaavanoa ane o faamaumauga. O le tau e lagolago ai ia ituaiga tulaga, o loo fausia i totonu o le tau o loo totogi uma e tagata faatau, pei lava foi o le tau ina ia faaaofia ai fusipa'u, nisi o vaega ole taavale, airbags e faasaoina mai ai soifua mai faalavelave.
3. **Opogi tulaga tatala.** Faatino faiga e tatala, aemaise lava i sootaga taatele ma manatu faavae faatatau i tulaga o tagata. Ia alofia manatu faavae e umia e faalapotopotoga pe afai o avanoa mai tulaga lautele.
4. **Saunia meafaigaluega mo faafouga.** O le tele o tagata faatau e tau mumusu e faaaoga le version mulimuli nei o le oloa, e aofia ai le faasoa o features fou ma sili atu ona mautu e pei o fesootaiga i sootaga mautu. E mafai e software manufacturers ona faateleina le faaaogaina e tagata faatau o faafouga e ala i le sauniaina o meafaigaluega e fesoasoani ai ile faaitiitia o tulaga le mautonu ma lamatia. O a matou laisene faia fua mo tagata faatau e faataitai ai upgrades poo faafouga ma mea toe faaleleia ise siosiomaga mo faataitaiga, ose auala e faatupumanatu i tagata faatau.

MANATU FAAVAE 2: Opogi le faamaoni o le faamalamalamaina o mea ma le mafai ona tali manino atu.

FAAMALAMALAMAGA

E tatau i software manufacturers ona mitamita i le kilivaina o ni oloa saogalemu ma mautu, aemaise o le tuueseina mai o latou mai le toatele o isi manufacturers i le komiuniti e fua i lo latou agavaa e faatino mea.

Se'i o tatou tagofia seisi popolega taatele e faatatau i le faamalamalamaina o mea. A faatalanoa e practitioners le faamalamalamaina o mea, e iai le faanaunauga mo lea talanoaga e iai sona faafaigata ona o popolega o loo o latou sauniaina se "faafanua mo le au osofai". Ui i lea, o le faamaoniga aupito sili, o le au osofai o loo sologa lelei pea i latou e aunoa ma sea faafanua, ma o ia ituaiga popolega e tatau ona faasee i le nofoa pito i tua mai le faamalamalamaina o mea, lea e penefiti ai tagata faatau e faatau sa'o mai oloa mai ia oe, tagata faatau e faatauina mai oloa mai se faleoloa siiatoa ma isi ituaiga faleoloa.

O le faamalamalaina o mea e fesoasoani ai ile auaunaga ia faia ni tauaofiaga- i nisi upu, pe o le a se vaaiga i se mea ae "lelei". E fesoasoani i le fesuiaiga o ia tauaofiaga mai lea taimi i lea taimi e tali atu ai i manaoga o tagata faatau, fesuiaiga i faamata'u, poo fesuiaiga o faiga tau tekonolosi. O le faamalamalamaina o mea e fesoasoani ai i manufacturers e itiiti alagaoa e a'oa'o mai ia i latou e umia alagaoa e sili atu. O talanoaga e faatatau i faamatalaga e faasoa atu, e tatau ona faalautele ia sili atu i lo faamata'u, ia aofia ai ma elemeni o lo'o taua atu i lalo.

O le faamalamalamaina o mea e faamalosia ai faaiuga e faatatau ile saogalemu ina ia vave faia lava i le taimi o loo faalautele ai se oloa, ma ia avea o se gaioiga faaauau a taitai o pisinisi aemaise le au inisinia ma le au polofesa i mataupu tau le puipuiga. O le faamalamalamaina o mea e afua ai ona mafai ona tuuina le tali manino atu i totonu o se oloa.

Fia faamauina se faamatalaga i le filifiliga o le upu faamatala o le “radical” i luma o le upu transparency (faamaoni ole faamalamalamaina o mea). O aso nei, e taatele le lomia e software manufacturers o faamatalaga auiliili pe na faapefea ona faalautele ma faamautuina software ae pe faapefea ona faa lava le silafia o a latou polokalame ile faaaogaina o faamatalaga mai lea taimi i lea taimi. I le auaunaga a le software poo polokalame tau le komipiuta, e toalaiti lava nai manufacturers o le a faia ni a latou faataitaiga o le faatulagana o le polokalame tau komipiuta (software). O loo iai ni nai avanoa mo software manufacturers e silasila ai pe faapefea faatulagana e isi faalapotopotoga o a latou polokalame SDLC, ae pe faapefea foi ona taofiofi ia polokalame i siomaga o le tagata faatau ma tetee atu i le au osofai moni lava. O le a manuia le auaunaga tuufaatasi mai le tele o faamatalaga faasoa i ulutala e pei o fuafuaga e fua i le tau o mea tau le puipuiga ua faaleagaina ma ia aveesea ai vasega o tulaga lamatia. O le tali la i nei ituaiga gaioiga, e tatau ai i soo se software manufacturer ona a’oa’o ia iloa tagofia tulaga tau le puipuiga pe a tuu na’o ia. Masalo o le le tuuina o se lafoga tele i luga o features tau le puipuiga, o le saogalemu ma le puipuia e avea la o se nofoaga e totogi (cost centre) ae le o se nofoaga autu tau polofiti, ma o le a penefiti foi ile faamama ai o le avega e ala i le galulue faatasi ma le faamalamalaina o mea.

Matou te fia taula’i i metotia o le a fai ma faatopetope ai le fesuiaiga o le faatamilosaga o le auaunaga tau software. E le o toe mafai ona o matou ausia le faia o nisi galuega faaleleia. Afai o le a o tatou lavasaia faatasi faamata’u e faia mai e fili atamamai ma fetu’utu’una’i, e tatau ona o tatou faamaopoopo ituaiga faamalamalamaina o mea o loo tatou lagonaina ile aso, ae o le a unaia ai foi i luma le auaunaga. O loo iai manufacturers i aso nei o loo latou faa aofia ai nisi o manatu faavae ole secure by design. Pei ona saunoa William Gibson, “o le lumanai, o loo ua iinei, ae pau le mea e le o tutusa lona tufatufaina”. **O le faamaoni o le faamalamalamaina o mea o le a fesoasoani i le tufatufaina o faamatalaga ma sili ona penefiti ai defenders (i latou o loo puipuia mea) nai lo o tatou fili.**

O le faamalamalamaina o mea e mafai ai ona tele se fesoasoani i isi faalapotopotoga ina ia lava tapena a latou SDLCs. O nisi e ono avea ma ni tagata faatau ma i latou e mafai ona inivesi, e mafai ona o latou a’oa’oina nisi mea e tele e faatatau i inivesi ma le faiga o fefaatauaiga e pei ona faia e manufacturers, ma le tulaga o iai le puipuiga o inivesi ia ua faia e tagata faatau. O manufacturers latou te opogi tulaga faamaoni ole faamalamalamaina o mea, o le a o latou tuuina faamatalaga i tagata faatau e fesoasoani e faia ai a latou faaiuga tau faatauga, e le gata ile tau ma features, ae faapea foi i le tulaga tau le puipuiga.

Pei ona galulue malosi faalapotopotoga ina ia faamautu le sapalai ma a latou SDLC, sa vaaia foi ile taimi ua tuanai sa iai i se tulaga lamatia fuafuaga tau le fausiaina o mea i se taimi e lei mamao atu. O le opogi o le faamalamalamaina o mea e tatau ona agai sa’o ai lava i le faalauiloaina faalauaitele o se osofaiga aemaise o mea faaleleia sa toe faia e le kamupani ina ia alofia ai ma iloagofie nisi osofaiga i le lumanai. O le ituaiga faasoaina lea o faamatalaga o le a fesoasoani ai i isi faalapotpotoga e a’oa’oina e aunoa ma se tigaina i le mea lava lea e tasi.

FAAPUPULAINA O LENEI MANATU FAAVAE

Ina ia faapupula mai lenei manatu faavae, e tatau i software manufacturers ona faia ni laasaga e aofia ai mea o loo taua atu i lalo:

FAIGA O LE SECURE BY DEFAULTS

1. **Lomia faamaumauga ua tuufaatasia tau le puipuiga ma ona fesuiaiga.** O nisi o ulutala faataitai e aofia ai le faaaogaina o le MFA e tagata faatau ma administrators ma le faaaogaina o ni aiaiga e lē saogalemu.
2. **Lomia faamaumauga o mea sa faaleleia.** Faamalamalama poo le a le pasene o tagata faatau o loo iai i le version mulimuli nei o le oloa, ma pe o le a o loo e faia e faafaigofie ai faafouga ma nisi faiga faatuatuaina.
3. **Lomia faamatalaga faatatau i faamanuiaga e le'i faaaogaina.** Lolomi faamatalaga tuufaatasia faatatau i le mau faatagana ua faia i tagata faatau aemaise o nisi o faamanatu ma isi suiga ua e faia ile oloa ina ia faaititia ai mea e mafai ona osofaia mai ai. O nei faamanuiaga e lei faaaogaina e ono avea o ni mea lelei mo faamanatu i le administrator, pei foi o le ii ane o fusipa'u.

FAIGA MAUTU O LE FAALAUTELEINA O OLOA

1. **Faatu ni faiga faatonutonu faalotoifale tau le puipuiga.** Ua tele kamupani ua o latou vaai i le lelei o le tuuina o a latou faamatalaga (data) i cloud providers (I latou e sauniaina mea e teu ai faamatalaga). O le taimi nei la ua agai ia i latou ia faiga a le au osofai. E tatau i providers a le Software as a Service (SaaS) ona lomia ni faamaumauga patino ile faatonutonuina o a latou galuega faalotoifale. Mo se faataitaiga, o providers a le SaaS e tatou ona o latou lomia faamaumauga e faatatau i le faasoaina faalotoifale o phishing-resistant MFA, like Fast Identity Online (FIDO) authentication. O le mea moni, e tatau ona mafai ona o latou faapea mai e leai se tagata faigaluega e mafai ona tagofia faamatalaga maaleale o tagata faatau ma isi faamatalaga e aunoa ma le faamaoniaina e ala i le phishing-resistant MFA.
2. **Lomia faataitaiga o faamata'u tetele.** E amata lava oloa a le secure by design i threat models poo faataitaiga o ni faamata'u ma faamatala ai mea o loo taumafai i latou na faia ina ia puipuia mai ai ae pe puipui foi mai ia ai. O effective threat models e faailoaina e ala i auala e tutupu ai ni osofaiga ile gaoā, ma e tatau ona ufitia uma ai le enterprise ma siosiomaga faalautele, ae le gata I lea o le auala o loo fuafua software manufacturers e faaaogaina ai i siosiomaga o tagata faatau
3. **Lomia tautinoga auiliili e faatatau i le secure SDLC.** O manufacturers o loo mulimuli ile NIST,SSDF ma isi faavaa talitutusa, o loo latou galulue agai i se tulaga faalauteleina mautu o le olaga o le software. O le lomia o se faamatalaga maumaututū o ituaiga faatonutonuga o loo fua i ai galuega a le manufacturer, ae pe o a foi oloa, o le a faailoa ai se tulaga ua gaua'i iai ile usitaia o ituaiga faiga aupito sili ma saunia ai se tulaga siitia i le faatuatuaina o a latou tagata faatau. O nisi taumafaiga ua faamaoniaina e aofia ai le Israel Cyber Supply Chain Methodology, mo se faataitaiga.
4. **Opogi tulaga maaleale ma lona faamalamalaina.** Lomia se tulaga gaua'i e faamautu o le a lomia tulaga maaleale ua iloa o se oloa, o ni CVE entries o loo sa'o ma ua mae'a. E matuai sa'o lenei mo le Common weakness enumeration field lea e iloa ai le mafuaaga tonu o tulaga maaleale. O le tele lava o le sa'o ma le mae'a lelei o le database a le public CVE, o le tele foi lea o le avanoa e mafai ai e le auaunaga ona tulimataia pe faapefea ona faamautu oloa, ae poo fea foi ituaiga o vasega o tulaga maaleale e mafai ona taofia. Ae ui i lea, ia faaeteete i le faaosoosoga ina ia faitau CVEs o se fua e le lelei, ona o ia numera o se faailoa foi lea o le iloiloina o se tulaga tau le soifua maloloina ma suesueina ai foi le komiuniti. A'o faatino e manafacturers se filosofia a le secure by design, e foliga e ono mafai ona faapea o le latou faitauga o le CVE o le a agai i luga ona o nisi o lavelave ua maua atoa ma le faaitiitia o tulaga maaleale i le code o loo iai. E tatau i manufacturers ona lomia se iloiloga o ni tulaga maaleale sa iai i le tuanai, e aofia ai ma nisi o faiga sa faia e tali atu ai i ituaiga vasega eseese o tulaga maaleale. Mo se faataitaiga, afai o se pasene tele o CVEs a se kamupani e iai se sootaga i le cross-site scripting (XSS), ole faamaumauina o le iloiloga o le faapogai o le faaletonu (pei o le faasee atu ile faavaa tau upega tafailagi e taofia ai le XSS), ma o le iuga la o le a faailo atu ai i tagata faatau o le a le aafia i latou i le ituaiga vasega o tulaga maaleale lea sa malamalama lava mai tausaga e tele, o se faiga e faaitiitia ai lea tulaga.
5. **Lomia Software Bills of Materials (SBOMs).** E tatau i manufacturers ona fai faatonuga o le faasologa o le gaosia ma le tufatufaina o oloa (supply chains). E tatau i faalapotopotoga ona fausia ma

faamautuina SBOMs [2] mo oloa taitasi, talosagaina faamatalaga mai a latou suppliers, ma ia faamautinoa le avanoa o SBOMs mo tagata faatau ma i latou e faaaogaina le auaunaga. O le a fesoasoani lea i le faailoaina o le iai pea o le malamalamaaga i mea o loo faaaogaina ile fausiaina o a latou oloa, lo latou agavaa e tali atu ai pe afai e aliae se tulaga maaaleale fou o se tasi o modules i le supply chain. Mo faamaumauga, o le Matagaluega tau Tamaoaiga, Fefaatauaiga ma Fale Gaosi Oloa (METI) sa o latou lomia le "Guide of Introduction of Software Bill of Materials (SBOM) for Software Management." O le faamalamalamaina o mea e tatau ona faasoo ane i le firmware o loo tuuina i totonu o masini ma le faamatalaga ma modules o loo faaaoga ile AI/le masini o loo fai ma faataitaiga (ML). I tua atu o le fesoasoani i le faia o ana faaiuga tau faatau ma agavaa faatatau ile faagaioia o mea, e tele se matafaioi taua a le SBOMs e faia ile siomaga o mea e matau ai ma tali atu i ni osofaiga ogaoga ile supply chain.

6. **Lomia se tautinoga patino o faiga faavae i tulaga maaleale.** Lomia se faiga faavae o tulaga maaleale ina ia (1) faataga ai le faataitaia o oloa o loo ofoina e le manufacturer atoa ma aiaiga o ia ituaiga faataitaiga, (2) saunia se faatamilosaga saogalemu faaletulafono mo gaioiga o loo faia pea e o gatasi ma le faiga faavae, aemaise (3) faataga ai le faalauiloaina faalauaitele o tulaga maaleale ile mae'a o se taimi sa faatulaga. E tatau i manufacturers ona faatino se iloiloga o le faapogai o le faaletonu e tusa ma tulaga maaleale sa maua, ma i lona tulaga aupito tele, ia faia ni gaioiga e aveesea ai vasega eseese o tulaga maaleale. Taga'i ane i le CISA's Vulnerability Disclosure Policy Template mo se faamaninoga o le gagana.

FAIGA E LAGOLAGO AI TULAGA TAU PUIPUIGA O LE PISINISI

1. **Ia faaigoa faalauaitele se lagolago sinia mo le secure by design.** I le tele o le mau faalapotopotoga, o le puipuiga (pei ole tulaga lelei) o loo faamamafa lava i ‘au o feagai ma masini (technical teams) e le lava lo latou agavaa e faia ai ni suiga e faaleleia ai le saogalemu o oloa. O le faailoaina faalauaitele o le suafa o se tagata sinia o le pisinisi o le a vaaia le polokalame o le secure by design, o le a suia ai le puipuiga o oloa i se popolega mo le pito i luga o le pisinisi.
2. **Lomia se faafanua o le secure by design.** E tatau i manufacturers ona faamaumau suiga ua faia i le SDLC ia faaleleia le puipuiga o tagata faatau, e aofia ai ma faamaumauga e faatatau i lipoti mai le faataitaiga na faia i le siomaga, gaioiga na faia e aveesea ai tulaga maaleale eseese, ma isi aitema ua lisi atu i isi manatu faavae. E pei ona iai ile mataupu e faatatau i le taumafaiga e faaleleia le tulaga o mea, polokalame faaleleia o tulaga tau le puipuiga,e iai ona vaega eseese o fuafuaga, faatonutonuga ma le faaleleia. Ile agaga fia faailoa ae le o le ta‘uina, o le lomia o le faafanua ma faamaumauga o loo aofia i tua mai o nei vaega eseese uma, o le a fausia ai se loto tele o oloa e secure by design. I le mae‘a ole ausia o le agai i luma, e tatau i manufacturers ona faamanino ma faamalamalama lelei i ni lipoti. O le faia o lea tulaga o le a le nao le faailoa atu ai o le gaua‘i i manatu faavae o le secure by design, ae o le a faaosofia ai foi isi e faaaoga polokalame tali tutusa e ala i le faailoaina o ni faamaoniga o iai.
3. **Lomia se faafanua o le saogalemu o le memory.** E mafai e manufacturers ona faia ni laasaga e aveese mai ai se tasi o vasega o tulaga maaleale e ala i le feaveaia o oloa o loo iai nei ma le fausia o oloa fou e faaaoga ai gagana saogalemu mo le teuina o mea. E ui e ono le mafai ona faatino lenei tulaga i mataupu uma, ae e mafai ona silasila le manufacturer i nisi o talosaga faalautele ma gagana saogalemu e faaaogaina ae le o le toe fai atoa o le talosaga. E mafai foi ona aofia ai ma le faatinoina o faafouga a manufacturers i le faafaigaluegaina, toleniina ma le iloiloina o codes atoa ma isi fuafuaga faalotoifale, aemaise o auala o loo latou fesoasoani ai ile komiuniti ina ia faatino lea tulaga.
4. **Lomia le iuga.** A‘o faafou a latou SDLC e faaaofia ai filosofia a le secure by design, ole a maua e faalapotopotoga ni nai manumalo poo faamanuiaga laiti, nisi faamanuiaga tau meafaitino ma nisi foi faatuai e lei faatalitalia. O le tauaaoina o a latou faamanuiaga ia faalotoifale ma mea ua avea ma poloka ile auala, e mafai ai e le auaunaga ona a’oa’oina mai i iuga.

MANATU FAAVAE 3: Lead from the Top

FAAMALAMALAMAAGA

E ui o le atoaga o le filosofia o le “secure by design”, o le mea o loo faamalosia ai mo le saogalemu o tagata faatau, e amata lava ae lei oo i le vaega o le oloa e amata faatulaga ai (design phase). E amata i ni moemitiga faapisinisi ma ni fuafuaga mautinoa ma le mautinoa atoa ai ma le iuga o loo faatalitalia. Sei vagana lava ua ave le faamuamua a taitai sinia o le pisinisi i tulaga tau le puipuiga, ma amata ai nisi o mea e faamalosia ai, aemaise o le faataitai i se aganuu i se tulaga lautele ina ia avea le tulaga tau le puipuiga o se mea e manaomia ona iai ile design, ona faatoa ausia lea ole iuga aupito lelei.

E ui o le malamalama aupito taua e manaomia mo le faatinoina o le tulaga lea, e taua tele i le puipuiga o le oloa, e le o se mataupu e tuuina tasi lava i le aufaigaluega i mataupu tau masini. O se mea e ave iai le faamuamua a le pisinisi ma e tatau lava ona amata mai le amataga.

O nisi tagata ua manatunatu poo opogi e software manufacturers o uluai manatu faavae e lua ma saunia mai ai ni tulaga taua ma uiga, ae pe e ono manaomia foi le manatu faavae lona tolu? O le faatuina o se visiona a le kamupani, misiona, talitonuga ma le aganuu, o le a aafia ai le oloa, ma o ia elemeni e fai si mamafa o le pito i luga. Ua o tatou vaaia lea tulaga i isi auaunaga lea ua faia iai ni galuega faaleleia i tulaga tau le saogalemu ma ituaiga. Tusia e le tagata ta‘uta‘ua o J.M. Juran:

> ***O le mauaina o ituaiga taitai lelei e manaomia ai pulega i luga ane e latou te faatonutonuina lea tulaga ina ia puleaina mo tulaga lelei. I kamupani sa o latou maua taitaiga lelei, na taitaia lelei lava e pulega i luga ane ia taumafaiga. Ou te le o iloaina nisi tulaga ese. [3]***

Matou te talitonu o le tulaga tau le puipuiga o se vaega o ituaiga o se oloa.
E avea loa le tulaga tau le puipuiga ma le ituaiga o ni mea (quality) e tatau lava ona faatino e le pisinisi nai lo nao se gaioiga e tuu patino atu i le aufaigaluega i mataupu tau masini, o le a vave loa ona mafai ona tali atu faalapotopotoga i manaoga tau le puipuiga o a latou tagata faatau ma o le a lelei faasoa foi. Ae le gata i lea, o le inivesi o meafaitino manaomia e faamautu ai le puipuiga o software/polokalame o le komipiuta, o se tulaga faapisinisi e ave iai le faamuamua mai lava i le amataga, o le a faaitiitia ai tau faaumiumi o le totogiina o le tagofia o faaletonu tau software, ma iu ai ina faaititia tulaga lamatia ile atunuu atoa.

O le auala lava foi lea e tasi ua faatino ai e le au taitai o latou polokalame, corporate social responsibility (CSR), o loo faatupulaia pea le silafia faatatau i pulega o falefaigaluega tetele, e aofia ai ma software manufacturers, e tatau ona gaioi i seisi gaioiga ola ile taitaia o polokalame tau cybersecurity. O le faaupuga, corporate cyber responsibility (CCR) e iai nisi taimi e faaaoga e faamatala ai le aikia fou lea ua aliae mai.

FAAPUPULAINA O LEA MANATU FAAVAE

Ina ia faapupula atu lenei manatu faavae, e tatau i software manufacturers ona faia ni laasaga e aofia ai mea o loo taua i lalo:

1. **Faaaofia faamaumauga o le polokalame o le secure by design i lipoti faaletupe a ofisa tetele.** Afai o le manufacturer o se kamupani fefaatauai lautele, faaopoopo se vaega i lipoti uma faaletausaga e agai sao i taumafaiga a le secure by design. E taatele mo lipoti faale tausaga o se taavale ona aofia ai vaega e faatatau i le saogalemu o avetaavale ma le pasese, e aofia ai ma faamatalaga e faatatau i komiti e feagai ma tulaga tau le saogalemu. O le faamaumauina o le polokalame o le secure by design i se lipoti faaletupe o le a faaāta ai o loo iai le sootaga o loo faia e le faalapotopotoga i le tulaga tau le puipuiga o tagata faatau ma le iuga o lipoti faaletupe a ofisa tetele ma e le o faaaogaina mai se faaupuga mai mea tau le maketiina ona o loo taatele.
2. **Saunia lipoti masani e ave i le fono faatonu.** E lipoti le Ofisa sili mo faamatalaga tau le puipuiga, Chief Information security officer (CISO) ile fono faatonu a ofisa tetele aemaise lava le aofia ai ma faamatalaga e faatatau i fuafuaga ua faia nei mo polokalame tau le puipuiga, faamata'u ma ni tulaga ua masalomia pe faamaonia ai tulaga tau le puipuiga, atoa ma isi faafouga ua ogatotonu tonu i le tulaga o le puipuiga ma le soifua maloloina o le kamupani. Faaopoopo atu i le mauaina o faamatalaga e faatatau i le tulaga tau le puipuiga o le ofisa, e tatau i le fono faatonu ona talosaga ni faamatalaga e faatatau i le saogalemu ma aafiaga o le oloa i le puipuiga o le tagata faatau. E le tatau i fono faatonu ona silasila tasi lava i le CISO, ae tatau ona taga'i i isi sui o le pulega a le kamupani latou te tuuina i lalo lamatiaga o iai.
3. **Faamalosia le ofisa sili o le secure by design.** E iai le eseese tele i le va o se faalapotopotoga e iai avanoa e aofia ai foi i le 'au o le aufaigaluega i masini, le tulaga sinia e tautala ai "executive buy-in", ma faalapotopotoga e pulea e taitai faapisinisi le tulaga tau le puipuiga e faaaoga ai le faasologa masani o pisinisi. O le faaupuga "executive buy-in" ua faapea mai e tatau i se tagata ona o latou faatau le aikia poo le manatu o se polokalame faatatau i le saogalemu o le tagata faatau ae le o se moemitiga faapisinisi a le vaega pito i luga. E tatau ona faamalosia le executive ina ia iai se aafiaga i inivesi mo le oloa ina ia ausia ai tulaga tau le puipuiga o tagata faatau.
4. **Amata fausia ni mea e faamalosia ai le lotoifale.** A'o tomanatu ai ia aua ne'i amataina pe faia ni mea le talafeagai e faamalosia ai, faatusatusa systems o loo maua ai ni taui ina ia faaleleia ai le puipuiga mo tagata faatau ma ia fetaui foi ma isi amioga ma iuga e tele le taua. Mai lava i le pulega a le secure by design seia oo i le pulega o le oloa, faalauteleina o le software, lagolago, faatauga, tulaga faaletulafono, ma isi faalapotopotoga, e lalaga le tulaga tau le puipuiga mo tagata faatau i totonu o le sailia o tagata faigaluega, faalauiloa,totogi, ponesi, nisi tulaga tau oloa ma isi foi ituaiga faiga i le faatamoeina o le pisinisi. Mo se faataitaiga, afai e faatuina se aiaiga mo le faalauiloaina o software developers, e aofia ai ma manatu faaalia mole faaleleia o le tulaga o le saogalemu o le oloa, aemaise nisi o aiaiga e pei o le uptime, faafiafiaga ma le faaleleia o features.
5. **Amataina se pulega a le secure by design.** I nisi o auaunaga, e taatele i se faalapotopotoga ona o latou amataina se pulega tutotonu o ituaiga, (central quality council), ma ia tuuina sui e feagai ma tulaga ia i vaega autu eseese o le pisinisi. O le faaaofia o sui e i le ogatotonu ma sui e tufa solo, o le a galulue ai ia kulupu e faaleleia le ituaiga o oloa faatusa i le pulega i luga atu ma a latou moemitiga ae o loo maua ai foi faamaumauga mai le lotoifale o le faalapotopotoga. E tai faapea foi la, o se pulega a le secure by design o le a o latou faaleleia le tulaga tau le puipuiga agai i moemitiga a le secure by design i le faalapotopotoga atoa.
6. **Amata ma faataamilo pulega mo tagata faatau.** O le toatele o software manufacturers e iai a latou pulega o tagata faatau e aofia ai tagata faatau mai vaipanoa eseese, auaunaga i soo se tele. O nei pulega e mafai ona o latou saunia se vaega tele o faamatalaga e faatatau i manuia ma luitau e feagai ma tagata faatau i le faasoaina o oloa a le kamupani. Faatulaga le faasologa o le fonotaga a le pulega ia aofia ai mataupu e tagofia ai le saogalemu o le tagata faatau, tusa pe le o aofia i le pito i luga o manatu o sui auai. Silasila poo fea e lipoti iai le pulega a tagata faatau ma pe faapefea foi ona fai i sui auai mo so latou silafia i le tulaga tau le puipuiga o le oloa ua faasoaina. Mo se faataitaiga, pe iai se tulaga manatu faapito o le pulega agai i le maketiina ma le faatauina ole oloa, poo le pulega foi o le oloa? O sui sinia o le secure by design e tatau ona o latou fesoasoani e tau aveese mai ia feutanaiga a tagata faatau ae faafesootai i latou ma isi elemeni i lenei pepa e pei o le siomaga mo suesuega.

METOTIA O LE SECURE BY DESIGN

O le Secure Software Development Framework (SSDF), lea foi e faaigoa o le National Institute of Standards and Technology's (NIST) SP 800-218, o se vaega autu o polokalame tau komipiuta (software)e maualuga lona tulaga e mafai ona tuufaatasia i vaega eseese ole faalauteleina o le olaga o le software (SDLC). O le taumulimuli i nei faiga e mafai ai ona fesoasoani i software producers ina ia sana iai ni aafiaga ile sailia ma le aveesea o tulaga maaleale i software ua faamatuu atu, faaitiitia aafiaga e ono iai o le faaaogaina o tulaga maaleale, ma tagofia le faapogai o le autu o le faafitauli o tulaga maaleale e alofia ai le toe tulai mai i le lumanai.

O ofisa o loo tuufaatasia lenei tusitusiga ua o latou unaia le faaaogaina o metotia a le secure by design, e aofia ai ma manatu faavae o loo agai sa'o i faiga ia o le SSDF. E tatau i software manufacturers ona faalautele se faafanua tusitusia e faaaoga ai nisi faiga faalautele ole software a le secure by design i vaega uma o loo faaaoga ai. O mea o loo taua i lalo o se lisi e le'i ma'ea atu o faafanua ma ona faiga aupito sili.

- **Memory safe programming languages (SSDF PW.6.1).** Faamuamua le faaaogaina o gagana saogalemu mo le teuina o mea i soo se mea e mafai ai. E faataua e ofisa o loo tuufaatasia lenei tusitusiga o nisi o faiga patino i le memory e ono fesoasoani i metotia pupuu mo le teuina o faamaumauga mo talaaga. O faataitaiga e aofia ai mea faaleleia i le gagana C/C++, faaitiitia o vaega o hardware, tagofia le faatulagana o avanoa (ASLR), le silafia ile faatonutonuina o agavaa (CFI) ma le nenefu. Ae peitai, o loo iai se finagalo ua faatupulaia ua ioeina ai o le faaaogaina o gagana saogalemu tau polokalame e mafai ona aveesea ai leisi lea faaletonu, ma e tatau i software manufacturers ona vaavaai i nisi auala e faaaoga ai ia mea. O nisi faataitaiga o le modern safe languages poo gagana saogalemu, e aofia ai C#, Rust, Ruby, Java, Go, and Swift. Faitau i le pepa o faamatalaga a le NSA's memory safety mo nisi faamatalaga.
- **Secure Hardware Foundation (Faavae Mautu o Meafaitino).** Ia tuufaatasi architectural features e mafai ai ona faaaoga le memory protection, faapei o mea o loo faamatala i le poo le Capability Hardware Enhanced RISC Instructions (CHERI), e mafai ai ona faalautele faatonuga tau hardware, hardware Instruction-Set Architectures (ISAs), aemaise isi features e pei o le Trusted Platform Modules ma le Hardware Security Modules Mo nisi faamatalaga, asiasi i le upega tafailagi a le Iunivesite o Cambridge CHERI webpage.
- **Secure Software Components (Tulaga mautu o mea o loo aofia i le polokalame tau komipiuta)(SSDF PW 4.1)** Ia maua ma faamautu mea tau software (faataitaiga, software libraries, modules, middleware, faavaa) mai pisinisi ua mae'a faamaonia ma isi lava third party developers e faamautinoa ai le malosi o le puipuiga i tulaga maaleale, ma ia faamautinoa ai tulaga saogalemu i oloa o software mo tagata faatau.
- **Web template frameworks (SSDF PW.5.1).** Faaaoga templates o faavaa o loo faatino ai automatic escaping mo le tagata e faaaogaina ia alofia ai osofaiga i le upega tafailagi e pei o le cross-site scripting.
- **Parameterized queries (SSDF PW 5.1).** Faaaoga parameterized queries ae le o le faaaofia ai o le user input in queries, ina ia alofia ai osofaiga, SQL injection attacks.
- **Static and dynamic application security testing (SAST/DAST)** (SSDF PW.7.2, PW.8.2). Faaaoga meafaigaluega ia (tools) e iloilo ai le product source code ma le ituaiga amioga a le talosaga ina ia matau ai ni faiga e le o sa'o ona fai. O nei meafaigaluega e aofia ai ma ni mataupu e amata mai i le le lelei o le puleaina o vaega o faamaumauga (faataitaiga, unescaped user input e oo ai ile SQL injection). O meafaigaluega a le SAST ma le DAST e mafai ona faa aofia i totonu o le faiga o le faalauteleina ma okometi ai ona faatamoe o se vaega o le faalauteleina o se software. E tatau i le SAST ma le DAST ona faamālō i isi ituaiga faataitaiga, e pei o le unit testing ma le integration testing, e faamautu ai o loo o gatasi oloa ma le ituaiga puipuiga o manaomia. Afai ae maitauina lea faaletonu, e tatau i manufacturers ona faatino loa le iloiloina o le faapogai o le faaletonu ina ia mafai ona tagofia ai ma tulaga maaleale.

- **Iloiloga o le code** (SSDF PW.7.1, PW.7.2) Finau e faamautinoa o le code ua tuuina i totonu o oloa o loo agai sa'o i metotia faatonutonu e pei o iloiloga a tagata(peer review o loo faagasolo e isi developers poo le "error seeding".
- **Software Bill of Materials (SBOM)** (SSDF PS.3.2, PW.4.1). Faaaofia ai ma le amataina o le SBOM[4] ina ia maua ai sina vaaiga i totonu o seti o software lea e agai sa'o i totonu o loa
- **Polokalame o tautinoga patino i tulaga maaleale.** (SSDF RV.1.3). Ia faatuina polokalame o tautinoga patino (disclosure programs) e faataga ai ona lipoti le ausuesue e lipoti ni tulaga lamatia o iai ma maua ai se tulaga saogalemu faaletulafono pe a faia lea tulaga. O se vaega la o lea mea, e tatau ai i suppliers ona faatuina ni faiga e faamautinoa ai le faapogai o faaletonu o tulaga maaleale ua maua. O ia ituaiga faiga e tatau ona aofia ai foi ma le faamautuina pe faaaoga foi o se faiga a le secure by design i lenei pepa (poo nisi faiga e tali tutusa) e ono taofia ai le faalauiloaina o tulaga maaleale.
- **CVE completeness.** Faamautu o loo aofia ai ma le faapogai o faaletonu poo le vaivaiga aupito taatele (CWE) ina ia faataga ai le iloiloga e faia i le auaunaga atoa e faatatau i faaletonu o le faatulagana o le software. A'o faamautu o loo sa'o uma ma mae'a lelei CVE uma, ia fai se taimi faaopoopo, e faataga ai disparate entities e maitau suiga tau le auaunaga e mafai ona penefiti uma ai le manufacturer ma le tagata faatau. Mo nisi faamatalaga e faatatau i le puleaina o tulaga maaleale, tagai i le taiala a le CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) guidance.
- **Puipuiga-i lona tulaga loloto.** Ia faatulaga infrastructure ina ia aua nei avea le lamatia o se tulaga tau le puipuiga se tasi e fai ma mafuaaga o le lamatia o le system atoa. Mo se faataitaiga, faamautinoa o loo saunia faamanuiaga mo i latou e faaaogaina le auaunaga (user priviledges) ma ia mafai ona tagofia lisi tau faatonutonu e faaitiitia ai aafiaga o le account ua lamatia. E le gata i lea, o ituaiga tomai o le software sandboxing e mafai ona faanofoesea ai se tulaga maaleale ina ia faaitiitia ai le lamatia ai o le talosaga atoa.
- **Ia faamalieina Moemitiga o Cybersecurity Performance(CPGs).** Faatulaga oloa e ausia faiga faavae tau le puipuiga. O moemitiga mo le Cybersecurity, CISA's Cybersecurity Performance Goals ua faataoto ane ai tulaga autu o le cybersecurity e tatau ona faatino e faalapotopopoga. Faaopoopo atu i lea, mo nisi auala e faamalosia atili ai le tulaga o lau faalapotopotoga, silasila i le UK's Cyber Assessment Framework lea e faasoa mai ai mea e tali tutusa ma le CISA's CPGs. Afai e le mafai ona ausia e se manufacturer CPGs—pei o le le manaomia o le phishing-resistant MFA mo ana tagata faigaluega—e le mafai la ona vaaia i latou ia o kilivaina oloa a le secure by design.

Ua maitauina e ofisa o loo tuufaatasia lenei tusitusiga o nei suiga o ni fesuiaiga taua tele i le tulaga o se faalapotopotoga. O lea la, o le faailoaina mai e ao ona ave i ai le faamuamua e fua i le tulaga ogaoga, faigata ma aafiaga o le pisinisi. O nei faiga uma e tatau ona faailoa foi mo software fou ma faalautele ai lava lea e aofia atu ai ma nisi mataupu ma oloa. I nisi mataupu, o le tulaga ogaoga ma le tulaga lamatia o se oloa, e ono manaomia ai se faatulagana faatopetope e faatino ai ia faiga. I nisi, o faiga ia e mafai ona faailoa i se legacy codebase ma fai lava ma toe faatumauina.

[4] O nisi o ofisa o loo tuufaatasia lenei tusitusiga o loo latou vaavaai i nisi faiga e ese mai e faamautuina ai le tulaga mautinoa o loo saogalemu le software supply chain.

METOTIA A LE SECURE BY DEFAULT

Faaopoopo atu i le faaaogaina o faiga faalautele a le secure by design, ua fautuaina e ofisa o loo tuufaatasia lenei tusitusiga, software manufacturers ia faamuamua le faatulagaina o le secure by default i a latou oloa. E mafai ai ona finau e faalelei oloa ia o gatasi ma ituaiga faiga ia pe a toe faafou. Mo se faataitaiga:

- **Aveese default passwords.** E le tatau ona aumai oloa o iai ni default passwords o loo faasoaina faasoloatoa. Ina ia aveese default passwords, e fautuaina e ofisa o loo tuufaatasia lenei tusitusiga le manaomia e oloa o administrators ia o latou faatulaga se password malosi ile taimi e amata faatuina ma faatulaga ai le oloa ina ia mafai ona lafo le oloa faatasi ma sona password malosi mo masini taitasi.
- **Faamalosia le faia o le multifactor authentication (MFA) mo i latou e faaaogaina.** Ua tatou maitauina o le tele o faasoa e faia a enterprises e puleaina lava e administrators e lei faia ni puipuiga mo a latou accounts faaaoga ai le MFA. Faapea la o administrators o nisi o loo taula'i atu iai ni osofaiga, e tatau la ona faatulaga oloa ia MFA opt-out ae le o le opt -in. I se isi itu, o le system e tatau ona fai ma faamanatu i le administrator ina ia lesitala i le MFA sei vagana ua mae'a ona faataga e faaola i lana account. O le NCSC a Netherlands e iai ana taiala e tali tutusa ma le CISA's, asiasi i le latou Mature Authentication Factsheet mo nisi faamatalaga.
- **Single sign-on (SSO).** O talosaga mo faamatalaga tau tekonolosi (IT applications) e tatau ona faatino ai le lagolago mo le single sign on tauala atu i le modern open standards. O faataitaiga e aofia ai le Security Assertion Markup Language (SAML) poo le OpenID Connect (OIDC.) E tatau ona faaavanoa atu lea agavaa by default ae leai se totogi faaopoopo.
- **Secure Logging.** Ia saunia faamaumauga tulaga maualuga mo tagata faatau e aunoa ma se isi totogi faaopoopo poo se isi fetuunaiga faaopoopo. E taua tele faamaumauga ua mae'a sueina mo le mataituina ma le faasee ese atu o ni tulaga e ono aafia ai le puipuiga. E taua foi i le taimi o se suesuega i se mataupu tau le puipuiga ua masalomia pe ua faamaonia foi. Silasila i ni faiga aupito lelei e pei o le saunia o se tuufaatasiga faigofie faatasi ma faamatalaga tau le puipuiga ma systems mo le puleaina o se faamoemoe faatasi ma le tagofia o le polokalame o le application programming interface (API) e faaaoga ai taimi (UTC), le taimi masani faatulagaina o le sone, ma isi ituaiga o le faiga o faamaumauga.
- **Software Authorization Profile.** E tatau i software suppliers ona o latou saunia mai ni fautuaga e faatatau i ni matafaioi faatagaina ma mea ua faaagana i ai lona faaaogaina. E tatau i manufacturers ona faaaofia ai ma se fautuaga tusitusia e faailoa ai i tagata faatau le faatupulaia o se tulaga lamatia pe afai latou te agai ese ma le faatagana ua fautuaina atu mo latou. Mo se faataitaiga, o fomai tau togafitiga e mafai ona o latou vaai i faamaumauga o gasegase, peitai o le tagata e faatulagaina le polokalame tau togafitiga e faatapulaa lona tagofia o faamatalaga patino e manaomia mo le faia o se appointment.
- **Forward-looking security over backwards compatibility.** Ua maitauina soo, o features ua faaigoa backwards-compatible legacy features o loo aofia atu, ma e masani foi ona faataga ona faaaoga, i oloa e ui e ono mafua ai ona tuuina se oloa ise tulaga lamatia o tulaga tau le puipuiga. Ia faamuamua le tulaga tau le puipuiga nai lo backwards compatibility, faamalosia 'au tau le puipuiga ia aveesea ai ni features e le mautinoa tusa lava pe afua ai ni suiga e faaletonu ai.
- **Saili ma faaitiitia le tele o le "taiala faamalosi".** Faaitiitia le tele o "hardening guides" poo taiala faamalosi o loo aofia atu i oloa ma ia finau e faamautu o le tele o le a o'o ina faaitiitia mai lea taimi i lea taimi ae ua amata faamatuu atu foi lea o nisi ituaiga fou o le software lea. Tuu faatasi mea o loo aofia i le "taiala faamalosi" e avea ma default configuration o le oloa. Ofisa o loo tuufaatasia lenei tusitusiga

maitau o taiala faamalosi ua faapupuuina e mafua mai i faiga faapaaga o loo faaauau pea ma nisi o tagata faatau o loo iai ma e aofia ai ma taumafaiga a le tele o ‘au o loo galulue i oloa (product teams), e aofia ai ma user experience (tomai mai le sa faaaogaina) (UX).

- **Silasila i tulaga o le malamalama mai le tagata na faaaogaina le auaunaga (user) e tusa o le faatulagana o tulaga tau le puipuiga.** O soo se faatulagana fou lava e faatupulaia ai le avega ia i latou e faaaogaina le oloa ma e ao ona vaavaai i ai faatasi ma le penefiti a le pisinisi e maua mai ai. O le tulaga sili, o le aua le iai o se faatulagana (setting); ae, o le faatulagana aupito mautu e tatau ona tuufaatasi i totonu o le oloa by default. Afai e mafai ona toe faatulaga, e tatau lava ona matuai mautinoa le mautu o le default option pe a faatusa i faamata‘u taatele.

O ofisa o loo tuufaatasia lenei tusitusiga ua o latou faataua nei suiga e ono iai ni aafiaga ile faafaigaluegaina o le software. O lea la, e taua tele le sao o le tagata faatau i le faapaleniina o finagalo faaalia i tulaga tau le faagaioia o galuega ma le tulaga tau le puipuiga. Matou te talitonu o le faalauteleina o ni faafanua tusitusia ma le lagolago a ofisa sinia e faamuamua ai nisi o nei manatu i oloa aupito taua a le faalapotopotoga, o le uluai laasaga lea i le faasee atu agai i se faiga faalautele e mautu mo le software. E ui e taua le sao o le tagata faatau, ua o tatou maitauina foi nisi o mataupu taua ua le manao ai le tagata faatau e faataga ona faaaoga tulaga ua toe faaleleia, masani lava i sootaga tau aiaiga faaletulafono. E taua tele mo manufacturers ona o latou amataina ni mea uiga e faamalosiau ai mo tagata faatau ina ia tumau ma ia aua foi nei faatagaina i latou e tumau ai pea i se tulaga lamatia mo se taimi e lē mailoa.

TAIALA FAAMALOSI VS TAIALA LUSI (LOOSENING)

O Taiala faamalosi e ono mafua mai le lē lava o tulaga faatonutonu tau le puipuiga mo se oloa mai lava i le amataga o lona faalauteleina. Ona o lea, e mafai ai foi e taiala faamalosi ona avea o se faafanua mo fili i le faasinoina ma le faaaogaina o features e lē mautinoa. E taatele mo le tele o faalapotopotoga lo latou le iloa o taiala faamalosi, o le ala lea e tuu ai a le faatulagana o a latou masini i se tulaga lē mautonu. O se tasi o model (faataitaiga) o se loosening guide poo se taiala lusi e tatau ona suitulaga atu i taiala faamalosi ma faamalamalama ai suiga e tatau ona faia e users poo tagata e faaaogaina le oloa, ae o loo lisi atu ai foi ma nisi o lamatiaga i le puipuiga e ono iai. O nei taiala e tatau ona tusia e security practitioners e mafai ona o latou faamalamalamaina le fefaatauaiga i ni gagana manino ia faatupulaia ai le avanoa o le faaaogaina sao o nei taiala.

Ese mai i le faalauteleina o taiala faamalosi lea e lisi atu ai metotia mo le faamautuina o oloa, ua fautuaina e ofisa o loo tuufaatasia lenei tusitusiga, software manufacturers ina ia faasee atu i le secure by default ma ia saunia atu ”loosening guides”, (taiala lusi) O nei taiala e faamalamalama ai le tulaga lamatia o faaiuga fai a le pisinisi i gagana faigofie, malamalamagofie, ma e mafai ai ona siitia le silafia o se faalapotopotoga i tulaga o lamatiaga ma le faalavelave mai o osofaiga ogaoga mai le initaneti. O fefaatauaiga tau le puipuiga e tatau ona faamautuina e se tagata sinia a se tagata faatau , ia faapaleni ai le tulaga tau le puipuiga ma isi manaomiaga faa pisinisi.

FAUTUAGA MO TAGATA FAATAU

Ua fautuaina e ofisa o loo tuufaatasia lenei tusitusiga, ia uu mau pea e faalapotopotoga, o software manufacturers o le a feagai ma iuga tau le puipuiga e tuu ane mo a latou oloa. O se vaega o lea faiga, ua fautuaina ai e ofisa o loo tuufaatasia lenei tusitusiga le faamuamua e ofisa sinia o le taua o le faatauina o oloa e secure by design ma secure by default. E mafai ona faamalosia lea e ala i le faatuina o ni faiga faavae e manaomia ai le vaega o le IT latou te mataitu le tulaga tau le puipuiga o le software ao lei faatauina, aemaise o le faamalosia o le vaega a le IT ina ia toe tuutuu atu teisi i tua pe afai e mafai. E tatau ona faamalosia vaega ale IT ia faalautele aiaiga mo le faatauina, aemaise ia faamamafa le taua o faiga o le secure by design ma le secure by default.(lea o loo faailoa atu i le pepa lenei ma isi sa faalautele e le faalapotopotoga). Faaopoopo atu i lea, e tatau ona lagolago le pulega sinia i le vaega a le IT mo le faamalosia o nei aiaiga i faiga faaiuga mo faatauga. O faaiuga faia a le faalapotopotoga ina ia talia le lamatiaga e aofia ai i nisi o oloa patino tau tekonolosi, e tatau ona faamauina aloaia, ioeina e se tagata ofisa sinia, ma ia fai lava ma tuuina i le fono faatonu.

O nisi o enterprise poo auaunaga tau IT latou te lagolagoina le tulaga tau le puipuiga a le faalapotopotoga, e pei o le enterprise network, enteprise identity ma le access management, vaega o galuega tau le puipuiga ma agavaa e tali atu ai, e tatau ona silasila iai o ni matafaioi taua ia a le pisinisi o loo faatupeina ina ia o gatasi ma lo latou taua i le manuia o le misiona a le pisinisi. O faalapotopotoga e tatau ona o latou faalautele se fuafuaga e faafou ai nei agavaa ia faatutusa lelei ma manufacturers latou te opogi se faiga e pei o le secure by design ma le secure by default.

Poo fea lava e fetaui i ai, e tatau i faalapotopotoga ona o latou finau ia faamalosia mafutaga ma a latou IT suppliers autu. O nei mafutaga e aofia ai le faatuatuaga i vaega eseese o le faalapotopotoga ma ia saunia ni tali e foia ai faaletonu ma iloa ai le faasoaina o mea o loo ave iai le faamuamua. O faaiuga faia a le faalapotopotoga ina ia talia le lamatiaga e aofia ai i nisi o oloa patino tau tekonolosi, e tatau ona faamauina aloaia, ioeina e se tagata ofisa sinia, ma ia fai lava ma tuuina i le fono faatonu E tatau i faalapotopotoga ona o latou faatalitalia le faamalamalamaina o mea mai a latou suppliers e faatatau i le tulaga o iai lona tulaga faatonutonu lelei faalotoifale aemaise o se faafanua agai i le faaaogaina o faiga a le secure by design ma le secure by default.

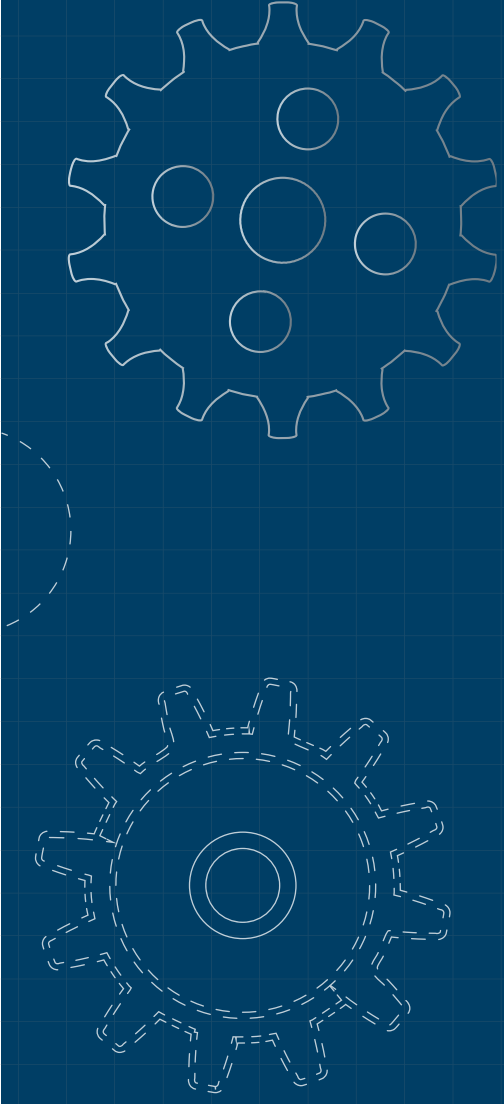
Faaopoopo atu i le ave o le faamuamua i le secure by default ise faalapotopotoga, e tatau i taitai o le IT ona galulue faatasi ma isi ile auaunaga ia malamalama ai poo fea oloa ma auaunaga e aupito lelei ona faaaogaina ai ia faatulagana faavae. O nei taitai e tatau ona o latou tuu faatasi a latou talosaga ina ia fesoasoani ai i manufacturers ia ave le faamuamua i ni taumafaiga tau le puipuiga o le a sosoo mai. O le galulue faatasi, o le a mafai ai ona fesoasoani le tagata faatau e saunia se sao e uiga mo manufacturers ma ia saunia ni mea e faamalosia ai i latou ina ia o latou faamuamua ai le tulaga tau le puipuiga.

Ile faatutusaina o cloud systems, e tatau i faalapotopotoga ona faamautinoa o loo latou malamalama i le matafaioi faasoa poo le responsibility model faatasi ai ma le latou technology supplier. O lea la, o faalapotopotoga e tatau ona iai se tulaga manino i matafaioi a le supplier ae lē nao matafaioi a le tagata faatau.

E tatau i faalapotopotoga ona faamuamua cloud providers o loo faamaoni ile tulaga o loo iai i latou ile itu tau le puipuiga, meafaatonutonu faalotoifale, ma le agavaa e lavasaia ai o latou matafaioi i lalo o le shared responsibility model.

TAUTINOGA PATINO

O faamatalaga i lenei lipoti ua saunia i le “tulaga o iai nei” mo nao faamoemoega lava tau faamatalaga. E lē ioeina e le CISA ma ofisa o loo tuufaatasia lenei tusitusiga, nisi o oloa faapisinisi poo auaunaga e aofia ai ni mataupu o loo iloiloina. Soo se tulaga e faasino i ofisa faapisinisi patino poo oloa tau pisinisi, o le faagasologa, poo auaunaga ua faailogaina, faailogaina faapisinisi, manufacturer, poo se isi lava mea e lē o iai se ioega, fautuaga poo se faiga faapito e le CISA ma ofisa o loo tuufaatasia lenei tusitusiga. O lenei pepa o se taumafaiga fai faatasi a le CISA ma e lē okometi ona avea o se pepa faaletulafono faatonutonu.



Puna'oa

CISA

- CISA's SBOM Guidance
- CISA's Cross-Sector Cybersecurity Performance Goals
- Guidelines on Technology Interoperability
- CISA and NIST's Defending Against Software Supply Chain Attacks
- The Cost of Unsafe Technology and What We Can Do About It | CISA
- Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (foreignaffairs.com)
- CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance
- CISA's Phishing Resistant MFA Fact Sheets
- Cyber Guidance for Small Businesses | CISA

NSA

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

FBI

- Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective
- The Cyber Threat - Response and Reporting
- FBI's Cyber Strategy

Ofisa Aoao o Faatulagana ma Tekonolosi (NIST)
National Institute of Standards and Technology (NIST)

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

Ofisa Autū a Ausetalia mo Mataupu tau puipuiga i Upega Tafailagi (ACSC)
Australian Cyber Security Centre (ACSC)

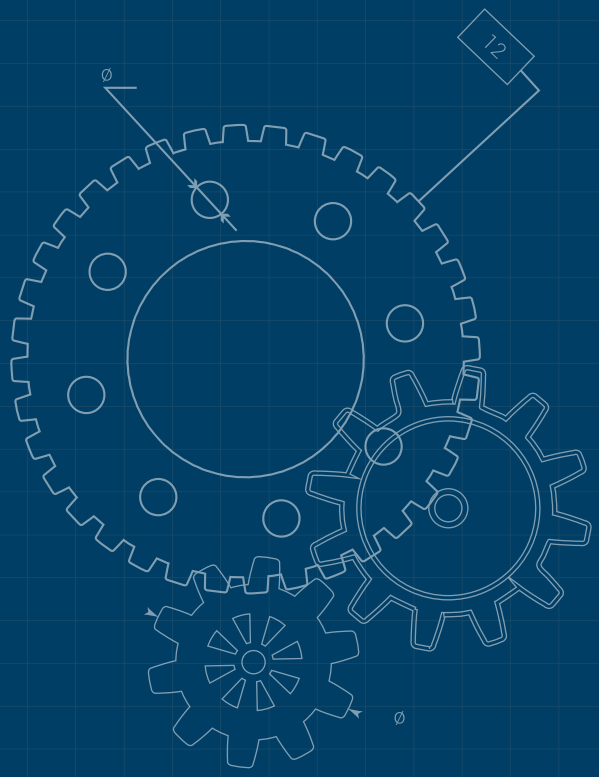
- ACSC's IoT Code of Practice Guidance for Manufacturers

Ofisa Autū a le UK mo Mataupu tau puipuiga i Upega Tafailagi (UK)
The United Kingdom's National Cyber Security Centre (UK)

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

Ofisa Autū a Kanata mo Mataupu tau puipuiga i Upega Tafailagi (CCCS)
Canadian Centre for Cyber Security (CCCS)

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



Ofisa tau feterale a Siamani mo Puipuiga o Faamatalaga (BSI)
Germany's Federal Office for Information Security (BSI)

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

Ofisa Autū a Netherlands mo Mataupu tau puipuiga i Upega Tafailagi
Netherland's National Cyber Security Centre

- NCSC-NL's Mature Authentication Factsheet

Ofisa Autū a Iapani i mataupu tau sauniuniga ma fuafuaga tau puipuiga i Upega Tafailagi (NISC)
Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC)

- Japan's National Cybersecurity Strategy

Matagaluega tau Tamaoaiga, Fefaatauaiga ma Fale gaosi oloa a Iapani (METI)
Japan's Ministry of Economy, Trade and Industry (METI)

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

Ofisa a Singapore mo Mataupu tau puipuiga i Upega Tafailagi
Cyber Security Agency of Singapore

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

Isi

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

MEA O LOO FAAUIGA IAI

[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.