TLP:CLEAR

សន្តិសុខតាមការរចនា

ការផ្លាស់ប្តូរតុល្យភាពនៃ
ហានិភ័យសន្តិសុខអ៊ីនធឺណិត៖

គោលការណ៍ និងវិធីសាស្ត្រសម្រាប់
សូហ្វវែរសន្តិសុខតាមការរចនា

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

មាតិកា

ទិដ្ឋភាពទូទៅ៖ ភាពងាយរងគ្រោះតាមការរចនា

បច្ចេកវិទ្យាត្រូវបានដាក់បញ្ចូលទៅក្នុងស្ទើរតែគ្រប់ទិដ្ឋភាពនៃជីវិតប្រចាំថ្ងៃ ដោយសារប្រព័ន្ធនានាដែលដាក់ដំណើរការតាមរយៈអ៊ីនធឺណិតភ្ជាប់យើងទៅប្រព័ន្ធសំខាន់ៗកាន់តែច្រើន ដែលជះឥទ្ធិពលដោយផ្ទាល់ទៅលើភាពចម្រុងចម្រើន ខាងសេដ្ឋកិច្ច ជីវភាពរស់នៅ និងសូម្បីតែសុខភាពរបស់យើងចាប់ពីការគ្រប់គ្រងអត្តសញ្ញាណផ្ទាល់ខ្លួន រហូតដល់ការថែទាំវេជ្ជសាស្ត្រ។ ឧទាហរណ៍មួយនៃគុណវិបត្តិនៃភាពងាយស្រួលបែបនេះ គឺការបំពានលើសុវត្ថិភាពអ៊ីនធឺណិតជាសកល ដែលបណ្តាលឱ្យមន្ទីរពេទ្យត្រូវលុបចោលការវះកាត់ និងបង្វែរការថែទាំអ្នកជំងឺ។ បច្ចេកវិទ្យាដែលគ្មានសន្តិសុខ និងភាពងាយរងគ្រោះនៅក្នុងប្រព័ន្ធសំខាន់ៗ អាចបង្កឱ្យមានការឈ្លានពានព្យាបាទតាមអ៊ីនធឺណិតដែលមានគំនិតទុច្ចរិត ដែលឈានទៅដល់ហានិភ័យ[1] សុវត្ថិភាពដែលអាចកើតឡើង។

ជាលទ្ធផល វាមានសារៈសំខាន់ណាស់សម្រាប់ក្រុមហ៊ុនផលិតសូហ្វវែរធ្វើឱ្យមានសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើមនូវចំណុចស្នូលនៃដំណើរការរចនា និងដំណើរការនៃការអភិវឌ្ឍផលិតផល។ អ្នកលក់មួយចំនួនបានបោះជំហានទៅមុខយ៉ាងសម្បើមក្នុងការជំរុញឧស្សាហកម្មនេះឆ្ពោះទៅមុខក្នុងការធានាដល់សូហ្វវែរ ខណៈពេលដែលអ្នកផ្សេងទៀតនៅយឺតយ៉ាវ។ ស្ថានប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ លើកទឹកចិត្តយ៉ាងខ្លាំងដល់ក្រុមហ៊ុនផលិតបច្ចេកវិទ្យាទាំងអស់ ឱ្យបង្កើតផលិតផលរបស់ពួកគេដោយផ្អែកលើការកាត់បន្ថយបន្ទុកនៃសន្តិសុខអ៊ីនធឺណិតលើអតិថិជន រួមទាំងការបង្ការពួកគេមិនឱ្យធ្វើការត្រួតពិនិត្យជាប្រចាំ ការធ្វើបច្ចុប្បន្នភាពជាប្រចាំ និងការគ្រប់គ្រងការខូចខាតលើប្រព័ន្ធរបស់ពួកគេ ដើម្បីកាត់បន្ថយការបំពានតាមអ៊ីនធឺណិត។ យើងក៏ជំរុញឱ្យក្រុមហ៊ុនផលិតសូហ្វវែរ បង្កើតផលិតផលរបស់ពួកគេតាមរបៀបមួយ ដែលសម្របសម្រួលស្ម័យប្រវត្តិកម្មនៃការកំណត់រចនាសម្ព័ន្ធ ការត្រួតពិនិត្យ និងការធ្វើបច្ចុប្បន្នភាពជាប្រចាំ។ ក្រុមហ៊ុនផលិតនានាត្រូវបានលើកទឹកចិត្តឱ្យទទួលយកភាពជាម្ចាស់ នៃការកែលម្អលទ្ធផលសន្តិសុខរបស់អតិថិជនពួកគេ។ ជាប្រវត្តិសាស្ត្រ ក្រុមហ៊ុនផលិតសូហ្វវែរ បានពឹងផ្អែកលើការជួសជុលភាពងាយរងគ្រោះដែលបានរកឃើញបន្ទាប់ពីអតិថិជនបានប្រើប្រាស់ផលិតផលរបស់ពួកគេ ដោយតម្រូវឱ្យអតិថិជនជួសជុលកង្វះខាតទាំងនោះ ដោយចំណាយផ្ទាល់ខ្លួនរបស់ពួកគេ។ មានតែតាមរយៈការដាក់បញ្ចូលការអនុវត្តសន្តិសុខតាមការរចនាប៉ុណ្ណោះ ដែលយើងនឹងបំបែកវដ្តទុច្ចរិតនៃការបង្កើត និងធ្វើការជួសជុលឥតឈប់ឈរ។ **កំណត់ចំណាំ៖** ពាក្យ "សន្តិសុខតាមការរចនា" រួមបញ្ចូលទាំងសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម។

ដើម្បីសម្រេចបាននូវស្តង់ដាខ្ពស់នៃសន្តិសុខសូហ្វវែរ ស្ថានប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យលើកទឹកចិត្ត ក្រុមហ៊ុនផលិតឱ្យផ្តល់អាទិភាពដល់ការដាក់បញ្ចូលសន្តិសុខផលិតផលជាលក្ខណៈតម្រូវជាមុនសំខាន់ៗ សម្រាប់លក្ខណៈពិសេសនៃផលិតផល និងល្បឿនទៅកាន់ទីផ្សារ។ យូរៗទៅ ក្រុមវិស្វករនឹងអាចបង្កើតចង្វាក់ស្ថិរភាពថ្មីមួយ ដែលសន្តិសុខត្រូវបានរចនាយ៉ាងពិតប្រាកដនៅក្នុងផលិតផល ហើយចំណាយការខិតខំប្រឹងប្រែងតិចតួចក្នុងការថែរក្សា។

ដោយឆ្លុះបញ្ចាំងពីទស្សនៈនេះ សហភាពអឺរ៉ុបបានពង្រឹងសារៈសំខាន់នៃសន្តិសុខផលិតផលនៅក្នុងច្បាប់ស្តីពីភាពធន់តាមប្រព័ន្ធអ៊ីនធឺណិត ដោយសង្កត់ធ្ងន់ថា ក្រុមហ៊ុនផលិតគួរតែអនុវត្តសន្តិសុខពេញវដ្តនៃជីវិតរបស់ផលិតផល ដើម្បីទប់ស្កាត់ក្រុមហ៊ុនផលិតពីការបញ្ចេញផលិតផលដែលងាយរងគ្រោះមកលក់ក្នុងទីផ្សារ។

[1] ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យទទួលស្គាល់ថាពាក្យ "សុវត្ថិភាព" មានអត្ថន័យច្រើន ដោយអាស្រ័យលើបរិបទដែលគេប្រើវា។ សម្រាប់គោលបំណងនៃការណែនាំនេះ "សុវត្ថិភាព" នឹងសំដៅលើការបង្កើនស្តង់ដារសន្តិសុខបច្ចេកវិទ្យា ដើម្បីការពារអតិថិជនពីសកម្មភាពទុច្ចរិតតាមអ៊ីនធឺណិត។

ដើម្បីបង្កើតអនាគតមួយដែលបច្ចេកវិទ្យា និងផលិតផលពាក់ព័ន្ធមានសុវត្ថិភាពជាងមុនសម្រាប់អតិថិជន ស្ថានប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ជំរុញឱ្យក្រុមហ៊ុនផលិតធ្វើការកែលម្អការរចនា និងកម្មវិធីអភិវឌ្ឍន៍របស់ពួកគេឡើងវិញ ដើម្បីអនុញ្ញាតឱ្យមានតែផលិតផលដែលមានសន្តិសុខតាមការរចនា និងតាមលំនាំដើមប៉ុណ្ណោះសម្រាប់ការដឹកជញ្ជូនទៅកាន់អតិថិជន។ មុនការអភិវឌ្ឍផលិតផលដែលមានសន្តិសុខតាមការរចនាត្រូវបានយល់ឃើញដោយមានសន្តិសុខរបស់អតិថិជន ថាជាគោលដៅអាជីវកម្មស្នូល មិនមែនគ្រាន់តែជាលក្ខណៈពិសេសបច្ចេកទេសប៉ុណ្ណោះទេ។ ផលិតផលដែលមានសន្តិសុខតាមការរចនាចាប់ផ្តើមជាមួយនឹងគោលដៅនោះ មុនពេលការអភិវឌ្ឍចាប់ផ្តើម។ ផលិតផលដែលមានស្រាប់អាចវិវឌ្ឍទៅរកស្ថានភាពសន្តិសុខតាមការរចនា ជាងការធ្វើម្តងទៀតជាច្រើនដង។ ផលិតផលដែលមានសន្តិសុខតាមលំនាំដើម គឺជាផលិតផលដែលមានសន្តិសុខក្នុងការប្រើប្រាស់ "ចេញពីប្រអប់" ដែលគ្មាន ឬមានការផ្លាស់ប្តូរចនាសម្ព័ន្ធចាំបាច់តិចតួច និងលក្ខណៈពិសេសនៃសន្តិសុខដែលអាចរកបានដោយគ្មានការចំណាយបន្ថែម។ រួមគ្នា ទស្សនទាំងពីរនេះផ្លាស់ទីបន្ទុកនៃការរក្សាសុវត្ថិភាពទៅក្រុមហ៊ុនផលិត ហើយកាត់បន្ថយឱកាសដែលអតិថិជននឹងរងគ្រោះដោយសារឧប្បត្តិហេតុសន្តិសុខ ដែលបណ្តាលមកពីការកំណត់រចនាសម្ព័ន្ធមិនត្រឹមត្រូវ ការជួសជុលកង្វះខាតរហ័សមិនបានគ្រប់គ្រាន់ ឬបញ្ហាទូទៅជាច្រើនផ្សេងទៀត។

ទីភ្នាក់ងារសន្តិសុខអ៊ីនធឺណិត និងសន្តិសុខហេដ្ឋារចនាសម្ព័ន្ធ (CISA), ទីភ្នាក់ងារសន្តិសុខជាតិ (NSA), ការិយាល័យស៊ើបអង្កេតសហព័ន្ធ (FBI) និងដៃគូអន្តរជាតិដូចខាងក្រោមនេះ[2] ផ្តល់អនុសាសន៍នៅក្នុងការណែនាំនេះ ថាជាផែនទីបង្ហាញផ្លូវសម្រាប់ក្រុមហ៊ុនផលិតសូហ្វវែរ ដើម្បីធានាសន្តិសុខផលិតផលរបស់ពួកគេ៖

- » មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតរបស់អូស្ត្រាលី (ACSC)
- » មជ្ឈមណ្ឌលកាណាដាសម្រាប់ការពារសន្តិសុខអ៊ីនធឺណិត (CCCS)
- » មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ចក្រភពអង់គ្លេស (NCSC-UK)
- » ការិយាល័យសហព័ន្ធសម្រាប់សន្តិសុខព័ត៌មាន (BSI) របស់អាល្លឺម៉ង់
- » មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ហូឡង់ (NCSC-NL)
- » មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ន័រវេស (NCSC-NO)
- » ក្រុមឆ្លើយតបបន្ទាន់តាមកុំព្យូទ័ររបស់នូវែលសេឡង់ (CERT NZ) និងមជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់នូវែលសេឡង់ (NCSC-NZ)
- » ទីភ្នាក់ងារសន្តិសុខ និងអ៊ីនធឺណិតរបស់កូរ៉េ (KISA)
- » អគ្គនាយកដ្ឋានអ៊ីនធឺណិតជាតិរបស់អ៊ីស្រាអែល (INCD)
- » មជ្ឈមណ្ឌលជាតិនៃការត្រៀមសម្រាប់ឧប្បត្តិហេតុ និងយុទ្ធសាស្ត្រសម្រាប់សន្តិសុខអ៊ីនធឺណិតរបស់ជប៉ុន (NISC) និងមជ្ឈមណ្ឌលសម្របសម្រួលក្រុមឆ្លើយតបបន្ទាន់តាមកុំព្យូទ័ររបស់ជប៉ុន (JPCERT/CC)
- » បណ្តាញ OAS/CICTE នៃក្រុមឆ្លើយតបឧប្បត្តិហេតុតាមអ៊ីនធឺណិតរបស់រដ្ឋាភិបាល (CSIRT) អាមេរិក
- » ទីភ្នាក់ងារសន្តិសុខអ៊ីនធឺណិតនៃប្រទេសសិង្ហបុរី (CSA)
- » ទីភ្នាក់ងារសន្តិសុខអ៊ីនធឺណិត និងព័ត៌មានជាតិនៃសាធារណរដ្ឋឆេក (NÚKIB)

ស្ថានប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ទទួលស្គាល់ចំពោះការរួមចំណែកដោយដៃគូវិស័យឯកជនជាច្រើនក្នុងការជំរុញសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម។ ផលិតផលនេះមានគោលបំណងជំរុញការសន្ទនាអន្តរជាតិអំពីអាទិភាពសំខាន់ៗ ការវិនិយោគ និងសេចក្តីសម្រេចដែលចាំបាច់ ដើម្បីសម្រេចបានអនាគតមួយដែលបច្ចេកវិទ្យាមានសុវត្ថិភាព សន្តិសុខ និងភាពធន់តាមការរចនា និងលំនាំដើម។ នៅចុងបញ្ចប់នោះ ស្ថានប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យស្វែងរកមតិកែលម្អលើផលិតផលនេះ ពីភាគីនានាដែលចាប់អារម្មណ៍ ហើយមានបំណងរៀបចំវគ្គស្តាប់ជាបន្តបន្ទាប់ដើម្បីកែលម្អបន្ថែមបញ្ហាក់ និងជំរុញការណែនាំរបស់យើង ដើម្បីសម្រេចបាននូវគោលដៅរួមរបស់យើង។

សម្រាប់ព័ត៌មានបន្ថែមអំពីសារៈសំខាន់នៃសុវត្ថិភាពផលិតផល សូមមើលអត្ថបទរបស់ CISA, តម្លៃនៃបច្ចេកវិទ្យាដែលមិនមានសុវត្ថិភាព និងអ្វីដែល យើងអាចធ្វើបានអំពីរឿងនេះ។

[2] តទៅនេះត្រូវបានហៅថា "ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ"។

អ្វីដែលថ្មី

ការបោះពុម្ពផ្សព្វផ្សាយដំបូងនៃរបាយការណ៍នេះ បានបង្កើតបរិមាណនៃការសន្ទនាដ៏សំខាន់នៅក្នុងឧស្សាហកម្មសូហ្វវែរ។ ព័ត៌មានប្រចាំថ្ងៃអំពីស្ថាប័ន និងបុគ្គលដែលបានរងនូវការវាយប្រហារតាមអ៊ីនធឺណិតគួសបញ្ជាក់ពីតម្រូវការសម្រាប់ការសន្ទនាបន្ថែមទៀត ទាក់ទងនឹងរបៀបដោះស្រាយបញ្ហារ៉ាំរ៉ៃ និងជាប្រព័ន្ធនៅក្នុងផលិតផលសូហ្វវែរ។

បន្ទាប់ពីការចេញផ្សាយនៅក្នុងខែមេសា ឆ្នាំ 2023 ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ (ពីនេះតទៅពាក្យ "យើង" និង "របស់យើង" ត្រូវបានប្រើជំនួស) បានទទួលមតិកែលម្អដែលមានការគិតគូរល្អិតល្អន់ពីបុគ្គល ក្រុមហ៊ុន និងសមាគមពាណិជ្ជកម្មរាប់រយ។ សំណើទូទៅបំផុតនៅក្នុងមតិកែលម្អគឺផ្តល់ព័ត៌មានលម្អិតបន្ថែមលើគោលការណ៍ទាំងបី ដោយព្រោះវាអនុវត្តចំពោះទាំងក្រុមហ៊ុនផលិតសូហ្វវែរ និងអតិថិជនរបស់ពួកគេ។ នៅក្នុងឯកសារនេះ យើងពង្រីកលើរបាយការណ៍ដើម ហើយពិភាក្សាលើប្រធានបទផ្សេងទៀតដូចជាទំហំក្រុមហ៊ុនផលិត និងអតិថិជន ភាពចាស់ទុំរបស់អតិថិជន និងវិសាលភាពនៃគោលការណ៍។

សូហ្វវែរមាននៅគ្រប់ទីកន្លែង ហើយគ្មានរបាយការណ៍តែមួយណាដែលនឹងអាចគ្របដណ្តប់បានគ្រប់គ្រាន់លើប្រព័ន្ធសូហ្វវែរទាំងមូល ការអភិវឌ្ឍផលិតផលសូហ្វវែរ ការប្រើប្រាស់ និងការថែទាំរបស់អតិថិជន និងការរួមបញ្ចូលជាមួយប្រព័ន្ធផ្សេងទៀតនោះឡើយ។ សម្រាប់ការណែនាំខាងក្រោមដែលមិនបានគូសផែនទីយ៉ាងច្បាស់ទៅនឹងបរិដ្ឋានជាក់លាក់ណាមួយ យើងទន្ទឹងរង់ចាំស្តាប់មតិកែលម្អពីសហគមន៍ អំពីរបៀបដែលការអនុវត្តដែលបានពិពណ៌នានៅក្នុងអត្ថបទនេះដែលនាំឱ្យមានការកែលម្អសុវត្ថិភាពជាពិសេស។

របាយការណ៍នេះអនុវត្តចំពោះក្រុមហ៊ុនផលិតប្រព័ន្ធ និងម៉ូដែលសូហ្វវែរ បញ្ញាសិប្បនិម្មិត (AI) ផងដែរ។ ខណៈពេលដែលពួកវាអាចខុសពីទម្រង់ប្រពៃណីនៃសូហ្វវែរ ការអនុវត្តសន្តិសុខជាមូលដ្ឋាននៅតែអនុវត្តចំពោះប្រព័ន្ធ និងម៉ូដែលនៃ AI។ ការអនុវត្តសន្តិសុខតាមការរចនាមួយចំនួនអាចត្រូវការកែប្រែដើម្បីគិតគូពីការពិចារណាជាក់លាក់របស់ AI ប៉ុន្តែគោលការណ៍សន្តិសុខតាមការរចនាទូលំទូលាយទាំងបី អនុវត្តចំពោះប្រព័ន្ធ AI ទាំងអស់។

យើងទទួលស្គាល់ថាការបន្លាស់វដ្តជីវិតនៃការអភិវឌ្ឍសូហ្វវែរ (SDLC) ដើម្បីសម្របជាមួយនឹងគោលការណ៍សន្តិសុខតាមការរចនាទាំងនេះ មិនមែនជាកិច្ចការសាមញ្ញនោះទេ ហើយប្រហែលជាត្រូវការពេលវេលា។ លើសពីនេះ ក្រុមហ៊ុនផលិតសូហ្វវែរតូចៗ អាចជួបការលំបាកក្នុងការអនុវត្តចំពោះការណែនាំទាំងនេះជាច្រើន។ យើងជឿជាក់ថា ឧស្សាហកម្មសូហ្វវែរចាំបាច់ត្រូវបង្កើតឱ្យមានឧបករណ៍ និងនីតិវិធីយ៉ាងទូលំទូលាយ ដែលធ្វើឱ្យផលិតផលកាន់តែមានសុវត្ថិភាព។ នៅពេលដែលមនុស្ស និងស្ថាប័នកាន់តែច្រើន ផ្តោតការយកចិត្តទុកដាក់របស់ពួកគេលើការកែលម្អសុវត្ថិភាពសូហ្វវែរ យើងជឿជាក់ថាមានឱកាសសម្រាប់ការច្នៃប្រឌិតដែល នឹងបង្រួមគម្លាតរវាងក្រុមហ៊ុនផលិតសូហ្វវែរធំៗ និងតូចៗ ដើម្បីជាប្រយោជន៍ដល់អតិថិជនទាំងអស់។

ការធ្វើបច្ចុប្បន្នភាពរបាយការណ៍ដើមនៃសន្តិសុខតាមការរចនានេះ គឺជាផ្នែកនៃការប្តេជ្ញាចិត្តរបស់យើងក្នុងការកសាងភាពជាដៃគូជាមួយសហគមន៍ភាគីពាក់ព័ន្ធដែលទាក់ទងគ្នាជាច្រើន ដែលគាំទ្រប្រព័ន្ធអេកូឡូស៊ីបច្ចេកវិទ្យារបស់យើង។ វាគឺជាលទ្ធផលនៃមតិកែលម្អពីផ្នែកជាច្រើននៃប្រព័ន្ធអេកូឡូស៊ីនោះ ហើយយើងនឹងបន្តស្តាប់ និងរៀនសូត្រពីទស្សនៈនានា។ ទោះបីជាមានបញ្ហាប្រឈមជាច្រើននៅខាងមុខក៏ដោយ យើងមានសុទិដ្ឋិនិយមគួរឱ្យជឿបាន ដោយសារយើងស្វែងយល់កាន់តែច្រើនអំពីមនុស្ស និងស្ថាប័ននានាដែលបានចាប់យកទស្សនសន្តិសុខតាមការរចនារួចហើយ ជាញឹកញាប់ទទួលបានជោគជ័យ។

របៀបប្រើឯកសារនេះ

យើងជំរុញឱ្យក្រុមហ៊ុនផលិតសូហ្វវែរ គោរពតាមគោលការណ៍នានានៅក្នុងឯកសារនេះ។ ក្រុមហ៊ុនផលិតសូហ្វវែរអាចបង្ហាញពីការប្តេជ្ញាចិត្តរបស់ពួកគេ ដោយចងក្រងជាសាធារណៈនូវសកម្មភាពរបស់ពួកគេដែលបានធ្វើឡើង ស្របតាមជំហាននានាដែលបានរាយខាងក្រោម។ យើងលើកទឹកចិត្តក្រុមហ៊ុនផលិតសូហ្វវែរ ឱ្យស្វែងរកយុទ្ធវិធីនានាដែលបំពេញតាមស្មារតីនៃគោលការណ៍នេះ ហើយបង្កើតអនុផលសូហ្វវែរ ដែលនឹងបង្កើតករណីគួរឱ្យទាក់ទាញមួយទាំងអតិថិជនបច្ចុប្បន្ន និងអនាគតដែលចេះតែសង្ស័យ ដែលពួកគេកំពុងដាក់បញ្ចូលទស្សនសន្តិសុខតាមការរចនា។

បន្ថែមពីលើសកម្មភាពនានាដែលក្រុមហ៊ុនផលិតសូហ្វវែរគួរចាត់វិធានការ អតិថិជនក៏អាចប្រើប្រាស់ឯកសារនេះដើម្បីទាញយកផលប្រយោជន៍ឱ្យបានច្រើនជាអតិបរិមាផងដែរ។ ក្រុមហ៊ុនដែលទិញសូហ្វវែរ គួរតែសួរសំណួរពិបាកៗអំពីអ្នកលក់របស់ពួកគេ ដោយទាញការបំផុសគំនិតពីឧទាហរណ៍នៃការប្រកាន់ខ្ជាប់នូវគោលការណ៍នានាដែលបានរាយក្នុងឯកសារនេះ។ ក្នុងការធ្វើដូច្នេះ អតិថិជនអាចជួយផ្លាស់ប្តូរទីផ្សារ ឆ្ពោះទៅរកផលិតផលសន្តិសុខជាងមុនតាមការរចនា។ ឧទាហរណ៍មួយនៃសំណួរដែលអតិថិជនអាចសួរអំពីអ្នកលក់ ត្រូវបានផ្តល់ឱ្យនៅក្នុង ការណែនាំរបស់ CISA សម្រាប់ការទិញបច្ចេកវិទ្យាសម្រាប់សាលារៀនសាធារណៈពីថ្នាក់មត្តេយ្យ ដល់ថ្នាក់ទី 12 (K-12)។

យើងលើកទឹកចិត្តអតិថិជនសហគ្រាស ឱ្យបញ្ចូលការអនុវត្តទាំងនេះទៅក្នុងដំណើរការលទ្ធកម្ម ការវាយតម្លៃការស៊ើបអង្កេតទៅលើសក្តានុពលរបស់អ្នកលក់ ការសម្រេចចិត្តទទួលយកហានិភ័យសហគ្រាស និងជំហានផ្សេងទៀតដែលបានធ្វើឡើងនៅពេលវាយតម្លៃអ្នកលក់។ អតិថិជនក៏គួរតែជំរុញអ្នកលក់របស់ពួកគេផងដែរ ដើម្បីឱ្យចងក្រងជាសាធារណៈនូវវិធានការសន្តិសុខតាមការរចនានានាដែលអ្នកលក់នីមួយៗធ្វើ។ ដោយធ្វើការរួមគ្នា នេះអាចបង្កើតសញ្ញាតម្រូវការដ៏រឹងមាំមួយសម្រាប់សន្តិសុខ ដែលអាចលើកទឹកចិត្ត និងផ្តល់លទ្ធភាពឱ្យក្រុមហ៊ុនផលិតសូហ្វវែរ ចាត់វិធានការឆ្ពោះទៅរកសន្តិសុខកាន់តែប្រសើរឡើង។ ម្យ៉ាងវិញទៀត ដូចដែលយើងព្យាយាមបង្កើតទស្សនសន្តិសុខតាមការរចនាដែលជ្រួតជ្រាបនៅក្នុងក្រុមហ៊ុនផលិតសូហ្វវែរ យើងត្រូវបង្កើតវប្បធម៌ "សន្តិសុខតាមតម្រូវការ" មួយ ជាមួយអតិថិជនរបស់ពួកគេ។

សន្តិសុខតាមការរចនា

"សន្តិសុខតាមការរចនា" មានន័យថា ផលិតផលបច្ចេកវិទ្យាត្រូវបានបង្កើតឡើងតាមរបៀបមួយដែលការពារដោយសមហេតុផល ប្រឆាំងនឹងបុគ្គលមានបំណងទុច្ចរិតតាមអ៊ីនធឺណិត ពីការចូលប្រើប្រាស់ដោយជោគជ័យនូវឧបករណ៍ ទិន្នន័យ និងហេដ្ឋារចនាសម្ព័ន្ធដែលបានតភ្ជាប់។ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែធ្វើការវាយតម្លៃហានិភ័យដើម្បីកំណត់អត្តសញ្ញាណ និងរៀបរាប់តាមលំដាប់ នូវការគំរាមកំហែងតាមអ៊ីនធឺណិតដែលរីករាលដាលដល់ប្រព័ន្ធសំខាន់ៗ ហើយបន្ទាប់ដាក់បញ្ចូលការការពារនៅក្នុងគម្រោងផែនការផលិតផល ដែលគិតគូរពីទិដ្ឋភាពនៃការគំរាមកំហែងតាមអ៊ីនធឺណិតដែលកំពុងវិវត្ត។

ការអនុវត្តការអភិវឌ្ឍបច្ចេកវិទ្យាព័ត៌មានសន្តិសុខ (IT) និងការការពារជាច្រើនជាន់ ដែលត្រូវបានគេស្គាល់ថាការការពារស៊ីជម្រៅ ក៏ត្រូវបានណែនាំផងដែរដើម្បីការពារអ្នកប្រព្រឹត្តទុច្ចរិតពីការធ្វើឱ្យប្រព័ន្ធងាយរងគ្រោះ ការវាយប្រហារតាមអ៊ីនធឺណិតឬការចូលយកទិន្នន័យរសើបដោយគ្មាន ការអនុញ្ញាត។ ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំបន្ថែមដល់ក្រុមហ៊ុនផលិត ឱ្យប្រើម៉ូដែលកំណត់ការគំរាមកំហែងតាមត្រូវការមួយក្នុងអំឡុងដំណាក់កាលនៃការអភិវឌ្ឍផលិតផល ដើម្បីដោះស្រាយរាល់ការគំរាមកំហែងដែលអាចកើតមានចំពោះប្រព័ន្ធ និងគណនីសម្រាប់ដំណើរការប្រើប្រាស់របស់ប្រព័ន្ធនីមួយៗ។

ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ជំរុញឱ្យអ្នកផលិតទទួលយកវិធីសាស្ត្រសន្តិសុខគ្រប់ជ្រុងជ្រោយសម្រាប់ផលិតផល និងវេទិការបស់ពួកគេ។ ការអភិវឌ្ឍសន្តិសុខតាមការរចនាតម្រូវឱ្យមានយុទ្ធសាស្ត្រលើការវិនិយោគធនធានបែងចែកសម្រាប់កិច្ចការនេះពីក្រុមហ៊ុនផលិតសូហ្វវែរ នៅស្រទាប់នីមួយៗនៃដំណើរការរចនា និងដំណើរការអភិវឌ្ឍដែលមិនអាច "ដាក់បន្ថែម" នៅពេលក្រោយបានទេ។ វាតម្រូវឱ្យមានភាពជាអ្នកដឹកនាំដ៏រឹងមាំដោយនាយកប្រតិបត្តិអាជីវកម្មកំពូលរបស់ក្រុមហ៊ុនផលិត ដើម្បីធ្វើឱ្យសន្តិសុខក្លាយជាចំណុចអាទិភាពរបស់អាជីវកម្ម មិនមែនគ្រាន់តែជាលក្ខណៈពិសេសផ្នែកបច្ចេកទេសប៉ុណ្ណោះទេ។ កិច្ចសហការរវាងអ្នកដឹកនាំអាជីវកម្ម និងក្រុមបច្ចេកទេសនេះ ពង្រីកពីដំណាក់កាលដំបូងនៃការរចនា និងការអភិវឌ្ឍតាមរយៈការប្រើប្រាស់ និងការថែទាំអតិថិជន។ ក្រុមហ៊ុនផលិតត្រូវបានលើកទឹកចិត្តឱ្យធ្វើការដោះដូរទំនិញ និងការវិនិយោគដ៏លំបាក រួមទាំងអ្វីដែលនឹង "មើលមិនឃើញ" សម្រាប់អតិថិជន (ឧទាហរណ៍ ការផ្លាស់ប្តូរទៅភាសាសរសេរកម្មវិធី ដែលលុបបំបាត់នូវភាពងាយរងគ្រោះដែលរីករាលដាល)។ ពួកគេគួរតែផ្តល់អាទិភាពដល់លក្ខណៈពិសេស យន្តការ និងការអនុវត្តឧបករណ៍ដែលការពារអតិថិជន ជាជាងលក្ខណៈពិសេសនៃផលិតផលដែលមើលទៅគួរឱ្យទាក់ទាញប៉ុន្តែពង្រីកផ្ទៃរូបភាពដែលអាចវាយប្រហារទៅវិញ។

មិនមានដំណោះស្រាយតែមួយ ដើម្បីបញ្ចប់ការគំរាមកំហែងជាបន្តបន្ទាប់នៃបុគ្គលមានបំណងទុច្ចរិតតាមអ៊ីនធឺណិត ដែលទាញយកប្រយោជន៍ពីភាពងាយរងគ្រោះផ្នែកបច្ចេកវិទ្យានោះទេ ហើយផលិតផលដែលមាន "សន្តិសុខតាមការរចនា" នឹងនៅតែបន្តរងគ្រោះ។ ទោះយ៉ាងណាក៏ដោយ ភាពងាយរងគ្រោះមួយឈុតធំ គឺមានដោយសារតែសំណុំរងតូចតាចនៃប្រភពដើមហេតុ។ ក្រុមហ៊ុនផលិតគួរតែបង្កើតផែនទីបង្ហាញផ្លូវជាលាយលក្ខណ៍អក្សរ ដើម្បីតម្រឹមផលប័ត្រផលិតផលដែលមានស្រាប់របស់ពួកគេ ជាមួយនឹងការអនុវត្តសន្តិសុខតាមការរចនាបន្ថែមទៀត ដោយធានាថានឹងអាចងាកចេញបានតែក្នុងស្ថានភាពពិសេសប៉ុណ្ណោះ។

ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យទទួលស្គាល់ថា ការទទួលយកភាពជាម្ចាស់នៃលទ្ធផលសន្តិសុខសម្រាប់អតិថិជន និងការធានាកម្រិតសន្តិសុខអតិថិជនអាចបង្កើនថ្លៃចំណាយលើការអភិវឌ្ឍ។ ទោះជាយ៉ាងណាក៏ដោយ ការវិនិយោគលើការអនុវត្តសន្តិសុខតាមការរចនា ខណៈពេលដែលកំពុងអភិវឌ្ឍផលិតផលបច្ចេកវិទ្យាប្រកបដោយភាពច្នៃប្រឌិត និងការរក្សានូវផលិតផលដែលមានស្រាប់ អាចធ្វើឱ្យប្រសើរឡើងច្រើននូវគោលជំហរសន្តិសុខរបស់អតិថិជន និងកាត់បន្ថយលទ្ធភាពរងការវាយប្រហារតាមអ៊ីនធឺណិត។ គោលការណ៍សន្តិសុខតាមការរចនាមិនត្រឹមតែពង្រឹងគោលជំហរសន្តិសុខសម្រាប់អតិថិជន និងកេរ្តិ៍ឈ្មោះម៉ាកសម្រាប់អ្នកអភិវឌ្ឍន៍ប៉ុណ្ណោះទេ ប៉ុន្តែការអនុវត្តក៏កាត់បន្ថយថ្លៃចំណាយលើការថែទាំ និងការជួសជុលសម្រាប់អ្នកផលិតក្នុងរយៈពេលវែងផងដែរ។

អនុសាសន៍សម្រាប់ក្រុមហ៊ុនផលិតសូហ្វវែរដែលបានរាយបញ្ជីខាងក្រោម ផ្តល់នូវបញ្ជីនៃការអនុវត្តនិងគោលនយោបាយអភិវឌ្ឍន៍ផលិតផល ដែលបានណែនាំសម្រាប់ក្រុមហ៊ុនផលិតដើម្បីពិចារណា។

សន្តិសុខតាមលំនាំដើម

"សន្តិសុខតាមលំនាំដើម" មានន័យថា ផលិតផលមានភាពធន់នឹងបច្ចេកទេសនៃការកេងប្រវ័ញ្ចដែលរីករាលដាល ចេញពីប្រអប់ដោយមិនគិតថ្លៃបន្ថែម។ ផលិតផលទាំងនេះការពារប្រឆាំងនឹងការគំរាមកំហែង និងភាពងាយរងគ្រោះដែលរីករាលដាលបំផុត ដោយពុំតម្រូវឱ្យអ្នកប្រើប្រាស់ចុងក្រោយ ត្រូវចាត់វិធានការបន្ថែមដើម្បីការពារសន្តិសុខផលិតផលនោះទេ។ ផលិតផលដែលមានសន្តិសុខតាមលំនាំដើម ត្រូវបានរចនាឡើងដើម្បីធ្វើឱ្យអតិថិជនដឹងយ៉ាងច្បាស់ថា នៅពេលដែលពួកគេងាកចេញពីសន្តិសុខតាមលំនាំដើម ពួកគេកំពុងបង្កើនលទ្ធភាពរងការវាយប្រហារតាមការវាយប្រហារតាមអ៊ីនធឺណិត លុះត្រាតែពួកគេអនុវត្តការត្រួតពិនិត្យសំណងបន្ថែម។ សន្តិសុខតាមលំនាំដើម គឺជាទម្រង់នៃសន្តិសុខតាមការរចនា។

- ការកំណត់រចនាសម្ព័ន្ធដែលមានសន្តិសុខ គួរតែជាបន្ទាត់មូលដ្ឋានលំនាំដើម។ ផលិតផលដែលមានសន្តិសុខតាមលំនាំដើមបើកដោយស្វ័យប្រវត្តិនូវការគ្រប់គ្រងសន្តិសុខដ៏សំខាន់បំផុត ដែលត្រូវការដើម្បីការពារសហគ្រាសពីបុគ្គលមានបំណងទុច្ចរិតតាមអ៊ីនធឺណិត ក៏ដូចជាផ្តល់នូវសមត្ថភាពក្នុងការប្រើប្រាស់ និងកំណត់រចនាសម្ព័ន្ធការគ្រប់គ្រងសន្តិសុខបន្ថែមទៀតដោយមិនគិតថ្លៃបន្ថែម។
- ភាពស្មុគស្មាញនៃការកំណត់រចនាសម្ព័ន្ធសន្តិសុខមិនគួរជាបញ្ហារបស់អតិថិជនទេ។ បុគ្គលិកផ្នែក IT របស់ស្ថាប័ន តែងតែទទួលបន្ទុកលើសលប់ជាមួយនឹងទំនួលខុសត្រូវផ្នែកសន្តិសុខ និងប្រតិបត្តិការ ដូច្នេះហើយទើបបណ្តាលឱ្យមានពេលវេលាកំណត់ក្នុងការយល់ដឹង និងអនុវត្តវិធានការពាក់ព័ន្ធ និងការកាត់បន្ថយសន្តិសុខដែលត្រូវការសម្រាប់គោលជំហរសន្តិសុខអ៊ីនធឺណិតដ៏រឹងមាំ។ ក្រុមហ៊ុនផលិតអាចជួយអតិថិជនរបស់ពួកគេ ការធ្វើឱ្យការកំណត់រចនាសម្ព័ន្ធផលិតផលដែលមានសន្តិសុខ-ដោយធានាថា "ផ្លូវលំនាំដើម" - ដោយធានាថាផលិតផលរបស់ពួកគេត្រូវបានផលិត ចែកចាយ និងប្រើប្រាស់ប្រកបដោយសន្តិសុខស្របតាមស្តង់ដារ "សន្តិសុខតាមលំនាំដើម"។

ក្រុមហ៊ុនផលិតផលិតផលដែលមាន "សន្តិសុខតាមលំនាំដើម" មិនគិតថ្លៃបន្ថែមសម្រាប់ការអនុវត្តការកំណត់រចនាសម្ព័ន្ធសន្តិសុខបន្ថែមទេ។ ជាជំនួសវិញនោះ ពួកគេដាក់បញ្ចូលវានៅក្នុងផលិតផលជាមូលដ្ឋាន ដូចជាខ្សែក្រវ៉ាត់សុវត្ថិភាពត្រូវបានដាក់ក្នុងរថយន្តថ្មីទាំងអស់នោះដែរ។

សន្តិសុខមិនមែនជាជម្រើសដ៏ប្រណិតនោះទេ ប៉ុន្តែគួរតែត្រូវបានចាត់ទុកថាជាសិទ្ធិមួយដែលអតិថិជនទទួលបាន ដោយមិនចាំបាច់ចរចា ឬបង់ប្រាក់បន្ថែម។

អនុសាសន៍សម្រាប់ក្រុមហ៊ុនផលិតសូហ្វវែរ

មគ្គុទ្ទេសក៍រួមនេះ ផ្តល់អនុសាសន៍ដល់ក្រុមហ៊ុនផលិតសម្រាប់ការអភិវឌ្ឍផែនទីបង្ហាញផ្លូវជាលាយលក្ខណ៍អក្សរដើម្បីអនុវត្ត និងធានាសន្តិសុខព័ត៌មានវិទ្យា។ ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យណែនាំក្រុមហ៊ុនផលិតសូហ្វវែរ ឱ្យអនុវត្តយុទ្ធសាស្ត្រដែលបានរៀបរាប់នៅក្នុងផ្នែកខាងក្រោម ដើម្បីទទួលនូវភាពជាម្ចាស់នៃលទ្ធផលសន្តិសុខរបស់អតិថិជនពួកគេ តាមរយៈគោលការណ៍សន្តិសុខតាមការរចនា និងតាមលំនាំដើម។

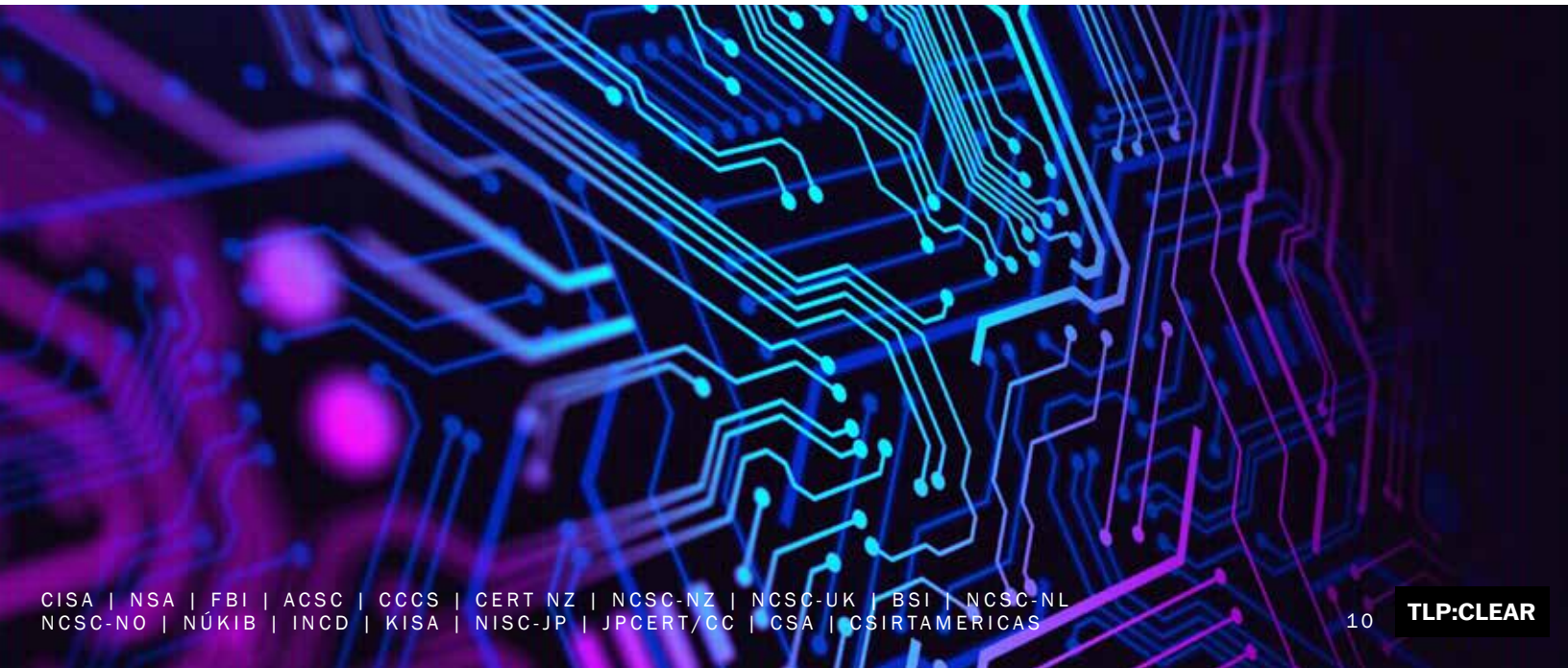
គោលការណ៍សន្តិសុខផលិតផលសូហ្វវែរ

ក្រុមហ៊ុនផលិតសូហ្វវែរត្រូវបានលើកទឹកចិត្តឱ្យទទួលយកការផ្តោតជាយុទ្ធសាស្ត្រ ដែលផ្តល់អាទិភាពលើសន្តិសុខសូហ្វវែរ។ ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ បានបង្កើតគោលការណ៍ស្នូលទាំងបីខាងក្រោម ដើម្បីណែនាំក្រុមហ៊ុនផលិតសូហ្វវែរក្នុងការបង្កើតសន្តិសុខសូហ្វវែរ ទៅក្នុងដំណើរការរចនារបស់ពួកគេមុនពេលបង្កើត កំណត់រចនាសម្ព័ន្ធ និងដឹកជញ្ជូនផលិតផលរបស់ពួកគេ។

1 **ទទួលយកភាពជាម្ចាស់នៃលទ្ធផលសន្តិសុខរបស់អតិថិជន** និងវិវត្តផលិតផលទៅតាមនោះ។ បន្ទុកសន្តិសុខមិនគួរធ្លាក់លើអតិថិជនតែម្នាក់នោះទេ។

2 **ទទួលយកតម្លាភាព និងគណនេយ្យភាពដាច់ខាត។**
ក្រុមហ៊ុនផលិតសូហ្វវែរគួរមានមោទនភាពក្នុងការផ្តល់នូវផលិតផលដែលមានសុវត្ថិភាព និងសន្តិសុខ ក៏ដូចជាការធ្វើឱ្យមានភាពខុសប្លែកគ្នាក្នុងចំណោមសហគមន៍ក្រុមហ៊ុនផលិតផ្សេងទៀត ដោយផ្អែកលើសមត្ថភាពរបស់ពួកគេក្នុងការធ្វើបែបនោះ។ នេះអាចរួមបញ្ចូលការចែករំលែកព័ត៌មានដែលពួកគេបានរៀនពីការប្រើប្រាស់របស់អតិថិជនពួកគេ ដូចជាការទទួលយកយន្តការផ្ទៀងផ្ទាត់ដ៏រឹងមាំតាមលំនាំដើម។ វាក៏រួមបញ្ចូលផងដែរនូវការប្តេជ្ញាចិត្តយ៉ាងមុតមាំក្នុងការធានាឱ្យបាននូវការប្រឹក្សាអំពីភាពងាយរងគ្រោះ និងកំណត់ត្រាភាពងាយរងគ្រោះ និងការប៉ះពាល់ទូទៅដែលពាក់ព័ន្ធ (CVE) គឺពេញលេញ ហើយត្រឹមត្រូវ។ ទោះជាយ៉ាងណាក៏ដោយ ចូរប្រយ័ត្ននឹងការល្បួងឱ្យរាប់ CVEs ជារង្វាស់អវិជ្ជមានព្រោះថាលេខបែបនេះក៏ជាសញ្ញានៃសហគមន៍វិភាគ និងការធ្វើតេស្តកូដដែលមានដំណើរការល្អផងដែរ។

3 **បង្កើតរចនាសម្ព័ន្ធស្ថាប័ន និងភាពជាអ្នកដឹកនាំ ដើម្បីសម្រេចបាននូវគោលដៅទាំងនេះ។**
ខណៈពេលដែលជំនាញផ្នែកបច្ចេកទេសមានសារៈសំខាន់ចំពោះសន្តិសុខផលិតផល នាយកប្រតិបត្តិជាន់ខ្ពស់គឺជាអ្នកធ្វើសេចក្តីសម្រេចចម្បង សម្រាប់ការអនុវត្តការផ្លាស់ប្តូរនៅក្នុងស្ថាប័នមួយ។ នាយកប្រតិបត្តិត្រូវកំណត់អាទិភាពសុវត្ថិភាព ជាធាតុសំខាន់នៃការអភិវឌ្ឍផលិតផលនៅទូទាំងស្ថាប័ន និងក្នុងភាពជាដៃគូជាមួយអតិថិជន។



ដើម្បីដំណើរការគោលការណ៍ទាំងបីនេះ ក្រុមហ៊ុនផលិតគួរតែពិចារណាអំពីយុទ្ធវិធីប្រតិបត្តិការមួយចំនួន ដើម្បីវិវត្តដំណើរការអភិវឌ្ឍរបស់ពួកគេ។

រៀបចំការប្រជុំជាប្រចាំជាមួយថ្នាក់ដឹកនាំប្រតិបត្តិរបស់ក្រុមហ៊ុន ដើម្បីជំរុញសារៈសំខាន់នៃសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើមនៅក្នុងស្ថាប័ន។ គោលនយោបាយ និងនីតិវិធីគួរតែបានបង្កើតឡើង ដើម្បីផ្តល់រង្វាន់ដល់ក្រុមផលិតកម្មដែលអភិវឌ្ឍផលិតផលដែលប្រកាន់ខ្ជាប់នូវគោលការណ៍ទាំងនេះ ដែលអាចរួមបញ្ចូលរង្វាន់សម្រាប់ការប្រតិបត្តិការអនុវត្តសន្តិសុខសូហ្វវែរដ៏ឆ្នើម ឬលាភការសម្រាប់ជណ្តើរវិជ្ជាជីវៈ និងលក្ខណៈវិនិច្ឆ័យនៃការដំឡើងឋានៈ។

ធ្វើប្រតិបត្តិការជុំវិញសារៈសំខាន់នៃសន្តិសុខសូហ្វវែរដើម្បីឈានទៅភាពជោគជ័យនៃអាជីវកម្ម។ ជាឧទាហរណ៍ ពិចារណាលើការចាត់តាំង "អ្នកដឹកនាំសន្តិសុខសូហ្វវែរ" ឬ "ក្រុមសន្តិសុខសូហ្វវែរ" ដែលគាំទ្រការអនុវត្តអាជីវកម្ម និងព័ត៌មានវិទ្យាដើម្បីភ្ជាប់ដោយផ្ទាល់នូវស្តង់ដារសន្តិសុខសូហ្វវែរ និងការទទួលខុសត្រូវរបស់ក្រុមហ៊ុនផលិត។ ក្រុមហ៊ុនផលិតគួរតែធានាថាពួកគេមានកម្មវិធីវាយតម្លៃសន្តិសុខផលិតផលឯករាជ្យ និងរឹងមាំសម្រាប់ផលិតផលរបស់ពួកគេ។

ម៉ូដែលកំណត់ការគំរាមកំហែងតាមត្រូវការក្នុងអំឡុងពេលបែងចែក និងការអភិវឌ្ឍធនធាន ដើម្បីផ្តល់អាទិភាពដល់លក្ខណៈពិសេសដែលមានផលប៉ះពាល់ខ្ពស់បំផុត និងខ្លាំងបំផុត។ ម៉ូដែលកំណត់ការគំរាមកំហែងពិចារណាករណីប្រើប្រាស់ជាក់លាក់របស់ផលិតផល និងអនុញ្ញាតឱ្យក្រុមអភិវឌ្ឍន៍ដើម្បីពង្រឹងផលិតផល។ ជាចុងក្រោយ ភាពជាអ្នកដឹកនាំជាន់ខ្ពស់គួរតែឱ្យក្រុមនានាទទួលខុសត្រូវចំពោះការផ្គត់ផ្គង់ផលិតផលដែលមានសន្តិសុខ ជាធាតុសំខាន់នៃឧត្តមភាព និងគុណភាពនៃផលិតផល។

ជាផ្នែកនៃការធ្វើបច្ចុប្បន្នភាពខែតុលា ឆ្នាំ 2023 ចំពោះការណែនាំនេះ គោលការណ៍ទាំងបីនេះត្រូវបានពង្រីកតាមរយៈការពន្យល់ការបង្ហាញ និងភស្តុតាងដូចខាងក្រោម។

គោលការណ៍ 1៖ ទទួលយកភាពជាម្ចាស់នៃលទ្ធផលសន្តិសុខរបស់អតិថិជន

ការពន្យល់

ការអនុវត្តល្អបំផុតសម័យទំនើបកំណត់ថា ក្រុមហ៊ុនផលិតសូហ្វវែរវិនិយោគលើកិច្ចខិតខំប្រឹងប្រែងសន្តិសុខផលិតផលដែលរួមមាន **ការពង្រឹងកម្មវិធី លក្ខណៈពិសេសកម្មវិធី** និងកម្មវិធី**ការកំណត់លំនាំដើម។**

ក្រុមហ៊ុនផលិតសូហ្វវែរត្រូវអនុវត្ត**ការពង្រឹងកម្មវិធី** ដោយប្រើដំណើរការ និងបច្ចេកវិទ្យាដែលបង្កើនតម្លៃចំណាយ សម្រាប់បុគ្គលមានបំណងទុច្ចរិតដែលចង់សម្របសម្រួលកម្មវិធី។ ពិធីការ និងនីតិវិធីនៃការពង្រឹងការអនុវត្តកម្មវិធី ជួយឱ្យផលិតផលទប់ទល់នឹងការវាយប្រហារដោយបុគ្គលមានបំណងទុច្ចរិតដែលឆ្លាតវៃ។ ពាក្យនានាដូចជាការពង្រឹងសន្តិសុខផលិតផល និងភាពធន់ គឺសុទ្ធតែទាក់ទងយ៉ាងជិតស្និទ្ធទៅនឹងគុណភាពផលិតផល។ គំនិតគឺថាសន្តិសុខត្រូវតែត្រូវបាន "រួមបញ្ចូលនៅក្នុងអ្វីផ្សេងទៀត ហើយមិនអាចបំបែកចេញបាន" និងមិនមែន "ដាក់បន្ថែម"។ [1] ដោយការរួមបញ្ចូលនៅក្នុងអ្វីផ្សេងទៀត ហើយមិនអាចបំបែកចេញបាននៅក្នុងសន្តិសុខ ក្រុមហ៊ុនផលិតសូហ្វវែរមិនត្រឹមតែអាចបង្កើនសន្តិសុខអតិថិជនរបស់ពួកគេប៉ុណ្ណោះទេ ប៉ុន្តែថែមទាំងបង្កើនគុណភាពផលិតផលរបស់ពួកគេផងដែរ។ យុទ្ធសាស្ត្រគំរូរួមមានការធានាថាការបញ្ចូលទិន្នន័យអ្នកប្រើប្រាស់ត្រូវបានផ្ទៀងផ្ទាត់ឱ្យត្រឹមត្រូវ និងត្រូវបានសម្អាត ហើយមិនត្រូវបានបញ្ចូលដោយផ្ទាល់ទៅក្នុងកូដ (ឧទាហរណ៍ ដោយប្រើវិធីស្នើសុំទិន្នន័យដែលមានដែនកំណត់ជំនួសវិញ) ដោយប្រើភាសាសរសេរកម្មវិធីសុវត្ថិភាពអង្គចងចាំ ការគ្រប់គ្រងវដ្តជីវិតនៃការអភិវឌ្ឍសូហ្វវែរយ៉ាងម៉ត់ចត់ (SDLC) និងការប្រើការគ្រប់គ្រងសោធ្វើកូដនីយកម្មផ្នែករឹង (hardware-backed cryptographic key management)។

កម្មវិធីចាំបាច់ត្រូវគាំទ្រ **លក្ខណៈពិសេសៗនៃកម្មវិធី** ដែលទាក់ទងនឹងសន្តិសុខអ៊ីនធឺណិត។ ពេលខ្លះគេហៅថា "សមត្ថភាព" លក្ខណៈពិសេសទាំងនេះពង្រីកមុខងារនៃផលិតផល ឬសេវាកម្មក្នុងវិធីដែលជួយថែទាំ ឬបង្កើនគោលជំហរសន្តិសុខរបស់អតិថិជន។

លក្ខណៈពិសេសដែលទាក់ទងនឹងសន្តិសុខគំរូរួមមាន ការគាំទ្រសន្តិសុខស្រទាប់ដឹកជញ្ជូន (TLS) សម្រាប់ការតភ្ជាប់បណ្តាញទាំងអស់, ការគាំទ្រការចុះឈ្មោះចូលតែមួយ (SSO), ការគាំទ្រការផ្ទៀងផ្ទាត់ពហុកត្តា (MFA), ការបើកចូលធ្វើសវនកម្មព្រឹត្តិការណ៍សន្តិសុខ, ការគ្រប់គ្រងការចូលដំណើរការដោយផ្អែកលើតួនាទី (RBAC) និងការគ្រប់គ្រងការចូលប្រើប្រាស់ដោយផ្អែកលើបុគ្គលិកលក្ខណៈ (ABAC)។

លក្ខណៈពិសេសមួយចំនួននៃផលិតផលទាំងនេះអាចកំណត់រចនាសម្ព័ន្ធបាន ដែលអនុញ្ញាតឱ្យអតិថិជនបញ្ចូលផលិតផលទៅក្នុងបរិដ្ឋាន និងលំហូរការងារដែលមានស្រាប់របស់ពួកគេយ៉ាងងាយស្រួល។ ការកំណត់រចនាសម្ព័ន្ធទាំងនោះមានន័យថា កម្មវិធីត្រូវតែមាន**ការកំណត់លំនាំដើម** ដែលបានកំណត់រហូតដល់អតិថិជនកំណត់រចនាសម្ព័ន្ធពួកគេ។ ការកំណត់លំនាំដើមទាំងនោះត្រូវកំណត់ដោយសន្តិសុខ "ចេញពីប្រអប់" ដូច្នេះអតិថិជនចំណាយធនធានតិចជាងមុន ដើម្បីធ្វើឱ្យផលិតផលបច្ចេកវិទ្យារបស់ពួកគេកាន់តែមានសន្តិសុខ។

ធាតុនីមួយៗទាំងនេះ – ការពង្រឹងកម្មវិធី លក្ខណៈពិសេសៗនៃសន្តិសុខកម្មវិធី និងការកំណត់លំនាំដើមរបស់កម្មវិធី – ដើរតួនាទីក្នុងសន្តិសុខនៃកម្មវិធី និងគោលជំហរសន្តិសុខដែលបានលទ្ធផលរបស់អតិថិជន។ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែគិតអំពីធាតុនីមួយៗទាំងនេះ និងរបៀបដែលវាទាក់ទងគ្នាទៅវិញទៅមក។ ក្រុមហ៊ុនផលិតគួរតែគិតឱ្យបានលើសពីការវិនិយោគរបស់ពួកគេ ដើម្បីដាក់បញ្ចូលធាតុទាំងនេះទៅក្នុងផលិតផលរបស់ពួកគេ។ ក្រុមហ៊ុនផលិតគួរតែឈានមួយជំហានទៀត ហើយពិចារណាពីរបៀបដែលធាតុទាំងនោះផ្លាស់ប្តូរគោលជំហរសន្តិសុខ ក្នុងពិភពជាក់ស្តែងរបស់អតិថិជនពួកគេបានប្រសើរជាង ឬអាក្រក់ជាង។

ក្រុមហ៊ុនផលិតគួរតែទទួលយកភាពជាម្ចាស់នៃលទ្ធផលសុវត្ថិភាពរបស់អតិថិជនពួកគេ ជាជាងការរាស់វែងខ្លួនឯងតែលើការខិតខំប្រឹងប្រែង និងការវិនិយោគរបស់ពួកគេ។ ទំនួលខុសត្រូវគួរតែត្រូវបានដាក់នៅខាងលើជាមួយក្រុមហ៊ុនផលិត ដែលវាមានលទ្ធភាពច្រើនបំផុតក្នុងការកាត់បន្ថយឱកាសរងការវាយប្រហារតាមអ៊ីនធឺណិត។

ជាអកុសល វាមិនមែនជាករណីនៅពេលបច្ចុប្បន្ននេះទេ។ មានក្រុមហ៊ុនផលិតច្រើនណាស់ដែលដាក់បន្ទុកសន្តិសុខលើអតិថិជនជាជាងការវិនិយោគលើ**ការពង្រឹងកម្មវិធីដ៏ទូលំទូលាយ។** ជាឧទាហរណ៍ នៅពេលដែលក្រុមហ៊ុនផលិតបានជួសជុលភាពងាយរងគ្រោះមួយ យើងតែងតែឃើញភាពងាយរងគ្រោះស្រដៀងគ្នានេះលេចឡើង ដោយសារតែពួកគេបានដោះស្រាយតែរោគសញ្ញា ជាជាងមូលហេតុឫសគល់នៃកង្វះខាតនោះ។ ផលិតផលនេះអាចអនុវត្តការកាត់បន្ថយផ្សេងៗគ្នានៅក្នុងផ្នែកផ្សេងៗនៃមូលដ្ឋានកូដ សម្រាប់ក្រុមនៃភាពងាយរងគ្រោះដូចគ្នា។ ជាករណីមួយ បន្ទាប់ពីក្រុមហ៊ុនផលិតបានជួសជុលភាពងាយរងគ្រោះនៃការសម្អាតទិន្នន័យបញ្ចូលមួយ អ្នកស្រាវជ្រាវ ឬអ្នកវាយប្រហារបានរកឃើញផ្លូវកូដ ដែលមិនទទួលបានអត្ថប្រយោជន៍ពីការសម្អាតទិន្នន័យបញ្ចូលដែលបានកែលម្អ។ ក្រុមហ៊ុនផលិតបានអនុវត្តការជួសជុលម្តងមួយៗ ជាជាងការបង្រួបបង្រួមមូលដ្ឋានកូដ ដើម្បីលុបបំបាត់ក្រុមនៃភាពងាយរងគ្រោះនោះនៅលើកម្មវិធីទាំងមូល។

លក្ខណៈពិសេសនៃកម្មវិធីអាចបង្កើតទាំងអត្ថប្រយោជន៍ និងហានិភ័យសម្រាប់អតិថិជន។ លក្ខណៈពិសេសដែលអនុញ្ញាតឱ្យចំណុចរួមបញ្ចូលជាមួយប្រព័ន្ធ និងកំណែខាងក្រៅជាច្រើន អាចបង្កើនតម្លៃផលិតផលបានយ៉ាងច្រើន។ ហើយការគាំទ្រលក្ខណៈពិសេសដោយគ្មានគម្រោងយកចេញមុនកំណត់ ដូចជាពិធីការភ្ជាប់បណ្តាញ អាចដាក់អតិថិជនស្ថិតក្នុងភាពងាយរងគ្រោះ ប្រសិនបើពួកគេខ្វះការយល់ដឹងអំពីផលប៉ះពាល់នៃការប្រើប្រាស់បន្តនៃលក្ខណៈពិសេសនោះ។ ឧទាហរណ៍ ផលិតផលមួយចំនួនបន្តប្រើពិធីការភ្ជាប់បណ្តាញ ដែលមានប្រភពដើមនៅក្នុងទសវត្សរ៍ឆ្នាំ 1990 ឬឆ្នាំ 2000 ហើយឥឡូវនេះត្រូវបានគេដឹងថាមិនមានសុវត្ថិភាពទេ។ មានកត្តាជាច្រើនដែលអាចពន្យឺតល្បឿនដែលអតិថិជនដំឡើងឱ្យប្រសើរឡើង និងដាក់ប្រើប្រាស់វិធានការសន្តិសុខទំនើបនានា។ ពួកគេអាចប្រើផលិតផលដែលរួមបញ្ចូលជាមួយបណ្តាញផ្សេងទៀតរបស់ស្ថាប័ន ប៉ុន្តែខ្វះវិធានការសន្តិសុខទំនើប ដែលទប់ស្កាត់ក្រុម IT ពីការធ្វើទំនើបកម្ម។ ទោះយ៉ាងណាក៏ដោយ ក្រុមហ៊ុនផលិតសូហ្វវែរអាចដាក់គំរូទាំងនេះ ចូលទៅក្នុងដំណើរការរៀបចំផែនការរបស់ពួកគេដើម្បីលើកទឹកចិត្តអតិថិជនឱ្យតាមទាន់បច្ចុប្បន្នភាព។

ការកំណត់លំនាំដើមកម្មវិធី គឺជាតំបន់នៃហានិភ័យបន្ថែមដែលអាចកើតមានសម្រាប់អតិថិជន។ ក្រុមហ៊ុនផលិតជាញឹកញាប់ជ្រើសរើសការកំណត់លំនាំដើមជាក់លាក់ ដែលធ្វើឱ្យវាកាន់តែងាយស្រួលសម្រាប់អតិថិជន ក្នុងការប្រើប្រាស់លក្ខណៈពិសេសនៃកម្មវិធីដែលពួកគេចង់បាន។ គុណវិបត្តិគឺថាការអនុវត្តនេះ បង្កើនផ្ទៃវាយប្រហារសម្រាប់អតិថិជនដែលប្រហែលជាមិនត្រូវការលក្ខណៈពិសេសនិងពិធីការជាក់លាក់មួយចំនួនដែលត្រូវបានបើកដំណើរការតាមលំនាំដើមនោះទេ។ លើសពីនេះ ការគ្រប់គ្រងសន្តិសុខជាច្រើនត្រូវបានបិទតាមលំនាំដើម ឬតម្រូវឱ្យអតិថិជនចំណាយពេលវេលាដើម្បីកំណត់រចនាសម្ព័ន្ធរបស់ពួកគេ ដើម្បីបង្កើនសន្តិសុខ។ ការបង្កើតគំរូការគំរាមកំហែងច្បាស់លាស់ គឺជាយុទ្ធវិធីដែលអាចជួយជូនដំណឹងដល់ការសម្រេចចិត្ត អំពីលក្ខណៈពិសេសណាមួយដែលគួរតែបើកដំណើរការតាមលំនាំដើម ឬការកំណត់ណាមួយដែលត្រូវការដើម្បីឱ្យមានសន្តិសុខតាមលំនាំដើម។ យុទ្ធវិធីមួយទៀតគឺការស៊ើបអង្កេតវិធីនានា ដើម្បីធ្វើឱ្យលក្ខណៈពិសេសកាន់តែអាចរកឃើញសម្រាប់អ្នកគ្រប់គ្រង។

ក្រុមហ៊ុនផលិតមួយចំនួនការដឹកជញ្ជូនផលិតផលតាមលំនាំដើម ដែលអាចបង្កើតហានិភ័យសម្រាប់អតិថិជនមួយចំនួន ឬទាំងអស់របស់ពួកគេ។ ជាជាងកំណត់លំនាំដើមដែលមានសុវត្ថិភាពជាងមុន ពួកគេតែងតែជ្រើសរើសផលិត **សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ** ដែលអតិថិជនត្រូវតែអនុវត្តដោយចំណាយផ្ទាល់ខ្លួនរបស់ពួកគេ។ សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធទទួលរងនូវបញ្ហាទូទៅមួយចំនួន។ សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធខ្លះពិបាករក ហើយមិនត្រូវបានគាំទ្រល្អទេ។ ខ្លះទៀតមានភាពស្មុគស្មាញក្នុងការអនុវត្ត ពេលខ្លះទាមទារឱ្យមានការអភិវឌ្ឍសូហ្វវែរដើម្បីសរសេរម៉ូឌុលបន្ថែម។ ទោះយ៉ាងណាក៏ដោយ ខ្លះទៀតសន្មត់ថា អ្នកអានមានបទពិសោធន៍សន្តិសុខអ៊ីនធឺណិតយ៉ាងទូលំទូលាយ ដើម្បីយល់ដឹងពីវិធីនានាដែលការកំណត់ផ្សេងៗផ្លាស់ប្តូរផ្ទៃវាយប្រហារ។ អ្នកអនុវត្តដែលមានការយល់ដឹងមិនពេញលេញអំពីវិធីដែលអ្នកវាយប្រហារធ្វើការអាចនឹងបរាជ័យ ក្នុងការអនុវត្តការណែនាំនៅក្នុងសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធត្រឹមត្រូវជាពិសេស ប្រសិនបើការណែនាំមិនធ្វើឱ្យមានការសម្របសម្រួលច្បាស់លាស់។ លើសពីនេះ មិនមែនសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធទាំងអស់ ត្រូវបានសរសេរដោយវិស្វកររដែលមានការយល់ដឹងច្បាស់លាស់អំពីយុទ្ធវិធីវាយប្រហារ និងសេដ្ឋកិច្ច ដែលបណ្តាលឱ្យពួកគេបង្កើតសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធដែលមិនមានប្រសិទ្ធភាព ទោះបីជាត្រូវបានអនុវត្តដោយទៀងត្រង់ក៏ដោយ។ អតិថិជនរាប់លាននាក់កំពុងទទួលខុសត្រូវលើការពង្រឹងកម្មវិធី ឬប្រព័ន្ធជាច្រើន ដែលជារឿយៗស្ថិតនៅក្នុងបរិស្ថានធនធានដែលមានកម្រិត។ ការពឹងផ្អែកលើសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធគ្មាននិរន្តភាពទេ។

ការកំណត់របស់កម្មវិធីគួរតែត្រូវបានវាយតម្លៃជាបន្តបន្ទាប់ ថាតើការកំណត់គឺជាលំនាំដើម ឬកំណត់ដោយអតិថិជន ទល់នឹងការយល់ដឹងបច្ចុប្បន្នរបស់ក្រុមហ៊ុនផលិតអំពីទិដ្ឋភាពគំរាមកំហែង។ កម្មវិធីគួរតែត្រូវបានធ្វើឡើងដោយមានសញ្ញាបង្ហាញច្បាស់លាស់អំពីហានិភ័យដែលអាចកើតមានពីការកំណត់ទាំងនោះ ហើយគួរតែធ្វើឱ្យគេបានស្គាល់ច្បាស់នូវសញ្ញាបង្ហាញទាំងនោះ។ ដូចជារថយន្តទំនើបមានសញ្ញាបង្ហាញអំពីខ្សែក្រវ៉ាត់សុវត្ថិភាព ហើយបង្ហាញសញ្ញាបង្ហាញនោះដោយបន្លឺសំឡេងរោទ៍ ប្រសិនបើអ្នកព្យាយាមបើកបរដោយមិនបានបំពាក់ក្រវ៉ាត់សុវត្ថិភាពនោះ សូហ្វវែរគួរតែបង្ហាញសញ្ញាអំពីស្ថានភាពសន្តិសុខនៃប្រព័ន្ធ។ ប្រសិនបើកម្មវិធីមួយត្រូវបានកំណត់រចនាសម្ព័ន្ធមិនតម្រូវឱ្យមាន MFA សម្រាប់គណនីអ្នកគ្រប់គ្រងទេ វាគួរតែធ្វើឱ្យអ្នកគ្រប់គ្រងដឹងជាទៀងទាត់ថាពួកគេ និងស្ថាប័នទាំងមូលរបស់ពួកគេស្ថិតក្នុងសភាពគ្រោះថ្នាក់ ប្រសិនបើពួកគេមិនកំណត់រចនាសម្ព័ន្ធ MFA។ លើសពីនេះទៀត ប្រសិនបើកម្មវិធីមួយត្រូវបានកំណត់រចនាសម្ព័ន្ធដើម្បីគាំទ្រពិធីការចាស់ៗ ដែលឥឡូវនេះត្រូវបានគេស្គាល់ថាអនុវត្តការធ្វើកូដនីយកម្មខ្សោយ វាគួរតែបញ្ជាក់ឱ្យបានទៀងទាត់ចំពោះអ្នកគ្រប់គ្រងថាស្ថាប័នស្ថិតក្នុងសភាពគ្រោះថ្នាក់ និងផ្តល់ធនធានដើម្បីដោះស្រាយស្ថានភាពនេះ។ យើងជំរុញក្រុមហ៊ុនផលិតឱ្យអនុវត្តការជំរុញជាប្រចាំដែលត្រូវបានបង្កើតឡើងនៅក្នុងផលិតផល ជាជាងពឹងផ្អែកលើអ្នកគ្រប់គ្រងដើម្បីឱ្យមានពេលវេលា ជំនាញ និងការយល់ដឹងក្នុងការបកស្រាយសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ។ ឱកាសមានយ៉ាងច្បាស់សម្រាប់ការច្នៃប្រឌិត ដើម្បីធ្វើឱ្យមានតុល្យភាពលើការពិចារណាលើសន្តិសុខ និងលទ្ធភាពប្រើប្រាស់។

ធាតុនីមួយៗខាងលើបង្កើតស្ថានភាពដែលមិនអាចដោះស្រាយបាន ដែលអតិថិជនចាំបាច់ត្រូវស្រាវជ្រាវ ផ្តល់មូលនិធិ ទិញ រៀបចំបុគ្គលិក ដាក់ប្រើប្រាស់ និងតាមដាន**ផលិតផលសន្តិសុខ**បន្ថែម ដើម្បីកាត់បន្ថយឱកាសរងការវាយប្រហារតាមអ៊ីនធឺណិត។ ស្ថាប័នខ្នាតតូចនិងមធ្យម (SMOs) ជាទូទៅមិនអាចសម្របសម្រួលជម្រើសទាំងនេះបានទេ។ ពួកគេប្រឈមមុខនឹងភាពខ្វះខាតផ្នែកជំនាញ ការផ្តល់មូលនិធិ និងពេលវេលាដែលកម្រិតសមត្ថភាពបញ្ជូនទិន្នន័យ និងមុខងារ ដែលបង្ខំឱ្យសន្តិសុខមានអាទិភាពទាបជាង ហើយសរុបមក បង្កើនហានិភ័យរួមកាន់តែធ្ងន់ធ្ងរ។ ផ្ទុយទៅវិញ ការវិនិយោគផ្នែកសន្តិសុខដោយក្រុមហ៊ុនផលិតមួយចំនួនដែលទាក់ទងគ្នានឹងមាននិរន្តភាព។ ឃ្លាទូទៅដែលសង្ខេបបញ្ហានេះគឺថា ឧស្សាហកម្មសូហ្វវែរចាំបាច់ត្រូវការផលិតផលដែលមានសន្តិសុខច្រើនជាង មិនមែនផលិតផលសន្តិសុខច្រើនជាងនោះទេ។ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែដឹកនាំការផ្លាស់ប្តូរនោះ។

> ***ឧស្សាហកម្មសូហ្វវែរចាំបាច់ត្រូវការផលិតផលដែលមានសន្តិសុខច្រើនជាង មិនមែនផលិតផលសន្តិសុខច្រើនជាងនោះទេ។ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែដឹកនាំការផ្លាស់ប្តូរនោះ។***

សព្វថ្ងៃនេះ ពេលខ្លះយើងអានមតិយោបល់ពីក្រុមហ៊ុនផលិតដែលពន្យល់ថាអតិថិជនបានរងនូវការវាយប្រហារតាមអ៊ីនធឺណិត ដោយសារតែការមិនបើកមុខងារសន្តិសុខជាក់លាក់ ឬធ្វើតាមគោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ។ ជាជំនួស បន្ទាប់ពីការវាយប្រហារតាមអ៊ីនធឺណិត ក្រុមហ៊ុនផលិតគួរតែពន្យល់ថាតើលក្ខណៈពិសេសសន្តិសុខជាក់លាក់ណាមួយ ឬគោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធជាក់លាក់ណាមួយ នឹងរារាំងការវាយប្រហារតាមអ៊ីនធឺណិត ហើយពិចារណាធ្វើឱ្យវាក្លាយជាលំនាំដើមដោយមិនគិតថ្លៃ។ ក្នុងករណីទាំងនោះដែលផលិតផលខ្លួនឯងមិនត្រូវបានពង្រឹងគ្រប់គ្រាន់ក្នុងដំណាក់កាលរចនា និងអនុវត្តន៍ ក្រុមហ៊ុនផលិតគួរតែពន្យល់ពីរបៀបដែលពួកគេកំពុងធ្វើការ ដើម្បីលុបបំបាត់ភាពងាយរងគ្រោះនោះចេញពីជួរផលិតផលរបស់ពួកគេ។

ក្រុមហ៊ុនផលិតសូហ្វវែរមានទំនួលខុសត្រូវក្នុងការធានាថា ផលិតផលរបស់ពួកគេត្រូវបានរចនា និងអភិវឌ្ឍដោយមានសន្តិសុខជាអាទិភាពកំពូល។ ដល់ទីបញ្ចប់ ពួកគេគួរតែ**វាស់វែងឱ្យបានម៉ត់ចត់នូវលទ្ធផល** នៃកិច្ចខិតខំប្រឹងប្រែងរបស់ពួកគេនៅក្នុងវិស័យនេះ។ យើងអំពាវនាវឱ្យក្រុមហ៊ុនផលិត មិនត្រឹមតែផ្តោតលើកិច្ចខិតខំប្រឹងប្រែងផ្នែកក្នុងរបស់ពួកគេប៉ុណ្ណោះទេ ប៉ុន្តែត្រូវធ្វើការវាស់វែងឱ្យបានម៉ត់ចត់ និងរាយការណ៍ឱ្យបានទៀងទាត់នូវលទ្ធផល និងប្រសិទ្ធភាពនៃកិច្ចខិតខំប្រឹងប្រែង និងការកំណត់រចនាសម្ព័ន្ធសន្តិសុខរបស់ផលិតផល និងបង្កើតជុំនៃមតិកែលម្អដែលបង្កើតការផ្លាស់ប្តូរនៅក្នុង SDLC ដែលនាំឱ្យមានការកែលម្អដែលអាចវាស់វែងបាននៅក្នុងសុវត្ថិភាពអតិថិជន និងផលិតផលដែលមានសន្តិសុខជាងមុន។ ការរាយការណ៍គួរតែរួមបញ្ចូលទិន្នន័យអនាមិកដែលសហគមន៍ស្រាវជ្រាវសម្រាប់ការសិក្សា និងសន្តិសុខអាចប្រើដើម្បីតាមដាននិន្នាការកម្រិតខ្ពស់ និងវាស់វែងប្រព័ន្ធអេកូរីកចម្រើនទាំងមូល។

ការបង្ហាញពីគោលការណ៍នេះ

ក្រុមហ៊ុនផលិតសូហ្វវែរ និងសេវាកម្មអនឡាញ គួរតែស្វែងរកវិធីនានាដើម្បីបង្ហាញពីភាពជោគជ័យក្នុងការអនុវត្តគោលការណ៍នេះ។ ពួកគេគួរតែស្វែងរកការផ្តល់ភស្តុតាងក្នុងទម្រង់ជាអនុផលសម្រាប់អ្នកខាងក្រៅដើម្បីពិនិត្យ។ គ្មានអនុផលណាមួយដោយខ្លួនវាផ្ទាល់នឹងបង្ហាញថា ក្រុមហ៊ុនផលិតកំពុងអនុវត្តកម្មវិធីសន្តិសុខតាមការរចនាដ៏រឹងមាំនោះទេ ប៉ុន្តែតាមរយៈការផ្តល់នូវអនុផលផ្សេងៗ ពួកគេនឹងបង្កើតករណីនៃការប្តេជ្ញាចិត្តរបស់ក្រុមហ៊ុនផលិតក្នុងការអភិវឌ្ឍផលិតផលដែលមានសន្តិសុខ។ វិធីសាស្ត្រនេះគឺស្ថិតនៅក្នុងស្មារតីនៃ "បង្ហាញជាជាងប្រាប់"។

ដើម្បីបង្ហាញពីគោលការណ៍នេះ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែពិចារណាពីជំហាននានាដូចជានៅក្នុងបញ្ជីខាងក្រោម។ ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យទទួលស្គាល់ថា ក្រុមហ៊ុនផលិតសូហ្វវែរមួយចំនួននឹងអាចអនុវត្តភ្លាមៗនូវការអនុវត្តទាំងនេះ និងផលិតវត្ថុដែលគង់នៅពីសម័យដើម ដែលត្រូវគ្នានៅពេលចាប់ផ្តើមនៃការធ្វើដំណើរប្រកបដោយសន្តិសុខតាមការរចនារបស់ពួកគេ។ លើសពីនេះ ក្រុមហ៊ុនផលិតសូហ្វវែរនឹងត្រូវកំណត់អាទិភាពក្នុងបញ្ជីនេះ អាស្រ័យលើរបៀបដែលអតិថិជនដាក់ប្រើប្រាស់ផលិតផលក្នុងវិស័យនេះ ដើម្បីទទួលបានអត្ថប្រយោជន៍សន្តិសុខធំបំផុត។

ការអនុវត្តសន្តិសុខតាមលំនាំដើម

1. **លុបពាក្យសម្ងាត់តាមលំនាំដើម។** ពាក្យសម្ងាត់តាមលំនាំដើមនៅតែបន្តជាប់ពាក់ព័ន្ធ ជាមូលហេតុនៃការវាយប្រហារជាច្រើនជារៀងរាល់ឆ្នាំ។ ការប្តេជ្ញាចិត្តដើម្បីលុបបំបាត់បញ្ហារ៉ាំរ៉ៃនេះ នឹងបដិសេធការចូលប្រើងាយស្រួលដល់អ្នកវាយប្រហារ។ ដូចគ្នានេះដែរ ក្រុមហ៊ុនផលិតគួរតែពិចារណាពីការអនុវត្តពាក្យសម្ងាត់ដែលគួរត្រូវបានអនុវត្ត ដូចជាប្រវែងពាក្យសម្ងាត់អប្បបរមា និងការមិនអនុញ្ញាតឱ្យប្រើពាក្យសម្ងាត់រងការបំពានដែលគេស្គាល់។

2. **អនុវត្តការធ្វើតេស្តផ្ទាល់នៅនឹងកន្លែង។** នៅពេលដែលបច្ចេកវិទ្យាបន្តវិវត្ត និងកាន់តែស្មុគស្មាញ វាមានសារៈសំខាន់កាន់តែខ្លាំងសម្រាប់ក្រុមហ៊ុនផលិតសូហ្វវែរដើម្បីធ្វើការធ្វើតេស្តអ្នកប្រើប្រាស់ដែលផ្តោតលើសន្តិសុខដើម្បីយល់ពីគោលជំហរសន្តិសុខផលិតផលរបស់ពួកគេនៅក្នុងវិស័យនេះ។ ដូចគ្នានឹងរបៀបដែលការស្រាវជ្រាវអ្នកប្រើប្រាស់ជូនដំណឹងអំពីតម្រូវការអភិវឌ្ឍកម្មវិធី ក្រុមហ៊ុនផលិតសូហ្វវែរក៏គួរតែធ្វើការស្រាវជ្រាវអ្នកប្រើប្រាស់ដែលផ្តោតលើសន្តិសុខផងដែរ ដើម្បីយល់ដឹងពីកន្លែងដែលបទពិសោធន៍អ្នកប្រើប្រាស់សន្តិសុខ (UX) ខ្វះខាត។ តាមរយៈការសង្កេតពីរបៀបដែលអតិថិជនដាក់ប្រើប្រាស់ និងប្រើប្រាស់ផលិតផលរបស់ពួកគេនៅក្នុងបរិយាកាសជាក់ស្តែង ក្រុមហ៊ុនផលិតសូហ្វវែរអាចទទួលបាននូវការយល់ដឹងដ៏មានតម្លៃអំពីលទ្ធភាពប្រើប្រាស់ និងប្រសិទ្ធភាពនៃមុខងារ និងការគ្រប់គ្រងសន្តិសុខរបស់ពួកគេ។ ការយល់ដឹងទាំងនេះអាចជួយកំណត់អត្តសញ្ញាណចំណុចសម្រាប់កែលម្អ និងកែលម្អផលិតផលរបស់ពួកគេ ដើម្បីបំពេញតម្រូវការសន្តិសុខរបស់អតិថិជនកាន់តែប្រសើរឡើង។ ឧទាហរណ៍ ការធ្វើតេស្តផ្ទាល់នៅនឹងកន្លែងអាចណែនាំការផ្លាស់ប្តូរនៅក្នុងលំហូរ UX លំនាំដើម ការប្រាប់ឱ្យដឹងពីគ្រោះថ្នាក់ និងការត្រួតពិនិត្យ។ ការធ្វើតេស្តផ្ទាល់នៅនឹងកន្លែង ក៏អាចបង្ហាញពីកន្លែងដែលការកែលម្អពីមុននៅក្នុងការរចនាផលិតផល កាត់បន្ថយល្បឿននៃការជួសជុលកង្វះខាតសុវត្ថិភាព កាត់បន្ថយកំហុសក្នុងការកំណត់រចនាសម្ព័ន្ធ និងកាត់បន្ថយផ្ទៃវាយប្រហារ។

ក្រុមហ៊ុនផលិតគួរតែពិចារណាដូចខាងក្រោម៖

- តើអតិថិជនអនុវត្តតាមសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធបានត្រឹមត្រូវដែរឬទេ?
- តើលក្ខណៈពិសេសនៃសន្តិសុខដែលមានស្រាប់របស់ផលិតផល ដំណើរការដូចការរំពឹងទុកនៅក្នុងវិស័យដែរឬទេ?
- តើលក្ខណៈពិសេសទាំងនោះពិតជាទប់ទល់នឹងការវាយប្រហារក្នុងពិភពពិតទេ?
- តើលក្ខណៈពិសេសមួយណាដែលអាចកាត់បន្ថយលទ្ធភាពរងការវាយប្រហារតាមអ៊ីនធឺណិតបានប្រសើរជាង?

កំណត់ចំណាំ៖ ដើម្បីទទួលបានការយល់ដឹងកាន់តែស៊ីជម្រៅអំពីធាតុទាំងនេះ ក្រុមហ៊ុនផលិតសូហ្វវែរអាចចង់ចាប់ដៃគូជាមួយអតិថិជនដើម្បីធ្វើលំហាត់ក្រុមក្រហម ដើម្បីមើលពីរបៀបដែលផលិតផលទប់ទល់នឹងការវាយប្រហារ។ ការធ្វើតេស្តផ្ទាល់នៅនឹងកន្លែងទាំងនេះអាចធ្វើឡើងនៅទីតាំងជាក់ស្តែងរបស់អតិថិជនតាមអនឡាញ ឬតាមរយៈការបញ្ជូនទិន្នន័យវាស់វែងពីចម្ងាយ (telemetry) ពីកម្មវិធីក្នុងលក្ខណៈរក្សាឯកជនភាព។

3. **កាត់បន្ថយទំហំនៃសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ។** ក្រុមហ៊ុនផលិតអាចកែលម្អគោលជំហរសន្តិសុខរបស់អតិថិជនដោយការធ្វើឱ្យកាន់តែមានប្រសិទ្ធភាព ឬសូម្បីតែការលុបបំបាត់សៀវភៅណែនាំស្តីពីការពង្រឹងផលិតផល និងផ្តោតលើវិធានការសុវត្ថិភាពដ៏សំខាន់បំផុតដែលអតិថិជនគួរតែផ្តល់អាទិភាពនៅពេលដាក់ប្រើប្រាស់ផលិតផលរបស់ពួកគេ។ ជាជាងការធ្វើឱ្យអតិថិជនវង្វេងមិនដឹងថាធ្វើយ៉ាងម៉េចជាមួយនឹងបញ្ជីត្រួតពិនិត្យវិធានការសន្តិសុខ ក្រុមហ៊ុនផលិតគួរតែកំណត់ហានិភ័យសន្តិសុខកំពូលនានា ថាផលិតផលរបស់ពួកគេងាយនឹងទទួល ហើយផ្តល់ការណែនាំច្បាស់លាស់ និងសង្ខេបអំពីរបៀបកាត់បន្ថយហានិភ័យទាំងនេះ។ លើសពីនេះ ក្រុមហ៊ុនផលិតគួរតែផ្តល់ឱ្យអតិថិជននូវឧបករណ៍ និងស្ថិយប្រវត្តិកម្មដែលសម្រួលដល់ដំណើរការនៃការអនុវត្តការគ្រប់គ្រងសុវត្ថិភាព ដូចជាលំដាប់នៃការណែនាំដែលអាចដាក់ឱ្យប្រើប្រាស់បានយ៉ាងងាយស្រួលនៅក្នុងបរិយាកាសរបស់ពួកគេ។ លើសពីនេះ ឧបករណ៍ទាំងនេះគួរតែអាចផ្ទៀងផ្ទាត់ និងបង្ហាញយ៉ាងច្បាស់នូវការផ្លាស់ប្តូរដែលបានធ្វើឡើងពីខ្សែបន្ទាត់គោលដើម។ តាមរយៈការធ្វើឱ្យមានប្រសិទ្ធភាពនូវសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ និងការផ្តល់ឱ្យអតិថិជននូវឧបករណ៍ងាយស្រួលប្រើ និងស្ថិយប្រវត្តិកម្ម ក្រុមហ៊ុនផលិតអាចកាត់បន្ថយបន្ទុកលើអតិថិជនរបស់ពួកគេ និងជួយធានាថាផលិតផលរបស់ពួកគេត្រូវបានដាក់ឱ្យប្រើប្រាស់ប្រកបដោយសុវត្ថិភាព។ យុទ្ធវិធីមួយនឹងពិចារណាលើការអនុវត្តគោលការណ៍ Pareto ដើម្បីកាត់បន្ថយចំនួនជំហានសម្រាប់ករណីប្រើប្រាស់ទូទៅ (80%) ហើយបន្ទាប់មក ផ្តល់ការណែនាំតាមបរិបទ និងឧបករណ៍សម្រាប់សេណារីយ៉ូទូទៅតិចជាង (20%)។ តាមរបៀបនេះ ក្រុមហ៊ុនផលិតសូហ្វវែរនឹងធ្វើឱ្យរឿងសាមញ្ញៗមានលក្ខណៈសាមញ្ញ ហើយអ្វីៗដែលពិបាកឱ្យអាចធ្វើទៅបាន។ ការធ្វើតេស្តផ្ទាល់នៅនឹងកន្លែងនឹង

ក្លាយជាឧបករណ៍ដ៏មានឥទ្ធិពលក្នុងការរាស់វែងរយៈពេលដែលអតិថិជនត្រូវការពេលដើម្បីស្វែងរក ស្វែងយល់ និងអនុវត្តតាមសៀវភៅនាំស្តីពីការពង្រឹងប្រព័ន្ធ។ ក្រុមហ៊ុនផលិតគួរតែពិចារណាពីរបៀបដែលផលិតផលអាចជំរុញអ្នកគ្រប់គ្រងឱ្យចាត់វិធានការនៅក្នុងផលិតផលខ្លួនវា ជាជាងការពឹងផ្អែកលើពួកគេដើម្បីអនុវត្តកិច្ចការពីសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ។

4. **រារាំងយ៉ាងសកម្មនូវការប្រើប្រាស់លក្ខណៈពិសេសកេរ្តិ៍ដំណែលដែលមិនមានសុវត្ថិភាព។** កំណត់អាទិភាពសន្តិសុខតាមរយៈផ្លូវដំឡើងឱ្យប្រសើរឡើងច្បាស់លាស់ ជាងភាពត្រូវគ្នាដែលថយក្រោយ។ បោះពុម្ពផ្សាយការបង្ហោះប្លុកដែលបង្ហាញពីការទទួលយកមកអនុវត្តនូវលក្ខណៈពិសេស និងពិធីការដែលមានសុវត្ថិភាពជាងមុន ហើយបដិសេធលក្ខណៈពិសេសដែលមិនមានសុវត្ថិភាពដោយការប្រកាស ដែលអាចមកពីក្នុងផលិតផលខ្លួនឯង។ អតិថិជនមួយចំនួនធំបានបង្ហាញថា ពួកគេនឹងមិនរក្សាប្រព័ន្ធរបស់ពួកគេឱ្យទាន់នឹងបណ្តាញទំនើបអត្តសញ្ញាណ និងលក្ខណៈពិសេសសុវត្ថិភាពសំខាន់ៗផ្សេងទៀតទេ។ ក្នុងករណីខ្លះ អតិថិជនបារម្ភថាមុខងារដែលមានស្រាប់ នឹងមិនដំណើរការជាមួយនឹងការដំឡើងឱ្យប្រសើរឡើងនោះទេ។ តាមរយៈការដំឡើងឱ្យប្រសើរឡើងឱ្យមានភាពរលូនតាមដែលអាចធ្វើទៅបាន អតិថិជនទំនងជានឹងការដំឡើងឱ្យប្រសើរឡើង និងទទួលបានការជួសជុលសន្តិសុខឱ្យបានញឹកញាប់ និងឆាប់រហ័ស។ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែជំរុញអតិថិជនឱ្យខ្លាំងឱ្យអនុវត្តតាមផ្លូវដំឡើង ឱ្យប្រសើរឡើងដែលកាត់បន្ថយហានិភ័យរបស់អតិថិជន។

5. **អនុវត្តការប្រាប់ឱ្យដឹងពីគ្រោះថ្នាក់ដែលទាក់ទាញការយកចិត្តទុកដាក់។** ស្រដៀងទៅនឹងសំឡេងរោទិ៍ខ្សែក្រវ៉ាត់សុវត្ថិភាពក្នុងរថយន្តដែលបញ្ចេញសំឡេងជាបន្តបន្ទាប់ នៅពេលមិនបានរឹតបន្តឹងខ្សែក្រវ៉ាត់សុវត្ថិភាព ក្រុមហ៊ុនផលិតគួរតែអនុវត្តការប្រាប់ឱ្យដឹងពីគ្រោះថ្នាក់ឱ្យទាន់ពេលវេលា និងម្តងហើយម្តងទៀតនៅពេលដែលអ្នកប្រើប្រាស់ ឬអ្នកគ្រប់គ្រងស្ថិតក្នុង ស្ថានភាពមិនមានសុវត្ថិភាព ដោយព្រមានអ្នកគ្រប់គ្រងថាពួកគេកំពុង ប្រើប្រាស់ពិធីការដែលបានបដិសេធក្នុងបរិស្ថានរបស់ពួកគេ និងណែនាំផ្លូវដំឡើងឱ្យប្រសើរឡើង។ អនុវត្តការប្រាប់ឱ្យដឹងពីគ្រោះថ្នាក់ឱ្យទាន់ពេលវេលា និងម្តងហើយម្តងទៀត នៅពេលដែលអ្នកប្រើប្រាស់ ឬអ្នកគ្រប់គ្រង ឬការកំណត់រចនាសម្ព័ន្ធកម្មវិធី ស្ថិតក្នុងស្ថានភាពមិនមានសុវត្ថិភាព។ ធ្វើឱ្យរបៀបមិនសុវត្ថិភាពមានភាពច្បាស់លាស់ចំពោះអ្នកគ្រប់គ្រងជាប្រចាំ។ លក្ខណៈពិសេសបន្ថែមអាចតម្រូវឱ្យអ្នកគ្រប់គ្រងឋានៈខ្ពស់ទទួលស្គាល់កង្វះ MFA នៅលើគណនីរបស់ពួកគេនៅពេលចូលបើកចូលម្តងៗ ឬសូម្បីតែបិទលក្ខណៈពិសេសសំខាន់ៗមួយចំនួន រហូតដល់ពួកគេបើកដំណើរការ MFA។ មានចន្លោះដើម្បីច្នៃប្រឌិតដើម្បីសម្រេចបាននូវគោលដៅទាំងនេះ ខណៈពេលដែលមិនបង្កើតភាពខ្សោយនៃប្រាប់ឱ្យដឹងពីគ្រោះថ្នាក់។

6. **បង្កើតគំរូកំណត់រចនាសម្ព័ន្ធសន្តិសុខ។** គំរូទាំងនេះអាចកំណត់រចនាសម្ព័ន្ធជាក់លាក់ជាមុនភ្ជាប់ ទៅនឹងការកំណត់សុវត្ថិភាពដោយផ្អែកលើកម្រិតហានិភ័យដែលអាចទទួលយកបានរបស់ស្ថាប័ន។ ខណៈពេលដែលវាអាចមានភាពសាមញ្ញពេកក្នុងការមានគំរូសន្តិសុខទាប/មធ្យម/ខ្ពស់នោះ ឧទាហរណ៍នោះបង្ហាញពីចំនួនការកំណត់អាចត្រូវបានអាប់ដេតដើម្បីគ្រប់គ្រងហានិភ័យសម្រាប់ស្ថាប័ន។ គំរូអាចត្រូវបានគាំទ្រដោយ សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ អំពីហានិភ័យនានាដែលក្រុមហ៊ុនផលិតបានកំណត់។

ការអនុវត្តការអភិវឌ្ឍផលិតផលដែលមានសន្តិសុខ

1. **ការអនុលោមតាមឯកសារស្របទៅនឹងក្របខ័ណ្ឌ SDLC ដែលមានសន្តិសុខ។** ក្របខណ្ឌ SDLC ដែលមានសន្តិសុខផ្តល់នូវគោលបំណង និងឧទាហរណ៍ទូទៅលើមនុស្ស ដំណើរការ និងបច្ចេកវិទ្យា។ ពិចារណាលើការផ្សព្វផ្សាយការពិពណ៌នាលម្អិតនៃការត្រួតពិនិត្យក្របខ័ណ្ឌ SDLC ដែលមានសន្តិសុខណាមួយត្រូវបានអនុវត្ត ហើយពណ៌នាអំពីការគ្រប់គ្រងជំនួសណាមួយដែលត្រូវបានប្រើប្រាស់។ នៅសហរដ្ឋអាមេរិក សូមពិចារណាប្រើប្រាស់ក្របខ័ណ្ឌអភិវឌ្ឍន៍សូហ្វវែរដែលមានសន្តិសុខ NIST (SSDF)។ ទោះបីមិនមែនជាបញ្ជីត្រួតពិនិត្យក៏ដោយ SSDF "ពិពណ៌នាអំពីសំណុំនៃការអនុវត្តត្រឹមត្រូវ ជាមូលដ្ឋានគ្រឹះសម្រាប់ការអភិវឌ្ឍសូហ្វវែរដែលមានសន្តិសុខ។"

2. **កត់ត្រាគោលដៅសមិទ្ធកម្មសន្តិសុខអ៊ីនធឺណិត (CPG) ឬការអនុលោមសមមូល។** នៅពេលដែលស្ថាប័នមួយបញ្ជាក់ថាពួកគេអនុលោមតាមស្តង់ដារ NIST SSDF ពួកគេកំពុងអះអាងថា SDLC របស់ពួកគេត្រូវបានជូនដំណឹង ដោយការអនុវត្តល្អបំផុតដែលបានយល់ដឹងច្បាស់។ ទោះយ៉ាងណាក៏ដោយ វាមិនគ្រប់គ្រាន់សម្រាប់ពួកគេក្នុងការមាន SDLC ដ៏រឹងមាំនោះទេ។ ពួកគេក៏ត្រូវការពារសហគ្រាស និងបរិស្ថានអភិវឌ្ឍន៍របស់ពួកគេផងដែរ ពីអ្នកប្រព្រឹត្តទុច្ចរិតដែលនឹងព្យាយាមប្រើប្រាស់លក្ខណៈសម្បត្តិសន្តិសុខ ផលិតផល ខណៈពេលដែលវាកំពុងស្ថិតក្រោមការអភិវឌ្ឍនៅឡើយ។ នេះមិនមែនជាប្រភេទការវាយប្រហារតាមទ្រឹស្តីទេ ប៉ុន្តែជាការវាយប្រហារមួយ ដែលត្រូវបានអនុវត្តដោយផលប៉ះពាល់អវិជ្ជមានដល់អតិថិជន និងដោយសន្តិសុខជាតិបន្ត។ ស្ថាប័ននានាគួរតែពិចារណាលើការបោះពុម្ពផ្សព្វផ្សាយព័ត៌មានលម្អិតស្តីពីការអនុលោមរបស់ស្ថាប័នទៅនឹង CISA CPGs ក្របខ័ណ្ឌសន្តិសុខអ៊ីនធឺណិត NIST (CSF) ឬក្របខ័ណ្ឌកម្មវិធីសន្តិសុខអ៊ីនធឺណិតផ្សេងទៀត។

3. **ការគ្រប់គ្រងភាពងាយរងគ្រោះ។** ក្រុមហ៊ុនផលិតមួយចំនួនមានកម្មវិធីគ្រប់គ្រងភាពងាយរងគ្រោះ ដែលផ្តោតលើការជួសជុលភាពងាយរងគ្រោះដែលបានរកឃើញនៅខាងក្នុង ឬខាងក្រៅ និងមិនច្រើនជាងនេះ។ កម្មវិធីដែលមានភាពចាស់ទុំកាន់តែច្រើនដាក់បញ្ចូលការវិភាគទិន្នន័យ យ៉ាងទូលំទូលាយអំពីភាពងាយរងគ្រោះ និងមូលហេតុឫសគល់របស់វា ដោយចាត់វិធានការជាប្រព័ន្ធដើម្បីលុបបំបាត់ប្រភេទនៃភាពងាយរងគ្រោះទាំងស្រុង[3]។ ពួកគេអនុវត្តកម្មវិធីផ្លូវការជុំវិញការកំណត់ផែនការគុណភាព ការត្រួតពិនិត្យគុណភាព ការកែលម្អគុណភាព និងការវាស់វែងគុណភាព។ ពួកគេចាត់ទុកការគ្រប់គ្រងកង្វះខាតជាបញ្ហាអាជីវកម្ម មិនមែនគ្រាន់តែជាបញ្ហាសន្តិសុខនោះទេ។ កម្មវិធីទាំងនេះមិនមែនប្លែកៗគ្នាក្នុងវិធីមួយចំនួនទៅនឹងកម្មវិធីគុណភាព និងសុវត្ថិភាពនៅក្នុងឧស្សាហកម្មផ្សេងទៀតទេ។

4. **ប្រើសូហ្វវែរដែលមានប្រភពបើកចំហដោយទទួលខុសត្រូវ។** នៅពេលដែលសូហ្វវែរដែលមានប្រភពបើកចំហត្រូវបានប្រើប្រាស់ សូមទទួលខុសត្រូវដោយការពិនិត្យមើលកញ្ចប់ដែលមានប្រភពបើកចំហ ជំរុញការរួមចំណែករបស់កូដត្រឡប់ទៅភាពពឹងផ្អែកវិញ ហើយជួយគាំទ្រការអភិវឌ្ឍ និងការថែរក្សាសមាសធាតុសំខាន់ៗ។ សម្រាប់ជាឯកសារយោង ក្រសួងសេដ្ឋកិច្ច ពាណិជ្ជកម្ម និងឧស្សាហកម្ម (METI) របស់ប្រទេសជប៉ុនបានបោះពុម្ពផ្សព្វផ្សាយ "ការប្រមូលឧទាហរណ៍ ករណីប្រើប្រាស់ទាក់ទងនឹងវិធីសាស្ត្រគ្រប់គ្រងសម្រាប់ការប្រើប្រាស់ OSS និងការធានាសន្តិសុខរបស់វា។"

5. **ផ្តល់សន្តិសុខលំនាំដើមសម្រាប់អ្នកអភិវឌ្ឍ។** ធ្វើឱ្យផ្លូវលំនាំដើមក្នុងអំឡុងពេលអភិវឌ្ឍសូហ្វវែរឱ្យមានសន្តិសុខ ដោយផ្តល់នូវប្លុកសាងសង់ដែលមានសុវត្ថិភាពសម្រាប់អ្នកអភិវឌ្ឍ។ ជាឧទាហរណ៍ ដោយសារប្រវ៉ាឡង់នៃភាពងាយរងគ្រោះនៃការចាក់បញ្ចូល SQL ដែលបង្កឱ្យមានគ្រោះថ្នាក់នៅក្នុងពិភពពិត ធានាថាអ្នកអភិវឌ្ឍប្រើប្រាស់បណ្ណាល័យដែលឱ្យមានការថែទាំយ៉ាងល្អ ដើម្បីការពារពីប្រភេទនៃភាពងាយរងគ្រោះនោះ។ ត្រូវបានគេស្គាល់ផងដែរថាជា "ផ្លូវដែលបានត្រួសត្រាយរួច" ឬ "ផ្លូវដែលមានពន្លឺគ្រប់គ្រាន់" ការអនុវត្តនេះធានាទាំងល្បឿន និងសន្តិសុខ និងកាត់បន្ថយកំហុសរបស់មនុស្ស។

6. **បង្កើតកម្លាំងពលកម្មអ្នកអភិវឌ្ឍសូហ្វវែរដែលយល់ដឹងពីសន្តិសុខ។** ត្រូវប្រាកដថាអ្នកអភិវឌ្ឍសូហ្វវែររបស់អ្នកយល់ដឹងពីសន្តិសុខ ដោយបណ្តុះបណ្តាលពួកគេអំពីការអនុវត្តល្អបំផុតក្នុងការសរសេរកូដដែលមានសន្តិសុខ។ លើសពីនេះ ជួយបំប្លែងកម្លាំងការងារឱ្យមានកាន់តែទូលំទូលាយ ដោយធ្វើបច្ចុប្បន្នភាពការអនុវត្តការជួល ដើម្បីវាយតម្លៃចំណេះដឹងផ្នែកសន្តិសុខ និងធ្វើការជាមួយសាកលវិទ្យាល័យ វិទ្យាល័យក្នុងសហគមន៍ សាលាបណ្តុះបណ្តាលទាហាន និងអ្នកអប់រំផ្សេងទៀត ដើម្បីភ្ជាប់សន្តិសុខទៅក្នុងកម្មវិធីសិក្សាផ្នែកវិទ្យាសាស្ត្រកុំព្យូទ័រ និងការអភិវឌ្ឍសូហ្វវែរ។

[3] NIST SSDF, PO 1.2, ឧទាហរណ៍ 2៖ "កំណត់គោលនយោបាយដែលបញ្ជាក់តម្រូវការសន្តិសុខសម្រាប់សូហ្វវែររបស់ស្ថាប័ន និងផ្ទៀងផ្ទាត់ការអនុលោមតាមចំណុចសំខាន់ៗនៅក្នុង SDLC (ឧទាហរណ៍ ប្រភេទនានានៃកំហុសសូហ្វវែរដែលត្រូវបានផ្ទៀងផ្ទាត់ដោយច្រកទ្វារ ការឆ្លើយតបចំពោះភាពងាយរងគ្រោះដែលបានរកឃើញនៅក្នុងសូហ្វវែរដែលបានចេញផ្សាយ)។"

7. **ធ្វើតេស្តការគ្រប់គ្រងព្រឹត្តិការណ៍ឧប្បត្តិហេតុសន្តិសុខ (SIEM) និងការដាក់បញ្ចូលការសម្របសម្រួលផ្នែកសន្តិសុខស្វ័យប្រវត្តិកម្ម និងការឆ្លើយតប (SOAR)។** បន្ថែមពីលើការធ្វើតេស្តផ្ទាល់នៅនឹងកន្លែង សូមធ្វើការរួមគ្នាជាមួយអ្នកផ្តល់សេវាកម្ម SIEM និង SOAR ដ៏ពេញនិយម ដោយភ្ជាប់ជាមួយអតិថិជនដែលបានជ្រើសរើស ដើម្បីយល់ដឹងពីរបៀបដែលក្រុមឆ្លើយតបឧប្បត្តិហេតុប្រើប្រាស់ កំណត់ហេតុ ដើម្បីស៊ើបអង្កេតឧប្បត្តិហេតុសន្តិសុខដែលសង្ស័យ ឬជាក់ស្តែង។ អ្នកអភិវឌ្ឍសូហ្វវែរមួយចំនួនមានបទពិសោធន៍ឆ្លើយតបនឹងឧប្បត្តិហេតុ ហើយអាចបង្កើតកំណត់ហេតុបើកចូល ដែលមិនជួយអ្នកឆ្លើយតបបានច្រើនដូចដែលពួកគេរំពឹងទុកទេ។ ដោយធ្វើការទាំងជាមួយបច្ចេកវិទ្យា SIEM និង SOAR និងអ្នកជំនាញឆ្លើយតបឧប្បត្តិហេតុជាក់ស្តែង ក្រុមការងារអភិវឌ្ឍអាចបង្កើតកំណត់ហេតុដែលប្រាប់រឿងត្រឹមត្រូវ និងពេញលេញ ដែលចំណេញពេលវេលា និងកាត់បន្ថយភាពមិនច្បាស់លាស់ក្នុងអំឡុងពេលមានឧប្បត្តិហេតុមួយ។

8. **តម្រឹមជាមួយស្ថាបត្យកម្មរក្សាសន្តិសុខដោយមិនទុកចិត្តនរណាម្នាក់ (Zero Trust Architecture-ZTA)។** តម្រឹមការណែនាំអំពីការដាក់ឱ្យប្រើប្រាស់ផលិតផលជាមួយ ជាឧទាហរណ៍ ម៉ូដែល NIST ZTA និង ម៉ូដែលមានភាពចាស់ទុំដោយមិនទុកចិត្តនរណាម្នាក់ (Zero Trust Model Maturity) របស់ CISA។ លើកទឹកចិត្តអតិថិជនឱ្យបញ្ចូលគោលការណ៍ទាំងនេះនៅក្នុងបរិយាកាសរបស់ពួកគេ។

ការអនុវត្តអាជីវកម្មដែលគាំទ្រសន្តិសុខ

1. **ផ្តល់ការកត់កំណត់ហេតុដោយមិនគិតថ្លៃបន្ថែម។** សេវាកម្ម Cloud គួរតែប្តេជ្ញាបង្កើត និងរក្សាទុកកំណត់ហេតុដែលទាក់ទងនឹងសុវត្ថិភាពដោយមិនគិតថ្លៃបន្ថែម។ ផលិតផលក្នុងអគារក៏គួរបង្កើតកំណត់ហេតុទាក់ទងនឹងសន្តិសុខផងដែរ ដោយមិនគិតថ្លៃបន្ថែម។ លើសពីនេះ ផលិតផលគួរតែកត់កំណត់ហេតុព្រឹត្តិការណ៍សន្តិសុខតាមលំនាំដើម ដោយសារអតិថិជនជាច្រើនប្រហែលជាមិនយល់ដឹងពីតម្លៃរបស់ពួកគេ រហូតដល់កើតមានឧប្បត្តិហេតុមួយ។ យុទ្ធវិធីទាំងនេះអាចតម្រូវឱ្យមានការពិនិត្យឡើងវិញឱ្យបានហ្មត់ចត់ អំពីព្រឹត្តិការណ៍សន្តិសុខអ្វីដែលគួរត្រូវបានកត់កំណត់ហេតុ ដើម្បីផ្តល់នូវការយល់ដឹងអំពីស្ថានភាពសន្តិសុខអ៊ីនធឺណិត របៀបដែលអតិថិជនអាចកំណត់រចនាសម្ព័ន្ធការកត់កំណត់ហេតុ រយៈពេលរក្សាទុកកំណត់ហេតុ របៀបដែលភាពសុចរិតនៃកំណត់ហេតុ និងការកន្លែងទុកត្រូវបានការពារ និងរបៀបដែលកំណត់ហេតុអាចត្រូវបានវិភាគ។ ក្នុងករណីខ្លះ ការពិនិត្យឡើងវិញអាចណែនាំពីតម្រូវការសម្រាប់ការកែរចនាសម្ព័ន្ធស្ថាបត្យកម្មគ្រប់គ្រងកំណត់ហេតុរបស់កម្មវិធី ដើម្បីជួយធ្វើឱ្យវាអាចធ្វើសកម្មភាពបាន និងក្នុងតម្លៃមួយសមស្របសម្រាប់ក្រុមហ៊ុនផលិត។ ការធ្វើការជាមួយអ្នកជំនាញឆ្លើយតបឧប្បត្តិហេតុ (IR) អាចបង្កើនឱកាសនានា ដែលកំណត់ហេតុនឹងមានប្រយោជន៍សម្រាប់អ្នកស៊ើបអង្កេតក្នុងវិស័យនេះ។ សូមមើលផ្នែកស្តីពី SIEMs។

2. **លុបបំបាត់ពន្ធដែលលាក់កំបាំង។** បោះពុម្ពផ្សព្វផ្សាយការប្តេជ្ញាចិត្តថានឹងមិនគិតថ្លៃលក្ខណៈពិសេសសន្តិសុខ ឬឯកជនភាព ឬការរួមបញ្ចូល។ ជាឧទាហរណ៍ ក្នុងវិសាលភាពធំនៃការគ្រប់គ្រងអត្តសញ្ញាណ និងសិទ្ធិចូលប្រើប្រាស់ (IAM) មានសេវាកម្មដែលហៅថាសេវាកម្មការចុះឈ្មោះចូលតែមួយ (SSO)។ ក្រុមហ៊ុនផលិតមួយចំនួនគិតថ្លៃបន្ថែមទៀតដើម្បីភ្ជាប់ប្រព័ន្ធរបស់ពួកគេទៅនឹងសេវាកម្ម SSO (ជួនកាលគេហៅថាអ្នកផ្តល់អត្តសញ្ញាណ)។ “ពន្ធ SSO” នេះមានន័យថា ការគ្រប់គ្រងអត្តសញ្ញាណ និងសិទ្ធិចូលប្រើប្រាស់ល្អ គឺមានតម្លៃថ្លៃមិនអាចបង់បានសម្រាប់ SMOs ជាច្រើន ដែលរារាំងពួកគេមិនឱ្យសម្រេចបាននូវគោលជំហរសន្តិសុខដ៏រឹងមាំ។ សេវាកម្មមួយចំនួនគិតថ្លៃបន្ថែមដើម្បីបើកដំណើរការ MFA សម្រាប់អ្នកប្រើប្រាស់។ **សន្តិសុខមិនគួរកំណត់តម្លៃជារបស់ល្អប្រណិតនោះទេ ប៉ុន្តែគួរតែបានចាត់ទុកថាជាសិទ្ធិរបស់អតិថិជន។** ក្រុមហ៊ុនផលិតមួយចំនួនបានប្រកែកថា អតិថិជនតិចតួចប៉ុណ្ណោះដែលស្នើសុំមុខងារទាំងនេះ ហើយពួកគេចំណាយប្រាក់កាន់តែច្រើនក្នុងការថែរក្សា។ អំណះអំណាងទាំងនេះមិនអើពើនឹងការពិតដែលថា អតិថិជនមួយចំនួនតូច នឹងទូរសព្ទទៅប្តឹងតវ៉ា ឬចរចា មិនមែនអតិថិជនទាំងអស់ពិតជាយល់ដឹងថា អត្ថប្រយោជន៍នៃលក្ខណៈពិសេសទាំងនេះជាអ្វីនោះទេ ហើយថាលក្ខណៈពិសេសទាំងអស់ត្រូវចំណាយប្រាក់ដើម្បីថែរក្សា។ ប៉ុន្តែយើងមិនទាន់ឃើញក្រុមហ៊ុនផលិតជាច្រើនគិតថ្លៃបន្ថែមសម្រាប់ភាពអាចរកបាន ឬភាពត្រឹមត្រូវនៃទិន្នន័យនោះទេ។ ការចំណាយប្រាក់សម្រាប់គាំទ្របុគ្គលិកលក្ខណៈសំខាន់ៗទាំងនោះ ត្រូវបានបង្កើតឡើងនៅក្នុងតម្លៃដែលអតិថិជនទាំងអស់ត្រូវបង់ ដូចជាថ្លៃដើមដាក់បញ្ចូលខ្សែក្រវ៉ាត់សុវត្ថិភាព ក្បាលដៃចង្កូតឡានដែលអាចបត់បាន និងពោងសុវត្ថិភាពដែលជួយសង្គ្រោះជីវិតមនុស្សក្នុងគ្រោះថ្នាក់។

3. **ទទួលយកស្តង់ដារបើកចំហ។** អនុវត្តស្តង់ដារបើកចំហ ជាពិសេសជុំវិញបណ្តាញទូទៅ និងពិធីការ អត្តសញ្ញាណ។ ជៀសវាងពិធីការដែលមានកម្មសិទ្ធិ នៅពេលដែលស្តង់ដារបើកចំហ អាចរកបាន។

4. **ផ្តល់ឧបករណ៍ដំឡើងឱ្យប្រសើរឡើង។** អតិថិជនជាច្រើនមានការស្ទាក់ស្ទើរក្នុងការទទួលយកកំណែចុងក្រោយបំផុតនៃផលិតផល រួមទាំងការដាក់ឱ្យប្រើប្រាស់លក្ខណៈពិសេសថ្មី និងមានសន្តិសុខ ជាងមុន ដូចជាការភ្ជាប់បណ្តាញសន្តិសុខជាដើម។ ក្រុមហ៊ុនផលិតសូហ្វវែរអាចបង្កើនការទទួលយករបស់អតិថិជននូវការដំឡើងឱ្យប្រសើរឡើងថ្មី ដោយផ្តល់នូវឧបករណ៍ដើម្បីជួយកាត់បន្ថយ ភាពមិនច្បាស់លាស់ និងហានិភ័យ។ ផ្តល់អាជ្ញាប័ណ្ណដោយឥតគិតថ្លៃសម្រាប់អតិថិជនដើម្បីធ្វើតេស្តការដំឡើងឱ្យប្រសើរឡើង និងការជួសជុលនៅក្នុងបរិយាកាសធ្វើតេស្តដែលជាមធ្យោបាយលើកទឹកចិត្តអតិថិជន។

គោលការណ៍ 2៖ ទទួលយកតម្លាភាព និងគណនេយ្យភាពដាច់ខាត

ការពន្យល់

ក្រុមហ៊ុនផលិតសូហ្វវែរគួរមានមោទនភាពក្នុងការផ្តល់នូវផលិតផលដែលមានសុវត្ថិភាព និងសន្តិសុខ ក៏ដូចជាការធ្វើឱ្យមានភាពខុសប្លែកគ្នាក្នុងចំណោមសហគមន៍ក្រុមហ៊ុនផលិតផ្សេងទៀត ដោយផ្អែកលើសមត្ថភាពរបស់ពួកគេក្នុងការធ្វើបែបនោះ។

ចូរយើងដោះស្រាយកង្វល់ទូទៅអំពីតម្លាភាព។ នៅពេលដែលអ្នកអនុវត្តន៍ពិភាក្សាអំពីតម្លាភាពដាច់ខាត មានទំនោរសម្រាប់ការសន្ទនាជាប់គាំងក្នុងក្តីបារម្ភថាពួកគេកំពុងផ្តល់ "ផែនទីបង្ហាញផ្លូវសម្រាប់អ្នកវាយប្រហារ"។ ទោះជាយ៉ាងណាក៏ដោយ ភ័ស្តុតាងដ៏លើសលប់គឺថា អ្នកវាយប្រហារកំពុងដំណើរការបានល្អដោយគ្មានផែនទីបង្ហាញផ្លូវបែបនេះ ហើយការព្រួយបារម្ភបែបនេះគួរតែផ្តល់សារសំខាន់ចំពោះតម្លាភាពជាមុនដែលផ្តល់អត្ថប្រយោជន៍ដល់អតិថិជនផ្ទាល់ អតិថិជនដោយប្រយោល ខ្សែសង្វាក់ផ្គត់ផ្គង់ និងឧស្សាហកម្មសូហ្វវែរទាំងមូល។

តម្លាភាពជួយឧស្សាហកម្មបង្កើតទម្លាប់នានា - ក្នុងពាក្យផ្សេងទៀត ពាក្យថា "ល្អ" នោះមើលទៅមានសភាពដូចម្តេចដែរ។ វាជួយឱ្យទម្លាប់ទាំងនោះផ្លាស់ប្តូរតាមពេលវេលា ដើម្បីឆ្លើយតបទៅនឹងតម្រូវការរបស់អតិថិជន ការផ្លាស់ប្តូរយុទ្ធវិធីរបស់អ្នកគំរាមកំហែង ឬសេដ្ឋកិច្ច ឬការវិវត្តបច្ចេកវិទ្យា។ តម្លាភាពជួយក្រុមហ៊ុនផលិតដែលមានធនធានតិច រៀនសូត្រពីអ្នកដែលមានធនធានចាស់ទុំ និងមានសមត្ថភាពជាង។ ការសន្ទនាអំពីការចែករំលែកព័ត៌មាន គួរតែពង្រីកលើសពីសូចនាករគំរាមកំហែងក្នុងពេលជាក់ស្តែង ដើម្បីដាក់បញ្ចូលធាតុខាងក្រោម។

តម្លាភាពបង្ខំឱ្យការសម្រេចចិត្តជុំវិញសន្តិសុខ ត្រូវធ្វើឡើងនៅដំណាក់កាលដំបូងក្នុងដំណើរការអភិវឌ្ឍ និងជាសកម្មភាពបន្តនៃអ្នកដឹកនាំអាជីវកម្ម ក៏ដូចជាវិស្វករ និងអ្នកជំនាញផ្នែកសន្តិសុខ។ តម្លាភាពបង្កើតគណនេយ្យភាពទៅក្នុងផលិតផល។

កំណត់សម្គាល់លើជម្រើសប្រើគុណនាម "ដាច់ខាត" នៅពីមុខ "តម្លាភាព"។ សព្វថ្ងៃនេះ វាជារឿងចម្លែកសម្រាប់ក្រុមហ៊ុនផលិតសូហ្វវែរដើម្បីបោះពុម្ពផ្សព្វផ្សាយព័ត៌មានលម្អិតអំពីរបៀបដែលពួកគេអភិវឌ្ឍ និងថែទាំសូហ្វវែរ និងរបៀបដែលពួកគេធ្វើឱ្យកម្មវិធីរបស់ពួកគេឱ្យមានភាពចាស់ទុំ ដោយប្រើទិន្នន័យក្នុងរយៈពេលវែង។ នៅក្នុងឧស្សាហកម្មសូហ្វវែរ ក្រុមហ៊ុនផលិតមួយចំនួនតូចផ្តល់ជូននូវដំណើរមើលដោយមានគេណែនាំអំពីរបៀបដែលពួកគេរចនាសូហ្វវែររបស់ពួកគេ។ មានឱកាសតិចតួចសម្រាប់ក្រុមហ៊ុនផលិតសូហ្វវែរ ដើម្បីមើលពីរបៀបដែលស្ថាប័នស្រដៀងគ្នារៀបចំរចនាសម្ព័ន្ធកម្មវិធី SDLC របស់ពួកគេ និងរបៀបដែលកម្មវិធីទាំងនោះរក្សានៅក្នុងបរិយាកាសអតិថិជន ប្រឆាំងនឹងអ្នកវាយប្រហារពិតប្រាកដ។ ឧស្សាហកម្មរួមនឹងទទួលបានអត្ថប្រយោជន៍ពីការចែករំលែកព័ត៌មានបន្ថែមលើប្រធានបទនានា ដូចជាយុទ្ធសាស្ត្រដើម្បីវាស់វែងតម្លៃនៃកង្វះខាតផ្នែកសន្តិសុខ និងដើម្បីលុបបំបាត់ប្រភេទនៃភាពងាយរងគ្រោះ។ ជាលទ្ធផលនៃការអនុវត្តទូទៅទាំងនេះ គ្រប់ក្រុមហ៊ុនផលិតសូហ្វវែរ ត្រូវតែរៀនសូត្រពីរបៀបដោះស្រាយរឿងសន្តិសុខផលិតផលដោយខ្លួនឯង។ ប្រហែលជាដោយការមិនដាក់ពន្ធប្រណិតលើលក្ខណៈពិសេសសន្តិសុខ សុវត្ថិភាព និងសន្តិសុខ ដូច្នេះហើយទើបក្លាយជាមជ្ឈមណ្ឌលចំណាយជាជាងជាមជ្ឈមណ្ឌលរកប្រាក់ចំណេញ ហើយក្រុមហ៊ុននឹងទទួលបានអត្ថប្រយោជន៍ដោយការសម្រាលបន្ទុកតាមរយៈការសហការ និងតម្លាភាព។

យើងចង់ផ្តោតលើយុទ្ធវិធី ដែលនឹងពន្លឿនការវិវត្តនៃឧស្សាហកម្មសូហ្វវែរបានលឿន។ យើងមិនអាចមានលទ្ធភាពធ្វើការកែលម្អដោយឆក់យកឱកាស និងបន្តិចម្តងទៀតទេ។ ប្រសិនបើយើងរួមគ្នាយកឈ្នះលើការគំរាមកំហែងដែលបង្កឡើងដោយសត្រូវដ៏ប៉ិនប្រសប់ និងសម្របខ្លួន យើងត្រូវទទួលយកកម្រិតនៃតម្លាភាពដែលនឹងមានអារម្មណ៍មិនស្រួលនៅថ្ងៃនេះ ប៉ុន្តែវានឹងជំរុញឱ្យឧស្សាហកម្មនេះឆ្ពោះទៅមុខ។ មានក្រុមហ៊ុនផលិតនាពេលបច្ចុប្បន្ននេះ ដែលដាក់បញ្ចូលគោលការណ៍សន្តិសុខតាមការរចនាទាំងនេះមួយចំនួន។ ដូចដែលលោក William Gibson បាននិយាយថា "អនាគតបានមកដល់ហើយ វាគ្រាន់តែមិនបានចែកចាយស្មើៗគ្នាប៉ុណ្ណោះ។" **តម្លាភាពដាច់ខាតនឹងជួយចែកចាយព័ត៌មាននោះ និងផ្តល់អត្ថប្រយោជន៍ដល់អ្នកការពារច្រើនជាងសត្រូវរបស់យើង។**

តម្លាភាពអាចធ្វើបានច្រើនជាងជួយស្ថាប័នស្រដៀងគ្នាធ្វើឱ្យ SDLCs របស់ពួកគេមានភាពចាស់ទុំ ។ អតិថិជន និងអ្នកវិនិយោគនាពេលអនាគត អាចស្វែងយល់បន្ថែមអំពីការវិនិយោគ និងការដោះដូរទំនិញដែលក្រុមហ៊ុនផលិតបានធ្វើ ហើយគោលជំហរសន្តិសុខ ដែលការវិនិយោគទាំងនោះបានបង្កើតសម្រាប់អតិថិជន។ ក្រុមហ៊ុនផលិតដែលទទួលយកតម្លាភាពដាច់ខាត នឹងផ្តល់ឱ្យអតិថិជននូវព័ត៌មានដើម្បីជួយពួកគេធ្វើការសម្រេចចិត្តទិញ មិនត្រឹមតែលើតម្លៃ និងលក្ខណៈពិសេសប៉ុណ្ណោះទេ ប៉ុន្តែនៅលើសន្តិសុខផងដែរ។

ពិបាកដូចគ្នាដែលស្ថាប័នធ្វើការដើម្បីធានាខ្សែសង្វាក់ផ្គត់ផ្គង់របស់ពួកគេ និង SDLC របស់ពួកគេ ដំណើរការបង្កើតសូហ្វវែររបស់ក្រុមហ៊ុនត្រូវបានរងនូវការវាយប្រហារតាមអ៊ីនធឺណិតក្នុងពេលកន្លងទៅថ្មីៗនេះ។ ការទទួលយកតម្លាភាពដាច់ខាតគួរតែនាំឱ្យមានការលាតត្រដាងជាសាធារណៈអំពីការវាយប្រហារ ក៏ដូចជាការកែលម្អដែលក្រុមហ៊ុនបានធ្វើដើម្បីការពារ និងរកឃើញការវាយប្រហារនាពេលអនាគត។ ទម្រង់នៃការចែករំលែកព័ត៌មាននោះ នឹងជួយឱ្យស្ថាប័នផ្សេងទៀតរៀនសូត្រ ដោយមិនចាំបាច់ទទួលរងជោគវាសនាដូចគ្នា។

ការបង្ហាញពីគោលការណ៍នេះ

ដើម្បីបង្ហាញពីគោលការណ៍នេះ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរចាត់វិធានការ រួមមានដូចខាងក្រោម៖

ការអនុវត្តសន្តិសុខតាមលំនាំដើម

1. **បោះពុម្ពផ្សព្វផ្សាយស្ថិតិ និងនិន្នាការពាក់ព័ន្ធសន្តិសុខសរុប។** ប្រធានបទឧទាហរណ៍រួមមានការទទួលយក MFA ដោយអតិថិជន និងអ្នកគ្រប់គ្រង និងការប្រើប្រាស់ពិធីការកេរ្តិ៍ដំណែលដែលមិនមានសុវត្ថិភាព។
2. **បោះពុម្ពផ្សព្វផ្សាយស្ថិតិការជួសជុល។** លម្អិតថាតើអតិថិជនប៉ុន្មានភាគរយកំពុងប្រើកំណែចុងក្រោយបំផុត នៃផលិតផល និងអ្វីដែលអ្នកកំពុងធ្វើដើម្បីធ្វើឱ្យការអាប់ដេតកាន់តែងាយស្រួល និងអាចទុកចិត្តបាន។
3. **បោះពុម្ពផ្សព្វផ្សាយទិន្នន័យស្តីពីសិទ្ធិដែលមិនបានប្រើ។** បោះពុម្ពផ្សព្វផ្សាយព័ត៌មានសរុបស្តីពីការអនុញ្ញាតច្រើនលើសលប់នៅទូទាំងមូលដ្ឋានអតិថិជនរបស់អ្នក ក៏ដូចជាការជំរុញ និងការផ្លាស់ប្តូរផ្សេងទៀតចំពោះផលិតផលដែលអ្នកកំពុងធ្វើ ដើម្បីកាត់បន្ថយផ្ទៃវាយប្រហាររបស់អតិថិជន។ សិទ្ធិដែលមិនបានប្រើទាំងនេះទំនងជាបេក្ខជនល្អសម្រាប់ការប្រាប់ឱ្យដឹងពីគ្រោះថ្នាក់ពីអ្នកគ្រប់គ្រង ដូចជាសំឡេងរោទ៍ខ្សែក្រវ៉ាត់សុវត្ថិភាព។

ការអនុវត្តការអភិវឌ្ឍផលិតផលដែលមានសន្តិសុខ

1. **បង្កើតការគ្រប់គ្រងសន្តិសុខផ្ទៃក្នុង។** ក្រុមហ៊ុនជាច្រើនបានឃើញអត្ថប្រយោជន៍នៃការផ្លាស់ប្តូរទិន្នន័យរបស់ពួកគេទៅកាន់អ្នកផ្តល់សេវាកម្ម cloud (ក្លៅ)។ ឥឡូវនេះអ្នកផ្តល់សេវាកម្ម cloud ទាំងនោះក្លាយជាគោលដៅរបស់អ្នកវាយប្រហារ។ អ្នកផ្តល់សូហ្វវែរជាសេវាកម្ម (Software as a Service-SaaS) គួរតែផ្សព្វផ្សាយស្ថិតិនៃការគ្រប់គ្រងផ្ទៃក្នុងរបស់ពួកគេ។ ជាឧទាហរណ៍ អ្នកផ្តល់ SaaS គួរតែបោះពុម្ពផ្សព្វផ្សាយស្ថិតិស្តីពីការដាក់ឱ្យប្រើប្រាស់ផ្ទៃក្នុងរបស់ពួកគេនៃ MFA ដែលធន់នឹងការបោកបញ្ឆោត ដូចជាការផ្ទៀងផ្ទាត់អត្តសញ្ញាណ តាមអ៊ីនធឺណិតលឿន (FIDO) ជាដើម។ ជាការប្រសើរបំផុត ពួកគេគួរតែអាចនិយាយបានថា គ្មានបុគ្គលិកណាម្នាក់អាចចូលប្រើទិន្នន័យអតិថិជន ឬទិន្នន័យរសើបផ្សេងទៀតបានដោយមិនចាំបាច់ផ្ទៀងផ្ទាត់តាមរយៈ MFA ដែលធន់នឹងការបោកបញ្ឆោតនោះទេ។

2. **បោះពុម្ពផ្សព្វផ្សាយម៉ូដែលគំរាមកំហែងកម្រិតខ្ពស់។** ផលិតផលសន្តិសុខតាមការរចនា ចាប់ផ្តើមជាមួយនឹងម៉ូដែលគំរាមកំហែងជាលាយលក្ខណ៍អក្សរ ដែលពិពណ៌នាអំពីអ្វីដែលអ្នកបង្កើត កំពុងព្យាយាមការពារ និងពីអ្នកណា។ ម៉ូដែលគំរាមកំហែងប្រកបដោយប្រសិទ្ធភាពត្រូវបានដឹងដោយវិធីដែលការឈ្លានពានកើតឡើងនៅទីដាច់ស្រយាល ហើយគួរតែគ្របដណ្តប់ទាំងសហគ្រាស និងបរិស្ថានអភិវឌ្ឍន៍ ក៏ដូចជាវិធីដែលក្រុមហ៊ុនផលិតសូហ្វវែរ មានបំណងប្រើវានៅក្នុងបរិយាកាសអតិថិជន។

3. **បោះពុម្ពផ្សព្វផ្សាយការបញ្ជាក់ដោយខ្លួនឯងអំពី SDLC សន្តិសុខលម្អិត។** ក្រុមហ៊ុនផលិតដែលធ្វើតាម NIST SSDF ឬក្របខ័ណ្ឌស្រដៀងគ្នាផ្សេងទៀត កំពុងធ្វើការយ៉ាងសកម្មឆ្ពោះទៅរកវដ្តជីវិតនៃការអភិវឌ្ឍសូហ្វវែរដែលមានភាពចាស់ទុំ។ ការបោះពុម្ពផ្សព្វផ្សាយការបញ្ជាក់ដោយខ្លួនឯងអំពីការគ្រប់គ្រងណាដែលក្រុមហ៊ុនផលិតបានអនុម័ត ហើយសម្រាប់ផលិតផលណាមួយ នឹងបង្ហាញពីការប្តេជ្ញាចិត្តក្នុងការប្រកាន់ខ្ជាប់នូវការអនុវត្តល្អបំផុតទាំងនេះ និងផ្តល់នូវកម្រិតនៃការបង្កើនទំនុកចិត្តដល់អតិថិជនរបស់ពួកគេ។ ឧទាហរណ៍ គម្រោងការបញ្ជាក់ផ្សេងទៀតរួមមានវិធីសាស្ត្រខ្សែសង្វាក់ផ្គត់ផ្គង់អ៊ីស្រាអែល។

4. **ទទួលយកតម្លាភាពនៃភាពងាយរងគ្រោះ។** បោះពុម្ពផ្សព្វផ្សាយការប្តេជ្ញាចិត្តដែលនឹងធានាថា ភាពងាយរងគ្រោះនៃផលិតផលដែលបានកំណត់អត្តសញ្ញាណនឹងត្រូវបានផ្សព្វផ្សាយជាការកំណត់ចូល CVE ដែលត្រឹមត្រូវ និងពេញលេញ។ នោះជាការពិតជាពិសេសសម្រាប់តំបន់គណនាភាពទន់ខ្សោយទូទៅ ដែលកំណត់អត្តសញ្ញាណមូលហេតុឫសគល់នៃភាពងាយរងគ្រោះ។ ការមានមូលដ្ឋានទិន្នន័យ CVE សាធារណៈកាន់តែត្រឹមត្រូវ និងពេញលេញ ឧស្សាហកម្មអាចតាមដានពីរបៀបដែលផលិតផលកាន់តែមានសន្តិសុខ ហើយប្រភេទនៃភាពងាយរងគ្រោះណាខ្លះដែលកើតមានច្រើនបំផុត។ ទោះជាយ៉ាងណាក៏ដោយ ចូរប្រយ័ត្ននឹងការប៉ុនប៉ងឱ្យរាប់ CVEs ជារង្វាស់អវិជ្ជមាន ពីព្រោះថាលេខបែបនេះក៏ជាសញ្ញានៃសហគមន៍វិភាគ និងធ្វើតេស្តកូដដែលមានសុខភាពល្អផងដែរ។ នៅពេលដែលក្រុមហ៊ុនផលិតអនុវត្តទស្សនសន្តិសុខតាមការរចនា វាអាចទៅរួចដែលថាដំបូងឡើយការរាប់ CVE ឆៅរបស់ពួកគេនឹងកើនឡើងដោយសារតែការរកឃើញកាន់តែទូលំទូលាយ និងការដោះស្រាយភាពងាយរងគ្រោះនៅក្នុងកូដដែលមានស្រាប់។ ក្រុមហ៊ុនផលិតគួរតែបោះពុម្ពផ្សព្វផ្សាយការវិភាគអំពីភាពងាយរងគ្រោះពីមុន រួមទាំងគំរូ និងវិធានការនានាណាមួយដែលបានធ្វើឡើង ដើម្បីដោះស្រាយប្រភេទនៃភាពងាយរងគ្រោះទាំងមូល។ ឧទាហរណ៍ ប្រសិនបើភាគរយច្រើននៃ CVEs របស់ក្រុមហ៊ុនទាក់ទងនឹងការសរសេរលំដាប់នៃការណែនាំឆ្លងគេហទំព័រ (XSS) ការចងក្រងឯកសារការវិភាគមូលហេតុឫសគល់ ការឆ្លើយតប (ដូចជា ការផ្លាស់ប្តូរទៅក្របខ័ណ្ឌគំរូគេហទំព័រដែលរារាំង XSS) ហើយលទ្ធផលនឹងផ្តល់សញ្ញាដល់អតិថិជនថាពួកគេ នឹងមិនត្រូវបានរងគ្រោះដោយប្រភេទនៃភាពងាយរងគ្រោះដោយការបន្ទួរបន្ថយត្រូវបានយល់ដឹងអស់ជាច្រើនទសវត្សរ៍មកហើយនោះទេ។

5. **បោះពុម្ពផ្សព្វផ្សាយបញ្ជីសារពើភ័ណ្ឌមូលដ្ឋានកូដសូហ្វវែរពេញលេញ (Software Bills of Materials -SBOMs)។** ក្រុមហ៊ុនផលិតគួរតែមានបទបញ្ជាអំពីខ្សែសង្វាក់ផ្គត់ផ្គង់របស់ពួកគេ។ ស្ថាប័នគួរតែបង្កើត និងថែរក្សា SBOMs [2] សម្រាប់ផលិតផលនីមួយៗ ស្នើសុំទិន្នន័យពីអ្នកផ្គត់ផ្គង់របស់ពួកគេ និងធ្វើឱ្យ SBOMs មានសម្រាប់អតិថិជន និងអ្នកប្រើប្រាស់ចុងក្រោយ។ ការនេះនឹងជួយបង្ហាញពីភាពឧស្សាហ៍ព្យាយាមរបស់ពួកគេក្នុងការយល់ដឹងអំពីសមាសធាតុដែលពួកគេប្រើប្រាស់ក្នុងការបង្កើតផលិតផលរបស់ពួកគេ សមត្ថភាពរបស់ពួកគេក្នុងការឆ្លើយតបទៅនឹងហានិភ័យដែលបានកំណត់អត្តសញ្ញាណថ្មី និងអាចជួយអតិថិជនឱ្យយល់ដឹងពីរបៀបឆ្លើយតបប្រសិនបើម៉ូឌុលមួយក្នុងចំណោមម៉ូឌុលនៅក្នុងខ្សែសង្វាក់ផ្គត់ផ្គង់មានភាពងាយរងគ្រោះដែលបានរកឃើញថ្មី។

សម្រាប់ជាឯកសារយោង ក្រសួងសេដ្ឋកិច្ច ពាណិជ្ជកម្ម និងឧស្សាហកម្មរបស់ប្រទេសជប៉ុន (METI) បានបោះពុម្ព ផ្សព្វផ្សាយ "សៀវភៅណែនាំអំពីការប្រើបញ្ជីសារពើភ័ណ្ឌមូលដ្ឋានកូដសូហ្វវែរពេញលេញ (SBOM) សម្រាប់ ការគ្រប់គ្រងសូហ្វវែរ។" តម្លាភាពគួរតែពង្រីកដល់ហ្វឺមវែរ (firmware) បង្កប់នៅក្នុងឧបករណ៍ និងទិន្នន័យ ហើយនិងម៉ូដែលដែលប្រើក្នុង AI/machine learning (ML)។ លើសពីការជួយក្នុងការសម្រេចចិត្តទិញ និងសមត្ថភាពប្រតិបត្តិការ SBOMs ដើរតួនាទីយ៉ាងសំខាន់ក្នុងហេដ្ឋារចនាសម្ព័ន្ធដើម្បីស្វែងរក និងឆ្លើយតបទៅ នឹងការវាយប្រហារទៅលើខ្សែសង្វាក់ផ្គត់ផ្គង់ដោយទុច្ចរិត។

6. **បោះពុម្ពផ្សព្វផ្សាយគោលនយោបាយស្តីពីការលាតត្រដាងភាពងាយរងគ្រោះ។** បោះពុម្ពផ្សព្វផ្សាយ គោលនយោបាយស្តីពីការលាតត្រដាងភាពងាយរងគ្រោះដែល (1) អនុញ្ញាតការធ្វើតេស្តទល់នឹងនឹងផលិតផលទាំងអស់ ដែលផ្តល់ដោយក្រុមហ៊ុនផលិត និងលក្ខខណ្ឌសម្រាប់ការធ្វើតេស្តទាំងនោះ (2) ផ្តល់នូវទីជម្រកសុវត្ថិភាពស្របច្បាប់ សម្រាប់សកម្មភាពដែលត្រូវបានអនុវត្តស្របតាមគោលនយោបាយ និង (3) អនុញ្ញាតឱ្យលាតត្រដាងជាសាធារណៈ អំពីភាពងាយរងគ្រោះបន្ទាប់ពីពេលវេលាបានកំណត់។ ក្រុមហ៊ុនផលិតគួរតែធ្វើការវិភាគឫសគល់នៃភាពងាយរងគ្រោះ ដែលបានរកឃើញ ហើយក្នុងកម្រិតធំបំផុតដែលអាចធ្វើទៅបាន ចាត់វិធានការដើម្បីលុបបំបាត់ថ្នាក់ភាពងាយរងគ្រោះ ទាំងមូល។ សូមមើល គំរូគោលនយោបាយស្តីពីការលាតត្រដាងភាពងាយរងគ្រោះ របស់ CISA សម្រាប់ភាសាយោង។

ការអនុវត្តអាជីវកម្មគាំទ្រសន្តិសុខ

1. **ប្រាប់ឈ្មោះអ្នកឧបត្ថម្ភនាយកប្រតិបត្តិជាន់ខ្ពស់ផ្នែកសន្តិសុខតាមការរចនាជាសាធារណៈ។** នៅក្នុងស្ថាប័នជាច្រើន សុវត្ថិភាព (ដូចគុណភាពដែរ) ត្រូវបានផ្ទេរទៅឱ្យក្រុមបច្ចេកទេសដែលមានសមត្ថភាពមានកម្រិត ដើម្បីធ្វើការផ្លាស់ប្តូររចនាសម្ព័ន្ធដើម្បីកែលម្អសន្តិសុខផលិតផលឱ្យប្រសើរច្រើន។ ការតែងតាំងឈ្មោះនាយកប្រតិបត្តិអាជីវកម្មកំពូលជាសាធារណៈ ដើម្បីត្រួតពិនិត្យសន្តិសុខតាមការរចនា នឹងផ្លាស់ប្តូរសន្តិសុខផលិតផលទៅជាកង្វល់ អាជីវកម្មកម្រិតកំពូល។

2. **បោះពុម្ពផ្សព្វផ្សាយផែនទីបង្ហាញផ្លូវសន្តិសុខតាមការរចនា។** ក្រុមហ៊ុនផលិតគួរតែចងក្រងជាឯកសារនូវការផ្លាស់ប្តូរនានាដែលបានធ្វើឡើងចំពោះ SDLC របស់ពួកគេ ដើម្បីបង្កើនសន្តិសុខអតិថិជន រួមទាំងព័ត៌មានលម្អិតអំពីរបាយការណ៍ធ្វើតេស្តផ្ទាល់នៅនឹងកន្លែងសកម្មភាពដែលបានធ្វើឡើងដើម្បីលុបបំបាត់ភាពប្រភេទនៃងាយរងគ្រោះទាំងមូល និងធាតុផ្សេងទៀតដែលបានរាយក្នុងគោលការណ៍ផ្សេងទៀត។ ដូចនៅក្នុងករណីនៃកិច្ចខិតខំប្រឹងប្រែងកែលម្អគុណភាព កម្មវិធីកែលម្អសុវត្ថិភាពមានដំណាក់កាលផ្សេងគ្នា គឺការធ្វើផែនការ ការគ្រប់គ្រង និងការកែលម្អ។ នៅក្នុងស្មារតីនៃការបង្ហាញជាជាងការប្រាប់ ការបោះពុម្ពផ្សព្វផ្សាយផែនទីបង្ហាញផ្លូវ និងព័ត៌មានលម្អិតនៅពីក្រោយដំណាក់កាលទាំងនេះ នឹងបង្កើតទំនុកចិត្តថាផលិតផលមានសន្តិសុខតាមការរចនា។ បន្ទាប់ពីសម្រេចបាននូវវឌ្ឍនភាពដ៏មានអត្ថន័យ ក្រុមហ៊ុនផលិតអាចរៀបរាប់ជាលម្អិតអំពីផលិតផលនៅក្នុងរបាយការណ៍តម្លាភាព។ ការធ្វើដូច្នេះមិនត្រឹមតែបង្ហាញពីការប្តេជ្ញាចិត្តចំពោះគោលការណ៍សន្តិសុខតាមការរចនាប៉ុណ្ណោះទេ ប៉ុន្តែអាចជំរុញចិត្តអ្នកផ្សេងទៀតឱ្យទទួលយកកម្មវិធីស្រដៀងគ្នាដោយបង្ហាញភស្តុតាងនៃអត្ថិភាព។

3. **បោះពុម្ពផ្សព្វផ្សាយផែនទីបង្ហាញផ្លូវសុវត្ថិភាពអង្គចងចាំ។** ក្រុមហ៊ុនផលិតអាចចាត់វិធានការដើម្បីលុបបំបាត់ប្រភេទមួយនៃប្រភេទធំនានានៃភាពងាយរងគ្រោះ ដោយផ្ទេរផលិតផលដែលមានស្រាប់ និងបង្កើតផលិតផលថ្មីៗ ដោយប្រើភាសាសុវត្ថិភាពអង្គចងចាំ។ ខណៈពេលដែលវាមិនអាចទៅរួចក្នុងគ្រប់ករណីទាំងអស់ ក្រុមហ៊ុនផលិតអាចពិចារណាបង្កើតស្រទាប់កម្មវិធីក្នុងភាសាសុវត្ថិភាពអង្គចងចាំ ជាជាងការសរសេរកម្មវិធីទាំងមូលឡើងវិញ។ នេះក៏អាចរួមបញ្ចូលពីរបៀបដែលក្រុមហ៊ុនផលិតកំពុងធ្វើបច្ចុប្បន្នភាពការជួលការបណ្តុះបណ្តាល ការត្រួតពិនិត្យកូដឡើងវិញ និងដំណើរការផ្ទៃក្នុងផ្សេងទៀត ក៏ដូចជាវិធីដែលពួកគេកំពុងជួយសហគមន៍ប្រភពបើកចំហឱ្យធ្វើដូចគ្នាដែរ។

4. **បោះពុម្ពផ្សព្វផ្សាយលទ្ធផល។** ខណៈពេលកំពុងអាប់ដេត SDLC របស់ពួកគេដើម្បីបញ្ចូលទស្សនសន្តិសុខតាមការរចនា ស្ថាប័ននឹងស្វែងរកការឈ្នះរហ័ស ការឈ្នះកាន់តែច្រើនលើការប្រើធនធានច្រើន និងការធ្លាក់ចុះដែលមិនរំពឹងទុកមួយចំនួន។ តាមរយៈការបង្ហាញពីភាពជោគជ័យផ្ទៃក្នុងនិងឧបសគ្គរបស់ពួកគេ ឧស្សាហកម្មទាំងមូលអាចរៀនសូត្រពីលទ្ធផលនានាបាន។

គោលការណ៍ 3៖ នាំមុខចាប់ពីថ្នាក់កំពូល

ការពន្យល់

ខណៈពេលដែលទស្សនទាំងមូលត្រូវបានគេហៅថា "សន្តិសុខតាមការរចនា" លាភការសម្រាប់សុវត្ថិភាពអតិថិជនចាប់ផ្តើមមុនពេលដំណាក់កាលរចនាផលិតផល។ ការលើកទឹកចិត្តចាប់ផ្តើមជាមួយនឹងគោលដៅអាជីវកម្ម និងគោលបំណងបង្កប់ និងច្បាស់លាស់ ហើយនិងលទ្ធផលដែលចង់បាន។ លុះត្រាតែមេដឹកនាំជាន់ខ្ពស់ធ្វើឱ្យសន្តិសុខជាអាទិភាពអាជីវកម្ម ការបង្កើតលាភការផ្ទៃក្នុង និងការជំរុញវប្បធម៌ទូទាំងស្ថាប័ន ដើម្បីធ្វើឱ្យសន្តិសុខជាតម្រូវការនៃការរចនាពួកគេនឹងសម្រេចបានលទ្ធផលល្អបំផុត។

ខណៈពេលដែលជំនាញផ្នែកបច្ចេកទេសមានសារៈសំខាន់ចំពោះសន្តិសុខ ផលិតផលវាមិនមែនជារឿងដែលអាចទុកសម្រាប់បុគ្គលិកបច្ចេកទេសតែម្នាក់ឯងនោះទេ។ វាជាអាទិភាពអាជីវកម្មដែលត្រូវតែចាប់ផ្តើមពីថ្នាក់កំពូល។

មនុស្សមួយចំនួនមានចម្ងល់ថាតើក្រុមហ៊ុនផលិតសូហ្វវែរកំពុងប្រកាន់យកគោលការណ៍ពីរដំបូង និងផលិតអនុផលដែលមានអត្ថន័យ ហើយថាតើគោលការណ៍ទីបីគឺចាំបាច់ឬ? របៀបដែលក្រុមហ៊ុនបង្កើតចក្ខុវិស័យ បេសកកម្ម គុណតម្លៃ និងវប្បធម៌របស់ខ្លួន នឹងប៉ះពាល់ដល់ផលិតផល ហើយធាតុទាំងនោះមានធាតុផ្សំធ្ងន់មួយស្ថិតនៅផ្នែកខាងលើ។ យើងឃើញរឿងនេះនៅក្នុងឧស្សាហកម្មផ្សេងទៀតដែលបានធ្វើឱ្យប្រសើរឡើងយ៉ាងខ្លាំងនៅក្នុងសុវត្ថិភាព និងគុណភាព។ អ្នកជំនាញគុណភាពដ៏ល្បីឈ្មោះ J.M. Juran បានសរសេរថា៖

> ***ការសម្រេចបាននូវភាពជាអ្នកដឹកនាំប្រកបដោយគុណភាព ទាមទារឱ្យអ្នកគ្រប់គ្រងថ្នាក់លើផ្ទាល់ ទទួលបន្ទុកការគ្រប់គ្រងសម្រាប់ធានាគុណភាព។ នៅក្នុងក្រុមហ៊ុននានាដែលទទួលបាននូវភាពជាអ្នកដឹកនាំប្រកបដោយគុណភាព អ្នកគ្រប់គ្រងថ្នាក់លើផ្ទាល់បានដឹកនាំគំនិតផ្តួចផ្តើមនេះ។ ខ្ញុំមិនដឹងពីករណីលើកលែងណាមួយនោះទេ។ [3]***

យើងជឿថាសុវត្ថិភាពគឺជាប្រភេទរងនៃគុណភាពផលិតផល។ នៅពេលដែលសន្តិសុខ និងគុណភាពក្លាយជាកត្តាចាំបាច់សម្រាប់អាជីវកម្ម ជាជាងមុខងារបច្ចេកទេសដែលទុកសម្រាប់តែបុគ្គលិកបច្ចេកទេស ស្ថាប័ននឹងអាចឆ្លើយតបទៅនឹងតម្រូវការសន្តិសុខរបស់អតិថិជនរបស់ពួកគេកាន់តែលឿន និងមានប្រសិទ្ធភាព។ ជាងនេះទៅទៀត ការធ្វើវិនិយោគធនធានចាំបាច់ដើម្បីធានាថា សន្តិសុខសូហ្វវែរគឺជាអាទិភាពរបស់អាជីវកម្មស្នូលចាប់តាំងពីដំបូង នឹងកាត់បន្ថយការចំណាយរយៈពេលវែងក្នុងការដោះស្រាយកង្វះខាតរបស់សូហ្វវែរ ហើយជាលទ្ធផលកាត់បន្ថយហានិភ័យសន្តិសុខជាតិ។

តាមរបៀបដូចគ្នាដែលក្រុមអ្នកដឹកនាំបានអនុវត្តកម្មវិធីទំនួលខុសត្រូវសង្គមសាជីវកម្ម (CSR) មានការយល់ដឹងកាន់តែច្រើនឡើងថាក្រុមប្រឹក្សាសាជីវកម្ម រួមទាំងក្រុមហ៊ុនផលិតសូហ្វវែរ គួរតែដើរតួយ៉ាងសកម្មបន្ថែមទៀតក្នុងការណែនាំកម្មវិធីសន្តិសុខអ៊ីនធឺណិត។ ពាក្យទំនួលខុសត្រូវតាមអ៊ីនធឺណិតរបស់សាជីវកម្ម (CCR) ជួនកាលត្រូវបានប្រើដើម្បីពិពណ៌នាអំពីគំនិតដែលកំពុងលេចចេញនេះ។

ការបង្ហាញពីគោលការណ៍នេះ

ដើម្បីបង្ហាញពីគោលការណ៍នេះ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរចាត់វិធានការនានា រួមមានដូចខាងក្រោម៖

1. **ដាក់បញ្ចូលព័ត៌មានលម្អិតនៃកម្មវិធីសន្តិសុខតាមការរចនា នៅក្នុងរបាយការណ៍ហិរញ្ញវត្ថុសាជីវកម្ម។** ប្រសិនបើក្រុមហ៊ុនផលិតគឺជាក្រុមហ៊ុនដែលធ្វើការជួញដូរជាសាធារណៈ ដាក់បន្ថែមផ្នែកមួយនៅក្នុងរបាយការណ៍ប្រចាំឆ្នាំនីមួយៗ ដែលបរិយាយអំពីកិច្ចខិតខំប្រឹងប្រែងសន្តិសុខតាមការរចនា។ វាជារឿងធម្មតាសម្រាប់របាយការណ៍ហិរញ្ញវត្ថុប្រចាំឆ្នាំរបស់ក្រុមហ៊ុនរថយន្តដើម្បីដាក់បញ្ចូលផ្នែកនានាស្តីពីសុវត្ថិភាពរបស់អ្នកបើកបរ និងអ្នកដំណើរ រួមទាំងព័ត៌មានអំពីគណៈកម្មការត្រួតពិនិត្យគុណភាព និងសុវត្ថិភាពដែលបានចែកចាយ និងប្រមូលផ្តុំ។ ការរៀបរាប់លម្អិតអំពីកម្មវិធីសន្តិសុខតាមការរចនានៅក្នុងរបាយការណ៍ហិរញ្ញវត្ថុ នឹងបង្ហាញថាស្ថាប័នកំពុងភ្ជាប់សន្តិសុខអតិថិជន និងលទ្ធផលហិរញ្ញវត្ថុសាជីវកម្ម ហើយមិនមែនគ្រាន់តែប្រើពាក្យនៅក្នុងសម្ភារៈទីផ្សារទេ ព្រោះវាមានភាពទាន់សម័យនោះទេ។

2. **ផ្តល់របាយការណ៍ទៀងទាត់ដល់ក្រុមប្រឹក្សាភិបាលរបស់អ្នក។** ប្រធានមន្ត្រីសន្តិសុខព័ត៌មាន (CISO) រាយការណ៍ទៅក្រុមប្រឹក្សាសាជីវកម្ម ជាធម្មតារួមមានព័ត៌មានអំពីកម្មវិធីសន្តិសុខបច្ចុប្បន្ន និងដែលបានគ្រោងទុក ការគំរាមកំហែង ឧប្បត្តិហេតុសន្តិសុខដែលសង្ស័យ និងបានបញ្ជាក់ និងការអាប់ដេតផ្សេងទៀតដែលផ្តោតលើគោលជំហរសន្តិសុខ និងសុខភាពរបស់ក្រុមហ៊ុន។ បន្ថែមពីលើការទទួលបានព័ត៌មានអំពីគោលជំហរសន្តិសុខរបស់សហគ្រាស ក្រុមប្រឹក្សាគួរតែស្នើសុំព័ត៌មានអំពីសន្តិសុខផលិតផល និងផលប៉ះពាល់ដែលវាមានលើសន្តិសុខអតិថិជន។ ក្រុមប្រឹក្សាភិបាលមិនគួរសម្លឹងមើលតែ CISO នោះទេ ប៉ុន្តែជាចម្បងចំពោះសមាជិកផ្សេងទៀតនៃអ្នកគ្រប់គ្រងក្រុមហ៊ុន ដើម្បីកាត់បន្ថយនិភ័យរបស់អតិថិជនឱ្យទាប។

3. **ផ្តល់អំណាចដល់នាយកប្រតិបត្តិសន្តិសុខតាមការរចនា។** មានភាពខុសប្លែកគ្នាខ្លាំងរវាងស្ថាប័នដែលក្រុមបច្ចេកទេសមាន "ការទទួលយល់ព្រមដោយនាយកប្រតិបត្តិ" និងស្ថាប័នដែលអ្នកដឹកនាំអាជីវកម្មគ្រប់គ្រងដំណើរការកែលម្អសន្តិសុខអតិថិជនដោយខ្លួនឯង ដោយប្រើដំណើរការអាជីវកម្មស្តង់ដារនានា។ ពាក្យ "ការទទួលយល់ព្រមដោយនាយកប្រតិបត្តិ" មានន័យថា នរណាម្នាក់ត្រូវលក់គំនិតនៃកម្មវិធីសន្តិសុខអតិថិជន ជាជាងវាជាគោលដៅអាជីវកម្មកម្រិតកំពូល។ នាយកប្រតិបត្តិនេះត្រូវតែមានសិទ្ធិអំណាចដើម្បីមានឥទ្ធិពលលើការវិនិយោគផលិតផល ដើម្បីសម្រេចបាននូវលទ្ធផលសន្តិសុខអតិថិជន។

4. **បង្កើតលាភការផ្ទៃក្នុងប្រកបដោយអត្ថន័យ។** ខណៈពេលដែលត្រូវចងចាំមិនបង្កើតលាភការដ៏ច្របូកច្របល់ តម្រឹមប្រព័ន្ធផ្តល់រង្វាន់ដើម្បីបង្កើនសន្តិសុខអតិថិជន ដើម្បីផ្គូផ្គងនឹងអាកប្បកិរិយា និងលទ្ធផលដ៏មានតម្លៃផ្សេងទៀត។ ចាប់ពីនាយកប្រតិបត្តិសន្តិសុខតាមការរចនា រហូតដល់ការគ្រប់គ្រងផលិតផល ការអភិវឌ្ឍសូហ្វវែរ ការគាំទ្រ ការលក់ ច្បាប់ និងស្ថាប័នផ្សេងទៀត ដាក់បញ្ចូលលាភការសន្តិសុខអតិថិជនទៅក្នុងការជួល ការដំឡើងឋានៈ បៀវត្សរ៍ ប្រាក់បន្ថែមលើកទឹកចិត្ត ជម្រើសភាគហ៊ុន និងដំណើរការទូទៅផ្សេងទៀតក្នុងការដំណើរការអាជីវកម្ម។ ឧទាហរណ៍ នៅពេលបង្កើតលក្ខណៈវិនិច្ឆ័យសម្រាប់ការដំឡើងឋានៈអ្នកអភិវឌ្ឍន៍សូហ្វវែរ ដាក់បញ្ចូលការពិចារណាសម្រាប់ការកែលម្អសន្តិសុខផលិតផល រួមជាមួយនឹងលក្ខណៈវិនិច្ឆ័យផ្សេងទៀតដូចជាពេលវេលាដំណើរការ ការបំពេញការងារ និងការកែលម្អលក្ខណៈពិសេស។

5. **បង្កើតក្រុមប្រឹក្សាសន្តិសុខតាមការរចនា។** នៅក្នុងឧស្សាហកម្មមួយចំនួន វាជារឿងធម្មតាសម្រាប់ស្ថាប័ននានាក្នុង ការបង្កើតក្រុមប្រឹក្សាត្រួតពិនិត្យគុណភាពកណ្តាល និងដាក់បញ្ចូលតំណាងត្រួតពិនិត្យគុណភាពនៅក្នុងសាខាសំខាន់ៗ ឬអង្គភាពអាជីវកម្ម។ ដោយការរួមបញ្ចូលទាំងសមាជិកមជ្ឈិម និងចែកចាយ ក្រុមទាំងនេះធ្វើការដើម្បីបង្កើនគុណភាពទល់នឹងគោលដៅកម្រិតកំពូល ខណៈពេលដែលទទួលបានការបញ្ជូនទិន្នន័យវាស់វែងពីចម្ងាយ (telemetry) ពីជម្រៅនៅក្នុងស្ថាប័ន។ ដូចគ្នាដែរ ក្រុមប្រឹក្សាសន្តិសុខតាមការរចនា នឹងកែលម្អសន្តិសុខទល់នឹងគោលដៅសន្តិសុខតាមការរចនាទូទាំងស្ថាប័ន។

6. **បង្កើត និងវិវត្តក្រុមប្រឹក្សាអតិថិជន។** ក្រុមហ៊ុនផលិតសូហ្វវែរជាច្រើនមានក្រុមប្រឹក្សាអតិថិជន ដែលរួមមានអតិថិជនមកពីតំបន់ឧស្សាហកម្ម និងទំហំផ្សេងៗគ្នា។ ក្រុមប្រឹក្សាទាំងនេះអាចផ្តល់ព័ត៌មានជាច្រើនអំពីភាពជោគជ័យ និងបញ្ហាប្រឈមរបស់អតិថិជន ក្នុងការប្រើប្រាស់ផលិតផលរបស់ក្រុមហ៊ុន។ រៀបចំរចនាសម្ព័ន្ធរបៀបវារៈរបស់ក្រុមប្រឹក្សា ដោយមានប្រធានបទជាក់លាក់ដែលដោះស្រាយអំពីសន្តិសុខអតិថិជន ទោះបីជាវាមិនមែនជាគំនិតសំខាន់សម្រាប់អ្នកចូលរួមក៏ដោយ។ ពិចារណាកន្លែងដែលក្រុមប្រឹក្សាអតិថិជនរាយការណ៍ និងរបៀបទាញយកផលប្រយោជន៍ពីអ្នកចូលរួមសម្រាប់ការយល់ដឹងអំពីសន្តិសុខផលិតផលដូចដែលបានដាក់ឱ្យប្រើប្រាស់។ ជាឧទាហរណ៍ តើក្រុមប្រឹក្សាមានការលំអៀងទៅរកគោលបំណងទីផ្សារ និងការលក់ ឬការគ្រប់គ្រងផលិតផលទេ? នាយកប្រតិបត្តិសន្តិសុខតាមការរចនា គួរតែជួយគ្រប់គ្រងអន្តរកម្មរបស់អតិថិជនទាំងនេះ ហើយគួរតែភ្ជាប់អន្តរកម្មទាំងនេះជាមួយធាតុផ្សេងទៀតនៅក្នុងឯកសារនេះ ដូចជាការសិក្សាផ្ទាល់នៅនឹងកន្លែង។

យុទ្ធវិធីសន្តិសុខតាមការរចនា

ក្របខ័ណ្ឌអភិវឌ្ឍន៍សូហ្វវែរដែលមានសន្តិសុខ (SSDF) ដែលត្រូវបានគេស្គាល់ ដែរថាជាវិទ្យាស្ថានជាតិស្តង់ដារ និងបច្ចេកវិទ្យាជាតិ (NIST's) SP 800-218 គឺជាសំណុំស្នូលនៃការអនុវត្តការអភិវឌ្ឍសូហ្វវែរដែលមានសន្តិសុខកម្រិតខ្ពស់ ដែលអាចត្រូវបានដាក់បញ្ចូលទៅក្នុងដំណាក់កាលនីមួយៗនៃវដ្តជីវិតនៃការអភិវឌ្ឍសូហ្វវែរ (SDLC)។ ការធ្វើតាមតាមការអនុវត្តទាំងនេះ អាចជួយឱ្យក្រុមហ៊ុនផលិតសូហ្វវែរកាន់តែមានប្រសិទ្ធភាពក្នុងការស្វែងរក និងលុបបំបាត់ភាពងាយរងគ្រោះនៅក្នុងសូហ្វវែរដែលបានចេញផ្សាយ កាត់បន្ថយផលប៉ះពាល់ដែលអាចកើតមាននៃការកេងប្រវ័ញ្ចលើភាពងាយរងគ្រោះ និងដោះស្រាយបញ្ហាឫសគល់នៃភាពងាយរងគ្រោះដើម្បីការពារការកើតឡើងម្តងទៀតនាពេលអនាគត។

ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ លើកទឹកចិត្តឱ្យប្រើយុទ្ធវិធីសន្តិសុខតាមការរចនា រួមទាំងគោលការណ៍នានាដែលយោងលើការអនុវត្ត SSDF។ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែបង្កើតផែនទីបង្ហាញផ្លូវជាលាយលក្ខណ៍អក្សរមួយ ដើម្បីទទួលយកការអនុវត្តការអភិវឌ្ឍសូហ្វវែរសន្តិសុខតាមការរចនាបន្ថែមទៀតនៅទូទាំងស្ថាប័នរបស់ពួកគេ។ ខាងក្រោមនេះ គឺជាការអនុវត្តល្អបំផុតនៃផែនទីបង្ហាញផ្លូវដែលមិនមែនជាបញ្ជីពេញលេញមួយ៖

- **ភាសាសរសេរកម្មវិធីសុវត្ថិភាពអង្គចងចាំ (SSDF PW.6.1)។** ផ្តល់អាទិភាពដល់ការប្រើប្រាស់ភាសាសុវត្ថិភាពអង្គចងចាំកន្លែងណាដែលអាចធ្វើទៅបាន។ ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យទទួលស្គាល់ថាការបន្ទូរបន្ទាប ជាក់លាក់នៃអង្គចងចាំ អាចជាយុទ្ធវិធីរយៈពេលខ្លីដ៏មានប្រយោជន៍ សម្រាប់មូលដ្ឋានកូដកេរ្តិ៍ដំណែល។ ឧទាហរណ៍នានារួមមានការកែលម្អភាសា C/C++ ការបន្ទូរបន្ទាបផ្នែករឹង ដោះស្រាយចៃដន្យនីយកម្មប្លង់ចន្លោះទីតាំងអង្គចងចាំ (ASLR), សុចរិតភាពនៃការគ្រប់គ្រងលំហូរ (CFI) និងការចាក់បញ្ចូលទិន្នន័យមិនត្រឹមត្រូវ។ ទោះជាយ៉ាងណាក៏ដោយ មានការយល់ស្របកាន់តែច្រើនឡើងដែលថា ការទទួលយកភាសាសរសេរកម្មវិធីដែលមានសុវត្ថិភាពនៃអង្គចងចាំ អាចលុបបំបាត់ប្រភេទនៃកង្វះខាតនេះ ហើយក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែស្វែងរកវិធីនានាដើម្បីទទួលយកភាសាសរសេរកម្មវិធីដែលមានសុវត្ថិភាពនៃអង្គចងចាំ ។ ឧទាហរណ៍មួយចំនួននៃភាសាសុវត្ថិភាពនៃអង្គចងចាំទំនើបរួមមាន C#, Rust, Ruby, Java, Go និង Swift។ សូមអានសន្លឹកព័ត៌មានស្តីពីសុវត្ថិភាពនៃអង្គចងចាំរបស់ NSA សន្លឹកព័ត៌មាន សម្រាប់ព័ត៌មានបន្ថែម។

- **មូលដ្ឋានផ្នែករឹងកុំព្យូទ័រដែលមានសន្តិសុខ។** ដាក់បញ្ចូលនូវលក្ខណៈពិសេសៗផ្នែកស្ថាបត្យកម្ម ដែលអនុញ្ញាតឱ្យមានការការពារអង្គចងចាំល្អិតល្អន់ ដូចដែលបានពិពណ៌នាដោយការណែនាំអំពី RISC ដែលបង្កើនសមត្ថភាពផ្នែករឹង (CHERI) ដែលអាចពង្រីកការណែនាំ-កំណត់ស្ថាបត្យកម្មតាមប្រពៃណី (ISAs) ក៏ដូចជាលក្ខណៈពិសេសផ្សេងទៀតដូចជាម៉ូឌុលវេទិកាដែលអាចទុកចិត្តបាន និងម៉ូឌុលសុវត្ថិភាពផ្នែករឹង។ សម្រាប់ព័ត៌មានបន្ថែម សូមចូលទៅកាន់ គេហទំព័រ CHERI របស់សាកលវិទ្យាល័យ Cambridge។

- **សមាសធាតុសូហ្វវែរដែលមានសន្តិសុខ (SSDF PW 4.1)។** ទទួលបាន និងថែរក្សាសមាសភាគសូហ្វវែរដែលមានសន្តិសុខល្អ (ឧទាហរណ៍ បណ្ណាល័យសូហ្វវែរ ម៉ូឌុល សូហ្វវែរភ្ជាប់គម្លាតរវាងកម្មវិធី និងប្រព័ន្ធប្រតិបត្តិការក្របខ័ណ្ឌ) ពីពាណិជ្ជកម្មដែលបានផ្ទៀងផ្ទាត់ ប្រភពបើកចំហ និងអ្នកអភិវឌ្ឍន៍ភាគីទីបីផ្សេងទៀត ដើម្បីធានាបាននូវសន្តិសុខដ៏រឹងមាំនៅក្នុងផលិតផលសូហ្វវែរសម្រាប់អ្នកប្រើប្រាស់។

- **ក្របខ័ណ្ឌគំរូគេហទំព័រ (SSDF PW.5.1)។** ប្រើក្របខ័ណ្ឌគំរូគេហទំព័រដែលអនុវត្តការគេចចេញដោយស្វ័យប្រវត្តិនៃការបញ្ចូលទិន្នន័យអ្នកប្រើប្រាស់ ដើម្បីជៀសវាងការវាយប្រហារតាមគេហទំព័រ ដូចជាការសរសេរស្ត្រីបឆ្លងគេហទំព័រជាដើម។

- **បញ្ចេកទេសកំណត់សំណួរតួលេខ (SSDF PW 5.1)។** ប្រើបញ្ចេកទេសកំណត់សំណួរតួលេខ ជាជាងដាក់បញ្ចូលទិន្នន័យអ្នកប្រើប្រាស់នៅក្នុងសំណួរតួលេខ ដើម្បីជៀសវាងការវាយប្រហារតាមរយៈការចាក់បញ្ចូល SQL។

- **ការធ្វើតេស្តសន្តិសុខកម្មវិធីរកមើលកំហុស និងគោលជំហរមុខងារប្រព័ន្ធសូហ្វវែរ (SAST/DAST)** (SSDF PW.7.2, PW.8.2)។ ប្រើឧបករណ៍ទាំងនេះដើម្បីវិភាគកូដប្រភពផលិតផល និងគោលជំហរកម្មវិធី ដើម្បីរកមើលការអនុវត្តដែលងាយមានកំហុស។ ឧបករណ៍ទាំងនេះគ្របដណ្តប់បញ្ហានានាចាប់ពីការគ្រប់គ្រងមិនត្រឹមត្រូវនៃអង្គចងចាំ រហូតដល់ការបង្កើតសំណួរមូលដ្ឋានទិន្នន័យដែលងាយមានកំហុស (ឧទាហរណ៍ ការបញ្ចូលទិន្នន័យអ្នកប្រើប្រាស់ដែលមិនបានគេចផុត ដែលនាំឱ្យមានការចាក់បញ្ចូល SQL)។ ឧបករណ៍ SAST និង DAST អាចត្រូវបានដាក់បញ្ចូលទៅក្នុងដំណើរការអភិវឌ្ឍ ហើយដំណើរការដោយស្វ័យប្រវត្តិជាផ្នែកនៃការអភិវឌ្ឍសូហ្វវែរ។ SAST និង DAST គួរតែបំពេញបន្ថែមប្រភេទផ្សេងទៀតនៃការធ្វើតេស្ត ដូចជាការធ្វើតេស្តសមាសភាគ និងការធ្វើតេស្តរួមបញ្ចូលគ្នាដើម្បីធានាថា ផលិតផលអនុលោមតាមតម្រូវការសន្តិសុខដែលរំពឹងទុក។ នៅពេលរកឃើញបញ្ហានានា ក្រុមហ៊ុនផលិតគួរតែធ្វើការវិភាគប្រភពដើមហេតុដើម្បីដោះស្រាយចំណុចខ្សោយជាប្រព័ន្ធ។

- **ការពិនិត្យកូដ** (SSDF PW.7.1, PW.7.2)។ ខិតខំដើម្បីធានាថាលេខកូដដែលបានដាក់បញ្ចូលទៅក្នុងផលិតផលត្រូវឆ្លងកាត់បច្ចេកទេសត្រួតពិនិត្យគុណភាព ដូចជាការពិនិត្យដោយអ្នកអភិវឌ្ឍន៍ផ្សេងទៀត ឬ "ការបណ្តុះកំហុស"។
- **បញ្ជីសារពើភ័ណ្ឌនៃសមាសភាគទាំងអស់នៅក្នុងកម្មវិធីសូហ្វវែរ (SBOM)** (SSDF PS.3.2, PW.4.1)។ ដាក់បញ្ចូលការបង្កើតនៃ SBOM[4] ដើម្បីផ្តល់ភាពមើលឃើញទៅក្នុងសំណុំសូហ្វវែរដែលដាក់ចូលទៅក្នុងផលិតផល។
- **កម្មវិធីលាតត្រដាងភាពងាយរងគ្រោះ** (SSDF RV.1.3)។ បង្កើតកម្មវិធីលាតត្រដាងភាពងាយរងគ្រោះ ដែលអនុញ្ញាតឱ្យអ្នកស្រាវជ្រាវផ្នែកសន្តិសុខរាយការណ៍ពីភាពងាយរងគ្រោះ ហើយទទួលបានជម្រកសុវត្ថិភាពស្របច្បាប់ក្នុងការធ្វើដូច្នេះ។ ជាផ្នែកនៃការនេះ អ្នកផ្គត់ផ្គង់គួរតែបង្កើតដំណើរការនានា ដើម្បីកំណត់ប្រភពដើមហេតុនៃភាពងាយរងគ្រោះដែលបានរកឃើញ។ ដំណើរការបែបនេះគួរតែរួមបញ្ចូល ការកំណត់ថាតើការទទួលយកការអនុវត្តសន្តិសុខតាមការរចនាណាមួយនៅក្នុងឯកសារនេះ (ឬការអនុវត្តស្រដៀងគ្នាផ្សេងទៀត) នឹងរារាំងដល់ការបង្កភាពងាយរងគ្រោះដែរឬទេ។
- **ភាពពេញលេញនៃ CVE។** ត្រូវប្រាកដថា CVEs ដែលបានបោះពុម្ពផ្សព្វផ្សាយ ដាក់បញ្ចូលការរៀបរាប់ពីប្រភពដើមហេតុឬភាពទន់ខ្សោយទូទៅ (CWE) ដើម្បីជួយដល់ការវិភាគទូទាំងឧស្សាហកម្មនៃកំហុសការរចនាសន្តិសុខសូហ្វវែរ។ ខណៈពេលដែលការធានាថា រាល់ CVE គឺត្រឹមត្រូវ ហើយពេញលេញអាចចំណាយពេលបន្ថែមក្តី វាអនុញ្ញាតឱ្យស្ថាប័នដែលមិនទាក់ទងគ្នាកត់សម្គាល់ឃើញនិន្នាការឧស្សាហកម្មដែលផ្តល់អត្ថប្រយោជន៍ដល់ក្រុមហ៊ុនផលិត និងអតិថិជនទាំងអស់។ សម្រាប់ព័ត៌មានបន្ថែមអំពីការគ្រប់គ្រងភាពងាយរងគ្រោះ សូមមើល ការណែនាំអំពីប្រភេទភាពងាយរងគ្រោះជាក់លាក់របស់ភាគីពាក់ព័ន្ធជាក់លាក់ (SSVC)។ របស់ CISA
- **ការការពារស៊ីជម្រៅ។** រចនាហេដ្ឋារចនាសម្ព័ន្ធ ដើម្បីឱ្យការរងការវាយប្រហារតាមអ៊ីនធឺណិតលើការគ្រប់គ្រងសន្តិសុខតែមួយមិនបណ្តាលឱ្យមានការរងការវាយប្រហារតាមអ៊ីនធឺណិតលើប្រព័ន្ធទាំងមូល។ ជាឧទាហរណ៍ ការធានាថាឯកសិទ្ធិអ្នកប្រើប្រាស់ត្រូវបានផ្តល់ជូនយ៉ាងតូចចង្អៀត ហើយបញ្ជីត្រួតពិនិត្យការចូលប្រើដែលបានអនុវត្ត អាចកាត់បន្ថយផលប៉ះពាល់នៃគណនីដែលត្រូវបានរងការវាយប្រហារតាមអ៊ីនធឺណិត។ ដូចគ្នានេះផងដែរ បច្ចេកទេសញែកសូហ្វវែរ អាចដាក់ភាពងាយរងគ្រោះនៅដាច់ដោយឡែក ដើម្បីដាក់ដែនកំណត់ការរងការវាយប្រហារតាមអ៊ីនធឺណិតលើកម្មវិធីទាំងមូល។
- **បំពេញគោលដៅបំពេញការងារសន្តិសុខអ៊ីនធឺណិត (CPGs)។** រចនាផលិតផលដែលបំពេញតាមការអនុវត្តសន្តិសុខជាមូលដ្ឋាន។ គោលដៅបំពេញការងារសន្តិសុខអ៊ីនធឺណិត របស់ CISA គូសបញ្ជាក់អំពីវិធានការសន្តិសុខតាមអ៊ីនធឺណិតនៅខ្សែបន្ទាត់គោលជាមូលដ្ឋានដែលស្ថាប័ននានាគួរតែអនុវត្ត។ លើសពីនេះទៀត សម្រាប់វិធីជាច្រើនទៀតដើម្បីពង្រឹងគោលជំហរស្ថាប័នរបស់អ្នក សូមមើលក្របខ័ណ្ឌការវាយតម្លៃសន្តិសុខអ៊ីនធឺណិតរបស់ចក្រភពអង់គ្លេស ដែលចែករំលែកពីភាពស្រដៀងគ្នានឹង CPGs របស់ CISA។ ប្រសិនបើក្រុមហ៊ុនផលិតបរាជ័យក្នុងការបំពេញតាម CPGs - ដូចជាមិនតម្រូវឱ្យមានការផ្ទៀងផ្ទាត់ពហុកត្តា (MFA) ដែលធន់នឹងការបោកបញ្ឆោតតាមអ៊ីមែលសម្រាប់បុគ្គលិកទាំងអស់ - នោះពួកគេមិនអាចត្រូវបានគេចាត់ទុកថាជាផ្តល់ផលិតផលដែលមានសន្តិសុខតាមការរចនានោះទេ។

ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យទទួលស្គាល់ថា ការផ្លាស់ប្តូរទាំងនេះគឺជាការផ្លាស់ប្តូរដ៏សំខាន់នៅក្នុងគោលជំហររបស់ស្ថាប័ន។ ដូចនេះ ការណែនាំរបស់ពួកគេគួរតែទទួលបានអាទិភាព ដោយផ្អែកលើម៉ូដែលកំណត់ការគំរាមកំហែងតាមត្រូវការ ភាពចាំបាច់ ភាពសុគស្មាញ និងផលប៉ះពាល់អាជីវកម្ម។ ការអនុវត្តទាំងនេះ អាចត្រូវបានណែនាំសម្រាប់សូហ្វវែរថ្មី ហើយពង្រីកជាលំដាប់ដើម្បីគ្របដណ្តប់ករណីប្រើប្រាស់ និងផលិតផលបន្ថែម។ ក្នុងករណីមួយចំនួន ភាពចាំបាច់ និងគោលជំហរហានិភ័យនៃផលិតផលជាក់លាក់មួយ អាចមានភាពល្អសមត្រូវនឹងកាលវិភាគដែលបានពន្លឿន ដើម្បីទទួលយកការអនុវត្តទាំងនេះ។ ក្នុងករណីផ្សេងទៀត ការអនុវត្តនានាអាចត្រូវបានណែនាំទៅក្នុងមូលដ្ឋានកូដកេរ្តិ៍ដំណែល ហើយត្រូវបានកែបំបាត់តាមពេលវេលា។

[4] ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យមួយចំនួន កំពុងស្វែងរកវិធីសាស្ត្រជំនួសនានា ដើម្បីទទួលបានការធានាសន្តិសុខជុំវិញខ្សែសង្វាក់ផ្គត់ផ្គង់សូហ្វវែរ។

យុទ្ធវិធីសន្តិសុខតាមលំនាំដើម

បន្ថែមពីលើការទទួលយកការអនុវត្តអភិវឌ្ឍន៍សន្តិសុខតាមការរចនា ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំក្រុមហ៊ុនផលិតសូហ្វវែរ ឱ្យផ្តល់អាទិភាពលើការកំណត់រចនាសម្ព័ន្ធសន្តិសុខតាមលំនាំដើមនៅក្នុងផលិតផលរបស់ពួកគេ។ ទាំងនេះគួរតែខិតខំធ្វើបច្ចុប្បន្នភាពផលិតផល ដើម្បីអនុលោមតាមការអនុវត្តទាំងនេះ នៅពេលត្រូវបានធ្វើឱ្យទាន់បច្ចុប្បន្នភាពឡើងវិញ។ ឧទាហរណ៍៖

- **លុបបំបាត់ពាក្យសម្ងាត់ដើម។** មិនគួរដាក់ភ្ជាប់ផលិតផលមកជាមួយពាក្យសម្ងាត់ដើម ដែលត្រូវបានចែករំលែកជាសកលនោះទេ។ ដើម្បីលុបបំបាត់ពាក្យសម្ងាត់ដើម ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំផលិតផលតម្រូវឱ្យអ្នកគ្រប់គ្រងកំណត់ពាក្យសម្ងាត់រឹងមាំ ក្នុងអំឡុងពេលដំឡើងកម្មវិធី និងកំណត់រចនាសម្ព័ន្ធ ឬដើម្បីដឹកជញ្ជូនផលិតផលជាមួយពាក្យសម្ងាត់រឹងមាំតែមួយគត់សម្រាប់ឧបករណ៍នីមួយៗ។

- **ការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវពហុកត្តាជាកាតព្វកិច្ច(MFA) សម្រាប់អ្នកប្រើប្រាស់ដែលមានឯកសិទ្ធិ។** យើងសង្កេតឃើញថា ការប្រើប្រាស់របស់សហគ្រាសជាច្រើន ត្រូវបានគ្រប់គ្រងដោយអ្នកគ្រប់គ្រងដែលមិនបានការពារគណនីរបស់ពួកគេដោយប្រើ MFA។ ដោយសារអ្នកគ្រប់គ្រងគឺជាគោលដៅមានតម្លៃខ្ពស់ ផលិតផលគួរតែធ្វើឱ្យ MFA ជាការជ្រើសយកការមិនចូលរួម ជាជាងជ្រើសយកការចូលរួម ។ លើសពីនេះ ប្រព័ន្ធគួរតែរម្លឹកអ្នកគ្រប់គ្រងឱ្យបានទៀងទាត់ដើម្បីចុះឈ្មោះក្នុង MFA រហូតដល់ពួកគេបានបើកដំណើរការវាដោយជោគជ័យនៅលើគណនីរបស់ពួកគេ។ NCSC របស់ហូឡង់ មានការណែនាំដែលស្របទៅនឹងការណែនាំរបស់ CISA សូមមើល សន្លឹកព័ត៌មានការផ្ទៀងផ្ទាត់ពហុកត្តាៈ របស់ពួកគេសម្រាប់ព័ត៌មានបន្ថែម។

- **ការចុះឈ្មោះចូលតែមួយ (SSO)។** កម្មវិធី IT គួរតែអនុវត្តការចុះឈ្មោះចូលតែមួយលើការគាំទ្រ តាមរយៈស្តង់ដារបើកចំហទំនើបនានា។ ឧទាហរណ៍រួមមានភាសាសម្គាល់ការអះអាងសុវត្ថិភាព (SAML) ឬការតភ្ជាប់អត្តសញ្ញាណបើកចំហ (ODC)។ សមត្ថភាពនេះគួរតែធ្វើឱ្យមានមកស្រាប់ដោយមិនគិតថ្លៃបន្ថែម។

- **ការបើកចូលដោយសុវត្ថិភាព។** ផ្តល់កំណត់ហេតុនៃការត្រួតពិនិត្យដែលមានគុណភាពខ្ពស់ ដល់អតិថិជនដោយមិនគិតថ្លៃបន្ថែម ឬការកំណត់រចនាសម្ព័ន្ធបន្ថែម។ កំណត់ហេតុនៃការត្រួតពិនិត្យមានសារៈសំខាន់សម្រាប់ការស៊ើបរក និងរាយការណ៍ពីឧប្បត្តិហេតុសន្តិសុខដែលអាចកើតមាន។ កំណត់ហេតុនៃការត្រួតពិនិត្យទាំងនេះក៏មានសារៈសំខាន់ផងដែរ ក្នុងអំឡុងពេលស៊ើបអង្កេតលើឧប្បត្តិហេតុសន្តិសុខដែលបានសង្ស័យ ឬបញ្ជាក់។ សូមពិចារណាប្រើការអនុវត្តល្អបំផុតនានា ដូចជាការផ្តល់នូវការរួមបញ្ចូលដ៏ងាយស្រួលជាមួយនឹងប្រព័ន្ធគ្រប់គ្រងសន្តិសុខព័ត៌មាន និងព្រឹត្តិការណ៍ ដែលមានអន្តរការីផ្តល់ និងទទួលព័ត៌មានអំពីការសរសេរកម្មវិធី (API) ការចូលប្រើប្រាស់ដែលប្រើពេលវេលាសកលដែលបានសម្របសម្រួល (UTC), ការផ្លាស់ប្តូរទម្រង់នៃពេលវេលាតាមតំបន់ លក្ខណៈស្តង់ដារ និងបច្ចេកទេសគ្រប់គ្រងឯកសារដ៏រឹងមាំ។

- **កម្រងព័ត៌មាននៃការអនុញ្ញាតឱ្យប្រើសូហ្វវែរ។** អ្នកផ្គត់ផ្គង់សូហ្វវែរគួរតែផ្តល់អនុសាសន៍អំពីតួនាទីកម្រងព័ត៌មានដែលមានការអនុញ្ញាត និងករណីប្រើប្រាស់ដែលបានកំណត់របស់ពួកគេ។ ក្រុមហ៊ុនផលិតគួរតែរួមបញ្ចូលការព្រមានដែលអាចមើលឃើញ ដែលជូនដំណឹងដល់អតិថិជនអំពីការកើនឡើងនៃហានិភ័យ ប្រសិនបើពួកគេងាកចេញពីការអនុញ្ញាតនៅក្នុងកម្រងព័ត៌មានដូចបានណែនាំ។ ជាឧទាហរណ៍ គ្រូពេទ្យអាចមើលកំណត់ត្រាអ្នកជំងឺទាំងអស់បាន ប៉ុន្តែអ្នករៀបចំកាលវិភាគវេជ្ជសាស្ត្រអាចចូលប្រើបាស់ដោយមានកម្រិតក្នុងការមើលព័ត៌មានមួយចំនួនដែលត្រូវការសម្រាប់ការរៀបចំពេលវេលាណាត់ជួប។

- **សន្តិសុខដែលគិតទៅថ្ងៃមុខសម្រាប់ភាពស៊ីសង្វាក់គ្នានឹងប្រព័ន្ធចាស់។** ជាញឹកញាប់ណាស់ លក្ខណៈពិសេសៗនៃប្រព័ន្ធចាស់ដែលស៊ីសង្វាក់គ្នានឹងប្រព័ន្ធចាស់ត្រូវបានដាក់បញ្ចូល ហើយជារឿយៗត្រូវបានបើកដំណើរការនៅក្នុងផលិតផល ទោះបីជាបង្កហានិភ័យដល់សន្តិសុខផលិតផលក៏ដោយ។ កំណត់សន្តិសុខជាអាទិភាព ជាងភាពស៊ីសង្វាក់គ្នានឹងប្រព័ន្ធចាស់ ដែលផ្តល់សិទ្ធិអំណាចដល់ក្រុមសន្តិសុខដើម្បីដកចេញនូវលក្ខណៈពិសេសដែលគ្មានសន្តិសុខ បើទោះបីជាវាមានន័យជាការបង្កឱ្យមានការផ្លាស់ប្តូរដែលនាំឱ្យមានការខូចដល់ផ្នែកផ្សេងក៏ដោយ។

- **តាមដាន និងកាត់បន្ថយទំហំ "សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ"។** កាត់បន្ថយទំហំ “សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ” ដែលបានដាក់បញ្ចូលជាមួយផលិតផល ហើយខិតខំដើម្បីធានាថាទំហំនឹងរួមតូចតាមពេលវេលា ដោយសារកំណែថ្មីនៃសូហ្វវែរត្រូវបានចេញផ្សាយ។ រួមបញ្ចូលសមាសធាតុនៃ “សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ” ជាការកំណត់រចនាសម្ព័ន្ធដើមនៃផលិតផល។ ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ទទួលស្គាល់ថា ការធ្វើសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធឱ្យខ្លី កើតចេញពីភាពជាដៃគូបន្ត ជាមួយអតិថិជនដែលមានស្រាប់ ហើយរួមបញ្ចូលការខិតខំប្រឹងប្រែងដោយក្រុមផលិតផលជាច្រើន រួមទាំងបទពិសោធន៍អ្នកប្រើប្រាស់ (UX) ផងដែរ។

- **ពិចារណាលើផលវិបាកបទពិសោធន៍អ្នកប្រើប្រាស់នៃការកំណត់សន្តិសុខ។** ការកំណត់ថ្មីនីមួយៗ បង្កើនបន្ទុកនៃការយល់ដឹងលើអ្នកប្រើប្រាស់ចុងក្រោយ ហើយគួរតែត្រូវបានវាយតម្លៃរួមជាមួយនឹងអត្ថប្រយោជន៍ អាជីវកម្មដែលទទួលបាន។ ជាការប្រសើរបំផុត ការកំណត់មិនគួរឱ្យមានទេ។ ជាជំនួសវិញ ការកំណត់សន្តិសុខបំផុតគួរតែបានដាក់បញ្ចូលទៅក្នុងផលិតផលដើម។ ពេលណាការកំណត់រចនាសម្ព័ន្ធមានភាពចាំបាច់ ជម្រើសដើមគួរតែមានសន្តិសុខយ៉ាងទូលំទូលាយប្រឆាំងនឹងការគំរាមកំហែងទូទៅ។

ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យទទួលស្គាល់ថា ការផ្លាស់ប្តូរទាំងនេះអាចមានផលប៉ះពាល់ផ្នែកប្រតិបត្តិការលើរបៀបដែលសូហ្វវែរត្រូវបានប្រើប្រាស់។ ដូច្នេះហើយ មតិយោបល់របស់អតិថិជនមានសារៈសំខាន់ក្នុងការធ្វើឱ្យមានតុល្យភាពលើការពិចារណាផ្នែកប្រតិបត្តិការ និងសន្តិសុខ។ យើងជឿថាការបង្កើតផែនទីបង្ហាញផ្លូវជាលាយលក្ខណ៍អក្សរ និងការគាំទ្រពីនាយកប្រតិបត្តិ ដែលផ្តល់អាទិភាពដល់គំនិតទាំងនេះទៅក្នុងផលិតផលដ៏សំខាន់បំផុតរបស់ស្ថាប័ន គឺជាជំហានដំបូងដើម្បីផ្លាស់ប្តូរឆ្ពោះទៅរក ការអនុវត្តការអភិវឌ្ឍន៍សូហ្វវែរដែលមានសន្តិសុខ។ ខណៈពេលដែលមតិយោបល់របស់អតិថិជនមានសារៈសំខាន់ យើងបានសង្កេតឃើញករណីសំខាន់ៗដែលអតិថិជនមិនមានបំណង ឬមិនអាចទទួលយកស្តង់ដារដែលបានកែលម្អ ជាញឹកញាប់គឺពិធីការបណ្តាញ។ វាមានសារៈសំខាន់សម្រាប់ក្រុមហ៊ុនផលិត ក្នុងការបង្កើតលាភការដ៏មានអត្ថន័យសម្រាប់អតិថិជនដើម្បីរក្សាបច្ចុប្បន្នភាព ហើយមិនអនុញ្ញាតឱ្យពួកគេនៅតែទទួលភាពងាយរងគ្រោះដោយគ្មានកំណត់នោះទេ។

សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធទល់នឹងការបន្ធូរបន្ថយប្រព័ន្ធ

សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធអាចបណ្តាលមកពីកង្វះនៃការគ្រប់គ្រងសន្តិសុខលិតផល ដែលត្រូវបានបង្កប់ទៅក្នុងស្ថាបត្យកម្មរបស់ផលិតផល ចាប់តាំងពីការចាប់ផ្តើមនៃការអភិវឌ្ឍ។ អាស្រ័យហេតុនេះ សៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធក៏អាចជាផែនទីបង្ហាញផ្លូវសម្រាប់សត្រូវផងដែរក្នុងការចង្អុលបង្ហាញ និងទាញយកប្រយោជន៍ពីលក្ខណៈពិសេសៗដែលគ្មានសន្តិសុខ។ វាជារឿងធម្មតាទេសម្រាប់ស្ថាប័នជាច្រើន ដែលមិនដឹងពីសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ ដូច្នេះពួកគេក៏ទុកចោលការកំណត់រចនាសម្ព័ន្ធឧបករណ៍របស់ពួកគេក្នុងស្ថានភាពមួយដែលគ្មានសន្តិសុខ។ ម៉ូដែលដាក់បញ្ច្រាសដែលគេស្គាល់ថាជាសៀវភៅណែនាំស្តីពីការបន្ធូរបន្ថយប្រព័ន្ធ គួរតែជំនួសសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធបែបនេះ ហើយពន្យល់ថាតើការផ្លាស់ប្តូរណាមួយដែលអ្នកប្រើប្រាស់គួរធ្វើខណៈពេលរាយបញ្ជីហានិភ័យសន្តិសុខដែលមានផងដែរ។ សៀវភៅណែនាំទាំងនេះគួរតែបានសរសេរដោយអ្នកអនុវត្តសន្តិសុខ ដែលអាចពន្យល់អំពីការដោះដូរជាភាសាច្បាស់លាស់ ដើម្បីបង្កើនឱកាសនៃការអនុវត្តឱ្យបានត្រឹមត្រូវ។

ជាជាងបង្កើតសៀវភៅណែនាំស្តីពីការពង្រឹងប្រព័ន្ធដែលរាយបញ្ជីវិធីសាស្ត្រនានាសម្រាប់ការធានាផលិតផល ស្ថាប័នបង្កើតកម្មវិធីនិងមូលដ្ឋានទិន្នន័យណែនាំក្រុមហ៊ុនផលិតសូហ្វវែរ ឱ្យផ្លាស់ប្តូរទៅវិធីសាស្ត្រសន្តិសុខតាមលំនាំដើមហើយផ្តល់នូវ "សៀវភៅណែនាំស្តីពីការបន្ធូរបន្ថយប្រព័ន្ធវិញ"។ សៀវភៅណែនាំទាំងនេះ ពន្យល់ពីហានិភ័យអាជីវកម្មស្តីពីសេចក្តីសម្រេចជាភាសាសាមញ្ញដែលអាចយល់បាន និងអាចបង្កើនការយល់ដឹងពីស្ថាប័ននានា អំពីហានិភ័យនៃការព្យាបាទតាមអ៊ីនធឺណិតដោយគំនិតទុច្ចរិត។ ការដោះដូរផ្នែកសុវត្ថិភាពគួរតែបានកំណត់ដោយនាយកប្រតិបត្តិជាន់ខ្ពស់របស់អតិថិជន ដោយធ្វើឱ្យមានតុល្យភាពសន្តិសុខជាមួយនឹងតម្រូវការអាជីវកម្មផ្សេងទៀត។

អនុសាសន៍សម្រាប់អតិថិជន

ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំស្ថាប័ននានា ឱ្យក្រុមហ៊ុនផលិតសូហ្វវែរសម្រាប់ផ្គត់ផ្គង់របស់ពួកគេ ទទួលខុសត្រូវចំពោះលទ្ធផលសន្តិសុខនៃផលិតផលរបស់ពួកគេ។ ជាផ្នែកមួយនៃចំណុចនេះ ស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យណែនាំថា នាយកប្រតិបត្តិរបស់ស្ថាប័ន ផ្តល់អាទិភាពដល់សារៈសំខាន់នៃការទិញផលិតផលដែលមានសន្តិសុខតាមការរចនា និងផលិតផលដែលមានសន្តិសុខតាមលំនាំដើម។ ការធ្វើបែបនេះអាចបង្ហាញឱ្យឃើញតាមរយៈការបង្កើតគោលនយោបាយដែលតម្រូវឱ្យការិយាល័យទទួលបន្ទុកផ្នែកព័ត៌មានវិទ្យា វាយតម្លៃសន្តិសុខសូហ្វវែរមុននឹងគេទិញវា ក៏ដូចជាការផ្តល់សិទ្ធិអំណាចឱ្យការិយាល័យទទួលបន្ទុកផ្នែកព័ត៌មានវិទ្យារុញត្រឡប់មកវិញ ប្រសិនបើចាំបាច់។ ការិយាល័យទទួលបន្ទុកផ្នែកព័ត៌មានវិទ្យាគួរតែបានផ្តល់សិទ្ធិអំណាចក្នុងការអភិវឌ្ឍលក្ខណៈវិនិច្ឆ័យ ការទិញដែលសង្កត់ធ្ងន់លើសារៈសំខាន់នៃការអនុវត្តសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម (ដែលចំណុចទាំងពីរនោះត្រូវបានគូសបញ្ជាក់នៅក្នុងឯកសារនេះ និងឯកសារផ្សេងទៀតដែលបានបង្កើតឡើងដោយស្ថាប័ន)។ លើសពីនេះ ការិយាល័យទទួលបន្ទុកផ្នែក IT គួរតែបានគាំទ្រដោយគណៈគ្រប់គ្រងប្រតិបត្តិ នៅពេលអនុវត្តលក្ខណៈវិនិច្ឆ័យទាំងនេះ ក្នុងការសម្រេចចិត្តទិញ។ ការសម្រេចចិត្តរបស់ស្ថាប័នដើម្បីទទួលយកហានិភ័យទាក់ទងនឹងផលិតផលបច្ចេកវិទ្យាជាក់លាក់ គួរតែបានចងក្រងជាឯកសារផ្លូវការដែលអនុម័តដោយនាយកប្រតិបត្តិអាជីវកម្មជាន់ខ្ពស់ ហើយបង្ហាញជាទៀងទាត់ទៅកាន់ក្រុមប្រឹក្សាភិបាល។

សេវាកម្មព័ត៌មានវិទ្យាសំខាន់ៗរបស់សហគ្រាស ដែលគាំទ្រគោលជំហរសន្តិសុខរបស់ស្ថាប័ន ដូចជាបណ្តាញសហគ្រាស អត្តសញ្ញាណសហគ្រាស និងការគ្រប់គ្រង ការចូលប្រើប្រាស់ ហើយនិងប្រតិបត្តិការសន្តិសុខ និងសមត្ថភាពឆ្លើយតប គួរតែត្រូវបានគេមើលឃើញថាជាមុខងារអាជីវកម្មដ៏សំខាន់ដែលត្រូវបានផ្តល់មូលនិធិដើម្បីកែតម្រូវឱ្យស្របនឹងសារៈសំខាន់របស់ពួកគេចំពោះភាពជោគជ័យនៃបេសកកម្មរបស់ស្ថាប័ន។ ស្ថាប័ននានាគួរតែបង្កើតផែនការមួយដើម្បីបង្កើនសមត្ថភាពទាំងនេះដើម្បីប្រើប្រាស់ឱ្យមានប្រសិទ្ធិភាពនូវក្រុមហ៊ុនផលិតដែលទទួលយកការអនុវត្ត សន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម។

កន្លែងណាដែលអាចធ្វើទៅបាន ស្ថាប័ននានាគួរតែខិតខំបង្កើតទំនាក់ទំនង ភាពជាដៃគូជាយុទ្ធសាស្ត្រជាមួយអ្នកផ្គត់ផ្គង់ព័ត៌មានវិទ្យាសំខាន់ៗរបស់ពួកគេ។ ទំនាក់ទំនងបែបនេះ រួមមានការជឿទុកចិត្តនៅកម្រិតជាច្រើននៃស្ថាប័ន ហើយផ្តល់ជាយានជំនិះដើម្បីដោះស្រាយបញ្ហា និងកំណត់អាទិភាពរួមគ្នា។ សន្តិសុខគួរតែជាធាតុសំខាន់នៃទំនាក់ទំនងបែបនេះ ហើយស្ថាប័នគួរតែខិតខំពង្រឹងសារៈសំខាន់នៃការអនុវត្តសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម ទាំងទម្រង់ផ្លូវការ (ឧទាហរណ៍ កិច្ចសន្យា ឬកិច្ចព្រមព្រៀងអ្នកលក់) និងទម្រង់ក្រៅផ្លូវការនៃទំនាក់ទំនងនេះ។ ស្ថាប័ននានាគួរតែរំពឹងទទួលបានតម្លាភាពពីអ្នកផ្គត់ផ្គង់បច្ចេកវិទ្យារបស់ពួកគេ អំពីគោលជំហរគ្រប់គ្រងផ្ទៃក្នុងរបស់ពួកគេ ក៏ដូចជាផែនទី បង្ហាញផ្លូវរបស់ពួកគេ ឆ្ពោះទៅរកការចាប់យកការអនុវត្តសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម។

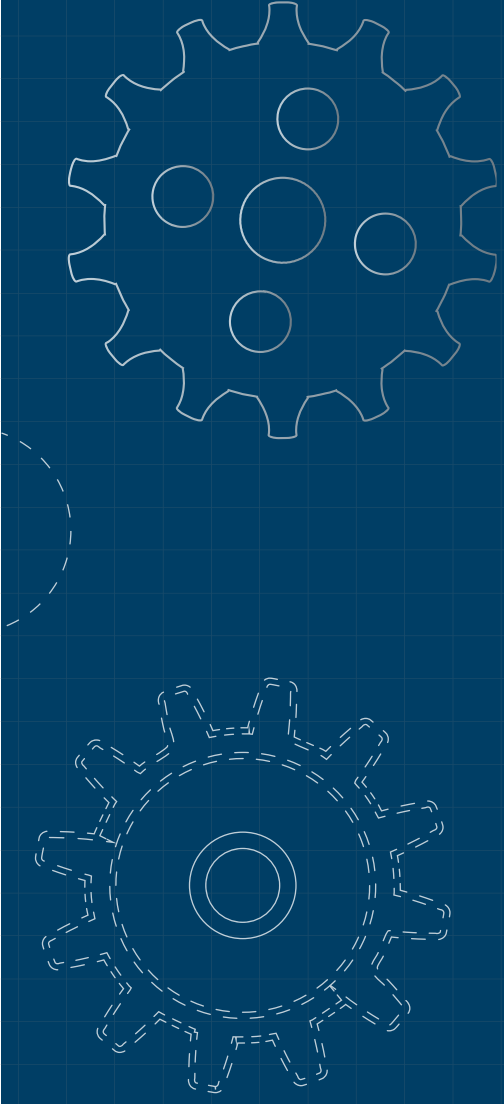
បន្ថែមពីលើការធ្វើឱ្យសន្តិសុខតាមលំនាំដើមជាអាទិភាពនៅក្នុងស្ថាប័ន អ្នកដឹកនាំផ្នែកព័ត៌មានវិទ្យាគួរសហការជាមួយដៃគូក្នុងឧស្សាហកម្មរបស់ពួកគេ ដើម្បីយល់ដឹងថាតើផលិតផល និងសេវាកម្មណាដែលល្អបំផុតធ្វើជាតំណាងឱ្យគោលការណ៍រចនាទាំងនេះ។ អ្នកដឹកនាំទាំងនេះគួរតែសម្របសម្រួលសំណើរបស់ពួកគេ ដើម្បីជួយក្រុមហ៊ុនផលិតក្នុងការកំណត់អាទិភាពគំនិតផ្តួចផ្តើមសន្តិសុខនាពេលខាងមុខរបស់ពួកគេ។ ដោយការធ្វើការរួមគ្នា អតិថិជនអាចជួយផ្តល់មតិយោបល់ដ៏មានអត្ថន័យដល់និងបង្កើតលាភការសម្រាប់ពួកគេក្នុងការកំណត់អាទិភាពសន្តិសុខ។

នៅពេលប្រើប្រាស់ប្រព័ន្ធ cloud (ក្លៅ) ឱ្យមានប្រសិទ្ធភាពស្ថាប័ននានាគួរតែធានាថាពួកគេយល់ដឹងអំពីម៉ូដែលទំនួលខុសត្រូវរួមគ្នា ជាមួយអ្នកផ្គត់ផ្គង់បច្ចេកវិទ្យារបស់ពួកគេ។ ដែលមានន័យថាស្ថាប័នគួរតែមានភាពច្បាស់លាស់លើទំនួលខុសត្រូវផ្នែកសន្តិសុខរបស់អ្នកផ្គត់ផ្គង់ ជាជាងទំនួលខុសត្រូវរបស់អតិថិជន។

ស្ថាប័នគួរតែផ្តល់អាទិភាពដល់អ្នកផ្តល់សេវាកម្មក្លៅដែលមានតម្លាភាពអំពីគោលជំហរសន្តិសុខ ការគ្រប់គ្រងផ្ទៃក្នុង និងសមត្ថភាពក្នុងបំពេញកាតព្វកិច្ចរបស់ពួកគេក្រោមម៉ូដែលទំនួលខុសត្រូវរួមគ្នា។

ការបដិសេធទំនួលខុសត្រូវ

ព័ត៌មាននៅក្នុងរបាយការណ៍នេះកំពុងត្រូវបានផ្តល់ជូន "ក្នុងស្ថានភាពបច្ចុប្បន្ន" សម្រាប់គោលបំណងជាព័ត៌មានតែប៉ុណ្ណោះ។ CISA និងស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ មិនគាំទ្រផលិតផល ឬសេវាកម្មពាណិជ្ជកម្មណាមួយ រួមទាំងស្ថិតក្រោមការវិភាគណាមួយឡើយ។ រាល់ការយោងទៅស្ថាប័នពាណិជ្ជកម្ម ជាក់លាក់ ឬផលិតផលពាណិជ្ជកម្ម ដំណើរការ ឬសេវាកម្មដោយផ្លាកសញ្ញាសេវាកម្ម សញ្ញាពាណិជ្ជកម្ម ក្រុមហ៊ុនផលិត ឬផ្សេងពីនេះ មិនជា ឬបញ្ជាក់ពីការយល់ព្រម អនុសាសន៍ ឬការអនុគ្រោះនិយមដោយ CISA និងស្ថាប័នបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យនោះទេ។ ឯកសារនេះគឺជាការផ្តួចផ្តើមរួមគ្នាដោយ CISA ដែលមិនបំពេញមុខការដោយស្វ័យប្រវត្តិជាឯកសារបទប្បញ្ញត្តិនោះទេ។



CISA

- » ការណែនាំ SBOM របស់ CISA
- » គោលដៅបំពេញការងារសន្តិសុខអ៊ីនធឺណិតឆ្លងវិស័យរបស់ CISA
- » សេចក្តីណែនាំស្តីពីអន្តរប្រតិបត្តិការបច្ចេកវិទ្យា
- » ការការពារប្រឆាំងនឹងការវាយប្រហារខ្សែសង្វាក់ផ្គត់ផ្គង់សូហ្វវែររបស់ CISA និង NIST
- » តម្លៃនៃបច្ចេកវិទ្យាដែលមិនមានសុវត្ថិភាព និងអ្វីដែលយើងអាចធ្វើបានអំពីរឿងនេះ | CISA
- » បញ្ឈប់ការចំណាយដុល្លារលើសន្តិសុខអ៊ីនធឺណិត៖ ហេតុអ្វីបានជាក្រុមហ៊ុននានាត្រូវបង្កើតសុវត្ថិភាពទៅក្នុងផលិតផលបច្ចេកវិទ្យា (foreignaffairs.com)
- » ការណែនាំអំពីប្រភេទភាពងាយរងគ្រោះរបស់ភាគីពាក់ព័ន្ធជាក់លាក់ (SSVC) របស់ CISA
- » សន្លឹកព័ត៌មាន MFA ដែលធន់នឹងការបោកបញ្ឆោតតាមអ៊ីមែលរបស់ CISA
- » ការណែនាំតាមអ៊ីនធឺណិតសម្រាប់អាជីវកម្មខ្នាតតូច | CISA

NSA

- » សន្លឹកព័ត៌មានសន្តិសុខអ៊ីនធឺណិតរបស់ NSA ស្តីពីសុវត្ថិភាពនៃអង្គចងចាំ
- » ESF (ក្របខ័ណ្ឌសន្តិសុខដែលឋិតថេរ) របស់ NSA ដែលធានាខ្សែសង្វាក់ផ្គត់ផ្គង់សូហ្វវែរ ៖ ការអនុវត្តល្អបំផុតសម្រាប់អ្នកផ្គត់ផ្គង់

FBI

- » ការយល់ដឹង និងការឆ្លើយតបទៅនឹងការវាយប្រហារខ្សែសង្វាក់ផ្គត់ផ្គង់ SolarWinds៖ ទស្សនវិស័យសហព័ន្ធ
- » ការគំរាមកំហែងតាមអ៊ីនធឺណិត - ការឆ្លើយតប និងការរាយការណ៍
- » យុទ្ធសាស្ត្រអ៊ីនធឺណិតរបស់ FBI

វិទ្យាស្ថានជាតិស្តង់ដារ និងបច្ចេកវិទ្យា (NIST)

- » សេចក្តីណែនាំអំពីអត្តសញ្ញាណឌីជីថលរបស់ NIST
- » ក្របខ័ណ្ឌសន្តិសុខអ៊ីនធឺណិតរបស់ NIST
- » ក្របខ័ណ្ឌអភិវឌ្ឍន៍សូហ្វវែរដែលមានសន្តិសុខរបស់ (SSDF) NIST

មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតអូស្ត្រាលី (ACSC)

- » ការណែនាំក្រមប្រតិបត្តិ IoT របស់ ACSC សម្រាប់ក្រុមហ៊ុនផលិត

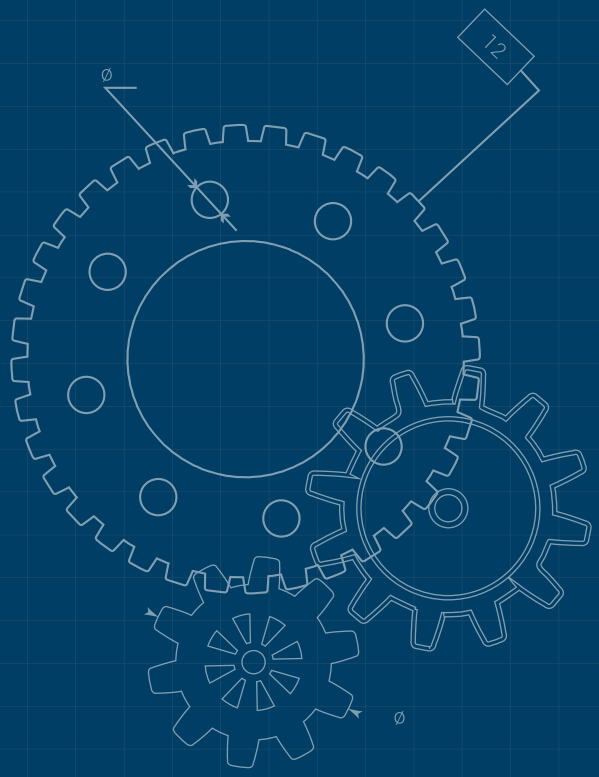
មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ចក្រភពអង់គ្លេស (UK)

- » ក្របខ័ណ្ឌការវាយតម្លៃអ៊ីនធឺណិតរបស់ចក្រភពអង់គ្លេស
- » ការណែនាំអំពីការអភិវឌ្ឍ និងការដាក់ប្រើប្រាស់ប្រកបដោយសន្តិសុខរបស់ NCSC ចក្រភពអង់គ្លេស
- » ការណែនាំអំពីការគ្រប់គ្រងភាពងាយរងគ្រោះរបស់ NCSC ចក្រភពអង់គ្លេស
- » ប្រអប់ឧបករណ៍ការលាតត្រដាងភាពងាយរងគ្រោះរបស់ NCSC ចក្រភពអង់គ្លេស
- » CHERI របស់សាកលវិទ្យាល័យ Cambridge
- » លាហើយចាំជួបគ្នាទៀត សូមអរគុណគ្រប់ដំបូន្មាននានា - NCSC.GOV.UK

មជ្ឈមណ្ឌលកាណាដាសម្រាប់សន្តិសុខអ៊ីនធឺណិត (CCCS)

- » ការណែនាំរបស់ CCCS ស្តីពីការការពារប្រឆាំងនឹងការវាយប្រហារខ្សែសង្វាក់ផ្គត់ផ្គង់សូហ្វវែរ
- » ខ្សែសង្វាក់ផ្គត់ផ្គង់តាមអ៊ីនធឺណិត៖ វិធីសាស្ត្រក្នុងការវាយតម្លៃហានិភ័យ
- » ការណែនាំអំពីមេរោគចាប់ជំរិត CONTI របស់មជ្ឈមណ្ឌលកាណាដាសម្រាប់សន្តិសុខអ៊ីនធឺណិត

ទិន្នផល



ការិយាល័យសហព័ន្ធសម្រាប់សន្តិសុខព័ត៌មាន (BSI) របស់អាល្លឺម៉ង់

» ឯកសារយោង BSI Grundschutz (ម៉ូឌុល CON.8)

» សុង់ដារអន្តរជាតិ IEC 62443 ផ្នែកទី 4-1

» របាយការណ៍ស្តីពីស្ថានភាពសន្តិសុខព័ត៌មានវិទ្យា នៅអាល្លឺម៉ង់ ឆ្នាំ 2022

» ការអនុវត្ត BSI នៃសន្តិសុខកម្មវិធីគេហទំព័រ

មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ហូឡង់

» សន្លឹកព័ត៌មានស្តីពីការធ្វើឱ្យធ្លាត់ភាពពេញក្នុណៈរបស់ NCSC-NL

មជ្ឈមណ្ឌលជាតិនៃការត្រៀមខ្លួន និងយុទ្ធសាស្ត្រសម្រាប់សន្តិសុខអ៊ីនធឺណិត (NISC) របស់ប្រទេសជប៉ុន

» យុទ្ធសាស្ត្រសន្តិសុខអ៊ីនធឺណិតជាតិជប៉ុន

ក្រសួងសេដ្ឋកិច្ច ពាណិជ្ជកម្ម និងឧស្សាហកម្មជប៉ុន (METI)

» គោលការណ៍ការណែនាំស្តីពីការណែនាំនៃសារពើភ័ណ្ឌមូលដ្ឋានកូដសូហ្វវែរពេញលេញ (SBOM) សម្រាប់ការគ្រប់គ្រងសូហ្វវែរ

» ការប្រមូលឧទាហរណ៍ករណីប្រើប្រាស់ទាក់ទងនឹងវិធីសាស្ត្រគ្រប់គ្រងសម្រាប់ការប្រើប្រាស់ OSS និងការធានាសន្តិសុខរបស់វា

ទីភ្នាក់ងារសន្តិសុខអ៊ីនធឺណិតនៃប្រទេសសិង្ហបុរី

» អត្ថបទផ្តល់យោបល់បច្ចេកទេសលើការអភិវឌ្ឍសន្តិសុខ API

» គោលនយោបាយលាតត្រដាងភាពងាយរងគ្រោះរបស់ SingCERT CSA

» បញ្ជីត្រួតពិនិត្យការឆ្លើយតបឧប្បត្តិហេតុរបស់ SingCERT CSA

» ផែនការឆ្លើយតបឧប្បត្តិហេតុសន្តិសុខអ៊ីនធឺណិតរបស់ SingCERT CSA

» ក្របខ័ណ្ឌសន្តិសុខតាមការរចនារបស់ CSA

» បញ្ជីត្រួតពិនិត្យក្របខ័ណ្ឌសន្តិសុខតាមការរចនា CSA

» សៀវភៅណែនាំរបស់ CSA ស្តីពីការធ្វើម៉ូដែលការគំរាមកំហែងតាមអ៊ីនធឺណិត

» គម្រោងដាក់ស្លាកសន្តិសុខអ៊ីនធឺណិតរបស់ CSA

ផ្សេងទៀត

» របៀបដែលប្រព័ន្ធសុគស្មាញបរាជ័យ

» ទិដ្ឋភាពថ្មីនៅក្នុងការបរាជ័យនៃប្រព័ន្ធសុគស្មាញ

ឯកសារយោង

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom និងឯកសារយោង SBOMs នៅក្នុង TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] Juran on Quality by Design by J.M. Juran, 1992។