بسم الله الرحمن الرحيم

ކްރިމިނަލް ކޯޓު
ދިވެހިރާއްޖެ

ނަންބަރު: 145-P/2024/12

ދިއުމަށް

ކްރިމިނަލް ކޯޓުގެ ބަޖެޓުގެ ތަފާތު ބަޔާންތަކާ ގުޅިގެން ދިވެހިރާއްޖެ ސަރުކާރުގެ ފައިނޭންސް ކޮމިޓީ ކުރީގައި ހާޒިރުވުމަށް.

ތިލަދުންމަތީ ކުލަ ދަތުރުފަތުރު ސާވިސް ކުންފުނި 2024 ފެब്രുവരി 19 ވަނަ ދުވަހު 10:00 ގަޑިއިރު ތިލަދުންމަތީ ބައްދަލުވުން ހޯދުމަށް 2024 ފެब്രുവരි 26 ވަނަ ދުވަހު 14:30 ގަޑިއަށް ކްރިމިނަލް ކޯޓަށް ތިލަދުންމަތީ ކުލަ ދަތުރުފަތުރު ސާވިސް ކުންފުނި procurement@criminalcourt·gov·mv ގައި ލިޔުމުން ދިވެހިރާއްޖެ ސަރުކާރުގެ ވެބްސައިޓް www.criminalcourt.gov.mv ގައި ބަޔާންކުރަންވާނެ.

04 ރަމަޟާން 1445

14 ފެब്രുവരි 2024

بسم الله الرحمن الرحيم

ކްރިމިނަލް ކޯޓު

މާލެ،

ދިވެހިރާއްޖެ

މަޢުލޫމާތު ކަރުދާސް

އިޢުލާން ނަންބަރު: 145-P/2024/12 (14 ޑިސެމްބަރު 2024)

1. ތަޢާރަފު

މިކޯޓަށް ބޭނުންވާ އި.ޕީ.ބީ.އެކްސް ސްޓޯރޭޖް ސިސްޓަމެއް ފޯރުކޮށްދޭނެ ފަރާތެއް ހޯދަން ބޭނުންވެއެވެ.

އިތުރު މަޢުލޫމާތު "ސްޓޭޓްމަންޓް އޮފް ރިކުއަޔަރމަންޓްސްގައި" އެވަނީއެވެ.

2. ވަސީލަތްތަކުގެ އަގު

އަންދާސީ ހިސާބު ހުށަހަޅާ ފޯމުގައި ބަޔާނީ ހުށަހަޅާ އަގުގެ ޖީ.އެސް.ޓީ ނުހިމަނާ އަގާއި ޖުމްލަ ވަސީލަތްތަކަށް ހިނގާނެ އަގެވެ.

3. ބިޑާއި ގުޅޭ މަޢުލޫމާތު ސާފުކުރުން

މި ބިޑާ ގުޅޭ މަޢުލޫމާތު ސާފުކުރުން ހުށަހަޅާނީ ލިޔުމުން ދުރުވެރިކޮށެވެ. މަޢުލޫމާތު ސާފުކުރުމަށް ލިޔުމުން ކުރާނީ procurement@criminalcourt.gov.mv އަށެވެ. މިގޮތުން މަޢުލޫމާތު ސާފުކުރުމަށް ކަނޑައަޅާފައިވާ ސުންގަޑިއަކީ 2024 ޑިސެމްބަރު 19 ވަނަ ދުވަހުގެ 10:00 އަށެވެ. ފޯނުކޯލް ނުވަތަ ޒާތީގޮތުން ދޭ ދެފުށިއްޔާ މަޢުލޫމާތު ސާފުކުރުމަށް ހުށަހަޅާ ހުށަހެޅުންތަކެއް ބަލައި ނުގަނެވޭނެއެވެ. ބިޑަށް ހުށަހެޅުމަށް ކަނޑައަޅާފައިވާ ތާރީޚުގެ ކުރިން ބިޑަށް އެއްވެސް އިޞްލާޙެއް ގެނައުން ޖެހިއްޖެ ހާލަތެއްގައި އެ މަޢުލޫމާތެއް ގެޒެޓުގައި ޝާއިޢުކުރެވޭނެއެވެ. މިގޮތުން ޝާއިޢުކުރެވޭ މަޢުލޫމާތުތަކީ މަޢުލޫމާތު ކަރުދާހުގެ ބައެކެވެ.

4. ބިޑް ބަލައިގަތުމާއި ހުޅުވުން

ބިޑް ބަލައިގަތުމާއި ހުޅުވުމަށް ބާއްވާ ބައްދަލުވުން އޮންނާނީ 2024 ޑިސެމްބަރު 26 ވަނަ ދުވަހުގެ 14:30 ގައި މިކޯޓުގައެވެ. ކަނޑައަޅާފައިވާ ވަގުތާއި ގަޑިއަށް ހާޒިރުނުވާ ބިޑް ހުށަހަޅާ ފަރާތްތަކުގެ ބިޑް ބަލައި ނުގަނެވޭނެއެވެ. ބިޑްތައް ހުޅުވާނީ ކަނޑައަޅާފައިވާ ގަޑީގައި އެވަގުތު އެތަނަށް ތިބި ބިޑުހުށަހަޅާފަރާތްތަކުގެ ހާޒިރުގައި، ހުށަހަޅާފައިވާ އެންވަލޮ

ބީލަންތައް ކަނޑާ ޕޮއިންޓުދެވޭނެއެވެ. އަދި ބީލަންވެރިން ހުށަހަޅާފައިވާ އަގާއި، މުއްދަތު އަދި ބީލަމާއެކު ހުށަހަޅަންޖެހޭ ޑޮކިއުމަންޓުތަކުގެ ތެރެއިން ހުށަހެޅި ޑޮކިއުމަންޓުތައް އަސާސީ ޝަރުތުތަކާ ފުރިހަމަކަން، ބަޔާންކޮށްފައިވާ ސްޕެކްގައި ބުނެފައިވާ ޤާބިލުކަން ސާބިތުކޮށް، ކުރީގެ ޤާބިލުކަން އަސާސްކޮށް ޕޮއިންޓު ދެވޭނެއެވެ.

5. ބީލަމުގެ މުއްދަތު

ހުށަހަޅާ ބީލަންތަކުގައި މަދުވެގެން 60 (ފަސްދޮޅަސް) ދުވަހުގެ މުއްދަތު އޮންނަންވާނެއެވެ.

6. ޝަރުތު ފުރިހަމަވާ ބީލަންތައް

- މި ބީލަމުގައި ބައިވެރިވެވޭނީ މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓްގައި ކުރި އަދި ދުރު ކުންފުނީގެ ވިޔަފާރީގެ ޕާޓްނަރޝިޕްގައި ރަޖިސްޓްރީ ކުރެވިފައިވާ ދިވެހި ވިޔަފާރިތަކަށެވެ.
- ބީލަމުގައި ބައިވެރިވާ ފަރާތަކީ ދައުލަތުގެ މާލިއްޔަތުގެ ޤަވާއިދުގެ 17 ވަނަ ބާބުގައިވާގޮތުގެ މަތިން ދައުލަތުގެ ބީލަމުގައި ބައިވެރިވުމުން ސަސްޕެންޑްކުރެވިފައިވާ ފަރާތަކަށް ނުވާންވާނެއެވެ.
- ބީލަން ހުށަހަޅާއިރު ތިރީގައި ބަޔާންކޮށްފައިވާ ލިޔުންތަކާއެކު ހުށަހަޅަންވާނެއެވެ. އަދި އެލިޔުންތަކާއެކު ހުށަހަޅާ ޤާބިލުކަމުގެ ބީލަން ބަލައިގަނެވޭނެއެވެ.

1. ފުރިހަމަ ކޮށްފައިވާ އަންދާސީ ހިސާބު ހުށަހަޅާ ފޯމް
2. ވިޔަފާރި ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓްގެ ކޮޕީ
3. އެސް.އެމް.އީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓްގެ ކޮޕީ / ކޮމްޕެނީ ޕްރޮފައިލް
4. ޖީ.އެސް.ޓީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓްގެ ކޮޕީ (ޖީ.އެސް.ޓީ ދައްކަންޖެހޭ ފަރާތްތަކުން)
5. ޓެކްސް ކްލިއަރެންސް ރިޕޯޓް (އިޢުލާނުކުރި ތާރީޚުން ފެށިގެން 3 މަސްދުވަހުގެ ތެރޭގައި ނަގާފައިވާ ރިޕޯޓަކަށް ވާންވާނެއެވެ)
6. ކޯޓޭޝަން

7. <u>ބިޑުތައް ދިރާސާކޮށް ފެންވަރު ބެލުން މިންގަނޑު (އިވެލުއޭޝަން ކްރައިޓީރިއާ)</u>

- ހުށަހަޅާފައިވާ ބިޑުތައް އިވެލުއޭޝަންކުރުމުގެ ކުރިން މިނިމަމް ރިކުއަޔަރމަންޓްސް ނުފުރޭ ބިޑުތައް ބާތިލުކުރެވޭނެއެވެ.
- ބިޑުތަކަށް ޕޮއިންޓް ދެވޭނީ ތިރީގައިވާ ގޮތަށެވެ.

1. އަގަށް 60 ޕޮއިންޓް؛ އެންމެ ކުޑަ އަގު ހުށަހަޅާ ފަރާތަކަށް އެންމެ ގިނަ ޕޮއިންޓްދީ ނިސްބަތުން ބަލައި ދެން ހުށަހަޅާ އަގުތަކަށް ޕޮއިންޓްދެވޭނެއެވެ.

2. މުއްދަތަށް 20 ޕޮއިންޓް؛ އެންމެ ކުރު މުއްދަތެއް ހުށަހަޅާ ފަރާތަކަށް އެންމެ ގިނަ ޕޮއިންޓްދީ ނިސްބަތުން ބަލައި ދެން ހުށަހަޅާ ފަރާތްތަކަށް ޕޮއިންޓްދެވޭނެއެވެ.

3. ފަންނީ ގާބިލްކަމަށް 10 ޕޮއިންޓް؛ މިބައިން ޕޮއިންޓް ދިނުމުގައި ބަލާނީ އިޢުލާނުގައިވާ ގޮތުން ވޭތުވެދިޔަ 3 އަހަރު ދުވަހުގެ ތެރޭގައި ކޮށްފައިވާ 'ކުރެވުނު 10 ޕްރޮޖެކްޓްގެ ލިސްޓް' ސިޓީ ނުވަތަ އެސްޓޭޖްގައި ހިމަނާ މަޢުލޫމާތު ހިމަނައިގެން ބިޑާ ހުށަހަޅާ ފަރާތުން ބަޔާންކޮށްފައިވާ ސިޓީގައި 10 މަސައްކަތް ހިމަނާ އެމަސައްކަތްތަކުގެ ލިޔުން ހުށަހަޅާފައިވާނަމަ 10 ޕޮއިންޓްދީ އަދި އެއަށްވުރެ މަދުން ލިޔުން ހުށަހަޅާފައިވާނަމަ ލިޔުމުގެ އަދަދަށެވެ.

4. މާލީ ގާބިލްކަމަށް 10 ޕޮއިންޓް؛ މިބައިން ޕޮއިންޓް ދިނުމުގައި ބަލާނީ އިޢުލާނުގައިވާ ގޮތުން ވޭތުވެދިޔަ 3 އަހަރު ދުވަހުގެ ތެރޭގައި ކޮށްފައިވާ މަސައްކަތްތަކުގެ ލިޔުން ހުށަހަޅާފައިވާ މަސައްކަތްތަކުގެ އަގަށެވެ. މިގޮތުން ލިޔުންތަކުން ބަލައި ހިސާބުކުރާ ޕްރޮޖެކްޓްތަކުގެ އަގު ހުށަހަޅާ ބިޑުގެ އަގަށްވުރެ ބޮޑުވާނަމަ 10 ޕޮއިންޓްދީ އަދި ހުށަހަޅާފައިވާ އަގާ އެއްވަރުގެ ނުވަތަ އެއަށްވުރެ ބޮޑު އަގެއްގެ މަސައްކަތެއް ކޮށްފައިނުވާނަމަ މާލީ ގާބިލްކަމަށް ޕޮއިންޓް އެއް ނުދެވޭނެއެވެ.

8. <u>ބިޑް އެވޯޑްކުރުމާއި ބިޑްވެލިޑިޓީ މުއްދަތުދިނުން</u>

ބިޑް އެވޯޑްކުރެވޭނީ ޕޮއިންޓް އުސޫލުން އެންމެ ގިނަ ޕޮއިންޓް ލިބޭ ފަރާތަކަށެވެ. ބިޑް ކާމިޔާބުވާ ފަރާތާއި ކޮންޓްރެކްޓް ހަވާލުކުރުމުގެ ކުރިން ބިޑުގައި ބައިވެރިވި ހުރިހާ ފަރާތްތަކަށް ބިޑް ކާމިޔާބުވި ކޮންޓްރެކްޓަރުގެ ނަމާއި އަދި ކާމިޔާބުނުވިކަން ފަރާތްތަކަށް ލިޔުމުން އަންގާނެއެވެ. މިގޮތުން އަންގާ އެންގުމާއި ވިދިގެން ބިޑާ ގުޅޭ ޝަކުވާއެއް ވާނަމަ އެކަމެއް ހުށަހެޅުމަށް ބިޑުގައި ބައިވެރިވި ފަރާތްތަކަށް 5 (ފަހެއް) ދުވަހުގެ މުއްދަތެއް ދެވޭނެއެވެ. ބިޑް ކާމިޔާބުވި ފަރާތާއި ކޮންޓްރެކްޓް ހަވާލުކުރެވޭނީ، ބިޑް ކާމިޔާބުނުވި ފަރާތްތަކުން ހުށަހަޅާ ޝަކުވާތައް ބަލައި، ހުށަހެޅޭ ސުވާލުތަކަށް ޖަވާބު ދިނުމަށްފަހުގައެވެ. ބިޑް އެވޯޑްކުރެވުނުކަމުގެ ބިޑަރަށް ވަކިން އެވޯޑް ނޯޓިސް އަންގާނެއެވެ.

9. ކޮންޓްރެކްޓް ބަދަލުކުރުން

މި މަސައްކަތް ބަދަލުކުރުމުގެ ގޮތުން ކޮންޓްރެކްޓްގައި ސާފު ކުރެވޭނީ ކުރިމަތިވާ ހާލަތް މަސައްކަތާ ބަދަލުވާގޮތުން ޕާސިބަލް، ދެފަރާތުގެ ޕާސިޓްގައި އެއްވަރުގެތާއީދުގައި ތަފާތުއެއްސަރު ދެ ކޮޕީގައެވެ. ދެފަރާތުގެ ދެފަރާތުގައި ވެސް އެއްބަސްވުމުގައި ސޮއިކުރުމުގެ ފުނޑި ހައިސިއްޔަތުން، ޗިޓުން ހުށަހަޅާ ފަރާތަށް ލިޔެގެން އަންގަންވާނެއެވެ.

10. އެޑްވާންސް ފައިސާ ދިނުން

ޕްރޮކިއުމަންޓްގެ ޖުމްލަ އަގު -/250،000 (ދެލައްކަ ފަންސާސްހާސް) ރުފިޔާ ހުރިހާއަށްވުރެ ބޮޑުވާނަމަ، މަސައްކަތް ބަދަލުވާވަރުގޮތުން މަސައްކަތާ ބަދަލުވާތާ 45 (ސާޅީސް ފަހެއް) ދުވަހުގެ ތެރޭގައި އެޑްވާންސްގެ ގޮތުގައި ފައިސާ ދިނުމަށް އެދިއްޖެނަމަ، ކޮންޓްރެކްޓްގެ ޖުމްލަ އަގުގެ 15% (ފަނަރަ އިންސައްތަ) ދޫކުރެވޭނެއެވެ. އަދި މިފަދައިން އެޑްވާންސް ފައިސާ ދޫކުރެވޭނީ އެންމެ ފަހަރަކުއެވެ.

11. ލިކުއިޑޭޓެޑް ޑެމޭޖަސްގެ ގޮތުގައި ފައިސާ ކެނޑުން

އެއްބަސްވުމުގައި ކަނޑައަޅާފައިވާ މުއްދަތުގައި މަސައްކަތް ނުނިމި ވަސީލަތްތަކުން ތިރީގައިވާ ގޮތުގެ މަތިން ޑިލޭޑަމޭޖުގެ ގޮތުގައި ފައިސާ ކެނޑޭނެއެވެ.

ޑިލޭޑަމޭޖުގެ ގޮތުގައި އިތުރުވާ ދުވަސްތަކަށް ކަނޑައަޅާ އަދަދު = CP*0.005*LD

CP = (ކޮންޓްރެކްޓް ޕްރައިސް): ކޮންޓްރެކްޓްގެ ޖުމްލަ އަގު.

LD = (ލޭޓް ޑިއުރޭޝަން): ކޮންޓްރެކްޓްގެ މުއްދަތަށްވުރެ އިތުރުވާ ދުވަސްތައް.

މުއްދަތަށް މަސައްކަތް ނުނިމިގެން ޑިލޭޑަމޭޖުގެ ގޮތުގައި ދައްކަންޖެހޭ އަދަދު މުޅި މަސައްކަތުގެ ޖުމްލަ އަގުގެ 15 އިންސައްތަ އަށްވުރެ އިތުރު ވެއްޖެނަމަ، އެހިސާބުން އެއްބަސްވުން ނިމުމަކަށް ގެނެވޭނެއެވެ.

12. މަސައްކަތް ފުރިހަމަކުރިކަމުގެ ލިޔުން ދިނުމާއި މަސައްކަތުގެ އަގު ދިނުން

ކޮންޓްރެކްޓް ކުރެވޭ މަސައްކަތް ނިމުމުން، ކޯޓުގެ ރިކުއަރމަންޓްއާއި މަސައްކަތާ ބަދަލުވިފައިވާގޮތުން ހަރަކާތްތަކާއި ކޯޓްސަރަހައްދު އަދި ދެފަރާތުން އެއްބަސްވުމާއި ޖެހޭ މަސައްކަތް ފުރިހަމަކޮށްފައިވާ ކަމާ ބަޔާންކުރާ މަސައްކަތް ފުރިހަމަކުރިކަމުގެ ލިޔުން ބަދަލުކުރެވޭނެއެވެ. މަސައްކަތަށް އެގޮތުން މަސައްކަތްނިމުމުން މަސައްކަތް ފުރިހަމަ ކުރިކަން މަސައްކަތް ބަދަލުކުރިގޮތުން ލިޔުން ދިނުމުން، މަސައްކަތާ ބަދަލުވާގޮތުން އިންވޮއިސް ހުށަހެޅުމުންނެވެ.

13. ބިޑާއިއެކު ހުށަހަޅަންޖެހޭ ތަކެތި:

1. ވިޔަފާރި ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓުގެ ކޮޕީ

2. އެސް.އެމް.އީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓުގެ ކޮޕީ / ކޯޕަރޭޓް ޕްރޮފައިލް

3. ޖީ.އެސް.ޓީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓުގެ ކޮޕީ (ޖީ.އެސް.ޓީ ދައްކަންޖެހޭ ފަރާތްތަކަށް)

4. ޓެކްސް ކްލިއަރަންސް ރިޕޯޓް (އިއުލާންކުރާ ތާރީޚުން ފެށިގެން ފާއިތުވީ 3މަސްދުވަހުގެ ތެރޭގައި ނަގާފައިވާ ރިޕޯޓެއްކަމުގައި ވާންވާނެއެވެ.)

5. ކޯޓޭޝަން

6. 'ގުޅުންހުރި 10 ޕްރޮޖެކްޓްގެ ރިކޯޑް' ސިޓީ (އިއުލާންކުރާ މުއްދަތުން ފެށިގެން ފާއިތުވި 3 އަހަރުދުވަހުގެ)

7. ކުރިން ކޯޓުގައިވާ މަސައްކަތުގެ ތަޖުރިބާ ލިބިފައިވާ ނަމަ ވަކިން ސާބިތުކުރާ ލިޔުން. (ފަހުގެ 10 މަސައްކަތުގެ ތަޖުރިބާ ލިޔުން)

STATEMENT OF REQUIREMENT
(IUL)145-P/2024/12 (14TH FEBRUARY 2024)

Specifications for 1x E.D.R Solution System

Index /Reference	Description
	Part 1: General Requirements
1.1	Product Manufacture/s
1.2	Product Versions
1.3	The solution must encompass licenses for 100 endpoints, valid for a duration of one year.
	Part 2: Eligibility Requirements
2.1	Solution should support both on-prem and Cloud hosted model where the vendor or their incident response partner provides the management infrastructure, operational monitoring, and upgrades.
2.2	The selected party must provide 24/7 technical support, including issue/problem reporting and assistance, with escalation paths for critical incidents.
2.3	The selected party is required to be an incident response partner of the solution vendor, ensuring authorized collaboration in incident management. Evidence of authorization as an IR partner from the vendor is required.
2.4	The selected party must provide at least five references for Incident Response services previously rendered in the Maldives. References should include details of the service provided and the contact information of the client for verification purposes.
2.5	The selected party must present a minimum of five verifiable references, demonstrating successful management of incidents utilizing the EDR platform.
2.6	The selected party must have a minimum of three qualified engineers based locally. Profiles or qualifications of these engineers, including their experience and expertise in handling EDR solutions is required to be submitted.
2.7	Solution must seamlessly integrate with all leading Security Information & Event Management (SIEM) Solution. Interested parties shall submit details of any dependencies together with the proposal.
2.8	Solution should be compliance with ISO & SOC standards such as (27001, SOC 2 Type II)
2.9	Proposed solution should be a leader in the Gartner Magic Quadrant for Endpoint Protection Platforms for the last 2 years.
2.10	Proposed solution should be in the top 3 performers of the MITRE ENGENUITY ATT&CK Evaluation from 2020 to 2022 on the visibility of sub-steps evaluated on.
2.11	Proposed solution shall run on a Single Agent (compatible for Windows, Mac, and Linux OS) and Single Console to reduce complexity.
2.12	The proposed solution should include a professional local IR support partner acknowledged by the OEM, proficient in configuring SIGMA rules and providing on-site support.
2.13	Proposed Solution should provide an on-premise option. If the customer selects cloud implementation, the solution must also include the capability for data residency, enabling the customer to choose the specific region for their data storage.
2.14	Proposed solution deployment and updates (agent, policies, settings, etc..) are available globally and where possible should not require forced rebooting (server endpoints) during installation/upgrade without degrading performance of the proposed Endpoint Detection & Threat Prevention solution and the respective endpoint.

2.15	The Incident Response Partner should collaborate with your team to develop and implement custom threat hunting rules based on your specific threat landscape and risk profile.
2.16	The Incident Response Partner should proactively conduct ongoing threat hunting campaigns across endpoints, utilizing the capabilities of the EDR platform.
2.17	The EDR agent on endpoints should incorporate advanced endpoint protection features, including malware detection and prevention, endpoint hardening, and application whitelisting.
2.18	The Incident Response Partner should provide incident response support during threat hunting campaigns, assisting with investigation, containment, and remediation of identified threats.
2.19	The Incident Response Partner should provide ongoing endpoint hygiene monitoring and reporting to identify and address potential security vulnerabilities and configuration issues.
2.20	Integration with endpoint configuration management tools (SCCM, Intune) may be desirable for advanced endpoint management and control.
2.21	The Incident Response Partner should provide regular reports on threat hunting findings, detected threats, and incident response activities.
2.22	The Incident Response Partner should establish clear communication protocols for proactive alerts, incident updates, and ongoing security status updates.
2.23	Dedicated security analysts from the Incident Response Partner should be available for direct communication and consultation on security concerns and incidents.
2.24	The proposed solution is required to encompass service level agreements stipulating a guaranteed response time from the incident response partner: within 1 hour for priority 1 incidents, within 2 hours for priority 2 incidents, and within 8 hours for priority 3 incidents. Additionally, the proposal must incorporate a categorization matrix for incidents and incident reporting structure.
2.25	The proposed solution needs to incorporate a detailed deployment plan and schedule, complete with technical specifications outlining the automated deployment mechanisms to be employed.
Part 3: Endpoint Protection & Response General Requirements	
3.1.	Proposed solution must be tamper-resistant and protect endpoint sensors against attempts to modify.

3.2.	Proposed solution must continuously collect data on all the entities and their activities within the environment such as: ○ File interaction – create, open, rename, delete, execute. ○ Process execution (including process tree). ○ User login. ○ Network traffic. ○ Registry changes. ○ Installed software.
3.3.	Proposed solution must support the display of entity and activity data. Search on behavioral patterns in all fields of coverage (users, files, machines, network traffic).
3.4.	The solution shall be able to easily identify root cause of security event. The Root cause analysis must simplify investigations for the team by identifying the sequence of events and root cause of alerts.
3.5.	Proposed solution must support queries. Search for the occurrence of process, file, network, or user activities across all endpoints.
3.6.	Proposed solution shall support exploit blocking, custom whitelisting, and blacklisting, behavioral, attack attribution, and adware blocking. Such protection shall exist whether the endpoint is online or offline and must not interfere with business-critical applications.
3.7.	Proposed solution must support the means to execute forensic investigation: • Investigation of running processes or files. • Machine-level investigation. • Memory activity investigation. • Obtain memory dump.
3.8.	Proposed solution should not rely on sending suspicious objects or parts of the memory to central node for sandboxing as a mechanism to detect and prevent malicious content and activity.
3.9.	The solution should provide a visual process tree browser for detected threats.
3.10.	Solution should provide the option to mark discovered items as suspicious or threats.
3.11.	Ability for an analyst to add notes/comments to an event.
3.12.	Options to set the status of an issue or event (i.e. resolved, in progress, unresolved) or similar workflow.
3.13.	Proposed solution must support isolation and mitigation of malicious presence and activity globally across the entire environment.
3.14.	Solution should provide the flexibility to mark an entire group of events as a threat and take response or remediation actions.
3.15.	The alert data related to threats detections should be made available in the Management Console for a period of at least 365 days.
3.16.	Proposed solution must support real-time dynamic identification and analysis of malicious content to detect and prevent zero-day attacks. It should provide in-depth forensics insights to help identify the source of threats and showcase a detail action tree of the incidents and should be accessible through the dashboards for other investigations, and should be accessible through the dashboards for further investigations regardless of the device state (online or offline) For example, • Local IP address of the endpoint. • Logged in User ID with timestamps. • All process & service execution including admin tools and CMD commands. • All PowerShell Activities on endpoint • Suspicious File Activities (Zip, RAR & Scripts written). • Removeable Media Usage • Registry Edits. • Network listening ports on endpoints. • Network connections details.

	• List of Usernames or Systems where remote logins have taken place.
3.17.	Proposed solution is required to encompass functionalities that allow for the creation of customized dashboards, utilizing metrics gathered by the endpoint agents.
3.18.	Proposed solution should include integration with a local IR Partner for proactive and automated threat hunting campaigns based on custom indicators of compromise (IOCs), tactics, techniques, and procedures (TTPs) aligned with our specific threat landscape.
3.19.	Proposed solution must support encrypted communication between the central EDR management console and the agents on the endpoints or servers, including those managed by the integrated Incident Response Partner.
3.20.	The agent should have the ability to configure proxy parameters to ensure the communication through a web proxy.
3.21.	Proposed solution must support isolation and mitigation of malicious presence and activity on the endpoint, via remote operations, including and not limited to: I. Ability to run a coordinated command (such as CMD interface). II. Running scripts or files from a network location or mapping a drive. III. Shutting down an endpoint or server. IV. Isolating an endpoint or server from the network. V. Deleting a file (including active run files). VI. Quarantine a file (including active run files). VII. Kill a process. VIII. Remove or delete a service or scheduled task
3.22.	Proposed solution shall have capabilities to perform or integrate with vulnerability assessment engines to identify missing security updates within endpoints and automate the patch process.
3.23.	Proposed solution shall provide the means to conduct Inventory Management. Map and correlate all assets within the environment such as endpoints, servers, installed apps, user accounts, and generate inventory reports.
3.24.	Proposed solution should enable the integration of 3rd party security solutions through API.
3.25.	Proposed solution should provide open EDR integration with 3rd party products.
3.26.	Proposed solution should have more than 70 pre-build 3rd party integrations out-of-the-box.
3.27.	Proposed solution should have mechanism to provide future integration for Identity Hygiene and reduce exposure of credentials, while to reduce identity-based attack threat landscape.
3.28.	Solution should have the capability to detect unprotected, un-managed devices.
3.29.	Proposed solution should include a rouge detector that can scan the network and identify IP devices.
3.30.	Solution should be able to mitigate new and emerging zero-day threats with custom detection rules.
3.31.	Solution custom detection rules should trigger automated workflows.
3.32.	Proposed solution should be able to detect the most amount of attack sub-steps and prevent malware, evasive and zero-day threats with minimal configuration changes. Please provide independent 3rd party documentation for evidence.
3.33.	Proposed solution should be able to track adversary Techniques, Tactics & Procedures. The details of adversary, Tactics, Techniques, and Procedures (TTP)s should be available in the management console
3.34.	Proposed solution should have in-built mechanism to initiate secure remote session for real-time response.
Part 4: Endpoint Detection & Threat Prevention Capabilities and Features	
4.1.	Solution should leverage machine learning and the expertise of the partnered Incident Response Partner to detect and block malicious files without relying solely on daily/weekly definition updates. Also, shall have the ability to detect and block bad behaviors exhibited from known-good files (such as outlined in the MITRE ATT&CK framework).
4.2.	The proposed solution shall be able to detect file less attack and script base attack without using signatures and automatically kill the process based on policy settings.

4.3.	The EDR solution should look for potentially unwanted programs.
4.4.	The solution shall use signature-less algorithm to prevent malware.
4.5.	The solution should protect the endpoint against malware, even when the system is not connected to the network. The agent needs to be fully autonomous meaning it does not need to have any dependency on Management Server/Cloud or resources external from the Agent to detect and respond appropriately to sophisticated threats (Zero Day, File-less, Ram-based, Zero Day exploits, Ransomware, Miners, Lateral movement, APT) in real time as the threats are detected. A threat protection mechanism that does not always rely on connectivity to a management server/console but can leverage the threat intelligence and analytical capabilities of the partnered Incident Responder, is preferred.
4.6.	The solution shall have the capability to quarantine unknown and zero-day malware.
4.7.	The solution should leverage Artificial Intelligence or Machine Learning to analyze files pre-execution.
4.8.	The solution should leverage Artificial Intelligence or Machine Learning to analyze behaviors while a file is running.
4.9.	Proposed solution must identify malicious files and prevent them from execution, including viruses, trojans, ransomware, spyware, and crypto miners using machine learning and behavioral techniques before it could create any damage to respective systems.
4.10.	Proposed solution must identify malicious behavior of executed files, running processes, registry modifications, or memory access and terminate them at runtime, or raise an alert (exploits, fileless, Macros, PowerShell, WMI, etc.)
4.11.	The solution should provide Firewall Control for Windows, MAC & Linux. The firewall control policy should provide context unique to each group of Endpoints and should support creation of rules based on FQDN's, IP, CIDR, Range.
4.12.	Should support to single firewall rule to apply for multiple operating systems.
4.13.	Proposed solution must support the creation of rules to allow or block traffic and communication for specific addresses/IP ranges.
4.14.	Proposed solution must identify and block privilege escalation attacks.
4.15.	Proposed solution must identify and block reconnaissance attacks.
4.16.	Proposed solution must identify, and block credential theft attempts occurring in memory (credential dump, brute force).
4.17.	Proposed solution must identify and block/alert on lateral movement (SMB relay, pass the hash).
4.18.	Proposed solution must identify user account malicious behavior, indicative of prior compromise.
4.19.	Proposed solution must identify malicious interaction with data files.
4.20.	Proposed solution must identify data exfiltration via legitimate protocols (DNS tunneling, ICMP tunneling).
4.21.	Proposed solution must provide visibility into encrypted traffic, without the need for a proxy or additional agents, to ensure full coverage of threats hiding within covert channels. The Incident Response Partner should provide guidance and best practices for implementing and interpreting this visibility for optimal threat detection.
4.22.	Proposed solution must identify and block usage of common attack tools (Metasploit, Empire, Cobalt etc.).
4.23.	Proposed solution must provide full protection for endpoints and servers that are offline (do not connect to the organization's network). A threat protection mechanism that do not always rely on connectivity to a management server/console.
4.24.	Proposed solution must collect endpoint, file, process, user activity and network traffic in a fully self-sustained manner. Eliminate the need for manual configuration of rules or policies or reliance on additional devices.
Part 5: Device Control Features	
5.1.	Solution should include the capability to manage and control the use of USB peripheral devices. (Allow Read & Write, Read Only, Block)

5.2.	Solution device control should provide easy configuration to allow blocked USB devices through device activity logs.
5.3.	Proposed solution device control should provide device control to be implemented through multiple device definition levels such as device id, device family, device type and etc.
5.4.	Proposed solution device control should log device activity of allowed and blocked devices.
5.5.	Solution must provide the USB device control management, configuration and visibility from the same single console.
5.6.	Proposed solution should have Bluetooth device control capabilities to allow & block.
5.7.	Proposed solution should provide the configuration of Bluetooth device control fine-grained policies to allow & block Bluetooth devices according to their type (e.g. keyboard, mouse, headset).
5.8.	Proposed solution Bluetooth device controller should enable to allow or block operation of Bluetooth devices based on the protocol version.
5.9.	Solution must provide the Bluetooth device control management, configuration, and visibility from the same single console.
Part 6: Vulnerability Management	
6.1.	Proposed solution should have a built-in vulnerability assessment scanner to discover vulnerabilities related to installed 3rd party applications.
6.2.	The proposed solution's 3rd party application vulnerability assessment scanner module should provide filtering of the identified vulnerabilities based on OS, Machine Type, etc.
6.3.	The proposed solution 3rd party vulnerability assessment scanner module should map the discovered vulnerabilities to the specific CVE ID.
6.4.	Solution must provide 3rd party application vulnerability module monitoring and visibility from the same single console.
Part 7: Agent Features	
7.1.	Fully autonomous Detection, Prevention and Remediation of malware even when the endpoint is not connected to the cloud/network.
7.2.	Use of signature-less algorithm to detect and prevent malware.
7.3.	Use of AI/ML powered Static and Behavioral analysis to detect and prevent a wide range of attacks in real time.
7.4.	Ransomware protection to restore encrypted files to a pre-attack state, effectively reversing the effects of a ransomware attack.
7.5.	Ability to do an initial scan of the endpoint to detect malware at agent deployment.
7.6.	Firewall controller to control network connectivity.
7.7.	Device controller to control USB and Bluetooth devices.
7.8.	Ability to discover unmanaged and unprotected endpoints.
7.9.	Application vulnerability scanner for application inventory and vulnerability mapping.
Part 8: Operating System Platform Support	
8.1.	Agent should support the deployment to the following Windows versions: • Windows Server Core 2012, 2016 and 2019 • Windows Server 2022, 2019, 2016, 2012 R2, 2012, 2008 R2 SP1 • Windows 7 SP1, 8, 8.1, 10, 11
8.2.	Agent should support deployment to the following legacy Windows versions: • Windows XP SP3 • Windows 2008 (Pre-R2)

8.3.	Agent support for the following virtual environments: • Citrix XenApp, • Citrix XenDesktop • Oracle VirtualBox • VMware vSphere • VMware Workstation • VMware Fusion • VMware Horizon • Microsoft Hyper-V
8.4.	Agents should support for macOS endpoints, spanning 3 years in alignment with Apple End of Life (EOL) policy: • macOS Big Sur • macOS Catlina • macOS Mojave • macOS Ventura • macOS Sonoma
8.5.	Agent support for mobile devices: • Android • iOS • ChromeOS
8.6.	Agent support for the following Linux environments: • CentOS (6.4+, 7.0-7.9, 8.0-8.3, 8.4) • Debian (8,9,10,11) • Oracle (6.9-6.10, 7.0-7.9, 8.0-8.7, 9.0) • RHEL (6.4+, 7.0-7.9, 8.0-8.7, 9.0-9.1) • SUSE Linux Enterprise (12.x, 15.x) • Ubuntu (18.04 - 22.04)
Part 9: Operations & Policy Management	
9.1.	Can be deployed on older machines and old version of Windows OS.
9.2.	Endpoints solution is fully manageable via Central Cloud Console Administrator.
9.3.	Deploy and set up policies, run tasks, collect logs, and get notifications and an overall security overview of the network via a central web-based management console.
9.4.	Makes it possible to handle all licenses transparently, from one place via web browser.
9.5.	Proposed solution must have a light footprint for minimal impact on the endpoint/server performance. Indicate the expected maximum RAM, CPU, Bandwidth consumption etc.
Part 10: Central Cloud Management Console	
10.1.	The solution should provide a web-based console that allow administrators to access the management interface from any machine.
10.2.	Management console should provide granular role-based access to a tenant at different levels and scopes in order enable structured management of various sites and locations, including granting specific access levels to the partnered Incident Responder for their designated tasks and functionalities.
10.3.	Solution should provide updates and console connectivity for closed environments that does not have direct outbound connectivity.
10.4.	Solution should provide integration & security for console connectivity and update content of such closed environments.

10.5.	Solution should provide secure communication and connectivity with the management console for both outbound and inbound.
10.6.	Enable deployment on multiple sites that report into a single console.
10.7.	Enable/disable certain types of notifications.
10.8.	Centrally collect and process alerts in real-time.
10.9.	The solution should have centralized policy management and reporting architecture that can scale on a single console.
10.10.	Solution should provide Ability to support policy inheritance across a group of devices.
10.11.	Proposed solution must support connection to Active Directory.
10.12.	Solution should have the option to provide dynamic policy assignment based on device attributes.
10.13.	The policy context should provide the option to turn ON or OFF unique engines or by Type of engine (Pre-Execution and Run-Time Engines).
10.14.	Policy modifications should be applied in near real time.
10.15.	Solution should be able to identify any rogue endpoints that are not yet protected by the proposed solution.
10.16.	The solution should have the ability to initiate off On-Demand Scans to look for malware (from console and/or endpoint)
10.17.	Specify a schedule for downloading updates, with the ability to disable automatic updates.
10.18.	Support integration with email infrastructure to notify security personnel and the designated Incident Response Partner contact in case of alerts.
10.19.	Proposed solution shall provide log collection, retention, and integration with SIEM.
	Part 11: Training
11.1.	The selected vendor must provide comprehensive training for one staff member responsible for managing and operating the proposed Endpoint Detection & Response (EDR) solution.
11.2.	Training sessions should be conducted by qualified trainers
11.3.	The training program should be interactive, providing hands-on exercises and simulations to enhance practical skills and understanding.
11.4.	Training materials, documentation, and access to additional resources should be provided to support continuous learning and reference.
11.5.	The vendor should offer a certification or acknowledgment upon the completion of the training program.
11.6.	Training sessions should be scheduled and conducted within a reasonable timeframe, ensuring that the staff member is adequately equipped to operate and manage the EDR solution effectively.

بسم الله الرحمن الرحيم

ކ.ތުލާދޫ ކޯޓު

ފައިލް،

ފެނުވަރަށް

ތަކުރާރު ހިނގާ ހުކުމް ކުރުން

ތިއުރިކްސ ނަންބަރ: 145-P/2024/12 (14 ފެބްރުވަރީ 2024)

ދަޢުވާތަކުގެ ތަފްޞީލު :.....

- ތާރީޚް: .....ބުނެވިގެ (ދިވެހި ބާރުގެ ދަށުން)
- ފެށުނު ތާރީޚް: .....ބުނެވިގެ (ދިވެހި ބާރުގެ ދަށުން)
- ފެށުނު ގަޑިތަކާ: .....ދުވަސް (ތަންކޮޅު ތަކުރާރު ދުވަސްތަކާ ދަދަށުން)

ތަކުރާރު ހިނގާ ފަރާތުގެ ތަފްޞީލު:

ނަން :.....

ދާއިމީ ގޭގެ:.....

ތާރީޚް ފެށުނު ނަންބަރ:.....

ވިލާގެއްގެ ނަން:.....

ވިލާގެއްގެ ތަނަވަސްކުރި ނަންބަރ:.....

ގޭގެ ކުރު:.....

ކުޑަ ނަންބަރ:.....

ފޯނު:.....

ވިލާގެއްގެ ސޮއި:

ސޮއި :.....

بسم الله الرحمن الرحيم

ކ.ގަދޫ،

ދިވެހިރާއްޖެ

ގުޅުންހުރި 10 ފާރާތްތަކުގެ ތަފްޞީލް

ތިއުރީ ނަންބަރު: 145-P/2024/12 (14 ފެބްރުވަރީ 2024)

ނަންބަރު	ގުޅުން ހުރި ފާރާތުގެ ނަން	ގުޅުން ހުރި ފާރާތާ ގުޅުންހުރި ގޮތް	ގުޅުން ހުރި ގޮތް
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			