Kibertəhdid Kəşfiyyatı Fəaliyyətinin Aşkarlanması və Rəqəmsal Ekspertizası

Adilə Kərimova
Azərbaycan Texniki Universiteti, Bakı, Azərbaycan
adila.karimova@aztu.edu.az

***Xülasə*— Rəqəmsal texnologiyaların dinamik inkişafı nəticəsində kibertəhdid kəşfiyyatı xeyli mürəkkəbləşmiş, ciddi təhlükə mənbəyinə çevrilmişdir. Kibertəhdidlərin mürəkkəb, dinamik və gizli xarakterli olmaları dövlətin, təşkilatların və ya qurumların informasiya sistemlərinin təhlükəsizliyinə ciddi risk yaratmaqdadır. Milli təhlükəsizlik, iqtisadi dayanıqlıq, sosial sabitlik və informasiya təhlükəsizliyinin təmin edilməsi baxımından proaktiv müdafiə strategiyası kritik əhəmiyyət kəsb edir. Bu tədqiqat işində kibertəhdid kəşfiyyatı fəaliyyətinin aşkarlanması və analizi üsulları araşdırılmış, rəqəmsal ekspertizanın bu sahədə rolu əsaslandırılmış və praktiki tətbiq imkanları nəzərdən keçirilmişdir. Aparılan tədqiqata əsasən, rəqəmsal ekspertiza metodlarının tətbiqi kibertəhdid kəşfiyyatı fəaliyyətinin real-vaxtda aşkarlanmasına, rəqəmsal sübutların hüquqi baxımdan etibarlılığının təmin edilməsinə imkan verir.**

Açar sözlər*— *kibertəhdid; kəşfiyyat fəaliyyəti; rəqəmsal ekspertiza; rəqəmsal sübutlar.

I. GİRİŞ

Rəqəmsal mühitdə kibertəhdidlər getdikcə daha mürəkkəb, dinamik və gizli xarakter hal almaqdadır. Hazırda dövlət qurumları, özəl sektorlar, kritik informasiya infrastrukturu və hətta fərdi istifadəçilər dəyişən intensivliklə müxtəlif kibertəhdidlərlə üzləşir

Kibertəhdid kəşfiyyatı - potensial və mövcud təhdidlər haqqında kritik məlumatların toplanması, emalı və paylaşılması prosesi hesab olunur.

Kibertəhdid kəşfiyyatı (ing. CTI - Cyber Threat Intelligence) reaktiv olmaqla yanaşı, proaktiv müdafiə strategiyasının da əsasını təşkil edir. Qeyd edək ki, aktorun taktika, texnika və prosedurlarını (ing. TTP - Tactics, Techniques and Procedures) əvvəlcədən bilmək təşkilata müdafiə strategiyalarını tənzimləməyə kömək edir.

Bu aspektdən, rəqəmsal kriminalistika hadisələrin texniki izlərini toplamaq, qorumaq, analiz etmək və hüquqi baxımdan qanuni, etibarlı sübutlara çevirmək prosesi hesab olunur [1].

Bu məqalənin məqsədi, CTI fəaliyyətinin aşkarlanması metodologiyasını, rəqəmsal ekspertiza prinsiplərini və bu iki sahənin inteqrasiyasını analitik cəhətdən nəzərdən keçirməkdir.

II. KİBERTƏHDİD KƏŞFİYYATININ KONSEPTUAL ÇƏRÇİVƏSİ

Kibertəhdid kəşfiyyatı mərhələli şəkildə həyata keçirilir. Hər bir mərhələ öz metodologiyasını, alətlər dəstini və keyfiyyət standartlarını tələb edir. Birinci mərhələdə loq faylları, şəbəkə trafiki, zərərverici proqram nümunələri, dark web və açıq mənbə məlumatları müxtəlif məlumat mənbələrindən toplanır. İkinci mərhələdə məlumatların emalı və korrelyasiyası prosesi həyata keçirilir. Yəni toplanmış məlumatlar strukturlaşdırılır, təmizlənir və təhdid indikatorları müəyyən olunur. Növbəti mərhələdə isə analitik qiymətləndirmə prosesi aparılır. Qiymətləndirmə prosesi zamanı aktorun motivasiyası, taktika, texnika və prosedurları analiz olunur. Nəticə olaraq, taktiki, strateji və operativ səviyyədə qərar qəbulu üçün kəşfiyyat hesabatı formalaşır. Qiymətləndirmədən sonra müdafiə tədbirləri həyata keçirilir [2]. Beləliklə, CTI-nin konseptual çərçivəsi kibertəhdidlərin aşkarlanması üçün metodoloji baza yaradır.

CTI-nin struktur baxımdan üç səviyyəsi mövcuddur. Bu səviyyələr hadisələrin araşdırılması və sübutların analizində həm texniki, həm də strateji qərarların verilməsində mühüm əhəmiyyət kəsb edir. Başqa sözlə, CTI səviyyələri rəqəmsal ekspertiza sahəsində hansı sübutların toplanacağını, hansı artefaktların prioritetləşdiriləcəyini və araşdırmanın hansı analitik dərinlikdə aparılacağını birbaşa müəyyən edir.

Strateji kəşfiyyat

Strateji CTI-da hansı aktor profillərinin rəsmi olaraq tanındığı, sübutun məhkəmə prosesləri üçün uyğunluğu, hücumların motivasiyası və gözlənilən risklər analiz olunur. Həmçinin, strateji kəşfiyyatda təşkilatın təhlükəsizlik sahəsinə ayırmalı olduğu investisiya həcmi müəyyən edilir.

Taktiki kəşfiyyat

Taktiki CTI səviyyəsi TTP-lər əsasında aktorun necə hərəkət etdiyini öyrənir. Rəqəmsal ekspertiza TTP-ləri aşağıdakı üç istiqamətdə araşdırır:

1 zərərverici proqramın davranışının analizi;

2 hücum vektorlarının analizi;

3 müdafiə mexanizmlərinin optimallaşdırılması.

Operativ kəşfiyyat

Operativ CTI konkret aktor qrupunun kimə hücum etdiyi, hansı üsullardan istifadə etdiyi və nə qədər müddət ərzində fəaliyyət göstərdiyini müəyyən edir. Rəqəmsal ekspertiza baxımından operativ CTI üç əsas funksiyanı yerinə yetirir:

1. hücumu həyata keçirən aktorun müəyyənləşdirilməsi;
2. araşdırmanın zaman çərçivəsinin müəyyənləşdirilməsi;
3. araşdırmanın əhatə dairəsinin formalaşdırılması.

DOI: 10.25045/forensic.gov.2026.22

Texniki kəşfiyyat

Rəqəmsal ekspertizada intensiv əməliyyat əlaqəsini quran səviyyə isə texniki CTI səviyyəsidir. Texniki səviyyədəki kəşfiyyat artefaktları - IP ünvanları, domen adları, fayl heş dəyərləri, reyestr açarları, YARA imzaları ekspertiza zamanı ilk növbədə nəyə diqqət yetiriləcəyinə müəyyən etməyə kömək edir.

Eyni zamanda qeyd etmək lazımdır ki, ekspertiza araşdırması nəticəsində aşkar edilmiş yeni artefaktlar - qeydə alınmamış C2 domen adları, naməlum PE fayl imzaları, unikal proses inyeksiya nümunələri də öz növbəsində texniki CTI bazasına əlavə olunur.

III. KİBERTƏHDİD aktorlarının klassifikasiyası

Kibertəhdid kəşfiyyatında əsas analitik əməliyyatlarından biri aktorun müəyyən edilməsidir. Bu səbəbdən, kibertəhdid kəşfiyyatı və rəqəmsal ekspertizada bu klassifikasiya mühüm əhəmiyyət kəsb edir. Aktorların əsas kateqoriyaları aşağıda verilmişdir [3]:

1. Dövlət sponsorlu APT qrupları - bu qruplar dövlət büdcəsi ilə maliyyələşir, uzun müddətli casusluq, sabotaj və ya geosiyasi məqsədlər güdən aktor qruplarıdır.
2. Kiberkriminal qruplar - bu qruplar maliyyə qazancı məqsədilə hərəkət edən, müxtəlif texniki potensial və təşkilati strukturda fəaliyyət göstərən aktor kateqoriyasıdır.
3. Hacktivistlər - siyasi, ideoloji və ya ictimai məqsədlər güdərək fəaliyyət göstərən aktor qruplarıdır.
4. Daxili təhdid (ing. Insider threat) - daxili aktor artıq sistemin içində olan, qanuni giriş icazəsinə malik və öz fəaliyyətini normal iş prosesinin bir hissəsi kimi gizlədə bilən aktor növüdür.
5. Script Kiddies - hazır alətlərdən istifadə edən, texniki biliyi məhdud olan aktorlar.

IV. KİBERTƏHDİD KƏŞFİYYATI FƏALİYYƏTİNİN AŞKARLANMASI

Kibertəhdid fəaliyyətinin aşkarlanması informasiya sistemlərində baş verən anomaliya xarakterli, şübhəli və ya zərərli davranışların müəyyən edilməsi prosesidir [4]. Kibertəhdid fəaliyyətinin aşkarlanması rəqəmsal ekspertiza sahəsində vacib proses hesab olunur. Çünki erkən aşkarlanma nəticəsində, ekspertizada istifadə olunacaq sübutun tamlığı yüksək olur. Həmçinin, qeyd etmək olar ki, aşkarlanmanın özü bir sübutdur.

SIEM əsaslı aşkarlama (ing. Security Information and Event Management)

Kibertəhdid fəaliyyətinin aşkarlanmasında istifadə edilən əsas yanaşmalardan SIEM platformaları xüsusi yer tutur. Bu platformalar təşkilatın bütün texniki infrastrukturunu vahid analitik çərçivədə nəzərdən keçirir. Şəbəkə cihazları, serverlər, tətbiqlər, firewall və endpoint sistemlər kimi müxtəlif mənbələrdən gələn loqlar vahid mərkəzdə birləşdirilir, nəzərdə tutulanstruktura gətirilir və korrelyasiya qaydaları vasitəsilə qiymətləndirilir [5].

Rəqəmsal ekspertizada SIEM platformaları iki funksiyanı yerinə yetirir:

1. Real-vaxt rejimində monitorinq - insidentə operativ reaksiya vermək imkanı və sübutların qorunması.
2. Hadisələrin korrelyasiyası və hadisələrin aşkarlanması – hadisənin əhatəsinin müəyyənləşdirilməsi və sübutun hüquqi keyfiyyətinin təmin edilməsi.

Şəbəkə trafikinin monitorinqi.

Şəbəkə trafikinin monitorinqi kibertəhdid fəaliyyətinin aşkarlanmasında əsas metodlardan biridir. Monitorinq prosesi şəbəkə daxilindəki və xaricindəki bütün kommunikasiya axınlarını - IP ünvanları arasındakı əlaqələri, port istifadəsini, protokol davranışlarını izləyir. Bu prosesdə IDS/IPS sistemləri, NDR (ing. Network Detection and Response) həlləri və paket analiz alətləri əsas texnoloji vasitələrdir.

Rəqəmsal ekspertiza baxımından şəbəkə trafikinin monitorinqi insidentlərin rekonstruksiyası üçün əhəmiyyətlidir. Disk üzərindəki artefaktların silinməsindən, yaddaş sahəsinin korlanmasından asılı olmayaraq, şəbəkə monitorinqi hücumun hansı mərhələlərdən keçdiyini, hansı sistemlərin əlaqəyə girildiyini və məlumatın hara ötürüldüyünü aşkar edir.

EDR (ing. Endpoint detection and response).

EDR platformaları aşkarlamanı son istifadəçi qurğuları səviyyəsində həyata keçirir. Şəbəkə monitorinqi zamanı trafik görünür, lakin EDR isə həmin trafikin mənşəyini, yəni konkret prosesi, istifadəçini, icra olunan əməliyyatı görür. EDR platformaları endpoint-də baş verən hər fəaliyyəti davamlı şəkildə izləyir. Nəticədə, hansı faylın icra edildiyi, hansı prosesin hansı digər prosesi başlatdığı, reyestrdə hansı dəyişikliklərin aparıldığı, yaddaşda hansı əməliyyatların həyata keçirildiyi və hansı şəbəkə bağlantılarının qurulduğu müəyyən olunur.Sistemdə şübhəli olan fəaliyyətlər bu yolla aşkarlanır.

Rəqəmsal ekspertizada EDR sistemləri insidentlərin texniki analizində mühüm sübut bazası rolunu oynayır [5].

Təhdid ovçuluğu (ing.Threat Hunting).

Mürəkkəb təhdid aktorları öz fəaliyyətlərini qanuni sistem prosesləri arxasında gizlətdiyindən, bəzi sistemlər müəyyən təhdidləri aşkarlaya bilmirlər. Bu səbəbdən, bu vəziyyətlərin aradan qaldırılmasında təhdid ovçuluğu mühüm rol oynayır. Təhdid ovçuluğunu digər sistemlərdən fərqli xüsusiyyəti proaktiv müdafiə strategiyasını formalaşdırmasıdır. Təhdid ovçuluğu analitiki xəbərdarlıq olmadan əvvəl axtarışa çıxır. Araşdırma zamanı anomal davranışlar, gizli kommunikasiya kanalları, məlumat exfiltrasiya cəhdləri aşkarlanır. CTI inteqrasiyasında kəşfiyyat analitikə "nəyə baxacağını" deyir, ovçuluq prosesi isə həmin istiqamətdə sistemli araşdırma aparır [3].

Təhdid ovçuluğu rəqəmsal ekspertizada xüsusi əhəmiyyət kəsb edir. Bu prosesdə aşkar edilmiş artefaktlar ekspertiza araşdırmasının başlanğıc nöqtəsini müəyyən edir.

Süni intellek əsaslı aşkarlanma.

Ənənəvi aşkarlama sistemləri əsasən öncədən məlum qaydalar və imzalar üzərindən işləyir. Bu cür sistemlər imzası

mövcud olmayan hücumları tanıya bilmir. Süni intellekt əsaslı aşkarlama məhz bu problemləri aradan qaldırmaq üçün tətbiq olunur [6], [7].

Süni intellekt alqoritmləri müxtəlif mənbələrdən əldə olunan şəbəkə trafiki, endpoint logları, SIEM hadisələri, CTI indikatorları kimi böyük həcmli məlumatları emal edərək sistemin fəaliyyət modelini öyrənir. Hər kənara çıxma avtomatik olaraq anomaliya kimi qiymətləndirilir.

CTI inteqrasiyasında IoC-lər və TTP nümunələri modelin öyrənmə bazasına daxil edildikdə süni intellekt həm məlum, həm də naməlum hücum nümunələrini daha dəqiq müəyyən edir.

Rəqəmsal ekspertiza baxımından süni intellekt əsaslı sistemlər iki mühüm funksiya yerinə yetirir [8]:

1. Böyük həcmli rəqəmsal məlumatların analizi və korrelyasiyası;
2. Kibertəhdidlərin aşkarlanması və hadisələrin interpretasiyası.

V. RƏQƏMSAL EKSPERTİZANIN HÜQUQİ ƏSASLARI

Kibertəhdid kəşfiyyatı fəaliyyətinin aşkarlanması sahəsində rəqəmsal ekspertizanın hüquqi əsasları sübutların etibarlılığını, qanuniliyini təmin edən hüquqi çərçivəni formalaşdırır. Beləliklə, rəqəmsal ekspertiza texniki proses olmaqla yanaşı, həm də hüquqi məsuliyyətə malik fəaliyyətdir. Ekspertiza texniki baxımdan nə qədər dəqiq aparılmış olsa belə, hüquqi tələblərə cavab verməyən araşdırmanın nəticələri məhkəmədə qəbul olunmaya bilər [1].

Qanunvericilik bazası. Rəqəmsal ekspertiza fəaliyyəti milli kibertəhlükəsizlik qanunvericiliyinə, cinayət-prosessual normalara və beynəlxalq standartlara əsaslanır.

CTI məlumatlarının hüquqi statusu.Kibertəhdid kəşfiyyatında toplanmış IoC-lər, log qeydləri və şəbəkə trafiki məlumatları hüquqi sübut kimi yalnız aşağıdakı üç şərt ödənildikdə qəbul olunur:

1. məlumatın tamlığı təmin olunmalıdır;
2. məlumatın mənbəyi və əldə olunma prosesi sənədləşdirilməlidir;
3. məlumatın dəyişdirilmə və müdaxilə ehtimalı istisnasız olaraq aradan qaldırılmalıdır.

Mühafizə zənciri (ing. Chain of Custody). Toplanmış hər bir sübutun kimin əlindən keçdiyi, nə vaxt toplandığı, hansı vasitə ilə saxlandığı fasiləsiz şəkildə qeydə alınmalıdır.

Konfidensiallıq və məlumatların qorunması. Kibertəhdid kəşfiyyatı fəaliyyəti zamanı şəxsi və təşkilati məlumatlar analizi zamanı şəxsi məlumatların qorunması qanunlarına və etik normalara uyğun aparılmalıdır [9].

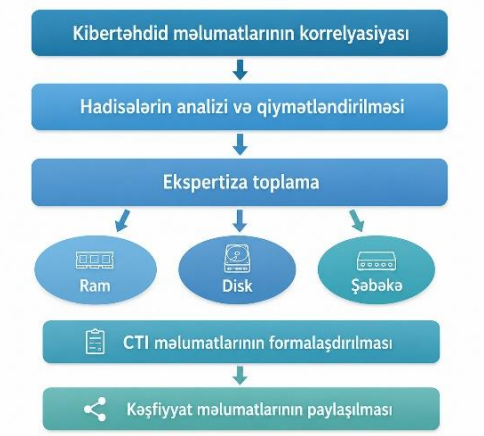
Məhkəmə qəbulolunma şərtləri. CTI əsaslı aşkarlama nəticəsində əldə edilmiş rəqəmsal sübutlar məhkəmədə istifadə oluna bilmək üçün aşağıdakı üç şərti ödəməlidir:

1 sübutun həqiqi və orijinal olmalıdır;

2 analiz prosesi müstəqil ekspert tərəfindən təkrarlanabilməlidir;

3 istifadə olunan alətlər və metodologiya tam şəkildə sənədləşdirilməlidir.

VI. KİBERTƏHDİD kəşfiyyatı və rəqəmsal ekspertizanın inteqrasiyası



Şəkil 1. Kibertəhdid kəşfiyyatı və rəqəmsal ekspertizanın inteqrasiyası.

CTI və rəqəmsal ekspertizanın inteqrasiyası təhdidlərin erkən aşkarlanmasını, sübutların daha düzgün analizini və kollektiv kibermüdafiənin güclənməsini təmin edir.

Kibertəhdid məlumatlarının korrelyasiyası.

Bu mərhələdə əsas məqsəd müxtəlif sistemlərdən (SIEM, EDR, DNS, NetFlow və s.) gələn məlumatları vahid mərkəzdə toplamaqdır. Müxtəlif sistemlərin hər biri ayrıca məlumat verir, lakin hamısı vahid analitik mühitdə korrelyasiya edildikdə, ayrı-ayrılıqda görünməyən şübhəli nümunələr aşkarlanır.

Hadisələrin analizi və qiymətləndirilməsi.

Aşkarlanan hadisələrin hər biri eyni dərəcədə əhəmiyyətli deyil. Bu mərhələnin əsas vəzifəsi məhz kritik əhəmiyyət kəsb edən hadisələrin müəyyən etməkdir. Bu mərhələdə əsas üç istiqamət nəzərdən keçirilir:

1. hadisənin ciddilik dərəcəsi qiymətləndirilir.
2. hadisənin təşkilatın hansı aktivlərinə təsir etdiyi müəyyən edilir.
3. hadisəyə aid bütün məlumatlar vahid araşdırma çərçivəsində toplanır.

Ekspertiza toplama.

Rəqəmsal ekspertizanın ən kritik addımıdır, çünki bu mərhələdə toplanmayan sübut sonradan geri qayıdıb tapıla bilməz. Toplama üç əsas sahəni əhatə edir:

- RAM. RAM-da aktiv proseslər, açıq şəbəkə bağlantıları və həmin an icra olunan kodlar saxlanılır. Sistem söndürüldükdə bu məlumatlar tamamilə itirilir. Bu səbəbdən RAM ən əvvəl toplanmalıdır.

- Disk. Fayllar, loq qeydləri, silinmiş məlumatlar, fayl yaradılma tarixləri və s. disk üzərindədir. RAM-dan fərqli olaraq sistem söndürüldükdə bu məlumatlar qalır. Lakin düşmən disk üzərindəki izləri silə biləcəyi üçün mümkün qədər tez toplanması vacibdir [8].
- Şəbəkə. Hansı IP ünvanlarına bağlantı var, hansı məlumat göndərilib, hansı domenlərlə əlaqə saxlanılıb və s. kimi məlumatlar şəbəkə loqlarındadır.

CTI məlumatlarının formalaşdırılması.

Əvvəlki mərhələlərdə sübutlar toplanılır, bu mərhələdə isə həmin sübutlardan faydalı məlumatlar çıxarılır. Bu proses üç istiqamətdə həyata keçirilir:

1. IoC-lərin müəyyən edilməsi;
2. TTP-lərin müəyyən edilməsi;
3. Toplanmış IoC-lər və TTP nümunələri mövcud aktor profilləri ilə müqayisə edilir.

Kəşfiyyat məlumatlarının paylanması.

Bu mərhələdə bir təşkilatın araşdırması yalnız özünə aid məlumat olaraq qalmır, həmçinin strukturlaşdırılmış formada digər təşkilatlarla paylaşılır.

NƏTİCƏ

Kibertəhdid kəşfiyyatı və rəqəmsal ekspertiza sahələrinin birlikdə inteqrasiyası təşkilatlara yalnız mövcud hücumlara cavab vermək deyil, gələcək təhdidləri əvvəlcədən görüb onlara qarşı cavab tədbirlərinin hazırlanmasını təmin edir.

CTI-nin effektivliyi rəqəmsal ekspertizadan gələn sübutların keyfiyyətindən birbaşa asılıdır. Hücumçuların davranış nümunələri, istifadə etdikləri alətlər və infrastruktur dərindən analiz edilmədən kəşfiyyat məlumatları öz dəyərini itirir.

Eyni zamanda, rəqəmsal ekspertiza da kəşfiyyat konteksti olmadan tam deyil. Belə ki, ekspertiza tək başına yalnız texniki faktları ortaya çıxarır. Hücumun əsl məqsədi, mənşəyi və daha geniş kampaniya konteksti isə cavabsız qalır.

Bununla belə, bu sahədə bir sıra ciddi çətinliklər hələ də mövcuddur:

- hücum üsullarının sürətlə dəyişməsi;
- milli hüquqi çərçivələr arasındakı uyğunsuzluq;
- məlumat paylaşımındakı etibarlılıq problem;
- peşəkar mütəxəssis çatışmazlığı.

Bu problemlərin aradan qaldırılması üçün texniki həllərlə yanaşı, strateji idarəetmə qərarları, beynəlxalq əməkdaşlıq və mütəmadi kadr hazırlığı tələb olunur.

MINNƏTDARLIQ

Bu iş Azərbaycan Texniki Universitetinin elmi-tədqiqat işlərinin və innovasiyaların dəstəklənməsi və inkişafı məqsədilə təqdim etdiyi daxili qrantın dəstəyi ilə həyata keçirilmişdir Müqavilə № AzTU-DQL-2025-M01/60182631.

ƏDƏBİYYAT

[1] M. I. Alghamdi, "Digital forensics in cyber security: Recent trends, threats, and opportunities," in Cybersecurity Threats with New Perspectives. Cham, Switzerland: Springer, 2021, pp. 1–13.

[2] M. Conti, T. Dargahi, and A. Dehghantanha, "Cyber threat intelligence: Challenges and opportunities," Cryptography and Security, pp. 1–6, 2018.

[3] D. P. Möller, "Threats and threat intelligence," in Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices. Cham, Switzerland: Springer, 2023, pp. 71–129.

[4] Y. Keim and A. K. Mohapatra, "Cyber threat intelligence framework using advanced malware forensics," International Journal of Information Technology, vol. 14, no. 2, pp. 521–530, 2022.

[5] A. E. A. Kareem, O. A. Oduwole, I. A. Akano, and A. A. Womiloju, "An overview of digital forensics investigations and threat intelligence tools," Journal of Science Innovation and Technology Research, pp. 1–14, 2025.

[6] S. Khan, N. Dilshad, N. Ahmad, S. Noor, and S. A. AlQahtani, "Integrating AI in security information and event management for real-time cyber defense," Scientific Reports, vol. 15, 2025.

[7] A. K. Tyagi, S. Kumari, and Richa, "Artificial intelligence-based cyber security and digital forensics: A review," in Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing. Singapore: Springer, 2024, pp. 391–419.

[8] S. S. Iyengar, S. Nabavirazavi, Y. Hariprasad, P. H. B., and C. K. Mohan, "Cyber threat intelligence and security for federated learning in digital forensics," in Artificial Intelligence in Practice. Cham, Switzerland: Springer, 2025, pp. 177–199.

[9] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. Pangalos, "Actionable threat intelligence for digital forensics readiness," Information & Computer Security, vol. 27, no. 2, pp. 273–291, 2019.

Cyber Threat İntelligence Activity Detection and Digital Forensics

Adila Karimova
Azerbaijan Technical University, Baku, Azerbaijan
adila.karimova@aztu.edu.az

Abstract- As a result of the dynamic development of digital technologies, cyber threat intelligence has become much more complex and has become a source of serious threats. The complex, dynamic and secret nature of cyber threats poses a serious risk to the security of information systems of the state, organizations or institutions. A proactive defense strategy is of critical importance in terms of ensuring national security, economic stability, social stability and information security. This research study examines the methods of detecting and analyzing cyber threat intelligence activities, substantiates the role of digital forensics in this field and considers practical application possibilities. According to the research conducted, the application of digital forensics methods allows for the detection of cyber threat intelligence activities in real time and the legal validity of digital evidence.

Keywords - cyber threat; intelligence activities; digital forensics; digital evidence.