UNIVERSITATEA NAȚIONALĂ DE ȘTIINȚĂ ȘI TEHNOLOGIE
POLITEHNICA BUCUREȘTI

Facultatea de Automatică și Calculatoare
Departamentul de Calculatoare

Rezumatul tezei doctorale

Prioritizarea vulnerabilităților bazată pe expunerea timpurie, tendințele emergente și scenariile contextuale de atac

Octavian Grigorescu

Conducător teză:

Prof. dr. ing. Răzvan Rughiniș

BUCUREȘTI
2023

CUPRINS

REZUMAT

Disciplina securității cibernetice a devenit din ce în ce mai importantă pentru protejarea proceselor societale în cadrul comunității globale interconectate de astăzi. Odată cu proliferarea utilizatorilor de internet, a dispozitivelor și a serviciilor, devine imperios necesar să se gestioneze protejarea eficienta împotriva amenințărilor cibernetice. Această teză utilizează capacitățile inteligenței artificiale (AI) pentru a transforma în mod fundamental metodologiile de securitate cibernetică, abordând și subiectul Internetul obiectelor (IoT). Deși IA crește probabilitatea amenințărilor la adresa securității cibernetice, ea prezintă, de asemenea, perspective fără precedent pentru strategii de apărare proactive. Prin utilizarea metodelor de ultimă generație ale inteligenței artificiale, acest studiu urmărește să obțină un avantaj față de adversari prin detectarea promptă a vulnerabilităților, evaluarea riscurilor sub toate aspectele relevante și conceperea unor abordări sofisticate în materie de securitate cibernetică.

Fiecare dintre cele trei întrebări fundamentale de cercetare abordate în teză motivează investigarea și dezvoltarea celor trei contribuții principale. Cercetarea inițială examinează potențialul de îmbunătățire a identificării timpurii a vulnerabilităților în materie de securitate cibernetică prin implementarea unor metode avansate de analiză a datelor și de învățare automată (ML). Secțiunea următoare examinează abordări și instrumente eficiente pentru evaluarea și controlul vulnerabilităților în materie de securitate cibernetică, punând accentul pe distincția dintre diversele amenințări cibernetice. Cea de-a treia componentă a cercetării examinează procesul prin care strategiile proactive de apărare a securității cibernetice, cum ar fi sistemele de evaluare a riscurilor și gestionarea continuă a securității, sunt dezvoltate și integrate în operațiunile unei organizații.

Contribuția preliminară investighează cercetarea empirică privind descoperirea timpurie a vulnerabilităților. Abordarea propusă cuprinde mai multe componente: dezvoltarea unui agregator de știri de securitate, aplicarea modelelor de învățare automată (ML) pentru a identifica vulnerabilitățile pe site-urile de știri și pe platforma Twitter, utilizarea descrierilor textuale pentru a prognoza gravitatea vulnerabilităților software și integrarea tehnicilor de procesare a limbajului natural (NLP) cu ontologiile preexistente pentru a extrage exploatările și vectorii de atac din știrile din domeniul securității cibernetice.

A doua contribuție se concentrează pe cercetarea empirică în domeniul evaluării riscurilor. Aceasta utilizează metodologii noi, cum ar fi honeytokens pentru a monitoriza execuția atacurilor, implementarea de honeypots pentru aplicații web, analiza prin modele lingvistice a tendințelor actuale în materie de securitate cibernetică și o examinare a tendințelor emergente în materie de vulnerabilități raportate în știrile din domeniul securității cibernetice.

Cea de-a treia contribuție la cercetarea empirică în domeniul apărării cibernetice proactive aduce o contribuție originală substanțială tehnologiilor actuale din domeniu. Proiectul implică mai multe componente-cheie: crearea amprentei CODA, care facilitează gestionarea continuă a securității, evaluări ale cadrelor și metodelor de evaluare a riscurilor, explorarea breșelor de securitate în Internetul obiectelor, implementarea modelelor de probabilitate și a graficului de

atac în cadrul unui sistem contextual de notare a riscurilor și utilizarea unui sistem contextual de notare a priorităților pentru a stabili prioritățile de corectare a vulnerabilităților.

Prin dezvoltarea, implementarea și validarea unor metode sofisticate de inteligență artificială, această teză aduce contribuții substanțiale la domeniul securității cibernetice în ansamblu. Lucrarea realizează și o analiză critică a metodologiilor propuse, subliniind avantajele acestora, dificultățile întâmpinate în timpul implementării și posibilele utilizări și dezvoltări viitoare. Contribuțiile tezei nu numai că introduc abordări inovatoare în domeniul securității cibernetice, dar stabilesc și un standard pentru investigațiile ulterioare în acest domeniu în continuă dezvoltare.

Keywords: Language Models, Natural Language Processing, Common Vulnerability Scoring System, MITRE Adversarial Tactics, Techniques, and Common Knowledge, Contextual Risk Scoring, Remediation Effort Prioritization

1 INTRODUCERE

1.1 Context

Tranzițiile rapide care au loc în domeniul securității cibernetice sunt determinate de complexitatea tot mai mare a mediilor digitale și de creșterea neîncetată a amenințărilor cibernetice. Complexitatea actorilor ostili a creat probleme semnificative pentru abordările actuale de detectare și gestionare a vulnerabilităților în materie de securitate cibernetică. Metodele convenționale sunt frecvent reactive și întâmpină dificultăți în abordarea adecvată a noilor pericole cibernetice.

În plus, este necesară o înțelegere aprofundată a naturii și a trăsăturilor amenințărilor cibernetice din cauza cantității și diversității imense a acestora. În prezent, este extrem de important să se identifice procese și instrumente eficiente pentru evaluarea și gestionarea riscurilor de securitate cibernetică, în special atunci când este vorba de diferențierea diferitelor amenințări cibernetice. Pe măsură ce întreprinderile și structurile guvernamentale caută să își consolideze apărarea, acestea depind din ce în ce mai mult de tehnologii de ultimă oră, cum ar fi inteligența artificială (AI), procesarea limbajului natural (NLP) și modelele de învățare automată (ML) sau de învățare profundă (DL) pentru a înțelege și a aborda amenințările cibernetice.

Deși este deja un lucru cunoscut în comunitatea de securitate cibernetică, utilizarea inteligenței artificiale ca instrument pentru a face față celor mai frecvente atacuri cibernetice (atacuri ransomware, atacuri IoT, atacuri cloud și atacuri blockchain) este evidențiată și de Mijwil et al. (2023) [376]. Nu numai că autorii descriu aceste atacuri ca fiind comune, dar și ca fiind în evoluție, în sensul că atacatorii continuă să găsească noi abordări tot mai sofisticate pentru a găsi și exploata vulnerabilitățile cibernetice.

Accentul pus pe tehnologia de ultimă oră ca răspuns la complexitatea peisajului cibernetic este ilustrat și de activitatea recentă din comunitatea academică în domeniul securității cibernetice. De exemplu, Nobrega & Rutkowski (2022) [377] susțin că Inteligența Artificială permite identificarea modelelor de atac și automatizarea anumitor proceduri de securitate cibernetică. Zhang et al. (2023) [378] [378] menționează proceduri specifice care pot fi automatizate prin intermediul IA. Baharadiya (2023) [379] discută aplicarea ML în securitatea cibernetică. Ahsan et al. (2023) [4] oferă o analiză cuprinzătoare a bazelor de date existente, a tehnicilor ML și a tehnicilor DL utilizate pentru securitatea cibernetică.

Există un interes crescut în ceea ce privește aplicarea modelelor DL în scopuri de securitate cibernetică, Dixit & Silakari (2021) [380] susțin că tehnicile de învățare profundă îmbunătățesc performanța sistemelor de securitate cibernetică, iar Sewak et. al (2022) [381] oferă o analiză

amplă a soluțiilor existente care utilizează învățarea profundă (DL) în scopuri de securitate cibernetică. Lin et. al (2020) [382] disting între diferite tipuri de abordări DL.

În acest context, cercetările prezentate în această teză au o importanță relevantă în peisajul actual al securității cibernetice. Pe de o parte, ea răspunde nevoii de a transforma cercetarea academică axată pe tehnici de ultimă oră pentru atenuarea amenințărilor cibernetice în soluții proactive viabile care pot fi aplicate în scenarii din lumea reală. Pe de altă parte, cercetarea actuală extinde cunoștințele teoretice privind aspectele legate de securitatea cibernetică, utilizând date empirice. Mai exact, întrebările și obiectivele de cercetare ale lucrării actuale urmăresc să contribuie cu progrese practice și teoretice în ceea ce privește detectarea timpurie, evaluarea riscurilor și strategiile proactive de apărare a securității cibernetice.

1.2 Enunțarea problemei

Problema abordată în cadrul cercetării actuale provine din două surse: nivelul de dezvoltare insuficient al sistemelor de securitate cibernetică existente care se bazează pe metode convenționale de detectare și atenuare a amenințărilor cibernetice și decalajul dintre progresele teoretice în domeniul securității cibernetice și implementarea lor practică în contexte organizaționale. Fiecare dintre cele două probleme este detaliată în rândurile următoare.

Sistemele convenționale de securitate cibernetică se confruntă cu provocări semnificative în peisajul în schimbare rapidă al amenințărilor cibernetice. Bazându-se pe metodele tradiționale de atenuare a amenințărilor cibernetice, aceste sisteme se străduiesc adesea să se adapteze la natura complexă și diversă a amenințărilor cibernetice contemporane. În consecință, organizațiile care utilizează astfel de sisteme devin mai susceptibile la exploatare.

În plus, este posibil ca metodele existente de evaluare și gestionare a riscurilor de securitate cibernetică să nu aibă granularitatea necesară pentru a face distincția între diferitele categorii de amenințări cibernetice. Insuficiența în a discerne între nuanțele atacurilor cibernetice împiedică abilitatea de a stabili în mod eficient prioritățile și de a aborda cele mai critice amenințări. Fără cadre cuprinzătoare de evaluare a riscurilor, organizațiile pot aloca resursele mai puțin eficient, ceea ce le face mai vulnerabile la atacuri cibernetice sofisticate și țintite. Acest lucru se adaugă la accentul pus pe măsurile reactive care predomină în cadrul strategiilor de securitate cibernetică ale organizațiilor, ceea ce ar putea împiedica dezvoltarea și punerea în aplicare a unor planuri de apărare proactive. În consecință, organizațiile pot fi expuse la amenințări cibernetice noi și neprevăzute.

Pe de altă parte, există un decalaj în ceea ce privește integrarea tehnologiilor de ultimă oră în sisteme și soluții practice de securitate cibernetică. Eșecul de a valorifica în mod eficient tehnologii precum NLP și AI, în special ML și DL, poate împiedica dezvoltarea unor alternative viabile la sistemele convenționale de securitate cibernetică. În lipsa unor soluții practice și accesibile, organizațiile ar putea întâmpina dificultăți în aplicarea practicilor de ultimă oră în materie de securitate cibernetică, neavând altă opțiune decât să recurgă la utilizarea sistemelor

și metodelor convenționale de securitate cibernetică, în ciuda dezavantajelor prezentate în rândurile anterioare.

1.3 Obiective

Având în vedere contextul și enunțul problemei prezentate în secțiunile anterioare, au fost adresate următoarele întrebări de cercetare:

- **Întrebare de cercetare 1** Cum poate fi îmbunătățită detectarea timpurie a vulnerabilităților în domeniul securității cibernetice utilizând tehnici avansate de analiză a datelor și de învățare automată?
- **Întrebare de cercetare 2** Care sunt metodologiile și instrumentele eficiente pentru evaluarea și gestionarea riscurilor în materie de securitate cibernetică, în special în ceea ce privește distincția între diferitele tipuri de amenințări cibernetice?
- **Întrebare de cercetare 3** În ce mod pot fi dezvoltate și integrate în practicile organizaționale strategii proactive de apărare în materie de securitate cibernetică, inclusiv sisteme de gestionare continuă a securității și de evaluare a riscurilor?

Întrebările au stat la baza identificării celor șapte obiective aferente cercetării actuale:

1. **Dezvoltarea de sisteme avansate de detectare și gestionare a securității cibernetice:** Proiectarea și punerea în aplicare a unor sisteme și instrumente inovatoare care să îmbunătățească detectarea, analiza și gestionarea amenințărilor la adresa securității cibernetice. Aceasta include crearea de platforme precum Yggdrasil și CODA Footprint, care oferă informații în timp real și capacități de gestionare continuă a securității. Aceste platforme au fost implementate și sunt în prezent funcționale.
2. **Utilizarea tehnologiilor de ultimă generație în domeniul securității cibernetice:** Utilizarea tehnologiilor de ultimă oră, cum ar fi modelele de învățare automată și de învățare profundă, procesarea limbajului natural și alte tehnici de inteligență artificială pentru îmbunătățirea eficienței și eficacității practicilor de securitate cibernetică. Aceasta implică utilizarea unor modele lingvistice avansate, cum ar fi BERT și RoBERTa, pentru sarcini precum detectarea vulnerabilităților, predicția gravității și analiza tendințelor.
3. **Analiză aprofundată a amenințărilor cibernetice și a tendințelor de vulnerabilitate:** Realizarea de studii cuprinzătoare care să analizeze și să clasifice diferite tipuri de amenințări și vulnerabilități cibernetice. Aceasta include înțelegerea comportamentului și a tehnicilor atacatorilor, evaluarea tendințelor emergente în domeniul securității cibernetice și identificarea amenințărilor critice care necesită o atenție imediată.
4. **Îmbunătățirea evaluării și prioritizării riscurilor în domeniul securității cibernetice:** Dezvoltarea și perfecționarea metodelor de evaluare și prioritizare a riscurilor

în materie de securitate cibernetică. Acest obiectiv cuprinde analiza cadrelor de evaluare a riscurilor, dezvoltarea de abordări de securitate bazate pe testare și implementarea modelelor de probabilitate și de grafice de atac pentru evaluarea contextuală a riscurilor.

5. **Explorarea abordărilor proactive în domeniul apărării cibernetice:** Deplasarea accentului de la strategii reactive la strategii proactive în domeniul securității cibernetice. Aceasta implică dezvoltarea de sisteme și metodologii care să permită detectarea timpurie și acțiunea preventivă împotriva amenințărilor cibernetice, reducând astfel impactul potențial al acestor amenințări.
6. **Integrarea soluțiilor practice în măsurile de securitate cibernetică:** Furnizarea de instrumente și cadre de lucru care pot fi integrate în operațiunile de securitate cibernetică de zi cu zi. Aceasta include oferirea de soluții pentru gestionarea continuă a securității și evaluarea riscurilor, care pot fi aplicate direct în diverse contexte organizaționale.
7. **Contribuția la cunoștințele teoretice și practice în domeniul securității cibernetice:** Îmbogățirea înțelegerii academice și practice a securității cibernetice, oferind perspective și constatări care pot fi valorificate de cercetători, practicieni și factori de decizie politică în domeniu.

1.4 Structura tezei

Cele șapte capitole ale lucrării de față sunt organizate în două părți, fiecare abordând aspecte specifice ale cercetării: stadiul actual al cunoașterii și studiile empirice. Ca atare, fiecare capitol este prezentat pe scurt în secțiunea actuală.

Capitolul 1 reprezintă introducerea tezei și cuprinde enunțarea contextului de cercetare împreună cu provocările care trebuie abordate, urmată de formularea a trei întrebări de cercetare și a șapte obiective care au ghidat activitatea noastră și de prezentarea structurii tezei.

Capitolul 2 oferă un studiu cuprinzător al stadiului actual al tehnologiei în domeniul securității cibernetice.Acesta explorează tehnicile avansate de detectare și gestionare timpurie a vulnerabilităților (secțiunea 2.1), strategiile în evoluție în domeniul evaluării și gestionării riscurilor în materie de securitate cibernetică (secțiunea 2.2) și trecerea la o paradigmă proactivă în domeniul securității cibernetice, cu accent pe gestionarea și prioritizarea vulnerabilităților (secțiunea 2.3).

Capitolul 3 analizează studiile empirice legate de expunerea timpurie la vulnerabilitate și propune contribuții originale pentru îmbunătățirea tehnologiilor din acest domeniu. Capitolul începe cu introducerea urmată de dezvoltarea unui agregator de știri de securitate (secțiunea 3.2). În continuare, sunt utilizate modele ML pentru detectarea timpurie a vulnerabilităților de pe site-urile de știri (secțiunea 3.3) și de pe platforma Twitter (secțiunea 3.4). Este explorată predicția severității vulnerabilităților software pe baza descrierii textului acestora (secțiunea 3.5), iar exploatările și vectorii de atac sunt extrași din știrile privind securitatea cibernetică cu ajutorul tehnicilor NLP (secțiunea 3.6) și sunt corelate cu ontologiile existente (secțiunea

3.7).

Capitolul 4 constă în studii empirice care avansează stadiul actual al tendințelor în materie de vulnerabilități și tactici de atac. Acesta implică utilizarea de honeytokens pentru a înțelege și influența executarea unui atac (secțiunea 4.2), publicarea unui honeypot de aplicații web în mediul natural (secțiunea 4.3), un studiu de caz bazat pe modele lingvistice pentru a analiza cele mai recente tendințe în materie de securitate cibernetică (secțiunea 4.4) și o analiză a tendințelor emergente în materie de vulnerabilitate în știrile din domeniul securității cibernetice (secțiunea 4.5).

Capitolul 5 avansează, prin studii empirice, stadiul actual al tehnologiei legate de apărarea cibernetică proactivă. Acesta include descrierea platformei de gestionare continuă a securității CODA Footprint (secțiunea 5.2), o analiză a cadrelor și metodelor de evaluare a riscurilor (secțiunea 5.3), o investigare a motivelor pentru care securitatea IoT eșuează și a necesității unei abordări de securitate bazate pe teste (secțiunea 5.4), aplicarea modelelor de probabilitate și a graficului de atac într-un sistem contextual de notare a riscurilor (secțiunea 5.5) și prioritizarea pe bază de context a vulnerabilităților și eforturilor de remediere (secțiunea 5.6).

Capitolul 6 oferă o analiză critică a abordărilor propuse, subliniind avantajele acestora (secțiunea 6.1) și problemele cu care s-au confruntat în timpul dezvoltării lor (secțiunea 6.2), precum și contexte de aplicabilitate (secțiunea 6.3).

Ultimul capitol (**Capitolul 7**) rezumă contribuțiile originale ale cercetării (Secțiunea 7.1) și subliniază potențialele direcții ale cercetărilor ulterioare (Secțiunea 7.2).

2 EXPUNEREA TIMPURIE LA VULNERABILITĂȚI

Contribuția inițială a studiilor empirice prezentate în această teză examinează sistemele și abordările noi care au fost dezvoltate pentru a îmbunătăți detectarea și gestionarea amenințărilor în domeniul securității cibernetice. Acest segment al tezei oferă o prezentare generală a șase lucrări de cercetare interconectate, care au adus contribuții substanțiale în domeniul securității cibernetice.

Crearea "Security News Aggregator" (Agregator de știri de securitate) reprezintă un efort inovator în gestionarea volumului copleșitor de conținut legat de securitatea cibernetică. Obiectivul principal al acestei platforme este de a prioritiza și filtra în mod eficient știrile critice din domeniul securității, punând un accent deosebit pe vulnerabilitățile emergente și pe atacurile de tip "zero-day". Costurile ridicate ale atacurilor cibernetice servesc drept dovadă a importanței critice a supravegherii eficiente a cantității enorme și în continuă expansiune de date privind securitatea cibernetică, pentru a asigura distribuirea la timp și eficientă a actualizărilor de nivel urgent și critic.

Ulterior, lucrarea de cercetare "Early Detection of Vulnerabilities from News Websites Using Machine Learning Models" (Detectarea timpurie a vulnerabilităților de pe site-urile de știri cu ajutorul modelelor de învățare automată) face progrese semnificative prin analizarea articolelor de știri pentru a găsi indicii ale amenințărilor cibernetice emergente, utilizând tehnici sofisticate de învățare automată. Prin valorificarea funcționalităților mașinilor vectoriale de suport, a clasificatorilor Multinomial Naïve Bayes și a unui model BERT fine-tuned, acesta demonstrează o precizie excepțională în detectarea vulnerabilităților. Acest lucru subliniază și mai mult eficiența procesării limbajului natural (NLP) în identificarea la timp a amenințărilor cibernetice.

Articolul "Yggdrasil – A CSCL System for the Early Detection of Cybernetic Vulnerabilities" (Yggdrasil - Un sistem CSCL pentru detectarea timpurie a vulnerabilităților cibernetice) prezintă un nou sistem automatizat care utilizează tweet-urile ca sursă de date pentru a identifica potențialele amenințări. Prin utilizarea modelului lingvistic BERT pentru a examina tweet-urile care conțin link-uri către articole de securitate cibernetică, această metodologie prezintă capacitatea învățării prin transfer de a spori învățarea colaborativă și detectarea oportună a amenințărilor în domeniul securității cibernetice.

În plus, "Severity Prediction of Software Vulnerabilities based on their Text Description" (Predicția severității vulnerabilităților software pe baza descrierii lor text) implementează o metodologie de învățare profundă pentru a evalua gravitatea vulnerabilităților software. Prezenta investigație utilizează un cadru de învățare multitask împreună cu un model BERT pre-antrenat pentru a prognoza nivelurile de gravitate ale vulnerabilităților exclusiv pe baza descrierilor textuale ale acestora. Această metodologie nouă exemplifică capacitatea învățării

profunde de a furniza evaluări prompte și precise ale gravității vulnerabilităților.

În lucrarea "Extracting Exploits and Attack Vectors from Cybersecurity News Using NLP" (Extragerea exploatărilor și a vectorilor de atac din știrile de securitate cibernetică folosind NLP) se propune o abordare eficientă pentru etichetarea automată a articolelor referitoare la securitatea cibernetică. Prin utilizarea recunoașterii entităților numite, această metodologie extrage și clasifică în mod eficient date cruciale referitoare la vulnerabilitățile emergente și la căile de atac, sporind astfel înțelegerea și adaptabilitatea în fața amenințărilor cibernetice.

În cele din urmă, lucrarea "CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques" (CVE2ATT&CK: Maparea cu ajutorul modelului BERT a CVE-urilor cu tehnicile MITRE ATT&CK) abordează problema crucială a asocierii anumitor tehnici de atac cu Vulnerabilitățile și expunerile comune (CVE). Obiectivul acestui studiu este de a stabili în mod autonom aceste conexiuni critice prin adnotarea CVE-urilor cu ajutorul tehnicilor derivate din cadrul MITRE ATT&CK și prin dezvoltarea de modele, inclusiv modele lingvistice bazate pe BERT. Realizarea acestui demers aduce o contribuție substanțială la capacitatea comunității de securitate cibernetică de a înțelege și de a atenua eficient amenințările cibernetice.

Împreună, aceste șase contribuții de cercetare constituie o investigație cuprinzătoare și multifațetată a metodologiilor și tehnicilor de ultimă oră în domeniul securității cibernetice. În lupta continuă împotriva amenințărilor cibernetice, se subliniază importanța detecției timpurii, a analizei avansate a datelor și a încorporării învățării automate și a procesării limbajului natural (NLP).

2.1 Sinteză

În domeniul securității cibernetice, contribuția inițială a segmentului de studii empirice dezvăluie strategii și sisteme noi care au fost dezvoltate pentru a detecta și gestiona amenințările cibernetice într-un stadiu incipient. Aceasta reprezintă punctul culminant al eforturilor de cercetare în acest domeniu. Acest segment al tezei integrează constatările și sugestiile pentru cercetări ulterioare din șase studii de cercetare distincte, care au adus toate contribuții la înțelegerea și progresul practicilor de securitate cibernetică.

Cercetarea "Security News Aggregator" a sugerat în mod eficient crearea unei platforme atotcuprinzătoare care să consolideze o gamă largă de știri din domeniul securității cibernetice, inclusiv corecții și vulnerabilități, breșe de securitate și CVE-uri. Procurându-și informațiile dintr-o gamă diversă de surse de încredere, această platformă servește drept punct central pentru evenimentele curente, putând contribui la detectarea amenințărilor de tip "zero-day" și a vulnerabilităților emergente. Eforturile ulterioare vor fi orientate spre creșterea funcționalităților platformei prin intermediul automatizării identificării utilizatorilor Twitter relevanți, prin fortificarea sistemului de evaluare a articolelor și prin investigarea kiturilor de exploatare a Dark Web. Necesitatea unor sisteme de informare dinamice și receptive în materie de securitate cibernetică este evidențiată de acest efort în curs de desfășurare.

În secțiunea intitulată "Early Detection of Vulnerabilities from News Websites Using Machine Learning Models" este prezentat un prototip de sistem conceput pentru a identifica amenințările cibernetice emergente în articolele de știri. În pofida rezultatelor încurajatoare obținute de modelul BERT, îmbunătățirile viitoare includ extinderea setului de date și efectuarea de teste cu modele lingvistice alternative. În plus, dezvoltarea ulterioară va implica integrarea acestui prototip într-un sistem mai cuprinzător care utilizează diverse informații din surse deschise (OSINT) pentru a identifica automat amenințările cibernetice timpurii. Obiectivul acestei extinderi sugerate este dublu: îmbunătățirea modelului existent și crearea unui sistem mai cuprinzător care să poată detecta amenințările într-un stadiu incipient.

"Yggdrasil – A CSCL System for the Early Detection of Cybernetic Vulnerabilities" este un articol care se axează pe criteriile de sarcină, integrare și concentrare pentru a dezvolta o tipologie avansată pentru sistemele CSCL în domeniul securității cibernetice. Atât experții, cât și cei care nu sunt experți sunt asistați de sistemul Yggdrasil în cunoștințele generate de comunitate cu privire la vulnerabilitățile cibernetice emergente. În urma unui experiment care implică învățarea prin transfer de la un model dezvoltat anterior [130], acest studiu validează capacitățile de predicție ale modelului BERT și ale metodelor de fuziune a datelor în ceea ce privește informațiile pertinente. Activitățile ulterioare cuprind creșterea setului de date și aprofundarea fezabilității învățării prin transfer ca metodologie de concepere a sistemelor CSCL în domeniul securității cibernetice. Acest studiu trasează o cale spre dezvoltarea unor instrumente automatizate care să sporească învățarea colaborativă și schimbul de cunoștințe în cadrul comunității de securitate cibernetică.

Segmentul următor al contribuției inițiale din cadrul secțiunii de studii empirice a tezei investighează în continuare abordări și sisteme noi în domeniul securității cibernetice. Acesta pune accentul în mod special pe utilizarea procesării limbajului natural (NLP) pentru a extrage informații despre atacurile cibernetice, pentru a lega CVE-urile de tehnicile MITRE ATT&CK și pentru a prezice gravitatea vulnerabilității.

Modelul de învățare profundă propus în studiul "Severity Prediction of Software Vulnerabilities based on their Text Description" simplifică procedura de evaluare a vulnerabilității. Prin utilizarea unei arhitecturi cu mai multe sarcini, acest model permite administratorilor de sistem să evalueze în mod eficient gravitatea amenințărilor reprezentate de vulnerabilitățile recent dezvăluite. Îmbunătățirile ulterioare vor cuprinde rafinarea hiperparametrilor modelului și integrarea acestuia într-o aplicație independentă care va furniza notificări instantanee privind amenințările critice și de risc ridicat. În plus, o explorare a unor arhitecturi mai extinse, cum ar fi RoBERTa [181], ar putea duce la o diminuare a inexactităților în ceea ce privește parametri prezișsi. Această cercetare reprezintă un progres semnificativ în conceperea unor metode accesibile și simplificate de evaluare a amenințărilor la adresa securității cibernetice de către neexperți.

Studiul intitulat "Extracting Exploits and Attack Vectors from Cybersecurity News using NLP" a prezentat o abordare nouă pentru clasificarea automată a articolelor referitoare la intruziuni și vulnerabilități. Serra et al. [179] au utilizat metode sofisticate de procesare a limbajului

natural (NLP), cum ar fi LSTM bidirecțional la nivel de cuvânt și modele personalizate care cuprind embeddings Bloom și CNN-uri reziduale [180]. Sunt justificate cercetări suplimentare pentru a încorpora în sursele de date kituri de exploatare a Dark Web și alte conținuturi legate de securitatea cibernetică. În plus, se va proiecta o interfață ușor de utilizat pentru a facilita filtrarea știrilor care sunt relevante pentru cerințele individuale ale utilizatorilor. Obiectivul acestei abordări este de a îmbunătăți capacitatea de utilizare și relevanța informațiilor privind securitatea cibernetică pentru utilizatorii finali prin optimizarea accesibilității și aplicabilității acestora.

În cele din urmă, proiectul de cercetare intitulat "CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques" a rezolvat o problemă importantă a modului în care se poate face legătura între CVE și tehnicile de atac în mod automat. Prin utilizarea unei metodologii de sarcini cu mai multe etichete și prin utilizarea în premieră a arhitecturilor bazate pe modelul BERT, acest proiect de cercetare a realizat progrese notabile în ceea ce privește etichetarea precisă a exploatărilor vulnerabilităților critice (CVE). Cercetările ulterioare vor fi dedicate îmbunătățirii corpusului CVE adnotat. Aceasta va implica investigarea unor abordări precum Few-Shot Learning [220] și Semi-Supervised Learning [221]. Aceste metode vor fi utilizate pentru a aborda dezavantajele legate de datele de instruire inadecvate și de dezechilibrul etichetelor. Planurile viitoare includ, de asemenea, încorporarea unor surse de informații suplimentare [222], cu scopul de a rectifica neconcordanțele prezente în descrierile CVE.

Cercetările extinse prezentate în aceste studii evidențiază caracteristicile în continuă schimbare și în progresul rapid ale domeniului securității cibernetice. În centrul acestor evoluții se află integrarea metodologiilor și tehnologiilor de ultimă oră, inclusiv a sistemelor de învățare colaborativă, a procesării limbajului natural și a învățării profunde. Prin implementarea acestor strategii cuprinzătoare, organizațiile pot monitoriza și aborda în mod eficient amenințările cibernetice în continuă schimbare, optimizând astfel detectarea și gestionarea amenințărilor într-un mod care să acorde prioritate nevoilor utilizatorilor.

Cercetările viitoare prezentate în aceste studii nu numai că au ca scop să îmbunătățească și să consolideze funcționalitățile sistemelor actuale, dar intenționează, de asemenea, să genereze progrese semnificative în domeniul mai larg al securității cibernetice. Inovarea continuă joacă un rol esențial în dezvoltarea unor sisteme intuitive și ușor de utilizat, care depășesc precizia și capacitatea de reacție, răspunzând în același timp nevoilor unei game largi de utilizatori. Accentul specific pus pe modelele de învățare automată indică o tranziție strategică către implementarea unor abordări proactive și mai bine informate pentru apărarea împotriva amenințărilor cibernetice.

În mod fundamental, cunoștințele acumulate în urma acestor eforturi de cercetare demonstrează un mediu de securitate cibernetică în continuă schimbare, caracterizat de o ingeniozitate și adaptare. Prin includerea tehnologiilor și metodologiilor de ultimă oră, aceste studii stabilesc bazele unei infrastructuri de securitate cibernetică mai rezistente și mai adaptabile, permițându-i să se confrunte în mod eficient cu complexitatea și dificultățile reprezentate de

amenințările cibernetice contemporane.

3 TENDINȚE ÎN MATERIE DE VULNERABILITĂȚI ȘI TACTICI DE ATAC

În cadrul domeniului dinamic al securității cibernetice, protejarea aplicațiilor web reprezintă o frontieră imperativă. Aceste aplicații tehnologice, care facilitează interacțiunea dintre utilizator și baza de date prin intermediul internetului, oferă avantaje substanțiale, dar prezintă și vulnerabilități de securitate importante. Vulnerabilitățile critice pot apărea din cauza programării necorespunzătoare sau a unor configurații greșite, permițând astfel persoanelor neautorizate să compromită sisteme întregi și să să obțină acces la date sensibile. Miza este extrem de mare, deoarece actorii rău intenționați caută în mod constant să monetizeze datele compromise, pe lângă faptul că aduc prejudicii de reputație. Cea de-a doua contribuție pe care am adus-o explorează acest domeniu prin intermediul a patru studii separate, fiecare dintre ele oferind perspective distincte asupra evoluțiilor în materie de securitate cibernetică, a vulnerabilităților și a noilor strategii defensive.

Acest capitol continuă cu "HUNT: Using Honeytokens to Understand and Influence the Execution of an Attack" (HUNT: Utilizarea honeytoken-urilor pentru a înțelege și influența executarea unui atac). Studiul de față prezintă un sistem avansat de detectare a intruziunilor care utilizează honeypots și honeytokens. Acesta a fost conceput în mod intenționat pentru a distinge atacurile extinse, fără scop, de amenințările mai concentrate și specifice. Sistemul folosește o abordare strategică a capcanelor care seamănă cu resurse atrăgătoare. Scopul este de a clasifica atacurile, a descifra motivațiile atacatorilor, a aduna probe criminalistice și, în cele din urmă, a elimina amenințările. Prin utilizarea unor honeytokens interconectați, care prezintă fiecare provocări de exploatare, se poate crea un scenariu cuprinzător în care pot fi evaluate abilitățile și motivațiile atacatorilor.

În continuare, "Web Application Honeypot Published in the Wild" (Honeypot de aplicație web publicat în Internet) este dedicată învățării tehnicilor de penetrare și detectării atacurilor cibernetice. Cercetarea presupune implementarea de honeypot-uri în cadrul unei infrastructuri cibernetice. Pentru a-i atrage pe atacatori, aceste honeypots sunt dotate cu provocări de tip "Capture the Flag". Cunoștințele dobândite pe parcursul a două luni de desfășurare pe internet constau în examinarea interacțiunilor umane și automate cu acești honeypots. Această analiză oferă informații semnificative despre tacticile și comportamentele amenințărilor.

"What are the Latest Cybersecurity Trends? A Case Study Grounded in Language Models" (Care sunt cele mai recente tendințe în materie de securitate cibernetică? Un studiu de caz bazat pe modele lingvistice) este o cercetare bazată pe procesarea limbajului natural care utilizează modelul de limbaj RoBERTa. Acest studiu examinează 2264 de articole de știri referitoare la securitate. Pentru a clasifica aceste articole în categorii relevante, se utilizează

embeddingurile textului, reducerea dimensionalității și gruparea subiectelor. Prin utilizarea acestei metodologii, este posibilă o evaluare amănunțită a dezvoltării și importanței diverselor tendințe în materie de securitate cibernetică, ceea ce oferă o perspectivă asupra situației actuale a amenințărilor și protecțiilor cibernetice.

Capitolul se finalizează prin articolul "Analysis of Emergent Vulnerability Trends in Cybersecurity News" (Analiza tendințelor de vulnerabilități emergente în știrile privind securitatea cibernetică). Acest studiu facilitează stabilirea priorităților de aplicare a patch-urilor software prin examinarea tendințelor în materie de vulnerabilitate. Acesta introduce un set de date substanțial de articole de știri din domeniul securității cibernetice adnotate manual prin utilizarea arhitecturilor de tip Transformer. Articolele sunt clasificate ca fiind pertinente sau inconsecvente de către modelele rafinate, care utilizează, de asemenea, tehnici de grupare pentru a identifica modelele recurente, în special în ceea ce privește expunerea furnizorului. Sistemul menționat mai sus funcționează ca un bun indispensabil pentru analiștii în domeniul securității cibernetice, sporindu-le competențele de investigație și cercetare de rutină.

Împreună, aceste studii oferă o perspectivă cuprinzătoare asupra mediului de securitate cibernetică, abordând dificultățile complexe asociate cu protejarea aplicațiilor web și a informațiilor pe care acestea le procesează. Fiecare studiu de cercetare oferă perspective și abordări distincte, care ne îmbunătățesc înțelegerea și capacitatea de a combate amenințările cibernetice.

3.1 Sinteză

Contribuția ulterioară din cadrul secțiunii de studii empirice a tezei oferă o analiză aprofundată a implementării strategice și a utilizării inventive a honeypots în domeniul securității cibernetice. Acest amplu efort de cercetare cuprinde o examinare a soluțiilor honeypot, precum și o investigare a celor mai recente tendințe în materie de securitate cibernetică prin intermediul unor modele lingvistice sofisticate.

Am examinat întregul continuum de soluții honeypot în "HUNT: Using Honeytokens to Understand and Influence the Execution of an Attack", de la inițiativele de cercetare academică până la implementările comerciale cu drepturi depline. Ancheta noastră a scos la iveală avantajele și dezavantajele honeypot-urilor cu interacțiune ridicată și cu interacțiune redusă. S-a observat că honeypots cu interacțiune ridicată (HIH) au prezentat o eficacitate remarcabilă în prevenirea amenințărilor persistente avansate și a atacurilor țintite. Ca urmare a acestor descoperiri, am conceput cadrul HUNT, care este o rețea de honeypot-uri descentralizată, compusă din dispozitive de aplicații web și gestionată eficient printr-o consolă centralizată. Capcanele, care funcționează ca microservicii în cloud, au fost proiectate cu atenție pentru a simboliza vulnerabilități distincte. Fiecare capcană are un nivel diferit de dificultate, acomodându-se atacatorilor cu un spectru larg de abilități. Un hacker care reușește să compromită cu succes un task HUNTER este direcționat către o sarcină suplimentară, mai dificilă, fiind astfel prins în această rețea complexă și notificând echipele de răspuns. Această configurație

garantează că mediul de producție pe care îl copiază nu este afectat în niciun fel. Fiecare capcană individuală transmite în mod independent datele de atac către consola centrală, facilitând compilarea și examinarea profilurilor atacatorilor, a identităților, precum și a tacticilor, tehnicilor și procedurilor (TTP). Ulterior, pentru a-i evalua eficacitatea, este necesar să se implementeze cadrul HUNT în medii de producție din lumea reală, simulând o aplicație autentică. În concordanță cu sistemele de securitate sofisticate, adaptarea continuă este esențială pentru menținerea unui avantaj competitiv împotriva amenințărilor contemporane. Pentru a-și menține eficacitatea împotriva unei game diverse de amenințări cibernetice, este important să se extindă acoperirea de protocoale pentru HUNT dincolo de HTTP.

Ulterior, am investigat încorporarea sistemelor honeypot în aplicațiile web ca parte a studiului exhaustiv "Web Application Honeypot Published in the Wild", având ca obiective detectarea și clasificarea atacatorilor, redirecționarea acestora către medii simulate și analiza acțiunilor lor. În virtutea metodologiei sale de pionierat, acest efort a demonstrat eficacitate în detectarea modelelor de atac și a instrumentelor utilizate împotriva aplicațiilor web. Creșterea numărului de atacuri și exploatarea vulnerabilităților în aplicațiile web utilizate pe scară largă - multe dintre acestea având încă probleme de securitate nerezolvate - subliniază necesitatea tot mai mare a unor astfel de soluții. Punerea în aplicare a honeypots prezintă dificultăți deosebite din cauza limitărilor și a necesității de a secretiza detaliile arhitecturale, ceea ce servește la împiedicarea încercărilor adversarilor de a ocoli aceste sisteme. Dezvoltat ca o măsură de securitate suplimentară la sistemele convenționale, cum ar fi sistemele de detectare a intruziunilor și firewall-urile, honeypot-ul nostru și-a demonstrat eficacitatea prin furnizarea de informații pertinente cu privire la instrumentele și activitățile actorilor rău intenționați. Prin integrarea în configurația honeypot-ului a unor versiuni securizate ale aplicațiilor lipsite de vulnerabilități cunoscute, crește probabilitatea de a descoperi exploatări de tip zero-day, care nu sunt încă cunoscute public, dar care sunt utilizate în mod activ în atacuri. Configurația honeypot-ului nostru, care este inspirată de un joc de tip Capture The Flag cu mai multe niveluri de dificultate, este concepută în mod intenționat pentru a evalua competența atacatorilor. Acest lucru determină ca honeypot-ul să fie atractiv, cât și suficient de dificil pentru a distinge instrumentele automate de intervenția umană în cazul unui atac. Statisticile și informațiile extrase din aceste atacuri capturate s-au dovedit a fi de o valoare imensă. În mod predictiv, intenționăm să îmbunătățim honeypot-ul pentru a permite un număr mai mare de interacțiuni umane, acumulând astfel un set de date mai cuprinzător pentru analiză. Bazându-ne pe o aplicație web utilizată pe scară largă, care este vizată în mod constant de actorii rău intenționați, garantăm un nivel substanțial de implicare a utilizatorilor. În plus, intenția noastră este de a aduce o serie de îmbunătățiri în sistem. Pentru început, vom prezenta o varietate de căi de explorare care valorifică informațiile privind vulnerabilitățile derivate din Top 10 Web Application Security Risks. Obiectivul nostru este de a dezvălui tehnici de hacking nou întâlnite. În al doilea rând, obiectivul nostru este de a construi noi căi de atac pentru potențialii atacatori, care să ofere oportunități de interacțiune îmbunătățite, cum ar fi accesul la shell-uri. Prin implementarea acestei configurații, vom avea capacitatea de a utiliza instrumente de supraveghere specializate pentru a le observa îndeaproape activitățile,

obținând astfel o înțelegere mai profundă a metodologiilor acestora. Aceste îmbunătățiri sunt vitale pentru a avansa în înțelegerea acțiunilor atacatorilor și vor oferi informații valoroase pentru crearea generațiilor ulterioare de honeypots sofisticate.

Al treilea studiu: "What are the Latest Cybersecurity Trends? A Case Study Grounded in Language Models" prezintă un nou pipeline automatizat care utilizează cele mai recente progrese în tehnologiile de procesare a limbajului natural (NLP) pentru a procesa articolele de știri din domeniul securității cibernetice. Prin utilizarea RoBERTa, un model de limbaj bazat pe Transformer, această metodă generează embeddinguri ale articolelor care sunt contextualizate. Înainte de a fi grupate, aceste embeddinguri sunt reduse în dimensiune. S-a stabilit că cea mai eficientă metodă de grupare a fost combinația dintre Hierarchical Density-Based Spatial Clustering of Applications with Noise (HDBSCAN) și UMAP (Uniform Manifold Approximation and Projection). Această metodologie nu numai că facilitează gruparea eficientă a articolelor, dar permite și extragerea și analiza cuprinzătoare a celor mai semnificative cuvinte-cheie din fiecare grup. Stadiul actual al proiectului pune bazele unei serii de îmbunătățiri ambițioase în viitor. Pentru început, am dezvoltat un sistem care să genereze notificări cu privire la potențialele amenințări la adresa securității cibernetice. Subiectele extrase de model vor sta la baza dezvoltării acestor notificări, care vor fi personalizate în mod special pentru aplicațiile software care rulează pe dispozitivele utilizatorilor. În plus, există intenția de a dezvolta o interfață specializată. Prin furnizarea de actualizări zilnice privind subiecte pertinente și prezentarea celor mai recente evoluții în domeniul securității cibernetice, această interfață va reprezenta un instrument deosebit de util pentru utilizatorii care doresc să rămână bine informați. În cele din urmă, există un obiectiv de a spori corpus-ul prin integrarea de surse suplimentare. Prin adoptarea acestei abordări, procesul de grupare poate fi îmbunătățit considerabil; prin încorporarea unei game mai diverse de subiecte în analiză, cantitatea de valori poate fi diminuată, rezultând observații mai precise și mai cuprinzătoare ale mediului de securitate cibernetică.

Studiul intitulat "Analysis of Emergent Vulnerability Trends in Cybersecurity News" prezintă în cele din urmă un sistem inovator care automatizează supravegherea știrilor din domeniul securității cibernetice în căutarea amenințărilor emergente. Această inovație semnifică un progres substanțial în domeniul analizei securității cibernetice. Utilizând ca bază modele avansate bazate pe Transformer, acest sistem reduce în mod eficient procesul laborios de analiză manuală a știrilor din domeniul securității cibernetice. Principalul scop al acestui sistem este de a îmbunătăți prioritizarea corecției vulnerabilităților software prin identificarea amenințărilor emergente și actuale. Pentru a realiza acest lucru, a fost compilat și aplicat un set de date extins pentru a rafina aceste modele bazate pe Transformer prin explorarea unor configurații și arhitecturi diverse. Infrastructura integrată a sistemului demonstrează competență în recuperarea articolelor, eliminarea conținutului străin, extragerea datelor relevante și, ulterior, construirea de clustere centrate pe vulnerabilitățile software detectate. În continuare, analiștilor de securitate li se prezintă aceste clustere, ceea ce simplifică substanțial procedura de analiză a știrilor din domeniul securității cibernetice. Scorul de acuratețe al modelului de clasificare care a fost implementat în cadrul sistemului este remarcabil, fiind de 0,91. În pofida acestor evoluții,

au fost identificate anumite aspecte care necesită îmbunătățiri suplimentare. Un exemplu de astfel de aspect este îmbunătățirea procedurii de grupare a articolelor, care, în prezent, este evaluată slab de Silhouette. Acest lucru sugerează că grupurile nu sunt suficient de separate și au tendința de a converge, reducând astfel eficiența algoritmului de grupare. În plus, este foarte important să se îmbunătățească procesul de extragere a informațiilor cuprinzătoare din articole care sunt considerate pertinente de către modelul de clasificare. O variantă pentru depășirea acestui obstacol este construirea unui model de etichetare a secvențelor. Modelul menționat mai sus posedă capacitatea de a extrage date precise și cuprinzătoare referitoare la vulnerabilitățile în materie de securitate cibernetică, inclusiv, dar fără a se limita la CVE (Common Vulnerabilities and Exposures - vulnerabilități și expuneri comune), vectori de atac și diverse categorii de vulnerabilități cibernetice. Prin încorporarea acestui model în sistem, profunzimea și acuratețea extragerii informațiilor ar putea fi îmbunătățite substanțial, consolidând astfel capacitatea sistemului de a detecta și evalua amenințările la adresa securității cibernetice.

În virtutea compilării lor, aceste studii nu numai că demonstrează eficacitatea metodologiilor noi în domeniul securității cibernetice, dar stabilesc și fundamentul pentru progresele ulterioare. Prin încorporarea honeypots, a metodelor de procesare a limbajului natural (NLP) și a metodelor automate, o organizație poate adopta o poziție strategică ca răspuns la provocările în continuă schimbare în materie de securitate cibernetică.

4 APĂRARE CIBERNETICĂ PROACTIVĂ - GESTIONAREA VULNERABILITĂȚILOR ȘI PRIORITIZAREA EFORTURILOR DE REMEDIERE

Această componentă a studiului doctoral are ca obiectiv central dezvoltarea unui sistem de cuantificare a vulnerabilităților și remedierilor ce poate fi utilizat în prioritizarea taskurilor echipei de securitate cibernetică. În plus, evoluția IoT a avut un impact profund asupra aspectelor legate de securitate și confidențialitate [297]. Pentru a reduce costurile și pentru a se adapta la condițiile fizice de funcționare, IoT este supus unor constrângeri tehnologice și de piață inerente, cum ar fi capacitățile limitate de stocare și de procesare ale unor dispozitive precum senzorii, în ciuda expansiunii sale rapide. Din cauza dependenței de baterii, aceste constrângeri, împreună cu nevoia critică de procesare în timp real și de eficiență energetică, contribuie la insuficiența măsurilor de securitate în numeroase sisteme IoT. Acest lucru a dus la o scădere a încrederii consumatorilor și a mediului de afaceri, care este exacerbată de incapacitatea industriei de a rezolva în mod convingător aceste probleme de securitate. Cercetările empirice privind provocările de securitate ale internetului obiectelor subliniază caracterul critic al dezvoltării de soluții noi în acest domeniu care evoluează rapid.

"CODA Footprint Continuous Security Management Platform" (Platforma CODA Footprint pentru monitorizarea continuă a securității) este titlul primului articolului. Această platformă funcționează ca o rezoluție atotcuprinzătoare pentru examinarea și evaluarea imediată a serviciilor critice ale unei organizații. În încercarea de a garanta funcționarea și protecția neîntreruptă a serviciilor critice, aceasta abordează complexitatea introdusă de proliferarea serviciilor cloud, de integrarea diferitelor dispozitive și de politicile de tip BYOD (bring-your-own-device). Platforma reprezintă un progres substanțial în gestionarea cerințelor complexe de securitate cibernetică ale organizațiilor contemporane, în special în ceea ce privește internetul obiectelor.

"Analyzing Risk Evaluation Frameworks and Risk Assessment Methods" (Analiza cadrelor de evaluare a riscurilor și a metodelor de evaluare a riscurilor) este subiectul următorului articol. Având în vedere prevalența tot mai mare a atacurilor cibernetice și a vulnerabilităților în domeniul digital, acest articol subliniază importanța tot mai mare a asigurărilor cibernetice. Acest articol abordează dificultățile cu care se confruntă inginerii de securitate atunci când încearcă să cuantifice consecințele monetare ale intruziunilor și să evalueze nivelul de expunere la risc la care este expusă o organizație. Cercetarea subliniază necesitatea unor cadre avansate de evaluare a riscurilor și în sectorul Internet of Things (IoT), îndemnând la îmbunătățiri ale protocoalelor folosite.

"Why IoT Security Is Failing – The Need for a Test-Driven Security Approach" (De ce eșuează

securitatea IoT - Necesitatea unei abordări de securitate bazate pe testare) este titlul celui de-al treilea articol al nostru, care oferă o analiză mai cuprinzătoare a securității cibernetice. Acest studiu oferă o investigație aprofundată a susceptibilităților de securitate inerente ecosistemului Internet of Things (IoT). Este sugerat un cadru de securitate bazat pe teste ca mijloc de supraveghere și de efectuare a testelor de securitate pentru aplicațiile Internet of Things (IoT) în fiecare etapă a dezvoltării acestora. Această metodologie este considerată un instrument esențial în abordarea riscurilor cibernetice emergente specifice internetului obiectelor, subliniind necesitatea unor evaluări de securitate permanente și stricte în cadrul IoT.

În plus, articolul "Probability and Attack Graph Models in Contextual Risk Scoring System" (Modele de probabilitate și grafice de atac în sistemul de evaluare a riscurilor contextuale) prezintă o soluție software cuprinzătoare care utilizează modele de grafuri de atac și metodologii bazate pe probabilități pentru a gestiona și cuantifica riscurile în rețelele de calculatoare. Prin generarea unui scor de rețea, care servește drept indicator cantitativ al expunerii la risc a rețelei, acesta demonstrează o abordare fiabilă și eficientă pentru evaluarea securității rețelelor de calculatoare. Această metodă este esențială în lumea digitală interconectată de astăzi, deoarece oferă o abordare flexibilă a securității cibernetice într-o varietate de medii. Importanța sa este subliniată de complexitatea tot mai mare a rețelelor și de obstacolul mondial de protejare a activelor digitale împotriva amenințărilor avansate.

În cele din urmă, lucrarea "Contextual Remediations Prioritization System designed to implement theoretical principles of CVSS v4" (Sistemul de prioritizare bazată pe context a remedierilor conceput prin implementarea principiilor teoretice ale CVSS v4) propune o modalitate nouă de prioritizare a vulnerabilităților cibernetice într-o eră a avansului tehnologic rapid și a interconectivității complexe a dispozitivelor. Extinderea rapidă a ecosistemului digital duce adesea la setări slabe sau insuficiente, ceea ce creează vulnerabilități în infrastructurile cibernetice. Problema esențială a prioritizării în cadrul gestionării riscurilor de vulnerabilitate (VRM) rămâne o preocupare. Acest studiu oferă o soluție nouă care se aliniază cu noile caracteristici ale CVSS v4, metoda aceasta utilizând un punctaj dinamic și informații contextuale despre vulnerabilități pentru a prioritiza mai eficient remedierile. Într-o economie digitală din ce în ce mai susceptibilă, acest lucru este esențial pentru securitatea și reziliența infrastructurilor cibernetice.

Pe scurt, cele patru articole menționate mai sus abordează în mod colectiv problemele complexe legate de securitate, atât în prioritizarea vulnerabilităților, cât și în ecosistemul IoT, introducând abordări și cadre noi care consolidează reziliența și securitatea mediilor. Prin punerea în aplicare a unor abordări de securitate bazate pe teste, a unei evaluări contextuale a riscurilor, precum și a unui management continuu al securității și a unei evaluări a riscurilor, aceste contribuții oferă o perspectivă vitală asupra securității în continuă expansiune.

4.1 Sinteză

Cea de-a treia contribuție din cadrul secțiunii de studii empirice a tezei oferă o examinare amănunțită a metodologiilor noi utilizate în domeniul securității cibernetice. Aceasta pune accentul în mod special pe cadrele de evaluare a riscurilor, pe sistemele de notare a riscurilor contextuale, pe securitatea IoT și pe gestionarea continuă a securității.

Lucrarea de cercetare intitulată "CODA Footprint Continuous Security Management Platform" prezintă o platformă centralizată inovatoare concepută pentru monitorizarea continuă a dispozitivelor conectate la o rețea. Dezvoltarea acesteia semnifică un progres substanțial în domeniul securității cibernetice pentru organizații. Scopul fundamental al acestui demers este de a proiecta și implementa un cadru software distribuit care să adune în mod eficient toate informațiile de configurare relevante de la o gamă largă de dispozitive conectate la rețea, precum mașinile virtuale (VM), serverele, routerele, switch-urile și firewall-urile. În urma transmiterii către un nod central, aceste informații sunt procesate și încorporate într-o amprentă virtuală pentru a facilita monitorizarea continuă. Obiectivul general al acestei cercetări este de a îmbunătăți substanțial funcționalitățile platformei de securitate CODA Footprint în viitorul apropiat. Îmbunătățirile propuse presupun consolidarea a trei module importante. Crearea unor sisteme de audit local bazate pe agenți constituie etapa inițială. Aceste sisteme vor efectua o investigație amplă a rețelei interne, generând o topologie automată care să descrie în mod cuprinzător mediul rețelei. Obiectivul celui de-al doilea modul este de a îmbunătăți funcționalitățile de analiză a rețelei ale platformei, oferind o perspectivă mai detaliată și mai cuprinzătoare a configurației și funcționării rețelei. În cele din urmă, cel de-al treilea modul, care prezintă cele mai inovatoare caracteristici, este autoreactiv, realizând decizii inteligente. Prin utilizarea unei combinații de date în timp real și date istorice, acest modul va deține capacitatea de a răspunde în mod independent la evenimente și de a ajunge la decizii bine informate. Se anticipează că încorporarea acestor module va spori semnificativ eficacitatea platformei în protejarea infrastructurilor organizaționale împotriva amenințărilor, oferind astfel o metodologie mai rezistentă și mai adaptabilă pentru administrarea securității cibernetice.

Articolul de cercetare intitulat "Analyzing Risk Evaluation Frameworks and Risk Assessment Methods" oferă o analiză cuprinzătoare a mai multor cadre de securitate cibernetică, inclusiv STIX, XCCDF, OVAL, SCAP și MAEC. Cercetarea evidențiază importanța standardizării în aceste cadre, punând la îndoială scopul existenței mai multor formate dacă obiectivul final este un limbaj universal de înțeles pentru specialiștii în securitate și pentru calculatoare. În plus, cercetarea investighează metodele de previzionare a vulnerabilităților care vor fi exploatate, spre deosebire de cele care vor rămâne neexploatate. Aceasta sugerează că o înțelegere mai cuprinzătoare a înclinațiilor și metodologiilor progresive ale hackerilor ar putea fi obținută prin examinarea datelor istorice, în special prin investigarea provenienței atacurilor semnificative care nu au fost dezvăluite până acum. Pentru a identifica tipare, această metodologie ar presupune efectuarea unei examinări exhaustive a fluxurilor Twitter, a știrilor istorice și a cronologiilor care descriu atacuri renumite. Studiul subliniază, de asemenea, importanța

înțelegerii modului în care pericolele se răspândesc în cadrul unei rețele. Având în vedere multitudinea de dispozitive care utilizează o infrastructură identică și, în consecință, vulnerabilități identice, ancheta de cercetare se referă la cea mai potrivită formulă de conversie a riscului într-o valoare numerică. Înțelegerea corelației dintre vulnerabilități și repercusiunile financiare pentru întreprinderi reprezintă un aspect financiar suplimentar al acestei probleme, având în vedere că întreprinderile sunt adesea reticente în a dezvălui informații referitoare la intruziuni. Datele istorice privind breșele și pierderile, în special cele care implică mărci renumite și atacuri semnificative, pot oferi informații valoroase, potrivit studiului, folosindu-se de tendința mass-media de a dezvălui informații, uneori împotriva voinței entităților implicate. Un aspect care este frecvent ignorat, potrivit cercetării, este elementul uman în securitatea cibernetică. Se recomandă ca cercetările ulterioare să monitorizeze o varietate de canale de știri, fluxurile Twitter și, cel mai important, Dark Web. Vulnerabilitățile emergente și exploatările de tip zero-day, inclusiv cele care sunt comercializate pe piața ilicită, pot fi descoperite prin această monitorizare. Obiectivul acestei cercetări este de a concepe contramăsuri și strategii pentru potențialele activități cibernetice prin dobândirea de cunoștințe privind resursele și tehnologiile pe care acestea le utilizează. Importanța unei înțelegeri multifațetate a securității cibernetice, care să ia în considerare factorii tehnici și umani care influențează dinamica amenințărilor cibernetice, este subliniată de această abordare exhaustivă.

În continuare, articolul intitulat "Why IoT Security is Failing: The Need for a Test Driven Security Approach" face o analiză critică a situației actuale a securității în domeniul Internet of Things (IoT) și propune o soluție inovatoare pentru a consolida măsurile de protecție în acest sector în plină dezvoltare. Obiectivul principal al modelului de Testare Dinamică a Securității Sistemelor IoT (DISST) este de a atenua riscurile și susceptibilitățile multiple care sunt intrinseci unei game largi de medii IoT. În acest model se subliniază importanța unui sistem de monitorizare continuă care poate evalua periodic întreaga infrastructură a aplicațiilor IoT pe parcursul ciclului de dezvoltare a acestora. Studiul subliniază caracterul inevitabil al problemelor de securitate și al vulnerabilităților în Internetul obiectelor (IoT) ca urmare a cantității mari de dispozitive interconectate, a complexității sistemelor și a varietății de dispozitive, aplicații, servicii și protocoale. Acesta evidențiază provocarea asociată cu detectarea incidentelor și propune abordări precum monitorizarea comunicațiilor în rețea, analiza înregistrărilor de activitate, efectuarea de teste de penetrare și implicarea în hacking etic pentru a descoperi punctele slabe și a aborda eficient incidentele. Cercetarea subliniază obligația critică a furnizorilor de IoT de a crea dispozitive mai sigure și de a susține securitatea acestora. Acesta susține că "Security by Design" este un concept crucial pentru atenuarea multiplelor provocări de securitate în Internetul obiectelor. Modelul DISST este propus ca un instrument auxiliar pentru eforturile de cercetare și dezvoltare în curs, facilitând identificarea vulnerabilităților și a punctelor slabe de securitate pe parcursul întregului ciclu de dezvoltare, fără a împiedica implementarea sau strategia tehnologică. În plus, este posibil să se încorporeze acest model cu cadre precum Anastasia pentru a antrena capacitățile sistemelor de detectare a intruziunilor (IDS) și ale sistemelor de gestionare a informațiilor și evenimentelor de securitate extinsă (XL-SIEM) în identificarea și abordarea anumitor modele de atac sau pentru a optimiza politicile.

În anticiparea evoluțiilor viitoare, cercetarea evidențiază necesitatea de a spori modelul DISST pentru a cuprinde o gamă largă de protocoale care acoperă mai multe niveluri de stive de rețea, precum și pentru a integra diverse industrii și numeroase categorii de dispozitive IoT. În plus, se pune un accent considerabil pe alocarea de resurse pentru inițiativele de învățare automată în vederea dezvoltării unui sistem mai sofisticat care să poată genera cazuri de testare a securității în mod autonom. Încorporarea și creșterea tehnologiilor sofisticate sunt esențiale pentru dezvoltarea securității IoT, garantând că aceasta rămâne în pas cu complexitatea și amploarea tot mai mare a infrastructurilor IoT, precum și cu domeniul în continuă schimbare al riscurilor de securitate cibernetică.

În plus, articolul de cercetare intitulat "Probability and Attack Graph Models in Contextual Risk Scoring System" introduce o abordare nouă care combină modelarea, prioritizarea, colectarea, selectarea și agregarea datelor pentru a calcula scorurile de risc pentru securitatea rețelelor. Acest demers implementează o strategie atotcuprinzătoare de evaluare a riscurilor prin combinarea modelelor bazate pe probabilități și a modelelor de grafuri de atac. Termenul "scor de risc", așa cum este definit în această cercetare, poate fi interpretat în diverse moduri, inclusiv probabilitatea atacurilor sistemului, gravitatea anumitor vulnerabilități și procentul de neconformitate. Aceste calcule sunt efectuate utilizând o combinație de modele experimentale și matematice care sunt susținute de fundamente teoretice stabilite. În pofida atingerii cu succes a obiectivelor sale principale, studiul recunoaște obstacolele întâmpinate în verificarea eficienței și preciziei soluției propuse. Provocarea menționată mai sus apare ca urmare a evoluției rapide a domeniului securității cibernetice și a construcției predominant empirice a modelelor de evaluare. În pofida eforturilor de standardizare a protocolului de automatizare a conținutului de securitate (Security Content Automation Protocol - SCAP) și a altor inițiative ale comunității, evaluarea precisă a riscurilor sistemului continuă să fie o sursă de ambiguitate. Cu toate acestea, cercetarea furnizează date și rezultate fiabile, prezentând un cadru versatil capabil să satisfacă cerințele actuale și viitoare de securitate a rețelelor prin integrarea conceptelor de ultimă oră și prin îmbunătățirea permanentă a API-urilor. Inițiativa se distinge de soluțiile actuale prin metodologia sa cuprinzătoare de agregare și evaluare a datelor în vederea efectuării analizei riscurilor. Pe lângă utilizarea unui model probabilistic pentru a evalua diverse categorii de date în context, aceasta pune accentul pe standardizarea datelor pentru o măsurătoare uniformă de evaluare a riscurilor. În plus, studiul subliniază importanța prioritizării proceselor și a luării în considerare a tipului de activitate atunci când se dezvoltă un cadru de calcul al riscurilor care poate fi modificat pentru a se adapta la activități organizaționale și obiective de securitate distincte. Această cercetare subliniază complexitatea evaluării rețelelor, recunoscând că utilizarea datelor experimentale previne includerea tuturor fațetelor printr-o singură metodă. Cu toate acestea, se presupune că o abordare care integrează elemente concrete, concepte matematice, metodologii statistice și repere de securitate comunitară poate produce rezultate aproximative. Constatările menționate mai sus joacă un rol crucial în evitarea defecțiunilor de sistem, a pierderilor financiare și a coruptiei datelor, sporind astfel eficacitatea generală a abordărilor privind securitatea rețelelor. Sunt necesare investigații suplimentare pentru a îmbunătăți modelul de calcul al riscului, pentru a reprezenta

mai exact peisajul în continuă schimbare al securității rețelelor. Această îmbunătățire va integra metodologii statistice și va fi conformă cu reperele de securitate ale comunității pentru a formula strategii de prevenire mai precise și mai proactive.

În cele din urmă, obiectivul principal al lucrării intitulate "Contextual Remediations Prioritization System designed to implement theoretical principles of CVSS v4" este de a găsi o soluție pentru prioritizarea remedierii vulnerabilităților, concepută pentru implementarea anumitor fundamente lipsă din CVSS V4. Obiectivul a fost atins prin implementarea unei soluții fundamentate pe combinarea mai multor tipuri de cunoștințe în modelarea unui sistem de calcul al riscurilor. Pentru a realiza acest lucru, am aprofundat soluțiile CVSS și am valorificat datele colectate de la un sistem de agenți inteligenți și de la Yggdrasil Threat Intelligence Service. Pe baza acestor date, am reușit să creăm trei indicatori utilizați în calcularea scorului vulnerabilității: static, dinamic și contextual. După cum au concluzionat Jung et al. [366], există unele limitări deoarece este greu de evaluat o nouă propunere, întrucât avem nevoie de o structură și de anumite standarde pentru a compara diferite abordări și a extrage viitoarele îmbunătățiri. Ceea ce diferențiază acest proiect de alte soluții consacrate este încorporarea a numeroase tipuri de date care au fost selectate în mod intenționat pentru evaluarea riscurilor, în plus față de evaluarea acestora cu ajutorul unui model probabilistic în contextul dat. Un beneficiu suplimentar al soluției noastre se referă la standardizarea datelor, ceea ce permite integrarea datelor respective prin utilizarea unor parametri consecvenți de evaluare a riscurilor. În această lucrare, am prezentat un model fundamental de calcul al riscurilor. Cu toate acestea, ierarhizarea aspectelor de securitate poate fi modificată în conformitate cu activitățile specifice ale organizației, în funcție de o structură în trepte de importanță distinctă. Acest proiect evidențiază faptul că evaluarea unei rețele este o activitate complexă care nu poate fi surprinsă pe deplin printr-o singură metodă, deoarece depinde de o multitudine de rezultate obținute din date empirice. Cu toate acestea, prin utilizarea unei metodologii care combină elemente concrete și principii matematice cu abordări statistice și norme de securitate din industrie, este posibil să se obțină rezultate aproximative care ajută la atenuarea riscurilor asociate cu corupția datelor, epuizarea monetară sau oprirea sistemului.

În ansamblu, aceste studii subliniază importanța inovării continue în domeniul securității cibernetice, evidențiind necesitatea unor strategii cuprinzătoare și adaptabile pentru a face față caracteristicilor în continuă schimbare ale amenințărilor cibernetice. Prin integrarea în aceste inițiative a unor sisteme de monitorizare sofisticate, a unor cadre de evaluare a riscurilor și a unor metodologii de securitate bazate pe teste, se creează o infrastructură digitală mai robustă și mai sigură.

5 CONCLUZII

5.1 Contribuții personale

În domeniul dinamic și în continuă schimbare al securității cibernetice, identificarea vulnerabilităților în timp util și în mod eficient este esențială. Contribuția inițială a acestui studiu, intitulată "Expunerea timpurie la vulnerabilități", explorează abordări și sisteme noi care încearcă să transforme procesul de detectare și control al vulnerabilităților în materie de securitate cibernetică încă din stadiile lor incipiente. Această secțiune a cercetării cuprinde o colecție de studii sofisticate care, prin combinarea celor mai recente evoluții în domeniul învățării automate și al procesării limbajului natural (NLP), explorează noi teritorii în detectarea vulnerabilităților. Fiecare studiu individual inclus în această contribuție nu numai că abordează problema gestionării eficiente a cantității tot mai mari de amenințări la adresa securității cibernetice, dar prezintă, de asemenea, puncte de vedere și metodologii distincte pentru a îmbunătăți eficacitatea și precizia evaluării vulnerabilităților. Introducerea menționată mai sus pune bazele unei examinări exhaustive a acestor studii, subliniind importanța lor colectivă și individuală în cadrul mai larg al securității cibernetice.

- "Security News Aggregator" introduce un progres substanțial în direcția creării unui cadru care poate selecta și clasifica în mod eficient știrile critice de securitate. Această aplicație este concepută pentru a gestiona administrarea unei cantități substanțiale de date zilnice privind securitatea cibernetică, cu accent pe amenințările de tip "zero-day", pe vulnerabilitățile recent descoperite și pe patch-urile critice.
- "Early Detection of Vulnerabilities from News Websites Using Machine Learning Models" stabilește un model de identificare a vulnerabilităților cibernetice emergente în articolele de știri, extinzând astfel această traiectorie. Acuratețea acestui model, care utilizează Mașini vectoriale de suport, clasificatori Multinomial Naïve Bayes și un model BERT ajustat fin, este foarte ridicată. Acest rezultat validează eficacitatea procesării limbajului natural (NLP) în detectarea timpurie a vulnerabilităților.
- "Yggdrasil – A CSCL System for the Early Detection of Cybernetic Vulnerabilities" prezintă un sistem automatizat de învățare colaborativă în domeniul securității cibernetice pentru identificarea amenințărilor din tweet-uri (mesajele postate în cadrul platformei Twitter). Prin utilizarea modelului lingvistic BERT pentru a analiza tweet-urile care sunt conectate la articole de securitate cibernetică, acest sistem demonstrează o acuratețe remarcabilă, subliniind astfel potențialul învățării prin transfer în acest domeniu.
- Abordarea denumită "Severity Prediction of Software Vulnerabilities based on their Text Description" redirecționează atenția către anticiparea severității vulnerabilității. Prin

utilizarea unei metodologii de învățare profundă și a unui cadru de învățare multitask care încorporează un model BERT preformat, această cercetare reușește să prevadă cu succes scorurile de gravitate bazate exclusiv pe descrierile textuale ale vulnerabilităților cu o precizie remarcabilă.

- În articolul "Extracting Exploits and Attack Vectors from Cybersecurity News using NLP" se propune o nouă metodologie pentru a eticheta automat articolele referitoare la vulnerabilități și atacuri cibernetice. Prin utilizarea recunoașterii entităților numite, această cercetare extrage și clasifică în mod eficient datele critice referitoare la vulnerabilitățile recent descoperite, îmbunătățind astfel înțelegerea vectorilor de atac și a exploatărilor.
- Lucrarea "CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques" abordează problema corelării CVE-urilor cu metodologiile de atac. Utilizând tehnicile MITRE ATT&CK pentru a adnota vulnerabilitățile critice (CVE) și dezvoltând modele, inclusiv modele lingvistice bazate pe BERT, acest efort a automatizat cu succes stabilirea acestor conexiuni vitale.

În domeniul divers al securității cibernetice, înțelegerea și evaluarea riscurilor sunt foarte importante pentru a proteja infrastructurile IT vitale. Contribuția următoare, intitulată "Tendințe în materie de vulnerabilități și tactici de atac", investighează metodologii noi pentru identificarea și controlul amenințărilor la adresa securității cibernetice. Acest segment cuprinde o colecție de articole de cercetare care examinează în detaliu complexitatea atacurilor cibernetice, aplicarea honeypots și honeytokens și evaluarea tendințelor în materie de securitate cibernetică. Obiectivul principal al fiecărui studiu este de a spori înțelegerea în ceea ce privește metodologiile de atac și de a concepe sisteme sofisticate care pot identifica și atenua amenințările cibernetice. Prin implementarea unor tehnologii avansate și a unor abordări analitice, aceste eforturi de cercetare aduc contribuții substanțiale la domeniul securității cibernetice, prezentând perspective noi asupra acțiunilor actorilor rău intenționați și a evoluției pericolelor cibernetice. Această secțiune introductivă oferă o prezentare cuprinzătoare a studiilor menționate mai sus, stabilind cadrul pentru o examinare aprofundată a abordărilor, rezultatelor și ramificațiilor acestora în cadrul domeniului mai larg al evaluării riscurilor în materie de securitate cibernetică.

- Lucrarea de cercetare intitulată "HUNT: Using Honeytokens to Understand and Influence the Execution of an Attack" prezintă un nou sistem de detectare a intruziunilor care utilizează honeypots și honeytokens. Acest sistem demonstrează că este capabil să facă diferența între atacurile la scară largă, fără scop, și pericolele mai specifice, cu țintă precisă. Cercetarea se străduiește să clasifice atacurile, să înțeleagă motivațiile atacatorilor, să colecteze probe criminalistice și, în cele din urmă, să elimine amenințarea prin construirea de capcane atractive. Prin desfășurarea de honeytokens interconectați, fiecare având un nivel unic de dificultate de exploatare, se poate crea un scenariu exhaustiv pentru a evalua capacitățile unui atacator.
- Obiectivul proiectului "Web Application Honeypot Published in the Wild" este de a dezvolta un sistem inteligent capabil să identifice atacurile cibernetice și să obțină cunoștințe

despre tehnicile de penetrare. Ca parte a acestui sistem integrat în infrastructura cibernetică, sunt construite honeypot-uri asemănătoare provocărilor de tip "Capture the Flag". Concluziile studiului oferă informații despre comportamentul atacatorilor, care se bazează pe observații ale interacțiunilor atât automate, cât și umane cu honeypot-ul în timpul expunerii acestuia în internet timp de două luni.

- "What Are the Latest Cybersecurity Trends? A Case Study Grounded in Language Models" identifică tendințele majore din știrile despre securitate prin utilizarea procesării limbajului natural, mai exact a modelului de limbaj RoBERTa. Cercetarea grupează articolele în clustere prin analizarea a 2264 de articole folosind încorporări de text, reducerea dimensionalității și gruparea pe subiecte. Această abordare facilitează o evaluare a progresului și a semnificației diverselor tendințe în materie de securitate cibernetică.
- Contribuția "Analysis of Emergent Vulnerability Trends in Cybersecurity News" oferă asistență în prioritizarea actualizării software-ului prin examinarea tendințelor în materie de vulnerabilitate. Această investigație prezintă o colecție extinsă de articole de știri din domeniul securității cibernetice care au fost adnotate cu minuțiozitate, pentru a fi apoi procesate prin arhitecturi Transformer. Utilizând tehnici de grupare, modelele rafinate clasifică articolele ca fiind relevante sau lipsite de importanță și descoperă modele referitoare la expunerea furnizorilor de software. Integrarea acestui sistem facilitează eforturile zilnice de cercetare și investigare ale analiștilor în domeniul securității cibernetice.

Într-o epocă caracterizată de proliferarea și sofisticarea tot mai mare a amenințărilor la adresa securității cibernetice, strategiile proactive de apărare sunt esențiale. "Apărare cibernetică proactivă - Gestionarea vulnerabilităților și prioritizarea eforturilor de remediere", cea de-a treia contribuție a acestei cercetări, se axează pe avansarea și implementarea unor sisteme și metodologii sofisticate concepute pentru a supraveghea și atenua în mod eficient vulnerabilitățile de securitate cibernetică. Acest segment cuprinde cercetări care examinează complexitatea infrastructurilor de date contemporane, obstacolele prezentate de Internetul obiectelor (IoT) și nuanțele evaluării riscurilor în domeniul securității cibernetice. Aceste studii urmăresc să îmbunătățească capacitatea profesioniștilor din domeniul securității cibernetice de a detecta și de a rezolva în mod proactiv vulnerabilitățile prin dezvoltarea unor cadre și modele noi. Ca urmare, postura de securitate a organizațiilor este consolidată. Introducerea menționată mai sus stabilește bazele unei examinări cuprinzătoare a acestor studii, subliniind contribuțiile lor la o strategie mai proactivă și mai bine informată în ceea ce privește securitatea cibernetică.

- "CODA Footprint Continuous Security Management Platform" prezintă o soluție cuprinzătoare pentru auditarea și analiza în timp real a serviciilor critice ale unei companii. Această platformă este menită să garanteze că serviciile esențiale ale organizației sunt suficient de bine protejate și că defensivele de securitate a informațiilor rămân operaționale în permanență. Aceasta abordează dificultățile prezentate de proliferarea serviciilor cloud, de încorporarea diverselor tipuri de dispozitive și de politici precum "bring your own device" (BYOD), care au amplificat substanțial complexitatea administrării securității cibernetice.

- Articolul "Analyzing Risk Evaluation Frameworks and Risk Assessment Methods" discută importanța tot mai mare a defensivelor cibernetice, pe măsură ce numărul atacurilor cibernetice, al vulnerabilităților și al expunerilor de date continuă să crească. Cercetarea subliniază obstacolele pe care le întâmpină inginerii de securitate atunci când încearcă să cuantifice impactul financiar al atacurilor cibernetice și complexitatea cu care se confruntă atunci când evaluează expunerea la risc a organizațiilor lor. Acest studiu evidențiază necesitatea implementării unor metodologii îmbunătățite în mediul de afaceri și în cel academic.
- "Why IoT Security Is Failing. The Need for a Test Driven Security Approach" explorează riscurile și complexitățile de securitate inerente Internetului obiectelor (IoT) în evoluția sa rapidă. Studiul prezintă un cadru pentru monitorizarea și testarea securității aplicațiilor Internet of Things (IoT). Acesta susține utilizarea unei metodologii bazate pe testare pentru a evalua securitatea pe parcursul întregului ciclu de dezvoltare. Folosind această strategie, sperăm să combatem formele noi de atacuri cibernetice care apar în ecosistemul IoT.
- Soluția software propusă în cadrul studiului "Probability and Attack Graph Models in Contextual Risk Scoring System" reprezintă o abordare globală a gestionării și cuantificării riscurilor în rețelele de calculatoare. Această soluție cuprinde abordări noi pentru colectarea, procesarea și evaluarea datelor de la dispozitivele de rețea, care utilizează modele de grafice de atac și modele bazate pe probabilități. Un scor de rețea este generat ca un evaluator cantitativ al expunerii la risc a rețelei; acesta oferă o metodă fiabilă și eficientă de evaluare a securității rețelelor de calculatoare.
- Cercetarea prezentată în "Contextual Remediations Prioritization System Designed to Implement Theoretical Principles of CVSS v4" introduce o abordare nouă pentru prioritizarea vulnerabilităților în infrastructurile cibernetice, dezvoltată pentru a trata provocările noii versiuni CVSS v4. Această metodă valorifică punctajul dinamic și informațiile contextuale, urmărind o strategie de prioritizare mai eficientă. Aceasta răspunde la neajunsurile soluțiilor actuale de gestionare a riscurilor vulnerabilităților, promițând o securitate sporită prin identificarea și abordarea cu acuratețe a vulnerabilităților.

Prima contribuție, intitulată "Expunerea timpurie la vulnerabilități", conține o metodologie cuprinzătoare și cu multiple fațete în ceea ce privește securitatea cibernetică, cu un accent deosebit pe gestionarea strategică și identificarea la timp a vulnerabilităților. Prin intermediul unei secvențe de investigații de pionierat, acest studiu nu numai că sporește înțelegerea existentă a detectării și gestionării vulnerabilităților, dar stabilește, de asemenea, o bază pentru viitoarele progrese în acest domeniu. Încorporarea unor metodologii sofisticate de învățare automată, în special a modelelor NLP și BERT, reprezintă un progres substanțial în gestionarea eficientă a riscurilor de securitate cibernetică. În ansamblu, aceste studii oferă practicienilor din domeniul securității cibernetice informații și instrumente valoroase care facilitează o abordare mai informată și proactivă a provocărilor tot mai complexe și mai frecvente în materie de securitate cibernetică. Rezultatele și abordările prezentate în această contribuție sunt poziționate pentru a genera o îmbunătățire consistentă care să conducă la un spațiu digital

mai sigur.

A doua contribuție, intitulată "Tendințe în materie de vulnerabilități și tactici de atac", oferă un cadru holistic pentru înțelegerea și controlul riscurilor de securitate cibernetică. Prin realizarea unui corpus extins de cercetări, acest studiu contribuie la avansarea cunoștințelor privind metodologiile utilizate în atacurile cibernetice și prezintă abordări noi pentru identificarea și reducerea riscurilor. Utilizarea tehnologiilor de ultimă generație, inclusiv honeytokens, honeypots și modele lingvistice sofisticate, dovedește capacitatea acestor instrumente de a face diferența între o multitudine de amenințări cibernetice. Perspectivele derivate din aceste studii nu numai că sporesc corpul de cunoștințe teoretice din domeniu, dar oferă profesioniștilor în domeniul securității cibernetice sisteme și instrumente practice. Descoperirile menționate mai sus joacă un rol crucial în formularea metodologiilor de evaluare a riscurilor, facilitând o reacție mai bine informată și mai eficientă la obstacolele din domeniul securității cibernetice. În general, contribuția face un pas înainte substanțial în ceea ce privește înțelegerea riscurilor de securitate cibernetică și crearea de instrumente care să atenueze eficient aceste riscuri.

Cea de-a treia contribuție, intitulată "Apărare cibernetică proactivă - Gestionarea vulnerabilităților și prioritizarea eforturilor de remediere", reprezintă un progres substanțial în domeniul securității cibernetice. Aceasta întruchipează o metodologie proactivă pentru supravegherea și reducerea riscurilor de securitate cibernetică, concentrându-se în mod special pe obstacolele emergente, cum ar fi securitatea IoT și complexitatea infrastructurilor IT contemporane. Articolele de cercetare cuprinse în această contribuție prezintă cadre și soluții noi care îi ajută pe practicienii din domeniul securității cibernetice în identificarea, evaluarea și prioritizarea vulnerabilităților. Încorporarea acestor metodologii reprezintă un progres semnificativ în protocoalele de securitate cibernetică, redirecționând atenția de la abordări reactive la abordări proactive. Această contribuție nu numai că îmbunătățește înțelegerea teoretică existentă a gestionării vulnerabilităților, dar oferă organizațiilor instrumente și metodologii practice pentru a-și îmbunătăți situația generală de securitate cibernetică. Constatările și cadrele stabilite prin această investigație joacă un rol crucial în direcționarea traiectoriei securității cibernetice în viitor, subliniind necesitatea unei strategii cuprinzătoare și progresive în gestionarea amenințărilor digitale.

5.2 Direcții de cercetare viitoare

În prezent, există o fascinație incontestabilă în jurul modelelor de limbaj în domeniul securității cibernetice, ceea ce reprezintă un domeniu de cercetare emergent, gata să fie explorat. Pe măsură ce reflectăm asupra cursului investigațiilor viitoare, viziunea noastră cuprinde o secvență de obiective ambițioase, dar realizabile, care urmăresc să ne îmbunătățească înțelegerea și capacitățile în acest domeniu esențial.

În ceea ce privește contribuția noastră inițială, sugerăm o metodologie nouă care presupune efectuarea de noi experimente utilizând cele mai recente modele lingvistice apărute în domeniu.

Aceasta presupune antrenarea unor modele de ultimă generație pentru prezicerea severității, cu un accent pe Common Vulnerabilities and Exposures care au fost făcute publice începând cu anul 2022. De asemenea, importanța de a rămâne la curent cu evoluțiile din domeniul securității cibernetice nu poate fi supraestimată, în special cele care apar din domeniile obscure ale Dark Web. În urmărirea obiectivului nostru, intenționăm să realizăm o serie de experimente utilizând arhitecturile LLM și T5 pe un set de date de corespondențe CVE-Mitre ATT&CK recent asamblat, care conține peste 10 000 de intrări. Îmbunătățirea setului nostru de date actual va necesita includerea atentă a unor detalii relevante pentru fiecare intrare, inclusiv articole cuprinzătoare care să explice proprietățile fiecărei expuneri comune a vulnerabilităților și enumerarea slăbiciunilor comune. Acest lucru va avea ca rezultat o îmbunătățire substanțială a eficacității de instruire a modelului.

Contribuția următoare pune accentul pe implementarea pragmatică a cercetării noastre în contexte concrete, din viața reală. Aceasta implică implementarea unui honeypot, care este atent conceput pentru a simula o aplicație autentică, oferind astfel o vizibilitate semnificativă asupra posibilelor riscuri de securitate cibernetică. Propunem ca, în demersul nostru de a acoperi în amănunt progresele în materie de securitate cibernetică, să încorporăm informații dintr-o varietate de surse de știri. Acest lucru ne va îmbunătăți baza de cunoștințe și va cultiva o înțelegere mai sofisticată a amenințărilor emergente. Elementul cheie al abordării propuse de noi este utilizarea metodelor de recunoaștere a entităților pentru a extrage date relevante, inclusiv versiunile de software care au fost compromise, gravitatea vulnerabilității și versiunile sigure. Cunoștințele dobândite prin această procedură vor fi esențiale pentru îmbunătățirea corespondenței dintre versiunile de software sigure și vulnerabile în cadrul sistemului de agenți CODA Footprint, consolidând astfel poziția de securitate în ansamblu.

Cea de-a treia contribuție a noastră vizează transformarea fundamentală a modului în care sunt evaluate și clasificate riscurile de securitate cibernetică. Prin utilizarea Contextual Risk Scoring System, intenționăm să implementăm o metodologie bazată pe probabilități, care ne va spori capacitatea de a clasifica scenariile de atac în ordinea importanței. Pentru a îmbunătăți și mai mult acest demers, vor fi integrate rezultatele scanărilor generate de agenți recent dezvoltați, adaptați pentru sistemele de operare Linux și MacOS. Componenta efortului de remediere va necesita ca Remediations Workflow System să fie supus unui ciclu continuu de testare și analiză. În plus, prin valorificarea colecției extinse de peste trei milioane de aplicații identificate, suntem dedicați construirii unui model NLP care poate prognoza Common Platform Enumeration (CPE) prin analiza formatelor variate ale aplicațiilor. Sistemul de stabilire a priorităților va fi îmbunătățit prin încorporarea în această inițiativă a datelor provenite din corespondențele CVE - Mitre ATT&CK, dezvăluind astfel scenarii de atac potențial periculoase care necesită o atenție imediată. În cele din urmă, o examinare cuprinzătoare a atacurilor de tip "kill chain", integrând informații din Adversarial Tactics, Techniques, and Common Knowledge (Tactici, tehnici și cunoștințe comune ale adversarilor), precum și din Contextual Risk Scoring System (Sistemul de evaluare a riscurilor contextuale), va stabili o bază fundamentală pentru un cadru de securitate cibernetică mai robust și mai adaptabil.

Prin aceste eforturi concertate, obiectivul nostru dublu este de a lărgi limitele investigației în domeniul securității cibernetice și de a crea un peisaj digital mai robust.

LISTA DE PUBLICAȚII

Jurnale

- **O. Grigorescu**, A. Nica, M. Dascalu, R. Rughinis. CVE2ATT&CK: BERT-Based Mapping of CVEs to MITRE ATT&CK Techniques. Algorithms. 2022; 15(9):314.
  https://doi.org/10.3390/a15090314
  WOS:000858120500001; IF(2022)=2.3
- **O. Grigorescu**, L. Botezatu, A. Mutu, D. Turcanu. Contextual Remediations Prioritization System Designed to Implement Theoretical Principles of CVSS v4
  (Acceptat pentru publicare)
- I Branescu, **O. Grigorescu**, M. Dascalu. Mapping Common Vulnerabilities and Exposures to MITRE ATT&CK Tactics. Advances in Cybersecurity and Reliability. 2024
  (Acceptat pentru publicare)
- C. Săndescu, A. Dinisor, C-V. Vladescu, **O. Grigorescu**, D. Corlatescu , M. Dascalu, R. Rughinis, Extracting Exploits and Attack Vectors from Cybersecurity News using NLP, Buletin UPB 2022
  WOS:000805648400006
- **O. Grigorescu**, V. Vitan, D. Iorga, M. Dascalu, and R. Rughinis. Analysis of Emergent Vulnerability Trends in Cybersecurity News
  (În process de publicare și indexare)

Conferințe

- **O. Grigorescu**, C. Săndescu and R. Rughiniș, "CODA footprint continuous security management platform", 2016 15th RoEduNet Conference: Networking in Education and Research, Bucharest, 2016, pp. 1-5, doi: 10.1109/RoEduNet.2016.7753223.
  WOS:000390713800024
- Sandescu, C., Rughinis, R., **Grigorescu, O.** (2017). HUNT: Using Honeytokens To Understand and Influence The Execution Of An Attack. In Proc. eLSe 2017 – The International Scientific Conference eLearning and Software for Education, Vol. 1, p. 511, Bucharest, "Carol I" National Defence University
- C. Săndescu, **O. Grigorescu**, R. Rughiniș, R. Deaconescu and M. Calin, "Why IoT security is failing. The Need of a Test Driven Security Approach", 2018 17th RoEduNet Conference: Networking in Education and Research (RoEduNet), Cluj-Napoca, 2018, pp. 1-6, doi: 10.1109/ROEDUNET.2018.8514135.
  WOS:000517570500013

- R. E. Radu, **O. Grigorescu** and R. V. Rughiniș, "Security News Aggregator", 2019 18th RoEduNet Conference: Networking in Education and Research (RoEduNet), Galati, Romania, 2019, pp. 1-8, doi: 10.1109/ROEDUNET.2019.8909609.
  WOS:000520513500024
- D. Iorga, D.Corlătescu, **O. Grigorescu**, C. Săndescu, M. Dascălu, R. Rughiniș "Early Detection of Vulnerabilities from News Websites using Machine Learning Models", 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Romania, 2020
  WOS:000654265900006
- R. Radu, C. Săndescu, **O. Grigorescu**, R. Rughiniș "Analyzing Risk Evaluation Frameworks and Risk Assessment Methods", 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Romania, 2020
  WOS:000654265900028
- **O. Grigorescu**, C. Săndescu, A. Caba "Web Application Honeypot Published in the Wild", 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), Romania, 2020
  WOS:000654265900020
- D. Iorga, D.Corlătescu, **O. Grigorescu**, C. Săndescu, M. Dascălu, R. Rughiniș "Yggdrasil—early detection of cybernetic vulnerabilities from Twitter", 2021 23rd International Conference on Control Systems and Computer Science (CSCS23) Romania, 2021
- I. Babalau, D. Corlatescu, **O. Grigorescu**, C. Sandescu and M. Dascalu, "Severity Prediction of Software Vulnerabilities based on their Text Description", 2021 23rd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2021, pp. 171-177, doi: 10.1109/SYNASC54541.2021.00037.
  WOS:000786477000026
- C. Vladescu, M. -A. Dinisor, **O. Grigorescu**, D. Corlatescu, C. Sandescu and M. Dascalu, "What are the Latest Cybersecurity Trends? A Case Study Grounded in Language Models", 2021 23rd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2021, pp. 140-146, doi: 10.1109/SYNASC54541.2021.00033.
  WOS:000786477000022
- **O. Grigorescu**, A. Minea, T. Dumitru and R. Rughiniș, "Probability and Attack Graph models in Contextual Risk Scoring System", 2022 21st RoEduNet Conference: Networking in Education and Research (RoEduNet), 2022, pp. 1-9, doi: 10.1109/RoEduNet57163.2022.9921100.

REFERINȚE

[1] S. N. Narayanan, A. Ganesan, K. Joshi, T. Oates, A. Joshi, and T. Finin, "Early detection of cybersecurity threats using collaborative cognition," in *2018 IEEE 4th international conference on collaboration and internet computing (CIC)*. IEEE, 2018, pp. 354–363.

[2] S. Narayanan, Ashwinkumar Ganesan, K. Joshi, T. Oates, A. Joshi, and Timothy W. Finin, "Cognitive Techniques for Early Detection of Cybersecurity Events," *arXiv.org*, 2018.

[3] Eugene Fink, Mehrbod Sharifi, and J. Carbonell, "Application of Machine Learning and Crowdsourcing to Detection of Cybersecurity Threats," 2011.

[4] M. Ahsan, K. E. Nygard, R. Gomes, M. M. Chowdhury, N. Rifat, and J. F. Connolly, "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning – A Review," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 527–555, jul 10 2022.

[5] A. Handa, A. Sharma, and S. K. Shukla, "Machine learning in cybersecurity: A review," *WIREs Data Mining and Knowledge Discovery*, vol. 9, no. 4, feb 17 2019.

[6] S. A. Salloum, M. Alshurideh, A. Elnagar, and K. Shaalan, *Machine Learning and Deep Learning Techniques for Cybersecurity: A Review*. Springer International Publishing, 2020, pp. 50–57.

[7] A. Salih, S. T. Zeebaree, S. Ameen, A. Alkhyyat, and H. M. Shukur, "A Survey on the Role of Artificial Intelligence, Machine Learning and Deep Learning for Cybersecurity Attack Detection," in *2021 7th International Engineering Conference "Research & Innovation amid Global Pandemic" (IEC)*. IEEE, feb 24 2021.

[8] S. B. Son, S. Park, H. Lee, Y. Kim, D. Kim, and J. Kim, "Introduction to MITRE ATT&CK: Concepts and use cases," in *2023 International Conference on Information Networking (ICOIN)*, 2023, pp. 158–161.

[9] M. Ahmed, S. Panda, C. Xenakis, and E. Panaousis, "MITRE ATT&CK-driven cyber risk assessment," in *Proceedings of the 17th International Conference on Availability, Reliability and Security*, ser. ARES '22. New York, NY, USA: Association for Computing Machinery, 2022. [Online]. Available: https://doi.org/10.1145/3538969.3544420

[10] T. Wang, S. Qin, and K. P. Chow, "Towards vulnerability types classification using pure self-attention: A common weakness enumeration based approach," in *2021 IEEE 24th*

International Conference on Computational Science and Engineering (CSE), 2021, pp. 146–153.

[11] F. Alenezi and C. P. Tsokos, "Machine learning approach to predict computer operating systems vulnerabilities," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*, 2020, pp. 1–6.

[12] F. N. Alenezi and T. Mehmood, "Data-driven predictive model of windows 10's vulnerabilities," in *2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME)*, 2022, pp. 1–5.

[13] C. Elbaz, L. Rilling, and C. Morin, "Fighting n-day vulnerabilities with automated cvss vector prediction at disclosure," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3407023.3407038

[14] ——, "Towards automated risk analysis of "one-day" vulnerabilities," in *RESSI 2019-Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*, 2019, pp. 1–3.

[15] A. K. S. Ruchi Sharma and H. Pham, "Software security evaluation using multilevel vulnerability discovery modeling," *Quality Engineering*, vol. 35, no. 2, pp. 341–352, 2023. [Online]. Available: https://doi.org/10.1080/08982112.2022.2132404

[16] P. Kuehn, D. N. Relke, and C. Reuter, "Common vulnerability scoring system prediction based on open source intelligence information sources," 2022.

[17] A. Bonandir and S. Yussof, "An analysis of common vulnerability and exposure (cve) of software products in the year 2016," *International Journal of Advanced Science and Technology*, vol. 112, pp. 157–166, 2018.

[18] M. Vanamala, X. Yuan, and K. Roy, "Topic modeling and classification of common vulnerabilities and exposures database," in *2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, 2020, pp. 1–5.

[19] C.-H. Han and C. Han, "Semi-quantitative cybersecurity risk assessment by blockade and defense level analysis," *Process Safety and Environmental Protection*, vol. 155, pp. 306–316, 11 2021.

[20] Z. Amin, "A practical road map for assessing cyber risk," *Journal of Risk Research*, vol. 22, no. 1, pp. 32–43, 2019. [Online]. Available: https://doi.org/10.1080/13669877.2017.1351467

[21] R. Leszczyna, "Review of cybersecurity assessment methods: Applicability perspective," *Computers & Security*, vol. 108, p. 102376, 9 2021.

[22] J. Crotty and E. Daniel, "Cyber threat: its origins and consequence and the use of qualitative and quantitative methods in cyber risk assessment," *Applied Computing and Informatics*, dec 26 2022.

[23] A. A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler, D. Marchese, and I. Linkov, "Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management," *Risk Analysis*, vol. 40, no. 1, pp. 183–199, sep 5 2017.

[24] I. D. Sánchez-García, J. Mejía, and T. San Feliu Gilabert, "Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation," *Applied Sciences*, vol. 13, no. 1, p. 395, dec 28 2022.

[25] S. F. Ahmed and N. A. Hikal, "A Review of Cyber-security Measuring and Assessment Methods for Modern Enterprises," *JOIV : International Journal on Informatics Visualization*, vol. 3, no. 3, aug 10 2019.

[26] O. Giuca, T. M. Popescu, A. M. Popescu, G. Prostean, and D. E. Popescu, *A Survey of Cybersecurity Risk Management Frameworks*. Springer International Publishing, aug 15 2020, pp. 240–272.

[27] M. Campos, E. Gomes, and R. Machado, "Sensors for detection of cyber threats on industrial environment using a high interaction ics/scada honeynet1," in *2022 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT)*, 2022, pp. 1–5.

[28] K. Chawda and A. D. Patel, "Dynamic & hybrid honeypot model for scalable network monitoring," in *International Conference on Information Communication and Embedded Systems (ICICES2014)*, 2014, pp. 1–5.

[29] Y. Xu, Y. Jiang, L. Yu, and J. Li, "Brief industry paper: Catching iot malware in the wild using honeyiot," in *2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2021, pp. 433–436.

[30] J. Danani and J. Jani, "Honeypot-a tool to trap website hackers," *Proceedings Published in International Journal of Computer Applications®(IJCA)*, pp. 8–13, 2012.

[31] A. Iskhakova, R. Meshcheryakov, A. Iskhakov, and S. Timchenko, "Analysis of the vulnerabilities of the embedded information systems of iot-devices through the honeypot network implementation," in *Proceedings of the IV International research conference "Information technologies in Science, Management, Social sphere and Medicine" (ITSMSSM 2017)*. Atlantis Press, 2017/12, pp. 363–367. [Online]. Available: https://doi.org/10.2991/itsmssm-17.2017.75

[32] M. Keramati, "Dynamic risk assessment system for the vulnerability scoring," *International Journal of Information and Communication Technology Research*, vol. 9, no. 4, pp. 57–68, 2017.

[33] S. Neuhaus and T. Zimmermann, "Security trend analysis with cve topic models," in *2010 IEEE 21st International Symposium on Software Reliability Engineering*, 2010, pp. 111–120.

[34] G. Spanos, A. Sioziou, and L. Angelis, "Wivss: A new methodology for scoring information systems vulnerabilities," in *Proceedings of the 17th Panhellenic Conference on Informatics*, ser. PCI '13. New York, NY, USA: Association for Computing Machinery, 2013, p. 83–90. [Online]. Available: https://doi.org/10.1145/2491845.2491871

[35] U. Bartwal, S. Mukhopadhyay, R. Negi, and S. Shukla, "Security orchestration, automation, and response engine for deployment of behavioural honeypots," in *2022 IEEE Conference on Dependable and Secure Computing (DSC)*. IEEE, 2022, pp. 1–8.

[36] F. Mayorga, J. Vargas, E. Álvarez, and H. D. Martinez, "Honeypot network configuration through cyberattack patterns," in *2019 International Conference on Information Systems and Computer Science (INCISCOS)*, 2019, pp. 150–155.

[37] R. Colbaugh and K. Glass, "Proactive defense for evolving cyber threats," in *Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 7 2011.

[38] A. Marotta and M. McShane, "Integrating a Proactive Technique Into a Holistic Cyber Risk Management Approach," *Risk Management and Insurance Review*, vol. 21, no. 3, pp. 435–452, 12 2018.

[39] P. Katsumata, J. Hemenway, and W. Gavins, "Cybersecurity risk management," in *2010 - MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*. IEEE, 10 2010.

[40] K.-J. Huang and K.-H. Chiang, "Toward a Self-Adaptive Cyberdefense Framework in Organization," *SAGE Open*, vol. 11, no. 1, p. 215824402098885, 1 2021.

[41] A. S. Makaryan and M. M. Putyato, "Conceptual Approach to the Implementation of the Proactive Defense Subsystem of the Operational Cybersecurity Center," in *2021 XXIV International Conference on Soft Computing and Measurements (SCM)*. IEEE, may 26 2021.

[42] K. G. Crowther, Y. Y. Haimes, and M. E. Johnson, "Principles for Better Information Security through More Accurate, Transparent Risk Scoring," *Journal of Homeland Security and Emergency Management*, vol. 7, no. 1, jan 11 2010.

[43] Humza Naseer, Atif Ahmad, S. Maynard, and G. Shanks, "Cybersecurity Risk Management Using Analytics: A Dynamic Capabilities Approach," *International Conference on Interaction Sciences*, 2018.

[44] Y. Badr, F. Biennier, and S. Tata, "The Integration of Corporate Security Strategies in Collaborative Business Processes," *IEEE Transactions on Services Computing*, vol. 4, no. 3, pp. 243–254, 7 2011.

[45] S. Cho, I. Han, H. Jeong, J. Kim, S. Koo, H. Oh, and M. Park, "Cyber kill chain based threat taxonomy and its application on cyber common operational picture," in *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*. IEEE, 2018, pp. 1–8.

[46] L. Sadlek, P. Čeleda, and D. Tovarňák, "Identification of attack paths using kill chain and attack graphs," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. IEEE, 2022, pp. 1–6.

[47] S. Yang, Y. Shi, and F. Guo, "Risk assessment of industrial internet system by using game-attack graphs," in *2019 IEEE 5th International Conference on Computer and Communications (ICCC)*. IEEE, 2019, pp. 1660–1663.

[48] T. W. Purboyo and Kuspriyanto, "A review of network security metrics," 2013. [Online]. Available: https://api.semanticscholar.org/CorpusID:212463847

[49] A. Kundu, N. Ghosh, I. Chokshi, and S. K. Ghosh, "Analysis of attack graph-based metrics for quantification of network security," in *2012 Annual IEEE India Conference (INDICON)*. IEEE, 2012, pp. 530–535.

[50] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, "A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow," *Ieee Access*, vol. 6, pp. 8599–8609, 2018.

[51] I. Shrestha and M. Hale, "Detecting dynamic security threats in multi-component iot systems," 2019.

[52] S.-S. Yoon, D.-Y. Kim, K.-K. Kim, and I.-C. Euom, "Vulnerability exploitation risk assessment based on offensive security approach," *Applied Sciences*, vol. 13, no. 22, p. 12180, 2023.

[53] S. Mishra, A. Albarakati, and S. K. Sharma, "Cyber threat intelligence for iot using machine learning," *Processes*, vol. 10, no. 12, p. 2673, 2022.

[54] X. Duan, M. Ge, T. H. M. Le, F. Ullah, S. Gao, X. Lu, and M. A. Babar, "Automated security assessment for the internet of things," in *2021 IEEE 26th Pacific Rim International Symposium on Dependable Computing (PRDC)*. IEEE, 2021, pp. 47–56.

[55] G. George and S. M. Thampi, "A graph-based decision support model for vulnerability analysis in iot networks," in *Security in Computing and Communications: 6th International Symposium, SSCC 2018, Bangalore, India, September 19–22, 2018, Revised Selected Papers 6*. Springer, 2019, pp. 1–23.

[56] P. Griffioen and B. Sinopoli, "Assessing risks and modeling threats in the internet of things," *arXiv preprint arXiv:2110.07771*, 2021.

[57] V. G. Massaro, L. Capacci, and R. Montanari, "Towards context-aware risk assessment scoring system for iot/iiot devices," 2023.

[58] R. Kasprzyk and A. Stachurski, "A concept of standard-based vulnerability management automation for it systems," 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:114936229

[59] D. Waltermire, S. D. Quinn, H. Booth, K. Scarfone, and D. Prisaca, "The technical specification for the security content automation protocol (scap): Scap version 1.3," 2016. [Online]. Available: https://api.semanticscholar.org/CorpusID:69690628

[60] U. Tariq, A. O. Aseeri, M. S. Alkatheiri, and Y. Zhuang, "Context-aware autonomous security assertion for industrial iot," *IEEE Access*, vol. 8, pp. 191 785–191 794, 2020.

[61] P. Anand, Y. Singh, A. K. Selwal, P. K. Singh, and K. Z. Ghafoor, "Ivqfiot: An intelligent vulnerability quantification framework for scoring internet of things vulnerabilities," *Expert Systems*, vol. 39, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:239202722

[62] V. Malik and S. Singh, "Security risk management in iot environment," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 22, pp. 697 – 709, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:203320904

[63] S. Rizvi, N. McIntyre, and J. Ryoo, "Computing security scores for iot device vulnerabilities," *2019 International Conference on Software Security and Assurance (ICSSA)*, pp. 52–59, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:231851175

[64] N. A. Khan, A. Awang, and S. A. A. Karim, "Security in internet of things: A review," *IEEE access*, vol. 10, pp. 104 649–104 670, 2022.

[65] J. Zheng, X.-s. Zhang, and X.-h. Pan, "A host deployed vulnerability assessment system based on oval," in *2010 International Conference on Computer Application and System Modeling (ICCASM 2010)*, vol. 2. IEEE, 2010, pp. V2–123.

[66] G. Lee, I.-s. Ko, and T.-h. Kim, "A vulnerability assessment tool based on oval in system block model," in *International Conference on Intelligent Computing*. Springer, 2006, pp. 1115–1120.

[67] K. Papachristou, T.-I. Theodorou, S. Papadopoulos, A. Protogerou, A. Drosou, and D. Tzovaras, "Runtime and routing security policy verification for enhanced quality of service of iot networks," *2019 Global IoT Summit (GIoTS)*, pp. 1–6, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:198145865

[68] M. Dayalan, "Cyber risks, the growing threat," *ResearchGate*, 2017.

[69] Z. M. Smith and E. Lostri, *The hidden costs of cybercrime*. McAfee, 2020.

[70] M. Fichtenkamm, G. F. Burch, and J. Burch, "Cybersecurity in a covid-19 world: Insights on how decisions are made," *ISACA Journal*, vol. 2, no. 1, pp. 1–11, 2022. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world

[71] K. Bissell, R. Lasalle, and P. Dal Cin, "2019 cost of cybercrime study— 9th annual— accenture," *Ninth Annual Cost of Cybercrime Study*, 2019. [Online]. Available: https://www.accenture.com/us-en/insights/security/cost-cybercrimestudy.

[72] L. Ponemon, "Cost of data breach study," *Ponemon Institute*, 2017.

[73] L. Columbus, "Roundup of cybersecurity forecasts and market estimates," Forbes, 2020. [Online]. Available: https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-ofcybersecurity-forecasts-and-market-estimates

[74] A. Talalaev, "Website hacking statistics you should know in 2021. patchstack. retrieved february 2, 2022," 2021. [Online]. Available: https://patchstack.com/website-hackingstatistics/

[75] "Faqs - cve," The MITRE Corporation. [Online]. Available: https://cve.mitre.org/about/faqs.html

[76] F. Cremer, B. Sheehan, M. Fortmann, A. N. Kia, M. Mullins, F. Murphy, and S. Materne, "Cyber risk and cybersecurity: a systematic review of data availability," *The Geneva Papers on risk and insurance-Issues and practice*, vol. 47, no. 3, pp. 698–736, 2022.

[77] "Common vulnerability scoring system sig," Forum of Incident Response and Security Teams. [Online]. Available: https://www.first.org/cvss

[78] "Common vulnerabilities and exposures," MITRE, 2023. [Online]. Available: https://cve.mitre.org/

[79] S. FIRST, "Common vulnerability scoring system sig," 2018. [Online]. Available: https://www.first.org/cvss

[80] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021.

[81] F. Ö. Sönmez, "Classifying common vulnerabilities and exposures database using text mining and graph theoretical analysis," *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*, pp. 313–338, 2021.

[82] E. Hemberg, J. Kelly, M. Shlapentokh-Rothman, B. Reinstadler, K. Xu, N. Rutar, and U.-M. O'Reilly, "Linking threat tactics, techniques, and patterns with defensive weaknesses, vulnerabilities and affected platform configurations for cyber hunting," *arXiv preprint arXiv:2010.00533*, 2020.

[83] R. Martin, S. Christey, and D. Baker, "A progress report on the cve initiative," in *Proceedings of the 14th Annual Computer Security Incident Handling Conference (FIRST)*, 2002.

[84] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, "Mitre att&ck: Design and philosophy," in *Technical report*. The MITRE Corporation, 2018.

[85] "Live cyber attack threat map," ThreatCloud Intelligence – Threatclqud, 2019. [Online]. Available: https://threatmap.checkpoint.com/ThreatPortal/livemap.html

[86] "Cyber threat intelligence," SecurityWizardry, 2019. [Online]. Available: https://www.securitywizardry.com/radar.htm

[87] B. Cui, S. Moskal, H. Du, and S. J. Yang, "Who shall we follow in twitter for cyber vulnerability?" in *Social Computing, Behavioral-Cultural Modeling and Prediction: 6th International Conference, SBP 2013, Washington, DC, USA, April 2-5, 2013. Proceedings 6*. Springer, 2013, pp. 394–402.

[88] S. Trabelsi, H. Plate, A. Abida, M. Aoun, A. Zouaoui, C. Missaoui, S. Gharbi, and A. Ayari, "Monitoring software vulnerabilities through social networs analysis," in *12th International Conference on Security and Cryptography, SECRYPT*, 2015.

[89] 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)*. IEEE, 2016, pp. 860–867.

[90] 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)*, 2015, pp. 1041–1056.

[91] T. Dumitras, "How to predict which vulnerabilities will be exploited," 2019.

[92] 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*, vol. 32, no. 1, 2018.

[93] O. C. Moholth, R. Juric, and K. M. McClenaghan, "Detecting cyber security vulnerabilities through reactive programming," in *Proceedings of the 52nd Hawaii International Conference on System Sciences, Grand Wailea, Maui, Hawaii, USA*, 2019, pp. 1–10.

[94] "Glossary of security terms — sans institute." [Online]. Available: https://www.sans.org/security-resources/glossary-of-terms/

[95] "Vocabulary — niccs - national initiative for cybersecurity careers and studies," Cybersecurity and Infrastructure Security Agency. [Online]. Available: https://niccs.us-cert.gov/about-niccs/glossary

[96] "Cybersecurity glossary and vocabulary — cybrary." [Online]. Available: https://www.cybrary.it/cybersecurity-glossary

[97] C. Hobbs, M. Moran, and D. Salisbury, *Open source intelligence in the twenty-first century: new approaches and opportunities*. Springer, 2014.

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

[99] D. R. Hayes and F. Cappa, "Open-source intelligence for risk assessment," *Business Horizons*, vol. 61, no. 5, pp. 689–697, 2018.

[100] 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. 42 156–42 168, 2019.

[101] 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*, 2019, pp. 3143–3152.

[102] 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)*. IEEE, 2019, pp. 1–8.

[103] 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)*. IEEE, 2018, pp. 1–4.

[104] 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.

[105] 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*, 2017, pp. 103–115.

[106] 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*, 2016, pp. 755–766.

[107] 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)*. IEEE, 2017, pp. 3648–3656.

[108] S. Lai, L. Xu, K. Liu, and J. Zhao, "Recurrent convolutional neural networks for text classification," in *Proceedings of the AAAI conference on artificial intelligence*, vol. 29, no. 1, 2015.

[109] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural Computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[110] T. K. Landauer and S. T. Dumais, "A solution to plato's problem: The latent semantic analysis theory of acquisition, induction, and representation of knowledge." *Psychological review*, vol. 104, no. 2, p. 211, 1997.

[111] J. Lafferty, A. McCallum, and F. C. Pereira, "Conditional random fields: Probabilistic models for segmenting and labeling sequence data," 2001.

[112] H. Schütze, C. D. Manning, and P. Raghavan, *Introduction to information retrieval*. Cambridge University Press Cambridge, 2008, vol. 39.

[113] Z. S. Harris, "Distributional structure," *Word*, vol. 10, no. 2-3, pp. 146–162, 1954.

[114] T. Joachims, "Text categorization with support vector machines: Learning with many relevant features," in *European conference on machine learning*. Springer, 1998, pp. 137–142.

[115] J. A. Suykens and J. Vandewalle, "Least squares support vector machine classifiers," *Neural processing letters*, vol. 9, pp. 293–300, 1999.

[116] A. M. Kibriya, E. Frank, B. Pfahringer, and G. Holmes, "Multinomial naive bayes for text categorization revisited," in *AI 2004: Advances in Artificial Intelligence: 17th Australian Joint Conference on Artificial Intelligence, Cairns, Australia, December 4-6, 2004. Proceedings 17*. Springer, 2005, pp. 488–499.

[117] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," in *Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Minneapolis, MN, USA*, 2018, pp. 4171—4186.

[118] S. Khan, "Bert, roberta, distilbert, xlnet—which one to use," *Towards Data Science*, 2019. [Online]. Available: https://towardsdatascience.com/bertroberta-distilbert-xlnet-which-one-to-use-3d5ab82ba5f8

[119] "The hacker news — 1 trusted cybersecurity news site." [Online]. Available: https://thehackernews.com/

[120] "Threatpost — the first stop for security news." [Online]. Available: https://threatpost.com/

[121] "Ars technica." [Online]. Available: https://arstechnica.com/

[122] "Security affairs - read, think, share ... security is everyone's responsibility." [Online]. Available: https://securityaffairs.co/wordpress/

[123] Scikit-learn, "Countvectorizer." [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.feature_extraction.text.CountVectorizer.html

[124] L. Lipponen, "Exploring foundations for computer-supported collaborative learning," in *Computer support for collaborative learning*. Routledge, 2023, pp. 72–81.

[125] P. Dillenbourg, "What do you mean by collaborative learning?" 1999.

[126] Á. M. De Jesús and I. F. Silveira, "Game-based collaborative learning framework for computational thinking development," *Revista Facultad de Ingeniería Universidad de Antioquia*, no. 99, pp. 113–123, 2021.

[127] N. Wahyuningtyas and I. Idris, "Increasing geographic literacy through the development of computer supported collaborative learning," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 15, no. 7, pp. 74–85, 2020.

[128] X. Huang, "Improving communicative competence through synchronous communication in computer-supported collaborative learning environments: A systematic review," *Education Sciences*, vol. 8, no. 1, p. 15, 2018.

[129] G. Stahl, "Investigation 2. a theory of group cognition in cscl," in *Theoretical investigations: Philosophical foundations of group cognition*. Springer, 2021, pp. 27–61.

[130] D. Iorga, D. Corlătescu, O. Grigorescu, C. Săndescu, M. Dascălu, and R. Rughiniș, "Early detection of vulnerabilities from news websites using machine learning models," in *2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet)*. IEEE, 2020, pp. 1–6.

[131] A. Halavais, "Computer-supported collaborative learning," *The International Encyclopedia of Communication Theory and Philosophy*, pp. 1–5, 2016.

[132] P. Dillenbourg, S. Järvelä, and F. Fischer, *The evolution of research on computer-supported collaborative learning: From design to orchestration*. Springer, 2009.

[133] H. Jeong, C. E. Hmelo-Silver, and K. Jo, "Ten years of computer-supported collaborative learning: A meta-analysis of cscl in stem education during 2005–2014," *Educational research review*, vol. 28, p. 100284, 2019.

[134] X. Tian and Z. Li, "Collaborative learning for information security topics: A pilot study." in *AMCIS*, 2020.

[135] X. Yuan, T. Zhang, A. A. Shama, J. Xu, L. Yang, J. Ellis, W. He, and C. Waters, "Teaching cybersecurity using guided inquiry collaborative learning," in *2019 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2019, pp. 1–6.

[136] J.-W. Strijbos, "Assessment of (computer-supported) collaborative learning," *IEEE transactions on learning technologies*, vol. 4, no. 1, pp. 59–73, 2010.

[137] J. Roschelle, "A review of the international handbook of computer-supported collaborative learning 2021," 2020.

[138] V. S. Kumar, "Computer-supported collaborative learning: issues for research," in *Eighth annual graduate symposium on Computer Science, University of Saskatchewan*. Citeseer, 1996.

[139] L. Silva, A. J. Mendes, and A. Gomes, "Computer-supported collaborative learning in programming education: A systematic literature review," in *2020 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 2020, pp. 1086–1095.

[140] J. Murphy PhD, E. Sihler, M. Ebben PhD, and G. Wilson, "Building a virtual cybersecurity collaborative learning laboratory (vccll)," in *2014 World Congress in Computer Science, Conference Proceedings: Computer Engineering and Applied Computing*, 2014.

[141] Á. Lédeczi, M. MarÓti, H. Zare, B. Yett, N. Hutchins, B. Broll, P. Völgyesi, M. B. Smith, T. Darrah, M. Metelko *et al.*, "Teaching cybersecurity with networked robots," in *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*, 2019, pp. 885–891.

[142] G. Stahl, T. D. Koschmann, and D. D. Suthers, *Computer-supported collaborative learning*. Citeseer, 2006.

[143] Z. Chen and C. Demmans, "Csclrec: Personalized recommendation of forum posts to support socio-collaborative learning." *International Educational Data Mining Society*, 2020.

[144] D. Zimbra, A. Abbasi, D. Zeng, and H. Chen, "The state-of-the-art in twitter sentiment analysis: A review and benchmark evaluation," *ACM Transactions on Management Information Systems (TMIS)*, vol. 9, no. 2, pp. 1–29, 2018.

[145] M. Thelwall, K. Buckley, G. Paltoglou, D. Cai, and A. Kappas, "Sentiment strength detection in short informal text," *Journal of the American society for information science and technology*, vol. 61, no. 12, pp. 2544–2558, 2010.

[146] M. Neethu and R. Rajasree, "Sentiment analysis in twitter using machine learning techniques," in *2013 fourth international conference on computing, communications and networking technologies (ICCCNT)*. IEEE, 2013, pp. 1–5.

[147] A. Severyn and A. Moschitti, "Twitter sentiment analysis with deep convolutional neural networks," in *Proceedings of the 38th international ACM SIGIR conference on research and development in information retrieval*, 2015, pp. 959–962.

[148] M. Pota, M. Ventura, R. Catelli, and M. Esposito, "An effective bert-based pipeline for twitter sentiment analysis: A case study in italian," *Sensors*, vol. 21, no. 1, p. 133, 2020.

[149] "Sentence transformers, sbert," HuggingFace, 2022. [Online]. Available: https://huggingface.co/sentence-transformers

[150] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg *et al.*, "Scikit-learn: Machine learning in python," *the Journal of machine Learning research*, vol. 12, pp. 2825–2830, 2011.

[151] F. Chollet *et al.*, "Keras: The python deep learning library," *Astrophysics source code library*, pp. ascl–1806, 2018.

[152] M. Honnibal, "Spacy 2: Natural language understanding with bloom embeddings, convolutional neural networks and incremental parsing, sentometrics research," Sentometrics Research. Available at: https://sentometrics-research.com, 2017.

[153] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," *Advances in neural information processing systems*, vol. 30, 2017.

[154] A. Wang, A. Singh, J. Michael, F. Hill, O. Levy, and S. R. Bowman, "Glue: A multi-task benchmark and analysis platform for natural language understanding," *arXiv preprint arXiv:1804.07461*, 2018.

[155] R. Caruana, "Multitask learning: A knowledge-based source of inductive bias1," in *Proceedings of the Tenth International Conference on Machine Learning*. Citeseer, 1993, pp. 41–48.

[156] Z. Han, X. Li, Z. Xing, H. Liu, and Z. Feng, "Learning to predict severity of software vulnerability using only vulnerability description," in *2017 IEEE International conference on software maintenance and evolution (ICSME)*. IEEE, 2017, pp. 125–136.

[157] T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient estimation of word representations in vector space," *arXiv preprint arXiv:1301.3781*, 2013.

[158] Y. Kim, "Convolutional neural networks for sentence classification," *arXiv preprint arXiv:1408.5882*, 2014.

[159] "National vulnerability database nvd - data feeds," National Institute of Standards and Technology. [Online]. Available: https://nvd.nist.gov/vuln/data-feeds

[160] J. X. Morris, E. Lifland, J. Y. Yoo, J. Grigsby, D. Jin, and Y. Qi, "Textattack: A framework for adversarial attacks, data augmentation, and adversarial training in nlp," *arXiv preprint arXiv:2005.05909*, 2020.

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

[162] R. Rehurek, "models.word2vec – word2vec embeddings — gensim." [Online]. Available: https://radimrehurek.com/gensim/models/word2vec.html

[163] M.-T. Luong, H. Pham, and C. D. Manning, "Effective approaches to attention-based neural machine translation," *arXiv preprint arXiv:1508.04025*, 2015.

[164] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," *arXiv preprint arXiv:1409.0473*, 2014.

[165] "Find pre-trained models — kaggle." [Online]. Available: https://www.kaggle.com/models?tfhub-redirect=true

[166] I. Turc, M.-W. Chang, K. Lee, and K. Toutanova, "Well-read students learn better: On the importance of pre-training compact models," *arXiv preprint arXiv:1908.08962*, 2019.

[167] Y. Zhu, R. Kiros, R. Zemel, R. Salakhutdinov, R. Urtasun, A. Torralba, and S. Fidler, "Aligning books and movies: Towards story-like visual explanations by watching movies and reading books," in *Proceedings of the IEEE international conference on computer vision*, 2015, pp. 19–27.

[168] Barkly, "Study reveals 64% of organizations experienced successful endpoint attack in 2018," *Business Wire*, 2018. [Online]. Available: https://www.businesswire.com/news/home/20181016005758/en/Study-Reveals-64-of-Organizations-Experienced-Successful-EndpointAttack-in-2018

[169] A. L. Queiroz, S. Mckeever, and B. Keegan, "Eavesdropping hackers: Detecting software vulnerability communication on social media using text mining," in *The Fourth International Conference on Cyber-Technologies and Cyber-Systems*, 2019, pp. 41–48.

[170] S. Trabelsi, H. Plate, A. Abida, M. M. B. Aoun, A. Zouaoui, C. Missaoui, S. Gharbi, and A. Ayari, "Monitoring software vulnerabilities through social networks analysis," in *2015 12th International Joint Conference on e-Business and Telecommunications (ICETE)*, vol. 4. IEEE, 2015, pp. 236–242.

[171] J. Wei and K. Zou, "Eda: Easy data augmentation techniques for boosting performance on text classification tasks," in *Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference Natural Language Processing, Hong Kong, China*, 2019, pp. 6381—-6387.

[172] V. Atliha and D. Šešok, "Text augmentation using bert for image captioning," *Applied Sciences*, vol. 10, no. 17, p. 5978, 2020.

[173] G. Lample, M. Ballesteros, S. Subramanian, K. Kawakami, and C. Dyer, "Neural architectures for named entity recognition," in *The 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, San Diego California, USA*, 2016, p. 260–270.

[174] X. Wu, S. Lv, L. Zang, J. Han, and S. Hu, "Conditional bert contextual augmentation," in *Computational Science–ICCS 2019: 19th International Conference, Faro, Portugal, June 12–14, 2019, Proceedings, Part IV 19*. Springer, 2019, pp. 84–95.

[175] B. Y. Lin, F. F. Xu, Z. Luo, and K. Zhu, "Multi-channel bilstm-crf model for emerging named entity recognition in social media," in *Proceedings of the 3rd Workshop on Noisy User-generated Text*, 2017, pp. 160–165.

[176] Q. Qiu, Z. Xie, L. Wu, L. Tao, and W. Li, "Bilstm-crf for geological named entity recognition from the geoscience literature," *Earth Science Informatics*, vol. 12, pp. 565–579, 2019.

[177] Q. Zhu, X. Li, A. Conesa, and C. Pereira, "Gram-cnn: a deep learning approach with local context for named entity recognition in biomedical text," *Bioinformatics*, vol. 34, no. 9, pp. 1547–1554, 2018.

[178] "spacy · industrial-strength natural language processing in python." [Online]. Available: https://spacy.io/

[179] J. Serrà and A. Karatzoglou, "Getting deep recommenders fit: Bloom embeddings for sparse binary input/output networks," in *Proceedings of the Eleventh ACM Conference on Recommender Systems*, 2017, pp. 279–287.

[180] K. Zhang, W. Zuo, Y. Chen, D. Meng, and L. Zhang, "Beyond a gaussian denoiser: Residual learning of deep cnn for image denoising," *IEEE transactions on image processing*, vol. 26, no. 7, pp. 3142–3155, 2017.

[181] Y. Liu, M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov, "Roberta: A robustly optimized bert pretraining approach," *arXiv preprint arXiv:1907.11692*, 2019.

[182] L. Ou-Yang, "Newspaper3k: Article scraping & curation—newspaper 0.0. 2 documentation," 2021. [Online]. Available: https://github.com/codelucas/newspaper

[183] "National institute of standards and technology: National vulnerability database (nvd), vulnerability metrics," National Institute of Standards and Technology, US. [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss#

[184] E. Ma, "Github - makcedward/nlpaug: Data augmentation for nlp." [Online]. Available: https://github.com/makcedward/nlpaug

[185] Y. Qi, "Github - qdata/textattack: Textattack is a python framework for adversarial attacks, data augmentation, and model training in nlp https://textattack.readthedocs.io/en/master/." [Online]. Available: https://github.com/QData/TextAttack

[186] "News and advice on the world's latest innovations — zdnet." [Online]. Available: https://www.zdnet.com/

[187] "National institute of standards and technology: National vulnerability database (nvd), nvd dashboard," National Institute of Standards and Technology, US. [Online]. Available: https://nvd.nist.gov/general/nvd-dashboard

[188] "Mapping MITRE ATT&CK® to cves for impact," The Center for Threat-Informed Defense, Bedford, MA, USA. [Online]. Available: https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/mapping-attck-to-cve-for-impact/

[189] J. Baker, "CVE + MITRE ATT&CK to understand vulnerability impact," Medium. [Online]. Available: https://medium.com/mitre-engenuity/cve-mitre-att-ck-to-understand-vulnerability-impact-c40165111bf7

[190] S. Roe, "Using MITRE ATT&CK with threat intelligence to improve vulnerability management." [Online]. Available: https://outpost24.com/blog/Using-mitre-attack-with-threat-intelligence-to-improve-vulnerability-management

[191] B. Ampel, S. Samtani, S. Ullman, and H. Chen, "Linking common vulnerabilities and exposures to the mitre att&ck framework: A self-distillation approach," *arXiv preprint arXiv:2108.01696*, 2021.

[192] A. Kuppa, L. Aouad, and N.-A. Le-Khac, "Linking cve's to mitre att&ck techniques," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–12.

[193] "Threat report ATT&CK mapping (TRAM)," Github. [Online]. Available: https://github.com/center-for-threat-informed-defense/tram/

[194] S. Yoder, "Automating Mapping to ATT&CK: The Threat Report ATT&CK Mapper (TRAM) Tool," Medium. [Online]. Available: https://medium.com/mitre-attack/automating-mapping-to-attack-tram-1bb1b44bda76

[195] M. T. Ribeiro, S. Singh, and C. Guestrin, "Model-agnostic interpretability of machine learning," *arXiv preprint arXiv:1606.05386*, 2016.

[196] O. Grigorescu, "CVE2ATT&CK dataset," TagTog. [Online]. Available: https://www.tagtog.com/readerbench/MitreMatrix/

[197] ——, "CVE2ATT&CK repository," GitHub. [Online]. Available: https://github.com/readerbench/CVE2ATT-CK

[198] "Vulnerability database." [Online]. Available: https://vuldb.com/

[199] "Exploit database-exploits for penetration testers, researchers, and ethical hackers." [Online]. Available: https://www.exploit-db.com/

[200] TagTog, "Api documentation v1." [Online]. Available: https://github.com/tagtog/tagtog-doc/blob/master/API-projects-v1.md

[201] N. Japkowicz and S. Stephen, "The class imbalance problem: A systematic study," *Intelligent data analysis*, vol. 6, no. 5, pp. 429–449, 2002.

[202] TextAttack, "Documentation webpage." [Online]. Available: https://textattack.readthedocs.io/en/latest/index.html

[203] Q. Yanjun, "Textattack. augmentation recipes." [Online]. Available: https://textattack.readthedocs.io/en/latest/3recipes/augmenter_recipes.html

[204] R. Alazaidah and F. K. Ahmad, "Trending challenges in multi label classification," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 10, pp. 127–131, 2016.

[205] "spacy 101: Everything you need to know," spaCy. [Online]. Available: https://spacy.io/usage/spacy-101

[206] G. Tsoumakas, I. Katakis, and I. Vlahavas, "Mining multi-label data," *Data mining and knowledge discovery handbook*, pp. 667–685, 2010.

[207] R. Rifkin and A. Klautau, "In defense of one-vs-all classification," *The Journal of Machine Learning Research*, vol. 5, pp. 101–141, 2004.

[208] G. Tsoumakas and I. Vlahavas, "Random k-labelsets: An ensemble method for multilabel classification," in *European conference on machine learning*. Springer, 2007, pp. 406–417.

[209] I. Rish *et al.*, "An empirical study of the naive bayes classifier," in *IJCAI 2001 workshop on empirical methods in artificial intelligence*, vol. 3, no. 22, 2001, pp. 41–46.

[210] J. Cervantes, F. Garcia-Lamont, L. Rodríguez-Mazahua, and A. Lopez, "A comprehensive survey on support vector machine classification: Applications, challenges and trends," *Neurocomputing*, vol. 408, pp. 189–215, 2020.

[211] "Grid search," Scikit. [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.GridSearchCV.html

[212] D. A. Forsyth, J. L. Mundy, V. di Gesú, R. Cipolla, Y. LeCun, P. Haffner, L. Bottou, and Y. Bengio, "Object recognition with gradient-based learning," *Shape, contour and grouping in computer vision*, pp. 319–345, 1999.

[213] W.-t. Yih, X. He, and C. Meek, "Semantic parsing for single-relation question answering," in *Proceedings of the 52nd Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers)*, 2014, pp. 643–648.

[214] N. Kalchbrenner, E. Grefenstette, and P. Blunsom, "A convolutional neural network for modelling sentences," *arXiv preprint arXiv:1404.2188*, 2014.

[215] "Word representation for cyber security vulnerability domain," Github. [Online]. Available: https://github.com/unsw-cse-soc/Vul_Word2Vec

[216] I. Beltagy, K. Lo, and A. Cohan, "Scibert: A pretrained language model for scientific text," *arXiv preprint arXiv:1903.10676*, 2019.

[217] "Secbert model," HuggingFace. [Online]. Available: https://huggingface.co/jackaduma/SecBERT

[218] "Bce with logit loss," Pytorch. [Online]. Available: https://pytorch.org/docs/stable/generated/torch.nn.BCEWithLogitsLoss.html

[219] Y. Dong, W. Guo, Y. Chen, X. Xing, Y. Zhang, and G. Wang, "Towards the detection of inconsistencies in public security vulnerability reports," in *28th USENIX security symposium (USENIX Security 19)*, 2019, pp. 869–885.

[220] Y. Wang, Q. Yao, J. T. Kwok, and L. M. Ni, "Generalizing from a few examples: A survey on few-shot learning," *ACM computing surveys (csur)*, vol. 53, no. 3, pp. 1–34, 2020.

[221] G. Kasieczka, B. Nachman, D. Shih, O. Amram, A. Andreassen, K. Benkendorfer, B. Bortolato, G. Brooijmans, F. Canelli, J. H. Collins *et al.*, "The lhc olympics 2020 a community challenge for anomaly detection in high energy physics," *Reports on progress in physics*, vol. 84, no. 12, p. 124201, 2021.

[222] "Common weakness enumeration webpage," MITRE, 2023. [Online]. Available: https://cwe.mitre.org/

[223] L. Spitzner, "Honeypots: Catching the insider threat," in *19th Annual Computer Security Applications Conference, 2003. Proceedings.* IEEE, 2003, pp. 170–179.

[224] G. H. Kim and E. H. Spafford, "Experiences with tripwire: Using integrity checkers for intrusion detection," 1994.

[225] A. Harper, E. Balas, and H. Gen III, "The birth of roo," *Black Hat Briefings*, 2005.

[226] N. Provos, "Honeyd-a virtual honeypot daemon," in *10th dfn-cert workshop, hamburg, germany*, vol. 2, 2003, p. 4.

[227] S. Kumar, P. Singh, R. Sehgal, and J. Bhatia, "Distributed honeynet system using gen iii virtual honeynet," *International Journal of Computer Theory and Engineering*, vol. 4, no. 4, p. 537, 2012.

[228] J. Levine, R. LaBella, H. Owen, D. Contis, and B. Culver, "The use of honeynets to detect exploited systems across large enterprise networks," in *IEEE Systems, Man and Cybernetics SocietyInformation Assurance Workshop, 2003.* IEEE, 2003, pp. 92–99.

[229] M. Müter, F. Freiling, T. Holz, and J. Matthews, "A generic toolkit for converting web applications into high-interaction honeypots," *University of Mannheim*, vol. 280, pp. 6–1, 2008.

[230] F. De Gaspari, S. Jajodia, L. V. Mancini, and A. Panico, "Ahead: A new architecture for active defense," in *Proceedings of the 2016 ACM workshop on automated decision making for active cyber defense*, 2016, pp. 11–16.

[231] A. Shabtai, M. Bercovitch, L. Rokach, Y. Gal, Y. Elovici, and E. Shmueli, "Behavioral study of users when interacting with active honeytokens," *ACM Transactions on Information and System Security (TISSEC)*, vol. 18, no. 3, pp. 1–21, 2016.

[232] A. Radovici, R. Cristian, and R. ŞERBAN, "A survey of iot security threats and solutions," in *2018 17th RoEduNet conference: networking in education and research (RoEduNet)*. IEEE, 2018, pp. 1–5.

[233] I. Florea, L. C. Ruse, and R. Rughinis, "Challenges in security in internet of things," in *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)*. IEEE, 2017, pp. 1–5.

[234] I. Florea, R. Rughinis, L. Ruse, and D. Dragomir, "Survey of standardized protocols for the internet of things," in *2017 21st International Conference on Control Systems and Computer Science (CSCS)*. IEEE, 2017, pp. 190–196.

[235] "Know your enemy: Defining virtual honeynets," September 2002. [Online]. Available: http://ivanlef0u.fr/repo/madchat/reseau/defense/DefiningVirtualHoneynets.pdf

[236] I. Livshitz, "What's the difference between a high interaction honeypot and a low interaction honeypot," 2020. [Online]. Available: https://www.guardicore.com/2019/1/high-interaction-honeypot-versus-low-interaction-honeypot/

[237] S. Symanovich, "What is a honeypot? how it can lure cyberattack ers," *NortonLifeLock, May*, vol. 26, 2020. [Online]. Available: https://us.norton.com/internetsecurity-iot-what-is-a-honeypot.html

[238] "Low, medium and high interaction honeypot," January 2019. [Online]. Available: https://www.guardicore.com/2019/1/high-interaction-honeypot-versus-low-interaction-honeypot/

[239] N. Provos, "Developments of the honeyd virtual honeypot," *http://honeyd.org*, 2005.

[240] "Using honeyd configurations to build honeypot systems," 2021. [Online]. Available: https://searchsecurity.techtarget.com/Using-HoneyD-configurations-to-build-honeypot-systems

[241] B. Lutkevich, "Lamp (linux, apache, mysql, php)," 2021. [Online]. Available: https://whatis.techtarget.com/definition/LAMP-Linux-Apache-MySQL-PHP

[242] "Usage statistics of apache." [Online]. Available: https://w3techs.com/technologies/details/ws-apache

[243] "Wordpress market share," 2023. [Online]. Available: https://kinsta.com/wordpress-market-share/

[244] "Wordpress: List of security vulnerabilities," 2023. [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-2337/product_id-4096/

[245] C. Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *Proceedings of the 2009 workshop on New security paradigms workshop*, 2009, pp. 133–144.

[246] I. Ion, R. Reeder, and S. Consolvo, "{"... No} one can hack my {Mind"}: Comparing expert and {Non-Expert} security practices," in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, 2015, pp. 327–346.

[247] A. Hern, "Wannacry, petya, notpetya: How ransomware hit the big time in 2017," *The Guardian*, vol. 30, no. 12, p. 2017, 2017. [Online]. Available: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware

[248] C. Li, H. Wang, Z. Zhang, A. Sun, and Z. Ma, "Topic modeling for short texts with auxiliary word embeddings," in *Proceedings of the 39th International ACM SIGIR conference on Research and Development in Information Retrieval*, 2016, pp. 165–174.

[249] F. Esposito, A. Corazza, F. Cutugno *et al.*, "Topic modelling with word embeddings." in *CLiC-it/EVALITA*, 2016.

[250] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado, and J. Dean, "Distributed representations of words and phrases and their compositionality," *Advances in neural information processing systems*, vol. 26, 2013. [Online]. Available: https://proceedings.neurips.cc/paper/2013/file/9aa42b31882ec039965f3c4923ce901b-Paper.pdf

[251] M. Grootendorst, "Bertopic: Leveraging bert and c-tf-idf to create easily interpretable topics," *Zenodo, Version v0*, vol. 9, 2020. [Online]. Available: https://doi.org/10.5281/zenodo.4381785

[252] R. J. Campello, D. Moulavi, and J. Sander, "Density-based clustering based on hierarchical density estimates," in *Pacific-Asia conference on knowledge discovery and data mining*. Springer, 2013, pp. 160–172.

[253] F. Hamborg, N. Meuschke, C. Breitinger, and B. Gipp, "news-please: A generic news crawler and extractor," pp. 218–223, 2017.

[254] C. Gormley and Z. Tong, *Elasticsearch: the definitive guide: a distributed real-time search and analytics engine*. "O'Reilly Media, Inc.", 2015.

[255] I. Montani, "spacy/spacy/lang/en/stop_words.py at master - explosion/spacy - github." [Online]. Available: https://github.com/explosion/spaCy/blob/master/spacy/lang/en/stop_words.py

[256] "sentence-transformers/roberta-base-nli-stsb-mean-tokens · hugging face." [Online]. Available: https://huggingface.co/sentence-transformers/roberta-base-nli-stsb-mean-tokens

[257] N. Reimers and I. Gurevych, "Sentence-bert: Sentence embeddings using siamese bert-networks," *arXiv preprint arXiv:1908.10084*, 2019.

[258] L. McInnes, J. Healy, and J. Melville, "Umap: Uniform manifold approximation and projection for dimension reduction," *arXiv preprint arXiv:1802.03426*, 2018.

[259] "Official documentation for umap parameters." [Online]. Available: https://umaplearn.readthedocs.io/en/latest/parameters.html

[260] I. T. Jolliffe and J. Cadima, "Principal component analysis: a review and recent developments," *Philosophical transactions of the royal society A: Mathematical, Physical and Engineering Sciences*, vol. 374, no. 2065, p. 20150202, 2016.

[261] A. Mohamed, "An effective dimension reduction algorithm for clustering arabic text," *Egyptian Informatics Journal*, vol. 21, no. 1, pp. 1–5, 2020.

[262] L. Van der Maaten and G. Hinton, "Visualizing data using t-sne." *Journal of machine learning research*, vol. 9, no. 11, 2008.

[263] "Official documentation for hdbscan parameters." [Online]. Available: https://hdbscan.readthedocs.io/en/latest/parameterselection.html

[264] "sklearn.cluster.meanshift — scikit-learn 1.4.1 documentation." [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.cluster.MeanShift.html

[265] "Python scikit-learn module accessible at." [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.featureextraction.text.TfidfVectorizer.html

[266] "Python scikit-learn module accessible at." [Online]. Available: https://scikit-learn.org/stable/modules/generated/sklearn.featureextraction.text.CountVectorizer.html

[267] [Online]. Available: https://amp-theguardian-com.cdn.ampproject.org/c/s/amp.theguardian.com/world/2020/jul/16/russian-state-sponsored-hackerstarget-covid-19-vaccine-researchers

[268] W. Helen, C. Clive, and F. Henry, "Russia-linked hackers accused of targeting covid-19 vaccine developers — ars technica." [Online]. Available: https://arstechnica.com/information-technology/2020/07/russia-linked-hackers-accused-of-targeting-covid-19-vaccine-developers/

[269] T. Seals, "Nation-state attackers actively target covid-19 vaccine-makers — threatpost." [Online]. Available: https://threatpost.com/russia-north-korea-attackingcovid-19-vaccine-makers/161205/

[270] P. Paganini, "Hackers target covid-19 vaccine supply chain and sell the vaccine in darkweb." [Online]. Available: https://securityaffairs.com/112433/hacking/covid-19-attacks-2.html

[271] T. Seals, "Lazarus group hits covid-19 vaccine-maker in espionage attack — threatpost." [Online]. Available: https://threatpost.com/lazarus-covid-19-vaccine-maker-espionage/162591/

[272] P. Paganini, "Ema: Some of pfizer/biontech covid-19 vaccine data was leaked online." [Online]. Available: https://securityaffairs.co/wordpress/113326/data-breach/ema-data-breach.htm

[273] "ENISA Threat Landscape 2022." [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

[274] "CVE Details." [Online]. Available: https://www.cvedetails.com/browse-by-date.php

[275] "CVSS v3.1 Specification Document." [Online]. Available: https://www.first.org/cvss/v3.1/specification-document

[276] L. Allodi and F. Massacci, "Comparing Vulnerability Severity and Exploits Using Case-Control Studies," *ACM Transactions on Information and System Security*, vol. 17, no. 1, pp. 1:1–1:20, Aug. 2014.

[277] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," May 2019.

[278] P. Frode de la Foret, S. Ruseti, C. Sandescu, M. Dascalu, and S. Travadel, "Interpretable Identification of Cybersecurity Vulnerabilities from News Articles," in *Proceedings of the International Conference on Recent Advances in Natural Language Processing (RANLP 2021)*. Held Online: INCOMA Ltd., Sep. 2021, pp. 428–436.

[279] I. Beltagy, M. E. Peters, and A. Cohan, "Longformer: The Long-Document Transformer," Dec. 2020.

[280] Y. Ming, P. Xu, H. Qu, and L. Ren, "Interpretable and steerable sequence learning via prototypes," in *Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, 2019, pp. 903–913.

[281] C. Vladescu, M.-A. Dinisor, O. Grigorescu, D. Corlatescu, C. Sandescu, and M. Dascalu, "What are the Latest Cybersecurity Trends? A Case Study Grounded in Language Models," in *2021 23rd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*, Dec. 2021, pp. 140–146.

[282] Y. Liu, M. Ott, N. Goyal, J. Du, M. Joshi, D. Chen, O. Levy, M. Lewis, L. Zettlemoyer, and V. Stoyanov, "RoBERTa: A Robustly Optimized BERT Pretraining Approach," Jul. 2019.

[283] V. Sanh, L. Debut, J. Chaumond, and T. Wolf, "Distilbert, a distilled version of bert: smaller, faster, cheaper and lighter," *arXiv preprint arXiv:1910.01108*, 2019.

[284] Z. Lan, M. Chen, S. Goodman, K. Gimpel, P. Sharma, and R. Soricut, "Albert: A lite bert for self-supervised learning of language representations," *arXiv preprint arXiv:1909.11942*, 2019.

[285] M. Liberato, "Secbert: Analyzing reports using bert-like models," Master's thesis, University of Twente, 2022.

[286] "HuggingFace Transformers." [Online]. Available: https://huggingface.co/docs/transformers/main/en/index

[287] "Scikit-learn-contrib/hdbscan," Jun. 2022. [Online]. Available: scikit-learn-contrib

[288] "PRAW: The Python Reddit API Wrapper — PRAW 7.6.0 documentation." [Online]. Available: https://praw.readthedocs.io/en/stable/

[289] K. McKee, "Kurtmckee/feedparser," Jun. 2022.

[290] "Newspaper3k: Article scraping & curation — newspaper 0.0.2 documentation." [Online]. Available: https://newspaper.readthedocs.io/en/latest/

[291] "PyMongo 4.1.1 Documentation — PyMongo 4.1.1 documentation." [Online]. Available: https://pymongo.readthedocs.io/en/stable/

[292] "MongoDB — Build Faster. Build Smarter." [Online]. Available: https://www.mongodb.com

[293] "FastAPI." [Online]. Available: https://fastapi.tiangolo.com/

[294] "Svelte - Cybernetically enhanced web apps." [Online]. Available: https://svelte.dev/

[295] "Carbon Design System." [Online]. Available: https://carbondesignsystem.com/carbondesignsystem.com

[296] M. Bostock, "D3.js - Data-Driven Documents." [Online]. Available: https://d3js.org/

[297] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer law & security review*, vol. 26, no. 1, pp. 23–30, 2010.

[298] J. Scambray, S. McClure, G. Kurtz, McClure, Scambray, and Kurtz, *Hacking exposed: network security secrets & solutions*. Osborne/McGraw-Hill New York, 2001, vol. 118.

[299] T. Mahmood and U. Afzal, "Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools," in *2013 2nd national conference on Information assurance (ncia)*. IEEE, 2013, pp. 129–134.

[300] B. R. Rowe and M. P. Gallaher, "Private sector cyber security investment strategies: An empirical analysis," in *The fifth workshop on the economics of information security (WEIS06)*, 2006.

[301] S. M. Tisdale, "Cybersecurity: Challenges from a systems, complexity, knowledge management and business intelligence perspective." *Issues in Information Systems*, vol. 16, no. 3, 2015.

[302] P. Herzog, "Open source security testing methodology manual (osstmm)," *ISECOM. Available: http://www.isecom.org/research/.[Accessed 2015]. Open Web Application Security Project (OWASP), Attack. Available: https://www.owasp.org/index.php/Category:Attack*, 2010. [Online]. Available: http://www.isecom.org/research/osstmm.html

[303] "Remediating computer security threats using distributed sensor computers." [Online]. Available: http://patents.justia.com/patent/9374385

[304] "Distribution of security rules among sensor computers." [Online]. Available: http://patents.justia.com/patent/9350750

[305] M. Souppaya, K. Scarfone *et al.*, "Guide to enterprise patch management technologies," *NIST Special Publication*, vol. 800, p. 40, 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

[306] "Continuous vulnerability assessment & remediation guideline," University of California, Berkeley, 2023, accessed: 2023-12-15. [Online]. Available: https://security.berkeley.edu/continuous-vulnerability-assessment-remediation-guideline

[307] S. G. Kelekar, "Systems and methods for real-time network-based vulnerability assessment," 2012, patent number US8127359. [Online]. Available: http://www.google.com/patents/US8127359

[308] C. M. Stuart, K. George, K. Robin, A. B. Marshall, J. M. Michael, M. P. Christopher, M. C. David, and A. Christopher, "System and method for network vulnerability detection and reporting," 2006, patent number US7152105. [Online]. Available: http://www.google.com/patents/US7152105

[309] OWASP, "OWASP ASVS – Open Web Application Security Project Application Security Verification Standard," 2023, accessed: 2023-12-15. [Online]. Available: https://github.com/OWASP/ASVS

[310] M. C. Ivan Arce, "Automating penetration tests - black hat," 2001, accessed: 2023-12-15. [Online]. Available: https://www.blackhat.com/presentations/bh-usa-01/IvanAcre/bh-usa-01-Ivan-Arce.ppt

[311] [Unknown Author], "The mathematics behind an automated penetration testing framework," 2014, accessed: 2023-12-15. [Online]. Available: https://www.securityforum.at/wpcontent/uploads/2014/05/SF14_Slides_Simos.pdf

[312] ——, "Continuous auditing: Is it fantasy or reality?" *Information Systems Control Journal*, vol. 5, 2002, accessed: 2023-12-15. [Online]. Available: http://www.isaca.org/Groups/Professional-English/continuous-monitoring-auditing/GroupDocuments/ISACA%20Continuous%20Auditing.pdf

[313] 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*. Citeseer, 2010, pp. 430–434.

[314] 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, no. 2, pp. 37–44, 2016.

[315] A. Khazaei, M. Ghasemzadeh, and V. Derhami, "An automatic method for cvss score prediction using vulnerabilities description," *Journal of Intelligent & Fuzzy Systems*, vol. 30, no. 1, pp. 89–96, 2016.

[316] T. Wen, Y. Zhang, Y. Dong, and G. Yang, "A novel automatic severity vulnerability assessment framework." *J. Commun.*, vol. 10, no. 5, pp. 320–329, 2015.

[317] G. Da, M. Xu, J. Zhang, and P. Zhao, "Joint cyber risk assessment of network systems with heterogeneous components," *arXiv preprint arXiv:2006.16092*, 2020.

[318] RSA, "The rsa digital risk index," 2020, accessed: November 1, 2020. [Online]. Available: https://www.rsa.com/en-us/tools/digital-risk-index-form

[319] Tenable, "3 things you need to know about prioritizing vulnerabilities," 2018, accessed: November 1, 2020. [Online]. Available: https://static.tenable.com/marketing/whitepapers/WhitepaperThree_Things_You_Need_to_Know_About_Prioritizing_Vulnerabilities_eBook.pdf

[320] ——, "Tenable lumin," 2020, accessed: November 14, 2020. [Online]. Available: https://www.tenable.com/products/tenable-lumin

[321] Trust Data Solutions, "Cyber security risk services," 2020, accessed: November 14, 2020. [Online]. Available: https://trustsds.com/consulting-services/enterprise-riskand-compliance/cyber-security-risk-assessment/

[322] UpGuard, "A complete third-party risk management platform," 2020, accessed: November 14, 2020. [Online]. Available: https://www.upguard.com/product/vendorrisk

[323] Cisco, "Cyber security and insurance," 2020, accessed: November 14, 2020. [Online]. Available: https://www.cisco.com/c/en/us/solutions/security/cyberinsurance/index.html

[324] Nationwide, "What is cyber insurance?" 2020, accessed: November 14, 2020. [Online]. Available: https://www.nationwide.com/lc/resources/smallbusiness/articles/what-is-cyber-insurance

[325] "Openscap," 2020, accessed: November 14, 2020. [Online]. Available: https://www.openscap.org/

[326] NIST, "National checklist program repository," 2020, accessed: November 14, 2020. [Online]. Available: https://nvd.nist.gov/ncp/repository

[327] Trusted Computing Group, "Trusted network communications," 2020, accessed: November 14, 2020. [Online]. Available: https://trustedcomputinggroup.org/workgroups/trusted-network-communications/

[328] Center for Internet Security, "Cis benchmarks," 2020, accessed: November 14, 2020. [Online]. Available: https://www.cisecurity.org/cis-benchmarks/

[329] Open Vulnerability and Assessment Language, "Open vulnerability and assessment language," MITRE, 2020, accessed: November 14, 2020. [Online]. Available: https://oval.mitre.org/

[330] C. Nie, J. Li, and S. Wang, "Modeling the effect of spending on cyber security by using surplus process," *Mathematical Problems in Engineering*, vol. 2020, 2020.

[331] Leader Team Global Insurance Broker, "Risk consulting," 2020, accessed: November 14, 2020. [Online]. Available: https://leaderteam.ro/practice/leader-team-riskconsulting/

[332] Corero, "Mirai botnet attack type," 2020, accessed: 2020. [Online]. Available: https://www.corero.com/resources/ddosattack-types/mirai-botnet-ddos-attack.html

[333] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, and T. Razafindralambo, "A survey on facilities for experimental internet of things research," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 58–67, 2011.

[334] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[335] OWASP, "Owasp fuzzing," 2020, accessed: 2020. [Online]. Available: https://www.owasp.org/index.php/Fuzzing

[336] Armour Project, "Generic test patterns and test models for iot security testing," 2016, accessed: 2020. [Online]. Available: https://www.armour-project.eu/wpcontent/uploads/2016/08/D21-Generic-test-patterns-and-test-modelsfor-IoT-security-testing.pdf

[337] Anastacia Project, "Attack threats analysis and contingency actions initial report," 2020, version 0.5. [Online]. Available: http://www.anastaciah2020.eu/deliverables/ANASTACIA-WP2-T2.2-CNR-D2.2-AttackThreatsAnalysisAndContingencyActionsInitialReport-v0.5.pdf

[338] ——, "Initial security enforcement manager report," 2020, version 1.0. [Online]. Available: http://www.anastaciah2020.eu/deliverables/ANASTACIA-WP3-T3.1-UMU-D3.1-InitialSecurityEnforcementManagerReport-v1.0.pdf

[339] H. Guo, J. Ren, D. Zhang, Y. Zhang, and J. Hu, "A scalable and manageable iot architecture based on transparent computing," *Journal of Parallel and Distributed Computing*, vol. 118, pp. 5–13, 2018.

[340] J. Mocnej, M. Miškuf, P. Papcun, and I. Zolotová, "Impact of edge computing paradigm on energy consumption in iot," *IFAC-PapersOnLine*, vol. 51, no. 6, pp. 162–167, 2018.

[341] OWASP, "Owasp top 10 application security risks," 2017, accessed: 2020. [Online]. Available: https://www.owasp.org/index.php/Top_10-2017_Top_10

[342] C. Martin, R. Nasr, M. Hoersken, and T. Fuechtler, "Automating information security assessments using intelligent software agents," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 736–744.

[343] resin-os, "Docker balena," 2020, accessed: 2020. [Online]. Available: https://github.com/resin-os/balena

[344] O. Grigorescu, C. Săndescu, and R. Rughiniș, "Coda footprint continuous security management platform," in *2016 15th RoEduNet Conference: Networking in Education and Research*. IEEE, 2016, pp. 1–5.

[345] S. Khan and S. Parkinson, "Review into state of the art of vulnerability assessment using artificial intelligence," *Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach*, pp. 3–32, 2018.

[346] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *2013 international conference on availability, reliability and security*. IEEE, 2013, pp. 546–555.

[347] K. Kent, S. D. Quinn, and P. Mell, "The security content automation program (scap): Automating compliance checking, vulnerability management, and security measurement," Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Report 7343, 2006.

[348] C. Xiaolin, T. Xiaobin, Z. Yong, and X. Hongsheng, "A markov game theory-based risk assessment model for network information system," in *2008 International Conference on Computer Science and Software Engineering*, vol. 3. IEEE, 2008, pp. 1057–1061.

[349] A. Karbowski, K. Malinowski, S. Szwaczyk, and P. Jaskóła, "Critical infrastructure risk assessment using markov chain model," *Journal of Telecommunications and Information Technology*, no. 2, pp. 15–22, 2019.

[350] F. Sun, J. Pi, J. Lv, and T. Cao, "Network security risk assessment system based on attack graph and markov chain," in *Journal of Physics: Conference Series*, vol. 910, no. 1. IOP Publishing, 2017, p. 012005.

[351] J. Shin, H. Son, and G. Heo, "Cyber security risk evaluation of a nuclear i&c using bn and et," *Nuclear Engineering and Technology*, vol. 49, no. 3, pp. 517–524, 2017.

[352] R. Munir, J. P. Disso, I. Awan, and M. R. Mufti, "A quantitative measure of the security risk level of enterprise networks," in *2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications*. IEEE, 2013, pp. 437–442.

[353] H. Gao, J. Zhu, and C. Li, "The analysis of uncertainty of network security risk assessment using dempster-shafer theory," in *2008 12th International Conference on Computer Supported Cooperative Work in Design*. IEEE, 2008, pp. 754–759.

[354] Y. Duan, Y. Cai, Z. Wang, and X. Deng, "A novel network security risk assessment approach by combining subjective and objective weights under uncertainty," *Applied Sciences*, vol. 8, no. 3, p. 428, 2018.

[355] H. Owen and B. Byers, "Automation support for cve retrieval," National Institute of Standards and Technology, Official API Documentation, 2021.

[356] V. L. Sujay, "Number of internet of things (iot) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030," Statista, 2023. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[357] "Security issues of IoT: Securing your IoT Device in 2023," Device Authority Ltd. [Online]. Available: https://www.deviceauthority.com/blog/security-issues-of-iot-securing-your-iot-device-in-2023/

[358] "Data security: How a proactive c-suite can reduce cyber-risk for the enterprise," The Economist Intelligence Unit, 2016. [Online]. Available: https://impact.economist.com/perspectives/technology-innovation/data-security-how-proactive-c-suite-can-reduce-cyber-risk-enterprise/article/data-security-how-proactive-c-suite-can-reduce-cyber-risk-enterprise

[359] "Common vulnerability scoring system version 4.0: Specification document." [Online]. Available: https://www.first.org/cvss/v4.0/specification-document

[360] "Why organizations struggle with vulnerability management?" [Online]. Available: https://heimdalsecurity.com/blog/vulnerability-management-challenges/

[361] "Forum of incident response and security teams." [Online]. Available: https://www.first.org/

[362] "Common vulnerability scoring system version 4.0: Specification document," Forum of Incident Response and Security Teams. [Online]. Available: https://www.first.org/cvss/v4.0/specification-document

[363] "Cisa known exploited vulnerabilities catalog." [Online]. Available: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[364] "Exploit prediction scoring system (epss)." [Online]. Available: https://www.first.org/epss/

[365] "Stakeholder-specific vulnerability catego- rization (svcc)." [Online]. Available: https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc

[366] B. Jung, Y. Li, and T. Bechor, "Cavp: A context-aware vulnerability prioritization model," *Computers Security*, vol. 116, p. 102639, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404822000384

[367] V. Ahmadi Mehri, P. Arlos, and E. Casalicchio, "Automated context-aware vulnerability risk management for patch prioritization," *Electronics*, vol. 11, no. 21, 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/21/3580

[368] "Rudder cve plugin," accessed: 2024. [Online]. Available: https://docs.rudder.io/reference/6.2/plugins/cve.html

[369] C. S. O. Grigorescu and R. Rughiniș, "Coda footprint continuous security management platform," 2016, pp. 1–5.

[370] "Automatic system for early detection of cyber vulnerabilities." [Online]. Available: https://yggdrasil.codaintelligence.com/

[371] "Cis benchmarks list," accessed: 2024. [Online]. Available: https://www.cisecurity.org/cis-benchmarks

[372] "Nist, security content automation protocol," 2022. [Online]. Available: https://csrc.nist.gov/projects/security-content-automation-protocol

[373] "Openscap portal." [Online]. Available: https://www.open-scap.org/

[374] 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)*. IEEE, 2021, pp. 463–468.

[375] I. Babalau, D. Corlatescu, O. Grigorescu, C. Sandescu, and M. Dascalu, "Severity prediction of software vulnerabilities based on their text description," in *2021 23rd International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*. IEEE, 2021, pp. 171–177.

[376] M. Mijwil, O. J. Unogwu, Y. Filali, I. Bala, and H. Al-Shahwani, "Exploring the top five evolving threats in cybersecurity: An in-depth overview," *Mesopotamian journal of cybersecurity*, vol. 2023, pp. 57–63, 2023.

[377] K. De Nobrega and A.-F. Rutkowski, "The ai family: The information security managers best frenemy?" 2022.

[378] Z. Zhang, H. Ning, F. Shi, F. Farha, Y. Xu, J. Xu, F. Zhang, and K.-K. R. Choo, "Artificial intelligence in cyber security: research advances, challenges, and opportunities," *Artificial Intelligence Review*, pp. 1–25, 2022.

[379] J. Bharadiya, "Machine learning in cybersecurity: Techniques and challenges," *European Journal of Technology*, vol. 7, no. 2, pp. 1–14, 2023.

[380] P. Dixit and S. Silakari, "Deep learning algorithms for cybersecurity applications: A technological and status review," *Computer Science Review*, vol. 39, p. 100317, 2021.

[381] M. Sewak, S. K. Sahay, and H. Rathore, "Deep reinforcement learning in the advanced cybersecurity threat detection and protection," *Information Systems Frontiers*, vol. 25, no. 2, pp. 589–611, 2023.

[382] G. Lin, S. Wen, Q.-L. Han, J. Zhang, and Y. Xiang, "Software vulnerability detection using deep neural networks: a survey," *Proceedings of the IEEE*, vol. 108, no. 10, pp. 1825–1848, 2020.