5.pielikums
iepirkuma
„Tehnisko resursu auditācijas pierakstu savākšanas, integrēšanas
un analīzes risinājuma atbalsta pakalpojumi”
(identifikācijas numurs: IeM IC 2017/19)
nolikumam

TEHNISKĀ SPECIFIKĀCIJA

1. Sniedzamo pakalpojumu apraksts

1.1. Pretendents nodrošina konsultāciju un rekomendāciju sniegšanu telefoniski, elektroniski vai klātienē Pasūtītāja telpās Pasūtītāja speciālistiem par Drošības informācijas un notikumu pārvaldības sistēmas (turpmāk – SIEM (*Security Information and Event Management*)) ekspluatācijas un uzturēšanas jautājumiem, vismaz šādās jomās:

1.1.1. nodrošina konsultācijas par SIEM administrēšanu, izmaiņu ieviešanu, konfigurācijas papildināšanu, t.sk., SIEM funkcionālajā darbībā.

1.1.2. konsultācijas par izmaiņu veikšanu avota sistēmu konfigurācijās:

1.1.2.1. Pasūtītāja avota sistēmu konfigurēšana ar mērķi izpildīt drošības prasības vai nodrošināt drošības incidenta novēršanu, atbilstoši Pasūtītāja informācijas sistēmas drošību reglamentējošiem ārējiem normatīvajiem aktiem un Pasūtītāja iekšējiem dokumentiem;

1.1.2.2. avota sistēmu funkcionālo parametru korekcijas ar mērķi nodrošināt nepārtrauktu atbilstošu sadarbību ar SIEM;

1.1.3. konsultācijas par izmaiņu veikšanu SIEM pārvaldības serverī:

1.1.3.1. palīdzība jauno un/vai nerealizēto risinājuma iespēju testēšanā un ieviešanā;

1.1.3.2. kļūdu un/vai anomāliju analīze un rekomendāciju sagatavošana izmaiņām kļūdu novēršanai;

1.1.3.3. specifisku trigeru, filtru un skriptu izveide;

1.1.3.4. SIEM komponenšu konfigurācijas korekciju veikšanai;

1.1.3.5. SIEM komponenšu programmatūras uzstādīšanai un atjaunošanai;

1.1.3.6. rekomendācijas un palīdzība ārējo programmatūru pieslēgšanai SIEM;

1.1.3.7. izmaiņu veikšana dokumentācijā, kas saistīta ar programmatūras izmaiņām;

1.1.3.8. SIEM komponenšu fiksēto notikumu skaidrojums;

1.1.3.9. konsultācijas latviešu valodā iekārtu slēguma maiņā vai uzlabošanā;

1.1.3.10. SIEM neesošu šablonu izveide, kas ļauj pievienot jauna tipa iekārtu, izveidotās konfigurācijas testēšana;

1.1.3.11. palīdzība jaunu, nerealizēta (neesošu standartšablonos) tipa avotu ieviešanas testēšana un ieviešana;

1.1.4. konsultācijas par drošības incidentu kontroli un preventīvām darbībām;

1.1.5. konsultācijas par novēršanas koncepciju un metodoloģiju, izmantojot SIEM kopā ar citām Pasūtītāja pieejamajām drošības sistēmām;

1.1.6. palīdzība prasību definēšanā, lai nodrošinātu Pasūtītāja informācijas sistēmās fiksēto augta riska notikumu nodošanu uz SIEM un attiecīgo nepieciešamo SIEM reakcijas darbību ieviešanu;

1.1.7. konsultācijas problēmu novēršanā SIEM programmatūras darbībā.

1.2. Konsultācijas un atbalsts tiek nodrošināti valsts valodā, telefoniski, izmantojot e-pastu (uz Pretendenta norādīto tel. numuru un elektroniskā pasta adresi) vai klātienē (Bruņinieku ielā 72B, Rīgā), darba dienās no plkst. 8.30 līdz 16.30. Reakcijas laiks uz problēmas pieteikumu darba laikā, darba dienā - ne vairāk kā 2 (divas) darba stundas. Ziņojumiem, kas pieteikti darba dienā pēc plkst. 16.30, brīvdienā vai svētku dienā, par pieteikšanas laiku tiek uzskatīts nākamās darba dienas rīts plkst. 8.30. Nepieciešamības gadījumā problēmu novēršana jāveic ārpus Pasūtītāja darba laika.

1.3. Pretendents nodrošina automātisku un/vai regulāru SIEM komponenšu programmatūras un attiecīgu datu bāžu atjaunināšanu.
1.4. Pretendents nodrošina programmatūras atteikumu cēloņu noteikšanu un novēršanu.
1.5. Pretendents nodrošina SIEM e-pasta ziņojumu par kritiskajiem un Pasūtītāja definētajiem notikumiem sūtīšanas funkcionalitātes ieviešanu.
1.6. Pēc attiecīgā darba uzdevuma saņemšanas Pretendents nodrošina darbu izpildi klātienē ar vismaz viena atbilstošās kvalifikācijas speciālista atrašanos Pasūtītāja telpās vai attālināti izmantojot e-pastu, ja tas neietekmē darba uzdevuma izpildi.
1.7. Pretendents iesniedz pasūtītājam atskaites par veiktajiem darbiem.

2. Pakalpojumu sniegšanas termiņš

2.1. SIEM atbalsta pakalpojumi ir jānodrošina no 2018.gada 1.janvāra līdz 2019.gada 31.decembrim.

3. Pakalpojumu sniegšanas vieta

3.1. Apkalpojamā SIEM komponentes atrodas Latvijas Republikas Iekšlietu ministrijas Informācijas centra telpās Bruņinieku ielā 72B, Rīgā.