CONSILIUL NAŢIONAL DE SOLUŢIONARE A CONTESTAŢIILOR

C. N. S. C.

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

În conformitate cu prevederile art.266 alin.2) din OUG nr.34/ 2006 privind atribuirea contractelor de achiziţie publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii, aprobată prin Legea nr. ... cu modificările şi completările ulterioare, Consiliul adoptă următoarea:

DECIZIE
Nr. ...
Data: ...

Prin contestaţia nr. ... înregistrată la CNSC cu nr. ... formulată de ... cu sediul în ... ..., judeţul ... înregistrată la Oficiul Registrul Comerţului sub nr. ... având CUI ..., reprezentată legal de ... - ... împotriva răspunsurilor la clarificări publicate, în SEAP, în data de 11.12.2013, de către autoritatea contractantă ... cu sediul în ... str. ..., referitoare la procedura de achiziţie, prin „licitaţie deschisă”, în vederea atribuirii contractului de achiziţie publică având ca obiect: „Contract de furnizare având ca obiect realizarea unei soluţii integrate de securizare a sistemului informatic în vederea certificarii ISO 27001 (cod CPV:30211300-4), conform configuraţiei şi cerinţelor minime obligatorii prevăzute în Sectiunea 2: Caietul de sarcini”, cod CPV: 30211300-4, 72265000-0, 72611000-6, s-a solicitat: ,,suspendarea procedurii de atribuire în cauză; modificarea documentaţiei de atribuire în conformitate cu prevederile legislaţiei din România legate de procesul achiziţiilor publice’’.

În baza documentelor depuse de părţi,
CONSILIUL NAŢIONAL DE SOLUŢIONARE A CONTESTAŢIILOR

DECIDE:

Respinge excepţia tardivităţii, invocată de autoritatea contractantă faţă de contestaţia formulată de ...

Respinge ca nefondată contestaţia formulată ... în contradictoriu cu autoritatea contractantă ...

Dispune continuarea procedurii de atribuire în cauză.

Prezenta decizie este obligatorie pentru părţi, în conformitate cu prevederile art. 280 alin. (3) din OUG nr. 34/2006 aprobată prin Legea nr. ... cu modificările şi completările ulterioare.

Împotriva prezentei decizii se poate formula plângere în termen de 10 zile de la comunicare.

MOTIVARE

În luarea deciziei s-au avut în vedere următoarele:

Prin contestaţia nr. ... înregistrată la CNSC cu nr. ... formulată de ... împotriva răspunsurilor la clarificări publicate, în SEAP, în data de 11.12.2013, de către ... în calitate de autoritate contractantă, s-a solicitat: ,,suspendarea procedurii de atribuire în cauză; modificarea documentaţiei de atribuire în conformitate cu prevederile legislaţiei din România legate de procesul achiziţiilor publice''.

În susţinerea cererilor sale, contestatorul menţionează că a solicitat clarificări cu privire la conţinutul caietului de sarcini, iar la data de 11.12.2013, autoritatea contractantă a publicat în SEAP precizări completatoare care, în opinia sa, favorizează un singur producător (IBM).

Contestatorul susţine că, în urma analizei documentaţiei de atribuire (fişa de date, caiet de sarcini, anexe la caietul de sarcini şi răspunsurile la solicitările de clarificari), a identificat abateri grave care încalcă prevederile legale privind achiziţiile publice şi restricţionează participarea operatorilor economici interesaţi în participarea la această procedură, prin încălcarea principiului liberei concurenţe şi favorizarea unui anumit producător.

Astfel, contestatorul susţine că, analizând caietul de sarcini şi clarificările emise de către autoritatea contractantă prin adresa nr. SC-DA- 28...2/11.12.2013, a constatat favorizarea intenţionată a unui singur producător (IBM), cu impact major asupra principiului liberei concurenţe, la nivelul descrierii cerinţelor funcţionale ale următoarelor componente:

1. „*Platforma de management pentru soluţiile de prevenire a intruziunilor: un sistem hardware dedicat (hardware appliance) plus toate licenţele aferente*”:

1.1 Răspunsurile la întrebările de clarificare 1 şi 61 din adresa nr. SC-DA-28...2/11.12.2013, referitoare la cerinţa 1.5.1.4 – „*Platforma de management pentru soluţiile de prevenire a intruziunilor: un sistem hardware dedicat (hardware appliance) plus toate licenţele aferente*”, menţin obligativitatea unei console de administrare centralizată a tuturor soluţiilor de prevenire a intruziunilor solicitate în caietul de sarcini la punctele 1.5.1.1, 1.5.1.2 şi 1.5.1.3. Cerinţele punctuale pentru respectivele soluţii IPS direcţionează numai către platforme

IBM, datorită impunerii livrării unei platforme hardware produsă numai de acest producător, cerută în mod specific: IBM SiteProtector System. Dovada se regăseşte prin accesarea linkului IBM SiteProtector System (http://www-03.ibm.com/software/products/en/site-protector- system).

În vederea dovedirii că soluţiile IPS cerute sunt posibil a fi ofertate numai de către IBM, contestatorul enumeră cerinţele precizate la data de 11.12.2013, care corespund cu caracteristicile producătorului IBM, publicate pe internet conform linkurilor indicate :

- capabilităţile de detecţie şi blocare ale „*engine*”-ului de protecţie sunt copiate în totalitate din foaia de catalog a unui singur producător - IBM - şi limitează ofertarea unei singure platforme - IBM GX4004 şi IBM GX5208 (http://www- 935.ibm.com/services/us/iss/ pdf/br proventia-network-intrusion-prevention- system protection-engine.pdf, http:// public.dhe.ibm.com/common/ssi/ecm/en/wgd 03002usen/WGD03Q02USEN.PDF);

- tehnologiile de detecţie şi prevenire a intruziunilor sunt copiate în totalitate din foaia de catalog a unui singur producător - IBM - şi limitează ofertarea unei singure platforme - IBM GX4004 + IBM GX5208 (http://www-935.ibm.com/services/us/iss/pdf/br proventia-network-intrusion-prevention-system protection-engine.pdf, http:// public.dhe.ibm.com/common/ssi/ecm/en/wgd03002usen/WGD03Q02USEN.PDF);

- capabilităţile de detecţie şi blocare ale „*engine*”-ului de protecţie sunt copiate în totalitate din foaia de catalog a unui singur producător - IBM - şi limitează ofertarea unei singure platforme: IBM Security Server Protection (ftp://ftp.software.ibm.com/ software/ in/ tivoli/Protocol Analysis Module- WGD03001USEN.PDF);

- tipurile de monitorizare solicitate sunt copiate în totalitate de pe site-ul oficial al unui singur producător - IBM - şi limitează ofertarea unei singure platforme - IBM Security Server Protection (http://www-03.ibm.com/software/products/ro/server-protection/);

- funcţionalităţile solicitate sunt copiate în totalitate din foaia de catalog a unui singur producător - IBM - şi limitează ofertarea unei singure platforme - IBM Security Virtual Server Protection for Vmware (ftp://public.dhe.ibm.com/software/hu/pdf/Tivoli ISS Overview Technical BP Enablement 2010.pdf).

1.2 Întrebarea nr. 6, referitoare la cerinţa *„Soluţie de prevenire a intruziunilor (IPS) la nivel de reţea, Performanţa în reţea, Nivel de echipare 1 (4 echipamente, 1 echipament de rezervă (cold spare), 5 hardware bypass dacă este necesar)*” solicită în mod expres lămurirea

necesităţii unui număr disproporţionat de sesiuni concurente cu numărul de conexiuni pe secundă şi cu traficul inspectat.

Contestatorul menţionează că răspunsul din adresa nr. SC-DA-28...2/11.12.2013 la această întrebare nu clarifică această solicitare, lăsând nemodificată cererea iniţială, care se dovedeşte a fi copiată în totalitate din foaia de catalog a unui singur producător - IBM - şi limitează ofertarea unei singure platforme – IBM GX4004 (http:// public.dhe.ibm.com/common/ssi/ecm/en/wgd03002usen/WGDQ3002USEN.PDF).

1.3 Întrebarea de clarificare nr. 8, referitoare la cerinţa *„Soluţie de prevenire a intruziunilor (IPS) la nivel de reţea, Performanţa în reţea, Nivel de echipare 2 (2 echipamente + 2 hardware bypass dacă este necesar)*" solicită, în mod expres, lămurirea necesităţii unui număr disproporţionat de sesiuni concurente cu numărul de conexiuni pe secundă şi cu traficul inspectat pentru IPS-ul la nivel de reţea, Nivel de echipare 2.

Contestatorul precizează că răspunsul din adresa nr. SC-DA-28...2/11.12.2013 la această întrebare nu clarifică această solicitare, lăsând nemodificată cererea iniţială, care se dovedeşte a fi copiată în totalitate din foaia de catalog a unui singur producător - IBM - şi limitează ofertarea unei singure platforme - IBM GX5208 (http:// public.dhe.ibm.com/common/ssi/ecm/en/wgd03002usen/ WGD03002 USEN.PDF).

1.4 Răspunsul din adresa nr. SC-DA-28...2/11.12.2013 la întrebarea nr. 23, referitoare la cerinţa *„Platforma de management pentru soluţiile de prevenire a intruziunilor: un sistem hardware dedicat (hardware appliance) plus toate licenţele, aferente, se va livra o platformă hardware de la acelaşi producător ca al soluţiei de management*", nu deschide posibilitatea ofertării altor soluţii în afara de cea IBM (exemplu: software de la furnizorul A instalat pe hardware de la furnizorul B - o soluţie uzuală în industrie).

Contestatorul menţionează că platforma de management solicitată aici este identificată a fi IBM SiteProtector (http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype= PM& appname=SWGEWGWGUSEN&htmlfid=WGD03013USEN& attachment =WG D03013USEN.PDF).

2. *„Soluţie de prevenire a intruziunilor (IPS) la nivel de server critic: 10 (zece) licenţe software*".

Răspunsul din adresa nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. 9, referitoare la cerinţa 1.5.1.2 *„Soluţie de prevenire a intruziunilor (IPS) la nivel de server critic: 10 (zece) licenţe software*", menţine cerinţa obligatorie ca soluţia să suporte sistemele de operare Windows Server, HP-UX, IBM-AIX şi Solaris SPARC. Această solicitare, coroborată cu informaţia de la punctul c) din

răspunsul întrebării nr. 59 referitoare la cerinţa 1.5.1.3 *„Soluţie de prevenire a intruziunilor (IPS) la nivel de server gazdă - host server”* (sistemele de operare ce rulează pe platformele .... sunt doar Windows şi Linux) limitează ofertarea la o singură platforma de tip Host IPS - IBM Security Server Protection, cu suport pentru sistemele de operare IBM-AIX şi Solaris, în ciuda faptului că sistemele de operare ce rulează pe platformele .... sunt doar Windows şi Linux, conform răspunsului autorităţii contractante (http:// www-03.ibm.com/software/products/ro/server-protection/);

3. *„Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, Integrare şi corelare cu sistemele IPS, să aibă capabilităţi de integrare a datelor furnizate de sisteme IPS şi corelare a acestora cu vulnerabilităţile descoperite, printr-o aplicaţie de management comună*”.

În răspunsul din adresa nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. 32, referitoare la cerinţa 1.5.3.1 *„Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, Integrare şi corelare cu sistemele IPS, să aibă capabilităţi de integrare a datelor furnizate de sisteme IPS şi corelare a acestora cu vulnerabilităţile descoperite, printr-o aplicaţie de management comună*”, se specifică că modulul de scanare de vulnerabilităţi şi IPS-ul trebuie să se integreze într-un mod specific unui singur furnizor - IBM - în timp ce bunele practici efectuează integrarea aceloraşi funcţionalităţi fără limitarea la un modul de corelare specific. Modul de licenţiere solicitat - separat pentru fiecare activ scanat în parte ce va importa baza de date cu vulnerabilităţi şi o va putea corela cu atacurile identificate de IPS – aparţine furnizorului IBM - modulul IBM SecurityFusion, specificat în mod explicit în foaia de catalog: Proventia Network Enterprise Scanner (http:// www.google.ro/ url?sa=t&rct=i&q=&esrc=s&source=web&cd=4&cad=ria&ved=0Cec QFiAD&url=http%3A0/o2F%2Fpic.dhe.ibm.com0/o2Finfocenter%2Fsp rotect0/o2Fv2r8mO%2Ftopic%2Fcom.ibm.siteprotector.doc%2Fpdfs% 2FSP 30 Security Fusión Module Guide.pdf&ei= Mbmp Utm 4B6mCyQPRslHwCg&usg=AFQiCNEcq7gEdKhPWFFFfqHWPPFzAtRYLg& bvm=bv.57967247,d.bGQ, http://www.ibm.com/ru/services/iss/ pdf/ proventia-network-enterprise-scanner-ss.pdf)

4. *„Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, Performanţele analizei, Capacitatea de a scana minim 24000 IP-uri pe oră, Capacitatea de a realiza analize complete pentru minim 800 active/oră (all non-DoS-enabled)*”.

Întrebarea nr. 30, referitoare la cerinţa 1.5.3.1 *„Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, Performanţele analizei, Capacitatea de a scana minim 24000 IP-uri pe oră, Capacitatea de a realiza analize complete pentru minim 800 active/ oră (all non-DoS-enabled)*" solicită, în mod expres, lămurirea necesităţii unor cerinţe de performanţă disproporţionate faţă de numărul de active: în condiţiile în care numărul total de active este 2000 (echipamente identificabile prin IP), nu este sustenabilă cererea de exact 24000 de IP-uri pe oră. Valorile de performanţă se regăsesc exact în două foi de catalog IBM, ataşate acestei contestaţii. În una din ele este copiat în clar textul *„all non-DoS-enabled: 803 devices/ hour*", referitor la cele 800 de active scanate pe oră. În a doua, se menţionează valoarea de scanari de 24000 de IP-uri pe oră (24.000: http://www.acagroup.com/upload/iblock/25d/ES ds SED03045USEN. pdf, 800 active: http://www.iss.net/documents/literature/IBM Proventia EnterpriseScanner Datasheet.pdf).

5. *„Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, -1 port serial - accesibil pe partea frontală cu conector RJ-45, 2 porturi USB 2.0 - accesibile pe partea frontală*".

Răspunsul din adresa nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. ... referitoare la cerinţa 1.5.3.1 *„Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, - 1 port serial - accesibil pe partea frontală cu conector RJ-45, 2 porturi USB 2.0 - accesibile pe partea frontală*" menţine cerinţa obligatorie de prezentare a următoarelor porturi: 1 port serial cu conector RJ-45 şi două porturi USB 2.0 pe partea frontală a echipamentului de management a vulnerabilităţilor. Cererea provine, în mod explicit, din foaia de catalog a aceluiaşi producător: IBM - Proventia Network Enterprise Scanner. Aceasta este încă o limitare la cerinţele caietului de sarcini pentru aceste soluţii.

În plus, răspunsul la întrebarea nr. 66 nu permite, în mod clar, ofertarea unei soluţii cu configuraţie hardware diferită, în condiţiile în care functionalităţile şi performanţele solicitate nu vor fi afectate. Ca urmare, nu se poate oferta decât echipamentul firmei IBM menţionat mai sus (http://www.iss.net/documents/literature/IBM Proventia Enterprise Scanner Datasheet.pdf).

6. Conform răspunsului din adresa nr. SC-DA-28...2/ 11.12.2013 la întrebările de clarificări 36 şi 37 referitoare la *„Echipament hardware dedicat (hardware appliance) pentru culegerea, înregistrarea, corelarea, interpretarea şi prioritizarea datelor referitoare la evenimente de securitate (SIEM), plus toate licenţele*

aferente", componentele necesare sunt: SIEM, Network Behavior Analysis şi Risk management, cu echipamente dedicate:

6.1 Pentru subcomponenta SIEM, aceasta se identifică, în mod unic, prin platforma IBM QRadar All-in one 3105. Conform paginii IBM seria 31xx, cu ID V7.2.0 include următoarele produse: QRadar SIEM, QRadar LogManager, QRadar Anomaly Network Detection, QRadar Risk manager şi QRadar Vulnerability Manager.

Contestatorul precizează că acestea acoperă exact componentele menţionate în întrebare/caietul de sarcini. Răspunsul la întrebare nu face decât să confirme ca subcomponenta SIEM trebuie să conţină Log Management, SIEM şi NBAD, alături de celelalte componente specificate în caiet: Network Behavior Analysis (identificat tot în mod unic ca şi produsul QRadar Flow Collector) şi Risk management (identificat ca QRadar Risk Manager).

De altfel, subcomponenta SIEM a fost identificata ca IBM QRadar All-in One 3105 pe baza cerinţelor de performantă cerute la 1.5.4.1.1. *„Performanţe*":

- Minim 1000 EPS (evenimente pe secundă). Posibilitatea creşterii la 2.500 şi 5.000 EPS doar prin licenţă (fără înlocuirea echipamentului).
- Minim 50.000 NetFlows/minut. Posibilitatea creşterii de la 50.000 la 400.000 NetFlows/minut doar prin licenţă (fără înlocuirea echipamentului).
- Minim 25.000 Flows/minut (Sflow, Jflow, Packeteer). Posibilitatea creşterii de la 25.000 la 200.000 Flows/minut doar prin licenţă (fără înlocuirea echipamentului).

Contestatorul menţionează că foaia de catalog este: http:// www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotvpe=OC& subtype =NA&htmlfid=897/ENUS5725-l52&appname=totalstorage

6.2 Subcomponenta QRadar Flow Collector a fost identificată ca modelul 1201, bazat pe foaia de catalog: http://public.dhe.ibm. com/common/ssi/ecm/en/wRd03019usen/WGD03019USEN.PDF şi a formatului şi funcţionalităţilor listate la punctul 1.5.4.1.2 *„Echipament hardware dedicat (hardware appliance) pentru colectarea şi analiza fluxurilor de date la nivel 7 OSI (OSI layer 7 flows) şi a log-urilor generate de activele de reţea plus toate licenţele aferente*".

6.3 Subcomponenta de management al riscului a fost identificată ca fiind IBM QRadar Risk Manager conform foii de catalog disponibilă pe http://public.dhe.ibm.com/ common/ssi/ecm/ en/wgd03019usen/WGD03019USEN.PDF şi a formatului şi functionalităţilor listate la 1.5.4.1.3 *„Echipament hardware dedicat (hardware appliance) pentru managementul riscului plus toate licenţele aferente*".

7. *„Echipament hardware dedicat pentru culegerea, înregistrarea, corelarea, interpretarea şi prioritizarea datelor referitoare la evenimentele de securitate (SIEM)*”:

7.1 Răspunsurile din adresa nr. SC-DA-28...2/11.12.2013 la întrebările de clarificare de la 44 la 48, respectiv 69, referitoare la cerinţa 1.5.4.1.1 – *„Echipament hardware dedicat pentru culegerea, înregistrarea, corelarea, interpretarea şi prioritizarea datelor referitoare la evenimentele de securitate (SIEM)*”, menţin obligativitatea unei console centrale de administrare a tuturor componentelor soluţiei (SIEM, Log Management, NBA şi Risk Management).

În opinia contestatorului este inacceptabil faptul că cerinţele punctuale pentru respectivele componente limitează ofertarea doar la produsele IBM (http://public.dhe.ibm.com/common/ssi/ecm/en/wgd 03019usen/ WGD03019USEN.PDF) : IBM Software Security QRadar SIEM all-in-one; IBM Security QRadar Flow Collector; IBM QRadar Risk Manager.

Contestatorul precizează că în piaţă există o multitudine de soluţii SIEM performante ale căror functionalităţi nu sunt astfel limitate şi permit integrarea cu produse de NBA şi Risk Management de la mai mulţi furnizori. Neluarea lor în considerare constituie o încălcare flagrantă a dreptului la libera competiţie.

7.2 Răspunsul din adresa nr. SC-DA-28...2/11.12.2013 la întrebarea nr. 55, referitoare la cerinţa 1.5.4.1.2 *„Echipament hardware dedicat (hardware appliance) pentru colectarea şi analiza fluxurilor de date la nivel 7 OSI (OSI layer 7 flows) şi a log-urilor generate de activele de reţea plus toate licenţele aferente*” subliniază necesitatea ofertării unui echipament dedicat pentru analiza fluxului de date şi a comportamentului reţelei, care să fie administrat de la de la o consolă unică centrală; indică exclusiv IBM Security QRadar Flow Collector, parte integrantă a IBM QRadar Security Intelligence Platform (http://www- 03.ibm.com/software/products/en/qradar).

7.3 Mai mult, în sprijinul afirmaţiilor de mai sus este şi caracterul proprietar al QFlow: fiind singurul tip de metadata de tip flow care - spre deosebire de NetFlow, SFlow, JFlow — conţine informaţia relevantă şi care, în aceste condiţii, permite analiza pana Layer 7 direct din flow-uri. Chiar pe unul din site-urile IBM se menţionează faptul că: „qFlow and vFlow differentiate QRadar from any other product that uses network information for SIEM” (http://www-03.ibm.com/certify/tests/obil95.shtml).

Conform art. 269 din OUG nr. 34/2006, *„procedura de soluţionare a contestaţiilor se desfăşoară cu respectarea principiilor legalităţii, celerităţii, contradictorialităţii şi a dreptului la apărare*”; având în vedere că autoritatea contractantă a invocat în punctul de

vedere nr. SC-DA-29325/23.12.2013, înregistrat la CNSC sub nr. 43948/23.12.2013, excepţia tardivităţii, Consiliul transmite prin fax contestatorului adresa nr. 27202/... ... solicitându-i opinia cu privire la excepţia invocată; contestatorul răspunzând prin adresa nr. 39/30.12.2013, înregistrată la CNSC cu nr. 3/06.01.2014.

Astfel, contestatorul solicită Consiliului solicită respingerea excepţiei ca neîntemeiată, pentru următoarele motive:

- procedura de licitaţia publică a fost demarată în luna octombrie 2013, prin publicarea în SEAP a anunţului de participare nr. ... 30.10.2013. Ulterior acestei date s-au solicitat clarificări cu privire la conţinutul caietului de sarcini;
- răspunsul la întrebările de clarificare, publicate în SEAP la data de 11.12.2013, prin adresa nr. SC-DA-28...2, au arătat faptul că este favorizat, în mod intenţionat, un singur producător (IBM), cu impact major asupra principiului liberei concurenţe, la nivelul descrierii cerinţelor funcţionale ale echipamentelor;
- în aceste condiţii a fost formulată prezenta contestaţie, iar termenul prevăzut de art. 256^2 alin. (2) al OUG nr. 34/2006 curge de la data la care a fost publicat în SEAP răspunsul nr. SC-DA-28...2, respectiv data de 11.12.2013 care completează şi prorogă totodată curgerea termenului de prescripţie;
- acest răspuns este actul autorităţii contractante considerat nelegal, act care afectează întreaga procedură de atribuire. Astfel, data la care s-a publicat acest răspuns în SEAP este cea de la care curge termenul de contestaţie.

Totodată, contestatorul precizează următoarele:

- clarificările urmează aceeaşi procedura ca şi caietul de sarcini, fiind ambele publicate în SEAP;
- aspectele lămuritoare ce au urmat, reprezintă parte a unui întreg şi nu pot fi tehnic şi juridic interpretate separat;
- răspunsul publicat în SEAP este public, astfel încât orice persoană interesată poate să facă contestaţie;
- termenul legal de contestaţie începe să curgă de la ultimul act publicat, respectiv de la data de 11.12.2013, iar contestaţia îndeplineşte condiţiile legale de 10 zile de la data publicării.

În consecinţă, pentru toate aspectele arătate mai sus, contestatorul solicită CNSC respingerea cererii formulate de către autoritatea contractantă în punctul de vedere SC-DA-29325/23.12.2013 privind respingerea contestaţiei ca tardivă.

În ceea ce priveşte fondul cauzei, pentru care autoritatea contractantă solicită CNSC în punctul de vedere nr. SC-DA-29326/ 23.12.2013, respingerea ca nefondată a contestaţiei, contestatorul precizează următoarele:

- în contestaţie s-au indicat câteva aspecte care prin menţinearea lor împiedică participarea liberă la procedură şi „*blochează*” caietul de sarcini pentru un singur producător (IBM);
- nu au fost contestate şi alte puncte din caietul de sarcini, care de asemenea indică un anumit producător, de exemplu:
„1.5.2.1. Soluţie de protecţie a porţii de acces web (web protection gateway) pentru minimum 700 utilizatori”, unde producătorul identificat este CYAN Network Security cu produsul Secure Web Appliance - Model RS8000-X, unicul care are soluţie de stocare *„1 x 64 GB SSD for Cache*”, conform http://www.cyan-networks.com/index.php/de/ressourcen/2013-07-Q3-17-14-28/knowledgebase/secure-web/52-secure-web/hardware/135-sichere-web-appliance-model-rs8000-x, sau
„1.5.2.2. Soluţie de prevenire a pierderilor de date (data loss prevention) la nivel de reţea”, unde producătorul identificat este Symantec, unicul producător care oferă integrarea solicitată cu soluţia de management al drepturilor de acces de la GigaTrust), conform http://www.symantec.com/data-loss-prevention/data-sheets-white-papers.

În situaţiile menţionate în contestaţie, datorită răspunsurilor de clarificare transmise de către autoritatea contractantă prin adresa nr. SC-DA-28...2/11.12.2013, publicată în SEAP, s-a constatat că nu există posibilitatea de a participa cu produse alternative;
- exemplele pe care le menţionează autoritatea contractantă în punctul de vedere nr. SC-DA-29326/23.12.2013, ca alternative, nu sunt deloc relevante şi arată că au fost menţionate doar ca să „*demonstreze*” CNSC că există produse similare pe piaţă;
- exemplele enumerate de către autoritatea contractantă sunt generice şi nu s-a putut identifica nici măcar unul singur care să arate că vreun produs alternativ menţionat satisface 100% cerinţele din caietul de sarcini;
- exemplele enumerate de către autoritatea contractantă menţionează, într-un mod evaziv, doar că produsul x sau y îndeplineşte cerinţele din caietul de sarcini dar, concret nu se poate identifica o soluţie similară, care să fie conformă cerinţelor cumulate din caietul de sarcini.

Contestatorul susţine că la o analiză atentă şi amănunţită aceste exemple nu pot satisface nici pe departe cerinţele din caietul de sarcini, deoarece:

1.1 Se solicită, conform caietului de sarcini al procedurii, la pct. 1.5.1.4 - Platforma de management pentru soluţiile de prevenire a intruziunilor: un sistem hardware dedicat (hardware appliance) plus toate licenţele aferente – *„Administrarea centralizată a soluţiei de securitate integrate, monitorizarea, controlul, corelarea si raportarea*

privind evenimentele de securitate înregistrate de sistemele de protective reţea, host si maşini virtuale. Soluţia trebuie să administreze centralizat elementele de protective împotriva intruziunilor la nivel de reţea, servere fizice şi servere gazdă (host-uri) pentru servere virtuale".

Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebările de clarificare nr. 1 şi nr. 61 (referitoare la pct. 1.5.1.4) menţine obligativitatea unei console de administrare centralizată a tuturor soluţiilor de prevenire a intruziunilor solicitate în caietul de sarcini la punctele 1.5.1.1, 1.5.1.2 si 1.5.1.3, deoarece aceasta consideră ca *„extrem de importantă facilitatea de administrare şi gestionare a tuturor soluţiilor de tip Intrusion Prevention System (IPS) necesare implementării în bune condiţii a soluţiei integrate dintr-un singur punct central, care să permită uşurinţă în utilizare, o integrare mai bună, precum şi uniformizarea politicilor aplicate*".

Conform punctului de vedere nr. SC-DA-29326/23.12.2013, *„Cerinţele pentru soluţiile de tip Host Intrusion Prevention (IPS) formulate în caietul de sarcini sunt generale şi au un caracter minimal, tocmai pentru a nu favoriza un producător anume*" şi sunt enumerate ca şi soluţii conforme cerinţelor din caietul de sarcini urmatoarele: McAfee - Network Security Manager cu licenţele aferente si respective platformele Network Security Platform, Cisco - Sourcefire: FireSIGHT Management Center cu FireAmp şi respectiv platformele NGIPS; HP TippingPoint Security Management System, cu licenţele aferente, respectiv platformele NGIPS.

Conform analizei contestatorului, menţinerea unei console de administrare comune împiedica participarea altor producători având în vedere faptul că numai produsele IBM de tip Network, Host şi Host Virtual au posibilitatea de a fi administrate centralizat; pentru diferite produse de tip Network, Host IPS şi Host Virtual IPS pot fi găsite variante compatibile, dar management-ul acestora nu se se poate face centralizat; dacă se deţine un produs de tip host IPS comaptibil cu cerinţele caietului de sarcini, acesta va putea fi administrat centralizat dintr-o consolă de management specifică acestui produs.

De asemenea, se poate identifica un al doilea produs de tip Network IPS care să satisfacă în mare parte cerinţele, dar şi acesta va putea fi administrat dintr-o consolă de management specifică acestui produs.

În acest caz, problema este că, deşi se pot identifica produse specifice de tip Network IPS şi Host IPS compatibile de la producători diferiţi, acestea nu vor putea fi administrate centralizat din aceeaşi consolă de management, având console de administrare proprietare fiecărui producător.

Cerinţele pentru Host IPS formulate în caietul de sarcini nu sunt generale, aşa cum susţine autoritatea contractantă în punctul de vedere nr. SC-DA-29326/23.12.2013 şi aşa cum s-a menţionat în contestaţie, indică un anumit producător: IBM.

Chiar şi în eventualitatea identificării unui alt producător care să satifacă aceste cerinţe, soluţia în ansamblu nu poate fi conformă din punct de vedere tehnic cu cerinţele din caietul de sarcini deoarece nu poate răspunde cerinţei de administrare centralizată pentru toate produsele IPS solicitate.

Identificarea de către autoritatea contractantă a unor produse *„similare*" de administrare centralizată nu este corectă din punct de vedere al arhitecturii şi a cerinţelor caietului de sarcini, după cum urmează:

- McAfee Network Security Manager - consola de administrare centralizată pentru produse de tip Network IPS şi Host IPS. Această platformă nu satisface cerinţele din caietul de sarcini, deoarece produsele McAfee Host IPS virtual nu sunt conforme cu cerinţele cumulate din caietul de sarcini;
- McAfee Network Security Manager + McAfee Netork Security platform nu răspund la cerinţele caietului de sarcini aşa cum sunt ele formulate şi, în plus, sunt menţionate fără ca măcar autoritatea contractantă să fi citit un sumar al capabilităţilor şi indică o încercare flagrantă de a ascunde faptul că aşa cum este formulat caietul de sarcini, doar produsele IBM se califică la licitaţie;
- Network Security Manager poate fi livrat ca un appliance, însă acesta poate face management la produse de tip network IPS. Deşi sumar se menţionează şi opţiunea de Host IPS, la o citire mai atentă a explicaţiilor din datasheet cât şi a manualului de administrare al soluţiei, reiese că produsul Network Security Manager poate face management doar la produsele de tip NETWORK IPS, iar produsele de tip HOST IPS sunt controlate dintr-o altă consolă de management distinctă, singurul lucru *„comun*" fiind faptul că alertele din consolă pentru produsele de tip Host IPS pot fi trimise şi către consola pentru produsele de tip Network IPS, însă doar pentru a genera alerte, fără a putea face în vreun fel management la aceste produse. Pe lângă aceste aspecte, produsele de tip HOST IPS de la McAfee rulează doar pe platforme Windows, Linux şi Solaris, neexistând suport pentru platformele de tip AIX (https://kc.mcafee.com/corporate/index?page=content&id=KB70778);
- CISCO SourceFire - consola de administrare centralizată pentru produse de tip Network IPS şi anti-malware. Produsele Sourcefire nu acoperă cerinţele de Host IPS şi Host IPS în mediul virtual. (Autoritatea contractantă confundă produsele de Host IPS cu cele de host anti-malware, aflate în portofoliul Cisco SourceFire);

Cisco FireSIGHT Management + FireAMP Connector + NGIPS nu răspund cerinţelor caietului de sarcini pentru că:

- FireAMP rulează doar pe platforme Windows, inclusiv pe maşini virtuale şi platforme mobile de tip Android, fără suport pentru sisteme de operare de tip Solaris sau AIX (https://na8.salesforce. eom/ sfc/p/80000000dRH9mGsP8Q4l9h0h0S0xcYvoz e6QHk =);

- SourceFire virtual appliance poate rula în medii virtualizare VMware sau RedHat Enterprise Virtualization, însă nu are capabilităţi de integrare la nivel de hypervizor pentru a inspecta traficul între maşinile virtuale din acelaşi subnet sau switch virtual (https://na8.salesforce.eom/sfc/p/80000000dRH9KXPUqkSwWBoW3e vtLbnXOyiNg=) şi drept urmare nu răspunde la cerinţele din caietul de sarcini;

- HP TippingPoint - consola de administrare centralizată pentru produse de tip Network IPS; Producătorul HP TippingPoint nu oferă soluţii de Host IPS nici soluţie pentru Host-uri fizice nici pentru host-uri virtuale, ca atare nu se poate folosi în contextul menţinerii cerinţei de administrare centralizata a tuturor soluţiilor IPS.

În opinia contestatorului, aceste exemple menţionate chiar de către autoritatea contractantă sunt elocvente pentru a accepta contestaţia în condiţiile în care susţine că nu se poate folosi o consolă de administrare centralizată de la un alt producător decât IBM în condiţiile îndeplinirii tuturor cerinţelor pentru Network IPS, Host IPS şi Host Virtual IPS din caietul de sarcini.

Contestatorul consideră că este evidentă încercarea .... de a găsi justificări pentru modul în care a fost construit caietul de sarcini, justificări care nu au legătură cu realitatea şi care pot induce în eroare Consiliul.

Totodată, contestatorul afirmă că toate cerinţele „*minimale şi obligatorii*" pentru acest tip de echipament au fost identificate în foaia de catalog a echipamentului IBM Site Protector produs de către IBM, aşa cum a fost menţionat în contestaţie.

1.2 Se solicita conform caietului de sarcini al procedurii, la pct. 1.5.1.1 - Soluţie de prevenire a intruziunilor (IPS) la nivel de reţea: *„Performanţa în reţea, Nivel de echipare 1 (4 echipamente, 1 echipament de rezerva (cold spare), 5 hardware bypass daca este necesar), Throughput trafic real inspectat: minimum 800 Mbps, Latenta: <250 microsecunde, Număr de sesiuni concurente: minimum 1.300.000, Număr de conexiuni/secunda: minimum 35.000*".

Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. 6 (referitoare la pct. 1.5.1.1) *„reiterează faptul că cerinţele enuntate în caietul de sarcini sunt minimale şi obligatorii, latent pentru echipamentul menţionat în*

întrebare trebuie să fie mai mică de 250 microsecunde, iar toate celelalte cerinţe specificate sunt capabilităţi şi caracteristici minimale ce trebuie îndeplinite de soluţia propusă".

Totodată, referitor la legătură dintre numărul de sesiuni concurente de 300.000 şi numărul de conexiuni/secundă de minim 35.000 corelat cu traficul real inspectat de minim 800 Mbps, răspunsul autorităţii contractante este că nu există nicio regulă de corelare între cei 3 parametrii, caracteristicile fiind minimale şi obligatorii, cu excepţia latenţei de 250 microsecunde care trebuie să fie menţinută la un nivel maxim de 250 microsecunde.

Potrivit contestatorului, întrebarea este de ce autoritatea contractantă acceptă ca toţi ceilalţi parametrii să fie minimali, iar pentru latenţă trebuie să fie maxim 250 de microsecunde? De altfel, se contestă acest răspuns care, în opinia contestatorului, modifică, într-un mod clar, documentaţia iniţială pentru că, dacă se dorea într-adevar imparţialitate, autoritatea contractantă ar fi trebuit să considere toate cerinţele minimale şi nu doar aleator.

În punctul de vedere se menţionează: *„De asemenea, considerăm că aceste cerinţe minimale aferente acestui punct (n.n: 1.5.1.1 - Soluţie de prevenire a intruziunilor (IPS) la nivel de reţea, Performanţă în reţea nivel de echipare 1), formulate de autoritatea contractantă în caietul de sarcini pot fi îndeplinite, pe lângă echipamentele menţionate de contestator, cel puţin de echipamentele produse de următorii producători: McAfee Network Security Platform; Cisco-Sourcefire; HP TippingPoint NX NGIPS*".

Chiar dacă unele produse au parametrii menţionaţi mai sus (numărul de sesiuni concurente, numărul de conexiuni/secundă şi throughput trafic real inspectat) conformi cu cerinţele caietului de sarcini şi chiar în condiţiile ofertării unui produs cu parametri superiori, nici unul din produsele enumerate mai sus nu corespunde 100% cerinţelor cumulate din caietul de sarcini pentru acest tip de echipamente, printre care:

- McAfee Network Security Platform M-4050 (conform cu cerinţele minimale şi obligatorii pentru numărul de sesiuni concurente, numărul de conexiuni/secunda şi throughput trafic real inspectat):

- nu deţine interfete de monitorizare 10/100/1000 Mbps cupru, aşa cum se solicită în cerinţele minimale şi obligatorii ale caietului de sarcini, şi anume *„4 x 10/100/1000 Mbps cupru*";

- nu se încadrează în cerinţele dimensionale ale caietului de sarcini, având dimensiunea 2RU, faţă de *„maximum 1U*", aşa cum este solicitat în cerinţele minimale şi obligatorii ale caietului de sarcini.

- Cisco - Sourcefire nu oferă suport IPv6 pe interfaţa de management („command and control”);

- HP TippingPoint NX NGIPS S2600NX (conform cu cerinţele minimale si obligatorii pentru numărul de sesiuni concurente, numărul de conexiuni/secunda şi throughput trafic real inspectat):

- nu se încadrează în cerinţele dimensionale ale caietului de sarcini, având dimensiunea 2RU, faţă de *„maximum 1U*” aşa cum este solicitat în cerinţele minimale şi obligatorii ale caietului de sarcini.

În opinia contestatorului, aceste exemple menţionate chiar de către autoritatea contractantă sunt elocvente pentru a accepta contestaţia în condiţiile în care arată clar că nu există un echipament de tip Network IPS de la un alt producător decât IBM în condiţiile îndeplinirii tuturor cerinţelor pentru Network IPS din caietul de sarcini.

1.3 Se solicită, conform caietului de sarcini al procedurii, la pct. 1.5.1.1 - Soluţie de prevenire a intruziunilor (IPS) la nivel de reţea: Performanţa în reţea, Nivel de echipare 2 (2 echipamente + 2 hardware bypass daca este necesar), Throughput trafic real inspectat: minimum 3 Gbps, Latenţă: <250 microsecunde, Număr de sesiuni concurente: minimum 2.200.000, Număr de conexiuni/ secundă: minimum 50.000.

Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. 8 (referitoare la pct. 1.5.1.1) *„reiterează faptul că cerinţele enuntate în caietul de sarcini sunt minimale şi obligatorii, latenţa pentru echipamentul menţionat în întrebare trebuie să fie mai mică de 250 microsecunde, iar toate celelalte cerinţe specificate sunt capabilităţi şi caracteristici minimale ce trebuie îndeplinite de soluţia propusă*”.

Totodată, referitor la legătură dintre numărul de sesiuni concurente de 2.200.000 şi numărul de conexiuni/secundă de minim 50.000 corelat cu traficul real inspectat de minim 3 Gbps, răspunsul este că nu există nicio regulă de corelare între cei 3 parametri, caracteristicile fiind minimale şi obligatorii, cu excepţia latenţei de 250 microsecunde care trebuie să fie menţinută la un nivel maxim de 250 microsecunde.

În continuare, contestatorul reiterează aceleaşi aspecte ca la punctul anterior.

1.4 Se solicită conform caietului de sarcini al procedurii, la pct. 1.5.1.4 - Platformă de management pentru soluţiile de prevenire a intruziunilor: *„un sistem hardware dedicat (hardware appliance) plus toate licenţele aferente având caracteristicile minimale obligatorii din tabelul de mai jos ... Se va livra o platformă hardware de la acelaşi producător ca al soluţiei de management*”.

Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebările de clarificare nr. 19 şi 23 (referitoare la pct. 1.5.1.4) a „*definit*" ceea ce reprezintă un „*hardware appliance*" şi a menţinut cerinţa referitoare la appliance-ul hardware al platformei de management care trebuie să fie al aceluiaşi producător.

Ca şi la celelalte puncte, susţine că nu se poate califica o altă platformă de management pentru toate produsele IPS care să poată satisface cumulate cerinţele caietului de sarcini, în afară de IBM Site Protector.

În sprijinul afirmaţiilor sale, contestatorul susţine că răspunsurile la întrebarea nr. 23 coroborata cu întrebarea nr.19 referitoare la cerinţa 1.5.1.4, pe lângă menţinerea cerinţei restrictive de a avea o platformă de management comunnă pentru administrarea tuturor soluţiilor IPS se cere în plus ca aceasta să fie livrată ca „*hardware appliance*". Deci, pe lângă faptul că platforma de management trebuie să administreze toate produsele IPS, mai există obligativitatea ca aceasta să fie livrată ca şi „*hardware appliance*" cu condiţia suplimentară ca echipamentul fizic care stă la baza hardware appliance-ului să fie produs de acelaşi producător cu cel al soluţiei de management.

În condiţiile în care ar exista un productor al platformei de management care ar putea sa administreze toate soluţiile de IPS cerute în caietul de sarcini şi acesta ar livra platforma de management ca soluţie software de sine stătătoare şi nu sub forma de „*hardware appliance*", atunci din nou nu se poate califica cu o atfel de soluţie. Ca urmare, consideră că această cerinţă este abuzivă.

De asemenea, în cadrul întrebării s-a încercat a se înţelege la ce exact face referire autoritatea contractantă când menţionează „*hardware appliance*"; răspunsul fiind următorul: „*Hardware appliance este considerat un echipament hardware fizic, dedicate realizarii/ îndeplinirii functionalitatilor/caracteristiciloir solicitate, furnizat de producătorul platformei de management pentru soluţiile de prevenire a intruziunilor, cu toate elementele software şi licenţele aferente integrate*".

Faţă de acest aspect, contestatorul susţine că există producători care oferă soluţiile de management sub forma unei platforme software care poate fi instalată pe echipamente fizice dedicate şi care nu sunt neapărat produse de acelaşi producător cu aplicaţia de management; şi această condiţie este restrictivă.

În opinia contestatorului, exemplele de platforme de management care pot oferi soluţia cerută în caietul de sarcini, enumerate de către autoritatea contractantă sunt total nerelevante atâta timp cât platformele de management menţionate nu pot face

administrarea centralizată a tuturor soluţiilor Network IPS, Host IPS si Host Virtual IPS.

Atât HP TippingPoint Security Management Center cât şi CISCO SourceFire FireSight Management Center nu pot administra produse de tip HOST IPS virtual şi de aceea nu pot fi luate în consideare în contextul arhitecturii şi a cerinţelor din caietul de sarcini. Menţionarea acestora arată ori necunoaştearea soluţiilor ori o încercare de a justifica din nou o cerinţă abuzivă.

2. Se solicită, conform caietului de sarcini al procedurii, la pct. 1.5.1.2 - Soluţie de prevenire a intruziunilor (host IPS) la nivel de server critic - 10 licenţe software, Arhitectura instalare Moduri de operare/funcţionare: Soluţia trebuie sa suporte cel puţin urmatoarele tipuri de sisteme de operare: Windows Server, HP-UX, IBM-AIX, Solaris SPARC. Linux Red Hat.

Se solicită, conform caietului de sarcini al procedurii, la pct. 1.5.1.3 - Soluţie de prevenire a intruziunilor (IPS) la nivel de server gazda (host server) pentru maşini virtuale, *„Arhitectura instalare Moduri de operare/funcţionare: Soluţia trebuie să suporte următoarele tipuri de maşini virtuale: VMware ESX, ESXi, Windows Server 2008 Hyper-V, IBM Power Systems logical partitions si workload partitions HP vPars si nPars Solaris Container*".

Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. 9 (referitoare la pct.1.5.1.2) menţine obligatorie cerinţa ca soluţia să suporte sistemele de operare Windows Server, HP-UX, IBM-AIX şi Solaris SPARC, în plus, menţionând că trebuie suportate cel puţin ultimele două versiuni majore ale acestor sisteme de operare.

Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. 59 (referitoare la pct. 1.5.1.3), punctul c) este că pe platformele sale (maşini virtuale) rulează doar sisteme de operare de tip Windows şi Linux.

Contestatorul susţine că răspunsul autorităţii contractante este în primul rând evaziv, în al doilea rând deşi sunt menţionaţi anumiţi producători consideraţi a fi având produse compatatibile cu caietul de sarcini, un studiu în detaliu al acestor producători relevă faptul că nu au produse compatibile cu caietul de sarcini, după cum urmează: McAfee nu are soluţie de tip HOST IPS pentru Solaris, AIX, HP-UX, Symantec are o soluţie minimala de tip HOST IPS pentru Solarius, AIX, HP-UX însă nu are o soluţie de tip Network IPS, de unde rezultă faptul că nu poate avea o consolă unică de management, Sophos are doar un produs de antivirus pentru HP-UX, AIX şi Solaris fără nici o capabilitate de tip HOST IPS.

Având în vedere cele de mai sus, contestatorul afirmă că prin răspunsul autorităţii contactante se încearcă ascunderea faptului că se favorizează, în mod clar, un singur producător.

Potrivit contestatorului, atâta timp cât în caietul de sarcini se specifică: *„Soluţia trebuie să fie licenţiată per server fizic, la nivel de hypervisor şi să protejeze un număr nelimitat de maşini virtuale găzduite pe hypervisor-ul respectiv. Licenţierea va avea în vedere numărul şi tipul de procesoare instalate pe serverul fizic*", dar nu se menţionează numărul acestora în caietul de sarcini, cum se poate licenţia corect un asfel de produs?; deci, întrebarea nr. 9 este perfect justificată. Totodată, afirmă contestatorul este normal să se cunoască versiunile sistemelor de operare de pe aceste maşini având în vedere că diferiţi producători nu suportă toate aceste versiuni sau nu au mai dezvoltat produse pe versiunile noi apărute având o altă strategie de dezvoltare.

În încercarea de a găsi un produs de tip HOST IPS virtual care să satisfacă cerinţele caietului de sarcini atât din punct de vedere al licenţierii cât şi din punct de vedere al versiunilor sistemelor de operare, întrebarea nr. 59 apare ca fiind perfect justificată.

Potrivit contestatorului, în exemplele menţionate de către autoritatea contractantă ca fiind conforme cu cerinţele din caietul de sarcini referitoare la sistemele de operare suportate, şi anume McAfee, Sophos, Symantec sau Cisco Sourcefire, nu se regăsesc soluţiile de HOST IPS virtual care să fie compatibile caietului de sarcini şi chiar dacă ar fi posibilă găsirea unui astfel de compatibilităţi producătorul respectiv nu ar satisface cerinţele cumulate de Network IPS, ale platformei de management comune precum şi ale hardware appliance-ului dedicat.

3. Se solicită conform caietului de sarcini al procedurii, la pct. 1.5.3.1 - Soluţie pentru managementul vulnerabilitatilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, integrare şi corelare cu sistemele IPS, să aibă capabilităţi de integrare a datelor furnizate de sisteme IPS şi corelare a acestora cu vulnerabilităţile descoperite, printr-o aplicaţie de management comună.

Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. 32 (referitoare la pct. 1.5.3.1) a fost ca *„cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii. Integrarea şi corelarea soluţiei pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP cu sistemele IPS se va realiza conform cerinţei - prin intermediul aplicaţiei de management centralizat comune. Aplicaţia de management centralizat trebuie să dispună de un modul de corelare ce va importa baza de date cu vulnerabilităţi şi o va putea*

corela cu atacurile identificate în timp real de echipamente dedicate pentru prevenirea intruziunilor (IPS). Modul de licenţiere al acestui modul trebuie să permită îndeplinirea tuturor cerinţelor solicitate pentru soluţia pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP. În caietul de sarcini nu sunt specificate cerinţe legate de: înglobarea acestui modul de corelare intr-o component anume sau daca este stand-alone, dacă platforma hardware pe care este livrat trebuie să aibă acelaşi producător ca şi în cazul platformei de management a soluţiei de detectare de intruşi. Furnizorul este cel ce poate detalia modul în care soluţia propusă răspunde cerinţelor şi mecanismelor utilizate pentru aceasta integrare".

Potrivit contestatorului, este specificată în mod clar cerinţa de integrare a soluţiei pentru managementul vulnerabilitatilor cu datele furnizate de sistemele IPS şi că se doreşte corelarea acestora printr-o aplicaţie de management comună; de aceea, prin întrebarea nr. 32 doreşte să clarifice ce înţelege autoritatea contractantă prin acestă platformă de management comună, dacă este diferită de platformă de management a soluţiei IPS, diferită de platforma de management a soluţiei de vulnerability management, dacă este integrată în acestea din urmă, dacă este de tip stand-alone, care este modalitatea de licenţiere s.a.m.d. şi în funcţie de aceste răspunsuri să se poata furniza un produs compatibil şi corect licenţiabil.

De asemenea, având în vedere că este o platformă de management, contestatorul susţine că a încercat să înţeleagă care a fost motivul pentru care la soluţia de management a IPS a fost cerută o platformă hardware livrată de acelaşi producător şi la această platformă de management nu a fost necesară această precizare.

Răspunsul autorităţii contractante menţionează folosirea unei aplicaţii de management centralizat comună. Adică atât soluţiile IPS cât şi soluţiile de Vulnerability management trebuie să poată fi administrate cu ajutorul unei aplicaţii de management comune care să asigure funcţionalităţile cerute în caietul de sarcini.

Contestaţia referitoare la aceast răspuns se referă la faptul că autoritatea contractantă obligă participanţii să folosească o aplicaţie de management comună celor doua soluţii IPS şi vulnerability management. Adică acelaşi producător pentru ambele soluţii şi aceeaşi platformă de management şi corelare.

Această cerinţă este restrictivă şi limitează cerinţele caietului de sarcini la producătorul menţionat, IBM şi în mod particular la IBM Security Fusion.

Exemplele de soluţii „*similare, care îndeplinesc cerinţele caietului de sarcini*" enumerate de către autoritatea contractantă arată posibilitatea de integrare a soluţiilor de management de tip IPS cu

soluţii de vulnerability management ceea ce este perfect posibil dar nu este îndeplinită cerinţa referitoare la platforma comună.

Produsele menţionate de către autoritatea contractantă provin de la producători diferiţi şi care au platforme de management diferite, nefiind posibil managementul lor şi al echipamentelor de tip IPS dintr-o platforma COMUNĂ.

Într-adevăr, produsul Proventia Enterprise Scanner identificat conform cerinţelor din caietul de sarcini nu mai este ofertat de catre IBM: http://www- 01.ibm.com/software/tivoli/products/network-enterprise-scanner/; pe de altă parte, problema ridicată nu se referă la soluţia de scanare, ci la soluţia de management comună a celor 2 soluţii IPS şi Vulnerability Management.

4. Se solicită conform caietului de sarcini al procedurii, la pct. 1.5.3.1 - Soluţie pentru managementul vulnerabilitatilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, performantele analizei, capacitatea de a scana minim 24000 IP-uri pe ora, Capacitatea de a realiza analize complete pentru minim 800 active/oră (all non-DoS-enabled).

Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. 30 (referitoare la pct. 1.5.3.1) a *„reiterat faptul că cerinţele enuntate in caietul de sarcini sunt minimale si obligatorii. Caracteristicile de performanţă solicitate şi anume capacitatea de a scana minim 24000 IP-uri pe oră şi capacitatea de a realiza analize complete pentru minim 800 active/ora (all non-DoS-enabled) sunt capabilităţi pe care trebuie să le deţină soluţia ofertată, astfel încât să nu necesite cheltuieli suplimentare pentru asigurarea scanării şi analizei unui număr mult mai mare de echipamente identificabile prin IP, acest necesar fiind în prezent de 2000 active*".

Contestaţia cu privire la această întrebare de clarificare a fost formulată pe fondul imposibilităţii autorităţii contractante de a formula o corelare logică între numărul de IP-uri scanate pe oră (24000), capacitatea de a realiza analize complete pentru minim 800 active/oră şi numărul de 2000 active solicitate în cadrul soluţiei.

Aşa cum a fost precizat în contestaţie, aceşti parametrii au fost preluaţi din două foi de catalog IBM (ataşate ca şi Anexa 5 şi 6), fără a exista o corelare logică la momentul elaborarii caietului de sarcini.

Având în vedere faptul că singurul producător care foloseste terminologia „all non-DOS enabled" pentru analize complete pentru cel puţin 800 de host-uri pe ora este IBM, reiese clar, în opinia contestatorului, că se favorizează IBM în detrimentul celorlalţi producători de pe piaţă.

Ulterior, în punctul de vedere nr. SC-DA-29326/23.12.2013, aceste valori sunt puse pe seama faptului că *„managementul*

vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP nu trebuie să se limiteze la nevoile curente şi în consecinţă trebuie să fie scalabilă pentru acoperirea necesităţilor viitoare pentru cel puţin o perioadă de 5,6 ani".

Contestatorul susţine că, chiar dacă autoritatea contractantă atrage atenţia asupra unui fapt cunoscut şi anume acela că produsul IBM Proventia Enterprise la care s-a făcut referire în contestaţie nu mai este ofertat de producătorul IBM încă din anul 2011, acest lucru nu motivează preluarea caracteristicilor enumerate mai sus din cele două foi de catalog IBM şi elaborarea caietului de sarcini pe baza acestor parametri.

5. Se solicită conform caietului de sarcini al procedurii, la pct. 1.5.3.1 - Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, 1 port serial accesibil pe partea frontal cu conector RJ-45 si 2 porturi USB 2.0 accesibile pe partea frontală.

- Răspunsul autorităţii contractante conform adresei nr. SC-DA-28...2/11.12.2013 la întrebarea de clarificare nr. ... (referitoare la pct. 1.5.3.1) *„a subliniat încă o dată că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii şi că se doreşte ca soluţia să fie livrată ca echipament hardware dedicat (hardware appliance), furnizat ca atare de producător având sistem de operare proprietar, complet securizat. Sunt solicitate în mod specific pe partea frontal doar 1 port serial cu conector RJ-45 si 2 porturi USB 2.0, nefiind menţionată si nici necesară o ordine anume a acestor porturi. Modul de distribuţie al celorlalte interfeţe solicitate este determinat de producătorul echipamentului. Descrierea interfeţelor furnizată în caietul de sarcini corespunde funcţionalităţilor solicitate*".

Potrivit contestatorului, întrebarea de clarificare nr. ... a încearcat să clarifice cerinţele hardware necesare aplicaţiei de management; în opinia sa, fiind evident faptul că aceste specificaţii au fost preluate de la produsul IBM Proventia Network Enterprise Scanner, singurul produs care dispunea de aceste interfeţe şi acest număr de interfeţe specific pe partea frontală a echipamentului.

Ulterior, în punctul de vedere nr. SC-DA-29326/23.12.2013, se menţionează uşurinţa în utilizare, ceea ce este corect din punct de vedere funcţional dar nu este justificabil din punct de vedere al arhitecturii şi de asemenea nu se fac precizări la numărul de intervenţii preconizat pentru acest echipament pentru a justifica o astfel de uşurinţă în accesare. Adică în condiţiile unei accesari dese şi nenumarate la acest echipament se poate justifica nevoia de uşurinţă în exploatare, dar autoritatea contractantă nu menţionează aceste lucruri.

Totodată, contestatorul arată că autoritatea contractantă a menţionat faptul că *„este mult mai uşor pentru un operator uman, atât din punctul de vedere al identificării echipamentului (în partea dorsală elementele de identificare sunt practic inexistente iar lungimea echipamentelor poate diferi foarte mult), cât şi din punct de vedere al uşurinţei în utilizare (în partea dorsală a unui rack plin de echipamente este evacuată toata căldură produsă de acestea fiind practic imposibil să se poată lucra într-o astfel de zonă mai mult de câteva minute)*”.

Explicaţia privind uşurinţa în identificarea echipamentului de către operatorul uman prin vizualizarea porturilor amplasate pe partea frontală, este total lipsită de logică, pentru că identificarea unui echipament se face cu ajutorul etichetelor (ce conţin de regulă tipul echipamentului, model, serie, data fabricaţiei, ţara de origine, producător) amplasate de producător pe echipament; un operator uman se conectează la porturile specificate mai sus doar în cazuri speciale când echipamentul nu poate fi accesat prin adresa IP, la instalare sau în cazul unei defecţiuni, accesarea echipamentului de către operator făcându-se întotdeauna prin intermediul cablurilor de management specifice (cu conectori RJ-45 sau USB), ce au lungimi variabile, ce permit lucrul la partea frontală a echipamentelor în condiţii de uşurinţă şi confort sporit.

Explicaţia funcţionalităţii dată de autoritatea contractantă arată încercarea de a justifica existenţa în caietul de sarcini a specificaţiilor identice cu cele ale echipamentului IBM Proventia Network Enterprise Scanner printr-un mod funcţional care nu poate fi acceptabil în condiţiile în care nici un echipament cerut în caiet nu are cerinţe similare.

Contestatorul arată că se contestă intenţia autorităţii contractante de a specifica cu stricteţe aceste porturi, de a menţiona exact numărul lor susţinând că au fost preluate de la un anumit producător.

6. Se solicită conform caietului de sarcini al procedurii, la pct. 1.5.4.1 - Echipament hardware dedicat (hardware appliance) pentru culegerea, înregistrarea, corelarea, interpretarea şi prioritizarea datelor referitoare la evenimentele de securitate (SIEM), plus toate licenţele aferente.

Conform răspunsului autorităţii contractante din adresa nr. SC-DA-28...2/11.12.2013 la întrebările de clarificare nr. 36 şi 37 (referitoare la pct. 1.5.4.1), *„cel puţin componentele SIEM, Network Behavior Analysis şi Risk Management să fie echipamente dedicate*”.

Analizând răspunsul la întrebările de clarificare, reiese, într-un mod evident, faptul că arhitectura solicitată este specifică soluţiei IBM

- QRadar All-în-One 3105 (subcomponente, denumiri şi caracteristici de performanţă).

6.1 Pentru subcomponenta SIEM (pct. 1.5.4.1.1), cele două soluţii identificate de către autoritatea contractantă ca *„putând îndeplini cu siguranţă cerinţele referitoare la scalabilitate*”, şi anume McAfee şi ArcSight permit de asemenea scalabilitate dar nu în modelul arhitectural cerut în caietul de sarcini (prin licenţă, fără înlocuirea echipamentului).

6.2 Pentru subcomponenta *„Echipament hardware dedicat (hardware appliance) pentru colectarea si analiza fluxurilor de date la nivel 7 OSI (OSI layer 7 flows) si a log-urilor generate de activele de reţea plus toate licenţele aferente (pcs. 1.5.4.1.2), soluţiile identificate de către .... care să poată îndeplini cerinţele specificate în caietul de sarcini*”, respectiv: McAfee Network Threat Behavior Analysis, precum şi integrare API pentru achiziţie NetFlow şi informaţii Layer 7 - ex. StealthWatch FlowCollector si respective integrarea acestuia cu diferite soluţii SIEM - HP ArcSight si TippingPoint, Cisco Cyber Threat Defense Solution, a identificat diferite echipamente de pe piaţă care pot achiziţiona Flow-uri şi infomatii layer 7, dar nu au aceeaşi consolă de management comună cu soluţia de SIEM aşa cum se cere în caietul de sarcini.

În răspunsul său, autoritatea contractantă menţine obligativitatea unei console centrale de administrare indiferent dacă în paralel se acceptă şi posibilitatea de realizare a managementului descentralizat; cu alte cuvinte, dacă soluţiile alternative oferă un management descentralizat specific fiecărei soluţii în parte, nu pot fi în acelaşi timp administrate şi centralizat, deci soluţia propusă nu este conformă; de aceea, contestaţia se referea la obligativitatea introdusă de autoritatea contractantă de a avea un managenent centralizat în orice situaţie, condiţie considerată ca fiind restrictivă pentru accesul altor producători de echipamente specific la această procedură de achiziţie prin licitaţie deschisă.

6.3 Referitor la subcomponenta *„Echipament hardware dedicat (hardware appliance) pentru managementul riscului plus toate licenţele aferente*” (pct. 1.5.4.1.3), soluţiile identificate de către autoritatea contractantă care „po*t îndeplini cerinţele specificate în caietul de sarcini*” şi care *„se integrează cu soluţii SIEM*”, şi anume: McAfee Risk Manager sau integrare HP ArcSight su Skybox Security, contestatorul susţine că nu se pot administra dintr-o singură consolă aşa cum cere caietul de sarcini şi unele dintre aceste soluţii propuse nu sunt compatibile cu cerinţele din caietul de sarcini.

Astfel, susţine contestatorul, deşi autoritatea contractantă menţionează că cere echipamente separate cu funcţionalităţi de tip SIEM, Log Management, Network Behavior Analysis, iar în capitolul

de arhitectură se cere o consolă de management centralizată, reiese clar faptul că toate echipamentele trebuie să fie de la acelaşi producător; în răspunsul autorităţii contractante, deşi se dau exemple de integrări între producători, aceasta se contrazice mai apoi insistând pe faptul că toate produsele trebuie să aibă o consolă centrală de management, lucru posibil doar dacă toate produsele cerute sunt de la acelaşi producător. Nu există producător în acest domeniu care să aibe în ofertă produse care fac managementul altor produse, mai ales ca de exemplu un produs de tip SIEM nu face management la nici un alt produs ci doar agrega, normalizeaza şi coreleaza loguri.

În răspunsul său, autoritatea contractantă menţine obligativitatea unei console centrale de administrare indiferent dacă în paralel se acceptă şi posibilitatea de realizare a managementului descentralizat; de aceea, contestatia se referă la obligativitatea introdusă de autoritatea contractantă de a avea un management centralizat în orice situaţie, condiţie considerată restrictivă pentru accesul altor producători de echipamente la această procedură de achiziţie publică.

7. Se solicită conform caietului de sarcini al procedurii, la pct. 1.5.4.1.1 - Echipament hardware dedicat (hardware appliance) pentru culegerea, înregistrarea, corelarea, interpretarea si prioritizarea datelor referitoare la evenimentele de securitate (SIEM).

7.1 Conform răspunsului autorităţii contractante din adresa nr. SC-DA-28...2/11.12.2013 la întrebările de clarificare de la nr. 44 la nr. 48, respective nr. 69 (pct. 1.5.4.1.1), se menţine obligativitatea unei console central de administrare a tuturor componentelor soluţiei (SIEM, Log Management, NBA şi Risk Management).

Contestatorul arată că autoritatea contractantă menţine obligativitatea unei console centrale de administrare indiferent dacă în paralel acceptă şi posibilitatea de realizare a managementului descentralizat; cu alte cuvinte, dacă soluţiile alternative oferă un management descentralizat specific fiecărei soluţii în parte şi nu pot fi în acelaşi timp administrate şi centralizat, soluţia propusă nu este conformă.

Având în vedere că autoritatea contractantă a identificat produse *„similare”* care pot răspunde punctual funcţionalităţilor cerute în caietul de sarcini, contestatorul îi **solicită** acesteia să explice Consiliului şi posibililor ofertanţi cum pot fi administrate aceste produse centralizat având în vedere că sunt producători diferiţi care folosesc console de management diferite.

În opinia contestatorului, menţinerea acestei cerinţe este abuzivă; ca urmare, contestă răspunsul la întrebările de la nr. 44 la nr. 48 si respectiv nr. 69, care menţin această cerinţă şi adaugă

cerinţa de descentralizare dar numai în contextul păstrării cerinţei de management centralizat, fapt care modifică cerinţele iniţiale ale caietului de sarcini.

7.2 Conform răspunsului autorităţii contractante din adresa nr. SC-DA-28...2/11.12.2013 la întrebarea de Clarificare nr. 55 (pct. 1.5.4.1.2), se subliniază necesitatea ofertării unui echipament dedicat pentru analiza fluxului de date şi a comportamentului reţelei şi trebuie să ofere ambele funcţionalităţi: analiza fluxului de date şi analiza log-urilor generate de activele de reţea.

Se contestă acest răspuns în condiţiile în care echipamentul identificat - IBM Security Qradar Flow Collector - este singurul care poate oferi aceste funcţionalităţi în condiţiile arhitecturii cerute de autoritatea contractantă (adică management centralizat obligatoriu pentru toate companenetele soluţiei); în acest sens, se pot identifica echipamente specifice pentru colectarea logurilor şi echipamente dedicate specifice pentru colectare de flows, dar nu se poate oferi o soluţie conformă în condiţiile menţinerii cerinţei respective de management centralizat având în vedere că aceste cerinţe pot fi realizate de către produse diferite care au şi administrare diferită.

În cazul exemplelor autorităţii contractante, McAfee Application Data Monitor - este un produs de sine stătător cu funcţionalităţi clare şi precise de a identifica anomalii, scurgeri de date şi alte activităţi care nu sunt acceptate într-un mediu de lucru, nicidecum de a exporta flow-uri într-un altfel de echipament, iar Sourcefire - nu are nici o legătură cu soluţiile de colectare simultană de flow şi de loguri.

7.3 Faţă de exemplul dat de către autoritatea contractantă privind *„alţi producători în afara celui identificat de contestatoare care oferă echipamente care pot colecta si analiza flow-uri de tip Qflow, cum ar fi de exemplu Juniper*”, contestatorul face menţiunea că producătorul Juniper foloseşte în produsele sale tehnologie OEM IBM QRadar, deci aceeaşi soluţie identificată şi menţionată în contestaţie.

Faţă de precizările din contestaţie şi din răspunsul la punctul de vedere al autorităţii contractante, contestatorul concluzionează că:

1. Nici una din soluţiile menţionate de către autoritatea contractantă ca fiind variante alternative de produse nu sunt conforme cu documentaţia de atribuire.

2. Autoritatea contractantă nu a arătat, în mod clar, pentru niciuna din soluţiile alternative propuse conformitatea de 1:1 cu cerinţele caietului de sarcini. Doar menţiunea că anumite produse sunt conforme cu anumite cerinţe punctuale, nu este relevantă.

3. De asemenea, răspunsul autorităţii contractante nu arată decât punctual modul în care anumite produse diferite de cele identificate în caietul de sarcini ar putea satisface cerinţele acestuia. Se omite în mod clar componenta de arhitectură şi funcţionalitate în

ansablu care introduc restricţiile menţionate pe parcursul acestui răspuns.

4. A explicat modalitatea de restrângere a soluţiilor conforme cu cerinţele cumulate din caietul de sarcini către un singur producător - IBM - prin introducerea şi menţinerea de platforme de management centralizat pentru soluţiile de securitate solicitate.

5. De asemenea în vederea transparenţei şi a corectitudinii, susţine că va cere producătorilor menţionaţi de autoritatea contractantă în punctul de vedere nr. SC-DA- 29326/23.12.2013 să specifice în mod clar dacă produsele în cauză sunt sau nu compatibile cu cerinţele din documentaţia de atribuire.

6. De asemenea, dacă se doreşte, se poate înainta această documentaţie pentru obţinerea unui punct de vedere şi Comitetului Tehnico-Economic pentru Societatea Informaţională din cadrul MCSI, pentru a obţine un punct de vedere şi din acest loc.

7. Dorinţa clar exprimată nu este de a bloca acest proces de achiziţie şi nici de a întârzia proiectul.

8. În cadrul contestaţiei precum şi al întrebărilor nu s-a insistat pe cerinţele din caietul de sarcini care ofereau deschidere către alţi producători.

9. În opinia contestatorului, nu se pot realiza cerinţele caietului de sarcini, cu excepţia folosirii doar a soluţiilor producătorului menţionat în contestaţie.

În vederea soluţionării contestaţiei depuse de ... Consiliul a solicitat autorităţii contractante, prin adresa nr. 26702/ .../... transmiterea dosarului achiziţiei, precum şi punctul de vedere cu privire la contestaţia în cauză, potrivit dispoziţiilor art. 274 alin. (1) din OUG nr. 34/2006; autoritatea contractantă, răspunzând prin adresa nr. SC-DA-29325/23.12.2013, înregistrată la CNSC sub nr. 43948/23.12.2013.

În punctul său de vedere, ... solicită Consiliului respingerea contestaţiei, pe cale de excepţie ca tardivă, iar pe fond, ca nefondată.

1. Pe cale de excepţie, în susţinerea excepţiei tardivităţii, autoritatea contractantă invocă dispoziţiile art. 256^2 din OUG nr. 34/2006 şi faptul că în partea introductivă a contestaţiei, chiar contestatorul menţionează expres că *„în urma analizei documentaţiei de atribuire: fişa de date, caiet de sarcini, anexe la caietul de sarcini şi răspunsurile la solicitările de clarificări, au fost identifiate abateri grave care încalcă prevederile legale privind achiziţiile publice...”*. Prin urmare, fiind vorba de o contestaţie cu privire la conţinutul documentaţiei de atribuire care a fost publicată în SEAP, conform art. 75 alin. (5) din OUG nr. 34/2006, în data de 30.10.2013, în conformitate cu prevederile art. 256^2 din OUG nr. 34/2006 citat mai sus, coroborate cu prevederile art. 3 lit. z) din acelaşi act normativ,

contestaţia trebuia înaintată Consiliului până la data de 11.11.2013. Întrucât ... a înaintat Consiliului această contestaţie referitoare la documentaţia de atribuire, la data de ... contestaţia în cauză trebuie respinsă ca tardivă.

Autoritatea contractantă consideră că se poate observa că ... încearcă să eludeze prevederile legale imperative menţionate mai sus (care statuează cu claritate că termenele privind formularea unei contestaţii cu privire la o documentaţie de atribuire curg de la data publicării acesteia în SEAP) şi încearcă să inducă ideea, contrazisă chiar de conţinutul contestaţiei, că actul atacat îl reprezintă răspunsul nr. SC-DA- 28...2/11.12.2013 publicat în SEAP, la solicitarea sa de clarificare. În acest sens, solicitarea de clarificări cuprinzând un număr foarte mare de întrebări (formulată de ... în ultima zi posibilă pentru solicitarea clarificărilor conform documentaţiei de atribuire şi conform art. 78 alin. (2) şi art.79 alin. (1) din OUG nr. 34/2006), nu urmăreşte lămurirea/ explicitarea/limpezirea prevederilor caietului de sarcini, ceea ce reprezintă funcţia şi scopul unei solicitări de clarificări conform prevederilor legale aplicabile, ci reprezintă cereri explicite de modificare a caietului de sarcini sau întrebări formulate critic cu privire la cerinţele din caietul de sarcini, cu scopul evident de a fabrica un temei pentru formularea unei contestaţii.

Autoritatea contractantă precizează că răspunsul său la solicitarea de clarificări, răspuns publicat în SEAP şi înregistrat cu nr. SC-DA-28...2/11.12.2013 nu aduce vreun element nou sau vreo interpretare nouă faţă de conţinutul documentaţiei de atribuire şi nu modifică conţinutul documentaţiei de atribuire, iar contestaţia formulată de ... nu se referă la modificări sau completări ale unor cerinţe menţionate expres în caietul de sarcini şi publicate în SEAP. Faptul că această contestaţie formulată nu vizează răspunsul la solicitările de clarificări, ci chiar conţinutul documentaţiei de atribuire, rezultă fără dubiu chiar din solicitarea formulată prin prezenta contestaţie.

Autoritatea contractantă evidenţiază faptul că ... solicită explicit modificarea documentaţiei de atribuire şi nu modificarea sau completarea răspunsului la solicitarea de clarificări pe care îl invocă drept temei al contestaţiei. Astfel, subliniază, pentru fiecare critică din cuprinsul contestaţiei, folosind numerotarea utilizată de contestator, aspectele din care, în opinia sa, rezultă cu claritate concluzia tardivităţii contestaţiei:

1.1. Întrebările de „*clarificare*” 1 şi 61 indicate, reprezintă de fapt solicitări de modificare a caietului de sarcini:

- la întrebarea nr. 1, faţă de cerinţa privind un sistem hardware dedicat, se solicită *„vă rugăm să clarificaţi dacă se acceptă administrarea tuturor produselor de protecţie împotriva intruziunilor*

din mai multe console specifice fiecărui tip de produs". Răspunsul autorităţii este că nu se modifică cerinţa din caietul de sarcini, se justifică răspunsul şi se detaliază cerinţa din caietul de sarcini;
- la întrebarea nr. 61, se solicită modificarea aceleiaşi cerinţe şi se primeşte acelaşi răspuns din partea autorităţii contractante;
- din cuprinsul contestaţiei pct.1.1 rezultă clar că se contestă faptul că răspunsurile *„menţin obligativitatea unei console de administrare centralizată a tuturor soluţiilor de prevenire a intruziunilor solicitate în caietul de sarcini la punctele 1.5.1.1, 1.5.1.2 şi 1.5.1.3*" adică menţin cerinţele caietului de sarcini.

1.2. Întrebarea de „*clarificare*" nr. 6 indicată de contestator, reprezintă de fapt o cerere de modificare a caietului de sarcini.
- la întrebarea nr. 6, faţă de cerinţa ca latenţa să fie mai mică de 250 microsecunde, se solicită să se accepte latenţa mai mare de 250 microsecunde;
- răspunsul este că se menţine cerinţa din caietul de sarcini;
- din cuprinsul contestaţiei pct.1.2 rezultă că se contestă faptul că răspunsurile autorităţii contractante *„lasă nemodificată cerinţa iniţială*" adică menţin cerinţele caietului de sarcini.

1.3 Aceeaşi situaţie ca în cazul 1.2. şi faţă de cerinţa explicită din caietul de sarcini privind latenţa mai mică de 250 microsecunde, prin întrebarea nr. 8 contestatorul solicită să se accepte latenţă mai mare de 250 microsecunde. Răspunsul este că se menţine cerinţa din caietul de sarcini, iar ... contestă că răspunsul autorităţii *„lasă nemodificată cerinţa iniţială*".

1.4. Similar cu cele de mai sus este şi cerinţa de a se livra o platformă hardware de la acelaşi producător ca al soluţiei de management, se solicită modificarea caietului de sarcini în sensul de a se accepta o platformă hardware din partea unui producător diferit. Răspunsul este că nu se acceptă modificarea caietului de sarcini, iar ... la pct. 1.4 contestă cerinţa din caietul de sarcini.

2. Răspunsurile la întrebările 9 şi 59 indicate de contestator reiterează că se menţin cerinţele din caietul de sarcini pe care le explică prin raportare la solicitarea de clarificări. Potrivit autorităţii contractante, nu se modifică niciuna dintre cerinţele din caietul de sarcini, iar contestatorul critică chiar cerinţa 1.5.1.2. din caiet pe care o cunoştea sau trebuia să o cunoască încă de la momentul publicării documentaţiei în SEAP.

3. Criticile de la pct. 3 sunt similare celor de la pct. 2: Răspunsul la întrebarea nr. 32 nu modifică cerinţa din caietul de sarcini ci doar explică această cerinţă arătând explicit că *„în caietul de sarcini nu sunt specificate cerinţe legate de: înglobarea acestui mod de corelare într-o componentă anume sau dacă este stand-alone, dacă platforma hardware pe care este livrat trebuie să aibă acelaşi*

producător ca şi în cazul platformei de detectare de intruşi". Se subliniază că „*furnizorul este cel ce poate detalia modul în care soluţia propusă răspunde cerinţelor şi mecanismele utilizate pentru integrare*".

4. Criticile de la acest punct relevă expres faptul că ... critică de fapt caietul de sarcini publicat în SEAP, iar scopul întrebării nr. 30 este de asemenea, de a critica aceste cerinţe fabricând astfel un temei pentru aparenţa unei contestaţii în termen. Astfel chiar în cuprinsul contestaţiei, contestatorul arată faptul că solicitarea de clarificări este pentru „*lămurirea necesităţii unor cerinţe de performanţă disproporţionate fată de numărul de active*". Nici cu privire la această întrebare, răspunsul nu modifică caietul de sarcini şi explică cerinţa criticată prin solicitarea de clarificări.

5. Şi la acest punct rezultă faptul că ... contestă decizia de a se „*menţine cerinţa obligatorie de prezentare a următoarelor porturi[...]*", adică de a nu modifica caietul de sarcini, ceea ce înseamnă în mod evident că se contestă tardiv caietul de sarcini.

6. Situaţia este similară punctului 1.1.; respectiv faţă de cerinţa unei platforme unificată, integrată prin întrebările 36 şi 37 se solicită modificarea caietului de sarcini prin acceptarea folosirii mai multor echipamente. Răspunsul este în sensul că nu se modifică cerinţa din caietul de sarcini, se justifică răspunsul şi se detaliază cerinţa din caietul de sarcini.

7. ... contestă decizia autorităţii contractante de a menţine „*obligativitatea unei console centrale de administrare a tuturor componentelor soluţiei [...]*" adică de a nu modifica caietul de sarcini.

Autoritatea contractantă subliniază că singurele obligaţii instituite prin lege în sarcina sa sunt acelea de a răspunde în mod clar, complet şi fără ambiguităţi şi cât mai repede posibil la orice clarificare solicitată, într-o perioadă care nu trebuie să depăşească, de regulă, 3 zile lucrătoare de la primirea unei astfel de solicitări din partea operatorului economic (art. 78 alin. (2) din OUG nr. 34/2006). Mai mult decât atât, după cum se poate observa, răspunsul din adresa nr. SC-DA-28...2/11.12.2013, este publicat în SEAP cu respectarea termenului legal, iar răspunsurile date sunt clare şi complete în sensul menţinerii cerinţelor din caietul de sarcini. De altfel, după cum rezultă clar din cuprinsul contestaţiei, nu se contestă lipsa de claritate a răspunsurilor autorităţii, ci menţinerea de către aceasta a cerinţelor din caietul de sarcini, ceea ce, în opinia contestatorului, reprezintă „*încălcarea principiului liberei concurenţe şi favorizarea unul anumit producător*".

În concluzie, pentru toate motivele arătate mai sus, autoritatea contractantă solicită respingerea ca tardivă a contestaţiei formulate de

... în conformitate cu prevederile art. 256^2 alin. (1) şi alin. (2), art. 271 alin. (1) şi art. 278 alin. (5) din OUG nr. 34/2006.

2. Pe fondul cauzei, autoritatea contractantă solicită Consiliului respingerea contestaţiei ca nefondată. Ca o observaţie generală, cu privire la conţinutul contestaţiei formulate de ... autoritatea contractantă subliniază faptul că aceasta solicită doar *„modificarea documentaţiei de atribuire*" fără a preciza măcar, în mod concret, schimbările care doreşte să fie dispuse de către Consiliu.

În continuare, autoritatea contractantă face precizări referitoare la criticile formulate de către contestator, susţinând că acuzaţiile de favorizare intenţionată a unui unic producător sunt nefondate, răspunsurile sale păstrând numerotarea contestatorului:

1.1. Întrebarea nr. 1 referitoare la cerinţa *„1.5.1.4 Platforma de management pentru soluţiile de prevenire a intruziunilor: un sistem hardware dedicat (hardware appliance) plus toate licenţele aferente*", care urmărea de fapt modificarea caietului de sarcini, cerea *„să se clarifice dacă se accepta administrarea tuturor produselor de protecţie împotriva intruziunilor din mai multe console specifice fiecărui tip de produs*".

Întrebarea de clarificare nr. 61 referitoare la cerinţa 1.5.1.4 Platforma de management pentru soluţiile de prevenire a intruziunilor: un sistem hardware dedicat (hardware appiiance) plus toate licenţele aferente – *„Administrarea centralizată a soluţiei de securitate integrate, monitorizarea, controlul, corelarea şi raportarea privind evenimentele de securitate înregistrate de sistemele de protecţie reţea, host şi maşini virtuale. Soluţia trebuie să administreze centralizat elementele de protecţie împotriva intruziunilor la nivel de reţea, servere fizice şi servere gazdă (host-uri) pentru servere virtuale*" cerea *„acceptarea unei soluţii integrate, iar administrarea politicilor avansate de IPS pentru reţea física si virtuala să se facă separat de administrarea politicilor avansate la nivel de endpoint*".

Răspunsurile menţin obligativitatea unei console de administrare centralizată a tuturor soluţiilor de prevenire a intruziunilor solicitate în caietul de sarcini la punctele 1.5.1.1, 1.5.1.2 si 1.5.1.3, deoarece consideră extrem de importantă facilitatea de administrare şi gestionare a tuturor soluţiilor de tip Intrusion Prevention System (IPS) necesare implementării în bune condiţii a soluţiei integrate dintr-un singur punct central, care să permită uşurinţă în utilizare, o integrare mai bună, precum şi uniformizarea politicilor aplicate.

Cerinţele pentru soluţiile de tip Host Intrusion Prevention (IPS) formulate în caietul de sarcini sunt generale şi au un caracter minimal, tocmai pentru a nu favoriza un producător anume.

Capabilităţile de detecţie şi blocare ale engine-urilor de protecţie, tehnologiile de detecţie şi prevenire a intruziunilor, tipurile de

monitorizare sunt capabilităţi şi caracteristici cheie pentru soluţiile de acest tip şi, contrar celor afirmate de contestator, sunt oferite de mai mulţi dintre producătorii de astfel de produse.

Astfel, în afară de soluţia la care se face referire în motivarea ...., mai pot fi identificate cel puţin următoarele soluţii comerciale care răspund cerinţelor formulate în caietul de sarcini:

- McAfee - Network Security Manager cu licenţele aferente (http://www.mcafee.com/us/products/network-security-manager. aspx) şi respectiv platformele Network Security Platform (http://www.mcafee.com/us/products/network-security-platform. aspx);
- Cisco-Sourcefire: FireSIGHTManagement Center (http:// www.sourcefire.com/products/firesight-management-center) cu FireAmp (http://www.sourcefire.com/products/fireamp-connectors) şi respectiv platformele NGIPS (http://www.sourcefire.com/ products/next- generation-network-security);
- HP TippingPoint Security Management System cu licenţele aferente (http://www8.hp.com/us/en/software-solutions/software. html?compURI=1344453#tab=TABl) şi respectiv platformele NGIPS (http://www8.hp.com/us/en/software-solutions/software,html?Comp URI =1343617#tab=TAB2).

- În concluzie, întrucât cerinţele formulate în caietul de sarcini sunt minimale şi, aşa cum s-a arătat mai sus, pot fi identificate cel puţin încă trei soluţii care corespund cerinţelor caietului de sarcini, rezultă că este total neîntemeiată afirmaţia contestatorului în sensul că se favorizează un unic producător.

1.2 Întrebarea numărul 6 referitoare la cerinţa *„1.5.1.1 Soluţie de prevenire a intruziunilor (IPS) la nivel de reţea: Performanţa în reţea, Nivel de echipare 1 (4 echipamente, 1 echipament de rezervă (coid spare), 5 hardware bypass dacă este necesar), Throughput trafic real inspectat: minimum 800 Mbps, Latenţa: < 250 microsecunde, Număr de sesiuni concurente: minimum 1.300.000, Număr de conexiuni/secundă: minimum 35.000*" cerea modificarea cerinţei din caietul de sarcini, şi anume: *„dacă la cerinţele de performanta în reţea se acceptă ca latenţa echipamentului să fie mai mare de 250 microsecunde*". De asemenea, se cerea *„să se clarifice dacă există o legătură între numărul de sesiuni concurente de 300.000 si numărul de conexiuni/secunda de min. 35.000 corelat cu traficul real inspectat de minim 800 Mbps*".

Răspunsul a reiterat faptul că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii, latenţa pentru echipamentul menţionat în întrebare trebuie să fie mai mică de 250 de microsecunde, iar toate celelalte cerinţe specificate sunt capabilităţi şi caracteristici minimale ce trebuie îndeplinite de soluţia propusă.

Nu există nicio regulă de corelare între cei 3 parametri specificaţi în întrebare, şi anume:

- Numărul de sesiuni concurente reprezintă numărul total de sesiuni care poate fi susţinut de platformă, inclusiv în cazul unui atac de tip DDoS, de exemplu. Dacă acest parametru este subdimensionat se poate ajunge foarte repede în situaţia în care traficul de date este complet blocat;
- Numărul de conexiuni pe secundă se referă la câte conexiuni pe secundă poate susţine echipamentul, din punct de vedere al stabilirii acestora (conexiuni noi). Suportarea unui număr mai mare de conexiuni pe secundă permite evitarea sau reducerea efectelor negative în cazul atacurilor care încearcă stabilirea unui număr foarte mare de conexiuni în unitatea de timp;
- Traficul inspectat exprimat în Mbps se referă în special la conţinutul / ataşamentul din sesiuni - poate exista situaţia cu câteva sesiuni cu 400 Mbps conţinut ataşat şi inspectat sau pot fi 10.000 sesiuni fiecare cu un total de 100 Mbps conţinut ataşat şi inspectat, în funcţie de specificul traficului şi respectiv în funcţie de politicile de inspecţie definite. Traficul suportat de acest echipament trebuie să fie astfel dimensionat încât să nu producă întârzieri în segmentele de reţea monitorizate.

Autoritatea contractantă susţine că marea majoritate a producătorilor de astfel de echipamente specifică aceşti parametri, multe dintre produsele lor având caracteristici superioare celor menţionate în caietul de sarcini aferent prezentei proceduri de atribuire.

De asemenea, cerinţele minimale aferente acestui punct, formulate în caietul de sarcini, pot fi îndeplinite, pe lângă echipamentele menţionate de contestator, cel puţin de echipamentele produse de următorii producători:

- McAfee Network Security Platform - http://www.mcafee.com/us/ resources/data- sheets/ds-network-security-platform-m-series.pdf;
- Cisco-Sourcefire- https://na8.salesforce.eom/sfc/p/80000000 dRH9My3 BforYGEqBReQN10GcF ZnLvOg=.;
- HP TippingPoint NX NGIPS - http://www8.hp.com/us/en/ software- solutions/software.html?compURI=1343617#tab=TAB2.

- În concluzie, autoritatea contractantă susţine, şi cu privire la acest subpunct, că acuzaţiile contestatorului sunt neîntemeiate.

1.3. Întrebarea numărul 8 referitoare la cerinţa *„1.5.1.1 Soluţie de prevenire a intruziunilor (IPS) la nivel de reţea: Performanţa în reţea, Nivel de echipare 2 (2 echipamente + 2 hardware bypass dacă este necesar), Throughput trafic real inspectat: minimum 3 Gbps Latenţa: < 250 microsecunde Număr de sesiuni concurente: minimum 2.200.000 Număr de conexiuni/secundă: minimum 50.000*”, cerea, în

fapt, modificarea caietului de sarcini, şi anume *„dacă la cerinţele de performanţă în reţea se acceptă ca latenţa echipamentului să fie mai mare de 250 microsecunde*”. De asemenea, se cere să se *„clarifice dacă există o legătură între numărul de sesiuni concurente de 2.200.000 şi numărul de conexiuni/secunda de min. 50.000 corelat cu traficul real inspectat de minim 3 Gbps*”.

- Răspunsul a reiterat faptul că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii, latenţa pentru echipamentul menţionat în întrebare trebuie să fie mai mică de 250 de microsecunde, iar toate celelalte cerinţe specificate sunt capabilităţi şi caracteristici minimale ce trebuie îndeplinite de soluţia propusă.

- Nu există nicio regulă de corelare între cei 3 parametri specificaţi în întrebare, şi anume:

- Numărul de sesiuni concurente reprezintă numărul total de sesiuni care poate fi susţinut de platformă, inclusiv în cazul unui atac de tip DDoS de exemplu. Dacă acest parametru este subdimensionat se poate ajunge foarte repede în situaţia în care traficul de date este complet blocat;
- Numărul de conexiuni pe secundă se referă la câte conexiuni pe secundă poate susţine echipamentul, din punct de vedere al stabilirii acestora (conexiuni noi). Suportarea unui număr mai mare de conexiuni pe secundă permite evitarea sau reducerea efectelor negative în cazul atacurilor care încearcă stabilirea unui număr foarte mare de conexiuni în unitatea de timp;
- Traficul inspectat exprimat în Mbps se referă în special la conţinutul / ataşamentul din sesiuni - poate exista situaţia cu câteva sesiuni cu 1 Gbps conţinut ataşat şi inspectat sau pot fi 50.000 sesiuni fiecare cu un total de 600 Mbps conţinut ataşat şi inspectat, în funcţie de specificul traficului şi respectiv în funcţie de politicile de inspecţie definite. Traficul suportat de acest echipament trebuie să fie astfel dimensionat încât să nu producă întârzieri în segmentele de reţea monitorizate.

Marea majoritate a producătorilor de astfel de echipamente specifică aceşti parametri, multe dintre produsele lor având caracteristici mai bune decât cele menţionate în caietul de sarcini criticat.

De asemenea, autoritatea contractantă consideră că cerinţele minimale aferente acestui punct, formulate de autoritatea contractanta în caietul de sarcini, pot fi îndeplinite, pe lângă echipamentele identificate de contestator, cel puţin de echipamentele produse de următorii producători:

- McAfee Network Security Platform - http://www.mcafee.com/us/ resources/data- sheets/ds-network-security-platform-m-series.pdf;

- Cisco-Sourcefire - https://na8.salesforce.eom/sfc/p/80000000 dRH9My3BforYGEqBReQN10GcF ZnLvOg=.;
- HP TippingPoint NX NGIPS - http://www8.hp.com/us/en/ software-solutions/software.html?compURI=1343617#tab=TAB2.

În concluzie, autoritatea contractantă susţine, şi cu privire la acest subpunct, că acuzaţiile contestatorului sunt neîntemeiate.

1.4. Întrebarea numărul 23 referitoare la cerinţa *„1.5.1.4 Platforma de management pentru soluţiile de prevenire a intruziunilor: un sistem hardware dedicat (hardware appiiance) plus toate licenţele aferente, Se va livra o platformă hardware de la acelaşi producător ca al soluţiei de management*" cerea modificarea caietului de sarcini în sensul *„dacă se acceptă şi oferirea unei platforme hardware din partea unui producător diferit faţă de soluţia de management?",* întrebarea nr. 19 referitoare la cerinţa „1*.5.1.4 Platforma de management pentru soluţiile de prevenire a intruziunilor: un sistem hardware dedicat (hardware appliance) plus toate licenţele aferente. Se vor livra un sistem hardware dedicat (hardware appiiance) şi licenţele software aferente având caracteristicile minimale obligatorii din tabelul de mai jos."*, cerea definirea termenului de *„hardware appliance*".

Răspunsul privind întrebarea nr.19 a fost ca *„hardware appliance*" este considerat un echipament hardware fizic, dedicat realizării/ îndeplinirii funcţionalităţilor/ caracteristicilor solicitate, furnizat de producătorul platformei de management pentru soluţiile de prevenire a intruziunilor, cu toate elementele software şi licenţele aferente integrate.

Răspunsul la întrebarea nr. 23 a fost că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii şi deci că nu se acceptă şi oferirea unei platforme hardware din partea unui producător diferit faţă de soluţia de management.

Cele două răspunsuri au fost corelate şi cu faptul că în industria echipamentelor de securitate este uzuală practica ca software-ul produs de un producător să fie instalat pe un hardware al aceluiaşi producător. Cerinţa în speţă specifică în mod clar livrarea unui sistem hardware dedicat (hardware appliance) plus toate licenţele aferente.

Pe lângă producătorul echipamentelor identificat de contestator, autoritatea contractantă menţionează, că există cel puţin încă 2 soluţii concurente pe piaţă care pot oferi soluţia cerută:

- HP TippingPoint Security Management System;
- Cisco Sourcefire FireSIGHT Management Center.

Ambele se instalează pe hardware de la aceleaşi producător - HP şi respectiv Cisco.

- În concluzie, şi cu privire la acest subpunct, acuzaţiile contestatoarei sunt complet neîntemeiate.

2. Întrebarea numărul 9 referitoare la cerinţa *„1.5.1.2 Soluţie de prevenire a intruziunilor (hostIPS) la nivel de server critic, Arhitectură instalare Moduri de operare /funcţionare: Soluţia trebuie să suporte cei puţin următoarele tipuri de sisteme de operare: Windows Server, HP-UX, IBM-AIX, Solaris SPARC, Linux Red Hat*", cerea detalierea versiunilor software ale sistemelor de operare cerute a fi suportate: Windows server, HP-UX, IBM-AIX, Solaris SPARC, Linux Red Hat, precum şi caracteristicile echipamentelor hardware pe care rulează aceste sisteme de operare în cadrul .....

Întrebarea nr. 59 menţionată de contestator se referă la o altă cerinţă şi anume cerinţa 1.5.1.3. Soluţie de prevenire a intruziunilor (IPS) la nivel de server gazda (host server) pentru maşini virtuale, *„Arhitectură instalare Moduri de operare/funcţionare: Soluţia trebuie să suporte următoarele tipuri de maşini virtuale:*

- *VMware ESX, ESXi*
- *Windows Server 2008 Hyper-V*
- *IBM Power Systems logical partitions şi workload partitions*
- *HP vPars şi nPars*
- *Solaris Container*"; aspectele ce se doreau clarificate fiind următoarele:

„a. Ca şi tipuri de maşini virtuale este obligatoriu să fie suportate partiţii logice si de workload de la sistemele IBM Power Systems si HP vPars si HP nPars si Solaris Container?
b. Care este funcţionalitatea acestor maşini virtuale şi ce anume aţi dori să obţineţi prin instalarea HIPS pe aceste maşini?
c. Ce OS rulează pe aceste platforme?".

La prima întrebare, autoritatea contractantă arată că a răspuns că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii şi că soluţia de prevenire a intruziunilor (HostIPS) la nivel de server critic trebuie să asigure suport pentru sistemele de operare enunţate, cel puţin ultimele două versiuni majore. Serverele aflate în proprietatea .... au configuraţii diverse, cu procesoare Intel Xeon de generaţii diferite şi memorie RAM între 4GB şi 128GB;

Cea de-a doua întrebare se referea la tipurile de Hypervisor pe care cealaltă soluţie trebuia să le suporte.; ori, cele doua întrebări nu pot fi coroborate, acestea referindu-se la soluţii diferite, iar răspunsul de la întrebarea nr. 59, punctul c) se referă doar la serverele (maşini virtuale) care rulează folosind resursele furnizate de soluţia de virtualizare existentă şi pe care sunt instalate doar sisteme de operare de tip Windows şi Linux.

Soluţia care se doreşte a fi achiziţionată trebuie să nu se limiteze în vreun fel la situaţia existentă, dat fiind faptul că în viitor pot apărea soluţii dezvoltate pe sisteme de operare de tipul celor menţionate în

întrebarea nr. 9 cum ar fi de exemplu Oracle Exadata care este bazată pe Solaris SPARC.

În afara produselor identificate de contestator, există tehnologii de securitate similare care suportă mai multe sisteme de operare şi care respectă cerinţele caietului de sarcini, cum ar fi cele produse de McAfee, Sophos, Symantec sau Cisco Sourcefire.

În concluzie, autoritatea contractantă susţine şi cu privire la acest subpunct, că acuzaţiile contestatorului sunt neîntemeiate.

3. Întrebarea nr. 32. se referă la cerinţa *„1.5.3.1 Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active; Integrare şi corelare cu sistemele IPS; Să aibă capabiiităţi de integrare a datelor furnizate de sisteme IPS şi corelare a acestora cu vulnerabilităţile descoperite, printr-o aplicaţie de management comună”* şi cere: *„clarificarea cerinţelor aplicaţiei de management comuna, la ce componente va asigura funcţionalitatea de management, la ce modul de corelare licenţiat separat pentru fiecare active scanat în parte se face referire în această cerinţă. Acest modul de corelare trebuie să fie licenţiate separate? Poate fi oferit ca parte a unei componente cerute sau poate fi de tip sand- alone?”*. De asemenea, se cere specificarea *„dacă platforma hardware a acestui modul de corelare trebuie să fie livrată de către acelaşi producător ca şi în cazul platformei de management a soluţiei de detectare de intruşi?”*

Răspunsul a fost că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii. Integrarea şi corelarea soluţiei pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP cu sistemele IPS se va realiza conform cerinţei - prin intermediul aplicaţiei de management centralizat comune. Aplicaţia de management centralizat trebuie să dispună de un modul de corelare ce va importa baza de date cu vulnerabilităţi şi o va putea corela cu atacurile identificate în timp real de echipamente dedicate pentru prevenirea intruziunilor (IPS). Modul de licenţiere al acestui modul trebuie să permită îndeplinirea tuturor cerinţelor solicitate pentru soluţia pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP. În caietul de sarcini nu sunt specificate cerinţe legate de: înglobarea acestui modul de corelare într-o componentă anume sau dacă este stand-alone, dacă platforma hardware pe care este livrat trebuie să aibă acelaşi producător ca şi în cazul platformei de management a soluţiei de detectare de intruşi. Furnizorul este cel ce poate detalia modul în care soluţia propusă răspunde cerinţelor şi mecanismele utilizate pentru aceasta integrare.

Autoritatea contractantă susţine că nu s-a limitat în vreun fel acest modul de corelare, afirmaţia contestatorului că există un singur producător care poate furniza acest modul, fiind falsă.

Soluţii similare, care îndeplinesc cerinţele caietului de sarcini, sunt furnizate de diverşi producători, mai jos fiind câteva exemple:

- Sourcefire cu Qualys - http://www.sourcefire.com/partners/ technology- partners/sourcefire-api;
- Sourcefire cu Rapid7 - http://www.rapid7.com/docs/pr_2011-sourcefire.pdf;
- McAfee sau HP (cu Qualys) http://www.qualys.com/company/ newsroom/news-releases/usa/2009-10- 21/.

În plus, produsul la care face referire contestatorul ... şi anume IBM Proventia Enterprise Scanner nu mai este ofertat de producătorul menţionat încă din anul 2011 după cum rezultă din link-ul următor: http://www-01.ibm.com/common/ssi/cgi-bin/ ssialias?subtype=ca&infotype=an&appname=iSource&supplier=897&l etternu m=ENUS911-082.

În concluzie, şi cu privire la acest subpunct, acuzaţiile contestatorului sunt neîntemeiate.

4. Întrebarea nr. 30 se referă la cerinţa *„1.5.3.1 Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active, Performanţele analizei, Capacitatea de a scana minim 24000 IP-uri pe oră, Capacitatea de a realiza analize complete pentru minim 800 active/oră (all non-DoS-enabled)”*, şi cere *„clarificarea numărului de IP-uri scanate pe ora min. 24000 şi capacitatea de a realiza analize complete pentru min. 800 active/ora în corelare cu numărul de 2000 de Ip-uri active cerute în cadrul soluţiei*”.

Răspunsul a reiterat faptul că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii. Caracteristicile de performanţă solicitate şi anume capacitatea de a scana minim 24000 IP-uri pe oră şi capacitatea de a realiza analize complete pentru minim 800 active/oră (all non-DoS-enabled) sunt capabilităţi pe care trebuie să le deţină soluţia ofertată, astfel încât să nu necesite cheltuieli suplimentare pentru asigurarea scanării şi analizei unui număr mult mai mare de echipamente identificabile prin IP, acest necesar fiind în prezent de 2000 de active.

Managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP nu trebuie să se limiteze la nevoile curente ale .... şi în consecinţă trebuie să fie scalabilă pentru acoperirea necesităţilor viitoare pentru cel puţin o perioada de 5, 6 ani.

Capacitatea de a scana un număr mare de IP-uri şi de a realiza analize complete pentru un număr mare de active pe oră determină un timp mult mai redus necesar realizării acestor operaţiuni şi implicit

o perioada mai scurtă în care sunt posibile reduceri ale vitezei de comunicare în reţea.

De asemenea, cerinţele formulate sunt uzuale şi mai există numeroşi alţi producători în afara celui identificat de contestatoare care produc astfel de soluţii având caracteristici similare care răspuns cerinţelor caietului de sarcini, spre exemplu: Nessus, Qualys, McAfee, Rapid7.

În plus, produsul la care face referire contestatorul şi anume IBM Proventia Enterprise Scanner nu mai este ofertat de producătorul menţionat încă din anul 2011: http://www-01.ibm.com/common/ ssi/ cgi-bin/ssialias?subtype=ca&infotype=an&appname=iSource&supplier =897&letternu m=ENUS911-082.

În concluzie, şi cu privire la acest subpunct, autoritatea contractantă susţine că acuzaţiile contestatorului sunt neîntemeiate.

5. Întrebarea nr. ... se refera la cerinţa *„1.5.3.1 Soluţie pentru managementul vulnerabilităţilor din reţea ia nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active; Format; - 1 port serial - accesibil pe partea frontală cu conector RJ-45 - 2 porturi USB 2.0 - accesibile pe partea frontală*", conform cerinţelor din caietul de sarcini fiind necesară livrarea unui echipament dedicat (hardware appliance) furnizat ca atare de producător şi având sistem de operare proprietar complet securizat. Potrivit autorităţii contractante, „*clarificările*" solicitate au fost următoarele:

- *„vă rugăm să specificaţi dacă se acceptă si livrarea unui echipament hardware stand- alone dar care să fíe produs de acelaşi producător ca şi aplicaţia software care satisface cerinţele caietului de sarcini.*
- *vă rugăm să specificaţi modalitatea de distribuire a interfeţelor cerute pentru acest echipament în concordanţă cu funcţionalităţi/e acestuia;*
- *vă rugăm să clarificaţi ordinea de distribuire pe partea frontala a echipamentului a unui 1 port serial cu conector RJ-45 si a 2 porturi USB 2.0 (conform cererii din caietul de sarcini). Este important pentru clarificarea soluţiei propuse să cunoaştem dacă distribuirea porturilor pe partea frontal se va face de la stânga la dreapta sau invers şi de asemenea să cunoaştem dacă se doreşte ca portul serial RJ-45 sa fie primul şi să fíe urmat de cele 2 porturi USB 2.0 sau viceversa. Vă rugăm să specificaţi cât mai dar aceste lucruri având în vedere importanţa acestora în arhitectura generala a soluţiei propuse*".

Întrebarea nr. 66, menţionată de contestator tot la acest punct, se referă la cerinţa 1.5.3.1 Soluţie pentru managementul vulnerabilităţilor din reţea la nivel de echipamente identificabile prin IP (IP-based) pentru 2000 active *„Sunt necesare următoarele interfeţe: 1 port Giga bit Ethernet - pentru administrare - 2 porturi Gigabit*

Ethernet integrate pe placa de bază, 8 porturi Gigabit Ethernet - identificate ca porturi independente ce pot fi conectate ia segmente de reţea diferite - pentru interfeţele de scanare. 1 port serial - accesibil pe partea frontală cu conector RJ-45, 2porturi USB 2.0 - accesibile pe partea frontal, Controler RAID SAS/SATA (0, 1, 10, 5), Capacitate de stocare după construirea matricii RAID minimum 500GB, maxim 2TB, HDD-uríie Instalate trebuie să fie clasificate de către producător ca făcând parte din clasa enterprise, Memorie instalată minimum 4GB PC3-10600ECC", iar prin întrebarea formulată se dorea modificarea caietului de sarcini, adică acceptarea unei soluţii cu aceleaşi funcţionalităţi, dar configuraţie hardware diferită (ex: 2 porturi Ethernet, 250 GB hard disk etc.), *„în condiţiile în care funcţionalltăţile şi performantele solicitate nu vor fi afectate*".

Răspunsul a subliniat, încă o dată, că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii şi că se doreşte ca soluţia să fie livrată ca echipament hardware dedicat (hardware appliance), furnizat ca atare de producător având sistem de operare proprietar, complet securizat. Sunt solicitate în mod specific pe partea frontală doar 1 port serial cu conector RJ-45 şi 2 porturi USB 2.0, nefiind menţionată şi nici necesară o ordine anume a acestor porturi. Modul de distribuţie al celorlalte interfeţe solicitate este determinat de producătorul echipamentului. Descrierea interfeţelor furnizată în caietul de sarcini corespunde funcţionalităţilor solicitate.

La întrebarea 66 se explică faptul că este considerată acceptabilă o soluţie oferită prin propunerea tehnică care să modifice numai numărul porturilor Gigabit Ethernet identificate ca porturi independente ce pot fi conectate la segmente de reţea diferite - pentru interfeţele de scanare, doar în condiţiile în care soluţia propusă poate să realizeze analiza vulnerabilităţilor simultan pe cel puţin 8 (opt) segmente de reţea, aşa cum este precizat în caietul de sarcini.

Cerinţele hardware pentru echipamentul menţionat sunt unele uzuale şi sunt justificate, mai ales cele referitoare la partea frontală, de faptul că este mult mai uşor pentru un operator uman, atât din punctul de vedere al identificării echipamentului (în partea dorsală elementele de identificare sunt practic inexistente iar lungimea echipamentelor poate diferi foarte mult), cât şi din punct de vedere al uşurinţei în utilizare (în partea dorsală a unui rack plin de echipamente este evacuată toata căldura produsă de acestea fiind practic imposibil să se poată lucra într-o astfel de zona mai mult de câteva minute). Instalarea porturilor menţionate în partea frontală a echipamentelor a devenit o practică adoptată de foarte mulţi producători.

Există şi alţi producători în afara celui menţionat de contestator care produc astfel de soluţii având caracteristici similare care corespund caietului de sarcini, spre ex.: HP, Cisco.

Produsul la care se face referire în cuprinsul contestaţiei şi anume IBM Proventia Enterprise Scanner nu mai este ofertat de producătorul menţionat încă din anul 2011, după cum rezultă din următorul link: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias ?subtype=ca&infotype=an&appname=iSource&supplier=897&letternum=ENUS911-082.

În concluzie, şi cu privire la acest subpunct, autoritatea contractantă susţine că acuzaţiile contestatorului sunt neîntemeiate.

6. Cu privire la întrebările nr. 36 si 37 indicate de contestator la acest subpunct, în opinia autorităţii contractante, acestea practic nu erau necesare, la punctul 1.5.4.1 fiind stipulate foarte clar echipamentele necesare realizării soluţiei şi funcţionalităţile acestora.

Cu privire subpunctul 6.1 din contestaţie, descrierea soluţiei care se doreşte a fi achiziţionată la punctul 1.5.4.1.1 din caietul de sarcini, autoritatea contractantă arată că subcapitolul *„Arhitectură”* întăreşte cerinţele formulate la punctul 1.5.4.1; *„Soluţia trebuie să poată fi instalată stand-alone, iar cei puţin componentele SIEN, Network Behavior Analysis şi Risk Management să fíe echipamente dedicate*”. Aceste cerinţe sunt edificatoare şi împreună cu celelalte cerinţe formulate dau o imagine de ansamblu clară asupra funcţionalităţilor şi caracteristicilor soluţiei, astfel încât acestea să corespundă necesităţii autorităţii contractante.

Solicitările de licenţiere s-au făcut pe baza unui calcul estimativ al necesarului actual şi au fost avute în vedere mai multe scenarii de evoluţie viitoare ale soluţiei care în mod sigur vor necesita extinderi ulterioare. Nu în ultimul rând, asigurarea protecţiei şi garanţiei acestei investiţii ce va trebui să funcţioneze o perioada de cel puţin 5, 6 ani reprezintă o necesitate şi un punct important în strategie.

Cerinţele formulate relativ la scalabilitate ca fiind legitime şi justificate, pot fi îndeplinite cu siguranţă şi de soluţiile din partea altor producători în afara celui identificat de posibilul ofertant, spre exemplu: McAfee, ArcSight, soluţii care permit scalabilitatea solicitată.

Cu privire la cele menţionate la subpunctul 6.2 din contestaţie, produsul identificat de contestator în legătură cu cerinţele specificate la punctul 1.5.4.1.2 – *„Echipament hardware dedicat (hardware appiiance) pentru colectarea şi analiza fluxurilor de date la nivel 7 OSI (OSI layer 7 flows) şi a log-urior generate de activele de reţea plus toate licenţele aferente*” nu este singurul prezent pe piaţa echipamentelor şi produselor de securitate care poate îndeplini cerinţele specificate în caietul de sarcini.

- Există şi alţi furnizori de SIEM care oferă componente separate de flow cum ar fi spre exemplu: McAfee Network Threat Behavior Analysis (http://www.mcafee.com/us/products/network-threat-behavior - analysis.aspx), precum şi integrare API pentru achiziţie NetFlow şi

informaţii Layer 7 - ex. StealthWatch FlowCollector (http://www. lancope. com/files/Lancope_StealthWatch_FlowCollector.pdf) şi respectiv integrarea acestuia cu diferite soluţii SIEM - HP ArcSight şi TippingPoint, Cisco Cyber Threat Defense Solution - http:// www.lancope.com/partners/technology-alliance- partners/.

Cu privire la cele menţionate la subpunctul 6.3 din contestaţie, produsul identificat de contestator în legătură cu cerinţele specificate la punctul 1.5.4.1.3 *„Echipament hardware dedicat (hardware appiiance) pentru managementul riscului plus toate licenţele aferente*", nu este singurul prezent pe piaţa echipamentelor şi produselor de securitate care poate îndeplini cerinţele specificate în caietul de sarcini.

Există si alţi producători şi furnizori de Risk Management care se integrează cu soluţii SIEM - McAfee Risk Manager http:// www.mcafee.com/uk/products/risk-and-compliance/risk-management .aspx, sau integrare HP ArcSight cu Skybox Security http://www. skyboxsecurity.com/resources/data-sheets/using-skybox-security-sol utions-arcsight.

În concluzie, şi cu privire la acest subpunct, autoritatea contractantă susţine că acuzaţiile contestatoarei sunt neîntemeiate.

7.1 Întrebările de la numărul 44 la numărul 48, respectiv numărul 69, referitoare la cerinţa 1.5.4.1.1 - *„Echipament hardware dedicat pentru culegerea, înregistrarea, corelarea, interpretarea si prioritizarea datelor referitoare ia evenimentele de securitate (SIEM)*" s-au referit în totalitate la consola de administrare centrală a soluţiei, la modalităţile prin care se pot administra componentele acestei soluţii, la modul de acces la consola, la interconectarea componentelor soluţiei, iar contestaţia critică decizia autorităţii contractante de a menţine obligativitatea unei console centrale de administrare a tuturor componentelor soluţiei (SIEM, Log Management, NBA si Risk Management).

Răspunsul formulat a fost de a reitera faptul că cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii. Administrarea centralizată şi comunicarea între componente prin intermediul unor protocoale sigure reprezintă o cerinţă cheie a arhitecturii solicitate asigurând atât uşurinţă în utilizare, precum şi o integrare mai bună şi uniformizare a politicilor aplicate. Se explică faptul că se acceptă şi soluţii care oferă ca funcţionalitate suplimentară şi posibilitatea de realizare a managementului în mod descentralizat în condiţiile în care acesta poate fi făcut şi în mod centralizat, conform cerinţelor enunţate în caietul de sarcini.

Produsele identificate de posibilul ofertant în legătură cu cerinţele specificate la punctul 1.5.4.1.1 - *„Echipament hardware dedicat pentru culegerea, înregistrarea, corelarea, interpretarea şi prioritizarea*

datelor referitoare ia evenimentele de securitate (SIEM)" nu sunt singurele existente pe piaţă care îndeplinesc cerinţele din caietul de sarcini, existând mai mulţi producători care oferă produse similare, conforme cerinţelor, inclusiv pentru consolele de management, fie nativ, fie prin interfeţe specializate gen API. De exemplu: McAfee (http://www.mcafee.com/us/products/network-security/network-behavior-analysis.aspx) sau Sourcefire FireSIGHT (http://investor.sourcefire.com/releasedetail.cfm?ReleaseID=651715) sau integrare prin Cisco Cyber Threat Defense Solution (http://www.cisco.com/web/strategy/docs/gov/cyber_threat_defense_so.pdf), care oferă acelaşi tip de integrare.

În concluzie, şi cu privire la acest subpunct, autoritatea contractantă susţine că acuzaţiile contestatorului sunt neîntemeiate.

7.2 Întrebarea nr. 55 referitoare la cerinţa *„1.5.4.1.2. Echipament hardware dedicat (hardware appiiance) pentru colectarea şi analiza fluxurilor de date la nivel 7 OSI (OSI layer 7 flows) şi a log-urilor generate de activele de reţea plus toate licenţele aferente; Format: Echipament de tip hardware appliance*" cerea confirmarea faptului că echipamentul hardware dedicat pentru analiza fluxului de date şi a comportamentului reţelei trebuie să permită atât analiza fluxului de date cât şi a log-urilor generate de activele de reţea.

Răspunsul este în sensul că, potrivit cerinţelor minime şi obligatorii din caietul de sarcini, echipamentul hardware appliance dedicat analizei fluxului de date şi a comportamentului reţelei trebuie să fie dedicat acestei funcţionalităţi.

Şi în cazul acesta, produsul identificat de contestator pentru cerinţele specificate la punctul 1.5.4.1.2 *„Echipament hardware dedicat (hardware appiiance) pentru colectarea şi analiza fluxurilor de date la nivel 7 OSI (OSI layer 7 flows) şi a log-urilor generate de activele de reţea plus toate licenţele aferente*" nu este singurul care îndeplineşte cerinţele caietului de sarcini, existând mai mulţi producători care oferă produse similare conforme cu specificaţiile tehnice cerute, spre exemplu: McAfee (http://www.mcafee.com/us/products/application-data-monitor.aspx) sau Sourcefire (http://investor.sourcefire.com/releasedetail.cfm7ReleaseIDs651715).

În concluzie, autoritatea contractantă aprecază şi cu privire la acest subpunct că acuzaţiile contestatorului sunt neîntemeiate.

7.3. Cu privire la cele menţionate de contestator la pct. 7.3, NetFlow (Cisco), Sflow (HP), Jflow (Juniper) şi Qflow (IBM) sunt tehnologii proprietar de colectare şi analiză a datelor relevante pentru traficul ce trece prin activele de reţea (îndeosebi routere şi switch-uri). Ele au o răspândire mai mare sau mai mică, în funcţie de gradul de *„adopţie*" al producătorilor acestor tipuri de echipamente.

În cuprinsul caietului de sarcini se enunţă în cadrul cerinţelor de la punctul 1.5.4.1.1 – *„Echipament hardware dedicat pentru culegerea, înregistrarea, corelarea, interpretarea şi prioritizarea datelor referitoare la evenimentele de securitate (SIEM)”*, *„Analiza Flow-urilor*" următoarele specificaţii tehnice:
- Soluţia trebuie să poată utiliza, ca surse de analiză a flow-rilor, surse ce includ atât Netflow, JFIow, sFIow, Packeteer, cât şi propriul flux;
- Soluţia trebuie să aibă capabilitatea de a genera un flux care să permită analiza traficului layer 7, în scopul detecţiei protocoalelor de aplicaţie, indiferent de modul în care acestea sunt utilizate;
- Soluţia trebuie să furnizeze o vizualizare normalizată şi complet configurabilă a fluxurilor de date (flow data);
- Soluţia trebuie să aibă capabilitatea de a afişa informaţiile legate de orice flow, în formate multiple;
- Soluţia trebuie să ofere opţiunea dezvoltării de reguli de analiză comportamentală, direcţionate către monitorizarea anumitor porţiuni ale reţelei;

Din câte se observă nu este specificată, în vreun fel, ca sursă de analiză a flow-urilor tehnologia proprietară Qflow şi, mai mult, prin răspunsul la întrebarea nr. ... referitoare la cerinţa 1.5.4.1 SIEM, categoria performanţe, *„Să dispună de generator de flow-uri la Layer 7 (OSI) ce permite culegerea de date şi transformarea acestora în format flow cu informaţii de utilizatori, pentru produsele ce nu pot furniza flow-uri în mod nativ*”, prin care se cerea acceptarea unei soluţii care sa permită la Layer 7 (OSI) culegerea de date si transformarea acestora intr-un format standard internaţional (CEF sau asemănător), şi nu în *„flowuri la Layer 7 (OSI)*” cu specificaţia că *„informaţiile conţinute în acel mesaj vor fi identice şi vor conţine informaţiile specificate in caietul de sarcini, ca si numele utilizatorului, durata sesiunii etc.”*, autoritatea contractantă a explicat că se acceptă şi propunerile tehnice care conţin soluţii care să permită la Layer 7 (OSI) culegerea de date şi transformarea acestora într-un format standard internaţional (de exemplu CEF), conform cerinţelor enunţate în caietul de sarcini.

Există şi alţi producători în afara celui identificat de contestator care oferă echipamente care pot colecta şi analiza flow-uri de tip Qflow, cum ar fi de exemplu Juniper: http://www.juniper.net/us/en/ local/pdf/datasheets/1000217- en.pdf.

În concluzie, autoritatea contractantă susţine şi cu privire la acest subpunct că acuzaţiile contestatorului sunt neîntemeiate.

Având în vedere toate cele arătate mai sus, ... susţine faptul că soluţia care face obiectul *„Contract de furnizare având ca obiect realizarea unei soluţii integrate de securizare a sistemului informatic în vederea certificarii ISO 27001 (cod CPV:30211300-4), conform*

configuraţiei şi cerinţelor minime obligatorii prevăzute în Sectiunea 2: Caietul de sarcini" poate fi realizată prin integrarea de tehnologii de securitate, echipamente hardware dedicate şi produse software specializate oferite de diverşi producători, alţii decât cel menţionat cu insistenţă de contestatorul ...

Autoritatea contractantă susţine că cerinţele înscrise în caietul de sarcini publicat în SEAP nu au fost concepute pentru favorizarea unui anume producător sau furnizor, ci reprezintă, conform prevederilor art. 35 alin. (2) din OUG nr. 34/2006 specificaţii tehnice descrise obiectiv astfel încât să corespundă necesităţii autorităţii contractante, necesitate care constă în obţinerea unei integrări cât mai bune între componentele soluţiei cerute, pentru asigurarea unui nivel foarte ridicat de protecţie a securităţii informaţiilor vehiculate prin sistemul informatic al autorităţii contractante, pentru asigurarea unei administrări şi exploatări facile şi pentru realizarea unei vizibilităţi şi capacităţi de comunicare de tip „*end to end*" între toate componentele soluţiei, rămânând la latitudinea ofertantului alegerea acelor sisteme de securitate, echipamente hardware dedicate şi produse software specializate şi integrarea lor într-o soluţie care să răspundă acestei nevoi individualizate de autoritatea contractantă prin cerinţele formulate în caietul de sarcini.

În consecinţă, pentru toate aspectele arătate mai sus, autoritatea contractantă solicită respingerea contestaţiei formulate de ... ca nefondată, în conformitate cu prevederile art. 278 alin. (5) din OUG nr. 34/2006.

Ultimul document, la dosarul cauzei, îl reprezintă adresa nr. 39/30.12.2013, transmisă de către contestator şi înregistrată la CNSC sub nr. 3/06.01.2013.

Conform prevederilor art. 278 alin. (1) din OUG nr. 34/2006, Consiliul trebuie să se pronunţe mai întâi asupra excepţiilor de procedură şi de fond, iar când se constată că acestea sunt întemeiate, nu mai procedează la analiza pe fond a cauzei.

Având în vedere norma anterior invocată, Consiliul va reţine faptul că, în cuprinsul punctului de vedere nr. SC-DA-29325/ 23.12.2013, autoritatea contractantă invocă excepţia tardivităţii faţă de contestaţia formulată de ... susţinând că „*această contestaţie nu vizează răspunsul autorităţii contractante la solicitările de clarificări ci chiar conţinutul documentaţiei de atribuire*".

Conform art. 269 din OUG nr. 34/2006, „*procedura de soluţionare a contestaţiilor se desfăşoară cu respectarea principiilor legalităţii, celerităţii, contradictorialităţii şi a dreptului la apărare*"; având în vedere că autoritatea contractantă a invocat în punctul de vedere nr. SC-DA-29325/23.12.2013, înregistrat la CNSC sub nr.

43948/23.12.2013, excepţia tardivităţii, Consiliul transmite prin fax contestatorului adresa nr. 27202/... ... solicitându-i opinia cu privire la excepţia invocată; contestatorul răspunzând prin adresa nr. 39/30.12.2013, înregistrată la CNSC cu nr. 3/06.01.2014, potrivit căreia *„răspunsul la întrebările de clarificare, publicate în SEAP la data de 11.12.2013, prin adresa nr. SC-DA-28...2, au arătat faptul că este favorizat, în mod intenţionat, un singur producător*" şi că *„acest răspuns este actul autorităţii contractante considerat nelegal, act care afectează întreaga procedură de atribuire*".

Subsecvent, Consiliul urmează a se raporta, în analiza excepţiei invocate, la data luării la cunoştinţă de către contestator a actului indicat de acesta, adresa nr. SC-DA-28...2, publicată în SEAP la data de 11.12.2013.

În acest sens, Consiliul va reţine că ... a transmis prin fax contestaţia nr. ... înregistrată la CNSC cu nr. ... în data de ... aşa cum rezultă din documentul anexat dosarului cauzei şi a notificat acest fapt autorităţii contractante în 17.12.2013, conform copiei postată pe SEAP de aceasta din urmă, în data de 17.12.2013.

De asemenea, Consiliul va lua în considerare faptul că documentul atacat de contestator, este, aşa cum rezultă din motivarea anterioară, prin adresa nr. SC-DA-28...2, document de al cărei conţinut contestatorul a luat la cunoştinţă în data de 11.12.2013, fiind publicat în SEAP sub identificatorul *„[CN...007] Raspuns 2 la clarificari ISO 27001.PDF"*.

Având în vedere faptul că în litigiul dedus judecăţii este vorba despre un contract de furnizare, iar valoarea estimată este mai mare decât pragurile valorice prevăzute la art. 55 alin. (2) lit. a) din OUG nr. 34/2006, aprobată prin Legea nr. ...7/2006 cu modificările şi completările ulterioare, sunt incidente prevederile art. 256² alin. (1) lit. a) din acelaşi act normativ potrivit căruia *„persoana vătămată poate sesiza Consiliul Naţional de Soluţionare a Contestaţiilor sau, după caz, instanţa judecătorească competentă în vederea anulării actului şi/sau recunoaşterii dreptului pretins ori a interesului legitim, în termen de: … 10 zile începând cu ziua următoare luării la cunoştinţă, în condiţiile prezentei ordonanţe de urgenţă, despre un act al autorităţii contractante considerat nelegal, în cazul în care valoarea contractului care urmează să fie atribuit, estimată conform prevederilor art. 23 şi ale cap. II secţiunea a 2-a, este egală sau mai mare decât pragurile valorice prevăzute la art. 55 alin. (2)*".

Art. 271 alin. (1) din OUG nr. 34/2006, aprobată prin Legea nr. ...7/2006 cu modificările şi completările ulterioare, cuprinzând şi modificarea şi completarea adusă prin OUG nr. 19 din 7 martie 2009, publicată în Monitorul Oficial al României, Partea I, nr. 156/12.03.2009, stipulează că „*Sub sancţiunea respingerii contestaţiei*

ca tardivă, aceasta se înaintează atât Consiliului, cât şi autorităţii contractante, nu mai târziu de expirarea termenelor prevăzute la art. 256[2]...”.

De asemenea, art. 3 lit. z) din OUG nr. 34/2006, aprobată prin Legea nr. ...7/2006 cu modificările şi completările ulterioare, cuprinzând şi modificarea şi completarea prin OUG nr. 76 din 30 iunie 2010, publicată în Monitorul Oficial al României, Partea I, nr. 453/02.07.2010, stipulează că *„(...) termenul exprimat în zile începe să curgă de la începutul primei ore a primei zile a termenului şi se încheie la expirarea ultimei ore a ultimei zile a termenului; ziua în cursul căreia a avut loc evenimentul sau s-a realizat un act al autorităţii contractante nu este luată în calculul termenului....”.*

Prin urmare, având în vedere cele de mai sus şi ţinând cont că data luării la cunoştinţă de către contestator, a clarificării în cauză, a fost 11.12.2013, iar contestaţia acestuia a fost transmisă către CNSC în data de ... şi către autoritatea contractantă în data de 17.12.2013, în mod evident termenul legal de 10 zile, în care aceasta putea fi transmisă a fost respectat, ultima zi fiind data de 23.12.2013.

Având în vedere cele de mai sus, Consiliul va respinge excepţia tardivităţii invocată autoritatea contractantă, urmând a analiza pe fond contestaţia.

Analizând actele existente la dosarul cauzei, Consiliul constată următoarele:

... a organizat, în calitate de autoritate contractantă, procedura de atribuire, prin „*licitaţie deschisă*”, în vederea atribuirii contractului de achiziţie publică având ca obiect: „*Contract de furnizare având ca obiect realizarea unei soluţii integrate de securizare a sistemului informatic în vederea certificarii ISO 27001 (cod CPV:30211300-4), conform configuraţiei şi cerinţelor minime obligatorii prevăzute în Sectiunea 2: Caietul de sarcini*”, CPV 30211300-4, 72265000-0, 72611000-6, elaborând, în acest sens, documentaţia de atribuire aferentă şi publicând, în SEAP, anunţul de participare nr. ...30.10.2013, conform căruia valoarea estimată a contractului este de 5.224.999,00 lei, fără TVA.

Conform cap. IV.2.1) din fişa de date, criteriul de atribuire al contractului este „oferta cea mai avantajoasă d.p.d.v. economic”, cu factorii de evaluare şi ponderea aferentă: „Preţul ofertei 50 %; Tehnici pentru analiza traficului – Analiza protocoalelor 10 %; Soluţie de prevenire a intruziunilor (IPS) la nivel de reţea – Performanta în retea – Latenta 5 % ; Soluţie de protecţie a porţii de acces web - Arhitectura – throughput 10 %; Solutie de protectie a bazelor de date critice – Remediere 5 %; Soluţie de prevenire a pierderilor de date (Data Loss Prevention) la nivel de reţea– Management unificat şi functionalităţi generale – tipuri de fisiere 10%; Soluţie pentru

managementul incidentelor şi evenimentelor de securitate – Format – Capacitate de stocare onboard 10 %.

Prin adresa nr. SC-DA-28...2/11.12.2013, publicată în SEAP sub identificatorul *„[CN...007] Raspuns 2 la clarificari ISO 27001.PDF”*, autoritatea contractantă a răspuns la o serie de solicitări de clarificare formulate de un oprator economic.

Ulterior luării la cunoştinţă a răspunsului autorităţii contractante, ... a formulat contestaţia dedusă soluţionării, susţinând că *„în data de 11.12.2013 au fost publicate în SEAP precizări completatoare care ne-au întărit convingerea că un singur producător (IBM) este favorizat*”.

Având în vedere cele de mai sus, Consiliul va soluţiona contestaţia analizând modalitatea în care a elaborat autoritatea contractantă adresa nr. SC-DA-28...2/11.12.2013, luând în considerare atât prevederile documentaţiei de atribuire cât şi legislaţia incidentă din domeniul achiziţiilor publice.

În acest sens, ca un prim aspect, Consiliul va respinge criticile contestatorului, aferente specificaţiilor tehnice din caietul de sarcini deoarece la data formulării contestaţiei, acestea sunt, în mod evident, tardive, urmând ca, în continuare, să analizeze, în mod exclusiv, modul în care a răspuns autoritatea contractantă la solicitarea de clarificări.

Totodată, Consiliul va lua în considerare că, potrivit prevederilor art. 78 din OUG nr. 34/2006, *„(1) Orice operator economic interesat are dreptul de a solicita clarificări privind documentaţia de atribuire. (2) Autoritatea contractantă are obligaţia de a răspunde, în mod clar, complet şi fără ambiguităţi, cât mai repede posibil, la orice clarificare solicitată, într-o perioadă care nu trebuie să depăşească, de regulă, 3 zile lucrătoare de la primirea unei astfel de solicitări din partea operatorului economic. (3) Autoritatea contractantă are obligaţia de a transmite răspunsurile - însoţite de întrebările aferente - către toţi operatorii economici care au obţinut, în condiţiile prezentei ordonanţe de urgenţă, documentaţia de atribuire, luând măsuri pentru a nu dezvălui identitatea celui care a solicitat clarificările respective*”.

În acest context, Consiliul va reţine că SC ... a solicitat, prin adresa fără număr de înregistrare la emitent, înregistrată la sediul autorităţii contractante sub nr. SC–28028/09.12.2013, o serie de clarificări; autoritatea contractantă răspunzând prin adresa nr. SC-DA-28...2/11.12.2013, publicată în SEAP sub identificatorul *„[CN...007] Raspuns 2 la clarificari ISO 27001.PDF”*.

Subsecvent, Consiliul apreciază că, în ceea ce priveşte termenul de răspuns, autoritatea contractantă a respectat condiţia de a răspunde „...*într-o perioadă care nu trebuie să depăşească, de regulă, 3 zile lucrătoare de la primirea unei astfel de solicitări din partea operatorului economic*”; termenul pentru transmiterea răspunsului la

cele 55 de întrebări fiind inferior celui prevăzut de norma juridică anterioară.

Totodată, din analiza clarificărilor aferente, Consiliul constată că autoritatea contractantă a confirmat că *„cerinţele enunţate în caietul de sarcini sunt minimale şi obligatorii”* şi că soluţia tehnică pentru cerinţele în cauză urmează a fi stabilită în funcţie de tehnologia specifică fiecărui ofertant.

În acest context, Consiliul apreciază că actul atacat de contestator, adresa nr. SC-DA-28...2/11.12.2013, constituie clarificare a documentaţiei de atribuire în sensul prevederilor art. 1 din Ordinul ANRMAP nr. 171/2012, potrivit cărora *„răspunsul autorităţii contractante la solicitarea de clarificări privind documentaţia de atribuire, precum şi clarificarea cu privire la conţinutul documentaţiei de atribuire emisă de autoritatea contractantă, reprezintă acte administrative prin care se aduc* ***lămuriri/explicitări/limpeziri*** *cu privire la conţinutul documentaţiei de atribuire şi prin care nu se pot aduce modificări cu privire la conţinutul acesteia din urmă, aşa cum a fost publicată în SEAP*”, aspect admis de contestator, în cuprinsul contestaţiei, prin sintagme de forma *„în data de 11.12.2013 au fost publicate în SEAP precizări completatoare care ne-au întărit convingerea că un singur producător (IBM) este favorizat*”, *„răspunsul (...) la această întrebare nu clarifică această solicitare, lăsând nemodificată cererea iniţială”* sau *„răspunsul (...) nu deschide posibilitatea ofertării altor soluţii*”.

Ori, întrucât autoritatea contractantă a răspuns la fiecare dintre întrebările contestatorului, iar criticile acestuia vizează, de fapt, refuzul acesteia de a modifica specificaţiile din caietul de sarcini, publicate în anexa anunţului de participare, Consiliul apreciază că, documentul în cauză poate fi caracterizat prin atributele *„clar, complet şi fără ambiguităţi*”, imperativ prevăzute la art. 78 alin. (2) din OUG nr. 34/2006.

În acest context, Consiliul nu va lua în considerare alegaţiile contestatorului, potrivit cărora, prin răspunsurile aferente întrebărilor 6 şi 8, autoritatea contractantă ar fi modificat specificaţia *„latenţă”* aferentă performanţelor în reţea solicitate pentru soluţia de prevenire a intruziunilor în reţea, deoarece la întrebarea *„vă rugăm să clarificaţă dacă la cerinţele de performanţă în reţea se acceptă ca latenţa echipamentului să fie mai mare de 250 microsecunde*”, autoritatea contractantă a răspuns *„latenţa pentru echipamentul menţionat în întrebare trebuie să fie mai mică de 250 de microsecunde*”, aspect care rezultă din specificaţiile în cauză, aflate la paginile 9 şi 10 din caietul de sarcini, publicat în SEAP, în anexa anunţului de participare sub identificatorul *„[CN...002] Partea 1-S2-caiet sarcini-ISO 27001.PDF.p7m*”, respectiv *„latenţa: < 250 microsecunde*”.

În opinia Consiliului, autoritatea contractantă a procedat corect, menţinând condiţia unei valori maxime acceptată pentru parametrul de mai sus, deoarece, prin raportare la natura, complexitatea şi valoarea estimată a sistemului care urmează a fi achiziţionat, se impune furnizarea unor echipamente care să aibă performanţe cât mai bune; în cazul de faţă, latenţă cât mai mică.

Totodată, Consiliul nu va lua în considerare nici alegaţiile contestatorului, potrivit cărora *„la data de 11.12.2013, autoritatea contractantă a publicat în SEAP precizări completatoare care, în opinia sa, favorizează un singur producător (IBM)"* deoarece, pe de o parte, autoritatea contractantă nu a „completat" specificaţiile tehnice din caietul de sarcini cu altele noi şi, pe de altă parte, pentru că, în mod contrar principiului de drept conform căruia *„actori incumbit probatio" – „sarcina probei incumbă, în mod exclusiv, reclamantului*", regăsit transpus în dreptul autohton, în cadrul dispoziţiilor art. 249 din NOUL COD DE PROCEDURĂ CIVILĂ, potrivit cărora, referitor la sarcina probei, *„cel care face o susţinere în cursul procesului trebuie să o dovedească, în afară de cazurile anume prevăzute de lege*", contestatorul se limitează la aformaţii de forma *„IBM Security Qradar Flow Collector este singurul care poate oferi aceste funcţionalităţi în condiţiile arhitecturii cerute de autoritatea contractantă*", fără a-şi proba afirmaţiile prin documente care să demonstreze incidenţa prevederilor art. 38 alin. (1) din OUG nr. 34/2006, potrivit cărora *„se interzice definirea în caietul de sarcini a unor specificaţii tehnice care indică o anumită origine, sursă, producţie, un procedeu special, o marcă de fabrică sau de comerţ, un brevet de invenţie, o licenţă de fabricaţie, care au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse*".

De altfel, Consiliul apreciază că aceeaşi concluzie rezultă din cuprinsul adresei nr. 39/30.12.2013, înregistrată la CNSC sub nr. 3/06.01.2014, prin care contestatorul recunoaşte că o serie din argumentele pe care se bazează contestaţia au fost formulate prin raportare la specificaţiile tehnice aferente unui produs care nu se mai fabrică din anul 2011 (IBM Proventia Enterprise).

Corelativ, Consiliul apreciază că autoritatea contractantă, prin publicarea adresei de mai sus în SEAP, fără a indica identitatea celui care a solicitat clarificările respective, a respectat şi prevederile alin. (3) al art. 78 din OUG nr. 34/2006, conform cărora *„Autoritatea contractantă are obligaţia de a transmite răspunsurile - însoţite de întrebările aferente - către toţi operatorii economici care au obţinut, în condiţiile prezentei ordonanţe de urgenţă, documentaţia de atribuire, luând măsuri pentru a nu dezvălui identitatea celui care a solicitat clarificările respective*".

Faţă de cele de mai sus, Consiliul, în temeiul art. 278 alin. (5) din OUG nr. 34/2006, aprobată prin Legea nr. ...7/2006 cu modificările şi completările ulterioare, urmează să respingă, ca nefondată, contestaţia formulată de ... în contradictoriu cu autoritatea contractantă ...

Pe cale de consecinţă, în temeiul art. 278 alin. (6) din ordonanţa de urgenţă, va dispune continuarea procedurii de atribuire în cauză.

PREŞEDINTE COMPLET
...

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

Redactat în 4 (patru) exemplare originale, conține 50 (cincizeci) pagini.