TLP:CLEAR

ការផ្លាស់ប្តូរតុល្យភាពនៃហានិភ័យសន្តិសុខអ៊ីនធឺណិត៖ គោលការណ៍ និងវិធីសាស្ត្រសម្រាប់សន្តិសុខតាមការរចនា និងតាមលំនាំដើម

ការបោះពុម្ពផ្សាយ៖ ថ្ងៃទី 13 ខែមេសា ឆ្នាំ 2023

ទីភ្នាក់ងារសន្តិសុខអ៊ីនធឺណិត និងសន្តិសុខហេដ្ឋារចនាសម្ព័ន្ធ

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

តារាងមាតិកា

ទិដ្ឋភាពទូទៅ៖ ភាពងាយរងគ្រោះដោយការរចនា

បច្ចេកវិទ្យាត្រូវបានដាក់បញ្ចូលទៅក្នុងស្ទើរតែគ្រប់ទិដ្ឋភាពនៃជីវិតប្រចាំថ្ងៃ។ ប្រព័ន្ធនានាដែលដាក់ដំណើរការតាមរយៈអ៊ីនធឺណិត ត្រូវបានភ្ជាប់ទៅប្រព័ន្ធសំខាន់ៗដែលជះឥទ្ធិពលដោយផ្ទាល់ទៅលើភាពចំរុងចម្រើនខាងសេដ្ឋកិច្ច ជីវភាពរស់នៅ និងសុម្មីតែសុខភាពរបស់យើងចាប់ពីការគ្រប់គ្រងអត្តសញ្ញាណផ្ទាល់ខ្លួន រហូតដល់ការថែទាំវេជ្ជសាស្ត្រ។ ជាឧទាហរណ៍តែមួយគត់ ការបំពានលើសុវត្ថិភាពអ៊ីនធឺណិតបានបណ្តាលឱ្យមន្ទីរពេទ្យលុបចោលការវះកាត់ និងបង្វែរការថែទាំអ្នកជំងឺទូទាំងពិភពលោក។ បច្ចេកវិជ្ជាដែលគ្មានសន្តិសុខ និងភាពងាយរងគ្រោះនៅក្នុងប្រព័ន្ធសំខាន់ៗ អាចបង្កឱ្យមានការឈ្លានពានព្យាបាទតាមអ៊ីនធឺណិតដែលមានគំនិតទុច្ចរិត ដែលឈានទៅដល់ហានិភ័យសុវត្ថិភាព[1] ដែលអាចកើតឡើងខ្ពស់។

ឥឡូវនេះច្រើនជាងពេលណាៗទាំងអស់ វាមានសារៈសំខាន់ណាស់សម្រាប់អ្នកផលិតបច្ចេកវិទ្យាធ្វើឱ្យមានសុវត្ថិភាពតាមការរចនា និងសុវត្ថិភាពតាមលំនាំដើម ចំណុចស្នូលនៃដំណើរការរចនា និងការអភិវឌ្ឍន៍ផលិតផល។ អ្នកលក់មួយចំនួនបានបោះជំហានទៅមុខយ៉ាងសម្បើម ក្នុងការជំរុញឧស្សាហកម្មឆ្ពោះទៅមុខក្នុងការធានាដល់សុវត្ថិភាព (ផ្នែកទន់) ខណៈពេលដែលអ្នកផ្សេងទៀតមានដំណើរយឺតយ៉ាវ។ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ លើកទឹកចិត្តយ៉ាងខ្លាំងដល់គ្រប់ក្រុមហ៊ុនផលិតបច្ចេកវិទ្យា ឱ្យបង្កើតផលិតផលរបស់ពួកគេតាមរបៀបមួយដែលការពារអតិថិជនពីការត្រួតពិនិត្យ ការធ្វើបច្ចុប្បន្នភាពជាប្រចាំ និងការគ្រប់គ្រងការខូចខាតលើប្រព័ន្ធរបស់ពួកគេ ដើម្បីកាត់បន្ថយការបំពានតាមអ៊ីនធឺណិត។ ក្រុមហ៊ុនផលិតនានាត្រូវបានលើកទឹកចិត្តឱ្យទទួលយកភាពជាម្ចាស់ នៃការកែលម្អលទ្ធផលសន្តិសុខរបស់អតិថិជនពួកគេ។ ជាប្រវត្តិសាស្ត្រ ក្រុមហ៊ុនផលិតបច្ចេកវិទ្យាបានពឹងផ្អែកលើការជួសជុលភាពងាយរងគ្រោះដែលបានរកឃើញ បន្ទាប់ពីអតិថិជនបានដាក់ប្រើប្រាស់ផលិតផល ដោយតម្រូវឱ្យអតិថិជនជួសជុលកង្វះខាតទាំងនោះពីការចំណាយផ្ទាល់ខ្លួនរបស់ពួកគេ។ មានតែតាមរយៈការដាក់បញ្ចូលការអនុវត្តសុវត្ថិភាពតាមការរចនាប៉ុណ្ណោះដែលយើងនឹងបំបែកវដ្តទុច្ចរិតនៃការបង្កើត និងការជួសជុល។

ដើម្បីសម្រេចបាននូវស្តង់ដារខ្ពស់នៃសន្តិសុខសូហ្វវែរ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ លើកទឹកចិត្តអ្នកផលិតឱ្យផ្តល់អាទិភាពដល់ការដាក់បញ្ចូលសន្តិសុខផលិតផលជាតម្រូវការជាមុនសំខាន់ៗសម្រាប់លក្ខណៈពិសេសនៃផលិតផល និងល្បឿនទៅកាន់ទីផ្សារ។ យូរៗទៅ ក្រុមវិស្វកររនឹងអាចបង្កើតចង្វាក់ស្ថិរភាពថ្មីមួយ ដែលសន្តិសុខត្រូវបានរចនាយ៉ាងពិតប្រាកដនៅក្នុងផលិតផល ហើយចំណាយការខិតខំប្រឹងប្រែងតិចតួចក្នុងការថែរក្សា។ ដោយឆ្លុះបញ្ចាំងពីទស្សនៈនេះ សហភាពអឺរ៉ុបបានពង្រឹងសារៈសំខាន់នៃសន្តិសុខផលិតផលនៅក្នុងច្បាប់ស្តីពីភាពធន់នឹងអ៊ីនធឺណិត ដោយសង្កត់ធ្ងន់ថាក្រុមហ៊ុនផលិតគួរតែអនុវត្តសន្តិសុខពេញវដ្តនៃជីវិតរបស់ផលិតផល ដើម្បីទប់ស្កាត់ក្រុមហ៊ុនផលិតពីការណែនាំផលិតផលដែលងាយរងគ្រោះចូលទៅក្នុងទីផ្សារ។

ដើម្បីបង្កើតអនាគតមួយដែលបច្ចេកវិទ្យា និងផលិតផលពាក់ព័ន្ធមានសុវត្ថិភាពជាងមុនសម្រាប់អតិថិជន ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យជំរុញឱ្យក្រុមហ៊ុនផលិតធ្វើការកែលម្អការរចនា និងកម្មវិធីអភិវឌ្ឍន៍របស់ពួកគេឡើងវិញ ដើម្បីអនុញ្ញាតឱ្យមានតែផលិតផលដែលមានសន្តិសុខតាមការរចនា និងតាមលំនាំដើមប៉ុណ្ណោះសម្រាប់ការដឹកជញ្ជូនទៅកាន់អតិថិជន។ ផលិតផលដែលមានសន្តិសុខតាមការរចនា គឺជាផលិតផលដែលមានសន្តិសុខរបស់អតិថិជនគឺជាគោលដៅអាជីវកម្មស្នូល មិនមែនគ្រាន់តែជាលក្ខណៈពិសេសផ្នែកបច្ចេកទេសប៉ុណ្ណោះនោះទេ។ ផលិតផលដែលមានសន្តិសុខតាមការរចនាចាប់ផ្តើមដោយមានគោលដៅនោះ មុនពេលការអភិវឌ្ឍន៍ចាប់ផ្តើម។ ផលិតផលដែលមានសន្តិសុខតាមលំនាំដើមគឺជាផលិតផលដែលមានសន្តិសុខក្នុងការប្រើប្រាស់ "ចេញពីប្រអប់" ដែលគ្មាន ឬមានការផ្លាស់ប្តូរចនាសម្ព័ន្ធចាំបាច់តិចតួច និងលក្ខណៈពិសេសនៃសន្តិសុខដែលអាចរកបានដោយគ្មានការចំណាយបន្ថែម។ រួមគ្នា គោលការណ៍ទាំងពីរនេះផ្លាស់ទីបន្ទុកនៃការរក្សាសុវត្ថិភាពទៅអ្នកផលិត ហើយកាត់បន្ថយឱកាសដែលអតិថិជននឹងរងគ្រោះដោយសារឧប្បត្តិហេតុសន្តិសុខ ដែលបណ្តាលមកពីការកំណត់រចនាសម្ព័ន្ធមិនត្រឹមត្រូវ ការជួសជុល

[1] ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ទទួលស្គាល់ថាពាក្យ "សុវត្ថិភាព" មានអត្ថន័យច្រើន ដោយអាស្រ័យលើបរិបទដែលគេប្រើវា។ សម្រាប់គោលបំណងនៃការណែនាំនេះ "សុវត្ថិភាព" នឹងសំដៅលើការបង្កើនស្តង់ដារសន្តិសុខបច្ចេកវិទ្យា ដើម្បីការពារអតិថិជនពីសកម្មភាពទុច្ចរិតតាមអ៊ីនធឺណិត។

រហ័សមិនបានគ្រប់គ្រាន់ ឬបញ្ហាទូទៅជាច្រើនទៀត។

ទីភ្នាក់ងារសន្តិសុខអ៊ីនធឺណិត និងសន្តិសុខហេដ្ឋារចនាសម្ព័ន្ធ (CISA), ទីភ្នាក់ងារសន្តិសុខជាតិ (NSA), ការិយាល័យស៊ើបអង្កេតសហព័ន្ធ (FBI) និងដៃគូអន្តរជាតិដូចខាងក្រោមនេះ[2] ផ្តល់អនុសាសន៍នៅក្នុងការណែនាំនេះថាជាផែនទីបង្ហាញផ្លូវសម្រាប់អ្នកផលិតបច្ចេកវិទ្យា ដើម្បីធានាសន្តិសុខនៃផលិតផលរបស់ពួកគេ៖

- មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតអូស្ត្រាលី (ACSC)
- មជ្ឈមណ្ឌលកាណាដាសម្រាប់ការពារសន្តិសុខអ៊ីនធឺណិត (CCCS)
- មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ចក្រភពអង់គ្លេស (NCSC-UK)
- ការិយាល័យសហព័ន្ធសម្រាប់សន្តិសុខព័ត៌មាន (BSI) របស់អាល្លឺម៉ង់
- មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ហូឡង់ (NCSC-NL)
- ក្រុមឆ្លើយតបបន្ទាន់តាមកុំព្យូទ័ររបស់នូវែលសេឡង់ (CERT NZ) និងមជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់នូវែលសេឡង់ (NCSC-NZ)។

ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ទទួលស្គាល់ចំពោះការរួមចំណែកដោយដៃគូវិស័យឯកជនជាច្រើន ក្នុងការជំរុញសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម។ ផលិតផលនេះមានគោលបំណងជំរុញការសន្ទនាអន្តរជាតិអំពីអាទិភាពសំខាន់ៗ ការវិនិយោគ និងសេចក្តីសម្រេចដែលចាំបាច់ ដើម្បីសម្រេចបានអនាគតមួយដែលបច្ចេកវិទ្យាមានសុវត្ថិភាព សន្តិសុខ និងភាពធន់តាមការរចនា និងលំនាំដើម។ នៅចុងបញ្ចប់នោះ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យស្វែងរកមតិកែលម្អលើផលិតផលនេះ ពីភាគីនានាដែលចាប់អារម្មណ៍ ហើយមានបំណងរៀបចំវគ្គស្តាប់ជាបន្តបន្ទាប់ ដើម្បីកែលម្អបន្ថែម បញ្ចាក់ និងជំរុញការណែនាំរបស់យើង ដើម្បីសម្រេចបាននូវគោលដៅរួមរបស់យើង។

សម្រាប់ព័ត៌មានបន្ថែមអំពីសារៈសំខាន់នៃសុវត្ថិភាពផលិតផល សូមមើលអត្ថបទរបស់ CISA [តម្លៃ នៃបច្ចេកវិទ្យាដែលមិនមានសុវត្ថិភាព និងអ្វីដែលយើងអាចធ្វើបានអំពីរឿងនេះ](#)។

សុវត្ថិភាពតាមការរចនា

"សុវត្ថិភាពតាមការរចនា" មានន័យថា ផលិតផលបច្ចេកវិទ្យាត្រូវបានបង្កើតឡើងតាមរបៀបមួយ ដែលការពារដោយសមហេតុផលប្រឆាំងនឹងបុគ្គលមានបំណងទុច្ចរិតតាមអ៊ីនធឺណិត ពីការចូលប្រើប្រាស់ដោយជោគជ័យនូវឧបករណ៍ ទិន្នន័យ និងហេដ្ឋារចនាសម្ព័ន្ធដែលបានតភ្ជាប់។ ក្រុមហ៊ុនផលិតសូហ្វវែរគួរតែធ្វើការវាយតម្លៃហានិភ័យដើម្បីកំណត់អត្តសញ្ញាណ និងរៀបរាប់តាមលំដាប់នូវការគំរាមកំហែងតាមអ៊ីនធឺណិតដែលរីករាលដាលដល់ប្រព័ន្ធសំខាន់ៗ ហើយបន្ទាប់មក រួមបញ្ចូលការការពារនៅក្នុងគម្រោងផែនការផលិតផល ដែលគិតគូរពីទិដ្ឋភាពនៃការគំរាមកំហែងតាមអ៊ីនធឺណិតដែលកំពុងវិវត្ត។

ការអនុវត្តការអភិវឌ្ឍន៍បច្ចេកវិទ្យាព័ត៌មានសន្តិសុខ (IT) និងការការពារដោច្រើនជាន់ ដែលត្រូវបានគេស្គាល់ថាការការពារស៊ីជម្រៅ ក៏ត្រូវបានណែនាំផងដែរដើម្បីការពារសកម្មភាពរបស់សត្រូវពីការសម្របសម្រួលប្រព័ន្ធ ឬការចូលប្រើប្រាស់ទិន្នន័យរសើបដោយគ្មានការអនុញ្ញាត។ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំអ្នកផលិត ឱ្យប្រើគំរូការគំរាមកំហែងដែលតម្រូវក្នុងអំឡុងដំណាក់កាលនៃការអភិវឌ្ឍន៍ផលិតផលដើម្បីដោះស្រាយរាល់ការគំរាមកំហែងដែលអាចកើតមានចំពោះប្រព័ន្ធ និងគណនីសម្រាប់ដំណើរការប្រើប្រាស់របស់ប្រព័ន្ធនីមួយៗ។

[2] តទៅនេះត្រូវបានហៅថា "ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ"។

ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ជំរុញឱ្យអ្នកផលិត ទទួលយកវិធីសាស្ត្រសន្តិសុខរួមសម្រាប់ផលិតផល និងវេទិការបស់ពួកគេ។ ការអភិវឌ្ឍន៍សន្តិសុខតាមការរចនាតម្រូវឱ្យមានការវិនិយោគធនធានសំខាន់ៗពីអ្នកផលិតសូហ្វវែរ នៅស្រទាប់នីមួយៗនៃដំណើរការរចនា និងការអភិវឌ្ឍផលិតផលដែលមិនអាច "ដាក់បន្ថែម" នៅពេលក្រោយ។ វាតម្រូវឱ្យមានភាពជាអ្នកដឹកនាំដ៏រឹងមាំដោយនាយកប្រតិបត្តិអាជីវកម្មកំពូលរបស់ក្រុមហ៊ុនផលិតដើម្បីធ្វើឱ្យសន្តិសុខក្លាយជាចំណុចអាទិភាពរបស់អាជីវកម្ម មិនមែនគ្រាន់តែជាលក្ខណៈពិសេសផ្នែកបច្ចេកទេសប៉ុណ្ណោះទេ។ កិច្ចសហការរវាងអ្នកដឹកនាំអាជីវកម្ម និងក្រុមបច្ចេកទេសនេះ ពង្រីកពីដំណាក់កាលដំបូងនៃការរចនា និងការអភិវឌ្ឍន៍តាមរយៈការប្រើប្រាស់ និងការថែទាំអតិថិជន។ អ្នកផលិតត្រូវបានលើកទឹកចិត្តឱ្យធ្វើការដោះដូរ និងការវិនិយោគដ៏លំបាក រួមទាំងអ្វីដែលនឹង "មើលមិនឃើញ" សម្រាប់អតិថិជន ដូចជាការផ្លាស់ប្តូរទៅភាសាសរសេរកម្មវិធីដែលលុបបំបាត់ភាពងាយរងគ្រោះដែលរីករាលដាល។ ពួកគេគួរតែផ្តល់អាទិភាពដល់លក្ខណៈពិសេស យន្តការ និងការអនុវត្តឧបករណ៍ដែលការពារអតិថិជន ជាជាងលក្ខណៈពិសេសនៃផលិតផលដែលមើលទៅគួរឱ្យទាក់ទាញ ប៉ុន្តែពង្រីកផ្ទៃរូបភាពដែលអាចវាយប្រហារទៅវិញ។

មិនមានដំណោះស្រាយតែមួយ ដើម្បីបញ្ចប់ការគំរាមកំហែងជាបន្តបន្ទាប់នៃបុគ្គលដែលមានបំណងទុច្ចរិតតាមអ៊ីនធឺណិត ដែលទាញយកប្រយោជន៍ពីភាពងាយរងគ្រោះផ្នែកបច្ចេកវិទ្យានោះទេ ហើយផលិតផលដែលមាន "សន្តិសុខតាមការរចនា" នឹងនៅតែបន្តរងគ្រោះ។ ទោះយ៉ាងណាក៏ដោយភាពងាយរងគ្រោះមួយឈុតធំគឺដោយសារតែផ្នែកតូចៗនៃប្រភពដើមហេតុដែលទាក់ទង។ អ្នកផលិតគួរតែបង្កើតផែនទីបង្ហាញផ្លូវដោលាយលក្ខណ៍អក្សរដើម្បីតម្រឹមផលប័ត្រផលិតផលដែលមានស្រាប់របស់ពួកគេ ជាមួយនឹងការអនុវត្តសន្តិសុខតាមការរចនាបន្ថែមទៀត ដោយជានាថានឹងអាចងាកចេញបានតែក្នុងស្ថានភាពពិសេសប៉ុណ្ណោះ។

ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ទទួលស្គាល់ថា ការទទួលយកភាពជាម្ចាស់នៃលទ្ធផលសន្តិសុខសម្រាប់អតិថិជន និងការធានាកម្រិតសន្តិសុខអតិថិជនអាចបង្កើនថ្លៃចំណាយលើការអភិវឌ្ឍន៍។ ទោះជាយ៉ាងណាក៏ដោយ ការវិនិយោគលើការអនុវត្ត "សន្តិសុខតាមការរចនា" ខណៈពេលដែលកំពុងអភិវឌ្ឍផលិតផលបច្ចេកវិទ្យាថ្មី និងការរក្សានូវផលិតផលដែលមានស្រាប់ អាចធ្វើឱ្យប្រសើរឡើងនូវគោលជំហរសន្តិសុខរបស់អតិថិជន និងកាត់បន្ថយលទ្ធភាពនៃការសម្របសម្រួល។ គោលការណ៍សន្តិសុខតាមការរចនា មិនត្រឹមតែពង្រឹងគោលជំហរសន្តិសុខសម្រាប់អតិថិជន និងកេរ្តិ៍ឈ្មោះម៉ាកសម្រាប់អ្នកអភិវឌ្ឍន៍ប៉ុណ្ណោះទេ ប៉ុន្តែក៏កាត់បន្ថយថ្លៃចំណាយលើការថែទាំ និងការជួសជុលសម្រាប់អ្នកផលិតក្នុងរយៈពេលវែងផងដែរ។

អនុសាសន៍សម្រាប់អ្នកផលិតសូហ្វវែរដែលបានរាយបញ្ជីខាងក្រោម ផ្តល់នូវបញ្ជីអនុសាសន៍ និងគោលនយោបាយអភិវឌ្ឍន៍ផលិតផលដែលបានណែនាំសម្រាប់អ្នកផលិតដើម្បីពិចារណា។

សន្តិសុខតាមលំនាំដើម

"សុវត្ថិភាពតាមលំនាំដើម" មានន័យថា ផលិតផលមានភាពធន់នឹងបច្ចេកទេសនៃការកេងប្រវ័ញ្ចដ៏ទូលំទូលាយ ចេញពីប្រអប់ដោយមិនគិតថ្លៃបន្ថែម។ ផលិតផលទាំងនេះការពារប្រឆាំងនឹងការគំរាមកំហែង និងភាពងាយរងគ្រោះដែលរីករាលដាលបំផុត ដោយពុំតម្រូវឱ្យអ្នកប្រើប្រាស់ចុងក្រោយ ត្រូវចាត់វិធានការបន្ថែមដើម្បីការពារផលិតផលនោះទេ។ ផលិតផលដែលមានសន្តិសុខតាមលំនាំដើម ត្រូវបានរចនាឡើងដើម្បីធ្វើឱ្យអតិថិជនដឹងយ៉ាងច្បាស់ថា នៅពេលដែលពួកគេងាកចេញពីសន្តិសុខតាមលំនាំដើម ពួកគេកំពុងបង្កើនលទ្ធភាពនៃការសម្របសម្រួល លុះត្រាតែពួកគេអនុវត្តការត្រួតពិនិត្យសំណងបន្ថែម។

- ការកំណត់រចនាសម្ព័ន្ធសន្តិសុខគួរតែជាបន្ទាត់មូលដ្ឋានលំនាំដើម។ ផលិតផលដែលមានសន្តិសុខតាមលំនាំដើមបើកដោយស្វ័យប្រវត្តិ

នូវការគ្រប់គ្រងសន្តិសុខដ៏សំខាន់បំផុត ដែលត្រូវការដើម្បីការពារសហគ្រាសពីបុគ្គលដែលមានបំណងទុច្ចរិតតាមអ៊ីនធឺណិត ក៏ដូចជាផ្តល់នូវសមត្ថភាពក្នុងការប្រើប្រាស់ និងកំណត់រចនាសម្ព័ន្ធការគ្រប់គ្រងសន្តិសុខបន្ថែមទៀតដោយមិនគិតថ្លៃបន្ថែម។

- ភាពស្មុគស្មាញនៃការកំណត់រចនាសម្ព័ន្ធសន្តិសុខមិនគួរជាបញ្ហារបស់អតិថិជនទេ។ បុគ្គលិកផ្នែក IT របស់ស្ថាប័ន តែងតែទទួលបន្ទុកលើសលប់ជាមួយនឹងទំនួលខុសត្រូវផ្នែកសន្តិសុខ និងប្រតិបត្តិការ ដូច្នេះហើយទើបបណ្តាលឱ្យមានពេលវេលាកំណត់ក្នុងការយល់ដឹង និងអនុវត្តផលប៉ះពាល់ និងការកាត់បន្ថយសន្តិសុខដែលត្រូវការសម្រាប់គោលជំហរសន្តិសុខតាមអ៊ីនធឺណិតដ៏រឹងមាំ។ តាមរយៈការបង្កើនប្រសិទ្ធភាពនៃការកំណត់រចនាសម្ព័ន្ធផលិតផលប្រកបដោយសន្តិសុខ—ការជានា "ផ្លូវលំនាំដើម"—អ្នកផលិតអាចជួយអតិថិជនរបស់ពួកគេដោយជានាថាផលិតផលរបស់ពួកគេត្រូវបានផលិត ចែកចាយ និងប្រើប្រាស់ប្រកបដោយសន្តិសុខស្របតាមស្តង់ដារ "សន្តិសុខតាមលំនាំដើម"។

អ្នកផលិតផលិតផលដែលមាន "សន្តិសុខតាមលំនាំដើម" មិនគិតថ្លៃបន្ថែមសម្រាប់ការអនុវត្តការកំណត់រចនាសម្ព័ន្ធសន្តិសុខបន្ថែមទេ។ ជាជំនួសវិញនោះ ពួកគេរួមបញ្ចូលវានៅក្នុងផលិតផលជាមូលដ្ឋាន ដូចជាខ្សែក្រវ៉ាត់សុវត្ថិភាពត្រូវបានដាក់ក្នុងរថយន្តថ្មីទាំងអស់នោះដែរ។ សន្តិសុខមិនមែនជាជម្រើសដ៏ប្រណិតនោះទេ ប៉ុន្តែវាកាន់តែខិតទៅជិតស្តង់ដារដែលអតិថិជនគ្រប់រូបគួររំពឹងដោយមិនចាំបាច់ចរចា ឬបង់ប្រាក់បន្ថែម។

អនុសាសន៍សម្រាប់អ្នកផលិតសូហ្វវែរ

មគ្គុទ្ទេសក៍រួមនេះ ផ្តល់អនុសាសន៍ដល់អ្នកផលិតសម្រាប់ការអភិវឌ្ឍន៍ផែនទីបង្ហាញផ្លូវដោលាយលក្ខណ៍អក្សរដើម្បីអនុវត្ត និងធានាសន្តិសុខព័ត៌មានវិទ្យា។ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំអ្នកផលិតសូហ្វវែរ ឱ្យអនុវត្តយុទ្ធសាស្ត្រដែលបានរៀបរាប់នៅក្នុងផ្នែកខាងក្រោម ដើម្បីទទួលបាននូវភាពជាម្ចាស់នៃលទ្ធផលសន្តិសុខរបស់អតិថិជនពួកគេ តាមរយៈគោលការណ៍សន្តិសុខតាមការរចនា និងតាមលំនាំដើម។

គោលការណ៍សន្តិសុខផលិតផលសូហ្វវែរ

អ្នកផលិតបច្ចេកវិទ្យាត្រូវបានលើកទឹកចិត្តឱ្យទទួលយកការផ្តោតជាយុទ្ធសាស្ត្រ ដែលផ្តល់អាទិភាពលើសន្តិសុខសូហ្វវែរ។ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ បានបង្កើតគោលការណ៍ស្នូលទាំងបីខាងក្រោម ដើម្បីណែនាំអ្នកផលិតសូហ្វវែរក្នុងការបង្កើតសន្តិសុខសូហ្វវែរ ទៅក្នុងដំណើរការរចនារបស់ពួកគេមុនពេលបង្កើត កំណត់រចនាសម្ព័ន្ធ និងដឹកជញ្ជូនផលិតផលរបស់ពួកគេ។

1. បន្ទុកសន្តិសុខមិនគួរធ្លាក់លើអតិថិជនតែម្នាក់នោះទេ។ អ្នកផលិតសូហ្វវែរគួរតែទទួលយកភាពជាម្ចាស់នៃលទ្ធផលសន្តិសុខនៃការទិញរបស់អតិថិជនពួកគេ ហើយវិវឌ្ឍផលិតផលរបស់ពួកគេទៅតាមការគួរ។
2. ទទួលយកតម្លាភាព និងគណនេយ្យភាពជាច់ខាត។ អ្នកផលិតសូហ្វវែរគួរមានមោទនភាពក្នុងការផ្តល់នូវផលិតផលដែលមានសុវត្ថិភាព និងសន្តិសុខ ក៏ដូចជាការធ្វើឱ្យមានភាពខុសប្លែកគ្នាក្នុងចំណោមសហគមន៍អ្នកផលិតផ្សេងទៀត ដោយផ្អែកលើសមត្ថភាពរបស់ពួកគេក្នុងការធ្វើបែបនោះ។ នេះអាចរួមបញ្ចូលការចែករំលែកព័ត៌មានដែលពួកគេបានរៀនពីការប្រើប្រាស់របស់អតិថិជនពួកគេ ដូចជាការទទួលយកយន្តការផ្ទៀងផ្ទាត់ដ៏រឹងមាំតាមលំនាំដើម។ វាក៏រួមបញ្ចូលផងដែរនូវការប្តេជ្ញាចិត្តយ៉ាងមុតមាំក្នុងការជានាឱ្យបាននូវការប្រឹក្សាអំពីភាពងាយរងគ្រោះ និងកំណត់ត្រាភាពងាយរងគ្រោះ និងការប៉ះពាល់ទូទៅដែលពាក់ព័ន្ធ (CVE) គឺពេញលេញ ហើយត្រឹមត្រូវ។ ទោះជាយ៉ាងណាក៏ដោយ ចូរប្រយ័ត្ននឹងការល្បួងឱ្យរាប់ CVEs ជារង្វាស់អរិជ្ជមានព្រោះថាលេខបែបនេះក៏ជាសញ្ញានៃសហគមន៍រីកាគ និងការធ្វើតេស្តកូដដែលមានសុខភាពល្អផងដែរ។

3. បង្កើតរចនាសម្ព័ន្ធអង្គភាព និងភាពជាអ្នកដឹកនាំ ដើម្បីសម្រេចបាននូវគោលដៅទាំងនេះ។ ខណៈពេលដែលជំនាញប្រធានបទបច្ចេកទេសមានសារៈសំខាន់ចំពោះសន្តិសុខផលិតផល នាយកប្រតិបត្តិជាន់ខ្ពស់គឺជាអ្នកធ្វើសេចក្តីសម្រេចចម្បង សម្រាប់ការអនុវត្តការផ្លាស់ប្តូរនៅក្នុងស្ថាប័នមួយ។ ការប្តេជ្ញាចិត្តកម្រិតប្រតិបត្តិសម្រាប់អ្នកផលិតសូហ្វវែរ ក្នុងការកំណត់អាទិភាពសន្តិសុខជាធាតុសំខាន់នៃការអភិវឌ្ឍន៍ផលិតផល ទាមទារឱ្យមានការអភិវឌ្ឍន៍ភាពជាដៃគូជាមួយអតិថិជនរបស់អង្គភាពដើម្បីយល់ដឹងពី៖

    ក. ការណែនាំអំពីស្ថានភាពនៃការដាក់ប្រើប្រាស់ផលិតផល រួមជាមួយនឹងគំរូគំរាមកំហែងដែលតម្រូវ

    ខ. ការអនុវត្តដែលបានស្នើឡើងសម្រាប់ការត្រួតពិនិត្យសន្តិសុខ ដើម្បីអនុលោមតាមគោលការណ៍សន្តិសុខតាមលំនាំដើម

    គ. យុទ្ធសាស្ត្របែងចែកធនធានដែលសមស្របតាមទំហំក្រុមហ៊ុន និងសមត្ថភាពក្នុងការជំនួសការអនុវត្តការអភិវឌ្ឍន៍កេរ្តិ៍ដំណែល ជាមួយនឹងការអនុវត្តសន្តិសុខតាមការរចនា

    ឃ. តម្រូវការដើម្បីរក្សាទំនាក់ទំនងបើកចំហសម្រាប់មតិកែលម្អខាងក្នុង និងខាងក្រៅ (ឧទាហរណ៍ មតិកែលម្អរបស់បុគ្គលិក និងអតិថិជន) ទាក់ទងនឹងបញ្ហាសន្តិសុខផលិតផល។ សន្តិសុខសូហ្វវែរគួរតែត្រូវបានសង្កត់ធ្ងន់នៅក្នុងវេទិកាផ្ទៃក្នុង (ឧទាហរណ៍ ពាក់ព័ន្ធនឹងអ្នកធ្វើគ្រប់រូប វគ្គប្រជុំ ឬបណ្តុះបណ្តាលអាជីវកម្មក្រៅផ្លូវការ) ក៏ដូចជាការធ្វើទីផ្សារផលិតផលខាងក្រៅ និងការចូលរួមរបស់អតិថិជន

    ង. ការវាស់វែងប្រសិទ្ធភាពនៅក្នុងការប្រើប្រាស់របស់អតិថិជន។ អ្នកដឹកនាំប្រតិបត្តិជាន់ខ្ពស់នឹងចង់ដឹងពីកន្លែងដែលការវិនិយោគលើសន្តិសុខតាមការរចនា និងតាមលំនាំដើម កំពុងជួយអតិថិជនដោយការបន្ថយល្បឿននៃវិធីបង្កើនសន្តិសុខ ការកាត់បន្ថយកំហុសក្នុងការកំណត់រចនាសម្ព័ន្ធ និងការកាត់បន្ថយផ្ទៃរូបភាពនៃការវាយប្រហារ។

ដើម្បជំណើរការគោលការណ៍ទាំងបីនេះ អ្នកផលិតគួរតែពិចារណាអំពីយុទ្ធសាស្ត្រប្រតិបត្តិការមួយចំនួន ដើម្បីវិវឌ្ឍន៍ដំណើរការអភិវឌ្ឍន៍របស់ពួកគេ។

រៀបចំការប្រជុំជាប្រចាំជាមួយថ្នាក់ដឹកនាំប្រតិបត្តិរបស់ក្រុមហ៊ុន ដើម្បីជំរុញសារៈសំខាន់នៃសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើមនៅក្នុងស្ថាប័ន។ គោលនយោបាយ និងនីតិវិធីគួរតែបានបង្កើតឡើង ដើម្បីផ្តល់រង្វាន់ដល់ក្រុមផលិតកម្មដែលអភិវឌ្ឍផលិតផលដែលប្រកាន់ខ្ជាប់នូវគោលការណ៍ទាំងនេះ ដែលអាចរួមបញ្ចូលរង្វាន់សម្រាប់ការប្រតិបត្តិការអនុវត្តសន្តិសុខសូហ្វវែរដ៏ឆ្នើម ឬការលើកទឹកចិត្តសម្រាប់ជណ្តើរវិជ្ជាជីវៈ និងលក្ខណៈវិនិច្ឆ័យនៃការដំឡើងឋានៈ។

ធ្វើប្រតិបត្តិការជុំវិញសារៈសំខាន់នៃសន្តិសុខសូហ្វវែរដើម្បីជោគជ័យអាជីវកម្ម។ ជាឧទាហរណ៍ ពិចារណាលើការចាត់តាំង "អ្នកដឹកនាំសន្តិសុខសូហ្វវែរ" ឬ "ក្រុមសន្តិសុខសូហ្វវែរ" ដែលគាំទ្រការអនុវត្តអាជីវកម្ម និងព័ត៌មានវិទ្យាដើម្បីភ្ជាប់ដោយផ្ទាល់នូវស្តង់ដារសន្តិសុខសូហ្វវែរ និងការទទួលខុសត្រូវរបស់អ្នកផលិត។ អ្នកផលិតគួរតែជានាថាពួកគេមានកម្មវិធីវាយតម្លៃសន្តិសុខផលិតផលឯករាជ្យ និងរឹងមាំសម្រាប់ផលិតផលរបស់ពួកគេ។

ប្រើគំរូគំរាមកំហែងតាមតម្រូវការក្នុងអំឡុងពេលអភិវឌ្ឍន៍ ដើម្បីផ្តល់អាទិភាពដល់ផលិតផលដែលមានឥទ្ធិពលបំផុត និងប៉ះពាល់ខ្លាំងបំផុត។ គំរូគំរាមកំហែងពិចារណាករណីប្រើប្រាស់ជាក់លាក់របស់ផលិតផល និងអនុញ្ញាតឱ្យក្រុមអភិវឌ្ឍន៍ដើម្បីពង្រឹងផលិតផល។ ជាចុងក្រោយ ភាពជាអ្នកដឹកនាំជាន់ខ្ពស់គួរតែឱ្យក្រុមនានាទទួលខុសត្រូវចំពោះការផ្តត់ផ្តង់ផលិតផលដែលមានសន្តិសុខ ជាធាតុសំខាន់នៃឧត្តមភាព និងគុណភាពផលិតផល។

យុទ្ធសាស្ត្រសន្តិសុខតាមការរចនា

ក្របខ័ណ្ឌអភិវឌ្ឍន៍សូហ្វវែរដែលមានសន្តិសុខ (SSDF) ត្រូវបានគេស្គាល់ដែរថាវិទ្យាស្ថានស្តង់ដារ និងបច្ចេកវិទ្យាជាតិ (NIST) របស់ SP 800-218, គឺជាសំណុំស្នូលនៃការអនុវត្តការអភិវឌ្ឍន៍សូហ្វវែរដែលមានសន្តិសុខកម្រិតខ្ពស់ ដែលអាចដាក់បញ្ចូលទៅក្នុងដំណាក់កាលនីមួយៗនៃវដ្តអភិវឌ្ឍន៍សូហ្វវែរ (SDLC)។ ការអនុលោមតាមការអនុវត្តទាំងនេះ អាចជួយឱ្យអ្នកផលិតសូហ្វវែរកាន់តែអាចស្វែងរក និងលុបបំបាត់ភាពងាយរងគ្រោះប្រកបដោយប្រសិទ្ធភាពនៅក្នុងសូហ្វវែរដែលបានចេញផ្សាយ កាត់បន្ថយផលប៉ះពាល់ដែលអាចកើតមានពីការកេងប្រវ័ញ្ចភាពងាយរងគ្រោះ និងដោះស្រាយប្រភពដើមហេតុនៃភាពងាយរងគ្រោះ ដើម្បីការពារការកើតឡើងម្តងទៀតនាពេលអនាគត។

ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ លើកទឹកចិត្តឱ្យប្រើយុទ្ធសាស្ត្រសន្តិសុខតាមការរចនា រួមទាំងគោលការណ៍នានាដែលយោងលើការអនុវត្ត SSDF។ អ្នកផលិតសូហ្វវែរគួរតែបង្កើតផែនទីបង្ហាញផ្លូវដោលាយលក្ខណ៍អក្សរមួយ ដើម្បីទទួលយកការអនុវត្តការអភិវឌ្ឍន៍សូហ្វវែរសន្តិសុខតាមការរចនាបន្ថែមទៀតនៅទូទាំងផលប័ត្ររបស់ពួកគេ។ ខាងក្រោមនេះគឺ ជាការអនុវត្តល្អបំផុតនៃផែនទីបង្ហាញផ្លូវដែលមិនមែនជាបញ្ជីពេញលេញមួយ៖

- ភាសាសរសេរកម្មវិធីសុវត្ថិភាពអង្គចងចាំ (SSDF PW.6.1)៖ ផ្តល់អាទិភាពដល់ការប្រើប្រាស់ភាសាសុវត្ថិភាពអង្គចងចាំ កន្លែងណាដែលអាចធ្វើទៅបាន។ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ទទួលស្គាល់ថា ការកាត់បន្ថយជាក់លាក់នៃអង្គចងចាំផ្សេងទៀត ដូចជាចៃដន្យនីយកម្មប្លង់ចន្លោះទីតាំងអង្គចងចាំ (ASLR), ភាពសុចរិតនៃការគ្រប់គ្រងលំហូរ (CFI), និងការចាក់បញ្ចូលទិន្នន័យមិនត្រឹមត្រូវ គឺមានប្រយោជន៍សម្រាប់មូលដ្ឋានកូដចាស់ ប៉ុន្តែមិនគ្រប់គ្រាន់ដើម្បីចាត់ទុកថាជាសន្តិសុខតាមការរចនា ដោយសារតែវាមិនបានការពារការកេងប្រវ័ញ្ចឱ្យបានគ្រប់គ្រាន់។ ឧទាហរណ៍មួយចំនួននៃភាសាសុវត្ថិភាពអង្គចងចាំទំនើបរួមមាន C#, Rust, Ruby, Java, Go និង Swift។ សូមអានសន្លឹកព័ត៌មានសុវត្ថិភាពអង្គចងចាំរបស់ NSA សម្រាប់ព័ត៌មានបន្ថែម។
- មូលដ្ឋានផ្នែករឹងកុំព្យូទ័រដែលមានសន្តិសុខ៖ ដាក់បញ្ចូលនូវលក្ខណៈពិសេសៗផ្នែកស្ថាបត្យកម្ម ដែលអនុញ្ញាតឱ្យមានការការពារអង្គចងចាំល្អិតល្អន់ ដូចដែលបានពិពណ៌នាដោយការណែនាំអំពី RISC ដែលបង្កើនសមត្ថភាពផ្នែករឹង (CHERI) ដែលអាចពង្រីកការណែនាំ-កំណត់ស្ថាបត្យកម្មតាមប្រពៃណី (ISAs)។ សម្រាប់ព័ត៌មានបន្ថែម សូមចូលទៅកាន់គេហទំព័រ CHERI របស់សាកលវិទ្យាល័យ Cambridge។
- សមាសភាគសូហ្វវែរដែលមានសន្តិសុខ (SSDF PW 4.1)៖ ទទួលបាន និងថែរក្សាសមាសភាគសូហ្វវែរដែលមានសន្តិសុខល្អ (ឧទាហរណ៍ បណ្ណាល័យសូហ្វវែរ ម៉ូឌុល សូហ្វវែរភ្ជាប់គម្លាតរវាងកម្មវិធី និងប្រព័ន្ធប្រតិបត្តិការក្របខ័ណ្ឌ) ពីពាណិជ្ជកម្មដែលបានផ្ទៀងផ្ទាត់ ប្រភពបើកចំហ និងអ្នកអភិវឌ្ឍន៍ភាគីទីបីផ្សេងទៀត ដើម្បីធានាបាននូវសន្តិសុខដ៏រឹងមាំនៅក្នុងផលិតផលសូហ្វវែរសម្រាប់អ្នកប្រើប្រាស់។
- ក្របខ័ណ្ឌគំរូគេហទំព័រ (SSDF PW.5.1)៖ ប្រើក្របខ័ណ្ឌគំរូគេហទំព័រដែលអនុវត្តការគេចចេញដោយស្វ័យប្រវត្តិនៃការបញ្ចូលទិន្នន័យអ្នកប្រើប្រាស់ ដើម្បីជៀសវាងការវាយប្រហារតាមគេហទំព័រ ដូចជាការសរសេរស្គ្រីបឆ្លងគេហទំព័រជាដើម។
  បញ្ចោកទេសកំណត់សំណួរតួលេខ (SSDF PW 5.1)៖ ប្រើបញ្ចោកទេសកំណត់សំណួរតួលេខ ជាជាងដាក់បញ្ចូលទិន្នន័យអ្នកប្រើប្រាស់នៅក្នុងសំណួរតួលេខ ដើម្បីជៀសវាងការវាយប្រហារតាមរយៈការចាក់បញ្ចូល SQL។
- ការធ្វើតេស្តសន្តិសុខកម្មវិធីរកមើលកំហុស និងគោលដំហរមុខងារប្រព័ន្ធសូហ្វវែរ (SAST/DAST) (SSDF PW.7.2, PW.8.2)៖

  ប្រើឧបករណ៍ទាំងនេះដើម្បីវិភាគកូដប្រភពផលិតផល និងគោលដំហរកម្មវិធី ដើម្បីរកមើលការអនុវត្តដែលងាយមានកំហុស។ ឧបករណ៍ទាំងនេះគ្របដណ្តប់បញ្ហានានាចាប់ពីការគ្រប់គ្រងមិនត្រឹមត្រូវនៃអង្គចងចាំ រហូតដល់ការបង្កើតសំណួរមូលដ្ឋានទិន្នន័យដែលងាយមានកំហុស (ឧទាហរណ៍ ការបញ្ចូលទិន្នន័យអ្នកប្រើប្រាស់ដែលមិនបានគេចផុត ដែលនាំឱ្យមានការចាក់បញ្ចូល SQL)។ ឧបករណ៍ SAST និង DAST អាចត្រូវបានដាក់បញ្ចូលទៅក្នុងដំណើរការអភិវឌ្ឍន៍ ហើយដំណើរការដោយស្វ័យប្រវត្តិជាផ្នែកនៃការអភិវឌ្ឍន៍សូហ្វវែរ។ SAST

និង DAST គួរតែបំពេញបន្ថែមប្រភេទផ្សេងទៀតនៃការធ្វើតេស្ត ដូចជាការធ្វើតេស្តសមាសភាគ និងការធ្វើតេស្តរួមបញ្ចូលគ្នាដើម្បីធានាថាផលិតផលអនុលោមតាមតម្រូវការសន្តិសុខដែលរំពឹងទុក។ នៅពេលរកឃើញបញ្ហានានា អ្នកផលិតគួរតែធ្វើការវិភាគប្រភពដើមហេតុដើម្បីដោះស្រាយចំណុចខ្សោយជាប្រព័ន្ធ។

- ការពិនិត្យកូដ (SSDF PW.7.1, PW.7.2)៖ ខិតខំដើម្បីធានាថាលេខកូដដែលបានដាក់ចូលទៅក្នុងផលិតផល ឆ្លងកាត់ការពិនិត្យដោយអ្នកបង្កើតផ្សេងទៀត ដើម្បីធានាបាននូវគុណភាពកាន់តែខ្ពស់។
- សារពើភ័ណ្ឌមូលដ្ឋានកូដសូហ្វវែរពេញលេញ (SBOM) (SSDF PS.3.2, PW.4.1)៖ ដាក់បញ្ចូលការបង្កើតនៃ SBOM[3] ដើម្បីផ្តល់ភាពមើលឃើញទៅក្នុងសំណុំសូហ្វវែរដែលដាក់ចូលទៅក្នុងផលិតផល។
- កម្មវិធីលាតត្រដាងភាពងាយរងគ្រោះ (SSDF RV.1.3)៖ បង្កើតកម្មវិធីលាតត្រដាងភាពងាយរងគ្រោះ ដែលអនុញ្ញាតឱ្យអ្នកស្រាវជ្រាវផ្នែកសន្តិសុខរាយការណ៍ពីភាពងាយរងគ្រោះ ហើយទទួលបានជម្រកសុវត្ថិភាពស្របច្បាប់ក្នុងការធ្វើដូច្នេះ។ ជាផ្នែកនៃការនេះ អ្នកផ្គត់ផ្គង់គួរតែបង្កើតដំណើរការនានាដើម្បីកំណត់ប្រភពដើមហេតុនៃភាពងាយរងគ្រោះដែលបានរកឃើញ។ ដំណើរការបែបនេះគួរតែរួមបញ្ចូលការកំណត់ថាតើការទទួលយកការអនុវត្តសន្តិសុខតាមការចនាណាមួយនៅក្នុងឯកសារនេះ (ឬការអនុវត្តស្រដៀងគ្នាផ្សេងទៀត) នឹងរារាំងដល់ការណែនាំអំពីភាពងាយរងគ្រោះដែរឬទេ។
- ភាពពេញលេញនៃ CVE៖ ត្រូវប្រាកដថា CVEs ដែលបានបោះពុម្ពផ្សាយ ដាក់បញ្ចូលការរៀបរាប់ពីប្រភពដើមហេតុ ឬការវិភាគលើភាពទន់ខ្សោយទូទៅ (CWE) ដើម្បីជួយដល់ការវិភាគទូទាំងឧស្សាហកម្មពីប្រភពដើមហេតុសន្តិសុខសូហ្វវែរ។ ខណៈពេលដែលការធានាថារាល់ CVE គឺត្រឹមត្រូវ ហើយពេញលេញអាចចំណាយពេលបន្ថែមក្តី វាអនុញ្ញាតឱ្យអង្គភាពដែលមិនទាក់ទងគ្នា កត់សម្គាល់ឃើញនិន្នាការឧស្សាហកម្មដែលផ្តល់អត្ថប្រយោជន៍ដល់អ្នកផលិត និងអតិថិជនទាំងអស់។ សម្រាប់ព័ត៌មានបន្ថែមអំពីការគ្រប់គ្រងភាពងាយរងគ្រោះ សូមមើលការណែនាំអំពី SVCC ភាគីពាក់ព័ន្ធ-ជាក់លាក់របស់ CISA។
- ការការពារស៊ីជម្រៅ៖ រចនាហេដ្ឋារចនាសម្ព័ន្ធ ដើម្បីឱ្យការសម្របសម្រួលនៃការគ្រប់គ្រងសន្តិសុខតែមួយ មិនបណ្តាលឱ្យមានការសម្របសម្រួលដល់ប្រព័ន្ធទាំងមូល។ ជាឧទាហរណ៍ ការធានាថាឯកសិទ្ធិអ្នកប្រើប្រាស់ត្រូវបានផ្តល់ជូនយ៉ាងតូចចង្អៀត ហើយបញ្ជីត្រួតពិនិត្យការចូលប្រើដែលបានអនុវត្ត អាចកាត់បន្ថយផលប៉ះពាល់នៃគណនីដែលត្រូវបានសម្របសម្រួល។ ដូចគ្នានេះផងដែរ បច្ចេកទេសទប់បាំងការពារសន្តិសុខសូហ្វវែរដោយបារខ្សាច់ (sandboxing) អាចដាក់ភាពងាយរងគ្រោះនៅដាច់ដោយឡែក ដើម្បីដាក់ដែនកំណត់ការសម្របសម្រួលនៃកម្មវិធីទាំងមូល។
- បំពេញគោលដៅប្រតិបត្តិការតាមអ៊ីនធឺណិត (CPGs)៖ រចនាផលិតផលដែលបំពេញតាមការអនុវត្តសន្តិសុខជាមូលដ្ឋាន។ គោលដៅប្រតិបត្តិការសន្តិសុខតាមអ៊ីនធឺណិតរបស់ CISA គួសបញ្ជាក់អំពីវិធានការសន្តិសុខតាមអ៊ីនធឺណិតខ្សែបន្ទាត់គោលជាមូលដ្ឋានដែលអង្គភាពនានាគួរតែអនុវត្ត។ លើសពីនេះទៀត សម្រាប់វិធីជាច្រើនទៀតដើម្បីពង្រឹងគោលជំហរស្ថាប័នរបស់អ្នក សូមមើលក្របខ័ណ្ឌការវាយតម្លៃសន្តិសុខអ៊ីនធឺណិតរបស់ចក្រភពអង់គ្លេស ដែលចែករំលែកពីភាពស្រដៀងគ្នាចំពោះ CPGs របស់ CISA។ ប្រសិនបើអ្នកផលិតបរាជ័យក្នុងការបំពេញតាម CPGs - ដូចជាមិនតម្រូវឱ្យមានការផ្ទៀងផ្ទាត់ពហុកត្តាដែលធន់នឹងការបោកបញ្ឆោតតាមអ៊ីមែលសម្រាប់បុគ្គលិកទាំងអស់ - នោះពួកគេមិនអាចត្រូវបានគេចាត់ទុកថាផ្តល់ផលិតផលដែលមានសន្តិសុខតាមការចនានោះទេ។

[3] ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យមួយចំនួន កំពុងស្វែងរកវិធីសាស្ត្រជំនួសនានា ដើម្បីទទួលបានការធានាសន្តិសុខជុំវិញខ្សែសង្វាក់ផ្គត់ផ្គង់សូហ្វវែរ។

ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ទទួលស្គាល់ថា ការផ្លាស់ប្តូរទាំងនេះគឺជាការផ្លាស់ប្តូរដ៏សំខាន់នៅក្នុងគោលជំហររបស់ស្ថាប័ន។ ដូចនេះ ការណែនាំរបស់ពួកគេគួរតែបានផ្តល់អាទិភាពដោយផ្អែកលើភាពធ្ងន់ធ្ងរ ភាពស្មុគស្មាញ និងផលប៉ះពាល់អាជីវកម្ម។ ការអនុវត្តទាំងនេះអាចត្រូវបាន ណែនាំសម្រាប់សូហ្វវែរថ្មី ហើយពង្រីកជាលំដាប់ដើម្បីគ្របដណ្តប់ករណីប្រើប្រាស់ និងផលិតផលបន្ថែម។ ក្នុងករណីមួយចំនួន ភាពធ្ងន់ធ្ងរ និងគោល ជំហរហានិភ័យនៃផលិតផលជាក់លាក់មួយ អាចមានភាពល្អសមត្រូវនឹងកាលវិភាគដែលបានពន្លឿនដើម្បីទទួលយកការអនុវត្តទាំងនេះ។ ក្នុងករណីផ្សេងទៀត ការអនុវត្តនានាអាចត្រូវបានណែនាំទៅក្នុងមូលដ្ឋានកូដចាស់ ហើយត្រូវបានកែបំបាត់តាមពេលវេលា។

យុទ្ធសាស្ត្រសន្តិសុខតាមលំនាំដើម

បន្ថែមពីលើការទទួលយកការប្រតិបត្តិការអភិវឌ្ឍន៍សន្តិសុខតាមការរចនា ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំអ្នកផលិតសូហ្វវែរឱ្យផ្តល់អាទិភាពលើការកំណត់រចនាសម្ព័ន្ធសន្តិសុខតាមលំនាំដើមនៅក្នុងផលិតផលរបស់ពួកគេ។ ទាំងនេះគួរតែខិតខំធ្វើបច្ចុប្បន្នភាពផលិតផលដើម្បីអនុលោមតាមការអនុវត្តទាំងនេះ នៅពេលត្រូវបានធ្វើឱ្យទាន់បច្ចុប្បន្នភាពឡើងវិញ។ ឧទាហរណ៍៖

- លុបបំបាត់ពាក្យសម្ងាត់ដើម៖ មិនគួរជាក់ភ្ជាប់ផលិតផលមកជាមួយពាក្យសម្ងាត់ដើម ដែលត្រូវបានចែករំលែកជាសកលនោះទេ។ ដើម្បីលុបបំបាត់ពាក្យសម្ងាត់ដើម ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំផលិតផលដែលតម្រូវឱ្យអ្នកគ្រប់គ្រងកំណត់ពាក្យ សម្ងាត់រឹងមាំក្នុងអំឡុងពេលដំឡើងកម្មវិធី និងកំណត់រចនាសម្ព័ន្ធ។
    - ការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវពហុកត្តាជាកាតព្វកិច្ច (MFA) សម្រាប់អ្នកប្រើប្រាស់ដែលមានឯកសិទ្ធិ។ យើងសង្កេតឃើញថាការប្រើប្រាស់របស់សហគ្រាសជាច្រើន ត្រូវបានគ្រប់គ្រងដោយអ្នកគ្រប់គ្រងដែលមិនបានការពារគណនីរបស់ពួកគេជាមួយ MFA។ ដោយសារអ្នកគ្រប់គ្រងគឺជាគោលដៅមានតម្លៃខ្ពស់ ផលិតផលគួរតែធ្វើឱ្យ MFA ជាការជ្រើសយកការមិនចូលរួមជាជាងជ្រើសយកការចូលរួម ។ លើសពីនេះ ប្រព័ន្ធគួរតែរម្លឹកអ្នកគ្រប់គ្រងឱ្យបានទៀងទាត់ដើម្បីចុះឈ្មោះក្នុង MFA រហូតដល់ពួកគេបានបើកដំណើរការវាដោយជោគជ័យនៅលើគណនីរបស់ពួកគេ។ NCSC របស់ប្រទេសហូឡង់ មានការណែនាំដែលស្របទៅនឹងការណែនាំរបស់ CISA។ សូមមើលសន្លឹកព័ត៌មានការផ្ទៀងផ្ទាត់ពេញលក្ខណៈរបស់ពួកគេសម្រាប់ព័ត៌មានបន្ថែម។
- ការចុះឈ្មោះចូលតែមួយ (SSO)៖ កម្មវិធី IT គួរតែអនុវត្តការចុះឈ្មោះចូលតែមួយលើបច្ចេកវិទ្យា តាមរយៈស្តង់ដារបើកចំហទំនើបនានា។ ឧទាហរណ៍រួមមាន ភាសាសម្គាល់ការអះអាងសុវត្ថិភាព (SAML) ឬ ការតភ្ជាប់អត្តសញ្ញាណបើកចំហ (ODC) ។ សមត្ថភាពនេះគួរតែធ្វើឱ្យមានមកស្រាប់ដោយមិនគិតថ្លៃបន្ថែម។
- ការបើកចូលដោយសុវត្ថិភាព៖ ផ្តល់កំណត់ហេតុពិនិត្យបញ្ជាក់ដែលមានគុណភាពខ្ពស់ ដល់អតិថិជនដោយមិនគិតថ្លៃបន្ថែម។ កំណត់ហេតុពិនិត្យបញ្ជាក់មានសារៈសំខាន់សម្រាប់ការស៊ើបរក និងបង្កើនឧប្បត្តិហេតុសន្តិសុខដែលអាចកើតមាន។ កំណត់ហេតុពិនិត្យបញ្ជាក់ទាំងនេះក៏មានសារៈសំខាន់ផងដែរ ក្នុងអំឡុងពេលស៊ើបអង្កេតលើឧប្បត្តិហេតុសន្តិសុខដែលបានសង្ស័យ ឬបញ្ជាក់។ សូមពិចារណាលើការអនុវត្តល្អបំផុតនានា ដូចជាការផ្តល់នូវការរួមបញ្ចូលដ៏ងាយស្រួលជាមួយនឹងប្រព័ន្ធព័ត៌មានសន្តិសុខ និងការគ្រប់គ្រងព្រឹត្តិការណ៍ (SIEM) ជាមួយនឹងគំរូផ្តល់និងទទួលព័ត៌មានអំពីការសរសេរកម្មវិធី (API) ដែលប្រើពេលវេលាសកលដែលបានសម្របសម្រួល (UTC), ការផ្លាស់ប្តូរទម្រង់នៃពេលវេលាតាមតំបន់លក្ខណៈស្តង់ដារ និងបច្ចេកទេសគ្រប់គ្រងឯកសារដ៏រឹងមាំ។
- សូហ្វវែរកម្រងព័ត៌មានដែលមានការអនុញ្ញាត៖ អ្នកផ្តត់ផ្តង់សូហ្វវែរគួរតែផ្តល់អនុសាសន៍អំពីតួនាទីកម្រងព័ត៌មានដែលមានការអនុញ្ញាត

និងករណីប្រើប្រាស់ដែលបានកំណត់របស់ពួកគេ។ អ្នកផលិតគួរតែរួមបញ្ចូលការព្រមានដែលអាចមើលឃើញ ដែលជូនដំណឹងដល់អតិថិជនអំពីការកើនឡើងនៃហានិភ័យ ប្រសិនបើពួកគេងាកចេញពីកម្រងព័ត៌មានដែលមានការអនុញ្ញាតដូចបានណែនាំ។ ជាឧទាហរណ៍៖ គ្រូពេទ្យអាចមើលកំណត់ត្រាអ្នកជំងឺទាំងអស់បាន ប៉ុន្តែអ្នករៀបចំកាលវិភាគវេជ្ជសាស្ត្រ មានការចូលប្រើបាស់ដោយមានកម្រិតក្នុងការមើលព័ត៌មានអាសយដ្ឋានដែលត្រូវការសម្រាប់ការរៀបចំពេលវេលាណាត់ជួប។

- សន្តិសុខអន្តរប្រតិបត្តិការរវាងប្រព័ន្ធទំនើប និងប្រព័ន្ធចាស់ដែលស៊ីសង្វាក់គ្នា៖ ជាញឹកញាប់ណាស់ លក្ខណៈពិសេសៗនៃប្រព័ន្ធចាស់ដែលស៊ីសង្វាក់គ្នាត្រូវបានដាក់បញ្ចូល ហើយជារឿយៗត្រូវបានបើកដំណើរការនៅក្នុងផលិតផល ទោះបីជាបង្កហានិភ័យដល់សន្តិសុខផលិតផលក៏ដោយ។ កំណត់សន្តិសុខប្រព័ន្ធចាស់ដែលស៊ីសង្វាក់គ្នាជាអាទិភាព ផ្តល់សិទ្ធិអំណាចដល់ក្រុមសន្តិសុខដើម្បីដកចេញនូវលក្ខណៈពិសេសដែលគ្មានសន្តិសុខ បើទោះបីជាវាមានន័យជាការបង្កឱ្យមានការផ្លាស់ប្តូរដែលនាំឱ្យមានការខូចក៏ដោយ។
- តាមដាន និងកាត់បន្ថយទំហំ "គោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ"៖ កាត់បន្ថយទំហំ "គោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ" ដែលផលិតសម្រាប់ផលិតផល ហើយខិតខំដើម្បីជានាថាទំហំនឹងរួមតូចតាមពេលវេលា នៅពេលដែលកំណែថ្មីនៃសូហ្វវែរត្រូវបានចេញផ្សាយ។ រួមបញ្ចូលសមាសធាតុនៃ "គោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ" ជាការកំណត់រចនាសម្ព័ន្ធដើមនៃផលិតផល។ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យទទួលស្គាល់ថា គោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធដែលរួមតូច កើតចេញពីភាពជាដៃគូបន្តជាមួយអតិថិជនដែលមានស្រាប់ ហើយរួមបញ្ចូលការខិតខំប្រឹងប្រែងដោយក្រុមផលិតផលជាច្រើន រួមទាំងបទពិសោធន៍អ្នកប្រើប្រាស់ (UX) ផងដែរ។
- ពិចារណាលើផលវិបាកបទពិសោធន៍អ្នកប្រើប្រាស់នៃការកំណត់សន្តិសុខ៖ ការកំណត់ថ្មីនីមួយៗ បង្កើនបន្ទុកនៃការយល់ដឹងលើអ្នកប្រើប្រាស់ចុងក្រោយ ហើយគួរតែបានវាយតម្លៃរួមជាមួយនឹងអត្ថប្រយោជន៍អាជីវកម្មដែលទទួលបាន។ ជាការប្រសើរបំផុត ការកំណត់មិនគួរឱ្យមានទេ។ ជាជំនួសវិញ ការកំណត់សន្តិសុខបំផុតគួរតែបានដាក់បញ្ចូលទៅក្នុងផលិតផលដើម។ ពេលណាការកំណត់រចនាសម្ព័ន្ធមានភាពចាំបាច់ ជម្រើសដើមគួរតែមានសន្តិសុខយ៉ាងទូលំទូលាយប្រឆាំងនឹងការគំរាមកំហែងទូទៅ។

ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ទទួលស្គាល់ថា ការផ្លាស់ប្តូរទាំងនេះអាចមានផលប៉ះពាល់ផ្នែកប្រតិបត្តិការលើរបៀបដែលសូហ្វវែរត្រូវបានប្រើប្រាស់។ ដូច្នេះហើយ ការបញ្ចូលទិន្នន័យរបស់អតិថិជនមានសារៈសំខាន់ក្នុងការធ្វើឱ្យមានតុល្យភាពលើការពិចារណាផ្នែកប្រតិបត្តិការ និងសន្តិសុខ។ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ជឿថា ការបង្កើតផែនទីបង្ហាញផ្លូវដោលាយលក្ខណ៍អក្សរ និងការគាំទ្រផ្នែកប្រតិបត្តិដែលផ្តល់អាទិភាពដល់គំនិតទាំងនេះទៅក្នុងផលិតផលដ៏សំខាន់បំផុតរបស់ស្ថាប័ន គឺជាជំហានដំបូងដើម្បីផ្លាស់ប្តូរឆ្ពោះទៅរកការអនុវត្តការអភិវឌ្ឍន៍សូហ្វវែរដែលមានសន្តិសុខ។ ខណៈពេលដែលការបញ្ចូលទិន្នន័យរបស់អតិថិជនមានសារៈសំខាន់ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យបានសង្កេតឃើញករណីសំខាន់ៗដែលអតិថិជនមិនមានបំណង ឬមិនអាចទទួលយកស្តង់ដារដែលបានកែលម្អ ជាញឹកញាប់គឺពិធីការបណ្តាញ។ វាមានសារៈសំខាន់សម្រាប់អ្នកផលិត ក្នុងការបង្កើតការលើកទឹកចិត្តដ៏មានអត្ថន័យសម្រាប់អតិថិជនដើម្បីរក្សាបច្ចុប្បន្នភាព ហើយមិនអនុញ្ញាតឱ្យពួកគេនៅតែទទួលភាពងាយរងគ្រោះដោយគ្មានកំណត់នោះទេ។

គោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ ទល់នឹងការបន្ទរបន្តយ

គោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធអាចបណ្តាលមកពីកង្វះនៃការគ្រប់គ្រងសន្តិសុខលិតផល ដែលត្រូវបានបង្កប់ទៅក្នុងស្ថាបត្យកម្មរបស់ផលិតផលចាប់តាំងពីការចាប់ផ្តើមនៃការអភិវឌ្ឍន៍។ អាស្រ័យហេតុនេះ គោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធក៏អាចជាផែនទីបង្ហាញផ្លូវសម្រាប់សត្រូវផងដែរក្នុងការចង្អុលបង្ហាញ និងទាញយកប្រយោជន៍ពីលក្ខណៈពិសេសៗដែលគ្មានសន្តិសុខ។ វាជារឿងធម្មតាទេសម្រាប់ស្ថាប័នជាច្រើនដែលមិនដឹងពីគោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធ ដូច្នេះពួកគេក៏ទុកចោលការកំណត់រចនាសម្ព័ន្ធឧបករណ៍របស់ពួកគេ ក្នុងស្ថានភាពមួយដែលគ្មានសន្តិសុខ។ គំរូដាក់បញ្ច្រាសដែលគេស្គាល់ថាជាគោលការណ៍ណែនាំស្តីពីការបន្ទរបន្តយ គួរតែជំនួសគោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធបែបនេះ ហើយពន្យល់ថាតើការផ្លាស់ប្តូរណាមួយដែលអ្នកប្រើប្រាស់គួរធ្វើខណៈពេលកំពុងរាយបញ្ជីដែលកើតអំពីហានិភ័យសន្តិសុខផងដែរ។

ជាជាងបង្កើតគោលការណ៍ណែនាំស្តីពីការពង្រឹងប្រព័ន្ធដែលរាយបញ្ជីវិធីសាស្ត្រនានាសម្រាប់ការធានាផលិតផល ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យណែនាំអ្នកផលិតសូហ្វវែរ ឱ្យផ្លាស់ប្តូរទៅវិធីសាស្ត្រសន្តិសុខតាមលំនាំដើមដោយផ្តល់នូវគោលការណ៍ណែនាំស្តីពីការបន្ទរបន្តយវិញ។ គោលការណ៍ណែនាំទាំងនេះ ពន្យល់ពីហានិភ័យអាជីវកម្មស្តីពីសេចក្តីសម្រេចជាភាសាសាមញ្ញដែលអាចយល់បាន និងអាចបង្កើនការយល់ដឹងពីអង្គភាពនានា អំពីហានិភ័យនៃការ ព្យាបាទតាមអ៊ីនធឺណិតដោយគំនិតទុច្ចរិត។ ការដោះដូរផ្នែកសុវត្ថិភាពគួរតែបានកំណត់ដោយនាយកប្រតិបត្តិជាន់ខ្ពស់របស់អតិថិជន ដោយធ្វើឱ្យមានតុល្យភាពសន្តិសុខជាមួយនឹងតម្រូវការអាជីវកម្មផ្សេងទៀត។

អនុសាសន៍សម្រាប់អតិថិជន

ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ ណែនាំអង្គភាពនានាឱ្យអ្នកផលិតបច្ចេកវិទ្យារបស់ពួកគេដែលផ្តត់ផ្តង់ផលិតផល ទទួលខុសត្រូវចំពោះលទ្ធផលសន្តិសុខនៃផលិតផលរបស់ពួកគេ។ ជាផ្នែកមួយនៃចំណុចនេះ ទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ បានណែនាំថា នាយកប្រតិបត្តិរបស់អង្គភាព ផ្តល់អាទិភាពដល់សារៈសំខាន់នៃការទិញផលិតផលដែលមានសន្តិសុខតាមការរចនា និងផលិតផលដែលមានសន្តិសុខតាមលំនាំដើម។ ការធ្វើបែបនេះអាចបង្ហាញឱ្យឃើញតាមរយៈការបង្កើតគោលនយោបាយដែលតម្រូវឱ្យការិយាល័យទទួលបន្ទុកផ្នែក IT វាយតម្លៃសន្តិសុខអ្នកផលិតសូហ្វវែរ មុនពេលទិញវា ក៏ដូចជាការផ្តល់សិទ្ធិអំណាចក្តារិយាល័យទទួលបន្ទុកផ្នែក IT រុញត្រឡប់មកវិញប្រសិនបើចាំបាច់។ ការិយាល័យទទួលបន្ទុកផ្នែក IT គួរតែបានផ្តល់សិទ្ធិអំណាចក្នុងការអភិវឌ្ឍន៍លក្ខណៈវិនិច្ឆ័យ ការទិញដែលសង្កត់ធ្ងន់លើសារៈសំខាន់នៃការអនុវត្តសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម (ដែលចំណុចទាំងពីរនោះត្រូវបានគូសបញ្ជាក់នៅក្នុងឯកសារនេះ និងឯកសារផ្សេងទៀតដែលបានបង្កើតឡើងដោយអង្គភាព)។ លើសពីនេះ ការិយាល័យទទួលបន្ទុកផ្នែក IT គួរតែបានគាំទ្រដោយអ្នកគ្រប់គ្រងប្រតិបត្តិ នៅពេលអនុវត្តលក្ខណៈវិនិច្ឆ័យទាំងនេះក្នុងការសម្រេចចិត្តទិញ។ ការសម្រេចចិត្តរបស់អង្គភាពដើម្បីទទួលយកហានិភ័យទាក់ទងនឹងផលិតផលបច្ចេកវិទ្យាជាក់លាក់ គួរតែបានចងក្រងជាឯកសារផ្លូវការដែលអនុម័តដោយនាយកប្រតិបត្តិអាជីវកម្មជាន់ខ្ពស់ ហើយបង្ហាញជាទៀងទាត់ទៅកាន់ក្រុមប្រឹក្សាភិបាល។

សេវាកម្ម IT សំខាន់ៗរបស់សហគ្រាស ដែលគាំទ្រគោលដំហរសន្តិសុខរបស់អង្គភាព ដូចជាបណ្តាញសហគ្រាស អត្តសញ្ញាណសហគ្រាស និងការគ្រប់គ្រងការចូលប្រើប្រាស់ ហើយនិងប្រតិបត្តិការសន្តិសុខ និងសមត្ថភាពឆ្លើយតប គួរតែត្រូវបានគេមើលឃើញថាជាមុខងារអាជីវកម្មដ៏សំខាន់ដែលត្រូវបានផ្តល់មូលនិធិដើម្បីកែតម្រូវឱ្យស្របនឹងសារៈសំខាន់របស់ពួកគេ ចំពោះភាពជោគជ័យនៃបេសកកម្មរបស់អង្គភាព។ អង្គភាពនានាគួរតែបង្កើតផែនការមួយដើម្បីបង្កើនសមត្ថភាពទាំងនេះ ក្នុងការជំរុញអ្នកផលិតដែលទទួលយកការអនុវត្តសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម។

កន្លែងណាដែលអាចធ្វើទៅបាន អង្គភាពនានាគួរតែខិតខំបង្កើតទំនាក់ទំនងភាពជាដៃគូជាយុទ្ធសាស្ត្រ ជាមួយអ្នកផ្គត់ផ្គង់ IT សំខាន់ៗរបស់ពួកគេ។ ទំនាក់ទំនងបែបនេះ រួមមានការជឿទុកចិត្តនៅកម្រិតជាច្រើននៃអង្គភាព ហើយផ្តល់ជាយានជំនិះដើម្បីដោះស្រាយបញ្ហា និងកំណត់អាទិភាពរួមគ្នា។ សន្តិសុខគួរតែជាធាតុសំខាន់នៃទំនាក់ទំនងបែបនេះ ហើយអង្គភាពគួរតែខិតខំពង្រឹងសារៈសំខាន់នៃការអនុវត្តសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម ទាំងទម្រង់ផ្លូវការ (ឧទាហរណ៍ កិច្ចសន្យា ឬកិច្ចព្រមព្រៀងអ្នកលក់) និងទម្រង់ក្រៅផ្លូវការនៃទំនាក់ទំនងនេះ។ អង្គភាពនានាគួរតែរំពឹងថានឹងមានតម្លាភាពពីអ្នកផ្គត់ផ្គង់បច្ចេកវិទ្យារបស់ពួកគេ អំពីគោលជំហរគ្រប់គ្រងផ្ទៃក្នុងរបស់ពួកគេ ក៏ដូចជាផែនទីបង្ហាញផ្លូវរបស់ពួកគេឆ្ពោះទៅរកការចាប់យកការអនុវត្តសន្តិសុខតាមការរចនា និងសន្តិសុខតាមលំនាំដើម។

បន្ថែមពីលើការធ្វើឱ្យសន្តិសុខតាមលំនាំដើមជាអាទិភាពនៅក្នុងអង្គភាព អ្នកដឹកនាំផ្នែកព័ត៌មានវិទ្យាគួរសហការជាមួយដៃគូក្នុងឧស្សាហកម្មរបស់ពួកគេ ដើម្បីយល់ដឹងថាតើផលិតផល និងសេវាកម្មណាដែលល្អបំផុត ដែលតំណាងឱ្យគោលការណ៍រចនាទាំងនេះ។ អ្នកដឹកនាំទាំងនេះគួរតែសម្របសម្រួលសំណើរបស់ពួកគេ ដើម្បីជួយអ្នកផលិតក្នុងការកំណត់អាទិភាពគំនិតផ្តួចផ្តើមសន្តិសុខនាពេលខាងមុខរបស់ពួកគេ។ ដោយការធ្វើការរួមគ្នា អតិថិជនអាចជួយផ្តល់នូវធាតុចូលដ៏មានអត្ថន័យដល់អ្នកផលិត និងបង្កើតការលើកទឹកចិត្តសម្រាប់ពួកគេក្នុងការកំណត់អាទិភាពសន្តិសុខ។

នៅពេលប្រើប្រាស់ប្រព័ន្ធ cloud (ក្លៅ) អង្គភាពនានាគួរតែជានាថាពួកគេយល់ដឹងអំពីគំរូទំនួលខុសត្រូវរួមគ្នា ជាមួយអ្នកផ្គត់ផ្គង់បច្ចេកវិទ្យារបស់ពួកគេ ដែលមានន័យថាអង្គភាពគួរតែមានភាពច្បាស់លាស់លើទំនួលខុសត្រូវផ្នែកសន្តិសុខរបស់អ្នកផ្គត់ផ្គង់ ជាជាងទំនួលខុសត្រូវរបស់អតិថិជន។ អង្គភាពគួរតែផ្តល់អាទិភាពដល់អ្នកផ្តល់សេវាកម្មក្លៅដែលមានតម្លាភាពអំពីគោលជំហរសន្តិសុខ ការគ្រប់គ្រងផ្ទៃក្នុង និងសមត្ថភាពក្នុងបំពេញកាតព្វកិច្ចរបស់ពួកគេក្រោមគំរូទំនួលខុសត្រូវរួមគ្នា។

ការបដិសេធ

ព័ត៌មាននៅក្នុងរបាយការណ៍នេះកំពុងត្រូវបានផ្តល់ជូន " ក្នុងស្ថានភាពបច្ចុប្បន្ន" សម្រាប់គោលបំណងជាព័ត៌មានតែប៉ុណ្ណោះ។ CISA និងទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យ មិនគាំទ្រផលិតផល ឬសេវាកម្មពាណិជ្ជកម្មណាមួយ រួមទាំងស្ថិតក្រោមការវិភាគណាមួយឡើយ។ រាល់ការយោងទៅអង្គភាពពាណិជ្ជកម្មជាក់លាក់ ឬផលិតផលពាណិជ្ជកម្ម ដំណើរការ ឬសេវាកម្មដោយផ្លាកសញ្ញាសេវាកម្ម សញ្ញាពាណិជ្ជកម្ម អ្នកផលិត ឬផ្សេងពីនេះ មិនបង្កើត ឬបញ្ជាក់ពីការយល់ព្រម ការណែនាំ ឬការអនុគ្រោះនិយមដោយ CISA និងទីភ្នាក់ងារបង្កើតកម្មវិធី និងមូលដ្ឋានទិន្នន័យនោះទេ។ ឯកសារនេះគឺជាការផ្តួចផ្តើមរួមគ្នាដោយ CISA ដែលមិនបំពេញមុខការដោយស្វ័យប្រវត្តិជាឯកសារបទប្បញ្ញត្តិនោះទេ។

ធនធាន

CISA

- ការណែនាំ SBOM របស់ CISA
- គោលដៅអនុវត្តសន្តិសុខអ៊ីនធឺណិតឆ្លងវិស័យរបស់ CISA
- គោលការណ៍ណែនាំស្តីពីអន្តរប្រតិបត្តិការបច្ចេកវិទ្យា
- ការការពារប្រឆាំងនឹងការវាយប្រហារខ្សែសង្វាក់ផ្គត់ផ្គង់សូហ្វវែររបស់ CISA និង NIST
- តម្លៃ នៃបច្ចេកវិទ្យាដែលមិនមានសុវត្ថិភាព និងអ្វីដែលយើងអាចធ្វើបានអំពីរឿងនេះ | CISA
- បញ្ឈប់ការឆ្លងកាត់ការខាតបង់លើសន្តិសុខអ៊ីនធឺណិត៖ ហេតុអ្វីបានជាក្រុមហ៊ុននានាត្រូវបង្កើតសុវត្ថិភាពទៅក្នុងផលិតផលបច្ចេកវិទ្យា (foreignaffairs.com)

- ការណែនាំអំពីប្រភេទភាពងាយរងគ្រោះរបស់ភាគីពាក់ព័ន្ធដាក់លាក់ (SSVC) របស់ CISA
- សន្លឹកព័ត៌មាន MFA ដែលធន់នឹងការបោកបញ្ឆោតតាមអ៊ីមែលរបស់ CISA
- ការណែនាំតាមអ៊ីនធឺណិតសម្រាប់អាជីវកម្មខ្នាតតូច | CISA NSA

NSA

- សន្លឹកព័ត៌មានសន្តិសុខអ៊ីនធឺណិតរបស់ NSA ស្តីពីស្ថេរភាពនៃអង្គចងចាំ
- ការធានាខ្សែសង្វាក់ផ្គត់ផ្គង់សូហ្វវែរ ESF៖ ការអនុវត្តល្អបំផុតសម្រាប់អ្នកផ្គត់ផ្គង់ FBI របស់ NSA

FBI

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

វិទ្យាស្ថានស្តង់ដារ និងបច្ចេកវិទ្យាជាតិ (NIST)

- គោលការណ៍ណែនាំអំពីអត្តសញ្ញាណឌីជីថលរបស់ NIST
- ក្របខ័ណ្ឌសន្តិសុខអ៊ីនធឺណិតរបស់ NIST
- ក្របខ័ណ្ឌអភិវឌ្ឍន៍សន្តិសុខសូហ្វវែររបស់ NIST (SSDF)

មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតអូស្ត្រាលី (ACSC)

- គោលការណ៍ណែនាំច្បាប់ប្រតិបត្តិ IoT សម្រាប់អ្នកផលិតរបស់ ACSC

មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ចក្រភពអង់គ្លេស (UK)

- ក្របខ័ណ្ឌការវាយតម្លៃអ៊ីនធឺណិតរបស់ចក្រភពអង់គ្លេស
- ការណែនាំអំពីការអភិវឌ្ឍន៍ និងការដាក់ប្រើប្រាស់ប្រកបដោយសន្តិសុខរបស់ NCSC ចក្រភពអង់គ្លេស
- ការណែនាំអំពីការគ្រប់គ្រងភាពងាយរងគ្រោះរបស់ NCSC ចក្រភពអង់គ្លេស
- ប្រអប់ឧបករណ៍ការលាតត្រដាងភាពងាយរងគ្រោះរបស់ NCSC ចក្រភពអង់គ្លេស
- CHERI របស់សាកលវិទ្យាល័យ Cambridge
- លាហើយចាំជួបគ្នាទៀត សូមអរគុណគ្រប់ដំបូន្មានតិចតួច - NCSC.GOV.UK

មជ្ឈមណ្ឌលកាណាដាសម្រាប់សន្តិសុខអ៊ីនធឺណិត (CCS)

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

ការិយាល័យសហព័ន្ធសម្រាប់សន្តិសុខព័ត៌មាន (BSI) របស់អាល្លឺម៉ង់

- សេចក្តីយោង BSI Grundschutz (ម៉ូឌុល CON.8)
- ស្តង់ដារអន្តរជាតិ IEC 62443 ផ្នែកទី 4-1
- របាយការណ៍ស្តីពីស្ថានភាពសន្តិសុខ IT នៅអាល្លឺម៉ង់ ឆ្នាំ 2022
- ការអនុវត្តន៍ BSI នៃសន្តិសុខកម្មវិធីគេហទំព័រ

មជ្ឈមណ្ឌលសន្តិសុខអ៊ីនធឺណិតជាតិរបស់ហូឡង់

- សន្លឹកព័ត៌មានស្តីពីការផ្ទៀងផ្ទាត់ភាពពេញលក្ខណៈរបស់ NCSC-NL

ផ្សេងទៀត

- របៀបដែលប្រព័ន្ធស្មុគស្មាញបរាជ័យ
- ទិដ្ឋភាពថ្មីនៅក្នុងការបរាជ័យនៃប្រព័ន្ធស្មុគស្មាញ