



ព្រះរាជាណាចក្រកម្ពុជា
ជាតិ សាសនា ព្រះមហាក្សត្រ

អង្គភាពសវនកម្មផ្ទៃក្នុង
នាយកដ្ឋានកិច្ចការទូទៅ

លេខ៖ អ.ជ.ក.

កំណត់បង្ហាញ

សូមគោរពជូន

ឯកឧត្តមប្រធានអង្គភាពសវនកម្មផ្ទៃក្នុង

ការសម្រេច
របស់ឯកឧត្តមប្រធានអង្គភាព

កម្មវត្ថុ៖ ការស្នើសុំផ្តល់តម្រូវការបច្ចេកទេសសម្រាប់ការរៀបចំមជ្ឈមណ្ឌលប្រតិបត្តិការសន្តិសុខបច្ចេកវិទ្យាព័ត៌មានរួមសម្រាប់ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ (MEF Security Operation Center - SOC)

យោង៖ លិខិតលេខ ៤៦៦៧ សហវ.ល.ស ចុះថ្ងៃទី២ ខែឧសភា ឆ្នាំ២០២៤។

សេចក្តីដូចមានចែងក្នុងកម្មវត្ថុ និងយោងខាងលើខ្ញុំសូមគោរពជម្រាបជូន **ឯកឧត្តមប្រធាន** មេត្តាជ្រាបដ៏ខ្ពង់ខ្ពស់ថា ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ (ក.ស.ហ.វ.) បានស្នើសុំផ្តល់តម្រូវការបច្ចេកទេសសម្រាប់ការរៀបចំ មជ្ឈមណ្ឌលប្រតិបត្តិការសន្តិសុខបច្ចេកវិទ្យាព័ត៌មានរួមសម្រាប់ក្រសួងសេដ្ឋកិច្ចនិងហិរញ្ញវត្ថុ (MEF Security Operation Center - SOC) ។

មជ្ឈមណ្ឌលប្រតិបត្តិការសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន (Security Operation Center - SOC) ជាប្រព័ន្ធព័ត៌មានវិទ្យាដែលតំឡើងដើម្បីធ្វើការត្រួតពិនិត្យសន្តិសុខបណ្តាញណេតវើក, ទូរស័ព្ទវៃឆ្លាត (smart phone), បច្ចេកវិទ្យាក្លោង (cloud computing), អ៊ីនធឺណិតនៃបរិក្ខារ (internet of things), ហេដ្ឋារចនាសម្ព័ន្ធខ្ទីរឌីជីថល, ប្រព័ន្ធទូទាត់សងប្រាក់អេឡិចត្រូនិក (e-payment), ប្រព័ន្ធបច្ចេកវិទ្យាឡូជីស្តិក, ថ្នាលឌីជីថល (platform), អត្តសញ្ញាណបណ្ណឌីជីថល, សុវត្ថិភាពទិន្នន័យ, សិទ្ធិឯកជននៃទិន្នន័យ, និងសន្តិសុខតាមប្រព័ន្ធអ៊ីនធឺណេត មជ្ឈមណ្ឌលប្រតិបត្តិការសន្តិសុខបច្ចេកវិទ្យាព័ត៌មានត្រូវបានប្រើប្រាស់ដោយ បណ្តាគ្រឹះស្ថានហិរញ្ញវត្ថុ និងស្ថាប័នរដ្ឋាភិបាលនៃប្រទេសមួយចំនួន ក្នុងការគ្រប់គ្រងសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន។

ក្នុងន័យនេះការិយាល័យគ្រប់គ្រងព័ត៌មានវិទ្យានៃនាយកដ្ឋានកិច្ចការទូទៅសូមផ្តល់នូវតម្រូវការបច្ចេកទេសសម្រាប់ការរៀបចំមជ្ឈមណ្ឌលប្រតិបត្តិការសន្តិសុខបច្ចេកវិទ្យាព័ត៌មានដូចខាងក្រោម៖

Human Resources ធនធានមនុស្ស
SOC Eneineering

យោង
របស់អនុប្រធានអង្គភាព

យោង
របស់ប្រធាននាយកដ្ឋាន

**យោបល់
របស់អនុប្រធាននាយកដ្ឋាន**

24/7 Operation
Content Management
Alert Triage
Investigator
Responder
Forensics
Cyber Range
Traning ការបណ្តុះបណ្តាល

Process ប្រតិបត្តិការ

Forensic Handing
Intelligence
Offence Handling
False Positive Handling
Infrasturture
Incident Response Playbooks
Log Management

Technology បច្ចេកវិទ្យា

Security information and event management (SIEM)
User behavior analytics+Machine Learning (UBA+ML)
Network Analytics
Intelligence
Data analytics
Security Orchestration Automation and Response
Endpoint Detection and Response
Incident Response Platform
Sandboxing

Capability សមត្ថភាពជំនាញ

Rapid Detection
Rapid Response
Complex Threat Detection
User Risk Detection
Risk Visualization

ដូចនេះការិយាល័យគ្រប់គ្រងព័ត៌មានវិទ្យានៃនាយកដ្ឋានកិច្ចការទូទៅសូម
គោរពជម្រាបជូន **ឯកឧត្តមប្រធាន** ពិនិត្យ និងជ្រាបជាបាយការណ៍។

សេចក្តីដូចបានជម្រាបជូនខាងលើ សូម **ឯកឧត្តមប្រធាន** មេត្តាជ្រាប
និងពិនិត្យដ៏ខ្ពង់ខ្ពស់។

សូម **ឯកឧត្តមប្រធាន** មេត្តាទទួលនូវការគោរពដ៏ខ្ពង់ខ្ពស់បំផុតពីខ្ញុំ

ថ្ងៃ

ខែ

ឆ្នាំរោង ឆស័ក ព.ស. ២៥៦៧

រាជធានីភ្នំពេញ ថ្ងៃទី ខែ ឆ្នាំ២០២៤

នាយកដ្ឋានកិច្ចការទូទៅ
ការិយាល័យគ្រប់គ្រងព័ត៌មានវិទ្យា
អនុប្រធាន

ចិន វាសនា