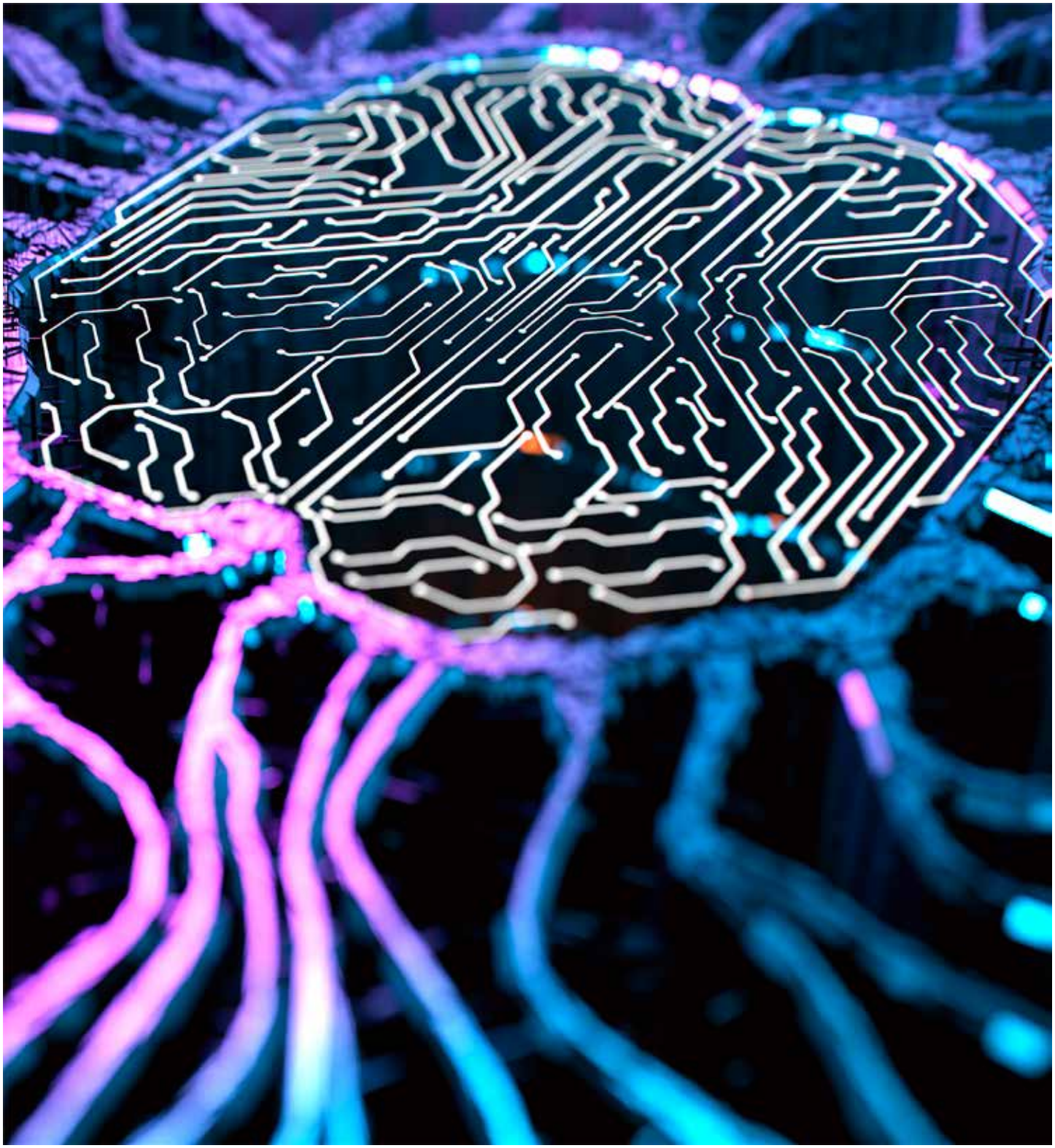
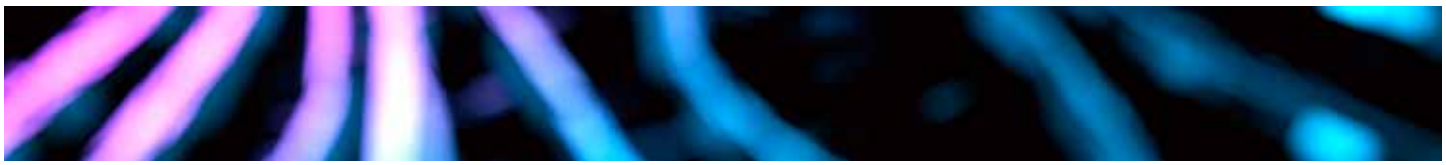
Ngaahi fakahinohino ki he fa'u 'o ha Polokālama 'Atamai Fa'u (AI) 'oku malu





National Cyber Security Centre
a part of GCHQ

CISA
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

National Cyber and Information Security Agency

Republic of Estonia
Information System Authority

Department of Justice
Federal Bureau of Investigation

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Federal Office for Information Security

INCD
Israel National Cyber Directorate

AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT

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

National Cyber Security Centre

NITDA

NSM
NORWEGIAN NATIONAL CYBER SECURITY CENTRE

National Security Agency
United States of America

NASK

국가정보원
National Intelligence Service

Ministerstwo Cyfryzacji

CSA SINGAPORE
Cyber Security Agency of Singapore

Fekau'aki mo e tohi fakamatala ni

Ko e tohi ni 'oku pulusi 'e he Senitā Fakafonua 'a Pilitānia ki he Malu 'a e Ngaahi Me'angāue Fakakomipiuta mei ha Fakatāmaki mei he 'initaneti (NCSC), Fakafofonga Kautaha 'a 'Amelika Tokanga'i 'a e Fokotu'utu'u mo e Malu 'a e Ngaahi Me'angāue Fakakomipiuta mei ha Fakatāmaki (CISA), pea mo e ngaahi hoangāue fakavaha'apulenga ko 'eni:

- Potungāue Fakafonua ki he Malu'i (NSA)
- Potungāue Fakatōtolo 'a e Fetalolo (FBI)
- Senitā Fakafofonga 'o 'Aositelelia ki he Malu'i 'a e Ngaahi Me'angāue Fakakomipiuta (ACSC)
- Senitā 'a Kanata ki he Malu 'a e Ngaahi Me'angāue Fakakomipiuta mei ha Fakatāmaki mei he 'Initaneti (CCCS)
- Senitā Fakafonua 'a Nu'usila ki he Malu 'a e Ngaahi Me'angāue Fakakomipiuta mei ha Fakatāmaki mei he 'Initaneti (NCSC-NZ)
- Timi Ngāue Fakavavevave "a e Pule'anga Silei ki ha Fakatāmaki fekau'aki mo ha Fakatāmaki ki he Me'a Fakakomipiuta
- Kautaha Fakafofonga Fakafonua 'o Sekisī ki he Fakamatala mo Fakatāmaki Faka'initaneti pe Fakamatala (NUKIB)
- Ma'u Mafai ki he Ngaahi Fakamatala Fakakomipiuta 'o 'Esitonia (RIA) mo e Senitā Fakafonua 'o 'Esitonia ki he Malu'i 'o e Ngaahi Me'angāue Fakakomipiuta mei ha Fakatāmaki mei he 'initaneti (NCSC-EE)
- Kautaha Fakafofonga 'o Falanise Tokanga'i 'a e Malu 'o e Ngaahi Me'angāue Fakakomipiuta mei ha Fakatāmaki he 'Initaneti (ANSSI)
- 'Ofisi 'a e Pule'anga Siamane ki he Malu 'o e Ngaahi Fakamatala (BSI)
- Kautaha Fakafofonga 'o 'Isileli Tokanga'i 'a e Malu 'o e Ngaahi Me'angāue Fakakomipiuta mei ha Fakatāmaki he 'Initaneti (INCD)
- Kautaha Fakafofonga Fakafonua 'a 'Itali ki he Malu'i 'o e Me'angāue Fakakomipiuta mei he Fakatāmaki he 'Initaneti (ACN)
- Senitā Fakafonua 'a Siapani ki he Mateuteu mo e Palani ki ha Fakatāmaki mei he 'initaneti (NISC)
- Va'a 'a Siapani ki he Saienisi, Tekinolosia pea mo e Fokotu'utu'u Fo'ou, mo e 'Ofisi Kapineti
- Fakafofonga Fakafonua 'o Naisilia ki he Fa'unga 'o e Fakamatala Fakatekinolosia (NITDA)
- Senitā Fakafonua 'o Nouei ki he Malu'i ha Fakatāmaki mei he 'initaneti (NCSC-NO)
- Potungāue ki he Ngaahi Me'a Faka'elekitulonika, 'a Pōlani
- Potungāue Fekumi Fakafonua 'o Pōlani (NASK)
- Potungāue Tokanga'i Va Fakatu'apule'anga 'o Kolea (NIS)
- Fakafofonga ki he Malu'i 'o e Fakatāmaki mei he 'Initaneti, 'o Singapoa (CSA)

Fakamo'oni'ii

Ko e ngaahi kautaha ni na'a nau tokoni ki hono fa'unga 'o e ngaahi fakahinohino ni:

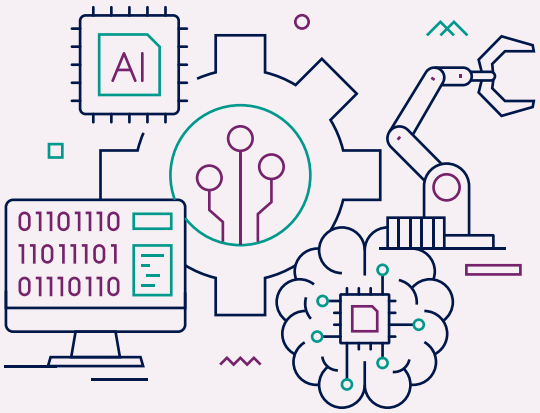
- 'Inisitītiuti Alan Turing
- Kautaha Fekumi 'Atolopiki
- Kautaha Fa'u Polokalama Komipiuta Teitapiliki
- 'Univesiti Georgetown ki he Tekinolosia Fo'ou mo Malu
- Kukolo
- Kautaha Fekumi 'Atamailoloto 'a e Kukolo
- IBM
- ImBue
- Microsoft
- OpenAI
- Palantir
- RAND
- Kautaha Fa'u Polokalama Komipiuta Me'afua AI
- Va'a ki he 'Enisinia Polokalama Komipiuta 'i he 'Univesiti Carnegie Mellon
- Senitā Sītenifooti ki he Malu 'o e Ngāue'aki 'o e Poto Fa'u 'e he Komipiuta
- Polokalama Stanford 'i he Politiki Fakafeitu'u, Tekinolosia mo e Pule

Fakaha

'Oku 'oatu 'a e fakamatala 'i he tohi fakamatala ko 'eni "'o hange ko e" fa'u 'e he NCSC mo e ngaahi kautaha fakamafai 'o 'ikai ke nau 'eke'i meiate kinautolu ha fa'ahinga mole, lavea pe maumau 'o ha fa'ahinga me'a na'e fakatupu mei hono faka'aonga'i 'o hange ko ia 'i he fiema'u 'e he lao. Ko e ngaahi fakamatala 'i he tohi fakamatala ni, 'oku 'ikai ke kau pe fakaha pe poupou ki ha fa'ahinga kautaha fika tolu, koloa, pe ngaue 'a e NCSC mo e ngaahi kautaha fakafofonga kuo fakamafai. Ko e ngaahi felave'i ki he ngaahi uepisaiti mo e ngaahi naunau 'a e hoa ngaue fika tolu 'oku tuku atu 'i he taumu'a ko e fakamatala 'ata'ata pe pea 'oku 'ikai ke ne fakaha ha poupou 'o e ngaahMe'angāueee pehee ki he ni'ihi kehe.

Ko e tohi fakamatala ni 'oku 'ata 'i ha TLP:Fakatefito MAHINO (https://www.first.org/tlp/).

Ngaahi Me'a 'i he Tohi Fakamatala ni



Fakamatala nounou

Ko e tohi fakamatala ni 'oku ne poupoua 'a e ngaahi fakahinohino ki he ngaahi kautaha 'o ha sisitemi ki he Ngāue'aki 'o e polokālama 'atamai fa'u (AI), pe ko e ngaahi sisitemi ko ia kuo fa'u kamata mei lalo pe ko e fa'u mei ha ngaahi me'a ngaue pe ngaue kuo 'omai 'e ha ngaahi feitu'u kehe. 'E tokoni hono fakahoko 'o e ngaahi fakahinohino ko 'eni ki he ngaahi kautaha fa'u sisitemi AI ke nau langa ha ngaahi founga 'o hange ko hono fakataumu'a, 'oku lava ke ma'u ia 'i he taimi 'oku fiema'u ai, pea ngaue 'o 'ikai fakaha ha ngaahi fakamatala pelepelengesi ki he ngaahi kupu 'oku 'ikai ha'anau mafai ki ai.

Ko e taumu'a 'uluaki 'a e tohi ko 'eni ki he ngaahi kautaha nau fo'u polokalama AI 'o ngāue'aki 'a e ngaahi Me'angāue 'oku tokanga'i 'e ha kautaha, pe 'oku nau faka'aonga'i 'a e ngaahi polokālama fakapolokalama mei tu'a (APIs). 'Oku mau tapou atu ki he **kotoa** ngaahi kauataha (kau ai 'a e kau saienisi 'i he fakamatala, kau fo'u polokālama, kau pulengāue, kau faitu'utu'uni mo nautolu na'u tokanga'i me'a fakatu'utamaki) ke lau 'a e ngaahi fakahinohino ko 'eni ke tokoni'i kinautolu ke nau fai ha ngaahi fili fekau'aki mo e **fokotu'utu'u**, **fakalakalaka**, **faingāue** mo e **fakalele ngāue** 'o e ngaahi polokālama 'Atamai Fa'u.

Fekau'aki mo e ngaahi fakahinohino

'Oku 'i ai ha ngaahi founga 'e lava ke 'omi ai ha ngaahi lelei lahi ki he sōsaieti. Neongo ia, koe'uhi ko e ngaahi faingamālie 'o e 'i ai e polokālama AI ke fakatokangā'i kakato, kuo pau ke fakatupulaki, pālani mo fakalele ia 'i ha founga malu mo falala'anga.

'Oku 'i ai ha ngaahi founga 'oku mo'ulaloa ai ki he ngaahi vaivai malu'i 'oku fiema'u ke fakakaukau'i fakataha mo e tu'unga mo'ui ngaahi maumau ki hono malu'i 'initaneti. 'I he taimi 'oku ma'olunga ai 'a e vave 'o e fakalakalaka – 'o hangē ko ia 'oku hoko 'i he AI – 'oku fa'a lava ke hoko 'a e malu'i ko ha fakakaukau kr toki fika ua mai. Ko e malu koe me'a fika 'uluaki ia, kae 'ikai 'i hono ngaohi pē, ka koe lolotonga ko ia e taimi 'oku fakahoko fatongia ai he sisitemi.

'I he 'uhinga ko 'eni, 'oku maumau'i ai 'a e ngaahi fakahinohino ki ha ngaahi tafa'aki mahu'inga 'e fa 'i he siakale 'o e fakalakalaka 'o e mo'ui: **malu hono fa'unga tīsaini**, **fa'unga 'oku malu**, **fa'unga malu hono tukuatu**, mo e **malu 'a e fakahoko ngāue mo hono tokanga'i**. 'Oku mau fokotu'u atu ki he konga takitaha ha ngaahi fakakaukau mo ha ngaahi me'a 'e tokoni ke fakasi'isi'i 'a e fakatu'utamaki fakalūkufua ki ha kauataha 'oku 'i ai e founga fakalakalaka'i 'o e polokālama.

1. **Malu hono fa'unga tīsaini**
   'Oku 'i he konga ko 'eni ha ngaahi fakahinohino 'oku fekau'aki mo e tu'unga 'o e fokotu'utu'u 'o e siakale fakalakalaka 'o e mo'ui. 'Oku ne 'ufi'ufi 'a e mahino 'o e ngaahi me'a 'oku tu'u fakatu'utāmaki mo e mōtolo kene tokanga'i maumau, pea pehē ki ha ngaahi kaveinga pau 'i he fefakatau'aki ke fakakaukau'i e polokālama mo e sīpinga 'o e tisaini hono fa'unga.

2. **Fa'unga 'oku malu**
   'Oku 'i he konga ko 'eni ha ngaahi fakahinohino 'oku fekau'aki mo e tu'unga fakalakalaka 'o e siakale 'o e fakalakalaka 'o e mo'ui, kau ai 'a e malu'i 'o e seini, me'a fakapepa, mo e koloa mo hono tokanga'i 'o e mo'ua fakatekinikale.

3. **Fa'unga malu hono tukuatu**
   'Oku 'i he konga ko 'eni ha ngaahi fakahinohino 'oku fekau'aki mo e tu'unga tukuatu ngāue 'o e siakale 'o e fakalakalaka 'o e mo'ui, kau ai hono malu'i 'o e fokotu'utu'u mo e kau ta sipinga mei he feveitokai'aki, uesia kene maumau'i pe mole, fakatupulaki e ngaahi founga tokanga'i 'o e me'a 'oku hoko, mo hono tuku atu hono fai 'o e fatongia.

4. **Malu 'a e fakahoko ngāue mo hono tokanga'i**
   'Oku 'i he konga ko 'eni 'a e ngaahi fakahinohino 'oku fekau'aki mo e ngāue malu mo hono tokanga'i 'o e 'oku 'i ai e siakale 'o e mo'ui fakalakalaka 'a e System. 'Oku ne 'omi ha ngaahi fakahinohino ki he ngaahi ngaue 'oku matu'aki mahu'inga 'i he taimi kuo palangi ai ha polokalama, kau ai 'a e loka mo hono vakai'i, fakatonutonu 'o e tokanga'i mo e fakamatala 'oku vahevahe.

'Oku muimui 'a e ngaahi fakahinohino ki ha ' malu 'i he founga kuo 'osi fakapolokalama'i, pea 'oku fenapasi vaofi mo e ngaahi founga ngaue 'oku faka'uhinga'i 'i he NCSC malu'i 'o e fakalakalaka mo deployment fakahinohino, NIST fa'unga fakalakalaka 'o e polokalama fakakomipiuta, mo e ' malu 'e he ngaahi tefito'i mo'oni' na'e pulusi 'e CISA, ko e NCSC mo e ngaahi kautaha fakavaha'apule'anga. 'Oku nau fakamu'omu'a:

- ko honau fatongia ke tokanga'i malu kasitoma
- tali kakato 'a e 'ata kitu'a mo e taliui
- ko hono langa e fa'unga 'o ha kautaha mo e anga fakataki 'oku malu 'i ha pālani ko ha me'a mahu'inga 'aupito ia

Talateu

Ko e polokalama 'Atamai Fa'u ('i ai) 'oku malava kene 'omi ha ngaahi lelei lahi ki he sōsaieti. Neongo ia, koe'uhi ko e ngaahi faingamālie ke ma'u kakato, kuo pau ke fakatupulaki, palani mo fakalele 'i ha founga malu mo falala'anga. Ko e malu 'initaneti 'oku 'uluaki fiema'u ia koe'uhi koe malu, mo matu'uaki, tau'ataina fakafo'ituitui, tu'unga taau, mo ma'u ola fiema'u mo ala falala'anga ki he ngaahi sisitemi polokālama AI.

Neongo ia, 'oku ala uesia e AI ha ngaahi palopālema fakakomiuta fo'ou 'o matavaivai ai pea 'oku fiema'u ke fakakaukau'i fakataha mo e ngaahi me'a 'oku tu'u fakatu'utamaki ki he malu 'initaneti.. 'I he taimi 'oku ma'olunga ai e vave 'o e fakalakalaka – 'o hange ko ia 'oku hoko 'i he 'i AI – 'oku fa'a hoko 'a e malu'i ko ha fakakaukau fika ua. Kuo pau ke hoko 'a e malu'i ko ha tefito'i fie ma'u, 'o 'ikai 'i he konga pe 'o e fakalakalaka, ka 'i he fuoloa ha ngāue 'a e polokālama ko ia.

'Oku fokotu'u atu 'e he fakamatala ko 'eni 'a e ngaahi fakahinohino ki he kau Fo'u Polokālama[1] 'o ha fa'ahinga sisitemi pe 'oku nau faka'aonga'i 'a e AI, 'o tatau ai pe pe kuo fa'u 'a e ngaahi polokālama ko ia mei ha ngaahi me'angāue mo e ngaahi ngaue 'oku 'omi 'e he ni'ihi kehe. 'E tokoni hono fakahoko 'o e ngaahi fakahinohino ko 'eni ki he kau Fo'u Polokālamai ke nau langa ha ngaahi founga 'oku ngaue 'o hange ko e taumu'a, 'oku lava ke ma'u ia 'i he taimi 'oku fiema'u ai, pea ngāue 'o 'ikai tuku kitu'a ha fakamatala pelepelengesi ki ni'ihi taefakamafai'i.

'Oku totonu ke fakakaukau'i fakataha 'a e ngaahi fakahinohino ko 'eni mo e malu'i 'i he 'Initaneti, tokanga'i 'o e ngaahi me'a 'oku tu'u fakatu'utamaki, mo e tali lelei taha ki he me'a 'oku hoko. Kae tautautefto,'oku mau teke e kau Fo'u Polokālama ke nau muimui ki he ' malu 'i he fa'unga tisainii '[2] ngaahi kaveinga kuo fatu 'e he Senitā 'a 'Amelika ki he Malu Ngaahi Kautaha Lalahi mo e Malu 'Initaneti (CISA), pehē ki he Senitā Fakafonua 'a UK ki he Malu 'initaneti (NCSC), pehe ki hotau ngaahi hoangāue fakavaha'apule'anga kotoa pe. 'Oku fakamu'omu'a 'a e ngaahi me'a ni:

- ko hoto fatongia ke mahino e malu 'a e kasitoma
- tali kakato e 'ata kitu'a mo e taliui
- ko hono langa 'o e fa'unga kautaha mo e anga fakataki 'oku malu 'i he palani ko ha me'a mahu'inga ia ki he pisinisi.

'Oku fiema'u ha ngaahi ma'u'anga tokoni mahu'inga 'i he muimui ki he kaveinga 'malu fa'unga tisaini 'oku fiema'u naunau lolotonga ko ia kei ngāue lelei 'a e polokālama. 'Oku 'uhinga eni kuo pau ko nautolu nau fo'u polokālama ke nau 'inivesi 'o fakamu'omu'a e **fotunga**, **founga ngāue**, pea mo hono **fokotu'u** 'o e ngaahi me'angāue 'oku ne malu'i 'a e kasitoma 'i he levolo takitaha 'o e polokālama kuo 'osi fa'u, pea kau e levolo kotoa hono fa'u ke lava 'o kei ngāue. 'I hono fai 'eni tene lava ke fakasi'isi'i hano toe fa'u fo'ou e fa'unga tisaini 'o e polokālama 'amuiange, pea pehē ki hono malu'i e kasitoma mo 'enau teita fakamatala 'i ha taimi 'oku vave ange.

Ko e hā 'oku kehe ai ngaahi polokālama malu'i 'a e AI?

'I he fakamatala ni 'oku ngāue'aki e "AI" 'o 'uhinga tonu ki he polokālama faka'uhingame'a ako e (ML) misini[3]. Ko e lahi tatau kotoa pē ngāue 'a e ML kotoa. 'Oku fakamatala'i 'a e ngaahi polokālama ML ko e polokālama ke ngāue'aki kau ai:

- ngaahi kongakonga 'o e polokālama fakakomipiuta (mōtolo) 'oku lavai he komipiuta kene fakatokanga'i pea lava ke faka'uhinga'i ai e peteni 'i he teita 'o 'ikai muimui ha tu'utu'uni kuo pau ke fakapolokālama'i 'e ha tangata
- Kene lava tala, ngaahi fkotu'u mai, pē ko ha tu'utu'uni 'o makatu'unga 'i he faka'uhinga fakasitetisitika

Pea pehē ki he ngaahi me'a 'oku tu'u fakatu'utāmaki ki he malu'i, 'oku lava pē ke uesia 'a e AI mei ha vailasi fakatu'utāmaki fo'ou. 'Oku ngāue'akii 'a e fo'i lea ko e ' mīsini fakakomipiuta kene takaihala'i ' (AML), 'o fakamatala ai ki hono maumau'i 'a e ngaahi konga tu'u laveangofua 'i he ML,kau ai e naunau fakakomipiuta, polokālama fakakomipiuta, anga fai 'o e ngāue mo e hokohoko hono faingāue. 'Oku hanga 'e he AML 'o 'ai ke lava 'e he ngaahi vailasi ke ne fakatupu ha to'onga faikehe 'i he sisitemi ML pea kau ai 'a e :

- uesia 'a e fakafa'ahinga 'o e mōtolo pea koviange 'ene ngāue
- Pea mālava ai ke nau fakahoko ha ngāue 'oku 'ikai ngofua
- 'o to'o e fakamatala pelepelengesi mei he mōtolo ko ia

'Oku lahi e ngaahi founga ke ma'u e ola ko 'eni, hangē ko hano 'ohofi he vailasi 'i he 'elia 'o e Mōtolo Ngaahi Lea Lālahi (LLM), pe ko hano maumau'i 'a e fakamatala teita ki he ako pē ko e fokotu'u fakakaukau nautolu nau ngāue'aki ('oku 'iloa ko e ' fakakonahi fakamatala ').

Ko hai 'oku totonu ke ne lau 'a e tohi ni?

'Oku fakataumu'a fakapātonu 'a e fakamatala ni ki he ngaahi Kautaha Fo'u Polokālama 'i he AI, 'o tatau ai pē 'oku makatu'unga 'i he ngaahi mōtolo 'oku tokanga'i 'e ha kautaha pe ngāue'aki 'o e ngaahi naunau fakapolokalama meii tu'a (APIs). Neongo ia, 'oku mau tapou atu ki he **kotoa** 'u kautaha (kau ai 'a e kau saienisi 'o e fakamatala, fo'u polokālama, kau pule, kau fai tu'utu'uni mo nautolu tokanga'i ha fakatu'utamaki) ke lau 'a e ngaahi fakahinohino ko 'eni ke tokoni'i kinautolu ke nau fai ha tu'utu'uni fakapotopoto fekau'aki mo e **tisaini**, **anga hono tukuatu** mo hono **fakalele ngāue** 'o 'enau sisitemi misini fakakomipiuta AI.

'A ia 'oku pehē, he'ikai ke 'aonga fakahangatonu 'a e ngaahi fakahinohino kotoa pe ki he ngaahi kautaha kotoa. 'E kehekehe pe 'a e tu'unga faingata'a mo e ngaahi founga hū vailasi 'o makatu'unga 'i he ngaahi polokālama 'oku tāketi'i ke takihala'i 'aki e AI, ko ia 'oku totonu ke fakakaukau'i 'a e ngaahi fakahinohino fakataha mo e ngaahi me'a 'oku faka'aonga'i 'e ho'o kautaha ki he ngaahi keisi kehekehe pea mo e fakamatala ki he ngaahi uesia 'e hoko.

Ko hai 'oku fatongia'aki 'a hono fo'u 'a e AI 'oku malu?

'Oku fa'a 'i ai hā ni'ihi tokolahi 'i he ngaahi fakahokohoko ngāue 'a e sisitemi AI 'o onoponi. 'Oku 'i ai ha founga faingofua ke ma'u ha me'a 'e ua:

- ko e "tokotaha fo'u polokālama" 'a ia 'oku ne tokanga'i hono filifili 'a e teita,'alakauālīsimi, fakalakalaka'i, tīsaini, tukuatu mo hono tokanga'i
- ko e "tokotaha ngāue", 'a ia 'oku ne fakahū mo ma'u fakamatala

Neongo 'oku ngāue'aki 'a e founga ngāue ko 'eni he tokotaha fo'u polokālama 'i he ngaahi me'angāue fakakomipiuta lahi, ka 'oku faka'au ke lahiange 'a e ngaahi me'a ta'e'amanekina 'oku hoko[4], 'e vakai 'a e ngaahi kautaha fo'u polokālama ke fakakau mai e polokālama fakakomipiuta, fakamatala teita, mōtolo mo e/pe ngaahi ngāue mama'o 'oku 'omi 'e ha sinongāue fika 3 ki he'enau ngaahi sisitemi. 'Oku hanga 'e he hokohoko seini e fokotu'utu'u faingata'a ko 'eni 'o 'ai ke faingata'a ange hono faka'osi 'e he tokotaha ngāue ke mahino 'a e feitu'u 'e fai mei honau fatongia ki hano malu'i ''o e AI.

'Oku 'ikai fa'a ma'u 'e kinautolu nau ngāue'aki (tatau ai pe pe ko e ' kau ngaue Fo'u Polokāla', 'oku nau fakakau mai ha konga kitu'a polokālama AI[5]) 'oku 'ikai ke nau fa'a fakatokanga'i mo/pe ai ha taukei ke mahino kakato, fakafuofua'i pe ngāue ki hengaahi me'a 'e tu'u fakatu'utamaki fekau'aki mo e ngaahi polokalama 'oku nau faka'aonga'i. 'I he'ene pehee, ke tatau mo e "malu 'i he ngaahi kaveinga fa'unga fakatisaini", **'oku totonu ke fatongia 'aki 'e he kau fo'u polokālama e ngaahi kongokonga 'o e AI ki he malu 'o e ola faka'opsi ngāue 'a kinautolu 'amui ange te nau ngāue'aki e polokālama.**

'Oku tonu ke fokotu'u he kau Fo'u Polokālama 'a e founga ke fakamalu'i ke malu'i'aki pea mo fakasi'isi'i 'o ka lava ai 'i he'enau ngaahi mōtolo, hokohoko laine paipa tufaki fakamatala mo e/pe sisitemi, pea mo e feitu'u 'oku faka'aonga'i ai, fakahoko 'a e founga malu taha ke fakapolokāma'i pau ia. 'I he tafa'aki 'oku 'ikai lava ke fakasi'isi'i ange ai 'a e ngaahi uesia fakakomipiuta, 'oku totonu ke fatongia 'aki 'e he tokotaha fo'u polokālama 'a e:

- fakahā ki he kau faka'aonga'i 'i he hokohoko seini hifo tufaki fakamatala fekau'aki mo e fakatu'utamaki 'oku nau ma'u pea (kapau 'oku kaunga ki ai) 'i he'enau tali ke faka'aonga'i
- fale'i kinautolu ki he founga 'oku malu ke nau ngāue'aki

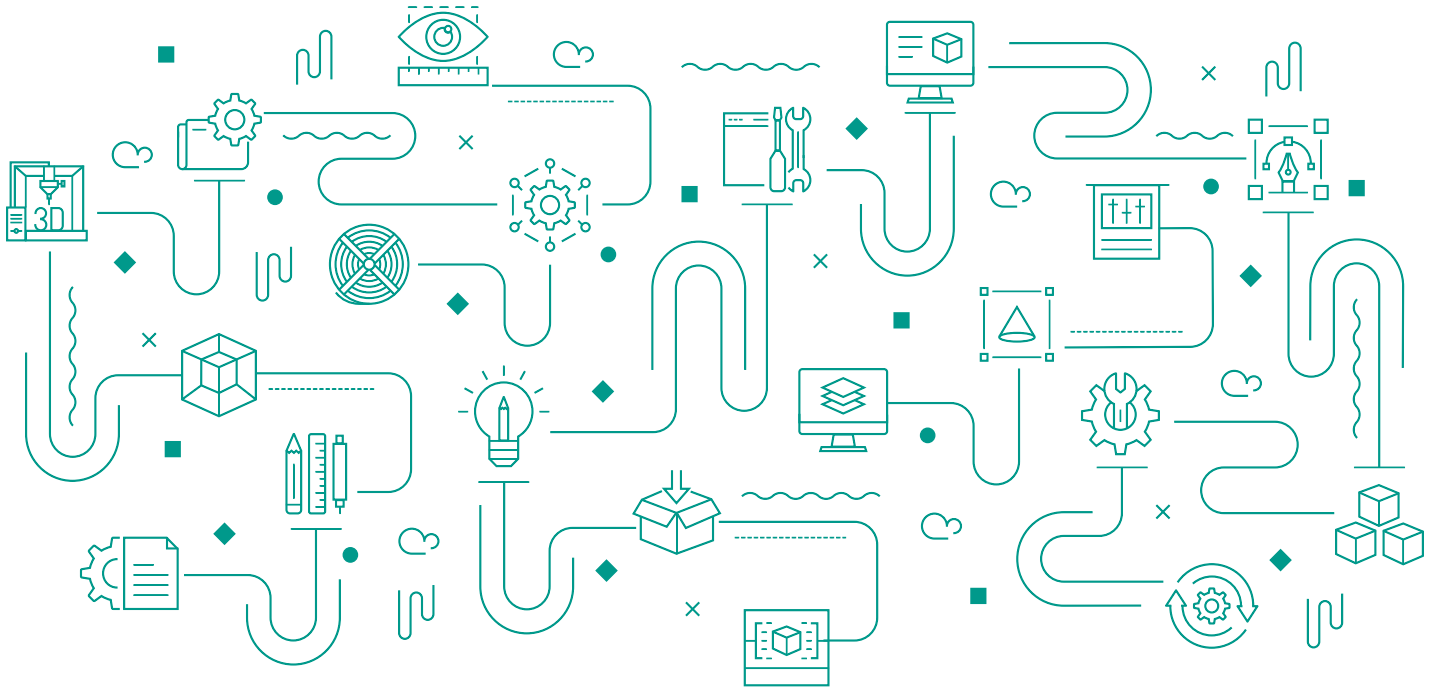
'I he feitu'u 'e lava ke iku ai 'a e feveitokai'aki 'o e polokalama ki ha maumau fakatu'asino pe reputational, mole lahi 'a e ngaahi ngaue fakapisinisi, mama 'o e fakamatala pelepelengesi pe 'ikai fakahahaholo pea/pe ngaahi 'uhinga fakalao, 'oku totonu ke hoko 'a e ngaahi me'a 'oku tu'u fakatu'utamaki ko e **mahu'inga.**

Ngaahi Fakahinohino ki hano fa'u ha sisitemi AI malu

'Oku maumau'i 'a e ngaahi fakahinohino ki ha ngaahi tafa'aki mahu'inga 'e fa 'i he siakale 'o e fakalakalaka 'o e mo'ui: **malu e fa'unga tīsaini**, **malu fakalakalaka'i polokālama**, **malu tukuatu polokālama**, mo e **malu ngāue mo hono tokanga'i**. 'I he tafa'aki takitaha, 'oku mau fokotu'u atu ha ngaahi fakakaukau mo ha ngaahi me'a 'e tokoni ke fakasi'isi'i 'a e fakatu'utamaki fakalukufua ki he kautaha 'i he founga fakalakalaka'i 'o e polokalama.

'Oku fēnapasi vaofi 'a e ngaahi fakahinohino 'oku fokotu'u atu 'i he fakamatala ko 'eni mo e ngaahi founga fakalakalaka 'o e mo'ui 'oku faka'uhinga'i 'i he:

- 'a e NCSC fakalakalaka mo deployment fakahinohino
- ko e 'inisitituti fakafonua 'o e ngaahi tu'unga mo'ui mo e tekinolosia (NIST) ko e fa'unga fakalakalaka 'o e polokalama fakakomipiuta (SSDF)[6]



1. Malu hono fa'unga tīsaini

'Oku 'i he konga ko 'eni ha ngaahi fakahinohino 'oku fekau'aki mo e **fokotu'utu'u** 'a e lōlōa lava ngāue ai ha polokālama kuo fa'u. 'Oku ne lave'i 'a 'ete mahino 'a e palopālema mo e mōtolo kene fakafepaki'i vailasi fakakomipiuta, pea pehē ki ha ngaahi kaveinga pau mo e fai fefakatau'aki ke fakakaukau'i 'i he polokālama mo e mōtolo tisani hono fa'unga.

Kake'i 'a e ako 'a e kau ngaue ke nau 'ilo'i e ngaahi fakamanamana mo e fakatu'utamaki

'Oku mahino ki he kau ma'u polokalama mo e kau taki ma'olunga 'a e ngaahi fakamanamana ke ma'u 'a e 'i ai mo 'enau clamps. 'Oku tauhi 'e ho'o kau saienisi 'o e fakamatala mo e developers ha 'ilo ki he ngaahi me'a 'oku tu'u fakatu'utamaki mo e ngaahi founga ta'elavame'a pea tokoni ki he kau ma'u 'oku tu'u fakatu'utamaki ke nau fai ha ngaahi tu'utu'uni. 'Oku ke 'oange ki he kau faka'aonga'i ha fakahinohino ki he ngaahi me'a 'oku tu'u fakatu'utamaki makehe 'oku fehangahangai mo e ngaahi System (hange ko 'eni, ko ha konga 'o e ako angamaheni InfoSec) mo e ako'i developers 'i he ngaahi founga 'oku malu mo malu mo falala'anga.

Faka'ali'ali ha ngaahi fakafe'atungia ki ho'o sisitemi

Ko e konga 'o ho'o founga tokanga'i 'o e ngaahi me'a 'oku tu'u fakatu'utamaki, 'oku ke faka'aonga'i ai ha founga holistic ke fakafuofua'i 'aki 'a e ngaahi fakamanamana ki ho'o polokalama, 'a ia 'oku kau ai 'a e mahino 'e lava ke ma'u 'e he polokalama, kau faka'aonga'i, organisations, mo e sosaieti lahi ange kapau 'oku 'i ai ha konga 'oku 'ikai ke 'i ai ha me'a pe ta'e'amanekina[7]. 'Oku kau 'i he founga ko 'eni 'a hono fakafuofua'i e ola 'o e ngaahi fakamanamana pau[8] mo hiki ho'o fili.

'Oku ke recognise 'e lava ke takiekina 'e he ongo'ingofua mo e fa'ahinga fakamatala 'oku faka'aonga'i 'i ho'o polokalama 'a hono mahu'inga ko ha taumu'a ki ha vailasi kainikavear. 'Oku totonu ke fakakaukau'i 'e ho'o fakafuofua'i 'e lava ke tupu ha ngaahi fakamanamana 'e ni'ihi 'o hange ko e 'oku fakautuutu hono mamata'i 'o e ngaahi founga mahu'inga ma'olunga, pea 'i he'ene hoko ko ha me'a fo'ou, 'ohofi taha ko ia pe polokālama.

Fa'ufa'u ho'o polokalama ki he malu pea pehe ki he ngaue mo e ngaue

'Oku ke ma'u ha loto falala 'oku fakamatala'i totonu taha 'a e ngaue 'i hono faka'aonga'i 'o e 'i ai. 'I ho'o fakapapau'i 'eni, 'oku ke fakafuofua'i ai 'a e totonu 'o ho'o ngaahi fili pau ki he palani. 'Oku ke fakakaukau ki ho'o sipinga fakamanamana mo e ngaahi me'a 'oku fekau'aki mo e malu'i 'oku fekau'aki mo e ngaue, a'usia 'a e tokotaha ngaue ki he polokalama, tukuatu kitu'a mei he 'atakai ko ia, ngāue, fakapapau'i, tokanga'i, ngaahi fie ma'u mo e ngaahi fie ma'u fakalao, mo ha ngaahi fakakaukau kehe. Hange ko 'eni:

- 'Oku ke fakakaukau ke malu'i 'a e seini 'i he taimi 'oku ke fili ai pe 'e fakatupulaki 'i he fale pe faka'aonga'i 'a e ngaahi konga 'i tu'a, hange ko 'eni:
    - ko ho'o fili ke ako'i ha sipinga fo'ou, faka'aonga'i ha sipinga lolotonga (mo e pe 'ikai ha fakatonutonu lelei) pe hu ki ha sipinga 'o fakafou 'i ha API 'i tu'a 'oku fe'unga mo ho'o ngaahi fie ma'u
    - 'oku kau 'i ho'o fili ke ngaue mo ha sipinga 'i tu'a ha fakafuofua'i 'o e malu'i 'a e kautaha ko ia
    - kapau 'oku ke faka'aonga'i ha laipeli 'i tu'a, te ke fakakakato ha fakafuofua'i 'o e faivelenga (hange ko 'eni, ke fakapapau'i 'oku pule'i 'e he laipeli 'a e ngaahi me'a 'oku ne ta'ofi 'a e kau ta sipinga 'oku 'ikai falala'anga 'o 'ikai ke nau fakahaa'i he taimi pe ko ia 'a e kouti pau[9])
    - 'oku ke fakahoko 'a hono faka'ata mo e fakamavahe'i/sandboxing 'i he taimi 'oku hiki mai ai 'a e kau ta sipinga fa'ahi tolu pe siuliolo 'ene mamafa, 'a ia 'oku totonu ke hoko ko ha kouti fa'ahi tolu 'oku 'ikai falala'anga pea 'e lava ke fakahoko ai 'a e kouti mama'o

- Kapau 'oku ke faka'aonga'i ha APIs 'i tu'a, 'oku ke faka'aonga'i 'a e pule'i totonu ki he fakamatala 'e lava ke 'ave ki he ngaahi ngaue mavahe mei he kautaha, hange ko e fiema'u ke hū 'a nautolu nau faka'aonga'i mo fakapapau'i kimu'a pea toki 'ave ha fakamatala pelepelengesi ko ia
- 'Oku ke faka'aonga'i 'a e ngaahi sieke totonu mo e sanitisation 'o e fakamatala mo e ngaahi me'a 'oku 'ikai ke 'i ai; 'Oku kau heni 'a e taimi 'oku fakakau ai 'a e fakamatala ki he tokotaha ngaue pe hokohoko atu hono ako 'o e fakamatala ki he motolo 'oku ne faktokanga'i mo faka'uhinga'i 'e fakamatala fakaako 'a e 'i he to'onga e polokālama komipiuta ko ia

- 'Oku ke fakataha'i 'a e fakalakalaka 'o e polokalama fakakomipiuta ki he fakalakalaka mo e ngaahi founga ngaue lelei taha; 'Oku hiki 'a e ngaahi 'elemeniti kotoa pe 'o e polokalama 'i he ngaahi 'atakai totonu 'o faka'aonga'i 'a e ngaahi founga ngāue mo e ngaahi lea fakafonua 'oku ne fakasi'isi'i pe to'o 'a e ngaahi kalasi 'oku 'ilo'i 'i he feitu'u ngali
- Kapau 'oku 'i ai ha ngaahi me'a 'oku fie ma'u ke ne fakatupu ha ngaahi ngāue, hange ko hono monomono ngaahi faile pe tataki 'a e me'a 'oku tukumai he ngaahi polokālama, 'oku ke faka'aonga'i 'a e ngaahi fakangatangata totonu ki he ngaahi ngāue 'e ala fai ('oku kau heni 'a e 'i tu'a mo e 'ikai ke toe fiemau ke mahino 'oku malu)
- hange ko 'eni, 'oku fakaha 'a e ngaahi tu'utu'uni 'i he fengaue'aki 'a e tokotaha ngaue 'i he ngaahi me'a 'oku tu'u fakatu'utamaki, hange ko 'eni:
  - 'oku 'omi 'e ho'o polokalama ha kau faka'aonga'i 'oku 'ikai ke nau lava 'o fakaha 'a e ngaahi tu'unga 'oku 'ikai mahu'inga ki ha me'a 'e malava attacker
  - kapau 'e fie ma'u, 'oku 'omi 'e ho'o polokalama ha ngaahi 'a pamu malu'i lelei 'i he sipinga
  - kapau te ke foaki ha API ki he kau fakatau mei tu'a pe collaborators, 'oku ke faka'aonga'i 'a e pule'i totonu 'oku ne fakasi'isi'i 'a e ngaahi 'ohofi 'i he polokalama 'o fakafou 'i he API
  - 'oku ke fakataha'i 'a e ngaahi feitu'u malu taha ki he polokalama 'i he peesi tu'uma'u
  - 'oku ke faka'aonga'i ha ngaahi tefito'i mo'oni faingamalie si'isi'i taha ke fakangatangata 'a e hu ki he polokalama 'a e polokalama
  - 'oku ke fakamatala'i riskier malava ke faka'aonga'i pea fie ma'u 'a e kau faka'aonga'i ke nau fili ke faka'aonga'i kinautolu; 'oku ke fetu'utaki ki he ngaahi me'a 'oku 'ikai ngofua ke faka'aonga'i, pea, 'i he feitu'u 'e lava ai, fakaha ki he kau faka'aonga'i 'o e ngaahi founga ke fakalelei'i 'aki

Fakakaukau ki he ngaahi lelei 'o e malu'i mo e fefakatau'aki 'i he taimi 'oku fili ai ho'o sipinga

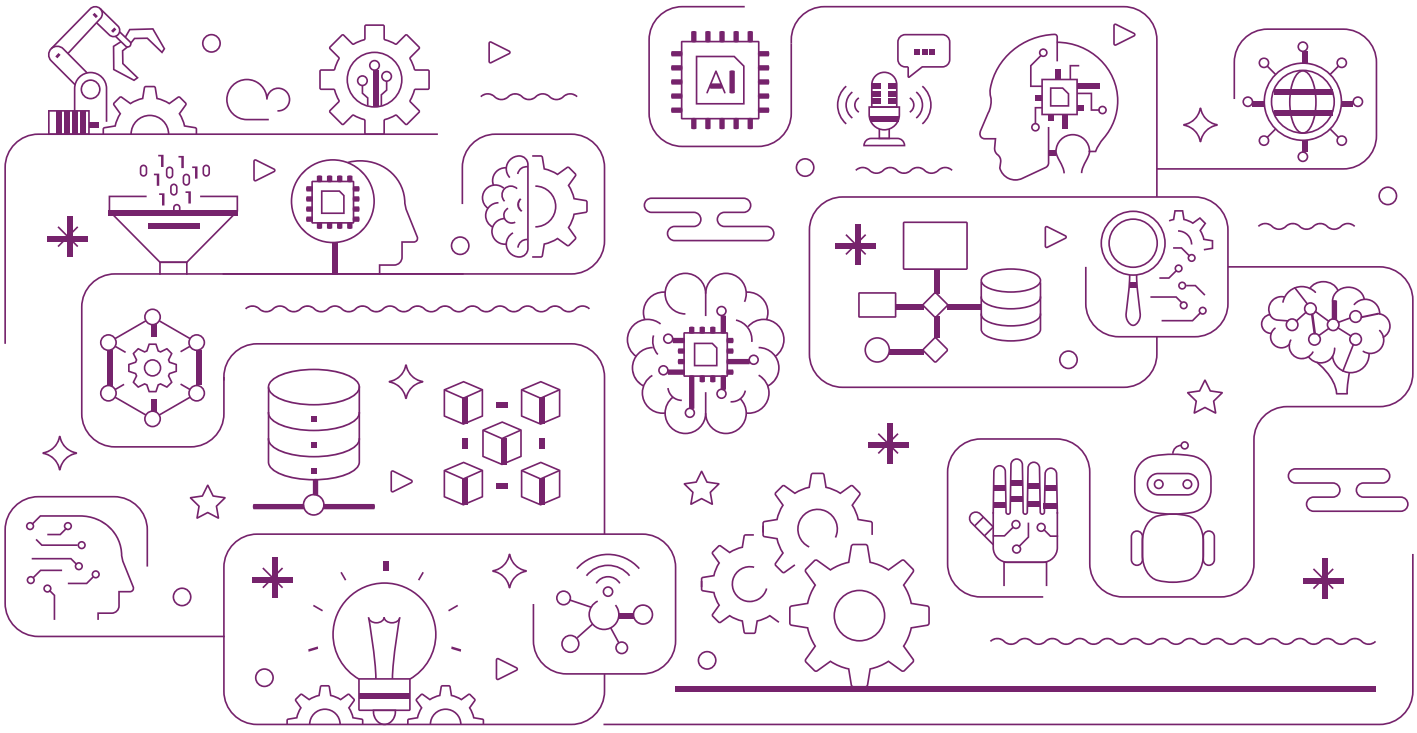
'E kau 'i ho'o fili 'a e sipinga 'oku 'i ai ha ngaahi fie ma'u kehekehe. 'Oku kau heni 'a e fili 'o e ngaahi fale, fokotu'utu'u, fakamatala ki he ako, ako 'alokaulīsimi mo e fuapalamita lalahi. 'Oku fakaha ho'o ngaahi fili 'e ho'o sipinga fakamanamana, pea 'oku reassessed ma'u pe ia 'i he ngaahi fakalakalaka 'o e fekumi ki he malu'i mo e mahino 'o e mafulifuli 'a e ngaahi fakātamaki.

'I he taimi 'oku ke fili ai ha sipinga, 'e ngalingali 'e kau 'i ho'o ngaahi fakakaukau, ka 'oku 'ikai fakangatangata pe ki he:

- 'a e faingata'a 'o e sipinga 'oku ke faka'aonga'i, 'a ia ko e ngaahi fale kuo fili mo e lahi 'o e ngaahi fakangatangata; 'e uesia 'e he ngaahi fale mo e lahi 'o e ngaahi fakangatangata kuo fili 'e ho'o motolo, 'a e lahi 'o e fakamatala ako 'oku fie ma'u pea mo e lahi 'o e ngaahi liliu 'i hono fakahu 'o e fakamatala 'i he taimi 'oku faka'aonga'i ai
- 'a e totonu 'o e sipinga ki ho'o faka'aonga'i mo e/pe feasibility 'o hono fulihi ia ki ho'o fie ma'u pau (hange ko 'eni 'aki ha fakatonutonu lelei)
- 'a e malava ko ia ke fenapasi, faka'uhinga'i mo fakamatala'i 'a e ngaahi me'a 'oku fai 'e ho'o sipinga (hange ko 'eni ki he tamate'i fanga ki'i manu vailasi, 'aotita pe talangofua ki ai); Mahalo 'e 'i ai ha ngaahi lelei ki hono faka'aonga'i 'o e ngaahi sipinga faingofua mo 'ikai puli 'i he ngaahi me'a lalahi mo faingata'a 'oku faingata'a ange ke faka'uhinga'i
- ngaahi 'ulungaanga 'o e ako dataset (ngaahi), kau ai 'a e lahi, angatonu, tu'unga lelei, ongo'ingofua, ta'u motu'a, mahu'inga mo e kehekehe

- 'a e mahu'inga 'o hono faka'aonga'i 'o e sipinga fakafefeka (hangē ko e ako ki he fili), regularisation mo e/pe ngaahi founga fakalahi 'o e tau'ataina fakafo'ituitui
- 'a e provenance mo e ngaahi seini 'o e ngaahi konga 'oku kau ai 'a e sipinga pe sipinga 'o e fakava'e, fakamatala ki he ako mo e ngaahi me'angaue 'oku fekau'aki mo ia

Ke ma'u ha fakamatala lahi ange fekau'aki mo e lahi 'o e ngaahi me'a ko 'eni 'oku ne uesia 'a e ngaahi ola malu'i, vakai ki he ngaahi tefito'i mo'oni 'o e NCSC ki hono malu'i 'o e misini ako ', kae tautautefito ki he fokotu'utu'u ki he malu(sipinga 'o e ngaahi fale).



2. Fa'unga 'oku malu

'Oku 'i he konga ko 'eni ha ngaahi fakahinohino 'oku fekau'aki mo e **fakalakalaka** 'i he tu'unga fakalakalaka 'o e polokālama mo e lōlōa ka ngāue ai, kau ai 'a e malu'i 'i he hokohoko seini hono tufaki fakamatala, me'a fakapepa, mo e koloa mo hono tokanga'i 'o e mo'ua fakatekinikale.

Malu'i ho'o kautaha tokoni

'Oku ke fakafuofua'i mo vakai'i 'a e malu 'o ho'o ngaahi seini 'i he siakale 'o e mo'ui 'a e polokalama, pea fie ma'u ha ngaahi kautaha hu koloa ke nau muimui ki he ngaahi tu'unga mo'ui tatau 'oku faka'aonga'i 'e ho'o organisation ki he ngaahi polokalama fakakomipiuta kehe. Kapau he 'ikai lava ke muimui 'a e ngaahi kautaha hu koloa ki he ngaahi tu'unga mo'ui 'a ho'o organisation, 'oku ke ngaue 'o fakatatau mo ho'o ngaahi tu'utu'uni ki hono tokanga'i 'o e ngaahi me'a 'oku tu'u fakatu'utamaki.

'I he feitu'u 'oku 'ikai fa'u ai 'i he fale, 'oku ke ma'u mo tauhi ha ngaahi naunau mo ha ngaahi polokalama fakakomipiuta lelei (hange ko 'eni, kau ta sipinga, fakamatala, ngaahi laipeli 'o e polokalama fakakomipiuta, 'eni, middleware, frameworks, mo e APIs 'i tu'a) mei hono fakapapau'i 'o e ma'u'anga tokoni fakakomesiale, fakaava, mo e fa'ahi tolu kehe developers ke fakapapau'i 'oku malu 'i ho'o polokalama.

'Oku ke mateuteu ke failover ki ha ngaahi founga kehe ki he ngaahi founga mahu'inga 'o e ngaue fakafaifekau, kapau 'oku 'ikai ke feau e tu'unga malu. 'Oku ke faka'aonga'i 'a e ngaahi ma'u'anga tokoni hange ko e NCSC ko e fakahinohino ki he seini mo e frameworks hange ko e ngaahi tu'unga 'o e seini ki he ngaahi koloa fakakomipiuta (SLSA)[10] ki hono muimui'i 'o e ngaahi seini mo e fakalakalaka 'o e polokalama ngaahi mo'ui 'a e polokalama.

Fakatokanga'i, muimui'i pea malu'i 'a ho'o ngaahi naunau

'Oku mahino kiate koe 'a e mahu'inga ki ho'o organisation 'o ho'o ngaahi koloa 'oku fekau'aki mo ia, kau ai 'a e kau ta sipinga, fakamatala (kau ai 'a e fakamatala ki he tokotaha ngaue), ue'i, polokalama fakakomipiuta, me'a fakapepa, sino'i 'akau mo e fakafuofua'i (kau ai 'a e fakamatala fekau'aki mo e ngaahi me'a 'oku 'ikai ke malu mo e ngaahi founga ta'elavame'a), recognising 'i he feitu'u 'oku nau fakafofonga'i ai ha attacker. 'Oku ke lau 'a e sino'i 'akau ko ha fakamatala pelepelengesi pea fakahoko 'a e pule'i ke malu'i 'enau tu'unga 'ikai fakahahaholo, angatonu mo e faingamalie.

'Oku ke 'ilo'i 'a e feitu'u 'oku nofo ai ho'o ngaahi koloa pea kuo ke fakafuofua'i mo tali ha fa'ahinga fakatu'utamaki 'oku fekau'aki mo ia. 'Oku 'i ai ho'o ngaahi founga ngaue mo e ngaahi me'angaue ke muimui'i, fakamo'oni'i, mapule'i mo malu'i ho'o ngaahi koloa, pea 'e lava ke toe fakafoki mai ki ha tu'unga lelei 'oku 'iloa 'i he me'a 'oku hoko.

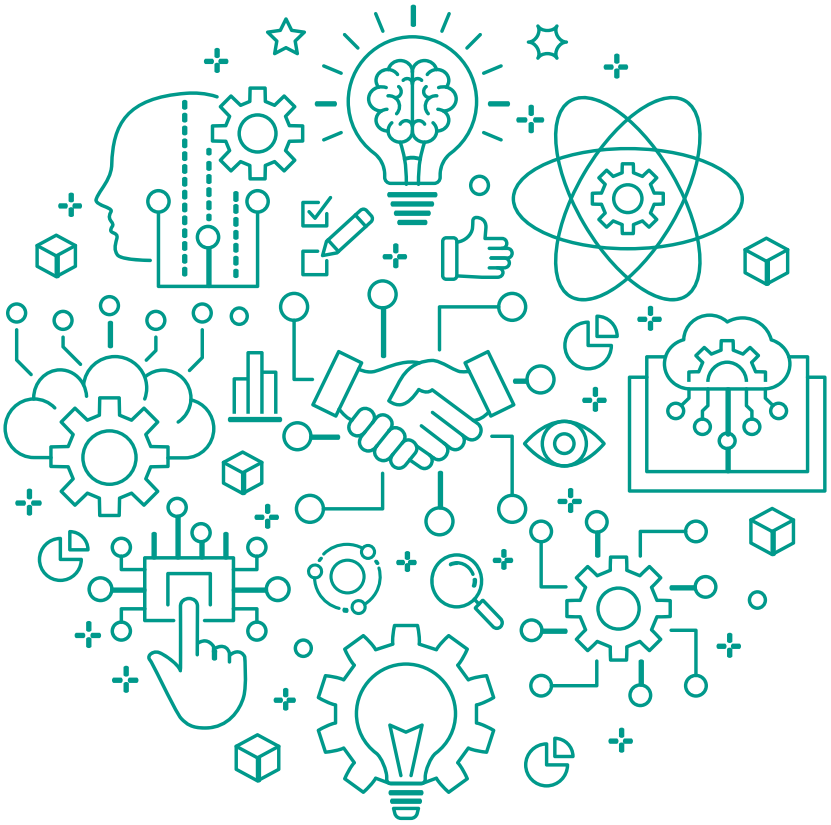
'Oku 'i ai ho'o ngaahi founga ngaue mo e pule'i ke tokanga'i 'a e me'a 'e lava ke ma'u 'e he ngaahi polokalama, pea ke tokanga'i 'a e me'a 'oku 'oatu 'e he 'i ai 'o fakatatau ki he'ene ongo'ingofua (pea mo e pelepelengesi 'o e ngaahi me'a na'e hoko 'i hono fa'u ia).

Faile 'a ho'o ngaahi fakamatala, ngaahi palani mo e ngaahi fakatokanga

'Oku ke hiki 'a e fakatupu, ngāue, mo hono tokanga'i 'o e mo'ui 'i ha fa'ahinga sipinga, seti hokohoko fakamatala mo e Sisitemi Vave Fakakomipiuta. 'Oku kau 'i ho'o fakamatala fakapepa 'a e fakamatala fekau'aki mo e malu'i hange ko e ngaahi ma'u'anga fakamatala ki he ako (kau ai 'a e fakamatala fakatonutonu lelei mo e fa'ahinga 'o e tangata pe ngaahi fakamatala kehe), 'a ia 'oku fakataumu'a ki ai 'a e lahi mo e ngaahi fakangatangata, ngaahi 'a pamu malu'i, cryptographic hashes pe fakamo'oni hingoa, taimi tauhi, 'oku fokotu'u atu ke toe vakai'i 'a e tu'o lahi mo e ngaahi founga 'e ala hoko. 'Oku kau 'i he ngaahi fale 'aonga ke tokoni 'i hono fai 'eni 'a e ngaahi kaati motolo, kaati fakamatala mo e ngaahi mo'ua 'o e polokālama fakakomipiuta (SBOMs). 'Oku poupou'i 'e hono fokotu'u 'o e fakamatala fakapepa faka'auliliki 'a e femahino'aki mo e taliui[11].

Tokanga'i ho'o mo'ua fakatekinikale

Hange ko ha fa'ahinga polokalama fakakomipiuta pe, 'oku ke 'ilo'i, muimui'i mo tokanga'i ho'o ' mo'ua fakatekinikale ' 'i he siakale 'o e mo'ui 'a e polokalama (ko e mo'ua fakatekinikale ko e feitu'u ia 'oku 'ikai ke 'i ai ha ngaahi founga lelei taha ke ma'u ai ha ngaahi ola taimi nounou, 'i he fakamole ki he ngaahi lelei taimi loloa ange). Hange ko e mo'ua fakapa'anga, 'oku 'ikai kovi 'a e mo'ua fakatekinikale, ka 'oku totonu ke tokanga'i ia mei he ngaahi 'uluaki tu'unga 'o e fakalakalaka[12]. 'Oku ke fakatokanga'i 'e lava ke faingata'a ange hono fai ia 'i ha tu'unga 'oku 'i ai 'i he polokalama fakakomipiuta angamaheni, pea 'oku ngalingali 'e ma'olunga ho'o ngaahi tu'unga 'o e mo'ua fakatekinikale koe'uhi ko e ngaahi fakalelei vave pe si'isi'i 'o e ngaahi me'a 'oku fokotu'u lelei mo e fofonga. 'Oku ke fakapapau'i 'oku ke 'ilo e palani 'o e taimi lava ai e polokālama 'o ngāue (kau ai 'a e ngaahi founga ki hono fakamafai'i e polokālama sisitemi ko ia) fakafuofua'i, fakahaa'i mo fakasi'isi'i 'a e ngaahi me'a 'oku tu'u fakatu'utamaki ki he ngaahi founga tatau 'i he kaha'u.



3. Fa'unga malu hono tukuatu

'Oku 'i he konga ko 'eni 'a e ngaahi fakahinohino 'oku fekau'aki mo e **deployment** 'i he tu'unga fakalakalaka 'o e mo'ui, kau ai hono malu'i 'o e fokotu'utu'u mo e kau ta sipinga mei he feveitokai'aki, fakamanamana pe mole, fakatupulaki e ngaahi founga tokanga'i 'o e me'a 'oku hoko, mo hono tuku atu 'o e fatongia.

Malu'i ho'o fokotu'utu'u

'Oku ke faka'aonga'i 'a e ngaahi tefito'i mo'oni malu'i lelei ki he fa'unga 'oku faka'aonga'i 'i he konga kotoa pe 'o e siakale 'o e mo'ui ho'o polokalama. 'Oku ke faka'aonga'i 'a e ngaahi founga totonu ki ho'o API, kau tā sipinga mo e fakamatala, pea ki he'enau ako mo e ngaue pipelines, 'i he fakatotolo mo e fakalakalaka pea pehē ki hono tuku atu. 'Oku kau heni 'a e vahevahe totonu 'o e ngaahi 'atakai 'oku ne pukepuke 'a e kouti pe fakamatala pelepelengesi. 'E toe tokoni foki 'eni ke fakasi'isi'i 'a e ngaahi 'ohofi malu'i angamaheni 'a ia 'oku fakataumu'a ke kaiha'asi ha sipinga pe uesia 'ene ngaue.

Malu'i hokohoko ho'o kalasi mōtolo ko ia

'E lava pe ke toe langa 'e he kau tau 'a e ngaue 'a ha sipinga[13] pe ko e fakamatala na'e ako'i 'i he[14], 'aki ha'o ma'u fakahangatonu ha sipinga ('aki hono ma'u ha sipinga mamafa) pe 'ikai fakahangatonu ('aki hano vakai'i e sipinga 'o fakafou 'i ha tohi kole pe ngāue tokoni). 'E lava foki ke kaunoa 'a e kau 'ohofi 'i he kau ta sipinga, fakamatala pe ue'i lolotonga pe hili 'a e ako, 'o fakahoko 'a e Output 'oku 'ikai falala'anga.

'Oku ke malu'i 'a e sipinga mo e fakamatala mei he hu fakahangatonu mo 'ikai fakahangatonu, 'aki 'a e:

- fakahoko 'o e ngaahi founga malu'i lelei taha 'i he 'Initaneti
- fakahoko hono pule'i 'o e fehu'i ke 'ilo'i mo ta'ofi e feinga ke hu, liliu, mo sivi 'i tu'a fakamatala 'oku 'ikai fakahahaholo

Ke fakapapau'i 'e lava 'e he ngaahi founga vela 'o fakapapau'i 'a e kau ta sipinga, 'oku ke fetukutuku mo vahevahe 'a e kalafi fakakulipitō mo e/pe ngaahi fakamo'oni hingoa 'o e ngaahi faile 'o e motolo (hange ko 'eni, sipinga mamafa) mo e seti fakamatala (kau ai 'a e lisi vakai'i) 'i he taimi pe 'oku ako'i ai 'a e sipinga. Hange ko ia 'oku hoko ma'u pe 'i he kalafifakakulipitō, 'oku mahu'inga 'a e tokanga'i lelei[15].

'E makatu'unga ho'o founga ki he tu'unga fakatu'utamaki 'oku 'ikai fakahahaholo 'i he me'a 'oku faka'aonga'i pea mo e sipinga fakamanamana. Hange ko 'eni, 'oku 'i ai ha ngaahi founga 'e ni'ihi 'oku kau ai 'a e fakamatala pelepelengesi, 'e ala fie ma'u ki ai ha ngaahi fakapapau'i faka'atamai 'e lava ke faingata'a pe mamafa ke faka'aonga'i. Kapau 'e fie ma'u, 'e lava ke faka'aonga'i 'a e ngaahi tekinolosia ki hono fakalahi 'o e tau'ataina fakafo'ituitui (hange ko e kehekehel fakafo'ituitui pe hahaka he hoko ha kovi fakakomipiuta) ke vakai'i pe fakapapau'i 'a e ngaahi tu'unga fakatu'utamaki 'oku fekau'aki mo e consumers, kau faka'aonga'i mo e kau faka'aonga'i 'oku nau lava 'o ma'u 'a e kau ta sipinga mo e ngaahi me'a 'oku nau ma'u.

Fa'ufa'u ha ngaahi founga ngāue ki hono tokanga'i 'o

'Oku ha 'a e pau 'o e ngaahi me'a 'oku hoko 'i he malu'i 'i ho'o tali ki he me'a 'oku hoko, fakafekiki tupulaki mo e ngaahi palani 'o e Fakalelei. 'Oku ha mei ho'o ngaahi palani ha ngaahi tukunga kehekehe pea 'oku reassessed ma'u pe ia ko e polokālama mo e fekumi lahi ange ki he'ene liliu. 'Oku ke tauhi ha ngaahi ma'u'anga tokoni faka'ilekitulonika mahu'inga 'i tokateu 'oku 'ikai ma'u ai e 'Initaneti. Kuo ako'i 'a e kinautolu ke nau Ngāue Fakavavevave ki ha me'a mo ngāue ki ha ngaahi me'a 'oku fekau'aki mo AI. 'Oku ke 'omi ha ngaahi sino'i 'aotita lelei mo ha ngaahi me'a malu'i kehe pe fakamatala ki he kau fakatau mo e kau faka'aonga'i 'i ha toe totongi, ke lava 'o fakahoko 'enau ngaahi founga tali ki he me'a 'oku hoko.

Tukuange fakapotopoto 'a e AI

'Oku ke tukuange 'a e kau ta sipinga, faka'aonga'i pe ngaahi polokalama hili pe hono fakamo'ulaloa'i kinautolu ki he fakafuofua'i totonu mo lelei 'o hange ko e benchmarking mo e teaming kulokula (pea pehe ki he ngaahi sivi kehe 'oku 'ikai ke 'i ai ha me'a ki he ngaahi fakahinohino ko 'eni, hange ko e malu pe tu'unga totonu), pea 'oku ke mahino ki ho'o kau faka'aonga'i fekau'aki mo e ngaahi fakangatangata pe ngaahi founga 'e ala hoko. 'Oku 'oatu 'a e fakaikiiki 'o e ngaahi laipeli ki hono sivi'i 'o e malu'i 'i he toe lau 'a e konga 'i he faka'osinga 'o e fakamatala ko 'eni.

Fakafaingofua ki he kau kasitoma kenau fai 'a e ngaahi me'a 'oku totonu

'Oku ke fakatokanga'i ko e feitu'u fo'ou pe fokotu'utu'u fo'ou kotoa pe ke fakafuofua'i fakataha mo e pisinisi 'oku 'aonga ki ai, pea mo ha fa'ahinga me'a 'oku tu'u fakatu'utamaki 'oku ne fakafe'iloaki mai. Ko hono mo'oni, ko e feitu'u malu taha 'e fakakau ia ki he polokalama ko e fili pe ia taha 'oku tonu ki ai. 'I he taimi 'oku fie ma'u ai 'a e fokotu'utu'u, 'oku totonu ke malu 'aupito 'a e fili kuo 'osi fakapolokalama'i mei he ngaahi fakamanamana angamaheni ('a ia, 'oku malu 'i he peesi tu'uma'u). 'Oku ke faka'aonga'i 'a e pule'i ke ta'ofi hono faka'aonga'i pe deployment ho'o polokalama 'i ha ngaahi founga kaka.

'Oku ke 'oange ki he kau faka'aonga'i ha fakahinohino ki hono faka'aonga'i totonu ho'o sipinga pe polokalama, 'a ia 'oku kau ai hono faka'ilonga'i 'o e ngaahi fakangatangata mo e ngaahi founga 'e ala hoko ai e ta'elavame'a. 'Oku ke fakamatala'i mahino ki he kau faka'aonga'i 'a e ngaahi tafa'aki 'o e malu'i 'oku nau fatongia 'aki, pea 'oku 'ikai puli 'a e feitu'u (mo e founga) 'e lava ke faka'aonga'i ai 'enau fakamatala, ma'u pe tauhi (hange ko 'eni, kapau 'oku faka'aonga'i ia ki he sipinga 'o e ako, pe toe vakai'i 'e he kau ngaue pe hoa).

4. Malu 'a e fakahoko ngāue mo hono tokanga'i

'Oku 'i he konga ko 'eni ha ngaahi fakahinohino 'oku fekau'aki mo e **ngaue malu mo hono tokanga'i** 'o e 'oku 'i ai e siakale 'o e mo'ui fakalakalaka 'a e System. 'Oku ne 'omi ha ngaahi fakahinohino ki he ngaahi ngaue 'oku matu'aki mahu'inga 'i he taimi kuo pālani ai ha polokalama, kau ai 'a e loka mo hono vakai'i, fakatonutonu 'o e tokanga'i mo e fakamatala 'oku vahevahe.

Vakai'i e behaviour ho'o polokalama

'Oku ke fakafuofua'i 'a e ngaahi me'a 'oku ne 'omi mo hono fakahoko ho'o motolo mo e polokālama koe'uhi ke ke lava 'o mamata ki he ngaahi liliu fakafokifa mo māmalie 'i ha to'onga 'oku ne uesia 'a e malu. Te ke lava 'o fakamatala'i mo 'ilo ki he ngaahi me'a 'e ala hoko mo uesia, pea pehe ki ha mafuli e fakamatala mo hono fa'unga fakanatula.

Vakai'i e ngaahi me'a 'oku fai 'e ho'o polokalama

'I he laine mo e ngaahi fie ma'u ki he malu'i 'o e fakamatala fakafo'ituitui mo e fakamatala, 'oku ke vakai'i mo lekooti 'a e ngaahi me'a 'oku fakahu ki ho'o polokalama (hange ko e ngaahi kole fakatonu'i, faka'eke'eke pe ue'i) ke lava 'o talangofua ki he ngaahi fatongia, 'aotita, fakatotolo mo e Fakalelei 'i he tu'unga 'o e feveitokai'aki pe faka'aonga'i hala. 'E lava ke kau heni 'a e fakatokanga mahino ki he ngaahi me'a 'oku fai ki ai e tufaki'anga naunau mo e/pe ko e ngaahi me'a 'oku fai ki ai e fili, kau ai 'a kinautolu 'oku fakataumu'a ke ngaue 'aki e ngaahi sitepu ki hono teuteu'i 'o e fakamatala (hange ko hono holoki mo e fakalahi pē fakasi'isi'i e ngaahi 'imisi).

Muimui 'i ha founga malu 'i he founga fokotu'utu'u ki he fakamatala fakamuimuitaha

'Oku ke fakakau 'a e ngaahi fakamatala fakamuimuitaha 'i he peesi tu'uma'u 'i he koloa kotoa pe pea faka'aonga'i 'a e ngaahi founga fakamuimuitaha 'o e fakamatala fakamuimuitaha ke tufaki kinautolu. 'Oku hanga 'e ho'o founga fakatonutonu (kau ai hono sivi'i mo fakafuofua'i fa'unga fakalele) 'o fakahaa'i 'a e fo'i mo'oni ko ia 'e lava ke iku 'a e ngaahi liliu ki he fakamatala, kau ta sipinga pe ue'i ki he ngaahi liliu 'i he Sistemi fakae'ulungaanga ngāue fakjakomipiuta (hange ko 'eni, 'oku ke fai ha ngaahi liliu lalahi hange ko e ngaahi polokālama fo'ou). 'Oku ke poupou'i 'a e kau faka'aonga'i ke nau fakafuofua'i mo tali 'a e ngaahi liliu ki he motolo (hange ko 'eni 'aki hono tomu'a vakai'i mo kalasi fo'ou 'o e API).

Tanaki mo vahevahe 'a e ngaahi lesoni kuo ako

'Oku ke kau 'i he ngaahi kolo 'oku nau vahevahe 'a e fakamatala, 'i he 'atakai fakaemamani lahi 'o e ngāue, ako'anga mo e ngaahi pule'anga ke vahevahe 'a e founga lelei taha 'o ka fiema'u. 'Oku ke tauhi 'a e ngaahi laine 'oku fakaava 'o e fetu'utaki ki he ngaahi fakamatala fekau'aki mo e malu'i 'o e polokalama, 'i loto mo tu'a fakatou'osi 'i he kautaha, kau ai 'a e fakangofua ki he kau fakatotolo malu'i ke nau fekumi mo lipooti 'a e ngaahi matavaivai fakakomipiuta. 'I he taimi 'oku fie ma'u ai, 'oku ke toe lahi ange 'a e ngaahi palopalema ki he kolo lahi ange, hange ko 'eni ko hono pulusi bulletins tali ki he disclosures laveangofua, kau ai 'a e fakaikiiki mo e ngaahi me'a angamaheni 'oku ala tu'u laveangofua hokohoko. 'Oku ke fai ha ngaue ke fakalelei'i mo remediate vave mo totonu 'a e ngaahi palopalema.

Tohi toe fakamatala ki ai

Fa'unga 'o e AI

Ngaahi tefito'i mo'oni ki hono malu'i 'o e ako 'o e misini
Ko e fakahinohino fakaikiiki 'a e NCSC ki hono fakatupulaki, tukuatu 'o e polokālama pe fakalele ha polokalama 'oku 'i ai ha konga ML.

Malu 'i hono fokotu'utu'u 'o e palanisi 'o e Malu 'Initaneti 'e tu'u fakatu'utamaki: Ngaahi tefito'i mo'oni mo e ngaahi founga ke malu'i 'aki e polokalama fakakomipiuta
Kaunga-fa'u 'e CISA, ko e NCSC mo e ngaahi kautaha kehe, 'oku fakamatala'i 'e he fakahinohino ko 'eni 'a e founga 'oku totonu ke fai ai 'e he kau fa'u polokalama fakakomipiuta, kau ai 'a e ngaahi sitepu ki he tu'unga malu 'o e fakalakalaka 'o e koloa, mo e ngaahi naunau 'oku ma'u mei he puha.

'Oku 'i ai ha ngaahi hoha'a ki he malu'i 'i ha tali mahino ngofua falute
Na'e fa'u 'e he 'ofisi 'o e Fetulolo 'o Siamane ki he malu'i 'o e fakamatala (BSI), 'oku 'omi 'e he fakamatala ko 'eni ha talateu ki he ngaahi 'ohofi 'e ala hoko 'i he founga ako 'o e misini mo e me'a 'e malava malu'i ngaahi 'ohofi ko ia.

Founga ngaue fakavaha'apule'anga ki hono fakatupulaki 'o e ngaahi houalotu ko hono fakatupulaki 'o e ngaahi System mo e Hiroshima founga ngaue fakavaha'apule'anga 'o e 'ulungaanga ma'a e ngaahi houalotu ko hono fakatupulaki 'o e ngaahi sisitemi
Ko e ngaahi fakamatala fakapepa ko 'eni, 'a ia na'e fa'u ko e konga 'o e G7 Hilosima 'oku 'i ai e founga ngaue, 'omi ha fakahinohino ki he NGAAHI Kautaha nau fakatupulaki 'o e ngaahi founga fakalakalaka taha, kau ai 'a e ngaahi sipinga 'o e fakava'e ma'olunga taha mo e ngaahi founga 'oku 'i ai e taumu'a 'o e malu, malu, mo falala'anga AI 'i he funga 'o e māmani.

Ko hono fakapapau'i 'e he AI
'A e Fa'unga Pule Lelei ke Tesi'i AI 'a Singapoa mo e polokālama fakakomipiuta 'oku ne fakapapau'i 'a e sai e fakahoko fatongia 'a e sisitemi AI ha'ane fehangahangai mo e ngaahi kaveinga fakamamani lahi 'i he fai ko ia hono tesi'i e tu'unga 'oku 'i ai.

'Oku 'i ai e Levolo kehekehe 'o e fa'unga ki he ngaahi founga lelei Malu 'o e 'Initaneti ki he AI — ENISA (europa.eu)
Ko ha fa'unga ke tataki 'a e kau ma'u mafai fakafonua mo e 'i ai stakeholders 'i he ngaahi sitepu 'oku fie ma'u ke nau muimui ki ai ke ma'u 'enau ngaahi polokalama, fakalele mo e founga ngāue.

ISO 5338: Ko e fuoloa pē taimi 'e lava e fakahoko fatongia 'a e Sisitemi 'o ha AI 'o ngāue ai('oku toe vakai'i)
Ko ha ngaahi founga ngāue mo ha ngaahi fakakaukau fekau'aki mo hono fakamatala'i e lōlōa 'e lava ngāue ai 'a e polokālama AI 'o fakatefito 'i he misini fakakomipiuta mo e sisitemi 'ako pe 'iate kita.

'Oku 'i ai e tu'unga 'o e ngaue tokoni 'i he 'ao Catalogue (AIC4)
'Oku 'i ai e tu'unga 'o e ngaue tokoni 'a e SI Catalogue 'oku ne 'omi ha ngaahi me'a pau, 'a ia 'e lava ke fakafuofua'i ai 'a e malu 'o ha ngāue e AIt.

NIST IR 8269 (fakaangaanga) ko ha Tekisinomi mo e ngaahi lea 'o e ako 'o e misini 'o e fili
Ko ha ngaahi founga ngaue mo ha ngaahi fakakaukau fekau'aki mo hono fakamatala'i 'o e siakale 'o e mo'ui 'o makatu'unga 'i he ako 'o e misini mo e ngaahi polokalama.

MITRE ATLAS
Ko ha fakava'e 'o e ngaahi founga 'a e fili, ngaahi founga, mo e ngaahi me'a ke ako mei ai ki he ako 'o e misini (ML), modelled hili mo fakafehokotaki ki MITRE ATT & CK fa'unga.

Ko ha vakaSenitālukufua ki he ngaahi me'a 'oku tu'u fakaSenitāmaki (2023)
Na'e fa'u 'e he senitaa ki he malu, 'oku fokotu'u 'e he fakamatala ko 'eni ha ngaahi feitu'u 'oku tu'u fakatu'utamaki 'i he 'i ai.

Kau ta sipinga 'o e lea fakafonua lalahi: Ngaahi faingamalie mo e ngaahi fakatu'utamaki ki he ngaue mo e kau ma'u mafai
Fakamatala na'e fa'u 'e he SI ma'a e ngaahi kautaha, kau ma'u mafai mo e developers 'oku nau fie ako lahi ange fekau'aki mo e ngaahi faingamalie mo e ngaahi fakatu'utamaki 'o e fakatupulaki, deploying mo e/pe faka'aonga'i 'a e LLMs.

Ngaahi ngaue ki hono fakaava 'o e ma'u'anga tokoni ke tokoni ki he kau faka'aonga'i 'o e sivi malu'i 'oku kau ai 'a e:

- Ko e Naunau ke Matatali Lahi Uesia Takihala'i 'o e Polokālama Fakakomipiuta (IBM)
- CleverHans ('Univesiti 'o Tolonitoo)
- TextAttack ('Univesiti 'o Veisinia)
- Ue'i 'a e sea (Microsoft)
- Counterfit (Microsoft)
- 'I ai hono fakapapau'i (Fakatāmakinfocomm mafai fakalakalaka 'o e mitiFakatāmakia)

Malu mei he Fakatamaki mei he 'Initaneti

Ngaahi taumu'a 'o e ngaue Cybersecurity 'a CISA
Ko ha ngaahi malu'i angamaheni 'oku totonu ke fakahoko 'e he ngaahi kautaha mahu'inga kotoa pe ke fakasi'isi'i 'a e malava mo e ola 'o e ngaahi me'a 'oku tu'u fakatu'utamaki mo e ngaahi founga 'a e fili.

NCSC CAF fa'unga
'Oku 'omi 'e he fa'unga 'o e fakafuofua'i 'o e 'Initaneti (CAF) ha fakahinohino ki organisations fatongia 'aki e ngaahi tokoni mo e ngaahi 'ekitiviti mahu'inga.

Ko e fa'unga malu'i 'o e seini MITRE
Ko ha fa'unga ki hono fakafuofua'i 'o e ngaahi kautaha hu koloa mo e kau ngaue tokoni 'i he seini.

Tokanga'i 'a e Tu'unga Fakatu'utmaki

NIST 'oku 'i ai ha fa'unga pule 'oku tu'u fakatu'utamaki ('i ai RMF)
'Oku fakamatala'i 'e he RMF 'a e founga ke tokanga'i 'aki e ngaahi me'a 'oku tu'u fakatu'utamaki ki he fakafo'ituitui, organisations, mo e sosaieti 'oku fekau'aki makehe mo e 'i ai.

ISO 27001: Oku 'omi 'e he tu'unga mo'ui ko 'eni 'a e malu'i 'o e fakamatala, Malu'i 'Initaneti mo e malu'i fakafo'ituitui
'Oku 'omi 'e he tu'unga mo'ui ko 'eni ha fakahinohino ki hono fokotu'u, fakahoko mo hono tokanga'i 'o ha fakamatala ki hono tokanga'i 'o e fakamatala.

Ngaahi Kautaha Fakavaha'apule'anga ki he Ngaahi Tu'unga Fakangaue (ISO) 31000: Tokanga'i 'a e Tu'unga Fakatu'utamaki
Ko ha tu'unga mo'ui fakavaha'apule'anga 'oku ne 'omi kautaha 'a e ngaahi fakahinohino mo e ngaahi tefito'i mo'oni ki hono tokanga'i 'o e ngaahi me'a 'oku tu'u fakatu'utamaki 'i he ngaahi kautaha.

NCSC e fakahinohino ki hono tokanga'i 'o e tu'unga fakatu'utamaki
'Oku tokoni 'a e fakahinohino ko 'eni ki he tu'unga malu 'o e malu'i ke mahino lelei ange mo tokanga'i 'a e ngaahi me'a 'oku tu'u fakatu'utamaki ki he malu'i 'oku ne uesia 'enau organisations.

Ngaahi Nouti

1. 'Oku faka'uhinga'i heni ko ha tokotaha, mafai fakapule'anga, tau'ataina ke fili pe ko ha sino kehe 'oku ne fakatupulaki ha founga 'oku 'i ai (pe 'oku 'i ai ha founga 'oku fakatupulaki) mo e ngaahi feitu'u 'oku 'i ai e polokalama 'i he maketi pe fokotu'u ia ki he ngaue tokoni 'i hono hingoa pe faka'ilonga
2. Ke ma'u ha fakamatala lahi ange fekau'aki mo e malu 'i he palani, vakai ki he CISA malu 'i he fokotu'utu'u peesi uepisaiti mo e fakahinohino liliu 'a e palanisi 'o Malu e 'Initaneti tu'u fakatu'utamaki: Ngaahi tefito'i mo'oni mo e ngaahi founga ke malu'i 'aki e Design Software
3. Kae 'ikai ko e ngaahi founga 'oku 'ikai ML ai 'a e ngaahi founga hange ko e ngaahi founga 'oku makatu'unga 'i he lao
4. 'Oku fakamatala'i 'e CEPS 'a e fa'ahinga kehekehe 'e fitu 'o e fengaue'aki fakalakalaka 'i he'enau pulusi 'fakatatau 'a e seini mahu'inga mo e ngaue 'a e EU poto loi'
5. ISO/IEC 22989:2022 (en) faka'uhinga'i 'eni ko ha ' 'elemeniti 'oku lele ke fa'u ai ha polokālama '
6. 'Oku tasked 'a e NIST 'i hono fa'u 'o e ngaahi fakahinohino (mo e ngaahi ngaue kehe) ke laka ki mu'a 'a e fakalakalaka malu, malu, mo falala'anga pea mo hono faka'aonga'i 'o e poto loi ('i ai). Vakai ki he ngaahi fatongia 'o NIST 'i he 'aho 30 'o 'Okatopa, 2023 'ota pule
7. 'Oku lava ke ma'u ha fakamatala lahi ange fekau'aki mo e mōtolo ke tala e fakamanamana pe palopalema mei he Kautaha Makatu'upau OWASP
8. Vakai, MITRE ATLAS ako 'o e misini 'o e fili 101
9. GitHub: RCE PoC ki he Tensorflow 'o faka'aonga'i ha me'a 'oku ne uesia Lambda
10. SLSA: 'malu'i Sisita Hetili angatonu 'i ha fa'ahinga polokalama fakakomipiuta pe'
11. METI (ngaue faka-Siapani 'o e tu'unga faka'ekonomika, fefakatau'aki mo e fa'a ngaue, 2023), 'fakahinohino ki hono fakafe'iloaki 'o e polokalama fakakomipiuta tohimo'ua 'o e ngaahi naunau (SBOM) ki hono tokanga'i 'o e polokalama fakakomipiuta'
12. Fekumi 'a e Kukolo: Ako 'o e misini fakakomipiuta: Ko e kaati fakamo'ua ma'olunga 'o e mo'ua fakatekinikale
13. Tramèr et Al 2016, Ngaahi Sipinga 'o e Ako 'a e Misini Fakakomipiuta ke Takihala'i ha polokālama 'o fakafou 'i hano Tala 'e he APIs
14. Boenisch, 2020, ngaahi 'ohofi ki he ako 'o e misin fakakomipiutai (konga 1): Sipinga 'o e ngaahi 'ohofi 'o e Senitāuaki mo e fa'unga IBM-ART
15. Senitā malu'i fakafonua 'o e 'Initaneti, 2020, fokotu'utu'u mo langa ha Fale Fakapule'anga Pau Ma'ae Kakai