REPUBLIKA E SHQIPËRISË
KOMISIONI I PROKURIMIT PUBLIK

Nr. 1636/ 6 prot. Datë 26/06/2026

V E N D I M
Nr. 877/2026

Komisioni i Prokurimit Publik, i përbërë nga:

Fiorent Zguro	Nënkryetar
Anila Malaj	Anëtar
Kreshnik Ternova	Anëtar
Gjergj Mersini	Anëtar

Në mbledhjen e datës 26/06/2026, shqyrtoi ankesën me:

Objekt: Vendim për mbylljen e çështjes për pjesën e pranuar mbi ankesën e paraqitur nga operatori ekonomik "*PC STORE*" SHPK, për procedurën e prokurimit "*E hapur, mbi kufirin e lartë monetar*", me Nr. *REF-85701-05-14-2026*, me objekt: "*Blerje suport për siem+licensa për EDR/XDR (1200 përdorues) licensa fireëall Proffesional për 4 (katër) vite*", me fond limit 63,970,667 (*gjashtëdhjetë e tre milion e nëntëqind e shtatëdhjetë mijë e gjashtëqind e gjashtëdhjetë e shtatë*) Lekë, pa TVSH ose 670,060 *(gjashtëqind e shtatëdhjetë mijë e një*) euro pa T.V.SH, parashikuar për t'u zhvilluar me datë 15.06.2026, nga autoriteti kontraktor Posta Shqiptare SHA.

	Modifikimin e dokumenteve të procedurës së prokurimit "*E hapur, mbi kufirin e lartë monetar*", me Nr. *REF-85701-05-14-2026*, me objekt: "*Blerje suport për siem+licensa për EDR/XDR (1200 përdorues) licensa fireëall Proffesional për 4 (katër) vite*", me fond limit 63,970,667 (*gjashtëdhjetë e tre milion e nëntëqind e shtatëdhjetë mijë e gjashtëqind e gjashtëdhjetë e shtatë*) Lekë, pa TVSH ose 670,060 *(gjashtëqind e shtatëdhjetë mijë e një*) euro pa T.V.SH, parashikuar për t'u zhvilluar me datë 15.06.2026, nga autoriteti kontraktor Posta Shqiptare SHA.
Ankimues:	Operatori ekonomik "*PC STORE*" SHPK me NIPT: L01606034A dhe me adresë: *Rruga e Dibrës, Vila nr.153, Kati i Parë, Tiranë.*
Autoriteti Kontraktor:	Posta Shqiptare SHA. *Adresa: Rruga "Reshit Çollaku" Nr. 4, Tiranë.*
Baza Ligjore:	Ligji nr. 162/2020 *"Për Prokurimin Publik*", i ndryshuar, Vendimi i Këshillit të Ministrave nr. 285, datë 19.05.2021 *"Për miratimin e rregullave të prokurimit publik"* i ndryshuar, Vendimi i Komisionit të Prokurimit Publik Nr. 766, datë 13.10.2021 "*Për miratimin e rregullave për organizimin dhe funksionimin e Komisionit të Prokurimit Publik*", Neni 4 i Vendimit të Komisionit të Prokurimit Publik nr. 500/2020 datë 5.11.2020 "*Rregullore për Marrjen e Masave Organizative për Ushtrimin e Veprimtarisë së Institucionit të Komisionit të Prokurimit Publik gjatë gjendjes së pandemisë së shkaktuar nga COVID -19"*.

Komisioni i Prokurimit Publik pasi shqyrtoi ankesën e paraqitur nga operatori ekonomik ankimues dhe pasi diskutoi çështjen në tërësi,

Vëren:

I

Vlerësimi paraprak

I.1. Vlera limit e përllogaritur për procedurën e prokurimit objekt-ankimi është mbi kufirin e lartë monetar, ndaj shqyrtimi dhe vendimmarrja do të bëhet nga të gjithë anëtarët, në përputhje me pikën 1, të nenit 30 të ligjit nr. 162/2020 "*Për prokurimin publik*" i ndryshuar dhe Rregullat e Prokurimit Publik.

I.2. Operatori ekonomik ka *prima facie* interes në këtë procedurë prokurimi dhe për këtë arsye legjitimohet për të paraqitur ankesë në lidhje me të.

I.3. Operatori ekonomik ankimues ka paraqitur ankesë pranë autoritetit kontraktor dhe njëherazi pranë Komisionit të Prokurimit Publik, në përputhje me kërkesat e përcaktuara në ligjin nr. 162/2020 "*Për prokurimin publik*" i ndryshuar.

I.4. Ankimuesi ka respektuar afatet ligjore të paraqitjes së ankesës pranë autoritetit kontraktor dhe Komisionit të Prokurimit Publik.

II

Rrethanat e çështjes

II.1. Në datën 15.05.2026 është publikuar në Sistemin e Prokurimeve Elektronike procedura e prokurimit "*E hapur, mbi kufirin e lartë monetar*", me Nr. *REF-85701-05-14-2026*, me objekt: "*Blerje suport për siem+licensa për EDR/XDR (1200 përdorues) licensa fireëall Proffesional për 4 (katër) vite*", me fond limit 63,970,667 (*gjashtëdhjetë e tre milion e nëntëqind e shtatëdhjetë mijë e gjashtëqind e gjashtëdhjetë e shtatë*) Lekë, pa TVSH ose 670,060 *(gjashtëqind e shtatëdhjetë mijë e një*) euro pa T.V.SH, parashikuar për t'u zhvilluar me datë 15.06.2026, nga autoriteti kontraktor Posta Shqiptare SHA.

II.2. Në datën 25.05.2026 pranë Komisionit të Prokurimit Publik dhe pranë autoritetit kontraktor është administruar ankesa me numër ankimi elektronik A/2026/6720 dhe me numër protokolli nr. 1636/2026 prot., datë 26.05.2026 e operatorit ekonomik "*PC STORE*" SHPK. Nga shqyrtimi paraprak i ankesës, u konstatua se objekti i saj lidhet me kërkesën për modifikimin e dokumenteve të procedurës së prokurimit objekt ankimi.

II.3. Bazuar në nenin 112, pika 3, të ligjit nr. 162/2020 "*Për prokurimin publik*", i ndryshuar Komisioni i Prokurimit Publik ka publikuar në bazën e të dhënave të tij, të dhëna për: a) ankimuesin, adresën dhe NUIS-in; b) të dhëna të plota për procedurën e prokurimit (objekt, numër reference, fond limit, datën e zhvillimit të procedurës) si dhe ankesën e plotë të ankimuesit.

II.4. Referuar informacionit të autoritetit kontraktor me anë të shkresën nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, është depozituar nga autoriteti kontraktor në Komisionin e Prokurimit Publik, informacioni lidhur me procedurën e mësipërme të prokurimit, si dhe vendimarrja për trajtimin e ankesës së operatorit ekonomik ankimues "*PC STORE*" SHPK, në të cilin konstatohet se Komisioni i Shqyrtimit të Ankesës ka vendosur pranimin pjesërisht të saj, duke argumentuar si më poshtë vijon:

"Kërkesë 6:
Kërkojmë: Korrigjim i kodit CPV me kodin e saktë dhe rishpallje e njoftimit nëse kodi i pasaktë ka kufizuar aksesueshmerine e procedurës.

<u>Përgjigja e Komisionit të Shqyrtimit të Ankesave</u>
Në lidhje me pretendimet e ngritura përsa i përket Kodit CPV, ku është kërkuar se:
Kodi sipas Fjalorit të Përbashkët të Prokurimit Paketa softëare për sisteme financiare 48442000-8
Komisioni i Shqyrtimit të Ankesës bëri verifikimin e kodit CPV të përcaktuar në dokumentat standarte të procedurës nga ku rezultoi se kodi i përdorur është për "Paketa softëare për sisteme financiar", kodi i saktë për këtë procedurë prokurimi është 48730000-4 "Paketa softëare për siguri"
<u>Pretendimet mbi këtë pikë vlerësohet si i drejtë nga "Komisioni i Shqyrtimit të Ankesës".</u>

...

c) Autoriteti Kontraktor ka specifikuar në Shtojcën 6 "Zgjidhja duhet të ofrojë ruajtje të pakufizuar në cloud (me licencë shtesë)."
Duke qënë se afekton hartimin dhe dorëzimin e ofertës së OE, Ak të saktësojë se çfarë nënkuptoni me përcaktimin Licensë shtesë.

<u>Përgjigja e Komisionit të Shqyrtimit të Ankesave</u>
Me termin "licencë shtesë" Autoriteti Kontraktor nënkupton që funksionaliteti i ruajtjes së pakufizuar në cloud duhet të mbështetet nga zgjidhja e propozuar dhe të jetë i disponueshëm si

opsion/licencë suplementare nga prodhuesi, por nuk konsiderohet pjesë e detyrueshme e licencimit bazë, përveçse nëse operatori ekonomik e përfshin atë në ofertë. Operatori ekonomik duhet të specifikojë qartë në ofertë mënyrën e licencimit, periudhën dhe kushtet përkatese të këtij funksionaliteti..".

II.5. Me anë të shkresën nr. 1060/12 prot, datë 08.06.2026, protokolluar me tonën me nr. 1636/2 prot, datë 10.06.2026, është depozituar nga autoriteti kontraktor në Komisionin e Prokurimit Publik, informacioni lidhur me procedurën e mësipërme të prokurimit, ku autoriteti kontraktor në zbatim të vendimit të Komisionit të Shqyrtimit të Ankesave lidhur me trajtimin e ankesës së operatorit ekonoik "PC STORE" SHPK, si dhe në zbatim të rekomandimeve të Agjencisë së Prokurimit Publik njofton se ka modifikuar dokumentat e tenderit, duke publikuar në sistemin e prokurimeve elektronike shtojcën përkatëse, si dhe vazhdon të mbajë të pezulluar procedurën e prokurimit, si më poshtë vijon:

"***NË SEKSIONIN 2 TË DST;***

PIKA 2.2 ISHTE:
Kodi sipas Fjalorit të Përbashkët të Prokurimit: Paketa softëare për sisteme financiare 48442000-8
PIKA 2.2 BËHET:
Kodi sipas Fjalorit të Përbashkët të Prokurimit: 48730000-4 "Paketa softëare për siguri"

PIKA 2.11 ISHTE:
Kohëzgjatja ***në muaj 48 ose ditë*** *120 (njëqind e njëzet) ditë implementimi i sistemit, 48 (dyzet e tetë) muaj mirëmbajtja e sistemit nga përfundimi i implementiit të sistemit.*
PIKA 2.11 BËHET:
Kohëzgjatja ***në muaj*** □□ ***ose ditë*** □□***,*** *48 (dyzet e tetë) muaj nga data e nënshkrimit të saj. Operatori Ekonomik duhet të përfundojë implementimin e sistemit brenda 4 (katër) muajve nga data e nënshkrimit të kontratës, ndërsa shërbimi i mirëmbajtjes do të ofrohet për pjesën e mbetur të afatit kontraktual.*

<u>NJOFTIMI I SHKURTUAR I KONTRATËS: ISHTE</u>
5. Kodi sipas Fjalorit të Përbashkët të Prokurimit (FPP): Paketa softëare për sisteme financiare 48442000-8
7. Kohëzgjatja e kontratës/marrëveshjes kuadër ose afati për zbatimin e saj: *Afati i ofrimit të shërbimit do të jetë 48 (dyzet e tetë) muaj nga hyrja në fuqi e kontratës, i strukturuar në dy faza, si më poshtë:*

- *120 (njëqind e njëzet) ditë për implementimin dhe konfigurimin e sistemit;*

- *48 (dyzet e tetë) muaj për ofrimin e shërbimit të mirëmbajtjes dhe suportit teknik të sistemit, duke filluar nga përfundimi i implementimit.*

<u>NJOFTIMI I SHKURTUAR I KONTRATËS: BËHET</u>

5. Kodi sipas Fjalorit të Përbashkët të Prokurimit (FPP): 48730000-4 "Paketa softëare për siguri"

7. Kohëzgjatja e kontratës/marrëveshjes kuadër ose afati për zbatimin e saj: *Afati i ofrimit të shërbimit 48 (dyzet e tetë) muaj nga data e nënshkrimit të saj. Operatori Ekonomik duhet të përfundojë implementimin e sistemit brenda 4 (katër) muajve nga data e nënshkrimit të kontratës, ndërsa shërbimi i mirëmbajtjes do të ofrohet për pjesën e mbetur të afatit kontraktual.*

- ***Në shtojcën 6 "FORMULARI I SPECIFIKIMEVE TEKNIKE"*** *të Dokumentave standarte të tenderit****, bëhen këto modifikime****:*

<u>ISHTE:</u>

2. Zgjidhje XDR (Extended Detection and Response)

• të jetë e pajtueshme me sistemet operative si Microsoft Ëindoës, Linux, macOS, Android dhe iOS;

a) Incidentet dhe Integrimi

Zgjidhja duhet të ketë aftësinë për integrim nativ me regjistrat nga fireëall-et (Fortinet, Cisco, Check Point, Palo Alto etj.).

4. Përgjigja ndaj alarmeve madhore.

Nëse operatori ekonomik nuk mund të përcaktojë nëpërmjet informacionit të mbledhur nga procedurat e troubleshooting shkakun e alarmit madhor, atëherë duhet të dërgojë një teknik shërbimi pranë POSTA SHQIPTARE brenda intervalit kohor prej dy (2) orësh nga momenti i marrjes së njoftimit për Alarm Madhor. Me të mbërritur, tekniku do të mbështetet me asistencë nga POSTA SHQIPTARE dhe do t'i jepet liri veprimi në mjediset dhe sistemet e mbuluara, për të filluar menjëherë procedurat e diagnostikimit dhe riparimit.

<u>BËHET:</u>

2. Zgjidhje XDR (Extended Detection and Response)

• të jetë e pajtueshme me sistemet operative si Microsoft Ëindoës, Linux, macOS, Android dhe iOS ***ose ekuivalente;***

a) Incidentet dhe Integrimi

Zgjidhja duhet të ketë aftësinë për integrim nativ me regjistrat nga fireëall-et (Fortinet, Cisco, Check Point, Palo Alto etj.) ***ose ekuivalente;***

4. Përgjigja ndaj alarmeve madhore.

Nëse operatori ekonomik nuk mund të përcaktojë nëpërmjet informacionit të mbledhur nga procedurat e troubleshooting shkakun e alarmit madhor, atëherë duhet sigurojë ndërhyrje të specializuar në vend pranë POSTA SHQIPTARE, me qëllim zgjidhjen e problematikës, brenda intervalit kohor prej dy (2) orësh nga momenti i marrjes së njoftimit për Alarm Madhor. Me të mbërritur, tekniku do të mbështetet me asistencë nga POSTA SHQIPTARE dhe do t'i jepet liri veprimi në mjediset dhe sistemet e mbuluara, për të filluar menjëherë procedurat e diagnostikimit dhe riparimit.

- ***Në Shtojca 9,*** *Kriteret e Veçanta për kualifikim të Dokumentave standarte të tenderit****, bëhen këto modifikime****:*

PIKA 2.3.1. ISHTE:

Operatori ekonomik duhet të paraqesë dëshmi për shërbimet e mëparshme të ngjashme, të kryera gjatë tre viteve të fundit nga data e shpalljes së njoftimit të kontratës, në një vlerë jo më e vogël se 39% e vlerës limit te kontrates qe prokurohet.

Për të vërtetuar përvojën e mëparshme të ngjashme, operatorët ekonomikë duhet të paraqesin dëshmitë e mëposhtme:

a) *për përvojën e mëparshme të realizuar me sektorin publik, operatori ekonomik duhet të paraqesë vërtetime të lëshuara nga një ent publik për përmbushjen me sukses të kontratës, ku të shënohen vlera, afati i përfundimit të kontratës, ose/dhe faturave tatimore të shitjes, të plotësuara sipas kërkesave të legjislacionit në fuqi, dhe të deklaruara në organet tatimore ku shënohen datat, shumat dhe shërbimet e realizuara.*

ose

b) *në rastin e përvojës së mëparshme të realizuar me sektorin privat, si dëshmi pranohen vetëm fatura tatimore të shitjes, të plotësuara sipas kërkesave të legjislacionit në fuqi, dhe të deklaruara në organet tatimore, ku shënohen datat, shumat dhe shërbimet e realizuara.*

Shënim: *Plotësimi i njërit prej dy kushteve të sipërpërmendura e bën ofertën të kualifikuar.*

PIKA 2.3.1. BËHET

Operatori ekonomik duhet të paraqesë dëshmi për shërbimet e mëparshme të ngjashme, të kryera gjatë tre viteve të fundit nga data e shpalljes së njoftimit të kontratës, në një vlerë jo më e vogël se 39% e vlerës limit te kontrates qe prokurohet.

Për të vërtetuar përvojën e mëparshme të ngjashme, operatorët ekonomikë duhet të paraqesin dëshmitë e mëposhtme:

c) *për përvojën e mëparshme të realizuar me sektorin publik, operatori ekonomik duhet të paraqesë vërtetime të lëshuara nga një ent publik për përmbushjen me sukses të kontratës,*

ku të shënohen vlera, afati i përfundimit të kontratës, ***dhe*** *faturave tatimore të shitjes, të plotësuara sipas kërkesave të legjislacionit në fuqi, dhe të deklaruara në organet tatimore ku shënohen datat, shumat dhe shërbimet e realizuara.*

ose

d) *në rastin e përvojës së mëparshme të realizuar me sektorin privat, si dëshmi pranohen vetëm fatura tatimore të shitjes, të plotësuara sipas kërkesave të legjislacionit në fuqi, dhe të deklaruara në organet tatimore, ku shënohen datat, shumat dhe shërbimet e realizuara.*

Shënim: *Plotësimi i njërit prej dy kushteve të sipërpërmendura e bën ofertën të kualifikuar.*

PIKA 2.3.3. ISHTE:

Operatori Ekonomik ofertues duhet të paraqesë Autorizim prodhuesi ose distributor të autorizuar për mallrat objekt prokurimi. Autorizimi duhet të përmbajë të dhëna të plota të prodhuesit si: telefon,e-mail, ëbsite kjo e nevojshme për Autoritetin Kontraktor në rast verifikimi nga ana e tij. Në rast se paraqitet autorizim distributori duhet të provohet lidhja midis prodhuesit dhe distributorit nëpërmjet një dokumenti zyrtar të vlefshëm (kontratë, certifikatë, deklaratë etj).

PIKA 2.3.3. BEHET

Operatori Ekonomik ofertues duhet të paraqesë autorizim nga Prodhuesi ose Distributori i Autorizuar për shitjen e produkteve objekt të këtij prokurimi. Autorizimi i lëshuar nga Prodhuesi ose Distributori i Autorizuar duhet të përmbajë të dhëna të plota mbi objektin dhe numrin e referencës së procedurës, si dhe detaje kontakti. Në rast se autorizimi paraqitet nga Distributori i Autorizuar, duhet të vërtetohet lidhja ndërmjet Prodhuesit dhe Distributorit të Autorizuar.

PIKA 2.3.4. ISHTE:

Për të vërtetuar që operatori ekonomik ka kapacitete njerëzore profesionale të mjaftueshme për realizimin në kohë e cilësi të kontrates, për planifikimin dhe menaxhimin me profesionalizëm të punës, operatori ekonomik ofertues duhet të disponojë staf të kualifikuar me kërkesat si më poshtë:

a) 1 (një) punonjës të pajisur me Certifikate për "Project Manager";
b) 1 (një) specialist te certifikuar CIR "Certified Incident Responder" ose ekuivalente;
c) 2 (dy) specialist te certifikuar per SIEM "Security Information and Event Management" ose ekuivalente;
d) 2 (dy) specialist te certifikuar Penetration Tester ose ekuivalente;
e) 1 (një) specialist te certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente;
f) 1 (një) specialist te certifikuar per Cybersecurity Analist ose ekuivalente;

g) *2 (dy) specialist te certifikuar ne nivel profesional CCNP Routing & Sëitching për rrjetin për te mirëmbajtur pajisjet ekzistuese te rrjetit, ose ekuivalente;*
h) *2 (dy) specialist te certifikuar ne nivel profesional CCNP Security për te mirëmbajtur sistemin ekzistues, ose ekuivalente;*
i) *2 (dy) specialist te certifikuar "Cyber Threat Hunting Professional" ose ekuivalente;*
j) *1 (një) punonjës te pajisur me Certifikate per menaxhimin e sherbimeve ITIL ose ekuivalente;*

Shënim:

- *Një punonjës mund të disponojë më shumë se një certifikim.*
- *Për çdo punonjës të certifikuar të përfshirë, Operatori Ekonomik duhet të paraqesë:*
- *Certifikatat sipas specifikave të mësipërme.*
- *Listëpagesat sipas formatit E-Sig 025 ose Vërtetimin për pagimin e kontributeve për individin (E-Sig 03/a), të konfirmuara nga Drejtoria e Tatimeve që vërtetojnë se punonjësi ka qenë i punësuar pranë operatorit ekonomik të paktën e muajin fundit nga data e fillimit të kësaj procedure.*

PIKA 2.3.4. BEHET

Për të vërtetuar që operatori ekonomik ka kapacitete njerëzore profesionale të mjaftueshme për realizimin në kohë e cilësi të kontrates, për planifikimin dhe menaxhimin me profesionalizëm të punës, operatori ekonomik ofertues duhet të disponojë staf të kualifikuar me kërkesat si më poshtë:

a) ***1 (një) punonjës të pajisur me Certifikate për "Project Manager" ose ekuivalente;***
b) *1 (një) specialist te certifikuar CIR "Certified Incident Responder" ose ekuivalente;*
c) *2 (dy) specialist te certifikuar per SIEM "Security Information and Event Management" ose ekuivalente;*
d) *2 (dy) specialist te certifikuar Penetration Tester ose ekuivalente;*
e) *1 (një) specialist te certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente;*
f) *1 (një) specialist te certifikuar per Cybersecurity Analist ose ekuivalente;*
g) *2 (dy) specialist te certifikuar ne nivel profesional CCNP Routing & Sëitching për rrjetin për te mirëmbajtur pajisjet ekzistuese te rrjetit, ose ekuivalente;*
h) *2 (dy) specialist te certifikuar ne nivel profesional CCNP Security për te mirëmbajtur sistemin ekzistues, ose ekuivalente;*
i) *2 (dy) specialist te certifikuar "Cyber Threat Hunting Professional" ose ekuivalente;*
j) *1 (një) punonjës te pajisur me Certifikate per menaxhimin e sherbimeve ITIL ose ekuivalente;*

Shënim:

- *Një punonjës mund të disponojë më shumë se një certifikim.*

- *Për çdo punonjës të certifikuar të përfshirë, Operatori Ekonomik duhet të paraqesë:*
- *Certifikatat sipas specifikave të mësipërme.*
- *Listëpagesat sipas formatit E-Sig 025 ose Vërtetimin për pagimin e kontributeve për individin (E-Sig 03/a), të konfirmuara nga Drejtoria e Tatimeve që vërtetojnë se punonjësi ka qenë i punësuar pranë operatorit ekonomik të paktën për muajin **Prill** nga data e fillimit të kësaj procedure.*

Shënim: *Kjo procedurë mbetet e pezulluar, dhe në mbështetje të nenit 75 të Ligjit 162/2020 "Për Prokurimet Publike" (i ndryshuar), do të njoftohet data për hapjen e ofertave.*
Kjo shtojcë e modifikimeve bëhet pjesë e dokumentacionit standart të tenderit.
Dokumentat e tjera të procedurës së prokurimit ngelen të pandryshuara.
Duke Ju falëndëruar për mirëkuptimin, ".

II.6. Me shkresën e datës 11.06.2026 me objekt "*Kërkesë për ndërhyrje të menjëhershme për pezullimi të procedurës së prokurimit, nr. REF-85701-05-14-2026, referuar ankesës në proces shqyrtimi A/2026/6720"* dërguar nëpërmjet sistemit elektronik të ankesa dhe protokolluar me tonën me nr. 1636/3 prot, datë 11.06.2026, operatori ekonomik ankimues "PC STORE" SHPK njofton Komisionin e Prokurimit Publik lidhur me shpezullimin e procedurës dhe publikimin e shtojcës për modifikimin e dokumentave të tenderit nga ana e autoritetit kontraktor, si dhe kërkon si më poshtë vijon;

"*.. Për sa më sipër, dhe bazuar në dispozitat ligjore në fuqi, kërkojme ndermarrjen e veprimeve te menjehershem nga Agjencia e Prokurimit Publik dhe Komisioni i Prokurimit Publik:*
1. Konstatimin e shkeljes së Ligjit nr.162/2020 "Për Prokurimin Publik" nga Autoriteti Kontraktor Posta Shqiptare sh.a.;
2. Konstatimin se vendimi i datës 09.06.2026 për çpezullimin e procedurës është marrë në mungesë kompetence ligjore;
3. Urdhërimin e pezullimit të menjëhershëm të procedurës së prokurimit deri në përfundimin e shqyrtimit të ankesës nr. A/2026/6720;
4. Konstatimin e pavlefshmërisë së veprimeve të ndërmarra nga Autoriteti Kontraktor pas datës së paraqitjes së ankesës në KPP;
5. Urdhërimin që data e ofertimit e publikuar nga Autoriteti Kontraktor për datën 15.06.2026 të mos prodhojë pasoja juridike deri në përfundimin e shqyrtimit të ankimit nga KPP. ".

III

Komisioni i Prokurimit Publik

pas shqyrtimit të pretendimeve të operatorit ekonomik ankimues, informacionit dhe dokumentacionit të paraqitur nga autoriteti kontraktor,

Arsyeton:

III.1. Lidhur me pretendimin e operatorit ekonomik ankimues "*PC STORE*" SHPK për modifikimin e dokumenteve të tenderit lidhur me përcaktimin e saktë të kodit CPV në pikën 2.2 "*Kodi sipas Fjalorit të Përbashkët të Prokurimit*" të Seksionit 2 "*Objekti i kontratës*" të dokumentave të tenderit dhe lidhur me kërkesën për sqarim përsa i përket termit "*Licensë shtesë*" të përcaktuar në Shtojcën 6 "*FORMULARI I SPECIFIKIMEVE TEKNIKE*" të dokumentave të tenderit, si në vijim: "*Kërkesë 6:*
Kërkojmë: Korrigjim i kodit CPV me kodin e saktë dhe rishpallje e njoftimit nëse kodi i pasaktë ka kufizuar aksesueshmerine e procedurës.
c) Autoriteti Kontraktor ka specifikuar nëe Shtojcëen 6 "Zgjidhja duhet të ofrojë ruajtje të pakufizuar në cloud (me licencë shtesë)."
Duke qëenëe se afekton hartimin dhe dorëezimin e ofertëes sëe OE, Ak tëe saktëesojëe se çfarëe nëenkuptoni me pëercaktimin Licensëe shtesëe..", të parashtruara në formularin e ankesës të ankimit elektronik me numër A/2026/6720, datë 25.05.2026 dhe me numër protokolli nr. 1636/2026 prot., datë 26.05.2026, Komisioni i Prokurimit Publik vëren se,

III.1.1. Referuar informacionit të autoritetit kontraktor me anë të shkresën nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, është depozituar nga autoriteti kontraktor në Komisionin e Prokurimit Publik, informacioni lidhur me procedurën e mësipërme të prokurimit, si dhe vendimarrja për trajtimin e ankesës së operatorit ekonomik ankimues "*PC STORE*" SHPK, në të cilin konstatohet se Komisioni i Shqyrtimit të Ankesës ka vendosur pranimin pjesërisht të saj, duke argumentuar si më poshtë vijon:

"Kërkesë 6:
Kërkojmë: Korrigjim i kodit CPV me kodin e saktë dhe rishpallje e njoftimit nëse kodi i pasaktë ka kufizuar aksesueshmerine e procedurës.

<u>Përgjigja e Komisionit të Shqyrtimit të Ankesave</u>
Në lidhje me pretendimet e ngritura përsa i përket Kodit CPV, ku është kërkuar se:
Kodi sipas Fjalorit të Përbashkët të Prokurimit Paketa softëare për sisteme financiare 48442000-8
Komisioni i Shqyrtimit të Ankesës bëri verifikimin e kodit CPV të përcaktuar në dokumentat standarte të procedurës nga ku rezultoi se kodi i përdorur është për "Paketa softëare për sisteme

financiar", kodi i saktë për këtë procedurë prokurimi është 48730000-4 "Paketa softëare për siguri"
Pretendimet mbi këtë pikë vlerësohet si i drejtë nga "Komisioni i Shqyrtimit të Ankesës".

...

c) Autoriteti Kontraktor ka specifikuar nëe Shtojcëen 6 "Zgjidhja duhet të ofrojë ruajtje të pakufizuar në cloud (me licencë shtesë)."
Duke qëenëe se afekton hartimin dhe dorëezimin e ofertëes sëe OE, Ak tëe saktëesojëe se çfarëe nëenkuptoni me pëercaktimin Licensëe shtesëe.

Përgjigja e Komisionit të Shqyrtimit të Ankesave
Me termin "licencë shtesë" Autoriteti Kontraktor nënkupton që funksionaliteti i ruajtjes së pakufizuar në cloud duhet të mbështetet nga zgjidhja e propozuar dhe të jetë i disponueshëm si opsion/licencë suplementare nga prodhuesi, por nuk konsiderohet pjesë e detyrueshme e licencimit bazë, përveçse nëse operatori ekonomik e përfshin atë në ofertë. Operatori ekonomik duhet të specifikojë qartë në ofertë mënyrën e licencimit, periudhën dhe kushtet përkatese të këtij funksionaliteti..".

III.1.2. Neni 30 i LPP, i ndryshuar parashikon shprehimisht se: "*1. Komisioni i Prokurimit Publik shqyrton ankesat e paraqitura para tij kur në mbledhje janë të pranishëm të paktën 3 nga 5 anëtarët e tij, një prej të cilëve kryetari ose nënkryetari. Në përfundim të shqyrtimit të ankesave, Komisioni vendos me shumicë votash.*
Vendimi deklarativ i dhënë sipas parashikimeve të nenit 115, pikat 2 dhe 3, të këtij ligji, jepet nga 3 anëtarë për procedurat e prokurimit nën kufirin e ulët monetar dhe nga 5 anëtarët për procedurat e tjera.
Shqyrtimi i ankesave për procedurat e prokurimit nën kufirin e ulët monetar do të bëhet nga 3 anëtarë të Komisionit të Prokurimit Publik.".

III.1.3. Neni 115 pika 1 dhe 2 e ligjit 162/2020 "*Për prokurimin Publik*", i ndryshuar i cili parashikon shprehimisht se:

"*1. Komisioni i Prokurimit Publik shqyrton ankesën e paraqitur, si dhe vendimin e autoritetit ose entit kontraktor, së bashku me dokumentet dhe shpjegimet shoqëruese, që mbështesin këtë vendim si më poshtë:*
a) në rastet kur autoriteti ose enti kontraktor ka vendosur pranimin pjesërisht të ankesës, Komisioni i Prokurimit Publik vazhdon shqyrtimin: i. për pjesën e ankesës/ pretendimeve që nuk janë pranuar; ii. e ankesës/ankesave për pjesën që është pranuar, nëse ka ankesa nga operatorët

ekonomikë të interesuar, të cilët kanë paraqitur argumentet e tyre për këtë pjesë në përputhje me nenin 113 të këtij ligji;
b) në rastet kur autoriteti ose enti kontraktor ka vendosur pranimin e plotë të ankesës, Komisioni i Prokurimit Publik do të vijojë shqyrtimin e ankesës, nëse ka ankesë nga operatorët ekonomikë të interesuar, të cilët kanë paraqitur argumentet e tyre në lidhje me ankesën në përputhje me nenin 113 të këtij ligji;
c) në rastet kur autoriteti ose enti kontraktor ka vendosur mos pranimin e ankesës.
2. Në rastin kur autoriteti ose enti kontraktor pranon pjesërisht ankesën për dokumentet e tenderit dhe në rastin e ankesave për vendimin e vlerësimit/klasifikimit kur nuk ka ankesa nga operatorët ekonomikë të interesuar, të cilët kanë paraqitur argumentet e tyre sipas pikës 1 të nenit 113 të këtij ligji, Komisioni i Prokurimit Publik vazhdon procedurën për pjesën tjetër të ankesës dhe me mbylljen e shqyrtimit të çështjes duhet të shprehet me vendimmarrje deklarative për pjesën e pranuar sipas parashikimeve të shkronjës "ç" të pikës 2 të nenit 118 të këtij ligji, së bashku me vendimmarrje për pjesën tjetër.".

III.1.4. Në rastin konkret, Komisioni gjykon, se objekti i pretendimeve të mësipërme të operatorit ekonomik ankimues "*PC STORE*" SHPK, lidhet me kërkesën për modifikimin e dokumenteve të tenderit lidhur me përcaktimin e saktë të kodit CPV në pikën 2.2 "*Kodi sipas Fjalorit të Përbashkët të Prokurimit*" të Seksionit 2 "*Objekti i kontratës*" të dokumentave të tenderit dhe lidhur me kërkesën për sqarim përsa i përket termit "*Licensë shtesë*" të përcaktuar në Shtojcën 6 "*FORMULARI I SPECIFIKIMEVE TEKNIKE*" të dokumentave të tenderit
Gjithashtu, KPP konstaton, se autoriteti kontraktor, në kthimin e përgjigjes të ankesës së operatorit ekonomik si më sipër cituam, rezulton, se e ka pranuar kërkesën e ankimuesit për modifikimin e dokumenteve të tenderit lidhur me përcaktimin e saktë të kodit CPV në pikën 2.2 "*Kodi sipas Fjalorit të Përbashkët të Prokurimit*" të Seksionit 2 "*Objekti i kontratës*" të dokumentave të tenderit, si dhe ka sqaruar ankimuesin përsa i përket termit "*Licensë shtesë*" të përcaktuar në Shtojcën 6 "*FORMULARI I SPECIFIKIMEVE TEKNIKE*" të dokumentave të tenderit.
Duke qenë, se pretendimet e mësipërme të operatorit ekonomik ankimues janë pranuar nga ana e komisionit të shqyrtimit të ankesës pranë autoritetit kontraktor referuar shkresës së autoritetit kontraktor me nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, KPP do të mbyllë shqyrtimin e çështjes në lidhje me kërkesat për sqarim të mësipërme të operatorit ekonomik ankimues, pasi gjykon, se vendimi i dhënë nga KSHA është shterues dhe pranues për operatorin ekonomik ankimues për këto kërkesa të tij.
Autoriteti në zbatim të nenit 75 të ligjit nr. 162/2020 "*Për Prokurimin Publik*", i ndryshuar të publikojë në sistemin e prokurimeve elektronike (SPE) shtojcën me ndryshimet dhe sqarimet e mësipërme, me qëllim që si operatori ekonomik ankimues dhe të gjithë operatorët ekonomik të

interesuar, që shfaqin interes për të marrë pjesë në procedurën e prokurimit, të njihen me këto sqarime.
Sa më sipër, referuar nenit 115 të Ligjit Nr. nr. 162/2020 "Për Prokurimin Publik", i ndryshuar, Komisioni i Prokurimit Publik, vendos të mbyllë çështjen për pjesën e pranuar të ankesës së operatorit ekonomik "*PC STORE*" SHPK dhe do të vazhdojë procedurën e shqyrtimit në themel për pretendimet e tjera të paraqitura në ankesë.

III.2. Lidhur me pretendimin e operatorit ekonomik ankimues "*PC STORE*" SHPK për modifikimin e kriterit kualifikues të përcaktuar në pikën 2.3.4 "Kapaciteti teknik" të Shtojcës 9 "*FORMULAR I I KRITEREVE TË PËRZGJEDHJES/KUALIFIKIMIT*" të dokumentave të tenderit të procedurës së prokurimit objekt ankimi, lidhur me disponimi nga ana e operatorit ekonomik ofertues në stafin e tij 1 (një) specialist tëe certifikuar CIR "Certified Incident Responder" ose ekuivalente, 2 (dy) specialist tëe certifikuar pëer SIEM "Security Information and Event Management" ose ekuivalente, 2 (dy) specialist tëe certifikuar Penetration Tester ose ekuivalente, 1 (një) specialist tëe certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente, 1 (një) specialist tëe certifikuar pëer Cybersecurity Analist ose ekuivalente dhe 2 (dy) specialist tëe certifikuar "Cyber Threat Hunting Professional" ose ekuivalente, duke pretenduar si në vijim : "*Për sa kemi paraqitur më sipër, në dritën e fakteve, bazuar në legjislacionin përkatës, përfundimisht kërkojmë:*
1.Pranimin e ankesës sonë.
2. KËRKESA: ".2.4, pika b "(një) specialist te certifikuar CIR "Certified Incident Responder" ose ekuivalente; , TË HIQET.
3. KËRKESA: "2.2.4, pika d) "(një) specialist te certifikuar CIR "Certified Incident Responder" ose ekuivalente; , TË HIQET.
4. KËRKESA: "2.2.4, pika e "1 (një) specialist të certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente, TË HIQET.
5. KËRKESA: "2.2.4, pika f "1 (një) specialist te certifikuar per Cybersecurity Analist ose ekuivalente; TË HIQET.." Komisioni i Prokurimit Publik vëren se,

III.2.1. Në shtojcën 9 "*FORMULAR I KRITEREVE TË PËRZGJEDHJES/KUALIFIKIMIT*" "*Kriteret e veçanta të kualifikimit*", pika 2.3.4 "*Kapaciteti teknik*", të dokumentave të tenderit nga ana e autoritetit kontraktor është kërkuar që operatorët ekonomikë ofertues të disponojnë në stafin e tyre, punonjësit e kualifikuar si më poshtë vijon:

"*2.3.4 Për të vërtetuar që operatori ekonomik ka kapacitete njerëzore profesionale të mjaftueshme për realizimin në kohë e cilësi të kontrates, për planifikimin dhe menaxhimin me profesionalizëm të punës, operatori ekonomik ofertues duhet të disponojë staf të kualifikuar me kërkesat si më poshtë:*

a) *1 (një) punonjës të pajisur me Certifikate për "Project Manager";*
b) *1 (një) specialist te certifikuar CIR "Certified Incident Responder" ose ekuivalente;*

c) *2 (dy) specialist te certifikuar per SIEM "Security Information and Event Management" ose ekuivalente;*
d) *2 (dy) specialist te certifikuar Penetration Tester ose ekuivalente;*
e) *1 (një) specialist te certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente;*
f) *1 (një) specialist te certifikuar per Cybersecurity Analist ose ekuivalente;*
g) *2 (dy) specialist te certifikuar ne nivel profesional CCNP Routing & Sëitching për rrjetin për te mirëmbajtur pajisjet ekzistuese te rrjetit, ose ekuivalente;*
h) *2 (dy) specialist te certifikuar ne nivel profesional CCNP Security për te mirëmbajtur sistemin ekzistues, ose ekuivalente;*
i) *2 (dy) specialist te certifikuar "Cyber Threat Hunting Professional" ose ekuivalente;*
j) *1 (një) punonjës te pajisur me Certifikate per menaxhimin e sherbimeve ITIL ose ekuivalente;*

Shënim:

- *Një punonjës mund të disponojë më shumë se një certifikim.*
- *Për çdo punonjës të certifikuar të përfshirë, Operatori Ekonomik duhet të paraqesë:*
- *Certifikatat sipas specifikave të mësipërme.*
- *Listëpagesat sipas formatit E-Sig 025 ose Vërtetimin për pagimin e kontributeve për individin (E-Sig 03/a), të konfirmuara nga Drejtoria e Tatimeve që vërtetojnë se punonjësi ka qenë i punësuar pranë operatorit ekonomik të paktën e muajin fundit nga data e fillimit të kësaj procedure.*

Sqarim: Përmbushja e kësaj kërkese në fazën e ofertimit do të bëhet nëpërmjet dorëzimit të formularit përmbledhës të vetëdeklarimit sipas shtojcës përkatëse të DST, sic parashikohet edhe nga pika 1 e nenit 26 të Vendimit të Këshillit të Ministrave Nr. 285, datë 19.05.2021 "Për miratimin e rregullave të Prokurimit Publik" i ndryshuar.".

III.2.2. Në procesverbalin "*PËR ARGUMENTIMIN E KRITEREVE TË VEÇANTA PËR KUALIFIKIM* ", të publikuar në SPE autoriteti kontraktor ka argumentuar vendosjen e këtij kriteri kualifikues, si më poshtë vijon:

"***Argumentim:*** *Në zbatim të nenit 77 të ligjit nr. 162/2020 "Për Prokurimin Publik" (i ndryshuar), si dhe nenit 41 të VKM nr. 285, datë 19.05.2021, (i ndryshuar), Autoriteti Kontraktor ka përcaktuar kriteret për kapacitetet profesionale të operatorëve ekonomikë, me qëllim garantimin e realizimit me sukses të kontratës, sigurimin e vazhdimësisë së shërbimeve kritike të teknologjisë së informacionit dhe sigurisë kibernetike, si dhe minimizimin e riskut operacional që mund të sjellë ndërprerja ose kompromet imi i sistemeve ekzistuese të Autoritetit Kontraktor.*

Kërkesat për personelin e certifikuar janë në përpjesëtim me natyrën, kompleksitetin dhe rëndësinë e shërbimeve objekt prokurimi, të cilat lidhen drejtpërdrejt me administrimin, monitorimin, mbrojtjen dhe mirëmbajtjen e infrastrukturës kritike teknologjike dhe të sigurisë kibernetike të Autoritetit Kontraktor.

Argumentim për pikën a): *Kërkesa për 1 (një) punonjës të pajisur me certifikim "Project Manager" ose ekuivalent është vendosur për të garantuar menaxhimin, planifikimin, koordinimin dhe ndjekjen me profesionalizëm të realizimit të kontratës gjatë gjithë periudhës së zbatimit të saj. Ky certifikim siguron që operatori ekonomik disponon kapacitetet e nevojshme menaxheriale për administrimin eficient të proceseve, burimeve njerëzore dhe afateve të realizimit të shërbimeve objekt prokurimi.*

Argumentim për pikën b): *Kërkesa për 1 (një) specialist të certifikuar CIR "Certified Incident Responder" ose ekuivalent është e nevojshme për garantimin e kapaciteteve profesionale në identifikimin, analizimin dhe menaxhimin e incidenteve të sigurisë kibernetike. Ky specialist është i domosdoshëm për të siguruar reagim të shpejtë dhe efektiv ndaj incidenteve që mund të cenojnë integritetin, konfidencialitetin dhe disponueshmërinë e sistemeve dhe të dhënave të Autoritetit Kontraktor.*

Argumentim për pikën c) *Kërkesa për 2 (dy) specialistë të certifikuar për SIEM "Security Information and Event Management" ose ekuivalent është vendosur për të garantuar monitorimin, analizimin dhe menaxhimin në kohë reale të ngjarjeve dhe incidenteve të sigurisë kibernetike në infrastrukturën teknologjike të Autoritetit Kontraktor. Këta specialistë do të kontribuojnë në identifikimin dhe menaxhimin e rreziqeve, si dhe në forcimin e kapaciteteve të AK-së për kundërpërgjigje ndaj sulmeve kibernetike. Duke qenë se shërbimet lidhen me sisteme kritike dhe me volum të konsiderueshëm të të dhënave dhe log-eve, kjo kërkesë është në përputhje me kompleksitetin e infrastrukturës ekzistuese dhe rëndësinë e garantimit të vijueshmërisë dhe sigurisë operacionale.*

Argumentim për pikën d) *Kërkesa për 2 (dy) specialistë të certifikuar "Penetration Tester" ose ekuivalent është vendosur për realizimin e testimeve të sigurisë, identifikimin paraprak të dobësive potenciale dhe analizimin e vulnerabiliteteve në sistemet dhe rrjetet ekzistuese të Autoritetit Kontraktor. Këta specialistë do të kontribuojnë në evidentimin dhe adresimin e rreziqeve që mund të shfrytëzohen nga sulme kibernetike, si dhe në forcimin e kapaciteteve të AK-së për mbrojtje dhe kundërpërgjigje ndaj incidenteve të sigurisë. Gjithashtu, ekspertiza e tyre mbështet implementimin e praktikave, procedurave dhe politikave të sigurisë kibernetike, në përputhje me kompleksitetin e infrastrukturës teknologjike ekzistuese dhe rëndësinë e garantimit të vijueshmërisë operacionale të sistemeve.*

Argumentim për pikën e) *Kërkesa për 1 (një) specialist të certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalent është vendosur për të garantuar ekspertizë të avancuar në analizimin e sigurisë së sistemeve, identifikimin e vulnerabiliteteve dhe realizimin e testimeve praktike të penetrimit. Ky specialist do të kontribuojë në forcimin e kapaciteteve të AK-së për mbrojtje dhe kundërpërgjigje ndaj sulmeve kibernetike, si dhe në implementimin e praktikave, procedurave dhe politikave të sigurisë kibernetike për mbrojtjen e sistemeve dhe të dhënave digjitale.*

Argumentim për pikën f) *Kërkesa për 1 (një) specialist të certifikuar "Cybersecurity Analyst" ose ekuivalent është e nevojshme për të vënë në zbatim ekspertizën e tij profesionale analizuese, monitoruese, raportuese dhe trajnuese, me qëllim forcimin e mbrojtjes ndaj sulmeve dhe rreziqeve kibernetike që mund të cenojnë sistemet dhe të dhënat digjitale të AK-së. Ky specialist do të kontribuojë në identifikimin, analizimin dhe menaxhimin e incidenteve të sigurisë, si dhe në implementimin e praktikave, procedurave dhe politikave të sigurisë kibernetike, duke mbështetur AK-në në rritjen e kapaciteteve të saj për kundërpërgjigje dhe garantimin e sigurisë operacionale të sistemeve.*

Argumentim për pikën g) *Kërkesa për 2 (dy) specialistë të certifikuar në nivel profesional CCNP Routing & Sëitching ose ekuivalent është vendosur për të suportuar dhe mirëmbajtur zgjidhjen e ofertuar, duke garantuar vijueshmërinë e shërbimit dhe mosndërprerjen e proceseve të punës së AK-së. Duke qenë se certifikimet e kompanisë multinacionale CISCO janë të specializuara dhe të dedikuara për teknologji specifike të rrjetit, kërkohet që certifikimet e paraqitura të jenë të një natyre ekuivalente me kërkesat e AK-së. Këta specialistë janë të nevojshëm për implementimin, suportin dhe mirëmbajtjen e infrastrukturës ekzistuese të rrjetit, e cila paraqet kompleksitet dhe shtrirje të konsiderueshme operacionale.*

Argumentim për pikën h) *Kërkesa për 2 (dy) specialistë të certifikuar në nivel profesional CCNP Security ose ekuivalent është e nevojshme për të garantuar administrimin, konfigurimin, monitorimin dhe mirëmbajtjen e vazhdueshme të infrastrukturës së sigurisë së rrjetit dhe sistemeve ekzistuese të AK-së. Specialistët kërkohen për të implementuar, suportuar si dhe për të mirëmbajtur zgjidhjen ekzistuese, e cila është relativisht voluminoze dhe me kohështrirje vjetore.*

Argumentim për pikën i) *Kërkesa për 2 (dy) specialistë të certifikuar "Cyber Threat Hunting Professional" ose ekuivalent është vendosur për të garantuar identifikimin, analizimin dhe parandalimin proaktiv të kërcënimeve kibernetike, si dhe për të siguruar mosndërprerjen e shërbimit dhe vijueshmërinë e punës së AK-së. Duke qenë se këto certifikime janë të*

specializuara dhe të dedikuara për sigurinë kibernetike, kërkohet që specialistët e paraqitur të disponojnë certifikime të përshtatshme dhe ekuivalente me kërkesat e AK-së.

Argumentim për pikën j) *Kërkesa për 1 (një) punonjës të pajisur me certifikim për menaxhimin e shërbimeve ITIL ose ekuivalent është vendosur për të garantuar menaxhimin efikas të shërbimeve IT, si dhe mosndërprerjen e shërbimit dhe vijueshmërinë e punës së AK-së. Duke qenë se këto certifikime janë të specializuara dhe të dedikuara për menaxhimin e shërbimeve të teknologjisë së informacionit, kërkohet që specialisti i paraqitur të disponojë certifikim në përputhje me kërkesat e AK-së. Kjo kërkesë synon të garantojë që operatorët ekonomikë të disponojnë staf të specializuar për menaxhimin, koordinimin dhe monitorimin e proceseve dhe shërbimeve IT*.".

III.2.3. Në shtojcën 6 "*FORMULAR I SPECVIFIKIMEVE TEKNIKE*", të dokumentave të tenderit nga ana e autoritetit kontraktor janë publikuar specifikimet teknike të objektit të prokurimit objekt ankimi, si më poshtë vijon:

Shtojca 6.

[Shtojcë për t'u plotësuar nga Autoriteti/Enti Kontraktor]

FORMULARI I SPECIFIKIMEVE TEKNIKE

Specifikimet Teknike të shërbimeve objekt i prokurimit, duhet të përshkruhen sa më saktë dhe plotësisht, për sa të jetë e mundur, duke krijuar kushte për konkurrencë të paanshme dhe të hapur midis të gjithë kandidatëve dhe ofertuesve. Specifikimet teknike, me përjashtim të rasteve plotësisht të justifikuara, duhet të hartohen në mënyrë të tillë që të marrin parasysh kriteret e aksesit për personat me aftësi të kufizuara ose projektimin për të gjithë përdoruesit, siç kërkohet nga ligji në fuqi.

SHËNIM: Në Specifikimet Teknike, nuk duhet të përshkruhet asnjë markë specifike prodhimi ose burim ose proces i veçantë, që karakterizon produktet ose shërbimet e ofruara nga një Operator specifik Ekonomik ose ndonjë markë tregtare, patentë, tip ose origjinë ose prodhim specifik, për të favorizuar ose eliminuar ndërmarrje ose produkte të caktuara. Një gjë e tillë lejohet vetëm në raste të jashtëzakonshme kur nuk ekziston një mënyrë e mjaftueshme, e saktë ose e kuptueshme për të përshkruar objektin e Kontratës. Referencat e tilla duhet të shoqërohen me fjalët "ose ekuivalent".

Në hartimin e specifikimeve teknike, autoritetet /entet kontraktore mbajnë në konsideratë detyrimet e përcaktuara në legjislacionin përkatës në fushat, si më poshtë:

a) Kërkesat minimale të performancës së energjisë, siç përcaktohet në legjislacionin në fuqi për efiçencën e energjisë dhe për performancën energjetike në ndërtesa, konsumin e energjisë dhe

burimeve të tjera të produkteve me ndikim në energji, përfshirë parashikimet për përdorimin e etiketave për produktet me ndikim në energji;
b) Specifikimet teknike për produkte të caktuara, siç përcaktohet në aktet ligjore dhe nënligjore të fushës me qëllim përmirësimin e performancës energjetike dhe uljen e ndikimit;
c) Çdo parashikim tjetër që buron nga legjislacioni mjedisor, energjetik, social dhe i punës.

Skicimet, parametrat teknik etj:
Specifikimi i Materialeve:
Përshkrimi i kërkesave të zbatimit të shërbimeve në lidhje me to:

1. Shërbimi për rinovimin e garancisë dhe licencave të pajisjeve Fireëall
Operatori ekonomik duhet të realizojë rinovimin e garancisë dhe mbështetjes teknike për pajisjet e sigurisë FortiGate-401F dhe FortiGate-601F për një periudhë prej 48 (dyzet e tetë) muajsh, duke filluar nga data e lidhjes së kontratës. Në të njëjtën kohë, operatori ekonomik duhet të sigurojë rinovimin e licencave të tipit "Unified Threat Protection (UTP)" për këto pajisje për të njëjtën periudhë kohore.
Pajisjet për të cilat kërkohet ky shërbim identifikohen përmes numrave serialë përkatës, konkretisht:
***Numrat Serial FortiGate-401F:** FG4H1FT923903187; FG4H1FT923903005;*
***Numrat Serial FortiGate-601F:** FG6H1FTB22906053; FG6H1FTB22905816*

2. Zgjidhje XDR (Extended Detection and Response)
Autoriteti Kontraktor kërkon implementimin e një zgjidhjeje të avancuar të tipit XDR (Extended Detection and Response), e cila duhet të jetë në gjendje të mbrojë minimalisht 1200 stacione pune përmes një agjenti të vetëm të instaluar në pikat fundore

Zgjidhja duhet të:
• ketë aftësinë e regjistrimit dhe integrimit përmes një konsole të vetme menaxhimi me platforma të rrjetit (si Syslog dhe Ëindoës Event Collection);
• ketë aftësinë për zbulimin e kërcënimeve të avancuara, reagim të shpejtë ndaj incidenteve dhe monitorimin e vazhdueshëm të të gjitha stacioneve të punës;
*• ketë aftësinë për të identifikuar sjellje të dyshimta dhe kompromet*ime të mundshme, si dhe izolimin e kërcënimeve dhe lehtësimin e korrigjimit për të ruajtur integritetin dhe sigurinë e infrastrukturës së IT-së;
• të jetë e pajtueshme me sistemet operative si Microsoft Ëindoës, Linux, macOS, Android dhe iOS;

• të përfshijë agjentë softuerësh që mund të instalohen dhe të ekzekutohen në mënyrë të kontrolluar në pikat fundore fizike ose virtuale (serverë, stacione pune, laptopë, pajisje mobile), si dhe një platformë të centralizuar për menaxhimin e agjentëve.

a) Incidentet dhe Integrimi

Zgjidhja duhet të ketë aftësinë për integrim nativ me regjistrat nga fireëall-et (Fortinet, Cisco, Check Point, Palo Alto etj.).

Zgjidhja duhet të ketë aftësinë për të kombinuar alarmet e rrjetit nga pajisjet e lartpërmendura me alarmet nga pikat fundore për të realizuar korrelacion dhe për të arritur një kontekst më të mirë të sigurisë.

Zgjidhja duhet të përfshijë një periudhë minimale ruajtjeje prej 30 ditësh për të dhënat e papërpunuara të marra nga agjentët dhe të ofrojë mundësinë e ruajtjes në cloud për një periudhë nga 6 deri në 12 muaj përmes një licence shtesë.

Zgjidhja duhet të ofrojë menaxhim incidentesh ku të gjithë përdoruesit, stacionet, proceset dhe alarmet e përfshira mund të vizualizohen në mënyrë të plotë.

Zgjidhja duhet të ofrojë mundësinë e caktimit të një analisti sigurie për një incident specifik.

Zgjidhja duhet, në mënyrë native, të përdorë të dhënat e rrjetit për të identifikuar pikat fundore pa agjent të instaluar.

Zgjidhja duhet të ketë aftësi nisjeje të shpejtë, duke ofruar shkurtore drejt zonave të ndryshme të konsolës së menaxhimit.

Zgjidhja duhet të ofrojë mundësinë e integrimit të alarmeve të shumëfishta dhe lidhjes automatike të tyre në një incident të vetëm kur është e nevojshme.

Zgjidhja duhet të ofrojë shfaqjen e burimeve të inteligjencës së kërcënimeve në pamjen e incidentit (të paktën VirusTotal).

Zgjidhja duhet të lejojë modifikimin manual të nivelit të incidentit (i lartë / mesatar / i ulët).

Zgjidhja duhet të lejojë eksportimin e alarmeve dhe incidenteve në skedar.

Zgjidhja duhet të lejojë krijimin dhe redaktimin e "Indicators of Attack / Behaviour Indicators of Compromise" nga ndërfaqja grafike e menaxhimit.

Zgjidhja duhet të lejojë shikimin dhe redaktimin e rregullave të paracaktuara të këtyre indikatorëve të ofruara nga prodhuesi.

b) Zbulimi dhe Parandalimi i Kërcënimeve

Zgjidhja duhet të jetë në gjendje të parandalojë exploit-e bazuar në teknikat specifike të Linux-it, si Brute Force Protection, Java Deserialization, Privilege Escalation, Reverse Shell Protection, ROP Mitigation, Shellcode Protection dhe SO Hijacking Protection.

Zgjidhja duhet të jetë në gjendje të parandalojë exploit-e bazuar në teknikat specifike të macOS, si Anti-Ransomëare, Dylib Hijacking Protection, Gatekeeper Enhancement, JIT Mitigation, Privilege Escalation dhe ROP Mitigation.

Zgjidhja duhet të ofrojë mundësinë për të shtuar procese në Ëindoës, Linux dhe macOS që do të mbrohen nga moduli i mbrojtjes së exploit-eve.
Zgjidhja duhet të ofrojë mbrojtje kundër sulmeve ndaj MBR-së.
Zgjidhja duhet të lejojë dërgimin automatik të skedarëve të panjohur në sandbox cloud për analizë dhe të ofrojë raporte të detajuara të analizës.
Zgjidhja duhet të mbështesë skedarë deri në 100 MB për analizë në sandbox.
Zgjidhja duhet të mbështesë sandboxing në bare-metal për rastet e anashkalimit të sandbox-it.
Zgjidhja duhet të lejojë krijimin e përjashtimeve për exploit-e bazuar në MITRE ATT&CK pa çaktivizuar mbrojtjen globale.
Zgjidhja duhet të lejojë vizualizimin e proceseve të mbrojtura në sistemet operative nga konsola qendrore.
Zgjidhja duhet të krijojë automatikisht incidente dhe të përfshijë hostet dhe përdoruesit përkatës.
Zgjidhja duhet të lejojë vendosjen manuale të një score incidenti nga 0 deri në 100.
Zgjidhja duhet të ofrojë vizualizim të informacionit të kërcënimeve sipas IP-ve, gjeolokacionit dhe rrjetit.
Zgjidhja duhet të ofrojë mbrojtje kundër reverse shell në Linux.
Zgjidhja duhet të ofrojë mbrojtje UEFI kundër sulmeve para nisjes.
Zgjidhja duhet të mbështesë mbrojtjen ndaj restart-it në Safe Mode.
Zgjidhja duhet të ofrojë modul të dedikuar kundër ransomëare për Ëindoës dhe macOS.
Zgjidhja duhet të ofrojë mbrojtje për IIS.
Zgjidhja duhet të mbështesë mbrojtjen ndaj bypass-it të UAC.
Zgjidhja duhet të mbrojë shellcode për procese 32-bit në Ëindoës.
Zgjidhja duhet të ofrojë gjuhë të avancuar query për analiza të dhënash dhe incidente.
Zgjidhja duhet të lejojë konvertimin e query-ve në format JSON.

c) Aftësitë Forensics
Zgjidhja duhet të lejojë mbledhjen e artefakteve për analiza forensics në Ëindoës dhe macOS për minimumi 50 agjentë.
Zgjidhja duhet të përdorë të njëjtin agjent për mbrojtje dhe forensics.
Zgjidhja duhet të ruajë log-et e auditimit dhe hetimit deri në një vit.

d) Izolimi në nivel agjenti
Zgjidhja duhet të lejojë izolimin e stacioneve të shumta me agjent të instaluar në të njëjtën kohë dhe njëkohësisht.
Zgjidhja duhet të lejojë anulimin e izolimit të stacioneve të shumta me agjentin e instaluar në të njëjtën kohë dhe njëkohësisht.
Zgjidhja duhet të pranojë një listë të proceseve të lejuara dhe adresave IPv4/IPv6 me të cilat stacioni mund të komunikojë gjatë një periudhe kur izolimi është aktiv në stacionin e punës.

e) Përgjigje në kohë reale

Zgjidhja duhet të lejojë ekzekutimin e skripteve Python në stacionet e punës Ëindoës, Linux ose Mac OS me agjentin e instaluar, pa pasur nevojë që Python të instalohet në stacionin përkatës të punës.

Zgjidhja duhet të ofrojë mundësinë për të ekzekutuar skripte Python të personalizuara në stacione me një agjent të instaluar (duke përfshirë stacionet Ëindoës).

Zgjidhja duhet të ofrojë mundësinë për të ekzekutuar komandat CMD dhe PoëerShell të Ëindoës për stacionet e punës me Ëindoës të instaluar.

Zgjidhja duhet të shfaqë menaxhimin e detyrave (task-eve) në ekran të plotë me të gjitha proceset në ekzekutim dhe të lejojë ndalimin, vendosjen në pauzë ose shkarkimin si skedar të cilitdo nga proceset në memorie.

Zgjidhja duhet të lejojë shfletimin e skedarëve në cilindo prej agjentëve duke përdorur ndërfaqen e menaxhimit të centralizuar për të riemërtuar, zhvendosur dhe shkarkuar lehtësisht cilindo prej këtyre skedarëve nga stacionet e punës Ëindoës, Linux ose Mac OS.

Zgjidhja duhet të përfshijë skripte korrigjimi të gatshme për ekzekutim (ekzekutimin e komandave për Ëindoës, Linux dhe MacOS, vendosjen dhe fshirjen e vlerave të regjistrit për stacionet e punës në Ëindoës, ndalimin e proceseve për Ëindoës, Linux dhe MacOS).

f) Niveli i inteligjencës së kërcënimit

Zgjidhja duhet të ofrojë mundësinë e integrimit dhe furnizimit me rrjedha të dhënash që lidhen me treguesit e kompromentimit dhe informacionin e kërcënimit, siç është VirusTotal.

Zgjidhja duhet të ofrojë vlerësime dhe raporte mbi të gjitha mostrat e ekzekutuara automatikisht në pikat fundore.

g) Kontrolli i pajisjeve USB

Zgjidhja duhet të ofrojë mbrojtje kundër pajisjeve të infektuara (p.sh., USB-ve) kur lidhen me pajisje Ëindoës dhe Mac OS.

h) Kriptimi i diskut

Zgjidhja duhet të ofrojë mbështetje për enkriptimin e diskut për pajisjet Mac OS dhe Ëindoës.

Zgjidhja duhet të ofrojë mbështetje për menaxhimin e pajisjeve të enkriptimit të diskut nga e njëjta konsolë menaxhimi e unifikuar, pa pasur nevojë për një konsolë menaxhimi të jashtme.

Zgjidhja duhet të ofrojë mbështetje për aplikimin dhe zbatimin e profileve të enkriptimit dhe dekriptimit në stacionet e agjentëve për sistemet operative Ëindoës dhe Mac OS.

i) Raporte dhe panele specifike

Zgjidhja duhet të ofrojë mbështetje për panele të personalizueshme.

Zgjidhja duhet të mbështesë gjenerimin e raporteve të personalizueshme dhe të ketë aftësinë për t'u eksportuar.
Zgjidhja duhet të mbështesë gjenerimin e raporteve në formatin PDF.
Zgjidhja duhet të ofrojë modele raportesh të paracaktuara (të gatshme për përdorim) për të ofruar shpejt një pamje holistike të mjedisit dhe me mundësinë e ruajtjes dhe eksportimit.
Zgjidhja duhet të ofrojë mundësinë e krijimit të ëidget-eve duke përdorur gjuhën e skriptimit të zgjidhjes së ofruar.
Zgjidhja duhet të ofrojë mundësinë e krijimit të ëidget-eve të personalizuara që mund të përdoren nga analistët e sigurisë në panele të ndryshme.
Zgjidhja duhet të lejojë filtrimin e të dhënave në të gjitha ëidget-et në panelin e kontrollit, si dhe mundësinë e thellimit me ndryshime kontekstuale që do të përdoren në rastin e një hetimi specifik (panelet dinamike të kontrollit).

j) Mbështetje API
Zgjidhja duhet të ofrojë mbështetje për ekzekutimin e skripteve Python dhe fragmenteve të kodit Python (shablloneve) nëpërmjet API-ve.
Zgjidhja duhet të ofrojë mbështetje për kufizimin e aksesit në API bazuar në adresën IP.

k) Funksionalitete të nivelit enterprise
Zgjidhja duhet të ofrojë mbështetje për aktivizimin ose çaktivizimin e dukshmërisë së ikonës së agjentit në stacionet në konsolën e menaxhimit.
Zgjidhja duhet të lejojë aktivizimin ose çaktivizimin e njoftimeve për aksesin në terminal me agjentin e instaluar nga konsola e menaxhimit.
Zgjidhja duhet të lejojë personalizimin e njoftimeve/mesazheve në stacionet me një agjent të instaluar.
Zgjidhja duhet të jetë në gjendje të mbrojë plotësisht stacionin e punës pasi agjenti të jetë instaluar, pa pasur nevojë për një rinisje/ristartim.
Zgjidhja e ofruar duhet të jetë në gjendje të ruajë të dhënat dhe regjistrat për ngjarjet EDR në memorien e agjentit lokal edhe pas një rinisjeje për sistemet Ëindoës, Linux dhe Mac OS.
Zgjidhja e ofruar duhet të ketë një qendër të centralizuar veprimi ku një analist sigurie mund të fillojë të gjitha veprimet e disponueshme:
• marrja e skedarëve nga stacionet;
• marrja e regjistrave nga stacionet me agjentë;
• fillimi i një skanimi për programe keqdashëse në një ose më shumë stacione;
• izolimi i një ose më shumë stacioneve;
• ekzekutimi i skripteve;
• shtimi i hasheve për lista lejuese ose bllokuese;
• përmirësimi ose çinstalimi i agjentëve;

• mbështetje për kërkimin dhe shkatërrimin e skedarëve;
• aftësi triazhimi për forenzikë – shkarkimi i të dhënave nga agjenti;
• kërkimi i skedarëve sipas shtegut, madhësisë ose hash-it;
• kërkimi në regjistër;
• kërkimi në log-e;
• mbledhja e imazheve të memories nga agjentët Ëindoës.
Zgjidhja duhet të jetë në gjendje të gjurmojë dhe regjistrojë veprimet e ndërmarra nga analistët e sigurisë, si:
• izolimi i stacionit;
• lidhja e terminalit të drejtpërdrejtë;
• ndërprerja e procesit;
• çinstalimi i agjentit;
• përditësimi i agjentit;
• shtimi i hasheve në lista lejuese ose bllokuese.
Zgjidhja duhet të ofrojë mbështetje për skanimin e planifikuar të programeve keqdashëse.
Zgjidhja duhet të ofrojë mbështetje për kontrollin e aksesit të bazuar në role.
Zgjidhja duhet të ketë një konsolë qendrore të unifikuar për menaxhim dhe reagim ndaj incidenteve.
Zgjidhja duhet të ofrojë ruajtje të pakufizuar në cloud (me licencë shtesë).
Zgjidhja duhet të mbështesë agjentë offline përmes serverëve proxy.
Zgjidhja duhet të mbështesë përditësime peer-to-peer.
Zgjidhja duhet të mbështesë një ndërfaqe të vetme administrative dhe hetimore.
Zgjidhja duhet të ofrojë mbështetje për endpoint-e pa agjent.
Zgjidhja duhet të lejojë krijimin e etiketave dinamike.
Zgjidhja duhet të mbështesë instalimin në:
• Ëindoës 7 SP1, 10, 11;
• Ëindoës Server 2008 R2 SP1;
• Ëindoës Server 2012 & 2012 R2;
• Ëindoës Server 2016;
• Ëindoës Server 2019;
• Ëindoës Server 2022;
• Ëindoës Server 2025;
• macOS 12.x, 13.x, 14.x, 15.x, 16.x;
• Alma Linux, Amazon Linux, CentOS, Oracle Linux, Red Hat Enterprise Linux, Rocky Linux, SUSE Linux Enterprise Server, Ubuntu.
Zgjidhja duhet të ketë një portal online me dokumentacion dhe materiale ndihmëse.

Zgjidhja duhet të përmbushë standardet:

• SOC 2 Type II Plus;
• ISO 27001;
• ISO 27701;
• ISO 27017;
• ISO 27018;
• ISO 27032.

l) Licencimi

Licencimi dhe mbështetja teknike duhet të ofrohen për një periudhë prej 48 muajsh për të paktën 1200 agjentë.

Operatori ekonomik duhet të ofrojë një zgjidhje të plotë "turnkey", e cila është plotësisht e projektuar, ndërtuar, dorëzuar dhe implementuar, dhe është gati për përdorim të menjëhershëm.

3. ZgjidhjeSIEM

a) Kërkesat të përgjithshme

Autoriteti Kontraktor kërkon një zgjidhje që kundërvepron me kërcënimet kibernetike, duke mundësuar zbulimin e tyre me mbështetjen e mekanizmave machine learning, duke siguruar automatizimin dhe orkestrimin e përgjigjeve ndaj kërcënimeve kibernetike.

Zgjidhja duhet të mundësojë konfigurimin on-prem, në të cilin të gjitha funksionalitetet dhe përpunimi i të dhënave do të zhvillohen tërësisht brenda infrastrukturës së autoritetit kontraktor, me funksionalitet të plotë në një zonë të ndarë nga interneti.

Zgjidhja duhet të ketë licencë të përhershme për 1200 asete me mbështetje për një periudhë prej 48 muajsh. Licenca për zgjidhjen e ofruar nuk mund të vendosë kufizime në sasinë e të dhënave të ruajtura, numrin e ngjarjeve të transmetuara (EPS) ose numrin e përdoruesve të kyçur njëkohësisht.

Zgjidhja duhet të ofrohet me 48 muaj mbështetje nga prodhuesi, duke përfshirë ofrimin falas të përditësimeve të softuerit, përditësimeve të kontekstit (duke përfshirë analizuesit, rregullat e korrelacionit dhe manualet) dhe trajtimin e gabimeve.

Është detyrë e operatorit ekonomik të ofrojë një zgjidhje të plotë "turnkey", nga fillimi në fund, e cila është plotësisht e projektuar, ndërtuar, dorëzuar dhe implementuar, dhe është gati për përdorim të menjëhershëm.

Zgjidhja duhet të ketë një ndërfaqe grafike që lejon menaxhimin e përditësimeve të softuerit në internet dhe kontekstit, duke përfshirë rregullat e korrelacionit, manualet, analizuesit, integrimet, udhëzimet e inteligjencës artificiale, listat e referencave dhe profilet UEBA për përdoruesit dhe kompjuterët.

Zgjidhja duhet të ofrojë mundësinë e transmetimit të telemetrisë te prodhuesi në mënyrë që të monitorojë funksionimin e saktë, duke përfshirë, ndër të tjera, komponentët individualë, analizën e ngarkesës së procesorit dhe memories, si dhe regjistrimin e ngjarjeve në disqe.

Zgjidhja duhet të jetë në gjendje të dërgojë një alarm në një adresë të caktuar email-i në rast të dështimit të shërbimit, gabimeve të regjistrimit ose mbingarkesës së burimeve. Shërbimi duhet të funksionojë (24 orë në ditë, 7 ditë në javë).
Instalimi i përditësimeve të reja duhet të jetë plotësisht automatik, duke i ofruar operatorit të paktën dy opsione: "instalo", "instalo dhe aktivizo", të disponueshme si butona ose menu përzgjedhjeje.
Ndërfaqja e zgjidhjes duhet të ketë një mekanizëm të integruar automatik të versionimit që ruan të gjitha versionet historike të kontekstit dhe lejon restaurimin e versioneve të përdorura më parë.
Zgjidhja duhet të sigurojë kontrollin e aksesit në të dhëna dhe funksionalitetet e tyre bazuar në role të përcaktuara (Role-Based Access Control).
Zgjidhja duhet të ofrojë mundësinë për të paraqitur statusin aktual të sigurisë së autoritetit kontraktor, statistikat dhe rezultatet e performancës; pamja dhe paraqitja e komponentëve individualë duhet të mund të personalizohet sipas nevojave të administratorit dhe përdoruesit.
Zgjidhja duhet të mundësojë gjenerimin e raporteve sipas një orari të caktuar dhe dërgimin automatik të tyre në adresat e email-it të një grupi të përcaktuar marrësish.
Zgjidhja duhet të përfshijë një ndërfaqe grafike të thjeshtë për konfigurimin e njoftimeve, duke lejuar përcaktimin e kushteve dhe kanaleve të njoftimit, specifikimin e grupeve të synuara, konfigurimin e agregimit dhe periodicitetit për to.

b) Kërkesat të përgjithshme

Zgjidhja duhet të mundësojë mbledhjen e log-eve të gjeneruara nga sistemet e sigurisë, sistemet e rrjetit, sistemet operative dhe aplikacionet duke përdorur protokollet e mëposhtme: Syslog, TLS Syslog, NetFloë, Ëindoës Event Forëarding, IMAPS, POP3S, MAPI.
Zgjidhja duhet të ketë mekanizma të integruar që sigurojnë mundësinë e shkarkimit të ngjarjeve duke përdorur RestFull API, drajverin ODBC dhe agjentin e leximit të skedarëve.
Zgjidhja duhet të jetë e pajisur me mekanizma për normalizimin (analizimin) e ngjarjeve të fituara, duke mundësuar ndarjen e tyre në fusha individuale, në bazë të të cilave mund të kryhet përpunimi dhe kërkimi i mëtejshëm i tyre në sistem.
Procesi i normalizimit duhet të mbështesë llojet e mëposhtme të sintaksës: CEF, LEEF, URI, SYSLOG, XML, JSON, REGEX dhe një listë çiftesh çelës-vlerë, ku log-et që përmbajnë, për shembull, "user=X" duhet të krijojnë një fushë "user" me vlerën "X".
Procesi i normalizimit të log-eve duhet të përfshijë mekanizma globalë të pasurimit të të dhënave, të përcaktuar në mënyrë të pavarur nga konfigurimi i analizuesve individualë, të cilët shtojnë fusha dhe vlera të reja në log-et e normalizuar bazuar në kushte specifike.
Zgjidhja duhet të jetë e pajisur me një ndërfaqe grafike për krijimin e rregullave shtesë të normalizimit (analizues) për ngjarjet nga burime jo standarde (p.sh., aplikacione proprietare).
Të gjitha log-et duhet të ruhen në formë të kompresuar.

Zgjidhja duhet të jetë në gjendje të njohë automatikisht burimet e log-eve që ridrejtohen tek ajo.
Ajo duhet të njohë automatikisht llojin e log-ut dhe të zgjedhë analizuesin e duhur për të, në mënyrë që të mos kërkohet asnjë veprim nga ana e administratorit.
Zgjidhja duhet të mundësojë ridrejtimin e log-eve në repozitore të ndryshme në varësi të përmbajtjes së tyre, duke përdorur rregulla të bazuara në fushat e ngjarjeve për këtë qëllim.
Zgjidhja duhet të menaxhojë në mënyrë të pavarur ruajtjen e të dhënave dhe të mundësojë arkivimin automatik në repozitore të jashtme të të dhënave.
Zgjidhja duhet të ofrojë mekanizma sigurie për të dhënat e ruajtura në repozitore kundër modifikimit të paautorizuar dhe t'u ofrojë operatorëve mekanizma për të verifikuar integritetin e tyre.
Zgjidhja duhet të regjistrojë dhe ruajë log-et e marra në formë të papërpunuar dhe të standardizuar, si edhe të mundësojë që ato të kërkohen në të dyja format.
Ndërfaqja duhet të paraqesë rezultatet e kërkimit duke përdorur filtra bazuar në vlerat e fushave, shprehjet logjike komplekse, specifikimet e intervalit kohor dhe burimin e të dhënave.
Ndërfaqja e kërkimit duhet të lejojë që pyetjet të ruhen për ripërdorim në të ardhmen.
Ndërfaqja e kërkimit duhet të mbështesë kërkimin me tekst të plotë.
Ndërfaqja e kërkimit duhet të mbështesë kërkimin automatik në repozitore të shumta pavarësisht nga vendndodhja e tyre pa pasur nevojë t'i specifikoni ato.
Zgjidhja duhet të mbështesë punën me log-e në katër mënyra: një pamje tabelare me mundësinë e personalizimit të kolonave të shfaqura, një pamje që paraqet një listë parametrash dhe vlerave të tyre, një pamje të papërpunuar të log-eve dhe një hartë interaktive të rrjetit me funksione të integruara vizualizimi (broëser grafik), i cili:
• të mundësojë akses në kërkimet e log-eve direkt nga menyja e kontekstit të secilit host;
• të lejojë vizualizimin, ndër të tjera, të trafikut të rrjetit, aktivitetit të procesit, modifikimeve të regjistrit dhe komandave të ekzekutuara (shembull: vizualizimi i të gjitha lidhjeve dalëse nga hosti, duke marrë parasysh zonat e sigurisë dhe sistemet e sigurisë);
• të mundësojë gjurmimin e komunikimit, me anë të të cilit analiza e trafikut nga një host në tjetrin, e ndjekur nga trafiku hyrës dhe dalës për hostin e dytë dhe proceset që funksionojnë në të;
• të jetë e disponueshme një menu konteksti nga secili objekt harte në broëser-in grafik, duke i lejuar përdoruesit të kalojë në një pamje tabelare të log-eve, me një filtër të aplikuar bazuar në kërkimin grafik;
• nëpërmjet menusë kontekstuale në kolonat që identifikojnë hostin, duhet të jetë e mundur të kalohet në një broëser grafik në formën e një harte interaktive të rrjetit.
Standardizimi i log-eve duhet të përfshijë një mekanizëm gjeolokacioni që lejon që fushat të pasurohen me emrin ose kodin e vendit duke përdorur bazën e të dhënave të integruar në produkt.

Ndërfaqja për krijimin e analizuesve duhet të ketë një asistent të integruar të inteligjencës artificiale që do të mundësojë gjenerimin automatik të një analizuesi bazuar në një regjistër të papërpunuar.
Shikuesi i log-eve duhet të ketë një asistent të integruar të inteligjencës artificiale që do të mundësojë interpretimin e çdo regjistri të aktivizuar nga menyja e kontekstit.
Zgjidhja duhet të jetë e aftë të instalojë agjentë për sistemet Ëindoës i gjithë spektri i funksionalitetit të agjentëve duhet të jetë i arritshëm nga konsola qendrore e menaxhimit.
Agjenti duhet të kontrollohet plotësisht përmes manualeve, duke mundësuar, ndër të tjera, veprime izolimi dhe bllokimi bazuar në kushtet që lidhen me ngjarjet e analizuara.
Agjenti duhet të mundësojë bllokimin në nivelin kernel.
Agjenti duhet të mbështesë modalitetin e komunikimit one-ëay, në të cilin nuk hap asnjë portë, por vetëm inicion lidhje me konsolën e menaxhimit.
Agjenti duhet të dërgojë gamën e plotë të të dhënave të telemetrisë në konsolën qendrore, duke përfshirë lidhjet e rrjetit, modifikimet e log-eve, nisjet e proceseve dhe komandave, aksesin në skedarë, për qëllime korrelacioni të të dhënave.
Agjenti duhet të mundësojë identifikimin e dobësive në hostin në të cilin do të instalohet.
Zgjidhja duhet të mundësojë korrelacionin e ngjarjeve që burojnë nga sisteme të ndryshme burimore bazuar në çdo fushë dhe variabël regjistri ose çdo të dhënë tjetër.
Zgjidhja duhet të mundësojë lidhjen e ngjarjeve të sigurisë me teknika specifike nga baza e njohurive MITRE ATT&CK dhe të ofrojë mekanizma për filtrimin e ngjarjeve sipas këtyre teknikave.
Zgjidhja duhet të ketë një ndërfaqe grafike për krijimin e rregullave të personalizuara të korrelacionit përgjegjëse për zbulimin e ngjarjeve specifike që ndodhin në sistem.
Rregullat e korrelacionit duhet të:
• lejojnë filtrimin duke përdorur operatorin LIKE dhe përputhjen e modeleve duke përdorur shprehje të rregullta (REGEX);
• marrin në konsideratë parametrat e objekteve në Active Directory, duke lejuar referencën ndaj një objekti të tillë në korrelacion bazuar në ngjarje që nuk përmbajnë informacion rreth tij (p.sh., trafiku i rrjetit që i referohet një llogarie përdoruesi që nuk kërkon fjalëkalim);
• marrin në konsideratë edhe parametrat që nuk përfshihen drejtpërdrejt në ngjarje (p.sh., një rregull që zbulon trafikun nga interneti në një server që është klasifikuar në CMDB si një burim që ofron shërbime ekskluzivisht në rrjetin lokal);
• mbështesin një modalitet dinamik që optimizon performancën përmes korrelacionit selektiv të rregullave (p.sh., nëse regjistri përmban informacion që tregon një ngjarje që lidhet me trafikun e rrjetit, atëherë aktivizohen vetëm rregullat përkatëse);

• kenë një mekanizëm për caktimin statik të tyre te burimet e duhura të log-eve në mënyrë që rregullat e dedikuara për sistemet Ëindoës të mos aktivizohen për burimet që dërgojnë loge nga sistemet Linux

Zgjidhja duhet të jetë plotësisht e konfigurueshme, duke i lejuar operatorit të zgjedhë mënyrën e fillimit të korrelacionit (statik ose dinamik) dhe duhet të përcaktojë kushtet duke përdorur një redaktues grafik për të gjitha paketat e rregullave (politikat).

Zgjidhja duhet të ketë një motor të integruar dhe plotësisht të modifikueshëm për vlerësimin e bazuar në rrezik (risk-score). Ky rrezik duhet të llogaritet veçmas për adresën burimore, adresën e destinacionit dhe llogarinë e përdoruesit të identifikuar të domenit.

Ndërfaqja për krijimin e rregullave të korrelacionit duhet të lejojë gjenerimin e emrave dhe përshkrimeve dinamike të rregullave. p.sh., një rregull i quajtur "Trafiku lokal i bllokuar" duhet t'i lejojë operatorit të konfigurojë se si shfaqet ngjarja nën emrin "Trafiku lokal i bllokuar nga 192.168.1.x në 10.1.1.x" dhe me përshkrimin "Trafiku lokal i bllokuar nga adresa IP 192.168.1.x në Zonën LAN në adresën IP 10.1.1.x në Zonën ËAN".

Zgjidhja duhet të ofrojë një ndërfaqe të dedikuar për akordimin e rregullave të korrelacionit, duke mundësuar analizën e tyre në lidhje me numrin e ngjarjeve që ato gjenerojnë, numrin e hosteve në të cilët ato shkaktohen dhe duke paraqitur në një grafik statistikat e tyre për muajt e fundit.

Ndërfaqja e akordimit të rregullave duhet të mundësojë përjashtimin e hosteve individuale, grupeve të hosteve, llogarive të përdoruesve, grupeve të domeneve dhe grupeve të përdoruesve të domeneve, si në rregullat e korrelacionit ashtu edhe për përpunim të mëtejshëm në modulin SOAR.

Ndërfaqja për krijimin e rregullave të korrelacionit duhet të përfshijë një asistent të IA-së me një opsion plotësisht të konfigurueshëm për gjenerimin automatik të rregullave bazuar në të dhënat hyrëse, p.sh., bazuar në një kategori të specifikuar MITRE ATT&CK.

Shikuesi i ngjarjeve të korreluara duhet të përfshijë një asistent të IA-së me opsionin për të interpretuar çdo ngjarje, të nisur nga menyja e kontekstit.

Metoda e interpretimit duhet të jetë plotësisht e konfigurueshme dhe të lejojë që menyja e kontekstit të zgjerohet me lloje të reja interpretimi.

Zgjidhja duhet të analizojë sjelljen e përdoruesit dhe kompjuterit duke përdorur machine learning për të krijuar dhe përditësuar automatikisht modele të sjelljes tipike për zbulimin e devijimeve nga norma.

Modelet e sjelljes duhet të krijohen automatikisht bazuar në analizën historike të të dhënave për grupet e përdoruesve, burimet (profilet) dhe të lejojnë rillogaritjen e tyre sipas kërkesës, p.sh., shtimit të një rregulli të ri, shtim automatikisht, në mënyrë ciklike, apo një herë në muaj.

Modelet e sjelljes duhet të jenë të konfigurueshme për të çaktivizuar profilet dhe rregullat specifike learning.

Zgjidhja duhet të ketë një grup prej të paktën 20 rregullash të paracaktuara dhe të konfigurueshme për caktimin automatik të përdoruesve dhe burimeve në profilet e duhura. Këto rregulla duhet të sigurojnë të paktën ndarjen e procesit learning për llogaritë e privilegjuara, jo të privilegjuara, të shërbimit, si dhe ndarjen e pajisjeve nga serverat dhe stacionet e punës.
Algoritmet Machine Learning duhet të mundësojnë analizën automatike dhe learning nga të dhënat statistikore, siç janë numri dhe llojet e ngjarjeve të gjeneruara dhe vlerësimet e rrezikut (score).
Algoritmet Machine Learning duhet të përdorin nyje izolimi për të zbuluar aktivitetin e pazakontë dhe anormal.
Mekanizmi i Machine Learning duhet të mundësojë identifikimin e vlerave në ngjarje që do të përdoren në procesin e learning dhe duhet t'i lidhë ato me kushtin e duhur kualifikues.
Algoritmi UEBA duhet të lejojë konfigurimin e mekanizmave për refuzimin e vlerave të jashtëzakonshme që mund të ndikojnë negativisht në rezultatet e procesit learning, si dhe për përjashtimin e profileve specifike të përdoruesve dhe rregullave të zbulimit nga analiza.
Zgjidhja duhet të ofrojë një ndërfaqe grafike të dedikuar që lejon verifikimin e përqindjes së progresit të procesit të learning për secilin profil aktiv, së bashku me informacionin rreth datës së përfundimit dhe numrit të algoritmeve të përdorura.
Ndërfaqja duhet të lejojë qasje në profil për të marrë të dhëna të detajuara rreth secilit algoritëm, siç janë emri, lloji i algoritmit, numri minimal i mostrave, numri i ditëve të nevojshme për të përfunduar learning si edhe vlera e devijimit.
Anomalitë e zbuluara duhet të gjenerojnë ngjarje të reja dhe t'i regjistrojnë ato në depozitën e log-eve.
Shikuesi grafik i ngjarjeve duhet të jetë plotësisht interaktiv, duke lejuar që informacioni i detajuar rreth secilit host të shfaqet nëpërmjet një menuje konteksti të lidhur me atë host.
Minimalisht të dhënat duhet të jenë të disponueshme mbi: informacionin e përpunuar, shërbimet kritike përkatëse, vendndodhjen e përdoruesve që përdorin hostin, vendndodhjen e serverëve që përdor, masat lokale të sigurisë në vend, numrin e dobësive, incidenteve të zbuluara, numrin e ngjarjeve të lidhura dhe llogaritë e përdoruesve të lidhura me të.
Broëseri duhet të lejojë ndërrimin e modalitetit të shfaqjes për një ngjarje të vetme, duke mundësuar që pamja që paraqet fushat e ngjarjes dhe vlerat e tyre të ndryshohet në një përshkrim ngjarjeje të gjeneruar automatikisht në bazë të fushave që ndodhin në një ngjarje të caktuar.
Përshkrimi i gjeneruar duhet të jetë plotësisht i konfigurueshëm, me mundësinë e përcaktimit të kushteve që ndikojnë në ndryshimin në formën e prezantimit të tij.
Lista e ngjarjeve të shoqëruara me një llogari përdoruesi duhet të lejojë shikimin e kompjuterëve në të cilët është regjistruar aktiviteti, si edhe llogaritë e përdoruesve të shoqëruara me një kompjuter të caktuar.

Zgjidhja duhet të ofrojë një paraqitje me hartë për të gjitha ngjarjet që lidhen me hostet dhe llogaritë e përdoruesve brenda një periudhe të caktuar kohore në matricën MITRE ATT&CK, duke mundësuar vlerësimin e mbulimit të saj.
Zgjidhja duhet të ketë mundësinë e dokumentimit të rrjetit, sistemeve dhe shërbimeve, duke mundësuar mbledhjen dhe redaktimin e të dhënave përkatëse për vlerësimin e ngjarjeve të sigurisë të gjeneruara.
Zgjidhja duhet të lejojë përcaktimin e parametrave të personalizuar për të gjitha llojet e objekteve të ruajtura në dokumentacionin elektronik të rrjetit.
Zgjidhja duhet të jetë e aftë të vizualizojë dokumentacionin në formën e një harte interaktive të rrjetit, që mbulon zonat e sigurisë, pajisjet e rrjetit dhe pikat fundore, duke përfshirë serverat dhe kompjuterët.
Dokumentacioni elektronik duhet të mundësojë menaxhimin e një katalogu shërbimesh, duke përfshirë parametrat e mëposhtëm për secilin shërbim: vlefshmëria, lloji, informacioni i përpunuar, varësitë dhe ndikimi në shërbime të tjera, cikli, aplikacionet e lidhura, portat e rrjetit, shërbimet, referencat (URL-të) dhe lidhjet me burimet e IT-së.
Dokumentacioni elektronik duhet të gjenerohet automatikisht bazuar në rregullat e ofruara nga prodhuesi (të paktën 50), të cilat, kur aktivizohen, përditësojnë automatikisht dokumentacionin pa ndërhyrjen e operatorit.
Zgjidhja duhet të mundësojë vlerësimin automatik të ndikimit të incidenteve të sigurisë së IT-së në operacionet e rrjetit në kontekstin e kërcënimeve të IT-së, midis çdo burimi IT, bazuar në dokumentacionin elektronik, matricën MITRE ATT&CK dhe dobësitë e zbuluara.
Vlerësimi i ndikimit të incidenteve të sigurisë së IT-së në operacionet e organizatës duhet të jetë i parakonfiguruar bazuar në rregulla të paracaktuara.
Zgjidhja duhet të ketë një bazë të dhënash të integruar që mundëson mbledhjen, ruajtjen dhe caktimin e treguesve të kompromentimit (IoC) për incidentet.
Zgjidhja duhet të mundësojë sinkronizimin e treguesve të kompromentimit (IoC) me platformat e disponueshme publikisht.
Të dhënat e mbledhura në bazën e të dhënave të treguesve të kompromisit (IoC) duhet të jenë të përdorshme në rregullat dhe playbooks.
Zgjidhja duhet të sigurojë që listat e referencave të mund të sinkronizohen me listat e disponueshme publikisht.
Zgjidhja duhet të ketë një asistent të integruar të AI që mbështet operatorin në trajtimin e ngjarjeve dhe dobësive.
Asistenti i AI duhet të mundësojë integrimin me modelet gjuhësore lokale dhe të disponueshme publikisht (LLM).
Asistenti i AI duhet të veprojë në kontekst, me aftësinë për të caktuar kërkesa të përshtatshme për secilin kontekst.

Asistenti i AI duhet të ofrojë mënyra të dedikuara operimi, duke përfshirë të paktën trajtimin e incidenteve dhe dobësive, analizën e ngjarjeve të regjistrit, si edhe integrimin dhe krijimin e analizuesit.
Asistenti i AI duhet të lejojë redaktimin e kërkesave dhe krijimin e kërkesave të reja.
Kërkesat duhet të jenë të disponueshme për shkarkim nga faqja e internetit e prodhuesit.
Asistenti i AI duhet të jetë i disponueshëm vazhdimisht dhe dinamikisht duke ndryshuar kontekstin në varësi të funksionaliteteve të përdorura.
Zgjidhja duhet të ketë një logjikë për caktimin automatik të ngjarjeve të kualifikuara për trajtim, së bashku me një njoftim për operatorin e caktuar për t'i trajtuar ato (p.sh., email, mesazh teksti - SMS).
Kualifikimi i ngjarjeve duhet të bazohet në një sërë rregullash që caktojnë automatikisht një ngjarje për trajtim ose ta refuzojnë atë.
Kualifikimi i operatorit për të trajtuar ngjarjen duhet të bazohet në kritere të përcaktuara në nivelin e ekipit të shërbimit dhe të përfshijë, ndër të tjera:
• metodën e caktimit të një ngjarjeje, të paktën: personit më pak të ngarkuar ose nëpërmjet menaxherit të ekipit;
• llojin e ngjarjes, p.sh.: cenueshmëri, rregull korrelacioni, raport;
• llojin e burimit, duke përfshirë: bazën e të dhënave, stacionin e punës, kontrolluesin e domenit, printerin, serverin, pajisjen;
• shërbimet e lidhura me burimin;
• informacionin e përpunuar;
• përkatësinë e burimit në një njësi organizative;
• softuerin e përcaktuar.
Ngjarjet e suportuara duhet të kenë një grup prej 30 skenarësh trajtimi të paracaktuar (udhëzues) dhe të lejojnë krijimin e skenarëve të trajtimit të personalizuar dhe redaktimin e tyre nga ndërfaqja grafike.
Zgjidhja duhet të marrë informacion nga sisteme të tjera dhe ta përdorë atë për të marrë vendime në lidhje me rrjedhën e mëtejshme të manualit.
Zgjidhja duhet të jetë e integruar me një vulnerability scanner dhe të sigurojë që këto dobësi të trajtohen brenda manualeve.
Zgjidhja duhet të jetë në gjendje t'u përgjigjet kërcënimeve si përmes integrimit me sisteme të tjera sigurie ashtu edhe direkt në stacionin e punës ose serverin e sulmuar, në nivel të agjentit të mbështetur.
Zgjidhja duhet të mundësojë kërkimin e regjistrave historikë, ngjarjeve të ndërlidhura, statistikave UEBA, informacionit të mbulimit të matricës MITRE ATT&CK dhe të dhënave nga baza e të dhënave e Inteligjencës së Kërcënimeve.

Zgjidhja duhet të mundësojë përcaktimin e parametrave SLA për të gjitha statuset e shërbimit, dhe t'i verifikojë ato kundrejt vlerave të përcaktuara. Rezultatet e matjeve të kohës së SLA duhet të përditësohen vazhdimisht dhe të paraqiten në një listë të ngjarjeve të kualifikuara për shërbim.
Manualet duhet të aktivizohen si në përgjigje të ngjarjeve specifike ashtu edhe në mungesë të një përgjigjeje brenda një afati kohor të caktuar për të mundësuar skenarët e përshkallëzimit.
Manualet duhet të mundësojnë kontroll të plotë duke përdorur AI, si edhe duke përfshirë kryerjen automatike të hapave pasues bazuar në përgjigjet e marra nga modeli LLM.
Manualet duhet të kenë një menaxher fjalëkalimesh të integruar për të ruajtur në mënyrë të sigurt të dhënat e nevojshme për integrimin, siç janë emrat e përdoruesit, fjalëkalimet dhe çelësat API.

c) Arkitektura

Zgjidhja duhet të ofrojë një arkitekturë fleksibile dhe të shkallëzueshme pa nevojën e blerjes së licencave shtesë për zgjerim.
Zgjidhja duhet të mundësojë ndarjen e shtresave funksionale të referuara si analizimi, ruajtja e logeve, korrelacioni i ngjarjeve, ruajtja e ngjarjeve dhe mekanizmat e të mësuarit automatik.
Zgjidhja duhet të përshkallëzohet pa limit duke shtuar makina virtuale shtesë ose makina fizike (kolektor), duke mundësuar kështu rritjen e performancës dhe besueshmërisë.
Kolektorët e ruajtjes së të dhënave nuk duhet të përdorin baza të dhënash klasike relacionale; vetëm bazat e të dhënave NoSQL ose zgjidhjet e rekomanduara nga prodhuesi lejohen për këtë qëllim.
Arkitektura e zgjidhjes duhet të mbështesë një konfigurim që ofron besueshmëri përmes përdorimit të një serie kolektorësh zëvendësues, të cilët aktivizohen në rast të një dështimi të njërit prej tyre.
Të gjithë kolektorët, si ai primar ashtu edhe ai zëvendësues, duhet të menaxhohen në mënyrë qendrore nga e njëjta konsolë.
Zgjidhja duhet të ketë një mekanizëm që mundëson bashkëpunimin me sisteme të jashtme si Load Balancer, i cili të verifikojë funksionimin e saktë të të gjithë kolektorëve.
Për të siguruar vazhdimësinë, kolektori primar duhet të jetë në gjendje të sinkronizojë ngjarjet me kolektorin rezervë. Në rast të një dështimi të kolektorit primar, ngjarjet e gjeneruara në atë kolektor duhet të përfshihen në korrelacionin në kolektorin rezervë.
Të gjitha llojet e kolektorëve, përfshirë agjentët XDR, duhet të jenë të konfigurueshëm dhe të specifikojnë kolektorët rezervë tek të cilët do të drejtohen të dhënat në rast të një dështimi të kolektorit primar.

4. Instalim dhe implementim për zgjidhjet XDR dhe SIEM

Autoriteti Kontraktor kërkon shërbime të sigurisë kibernetike për instalimin, konfigurimin, integrimin dhe operacionalizimin e zgjidhjeve Extended Detection and Response (XDR) dhe një zgjidhjeje Security Information and Event Management (SIEM).
Objektivi është përmirësimi i operacioneve të sigurisë, reduktimi i kohës së zbulimit dhe reagimit ndaj incidenteve, automatizimi i inteligjencës së kërcënimeve dhe përmbushja e standardeve.

a) Shërbimet e Implementimit të XDR

- *Deploy dhe konfigurim i zgjidhjes*
- *Integrim me endpoint-e, serverë, pajisje rrjeti, fireëall, ëorkload-e*
- *Konfigurim i feed-eve të inteligjencës së kërcënimeve*
- *Rregullim i politikave dhe optimizim i alarmeve*
- *Krijimi i ëorkfloë-ve të automatizuara të reagimit*
- *Konfigurimi i aksesit dhe roleve*
- *Fortifikim i platformës*
- *Transferim njohurish*

b) Shërbimet e Implementimit të SIEM

- *Instalimi i platformës SIEM (on-premise)*
- *Onboarding i burimeve të log-eve (serverë, aplikacione, fireëall, identitet, cloud, etj.)*
- *Parsing, normalizim dhe krijim rregullash korrelacioni*
- *Zhvillim i use-case-ve sipas riskut të autoritetit*
- *Krijim dashboard-esh dhe raportesh*
- *UEBA dhe SOAR*
- *Raportim i pajtueshmërisë*
- *Optimizim i performancës*

c) Kërkesa Teknike
Kërkesat për XDR

- *Zbulim bazuar në sjellje dhe signature*
- *Orkestrimi i automatizuar i reagimit*
- *Integrim me EDR, sisteme identiteti*
- *Mbështetje API*
- *Korrelacion me inteligjencë kërcënimesh*
- *Monitorim dhe alarmim i vazhdueshëm*

Kërkesat për SIEM

- *Ingestion dhe korrelacion në kohë reale*
- *Arkitekturë e shkallëzueshme*

- *Kontroll aksesi (RBAC)*
- *Integrim me sistemet ekzistuese të autentikimit*
- *Analitika të avancuara*
- *Gjuhë fleksibël kërkimi*
- *Mbështetje për ëorkfloë të incidenteve*

5. Shërbim mirëmbajtje Fireëall XDR dhe SIEM

Operatori ekonomik duhet të ofrojë shërbime të mirëmbajtjes sipas niveleve të shërbimit dhe metodikës të përshkruar më poshtë:

1.Suport proaktiv.

Operatori ekonomik duhet të ndërmarrë, në mënyrë periodike një herë në muaj, shërbime dhe suport proaktiv, të cilët duhet të mundësojnë detektimin në kohë të problematikave dhe duhet të mundësojnë ndërmarrjen në kohë të hapave rekuperues, për të mos pasur ndërprerje të shërbimit. Të gjitha shërbimet e suportit proaktiv duhet të kryhen pranë ambienteve të POSTA SHQIPTARE sh. a., përveç rasteve kur POSTA SHQIPTARE përcakton një vendndodhje të re për kryerjen e këtyre shërbimeve.

2. Shërbime riparimi në vendndodhje (mjediset e POSTA SHQIPTARE).

Operatori ekonomik duhet të jetë në dispozicion gjatë intervalit kohor, nga e Hëna në të Dielë, 24/7, për të ofruar shërbime të riparimit në përgjigje të "Alarmeve Madhore" të raportuara nga personeli i autorizuar i POSTA SHQIPTARE (“Emergency On-Call Hours").

Për këtë qëllim, me termin Alarm Madhor do të kuptohet parashtrimi i kërkesës për shërbime riparimi të ndërmarra në rast të keqfunksionimit të sistemeve të mbuluara që i pengon ato të operojnë në përputhje me specifikimet dhe shkaktojnë ndërprerje të menjëhershme e të konsiderueshme të sistemit dhe që nuk mund të shmangen me anë të ndërhyrjeve dhe riparimeve minore të kryera nga stafi teknik i POSTA SHQIPTARE, të rekomanduara nga Kompania. Problemet që nuk i përkasin "Alarmeve Madhore" duhet të adresohen nën shërbime të suportit proaktiv.

3. Njoftimi dhe njohja e alarmeve madhore.

POSTA SHQIPTARE do të njoftojë me telefon, postë elektronike ose duke sinjalizuar nëpërmjet një ndërfaqeje ëeb të vënë në dispozicion dhe do të presë të kontaktohet nga ne me telefon, gjatë "Emergency On-Call Hours". Operatori ekonomik duhet të kontaktojë POSTA SHQIPTARE sh.a. dhe të konfirmojë marrjen e Alarmit Madhor, brenda 30 minutave nga marrja e njoftimit nga personeli i autorizuar i POSTA SHQIPTARE. Në momentin e njohjes së thirrjes, POSTA SHQIPTARE do të vendosë në dispozicion informacione të paracaktuara në procedurat e troubleshooting dhe do të asistojë OE gjatë diagnostikimit të problemit të raportuar. POSTA

SHQIPTARE do të bashkëpunojë me kërkesën e OE për të ndihmuar në përcaktimin e shkakut të problemit të raportuar dhe në përcaktimin e nevojës për vizitë në vendndodhje për të kryer shërbimet e riparimit.

4. Përgjigja ndaj alarmeve madhore.

Nëse operatori ekonomik nuk mund të përcaktojë nëpërmjet informacionit të mbledhur nga procedurat e troubleshooting shkakun e alarmit madhor, atëherë duhet të dërgojë një teknik shërbimi pranë POSTA SHQIPTARE brenda intervalit kohor prej dy (2) orësh nga momenti i marrjes së njoftimit për Alarm Madhor. Me të mbërritur, tekniku do të mbështetet me asistencë nga POSTA SHQIPTARE dhe do t'i jepet liri veprimi në mjediset dhe sistemet e mbuluara, për të filluar menjëherë procedurat e diagnostikimit dhe riparimit.

5. Veprimtaritë e diagnostikimit dhe riparimit.

Me të mbërritur në vendndodhje, tekniku i shërbimit duhet të fillojë procedurat e diagnostikimit dhe riparimit. Këto veprimtari duhet të vazhdojnë derisa:

a) *Alarmi madhor të jetë korrektuar ose të jetë "zgjidhur në mënyrë të tërthortë";*
b) *tekniku të jetë zëvendësuar nga një person tjetër;*
c) *të përcaktohet se problemi i raportuar nuk është shkaktuar nga ndonjë keqfunksionim i sistemeve të mbuluara;*
d) *të arrihet në konkluzion që diagnostikimi ose korrektimi i mëtejshëm mund të shtyhet deri në mbërritjen e pjesëve të këmbimit.*

Teknikët e shërbimit të operatorit ekonomik duhet të jenë të trajnuar, të certifikuar dhe të autorizuar për të ndërvepruar në mënyrë të drejtpërdrejtë me prodhuesin. Në rast se do të jetë i nevojshëm zëvendësimi i pjesëve të këmbimit, atëherë OE duhet të kryejë të gjitha procedurat respektive me prodhuesin për lokalizimin e pjesës, heqjen, eksportin, transportin, importin, vendosjen dhe rikonfigurimet përkatëse. Kostot e pjesëve të dëmtuara dhe kostot e shërbimit do të merren përsipër nga operatori ekonomik për të gjithë periudhën e kontratës.

6. Shërbimet e tjera.

Operatori ekonomik duhet të krijojë/diskutojë me POSTA SHQIPTARE sh.a. një axhendë periodike kontrollesh si më poshtë:

Javore

i. *Kontrolle të log-eve të pajisjeve të rrjetit;*
ii. *Mirëmbajtje proaktive.*

Mujore

iii. Testim / kontroll i kompletuar i pjesëve më kritike të infrastrukturës HË të POSTA SHQIPTARE sh. a.;

iv. Kontroll i detajuar i të gjithë log-eve hardëare, analizë e tyre;

v. Rekomandime për upgrade të mundshme hardëare.

III.2.4. Në shtojcën 7 "*FORMULAR I SHËRBIMEVE DHE GRAFIKUT TË EKZEKUTIMIT*", të dokumentave të tenderit nga ana e autoritetit kontraktor janë publikuar llojet dhe sasia e shërbimeve objekt prokurimi, si më poshtë vijon:

Shtojca 7.

(Shtojcë për t'u plotësuar nga Autoriteti/Enti Kontraktor)

(Kjo Shtojcë në rastin e Marrëveshjes Kuadër do të plotësohet nga autoriteti/enti kontraktor vetëm gjatë rihapjes së procesit të mini-konkursit)

FORMULARI I SHËRBIMEVE DHE GRAFIKUT TË EKZEKUTIMIT

Shërbimi që kërkohet: *Konsiston në furnizimin, implementimin, konfigurimin, integrimin dhe mirëmbajtjen e një infrastrukture të avancuar të sigurisë kibernetike për Posta Shqiptare, e cila përfshin rinovimin e garancisë dhe licencave për pajisjet fireëall FortiGate-401F dhe FortiGate-601F, implementimin e një zgjidhjeje XDR/EDR për minimumi 1200 përdorues, implementimin e një zgjidhjeje SIEM on-premise me funksionalitete të avancuara të monitorimit, korrelacionit dhe analizës së kërcënimeve kibernetike, si dhe ofrimin e shërbimeve të instalimit, konfigurimit, integrimit, suportit teknik dhe mirëmbajtjes 24/7 për një periudhë prej 48 muajsh, me qëllim garantimin e vazhdimësisë së operacioneve, rritjen e nivelit të sigurisë së sistemeve dhe reagimin në kohë ndaj incidenteve të sigurisë kibernetike.*

Afatet e ekzekutimit:

	PËRSHKRIMI I PRODUKTEVE	***NJËSIA***	***SASIA***	***VITE***
1	*SHËRBIM PËR RINOVIMIN E GARANCISË DHE LICENCAVE TË PAJISJEVE FIREËALL*	*copë*	*4*	*4*
2	*ZGJIDHJE XDR*	*copë*	*1200*	*4*
3	*ZGJIDHJE SIEM*	*copë*	*1200*	*4*
4	*INSTALIMI DHE IMPLEMENTIMI I SHËRBIMEVE XDR DHE SIEM*	*set*	*1*	

5	*SHËRBIM MIRËMBAJTJE FIREËALL XDR DHE SIEM*	*set*	*1*	*4*

III.2.5. Në shtojcën 8 "*FORMULAR I TERMAVE TË REFERENCËS*", të dokumentave të tenderit nga ana e autoritetit kontraktor janë publikuar termat e referencës së shërbimeve objekt prokurimi, si më poshtë vijon:

Shtojca 8.

(Shtojcë për t'u plotësuar nga Autoriteti/Enti Kontraktor)

FORMULARI I TERMAVE TË REFERENCËS

Objekti dhe qëllimi i shërbimeve: ***"Blerje suport për SIEM + licensa për EDR/XDR (1200 përdorues) + licensa fireëall Professional për 4 (katër) vite".***

Qëllimi i këtij shërbimi është sigurimi i një infrastrukture të integruar të sigurisë kibernetike për Posta Shqiptare, nëpërmjet rinovimit të licencave dhe garancive për pajisjet fireëall ekzistuese, implementimit të zgjidhjeve moderne XDR dhe SIEM, monitorimit dhe analizimit të vazhdueshëm të ngjarjeve të sigurisë, rritjes së kapaciteteve të zbulimit dhe reagimit ndaj incidenteve kibernetike, si dhe garantimit të mirëmbajtjes dhe suportit teknik për funksionimin e pandërprerë të sistemeve për një periudhë 48 mujore.

Detyrat:

- *Rinovimin e garancisë dhe licencave "Unified Threat Protection (UTP)" për pajisjet fireëall FortiGate-401F dhe FortiGate-601F për një periudhë 48 mujore;*
- *Furnizimin dhe implementimin e një zgjidhjeje XDR/EDR për minimumi 1200 përdorues;*
- *Furnizimin dhe implementimin e një zgjidhjeje SIEM on-premise për monitorimin dhe menaxhimin e incidenteve të sigurisë;*
- *Instalimin, konfigurimin dhe integrimin e zgjidhjeve XDR dhe SIEM me infrastrukturën ekzistuese të Autoritetit Kontraktor;*
- *Konfigurimin e politikave të sigurisë, ëorkfloë-ve të automatizuara dhe mekanizmave të reagimit ndaj incidenteve;*
- *Integrimin me fireëall, endpoint-e, serverë, sisteme identiteti, log-e dhe burime të tjera të të dhënave;*
- *Kryerjen e testimeve funksionale dhe operacionalizimin e plotë të sistemeve;*
- *Transferimin e njohurive dhe asistencën teknike për stafin e Autoritetit Kontraktor;*
- *Ofrimin e mirëmbajtjes proaktive dhe suportit teknik 24/7 gjatë gjithë periudhës së kontratës;*
- *Reagimin ndaj alarmeve madhore sipas niveleve të shërbimit të përcaktuara në specifikimet teknike;*
- *Kryerjen e kontrolleve periodike, analizave të log-eve dhe rekomandimeve për optimizimin e infrastrukturës së sigurisë.*

Shpërndarja: Shërbimet dhe licencat do të dorëzohen, implementohen dhe aktivizohen sipas spias specifikimeve teknike, duke përfshirë:

- *aktivizimin e licencave fireëall;*
- *instalimin dhe konfigurimin e zgjidhjes XDR/EDR për 1200 përdorues;*
- *instalimin dhe konfigurimin e platformës SIEM;*
- *integrimin me sistemet ekzistuese;*
- *dorëzimin e dokumentacionit teknik dhe kredencialeve të administrimit;*
- *ofrimin e suportit dhe mirëmbajtjes për 48 muaj.*

Vendi i kryerjes së shërbimeve: Shërbimet do të kryhen pranë ambienteve të Drejtorisë së Përgjithshme të Posta Shqiptare dhe në të gjitha zyrat e filialeve të saj.

III.2.6. Lidhur me pretendimet e mësipërme të operatorit ekonomik ankimues "*PC STORE*" ShPK autoriteti kontraktor me shkresën nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, e ka shqyrtuar këtë pretendim të ankimuesit, duke argumentuar si më poshtë vijon:

"*Arsyetim për kërkesën e specialistit të certifikuar* ***CIR (Certified Incident Responder)*** *ose ekuivalent në procedurën e tenderimit për SIEM dhe XDR.*
Implementimi dhe operimi i platformave SIEM (Security Information and Event Management) dhe XDR (Extended Detection and Response) përbëjnë komponentë kritikë të sigurisë kibernetike, të cilët kanë rol thelbësor në monitorimin, identifikimin, analizimin dhe reagimin ndaj incidenteve të sigurisë në infrastrukturat IT të institucionit.

Për shkak të kompleksitetit teknik dhe rëndësisë së lartë operacionale të këtyre sistemeve, kërkohet që operatori ekonomik të disponojë staf të specializuar dhe të certifikuar në fushën e reagimit ndaj incidenteve të sigurisë kibernetike, siç është certifikimi CIR (Certified Incident Responder) ose një certifikim ekuivalent i njohur ndërkombëtarisht.

Kjo kërkesë argumentohet mbi bazën e faktoreve të mëposhtëm:

- *Menaxhimi profesional i incidenteve tee sigurisee*

Platforma SIEM dhe XDR kanë si funksion kryesor identifikimin dhe trajtimin e incidenteve të sigurisë në kohë reale. Një specialist i certifikuar CIR zotëron njohuri dhe aftësi praktike për analizimin, klasifikimin, investigimin dhe neutralizimin e kërcënimeve kibernetike, duke garantuar reagim të shpejtë dhe efektiv ndaj incidenteve.

- *Reduktimi i riskut operacional dhe te sigurise*

Konfigurimi jo korrekt ose mungesa e ekspertizës në menaxhimin e alarmeve dhe ngjarjeve të sigurisë mund të sjellë pasoja serioze, përfshirë mosidentifikimin e sulmeve, vonesa në reagim apo kompromet im të sistemeve kritike. Certifikimi CIR garanton se specialisti posedon kompetencat e nevojshme për të minimizuar këto rreziqe.

- *Kërkesë në përputhje me praktikat dhe standardet ndërkombetare*

Angazhimi i specialistëve të certifikuar neë incident response është praktike standarde në projektet moderne të sigurisë kibernetike dhe rekomandohet nga kuadrot ndërkombetarë të sigurisë si NIST, ISO/IEC 27035 dhe standardet e operimit të SOC (Security Operations Center).

- *Garantimi i cilësisë së shërbimit*

Certifikimet profesionale si CIR ose ekuivalente dëshmojnë që personeli ka kaluar trajnim dhe Vlerësim teknik të specializuar në fushën e incident response dhe cyber defense, duke ritur besueshmërinë dhe cilësinë e shërbimit të ofruar.

- *Përputhshmëria me natyrën kritike të sistemeve SIEM/DR*

Duke qënë se sistemet SIEM dhe DR lidhen dretpërdrejt me mbrojtien e aseteve kritike të institucionit, kërkohet nivel i avancuar ekspertize për administrimin, tuning-un e regullave të detektimit, analizën e log-eve, korelacionin e ngjarjeve dhe reagimin ndaj sulmeve të avancuara.

Për sa më sipër, kërkesa për një specialist të certifikuar CIR ose ekuivalent konsiderohet proporcionale, e arsyeshme dhe e lidhur dretpërdrejt me objektin e kontratës, me qëllim garantimin e sigurisë, cilësisë dhe vazhdimësisë së shërbimeve të kërkuara.

Arsyetim për kërkesën e një specialisti të certifikuar ***OSCP (Offensive Security Certified Professional)*** *ose ekuivalent në proceduren e tenderimit për SIEM dhe XDR.*

Kërkesa për angazhimin e të pakten një specialisti të certifikuar OSCP (Offensive Security Certified Professional) ose ekuivalent konsiderohet e domosdoshme për realizimin me sukses të implementimit, konfigurimit dhe optimizimit të sistemeve SIEM (Security Information and Event Management) dhe DR (Extended Detection and Response), për shkak të nivelit të lartë teknik dhe kritik të sigurisë që këto sisteme përfaqësojnë.

Sistemet SIEM dhe XDR kane rol kyç në identifikimin, analizimin, korelacionin dhe reagimin ndaj incidenteve të sigurisë kibernetike në kohë reale. Implementimi i tyre kërkon njohuri të avancuara në:

- *monitorimin dhe analizën e logeve të sigurisë;*
- *identifikimin e teknikave të avancuara të sulmeve kibernetike;*

- *threat hunting dhe incident response;*
- *konfigurimin e use-case-ve të sigurisë;*
- *validimin e mekanizmave të detektimit përmes simulimit të sulmeve reale;*
- *analizën e vulnerabiliteteve dhe teknikave të kompromet imit të sistemeve*

Certifikimi OSCP është një nga certifikimet më të njohura ndërkombëtarisht në fushën e sigurisë offensive dhe testimit praktik të penetrimit. Ky certifikim vërteton që specialisti zotëron aftësi praktike për të identifikuar, shfrytëzuar dhe analizuar dobësi reale në infrastrukturat IT, si dhe për të kuptuar metodologjitë dhe taktikat që përdoren nga aktorët keqdashës.

Perfshirja e një specialisti me këtë nivel certifikimi garanton që:

- *konfigurimet dhe rregullat e detektimit në SIEM/XDR do të ndërtohen mbi skenarë reale kërcënimesh;*
- *sistemi do të jetë në gjendje të identifikojëë sulme komplekse dhe tentativa kompromet imi;*
- *do të minimizohen "false positive" dhe "false negative";*
- *do të realizohet validimi praktik i use-case-ve të sigurisë;*
- *organizata do të përfitojë një nivel më të lartë mbrojtjeje dhe reagimi ndaj incidenteve kibernetike.*

Gjithashfu, duke qenë se SIEM dhe XDR përbëjnë sisteme kritike për mbrojtjen e infrastrukturës së teknologjisë së informacionit, kërkesa për specialist të certifikuar OSCP ose ekuivalent është në përputhje me praktikat më të mira ndërkombëtare për projekte të sigurisë kibernetike dhe synon të sigurojë cilësi, ekspertize teknike dhe besueshmëri në realizimin e kontratës.

Pranimi i certifikimeve ekuivalente lejon konkurrencë të hapur dhe pjesëmarrje më të gjërë të operatorëve ekonomike, duke ruajtur njëkohësisht standardin e kërkuar profesional dhe teknik për realizimin e projektit.

Arsyetim mbi kërkesën për Specialist teë ***Certifikuar Cybersecurity Analyst*** *ose ekuivalent në procedurën e tenderimit për SIEM dhe XDR.*
Kërkesa për disponimin e një specialisti të certifikuar në fushën e Cybersecurity Analyst ose ekuivalente është e domosdoshme për natyrën dhe kompleksitetin e projektit që lidhet me implementimin, konfigurimin dhe menaxhimin e sistemeve SIEM (Security Information and Event Management) dhe XDR (Extended Detection and Response).

Zgjidhjet SIEM dhe XDR përbëjnë komponentë kritikë të sigurisë kibernetike të infrastrukturës IT, pasi ato mundësojnë monitorimin në kohe reale, analizimin e ngjarjeve të sigurisë, identifikimin e incidenteve, korrelacionin e log-eve dhe reagimin ndaj kërcënimeve kibernetike.

Implementimi dhe administrimi korrekt i këtyre platformave kërkon njohuri të avancuara teknike në analizën e sigurisë, menaxhimin e incidenteve, threat hunting, incident response dhe interpretimin e ngjarjeve të sigurisë.

Për këtë arsye, operatori ekonomik duhet të disponojë staf të kualifikuar dhe të certifikuar, i cili garanton se shërbimet do të realizohen sipas standardeve më të mira ndërkombëtare të sigurisë kibernetike. Certifikimi si Cybersecurity Analyst ose ekuivalent vërteton kompetencën profesionale të specialistit në:

- *monitorimin dhe analizimin e incidenteve të sigurisë;*
- *identifikimin dhe reagimin ndaj kërcënimeve kibernetike;*
- *përdorimin dhe administrimin e platformave SIEM/XDR;*
- *analizën e log-eve dhe korrelacionin e ngjarjeve;*
- *implementimin e praktikave të sigurisë sipas standardeve ndërkombëtare.*

Gjithashtu, për shkak të ndjeshmërisë së sistemeve që do të monitorohen dhe ndikimit që një konfigurim i pasaktë mund të ketë në sigurinë e institucionit, prania e një eksperti të certifikuar minimizon rrezikun operacional dhe garanton cilësi, besueshmëri dhe vazhdimësi në ofrimin e shërbimit.
Kjo kërkesë eshtë në përpjesëtim me objektin e kontratës dhe nuk kufizon konkurrencën, pasi pranohen certifikime ekuivalente të njohura ndërkombëtarisht në fushën e sigurisë kibernetike.

*Arsyetim për kërkesën e stafit të certifikuar "**Cyber Threat Hunting Professional**" ose ekuivalente në procedurën e prokurimit për SIEM dhe XDR*
Kërkesa që operatori ekonomik pjesëmarrës në procedurën e prokurimit të disponojë të paktën 2 (dy) specialistë të certifikuar "Cyber Threat Hunting Professional" ose ekuivalente. konsiderohet e domosdoshme dhe proporcionale me natyrën, kompleksitetin dhe rëndësinë e shërbimeve që lidhen me implementimin, konfigurimin dhe operimin e platformave SIEM (Security Information and Event Management) dhe XDR (Extended Detection and Response).

Zgjidhjet SIEM dhe XDR përbëjnë komponentë kritikë të sigurisë kibernetike, të cilët kanë si funksion monitorimin në kohë reale, analizimin e ngjarjeve të sigurisë, identifikimin e kërcënimeve të avancuara, korelacionin e log-eve dhe reagimin ndaj incidenteve kibernetike.

Për shkak të natyrës dinamike dhe sofistikimit në rritje të sulmeve kibernetike, kërkohet personel me ekspertizë të specializuar në "threat hunting", analizë proaktive të kërcënimeve dhe identifikim të anomalive që nuk evidentohen nga mekanizmat standardë të sigurisë.

Certifikimi "Cyber Threat Hunting Professional" ose ekuivalent garanton që specialistët posedojnë njohuri dhe aftësi të avancuara në:

- *identifikimin proaktiv të kërcënimeve kibernetike;*
- *analizimin e indikatorëve të kompromet imit (IOC);*
- *përdorimin efektiv të platformave SIEM/XDR;*
- *investigimin dhe korrelacionin e ngjarjeve të sigurisê;*
- *reagimin ndaj incidenteve dhe minimizimin e riskut operacional.*

Kerkesa për minimumi 2 (dy) specialistë është vendosur për të garantuar:

- *vazhdimësinë e shërbimit dhe mbulimin operacional;*
- *redundancën teknike dhe shmangien e varësisë nga një individ i vetëm;*
- *përballimin e volumeve të larta të analizës së ngjarjeve dhe incidenteve;*
- *disponueshmërinë e ekspertizës gjatë gjithë ciklit të implementimit dhe suportit të zgjidhjes.*

Gjithashtu, kjo kërkesë lidhet drejtpërdrejt me rëndësinë e mbrojtjes së infrastruktures kritike të teknologjisë së informacionit, ruajtjen e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave, si dhe me nevojën për të garantuar standarde të larta të sigurisë kibernetike gjatë ekzekutimit të kontratës.
Përrjedhojë, kërkesa konsiderohet objektive, e arsyeshme, proporcionale dhe në funksion të garantimit të cilësisë, sigurisë dhe besueshmërisë së shërbimit që prokurohet.

Pretendimet tuaja mbi këtë kriterin 2.3.4 pikat b), d), e), f) dhe i), vlerësohen si jo të drejta nga "Komisioni i Shqyrtimit të Ankesës".".

III.2.7. Në Nenin 2 "*Qëllimi*" të ligjit 162/2021 "*Për prokurimin publik*", i ndryshuar parashikohet se:

"*Qëllim i këtij ligji është:*
a) të rrisë efiçencën dhe efikasitetin në procedurat e prokurimit publik;
b) të sigurojë mirëpërdorim të fondeve publike dhe të ulë shpenzimet procedurale;
c) të nxisë pjesëmarrjen e operatorëve ekonomikë në procedurat e prokurimit publik;
ç) të nxisë konkurrencën ndërmjet operatorëve ekonomikë;
d) të sigurojë një trajtim të barabartë dhe jodiskriminues për të gjithë operatorët ekonomikë, pjesëmarrës në procedurat e prokurimit publik;
dh) të sigurojë integritet, besim publik dhe transparencë në procedurat e prokurimit publik.".

Ndërsa në Nenin 3 "*Parime të përgjithshme*" të ligjit 162/2021 "*Për prokurimin publik*", i ndryshuar, parashikohet se:

"*1. Autoritetet dhe entet kontraktore garantojnë trajtim të barabartë dhe jodiskriminues për operatorët ekonomikë, si dhe veprojnë me transparencë e në mënyrë proporcionale.*
2. Autoritetet dhe entet kontraktore nuk duhet të shmangin fushën e zbatimit të këtij ligji ose të ngushtojnë në mënyrë artificiale konkurrencën. Konkurrenca konsiderohet se është ngushtuar artificialisht kur prokurimi përgatitet me qëllimin për të favorizuar ose dëmtuar në mënyrë të padrejtë operatorë ekonomikë të caktuar.
3. Autoritetet dhe entet kontraktore janë të detyruara të zbatojnë detyrimet e përcaktuara në legjislacionin mjedisor, social e të punës dhe në dispozitat e marrëveshjeve dhe konventat ndërkombëtare, të ratifikuara në përputhje me Kushtetutën.".

III.2.8. Në Nenin 21 *"Autoriteti ose enti kontraktor*" të ligjit 162/2021 "*Për prokurimin publik*", i ndryshuar, parashikohet se:

"*1. Autoriteti ose enti kontraktor është përgjegjës për prokurimin në përputhje me dispozitat e këtij ligji dhe të akteve nënligjore të nxjerra në zbatim të tij, duke garantuar respektimin e parimeve të trajtimit të barabartë, transparencës, konkurrencës dhe mosdiskriminimit, të parashikuara në këtë ligj*.
Në kuptim të kësaj pike, autoriteti ose enti kontraktor ka detyrimin të mirëplanifikojë në cilësi dhe në kohë fondet publike e nevojat e tij dhe të prokurojë e të zbatojë kontratën në përputhje me legjislacionin në fuqi.".

III.2.9. Në Nenin 77 "*Kërkesat për kualifikim*", pika 4, të ligjit nr.162/2020 "*Për prokurimin publik*", i ndyshuar, parashikohet shprehimisht se:

"*4. Në lidhje me aftësitë teknike dhe profesionale, autoritetet ose entet kontraktore mund të vendosin kërkesa që garantojnë se operatorët ekonomikë zotërojnë burimet e nevojshme njerëzore e teknike, si dhe përvojën e nevojshme për të zbatuar kontratën sipas një standardi të përshtatshëm cilësie. Autoritetet ose entet kontraktore, në veçanti, mund të kërkojnë që operatorët ekonomikë të kenë një nivel të mjaftueshëm përvoje që vërtetohet nga referenca të përshtatshme nga kontratat e zbatuara në të shkuarën. Aftësia profesionale e operatorëve ekonomikë për të ofruar shërbimin, punën, mallin vlerësohet në lidhje me aftësitë organizative, reputacionin dhe besueshmërinë, përvojën e duhur, si dhe personelin e nevojshëm për të zbatuar kontratën, siç është përshkruar nga autoriteti ose enti kontraktor në njoftimin e objektit të kontratës*.".

III.2.10. Në nenin 41, pika 4 "*Kërkesa të veçanta për kontratat shërbimeve*" të VKM Nr. 285 datë 19.5.2021 "*Për miratimin e rregullave të prokurimit publik*", i ndryshuar, parashikohet se:

"*4. Për të provuar përshtatshmërinë për të kryer veprimtarinë profesionale, kapacitetet teknike dhe profesionale, autoriteti/enti kontraktor kërkon:*
a) licenca profesionale për realizimin e shërbimeve, objekt i kontratës, të lëshuara nga autoritetet kompetente shtetërore; dhe/ose
b) një listë të personelit kryesor, të nevojshëm për të zbatuar objektin e prokurimit dhe/ose komponentët e saj. Lista e personelit kryesor duhet të përfshijë CV-të e tyre dhe licencat profesionale, kur kanë të tilla sipas legjislacionit përkatës; dhe/ose
c) fuqinë punëtore të operatorit ekonomik të nevojshëm për ekzekutimin e objektit të prokurimit; dhe/ose
ç) mjetet dhe pajisjet teknike që ka në dispozicion apo që mund t'i vihen në dispozicion operatorit ekonomik për të përmbushur kontratën;
d) Në rastin e prokurimit të shërbimeve me natyrë intelektuale, ku nuk mbizotërojnë aspektet fizike të veprimtarisë dhe që kërkojnë ekspertizë të posaçme, stafi i angazhuar të paraqesë deklaratë disponueshmërie për kryerjen e shërbimeve që ka marrë përsipër të realizojë.".

III.2.11. Komisioni i Prokurimit Publik gjykon, se kriteret për kualifikim vendosen që ti shërbejnë autoritetit kontraktor për njohjen e gjendjes dhe kapaciteteve të operatorëve ekonomikë, të cilët, nëpërmjet dokumentacionit të paraqitur duhet të vërtetojnë se zotërojnë kualifikimet e nevojshme teknike, profesionale, kapacitetet organizative, makineritë, pajisjet e asete të tjera fizike, reputacionin dhe besueshmërinë, përvojën e duhur, si dhe personelin e nevojshëm, gjithçka në funksion të realizimit me sukses të kontratës. Në këtë kuptim, për autoritetin kontraktor është e rëndësishme të provohet që operatorët ekonomikë pjesëmarrës në procedurën e prokurimit zotërojnë kapacitetin teknik e konkretisht dëshmi për përvojën e mëparshme. Autoriteti kontraktor është organi përgjegjës për prokurimin e fondeve publike, në përputhje me dispozitat ligjore e nënligjore në fuqi, ndaj dhe përcaktimi i kritereve të veçanta për kualifikim është lënë nën përgjegjësinë e autoritetit kontraktor, gjithnjë në përputhje e përpjesëtim me objektin e natyrën e kontratës së prokurimit. Dokumentet e tenderit dhe kriteret për kualifikim duhet të hartohen në përputhje me LPP-në dhe rregullat e prokurimit publik, në mënyrë të tillë që të nxisin pjesëmarrjen dhe konkurrencën e operatorëve ekonomikë, të stimulojnë pjesëmarrjen e biznesit të vogël dhe të mesëm, si dhe të sigurojnë një trajtim të barabartë dhe jodiskriminues për të gjithë operatorët ekonomikë, pjesëmarrës në këto procedura, për realizimin me sukses të kontratës me qëllim zgjerimin e rrethit të pjesëmarrjes së operatorëve ekonomikë në respekt të nenit 2 të LPP-së.

III.2.12. Lidhur me pretendimin e operatorit ekonomik ankimues përsa i përket kërkesës së autoritetit kontraktor të përcaktuar në pikën 2.3.4 "*Kapaciteti teknik*" të Shtojcës 9 "*FORMULAR I KRITEREVE TË PËRZGJEDHJES/KUALIFIKIMIT*" të dokumentave të tenderit, Komisioni konstaton se operatori ekonomik ankimues në formularin e ankesës elektronike me numër ankimi elektronik A/2026/6720 dhe me numër protokolli nr. 1636/2026 prot., datë 26.05.2026 ka ngritur pretendime për heqjen e kërkesë së autoritetit kontraktor lidhur me disponimin në stafin e operatorëve ekonomik ofertues të punonjësve të kualifikuar, si në vijim: "*1 (një) specialist tëe certifikuar CIR "Certified Incident Responder" ose ekuivalente, 2 (dy) specialist tëe certifikuar pëer SIEM "Security Information and Event Management" ose ekuivalente, 2 (dy) specialist tëe certifikuar Penetration Tester ose ekuivalente, 1 (një) specialist tëe certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente, 1 (një) specialist tëe certifikuar pëer Cybersecurity Analist ose ekuivalente dhe 2 (dy) specialist tëe certifikuar "Cyber Threat Hunting Professional" ose ekuivalente*.", duke kërkuar heqjen e kërkesë për disponimin në stafin e operatorit ekonomik ofertues të punonjësve të pajisur me 5 (pesë) lloje certifikimesh, ndërkohë që në konkluzionet e pretendimeve të parashtruara në formularin e ankesës ka ngritur pretendime për heqjen e kërkesës për disponimin në stafin e operatorit ekonomik të punonjësve të pajisur me 4 (katër) lloje certifikimesh dhe konkretisht, si në vijim: "*Për sa kemi paraqitur më sipër, në dritën e fakteve, bazuar në legjislacionin përkatës, përfundimisht kërkojmë:*

1. Pranimin e ankesës sonë.

2. KËRKESA: ".2.4, pika b "(një) specialist te certifikuar CIR "Certified Incident Responder" ose ekuivalente; , TË HIQET.

3. KËRKESA: "2.2.4, pika d) "(një) specialist te certifikuar CIR "Certified Incident Responder" ose ekuivalente; , TË HIQET.

4. KËRKESA: "2.2.4, pika e "1 (një) specialist të certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente, TË HIQET.

5. KËRKESA: "2.2.4, pika f "1 (një) specialist te certifikuar per Cybersecurity Analist ose ekuivalente; TË HIQET.

6. KËRKESA: "2.2.4, pika i "2 (dy) specialist te certifikuar "Cyber Threat Hunting Professional" ose ekuivalente; TË HIQET.", por nga shqyrtimi i pretendimeve Komisioni vlerëson që të trajtojë pretendimet e ankimuesit për të 5 (pesë) llojet e certifikimeve.

Nga shqyrtimi i dokumentave të tenderit, Komisioni konstaton se autoriteti kontraktor në kriterin kualifikues të përcaktuar në pikën 2.3.4 "*Kapaciteti teknik*" të Shtojcës 9 "*FORMULAR I KRITEREVE TË PËRZGJEDHJES/KUALIFIKIMIT*" të dokumentave të tenderit ka përcaktuar se operatorët ekonomike ofertues që të kualifikohen në këtë procedurë prokurimi duhet që të dëshmojnë se disponojnë në stafin e tyre punonjës të kualifikuar, si në vijim: "*1 (një) specialist tëe certifikuar CIR "Certified Incident Responder" ose ekuivalente, 2 (dy) specialist tëe certifikuar pëer SIEM "Security Information and Event Management" ose ekuivalente, 2 (dy) specialist tëe certifikuar Penetration Tester ose ekuivalente, 1 (një) specialist tëe certifikuar*

OSCP "Offensive Security Certified Professional" ose ekuivalente, 1 (një) specialist tëe certifikuar pëer Cybersecurity Analist ose ekuivalente dhe 2 (dy) specialist tëe certifikuar "Cyber Threat Hunting Professional" ose ekuivalente.".

Nga shqyrtimi i procesverbalit të argumentimit të kritereve dhe specifikimeve teknike të publikuar në sistemin e prokurimeve elektronike, Komisioni konstaton se autoriteti kontraktor ka argumentuar vendosjen e kriterit të mësipër, duke arsyetuar, si në vijim: "***Argumentim:*** *Në zbatim të nenit 77 të ligjit nr. 162/2020 "Për Prokurimin Publik" (i ndryshuar), si dhe nenit 41 të VKM nr. 285, datë 19.05.2021, (i ndryshuar), Autoriteti Kontraktor ka përcaktuar kriteret për kapacitetet profesionale të operatorëve ekonomikë, me qëllim garantimin e realizimit me sukses të kontratës, sigurimin e vazhdimësisë së shërbimeve kritike të teknologjisë së informacionit dhe sigurisë kibernetike, si dhe minimizimin e riskut operacional që mund të sjellë ndërprerja ose kompromet*imi *i sistemeve ekzistuese të Autoritetit Kontraktor.**Argumentim për pikën b):*** *Kërkesa për 1 (një) specialist të certifikuar **CIR "Certified Incident Responder**" ose ekuivalent është e nevojshme për garantimin e kapaciteteve profesionale në identifikimin, analizimin dhe menaxhimin e incidenteve të sigurisë kibernetike. Ky specialist është i domosdoshëm për të siguruar reagim të shpejtë dhe efektiv ndaj incidenteve që mund të cenojnë integritetin, konfidencialitetin dhe disponueshmërinë e sistemeve dhe të dhënave të Autoritetit Kontraktor.*

Argumentim për pikën d) *Kërkesa për 2 (dy) specialistë të certifikuar "**Penetration Tester**" ose ekuivalent është vendosur për realizimin e testimeve të sigurisë, identifikimin paraprak të dobësive potenciale dhe analizimin e vulnerabiliteteve në sistemet dhe rrjetet ekzistuese të Autoritetit Kontraktor. Këta specialistë do të kontribuojnë në evidentimin dhe adresimin e rreziqeve që mund të shfrytëzohen nga sulme kibernetike, si dhe në forcimin e kapaciteteve të AK-së për mbrojtje dhe kundërpërgjigje ndaj incidenteve të sigurisë. Gjithashtu, ekspertiza e tyre mbështet implementimin e praktikave, procedurave dhe politikave të sigurisë kibernetike, në përputhje me kompleksitetin e infrastrukturës teknologjike ekzistuese dhe rëndësinë e garantimit të vijueshmërisë operacionale të sistemeve.*

Argumentim për pikën e) *Kërkesa për 1 (një) specialist të certifikuar **OSCP "Offensive Security Certified Professional**" ose ekuivalent është vendosur për të garantuar ekspertizë të avancuar në analizimin e sigurisë së sistemeve, identifikimin e vulnerabiliteteve dhe realizimin e testimeve praktike të penetrimit. Ky specialist do të kontribuojë në forcimin e kapaciteteve të AK-së për mbrojtje dhe kundërpërgjigje ndaj sulmeve kibernetike, si dhe në implementimin e praktikave, procedurave dhe politikave të sigurisë kibernetike për mbrojtjen e sistemeve dhe të dhënave digjitale.*

Argumentim për pikën f) *Kërkesa për 1 (një) specialist të certifikuar "**Cybersecurity Analyst**" ose ekuivalent është e nevojshme për të vënë në zbatim ekspertizën e tij profesionale analizuese, monitoruese, raportuese dhe trajnuese, me qëllim forcimin e mbrojtjes ndaj sulmeve dhe rreziqeve kibernetike që mund të cenojnë sistemet dhe të dhënat digjitale të AK-së. Ky specialist do të kontribuojë në identifikimin, analizimin dhe menaxhimin e incidenteve të sigurisë, si dhe në*

implementimin e praktikave, procedurave dhe politikave të sigurisë kibernetike, duke mbështetur AK-në në rritjen e kapaciteteve të saj për kundërpërgjigje dhe garantimin e sigurisë operacionale të sistemeve.

Argumentim për pikën i) *Kërkesa për 2 (dy) specialistë të certifikuar "**Cyber Threat Hunting Professional**" ose ekuivalent është vendosur për të garantuar identifikimin, analizimin dhe parandalimin proaktiv të kërcënimeve kibernetike, si dhe për të siguruar mosndërprerjen e shërbimit dhe vijueshmërinë e punës së AK-së. Duke qenë se këto certifikime janë të specializuara dhe të dedikuara për sigurinë kibernetike, kërkohet që specialistët e paraqitur të disponojnë certifikime të përshtatshme dhe ekuivalente me kërkesat e AK-së.*", duke i argumentuar se këto kërkesa janë hartuar duke u mbështetur në parashikimet ligjore të të nenit 77 të ligjit nr. 162/2020 "*Për Prokurimin Publik*", i ndryshuar dhe nenit 41 të VKM nr. 285, datë 19.05.2021"Për miratimin e rregullave të prokurimit publik", i ndryshuar, si dhe në natyrën e objektit të prokurimit, e cila lidhet me shërbimin e sigurisë kibrnetike të sistemeve të teknologjisë së informacionit që disponon autoriteti kontraktor.

Nga shqyrtimi i specifikimeve teknike të përcaktuara në Shtojceën 6 "*FORMULARI I SPECIFIKIMEVE TEKNIKE*" të dokumentave të tenderit dhe termave të referencës së shërbimit object prokurimi të përcaktuara në Shtojcën 8 "*FORMULARI I TERMAVE TË REFERENCËS*" të dokumentave të tenderit, Komisioni konstaton se objekti i prokurimit është shërbimi për rinovimin e garancisë dhe licencave për pajisjet e sigurië FortiGate-401F dhe FortiGate-601F, si dhe mbështetjes teknike për një periudhë prej 48 (dyzet e tetë) muajsh, duke implementuar **zgjidhje të avancuar të tipit XDR (Extended Detection and Response) të tipit "Turnkey"** e cila është plotësisht e projektuar, ndërtuar, dorëzuar dhe implementuar, dhe është gati për përdorim të menjëhershëm, si dhe duhet të jetë në gjendje të mbrojë minimalisht 1200 stacione pune përmes një agjenti të vetëm të instaluar në pikat fundore, si dhe **implementimin e zgjidhjes SIEM**, e cila është një zgjidhje të plotë "turnkey", nga fillimi në fund, e cila është plotësisht e projektuar, ndërtuar, dorëzuar dhe implementuar dhe është gati për përdorim të menjëhershëm, e cila kundërvepron me kërcënimet kibernetike, duke mundësuar zbulimin e tyre me mbështetjen e mekanizmave machine learning, duke siguruar automatizimin dhe orkestrimin e përgjigjeve ndaj kërcënimeve kibernetike, e cila mundëson konfigurimin on-prem, e cila duhet të ketë licencë të përhershme për 1200 asete me mbështetje për një periudhë prej 48 muajsh.

Gjithashtu në specifikimet teknike dhe termat e referencës autoriteti kontraktor ka përcaktuar se operatori ekonomik i suksesshëm gjatë zbatimit të kontratës do të ofrojë shërbime të sigurisë kibernetike për instalimin, konfigurimin, integrimin dhe operacionalizimin e **zgjidhjeve Extended Detection and Response (XDR)** dhe **një zgjidhjeje Security Information and Event Management (SIEM)**, ku implementimi i **zgjidhjeve Extended Detection and Response (XDR)** përfshin: "*Deploy dhe konfigurim i zgjidhjes; Integrim me endpoint-e, serverë, pajisje rrjeti, fireëall, ëorkload-e; Konfigurim i feed-eve të inteligjencës së kërcënimeve; Rregullim i politikave dhe optimizim i alarmeve; Krijimi i ëorkfloë-ve të automatizuara të reagimit; Konfigurimi i aksesit dhe roleve; Fortifikim i platformës dhe Transferim njohurish*",

ndërsa implementimi i **zgjidhjes Security Information and Event Management (SIEM) përfshin: "***Instalimi i platformës SIEM (on-premise); Onboarding i burimeve të log-eve (serverë, aplikacione, fireëall, identitet, cloud, etj.); Parsing, normalizim dhe krijim rregullash korrelacioni; Zhvillim i use-case-ve sipas riskut të autoritetit; Krijim dashboard-esh dhe raportesh; UEBA dhe SOAR; Raportim i pajtueshmërisë dhe Optimizim i performancës.*", ndërkohë që kontraktori duhet të ofrojë shërbime të mirëmbajtjes së këtyre zgjidhjeve, duke përfshirë: "*Shërbime dhe suport proaktiv (një herë në muaj), të cilët duhet të mundësojnë detektimin në kohë të problematikave dhe duhet të mundësojnë ndërmarrjen në kohë të hapave rekuperues, për të mos pasur ndërprerje të shërbimit; shërbime të riparimit në përgjigje të "Alarmeve Madhore" të raportuara nga personeli i autorizuar i autoritetit kontraktor, Kontrolle të log-eve të pajisjeve të rrjetit, Rekomandime për upgrade të mundshme hardëare; Rinovimin e garancisë dhe licencave "Unified Threat Protection (UTP)" për pajisjet fireëall FortiGate-401F dhe FortiGate-601F për një periudhë 48 mujore*; *Furnizimin dhe implementimin e një zgjidhjeje XDR/EDR për minimumi 1200 përdorues; Furnizimin dhe implementimin e një zgjidhjeje SIEM on-premise për monitorimin dhe menaxhimin e incidenteve të sigurisë; Instalimin, konfigurimin dhe integrimin e zgjidhjeve XDR dhe SIEM me infrastrukturën ekzistuese të Autoritetit Kontraktor; Konfigurimin e politikave të sigurisë, ëorkfloë-ve të automatizuara dhe mekanizmave të reagimit ndaj incidenteve; Integrimin me fireëall, endpoint-e, serverë, sisteme identiteti, log-e dhe burime të tjera të të dhënave; Kryerjen e testimeve funksionale dhe operacionalizimin e plotë të sistemeve; Transferimin e njohurive dhe asistencën teknike për stafin e Autoritetit Kontraktor; Ofrimin e mirëmbajtjes proaktive dhe suportit teknik 24/7 gjatë gjithë periudhës së kontratës; Reagimin ndaj alarmeve madhore sipas niveleve të shërbimit të përcaktuara në specifikimet teknike; Kryerjen e kontrolleve periodike, analizave të log-eve dhe rekomandimeve për optimizimin e infrastrukturës së sigurisë.*".

Gjithashtu lidhur me pretendimin e ankimuesit për këtë kriter kualifikues Komisioni i Shqyrtimit të Ankesës me shkresën shkresën nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, nuk ka pranuar pretendimet e ankimuesit, duke argumentuar si në vijim: "*Arsyetim për kërkesën e specialistit të certifikuar* ***CIR (Certified Incident Responder)*** *ose ekuivalent në procedurën e tenderimit për SIEM dhe XDR.*

Implementimi dhe operimi i platformave SIEM (Security Information and Event Management) dhe XDR (Extended Detection and Response) përbëjnë komponentë kritikë të sigurisë kibernetike, të cilët kanë rol thelbësor në monitorimin, identifikimin, analizimin dhe reagimin ndaj incidenteve të sigurisë në infrastrukturat IT të institucionit.

Për shkak të kompleksitetit teknik dhe rëndësisë së lartë operacionale të këtyre sistemeve,

kërkohet që operatori ekonomik të disponojë staf të specializuar dhe të certifikuar në fushën e reagimit ndaj incidenteve të sigurisë kibernetike, siç është certifikimi CIR (Certified Incident Responder) ose një certifikim ekuivalent i njohur ndërkombëtarisht.

Kjo kërkesë argumentohet mbi bazën e faktoreve të mëposhtëm:

- *Menaxhimi profesional i incidenteve tee sigurisee*

Platforma SIEM dhe XDR kanë si funksion kryesor identifikimin dhe trajtimin e incidenteve të sigurisë në kohë reale. Një specialist i certifikuar CIR zotëron njohuri dhe aftësi praktike për analizimin, klasifikimin, investigimin dhe neutralizimin e kërcënimeve kibernetike, duke garantuar reagim të shpejtë dhe efektiv ndaj incidenteve.

- *Reduktimi i riskut operacional dhe te sigurise*

Konfigurimi jo korrekt ose mungesa e ekspertizës në menaxhimin e alarmeve dhe ngjarjeve të sigurisë mund të sjellë pasoja serioze, përfshirë mosidentifikimin e sulmeve, vonesa në reagim apo kompromet im të sistemeve kritike. Certifikimi CIR garanton se specialisti posedon kompetencat e nevojshme për të minimizuar këto rreziqe.

- *Kërkesë në përputhje me praktikat dhe standardet ndërkombetare*

Angazhimi i specialistëve të certifikuar neë incident response është praktike standarde në projektet moderne të sigurisë kibernetike dhe rekomandohet nga kuadrot ndërkombetarë të sigurisë si NIST, ISO/IEC 27035 dhe standardet e operimit të SOC (Security Operations Center).

- *Garantimi i cilësisë së shërbimit*

Certifikimet profesionale si CIR ose ekuivalente dëshmojnë që personeli ka kaluar trajnim dhe Vlerësim teknik të specializuar në fushën e incident response dhe cyber defense, duke ritur besueshmërinë dhe cilësinë e shërbimit të ofruar.

- *Përputhshmëria me natyrën kritike të sistemeve SIEM/DR*

Duke qënë se sistemet SIEM dhe DR lidhen dretpërdrejt me mbrojtien e aseteve kritike të institucionit, kërkohet nivel i avancuar ekspertize për administrimin, tuning-un e regullave të detektimit, analizën e log-eve, korelacionin e ngjarjeve dhe reagimin ndaj sulmeve të avancuara.
Për sa më sipër, kërkesa për një specialist të certifikuar CIR ose ekuivalent konsiderohet proporcionale, e arsyeshme dhe e lidhur dretpërdrejt me objektin e kontratës, me qëllim garantimin e sigurisë, cilësisë dhe vazhdimësisë së shërbimeve të kërkuara.
Arsyetim për kërkesën e një specialisti të certifikuar ***OSCP (Offensive Security Certified Professional)*** *ose ekuivalent në proceduren e tenderimit për SIEM dhe XDR.*
Kërkesa për angazhimin e të pakten një specialisti të certifikuar OSCP (Offensive Security Certified Professional) ose ekuivalent konsiderohet e domosdoshme për realizimin me sukses të implementimit, konfigurimit dhe optimizimit të sistemeve SIEM (Security Information and Event Management) dhe DR (Extended Detection and Response), për shkak të nivelit të lartë teknik dhe kritik të sigurisë që këto sisteme përfaqësojnë.

Sistemet SIEM dhe XDR kane rol kyç në identifikimin, analizimin, korelacionin dhe reagimin ndaj incidenteve të sigurisë kibernetike në kohë reale. Implementimi i tyre kërkon njohuri të avancuara në:

- *monitorimin dhe analizën e logeve të sigurisë;*
- *identifikimin e teknikave të avancuara të sulmeve kibernetike;*
- *threat hunting dhe incident response;*

- *konfigurimin e use-case-ve të sigurisë;*
- *validimin e mekanizmave të detektimit përmes simulimit të sulmeve reale;*
- *analizën e vulnerabiliteteve dhe teknikave të kompromet imit të sistemeve*

Certifikimi OSCP është një nga certifikimet më të njohura ndërkombëtarisht në fushën e sigurisë offensive dhe testimit praktik të penetrimit. Ky certifikim vërteton që specialisti zotëron aftësi praktike për të identifikuar, shfrytëzuar dhe analizuar dobësi reale në infrastrukturat IT, si dhe për të kuptuar metodologjitë dhe taktikat që përdoren nga aktorët keqdashës.

Perfshirja e një specialisti me këtë nivel certifikimi garanton që:

- *konfigurimet dhe rregullat e detektimit në SIEM/XDR do të ndërtohen mbi skenarë reale kërcënimesh;*
- *sistemi do të jetë në gjendje të identifikojëë sulme komplekse dhe tentativa kompromet imi;*
- *do të minimizohen "false positive" dhe "false negative";*
- *do të realizohet validimi praktik i use-case-ve të sigurisë;*
- *organizata do të përfitojë një nivel më të lartë mbrojtjeje dhe reagimi ndaj incidenteve kibernetike.*

Gjithashfu, duke qenë se SIEM dhe XDR përbëjnë sisteme kritike për mbrojtjen e infrastrukturës së teknologjisë së informacionit, kërkesa për specialist të certifikuar OSCP ose ekuivalent është në përputhje me praktikat më të mira ndërkombëtare për projekte të sigurisë kibernetike dhe synon të sigurojë cilësi, ekspertize teknike dhe besueshmëri në realizimin e kontratës.

Pranimi i certifikimeve ekuivalente lejon konkurrencë të hapur dhe pjesëmarrje më të gjërë të operatorëve ekonomike, duke ruajtur njëkohësisht standardin e kërkuar profesional dhe teknik për realizimin e projektit.

Arsyetim mbi kërkesën për Specialist teë ***Certifikuar Cybersecurity Analyst*** *ose ekuivalent në procedurën e tenderimit për SIEM dhe XDR.*

Kërkesa për disponimin e një specialisti të certifikuar në fushën e Cybersecurity Analyst ose ekuivalente është e domosdoshme për natyrën dhe kompleksitetin e projektit që lidhet me implementimin, konfigurimin dhe menaxhimin e sistemeve SIEM (Security Information and Event Management) dhe XDR (Extended Detection and Response).

Zgjidhjet SIEM dhe XDR përbëjnë komponentë kritikë të sigurisë kibernetike të infrastrukturës IT, pasi ato mundësojnë monitorimin në kohe reale, analizimin e ngjarjeve të sigurisë, identifikimin e incidenteve, korrelacionin e log-eve dhe reagimin ndaj kërcënimeve kibernetike. Implementimi dhe administrimi korrekt i këtyre platformave kërkon njohuri të avancuara teknike në analizën e sigurisë, menaxhimin e incidenteve, threat hunting, incident response dhe interpretimin e ngjarjeve të sigurisë.

Për këtë arsye, operatori ekonomik duhet të disponojë staf të kualifikuar dhe të certifikuar, i cili garanton se shërbimet do të realizohen sipas standardeve më të mira ndërkombëtare të sigurisë

kibernetike. Certifikimi si Cybersecurity Analyst ose ekuivalent vërteton kompetencën profesionale të specialistit në:

- *monitorimin dhe analizimin e incidenteve të sigurisë;*
- *identifikimin dhe reagimin ndaj kërcënimeve kibernetike;*
- *përdorimin dhe administrimin e platformave SIEM/XDR;*
- *analizën e log-eve dhe korrelacionin e ngjarjeve;*
- *implementimin e praktikave të sigurisë sipas standardeve ndërkombëtare.*

Gjithashtu, për shkak të ndjeshmërisë së sistemeve që do të monitorohen dhe ndikimit që një konfigurim i pasaktë mund të ketë në sigurinë e institucionit, prania e një eksperti të certifikuar minimizon rrezikun operacional dhe garanton cilësi, besueshmëri dhe vazhdimësi në ofrimin e shërbimit.

Kjo kërkesë eshtë në përpjesëtim me objektin e kontratës dhe nuk kufizon konkurrencën, pasi pranohen certifikime ekuivalente të njohura ndërkombëtarisht në fushën e sigurisë kibernetike.

*Arsyetim për kërkesën e stafit të certifikuar "**Cyber Threat Hunting Professional**" ose ekuivalente në procedurën e prokurimit për SIEM dhe XDR*

Kërkesa që operatori ekonomik pjesëmarrës në procedurën e prokurimit të disponojë të paktën 2 (dy) specialistë të certifikuar "Cyber Threat Hunting Professional" ose ekuivalente. konsiderohet e domosdoshme dhe proporcionale me natyrën, kompleksitetin dhe rëndësinë e shërbimeve që lidhen me implementimin, konfigurimin dhe operimin e platformave SIEM (Security Information and Event Management) dhe XDR (Extended Detection and Response).

Zgjidhjet SIEM dhe XDR përbëjnë komponentë kritikë të sigurisë kibernetike, të cilët kanë si funksion monitorimin në kohë reale, analizimin e ngjarjeve të sigurisë, identifikimin e kërcënimeve të avancuara, korelacionin e log-eve dhe reagimin ndaj incidenteve kibernetike.

Për shkak të natyrës dinamike dhe sofistikimit në rritje të sulmeve kibernetike, kërkohet personel me ekspertizë të specializuar në "threat hunting", analizë proaktive të kërcënimeve dhe identifikim të anomalive që nuk evidentohen nga mekanizmat standardë të sigurisë.

Certifikimi "Cyber Threat Hunting Professional" ose ekuivalent garanton që specialistët posedojnë njohuri dhe aftësi të avancuara në:

- *identifikimin proaktiv të kërcënimeve kibernetike;*
- *analizimin e indikatorëve të kompromet imit (IOC);*
- *përdorimin efektiv të platformave SIEM/XDR;*
- *investigimin dhe korrelacionin e ngjarjeve të sigurisê;*
- *reagimin ndaj incidenteve dhe minimizimin e riskut operacional.*

Kerkesa për minimumi 2 (dy) specialistë është vendosur për të garantuar:

- *vazhdimësinë e shërbimit dhe mbulimin operacional;*
- *redundancën teknike dhe shmangien e varësisë nga një individ i vetëm;*
- *përballimin e volumeve të larta të analizës së ngjarjeve dhe incidenteve;*

- *disponueshmërinë e ekspertizës gjatë gjithë ciklit të implementimit dhe suportit të zgjidhjes.*

Gjithashtu, kjo kërkesë lidhet drejtpërdrejt me rëndësinë e mbrojtjes së infrastruktures kritike të teknologjisë së informacionit, ruajtjen e konfidencialitetit, integritetit dhe disponueshmërisë së të dhënave, si dhe me nevojën për të garantuar standarde të larta të sigurisë kibernetike gjatë ekzekutimit të kontratës.

Përrjedhojë, kërkesa konsiderohet objektive, e arsyeshme, proporcionale dhe në funksion të garantimit të cilësisë, sigurisë dhe besueshmërisë së shërbimit që prokurohet.

Pretendimet tuaja mbi këtë kriterin 2.3.4 pikat b), d), e), f) dhe i), vlerësohen si jo të drejta nga "Komisioni i Shqyrtimit të Ankesës".".

Nga shqyrtimi i pretendimeve të ankimuesit dhe i dokumentave të tenderit, Komisioni konstaton se objekti i prokurimi është instalimi dhe implementimi i zgjidhjeve XDR dhe SIEM" e cila nënkupton një projekt të plotë teknik dhe jo thjesht blerjen e licencave, duke përfshirë furnizimin e platformës dhe licencave, instalimin e agjentëve në kompjuterë dhe serverë, lidhjen e fireëall-eve, sëitch-eve, router-ave dhe sistemeve të tjera, integrimin me Active Directory ose sistemet e identitetit, konfigurimin e burimeve të log-eve, integrimin e sistemeve, lidhjen e email-it, cloud-it dhe aplikacioneve, konfigurimin e dërgimit të log-eve drejt SIEM-it, integrimin e XDR me burimet e sigurisë, krijimin e rregullave dhe alarmeve, rregulla për zbulimin e sulmeve, korelacionin e ngjarjeve, dashboard-e monitorimi, njoftime automatike, testimin dhe vënien në punë, testimin e funksionimit, simulimin e incidenteve, verifikimin e alarmeve, trajnimin dhe dokumentimin, duke mos u mjaftuar vetëm në dorëzimin e licensave por edhe në kryerjen e punës profesionale për ta bërë sistemin funksional dhe operacional, ndaj dhe për realizimin e objektit të prokurimit është e nevojshme që operatorët ekonomikë ofertues të disponojnë në stafin e tyre punonjës të kualifikuar në fushën e sigurisë kibernetike, vërtetuar kjo me anë të certifikatave përkatëse dhe ku aftësia profesionale e këtyre punonjësve është shumë e rëndësishme për realizimin e objektit të prokurimit, i cili është shumë sensistiv për autoritetin kontraktor, pasi është e lidhur ngushtësisht me sigurinë e sistemeve elektronike që disponon autoriteti kontraktor për ofrimin e një shërbimi sa më "*1 (një) specialist tëe certifikuar CIR "Certified Incident Responder" ose ekuivalente, 2 (dy) specialist tëe certifikuar pëer SIEM "Security Information and Event Management" ose ekuivalente, 2 (dy) specialist tëe certifikuar Penetration Tester ose ekuivalente, 1 (një) specialist tëe certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente, 1 (një) specialist tëe certifikuar pëer Cybersecurity Analist ose ekuivalente dhe 2 (dy) specialist tëe certifikuar "Cyber Threat Hunting Professional" ose ekuivalente*."me pretendimet e mësipërme të operatorit ekonomik ankimues, Komisioni gjykon se nuk qëndrojnë, pasi kërkesa e autoritetit kontraktor që operatorët ekonomikë ofertues të dëshmojnë se disponojnë në stafin e tyre 1 (një) specialist tëe certifikuar CIR "Certified Incident Responder" ose ekuivalente, 2 (dy) specialist tëe certifikuar pëer SIEM "Security Information and Event Management" ose ekuivalente, 2 (dy) specialist tëe certifikuar Penetration Tester ose ekuivalente, 1 (një) specialist tëe certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente, 1 (një) specialist tëe certifikuar pëer Cybersecurity Analist ose ekuivalente dhe 2 (dy) specialist tëe certifikuar "Cyber Threat Hunting Professional" ose ekuivalente është një kërkesë në porporcion me natyrën dhe volumin e objektit të prokurimit,

pasi sikurse theksuam edhe më lart objekti i prokurimit është shërbimi i sigurisë kibernetike ndërkohë që edhe certifikatat e kërkuara dëshmojnë se mbajtësit e këtyre certifikatave zoterojnë aftësi profesionale në fushën e sigurisë kibernetike, si një fushë shumë sensitive për sigurinë e sistemeve, si dhe janë të nevojshëm për të realizuar shërbimet objekt prokurimi. Nga shqyrtimi i specifikimeve teknike dhe termave të referencës Komisioni konstaton se objekti i prokurimi është instalimi dhe implementimi i zgjidhjeve XDR dhe SIEM" e cila nënkupton një projekt të plotë teknik dhe jo thjesht blerjen e licencave, duke përfshirë furnizimin e platformës dhe licencave, instalimin e agjentëve në kompjuterë dhe serverë, lidhjen e fireëall-eve, sëitch-eve, router-ave dhe sistemeve të tjera, integrimin me Active Directory ose sistemet e identitetit, konfigurimin e burimeve të log-eve, integrimin e sistemeve, lidhjen e email-it, cloud-it dhe aplikacioneve, konfigurimin e dërgimit të log-eve drejt SIEM-it, integrimin e XDR me burimet e sigurisë, krijimin e rregullave dhe alarmeve, rregulla për zbulimin e sulmeve, korelacionin e ngjarjeve, dashboard-e monitorimi, njoftime automatike, testimin dhe vënien në punë, testimin e funksionimit, simulimin e incidenteve, verifikimin e alarmeve, trajnimin dhe dokumentimin, duke mos u mjaftuar vetëm në dorëzimin e licensave por edhe në kryerjen e punës profesionale për ta bërë sistemin funksional dhe operacional.

KPP gjykon se kriteret për kualifikim vendosen që ti shërbejnë autoritetit kontraktor për njohjen e gjendjes dhe kapaciteteve të operatorëve ekonomikë, të cilët, nëpërmjet dokumentacionit të paraqitur duhet të vërtetojnë se zotërojnë kualifikimet e nevojshme teknike, profesionale, kapacitetet organizative, makineritë, pajisjet e asete të tjera fizike, reputacionin dhe besueshmërinë, përvojën e duhur, si dhe personelin e nevojshëm, gjithçka në funksion të realizimit me sukses të kontratës. Autoriteti kontraktor harton dokumentet e tenderit, në përputhje me dispozitat ligjore e nënligjore në fuqi ndaj dhe përcaktimi i kritereve të veçanta për kualifikim është lënë nën përgjegjësinë e autoritetit kontraktues, gjithnjë në përputhje e përpjesëtim me objektin e natyrën e kontratës së prokurimit. Në varësi të kontratës dhe volumit të saj autoriteti kontraktor përcakton kërkesat e veçanta për kualifikim, të cilat janë të detyrueshme për t'u përmbushur nga operatorët ekonomikë pjesëmarrës në procedurat e prokurimit. Lidhur me pretendimin e operatorit ekonomik ankimues "*PC STORE*" SHPK për kundërshtimin e dokumentave të tenderit lidhur me kriterin e veçantë të kualifikimit të përcaktuar në pikën 2.3.4 "*Kapaciteti teknik*" të Shtojcës 9 "*FORMULAR I KRITEREVE TË PËRZGJEDHJES/KUALIFIKIMIT*" të dokumentave të tenderit, për pretendimin për heqjen e. kërkesës që operatorët ekonomikë ofertues të kenë të punësuar në stafin e tyre punonjës të kualifikuar, sin ë vijim: "*1 (një) specialist tëe certifikuar CIR "Certified Incident Responder" ose ekuivalente, 2 (dy) specialist tëe certifikuar pëer SIEM "Security Information and Event Management" ose ekuivalente, 2 (dy) specialist tëe certifikuar Penetration Tester ose ekuivalente, 1 (një) specialist tëe certifikuar OSCP "Offensive Security Certified Professional" ose ekuivalente, 1 (një) specialist tëe certifikuar pëer Cybersecurity Analist ose ekuivalente dhe 2 (dy) specialist tëe certifikuar "Cyber Threat Hunting Professional" ose ekuivalente*.", Komisioni i Prokurimit Publik nga shqyrtimi i dokumentave të tenderit konkretisht specifikimeve teknike të shërbimit object prokurimi të përcaktuara në Shtojceën 6 "*FORMULARI I SPECIFIKIMEVE*

TEKNIKE” të dokumentave të tenderit dhe termave të referencës së shërbimit objekt prokurimi të përcaktuara në Shtojcën 8 “*FORMULARI I TERMAVE TË REFERENCËS*” të dokumentave të tenderit, konstaton, se kemi të bëjmë me një procedurë specifike dhe sensitive referuar objektit të prokurimit që është shërbimi i zhvillimit dhe implementimit të zgjidhjeve të sigurisë kibernetike për sistemet infomatike jetike që ka në përdorim autoriteti kontraktor. Për realizimin e procedurës objekt ankimi nevojitet një staf i specializuar për të cilin për të patur sigurinë për realizimin me sukses të objektit të procedurës autoriteti kontraktor ka kërkuar dorëzimin e certifikatave sipas kategorive të caktuara, referuar profilit të secilit prej punonjësve ose të certifikatave ekuivalente. Nisur nga pretendimi i operatorit ekonomik ankimues Komisioni konstaton, se operatori ekonomik nuk ka arritur të argumentojë se si kërkesa e autoritetit kontraktor për dorëzimin e certifikatave të kërkuara apo certifikave ekuivalente të tyre cënon interesin e tij të ligjshëm dhe ngushton konkurencën. Nga ana tjetër referuar procesverbalit “Për argumentimin dhe miratimin e specifikimeve teknike dhe kritereve për kualifikim”, autoriteti kontraktor ka argumentuar nevojën për secilin nga specialistët për realizimin me sukses të kontratës. Akoma më tej Komisioni gjykon, se punonjësit e kërkuar si dhe kualifikimet e tyre janë përcaktuar bazuar në natyrën e shërbimit, duke u përputhur me specifikimet teknike, termat e referencës, objektin e prokurimit dhe proceset e punës që do të kryejë secili. Referuar natyrës së punës që do të kryejë secili prej punonjësve për punonjësit e përcaktuar në pikat b, d, e, f, i, të kriterit kualifikues të pikës 2.3.4 “*Kapaciteti teknik*” të Shtojcës 9 “*FORMULAR I KRITEREVE TË PËRZGJEDHJES/KUALIFIKIMIT*” të dokumentave të tenderit për shkak të natyrës së punës Komisioni gjykon, se kërkesa e autoritetit kontraktor për paraqitjen e certifikatave përkatëse i shërben synimit të autoritetit kontraktor dhe nuk shkon përtej asaj, se çfarë është e nevojshme për realizimin e synimit, pasi nisur nga detyrat që do të kryejnë është e nevojshme që të zotërojnë njohuri më të thelluara të cilat mund të vërtetohen përmes paraqitjes së certifikatës përkatëse ose certifikatës ekuivalente, pasi janë njohuri që nuk mund të fitohen nëpërmjet trajnimeve. Pra paraqitja e certifikatës është proporcionale me objektin e prokurimit dhe në përpjesëtim dhe e lidhur ngushtë me objektin e kontratës. KPP gjykon, se ky kriter është i përshtatshëm për arritjen e synimit të kërkuar dhe nuk shkon përtej asaj, se çfarë është e nevojshme për të arritur synimin duke përmbushur në këtë mënyrë edhe testin e proporcionalitetit në lidhje me hartimin e tij. Komisioni gjykon, se formimi profesional i personelit përbën domosdoshmëri dhe garanton autoritetin kontraktor për kapacitetet profesionale të ofertuesve për përmbushjen me sukses të kontratës, gjë e cila vërtetohet vetëm me certifikatën sipas kategorive dhe shërbimeve që do të kryejë secili nga punonjësit. Akoma më tej referuar ankesës me numër ankimi elektronik A/2026/6720, datë 25.05.2026 dhe me numër protokolli nr. 1636/2026 prot., datë 26.05.2026operatorit ekonomik nuk ka argumentuar se si ky kriter cënon interesin e tij të ligjshëm dhe cënon konkurrencën.

Përsa më sipër, pretendimi i operatorit ekonomik ofertues “PC STORE” SHPK nuk qëndron.

III.3. Lidhur me pretendimin e operatorit ekonomik ankimues "*PC STORE*" SHPK për sqarim dhe për modifikimin e specifikimeve teknike të përcaktuarsa në Shtojcën 6 "*FORMULARI I SPECIFIKIMEVE TEKNIKE*" të dokumentave të tenderit të procedurës së prokurimit objekt ankimi, të parashtruara në formularin e ankesës, në kërkesën nr. 7, në kërkesën nr. 8.1, në kërkesën nr. 8.2, në kërkesën nr. 8.3, në kërkesën nr. 8.4 dhe në kërkesën nr. 8.5, në ankesën me numër ankimi elektronik A/2026/6720 dhe me numër protokolli nr. 1636/2026 prot., datë 26.05.2026, Komisioni i Prokurimit Publik vëren se,

III.3.1. Në shtojcën 6 "*FORMULAR I SPECVIFIKIMEVE TEKNIKE*", të dokumentave të tenderit nga ana e autoritetit kontraktor janë publikuar specifikimet teknike të objektit të prokurimit objekt ankimi, si më poshtë vijon:

Shtojca 6.

[Shtojcë për t'u plotësuar nga Autoriteti/Enti Kontraktor]

FORMULARI I SPECIFIKIMEVE TEKNIKE

Specifikimet Teknike të shërbimeve objekt i prokurimit, duhet të përshkruhen sa më saktë dhe plotësisht, për sa të jetë e mundur, duke krijuar kushte për konkurrencë të paanshme dhe të hapur midis të gjithë kandidatëve dhe ofertuesve. Specifikimet teknike, me përjashtim të rasteve plotësisht të justifikuara, duhet të hartohen në mënyrë të tillë që të marrin parasysh kriteret e aksesit për personat me aftësi të kufizuara ose projektimin për të gjithë përdoruesit, siç kërkohet nga ligji në fuqi.

SHËNIM: Në Specifikimet Teknike, nuk duhet të përshkruhet asnjë markë specifike prodhimi ose burim ose proces i veçantë, që karakterizon produktet ose shërbimet e ofruara nga një Operator specifik Ekonomik ose ndonjë markë tregtare, patentë, tip ose origjinë ose prodhim specifik, për të favorizuar ose eliminuar ndërmarrje ose produkte të caktuara. Një gjë e tillë lejohet vetëm në raste të jashtëzakonshme kur nuk ekziston një mënyrë e mjaftueshme, e saktë ose e kuptueshme për të përshkruar objektin e Kontratës. Referencat e tilla duhet të shoqërohen me fjalët "ose ekuivalent".

Në hartimin e specifikimeve teknike, autoritetet /entet kontraktore mbajnë në konsideratë detyrimet e përcaktuara në legjislacionin përkatës në fushat, si më poshtë:

a) Kërkesat minimale të performancës së energjisë, siç përcaktohet në legjislacionin në fuqi për efiçencën e energjisë dhe për performancën energjetike në ndërtesa, konsumin e energjisë dhe burimeve të tjera të produkteve me ndikim në energji, përfshirë parashikimet për përdorimin e etiketave për produktet me ndikim në energji;

b) Specifikimet teknike për produkte të caktuara, siç përcaktohet në aktet ligjore dhe nënligjore të fushës me qëllim përmirësimin e performancës energjetike dhe uljen e ndikimit;
c) Çdo parashikim tjetër që buron nga legjislacioni mjedisor, energjetik, social dhe i punës.

Skicimet, parametrat teknik etj:
Specifikimi i Materialeve:
Përshkrimi i kërkesave të zbatimit të shërbimeve në lidhje me to:

1. Shërbimi për rinovimin e garancisë dhe licencave të pajisjeve Fireëall
Operatori ekonomik duhet të realizojë rinovimin e garancisë dhe mbështetjes teknike për pajisjet e sigurisë FortiGate-401F dhe FortiGate-601F për një periudhë prej 48 (dyzet e tetë) muajsh, duke filluar nga data e lidhjes së kontratës. Në të njëjtën kohë, operatori ekonomik duhet të sigurojë rinovimin e licencave të tipit "Unified Threat Protection (UTP)" për këto pajisje për të njëjtën periudhë kohore.
Pajisjet për të cilat kërkohet ky shërbim identifikohen përmes numrave serialë përkatës, konkretisht:
***Numrat Serial FortiGate-401F:** FG4H1FT923903187; FG4H1FT923903005;*
***Numrat Serial FortiGate-601F:** FG6H1FTB22906053; FG6H1FTB22905816*

2. Zgjidhje XDR (Extended Detection and Response)
Autoriteti Kontraktor kërkon implementimin e një zgjidhjeje të avancuar të tipit XDR (Extended Detection and Response), e cila duhet të jetë në gjendje të mbrojë minimalisht 1200 stacione pune përmes një agjenti të vetëm të instaluar në pikat fundore

Zgjidhja duhet të:
• ketë aftësinë e regjistrimit dhe integrimit përmes një konsole të vetme menaxhimi me platforma të rrjetit (si Syslog dhe Ëindoës Event Collection);
• ketë aftësinë për zbulimin e kërcënimeve të avancuara, reagim të shpejtë ndaj incidenteve dhe monitorimin e vazhdueshëm të të gjitha stacioneve të punës;
*• ketë aftësinë për të identifikuar sjellje të dyshimta dhe kompromet*ime të mundshme, si dhe izolimin e kërcënimeve dhe lehtësimin e korrigjimit për të ruajtur integritetin dhe sigurinë e infrastrukturës së IT-së;
• të jetë e pajtueshme me sistemet operative si Microsoft Ëindoës, Linux, macOS, Android dhe iOS;
• të përfshijë agjentë softuerësh që mund të instalohen dhe të ekzekutohen në mënyrë të kontrolluar në pikat fundore fizike ose virtuale (serverë, stacione pune, laptopë, pajisje mobile), si dhe një platformë të centralizuar për menaxhimin e agjentëve.

a) Incidentet dhe Integrimi

Zgjidhja duhet të ketë aftësinë për integrim nativ me regjistrat nga fireëall-et (Fortinet, Cisco, Check Point, Palo Alto etj.).

Zgjidhja duhet të ketë aftësinë për të kombinuar alarmet e rrjetit nga pajisjet e lartpërmendura me alarmet nga pikat fundore për të realizuar korrelacion dhe për të arritur një kontekst më të mirë të sigurisë.

Zgjidhja duhet të përfshijë një periudhë minimale ruajtjeje prej 30 ditësh për të dhënat e papërpunuara të marra nga agjentët dhe të ofrojë mundësinë e ruajtjes në cloud për një periudhë nga 6 deri në 12 muaj përmes një licence shtesë.

Zgjidhja duhet të ofrojë menaxhim incidentesh ku të gjithë përdoruesit, stacionet, proceset dhe alarmet e përfshira mund të vizualizohen në mënyrë të plotë.

Zgjidhja duhet të ofrojë mundësinë e caktimit të një analisti sigurie për një incident specifik.

Zgjidhja duhet, në mënyrë native, të përdorë të dhënat e rrjetit për të identifikuar pikat fundore pa agjent të instaluar.

Zgjidhja duhet të ketë aftësi nisjeje të shpejtë, duke ofruar shkurtore drejt zonave të ndryshme të konsolës së menaxhimit.

Zgjidhja duhet të ofrojë mundësinë e integrimit të alarmeve të shumëfishta dhe lidhjes automatike të tyre në një incident të vetëm kur është e nevojshme.

Zgjidhja duhet të ofrojë shfaqjen e burimeve të inteligjencës së kërcënimeve në pamjen e incidentit (të paktën VirusTotal).

Zgjidhja duhet të lejojë modifikimin manual të nivelit të incidentit (i lartë / mesatar / i ulët).

Zgjidhja duhet të lejojë eksportimin e alarmeve dhe incidenteve në skedar.

Zgjidhja duhet të lejojë krijimin dhe redaktimin e "Indicators of Attack / Behaviour Indicators of Compromise" nga ndërfaqja grafike e menaxhimit.

Zgjidhja duhet të lejojë shikimin dhe redaktimin e rregullave të paracaktuara të këtyre indikatorëve të ofruara nga prodhuesi.

b) Zbulimi dhe Parandalimi i Kërcënimeve

Zgjidhja duhet të jetë në gjendje të parandalojë exploit-e bazuar në teknikat specifike të Linux-it, si Brute Force Protection, Java Deserialization, Privilege Escalation, Reverse Shell Protection, ROP Mitigation, Shellcode Protection dhe SO Hijacking Protection.

Zgjidhja duhet të jetë në gjendje të parandalojë exploit-e bazuar në teknikat specifike të macOS, si Anti-Ransomëare, Dylib Hijacking Protection, Gatekeeper Enhancement, JIT Mitigation, Privilege Escalation dhe ROP Mitigation.

Zgjidhja duhet të ofrojë mundësinë për të shtuar procese në Ëindoës, Linux dhe macOS që do të mbrohen nga moduli i mbrojtjes së exploit-eve.

Zgjidhja duhet të ofrojë mbrojtje kundër sulmeve ndaj MBR-së.

Zgjidhja duhet të lejojë dërgimin automatik të skedarëve të panjohur në sandbox cloud për analizë dhe të ofrojë raporte të detajuara të analizës.
Zgjidhja duhet të mbështesë skedarë deri në 100 MB për analizë në sandbox.
Zgjidhja duhet të mbështesë sandboxing në bare-metal për rastet e anashkalimit të sandbox-it.
Zgjidhja duhet të lejojë krijimin e përjashtimeve për exploit-e bazuar në MITRE ATT&CK pa çaktivizuar mbrojtjen globale.
Zgjidhja duhet të lejojë vizualizimin e proceseve të mbrojtura në sistemet operative nga konsola qendrore.
Zgjidhja duhet të krijojë automatikisht incidente dhe të përfshijë hostet dhe përdoruesit përkatës.
Zgjidhja duhet të lejojë vendosjen manuale të një score incidenti nga 0 deri në 100.
Zgjidhja duhet të ofrojë vizualizim të informacionit të kërcënimeve sipas IP-ve, gjeolokacionit dhe rrjetit.
Zgjidhja duhet të ofrojë mbrojtje kundër reverse shell në Linux.
Zgjidhja duhet të ofrojë mbrojtje UEFI kundër sulmeve para nisjes.
Zgjidhja duhet të mbështesë mbrojtjen ndaj restart-it në Safe Mode.
Zgjidhja duhet të ofrojë modul të dedikuar kundër ransomëare për Ëindoës dhe macOS.
Zgjidhja duhet të ofrojë mbrojtje për IIS.
Zgjidhja duhet të mbështesë mbrojtjen ndaj bypass-it të UAC.
Zgjidhja duhet të mbrojë shellcode për procese 32-bit në Ëindoës.
Zgjidhja duhet të ofrojë gjuhë të avancuar query për analiza të dhënash dhe incidente.
Zgjidhja duhet të lejojë konvertimin e query-ve në format JSON.

c) Aftësitë Forensics
Zgjidhja duhet të lejojë mbledhjen e artefakteve për analiza forensics në Ëindoës dhe macOS për minimumi 50 agjentë.
Zgjidhja duhet të përdorë të njëjtin agjent për mbrojtje dhe forensics.
Zgjidhja duhet të ruajë log-et e auditimit dhe hetimit deri në një vit.

d) Izolimi në nivel agjenti
Zgjidhja duhet të lejojë izolimin e stacioneve të shumta me agjent të instaluar në të njëjtën kohë dhe njëkohësisht.
Zgjidhja duhet të lejojë anulimin e izolimit të stacioneve të shumta me agjentin e instaluar në të njëjtën kohë dhe njëkohësisht.
Zgjidhja duhet të pranojë një listë të proceseve të lejuara dhe adresave IPv4/IPv6 me të cilat stacioni mund të komunikojë gjatë një periudhe kur izolimi është aktiv në stacionin e punës.

e) Përgjigje në kohë reale

Zgjidhja duhet të lejojë ekzekutimin e skripteve Python në stacionet e punës Ëindoës, Linux ose Mac OS me agjentin e instaluar, pa pasur nevojë që Python të instalohet në stacionin përkatës të punës.
Zgjidhja duhet të ofrojë mundësinë për të ekzekutuar skripte Python të personalizuara në stacione me një agjent të instaluar (duke përfshirë stacionet Ëindoës).
Zgjidhja duhet të ofrojë mundësinë për të ekzekutuar komandat CMD dhe PoëerShell të Ëindoës për stacionet e punës me Ëindoës të instaluar.
Zgjidhja duhet të shfaqë menaxhimin e detyrave (task-eve) në ekran të plotë me të gjitha proceset në ekzekutim dhe të lejojë ndalimin, vendosjen në pauzë ose shkarkimin si skedar të cilitdo nga proceset në memorie.
Zgjidhja duhet të lejojë shfletimin e skedarëve në cilindo prej agjentëve duke përdorur ndërfaqen e menaxhimit të centralizuar për të riemërtuar, zhvendosur dhe shkarkuar lehtësisht cilindo prej këtyre skedarëve nga stacionet e punës Ëindoës, Linux ose Mac OS.
Zgjidhja duhet të përfshijë skripte korrigjimi të gatshme për ekzekutim (ekzekutimin e komandave për Ëindoës, Linux dhe MacOS, vendosjen dhe fshirjen e vlerave të regjistrit për stacionet e punës në Ëindoës, ndalimin e proceseve për Ëindoës, Linux dhe MacOS).

f) Niveli i inteligjencës së kërcënimit

Zgjidhja duhet të ofrojë mundësinë e integrimit dhe furnizimit me rrjedha të dhënash që lidhen me treguesit e kompromentimit dhe informacionin e kërcënimit, siç është VirusTotal.
Zgjidhja duhet të ofrojë vlerësime dhe raporte mbi të gjitha mostrat e ekzekutuara automatikisht në pikat fundore.

g) Kontrolli i pajisjeve USB

Zgjidhja duhet të ofrojë mbrojtje kundër pajisjeve të infektuara (p.sh., USB-ve) kur lidhen me pajisje Ëindoës dhe Mac OS.

h) Kriptimi i diskut

Zgjidhja duhet të ofrojë mbështetje për enkriptimin e diskut për pajisjet Mac OS dhe Ëindoës.
Zgjidhja duhet të ofrojë mbështetje për menaxhimin e pajisjeve të enkriptimit të diskut nga e njëjta konsolë menaxhimi e unifikuar, pa pasur nevojë për një konsolë menaxhimi të jashtme.
Zgjidhja duhet të ofrojë mbështetje për aplikimin dhe zbatimin e profileve të enkriptimit dhe dekriptimit në stacionet e agjentëve për sistemet operative Ëindoës dhe Mac OS.

i) Raporte dhe panele specifike

Zgjidhja duhet të ofrojë mbështetje për panele të personalizueshme.
Zgjidhja duhet të mbështesë gjenerimin e raporteve të personalizueshme dhe të ketë aftësinë për t'u eksportuar.

Zgjidhja duhet të mbështesë gjenerimin e raporteve në formatin PDF.
Zgjidhja duhet të ofrojë modele raportesh të paracaktuara (të gatshme për përdorim) për të ofruar shpejt një pamje holistike të mjedisit dhe me mundësinë e ruajtjes dhe eksportimit.
Zgjidhja duhet të ofrojë mundësinë e krijimit të ëidget-eve duke përdorur gjuhën e skriptimit të zgjidhjes së ofruar.
Zgjidhja duhet të ofrojë mundësinë e krijimit të ëidget-eve të personalizuara që mund të përdoren nga analistët e sigurisë në panele të ndryshme.
Zgjidhja duhet të lejojë filtrimin e të dhënave në të gjitha ëidget-et në panelin e kontrollit, si dhe mundësinë e thellimit me ndryshime kontekstuale që do të përdoren në rastin e një hetimi specifik (panelet dinamike të kontrollit).

j) Mbështetje API
Zgjidhja duhet të ofrojë mbështetje për ekzekutimin e skripteve Python dhe fragmenteve të kodit Python (shablloneve) nëpërmjet API-ve.
Zgjidhja duhet të ofrojë mbështetje për kufizimin e aksesit në API bazuar në adresën IP.

k) Funksionalitete të nivelit enterprise
Zgjidhja duhet të ofrojë mbështetje për aktivizimin ose çaktivizimin e dukshmërisë së ikonës së agjentit në stacionet në konsolën e menaxhimit.
Zgjidhja duhet të lejojë aktivizimin ose çaktivizimin e njoftimeve për aksesin në terminal me agjentin e instaluar nga konsola e menaxhimit.
Zgjidhja duhet të lejojë personalizimin e njoftimeve/mesazheve në stacionet me një agjent të instaluar.
Zgjidhja duhet të jetë në gjendje të mbrojë plotësisht stacionin e punës pasi agjenti të jetë instaluar, pa pasur nevojë për një rinisje/ristartim.
Zgjidhja e ofruar duhet të jetë në gjendje të ruajë të dhënat dhe regjistrat për ngjarjet EDR në memorien e agjentit lokal edhe pas një rinisjeje për sistemet Ëindoës, Linux dhe Mac OS.
Zgjidhja e ofruar duhet të ketë një qendër të centralizuar veprimi ku një analist sigurie mund të fillojë të gjitha veprimet e disponueshme:
• marrja e skedarëve nga stacionet;
• marrja e regjistrave nga stacionet me agjentë;
• fillimi i një skanimi për programe keqdashëse në një ose më shumë stacione;
• izolimi i një ose më shumë stacioneve;
• ekzekutimi i skripteve;
• shtimi i hasheve për lista lejuese ose bllokuese;
• përmirësimi ose çinstalimi i agjentëve;
• mbështetje për kërkimin dhe shkatërrimin e skedarëve;
• aftësi triazhimi për forenzikë – shkarkimi i të dhënave nga agjenti;

• kërkimi i skedarëve sipas shtegut, madhësisë ose hash-it;
• kërkimi në regjistër;
• kërkimi në log-e;
• mbledhja e imazheve të memories nga agjentët Ëindoës.
Zgjidhja duhet të jetë në gjendje të gjurmojë dhe regjistrojë veprimet e ndërmarra nga analistët e sigurisë, si:
• izolimi i stacionit;
• lidhja e terminalit të drejtpërdrejtë;
• ndërprerja e procesit;
• çinstalimi i agjentit;
• përditësimi i agjentit;
• shtimi i hasheve në lista lejuese ose bllokuese.
Zgjidhja duhet të ofrojë mbështetje për skanimin e planifikuar të programeve keqdashëse.
Zgjidhja duhet të ofrojë mbështetje për kontrollin e aksesit të bazuar në role.
Zgjidhja duhet të ketë një konsolë qendrore të unifikuar për menaxhim dhe reagim ndaj incidenteve.
Zgjidhja duhet të ofrojë ruajtje të pakufizuar në cloud (me licencë shtesë).
Zgjidhja duhet të mbështesë agjentë offline përmes serverëve proxy.
Zgjidhja duhet të mbështesë përditësime peer-to-peer.
Zgjidhja duhet të mbështesë një ndërfaqe të vetme administrative dhe hetimore.
Zgjidhja duhet të ofrojë mbështetje për endpoint-e pa agjent.
Zgjidhja duhet të lejojë krijimin e etiketave dinamike.
Zgjidhja duhet të mbështesë instalimin në:
• Ëindoës 7 SP1, 10, 11;
• Ëindoës Server 2008 R2 SP1;
• Ëindoës Server 2012 & 2012 R2;
• Ëindoës Server 2016;
• Ëindoës Server 2019;
• Ëindoës Server 2022;
• Ëindoës Server 2025;
• macOS 12.x, 13.x, 14.x, 15.x, 16.x;
• Alma Linux, Amazon Linux, CentOS, Oracle Linux, Red Hat Enterprise Linux, Rocky Linux, SUSE Linux Enterprise Server, Ubuntu.
Zgjidhja duhet të ketë një portal online me dokumentacion dhe materiale ndihmëse.

Zgjidhja duhet të përmbushë standardet:
• SOC 2 Type II Plus;
• ISO 27001;

• ISO 27701;
• ISO 27017;
• ISO 27018;
• ISO 27032.

l) Licencimi

Licencimi dhe mbështetja teknike duhet të ofrohen për një periudhë prej 48 muajsh për të paktën 1200 agjentë.

Operatori ekonomik duhet të ofrojë një zgjidhje të plotë "turnkey", e cila është plotësisht e projektuar, ndërtuar, dorëzuar dhe implementuar, dhe është gati për përdorim të menjëhershëm.

3. ZgjidhjeSIEM

a) Kërkesat të përgjithshme

Autoriteti Kontraktor kërkon një zgjidhje që kundërvepron me kërcënimet kibernetike, duke mundësuar zbulimin e tyre me mbështetjen e mekanizmave machine learning, duke siguruar automatizimin dhe orkestrimin e përgjigjeve ndaj kërcënimeve kibernetike.

Zgjidhja duhet të mundësojë konfigurimin on-prem, në të cilin të gjitha funksionalitetet dhe përpunimi i të dhënave do të zhvillohen tërësisht brenda infrastrukturës së autoritetit kontraktor, me funksionalitet të plotë në një zonë të ndarë nga interneti.

Zgjidhja duhet të ketë licencë të përhershme për 1200 asete me mbështetje për një periudhë prej 48 muajsh. Licenca për zgjidhjen e ofruar nuk mund të vendosë kufizime në sasinë e të dhënave të ruajtura, numrin e ngjarjeve të transmetuara (EPS) ose numrin e përdoruesve të kyçur njëkohësisht.

Zgjidhja duhet të ofrohet me 48 muaj mbështetje nga prodhuesi, duke përfshirë ofrimin falas të përditësimeve të softuerit, përditësimeve të kontekstit (duke përfshirë analizuesit, rregullat e korrelacionit dhe manualet) dhe trajtimin e gabimeve.

Është detyrë e operatorit ekonomik të ofrojë një zgjidhje të plotë "turnkey", nga fillimi në fund, e cila është plotësisht e projektuar, ndërtuar, dorëzuar dhe implementuar, dhe është gati për përdorim të menjëhershëm.

Zgjidhja duhet të ketë një ndërfaqe grafike që lejon menaxhimin e përditësimeve të softuerit në internet dhe kontekstit, duke përfshirë rregullat e korrelacionit, manualet, analizuesit, integrimet, udhëzimet e inteligjencës artificiale, listat e referencave dhe profilet UEBA për përdoruesit dhe kompjuterët.

Zgjidhja duhet të ofrojë mundësinë e transmetimit të telemetrisë te prodhuesi në mënyrë që të monitorojë funksionimin e saktë, duke përfshirë, ndër të tjera, komponentët individualë, analizën e ngarkesës së procesorit dhe memories, si dhe regjistrimin e ngjarjeve në disqe.

Zgjidhja duhet të jetë në gjendje të dërgojë një alarm në një adresë të caktuar email-i në rast të dështimit të shërbimit, gabimeve të regjistrimit ose mbingarkesës së burimeve. Shërbimi duhet të funksionojë (24 orë në ditë, 7 ditë në javë).

Instalimi i përditësimeve të reja duhet të jetë plotësisht automatik, duke i ofruar operatorit të paktën dy opsione: "instalo", "instalo dhe aktivizo", të disponueshme si butona ose menu përzgjedhjeje.
Ndërfaqja e zgjidhjes duhet të ketë një mekanizëm të integruar automatik të versionimit që ruan të gjitha versionet historike të kontekstit dhe lejon restaurimin e versioneve të përdorura më parë.
Zgjidhja duhet të sigurojë kontrollin e aksesit në të dhëna dhe funksionalitetet e tyre bazuar në role të përcaktuara (Role-Based Access Control).
Zgjidhja duhet të ofrojë mundësinë për të paraqitur statusin aktual të sigurisë së autoritetit kontraktor, statistikat dhe rezultatet e performancës; pamja dhe paraqitja e komponentëve individualë duhet të mund të personalizohet sipas nevojave të administratorit dhe përdoruesit.
Zgjidhja duhet të mundësojë gjenerimin e raporteve sipas një orari të caktuar dhe dërgimin automatik të tyre në adresat e email-it të një grupi të përcaktuar marrësish.
Zgjidhja duhet të përfshijë një ndërfaqe grafike të thjeshtë për konfigurimin e njoftimeve, duke lejuar përcaktimin e kushteve dhe kanaleve të njoftimit, specifikimin e grupeve të synuara, konfigurimin e agregimit dhe periodicitetit për to.

b) Kërkesat të përgjithshme

Zgjidhja duhet të mundësojë mbledhjen e log-eve të gjeneruara nga sistemet e sigurisë, sistemet e rrjetit, sistemet operative dhe aplikacionet duke përdorur protokollet e mëposhtme: Syslog, TLS Syslog, NetFloë, Ëindoës Event Forëarding, IMAPS, POP3S, MAPI.
Zgjidhja duhet të ketë mekanizma të integruar që sigurojnë mundësinë e shkarkimit të ngjarjeve duke përdorur RestFull API, drajverin ODBC dhe agjentin e leximit të skedarëve.
Zgjidhja duhet të jetë e pajisur me mekanizma për normalizimin (analizimin) e ngjarjeve të fituara, duke mundësuar ndarjen e tyre në fusha individuale, në bazë të të cilave mund të kryhet përpunimi dhe kërkimi i mëtejshëm i tyre në sistem.
Procesi i normalizimit duhet të mbështesë llojet e mëposhtme të sintaksës: CEF, LEEF, URI, SYSLOG, XML, JSON, REGEX dhe një listë çiftesh çelës-vlerë, ku log-et që përmbajnë, për shembull, "user=X" duhet të krijojnë një fushë "user" me vlerën "X".
Procesi i normalizimit të log-eve duhet të përfshijë mekanizma globalë të pasurimit të të dhënave, të përcaktuar në mënyrë të pavarur nga konfigurimi i analizuesve individualë, të cilët shtojnë fusha dhe vlera të reja në log-et e normalizuar bazuar në kushte specifike.
Zgjidhja duhet të jetë e pajisur me një ndërfaqe grafike për krijimin e rregullave shtesë të normalizimit (analizues) për ngjarjet nga burime jo standarde (p.sh., aplikacione proprietare).
Të gjitha log-et duhet të ruhen në formë të kompresuar.
Zgjidhja duhet të jetë në gjendje të njohë automatikisht burimet e log-eve që ridrejtohen tek ajo.
Ajo duhet të njohë automatikisht llojin e log-ut dhe të zgjedhë analizuesin e duhur për të, në mënyrë që të mos kërkohet asnjë veprim nga ana e administratorit.

Zgjidhja duhet të mundësojë ridrejtimin e log-eve në repozitore të ndryshme në varësi të përmbajtjes së tyre, duke përdorur rregulla të bazuara në fushat e ngjarjeve për këtë qëllim.
Zgjidhja duhet të menaxhojë në mënyrë të pavarur ruajtjen e të dhënave dhe të mundësojë arkivimin automatik në repozitore të jashtme të të dhënave.
Zgjidhja duhet të ofrojë mekanizma sigurie për të dhënat e ruajtura në repozitore kundër modifikimit të paautorizuar dhe t'u ofrojë operatorëve mekanizma për të verifikuar integritetin e tyre.
Zgjidhja duhet të regjistrojë dhe ruajë log-et e marra në formë të papërpunuar dhe të standardizuar, si edhe të mundësojë që ato të kërkohen në të dyja format.
Ndërfaqja duhet të paraqesë rezultatet e kërkimit duke përdorur filtra bazuar në vlerat e fushave, shprehjet logjike komplekse, specifikimet e intervalit kohor dhe burimin e të dhënave.
Ndërfaqja e kërkimit duhet të lejojë që pyetjet të ruhen për ripërdorim në të ardhmen.
Ndërfaqja e kërkimit duhet të mbështesë kërkimin me tekst të plotë.
Ndërfaqja e kërkimit duhet të mbështesë kërkimin automatik në repozitore të shumta pavarësisht nga vendndodhja e tyre pa pasur nevojë t'i specifikoni ato.
Zgjidhja duhet të mbështesë punën me log-e në katër mënyra: një pamje tabelare me mundësinë e personalizimit të kolonave të shfaqura, një pamje që paraqet një listë parametrash dhe vlerave të tyre, një pamje të papërpunuar të log-eve dhe një hartë interaktive të rrjetit me funksione të integruara vizualizimi (broëser grafik), i cili:
• të mundësojë akses në kërkimet e log-eve direkt nga menyja e kontekstit të secilit host;
• të lejojë vizualizimin, ndër të tjera, të trafikut të rrjetit, aktivitetit të procesit, modifikimeve të regjistrit dhe komandave të ekzekutuara (shembull: vizualizimi i të gjitha lidhjeve dalëse nga hosti, duke marrë parasysh zonat e sigurisë dhe sistemet e sigurisë);
• të mundësojë gjurmimin e komunikimit, me anë të të cilit analiza e trafikut nga një host në tjetrin, e ndjekur nga trafiku hyrës dhe dalës për hostin e dytë dhe proceset që funksionojnë në të;
• të jetë e disponueshme një menu konteksti nga secili objekt harte në broëser-in grafik, duke i lejuar përdoruesit të kalojë në një pamje tabelare të log-eve, me një filtër të aplikuar bazuar në kërkimin grafik;
• nëpërmjet menusë kontekstuale në kolonat që identifikojnë hostin, duhet të jetë e mundur të kalohet në një broëser grafik në formën e një harte interaktive të rrjetit.
Standardizimi i log-eve duhet të përfshijë një mekanizëm gjeolokacioni që lejon që fushat të pasurohen me emrin ose kodin e vendit duke përdorur bazën e të dhënave të integruar në produkt.
Ndërfaqja për krijimin e analizuesve duhet të ketë një asistent të integruar të inteligjencës artificiale që do të mundësojë gjenerimin automatik të një analizuesi bazuar në një regjistër të papërpunuar.

Shikuesi i log-eve duhet të ketë një asistent të integruar të inteligjencës artificiale që do të mundësojë interpretimin e çdo regjistri të aktivizuar nga menyja e kontekstit.
Zgjidhja duhet të jetë e aftë të instalojë agjentë për sistemet Ëindoës i gjithë spektri i funksionalitetit të agjentëve duhet të jetë i arritshëm nga konsola qendrore e menaxhimit.
Agjenti duhet të kontrollohet plotësisht përmes manualeve, duke mundësuar, ndër të tjera, veprime izolimi dhe bllokimi bazuar në kushtet që lidhen me ngjarjet e analizuara.
Agjenti duhet të mundësojë bllokimin në nivelin kernel.
Agjenti duhet të mbështesë modalitetin e komunikimit one-ëay, në të cilin nuk hap asnjë portë, por vetëm inicion lidhje me konsolën e menaxhimit.
Agjenti duhet të dërgojë gamën e plotë të të dhënave të telemetrisë në konsolën qendrore, duke përfshirë lidhjet e rrjetit, modifikimet e log-eve, nisjet e proceseve dhe komandave, aksesin në skedarë, për qëllime korrelacioni të të dhënave.
Agjenti duhet të mundësojë identifikimin e dobësive në hostin në të cilin do të instalohet.
Zgjidhja duhet të mundësojë korrelacionin e ngjarjeve që burojnë nga sisteme të ndryshme burimore bazuar në çdo fushë dhe variabël regjistri ose çdo të dhënë tjetër.
Zgjidhja duhet të mundësojë lidhjen e ngjarjeve të sigurisë me teknika specifike nga baza e njohurive MITRE ATT&CK dhe të ofrojë mekanizma për filtrimin e ngjarjeve sipas këtyre teknikave.
Zgjidhja duhet të ketë një ndërfaqe grafike për krijimin e rregullave të personalizuara të korrelacionit përgjegjëse për zbulimin e ngjarjeve specifike që ndodhin në sistem.
Rregullat e korrelacionit duhet të:
• lejojnë filtrimin duke përdorur operatorin LIKE dhe përputhjen e modeleve duke përdorur shprehje të rregullta (REGEX);
• marrin në konsideratë parametrat e objekteve në Active Directory, duke lejuar referencën ndaj një objekti të tillë në korrelacion bazuar në ngjarje që nuk përmbajnë informacion rreth tij (p.sh., trafiku i rrjetit që i referohet një llogarie përdoruesi që nuk kërkon fjalëkalim);
• marrin në konsideratë edhe parametrat që nuk përfshihen drejtpërdrejt në ngjarje (p.sh., një rregull që zbulon trafikun nga interneti në një server që është klasifikuar në CMDB si një burim që ofron shërbime ekskluzivisht në rrjetin lokal);
• mbështesin një modalitet dinamik që optimizon performancën përmes korrelacionit selektiv të rregullave (p.sh., nëse regjistri përmban informacion që tregon një ngjarje që lidhet me trafikun e rrjetit, atëherë aktivizohen vetëm rregullat përkatëse);
• kenë një mekanizëm për caktimin statik të tyre te burimet e duhura të log-eve në mënyrë që rregullat e dedikuara për sistemet Ëindoës të mos aktivizohen për burimet që dërgojnë loge nga sistemet Linux

Zgjidhja duhet të jetë plotësisht e konfigurueshme, duke i lejuar operatorit të zgjedhë mënyrën e fillimit të korrelacionit (statik ose dinamik) dhe duhet të përcaktojë kushtet duke përdorur një redaktues grafik për të gjitha paketat e rregullave (politikat).
Zgjidhja duhet të ketë një motor të integruar dhe plotësisht të modifikueshëm për vlerësimin e bazuar në rrezik (risk-score). Ky rrezik duhet të llogaritet veçmas për adresën burimore, adresën e destinacionit dhe llogarinë e përdoruesit të identifikuar të domenit.
Ndërfaqja për krijimin e rregullave të korrelacionit duhet të lejojë gjenerimin e emrave dhe përshkrimeve dinamike të rregullave. p.sh., një rregull i quajtur "Trafiku lokal i bllokuar" duhet t'i lejojë operatorit të konfigurojë se si shfaqet ngjarja nën emrin "Trafiku lokal i bllokuar nga 192.168.1.x në 10.1.1.x" dhe me përshkrimin "Trafiku lokal i bllokuar nga adresa IP 192.168.1.x në Zonën LAN në adresën IP 10.1.1.x në Zonën ËAN".
Zgjidhja duhet të ofrojë një ndërfaqe të dedikuar për akordimin e rregullave të korrelacionit, duke mundësuar analizën e tyre në lidhje me numrin e ngjarjeve që ato gjenerojnë, numrin e hosteve në të cilët ato shkaktohen dhe duke paraqitur në një grafik statistikat e tyre për muajt e fundit.
Ndërfaqja e akordimit të rregullave duhet të mundësojë përjashtimin e hosteve individuale, grupeve të hosteve, llogarive të përdoruesve, grupeve të domeneve dhe grupeve të përdoruesve të domeneve, si në rregullat e korrelacionit ashtu edhe për përpunim të mëtejshëm në modulin SOAR.
Ndërfaqja për krijimin e rregullave të korrelacionit duhet të përfshijë një asistent të IA-së me një opsion plotësisht të konfigurueshëm për gjenerimin automatik të rregullave bazuar në të dhënat hyrëse, p.sh., bazuar në një kategori të specifikuar MITRE ATT&CK.
Shikuesi i ngjarjeve të korreluara duhet të përfshijë një asistent të IA-së me opsionin për të interpretuar çdo ngjarje, të nisur nga menyja e kontekstit.
Metoda e interpretimit duhet të jetë plotësisht e konfigurueshme dhe të lejojë që menyja e kontekstit të zgjerohet me lloje të reja interpretimi.
Zgjidhja duhet të analizojë sjelljen e përdoruesit dhe kompjuterit duke përdorur machine learning për të krijuar dhe përditësuar automatikisht modele të sjelljes tipike për zbulimin e devijimeve nga norma.
Modelet e sjelljes duhet të krijohen automatikisht bazuar në analizën historike të të dhënave për grupet e përdoruesve, burimet (profilet) dhe të lejojnë rillogaritjen e tyre sipas kërkesës, p.sh., shtimit të një rregulli të ri, shtim automatikisht, në mënyrë ciklike, apo një herë në muaj.
Modelet e sjelljes duhet të jenë të konfigurueshme për të çaktivizuar profilet dhe rregullat specifike learning.
Zgjidhja duhet të ketë një grup prej të paktën 20 rregullash të paracaktuara dhe të konfigurueshme për caktimin automatik të përdoruesve dhe burimeve në profilet e duhura. Këto rregulla duhet të sigurojnë të paktën ndarjen e procesit learning për llogaritë e privilegjuara, jo të privilegjuara, të shërbimit, si dhe ndarjen e pajisjeve nga serverat dhe stacionet e punës.

Algoritmet Machine Learning duhet të mundësojnë analizën automatike dhe learning nga të dhënat statistikore, siç janë numri dhe llojet e ngjarjeve të gjeneruara dhe vlerësimet e rrezikut (score).

Algoritmet Machine Learning duhet të përdorin nyje izolimi për të zbuluar aktivitetin e pazakontë dhe anormal.

Mekanizmi i Machine Learning duhet të mundësojë identifikimin e vlerave në ngjarje që do të përdoren në procesin e learning dhe duhet t'i lidhë ato me kushtin e duhur kualifikues.

Algoritmi UEBA duhet të lejojë konfigurimin e mekanizmave për refuzimin e vlerave të jashtëzakonshme që mund të ndikojnë negativisht në rezultatet e procesit learning, si dhe për përjashtimin e profileve specifike të përdoruesve dhe rregullave të zbulimit nga analiza.

Zgjidhja duhet të ofrojë një ndërfaqe grafike të dedikuar që lejon verifikimin e përqindjes së progresit të procesit të learning për secilin profil aktiv, së bashku me informacionin rreth datës së përfundimit dhe numrit të algoritmeve të përdorura.

Ndërfaqja duhet të lejojë qasje në profil për të marrë të dhëna të detajuara rreth secilit algoritëm, siç janë emri, lloji i algoritmit, numri minimal i mostrave, numri i ditëve të nevojshme për të përfunduar learning si edhe vlera e devijimit.

Anomalitë e zbuluara duhet të gjenerojnë ngjarje të reja dhe t'i regjistrojnë ato në depozitën e log-eve.

Shikuesi grafik i ngjarjeve duhet të jetë plotësisht interaktiv, duke lejuar që informacioni i detajuar rreth secilit host të shfaqet nëpërmjet një menuje konteksti të lidhur me atë host.

Minimalisht të dhënat duhet të jenë të disponueshme mbi: informacionin e përpunuar, shërbimet kritike përkatëse, vendndodhjen e përdoruesve që përdorin hostin, vendndodhjen e serverëve që përdor, masat lokale të sigurisë në vend, numrin e dobësive, incidenteve të zbuluara, numrin e ngjarjeve të lidhura dhe llogaritë e përdoruesve të lidhura me të.

Broëseri duhet të lejojë ndërrimin e modalitetit të shfaqjes për një ngjarje të vetme, duke mundësuar që pamja që paraqet fushat e ngjarjes dhe vlerat e tyre të ndryshohet në një përshkrim ngjarjeje të gjeneruar automatikisht në bazë të fushave që ndodhin në një ngjarje të caktuar.

Përshkrimi i gjeneruar duhet të jetë plotësisht i konfigurueshëm, me mundësinë e përcaktimit të kushteve që ndikojnë në ndryshimin në formën e prezantimit të tij.

Lista e ngjarjeve të shoqëruara me një llogari përdoruesi duhet të lejojë shikimin e kompjuterëve në të cilët është regjistruar aktiviteti, si edhe llogaritë e përdoruesve të shoqëruara me një kompjuter të caktuar.

Zgjidhja duhet të ofrojë një paraqitje me hartë për të gjitha ngjarjet që lidhen me hostet dhe llogaritë e përdoruesve brenda një periudhe të caktuar kohore në matricën MITRE ATT&CK, duke mundësuar vlerësimin e mbulimit të saj.

Zgjidhja duhet të ketë mundësinë e dokumentimit të rrjetit, sistemeve dhe shërbimeve, duke mundësuar mbledhjen dhe redaktimin e të dhënave përkatëse për vlerësimin e ngjarjeve të sigurisë të gjeneruara.
Zgjidhja duhet të lejojë përcaktimin e parametrave të personalizuar për të gjitha llojet e objekteve të ruajtura në dokumentacionin elektronik të rrjetit.
Zgjidhja duhet të jetë e aftë të vizualizojë dokumentacionin në formën e një harte interaktive të rrjetit, që mbulon zonat e sigurisë, pajisjet e rrjetit dhe pikat fundore, duke përfshirë serverat dhe kompjuterët.
Dokumentacioni elektronik duhet të mundësojë menaxhimin e një katalogu shërbimesh, duke përfshirë parametrat e mëposhtëm për secilin shërbim: vlefshmëria, lloji, informacioni i përpunuar, varësitë dhe ndikimi në shërbime të tjera, cikli, aplikacionet e lidhura, portat e rrjetit, shërbimet, referencat (URL-të) dhe lidhjet me burimet e IT-së.
Dokumentacioni elektronik duhet të gjenerohet automatikisht bazuar në rregullat e ofruara nga prodhuesi (të paktën 50), të cilat, kur aktivizohen, përditësojnë automatikisht dokumentacionin pa ndërhyrjen e operatorit.
Zgjidhja duhet të mundësojë vlerësimin automatik të ndikimit të incidenteve të sigurisë së IT-së në operacionet e rrjetit në kontekstin e kërcënimeve të IT-së, midis çdo burimi IT, bazuar në dokumentacionin elektronik, matricën MITRE ATT&CK dhe dobësitë e zbuluara.
Vlerësimi i ndikimit të incidenteve të sigurisë së IT-së në operacionet e organizatës duhet të jetë i parakonfiguruar bazuar në rregulla të paracaktuara.
Zgjidhja duhet të ketë një bazë të dhënash të integruar që mundëson mbledhjen, ruajtjen dhe caktimin e treguesve të kompromentimit (IoC) për incidentet.
Zgjidhja duhet të mundësojë sinkronizimin e treguesve të kompromentimit (IoC) me platformat e disponueshme publikisht.
Të dhënat e mbledhura në bazën e të dhënave të treguesve të kompromisit (IoC) duhet të jenë të përdorshme në rregullat dhe playbooks.
Zgjidhja duhet të sigurojë që listat e referencave të mund të sinkronizohen me listat e disponueshme publikisht.
Zgjidhja duhet të ketë një asistent të integruar të AI që mbështet operatorin në trajtimin e ngjarjeve dhe dobësive.
Asistenti i AI duhet të mundësojë integrimin me modelet gjuhësore lokale dhe të disponueshme publikisht (LLM).
Asistenti i AI duhet të veprojë në kontekst, me aftësinë për të caktuar kërkesa të përshtatshme për secilin kontekst.
Asistenti i AI duhet të ofrojë mënyra të dedikuara operimi, duke përfshirë të paktën trajtimin e incidenteve dhe dobësive, analizën e ngjarjeve të regjistrit, si edhe integrimin dhe krijimin e analizuesit.
Asistenti i AI duhet të lejojë redaktimin e kërkesave dhe krijimin e kërkesave të reja.

Kërkesat duhet të jenë të disponueshme për shkarkim nga faqja e internetit e prodhuesit.
Asistenti i AI duhet të jetë i disponueshëm vazhdimisht dhe dinamikisht duke ndryshuar kontekstin në varësi të funksionaliteteve të përdorura.
Zgjidhja duhet të ketë një logjikë për caktimin automatik të ngjarjeve të kualifikuara për trajtim, së bashku me një njoftim për operatorin e caktuar për t'i trajtuar ato (p.sh., email, mesazh teksti - SMS).
Kualifikimi i ngjarjeve duhet të bazohet në një sërë rregullash që caktojnë automatikisht një ngjarje për trajtim ose ta refuzojnë atë.
Kualifikimi i operatorit për të trajtuar ngjarjen duhet të bazohet në kritere të përcaktuara në nivelin e ekipit të shërbimit dhe të përfshijë, ndër të tjera:
• metodën e caktimit të një ngjarjeje, të paktën: personit më pak të ngarkuar ose nëpërmjet menaxherit të ekipit;
• llojin e ngjarjes, p.sh.: cenueshmëri, rregull korrelacioni, raport;
• llojin e burimit, duke përfshirë: bazën e të dhënave, stacionin e punës, kontrolluesin e domenit, printerin, serverin, pajisjen;
• shërbimet e lidhura me burimin;
• informacionin e përpunuar;
• përkatësinë e burimit në një njësi organizative;
• softuerin e përcaktuar.
Ngjarjet e suportuara duhet të kenë një grup prej 30 skenarësh trajtimi të paracaktuar (udhëzues) dhe të lejojnë krijimin e skenarëve të trajtimit të personalizuar dhe redaktimin e tyre nga ndërfaqja grafike.
Zgjidhja duhet të marrë informacion nga sisteme të tjera dhe ta përdorë atë për të marrë vendime në lidhje me rrjedhën e mëtejshme të manualit.
Zgjidhja duhet të jetë e integruar me një vulnerability scanner dhe të sigurojë që këto dobësi të trajtohen brenda manualeve.
Zgjidhja duhet të jetë në gjendje t'u përgjigjet kërcënimeve si përmes integrimit me sisteme të tjera sigurie ashtu edhe direkt në stacionin e punës ose serverin e sulmuar, në nivel të agjentit të mbështetur.
Zgjidhja duhet të mundësojë kërkimin e regjistrave historikë, ngjarjeve të ndërlidhura, statistikave UEBA, informacionit të mbulimit të matricës MITRE ATT&CK dhe të dhënave nga baza e të dhënave e Inteligjencës së Kërcënimeve.
Zgjidhja duhet të mundësojë përcaktimin e parametrave SLA për të gjitha statuset e shërbimit, dhe t'i verifikojë ato kundrejt vlerave të përcaktuara. Rezultatet e matjeve të kohës së SLA duhet të përditësohen vazhdimisht dhe të paraqiten në një listë të ngjarjeve të kualifikuara për shërbim.
Manualet duhet të aktivizohen si në përgjigje të ngjarjeve specifike ashtu edhe në mungesë të një përgjigjeje brenda një afati kohor të caktuar për të mundësuar skenarët e përshkallëzimit.

Manualet duhet të mundësojnë kontroll të plotë duke përdorur AI, si edhe duke përfshirë kryerjen automatike të hapave pasues bazuar në përgjigjet e marra nga modeli LLM.
Manualet duhet të kenë një menaxher fjalëkalimesh të integruar për të ruajtur në mënyrë të sigurt të dhënat e nevojshme për integrimin, siç janë emrat e përdoruesit, fjalëkalimet dhe çelësat API.

c) Arkitektura
Zgjidhja duhet të ofrojë një arkitekturë fleksibile dhe të shkallëzueshme pa nevojën e blerjes së licencave shtesë për zgjerim.
Zgjidhja duhet të mundësojë ndarjen e shtresave funksionale të referuara si analizimi, ruajtja e logeve, korrelacioni i ngjarjeve, ruajtja e ngjarjeve dhe mekanizmat e të mësuarit automatik.
Zgjidhja duhet të përshkallëzohet pa limit duke shtuar makina virtuale shtesë ose makina fizike (kolektor), duke mundësuar kështu rritjen e performancës dhe besueshmërisë.
Kolektorët e ruajtjes së të dhënave nuk duhet të përdorin baza të dhënash klasike relacionale; vetëm bazat e të dhënave NoSQL ose zgjidhjet e rekomanduara nga prodhuesi lejohen për këtë qëllim.
Arkitektura e zgjidhjes duhet të mbështesë një konfigurim që ofron besueshmëri përmes përdorimit të një serie kolektorësh zëvendësues, të cilët aktivizohen në rast të një dështimi të njërit prej tyre.
Të gjithë kolektorët, si ai primar ashtu edhe ai zëvendësues, duhet të menaxhohen në mënyrë qendrore nga e njëjta konsolë.
Zgjidhja duhet të ketë një mekanizëm që mundëson bashkëpunimin me sisteme të jashtme si Load Balancer, i cili të verifikojë funksionimin e saktë të të gjithë kolektorëve.
Për të siguruar vazhdimësinë, kolektori primar duhet të jetë në gjendje të sinkronizojë ngjarjet me kolektorin rezervë. Në rast të një dështimi të kolektorit primar, ngjarjet e gjeneruara në atë kolektor duhet të përfshihen në korrelacionin në kolektorin rezervë.
Të gjitha llojet e kolektorëve, përfshirë agjentët XDR, duhet të jenë të konfigurueshëm dhe të specifikojnë kolektorët rezervë tek të cilët do të drejtohen të dhënat në rast të një dështimi të kolektorit primar.

4. Instalim dhe implementim për zgjidhjet XDR dhe SIEM
Autoriteti Kontraktor kërkon shërbime të sigurisë kibernetike për instalimin, konfigurimin, integrimin dhe operacionalizimin e zgjidhjeve Extended Detection and Response (XDR) dhe një zgjidhjeje Security Information and Event Management (SIEM).
Objektivi është përmirësimi i operacioneve të sigurisë, reduktimi i kohës së zbulimit dhe reagimit ndaj incidenteve, automatizimi i inteligjencës së kërcënimeve dhe përmbushja e standardeve.

a) Shërbimet e Implementimit të XDR

- *Deploy dhe konfigurim i zgjidhjes*
- *Integrim me endpoint-e, serverë, pajisje rrjeti, fireëall, ëorkload-e*
- *Konfigurim i feed-eve të inteligjencës së kërcënimeve*
- *Rregullim i politikave dhe optimizim i alarmeve*
- *Krijimi i ëorkfloë-ve të automatizuara të reagimit*
- *Konfigurimi i aksesit dhe roleve*
- *Fortifikim i platformës*
- *Transferim njohurish*

b) Shërbimet e Implementimit të SIEM

- *Instalimi i platformës SIEM (on-premise)*
- *Onboarding i burimeve të log-eve (serverë, aplikacione, fireëall, identitet, cloud, etj.)*
- *Parsing, normalizim dhe krijim rregullash korrelacioni*
- *Zhvillim i use-case-ve sipas riskut të autoritetit*
- *Krijim dashboard-esh dhe raportesh*
- *UEBA dhe SOAR*
- *Raportim i pajtueshmërisë*
- *Optimizim i performancës*

c) Kërkesa Teknike

Kërkesat për XDR

- *Zbulim bazuar në sjellje dhe signature*
- *Orkestrimi i automatizuar i reagimit*
- *Integrim me EDR, sisteme identiteti*
- *Mbështetje API*
- *Korrelacion me inteligjencë kërcënimesh*
- *Monitorim dhe alarmim i vazhdueshëm*

Kërkesat për SIEM

- *Ingestion dhe korrelacion në kohë reale*
- *Arkitekturë e shkallëzueshme*
- *Kontroll aksesi (RBAC)*
- *Integrim me sistemet ekzistuese të autentikimit*
- *Analitika të avancuara*
- *Gjuhë fleksibël kërkimi*
- *Mbështetje për ëorkfloë të incidenteve*

5. Shërbim mirëmbajtje Fireëall XDR dhe SIEM

Operatori ekonomik duhet të ofrojë shërbime të mirëmbajtjes sipas niveleve të shërbimit dhe metodikës të përshkruar më poshtë:

1.Suport proaktiv.

Operatori ekonomik duhet të ndërmarrë, në mënyrë periodike një herë në muaj, shërbime dhe suport proaktiv, të cilët duhet të mundësojnë detektimin në kohë të problematikave dhe duhet të mundësojnë ndërmarrjen në kohë të hapave rekuperues, për të mos pasur ndërprerje të shërbimit. Të gjitha shërbimet e suportit proaktiv duhet të kryhen pranë ambienteve të POSTA SHQIPTARE sh. a., përveç rasteve kur POSTA SHQIPTARE përcakton një vendndodhje të re për kryerjen e këtyre shërbimeve.

2. Shërbime riparimi në vendndodhje (mjediset e POSTA SHQIPTARE).

Operatori ekonomik duhet të jetë në dispozicion gjatë intervalit kohor, nga e Hëna në të Dielë, 24/7, për të ofruar shërbime të riparimit në përgjigje të "Alarmeve Madhore" të raportuara nga personeli i autorizuar i POSTA SHQIPTARE (“Emergency On-Call Hours").

Për këtë qëllim, me termin Alarm Madhor do të kuptohet parashtrimi i kërkesës për shërbime riparimi të ndërmarra në rast të keqfunksionimit të sistemeve të mbuluara që i pengon ato të operojnë në përputhje me specifikimet dhe shkaktojnë ndërprerje të menjëhershme e të konsiderueshme të sistemit dhe që nuk mund të shmangen me anë të ndërhyrjeve dhe riparimeve minore të kryera nga stafi teknik i POSTA SHQIPTARE, të rekomanduara nga Kompania. Problemet që nuk i përkasin "Alarmeve Madhore" duhet të adresohen nën shërbime të suportit proaktiv.

3. Njoftimi dhe njohja e alarmeve madhore.

POSTA SHQIPTARE do të njoftojë me telefon, postë elektronike ose duke sinjalizuar nëpërmjet një ndërfaqeje ëeb të vënë në dispozicion dhe do të presë të kontaktohet nga ne me telefon, gjatë "Emergency On-Call Hours". Operatori ekonomik duhet të kontaktojë POSTA SHQIPTARE sh.a. dhe të konfirmojë marrjen e Alarmit Madhor, brenda 30 minutave nga marrja e njoftimit nga personeli i autorizuar i POSTA SHQIPTARE. Në momentin e njohjes së thirrjes, POSTA SHQIPTARE do të vendosë në dispozicion informacione të paracaktuara në procedurat e troubleshooting dhe do të asistojë OE gjatë diagnostikimit të problemit të raportuar. POSTA SHQIPTARE do të bashkëpunojë me kërkesën e OE për të ndihmuar në përcaktimin e shkakut të problemit të raportuar dhe në përcaktimin e nevojës për vizitë në vendndodhje për të kryer shërbimet e riparimit.

4. Përgjigja ndaj alarmeve madhore.

Nëse operatori ekonomik nuk mund të përcaktojë nëpërmjet informacionit të mbledhur nga procedurat e troubleshooting shkakun e alarmit madhor, atëherë duhet të dërgojë një teknik

shërbimi pranë POSTA SHQIPTARE brenda intervalit kohor prej dy (2) orësh nga momenti i marrjes së njoftimit për Alarm Madhor. Me të mbërritur, tekniku do të mbështetet me asistencë nga POSTA SHQIPTARE dhe do t'i jepet liri veprimi në mjediset dhe sistemet e mbuluara, për të filluar menjëherë procedurat e diagnostikimit dhe riparimit.

5. Veprimtaritë e diagnostikimit dhe riparimit.
Me të mbërritur në vendndodhje, tekniku i shërbimit duhet të fillojë procedurat e diagnostikimit dhe riparimit. Këto veprimtari duhet të vazhdojnë derisa:

e) Alarmi madhor të jetë korrektuar ose të jetë "zgjidhur në mënyrë të tërthortë";
f) tekniku të jetë zëvendësuar nga një person tjetër;
g) të përcaktohet se problemi i raportuar nuk është shkaktuar nga ndonjë keqfunksionim i sistemeve të mbuluara;
h) të arrihet në konkluzion që diagnostikimi ose korrektimi i mëtejshëm mund të shtyhet deri në mbërritjen e pjesëve të këmbimit.

Teknikët e shërbimit të operatorit ekonomik duhet të jenë të trajnuar, të certifikuar dhe të autorizuar për të ndërvepruar në mënyrë të drejtpërdrejtë me prodhuesin. Në rast se do të jetë i nevojshëm zëvendësimi i pjesëve të këmbimit, atëherë OE duhet të kryejë të gjitha procedurat respektive me prodhuesin për lokalizimin e pjesës, heqjen, eksportin, transportin, importin, vendosjen dhe rikonfigurimet përkatëse. Kostot e pjesëve të dëmtuara dhe kostot e shërbimit do të merren përsipër nga operatori ekonomik për të gjithë periudhën e kontratës.

6. Shërbimet e tjera.
Operatori ekonomik duhet të krijojë/diskutojë me POSTA SHQIPTARE sh.a. një axhendë periodike kontrollesh si më poshtë:

Javore

vi. Kontrolle të log-eve të pajisjeve të rrjetit;
vii. Mirëmbajtje proaktive.

Mujore

viii. Testim / kontroll i kompletuar i pjesëve më kritike të infrastrukturës HË të POSTA SHQIPTARE sh. a.;
ix. Kontroll i detajuar i të gjithë log-eve hardëare, analizë e tyre;
x. Rekomandime për upgrade të mundshme hardëare.

III.3.2. Në procesverbalin "*PËR ARGUMENTIMIN E KRITEREVE TË VEÇANTA PËR KUALIFIKIM*", të publikuar në SPE autoriteti kontraktor ka argumentuar vendosjen especifikimeve teknike, si më poshtë vijon:

“*II. Argumentimi i specifikimeve teknike*

*Specifikimet teknike të procedurës për **“Blerje suport për SIEM + licenca për EDR/XDR (1200 përdorues) dhe licenca Fireëall Professional për 4 (katër) vite”**, janë hartuar mbi bazën e Urdhrit të brendshëm nr. 24, datë 12.03.2026, të Administratorit të “Posta Shqiptare” sh.a., në përputhje me nenin 4, pika 38/b dhe nenin 36 të ligjit nr. 162/2020 “Për Prokurimin Publik”, si dhe nenin 41, pika 1 të VKM nr. 285, datë 19.05.2021 “Për miratimin e rregullave të prokurimit publik” (i ndryshuar).*

Specifikimet teknike të shërbimit objekt prokurimi janë hartuar duke u diktuar nga nevoja për forcimin, mbrojtjen dhe monitorimin e infrastrukturës së teknologjisë së informacionit të Autoritetit Kontraktor, nëpërmjet implementimit dhe përdorimit të zgjidhjeve të avancuara të sigurisë kibernetike, përfshirë sistemin SIEM, licencat EDR/XDR për 1200 përdorues dhe licencat Fireëall Professional, të cilat garantojnë mbrojtje në kohë reale, analizë të ngjarjeve të sigurisë dhe parandalim të kërcënimeve kibernetike.

Këto specifikime teknike shprehin tërësinë e elementeve funksionale, teknike dhe operacionale të domosdoshme për sigurimin e vazhdimësisë së shërbimit, nivelit të kërkuar të sigurisë (SLA), si dhe përputhshmërinë me standardet bashkëkohore të sigurisë së informacionit dhe kërkesat operacionale të Autoritetit Kontraktor.”.

III.3.3. Lidhur me pretendimet e mësipërme të operatorit ekonomik ankimues “*PC STORE*” ShPK autoriteti kontraktor me shkresën nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, e ka shqyrtuar këtë pretendim të ankimuesit, duke argumentuar si më poshtë vijon:

“Në lidhje me pretendimet e ngritura përsa i përket shtojcës 6 Specifikimet teknike ju sqarojmë se;

Ndryshimi i kërkesës nga një listë e qartë dhe specifike e teknikave të mbrojtjes drejt një formulimi të përgjithshem "behavioral detection dhe exploit prevention" ul nivelin e qartësisë teknike dhe të matshmërisë së kërkesës.

Në vërsionin ekzistues, kërkesat përcaktojnë në mënyrë të drejtpërdrejtë mekanizmat dhe teknikat konkrete që zgjidhja duhet të mbështesë për Linux dhe macOS, si p.sh. Brute Force Protection, Java Deserialization Protection, Reverse Shell Protection, ROP Mitigation, Shellcode Protection, SO/Dylib Hijacking Protection, Gatekeeper Enhancement dhe Anti- Ransomeare. Kjo qasje siguron:

- *Qartësi teknike mbi funksionalitetet minimale të kërkuara;*

- *Mundësi objektive për verifikim dhe testim gjatë fazës së vlerësimit;*
- *Krahasim të drejtë ndërmjet ofertuesve;*
- *Eliminim të interpretimeve subjektive nga operatorët ekonomikë;*

Garanci që zgjidhja mbulon teknika specifike dhe të njohura sulmi për secilin sistem operativ.

Ndërsa formulimi i ri përdor tërma të përgjithshem si "mekanizma të avancuar", "behavioral detection" dhe "aftësi për të identifikuar dhe parandaluar teknika të njohura sulmi", pa specifikuar kontrollet konkrete që duhet të ekzistojnë. Kjo krijon paqartësi në interpretim dhe mund të lejojeë paraqitjen e zgjidhjeve që dekarojnë mbështetje të përgjithshme, por që në praktikë nuk ofrojnë mbrojtje të dedikuar për teknikat specifike të kerkuara.
Gjithashtu, lista aktuale e teknikave nuk është kufizuese, por përfaqëson një minimum të domosdoshëm sigurie për mbrojtjen e endpoint-eve Linux dhe macOS ndaj teknikave modeme të exploit-eve dhe privilege escalation. Heqja e tyre mund të sjellë ulje teë standardit të sigurisë dhe vështirësi në validimin e përputhshmërisë së ofertës me kërkesat teknike.

Për këtë arsye, kërkesa ekzistuese duhet të ruhet në formën aktuale, pa hequr listën konkrete të mekanizmave dhe teknikave të mbrojtjes të kërkuara.
Ndryshimi i propozuar nuk mund të miratohet, pasi formulimi ekzistues është më i qartë, me i drejtpërdrejtë dhe teknikisht me i matshëm në kuadër të keërkesave të tenderit/specifikimeve.

Arsyetimi:
Formulimi aktual përcakton qartë dhe në mënyrë konkrete funksionalitetet minimale që duhet të mbeshteten nga sistemi, konkretisht:

- *filtrimin me operatorin LIKE;*
- *përputhjen e modeleve me REGEX.*

Këto janë kërkesa të verifikueshme dhe të testueshme gjatë fazës së vlerësimit teknik.
Formulimi i ri përdor terma më të përgjithshëm dhe interpretues si:

- *"filtrim dhe përputhje të avancuar";*
- *"operatore eildcard";*
- *"ndërtimin e rregullave të avancuara".*

Këto shprehje nuk përcaktojnë qartë kufijtë minimale teknike dhe krijojnë hapësirë për interpretime të ndryshme nga operatorët ekonomike.

Përdorimi i termit "p.sh. LIKE" e bën mbështetjen e operatorit LIKE jo detyrim të drejtpërdrejtë, por vetëm shëmbull ilustrues. Kjo mund të sjellë paqartësi gjatë implementimit dhe verifikimit të përputhshmërisë seë ofertave.

Kërkesa ekzistuese është neutrale dhe standarde nga pikëpamja teknike, ndërsa formulimi i ri zgjeron në mënyre të panevojshme përshkrimin funksional pa shtuar vlerë reale teknike apo operacionale.
Ruajtja e formulimit aktual ndihmon në:

- *shmangien e interpretimeve subjektive;*
- *garantimin e trajtimit të barabartë të operatorëve ekonomikë;*
- *lehtësimin e procesit të verifikimit të përmbushjes se kërkesave teknike.*

Për rrjedhojë, të mos ndryshohet formulimi aktual i kërkesës dhe të mbetet teksti ekzistues i Shtojcës 6.

Ndryshimi i kërkesës së përcaktuar ne Shtojcën 6 nuk mundësohet, pasi formulimi ekzistues garanton qartësi teknike, standardizim dhe përcaktim të saktë të funksionaliteteve minimale që duhet të ofrojë zgjidhja. Heqja e protokolleve specifike si IMAPS, POP3S dhe MAPI dhe zëvendësimi me termin e përgjithshem "etj." krijon pagartësi në interpretim dhe lë hapësirë për trajtime të ndryshme nga operatorët ekonomikë gjatë ofertimit.
Kërkesa aktuale përcakton në mënyrë eksplicite protokollet që duhet të suportohen, duke siguruar që zgiidhja të jetë e aftë të mbledhë log-e edhe nga sistemet e komunikimit dhe shërbimeve email, të cilat janë komponente të rëndësishëm për monitorimin e sigurisë dhe analizën e incidenteve. Nëse këto protokolle hiqen nga kërkesa, ekziston rreziku që operatorë të ndryshëm të ofrojnë zgjidhje me nivele të ndryshme funksionaliteti, duke vështirësuar krahasimin objektiv të ofertave dhe duke krijuar mundësi për implementim të një zgjidhjeje që nuk mbulon të gjitha nevojat operative të autoritetit kontraktor.

Gjithashtu, perdorimi i termit "etj." nuk përbën specifikim teknik të matshëm dhe mund të sjellë paqartësi gjatë fazës së implementimit dhe pranimit të sistemit, pasi nuk përcaktohen qartë standardet minimale të kërkuara. Në procedurat e prokurimit publik rekomandohet që kërkesat teknike të jenë sa më të detajuara dhe të verifikueshme, me qëllim garantimin e transparencës, konkurrencës së ndershme dhe shmangien e interpretimeve subjektive.
<u>Për këto arsye, formulimi ekzistues duhet të mbetet i pandryshuar.</u>

Ndryshimi i propozuar nuk mund të pranohet, pasi heqja e mbështetjes për formatin LEEF nga kërkesat e normalizimit kufizon kompatibilitetin dhe ndërveprueshmërinë e sistemit me burime të ndryshme log-esh dhe platforma SIEM/security monitoring.

Arsyetimi është si më poshtë:

Formati LEEF (Log Event Extended Format) është një standard i përdorur gjërësisht nga shumë pajisje dhe zgjidhje sigurie dhe prodhues të ndryshëm të sigurisë (si prsh, Splunk, Microsoft Sentinel, LogScale, etj).
Heqja e këtij formati nga kërkesa teknike mund të krijojë kufizime në integrimin e ardhshëm me sisteme ekzistuese ose të reja që gjenerojnë log-e në formatin LEEF.
Ruajtja e mbështetjes për LEEF nuk krijon konflikt me formatet e tjera të listuara dhe nuk ndikon negativisht në funksionalitetin e kërkuar; përkundrazi, rrit fleksibilitetin dhe shkallëzueshmërinë e zgjidhjes.
Në aspektin e konkurrencës dhe neutralitetit teknik, përfshirja e LEEF siguron që kërkesa të mos kufizojë operatorë apo produkte që përdorin këtë standard.
Heqja e një formati të mbështetur pa një arsye teknike të argumentuar bie ndesh me praktikën e ruajtjes së kompatibilitetit maksimal në sistemet e menaxhimit dhe analizës së log-eve.
<u>Për këto arsye, formulimi ekzistues të mbetet i pandryshuar, duke ruajtur edhe mbështetjen për sintaksën LEEF.</u>

Referuar kërkesës suaj për sqarim lidhur me termin "1200 stacione pune", ju bëjme me dije se kërkesa teknike e përcaktuar në Shtojcën 6 është formuluar në mënyrë të qartë dhe të mjaftueshme për hartimin dhe paraqitjen e ofertës nga operatorët ekonomike.
Në këtë kuadër, Autoriteti Kontraktor ka përcaktuar kërkesën për implementimin e një zgjidhjeje XDR që të mbrojë minimalisht 1200 stacione pune përmes një agjenti të vetëm në pikat fundore, sipas termave dhe nevojave funksionale të përcaktuara në dokumentet e procedurës.
nuk vlerësohet e nevojshme dhënia e një interpretimi shtesë përtej formulimit të specifikimit teknik;
operatorët ekonomike duhet të mbështeten në kërkesat e publikuara në dokumentacionin e tenderit për përgatitjen e ofertës;

b) Autoriteti Kontraktor ka percaktuar ne Shtojcen 6:
Zgiidhja duhet të ketë aftësinë për integrim nativ me registrat nga fireëall-et (Fortinet, Cisco, Check Point, Palo Alto etj.).
Zgjidhja duhet të ketë aftësinë për të kombinar alarmet e rrijetit nga pajisjet e lartpërmendura me alarmet nga pikat fundore për të realizuar korrelacion dhe për të arritur një kontekst më të mirë të sigurisë.
Zgjidhja duhet të përfshijë një periudhë minimale ruajtjeje prej 30 ditësh për të dhënat e papeërpunuara të marra nga agjentët dhe të ofrojë mundësinë e ruajtjes në cloud për një periudhë nga 6 deri në 12 muaj përmes një licence shtesë.
Duke qënë se afekton hartimin dhe dorëzimin e ofertës së OE, Ak të sqarojë:

- *Ak i ka të instaluar këto pajisje sepse në këtë procedure ka specifikuar se do kryejë suportin vetëm të pajisjeve Fortinet?*

- *Është kusht që në suportin e mirëmbajtjes të kryej dhe integrimin me pajisje shtesë?*

Referuar kërkesës lidhur me Shtojcën 6 të specifikimeve teknike, ju bëjmë me dije se kërkesat e percaktuara ne dokumentet e tenderit janë formular në mënyrë të qartë dhe të plotë, duke pasqyruar nevojat funksionale dhe teknike te Autoritetit Kontraktor.

Në këtë kuadër:
Specifikimi mbi aftësinë e zgjidhjes për integrim me pajisje të ndryshme fireëall (Fortinet, Cisco, Check Point, Palo Alto, etj.) i referohet kërkesës për interoperabilitet dhe fleksibilitet të platformës, dhe nuk nënkupton domosdoshmërisht ekzistencën aktuale të të gjitha këtyre pajisjeve nee infrastruktureen e Autoritetit Kontraktor.
Po ashtu, kerkesa peer integrim dhe korrelacion tee alarmeve synon funksionalitetin e zgjidhjes që është përcaktuar në objektin dhe specifikimet e procedurës.
Shërbimet do të realizohen sipas kërkesave dhe kufijve të përcaktuara në dokumentet e tenderit.
Për rrjedhojë, nuk vlerësohet e nevojshme dhënia e sqarimeve shtesë, pasi kërkesat janë të mjaftueshme për hartimin dhe doërezimin e ofertës nga operatorët ekonomikë.

c) Autoriteti Kontraktor ka specifikuar në Shtojcën 6
Zgiidhja duhet të ofroje ruajtje të pakufizuar në cloud (me licencë shtesë).
Duke qëne se afekton hartimin dhe dorëzimin e ofertës së OE, Ak të saktësojë se çfarë nënkuptoni me përcaktimin Licensë shtesë

Me termin "licencë shtesë" Autoriteti Kontraktor nënkupton që funksionaliteti i ruajtjes së pakufizuar në cloud duhet të mbështetet nga zgjidhja e propozuar dhe të jetë i disponueshëm si opsion/licencë suplementare nga prodhuesi, por nuk konsiderohet pjesë e detyrueshme e licencimit bazë, përveçse nëse operatori ekonomik e përfshin atë në ofertë. Operatori ekonomik duhet të specifikojë qartë në ofertë mënyrën e licencimit, periudhën dhe kushtet përkatese të këtij funksionaliteti.
Pretendimet tuaja mbi shtojcën 6 Specifikimet Teknike vlerësohen si jo të drejta nga "Komisioni i Shqyrtimit të Ankesës".
Nga shqyrtimi i ankesës suaj dhe në mbështetje me neneve 90 e në vijim të Ligiit Nr. 162. date 23.12.2020 "Për Prokurimin Publik", i ndryshuar, VKM-s Nr. 285, datë 19.05.2021 "Për Miratimin e Rregullave të Prokurimit Publik" si dhe Dokumenteve Standarde të Tenderit, u konstatua se pretendimet tuaja vlerësohen pjesërisht të drejta.".

III.3.4. Në Nenin 2 "*Qëllimi*" të ligjit 162/2021 "*Për prokurimin publik*", i ndryshuar parashikohet se:

"*Qëllim i këtij ligji është:*
a) të rrisë efiçencën dhe efikasitetin në procedurat e prokurimit publik;
b) të sigurojë mirëpërdorim të fondeve publike dhe të ulë shpenzimet procedurale;
c) të nxisë pjesëmarrjen e operatorëve ekonomikë në procedurat e prokurimit publik;
ç) të nxisë konkurrencën ndërmjet operatorëve ekonomikë;
d) të sigurojë një trajtim të barabartë dhe jodiskriminues për të gjithë operatorët ekonomikë, pjesëmarrës në procedurat e prokurimit publik;
dh) të sigurojë integritet, besim publik dhe transparencë në procedurat e prokurimit publik.".

Ndërsa në Nenin 3 "*Parime të përgjithshme*" të ligjit 162/2021 "*Për prokurimin publik*", i ndryshuar, parashikohet se:

"*1. Autoritetet dhe entet kontraktore garantojnë trajtim të barabartë dhe jodiskriminues për operatorët ekonomikë, si dhe veprojnë me transparencë e në mënyrë proporcionale.*
2. Autoritetet dhe entet kontraktore nuk duhet të shmangin fushën e zbatimit të këtij ligji ose të ngushtojnë në mënyrë artificiale konkurrencën. Konkurrenca konsiderohet se është ngushtuar artificialisht kur prokurimi përgatitet me qëllimin për të favorizuar ose dëmtuar në mënyrë të padrejtë operatorë ekonomikë të caktuar.
3. Autoritetet dhe entet kontraktore janë të detyruara të zbatojnë detyrimet e përcaktuara në legjislacionin mjedisor, social e të punës dhe në dispozitat e marrëveshjeve dhe konventat ndërkombëtare, të ratifikuara në përputhje me Kushtetutën.".

III.3.5. Në Nenin 21 *"Autoriteti ose enti kontraktor*" të ligjit 162/2021 "*Për prokurimin publik*", i ndryshuar, parashikohet se:

"*1. Autoriteti ose enti kontraktor është përgjegjës për prokurimin në përputhje me dispozitat e këtij ligji dhe të akteve nënligjore të nxjerra në zbatim të tij, duke garantuar respektimin e parimeve të trajtimit të barabartë, transparencës, konkurrencës dhe mosdiskriminimit, të parashikuara në këtë ligj*.
Në kuptim të kësaj pike, autoriteti ose enti kontraktor ka detyrimin të mirëplanifikojë në cilësi dhe në kohë fondet publike e nevojat e tij dhe të prokurojë e të zbatojë kontratën në përputhje me legjislacionin në fuqi.".

III.3.6. Në nenin 75 "*Sqarimet dhe ndryshimi në dokumentet e tenderit*" të ligjit 162/2021 "*Për prokurimin publik*", i ndryshuar, parashikohet se:

"*1. Ofertuesi i mundshëm mund të kërkojë sqarime për dokumentet e tenderit 26 nga autoriteti ose enti kontraktor, i cili duhet t'i përgjigjet çdo kërkese për sqarim të dokumenteve të tenderit,*

të bërë nga çdo operator ekonomik, me kusht që kërkesa të jetë marrë jo më vonë se 6 ditë para afatit përfundimtar të dorëzimit të ofertave. Autoriteti kontraktor ose enti duhet të përgjigjet brenda 3 ditëve nga depozitimi i kërkesës, në mënyrë që të bëjë të mundur dorëzimin e ofertës në kohë nga operatori ekonomik dhe, pa identifikuar burimin e kërkesës, duhet t'ua komunikojë sqarimin përkatës të gjithë operatorëve ekonomikë, që kanë tërhequr dokumentet e tenderit. Në çdo rast, sqarimi i dokumenteve të tenderit nuk do të konsiderohet shtim, pakësim ose ndryshim i kërkesave të përcaktuara nga autoriteti ose enti kontraktor në dokumentet e tenderit.
2. Autoriteti ose enti kontraktor, nga momenti i shpalljes së njoftimit të kontratës deri përpara mbarimit të afatit të fundit për dorëzimin e ofertave dhe për çfarëdolloj arsyeje, me nismën e vet ose me kërkesë të palëve të interesuara, mund të vendosë të bëjë ndryshime në dokumentet e tenderit përmes hartimit të një shtojce. Nëse ndryshimi i dokumenteve të tenderit bëhet në gjysmën e parë të afatit të pranimit të ofertave, autoriteti ose enti kontraktor mund të zgjasë afatin kohor të pritjes së ofertave. Nëse ndryshimi i dokumenteve të tenderit bëhet në gjysmën e dytë të afatit të pranimit të ofertave, autoriteti ose enti kontraktor zgjat afatin kohor për dorëzimin e ofertës me të paktën 10 ditë për procedurat mbi kufirin e lartë monetar dhe me të paktën 7 ditë për procedurat nën kufirin e lartë monetar.
3. Çdo shtojcë për ndryshim të dokumenteve të tenderit komunikohet në të njëjtën mënyrë që është bërë publikimi i njoftimit të procedurës.",

III.3.7. Në Nenin 77 "*Kërkesat për kualifikim*", pika 4, të ligjit nr.162/2020 "*Për prokurimin publik*", i ndyshuar, parashikohet shprehimisht se:
"*4. Në lidhje me aftësitë teknike dhe profesionale, autoritetet ose entet kontraktore mund të vendosin kërkesa që garantojnë se operatorët ekonomikë zotërojnë burimet e nevojshme njerëzore e teknike, si dhe përvojën e nevojshme për të zbatuar kontratën sipas një standardi të përshtatshëm cilësie. Autoritetet ose entet kontraktore, në veçanti, mund të kërkojnë që operatorët ekonomikë të kenë një nivel të mjaftueshëm përvoje që vërtetohet nga referenca të përshtatshme nga kontratat e zbatuara në të shkuarën. Aftësia profesionale e operatorëve ekonomikë për të ofruar shërbimin, punën, mallin vlerësohet në lidhje me aftësitë organizative, reputacionin dhe besueshmërinë, përvojën e duhur, si dhe personelin e nevojshëm për të zbatuar kontratën, siç është përshkruar nga autoriteti ose enti kontraktor në njoftimin e objektit të kontratës*.".

III.3.8. Neni 36 "*Specifikimet teknike*" të ligjit 162/2020 "*Për prokurimin publik*", i ndryshuar parashikon shprehimisht se:

"*1. Specifikimet teknike, siç përcaktohen në nenin 4 të këtij ligji, duhet të përshkruhen në dokumentet e tenderit. Në specifikimet teknike përcaktohen qartë karakteristikat e punëve, shërbimit ose furnizimit që do të prokurohet.*

Këto karakteristika mund të lidhen edhe me procesin specifik ose metodën e prodhimit ose ofrimit të punëve, furnizimeve ose shërbimeve të kërkuara ose me një proces specifik për një fazë tjetër të ciklit jetësor edhe kur këta faktorë nuk përbëjnë përmbajtjen e saj thelbësore nëse ato janë të lidhura me objektin e kontratës dhe proporcionale me vlerën dhe objektivat e saj.

Në specifikimet teknike mund të specifikohet edhe nëse do të jetë i nevojshëm transferimi i të drejtave të pronësisë intelektuale.

Specifikimet teknike, me përjashtim të rasteve të justifikuara plotësisht, hartohen në mënyrë të tillë që të marrin në konsideratë kriteret e aksesueshmërisë për personat me aftësi të kufizuar ose projektimit për të gjithë përdoruesit, sipas kërkesave në legjislacionin në fuqi.

2. Specifikimet teknike duhet të mundësojnë trajtim të barabartë për të gjithë kandidatët dhe ofertuesit dhe të mos shërbejnë si pengesa për konkurrencën e hapur në prokurimin publik.

3. Specifikimet teknike duhet të përshkruajnë qartë kërkesat e autoritetit ose entit kontraktor, duke iu referuar:

a) kërkesave funksionale ose të performancës, përfshirë karakteristikat mjedisore, me kusht që parametrat të jenë të saktë në mënyrë që t'u japin mundësi ofertuesve të përcaktojnë objektin e kontratës dhe autoriteteve ose enteve kontraktore të japin kontratën;

b) standardeve kombëtare, që mbështeten në ato ndërkombëtare, miratimeve teknike ndërkombëtare, specifikimeve teknike të përgjithshme, standardeve ndërkombëtare apo sistemeve të tjera teknike të referimit, të përcaktuara nga organet ndërkombëtare të standardizimit. Kur këto nuk ekzistojnë, ato u referohen standardeve kombëtare, miratimeve teknike kombëtare ose specifikimeve teknike kombëtare, që lidhen me projektimin, përllogaritjen dhe ekzekutimin e punëve ose përdorimin e produkteve;

c) kërkesave në terma funksionalë sipas shkronjës "a", referuar specifikimeve teknike sipas shkronjës "b" të kësaj pike, si mënyrë që nënkupton pajtueshmëri me kërkesat funksionale;

ç) të dyja metodave të përcaktuara në shkronjat "a" dhe "b" të pikës 3 të këtij neni, për mallra, shërbime ose punë të ndryshme, të përfshira në të njëjtin objekt kontrate. Çdo referencë duhet të shoqërohet nga fjalët "ose ekuivalenti i tij/saj".

4. Në specifikimet teknike, nëse nuk e justifikon objekti i kontratës, nuk duhet të përmendet asnjë markë prodhimi ose burim specifik apo proces i veçantë, që karakterizon produktet ose shërbimet e ofruara nga një operator ekonomik specifik apo asnjë markë tregtare, patentë, tipi ose origjinë apo prodhim specifik, me qëllim favorizimin ose eliminimin e disa sipërmarrjeve ose produkteve. Një gjë e tillë lejohet vetëm në raste përjashtimore kur nuk ekziston një mënyrë e mjaftueshme, e saktë apo e kuptueshme e përshkrimit të objektit të kontratës, sipas pikës 3 të këtij neni. Referime të tilla duhet të shoqërohen nga fjalët "ose ekuivalente".

5. Në rast se autoriteti ose enti kontraktor përcakton specifikimet teknike në bazë të shkronjës "b" të pikës 3 të këtij neni, nuk mund të refuzojë një ofertë me argumentin se punët, furnizimet apo shërbimet për të cilat është dorëzuar oferta nuk plotësojnë specifikimet teknike, të cilave u referohen, për sa kohë që ofertuesi provon në ofertën e tij me çdo mjet të përshtatshëm që

zgjidhjet e propozuara përmbushin kërkesat e përcaktuara në specifikimet teknike në mënyrë ekuivalente.

6. Në rast se autoriteti ose enti kontraktor përcakton specifikimet teknike në bazë të shkronjës "a" të pikës 3 të këtij neni, ai nuk mund të refuzojë një ofertë për punë, mallra apo shërbime, e cila është në përputhje me standardet kombëtare, që mbështeten në ato ndërkombëtare, miratimet teknike ndërkombëtare, specifikimet teknike të përgjithshme, standardet ndërkombëtare apo sistemet e tjera teknike të referimit, të përcaktuara nga organet ndërkombëtare të standardizimit kur këto specifikime teknike përmbushin kriteret funksionale, të përcaktuara nga autoriteti/enti kontraktor.

7. Autoriteti ose enti kontraktor në hartimin e specifikimeve teknike, referuar parashikimeve të mësipërme, kryen verifikim në Sistemin e Prokurimit Elektronik përmes ndërveprimit me sisteme të tjera kombëtare në rast se ekzistojnë standarde kombëtare ose ndërkombëtare në fuqi për mallrat, punët dhe shërbimet. Sistemi duhet të zhvillohet duke përdorur teknologji të avancuar të inteligjencës artificiale dhe procese të robotizuara në përputhje me parashikimet evropiane.".

III.3.9. Në nenin 41, pika 1 "*Kërkesa të veçanta për kontratat shërbimeve*" të VKM Nr. 285 datë 19.5.2021 "*Për miratimin e rregullave të prokurimit publik*", i ndryshuar, parashikohet se:

"*1. Në procedurat e prokurimit për shërbime, autoriteti/enti kontraktor duhet të përcaktojë qartë në termat e referencës, natyrën, objektin, qëllimin, specifikimet teknike dhe afatet kohore të shërbimit që do të kryhet*.".

III.3.10. Komisioni i Prokurimit Publik, gjykon, se është e nevojshme të ndalet në një interpretim të zgjeruar të dispozitës së lex specialis, mbi mënyrën e hartimit të specifikimeve teknike. Autoritetet kontraktore në hartimin e specifikimeve teknike, krahas përshkrimit të saktë të nevojave të këtij të fundit, duhet të kenë në vëmendje faktin, se hartimi i specifikimeve teknike duhet bërë në një mënyrë gjithëpërfshirëse duke krijuar kushte për konkurrim të paanshëm e të hapur ndërmjet të gjithë kandidatëve e ofertuesve, duke përshkruar sa më saktë dhe në mënyrë të plotë karakteristikat e mallrave/shërbimeve/punëve dhe në përputhshmëri me objektin e kontratës. Për këtë qëllim ligjvënësi ka parashikuar, se këto karakteristika mund të lidhen edhe me procesin specifik ose metodën e prodhimit ose ofrimit të punëve, furnizimeve ose shërbimeve të kërkuara ose me një proces specifik për një fazë tjetër të ciklit jetësor, edhe kur këta faktorë nuk përbëjnë përmbajtjen e saj thelbësore, nëse ato janë të lidhura me objektin e kontratës dhe proporcionale me vlerën dhe objektivat e saj. Ligjvënësi ka parashikuar qartësisht në nenin 36 pika 1 paragrafi 4 të ligjit nr.162/2020 "*Për prokurimin publik*", i ndryshuar, se duhet të mundësojnë trajtim të barabartë për të gjithë kandidatët dhe ofertuesit dhe të mos shërbejnë si pengesa për konkurrencën e hapur në prokurimin publik.Në respekt të parimit të mësipërm,

specifikimet teknike, në asnjë rast nuk duhet të diskriminojnë/përjashtojnë nga konkurrimi operatorët ekonomikë ofertues dhe/ose prodhuesit qofshin këta kombëtar apo ndërkombëtarë. Në hartimin e specifikimeve teknike autoritetet kontraktore duhet të shmangin çdo formë diskriminimi, qoftë ato të dukshme, qoftë ato të fshehta, të cilat kanë të njëjtin efekt. Në asnjë rast, specifikimet teknike nuk duhet të hartohen në mënyrë që të drejtojnë drejt një produkti/malli/shërbimi, që ofrohen nga një operator i vetëm ekonomik ose nga një prodhues i vetëm. KPP gjykon, se parashikimet e mësipërme duhet të zbatohen në të gjitha procedurat e prokurimit, me përjashtim të rasteve ku vetë ligji i prokurimit publik, parashikon një përjashtim të tillë. Në hartimin e specifikimeve teknike autoritetet kontraktore duhet të mbajnë në vëmendje faktin se specifikimet teknike duhet të përshkruajnë minimumin ose tërësinë e elementeve më të rëndësishme përbërëse, që garantojnë cilësinë e kërkuar, në përputhje me nenin 36 të LPP dhe që i vlerëson punët/mallrat/shërbimet si të pranueshme për funksionet e kërkuara. Gjithashtu, duke u ndalur në pikën 3 të nenit 36 të ligjit për prokurimin publik, KPP gjykon se, ligjvënësi ka parashikuar katër metoda kryesore në hartimin e specifikimeve teknike. Metoda e parë lidhet me kërkesat funksionale ose të performancës, përfshirë karakteristikat mjedisore, me kusht që parametrat të jenë të saktë në mënyrë që t'u japin mundësi ofertuesve të përcaktojnë objektin e kontratës dhe autoriteteve ose enteve kontraktore të japin kontratën. Metoda e dytë mbështetet në standardet kombëtare, që mbështeten në ato ndërkombëtare, miratimeve teknike ndërkombëtare, specifikimeve teknike të përgjithshme, standardeve ndërkombëtare apo sistemeve të tjera teknike të referimit, të përcaktuara nga organet ndërkombëtare të standardizimit. Kur këto nuk ekzistojnë, ato u referohen standardeve kombëtare, miratimeve teknike kombëtare ose specifikimeve teknike kombëtare, që lidhen me projektimin, përllogaritjen dhe ekzekutimin e punëve ose përdorimin e produkteve. Metoda e tretë përfshin kërkesat në termat funksionalë sipas metodës së parë, por referuar specifikimeve teknike të hartuara sipas metodës së dytë, si një mënyrë që nënkupton pajtueshmëri me kërkesat funksionale, si edhe të të dyja metodave të përcaktuara në shkronjat "a" dhe "b" të pikës 3 të nenit 36 të ligjit për prokurimin publik, për mallra, shërbime ose punë të ndryshme, të përfshira në të njëjtin objektkontrate. Çdo referencë duhet të shoqërohet nga fjalët "ose ekuivalenti i tij/saj". Nga interpretimi teleologjik (qëllimi i normës juridike), arrijmë në përfundim, se e rëndësishme është që përmes specifikimeve teknike, autoriteti kontraktor të mundësojë një konkurrim të drejtë, të hapur, e gjithëpërfshirës, të barabartë dhe jodiskriminues për të gjithë operatorët ekonomikë, si edhe të mos drejtohen drejt një produkti të vetëm të ofruar nga një operator i vetëm ose nga një numër i 32 kufizuar operatorësh ekonomikë.

Gjithashtu, referuar nenit 42 të Direktivës 24/2014 "*Për prokurimin publik*" KE, parashikohet se: "*Specifikimet teknike siç përcaktohen në pikën 1 të Shtojca VII do të përcaktohet në dokumentet e prokurimit. Specifikimi teknik përcakton karakteristikat që kërkohen për një punë, shërbim ose furnizim*".

Gjithashtu, në nenin 4 paragrafi 38 të ligjit nr.162/2020 "*Për prokurimin publik*", i dryshuar përcaktohet "Specifikime teknike" janë: a) në rast të prokurimit publik të punëve, përmbledhje e të dhënave teknike të përfshira në dokumentacionin e tenderit, me të cilat janë përkufizuar karakteristikat e nevojshme të materialeve, prodhimeve ose mallrave për t'u përshtatur me përdorimin që i duhet autoritetit ose entit kontraktor. Këto karakteristika përfshijnë ndikimin mbi mjedisin jetësor dhe ndikime klimatike, përshkrim i të gjitha kushteve, duke përfshirë edhe procedurat për sigurim të cilësisë, terminologjinë, simbolet, metodat e testimit, paketimit, shënimit dhe etiketimit, si dhe udhëzime për shfrytëzim, proceset dhe metodat e prodhimit të objektit. Gjithashtu, këto karakteristika, përfshijnë rregulla nga projekti dhe rregulla për vlerësim të shpenzimeve, kushte për testim, për inspektim dhe për pranim të punëve të realizuara, metoda ose teknika ndërtimore, si dhe të gjitha kushtet e tjera teknike, të cilat autoriteti ose enti kontraktor ka të drejtë t'i përcaktojë në pajtim me rregullat e përgjithshme dhe të veçanta në lidhje me objektin dhe materialet ose pjesët e përfshira; b) në rast të prokurimit publik të mallrave ose shërbimeve, specifikimi me të cilin përkufizohen karakteristikat e prodhimit ose shërbimit, siç janë niveli i cilësisë, ndikimi mbi mjedisin jetësor dhe ndikimet klimatike, përshkrim i të gjitha kushteve, duke përfshirë edhe arritshmëri për persona me aftësi të kufizuar dhe vlerësim të përputhshmërisë, niveli i realizimit, shfrytëzim i prodhimit, siguri ose dimensione, duke i përfshirë edhe kërkesat relevante për produktin në raport me emërtimin me të cilin shitet, terminologjinë, simbolet, testimet dhe metodat për testim, paketimin, shënimin dhe etiketimin, si dhe udhëzime për përdorim, proceset dhe metodat e prodhimit në secilën fazë të jetëgjatësisë së mallrave dhe shërbimeve, si dhe procedura për vlerësim të përputhshmërisë." Ndërsa, në pikën 1 të Shtojcës VII të Direktivës parashikohet se: "specifikim teknik" nënkupton njërën nga sa vijon: b) në rastin e kontratave të furnizimit publik ose shërbimeve, një specifikim në një dokument që përcakton karakteristikat e kërkuara të një produkti ose një shërbimi, siç janë nivelet e cilësisë, nivelet e performancës mjedisore dhe klimatike, modelimi për të gjithë kërkesat (përfshirë aksesin e personave me aftësi të kufizuara) dhe vlerësimin e konformitetit, performancën, përdorimin e tyre produkti, siguria ose dimensionet, përfshirë kërkesat që lidhen me produktin në lidhje me emrin nën të cilin produkti shitet, terminologji, simbole, metodat e provës dhe provës, paketimin, markimin dhe etiketimin, përdorues-udhëzimet, proceset e prodhimit dhe metodat në çdo fazë të ciklit jetësor të furnizimit ose shërbimit dhe procedurat e vlerësimit të konformitetit; Në vendimin e GJED Çështja C-368/10 "Komisioni Europian vs. Mbretëria e Holandës" inter allia dhe mutatis mutandis është arsyetuar se: "Specifikimet teknike të hartuara nga blerësit publik duhet të lejojnë që prokurimet publike të hapen në konkurrencë. Për këtë qëllim, duhet të jetë e mundur të dorëzohen tenderë që pasqyrojnë larminë e zgjidhjeve teknike. Prandaj, duhet të jetë e mundur të hartohen specifikimet teknike për sa i përket performancës funksionale dhe kushteve, dhe kur referimi bëhet në standardin Evropian ose, në 33 mungesë të tij, ndaj standardit kombëtar, ofertuesit bazuar në marrëveshje ekuivalente duhet të merren në konsideratë nga autoritetet kontraktuese." Gjithashtu, nga ana tjetër Komisioni i

Prokurimit Publik gjen me vend të sqarojë, se është në të drejtë të operatorëve ekonomikë që në respekt të nenit 109 e vijues të ligjit nr.162/2020 ”Për prokurimin publik” të parashtrojnë pretendime mbi modifikimin e dokumenteve të procedurës së prokurimit përfshirë edhe specifikimet teknike të procedurës, brenda afatit të përcaktuar në nenin 110 pika 1 të ligjit. Komisioni i Prokurimit Publik vlerëson, se ligji 162/2020 ”Për prokurimin publik” është përafruar pjesërisht edhe me Direktivën e Këshillit 89/665/KEE, datë 21 dhjetor 1989 “Mbi koordinimin e ligjeve, rregulloreve dhe dispozitave administrative në lidhje me zbatimin e procedurave të rishikimit për dhënien e kontratave të furnizimit publik dhe punëve publike”, e ndryshuar”. Numri CELEX 31989L0665, Fletorja Zyrtare e Bashkimit Europian, Seria L, nr.395, datë 30.12.1989, fq. 33. Në dritën e direktivës, ekzistojnë dy kushte të përmendura në lidhje me qasjen në procedurat e rishikimit (neni 1 (3): "Procedurat e rishikimit duhet të jenë në dispozicion (...) të paktën për çdo person që ka ose ka pasur interes për të marrë një kontratë të veçantë dhe që ka qenë ose rrezikon të dëmtohet nga një shkelje e pretenduar". Në nenin 94 pika 1 të Vendimit të Këshillit të Ministrave nr. 285, datë 19.05.2021 “*Për miratimin e rregullave të prokurimit publik*” i ndryshuar parashikohet se: “Çdo person, që ka ose ka pasur interes në një procedurë prokurimi dhe kur është dëmtuar ose rrezikohet të dëmtohet nga një vendim i autoritetit kontraktor, që bie në kundërshtim me LPP, mund ta kundërshtojë këtë vendim.” Në interpretim literal, sistematik dhe teologjik me synim vendosjen në pah të ratio legis, mbështetur edhe në parimin e së drejtës se ratio legis est anima legis, (qëllimi i ligjit është edhe shpirti i ligjit), interesi i ligjshëm i operatorëve për të paraqitur ankim pranë autoritetit kontraktor, si edhe pranë Komisionit të Prokurimit Publik duhet të jetë dëmtuar ose rrezikohet të dëmtohet nga një vendim i marrë nga autoriteti kontraktor në kundërshtim me ligjin e prokurimit publik. KPP thekson, se fakti se nëse një ose disa produkte të një ose disa prodhuesve vendas ose ndërkombëtarë nuk përmbushin minimumin e specifikimeve teknike të përcaktuara nga ana e autoritetit kontraktor nuk përbën një kusht sine qua non, se specifikimet teknike janë hartuar në kundërshtim me ligjin për prokurimin publik. Komisioni i Prokurimit Publik gjykon, se në rastin konkret ndodhemi në kuptimin klasik të barrës së provës referuar parimit juridik onus probandi incubit actor (barra e provës i bie kërkuesit) si edhe në përputhje me nenin 82 pika 1 të ligjit nr.44/2015 “Kodi i Procedurave Administrative i Republikës së Shqipërisë”, në të cilin parashikohet se: “në procedurat administrative, të filluara me kërkesë të palës që inicion procedurën, barra e provës për faktet e pretenduara bie mbi këtë palë, pavarësisht nga detyrimi i organit publik për të vënë në dispozicion të palëve provat e zotëruara prej saj”. Pra, operatorët ekonomikë duhet të argumentojnë/dëshmojnë, se specifikimet teknike të hartuara nga autoriteti kontraktor janë në kundërshtim me ligjin e prokurimit publik dhe jo mbi faktin se këto të fundit nuk plotësohen nga një ose disa prodhues kombëtar/ndërkombëtarë me reputacion.

III.3.11. Komisioni i Prokurimit Publik gjykon, se është e nevojshme të ndalet në një interpretim të zgjeruar të dispozitës së Lex specialis, mbi mënyrën e hartimit të specifikimeve teknike.

Autoritetet kontraktore në hartimin e specifikimeve teknike, krahas përshkrimit të saktë të 34 nevojave të këtij të fundit, duhet të kenë në vëmendje faktin, se hartimi i specifikimeve teknike duhet bërë në një mënyrë gjithëpërfshirëse duke krijuar kushte për konkurrim të paanshëm e të hapur ndërmjet të gjithë kandidatëve e ofertuesve, duke përshkruar sa më saktë dhe në mënyrë të plotë karakteristikat e mallrave/shërbimeve/punëve dhe në përputhshmëri me objektin e kontratës. Për këtë qëllim ligjvënësi ka parashikuar, se këto karakteristika mund të lidhen edhe me procesin specifik ose metodën e prodhimit ose ofrimit të furnizimeve ose shërbimeve të kërkuara ose me një proces specifik për një fazë tjetër të ciklit jetësor edhe kur këta faktorë nuk përbëjnë përmbajtjen e saj thelbësore nëse ato janë të lidhura me objektin e kontratës dhe proporcionale me vlerën dhe objektivat e saj.
Ligjvënësi ka parashikuar qartësisht në nenin 36 pika 2 të ligjit nr.162/2020 "Për prokurimin publik", i ndryshuar, thuhet se: Specifikimet teknike duhet të mundësojnë trajtim të barabartë për të gjithë kandidatët dhe ofertuesit dhe të mos shërbejnë si pengesa për konkurrencën e hapur në prokurimin publik.
Në respekt të parimit të mësipërm, specifikimet teknike në asnjë rast nuk duhet të diskriminojnë/ përjashtojnë nga konkurrimi operatorët ekonomikë ofertues dhe/ose prodhuesit qofshin këta kombëtarë apo ndërkombëtarë. Në hartimin e specifikimeve teknike autoritetet kontraktore duhet të të orientojnë operatorët ekonomikë në përgatitjen e ofertave.
Në hartimin e specifikimeve teknike autoritetet kontraktore duhet të mbajnë në vëmendje faktin, se specifikimet teknike duhet të përshkruajnë minimumin ose tërësinë e elementeve më të rëndësishme përbërëse, që garantojnë cilësinë e kërkuar, në përputhje me nenin 36 të LPP dhe që i vlerëson punët/mallrat/shërbimet si të pranueshme për funksionet e kërkuara. Gjithashtu, nga ana tjetër Komisioni i Prokurimit Publik gjen me vend të sqarojë, se është në të drejtë të operatorëve ekonomikë, që në respekt të nenit 109 e vijues të ligjit nr.162/2020 "Për prokurimin publik", i ndryshuar, të ushtrojnë të drejtën e ankimimit mbi modifikimin e dokumenteve të procedurës së prokurimit, përfshirë edhe specifikimet teknike të procedurës, brenda afatit të përcaktuar në nenin 110, pika 1 të ligjit nr.162/2020.

III.3.12.1. Nisur nga pretendimi i operatorit ekonomik ankimues, si në vijim: "*... Bazuar në pikën 2 të nenit 78 të VKM-së nr. 285, datë 19.05.2021 "Për miratimin e rregullave të prokurimit publik", i ndryshuar ku parashikohet se: "2. Hartimi i kërkesave për kualifikim, që lidhen me kapacitetin teknik, specifikimet teknike, kriteret për shpalljen e ofertës fituese (nëse është rasti) dhe çdo informacion tjetër specifik i nevojshëm, bëhen nga specialisti i fushës, anëtar i njësisë së prokurimit. Në varësi të objektit të prokurimit, nëse nuk është vlerësuar e nevojshme caktimi i një specialisti fushe, hartimi i kërkesave si më sipër bëhet nga njësia e prokurimit. Në çdo rast, hartimi i tyre duhet të argumentohet teknikisht dhe ligjërisht, si dhe të dokumentohet në një procesverbal të mbajtur nga personat e ngarkuar për përgatitjen e tyre. Ky procesverbal i vihet në dispozicion personit/ave përgjegjës për prokurimin, i cili/të cilët e bën/bëjnë pjesë të dosjes së*

tenderit. Seti përfundimtar i dokumenteve të tenderit nënshkruhet në çdo faqe nga anëtarët e njësisë së prokurimit",

Në përputhje dhe me praktiken e unifikuar të KPP (sipas vendimit nr. Nr. 671/2026) autoriteti kontraktor duhet të argumentojë teknikisht vendosjen e specifikimeve teknike dhe ta publikojë në SPE në mënyrë që të bëhet e njohur për të gjithë operatorët ekonomikë të interesuar.

Kërkesë 7:

*Kërkojme: Autoriteti kontraktor duhet të argumentojë teknikisht vendosjen e specifikimeve teknike dhe ta publikojë në SPE në mënyrë që të bëhet e njohur për të gjithë operatorët ekonomikë të interesuar.***", s**i dhe nga verifikimi i procesverbalit "*Për argumentimin dhe miratimin e specifikimeve teknike dhe kritereve për kualifikim*", Komsioni konstaton, se autoriteti kontraktor ka argumentuar si vijon: "[..]***"II. Argumentimi i specifikimeve teknike***

Specifikimet teknike të procedurës për ***"Blerje suport për SIEM + licenca për EDR/XDR (1200 përdorues) dhe licenca Fireëall Professional për 4 (katër) vite"****, janë hartuar mbi bazën e Urdhrit të brendshëm nr. 24, datë 12.03.2026, të Administratorit të "Posta Shqiptare" sh.a., në përputhje me nenin 4, pika 38/b dhe nenin 36 të ligjit nr. 162/2020 "Për Prokurimin Publik", si dhe nenin 41, pika 1 të VKM nr. 285, datë 19.05.2021 "Për miratimin e rregullave të prokurimit publik" (i ndryshuar).*

Specifikimet teknike të shërbimit objekt prokurimi janë hartuar duke u diktuar nga nevoja për forcimin, mbrojtjen dhe monitorimin e infrastrukturës së teknologjisë së informacionit të Autoritetit Kontraktor, nëpërmjet implementimit dhe përdorimit të zgjidhjeve të avancuara të sigurisë kibernetike, përfshirë sistemin SIEM, licencat EDR/XDR për 1200 përdorues dhe licencat Fireëall Professional, të cilat garantojnë mbrojtje në kohë reale, analizë të ngjarjeve të sigurisë dhe parandalim të kërcënimeve kibernetike.

Këto specifikime teknike shprehin tërësinë e elementeve funksionale, teknike dhe operacionale të domosdoshme për sigurimin e vazhdimësisë së shërbimit, nivelit të kërkuar të sigurisë (SLA), si dhe përputhshmërinë me standardet bashkëkohore të sigurisë së informacionit dhe kërkesat operacionale të Autoritetit Kontraktor."." Referuar argumentimit të dhënë nga autoriteti kontraktor Komisioni konstaton, se autoriteti kontraktor ka argumentuar teknikisht specifikimimet teknike të përcaktuara në dokumentat e tenderit, si dhe ka dhënë vetëm argumentimin ligjor. Bazuar në pikën 2 të nenit 78 të VKM-së nr. 285, datë 19.05.2021 "*Për miratimin e rregullave të prokurimit publik*", i ndryshuar ku parashikohet se: "*2. Hartimi i kërkesave për kualifikim, që lidhen me kapacitetin teknik, specifikimet teknike, kriteret për shpalljen e ofertës fituese (nëse është rasti) dhe çdo informacion tjetër specifik i nevojshëm, bëhen nga specialisti i fushës, anëtar i njësisë së prokurimit. Në varësi të objektit të prokurimit, nëse nuk është vlerësuar e nevojshme caktimi i një specialisti fushe, hartimi i kërkesave si më sipër bëhet nga njësia e prokurimit. Në çdo rast, hartimi i tyre duhet të argumentohet teknikisht dhe ligjërisht, si dhe të dokumentohet në një procesverbal të mbajtur nga personat e ngarkuar për përgatitjen e tyre. Ky procesverbal i vihet në dispozicion personit/ave përgjegjës për*

prokurimin, i cili/të cilët e bën/bëjnë pjesë të dosjes së tenderit. Seti përfundimtar i dokumenteve të tenderit nënshkruhet në çdo faqe nga anëtarët e njësisë së prokurimit", Komisioni gjykon, se autoriteti kontraktor ka argumentuar teknikisht vendosjen e specifikimeve teknike dhe ta publikojë në SPE në mënyrë që të bëhet e njohur për të gjithë operatorët ekonomikë të interesuar.

Përsa më sipër, pretendimi i operatorit ekonomik ankimues "*PC STORE*" SHPK nuk qëndron.

III.3.12.2. Nisur nga pretendimi i operatorit ekonomik ankimues, si në vijim: "*... Kërkesë 8:*
Ankesë 8.1 Zgjidhje XDR (Extended Detection and Response)
a) Tek Shtojca 6, Formulari i Specifikimeve teknike , konkretisht ak është shprehur
a) Autoriteti Kontraktor kërkon implementimin e një zgjidhjeje të avancuar të tipit XDR (Extended Detection and Response), e cila duhet të jetë në gjendje të mbrojë minimalisht 1200 stacione pune përmes një agjenti të vetëm të instaluar në pikat fundore
Duke qënë se afekton hartimin dhe dorëzimin e ofertës së OE, Ak të sqarojë nëse me termin "1200 stacione pune" Autoriteti Kontraktor nënkupton:
- vetëm endpoint/ëorkstation;
- servera;
- pajisje rrjeti;
- apo çdo asset tjetër të lidhur në infrastrukturë."**,** Komisioni gjykon se se objekti i pretendimit të operatorit ekonomik ankimues është paqartësi mbi kërkesat teknike të dokumentave të tenderit. Autoriteti kontraktor ka dhënë sqarime por KPP gjykon se këto sqarime nuk janë shteruese, pasi autoriteti kontraktor nuk ka shpjeguar qartësisht dhe konkretisht paqartësitë e ankimuesit lidhur me faktin se çfarë nënkupton termi "Poste pune" duke sqaruar qartësisht ankimuesin lidhur me llojin e pajisjeve që janë të instaluara në këto poste pune sipas kërkesave të bëra nga ankimuesi, në mënyrë që oferuesit të qartësohen lidhur me hartimin e ofertës ekonomike. Për pasojë, KPP gjykon se autoriteti kontraktor, përvecse të sqarojë ankimuesin në mënyrë shteruese për të gjitha paqartësitë e tij, këto sqarime dhe ndryshime të dokumentave të tenderit duhet tu bëhen me dije edhe ofertuesve të interesuar për procedurën e mësipërme të prokurimit, në përputhje me përcaktimet e nenit 75 të LPP-së si më sipër cituar.

Përsa më sipër, pretendimi i operatorit ekonomik ankimues "PC STORE" SHPK qëndron.

III.3.12.3. Nisur nga pretendimi i operatorit ekonomik ankimues, për modifikimin e specifikimeve tenike të përcaktuara në Shtojcën 6 "FORMULARI I SPECIFIKIMEVE TEKNIKE" të dokumentave të tenderit, të parashtuara në kërkesën nr. 8.2 si në vijim: "*... Kërkojmë modifikimin e keësaj kërkese teknike dhe riformulimin ligjor të saj si më poshtë vijon: "Zgjidhja duhet të mbështesë mekanizma të avancuar të mbrojtjes për Linux dhe macOS, të bazuar në behavioral detection dhe exploit prevention, me aftësi për të identifikuar dhe parandaluar teknika të njohura sulmi, përfshirë por pa u kufizuar në privilege escalation, reverse shell, ransomëare activity, memory exploitation, hijacking dinamike dhe ekzekutim të paautorizuar të kodit.".*", si dhe referuar shkresës nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, të autoritetit kontraktor, ku ka argumentuar mospranimin e këtij pretendimi të ankimmuesit, si në vijim: "*Ndryshimi i kërkesës nga një listë e qartë dhe specifike e teknikave të mbrojtjes drejt një formulimi të përgjithshem "behavioral detection dhe exploit prevention" ul nivelin e qartësisë teknike dhe të matshmërisë së kërkesës.*

Në vërsionin ekzistues, kërkesat përcaktojnë në mënyrë të drejtpërdrejtë mekanizmat dhe teknikat konkrete që zgjidhja duhet të mbështesë për Linux dhe macOS, si p.sh. Brute Force Protection, Java Deserialization Protection, Reverse Shell Protection, ROP Mitigation, Shellcode Protection, SO/Dylib Hijacking Protection, Gatekeeper Enhancement dhe Anti- Ransomeare. Kjo qasje siguron:

- *Qartësi teknike mbi funksionalitetet minimale të kërkuara;*
- *Mundësi objektive për verifikim dhe testim gjatë fazës së vlerësimit;*
- *Krahasim të drejtë ndërmjet ofertuesve;*
- *Eliminim të interpretimeve subjektive nga operatorët ekonomikë;*

Garanci që zgjidhja mbulon teknika specifike dhe të njohura sulmi për secilin sistem operativ.

Ndërsa formulimi i ri përdor tërma të përgjithshem si "mekanizma të avancuar", "behavioral detection" dhe "aftësi për të identifikuar dhe parandaluar teknika të njohura sulmi", pa specifikuar kontrollet konkrete që duhet të ekzistojnë. Kjo krijon paqartësi në interpretim dhe mund të lejojeë paraqitjen e zgjidhjeve që dekarojnë mbështetje të përgjithshme, por që në praktikë nuk ofrojnë mbrojtje të dedikuar për teknikat specifike të kerkuara.

Gjithashtu, lista aktuale e teknikave nuk është kufizuese, por përfaqëson një minimum të domosdoshëm sigurie për mbrojtjen e endpoint-eve Linux dhe macOS ndaj teknikave modeme të exploit-eve dhe privilege escalation. Heqja e tyre mund të sjellë ulje teë standardit të sigurisë dhe vështirësi në validimin e përputhshmërisë së ofertës me kërkesat teknike.

Për këtë arsye, kërkesa ekzistuese duhet të ruhet në formën aktuale, pa hequr listën konkrete të mekanizmave dhe teknikave të mbrojtjes të kërkuara.

Ndryshimi i propozuar nuk mund të miratohet, pasi formulimi ekzistues është më i qartë, me i drejtpërdrejtë dhe teknikisht me i matshëm në kuadër të keërkesave të tenderit/specifikimeve.", Komisioni i Prokurimit Publik konstaton se operatori ekonomik ankimues nuk ka argumentuar teknikisht se si këto specifikime janë hartuar në kundërshtim me legjislacionin në fuqi për

prokurimin publik. Gjithashtu, nuk është provuar se si këto kërkesa ngushtojnë konkurrencën apo favorizojnë një markë të caktuar. Përshkrimi aftësisë zbuluese dhe parandalimit të kërzënimeve të zgjidhjes XDR (Extended Detecion and Response), si në vijim: "*Zgjidhja duhet të jetë në gjendje të parandalojë exploit-e bazuar në teknikat specifike të Linux-it, si Brute Force Protection, Java Deserialization, Privilege Escalation, Reverse Shell Protection, ROP Mitigation, Shellcode Protection dhe SO Hijacking Protection.*
Zgjidhja duhet të jetë në gjendje të parandalojë exploit-e bazuar në teknikat specifike të macOS, si Anti-Ransomëare, Dylib Hijacking Protection, Gatekeeper Enhancement, JIT Mitigation, Privilege Escalation dhe ROP Mitigation.", nuk përbën një markë tregtare apo specifikime teknike që të çojnë drejt një marke të caktuar tregtare, por është një emërtim i cili përcakton aftësisë zbuluese dhe parandalimit të kërcënimeve të zgjidhjes XDR (Extended Detecion and Response). Autoriteti Kontraktor gëzon të drejtën ligjore të përcaktojë kriteret dhe specifikimet teknike sipas nevojave të tij, duke kërkuar që produktet objekt prokurimi të përmbushin standardet më të larta të cilësisë. Komisioni i Prokurimit Publik, gjykon se, autoriteti kontraktor është organi përgjegjës për procedurën e prokurimit dhe është përgjegjësi e tij të përcaktojë kritere që janë në funksion të realizimit me sukses të kontratës. Rrjedhimisht autoriteti kontraktor është në të drejtën e tij për të përcaktuar kritere dhe specifikime teknike në lidhje me produktin e kërkuar, por pa përcaktuar kritere/specifikime teknike të cilat të çojnë drejt një marke të caktuar, apo që nuk ndikojnë në performancën e produktit, pasi përcaktime të tilla janë diskriminuese dhe përjashtuese nga pjesëmarrja në procedurë të operatorëve ekonomikë të interesuar. Në asnjë moment autoriteti kontraktor nuk duhet të vendose kritere apo të hartojë specifikime teknike të cilat të drejtojnë në një emër të caktuar marke apo prodhuesi, duke u bërë kështu përjashtues për operatorë të tjerë.

Përsa më sipër, pretendimi i operatorit ekonomik ankimues "PC STORE" SHPK nuk qëndron.

III.3.12.5. Nisur nga pretendimi i operatorit ekonomik ankimues, për modifikimin e specifikimeve tenike të përcaktuara në Shtojcën 6 "FORMULARI I SPECIFIKIMEVE TEKNIKE" të dokumentave të tenderit, të parashtuara në kërkesën nr. 8.3 si në vijim: "*...Kërkesë 8.3*
Për të garantuar kërkesen për hartimin e kritereve teknike në porpocionalitet, në lidhje me objektin e kontratës dhe duke respektuar parimin e konkurrencës, kërkojmë që kërkesa të riformulohet si më poshtë:

“Motori i korrelacionit duhet të mbështesë filtrim dhe përputhje të avancuar të modeleve në evente/log-e, përfshirë operatorë ëildcard (p.sh. LIKE) dhe shprehje të rregullta (REGEX), për ndërtimin e rregullave të avancuara të detektimit dhe korrelacionit”.”, si dhe referuar shkresës nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, të autoritetit kontraktor, ku ka argumentuar mospranimin e këtij pretendimi të ankimmuesit, si në vijim: “*Formulimi aktual përcakton qartë dhe në mënyrë konkrete funksionalitetet minimale që duhet të mbeshteten nga sistemi, konkretisht:*

- *filtrimin me operatorin LIKE;*
- *përputhjen e modeleve me REGEX.*

Këto janë kërkesa të verifikueshme dhe të testueshme gjatë fazës së vlerësimit teknik.
Formulimi i ri përdor terma më të përgjithshëm dhe interpretues si:

- *"filtrim dhe përputhje të avancuar";*
- *"operatore eildcard";*
- *"ndërtimin e rregullave të avancuara".*

Këto shprehje nuk përcaktojnë qartë kufijtë minimale teknike dhe krijojnë hapësirë për interpretime të ndryshme nga operatorët ekonomike.
Përdorimi i termit "p.sh. LIKE" e bën mbështetjen e operatorit LIKE jo detyrim të drejtpërdrejtë, por vetëm shëmbull ilustrues. Kjo mund të sjellë paqartësi gjatë implementimit dhe verifikimit të përputhshmërisë seë ofertave.
Kërkesa ekzistuese është neutrale dhe standarde nga pikëpamja teknike, ndërsa formulimi i ri zgjeron në mënyre të panevojshme përshkrimin funksional pa shtuar vlerë reale teknike apo operacionale.
Ruajtja e formulimit aktual ndihmon në:

- *shmangien e interpretimeve subjektive;*
- *garantimin e trajtimit të barabartë të operatorëve ekonomikë;*
- *lehtësimin e procesit të verifikimit të përmbushjes se kërkesave teknike.*

Për rrjedhojë, të mos ndryshohet formulimi aktual i kërkesës dhe të mbetet teksti ekzistues i Shtojcës 6..”, Komisioni i Prokurimit Publik konstaton se operatori ekonomik ankimues nuk ka argumentuar teknikisht se si këto specifikime janë hartuar në kundërshtim me legjislacionin në fuqi për prokurimin publik. Gjithashtu, nuk është provuar se si këto kërkesa ngushtojnë konkurrencën apo favorizojnë një markë të caktuar. Përshkrimi rregullave të korelacionit të të kërzënimeve të zgjidhjes SIEM, si në vijim: “• *lejojnë filtrimin duke përdorur operatorin LIKE dhe përputhjen e modeleve duke përdorur shprehje të rregullta (REGEX);*”, nuk përbën një markë tregtare apo specifikime teknike që të çojnë drejt një marke të caktuar tregtare, por është një emërtim i cili përcakton rregullat e korelacionit të zgjidhjes SIEM. Autoriteti Kontraktor gëzon të drejtën ligjore të përcaktojë kriteret dhe specifikimet teknike sipas nevojave të tij, duke kërkuar që produktet objekt prokurimi të përmbushin standardet më të larta të cilësisë. Komisioni i Prokurimit Publik, gjykon se, autoriteti kontraktor është organi përgjegjës për procedurën e prokurimit dhe është përgjegjësi e tij të përcaktojë kritere që janë në funksion të realizimit me

sukses të kontratës. Rrjedhimisht autoriteti kontraktor është në të drejtën e tij për të përcaktuar kritere dhe specifikime teknike në lidhje me produktin e kërkuar, por pa përcaktuar kritere/specifikime teknike të cilat të çojnë drejt një marke të caktuar, apo që nuk ndikojnë në performancën e produktit, pasi përcaktime të tilla janë diskriminuese dhe përjashtuese nga pjesëmarrja në procedurë të operatorëve ekonomikë të interesuar. Në asnjë moment autoriteti kontraktor nuk duhet të vendose kritere apo të hartojë specifikime teknike të cilat të drejtojnë në një emër të caktuar marke apo prodhuesi, duke u bërë kështu përjashtues për operatorë të tjerë.

Përsa më sipër, pretendimi i operatorit ekonomik ankimues "PC STORE" SHPK nuk qëndron.

III.3.12.6. Nisur nga pretendimi i operatorit ekonomik ankimues, për modifikimin e specifikimeve tenike të përcaktuara në Shtojcën 6 "FORMULARI I SPECIFIKIMEVE TEKNIKE" të dokumentave të tenderit, të parashtuara në kërkesën nr. 8.4 dhe kërkesën nr. 8.5 si në vijim: **"***...Kërkesë 8.4*
Kërkojmë modifikimin e kësaj kërkese teknike dhe të vendosen si me poshtë një version më formal për tender/specifikim teknik:
"Zgjidhja duhet të mundësojë mbledhjen e log-eve të gjeneruara nga sistemet e sigurisë, sistemet e rrjetit, sistemet operative dhe aplikacionet duke përdorur protokollet e mëposhtme: Syslog, TLS Syslog, NetFloë, Ëindoës Event Forëarding, etj".
Kërkesë 8.5
Kërkojmë modifikimin e kësaj kërkese teknike dhe të vendosen si më poshtë një version më formal për tender/specifikim teknik:
*Procesi i normalizimit duhet të mbështesë llojet e mëposhtme të sintaksës: CEF, URI, SYSLOG, XML, JSON, REGEX dhe një listë çiftesh çelës-vlerë, ku log-et që përmbajnë, për shembull, "user=X" duhet të krijojnë një fushë "user" me vlerën "X".***"**, si dhe referuar shkresës nr. 1060/7 prot, datë 03.06.2026, protokolluar me tonën me nr. 1636/1 prot, datë 05.06.2026, të autoritetit kontraktor, ku ka argumentuar mospranimin e këtij pretendimi të ankimmuesit, si në vijim: "*Ndryshimi i kërkesës së përcaktuar ne Shtojcën 6 nuk mundësohet, pasi formulimi ekzistues garanton qartësi teknike, standardizim dhe përcaktim të saktë të funksionaliteteve minimale që duhet të ofrojë zgjidhja. Heqja e protokolleve specifike si IMAPS, POP3S dhe MAPI dhe zëvendësimi me termin e përgjithshem "etj." krijon pagartësi në interpretim dhe lë hapësirë për trajtime të ndryshme nga operatorët ekonomikë gjatë ofertimit.*
Kërkesa aktuale përcakton në mënyrë eksplicite protokollet që duhet të suportohen, duke siguruar që zgiidhja të jetë e aftë të mbledhë log-e edhe nga sistemet e komunikimit dhe shërbimeve email, të cilat janë komponente të rëndësishëm për monitorimin e sigurisë dhe analizën e incidenteve. Nëse këto protokolle hiqen nga kërkesa, ekziston rreziku që operatorë të ndryshëm të ofrojnë zgjidhje me nivele të ndryshme funksionaliteti, duke vështirësuar krahasimin

objektiv të ofertave dhe duke krijuar mundësi për implementim të një zgjidhjeje që nuk mbulon të gjitha nevojat operative të autoritetit kontraktor.

Gjithashtu, perdorimi i termit "etj." nuk përbën specifikim teknik të matshëm dhe mund të sjellë paqartësi gjatë fazës së implementimit dhe pranimit të sistemit, pasi nuk përcaktohen qartë standardet minimale të kërkuara. Në procedurat e prokurimit publik rekomandohet që kërkesat teknike të jenë sa më të detajuara dhe të verifikueshme, me qëllim garantimin e transparencës, konkurrencës së ndershme dhe shmangien e interpretimeve subjektive.
Për këto arsye, formulimi ekzistues duhet të mbetet i pandryshuar.

Ndryshimi i propozuar nuk mund të pranohet, pasi heqja e mbështetjes për formatin LEEF nga kërkesat e normalizimit kufizon kompatibilitetin dhe ndërveprueshmërinë e sistemit me burime të ndryshme log-esh dhe platforma SIEM/security monitoring.
Arsyetimi është si më poshtë:
Formati LEEF (Log Event Extended Format) është një standard i përdorur gjërësisht nga shumë pajisje dhe zgjidhje sigurie dhe prodhues të ndryshëm të sigurisë (si prsh, Splunk, Microsoft Sentinel, LogScale, etj).
Heqja e këtij formati nga kërkesa teknike mund të krijojë kufizime në integrimin e ardhshëm me sisteme ekzistuese ose të reja që gjenerojnë log-e në formatin LEEF.
Ruajtja e mbështetjes për LEEF nuk krijon konflikt me formatet e tjera të listuara dhe nuk ndikon negativisht në funksionalitetin e kërkuar; përkundrazi, rrit fleksibilitetin dhe shkallëzueshmërinë e zgjidhjes.
Në aspektin e konkurrencës dhe neutralitetit teknik, përfshirja e LEEF siguron që kërkesa të mos kufizojë operatorë apo produkte që përdorin këtë standard.
Heqja e një formati të mbështetur pa një arsye teknike të argumentuar bie ndesh me praktikën e ruajtjes së kompatibilitetit maksimal në sistemet e menaxhimit dhe analizës së log-eve.
Për këto arsye, formulimi ekzistues të mbetet i pandryshuar, duke ruajtur edhe mbështetjen për sintaksën LEEF.", Komisioni i Prokurimit Publik konstaton se operatori ekonomik ankimues nuk ka argumentuar teknikisht se si këto specifikime janë hartuar në kundërshtim me legjislacionin në fuqi për prokurimin publik. Gjithashtu, nuk është provuar se si këto kërkesa ngushtojnë konkurrencën apo favorizojnë një markë të caktuar. Përshkrimi i kërkesave të përgjithshme të zgjidhjes SIEM, si në vijim: "*Zgjidhja duhet të mundësojë mbledhjen e log-eve të gjeneruara nga sistemet e sigurisë, sistemet e rrjetit, sistemet operative dhe aplikacionet duke përdorur protokollet e mëposhtme: Syslog, TLS Syslog, NetFloë, Ëindoës Event Forëarding, IMAPS, POP3S, MAPI. Procesi i normalizimit duhet të mbështesë llojet e mëposhtme të sintaksës: CEF, LEEF, URI, SYSLOG, XML, JSON, REGEX dhe një listë çiftesh çelës-vlerë, ku log-et që përmbajnë, për shembull, "user=X" duhet të krijojnë një fushë "user" me vlerën "X""*", nuk përbën një markë tregtare apo specifikime teknike që të çojnë drejt një marke të caktuar tregtare,

por është një emërtim i cili përcakton kërkesat e përgjithshme që duhet të plotësojë zgjidhja SIEM. Autoriteti Kontraktor gëzon të drejtën ligjore të përcaktojë kriteret dhe specifikimet teknike sipas nevojave të tij, duke kërkuar që produktet objekt prokurimi të përmbushin standardet më të larta të cilësisë. Komisioni i Prokurimit Publik, gjykon se, autoriteti kontraktor është organi përgjegjës për procedurën e prokurimit dhe është përgjegjësi e tij të përcaktojë kritere që janë në funksion të realizimit me sukses të kontratës. Rrjedhimisht autoriteti kontraktor është në të drejtën e tij për të përcaktuar kritere dhe specifikime teknike në lidhje me produktin e kërkuar, por pa përcaktuar kritere/specifikime teknike të cilat të çojnë drejt një marke të caktuar, apo që nuk ndikojnë në performancën e produktit, pasi përcaktime të tilla janë diskriminuese dhe përjashtuese nga pjesëmarrja në procedurë të operatorëve ekonomikë të interesuar. Në asnjë moment autoriteti kontraktor nuk duhet të vendose kritere apo të hartojë specifikime teknike të cilat të drejtojnë në një emër të caktuar marke apo prodhuesi, duke u bërë kështu përjashtues për operatorë të tjerë.

Përsa më sipër, pretendimi i operatorit ekonomik ankimues "PC STORE" SHPK nuk qëndron.
Për sa më sipër, në mbështetje të neneve 30, dhe 118 të ligjit nr. 162/2020 "*Për Prokurimin Publik*", i ndryshuar, Vendimit të Këshillit të Ministrave nr. 285, datë 19.05.2021 "*Për miratimin e rregullave të prokurimit publik*", i ndryshuar, Vendimit të Këshillit të Ministrave nr. 236, datë 20.04.2023 "*Për përcaktimin e rregullave dhe tarifës së pagesës për ankimin në një procedurë prokurimi pranë Komisionit të Prokurimit Publik*", Vendimit të Komisionit të Prokurimit Publik Nr. 766/2021, datë 13.10.2021"*Për miratimin e rregullave "Për Organizimin dhe Funksionimin e Komisionit të Prokurimit Publik*", Nenit 4, të Vendimit të Komisionit të Prokurimit Publik nr. 500/2020 datë 5.11.2020 "*Rregullore për Marrjen e Masave Organizative për Ushtrimin e Veprimtarisë së Institucionit të Komisionit të Prokurimit Publik gjatë gjendjes së pandemisë së shkaktuar nga COVID -19*", Komisioni i Prokurimit Publik, njëzëri,

Vendos

1. Të mbyllë çështjen për pjesën e pranuar të ankesës së operatorit ekonomik "*PC STORE*" ShPK për procedurën e prokurimit "*E hapur, mbi kufirin e lartë monetar*", me Nr. *REF-85701-05-14-2026*, me objekt: "*Blerje suport për siem+licensa për EDR/XDR (1200 përdorues) licensa fireëall Proffesional për 4 (katër) vite*", me fond limit 63,970,667 (*gjashtëdhjetë e tre milion e nëntëqind e shtatëdhjetë mijë e gjashtëqind e gjashtëdhjetë e shtatë*) Lekë, pa TVSH ose 670,060 *(gjashtëqind e shtatëdhjetë mijë e një*) euro pa T.V.SH, parashikuar për t'u zhvilluar me datë 15.06.2026, nga autoriteti kontraktor Posta Shqiptare SHA.

2. Të pranojë pjesërisht ankesën e operatorit ekonomik "PC STORE" ShPK për procedurën e prokurimit "*E hapur, mbi kufirin e lartë monetar*", me Nr. *REF-85701-05-14-2026*, me

objekt: "*Blerje suport për siem+licensa për EDR/XDR (1200 përdorues) licensa fireëall Proffesional për 4 (katër) vite*", me fond limit 63,970,667 (*gjashtëdhjetë e tre milion e nëntëqind e shtatëdhjetë mijë e gjashtëqind e gjashtëdhjetë e shtatë*) Lekë, pa TVSH ose 670,060 *(gjashtëqind e shtatëdhjetë mijë e një*) euro pa T.V.SH, parashikuar për t'u zhvilluar me datë 15.06.2026, nga autoriteti kontraktor Posta Shqiptare SHA.

3. Autoriteti kontraktor të publikojë të gjitha ndryshimet dhe sqarimet në Sistemin Elektronik të Prokurimeve.

4. Autoriteti kontraktor, brenda 5 ditëve, të vërë në dijeni Komisionin e Prokurimit Publik për zbatimin e këtij vendimi.

5. Ngarkohet zyra e financës që të bëjë kthimin e tarifës financiare të paguar nga operatori ekonomik ankimues "*PC STORE*" ShPK.

6. Kundër këtij vendimi, mund të bëhet ankim në Gjykatën Administrative të Apelit.

7. Kopje e këtij vendimi i dërgohet për njoftim Agjencisë së Prokurimit Publik.

Ky vendim hyn në fuqi menjëherë.

KOMISIONI I PROKURIMIT PUBLIK

Anëtar	**Anëtar**	**Anëtar**
Anila Malaj	**Kreshnik Ternova**	**Gjergj Mersini**

Nënkryetar
Fiorent Zguro