UNIVERSITATEA POLITEHNICA DIN BUCUREȘTI
FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE
DEPARTAMENTUL DE CALCULATOARE

Teză de doctorat

în Calculatoare și Tehnologia Informației

Sistem și metodă de pentru reducerea suprafeței de atac și optimizarea răspunsului la incidente de securitate cibernetică

Autor:

Ing. Cristian Săndescu

Coordonator științific:

Prof. dr. ing. Răzvan-Victor Rughiniș

București

2022

Cuprins

Listă Figuri

Listă Tabele

1 Introducere

1.1 Perspectivă Generală

Pentru a răspunde la provocarea amenințărilor cibernetice, industria securității cibernetice se vede nevoită să inoveze constant în vederea dezvoltării de noi mecanisme care să asigure monitorizarea și apărarea continuă a sistemelor informatice. Această sarcină este cu atât mai complexă cu cât apariția noilor tehnologii care amplifică riscul de exploatare de către actorii rău intenționați crește.

Într-o piața liberă caracterizată de competiție, succesul produselor și serviciilor software depinde de viteza de lansare. Deși benefică, această caracteristică a pieței libere, și în special a industriei IT, aduce cu sine o consecința neintenționată: expunerea în fața atacurilor cibernetice. Vulnerabilitățile tehnice apărute ca rezultat al presiunii mediului de afaceri asupra implementării tehnice rapide creează riscuri de exploatare și pierderi materiale sau intelectuale. Astfel, domeniul securității cibernetice oferă un răspuns la paradigma curentă a dezvoltării soluțiilor informatice caracterizată de o viteză și de o complexitate exponențiale. Acest răspuns se referă la dezvoltarea de tehnici și sisteme pentru reducerea riscului de exploatare a vulnerabilităților cibernetice.

Atât starea de fapt, cât și estimările experților din domeniul securității cibernetice arată faptul că avansul tehnologic creează un mediu informatic complex în care mijloacele de exploatare a vulnerabilităților cibernetice devin din ce în ce mai sofisticate, rapide și eficiente. O analiză a costurilor create de exploatarea vulnerabilităților din 2015 cibernetice ilustrează costuri anuale de 300 de miliarde de euro [1]. O analiză descriptivă din 2016 a unui set de date cu atacuri cibernetice arată că un cost minim al unui atac cibernetic este de 200.000 de euro [2]. Reiese de aici că mijloacele de reducere a riscului exploatării vulnerabilităților cibernetice reprezintă elemente esențiale în vederea evitării de costuri.

Timpul necesar mediu pentru identificarea si remedierea unei breșe de securitate este de 287 zile, iar 53% dintre organizații nu sunt conștiente de existenta desfășurării atacului, in tot acest timp, conform celui mai recent studiu Ponemon, IBM [3]. Echipele care lucrează in centrele de operațiuni de securitate cibernetica (SOC) sunt copleșiți de numărul mediu de 11 mii de alerte pe zi la care aceștia trebuie sa răspundă, plasând astfel industria actuala de securitate cibernetica la un deficit de 2.7 milioane de profesioniști - ISC2 [4]. In contextul de

mai sus, influențat si de schimbările impuse de pandemie, numărul de atacuri de tip ransomware a crescut de 13 ori in prima jumătate a lui 2021, comparativ cu aceeași perioada din 2020, arată raportul Trend Micro [5].

Există două abordări pentru reducerea riscurilor de exploatare a vulnerabilităților cibernetice din infrastructurile informatice. În primul rând, este vorba de abordarea reactivă care presupune un răspuns în timp real în fața tentativelor de exploatare a vulnerabilităților cibernetice. A doua abordare pune accentul pe proactivitate și presupune tratarea vulnerabilităților înainte de exploatarea propriu-zisă. Reiese de aici că mitigarea riscului prin cea de-a doua abordare (abordarea proactivă) reprezintă un proces continuu care are ca fundație principală operația de prioritizare a vulnerabilităților cibernetice identificate într-o infrastructură informatică. Altfel spus, abordarea proactivă presupune monitorizarea permanentă a unei infrastructuri cibernetice în vederea identificării și prioritizării vulnerabilităților cibernetice pentru remedierea acestora înaintea exploatării.

Abordarea proactivă în vederea asigurării securității cibernetice presupune o serie de măsuri preventive luate în vederea reducerii riscului de exploatare a vulnerabilităților cibernetice. Aceste măsuri mizează pe reducerea riscului de exploatare prin prioritizarea acțiunilor de remediere a punctelor slabe dintr-o infrastructura cibernetică. Procesul de prioritizare menționat este realizat prin cuantificarea riscului asociat unei expuneri prin raportare la o serie de parametrii.

Un prim tip de parametrii propuși în această teză se referă la parametrii interni. Parametrii interni utilizați în abordarea proactivă de reducere a riscului cibernetic pot fi definiți în termeni de variabile care reprezintă trăsăturile sistemului ce se vrea a fi protejat. Procesul prin care aceste variabile sunt utilizate ca punct de referință în prioritizarea vulnerabilităților existente este bazat pe o metodă de evaluare a riscului ce pune accentul pe impactul pe care exploatarea unei vulnerabilități îl are asupra infrastructurii vizate. Această metodă accentuează contextul organizațional al infrastructurii ce se dorește a fi protejată.

Al doilea tip de parametrii propuși se referă la parametrii externi. Parametrii externi utilizați în abordarea proactivă de reducere a riscului cibernetic pot fi definiți în termeni de variabile ce reprezintă dinamica mediului extern al unei infrastructuri cibernetice. În acest caz, accentul cade pe probabilitatea exploatării unei vulnerabilități cibernetice date fiind

motivațiile, obiectivele și capacitățile agenților care intenționează exploatarea sistemului ce se vrea a fi protejat.

Așadar, această teză prezintă o serie de studii empirice realizate în vederea dezvoltării componentelor unui sistem de reducere proactivă a riscului amenințărilor cibernetice. Sistemul propus are ca scop cuantificarea parametrilor interni și externi în vederea prioritizării vulnerabilităților cibernetice ale unui sistem informatic. Astfel, sistemul propus se dorește a primi ca intrare o serie de parametrii interni și externi care caracterizează o infrastructură cibernetică și a oferi ca ieșire o listă de vulnerabilități cibernetice prioritizate în funcție de riscul de exploatare. Figura *1* oferă o reprezentare grafică a sistemului.

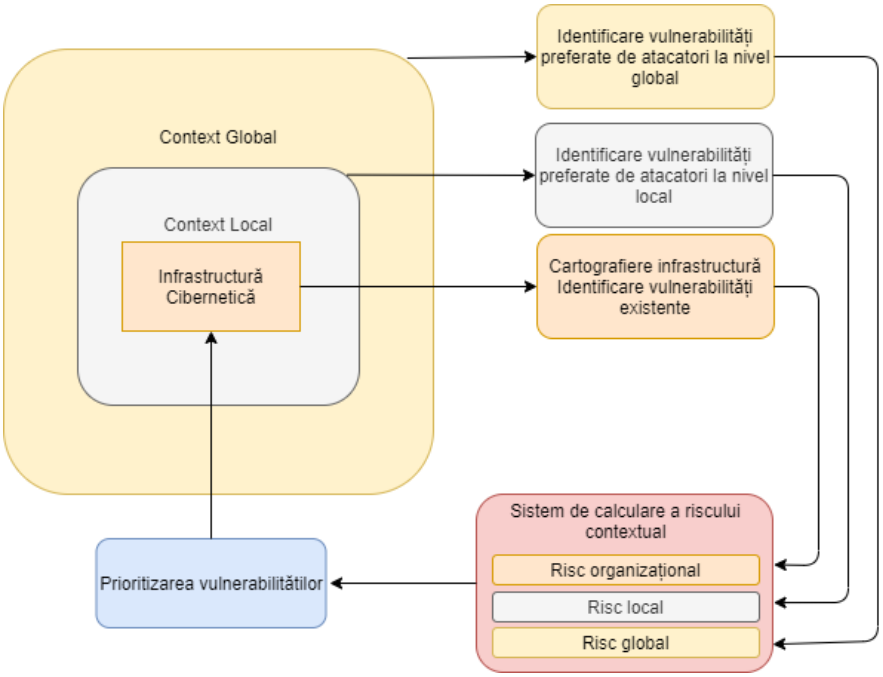

Figura 1. Perspectiva de ansamblu asupra sistemului propus.

1.2 Structura Tezei

Teza este organizată în cinci secțiuni principale. Următoarea secțiune prezintă aspectele teoretice care acționează ca fundament pentru studiile empirice dezvoltate în secțiunea ulterioară. Sunt prezentate aspecte teoretice ce țin de tehnicile si modelele utilizate in procesul de cercetare. Acestea acoperă metodele de procesare a limbajului natural, sisteme de tip honeypot și metode de evaluare a riscului unei vulnerabilități de securitate. Fiecare dintre

secțiunile menționate facilitează prezentarea rezultatelor studiilor empirice. Fiecare studiu empiric prezintă una din cele trei componente prezentate în Figura 1: modelul pentru identificarea timpurie a vulnerabilităților de securitate cibernetica, modelul de optimizare a răspunsului la atacuri cibernetice folosind sisteme de tip „Honeypot", si modelul de calcul integrat al riscului contextual pentru reducerea suprafeței cibernetice de atac. Sunt prezentate trei studii empirice care vizează dezvoltarea modulelor necesare proiectării, implementării si evaluării performantelor modelelor propuse.

Primul studiu empiric descrie implementarea și rezultatele unui sistem de identificare a vulnerabilităților timpurii. Rezultatele acestuia demonstrează fezabilitatea dezvoltării unor modele de învățare automata, bazate pe înțelegerea limbajului natural care să permită descoperirea timpurie a noilor vulnerabilității, precum si reducerea timpului de detecție pentru echipele de tip SecOps. Studiul are ca scop cuantificarea parametrilor externi globali preluați din surse deschise precum platformele de știri de specialitate si rețelele de socializare unde sunt prezente comunitățile de cercetători precum Twitter. Secțiunea 3.1 asociată prezintă rezultatele implementării unui sistem bazat pe algoritmi de procesare a limbajului natural și învățare automată care permite cuantificarea tendințelor globale de atac din date de tip OSINT, in timp ce aspectele teoretice utilizate sunt prezentate in Secțiunea 2.1 a prezentului document.

Secțiunea asociată celui de-al doilea studiu empiric prezintă rezultatele proiectării, implementării si evaluării performantei unui sistem inovativ de tip „honeypot" denumit Hunt. Acest sistem presupune dezvoltarea unei arhitecturi de agent dezvoltată pentru a cartografia în detaliu infrastructura cibernetică ce se dorește a fi protejată în vederea obținerii de date necesare pentru dezvoltarea unui sistem de tip honeypot care să permită analiza tendințelor locale de atac ale actorilor rău intenționați – agentul de camuflare. A doua componenta este reprezentata de subsistemul de profilare al atacatorilor folosind elemente din teoria jocurilor. De asemenea, această secțiune prezintă rezultatele implementării unui sistem de tip honeypot pentru o infrastructură cibernetică reala, prin testarea sistemului camuflat intre paginile unei aplicații web reale. Spre deosebire de sistemele tradiționale de tip honeypot, sistemul propus folosește doua componente noi: un sistem de camuflare, si un sistem de gamificare a atacatorului. O astfel de abordare necesită simularea mediului ce se vrea a fi protejat și atragerea unor atacatori reali pentru a le înțelege strategiile și țintele de atac. Secțiunea 2.2

dezvoltă pe larg aspectele teoretice ale unei abordări în acest sens bazată pe honeypot, in timp ce secțiunea 3.2 prezinta modul de lucru si rezultatele studiului.

Cel de-al treilea studiu empiric descrie implementarea și rezultatele unui algoritm de calcul al riscului contextual organizațional al unei infrastructuri cibernetice. Acesta are ca scop cuantificarea parametrilor interni si externi în vederea prioritizării vulnerabilităților cibernetice identificate pentru reducerea nivelului de zgomot la nivelul unei infrastructuri complexe. Secțiunea 3.3 asociată acestui studiu empiric prezintă rezultatele implementării unui algoritm si a unui sistem de prioritizare a vulnerabilităților dezvoltate pentru analiza infrastructurii cibernetice ce se vrea a fi protejată precum și rezultatele metodologiei folosite pentru reducerea suprafeței de atac a organizației de către echipele SecOps in mod eficient. Elementele de teorie utilizate in acest studiu sunt prezentate pe larg in cadrul secțiunii 2.3 a prezentei teze.

Împreună, rezultatele celor trei studii empirice permit deschiderea unei secțiuni de discuții în care sunt prezentate limitările și oportunitățile de integrare în vederea implementării unui sistem care sa asigure eficientizarea proceselor din centrele de securitate operațională, vizând cele doua arii de baza ale funcționarii acestora. Această secțiune este urmată de o secțiune în care sunt prezentate pe scurt rezultatele si concluziile fiecăruia dintre studii împreuna cu posibilitățile ulterioare de optimizare.

2 Aspecte teoretice

În această secțiune sunt descrise aspectele teoretice relevante pentru implementarea sistemului propus. Astfel, sunt discutate aspecte teoretice ce țin de detecția timpurie folosind tehnici de prelucrare a limbajului natural, aspecte ce țin de sisteme de tip honeypot și aspecte ce țin de riscul contextual de exploatare a unei vulnerabilități cibernetice.

2.1 Detecţia timpurie folosind tehnici de prelucrare a limbajului natural

Prelucrarea limbajului natural este o componentă esențială în vederea dezvoltării unui sistem de estimare a riscului contextual global de exploatare a unei vulnerabilități cibernetice. Așadar, această secțiune descrie diferite tehnici și proceduri pentru implementarea și optimizarea unui algoritm care să permită prelucrarea datelor din surse deschise în vederea identificării informațiilor despre vulnerabilități cibernetice.

În primul rând sunt descrise procese din secvența de prelucrare a limbajului natural Spacy [6]. Pentru fiecare proces, sunt analizate diferite tehnici de implementare și optimizare prin raportare la informațiile identificate în lucrări precum: Jurafsky and Martin [7], Pulford [8], Nair and Hinton [9], Bouchard [10], Shore and Johnson [11], Kingma and Ba [12], Gal and Ghahramani [13], Honnibal and Johnson [14].

Adițional, sunt analizate tehnici și proceduri de clasificare a textului prin algoritmi de învățare automată propuse de Zhang [15], Rennie, et al. [16], McCallum and Nigam [17], Vryniotis [18]., Nigam, et al. [19], Cortes and Vapnik [20], Platt [21], Wu, et al. [22], Crammer and Singer [23], Mola [24], Quinlan [25], Breiman [26], Dumais [27], Mikolov, et al. [28], Pennington, et al. [29], Landauer, et al. [30], Zhila, et al. [31], DeepLizard [32], Ognjanovski [33], Ruder [34], Brownlee [35], Senior, et al. [36], Sumit [37], Jacovi, et al. [38], Zhang, et al. [39], De Mulder, et al. [40], Hochreiter and Schmidhuber [41], Sherstinsky [42], Bahdanau, et al. [43], Su and Kuo [44], Vaswani, et al. [45], Horev [46] și alții.

Această secțiune reușește așadar să ofere o perspectivă de ansamblu asupra mijloacelor existente prin care este posibilă dezvoltarea unui sistem pentru detecția timpurie a vulnerabilităților cibernetice prin intermediul de tehnici de prelucrare a limbajului natural.

2.2 Optimizarea răspunsurilor la atacuri cibernetice folosind sisteme de tip honeypot

Mediul extern al unei infrastructuri cibernetice este compus din mediul local și mediul global. Fiecare tip de mediu aduce cu sine un alt tip de risc de exploatare. Riscul local se referă la tendințele în materie de atacuri cibernetice care vizează cu precădere o infrastructură cibernetică specifică. În timp ce calcularea pe baza riscului contextual organizațional permite prioritizarea vulnerabilităților prin raportare la importanța componentelor și probabilitatea de exploatare dată fiind susceptibilitatea acestora în fața atacurilor, profilarea atacatorilor permite prioritizarea vulnerabilităților prin raportare la tipurile și țintele de atac preferate de actorii rău intenționați.

În acest sens, aspectele teoretice discutate în secțiunea de față permit identificarea direcțiilor de implementare a unui sistem modular de evaluare a riscului contextual local de exploatare a vulnerabilităților cibernetice dintr-o infrastructură informatică în vederea optimizării răspunsurilor la atacuri cibernetice. Astfel, această secțiune începe prin utilizarea unor lucrări precum cele propuse de Spitzner [47], Pouget, et al. [48], Barnett [49], Livshitz [50] și HoneynetProject [51] pentru a defini trei concepte importante: honeypot, honeynet și honeytoken.

Mai departe, această secțiune pornește de la sinteza propusă de Nawrocki, et al. [52] în vederea analizării sistemelor de tip honeypot existente. În acest sens, sunt analizate sistemele propuse de Portokalidis, et al. [53], Sharma and Sran [54], HiHatProject [55], Zhuge, et al. [56], TheHoneynetProject [57], Oosterhof [58], Provos [59], Rapid7 [60] și Osquery [61]. Analiza sistemelor de mai sus permite așadar identificarea punctelor de referințe în vederea implementării sistemului de evaluare a riscului contextual local de exploatarea a unei vulnerabilități cibernetice și optimizarea răspunsurilor.

Obținerea datelor din cadrul unui honeypot permite mai departe rezolvarea unor probleme precum nevoia de informație a “echipelor albastre” și nevoia identificării de indicatori pentru prevenirea vulnerabilităților de tip zero-day. Un sistem tip honeypot reușește astfel să expună punctele slabe necunoscute dintr-o infrastructură cibernetică pentru echipele responsabile de remediere. Mai mult, informațiile obținute de un astfel de sistem pot fi cuantificate și utilizate în calcularea riscului de exploatare a diferitelor componente ale unei infrastructuri cibernetice.

2.3 Riscul contextual de exploatare a unei vulnerabilităţi cibernetice

Definirea riscului contextual de exploatare a vulnerabilităților cibernetice este încadrată în discuția mai largă despre diferența dintre abordarea proactivă și reactivă a securității cibernetice. Un studiu întreprins de FireEye arată faptul că aproape jumătate (42%) dintre exploatările vulnerabilităților cibernetice sunt realizate după eliberarea unei versiuni a software-ului țintă care tratează acea vulnerabilitate [62]. Acest lucru atestă faptul că un proces de prioritizare a vulnerabilităților cibernetice adecvat – care presupune calcularea riscului de exploatare- poate reduce semnificativ pierderile cauzate de atacuri cibernetice.

Procedurile de evaluare a riscului în securitatea cibernetică sunt metodologii de punctare a vulnerabilităților identificate într-o infrastructură informatică. Majoritatea procedurilor existente de evaluare a riscului utilizează un sistem standardizat de evaluare a vulnerabilităților comune denumit CVSS [63]. Acest sistem reprezintă rezultatul eforturilor de centralizare a tuturor vulnerabilităților cibernetice identificate și adnotarea acestora cu un scor de impact. Astfel, sistemele de monitorizare pentru amenințările cibernetice au ca funcție identificarea și cuantificarea riscului vulnerabilităților dintr-o infrastructură cibernetică pe baza sistemului standardizat CVSS.

Deși eficientă, abordarea bazată pe sistemul standardizat de tip CVSS ridică o problemă majoră în ceea ce privește asigurarea securității cibernetice. Această abordare bazată pe baze de date internaționale tinde să ignore contextul infrastructurii cibernetice. În acest sens, pot fi identificate abordări care propun includerea de parametrii adiționali care consideră aspecte contextuale ale infrastructurii cibernetice.

Mai departe, această secțiune descrie diferite abordări teoretice și empirice identificate în urma cercetării literaturii de specialitate care propun diferite metode de calcul al riscului de exploatare a vulnerabilităților cibernetice folosind informații adiționale față de sistemul CVSS. Astfel, sunt prezentate soluții precum cele descrise de Joh and Malaiya [64], Singh, et al. [65], Rapid7 [66] și Secureworks [67] care iau în considerare variabile interne infrastructurii cibernetice pentru calcularea riscului de exploatare a vulnerabilităților cibernetice. Reiese de aici prima tipologie de risc contextual definit în termeni de risc contextual organizațional, care permite prioritizarea vulnerabilităților prin raportare la importanța componentelor infrastructurii și probabilitatea de exploatare dată fiind susceptibilitatea acestora în fața atacurilor.

Pornind de la observațiile făcute de Chen, et al. [68], este propusă o a doua tipologie de risc contextual de exploatare a vulnerabilităților cibernetice care ia în considerare variabile din mediul extern infrastructurii cibernetice. Mediul extern al unei infrastructuri cibernetice este compus din mediul local și mediul global. Fiecare tip de mediu aduce cu sine un alt tip de risc de exploatare. Riscul local se referă la tendințele în materie de atacuri cibernetice care vizează cu precădere o infrastructură cibernetică specifică. În timp ce punctarea pe baza riscului contextual organizațional permite prioritizarea vulnerabilităților prin raportare la importanța componentelor și probabilitatea de exploatare dată fiind susceptibilitatea acestora în fața atacurilor, punctarea riscului local permite prioritizarea vulnerabilităților prin raportare la tipurile și țintele de atac preferate de actorii rău intenționați.

Spre deosebire de punctarea contextuală a riscului, punctarea locală folosește parametrii din mediul extern infrastructurii pentru a prioritiza vulnerabilitățile identificate. O astfel de abordare necesită simularea mediului ce se vrea a fi protejat și atragerea unor atacatori reali pentru a le înțelege strategiile și țintele de atac. Astfel, secțiunea dezvoltă pe larg aspectele teoretice ale unei abordări în acest sens bazată pe honeypot. Rezumând, abordarea contextuală proactivă în mitigarea riscului exploatării vulnerabilităților cibernetice ale unei infrastructuri informatice prin raportare la contextul organizațional poate fi îmbunătățită prin analiza tendințelor de atac din mediului extern local.

Mediul extern global al unei infrastructuri cibernetice prezintă aceleași caracteristici cu mediul local dar la o scală mai mare. Astfel, riscul asociat acestui mediu, riscul global, referă la tendințele în materie de atacuri cibernetice care vizează cu precădere o componentă comună din infrastructurile cibernetice. În alte cuvinte, riscul global presupune o cuantificare a popularității de exploatare a unui vulnerabilități la nivel global.

O alternativă pentru cuantificarea riscului contextual global de exploatare a vulnerabilităților cibernetice este utilizarea metodelor OSINT (Open-Source Intelligence). În acest sens, această secțiune documentează articole din literatură de specialitate precum cele redactate de Hayes and Cappa [69], Horawalavithana, et al. [70], Hobbs [71], Andrew, et al. [72], Rosa, et al. [73] și Day, et al. [74]. De asemenea, sunt descrise diferite implementări tehnice ale algoritmilor pentru prelucrarea datelor OSINT precum cele propuse de Chen, et al. [75], Mittal, et al. [76], Sabottke, et al. [77], Dionísio, et al. [78], Abdullah, et al. [79], Zhou, et al. [80], Liao, et al. [81], Husari, et al. [82], Tavabi, et al. [83] și Deliu, et al. [84].

3 Studii Empirice

În vederea dezvoltării sistemului propus în Figura 1 sunt vizate implementarea a trei module complementare. Este vorba în primul rând despre dezvoltarea unui sistem care să permită detecția timpurie a vulnerabilităților cibernetice din surse de date deschise („EVE”). În al doilea rând, este vorba despre un sistem care să permită optimizarea răspunsului la atacuri cibernetice prin intermediul unei arhitecturi de tip honeypot („HUNT”). În al treilea rând este vorba despre un sistem integrat de calcul al riscului cibernetic contextual pentru reducerea suprafeței de atac („CRS”).

Primul sistem este compus dintr-un model de prelucrare a limbajului natural care permite identificarea vulnerabilităților cibernetice din surse de date deschise precum site-uri Web și platforma Twitter. Acest sistem permite automatizarea procesului de identificare a unei strategii existente pentru exploatarea vulnerabilităților cibernetice și identificarea de vulnerabilități cibernetice noi. Astfel, pot fi identificate vulnerabilități cibernetice preferate de atacatori la nivel global.

Al doilea sistem este compus dintr-un agent de scanare al infrastructurii cibernetice și un model pentru dezvoltarea unei replici de tip honeypot a infrastructurii. Scopul acestui sistem vizează replicarea infrastructurii cibernetice în vederea expunerii acesteia la atacuri cibernetice și identificarea vulnerabilităților preferate de atacatori locali. În secțiunea dedicată acestui sistem, sunt prezentate eforturile de implementare ale agentului într-o infrastructură reală precum și eforturile de implementare ale unui sistem honeypot.

Ultimul sistem propus are drept elemente centrale o componentă pentru cartografierea infrastructurii cibernetice și o componentă pentru identificarea și evaluarea vulnerabilităților cibernetice. Împreună, cele două componente permit implementarea unui sistem de calcul al riscului contextual organizațional. În cadrul implementării acestui sistem într-o infrastructură cibernetică reală, a fost dezvoltată o metodologie de calculare a riscului contextual organizațional.

În rândurile ce urmează sunt prezentate pe rând eforturile celor trei studii empirice care au avut ca scop implementarea sistemelor prezentate mai sus.

3.1 Detecţia timpurie a vulnerabilităţilor din surse de date deschise („EVE”)

Sistemul modular de estimare a riscului contextual global presupune utilizarea de tehnici de procesare a limbajului natural prin tehnologii de tip învățare automată și prelucrare a limbajului natural în vederea identificării de vulnerabilități cibernetice din surse de date deschise. Caracterul inovativ al soluției propuse este dat de secvența de procesare a sistemului care fuzionează date din două surse de tip OSINT: postări din platforma Twitter și articole de specialitate.

Pentru dezvoltarea sistemului propus, au fost folosite o serie de seturi de date. Primul set de date folosit este reprezentat de un corpus de 1000 de articole de securitate cibernetică extrase în principal din The Hacker News și completate cu articole din Threat Post, Ars Technica și Security Affairs. Al doilea set de date este reprezentat de un total de 3100 de tweets din comunitățile Twitter, în care schimbul de cunoștințe despre noile vulnerabilități cibernetice este o practică obișnuită. Adițional a fost creat un nou set de date neetichetat prin extragerea automată din website-uri de specialitate. Noul corpus a fost extras din 20 de website-uri de specialitate și a conținut 65.8 milioane de token-uri și un vocabular de 63.000 de cuvinte. Ultimul set de date este reprezentat de evaluările de utilizabilitate aplicate asupra unui eșantion de convenienţă de 20 de indivizi.

Figura 2 prezintă o perspectivă de ansamblu asupra sistemului propus, dezvoltată în urma eforturilor prezentate în activitatea de laborator [85, 86]. Pentru componenta de analiză, predicție și clasificare a textului, au fost folosite o serie de abordări bazate pe tehnici de învățare automată și prelucrare a limbajului natural. Astfel, primele două seturi de date au fost folosite pentru implementarea modulelor de analiză a textului din articole de specialitate și postări Twitter. Mai departe, următorul set de date a fost folosit pentru implementarea unui model interpretabil de analiză, predicție și clasificare a datelor. În final, ultimul set de date a fost folosit pentru evaluarea interfeței cu utilizatorul a sistemului propus.

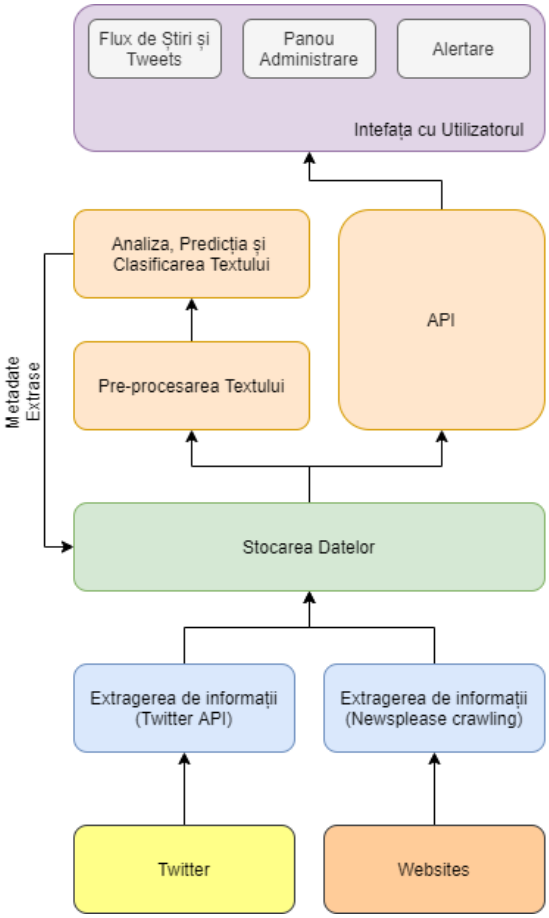

Figura 2. Arhitectura sistemului de identificare timpurie de vulnerabilități.

Rezultatele din Tabelul 1 arată că metoda de clasificare BERT are o performanță generală ușor mai bună în ceea ce privește precizia (85,50%) decât SVM, în timp ce MNB are o performanță considerabil mai scăzută.

Tabelul 1. Evaluarea alternativelor de implementare pentru modulul de analiză bazat pe știri.

Model	**Minim**	**Maxim**	**Medie**
SVM	**83.00**	87.00	85.05
MNB	72.50	81.50	76.60
BERT	82.50	**88.00**	**85.50**

În ceea ce privește algoritmul pentru detectarea vulnerabilităților cibernetice care folosește exclusiv date din platforme Web specializate în postarea știrilor din domeniul securității cibernetice, prototipul propus obține o acuratețe medie de 85.5%. Rezultatele obținute în cazul altor soluții similare variază între 90% și 95% [80-82]. Totuși, în Tabelul 2 este demonstrat că atunci când sunt considerate articole de specialitate conținute în postările din platforma Twitter, dar și a anumitor metrici precum numărul de aprecieri și distribuiri, este obținută o acuratețe aproximativ egală cu cea mai performantă identificată în literatura de specialitate

Tabelul 2. Evaluarea alternativelor de implementare pentru modulul bazat pe știri din postări Twitter.

Model	**Acuratețe (text articole)**	**Acuratețe (text +tweet-uri +retweet-uri)**
BERT	93.33%	93.97%
SVM	90.96%	90.97%
CNN	**93.97%**	**94.96%**

Rezultatele din Tabelul 3 prezintă performanțele obținute de modelele instruite doar pe textele de tweet utilizate; ca atare, textul disponibil a fost redus la o lungime maximă de 144 de caractere. Și aici, modelul BERT are performanțe mai bune decât celelalte cu o precizie de 92,31%, depășind modelul CNN cu aproximativ 1%.

Tabelul 3. Evaluarea alternativelor de implementare pentru modulul bazat pe postări Twitter

Model	**Acuratețe (text articole)**	**Acuratețe (text +tweet-uri +retweet-urii)**
BERT	**91.91%**	**92.39%**
SVM	75.90%	76.06%
CNN	90.80%	91.28%

În cea ce privește algoritmul pentru detectarea vulnerabilităților cibernetice care folosește exclusiv date din platforma Twitter, prototipul propus obține o acuratețe de 92.39%. Aceste rezultate depășesc standardul algoritmilor existenți identificați a căror acuratețe variază între 45% și 92% [75-78].

În Tabelul 4, pot fi observate rezultatele diferitelor alternative de implementare desfășurate pentru dezvoltarea unui model interpretabil. Primul model (MNB) a oferit o punct de

referință pentru a compara rezultatele, acesta fiind un model interpretabil. Următoarele modele au presupus fie utilizarea exclusivă a setului de date agregat cules în mod automat, fie ajustat prin intermediul setului de date cu articole adnotate. Al treilea model a presupus adăugarea unei componente de interpretabilitate care permite explicarea rezultatelor de clasificare prin intermediul de prototipuri (articole exemplare pentru clasele de text).

Tabelul 4. Performanța modelelor interpretabile.

Model	Acuratețe	Precizie	Recall	Scor F2	Interpretabil
MNB	0.84	**0.92**	0.62	0.66	Da
Longformer (fără ajustare)	**0.87**	0.76	0.95	0.90	Nu
Longformer (ajustat)	0.86	0.73	**0.98**	**0.92**	Nu
Longformer + ProSeNet	**0.87**	0.78	0.91	0.88	Da

Adițional, a fost desfășurată o analiză de utilizabilitate a interfeței grafice a sistemului. Contribuția originală în acest sens se referă la utilizarea machetei interfeței grafice ca obiect de evaluare, în vederea obținerii de feedback timpuriu. Conform metodei de evaluare propuse, interfața grafică ar putea fi etichetată ca fiind oricare dintre următoarele: superfluă, neutră, prea orientată spre sarcini, prea auto-orientată, orientată spre sarcini sau dorită. Conform metodei de evaluare AttrackDiff, macheta poate fi etichetată ca fiind orientată spre sarcini. Mai mult, metoda de evaluare a utilizabilității a permis identificare oportunităților de îmbunătățire a interfeței cu utilizatorul. În figura de mai jos, este prezentat un exemplu de ecran din cadrul interfeței grafice.

Figura 3. Exemplu ecran din interfața grafică a sistemului de estimare a riscului contextual global

3.2 Optimizarea răspunsului la atacuri cibernetice folosind sisteme de tip honeypot („HUNT”)

Această secțiune prezintă implementarea unui sistem care să permită calcularea riscului contextual local de exploatare a unei vulnerabilități cibernetice. Abordarea propusă vizează realizarea unei arhitecturi de tip agent și realizarea unui arhitecturi de tip honeypot capabilă să simuleze un mediu virtual, să distragă atacatorii acelui mediu virtual precum și să colecteze informații referitoare la mijloacele de atac folosite.

Primul set de date folosit pentru evaluarea implementării conține informații colectate prin intermediul agentului de scanare dezvoltat din cadrul unei infrastructuri care cuprinde 12 dispozitive. Pentru fiecare dispozitiv, agentul de scanare a putut obține informații referitoare la numele aplicațiilor, descrierea acestora, numerele de identificare, data de instalare, limba, pachet local, tipul de cod, furnizorul componentei, versiunea componentei și alte detalii precum porturile conectate. Dintre acestea, evaluarea a fost realizată prin raportare la numele componentei, versiunea acesteia, descrierea componentei precum și portul asociat pentru un dispozitiv. Alegerea acestor dimensiuni a fost făcută prin raportare la standardul minim de informații necesare pentru inferarea vulnerabilităților cibernetice din infrastructură.

Al doilea set de date este reprezentat de răspunsurile unei componente de tip ALB („application load balancer”) în fața unor mecanisme de scanare precum Nikto, Nmap și DIRB. Un total de 317.709 de pachete au fost trimise către componenta ALB pentru a identifica eficiența acesteia în redirecționarea traficului suspicios către sistemul honeypot dezvoltat. Astfel, au fost raportate detectarea pozitivă sau negativă a traficului suspicios alături de numărul de pachete pentru fiecare mecanism.

Al treilea set de date este obținut în urma realizării unui experiment în care a fost evaluată performanța sistemului honeypot. Datele obținute se referă la numărul de pachete trimise în decurs de 24 de ore de atacatori cibernetici, un identificator unic pentru atacatori, țara de origine a atacului și nivelul de vulnerabilizare a sistemului atins de atacatori în honeypot. Adițional, aceste rezultate au fost comparate cu rezultatele unui sistem honeypot de tip tradițional dezvoltat în vederea obținerii unui punct de referință.

Așa cum se poate observa în Figura 4, sistemul este compus dintr-un balansor care direcționează traficul suspect către sistemul honeypot, un sistem honeypot care simulează

infrastructura cibernetică reală printr-un sistem de tip „capture the flag” pe patru niveluri, și un agent de camuflare care acționează pentru culegerea datelor referitoare la caracteristicile infrastructurii cibernetice. Propunerea unei astfel de arhitecturi este justificată de activitățile de cercetare din laborator [87, 88].

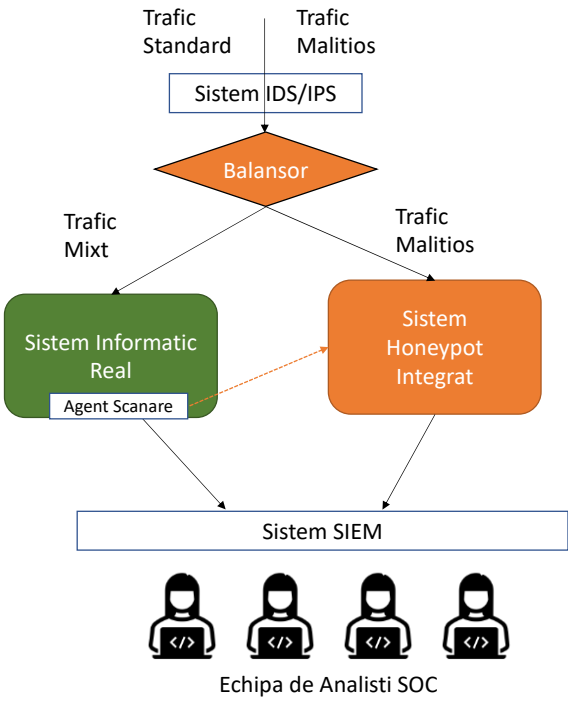

Figura 4. Arhitectura sistemului de tip honeypot HUNT integrat prin balansor

Pentru evaluarea sistemului propus, sunt analizate pe rând rezultatele aplicării agentului asupra unei infrastructuri cibernetice reale, rezultatele load balancer în cazul unui sistem de tip honeypot implementat asupra unui site Web și rezultatele honeypot într-un interval de 24 de ore în fața atacatorilor cibernetici.

În urma implementării agentului în cadrul unei infrastructuri cibernetice au fost obținute o serie de date precum: date referitoare la aplicații, date referitoare la drivere, date referitoare la firewall, date referitoare la componentele hardware, date referitoare la caracteristicile instalate, date referitoare la procese, date referitoare la utilizatori, date referitoare la rețea, date referitoare la sistemul de operare, date referitoare la pachete și altele. Tabelul 5 prezintă un eșantion de date extras din cadrul unui singur dispozitiv al unei infrastructuri. Datele precum cele din Tabelul 5 pot fi folosite pentru a crea un sistem honeypot care să simuleze infrastructura ce se dorește a fi protejată. Agentul dezvoltat se pliază atât pentru

implementarea ulterioară a sistemului honeypot cât și pentru obținerea de informații adiționale pentru sistemul de analiză al infrastructurii cibernetice. În acest sens, agentul poate oferi informații adiționale pentru calcularea riscului contextual organizațional.

Tabelul 5. Eșantion date colectate de agent.

Aplicație	Versiune	Descriere	Port
Microsoft Windows Operating System	10.0.17763.1	Distributed File System Replication	49913
Microsoft Windows Operating System	10.0.17763.719	Domain Name System (DNS) Server	49700
Microsoft Windows Operating System	10.0.17763.1	Spooler SubSystem App	49677
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	49675
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	49674
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	49668
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	49667
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	49666
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	49665
Microsoft (R) Windows (R) Operating System	10.0.17763.1	Microsoft.ActiveDirectory.WebServices	9389
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	3389
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	3269
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	3268
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	636
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	593
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	464
Apache HTTP Server	2.4.47	Apache HTTP Server	443
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	389
Microsoft Windows Operating System	10.0.17763.1	Host Process for Windows Services	135
Microsoft Windows Operating System	10.0.17763.1	Local Security Authority Process	88
Apache HTTP Server	2.4.47	Apache HTTP Server	80
Microsoft Windows Operating System	10.0.17763.719	Domain Name System (DNS) Server	53

Mai departe, sunt rezumate rezultatele aplicării direcționării de trafic suspect prin intermediul Nikto, Nmap și DIRB către componenta load balancer. Așa cum se poate observa în Tabelul 6, au fost măsurați indicatori ce țin de numărul de pachete trimise, dimensiunea traficului generat, numărul de răspunsuri ce au întors eroarea 404, precum și detectarea traficului suspicios la nivel de porturi de către load balancer.

Tabelul 6. Trafic redirecționat către honeypot de către componenta Load Balancer.

Mecanism	**Nr. pachete trimise**	**Nr. răspunsuri 404**	**Detectare la nivel de port**	**Redirecționat către honeypot**
Nikto (123)	2340	978	Negativ	Pozitiv
Nikto (ade)	2123	900	Negativ	Pozitiv
Nikto (4890)	2000	874	Negativ	Pozitiv
Nikto (567)	1988	850	Negativ	Pozitiv
Nmap (TCP)	1005	-	Pozitiv	Pozitiv
Nmap (Stealth)	1004	-	Pozitiv	Pozitiv
Nmap (Fin)	1009	-	Pozitiv	Pozitiv
Nmap (Null)	1007	-	Pozitiv	Pozitiv
Nmap (UDP)	1008	-	Pozitiv	Pozitiv
Nmap (UDP)	1006	-	Pozitiv	Pozitiv
Nmap (X-mas)	1004	-	Pozitiv	Pozitiv
DIRB (imp)	120321	60594	Pozitiv	Pozitiv
DIRB (nerec)	50344	12456	Negativ	Pozitiv
DIRB (404)	120321	60594	Pozitiv	Pozitiv
DIRB (IM)	11229	56789	Pozitiv	Pozitiv
Total	317,709	142,924	N/A	N/A

În final, sunt prezentate rezultatele obținute de sistemul honeypot dezvoltat pentru același Website. Așa cum se poate observa în Tabelul 7, sunt ilustrate informații despre atacatori și nivelul de vulnerabilizare atins al sistemului honeypot. Prin comparație cu un sistem honeypot tradițional, sistemul dezvoltat este de 4.4 ori mai performant.

Tabelul 7. Statistici atacatori sistem Hunt măsurat pe durata a 24h.

Id Atacator	**Nr Pachete Trimise**	**IP Atacator**	**Tara Atacator**	**Nivel Atins**
THA1	73,492	121.235.179.x	China	L2
THA2	45,334	195.82.150.x	Ucraina	L2
THA3	39,975	159.75.52.x	China	L2
THA4	25,648	109.195.179.x	Rusia	L1
THA5	16,811	35.232.230.x	USA	N/A
THA6	16,654	161.35.59.x	USA	L1
THA7	13,543	221.158.220.x	Korea de Nord	N/A
THA8	11,582	213.142.159.x	Turcia	L1
THA9	10,902	89.216.121.x	Serbia	L1
THA10	7,503	49.85.59.x	China	L1
THA11	7,326	178.63.41.x	Germania	N/A
THA12	7,219	77.47.247.	Ucraina	N/A
THA13	5,998	178.172.137.x	Belarus	N/A
THA14	5,863	124.244.3.x	Hong Kong	N/A
THA15	5,694	94.103.91.x	Rusia	N/A
THA16	5,869	185.156.43.x	Ucraina	L3
THA17	5,728	52.42.115.x	USA	N/A
THA18	4,619	201.163.247.x	Mexic	N/A
THA19	2,802	15.229.2.x	Brazilia	N/A
THA20	2,661	89.137.217.x	Romania	N/A
THA21	2,487	175.24.114.x	China	N/A

Aceste rezultate confirmă dezvoltarea componentelor necesare implementării unui sistem de tip honeypot ca parte constituentă a unui sistem pentru reducerea riscului exploatării vulnerabilităților cibernetice ale unei infrastructuri informatice. Spre deosebire de soluții similare pentru scanare pe bază de agent [53-61], sistemul propus se distinge prin capacitatea superioară de reproducere a infrastructurii vizate, dată de plauzibilitatea replicării elementelor pe baza datelor colectate de agent.

3.3 Sistem integrat de calcul al riscului contextual pentru reducerea suprafeței de atac („CRS”)

În vederea implementării unui sistem pentru calcularea riscului contextual organizațional de exploatare a vulnerabilităților cibernetice dintr-o infrastructură informatică sunt vizate dezvoltarea unei componente de monitorizare continuă a unei infrastructuri cibernetice și dezvoltarea unei metodologii pentru calcularea scorului contextual al vulnerabilităților identificate. Această alegere a fost motivată în urma cercetărilor de laborator [89, 90]

Pentru dezvoltarea componente de monitorizare continuă au fost implementate mijloace de scanare externă (ex: Nmap) și internă (bazate pe o mașină virtuală instalată în infrastructura țintă). Pentru dezvoltarea metodologiei a fost utilizat un set de date obținut în urma desfășurării unor procese de scanare internă și externă asupra unei infrastructuri cibernetice reale. Setul de date obținut conține 133 de intrări care reprezintă dispozitive identificate prin mijloacele de scanare. Pentru fiecare dispozitiv, au fost colectate o serie de caracteristici precum: numele produsului, versiunea, numărul de identificare cpe, tipul de sistem de operare, port, protocol de transport și url. De asemenea, pentru identificarea vulnerabilităților cibernetice au fost folosite sistemele internaționale de indexare vulnerabilitați CVE și CVSS. În total, au fost identificate 63 de vulnerabilități cibernetice prezente în sistemul analizat.

Adițional, au fost colectate date cu referire la impactul fiecărei componente asupra infrastructurii cibernetice. Aceste date au fost introduse de administratorul infrastructurii cibernetice prin intermediul unei interfețe vizuale dezvoltată special în acest sens. Mai mult, au fost inferate o serie de informații despre gradul de expunere al dispozitivelor prin raportare la informațiile obținute prin intermediul scanării interne și externe. Detalii despre metodologia folosită pentru inferarea acestor date sunt prezentate într-o secțiune ulterioară. Figura 5 prezintă arhitectura sistemului.

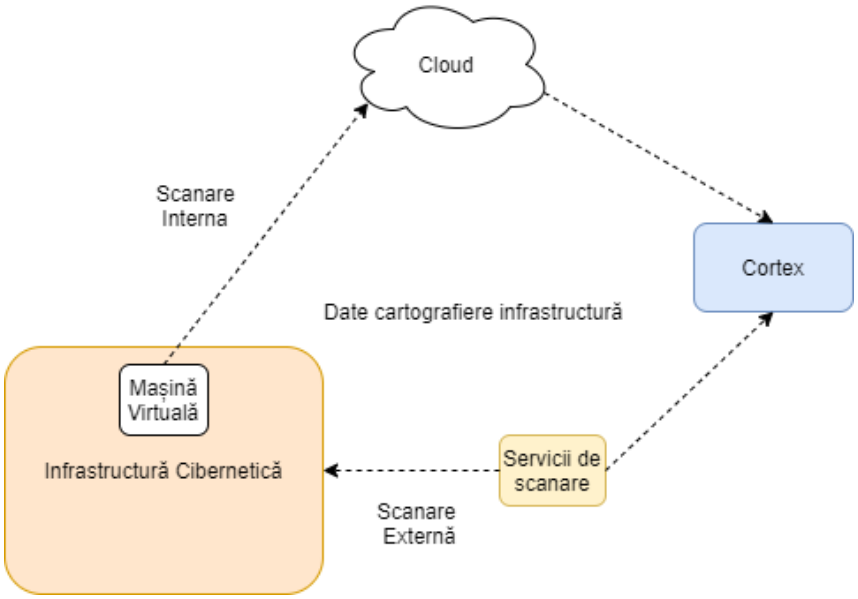

Figura 5. Arhitectura sistemului de analiză a infrastructurii cibernetice.

Mijloacele de scanare externă și internă permit colectarea datelor referitoare la infrastructura cibernetică și identificarea vulnerabilităților cibernetice. Componenta „Cortex" permite utilizarea datelor extrase pentru calcularea scorului de risc contextual organizațional. În acest scop, au fost implementată o procedură de evaluare a riscului individual al fiecărui dispozitiv prin raportare la sistemul CVSS. După aplicarea procedurii de notare a riscului individual, sistemul calculează scorul de risc contextual al fiecărui dispozitiv. Scorul de risc contextual al unui dispozitiv este compus din gradul de expunere al dispozitivului prin raportare la ușurința de accesare din internet (ZE), probabilitatea de exploatare dată fiind existența unei strategii făcute publice (ES) și gradul de expunere al dispozitivului la tipul de utilizatori umani sau computaționali care accesează sistemul (UE). În formula de mai jos sunt reprezentate cele trei elemente (ZE, ES,UE) și ponderile asociate (PZ,PE,PU).

$$CRS = PZ * ZE + PE * ES + PU * UE$$

Această formulă permite cuantificarea riscului contextual organizațional prin raportare la susceptibilitatea componentelor la atacuri cibernetice. Ponderile asociate sunt prezentate în Tabelul 8 și au fost atribuite printr-o decizie bazată pe consensul experților în securitate cibernetică implicați în proiect.

Tabelul 8. Punctarea contextului dispozitivelor.

ZE		UE	
Tip context ZE	Scor	Tip context UE	Scor
Internet	100	Servere & Utilizatori	100
WAN	60	Doar Utilizatori	60
Utilizatori izolați	40	Doar Servere	40
Servere izolate	20	Fără acces	0
Offline	0		

Mai departe, a fost dezvoltată o formulă care să considere de asemenea importanța dispozitivelor pentru procesele organizaționale prin raportare la datele oferite de administratorul de rețea. Astfel, formula finală ia în considerare scorul de risc individual bazat pe CVSS, scorul de risc contextual descris mai sus (CRS) și impactul pe care exploatarea dispozitivului l-ar avea supra afacerii (BI). În formula de mai jos, sunt prezentate cele trei elemente (CVSS, BI și CRS) alături de ponderile aferente (PC, PB și PS), a căror valoare este determinată empiric.

$$ORS = PC * CVSS + PB * BI + PS * CRS$$

Tabelul 9 prezintă un eșantion al rezultatelor obținute prin aplicarea formulelor de calcul a riscului contextual. Datele referitoare la IP și DNS au fost anonimizate. De asemenea, în tabel sunt incluse scorurile pentru elementele constituente ale fiecărei formule. Pentru exemplu de mai jos, au fost folosite ponderile PZ (0.3), PE (0.5) și PU (0.2) dar și PC (0.5), PB (0.25), și PS (0.25).

Tabelul 9. Rezultatele aplicării formulei de calculare a riscului contextual al organizației asupra unui eșantion cu vulnerabilități cibernetice identificate.

CVE	IP/DNS	CVSS	ZE	UE	ES	CRS	BI	ORS
CVE-2018-20148	Anonymized	98	100	100	100	100	55	87.75
CVE-2017-14723	Anonymized	98	100	100	100	100	55	87.75
CVE-2017-16510	Anonymized	98	100	100	100	100	55	87.75
CVE-2020-11984	Anonymized	98	100	100	100	100	55	87.75
CVE-2019-0398	Anonymized	88	100	100	50	75	100	87.75
CVE-2015-4603	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4073	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-6834	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4072	Anonymized	98	100	100	100	100	50	86.5

CVE-2015-6835	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4599	Anonymized	98	100	100	100	100	50	86.5
CVE-2014-9912	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4600	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4602	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4071	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4603	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4073	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-6834	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4072	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4599	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4600	Anonymized	98	100	100	100	100	50	86.5
CVE-2015-4602	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4071	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-7127	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-6288	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-6290	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-5771	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-2554	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-4538	Anonymized	98	100	100	100	100	50	86.5
CVE-2016-9137	Anonymized	98	100	100	100	100	50	86.5
CVE-2019-9641	Anonymized	98	100	100	100	100	50	86.5

Așa cum se poate observa, formula de calcul a riscului contextual (CRS) permite diferențierea unui CVE ca fiind mai puțin urgent, din punct de vedere contextual, acest lucru fiind transpus apoi în formula finală de calcul a riscului de exploatare. De asemenea, se poate observa că, formula de calcul a riscului de exploatare contextual organizațional (ORS) permite o mai bună prioritizare a vulnerabilităților cibernetice identificate în infrastructura cibernetică decât scorul CVSS.

Studiul empiric descris în această secțiune aduce în plus, față de ale soluții similare precum Nextpose [66] sau metodele propuse de Joh and Malaiya [64] și Singh, et al. [65] prezentate în secțiunea dedicată din Capitolul 2.1, o prioritizare bazată pe factori adiționali celor din bazele de date internaționale precum CVSS. Este vorba în primul rând de introducerea unui parametru care indică importanța dispozitivului pentru desfășurarea activității organizației deci, și importanța de remediere a vulnerabilităților identificate pe acest dispozitiv. De asemenea, este vorba despre inferarea anumitor parametrii din datele obținute prin intermediul scanării din exteriorul și interiorul rețelei.

4 Discuție

Această secțiune discută oportunitățile de integrare ale celor trei sisteme dezvoltate prin intermediul studiilor empirice prezentate. Sistemele EVE (3.1) si CRS (3.3) au ca scop îmbunătățirea formulei de calcul a riscului contextual prin luarea în calcul a parametrilor externi. Sistemul de identificare timpurie a vulnerabilităților de securitate cibernetică oferă posibilitatea de îmbunătățire a formulei de calcul a riscului contextual organizațional de exploatare a unei vulnerabilități. De exemplu, parametrul exploit score (ES) presupune identificarea existenței unui mijloc de exploatare a vulnerabilităților cibernetice. Prin identificarea timpurie a vulnerabilităților cibernetice poate fi identificată existența unei strategii de exploatare dată fiind menționarea vulnerabilității în comunității online. Mai mult, scorul aferent poate în acest fel să obțină valori cuprinse între 1 și 100, nefiind limitat doar la existența sau lipsa de existență a cunoașterii responsabililor de sistem referitor la strategiile de exploatare a vulnerabilităților cibernetice.

O integrare între sistemele Hunt (3.2) si EVE (3.1) poate fi proiectată în mod bidirecțional, așa încât componenta de Honeypot să transmită modulului de identificare timpurie noi vectori de atac necunoscuți până atunci, iar componenta de identificare timpurie a vulnerabilităților noi să transmită modulului CTF din Hunt noi vulnerabilității emergente, pe care acesta să le integreze în fluxul de profilare al atacatorilor. În aceiași maniera, putem considera oportună integrarea între Hunt (3.2) si CRS (3.3), caz în care sistemul de calcul al riscului contextual poate furniza componentei CTF din Hunt lista vulnerabilităților celor mai importante sisteme pentru a le expune spre exploatare, si a profila atacatorii care sunt capabili să le exploateze. Totodată subliniez importanta transferului de date intre sistemele EVE (3.1), Hunt (3.2) si CRS (3.3) către sistemele de tip SIEM /SOAR utilizate in cadrul activităților de zi cu zi ale echipelor SecOps pentru analiza si răspuns la incidente de securitate.

Nu în ultimul rând, identificarea de noi tipuri de parametrii interni și externi poate duce la identificare de noi abordări în vederea integrării celor trei sisteme. În concluzie, această teză prezintă studiile realizate pentru reducerea suprafeței de atac si optimizarea răspunsului la incidente de securitate cibernetică în infrastructuri complexe pentru echipele din centrele de securitate operațională (SOC), dar și oportunitățile de integrare între componentele descrise mai sus.

5 Concluzii și dezvoltări ulterioare

Această teză prezintă eforturile de cercetare pe care le-am depus în vederea dezvoltării componentelor unui sistem integrat pentru eficientizarea proceselor centrelor de securitate operaționale (SOC) prin reducerea suprafeței de atac si optimizarea răspunsului la incidente în infrastructuri IT complexe. Un astfel de sistem răspunde la problemele de scalare a echipelor de securitate operaționala (SecOps), caracterizate de viteză și de o complexitate exponențiale și care aduc cu sine o expunere amplificată în fața riscurilor cibernetice. În acest sens, soluțiile inovative propuse in cadrul celor 3 studii oferă metode de identificare timpurie a noilor vulnerabilități, de optimizare a răspunsului la atacuri cibernetice folosind sisteme de tip honeypot moderne, precum si de prioritizare a vulnerabilităților cibernetice cunoscute pentru reducerea suprafeței de atac. Rezultatele obținute în cadrul studiilor promit să eficientizeze activitatea centrelor de securitate operațională. Mai mult, dezvoltările ulterioare vizează îmbunătățirea performanței sistemelor propuse și integrarea acestora într-un sistem unitar.

5.1 Contribuții Originale

În ceea ce privește contribuțiile originale prezentate în teza de față, sunt enumerate:

- CO1: Proiectarea, dezvoltarea și testarea a două modele automate de prelucrare a limbajului natural pentru identificarea timpurie a vulnerabilităților cibernetice folosind surse de date deschise.
- CO2. Dezvoltarea și testarea unui model automat interpretabil de prelucrare a limbajului natural pentru explicarea rezultatelor obținute.
- CO3: Conceperea și aplicarea unei metodologii inovative pentru evaluarea utilizabilității interfețelor grafice ale aplicațiilor web de securitate cibernetică.
- CO4: Proiectarea, dezvoltarea si testarea unui sistem informatic de tip honeypot cu capacitate de camuflare în infrastructura reala a unei organizații.
- CO5: Proiectarea, implementarea și testarea impactului unei metode de profilare a atacatorilor în sisteme de tip honeypot folosind teoria jocurilor.
- CO6: Proiectarea si testarea unei metode si a unui algoritm care să permită cuantificarea riscului contextual de exploatare a vulnerabilităților cibernetice din cadrul unei infrastructuri informatice complexe bazată pe meta-date externe si interne.

5.2 Lista publicațiilor

Grigorescu, O., **Săndescu, C**., & Rughiniș, R. (2016, September). CODA footprint continuous security management platform. In *2016 15th RoEduNet Conference: Networking in Education and Research* (pp. 1-5). Bucharest:IEEE.

Săndescu, C., Rughinis, R., & Grigorescu, O. (2017). Hunt: Using honeytokens to understand and influence the execution of an attack. In *The International Scientific Conference eLearning and Software for Education* (Vol. 1, p. 511). Bucharest:" Carol I" National Defence University.

Iorga, D., Corlătescu, D., Grigorescu, O., **Săndescu, C**., Dascălu, M., & Rughiniș, R. (2020, December). Early Detection of Vulnerabilities from News Websites using Machine Learning Models. In *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). Bucharest:IEEE.

Radu, R., **Săndescu, C.**, Grigorescu, O., & Rughiniș, R. (2020, December). Analyzing Risk Evaluation Frameworks and Risk Assessment Methods. In *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). IEEE.

Grigorescu, O., **Săndescu, C**., & Caba, A. (2020, December). Web Application Honeypot Published in the Wild. In *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). Bucharest:IEEE.

Iorga, D., Corlatescu, D. G., Grigorescu, O., **Săndescu, C**., Dascalu, M., & Rughinis, R. (2021, May). Yggdrasil—Early Detection of Cybernetic Vulnerabilities from Twitter. In *2021 23rd International Conference on Control Systems and Computer Science (CSCS)* (pp. 463-468). Bucharest:IEEE.

Frode de la Foret, P., Ruseti, S., **Săndescu**, C., Dascalu, M., & Travadel, S. (2021). Interpretable Identification of Cybersecurity Vulnerabilities from News Articles. In Int. Conf. on Recent Advances in Natural Language Processing (RANLP 2021) (pp. 428-436). Varna, Bulgaria (Online): ACL.

Iorga, D., Grigorescu, O., Predoiu, M., **Săndescu**, C., Dascalu, M., & Rughinis, R. (2021). Early Usability Evaluation to Enhance User Interfaces – A Use Case on the Yggdrasil

Cybersecurity Mockup –. In International Conference on Human-Computer Interaction (RoCHI2021). (pp.103-111) Bucharest, Romania (Online): MatrixRom.

Săndescu C., Dinișor A., Vlădescu C-V, Grigorescu O., Corlătescu D., Dascălu M., Rughiniș R. (in press) Extracting Exploits and Attack Vectors from cybersecurity news using NLP. In *Buletin Ştiinţific Universitatea Politehnica din Bucureşti*

Babalau I, Corlatescu D.,Grigorescu O., **Săndescu C**., Dascălui, M. (in press) Severity Prediction of Software Vulnerabilities based on their Text Description In 2021 International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2021), Timișoara, România (Online)

Vlădescu C., Dinișor M-A, Grigorescu O., Corlătescu D., **Săndescu C**., Dascălu M. (in press) What are the Latest Cybersecurity Trends? A Case Study Grounded in Language Models In 2021 International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2021), Timișoara, România (Online)

6 Referințe

[1] J. Armin, B. Thompson, D. Ariu, G. Giacinto, F. Roli, and P. Kijewski, "2020 cybercrime economic costs: No measure no solution," in *2015 10th International Conference on Availability, Reliability and Security*, Toulouse, 2015, pp. 701-710.

[2] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, vol. 2, pp. 121-135, 2016.

[3] Ponemon IBM, "*Cost of Data Breach Report 2021*", 2021. [Online]. Available: https://www.ibm.com/security/data-breach [Accessed: February, 2022]

[4] The International Information System Security Certification Consortium, "*A Resilient Cybersecurity Profession Charts the Path Forward*", 2021. [Online]. Available: https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx [Accessed: February, 2022]

[5] Trend Micro, "*Attacks Surge in 1H 2021 as Trend Micro Blocks 41 Billion Cyber Threats*", 2021. [Online]. Available: https://newsroom.trendmicro.com/2021-09-14-Attacks-Surge-in-1H-2021-as-Trend-Micro-Blocks-41-Billion-Cyber-Threats [Accessed: February, 2022]

[6] Spacy, "*Language Processing Pipelines*", n.d. [Online]. Available: https://spacy.io/usage/processing-pipelines. [Accessed: September 2021]

[7] D. Jurafsky and J. Martin, "*Speech and Language Processing* ", 2020. [Online]. Available: https://web.stanford.edu/~jurafsky/slp3/. [Accessed: June 2020]

[8] G. Pulford, "The Viterbi algorithm," in *IEEE Seminar on Target Tracking: Algorithms and Applications*, Enschede, 2006, pp. 53-65.

[9] V. Nair and G. E. Hinton, "Rectified linear units improve restricted boltzmann machines," in *Proceedings of the 27 th International Conference on Machine Learning*, Haifa, 2010.

[10] G. Bouchard, "Efficient bounds for the softmax function, applications to inference in hybrid models," in *Presentation at the Workshop for Approximate Bayesian Inference in Continuous/Hybrid Systems at NIPS-07*, Hilton, 2007.

[11] J. Shore and R. Johnson, "Axiomatic derivation of the principle of maximum entropy and the principle of minimum cross-entropy," *IEEE Transactions on information theory*, vol. 26, pp. 26-37, 1980.

[12] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.

[13] Y. Gal and Z. Ghahramani, "A theoretically grounded application of dropout in recurrent neural networks," *Advances in neural information processing systems*, vol. 29, pp. 1019-1027, 2016.

[14] M. Honnibal and M. Johnson, "An improved non-monotonic transition system for dependency parsing," in *Proceedings of the 2015 conference on empirical methods in natural language processing*, Lisabon, 2015, pp. 1373-1378.

[15] H. Zhang, "The Optimality of Naive Bayes," presented at the FLAIRS2004 Conference, Canada, 2004.

[16] J. D. Rennie, L. Shih, J. Teevan, and D. R. Karger, "Tackling the poor assumptions of naive bayes text classifiers," in *Proceedings of the 20th international conference on machine learning (ICML-03)*, Washington, 2003, pp. 616-623.

[17] A. McCallum and K. Nigam, "A comparison of event models for naive bayes text classification," in *AAAI-98 workshop on learning for text categorization*, Madison, 1998, pp. 41-48.

[18] V. Vryniotis, "*Machine Learning Blog & Software Development News*", 2013. [Online]. Available: https://blog.datumbox.com/machine-learning-tutorial-the-max-entropy-text-classifier/. [Accessed: June 2021]
[19] K. Nigam, J. Lafferty, and A. McCallum, "Using maximum entropy for text classification," in *IJCAI-99 workshop on machine learning for information filtering*, 1999, pp. 61-67.
[20] C. Cortes and V. Vapnik, "Support-vector networks," *Machine learning,* vol. 20, pp. 273-297, 1995.
[21] J. Platt, "Probabilistic outputs for support vector machines and comparisons to regularized likelihood methods," *Advances in large margin classifiers,* vol. 10, pp. 61-74, 1999.
[22] T.-F. Wu, C.-J. Lin, and R. C. Weng, "Probability estimates for multi-class classification by pairwise coupling," *Journal of Machine Learning Research,* vol. 5, pp. 975-1005, 2004.
[23] K. Crammer and Y. Singer, "On the algorithmic implementation of multiclass kernel-based vector machines," *Journal of machine learning research,* vol. 2, pp. 265-292, 2001.
[24] F. Mola, "Classification and regression trees software and new developments," in *Advances in Data Science and Classification*, ed Rome: Springer, 1998, pp. 311-318.
[25] J. R. Quinlan, *C4. 5: programs for machine learning*. California: Elsevier, 2014.
[26] L. Breiman, "Random forests," *Machine learning,* vol. 45, pp. 5-32, 2001.
[27] S. T. Dumais, "Latent semantic analysis," *Annual review of information science and technology,* vol. 38, pp. 188-230, 2004.
[28] T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient estimation of word representations in vector space," *arXiv preprint arXiv:1301.3781*, 2013.
[29] J. Pennington, R. Socher, and C. D. Manning, "Glove: Global vectors for word representation," in *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)*, 2014, pp. 1532-1543.
[30] T. K. Landauer, P. W. Foltz, and D. Laham, "An introduction to latent semantic analysis," *Discourse processes,* vol. 25, pp. 259-284, 1998.
[31] A. Zhila, W.-t. Yih, C. Meek, G. Zweig, and T. Mikolov, "Combining heterogeneous models for measuring relational similarity," in *Proceedings of the 2013 conference of the North American chapter of the association for computational linguistics: Human language technologies*, Atlanta, 2013, pp. 1000-1009.
[32] DeepLizard, "*Machine Learning & Deep Learning Fundamentals*", n.d. [Online]. Available: https://deeplizard.com/learn/video/gZmobeGL0Yg. [Accessed: July 2021]
[33] G. Ognjanovski, "*Everything you need to know about Neural Networks and Backpropagation — Machine Learning Easy and Fun*", 2019. [Online]. Available: https://towardsdatascience.com/everything-you-need-to-know-about-neural-networks-and-backpropagation-machine-learning-made-easy-e5285bc2be3a. [Accessed: July 2019]
[34] S. Ruder, "*An overview of gradient descent optimization algorithms*", 2016. [Online]. Available: https://ruder.io/optimizing-gradient-descent/. [Accessed: July 2021]
[35] J. Brownlee, "*Understand the Impact of Learning Rate on Neural Network Performance*", 2020. [Online]. Available:

https://machinelearningmastery.com/understand-the-dynamics-of-learning-rate-on-deep-learning-neural-networks/. [Accessed: July 2021]
[36] A. Senior, G. Heigold, M. a. Ranzato, and K. Yang, "An empirical study of learning rates in deep neural networks for speech recognition," in *2013 IEEE international conference on acoustics, speech and signal processing*, Vancouver, 2013, pp. 6724-6728.
[37] S. Sumit, "*A Comprehensive Guide to Convolutional Neural Networks—the ELI5 way*", 2018. [Online]. Available: https://towardsdatascience.com/a-comprehensive-guide-to-convolutional-neural-networks-the-eli5-way-3bd2b1164a53. [Accessed: July 2021]
[38] A. Jacovi, O. S. Shalom, and Y. Goldberg, "Understanding convolutional neural networks for text classification," *arXiv preprint arXiv:1809.08037*, 2018.
[39] X. Zhang, J. Zhao, and Y. LeCun, "Character-level convolutional networks for text classification," *Advances in neural information processing systems*, vol. 28, pp. 649-657, 2015.
[40] W. De Mulder, S. Bethard, and M.-F. Moens, "A survey on the application of recurrent neural networks to statistical language modeling," *Computer Speech & Language*, vol. 30, pp. 61-98, 2015.
[41] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, pp. 1735-1780, 1997.
[42] A. Sherstinsky, "Fundamentals of recurrent neural network (RNN) and long short-term memory (LSTM) network," *Physica D: Nonlinear Phenomena*, vol. 404, p. 132306, 2020.
[43] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," *arXiv preprint arXiv:1409.0473*, 2014.
[44] Y. Su and C.-C. J. Kuo, "On extended long short-term memory and dependent bidirectional recurrent neural network," *Neurocomputing*, vol. 356, pp. 151-161, 2019.
[45] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, L. Kaiser, and I. Polosukhin, "Attention is all you need," *arXiv preprint arXiv:1706.03762*, 2017.
[46] R. Horev, "*BERT Explained: State of the art language model for NLP*", 2018. [Online]. Available: https://towardsdatascience.com/bert-explained-state-of-the-art-language-model-for-nlp-f8b21a9b6270. [Accessed: July 2021]
[47] L. Spitzner, "*Honeytokens: The Other Honeypot*", 2020. [Online]. Available: https://bit.ly/2Ue1QTZ. [Accessed: June 2021]
[48] F. Pouget, M. Dacier, and H. Debar, "White paper: honeypot, honeynet, honeytoken: terminological issues," *Rapport technique EURECOM*, vol. 1275, p. 09, 2003.
[49] R. Barnett, "*Monitoring VMare Honeypot*", 2002. [Online]. Available: http://honeypots.sourceforge.net/monitoring_vmware_honeypots.html. [Accessed: June 2021]
[50] I. Livshitz, "*Low, Medium and High Interaction Honeypot Security | Guardicore*", 2019. [Online]. Available: https://www.guardicore.com/blog/high-interaction-honeypot-versus-low-interaction-honeypot-comparison/. [Accessed: June 2021]
[51] HoneynetProject, "*Know Your Enemy: Defining Virtual Honeynets*", 2002. [Online]. Available: https://ivanlef0u.fr/repo/madchat/reseau/defense/DefiningVirtualHoneynets.pdf. [Accessed: June 2021]

[52] M. Nawrocki, M. Wählisch, T. C. Schmidt, C. Keil, and J. Schönfelder, "A survey on honeypot software and data analysis," *arXiv preprint arXiv:1608.06249,* 2016.
[53] G. Portokalidis, A. Slowinska, and H. Bos, "Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation," *ACM SIGOPS Operating Systems Review,* vol. 40, pp. 15-27, 2006.
[54] N. Sharma and S. S. Sran, "Detection of threats in Honeynet using Honeywall," *International Journal on Computer Science and Engineering,* vol. 3, pp. 3332-3336, 2011.
[55] HiHatProject, "*High Interaction Honeypot Analysis Tool*", 2007. [Online]. Available: https://sourceforge.net/projects/hihat/. [Accessed: August 2021]
[56] J.-w. Zhuge, X.-h. Han, Y.-l. Zhou, C.-y. Song, J.-p. Guo, and W. Zou, "HoneyBow: An automated malware collection tool based on the high-interaction honeypot principle," *JOURNAL-CHINA INSTITUTE OF COMMUNICATIONS,* vol. 28, p. 8, 2007.
[57] TheHoneynetProject, "*Know your Enemy: Sebek2*", 2003. [Online]. Available: http://web.mit.edu/6.857/OldStuff/Fall03/handouts/sebek.pdf. [Accessed: August 2021]
[58] M. Oosterhof, "*Cowrie*", 2014. [Online]. Available: https://cowrie.readthedocs.io/en/latest/README.html. [Accessed: August 2021]
[59] N. Provos, "*Developments of the Honeyd VIrtual Honeypot*", 2008. [Online]. Available: http://www.honeyd.org/. [Accessed: August 2021]
[60] Rapid7, "*InsightVM*", n.d. [Online]. Available: https://www.rapid7.com/products/insightvm/. [Accessed: June 2021]
[61] Osquery, "*Osquery Honeypot*", n.d. [Online]. Available: https://osquery.io/. [Accessed: August 2021]
[62] FireEye, "*Think Fast: Time Between Disclosure, Patch Release and VulnerabilityExploitation — Intelligence for Vulnerability Management, Part Two*", 2021. [Online]. Available: https://www.fireeye.com/blog/threat-research/2020/04/time-between-disclosure-patch-release-and-vulnerability-exploitation.html. [Accessed: June 2021]
[63] FIRST, "*Common Vulnerability Scoring System SIG*", 2005. [Online]. Available: https://www.first.org/cvss/. [Accessed: September 2021]
[64] H. Joh and Y. K. Malaiya, "A framework for software security risk evaluation using the vulnerability lifecycle and cvss metrics," in *Proc. International Workshop on Risk and Trust in Extended Enterprises,* California, 2010, pp. 430-434.
[65] U. K. Singh, C. Joshi, and N. Gaud, "Information security assessment by quantifying risk level of network vulnerabilities," *International Journal of Computer Applications,* vol. 156, pp. 37-44, 2016.
[66] Rapid7, "*Nexpose Vulnerability Scanner*", n.d. [Online]. Available: https://www.rapid7.com/products/nexpose/. [Accessed: August 2021]
[67] Secureworks, "*Taegis*", n.d. [Online]. Available: https://www.secureworks.com/products/taegis/xdr. [Accessed: August 2021]
[68] Y.-Z. Chen, Z.-G. Huang, S. Xu, and Y.-C. Lai, "Spatiotemporal patterns and predictability of cyberattacks," *PloS one,* vol. 10, p. e0124472, 2015.
[69] D. R. Hayes and F. Cappa, "Open-source intelligence for risk assessment," *Business Horizons,* vol. 61, pp. 689-697, 2018.
[70] S. Horawalavithana, A. Bhattacharjee, R. Liu, N. Choudhury, L. O. Hall, and A. Iamnitchi, "Mentions of security vulnerabilities on reddit, twitter and github," in

IEEE/WIC/ACM International Conference on Web Intelligence, Melbourne, 2019, pp. 200-207.

[71] C. Hobbs, Moran, M., Salisbury, D, *Open Source Intelligence in the Twenty-First Century - New Approaches and Opportunities*. London: Palgrave Macmillan, 2021.

[72] C. Andrew, R. J. Aldrich, and W. K. Wark, *Secret intelligence: A reader*. London: Routledge, 2009.

[73] L. Rosa, M. Freitas, S. Mazo, E. Monteiro, T. Cruz, and P. Simões, "A comprehensive security analysis of a scada protocol: From OSINT to Mitigation," *IEEE Access*, vol. 7, pp. 42156-42168, 2019.

[74] T. Day, H. Gibson, and S. Ramwell, "Fusion of OSINT and non-OSINT data," in *Open Source Intelligence Investigation*, ed Cham: Springer, 2016, pp. 133-152.

[75] H. Chen, R. Liu, N. Park, and V. Subrahmanian, "Using twitter to predict when vulnerabilities will be exploited," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, New York, 2019, pp. 3143-3152.

[76] S. Mittal, P. K. Das, V. Mulwad, A. Joshi, and T. Finin, "CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities," in *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, 2016, pp. 860–867.

[77] C. Sabottke, O. Suciu, and T. Dumitraș, "Vulnerability disclosure in the age of social media: Exploiting twitter for predicting real-world exploits," in *24th USENIX Security Symposium USENIX Security 15*, Washington, 2015, pp. 1041-1056.

[78] N. Dionísio, F. Alves, P. M. Ferreira, and A. Bessani, "Cyberthreat detection from twitter using deep neural networks," in *2019 International Joint Conference on Neural Networks (IJCNN)*, Budapest, 2019, pp. 1-8.

[79] M. S. Abdullah, A. Zainal, M. A. Maarof, and M. N. Kassim, "Cyber-attack features for detecting cyber threat incidents from online news," in *2018 Cyber Resilience Conference (CRC)*, Malaysia, 2018, pp. 1-4.

[80] S. Zhou, Z. Long, L. Tan, and H. Guo, "Automatic identification of indicators of compromise using neural-based sequence labelling," *arXiv preprint arXiv:1810.10156*, 2018.

[81] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. Beyah, "Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, Viena, 2016, pp. 755-766.

[82] G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, and X. Niu, "Ttpdrill: Automatic and accurate extraction of threat actions from unstructured text of cti sources," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, New York, 2017, pp. 103-115.

[83] N. Tavabi, P. Goyal, M. Almukaynizi, P. Shakarian, and K. Lerman, "Darkembed: Exploit prediction with neural language models," in *Proceedings of the AAAI Conference on Artificial Intelligence*, New Orelans, 2018.

[84] I. Deliu, C. Leichter, and K. Franke, "Extracting cyber threat intelligence from hacker forums: Support vector machines versus convolutional neural networks," in *2017 IEEE International Conference on Big Data (Big Data)*, Boston, 2017, pp. 3648-3656.

[85] D. Iorga, D. Corlătescu, O. Grigorescu, C. Săndescu, M. Dascălu, and R. Rughiniş, "Early Detection of Vulnerabilities from News Websites using Machine

Learning Models," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, 2020, pp. 1-6.
[86] D. Iorga, D.-G. Corlatescu, O. Grigorescu, C. Sandescu, M. Dascalu, and R. Rughinis, "Yggdrasil—Early Detection of Cybernetic Vulnerabilities from Twitter," in *2021 23rd International Conference on Control Systems and Computer Science (CSCS)*, Bucharest, 2021, pp. 463-468.
[87] O. Grigorescu, C. Săndescu, and A. Caba, "Web Application Honeypot Published in the Wild," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, 2020, pp. 1-6.
[88] C. Săndescu, R. Rughinis, and O. Grigorescu, "Hunt: Using honeytokens to understand and influence the execution of an attack," in *The International Scientific Conference eLearning and Software for Education*, Bucharest, 2017, p. 511.
[89] O. Grigorescu, C. Săndescu, and R. Rughiniş, "CODA footprint continuous security management platform," in *2016 15th RoEduNet Conference: Networking in Education and Research*, Bucharest, 2016, pp. 1-5.
[90] R. Radu, C. Săndescu, O. Grigorescu, and R. Rughiniş, "Analyzing Risk Evaluation Frameworks and Risk Assessment Methods," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, 2020, pp. 1-6.