(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) **RO 130998 A2**
(51) **Int.Cl.**
G06F 21/50 (2013.01)

(12) # CERERE DE BREVET DE INVENȚIE

(21) Nr. cerere: **a 2014 00618**

(22) Data de depozit: **13/08/2014**

(41) Data publicării cererii:
30/03/2016 BOPI nr. **3/2016**

(71) Solicitant:
• **Q-EAST SOFTWARE S.R.L.**,
STR.BRAŞOV NR.19, BL.OD5, SC.5, ET.3, AP.157, SECTOR 6, BUCUREŞTI, B, RO

(72) Inventatori:
• **INVENTATORI NEDECLARAȚI**, *, *RO*

(74) Mandatar:
WEIZMANN ARIANA & PARTNERS AGENȚIE DE PROPRIETATE INTELECTUALĂ S.R.L., *STR.11 IUNIE NR.51, SC.A, ET.1, AP.4, BUCUREŞTI*

(54) # PLATFORMĂ INOVATIVĂ INTEGRATĂ DE MONITORIZARE ŞI SECURITATE IT A FLUXURILOR INFORMAȚIONALE ALE UNEI FIRME - PITQEAST

(57) **Rezumat:**

Invenția se referă la o platformă integrată de monitorizare şi securitate IT a fluxurilor informaționale ale unei firme. Platforma conform invenției cuprinde componente hardware şi software care asigură extragerea datelor de securitate din sisteme existente, de tip "EventLogManagement" sau "SIEM", procesarea acestora şi oferirea pentru vizualizare a informațiilor obținute şi a legăturilor dintre ele.

Revendicări: 2

RO 130998 A2

12.2 Descriere

Titlul brevetului este „Platformă inovativă integrată de monitorizare și securitate IT a fluxurilor informaționale ale unei firme - PITQEAST".

Echipamentul de procesare ce urmeaza a fi brevetat (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.

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.

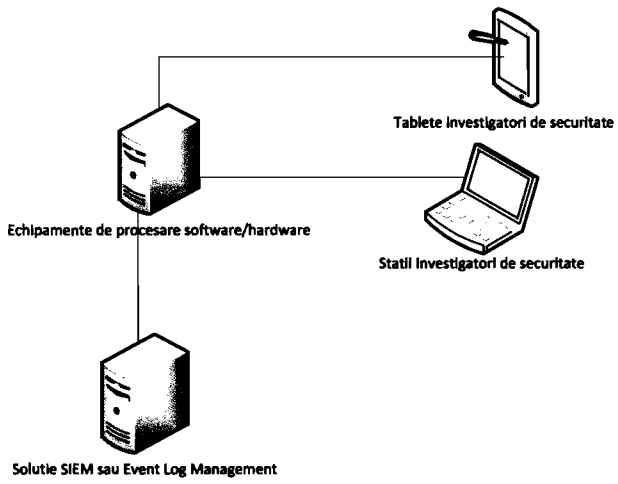
Aceste doua tipuri de solutii, ofera pentru partea de investigatii de securitate rapoarte, pentru diferite in functie de specificul aplicatiei, servere-lor. Un exemplu concludent ar fi existenta rapoartelor standard de access ale utilizatorilor la resursele companiilor. In acest fel,o implementare tipica 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.

Arhitectura logica si functionala a solutiei propuse are urmatoarele componente.



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 not-only-sql DB si se vor aplica algoritmi de procesare pe tot volumul de date.

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 C++ si 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 il cream.

Principalele componente (revendicari) 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.

12.3 Revendicari

Titlul brevetului este „Platformă inovativă integrată de monitorizare și securitate IT a fluxurilor informaționale ale unei firme - PITQEAST".

Principalele componente (revendicari) 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.