CONSILIUL NAȚIONAL DE SOLUȚIONARE A CONTESTAȚIILOR

C.N.S.C.

Str. Stavropoleos nr.6, Sectorul 3, București, România, CP 030084, CIF 20329980
Tel. +4 021 3104641 Fax. +4 021 3104642 Fax. +4 021 8900745 www.cnsc.ro

În conformitate cu prevederile art. 12 alin. (1) și ale art. 27 alin. (1) din Legea nr. 101/2016 privind remediile și căile de atac în materie de atribuire a contractelor de achiziție publică, a contractelor sectoriale și a contractelor de concesiune de lucrări și concesiune de servicii, precum și pentru organizarea și funcționarea Consiliului Național de Soluționare a Contestațiilor, Consiliul adoptă următoarea

DECIZIE
Nr. ...
Data: ...

Prin contestația nr. ..., transmisă prin mijloace electronice (e-mail) și ulterior prin poștă, înregistrată la Consiliu sub nr. ... și respectiv sub nr. ..., ..., cu sediul în ..., înregistrată la Oficiul Registrului Comerțului sub nr. ..., având CIF RO ..., reprezentată legal prin administrator ..., a contestat adresa nr. ... reprezentând comunicarea rezultatului procedurii de atribuire prin „licitație deschisă", online, cu etapă finală de licitație electronică, a contractului de achiziție publică, având ca obiect „Furnizare echipamente de rețea", **lot 1** – „Echipamente de rețea – routere", cod CPV 32420000-3 (Rev.2) inițiată de ..., în calitate de autoritate contractantă, cu sediul în ... și a solicitat următoarele:

- anularea adresei nr. ... și a măsurii dispuse și comunicate pe calea acesteia, respectiv respingerea ofertei contestatoarei;
- anularea oricăror acte subsecvente actului atacat;
- obligarea autorității contractante la reevaluarea ofertei contestatoarei ca urmare a admiterii capetelor de cerere precedente.

CONSILIUL NAȚIONAL DE SOLUȚIONARE A CONTESTAȚIILOR,
asupra cauzei de față, constată următoarele:

În susținerea contestației, autoarea acesteia arată că prin adresa nr. ... i s-a comunicat că oferta sa a fost declarată neconformă în baza prevederilor art. 137 alin. (3) lit. a) din HG nr. 395/2016.

În cele ce urmează ... susține că motivul de respingere a ofertei sale potrivit căruia *„oferta tehnică nu îndeplinește cerințele tehnice*

minimale din caietul de sarcini, respectiv întreagă telemetrie de rețea și de la nivelul stațiilor de lucru, se colectează dar nu se corelează și nu afișează într-o singură consolă de incidente, iar datorită faptului că logurile provenite de la echipamentele ... ofertate, nu ajung la modulul ..., aceste log-uri nu beneficiază de funcțiile matematice avansate de tip «unsupervised machine learning»" este nereal și denotă faptul că membrii comisiei de evaluare nu au înțeles/nu au studiat suficient documentația tehnică pusă la dispoziție de ofertant și răspunsul la solicitările de clarificare transmise. Astfel, colectarea și corelarea centralizată a întregii telemetrii la nivel de rețea la nivelul echipamentelor celor doi producători (... și ...) se va face prin protocolul .... va colecta prin ... log-urile, atât de la echipamentele ..., cât și de la ..., și/sau alte eventuale echipamente din rețea și le va afișa pe o singură consolă de incidente.

De asemenea, contestatoarea menționează că ..., ca parte din ... este un sistem de monitorizare cuprinzător pentru o rețea care integrează și corelează date în timp real și istorice într-o singură vizualizare. Poate loga și monitoriza amenințările la adresa rețelelor, filtrează date pe mai multe nivele, ține evidența activității administrative și multe altele.

Totodată, ... subliniază că ... permite utilizarea de mai multe filtre în console, permițând îngustarea vederii la un anumit moment, prin ID-ul utilizatorului sau prin adresa IP locală, prin aplicație și altele. Poate fi utilizată pentru a investiga activitatea de trafic, cum ar fi încărcările/descărcările de utilizatori sau videoclipurile vizionate pe YouTube într-un grup de utilizatori la nivel de rețea sau la nivel de utilizator individual. Prezintă informații, atât în format text, cât și vizual. Pot fi vizualizate rezumatele datelor din jurnal în ..., cum ar fi cele mai importante amenințări la adresa unei rețele, sursele de trafic de rețea de vârf și destinațiile de top ale traficului din rețea. În funcție de rezumatul care este vizualizat, pot fi urmărite informații sumare în diferite formate: tabel, balon, hartă sau țiglă. Pentru fiecare vizualizare sumară, pot fi detaliate informațiile.

Mai mult decât atât, contestatoarea precizează că ... permite o prezentare generală a celor mai utilizate moduri de vizualizare și corelarea telemetriei de rețea. Fiecare vizualizare sumară este un widget. Pot fi configurate setările de vizualizare pentru fiecare widget, inclusiv adăugarea aceluiași widget de mai multe ori, fiecare afișând o vizualizare diferită. De exemplu, pot fi adăugate două widget-uri de tip Top Threats: unul care afișează vizualizarea Top 10 Threats într-o diagramă cu bule, iar cealaltă arată cele 20 de amenințări de top dintr-un tabel. Pentru a vedea detaliile fiecărei vizualizări rezumate, poate fi detaliată fiecare vizualizare sumară sau poate fi utilizat meniul copac pentru a vizualiza o pagină individuală.

... mai arată că potrivit documentației tehnice ce se regăsește la adresa ..., începând cu pagina 68, produsul ... permite afișarea într-o singură consolă de incidente a cel puțin următoarelor vizualizări:

Categorie	**Tip afișare**	**Descriere**
Rezumat	Privire de ansamblu	O prezentare generală a celor mai utilizate vizualizări rezumate .... Puteți selecta ce widgeturi să fie afișate în rezumat.
Amenințări	Clasament amenințări	Listează amenințările de top pentru rețea. Următoarele incidente sunt considerate amenințări: 1. Aplicații de risc detectate de controlul aplicațiilor. Incidentele de intruziune detectate de IPS. Site-uri web malițios intenționate detectate prin filtrarea pe web. Malware/botnets detectate de antivirus.
	Harta amenințărilor	Afișează o hartă a lumii care arată culoarea cea mai de sus țintă a destinației de trafic. Amenințările sunt afișate atunci când nivelul este egal sau mai mare decât avertismentul și sursa IP este o adresă IP publică. Lista de amenințări din partea de jos indică locația, amenințarea, gravitatea și timpul atacurilor. Gradientul de culoare al săgeților pe hartă indică riscul de trafic, unde roșu indică riscul mai critic.
	Gazda compromisă	Afișează utilizatorii finali cu compromisuri suspecte de utilizare a paginilor web, inclusiv adresele IP ale utilizatorilor finali, evaluarea generală a amenințărilor și numărul de amenințări.
	Detectarea FortiSandbox	Afișează un rezumat al detectărilor legate de FortiSandbox. Se afișează următoarele informații: Numele fișierului Utilizator final și / sau IP Destinație IP Analiza (Evaluare curată, suspectă sau rău intenționată) 1 Acțiune (Pasul, Blocat, etc.) Serviciu (HTTP, FTP, SMTP, etc.)
Trafic	Clasament surse de trafic	Afișează cel mai mare trafic de rețea prin adresa IP a sursei și interfața, dispozitivul, scorul de pericol (blocat și permis), sesiunile (blocate și permise) și octeți (trimise și primite).
	Clasament destinații	Afișează traficul de rețea cel mai mare după adresele IP destinație, aplicațiile utilizate pentru a accesa destinația, sesiunile și octeții. Dacă este disponibil, dați clic pe pictograma de lângă adresa IP pentru a vedea informațiile WHOIS.
	Clasament țări	Afișează cel mai mare trafic de rețea în funcție de țară în ceea ce privește sesiunile de trafic, inclusiv destinația, scorul de

		pericol, sesiunile și octeții.
	Politici de securitate	Afișează încălcările de politică după nume politică, nume dispozitiv, VDOM, număr de accesări, octeți și data și ora ultimei utilizări.
Aplicații și site-uri web	Clasament aplicații	Afișează aplicațiile de top utilizate în rețea, inclusiv numele aplicației, categoria, nivelul de risc, numărul de clienți, sesiunile blocate și permise și octeți trimise și primite
	Clasament aplicații de tip Cloud	Afișează aplicațiile de top din cloud folosite în rețea.
	Clasament site-uri web	Afișează site-urile web permise și blocate în rețea. Puteți vizualiza informații pe domenii sau categorii utilizând opțiunile din partea dreaptă sus din bara de instrumente.
	Clasament utilizatori	Afișează utilizatorii de top, inclusiv sursa, grupul, numărul de site-uri vizitate, timpul de navigare și numărul de octeți trimise și primite.
VPN	SSL și Dialup IPsec	Afișează utilizatorii care accesează rețeaua utilizând următoarele tipuri de securitate pe un tunel de rețea privată virtuală (VPN): straturi socket securizate (SSL) și securitate IPsec (Internet Protocol Security). Puteți vizualiza traficul VPN pentru un anumit utilizator din vizualizările de sus și din vizualizările derulate. În vizualizarea de sus, faceți dublu clic pe un utilizator pentru a vedea traficul VPN pentru utilizatorul respectiv. În vizualizarea drilldown, dați clic pe o intrare din tabel pentru a afișa jurnalele de trafic care se potrivesc cu utilizatorul VPN și cu destinația.
	Site-to-Site IPsec	Afișează numele de tuneluri VPN cu securitatea protocolului Internet (IPsec) care accesează rețeaua.
Wi-Fi	AP de tip Rogue	Afișează identificatorii setului de servicii (SSID) de puncte de acces neautorizate WiFi din rețea.
	AP autorizate	Afișează numele punctelor de acces WiFi autorizate în rețea.
	SSID-uri autorizate	Afișează identificatorii setului de servicii (SSID) din punctele de acces WiFi autorizate din rețea.
	WiFi Clients	Listează numele și adresele IP ale dispozitivelor înregistrate în rețeaua WiFi.
Sistem	Admin Logins	Afișează utilizatorii care au accesat dispozitivul gestionat.
	Evenimente de sistem	Afișează evenimentele pe dispozitivul gestionat.
	Utilizarea resurselor	Afișează procesorul dispozitivului, memoria, înregistrarea și alte informații despre performanță pentru dispozitivul gestionat.
	Autentificare	Afișează adresele IP ale utilizatorilor care nu

	nereușită	au reușit să se conecteze la dispozitivul „Attempts managed”.
Client final	Clasament vulnerabilități	Afișează informații despre vulnerabilitatea punctelor finale ... înregistrate la anumite dispozitive .... Vizualizați după dispozitiv sau Vulnerabilitate. În ecranul Dispozitiv, tabelul prezintă dispozitivul, sursa, numărul și severitatea vulnerabilităților și categoria. În vizualizarea Vulnerabilitate, selectați tabelul sau formatul bulelor. Formatul tabelului prezintă numele vulnerabilității, severitatea, categoria, codul CVE și numărul de gazde. Formatul graficului cu bule arată vulnerabilitatea după severitate și frecvență.
	Clasament amenințări	Afișează amenințările de vârf pentru obiectivele ... înregistrate, inclusiv amenințarea, nivelul de amenințare și numărul de incidente (blocate și permise).
	Clasament aplicații	Afișează aplicațiile de vârf utilizate de către obiectivele înregistrate ..., inclusiv numele aplicației, nivelul de risc, sesiunile blocate și permise, și octeții trimise și primite.
	Clasament site-uri web	Afișează site-urile Web permise și blocate în rețea.

În cele ce urmează, contestatoarea invocă și redă art. 215 alin. (5) din Legea nr. 98/2016, subliniind că a indicat, atât în propunerea sa tehnică, cât și prin răspunsul la solicitările de clarificări, cum anume sunt îndeplinite cerințele documentației de atribuire.

În vederea soluționării contestației formulată de ..., Consiliul, prin adresa nr. ..., în temeiul art. 61^1 din Legea nr. 101/2016, modificată și completată prin OUG nr. 45/2018, a solicitat contestatoarei să transmită, în termen de 3 zile de la data primirii adresei, sub sancțiunea respingerii contestației ca inadmisibilă, recipisa de consemnare a cauțiunii, în original, în cuantumul prevăzut de lege, cu precizarea că modalitatea de constituire a cauțiunii se va face conform art. 1057 din Codul de procedură civilă, coroborat cu art. 68 din Legea nr. 101/2016 la CEC Bank - S.A., Trezoreria Statului sau la orice altă instituție de credit care efectuează astfel de operațiuni, pe numele părții respective, la dispoziția CNSC.

De asemenea, Consiliul a solicitat, înaintarea contestației, în original.

Prin corespondența înregistrată la CNSC sub nr. ..., contestatoarea a confirmat primirea adresei nr. ....

Prin corespondența înregistrată la CNSC sub nr. ..., ... a solicitat următoarele: *„vă rog să ne confirmați că putem constitui cauțiunea prin instituțiile financiare non-bancare (IFN-uri înscrise în registrul BNR) care*

au dreptul de a emite scrisori de garanție care sunt considerate «instrumente financiare care pot servi ca instrumente de plată»".

Prin adresa nr. ..., Consiliul a adus la cunoștință contestatoarei dispozițiile art. 1058 din Codul de Procedură Civilă. De asemenea, i-a solicitat ..., ca aceasta să se conformeze solicitărilor din cadrul adresei CNSC nr. ..., încadrându-se în termenul acordat prin aceasta.

Prin corespondența înregistrată la CNSC sub nr. ..., contestatoarea a confirmat primirea adresei nr. ....

Prin adresa nr. ..., înregistrată la CNSC sub nr. ..., autoritatea contractantă arată că nu este de acord cu solicitarea formulată de către ..., respectiv constituirea cauțiunii prin instituții financiare non-bancare.

Prin adresa nr. ..., înregistrată la Consiliu sub nr. ..., ... a comunicat, în original, recipisa de consemnare nr. ... din 29.07.2019, emisă de CEC Bank – ..., în valoare de 83.121 lei.

Prin adresa nr. ..., depusă în original la registratura CNSC, înregistrată la Consiliu sub nr. ..., ... a înaintat punctul său de vedere referitor la contestația formulată de către ..., o parte din dosarul achiziției publice și oferta depusă de ....

Autoritatea contractantă prezintă un scurt istoric al procedurii, precum și echipamentele ofertate de contestatoare, concluzionând că aceasta a ofertat o soluție folosind strategia dual-vendor, deci conform caietului de sarcini propunerea tehnică trebuie să îndeplinească cerința potrivit căreia: *„În cazul în care ofertantul propune o soluție folosind strategia dual-vendor, atunci se acceptă o singură soluție de management și corelare de evenimente. Soluția de management și corelare va trebui să absoarbă și să coreleze datele expuse de toate echipamentele*". Ori, întrucât din propunerea tehnică prezentată de ... nu rezultă faptul că soluția de management și corelare ofertată, respectiv ..., absoarbe și corelează datele expuse de toate tipurile de echipamente ofertate (... și ...) comisia de evaluare a solicitat o serie de clarificări.

În cele ce urmează, ... redă întrebarea nr. 6 din clarificarea nr. ... și răspunsul contestatoarei la acesta din cadrul adresei nr. ..., concluzionând că răspunsul ... conține explicații referitoare la stațiile de lucru protejate de echipamentele ... și la stațiile de lucru neprezente în organizație, însă nu conține explicații legate de stațiile de lucru protejate de echipamentele .... Componenta EMS poate fi utilizată numai împreună cu echipamentele ..., așa cum specifică producătorul ... în documentația oficială, care se regăsește la adresa: ..., Ori, ofertantul răspunde doar la prima parte a solicitării, referitoare la motorul de filtrare web, însă nu menționează nimic referitor la cerința ca întreaga telemetrie la nivel de rețea și de la nivelul stațiilor de lucru, să se colecteze, coreleze și să se afișeze într-o singură consolă de incidente.

De asemenea, autoritatea contractantă redă întrebarea nr. 7 din solicitarea de clarificări nr. ... și răspunsul contestatoarei la acesta din

cadrul adresei nr. ..., subliniind că ... doar precizează cum se integrează echipamentele ..., fără a menționa cum sunt integrate, ca un tot unitar și echipamentele .... Ori, prin caietul de sarcini se solicită corelarea datelor de la toate echipamentele, pentru a minimiza riscurile în cazul unui atac cibernetic, însă contestatoarea indică doar modul în care se corelează doar datele de la echipamentele ....

Totodată, ... redă întrebarea nr. 8 din solicitarea de clarificări nr. ..., precum și răspunsul contestatoarei la acesta din cadrul adresei nr. ..., susținând că ... nu detaliază modul în care sunt colectate logurile și modalitatea prin care acestea sunt procesate și îmbogățite. Mai mult, nu detaliază modalitatea prin care soluția propusă oferă funcții de căutare avansată și rapidă, precum și capabilități de identificare de anomalii, folosind algoritmi și funcții matematice avansate de tip „unsupervised machine learning".

În plus, autoritatea contractantă redă întrebarea nr. 4 din clarificarea nr. ..., precum și răspunsul contestatoarei la acesta din conținutul adresei nr. ..., arătând că în referința tehnică precizată de ..., producătorul declară că logurile de tip ... sunt tratate ca loguri de tip generic. Ori, conform producătorului, acest tip de loguri nu sunt afișate pe consola de incidente numită .... În acest sens, ... face trimitere la referința tehnică de la adresa: ...

Cu privire la răspunsul contestatoarei din conținutul adresei nr. ... la solicitarea de clarificări nr. ..., ... subliniază că potrivit afirmațiilor ..., echipamentele ... ..., ...with firepower services, ...with firepower services suportă logarea către un server de ..., prin urmare se pot integra cu ... VM, dar conform caietului de sarcini, aceste loguri trebuie să ajungă în consola unică de incidente, denumită ... de către producător. Ori, la adresa de referință ..., în tabelul de la paginile 13-14, producătorul specifică faptul că logurile provenite prin protocolul ... de la echipamentele ..., nu beneficiază de facilitatea ... din ..., prin urmare aceste loguri nu pot fi corelate cu logurile provenite de la echipamentele ....

În altă ordine de idei, autoritatea contractantă subliniază că ..., așa cum este descris și în contestație, expune câteva detalii ale stațiilor de lucru prin folosirea agentului ... și anume: Clasament (top) vulnerabilități, clasament (top) amenințări, Clasament (top) aplicații, Clasament (top) site-uri web; clasamentele top dau o vedere generală de ansamblu a amenințărilor dar nu oferă capabilitatea de a urmări care a fost prima victimă, propagarea în rețea de la o stație de lucru la alta, așa cum este cerut în specificații. De asemenea, cerința trebuie să coreleze evenimente de pe stațiile de lucru, nu doar vulnerabilități, amenințări, aplicații și site-uri web. Ori, un eveniment care este relevant într-un incident de securitate este spre exemplu și execuția rău intenționată pe stația de lucru, a aplicației legitime powershell. Totodată, se poate răspândi un incident de la o stația de lucru la alta prin rețea, folosind doar comenzi powershell, riscul major fiind să nu apară în Top

Amenințări sau Top Vulnerabilități sau să nu apară deloc. Aceasta este motivația prin care evenimentele înseamnă mai mult decât amenințări sau vulnerabilități.

În plus, ... arată că nu este menționat nicăieri în documentația ... cum se asociază evenimentele (folosind aceeași terminologie) de la terminalele mobile. Susținerea cerințelor de a corela evenimentele de pe stațiile de lucru ce nu țin neaparat de detecția de malware, sunt descrise în caietul de sarcini. Cerința cu privire la acest aspect menționează explicit corelarea de evenimente care nu au neaparat legătură cu vulnerabilități, amenințări, aplicații sau site-uri web, ci cu modalități de a urmări comportamentul rău intenționat evidențiat prin evenimente corelate în ordine cronologică, atât pe stațiile de lucru, terminale mobile și tranzit logat din rețea.

În acest sens, autoritatea contractantă precizează că nu regăsește în documentația ... modalitatea prin care se face detecția de comportament de „dropper" nici modalitatea de legare a fiecărei tranzacții făcute către internet, de procesul de pe stația de lucru care a generat traficul.

... mai arată că din motivele de mai sus este necesară a treia cerință, anume să furnizeze *„funcții de căutare avansată și rapidă, precum și capabilități de identificare de anomalii, folosind algoritmi și funcții matematice avansate de tip «unsupervised machine leaning». Soluția propusă va permite interacțiunea cu alte aplicații de management sau de producție prin intermediul tehnologiilor RESTfull API și JSON. Soluția va folosi o bază de date distribuită care să permită căutarea în timp real, vizualizarea, raportarea și stocarea istorică a log-urilor pe o perioadă de 30 de zile cu posibilitate de extindere la 90 de zile*".

În acest sens, autoritatea contractantă arată că ia în calcul riscul de a fi ținta unor atacuri personalizate, care pot depăși inclusiv mecanismele de protecție și detecție descrise mai sus, iar a căror detecție să poată fi posibilă prin analiza în timp a logurilor de către algoritmi matematici avansați. Ori, nu a regăsit în documentație funcțiile de unsupervised machine learning implimentate în ... sau .... De asemenea, nu regăsește în documentație detalii despre analiza funcțiilor matematice, prin care să se confirme că aceasta folosește datele absorbite prin ... de ambii producători.

Prin adresa nr. ..., înregistrată la CNSC sub nr. ..., autoritatea contractantă a înaintat documente în completarea dosarului achiziției.

Prin adresa nr. ..., Consiliul a solicitat ... eventuale susțineri cu privire la punctul de vedere al autorității contractante.

Prin corespondența înregistrată la CNSC sub nr. ..., contestatoarea a confirmat primirea adresei nr. ....

Prin corespondența înregistrată la CNSC sub nr. ... transmisă prin mijloace electronice (e-mail), autoritatea contractantă a înaintat un set de documente analizate de aceasta în evaluarea ofertei contestatoarei.

Prin adresa nr. ..., înregistrată la Consiliu sub nr. ..., autoritatea contractantă a remis Consiliului documentele transmise în format electronic la data de 08.08.2019.

Din documentele depuse la dosarul cauzei și din susținerile părților, Consiliul constată următoarele:

..., în calitate de autoritate contractantă, a organizat procedura de atribuire prin „licitație deschisă" online, cu etapă finală de licitație electronică, a contractului de achiziții publice, având ca obiect „Furnizare echipamente de rețea", **lot 1** – „Echipamente de rețea – routere", cod CPV 32420000-3 (Rev.2), prin publicarea în SEAP a anunțului de participare nr. ... stabilind termenul limită pentru primirea ofertelor la 30.10.2018, criteriul de atribuire „cel mai bun raport calitate-preț" și valoarea estimată de 5.159.040 lei, fără TVA.

În cadrul procedurii de atribuire în cauză, lotul nr. 1, au fost depuse trei oferte așa cum rezultă din Procesul-verbal nr. ... al ședinței de vizualizare a ofertelor și din Declarația de participare nr. ... întocmită de autoritatea contractantă conform dispozițiilor art. 63 alin. (2) din Legea nr. 98/2016.

Prin Procesul verbal nr. ..., Comisia de evaluare a respins ca neconformă oferta depusă de ...(fosta ...) în cadrul lotului 1, acest aspect regăsindu-se și în Raportului procedurii nr. ... aferent lotului nr. 1, prin care a fost declarată câștigătoare oferta depusă de ....

Prin adresa nr. ..., autoritatea contractantă a comunicat ofertantului ...(fosta ...) respingerea ofertei acestuia, „în baza art. 137 alin. (3) lit. a) din HG nr. 395/2016 întrucât nu satisface în mod corespunzător cerințele caietului de sarcini".

Nemulțumită de decizia autorității, ...a transmis Consiliului prin mijloace electronice (e-mail) și prin poștă, contestația care formează obiectul prezentului dosar.

...a prezentat Consiliului recipisa de consemnare a cauțiunii nr. ... din data de 29.07.2019 în valoare de 83.121 RON, eliberată de CEC BANK – Sucursala ....

Cauțiunea se va restitui contestatoarei în condițiile stipulate de art. 1.064 C. proc. civ. [*„(1) Cauțiunea depusă se va restitui, la cerere, după soluționarea prin hotărâre definitivă a procesului în legătură cu care s-a stabilit cauțiunea, respectiv după încetarea efectelor măsurii pentru care aceasta s-a depus. (2) Cauțiunea se restituie celui care a depus-o în măsura în care asupra acesteia cel îndreptățit nu a formulat cerere pentru plata despăgubirii cuvenite până la împlinirea unui termen de 30 de zile de la data rămânerii definitive a hotărârii sau, după caz, de la data încetării efectelor măsurii, prevăzute la alin. (1). Cu toate acestea, cauțiunea se restituie de îndată dacă partea interesată declară în mod expres că nu urmărește obligarea celui care a depus-o la despăgubiri pentru prejudiciile cauzate prin încuviințarea măsurii pentru care aceasta*

s-a depus"], coroborate cu dispozițiile art. 61^1 alin. (5), (6) și (7) din Legea nr. 101/2016, cu modificările și completările ulterioare [*„(5) Cauțiunea depusă se restituie, la cerere, după soluționarea prin hotărâre definitivă a plângerii, respectiv după încetarea efectelor suspendării procedurii de atribuire şi/sau a executării contractului. (6) Cauțiunea se restituie celui care a depus-o, nu mai devreme de 30 de zile de la data rămânerii definitive a hotărârii sau, după caz, de la data încetării efectelor suspendării procedurii de atribuire şi/sau a executării contractului. (7) Consiliul sau instanța, după caz, se pronunță asupra cererii de restituire a cauțiunii cu citarea părților, printr-o încheiere supusă numai recursului la instanța ierarhic superioară. Recursul este suspensiv de executare*"].

Pe fondul cauzei, Consiliul reține că prin adresa nr. ..., autoritatea contractantă a comunicat contestatoarei faptul că oferta acesteia a fost declarată neconformă în baza art. 137 alin. (3) lit. a) din HG nr. 395/2016 – *„propunerea tehnică nu satisface în mod corespunzător cerințele caietului de sarcini"* deoarece *„în urma verificării răspunsului (...) la solicitarea de clarificări nr. ..., comisia de evaluare a constatat că oferta tehnică nu îndeplinește cerințele minime din caietul de sarcini, respectiv întreaga telemetrie la nivel de rețea și de la nivelul stațiilor de lucru, se colectează dar nu se corelează și nu se afișează într-o singură consolă de incidente, iar datorită faptului că logurile provenite de la echipamentele ... ofertate, nu ajung în modulul ..., aceste loguri nu beneficiază de funcțiile matematice avansate de tip «unsupervised machine lerning»".*

Analizând prevederile caietului de sarcini (punctul 2.2 – Obiectul achiziției), Consiliul reține că în cadrul lotului 1 autoritatea contractantă urmărește achiziționarea următoarelor Echipamente de rețea - Router

- Echipamente de rețea tip 1 - 4 bucăți;
- Echipamente de rețea tip 2 – 46 bucăți;
- Echipamente de rețea tip 3 – 96 bucăți;
- Echipamente de rețea tip 4 – 34 bucăți.

În cadrul Capitolului 3 – Descrierea echipamentelor solicitate, respectiv punctele 3.3.1.1, 3.3.1.2, 3.3.1.3 și 3.3.1.4 se regăsesc specificațiile tehnice și cerințele specifice aferente fiecărui tip de echipament de rețea de tip 1, 2, 3 și 4. Pentru fiecare echipament, la caracteristica „Management", sunt inserate 3 note cu conținut identic, **Nota nr. 2** precizând următoarele:

„În cazul în care ofertantul propune în cadrul ofertei pentru întreg lotul 1 mai multe echipamente de la același producător se acceptă o singură soluție de management și monitorizare pentru toate echipamentele care provin de la același producător. În cazul în care ofertantul propune o soluție folosind strategia dual-vendor, atunci este acceptată o singura soluție de management și corelare de evenimente.

Soluția de management și corelare va trebui să absoarbă și să coreleze datele expuse de toate echipamentele".

De asemenea, analizând conținutul Caietului de sarcini, Consiliul reține că la punctul 3.3.1.5 – „Cerințe de management, integrare, automatizare, corelare evenimente și loguri" – Cerințe generale, se regăsesc următoarele mențiuni: *„În cazul ofertelor ce conțin strategia dual-vendor, se cere ca întreaga telemetrie la nivel de rețea și de la nivelul stațiilor de lucru, să se colecteze, coreleze și să se afișeze într-o singură consolă de incidente. Pentru implementarea acestei strategii, ofertantul poate folosi tehnologii de partajare de date specifice sau cunoscute după cum urmează: REST-API, Netflow, ... (...) Soluția trebuie să furnizeze funcții de căutare avansată și rapidă, precum și capabilități de identificare de anomalii, folosind algoritmi și funcții matematice avansate de tip «unsupervised machine learning», toate descrise mai jos".*

În cadrul Fișei de date a achiziției, Consiliul reține că la punctul IV.4.1 *Modul de prezentare al propunerii tehnice*, autoritatea contractantă a menționat următoarele:

„Propunerea tehnică se va prezenta la rubrica special prevăzută în S.E.A.P. în acest sens, respectiv «Documente de calificare și propunere tehnică».

Propunerea tehnică va fi întocmită în conformitate cu solicitările din caietul de sarcini, acestea fiind considerate minime și obligatorii și va fi structurată în conformitate cu Formularul 10 – Formular de Ofertă Tehnică, din cadrul secțiunii Formulare.

În cadrul propunerii tehnice se va face dovada conformității produselor care urmează să fie livrate, cu cerințele Caietului de sarcini.

În acest scop, propunerea tehnică va conține un comentariu, articol cu articol, privind toate cerințele conținute în Caietul de sarcini, prin intermediul cărora ofertantul va demonstra corespondența propunerii tehnice cu prevederile caietului de sarcini - se va elabora, în acest sens, o matrice de corespondență, în format digital editabil (semnată cu semnătură electronică) conținând următoarele coloane:

- Nr. crt.;

- Cerința din Caietul de sarcini (Descriere și Referință);

- Specificație ofertată (Descriere și Referință);

- Observații (dacă este cazul);

Se solicită descrierea detaliată a modului de îndeplinire a cerințelor minime prevăzute în caietul de sarcini, prin care să se demonstreze corespondența propunerii tehnice cu toate cerințele prevăzute.

Pentru a demonstra că propunerea tehnică depusă respectă cerințele minime din caietul de sarcini, se vor descrie în detaliu:

- toate informațiile din care să se poată aprecia dacă sunt îndeplinite cerințele din caietul de sarcini;

- alte informații considerate semnificative pentru evaluarea corespunzătoare a propunerii tehnice.

Nu se admite prezentarea pe post de propunere tehnică a caietului de sarcini semnat/ștampilat de ofertant, iar comentariile de tipul DA/NU nu reprezintă îndeplinirea cerințelor solicitate, ***sub sancțiunea declarării propunerii tehnice ca fiind neconformă.***

Nerespectarea tuturor cerințelor tehnice minimale obligatorii sau a altor cerințe obligatorii, atrage automat declararea ofertei ca fiind neconformă în temeiul prevederilor art. 137 alin (3), lit. a) din HG 395/2016, cu modificările și completările ulterioare.

Documentele propunerii tehnice trebuie redactate într-o manieră organizată, astfel încât, în procesul de evaluare a ofertelor, să permită identificarea facilă a corespondenței informațiilor cuprinse în ofertă cu cerințele caietului de sarcini.

Ofertanții și, dacă este cazul, subcontractanții, au obligația de a prezenta o Declarație pe proprie răspundere din care să rezulte că la elaborarea ofertei au ținut cont de obligațiile relevante din domeniile mediului, social și al relațiilor de munca, așa cum sunt acestea indicate la art. 51 alin (1) din Legea 98/2016. De asemenea, în această declarație se va menționa că se vor respecta condițiile de mediu, social și cu privire la relațiile de muncă pe toată durata de îndeplinire a contractului de furnizare de produse. (...) Propunerea tehnică și toate documentele ofertei se vor redacta și prezenta în limba română.

Ofertanții au obligația de a verifica, înainte de încărcarea în SEAP a fișierului/fișierelor reprezentând Propunerea tehnică, dacă acestea se deschid și dacă sunt vizibile. În cazul în care documentele încărcate, în fișierul având denumirea Propunere Tehnică, nu sunt vizibile sau nu conțin informațiile aferente propunerii tehnice, întocmită pe baza cerințelor din caietul de sarcini, oferta va fi respinsă.

Ofertantul nu are dreptul de a completa propunerea tehnică cu alte documente, după data limita de depunere a ofertelor, cu excepția situațiilor prevăzute la art. 134 alin. (7) din HG 395/2016, cu modificările și completările ulterioare. (...)".

Analizând propunerea tehnică a ofertantei contestatoare, Consiliul reține următoarele:

- pentru echipamentele de rețea de tip 1, a ofertat echipamentul ... ...;
- pentru echipamentele de rețea de tip 2, a ofertat echipamentul ... ...
- pentru echipamentele de rețea de tip 3, a ofertat echipamentul ... ...with Firepower Services;
- pentru echipamentele de rețea de tip 4, a ofertat echipamentul ...-Xwith Firepower Services;

Propunerea tehnică a fost prezentată de ofertant sub forma unui tabel cu patru coloane intitulate „Cerințe", „Detalii cerințe", „Conformitate" și „Răspuns ofertant", pentru fiecare echipament de rețea ofertat (tip 1, 2, 3 și 4), ofertanta contestatoare indicând linkurile cu referințele tehnice.

Raportat la cerințele caietului de sarcini, reproduse la pag. 11 – 12 a prezentei decizii, în cadrul propunerii tehnice, ofertanta contestatoare a menționat, la pag. 12, 23, 36 și 49 [pentru fiecare echipament de rețea ofertat (tip 1, 2, 3 și 4)], în referire la Nota nr. 2 având următorul cuprins: *„În cazul în care ofertantul propune în cadrul ofertei pentru întreg lotul 1 mai multe echipamente de la același producător se acceptă o singură soluție de management și monitorizare pentru toate echipamentele care provin de la același producător. În cazul în care ofertantul propune o soluție folosind strategia dual-vendor, atunci este acceptată o singura soluție de management și corelare de evenimente. Soluția de management și corelare va trebui să absoarbă și să coreleze datele expuse de toate echipamentele”,* următoarele: „Soluția de management permite corelarea evenimentelor precum și absorbirea datelor expuse de toate echipamentele ofertate”.

În referire la cerința: *„În cazul ofertelor ce conțin strategia dual-vendor, se cere ca întreaga telemetrie la nivel de rețea și de la nivelul stațiilor de lucru, să se colecteze, coreleze și să se afișeze într-o singură consolă de incidente. Pentru implementarea acestei strategii, ofertantul poate folosi tehnologii de partajare de date specifice sau cunoscute după cum urmează: REST-API, Netflow, ...”,* ofertanta contestatoare a menționat în propunerea tehnică (pag. 53) următoarele: *„Întreaga telemetrie la nivel de rețea și la nivelul stațiilor de lucru, colectează, corelează și va afișa într-o singură consolă de incidente. Acest lucru se va realiza prin folosirea tehnologiilor de partajare a datelor specifice sau cunoscute după cum urmează: REST-API, Netflow, ...”*, iar în referire la cerința: *„Soluția trebuie să furnizeze funcții de căutare avansată și rapidă, precum și capabilități de identificare de anomalii, folosind algoritmi și funcții matematice avansate de tip «unsupervised machine learning», toate descrise mai jos”,* ofertanta contestatoare a menționat în propunerea tehnică, tot la pag. 53, următoarele: *„Soluția furnizează funcții de căutare avansată și rapidă, precum și capabilități de identificare de anomalii, folosind algoritmi și funcții matematice avansate de tip «unsupervised machine learning», toate descrise mai jos”.*

Din verificarea propunerii tehnice a contestatoarei, pag. 51, punctul 3.3.1.5 – Cerințe de management, integrare, automatizare, corelare și loguri (pag. 51) rezultă că soluția ofertată este ... ...-VM, pentru care s-a depus și specificația tehnică (pag. 13 – 7).

Verificând lucrările membrilor Comisiei de evaluare, Consiliul reține că aceștia au solicitat contestatoarei clarificări, prin adresa **nr. ...,** relevante în soluționare fiind următoarele aspecte:

*„**6.** În cadrul capitolului cap.3.3.1.5. INTEGRARE, AUTOMATIZARE, CORELARE, **vă rugăm să detaliaţi îndeplinirea următoarelor cerinţe:***

- «Motorul de filtrare WEB va permite integrarea şi acceptarea de destinaţii blocate de la sistemul de management centralizat, cu efect a întregii flote de echipamente de reţea administrate cât şi asupra staţiilor

de lucru aflate sub influența politicii de filtrare WEB dar neprezente în organizaţie»;

- «în cazul ofertelor ce conţin strategia dual-vendor, se cere ca întreaga telemetrie la nivel de reţea şi de la nivelul staţiilor de lucru, să se colecteze, coreleze şi să se afişeze într-o singură consolă de incidente».

***7.** În cadrul capitolului cap.3.3.1.5. INTEGRARE, AUTOMATIZARE, CORELARE, pentru cerinţa: «Echipamentele, licenţele, software-ul de management, mecanismele de filtrare, de audit sau de telemetrie trebuie livrate integrate, ca un ansamblu unitar, cu scopul de a minimiza riscul atacurilor cibernetice şi de a expune operatorilor un ansamblu de date corelat» - punctul 3.3.1.5, **vă rugăm să ne detaliați:** modalitatea de integrare, ca un tot unitar între toate echipamentele propuse, modalitatea de corelare a datelor precum și, modalitatea de minimizare a riscurilor în cazul unui atac cibernetic ipotetic, folosind acest ansamblu integrat, ce furnizează date corelate;*

***8.** În cadrul capitolului cap.3.3.1.5. INTEGRARE, AUTOMATIZARE, CORELARE, **vă rugam să ne detaliați** modalitatea de implementare a cerinţei descrise la punctul 3.3.1.5 - «Soluţia propusă va colecta, procesa, îmbogăţi (enrich), vizualiza cantităţi masive de log-uri generate de evenimente semnificative la nivelul aplicaţiilor, sistemelor de operare, echipamentelor de reţea, echipamentelor de securitate ori alte echipamente şi soluţii descrise în documentul de faţă. Soluţia trebuie să furnizeze funcţii de căutare avansată şi rapidă, precum şi capabilităţi de identificare de anomalii, folosind algoritmi şi funcţii matematice avansate de tip <unsupervised machine learning>, toate descrise mai jos. Soluţia propusă va permite interacţiunea cu alte aplicaţii de management sau de producţie, prin intermediul tehnologiilor RESTfull API şi JSON. Soluţia va folosi o bază de date distribuită care să permită căutarea în timp real, vizualizarea, raportarea şi stocarea istorică a log-urilor pe o perioadă de 30 de zile cu posibilitate de extindere la 90 de zile»".*

La această solicitare de clarificări, contestatoarea a răspuns prin adresa nr. **...**, înregistrată la autoritatea contractantă sub nr. **...**precizând următoarele:

*„**6.** Management-ul filtrării web pe stațiile de lucru se face prin EMS. ...-ul poate trimite log-uri către ... prin VPN și corelate cu FAZ, pentru o centralizare a întregii vizibilități (...- Admin/1400 Settings/0410 Send% 20logs%20to%20FAZ%20or% 20FMG.htm#). Mai mult, ... se poate configura să fie mereu conectat la VPN, astfel că stația de lucru nu va face trafic fără ca acesta să treacă prin filtrarea ...-ului (... 11 …)";*

***7.** Integrarea se face direct între echipamentele ... propuse și soluţiile de FortiManager și .... Echipamentul de colectare primeşte loguri de la echipementele firewall cu posibilitatea ca acestea să fie incriptate pentru a securiza transmisia de loguri. Având vizibilitate asupra întregii reţele compuse din echipamentele de securitate ..., se poate acţiona asupra evenimentelor de securitate detectate de ..., restricţionând traficul*

vulnerabil în cel mai scurt timp. Mai mult, prin serviciul de IOC (Indicators of Compromise) se pot monitoriza toate stațiile de lucru compromise pentru a se acţiona asupra lor;
***8.a)** Corelarea și analiza de anomalii se face prin serviciul de Indicators of Compromise (…)*
***8. b**) Poate satisface cerinţele de integrare folosind XML API*
(...) și JSON API, cu informaţia pe Developer Network: ... (JSON API)
***8.c)** ... împarte logurile în Analytics logs și Archived logs. Analytics reprezintă logurile ce pot fi vizualizate și analizate în timp real. Analytics retention period se poate seta și pana la 90 de zile (…)".*

Prin adresa **nr. ...,** membrii comisiei de evaluare au solicitat contestatoarei să clarifice următorul aspect:

„Având în vedere cerinţa generală de la capitolul 3.3.1.5., din Caietul de sarcini: (...) vă rugăm să precizaţi următoarele:

(...)

*4. Datorită faptului că oferta dvs. conţine o strategie dual vendor (... si ...), **vă rugăm să descrieţi** cum veți colecta și corela întreaga telemetrie la nivel de reţea și la nivelul stațiilor de lucru, într-o singură consolă de incidente".*

Contestatoarea a răspuns prin adresa nr. ..., înregistrată la autoritatea contractantă sub nr. ..., în cuprinsul căreia a menționat următoarele:

„Colectarea și corelarea centralizată a întregii telemetry la nivel de reţea la nivelul echipamentelor celor doi producători (... și ...) se va face prin protocolul .... Astfel: ... va colecta prin ... log-urile atât de la echipamentele ..., cât și de la ..., și/sau alte echipamente și le va afişa pe o singura consolă de incidente.

La nivelul stațiilor de lucru colectarea și corelarea centralizată a întregii telemetry se va face de către ...prin intermediul licenţelor de ... ...& ...și care le va afişa pe o singură consolă de incidente.

Referinţa Tehnica la adresa:

...".

Prin adresa **nr....,** membrii comisiei de evaluare au solicitat contestatoarei să clarifice următorul aspect:

„2. Clarificare referitoare la management şi integrare

În caietul de sarcini în specificaţiile aferente capitolelor:

- *3.3.1.1 Echipamente de reţea tip 1 - 4 bucăţi"*
- *3.3.1.2 Echipamente de reţea tip 2 - 46 bucăţi"*
- *3.3.1.3 Echipamente de reţea tip 3 - 96 bucăţi"*
- *3.3.1.4 Echipamente de reţea tip 4 - 34 bucăţi"*

Secţiunea «Management: Note» se solicită:

«2. în cazul în care ofertantul propune în cadrul ofertei pe întreg lotul 1 mai multe echipamente de la acelaşi producător se acceptă o singură soluţie de management şi monitorizare pentru toate echipamentele care provin de la acelaşi producător. În cazul în care ofertantul propune o soluţie folosind strategia dual-vendor, atunci se

acceptă o singură soluţie de management şi corelare de evenimente. Soluţia de management şi corelare va trebui să absoarbă şi să coreleze datele expuse de toate echipamentele».

În caietul de sarcini, în specificaţiile aferente capitolului:

3.3.1.5 Cerinţe de management, integrare, automatizare, corelare evenimente şi loguri - Secţiunea «Management: Note» se solicită:

«În cazul ofertelor ce conţin strategia dual-vendor, se cere ca întreaga telemetrie la nivel de reţea şi de la nivelul staţiilor de lucru, să se colecteze, coreleze şi să se afişeze într-o singură consolă de incidente. Pentru implementarea acestei strategii, ofertantul poate folosi tehnologii de partajare de date specifice sau cunoscute după cum urmează: REST- API, Netflow, ...».

Soluţia tehnică oferită de compania dumneavoastră pentru componenta de management, integrare, automatizare, corelare evenimente şi loguri este ...Analyzer-VM.

Înţelegem din fişa de date indicată:

... că platforma ... se integreaza cu toate componentele ... ofertate (... ... ...),

Întrucât nu identificam funcţionalitatea, funcţia, modulul, fluxul de acţiuni necesare, ***vă rugăm să ne indicaţi*** *în clar, modul de adăugare ca şi sursă de loguri a echipamentelor ... ..., ...with Firepower Services, ...with Firepower Services în platforma ofertată".*

Contestatoarea a răspuns prin adresa nr. ..., înregistrată la autoritatea contractantă sub nr. ..., precizând următoarele:

„Modul de adăugare ca si sursă de loguri a echipamentelor ... ..., ...with Firepower Services, ...-X, with Firepower Services în platforma ofertata, ...este detaliat în cele ce urmează:

Conform link-ului public din documentaţia de ... de mai jos: ... administration-guide/363038/types-of-logs-collected-for-each-device, echipamentele care pot genera și trimite loguri în format ... pot fi integrate în ....

Echipamentele ... ..., ...with firepower services, ...with firepower services suportă logarea către un server de ..., prin urmare se pot integra cu ... VM.

Dispozitivele ce se pot loga în ... pot fi adăugate manual sau automat din consolă, iar procesul manual este descris mai jos:

...

....

Acest proces se bazează pe ADOM-ul ... unde vor fi adăugate sursele ce generează loguri de tip ....

Pot fi create mai multe ADOM-uri pentru ... în cazul în care este nevoie Despre ADOM-uri puteți consulta documentaţia specifică:

...

administration-fluide/697440/adoms

…

administration-fiuide/6Q571/managing-adoms

Pentru procesul automat de adăugare, echipamentul care va genera loguri, trebuie configurat să trimită logurile către ... server, acesta fiind .... În consola de ... se aprobă echipamentul și va fi automat alocat ADOM-ului corespunzător, în cazul nostru ADOM-ul ...".

Analizând decizia autorității contractante de a respinge oferta contestatoarei, prin raportare la prevederile documentației de atribuire, solicitările de clarificări adresate de autoritatea contractantă contestatoarei și răspunsurile acesteia, Consiliul o apreciază ca fiind întemeiată pentru următoarele motive:

În cadrul Fișei de date a achiziției, la punctul IV.4.1 - Modul de prezentare al propunerii tehnice, autoritatea contractantă a solicitat ca propunerea tehnică să conțină **un comentariu, articol cu articol, privind toate cerințele conținute în Caietul de sarcini, prin intermediul cărora ofertantul va demonstra corespondența propunerii tehnice cu prevederile caietului de sarcini.** Astfel, s-a solicitat ca ofertanții să prezinte o **descrierea detaliată** a modului de îndeplinire a cerințelor minime prevăzute în caietul de sarcini, prin care să se demonstreze corespondența propunerii tehnice cu toate cerințele prevăzute.

*„Pentru a demonstra că propunerea tehnică depusă respectă cerințele minime din caietul de sarcini, se vor descrie în **detaliu:***

- toate informațiile din care să se poată aprecia dacă sunt îndeplinite cerințele din caietul de sarcini;

- alte informații considerate semnificative pentru evaluarea corespunzătoare a propunerii tehnice.

*Nu se admite prezentarea pe post de propunere tehnică a caietului de sarcini semnat/ștampilat de ofertant, iar comentariile de tipul DA/NU nu reprezintă îndeplinirea cerințelor solicitate, **sub sancțiunea declarării propunerii tehnice ca fiind neconformă".***

Analizând modul în care ofertanta contestatoare a răspuns cerințelor menționate în cadrul Fișei de date a achiziției anterior reproduse, Consiliul constată că aceasta a indicat o serie de linkuri ca referințe tehnice, iar în ceea ce privește cerințele tehnice reproduse la pag. 11 – 12 a prezentei decizii, în cadrul coloanei intitulată „răspuns ofertant", care ar fi trebuit să conțină **descrieri detaliate** cu privire la modul de îndeplinire a cerințelor, s-a limitat la copierea **întocmai** a cerinței din caietul de sarcini, a se vedea în acest sens, următoarele mențiuni:

- „Soluția de management permite corelarea evenimentelor precum și absorbirea datelor expuse de toate echipamentele ofertate".

- „Întreaga telemetrie la nivel de rețea și la nivelul stațiilor de lucru, colectează, corelează și va afișa într-o singură consolă de incidente. Acest lucru se va realiza prin folosirea tehnologiilor de partajare a datelor specifice sau cunoscute după cum urmează: REST-API, Netflow, ...",

- *„Soluția furnizează funcții de căutare avansată și rapidă, precum și capabilități de identificare de anomalii, folosind algoritmi și funcții matematice avansate de tip «unsupervised machine learning», toate descrise mai jos”.*

Deși autoritatea contractantă nu a dorit prezentarea propunerii tehnice într-o asemenea manieră (a se vedea în acest sens prevederile Fișei de date a achiziției, punctul IV.4.1), Consiliul constată că membrii Comisiei de evaluare au manifestat un rol activ și au solicitat contestatoarei detalierea/descrierea/precizare modului în care sunt îndeplinite unele specificații tehnice, răspunsurile la clarificări fiind neconcludente în conformitate cu dispozițiile art. 134 alin. (5) din HG nr. 395/2016, nefiind astfel demonstrată de către ofertantul în discuție îndeplinirea cerințelor din caietul de sarcini, oferta intrând sub incidența dispozițiilor art. 137 alin. (3) lit. a) din HG nr. 395/2016. În cadrul răspunsurile la clarificări, contestatoarea a continuat prezentarea informațiilor în aceeași manieră superficială, prin indicarea unor link-uri și neformularea unor răspunsuri concrete cu privire la toate aspectele pe care autoritatea contractantă a intenționat să le clarifice prin solicitările de clarificări transmise contestatoarei. Această manieră de redactare atât a propunerii tehnice cât și a răspunsurilor la clarificări îi este imputabilă exclusiv ofertantei contestatoarei.

Astfel, Consiliul constată că răspunsul contestatoarei la clarificări nr. **...**, înregistrat la autoritatea contractantă sub nr. **...**, este neconcludent pentru următoarele motive:

● **răspunsul nr. 6** acoperă doar prima parte a solicitării de clarificări referitoare la motorul de filtrare web, nemenționând nimic cu privire la cerința ca întreaga telemetrie la nivel de rețea și la nivelul stațiilor de lucru să se colecteze, coreleze și să se afișeze într-o singură consolă de incidente, deși solicitarea de clarificări a fost clară: „ (...) ***vă rugăm să detaliaţi îndeplinirea următoarelor cerinţe:***

- *«Motorul de filtrare WEB va permite integrarea şi acceptarea de destinaţii blocate de la sistemul de management centralizat, cu efect a întregii flote de echipamente de reţea administrate cât şi asupra staţiilor de lucru aflate sub influenta politicii de filtrare WEB dar neprezente în organizaţie»;*

- ***«în cazul ofertelor ce conţin strategia dual-vendor, se cere ca întreaga telemetrie la nivel de reţea şi de la nivelul staţiilor de lucru, să se colecteze, coreleze şi să se afişeze într-o singură consolă de incidente»”.***

• **răspunsul nr. 7** precizează cum se integrează echipamentele ... fără a menționa cum sunt integrate, ca un tot unitar, și echipamentele ..., deși solicitarea de clarificări a fost clară, în sensul: ***„vă rugăm să ne detaliați:*** *modalitatea de integrare,* ***ca un tot unitar între toate echipamentele propuse,*** *modalitatea de corelare a datelor precum și, modalitatea de minimizare a riscurilor în cazul unui atac cibernetic ipotetic, folosind acest ansamblu integrat, ce furnizează date*

corelate". În acest context, Consiliul reiterează faptul că autoarea contestației a ofertat în cadrul lotului 1, echipamente ... și ....

- **răspunsul nr. 8** nu detaliază modalitatea prin care soluția propusă oferă funcții de căutare avansată și rapidă, precum și capabilități de identificare de anomalii, folosind algoritmi și funcții matematice avansate de tip „unsupervised machine learnig", deși solicitarea de clarificări a fost clară, în sensul: *„**vă rugam să ne detaliați** modalitatea de implementare a cerinţei descrise la punctul 3.3.1.5 – (...) Soluţia trebuie să furnizeze funcţii de căutare avansată şi rapidă, precum şi capabilităţi de identificare de anomalii, folosind algoritmi şi funcţii matematice avansate de tip <unsupervised machine learning> (...)".*

Având în vedere cele mai sus menționate, Consiliul constată că răspunsul contestatoarei la clarificări nr. **...**, înregistrat la autoritatea contractantă sub nr. **...**, este neconcludent, în speță fiind incidente dispozițiile art. 134 alin. (5) din HG nr. 395/2016, care stipulează următoarele: *„În cazul în care comisia de evaluare solicită unui candidat/ofertant clarificări şi, după caz, completări ale documentelor prezentate de acesta în cadrul ofertei sau solicitării de participare, potrivit dispoziţiilor art. 209 din Lege, iar candidatul/ofertantul nu transmite în termenul precizat de comisia de evaluare clarificările/completările solicitate sau clarificările/completările transmise nu sunt concludente, oferta sa va fi considerată inacceptabilă",* la acel moment autoritatea contractantă având obligația de a respinge oferta contestatoarei, conform temeiului de drept anterior menționat.

Consiliul apreciază că, în etapa de evaluare a ofertelor, autoritatea contractantă nu poate solicita unui ofertant clarificarea aceluiași aspect de mai multe ori, în condițiile în care ofertantul în discuție nu formulează niciun fel de susțineri cu privire la anumite solicitări ale autorității contractante, deoarece în speță devin incidente dispozițiile art. 209 alin. (2) din Legea nr. 98/2016, care stipulează următoarele: *„Autoritatea contractantă nu are dreptul ca prin clarificările/completările solicitate să determine apariţia unui avantaj evident în favoarea unui ofertant/candidat".*

Deși răspunsul nr. 6 din adresa contestatoarei nr. **...**, înregistrată la autoritatea contractantă sub nr. **...**, este neconcludent (așa cum s-a reținut anterior) deoarece nu menționa nimic cu privire la cerința ca întreaga telemetrie la nivel de rețea și la nivelul stațiilor de lucru să se colecteze, coreleze și să se afișeze într-o singură consolă de incidente, autoritatea contractantă îi trimite contestatoarei o nouă solicitare de clarificări în legătură cu același aspect, respectiv, întrebarea nr. 4 din solicitarea de clarificări nr. **nr. ...:**

„Având în vedere cerinţa generală de la capitolul 3.3.1.5., din Caietul de sarcini: (...) vă rugăm să precizaţi următoarele:

(...)

*4. Datorită faptului că oferta dvs. conţine o strategie dual vendor (... si ...), **vă rugăm să descrieţi** cum veți colecta și corela*

întreaga telemetrie la nivel de reţea și la nivelul stațiilor de lucru, într-o singură consolă de incidente”.

Analizând răspunsul contestatoarei (adresa nr. ..., înregistrată la autoritatea contractantă sub nr. ...), Consiliul constată că producătorul declară că logurile de tip ... sunt tratate la loguri de tip generic, iar conform producătorului aceste loguri nu sunt afișate pe consola de incidente ..., în acest context nefiind îndeplinită următoarea cerință din caietul de sarcini, care prevede: *„**în cazul ofertelor ce conţin strategia dual-vendor, se cere ca întreaga telemetrie la nivel de reţea şi de la nivelul staţiilor de lucru, să se colecteze, coreleze şi să se afişeze într-o singură consolă de incidente”,*** astfel încât Consiliul apreciază că oferta contestatoarei intră sub incidența dispozițiilor art. 137 alin. (3) lit. a) din HG nr. 395/2016, care stipulează următoarele: „

„În condiţiile art. 215 alin. (5) din Lege, oferta este considerată neconformă în următoarele situaţii:

a) nu satisface în mod corespunzător cerinţele caietului de sarcini”.

De asemenea, Consiliul mai analizează și adresa contestatoarei nr. ..., înregistrată la autoritatea contractantă sub nr. ..., reprezentând răspunsul la solicitarea de clarificări nr. ... și reține ca relevante susținerile autorității contractante din cadrul punctului de vedere nr. ..., necombătute de către contestatoare, referitoare la următorul aspect:

„Contestatoarea afirmă faptul că Echipamentele ... ..., ...with firepower services, ...with firepower services suportă logarea către un server de ..., prin urmare se pot integra cu ... VM, dar conform caietului de sarcini aceste loguri trebuie sa ajungă în consola unică de incidente, denumită ... de către producător. La adresa de referinţă ... (...) în tabelul de la paginile 13-14, producătorul specifică faptul că logurile provenite prin protocolul ... de la echipamentele ..., nu beneficiază de facilitatea ... din .... Prin urmare aceste loguri nu pot fi corelate cu logurile provenite de la echipamentele ...”.

În legătură cu următorul aspect care se regăsește în cadrul actului atacat „logurile provenite de la echipamentele ... ofertate, nu ajung în modulul ..., aceste loguri nu beneficiază de funcțiile matematice avansate de tip «unsupervised machine lerning»”, Consiliul constată că, autoarea contestației nu face niciun fel de susțineri, în cadrul actului de sesizare a Consiliului, sub acest aspect fiind relevante următoarele susțineri ale autorității contractante din cadrul punctului de vedere: *„Nu regăsim în documentaţie funcţiile de unsupervised machine learning implementate în ... sau .... Nu regăsim în documentaţie detalii despre analiza funcţiilor matematice, prin care să se confirme că aceasta folosește datele absorbite prin ..., de la ambii producători”.*

În acest context, Consiliul constată că, deși punctul de vedere formulat de către autoritatea contractantă în prezenta cauză a fost comunicat contestatoarei la data de 29.07.2019 (conform dovezii aflată la dosarul cauzei), iar prin adresa nr. ..., Consiliul i-a dat posibilitatea

acesteia să formuleze o replică în legătură cu acest document, ..., deși a confirmat primirea adresei CNSC la data de 07.08.2019, până la data emiterii prezentei decizii nu a înțeles să răspundă argumentelor tehnice prezentate de către autoritatea contractantă, deși termenul acordat de Consiliu a expirat.

Luând în considerare aspectele de fapt și de drept mai sus menționate, în temeiul art. 26 alin. (6) din Legea nr. 101/2016, Consiliul va respinge, ca nefondată, contestaţia formulată de ..., în contradictoriu cu autoritatea contractantă ....

Prezenta decizie este obligatorie pentru părți, în conformitate cu dispozițiile art. 28 alin. (1) din Legea nr. 101/2016.

Pentru aceste motive,
în baza legii și a mijloacelor de probă aflate la dosar,

CONSILIUL DECIDE:

Respinge, ca nefondată, contestația formulată de ..., în contradictoriu cu ....

Împotriva prezentei decizii se poate formula plângere, în termen de 10 zile lucrătoare de la comunicare pentru părţile cauzei, respectiv de la data luării la cunoştinţă de către alte persoane vătămate.

PREȘEDINTE COMPLET
...

MEMBRU COMPLET **MEMBRU COMPLET**
... **...**

Redactat în 4 exemplare originale, conține 23 pagini.