Caiet de sarcini

-Achizitie cunostiinte tehnice PITQEAST-

Contents

Preambul

Q-East Software este o companie cu expertiza in furnizarea de solutii pentru managementul sistemelor, al bazelor de date si al aplicatiilor. Q-East Software are la activ implementari de sisteme de administrare, management si protectie la dezastre pentru infrastructura informatica. De asemenea furnizeaza solutii de arhivare, replicare si recuperare in caz de dezastru pentru baze de date.
In domeniul securitatii informatiei si conformitatii cu standardele de securitate existente, Q-East Software implementeaza solutii de securitate si event-log management, avand in Romania peste 20 astfel de implementari, totalizand peste 2,000 servere si 10,000 utilizatori.

Q-East Software, unicul reprezentant autorizat al companiei Dell (Quest) Software pentru Romania, Moldova, Bulgaria si regiunea Adriatica, are ca principal obiect de activitate dezvoltarea, comercializarea si implementarea de solutii software precum si acordarea de consultanta in domeniul IT.
Partener strategic cu Oracle, IBM, Dell, HP si Microsoft ISV Partner in 2007, 2009, 2010 si 2011, Dell (Quest) Software Inc. este astazi un furnizor de solutii ce ajuta clientii sa obtine mai multa performanta, mai multa productivitate, mai multa siguranta si nu in ultimul rand conformitate cu standardele de securitate (SOX, ISO 27002, Basel II, PCI, etc)

Descriere sumara a serviciilor si a proiectului

Q-East Software a castigat in anul 2013 un proiect POS CCE pe Axa Prioritara „COMPETITIVITATE PRIN CERCETARE, DEZVOLTARE TEHNOLOGICA și INOVARE” Operatiunea O.2.3.3 „Promovarea inovării în cadrul întreprinderilor”. Titlul acestui proiect este „Platformă inovativă integrată de monitorizare și securitate IT a fluxurilor informaționale ale unei firme - PITQEAST” si ca scop principal cresterea calitatii serviciilor oferite și a siguranței în cadrul fluxurilor de date.
Principalele produse care se vor construi, ca rezultat al cercetarii-dezvoltarii sunt:

1. O platforma (appliance) incluzand elemente hardware si software destinata imbunatatirii securitatii IT si a securitatii fluxurilor de date;
2. Servicii de supraveghere a fluxurilor de date pentru clienti care nu doresc intreaga platforma, ci numai aplicatii care sa ruleze local, in reteaua privata a firmei. Aplicatiile software asociate reprezinta suportul software pentru mediul de procesare. Aici, avem 2 tipuri de aplicatii:
   - Aplicatii server:
     - Aplicatie de culegere date din sisteme de SIEM sau “Event Log Management”.
     - Aplicatie de procesare date.
     - Aplicatie desktop sau web:
   - Aplicatiile de vizualizare/creare de investigatii. Aceste aplicatii trebuie sa ofere comunicatie cu server-ul de procesare pentru asigurarea interactivitatii descoperirea evenimentelor asociate. Acestea trebuie sa poata salva, modifica, crea noi investigatii in mod interactiv sau pe baza de sabloane.
3. Servicii de mentenanta si suport pentru baza de date astfel dezvoltata

Descriere sumara a obiectivelor si asteptarilor noastre

Rezultatele asteptate de la furnizorii care vor raspunde la acest caiet de sarcini sunt livrabile care se vor materializa sub forma de cunostinte tehnice (studii / documentatie / manuale) care sa raspunda in intregime ipotezei de dezvoltare a proiectului.
Exista mai multe categorii de cunostinte tehnice pe care dorim sa le achizitionam si un calendar de livrare a acestora. Astfel:

Capitol	Termen
Achizitia de cunostinte tehnice privind modalitatea de experimentare a componentelor hardware-software prin aplicarea unor algoritmi specifici de cautare	in max 1 luna de la contractare
Achizitia de cunostinte tehnice privind modalitatea de proiectare a moduleleor software imbarcate pe modulele hardware	In maxim 4 luni de la contractare
Achizitia cunostinte tehnice privind modalitatea de asamblare optima a modulelor hardware si software	In maxim 7 luni de la contractare
Achizitia de cunostinte tehnice pentru testarea hardware conforma cu standardele impuse	In maxim 10 luni de la contractare
Achizitia de cunostinte tehnice privind modalitatea de testare a software-ului imbarcat, in vederea avizarii	In maxim 10 luni de la contractare

Toate rezultatele vor fi livrate in format hard copy precum si in format electronic editabil.

Rezumat ipoteza initiala a proiectului

In contextual actual, tot mai multe organizatii sunt din ce in ce mai preocupate de starea de securitate IT. Din aceasta cauza, in ultimii ani, s-a dezvoltat atat la nivel international cat si local o cerere mare pentru produse de securitate IT. Acestea au evoluat in decursul timpului de la solutii simpliste de “Event Log Management” la solutii de “SIEM” – Security Incident and Event Log Management.
Rolul solutiilor de “Event Log Management” este acela de a colecta toate jurnalele de securitate generate de toate serverele si aplicatiile organizatiilor. Intr-o implementare clasica, solutiile de Event log Management stocheaza aceste informatii de securitate in baze de date sau structuri comprimate propietare la nivel de sistem de fisiere.
Solutiile denumite generic “SIEM” se ocupa in plus fata de solutiile de “Event Log management” de adminitrarea/tratarea incidentelor de securitate IT prezente in jurnalele de access ale serverelor sau/si a aplicatiilor. Tipic, o implementare tipica de SIEM ofera detalii despre gradul de securitate a retelei, a aplicatiilor si a companiei.
Aceste doua tipuri de solutii, ofera pentru partea de investigatii de securitate rapoarte, pentru diferite in functie de specificul aplicatiei, servere-lor. Un exemplu concludent ar fi existenta rapoartelor standard de access ale utilizatorilor la resursele companiilor. In acest fel,o implementare tipica de SIEM are acess la urmatoarele tipuri de rapoarte:

- Rapoarte de autentificare la retea (domeniu de Active Directory)
- Rapoarte de autentificare la aplicatii (pot fi aplicatii Oracle, .Net, etc)
- Rapoarte de access la resurse
    - Aplicatii

    - Documente
    - Email
    - Imprimante
    - Etc.
- Rapoarte de conformitate cu standarde interne sau externe de securitate
- Deficientele acestor metode de investigatie sunt evidente:
- Corelarea datelor dintre diverse sisteme de calcul, aplicatii etc. este greoaie
- Nu se pot stabili usor pattern-uri de access pentru diversi utilizatori/aplicatii etc.

Din aceste motive, am cautat noi metode investigationale ce vor ajuta companiile sa se protejeze mai bine impotriva atacurile interne si externe.
Imbunatatirile gasite si sugerate in acest document sunt destinate oricarei organizatii ce doreste sa isi inbunatateasca gradul de securitate IT. Departamentele interne ale acestora de "securitate IT" sunt pricipalii beneficiari ale acestor imbunatatiri posibile.

Context international

In SUA, nevoia de audit extins asupra sistemelor informatice a inceput odata cu prabusirea gigantului Enron. Aceasta prabusire financiara a marcat inceputul crearii mediului legislativ ce reglementa urmarirea activitatilor IT ale organizatiilor. In acest fel, companiile listate la bursa din SUA trebuie sa satisfaca o serie de cerinte de control intern asupra procesului de raportare financiara si de securitate - cerinte specificate in legea Sarbanes–Oxley din 2002 (denumita si legea SOX). Conform acestei legi , din punct de vedere IT, toate activitatile utilizatorilor trebuiesc auditate. In acest fel, toate aplicatiile, servere-le si echipamentelor acestor companii trebuiesc sa genereze loguri de access si securitate. Aceste jurnale (log-uri), trebuiesc colectate, stocate (pe o perioada de minim 3 ani) si raportate. Auditorii autorizati verifica periodic aceste implementari de audit si rapoarte pentru a se exista o evidenta corecta asupra acceselor la datele companiei. Din aceasta cauza, si, datorita cerintelor interne de securitate, companiile au implementat solutii de "Event Log management" si SIEM ("Security incident and event log management").
Ecourile acestor legi si incidente financiare (SOX, Enron si World .com) au avut ca rezultat crearea unor standarde speciale de securitate pentru companii:
Iata o lista neexhaustiva a acestor standarde:
BASEL II - Bank for International Settlements - Revised international capital framework – http://www.bis.org/publ/bcbsca.htm
BASEL III - International regulatory framework for banks - http://www.bis.org/bcbs/basel3.htm
CIS Benchmarks - Center for Internet Security. Various standards - http://www.cisecurity.org/
COBIT Control Objectives for Information and related Technology - http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx
DISA STIGs - Defence Information Systems Agency - Security Technical Implementation Guide - http://en.wikipedia.org/wiki/Security_Technical_Implementation_Guide
FDCC - Federal Desktop Core Configuration - http://nvd.nist.gov/fdcc/index.cfm
FIPS-199 - Federal Information Processing Standard - http://www.itl.nist.gov/lab/bulletns/bltnmar04.htm
FISMA - Federal Information Security Management Act http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act
GLBA - Gramm Leach Blily Act) http://www.ftc.gov/privacy/glbact/glbsub1.htm
HIPAA - Health Insurance Portability and Accountability - http://searchdatamanagement.techtarget.com/definition/HIPAA
ISAP - Information Security Automation Programme http://en.wikipedia.org/wiki/Information_Security_Automation_Program
ISO-17799:2005 Information technology - Security techniques -Code of practice for information security management - http://en.wikipedia.org/wiki/ISO/IEC_27002
ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems - http://en.wikipedia.org/wiki/ISO/IEC_27001

ITIL - Information Technology Infrastructure Library http://www.itil-officialsite.com/
NERC CIP - North American Electric Reliability Corporation - Critical Infrastructure Protection http://searchcompliance.techtarget.com/feature/What-is-NERC-CIP-and-ITs-role-in-critical-infrastructure-protection
PCI – DSS - Payment Card Industry - Data Security Standards https://www.pcisecuritystandards.org/security_standards
SCAP Security Content Automation Protocol http://scap.nist.gov/
Aceaste cerinte au implicatii majore asupra modului de gestiune a securitatii sistemelor informatice ale companiilor.
Tara noastra a inceput sa recupereze din urma tarile mai dezvoltate in ceea ce priveste securitatea IT. Foarte multe companii au investit in proiecte de SIEM sau Event Log Management ca raspuns la cerinte de securitate impuse la nivel intern sau de catre auditori ai diverselor standarde de securitate. Cel mai folosit standard de securitate in companiile ce isi desfasoara activitatea in tara noastra este ISO/IEC 27001. Exista companii ce implementeaza si alte standarde (ca masuri preventive) cum ari fi SOX sau/si Basel II sau Basel III.
La nivel guvernamental, exista deja institutii specializate pe combaterea criminalitatii cibernetice cu ar fi "Centrul National de raspuns la incidente de securitate Cibernetica" (http://www.cert-ro.eu) sau "Serviciul de combatere a criminalitatii informatice" - structura a Politiei Romane (http://www.efrauda.ro). Acestea lucreaza impreuna cu companiile de stat si private pentru mediului de securitate.
Solutiile existente de Event Log Management si de SIEM s-au dezvoltat pe parcursul timpului ca raspuns la cerintele pietei si ofera capabilitati complexe de raportare si gestiune a informatiilor de securitate. Cele mai importante produse si companii au patruns si pe piata autohtona si ofera intrumentele elementare de gestionare a securitatii informatice a companiilor. Cele mai importante produse existente sunt:

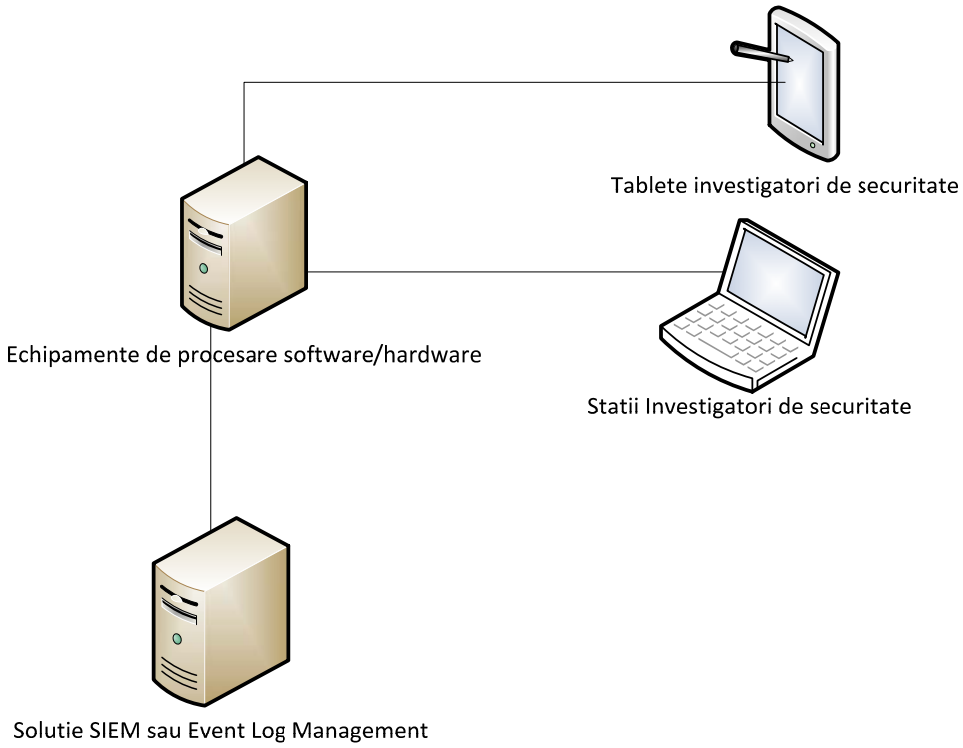
- HP Arcsight
- Dell Intrust si Dell Change Auditor
- IBM Q1 Labs QRadar SIEM
- Alienvault
- CorreLog
- elQnetworks SecureVue
- Loglogic
- Etc.

Aceste produse ofera companiilor ce au decis sa le implementeze instrumetele de baza necesare pentru securizarea propiului mediului IT. Toate solutiile ofera rapoarte de securitate pentru diverse tehnologii/servere sau/si aplicatii.
In mod traditional, companiile investesc sume considerabile de bani in tehnologie de procesare a acestor informatii reprezentand servere puternice de baze de date ce sa poata genera rapoarte pe volumul mare de date intr-un timp cat mai scurt.

Acest sistem va citi evenimentele de securitate colectate de o solutie clasica de SIEM sau Event Log Management. Scopul nu este conectarea acestuia la toate sursele generatoare de evenimente de securitate ci citirea datelor deja existente din solutii SIEM ce le colecteaza. In acest fel, se vor putea genera aceste grafuri interactive direct din datele existente doar prin conectarea la sursa normalizata de date (sistemul SIEM).

Beneficiarii acestei solutii vor fi companiile ce si-au implementat un sistem de "SIEM" sau de "Event Log Management". Conform ultimelor studii, majoritatea companiilor ce trec de un anumit numar de angajati (minim 500) au achizitionat sau sunt in curs de achizitionare a unui sistem de securitate.

Pe masura ce departamentele lor de securitate IT vor face investigatii de securitate, nevoia unor instrumente mai usoare si mai rapide de investigatie va fi din ce in ce mai mare.
Pentru implementarea acestei solutii, este nevoie crearea unui produs integrat software-hardware pentru procesarea acestor informatii si oferirea de rezultate in mod grafic intr-o consola web sau desktop.
Astfel, produsul final va avea urmatoarea arhitectura:



Echipamentul de procesare (denumit appliance) va extrage datele de securitate din solutia existenta de “Event Log Management” sau “SIEM”, la va procesa si va oferi aceste informatii si cu legaturile dintre ele pentru vizualizare intr-o interfata web sau intr-un client desktop. Aplicatia client (ce se poate crea si pentru tablete), va trimite in mod interactiv selectiile utilizatorilor catre server-ul de procesare care va intoarce doar informatiile pe un nivel asociate punctului de graf curent. Aplicatia de vizualizare va afisa informatia primita in mod grafic.

Figura 1 prezinta arhitectura logica si functionala a solutiei propuse.

a) Componente:
b) Appliance de procesare
c) Server Solutie SIEM
d) Clienti

Appliance-ul de procesare are rolul de a extrage datele din sistemul SIEM am beneficiarului. Odata extrase, aceste date vor fi stocate intr-o structura de tip MongoDB si se vor aplica algoritmi de procesare pe tot volumul de date.
Datele extrase din sistemul SIEM se vor stoca intr-o structura MongoDB.

Arhitectura hardware al acestui appliance va fi minim urmatorea:

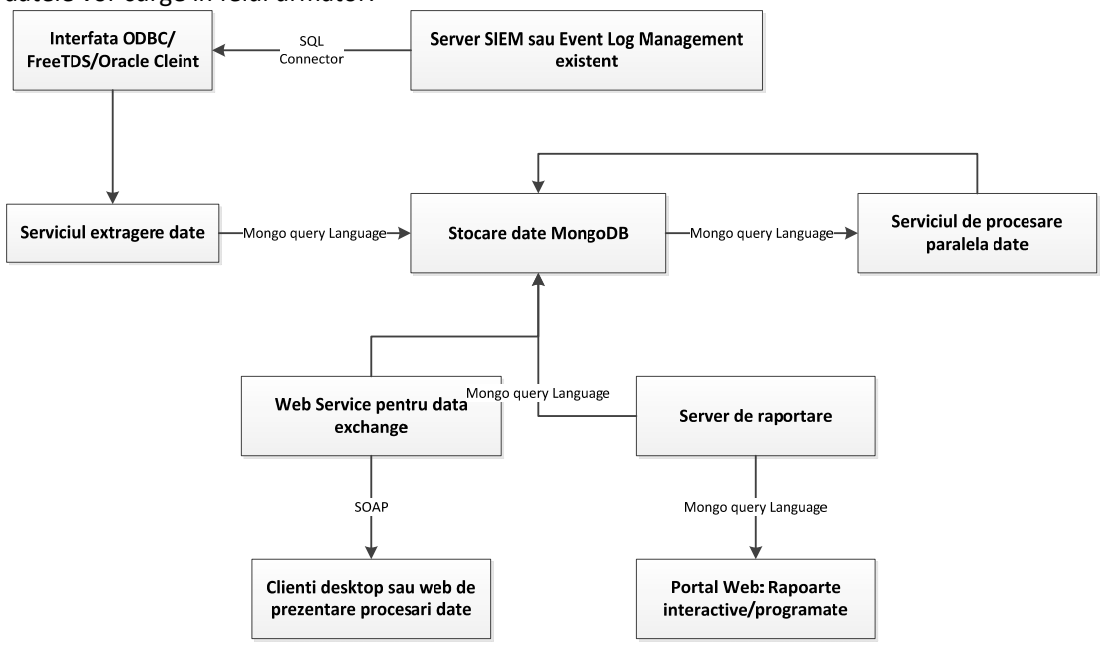
- Server(e) cu Procesor/Procesoare XEON dual 6 core sau echivalent.
- Memorie minima 32 GB

- Spatiu de stocare : 5 TB cu storage RAID 10

Din punct de vedere software suport vom avea:

- Sistem de operare: Debian Linux 6 x64
- Suport NoSQL database: MongoDB
- Suport extragere date din baze de date SQL Server: FreeTDS
- Suport extragere date din baze de date Oracle: Oracle client
- Suport alte baze de date: Linux ODBC
- Nginx pentru server de web cu suport de PHP-FPM
- Rapoarte cu apache Tomcat si BIRT Reports

Aceste aplicatii vor constitui baza software pentru aplicatiile de procesare. Din punct de vedere logic, datele vor curge in felul urmator:



Sistemul de stocare (MongoDB) este optimizat pentru volume mari de date astfel incat sa putem stoca/extrage extrem de rapid informatii

Componentele software aditionale sunt:

1. Serviciul de extragere de date
2. Serviciul de procesare paralela
3. Serviciul de interfatare cu clientii desktop
4. Server de raportare
5. Portal WEB

1. Serviciul de extragere de date

Acest serviciu va folosi interfetele definite pe sistem(ODBC, FreeTDS, Oracle client) pentru extragerea de date din sistemele SIEM folosind unul dintre conectorii special definiti pentru acestea. Definitia unui conector catre SIEM se va face din portalul web si vom oferi suport initial pentru 3 sau 4 aplicatii de SIEM. Serviciul va rula permanent si va colecta date imediat ce acestea sunt disponibile in sistemul de SIEM.

Limbajul de programare al acestui serviciu va fi ori C++ ori Python.

2. Serviciul de procesare paralela de date

Rolul acestui serviciu este de a procesa datele obtinute din sistemele SIEM. Folosind algoritmi de calcul paraleli si ajutat de facilitatile de calcul la nivel hardaware din proceso si placa video, acest serviciu va calcula grafuri pe diverse modele de investigatii folosind datele din sistemele SIEM. Rezultatele acestor procesari se vor salva in sistemul de stocare pentru a fi usor de interogat prin serviciul web de catre aplicatiile client.
Limbajul de programare al acestui serviciu va fi ori C++ ori Python.

3. **Serviciul de schimb de date**

Rolul acestui serviciu este de a asigura data exchange-ul dintre rezultatele procesarilor si clienti. El va folosi pentru data exchange SOAP- Simple Object Access Protocol, protocol bazat pe XML.
Acest serviciu se va ocupa si de partea de autentificare si autorizare in sistem a clientilor.
Limbajul de programare al acestui serviciu va fi PHP 5.3.

4. **Server de raportare**

Acest serviciu va asigura metoda de procesare a rapoartelor interactive sau pe baza de schedule create din portalul web. El va fi interfata dintre portalul web si datele brute stocate la nivel de serviciu de stocare. Va folosi pentru interconectare “mongodb-oda-birt-plugin” intrucat MongoDB nu este o baza de date tipica relationala.

5. **Portal Web**

Acest portal are mai multe roluri:

a) Interfata de configurare a echipamentului (setari IP, permisiuni, useri etc)
b) Interfata de configurare a conectorilor catre SIEM-uri
c) Interfata de raportare cu dashboard-uri

Interfata de raportare va gestiona un numar predefinit de rapoarte grupate pe Report pack-uri. Initial vom oferi urmatoarele categorii de rapoarte:

- Rapoarte standard acces appliance
  - Jurnal investigatii
  - Jurnal accesari
  - Istoric
- Rapoarte pentru aplicatii standard
  - Rapoarte Active Directory
  - Rapoarte MS Exchange

- Dashboard-uri configurabile ce prezinta un overview al starii de securitate a companiei

Aceste specificatii de inceput reprezinta baza sistemului pe care dorim sa il cream.

Cerinte

Se solicita elaborarea unor studii, documentatii, manuale tehnice dupa cum urmeaza:

Cunostinte tehnice privind modalitatea de experimentare a componentelor hardware-software prin aplicarea unor algoritmi specifici de cautare

A. Cerinte generale privind modalitatea de experimentare a componentelor hardware-software

Manualul trebuie sa descrie metodologia de experimentare a componentelor hardware.
Manualul trebuie sa descrie metodologia de experimentare a componentelor software, urmarind cadrul hardware specific
Intreaga metodologie va face referire fundamentata la lucrari tehnice de experimentare hardware-software, acceptate ca referinta in industrie
Metodologia va reproduce cu titlu de certificare, teste de laborator pe medii hardware si software similare mediului de cercetare-dezvoltare din cadrul proiectului

B. Cerinte privind metodologia de dimensionare a componentei hardware-software

Manualul va face referire la metodologia de experimentare descrisa in cadrul subcapitolului (A)
Manualul trebuie sa descrie exact rezultatul aplicarii metodologiei de experimentare, in urma caruia se evidentiaza ca si concluzie, parametrii de dimensionare a componentei hardware
Manualul trebuie sa descrie exact rezultatul aplicarii metodologiei de experimentare, din care rezulta recomandarile de parametrizare software pentru componenta software
Manualul va furniza exemple si studii de caz din metodologiile folosite in dimensionarea echipamentelor ce integreaza multiple functii de securitate a retelei, diferentiat in functie de:

- Numarul de utilizatori pentru care poate fi scalata solutia: sub 100 utilizatori, respectiv intre 100 – 1.000 utilizatori, 1.000 – 10.000 utilizatori si peste 10.000 utilizatori
- Tehnologiile, solutiile si metodele din gama UTM (Unified Threat Management), SIEM (Security Information and Event Management), DLP (Data Loss Prevention), EPP (Endpoint Protection Platforms), MDP (Mobile Data Protection) cu care produsul de cercetare urmeaza sa se integreze

Manualul va furniza detaliere tehnologica a metodologiei de dimensionare pentru principalele tehnologii mentionate, detaliat pe componente si caracteristici, precum si detaliere tehnologica privind metodologia de dimensionare relativa la integrarea cu aceste tehnologii sau relativa la capabilitatile pe care solutia trebuie sa le reproduca:

- Pentru tehnologiile de administrare unificata a amenintarilor, in functie de caracteristica de baza a numarului de utilizatori adresati
- Pentru tehnologiile de administrare a evenimentelor si informatiilor de securitate, in functie de ponderea componentei SIM (Security Information Management) sau SEM (Security Event Management) din arhitectura solutiei
- Pentru tehnologiile de prevenire a pierderilor de date, in functie de caracteristica de baza a numarului de utilizatori adresati (enterprise, de nivel inalt, sau de nisa, de nivel redus)
- Pentru tehnologiile de protectie a dispozitivelor tip endpoint, in functie de functionalitatile inglobate: antimalware, antispyware, firewall, prevenire a intruziunilor, controlul porturilor si echipamentelor, criptare la nivel de fisier si disc, DLP, controlul aplicatiilor si controlul vulnerabilitatii aplicatiilor

- Pentru tehnologiile de protectie a datelor de pe echipamente mobile, in functie de numarul de utilizatori adresati si plaja tehnologica de adresare

C. Cerinte specifice privind metodologia tehnica de experimentare calitativa pentru componenta hardware

Manualul va face referire la metodologia de experimentare descrisa in cadrul subcapitolului (A)
Manualul va descrie metoda de aplicare a rezultatelor de dimensionare hardware detaliate la subcapitolul (B), cu ajutorul careia pot fi experimentati parametrii calitativi hardware specifici, si de unde sa rezulte specificatiile relative la componenta hardware
Intreaga metodologie va face referire fundamentata la lucrari tehnice de experimentare hardware, acceptate ca referinta in industrie
Manualul va include studii relative la metodologii tehnice de experimentare calitativa hardware, cu indicarea solutiilor standard de industrie dezvoltate (sau extinse) in urma aplicarii acestor metodologii.
Astfel, manualul va descrie metodologiile de experimentare folosite in arhitecturarea solutiilor de administrare unificata a amenintarilor. Avem in vedere indesosebi:

- Metodologii de experimentare calitativa hardware pentru solutii Cisco
- Metodologii de experimentare calitativa hardware pentru solutii Clavister
- Metodologii de experimentare calitativa hardware pentru solutii Cyberoam
- Metodologii de experimentare calitativa hardware pentru solutii SonicWall
- Metodologii de experimentare calitativa hardware pentru solutii Sophos
- Metodologii de experimentare calitativa hardware pentru solutii Fortinet
- Metodologii de experimentare calitativa hardware pentru solutii Huawei
- Metodologii de experimentare calitativa hardware pentru solutii Juniper Networks
- Metodologii de experimentare calitativa hardware pentru solutii Trustwave
- Metodologii de experimentare calitativa hardware pentru solutii Netgear

De asemenea, manualul va descrie metodologiile de experimentare folosite in arhitecturarea solutiilor de tip SIEM (Security Information and Event Management). Avem in vedere indeosebi:

- Metodologii de experimentare calitativa hardware pentru solutii AlienVault
- Metodologii de experimentare calitativa hardware pentru solutii eIQnetworks
- Metodologii de experimentare calitativa hardware pentru solutii EMC
- Metodologii de experimentare calitativa hardware pentru solutii ArcSight
- Metodologii de experimentare calitativa hardware pentru solutii Q1 Labs
- Metodologii de experimentare calitativa hardware pentru solutii LogLogic
- Metodologii de experimentare calitativa hardware pentru solutii LogRhythm
- Metodologii de experimentare calitativa hardware pentru solutii NitroSecurity
- Metodologii de experimentare calitativa hardware pentru solutii Novell
- Metodologii de experimentare calitativa hardware pentru solutii Symantec
- Metodologii de experimentare calitativa hardware pentru solutii TriGeo
- Metodologii de experimentare calitativa hardware pentru solutii Trustwave

Manualul va livra metodologia tehnica de experimentare calitativa pentru toate specificatiile hardware necesare:

- Tehnologia procesor necesara indeplinirii functionalitatilor
- Tehnologia memorie necesara indeplinirii functionalitatilor
- Tehnologia RAID necesara indeplinirii functionalitatilor
- Tehnologia relativa la suportul hardware pentru arhitectura RAID recomandata

- Tehnologia hard disk necesara indeplinirii functionalitatilor
- Tehnologia retea necesara indeplinirii functionalitatilor
- Detaliile referitoare la calitatea sursei de energie necesara indeplinirii functionalitatilor
- Detaliile referitoare la metodologia de utilizare si arhitecturare a surselor de energie interne, astfel incat sa se furnizeze nivelele de performanta si disponibilitate continua solicitate
- Metodologia de experimentare a mediului energetic extern, necesar asigurarii performantei de procesare si stocare, dar si disponibilitatii continue a solutiei
- Tehnologia de racire interna necesara indeplinirii functionalitatilor
- Tehnologia de racire externa necesara indeplinirii funtionalitatilor

Manualul va livra metodologia tehnica de experimentare calitativa pentru toate specificatiile hardware necesare:

- Metodologia de experimentare in vederea alegerii tehnologiei procesor optime
- Metodologia de experimentare in vederea alegerii tehnologiei de memorie optime
- Metodologia de experimentare in vederea alegerii tehnologiei RAID optime
- Metodologia de experimentare in vederea alegerii tehnologiei hard disk optime
- Metodologia de experimentare in vederea alegerii tehnologiei retea optime
- Metodologia de experimentare in vederea alegerii tehnologiei de putere optime
- Metodologia de experimentare in vederea alegerii tehnologiei de racire optime

Pentru fiecare componenta hardware pentru care se documenteaza metodologia de experimentare calitativa, furnizorul va efectua demonstratie in laborator care sa ateste validitatea metodologiei de experimentare. Astfel:

- Furnizorul va demonstra in mediu de laborator, metodologia de experimentare relativa la tehnologia procesor
- Furnizorul va demonstra in mediu de laborator, metodologia de experimentare relativa la tehnologia memorie
- Furnizorul va demonstra in mediu de laborator, metodologia de experimentare relativa la tehnologia de stocare interna
- Furnizorul va demonstra in mediu de laborator, metodologia de experimentare relativa la tehnologia retea
- Furnizorul va demonstra in mediu de laborator, metodologia de experimentare relativa la tehnologia de putere
- Furnizorul va demonstra in mediu de laborator, metodologia de experimentare relativa la tehnologia de racire

D. Cerinte specifice privind metodologia tehnica de experimentare calitativa pentru software specificat

Manualul va face referire la metodologia de experimentare descrisa in cadrul subcapitolului (A)
Manualul va descrie metoda de aplicare a rezultatelor de dimensionare software detaliate la subcapitolul (B), cu ajutorul careia pot fi experimentati parametrii calitativi software specifici, si de unde sa rezulte specificatiile relative la componenta software
Intreaga metodologie va face referire fundamentata la lucrari tehnice de experimentare software, acceptate ca referinta in industrie
Manualul va include studii relative la metodologii tehnice de experimentare calitativa software, cu indicarea solutiilor standard de industrie dezvoltate (sau extinse) in urma aplicarii acestor metodologii.

Astfel, manualul va descrie metodologiile de experimentare folosite in arhitecturarea solutiilor de administrare unificata a amenintarilor. Avem in vedere indesosebi:

- Metodologii de experimentare calitativa software pentru solutii CheckPoint
- Metodologii de experimentare calitativa software pentru solutii Clavister
- Metodologii de experimentare calitativa software pentru solutii Cyberoam
- Metodologii de experimentare calitativa software pentru solutii SonicWall
- Metodologii de experimentare calitativa software pentru solutii Sophos
- Metodologii de experimentare calitativa software pentru solutii Fortinet
- Metodologii de experimentare calitativa software pentru solutii GateProtect
- Metodologii de experimentare calitativa software pentru solutii Huawei
- Metodologii de experimentare calitativa software pentru solutii Juniper Networks
- Metodologii de experimentare calitativa software pentru solutii Kerio
- Metodologii de experimentare calitativa software pentru solutii Microsoft
- Metodologii de experimentare calitativa software pentru solutii Netasq
- Metodologii de experimentare calitativa software pentru solutii Trustwave
- Metodologii de experimentare calitativa software pentru solutii Netgear
- Metodologii de experimentare calitativa software pentru solutii WatchGuard

De asemenea, manualul va descrie metodologiile de experimentare folosite in arhitecturarea solutiilor de tip SIEM (Security Information and Event Management). Avem in vedere indeosebi:

- Metodologii de experimentare calitativa software pentru solutii AlienVault
- Metodologii de experimentare calitativa software pentru solutii CorreLog
- Metodologii de experimentare calitativa software pentru solutii eIQnetworks
- Metodologii de experimentare calitativa software pentru solutii EMC
- Metodologii de experimentare calitativa software pentru solutii ArcSight
- Metodologii de experimentare calitativa software pentru solutii Dell Software
- Metodologii de experimentare calitativa software pentru solutii Q1 Labs
- Metodologii de experimentare calitativa software pentru solutii LogLogic
- Metodologii de experimentare calitativa software pentru solutii LogRhythm
- Metodologii de experimentare calitativa software pentru solutii Microsoft
- Metodologii de experimentare calitativa software pentru solutii NitroSecurity
- Metodologii de experimentare calitativa software pentru solutii Novell
- Metodologii de experimentare calitativa software pentru solutii Prism
- Metodologii de experimentare calitativa software pentru solutii S21sec
- Metodologii de experimentare calitativa software pentru solutii Sensage
- Metodologii de experimentare calitativa software pentru solutii SolarWinds
- Metodologii de experimentare calitativa software pentru solutii Splunk
- Metodologii de experimentare calitativa software pentru solutii Symantec
- Metodologii de experimentare calitativa software pentru solutii Tango
- Metodologii de experimentare calitativa software pentru solutii Tenable
- Metodologii de experimentare calitativa software pentru solutii Tier-3
- Metodologii de experimentare calitativa software pentru solutii TriGeo
- Metodologii de experimentare calitativa software pentru solutii Trustwave

In perspectiva acoperirii unor viitoare cerinte tehnologice si integrarii cu solutii de prevenire a pierderilor de date, precum si cu solutii de protectie a datelor pe dispozitive tip endpoint, respectiv echipamente mobile, manualul trebuie sa includa metodologiile de experimentare folosite in arhitecturarea solutiilor de tip DLP, MDP si EPP:

- Metodologii de experimentare calitativa software pentru solutii CheckPoint
- Metodologii de experimentare calitativa software pentru solutii Computer Associates
- Metodologii de experimentare calitativa software pentru solutii Code Green
- Metodologii de experimentare calitativa software pentru solutii Credant
- Metodologii de experimentare calitativa software pentru solutii Dell Software
- Metodologii de experimentare calitativa software pentru solutii eEye
- Metodologii de experimentare calitativa software pentru solutii EMC
- Metodologii de experimentare calitativa software pentru solutii ESET
- Metodologii de experimentare calitativa software pentru solutii F-Secure
- Metodologii de experimentare calitativa software pentru solutii Fidelis
- Metodologii de experimentare calitativa software pentru solutii GFI
- Metodologii de experimentare calitativa software pentru solutii GTB
- Metodologii de experimentare calitativa software pentru solutii IBM
- Metodologii de experimentare calitativa software pentru solutii Kaspersky
- Metodologii de experimentare calitativa software pentru solutii LANDesk
- Metodologii de experimentare calitativa software pentru solutii Lumension
- Metodologii de experimentare calitativa software pentru solutii McAfee
- Metodologii de experimentare calitativa software pentru solutii Microsoft
- Metodologii de experimentare calitativa software pentru solutii Novell
- Metodologii de experimentare calitativa software pentru solutii Palisade
- Metodologii de experimentare calitativa software pentru solutii Panda
- Metodologii de experimentare calitativa software pentru solutii Safend
- Metodologii de experimentare calitativa software pentru solutii Secude
- Metodologii de experimentare calitativa software pentru solutii SkyRecon
- Metodologii de experimentare calitativa software pentru solutii Sophos
- Metodologii de experimentare calitativa software pentru solutii Symantec
- Metodologii de experimentare calitativa software pentru solutii Trend Micro
- Metodologii de experimentare calitativa software pentru solutii TrustWave
- Metodologii de experimentare calitativa software pentru solutii Verdasys
- Metodologii de experimentare calitativa software pentru solutii Wave
- Metodologii de experimentare calitativa software pentru solutii Websense
- Metodologii de experimentare calitativa software pentru solutii WinMagic

Manualul va livra metodologia tehnica de experimentare calitativa pentru toate specificatiile software necesare:

- Metodologia de experimentare in vederea alegerii sistemului de operare optim ca si suport de platforma
- Metodologia de experimentare in vederea alegerii tehnologiei de stocare tip repository, optime, arhitecturat in cadrul serviciului de procesare paralela
- Metodologia de experimentare pentru suportul de extragere date din baze de date SQL Server, arhitecturat in cadrul serviciului de extragere date
- Metodologia de experimentare pentru suportul de extragere date din baze de date Oracle, arhitecturat in cadrul serviciului de extragere date
- Metodologia de experimentare pentru suportul de extragere date din alte baze de date, arhitecturat in cadrul serviciului de extragere date
- Metodologia de experimentare in vederea alegerii tehnologiei optime web server, arhitecturat in cadrul portalului web si serviciului de interfatare cu clientii

- Metodologia de experimentare in vederea alegerii tehnologiei de raportare optime, arhitecturat in cadrul serviciului de raportare

Pentru fiecare componenta software pentru care se documenteaza metodologia de experimentare calitativa, furnizorul va efectua demonstratie in laborator care sa ateste validitatea metodologiei de experimentare. Astfel:

- Furnizorul va demonstra cunostinte expert de implementare a tehnologiilor de stocare date
- Furnizorul va demonstra cunostinte expert de implementare a tehnologiilor de extragere date din baze de date SQL Server, Oracle si alte tipuri de baze de date
- Furnizorul va demonstra cunostinte expert de implementare a tehnologiilor de tip portal
- Furnizorul va demonstra cunostinte expert de implementare a tehnologiilor de raportare

Aditional referirilor solicitate, referitoare la lucrarile tehnice de experimentare software, furnizorul va documenta aspectele relative la fundamentarea implementarii solutiei in medii informatice tip enterprise. Suntem interesati de punctul de vedere al furnizorului de documentatie (metodologie) relativ la un set de bune practici si recomandari recunoscute in industrie, dat fiind ca viitoarea solutie – pentru care se elaboreaza metodologia de experimentare – va trebui sa acopere un set de cerinte fundamentala de conformitate si securitate, protectie de sisteme si date, respectiv integrare cu platforme enterprise terte destinate unor astfel de scopuri.
De aceea, solicitam fundamentarea urmatoarelor aspecte teoretice, in vederea unei ulterioare abordari in practica:

- Fundamentele administrarii Windows Server si Windows Active Directory Directory Services, din perspectiva auditului de conformitate si securitate
- Bunele practici ale auditului de identitate si acces in mediile eterogene
- Un ghid de bune practici pentru guvernarea si conformitatea IT
- Bune practici referitoare la integrarea unei solutii de securitate informatica cu tehnologiile de audit Microsoft Audit Collection Services si Quest InTrust
- Bune practici referitoare la integrarea unei solutii de securitate informatica cu tehnologiile de audit HP ArcSight si Quest ChangeAuditor
- Bunele practici referitoare la integrarea solutiilor de management al identitatii si controlului de acces cu solutii de securitate si audit de securitate informatica
- Strategii de implementare pentru atingerea si mentinerea conformitatii IT
- Colectarea evidentelor de conformitate – rolul logurilor de evenimente
- Bunele practici referitoare la combaterea provocarilor de securitate si conformitate
- Atingerea cerintelor de management al schimbarilor si conformitate a monitorizarii intr-o retea centrata Microsoft
- Atingerea provocarii privind managementul logurilor pentru sisteme Unix si Linux
- Bunele practici de industrie privind satisfacerea cerintelor referitoare la standardul PCI DSS
- Bunele practici de industrie relative la atingerea scopului de guvernare a accesului la date
- Provocarile si bunele practici pentru acoperirea cerintelor FICAM si FISMA

E. Cerinte specifice privind metodologia tehnica de experimentare calitativa a componentei hardware-software cu aplicarea algoritmilor specificati

Manualul va face referire la metodologia de experimentare descrisa in cadrul subcapitolului (A)
Manualul va face referire la metodologia de dimensionare a componentei hardware-software, descrisa la subcapitolul (B)
Manualul va detalia metodologia de experimentare calitativa a componentei hardware-software, asa cum a fost descrisa in cadrul subcapitolelor (C) si (D), astfel incat sa rezulte un set de directive cadru

pentru aplicarea algoritmilor specificati, si din care sa reiasa specificatiile ghid pentru creionarea componentei hardware-software.
Manualul va detalia metodologia tehnica de experimentare calitativa a componentei hardware-software, cu aplicarea algoritmilor specificati, diferentiat pe fiecare familie de functionalitati si suport tehnologic de baza, dupa cum urmeaza:

1. In ceea ce priveste managementul datelor si capabilitatile analitice, se va avea in vedere experimentarea in scopul obtinerii:
    a. unui pachet complet de hardware si software destinat generarii de rapoarte, analize si modele analitice care sa raspunda nevoilor specifice de business ale posibililor beneficiari
    b. unui design unificat si a unei configuratii preconstruite, destinate managementului de date integrate
    c. unei platforme deosebit de performante, de ultima generatie
    d. suportului complet pentru cerinte de business intelligence
    e. suportului complet pentru conectarea la surse de date tip cloud si on-premise
    f. de functionalitati tip data warehouse, cu capabilitati de interogare rapida, partitionare de tabele, integrare cu unelte de analiza terte si stocarea de obiecte binare de mari dimensiuni (BLOBs) – intr-o locatie storage interna sau externa
    g. unui produs compact destinat pietei SMB pana la midsize, dar si integrarii in cadrul unor solutii enterprise
2. In ceea ce priveste managementului sistemelor client, se va avea in vedere experimentarea in scopul integrarii cu:
    a. Solutii de tip UTM, SIEM, DLP
    b. Solutii de management operational la nivel de client si server
    c. Solutii de protectie a dispozitivelor tip endpoint si echipamentelor mobile
3. In ceea ce priveste infrastructura suport, se va avea in vedere experimentarea in scopul obtinerii:
    a. Unei solutii facil de scalat prin conectarea rapida la o infrastructura convergenta
    b. Unei solutii rackabile, facil de integrat in orice arhitectura client
    c. Unei solutii ce poate aduce beneficii imediate si semnificative in orice proiect major de tip enterprise:
        i. Data Center si Cloud Management, respectiv proiecte destinate optimizarii operatiunilor in centrele de date si simplificarii managementului IT
        ii. Data Protection, respectiv proiecte destinate protejarii datelor critice din mediile fizice, virtuale, de aplicatii sau de cloud
        iii. Information Management, respectiv proiecte destinate administrarii datelor de pe orice platforma
        iv. Mobile Workforce Management, respectiv proiecte destinate protejarii si gestionarii dispozitivelor mobile de orice natura, dar si desktop-urilor si laptop-urilor
        v. Security, respectiv proiecte destinate protejarii sistemelor si datelor din organizatie
4. In ceea ce priveste securitatea retelelor si datelor, se va avea in vedere experimentarea in scopul obtinerii unui produs care sa furnizeze performanta si securitate fara compromis:
    a. O platforma care sa acopere cerinte de securitate avansata a retelei, la viteze multigigabit, totul intr-un design compact si eficient
    b. Arhitectura multi-core de ultima generatie
    c. Tehnologie de inspectie avansata a pachetelor

d. Controlul aplicatiilor si prevenirea amenintarilor

5. In ceea ce priveste scalabilitatea hardware / software, se va avea in vedere experimentarea in scopul integrarii in infrastructuri de mare performanta:
    a. Infrastructuri fizice si virtuale unificate – produsul va trebui sa poata adresa echipamente de mare complexitate si capacitate, cum ar fi switch-uri/routere enterprise, ecosisteme wireless, centre de date si medii cloud
    b. Echipamente de stocare in diverse tehnologii (NAS, SAN, DAS) – produsul va trebui sa poata fi scalat cu usurinta, prin utilizarea unui storage extern de orice tip; totodata, produsul va oferi protectie si securitate pentru aceste sisteme de stocare
    c. Sisteme server tip rack – produsul va fi construit pe suport tehnologic tip rack de ultima generatie

Cunostinte tehnice privind modalitatea de proiectare a modulelor software imbarcate pe modulele hardware

a. Cerinte specifice privind evaluarea sistemelor de operare
    i. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Microsoft Windows Server 2008
    ii. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Microsoft Windows Server 2012
    iii. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Linux – Red HatEnterprise Linux 6
    iv. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Linux – Red HatEnterprise Linux 7
    v. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Linux – Ubuntu Server 12
    vi. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Linux – Ubuntu Server 13
    vii. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Linux – Debian 6
    viii. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Linux – Debian 7
    ix. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Unix – FreeBSD 8
    x. Manualul trebuie sa prevada metodologia de evaluarea a sistemului de operare Unix – FreeBSD 9
    xi. Manualul trebuie sa prevada criterii diferentiatori pentru fiecare sistem de operare evaluat.
b. Cerinte specifice privind evaluarea limbajelor de programare cu accent pe performanta acestora in stransa legatura cu sistemul de operare evaluat anterior. Se va pune accent pe limbajele de programare functionale in cadrul mai multor sisteme de operare.
    i. Manualul trebuie sa prevada metodologia de evaluare a limbajului de programare C++
    ii. Manualul trebuie sa prevada metodologia de evaluare a limbajului de programare C#
    iii. Manualul trebuie sa prevada metodologia de evaluare a limbajului de programare ASP
    iv. Manualul trebuie sa prevada metodologia de evaluare a limbajului de programare PHP

v. Manualul trebuie sa prevada metodologia de evaluare a limbajului de programare JAVA
vi. Manualul trebuie sa prevada metodologia de evaluare a limbajului de programare PERL
vii. Manualul trebuie sa prevada metodologia de evaluare a limbajului de programare RUBY
viii. Manualul trebuie sa prevada metodologia de evaluare a limbajului de programare PYTHON
ix. Manualul trebuie sa prevada metodologia de evaluare a frameworkurilor de tipul MVC - specifice limbajelor de programare evaluate

c. Cerinte specifice privind modalitatea de proiectare a modulelor software
   i. Manualul trebuie sa prevada metodologii pentru proiectare a softwareului, de tipul AGILE – Agile Modeling
   ii. Manualul trebuie sa prevada metodologii pentru proiectare a softwareului, de tipul AGILE - Dynamic Systems Development Method
   iii. Manualul trebuie sa prevada metodologii pentru proiectare a softwareului, de tipul AGILE – Extreme Programming
   iv. Manualul trebuie sa prevada metodologii pentru proiectare a softwareului, de tipul AGILE – Lean Software Development
   v. Manualul trebuie sa prevada metodologii pentru proiectare a softwareului, de tipul AGILE – SCRUM
d. Cerinte generale privind modalitatea de proiectare a modulelor software imbarcate pe modulele hardware
   i. Manualul trebuie sa prevada metodologii de imbarcare a modulelor software dezvoltate in cadrul modulelor hardware.
   ii. Manualul trebuie sa contina indicatorii de performanta pentru sistemele software imbarcate pe modulele hardware
   iii. Manualul trebuie sa contina indicatorii necesari pentru cotarea nivelului de succes al procedurii de imbarcare a modulelor software pe modulele hardware

Cunostinte tehnice privind modalitatea de asamblare optima a modulelor hardware si software

Un appliance este un intrument dedicat unor anumite activitati specifice. In cazul nostru, un appliance va fi rezultatul asteptat ca livrabil in cadrul proiectului de cercetare la care lucram. Acesta va avea 2 componente principale:

- Module de tip software
- Module de tip hardware

Pentru crearea si optimizarea acestui appliance, se impune crearea de configuratii/teste specifice pe hard/soft pentru obtinerea maximului de performanta, disponibilitate si eficienta.

Astfel, ofertantul trebuie sa ne puna la dispozitie urmatoarele:

- Metodologie generala de asamblare hardware pe arhitectura de tip Intel pentru procesoare x64.
- Metodologie generala de asamblare si interconexiune, pe module specifice de software:
  - Serviciul de procesare date
  - Serviciul de extragere date
  - Serviciul de detectie a anomaliilor

Oferantul trebuie sa ofere cunostinte tehnice pentru:

a) Asamblarea hardware
   - Asamblarea si optimizarea din punct de vedere CPU.
   - Asamblare si optimizare din punct de vedere memorie.
   - Asamblare si optimizare din punct de vedere I/O.
   - Alegerea necesarului de hardware disponibl.
   - Stabilirea factorului de marime pentru hardware.
   - Asamblarea optima in conditii de ventilatie slaba.
   - Stabilire necesar hardware si in functie de specificatiile software. Trebuie luat in calcul doar volumul de date necesar precalcularilor - adica MB/s.
   - Formula de calcul necesar in functie de parametrul de MB/s
   - Modalitati tehnice de protectie a accesului fizic la appliance
   - Modalitati tehnice de asigurare a redundantei
   - Modalitati tehnice de asigurare a inaltei disponibilitati

b) Asamblare module software
   - Optimizarea module software pentru hardware
   - Optimizarea module software – pentru intercomunicatie generala
   - Optimizarea module software – pentru volume mici de date
   - Optimizarea module software – pentru volume mari de date
   - Optimizarea procesare date – pentru calcul paralel de legaturi intre evenimente sau display de date
   - Optimizare module pentru aplicatii multi-procesor si multithreading
   - Optimizare module prin crearea si gestionarea dinamica de buffere pentru I/O
   - Optimizare module prin crearea si gestionarea dinamica de buffere pentru CPU
   - Optimizare module prin crearea si gestionarea dinamica de buffere pentru memorie
   - Optimizare module prin crearea si gestionarea dinamica de buffere pentru partea de display
   - Compatibilitatea perfecta cu sistemul de operare gazda
   - Compatibilitatea si optimizarea pe hardware-ul disponibil.
   - Asamblarea dinamica de bufferi pentru precalcularea de informatii specifice
     - Prin procesare in placa grafica
     - Prin procesare in CPU
     - Pentru calcul serial
     - Pentru calcul paralel
   - Stabilirea necesarului de bufferi pentru un volum mare de date/secunda
     - Stabilire necesar de I/O – formula de calcul de IOPS
     - Stabilire necesar de CPU
     - Stabilirea necesar de Memorie
   - Gestiune de memorie in contextul modulelor individuale
   - Gestiune de memorie in contextul general (OS + APPLICATII + MODULE Aditionale)
   - Stabilire necesar individual pentru fiecare modul de:
     - CPU (in Mhz)
     - Memorie (in MB)
     - Operatii/secunda (pentru placi grafice)
   - Stabilire necesar general pentru toate modulele software
   - Stabilire functii de calcul de putere pentru hardware (masurat in volum de date/secunda).
   - Stabilire metodei de calcul pentru media de utilizare a componentelor software/hardware. Din aceasta functie trebuie facuta scalarea software/hardware.

Cunostinte tehnice pentru testarea hardware conforma cu standardele impuse

e. Cerinte generale privind modalitatea de testare hardware
    i. Modalitatea de construire a mediului de test
        1. Manualul trebuie sa contina metodologia de construire a unui mediu de test pentru modulele hardware folosite.
        2. Manualul trebuie sa contina metodologia de evaluare a consistentei mediului de testare pentru modulele hardware.
        3. Manualul trebuie sa contina criterii de evaluare pentru urmatoarele componente
            a. Placa Grafica
            b. Procesor
            c. Memorie Volatila
            d. Mediu de stocare
                i. HDD
                ii. Discuri de tip solid-state
        4. Manualul trebuie sa contina costul estimativ pentru componentele hardware necesare testarii
    ii. Scenarii de testare
        1. Manualul trebuie sa contina scenarii de testare de tipul STRESS TEST HALT pentru echipamentele hardware
        2. Manualul trebuie sa contina scenarii de testare de tipul LOAD TESTING pentru echipamentele hardware
        3. Manualul trebuie sa contina metodologia de evaluare a rezultatelor testelor
    iii. Proceduri de testare
        1. Manualul trebuie sa contine proceduri de testare manuala pentru componentele hardware.
        2. Manualul gtrebuie sa contina proceduri de testare automata pentru componentele hardware

Cunostinte tehnice privind modalitatea de testare a software-ului imbarcat, in vederea avizarii

f. Cerinte generale privind modalitatea de testare software
    i. Modalitatea de construire a mediului de test
        1. Manualul trebuie sa contina metodologia de construire a unui mediu de test pentru modulele software folosite.
        2. Manualul trebuie sa contina metodologia de evaluare a consistentei mediului de testare pentru modulele software.
    ii. Scenarii de testare
        1. Manualul trebuie sa contina criterii de evaluare pentru minim urmatoarele tipuri de componente software
            a. Formulare
                i. HTML
                ii. In cadrul aplicatiilor desktop
            b. Campuri de tip INPUT
            c. Module de procesare de date
            d. Module de evaluare conditii
            e. Module de selectare de tip
                i. Range
                ii. Data

iii. Exclusiv numeric
iv. Alfanumeric

2. Manualul trebuie sa contina scenarii de testare de tipul BLACK BOX pentru modulele software
3. Manualul trebuie sa contina scenarii de testare de tipul STRESS TEST pentru modulele software
4. Manualul trebuie sa contina scenarii de testare de tipul LOAD TEST pentru modulele software
5. Manualul trebuie sa contina scenarii de testare de tipul PENTEST, cu specific pe teste de tipul buffer overflow pentru modulele software
6. Manualul trebuie sa contina metodologia de evaluare a rezultatelor testelor

iii. Proceduri de testare

1. Manualul trebuie sa contine proceduri de testare manuala pentru componentele software.
2. Manualul trebuie sa propuna tehnologiile de testare automata in functie de specificul modulelor software dezvoltate de catre beneficiar
3. Manualul trebuie sa contina proceduri de testare automata pentru componentele software

Inainte de semnarea contractului, ofertantul desemnat castigator va trebui sa organizeze o sesiune practica prin care sa demonstreze competentele in tehnologiile solicitate. Intrucat solicitam livrarea unei metodologii aplicabile in practica, dorim sa vedem in cadrul acestui demo punctele esentiale care sa demonstreze aplicabilitatea in practica a metodologiilor mai sus cerute. In cadrul acestui demo se vor selecta aleator 5 metodologii.