AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

YÜKSƏK TƏHSİL İNSTİTUTU

Əlyazması hüququnda

Abbasova Əminə Elşad qızı
Bağırova Fidan İlham qızı
Camalzadə Nuranə İqbal qızı
Civişov Elxan Elman oğlu
Məmmədova Fidan Həzi qızı

(Magistrantların S.A.A.)

“Açıq Kodlu Kibertəhdid Kəşfiyyatı Sisteminin İşlənməsi”

mövzusunda

MAGİSTRLİK DİSSERTASİYASI

060632 - İnformasiya texnologiyaları və sistemləri mühəndisliyi
(İxtisasın şifri və adı)

İnformasiya mühafizəsi və təhlükəsizliyi
(İxtisaslaşmanım adı)

Elmi rəhbər: **A. Y. KƏRİMOVA**

BAKI – 2024

AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

YÜKSƏK TƏHSİL İNSTİTUTU

MAGİSTRANTIN ANDI

"Açıq kodlu kibertəhdid kəşfiyyatı sisteminin işlənməsi" mövzusunda təqdim etdiyimiz magistrlik dissertasiyasını elmi əxlaq normalarına və istinad qaydalarına tam riayət etməklə və istifadə etdiyimiz bütün mənbələri ədəbiyyat siyahısında əks etdirməklə yazdığımıza and içirik və magistrlik dissertasiyasının AzTU Kitabxana İnformasiya Mərkəzində saxlanılsması, həmin mərkəz tərəfindən AzTU Rəqəmsal Repozitoriyasına daxil edilərək repozitoriyanın veb saytında yerləşdirilməsinə icazə veririk.

Abbasova Əminə Elşad qızı	
(Soyadı, Adı, Ata adı)	(imza)
Bağırova Fidan İlham qızı	
(Soyadı, Adı, Ata adı)	(imza)
Camalzadə Nuranə İqbal qızı	
(Soyadı, Adı, Ata adı)	(imza)
Civişov Elxan Elman oğlu	
(Soyadı, Adı, Ata adı)	(imza)
Məmmədova Fidan Həzi qızı	
(Soyadı, Adı, Ata adı)	(imza)

Tarix: *04.06.2024*

MÜNDƏRİCAT

İXTİSARLARIN SİYAHISI

API	Application Program Interface – *Tətbiqi proqramlaşdırma interfeysi*
CERT	Computer Emergency Response Team – *Kompüter insidentlərinə cavab komandası*
CIDR	Classless Inter-Domain Routing – *Sinifsiz Domenlərarası Marşrutlaşdırma*
CSV	Comma Separated Values – *Vergüllə ayrılmış dəyərlər*
CTI	Cyber Threat intelligence – *Kibertəhdid kəşfiyyatı*
CTI-TC	Cyber Threat Intelligence Technical Commitee – *Kibertəhdid kəşfiyyatı texniki komitəsi*
CVE	Common Vulnerabilities and Exposures – *Boşluqların ümumi tezaurusu*
CybOX	Cyber Observable eXpression – *Kiberdomendə müşahidələrin təsviri*
CyDefSIG	Cyber Defence Signatures – *Kiber Müdafiə İmzaları*
EDR	Endpoint Detection and Response – *Son nöqtənin aşkarlanması və cavablandırılması*
ENISA	European Network and Information Security Agency – *Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi*
GDPR	General Data Protection Regulation – *Ümumi Məlumatların Mühafizəsi Qaydası*
HTML	HyperText Markup Language – *Hipermətni nişanlama dili*
HTTP	HyperText Transfer Protocol – *Hipermətni ötürmə protokolu*
IoC	Indicators of Compromise – *Kompromis göstəriciləri*
IODEF	Incident Object Description Exchange Format – *Hadisə Obyektinin Təsviri Mübadilə Formatı*
IP	Internet Protocol – *İnternet Protokolu*

ISAC	Information Sharing and Analysis Centers – *Məlumat mübadiləsi və təhlil mərkəzləri*
JSON	JavaScript Object Notation – *Java Skript Obyekt İşarələri*
MISP	Malware Information Sharing Platform – *Zərərli proqram Məlumat Paylaşma Platforması*
OSINT	Open Source Intelligence – *Açıq Mənbə Kəşfiyyatı*
OSSIM	Open Source Security Information Management – *Açıq Mənbə Təhlükəsizliyi Məlumat İdarəetməsi*
OTX	Open Threat Exchange – *Açıq Təhdid Mübadiləsi*
SIEM	Security Information and Event Management – *İnformasiya təhlükəsizliyi məlumatlarının və hadisələrinin idarə edilməsi*
SOC	Security Operations Center – *Təhlükəsizlik Əməliyyatları Mərkəzi*
STIX	Structured Threat Information eXpression – *Strukturlaşdırılmış Təhdid Məlumatının İfadəsi*
TAXII	Trusted Automated Exchange of Indicator Information – *Kibertəhdid məlumatlarının avtomatlaşdırılmış etibarlı mübadiləsi*
TIP	Threat Intelligence Platform – Təhdid Kəşfiyyatı Platforması
TTP	Tactics, Techniques and Procedures – *Taktika, Texnika və Prosedurlar*
URL	Uniform Resource Locator – *Vahid resurs ünvanı*
US-CERT	United States Computer Emergency Readiness Team – *ABŞ Kompüter Fövqəladə Hallara Hazırlıq Komandası*
USM	Unified Security Management – *Vahid təhlükəsizlik idarəetməsi*
XML	Extensible Markup Language – *Genişlənən İşarələmə Dili*

GİRİŞ

İnformasiya texnologiyalarının sürətli inkişafı və hər bir sahədə istifadəsi kiber dünyada təhlükəsizlik məsələlərini ön plana çıxarır. Müasir dövrdə insanlar özlərinə aid olan informasiyaların böyük hissəsini kompüter, telefon və ya digər yaddaş qurğularında mühafizə edirlər. Əlavə olaraq müxtəlif dövlət orqanları, nazirliklər, hökümət təşkilatları və hərbi idarələr də dövlət əhəmiyyətli gizli informasiyaları elektronlaşmış şəkildə texnoloji sistemlərin daxilində yaradır, ötürür və saxlayırlar. Bununla da əgər bədniyyətli şəxs kompüter sisteminə giriş əldə edərsə informasiyaya icazəsiz baxa, dəyişdirə, silə və/və ya digər bu kimi ciddi fəsadlara səbəb ola bilər. Bu kimi təhlükələr nəzərə alınaraq dissertasiya işində informasiyanın qarşılaşa biləcəyi təhdidlərin aşkarlanması üsulları araşdırılmış, onların müqayisəsi aparılmış, təşkilat məlumatlarının mühafizəsi üçün müxtəlif kibertəhdid kəşfiyyatı metodları izah olunaraq onların xarakteristikaları araşdırılmışdır.

Mövzunun aktuallığı. Cari dövrdə kiberfəzada təhdidlər çox sürətlə inkişaf edir. Bununla da bir çox təşkilatlar daim mürəkkəb və bədniyyətli təhdidlərlə qarşılaşırlar. Kibercinayətkarlar əvvəllər olduğundan daha təkmil bacarıqlara malikdirlər, yaxşı təşkilatlanıblar və maliyyələşdiriliblər. Hal-hazırda kiberhücumların artmasının qarşısını almaq və onları erkən mərhələdə aşkarlamaq üçün kibertəhdid kəşfiyyatı (CTI) aktual mövzuya çevrilib. Tədqiqatda işlənilən sistem açıq mənbə prinsiplərini qəbul etməklə, kibertəhlükəsizlik üzrə qlobal miqyaslı ekspertlər, akademiklər və təşkilatlar arasında əməkdaşlığı və məlumat mübadiləsini təşviq edir. Bu əməkdaşlıq vaitəsilə inkişaf etməkdə olan kibertəhdidlərin daha tez aşkarlanması, araşdırılması və azaldılması mümkün olur. Bütün bunlar nəticə etibarilə kibertəhdidlərdən kollektiv müdafiə üsullarını təkmilləşdirir. Qeyd edilməlidir ki, CTI şəffaflığı və əlçatanlığı artırır. O, məhdud resursları olan təşkilatlara ən müasir təhdid kəşfiyyatı alətlərindən istifadə etməyə şərait yaradır. Bu həll yolu kibertəhlükəsizlik cəmiyyətinə qabaqcıl hücumlara qarşı daha qüvvətli müdafiə üsulları yaratmağa zəmin yaradır. CTI sisteminin yaradılması və işlənməsi kibertəhlükəsizliyi təmin etmək üçün birgə və icma əsaslı metodlarla doğru yanaşma aparılmasını hədəfləyir. Bu yanaşma daim

təkmilləşən kibertəhdidlərlə mübarizə zamanı effektivlik və çeviklik baxımından bir çox üstünlüklər təklif edə bilər.

Tədqiqatın məqsədi və məsələləri. Tədqiqat işinin məqsədi CTI platformalarının iş prinsipləri, standartları və formatlarının analiz edilməsi, belə sistemləri qurmaq üçün mövcud açıq kodlu proqram təminatının əsasında CTI sisteminin prototipinin yaradılmasıdır. Tədqiqat işinin məsələlərinə isə aşağıdakılar daxildir:

- Mövcud açıq kodlu təhdid kəşfiyyatı sistemlərinin analizi
- Təhdid kəşfiyyatı sisteminin işlənməsi üçün informasiya mənbələrinin müəyyən edilməsi
- Təhdid kəşfiyyatı sisteminin işlənməsi üçün informasiya mənbələrinin qiymətləndirilməsi metrikalarının işlənməsi
- Veb tətbiqin layihələndirilməsi və işlənməsi

Tədqiqatın obyekti və predmeti. Tədqiqatın obyekti təhdid kəşfiyyatı sistemləridir. Tədqiqatın predmeti isə açıq kodlu proqram təminatı əsasında kibertəhdid kəşfiyyatı sisteminin işlənməsidir. Tədqiqat metodu kimi maşın öyrənmə texnologiyalarından istifadə edilir. Eyni zamanda, ən son elmi nəşrlər əsasında mövcud tədqiqatların vəziyyəti də analiz edilir.

Tədqiqatın elmi yeniliyi və praktiki əhəmiyyəti. Tədqiqatda aşağıdakı elmi yeniliklər əldə edilmişdir:

- Təhdid kəşfiyyatı, onun mərhələləri, standartları, CTI platformalarının analizi konsepsiyalarına əsasən informasiya mühafizəsi üçün əsas prinsiplər araşdırılaraq təhid kəşfiyyatı sistemi haqqında analiz aparılmışdır.
- Açıq kodlu təhdid kəşfiyyatı sistemləri olan AlienVault OTX, CTI4SOC, DOCGuard, MISP və OpenCTI platformaları analiz olunaraq, onların müqayisəli təhlili aparılmışdır;
- Kibertəhlükəsizliyinin təmin olunması məqsədilə açıq kodlu təhdid kəşfiyyatının (OSINT) informasiya mənbələri müəyyən olunmuş, onlara əsasən

veb saytın layihələndirilməsi icra edilmiş və nəticədə yeni CTI sisteminin işlənməsi həyata keçirilmişdir.

Dissertasiya işinin strukturu: Tədqiqat işi giriş, 3 fəsil, nəticə, 63 ədəbiyyat mənbəyindən ibarət olmaqla 87 səhifədə təşkil olunmuşdur. İşdə 8 cədvəl, 24 şəkil yer almışdır.

Birinci fəsildə təhdid kəşfiyyatı anlayışının əsas prinsipləri haqqında məlumat verilmiş, təhdid kəşfiyyatı standartları və TIP-lərin mərhələləri analiz edilmişdir. Mövcud açıq kodlu CTI sistemləri haqqında məlumatlar qeyd olunmuşdur. Bununla yanaşı məqsədindən asılı olaraq ən çox istifadə edilən TIP-lər (ThreatConnect, Rapid7, Anomali, Mandiant Advantage və Recorded Future) analiz edilərək yarana biləcək təhdidlərə qarşı onların müdafiə üsulları müzakirə edilmişdir. Son olaraq isə tədqiqat məsələsinin qoyuluşuna baxılmışdır.

İkinci fəsildə açıq kodlu CTI sistemləri olan AlienVault OTX, CTI4SOC, DOCGuard, MISP, OpenCTI kimi OSINT platformalarının hər birinin xarakteristikası verilmiş, müxtəlif ədəbiyyatlardan götürülmüş xüsusiyyətləri analiz edilmişdir. Hər birinin istifadə məqsədləri də ayrı-ayrılıqda izah olunmuş və təhdidlərdən müdafiə yollarının müzakirəsi aparılmışdır.

Üçüncü fəsildə daha çox praktiki məsələlərə diqqət ayrılmış, informasiya təhlükəsizliyinin təmin olunması məqsədilə CTI sisteminin informasiya mənbələri haqqında ətraflı məlumat verilmiş, həmçinin seçilən mənbəyə uyğun veb tətbiqin layihələndirilməsi və işlənməsi məsələləri icra edilmişdir. Sonda veb saytın funksiyalarını göstərən eksperiment aparılmışdır. Dissertasiya işinin yekununda dissertasiyanın əsas elmi və praktiki nəticələri qeyd olunmuşdur.

Qrup üzvləri tərəfindən görülən işlər.

Elxan Civişov Elman oğlu tərəfindən təhdid kəşfiyyatının standartları, kəşfiyyat platformalarının analizi, OpenCTI platforması, informasiya mənbələrinin siyahısının müəyyən edilməsi, veb tətbiqin layihələndirilməsi və işlənməsi, sonda isə eksperimentlərin aparılması hissələri işlənilmişdir.

Əminə Abbasova Elşad qızı tərəfindən təhdid kəşfiyyatı anlayışının mahiyyəti, MISP Threat Sharing platforması, informasiya mənbələrinin siyahısının müəyyən edilməsi və nəticə hissələri işlənilmişdir.

Fidan Bağırova İlham qızı tərəfindən təhdid kəşfiyyatının standartları, AlienVault OTX platforması, CTI4SOC platforması və ixtisarların siyahısı hissələri işlənmişdir.

Fidan Məmmədova Həzi qızı tərəfindən giriş, təhdid kəşfiyyatı anlayışının mahiyyəti, tədqiqat məsələsinin qoyuluşu və ədəbiyyat siyahısı hissələri işlənilmişdir.

Nuranə Camalzadə İqbal qızı tərəfindən mündəricat, ixtisarların siyahısı, təhdid kəşfiyyatı proseslərinin mərhələləri, kəşfiyyat platformalarının analizi, kəşfiyyat standartları, tədqiqat məsələsinin qoyuluşu, DOCGuard platforması, informasiya mənbələrinin siyahısının müəyyən edilməsi, veb tətbiqin layihələndirilməsi və işlənməsi, eksperimentlərin aparılması və nəticə hissələri işlənilmişdir.

I FƏSİL. TƏHDİD KƏŞFİYYATI.

1.1. Təhdid kəşfiyyatı anlayışının mahiyyəti

Rəqəmsal informasiya texnologiyaları dövründə ən önəmli və çətin məsələlərdən biri əhəmiyyətli gizli təşkilat məlumatlarının təhlükəsizliyini təmin etməkdir. Kibercinayətkarlıqla mübarizədə təhdid kəşfiyyatı təşkilatları düşməndən bir addım qabaqda saxlamaq üçün təchiz edilən sursatdır (Seker E., 2019). Araşdırmalara əsasən son illərdə müxtəlif kibertəhdid növləri yaranmış və təhdidlə üzləşən sistemlərin saylarında kəskin artım olmuşdur. Kibertəhdid dedikdə sistemdə və ya təşkilat daxilində insidentə səbəb ola biləcək hər hansı bir kiber hadisə nəzərdə tutulur. Təhdidlərə misal olaraq sistemə icazəsiz girişləri, məlumatların dəyişdirilməsini, ələ keçirilməsini, pozulmasını və xidmətdən imtina olan DDoS hücumlarını göstərmək olar. Təhdidlər informasiya təhlükəsizliyinin üç əsas aspekti olan konfidensiallıq, tamlıq, əlyetərlik (ing. confidentiality, integrity, and availability) prinsiplərinin pozulmasına yönəlir (Mahmudova R., Daşdəmirova K., 2021).

Kibertəhdidlərin sürətli inkişafı nəticəsində təhdidləri aşkar və analiz etmək, onlara qarşı müdafiə olunmaq, eləcə də, onların qarşısını almaq çətin bir hal almışdır. Araşdırmalarda da görülür ki, hücumların xüsusiyyətlərini dərindən analiz etmədən, təhdid kəşfiyyatı və müvafiq müdafiə tədbirləri həyata keçirmədən iri miqyaslı hücumların qarşısını almaq qeyri-mümkündür. Buna görə də mütəxəssislər tərəfindən yeni termin olan təhdid kəşfiyyatı (ing. Threat Intelligence) anlayışı irəli sürülmüşdür. Bu anlayışın özü də tərkibində təhlükəsizlik təhdidləri, təhdid aktorları, zərərli proqramlar, boşluqlar ilə bağlı toplanan, qiymətləndirilən və tətbiq olunan məlumatlar toplusunu ehtiva edir (Friedman J., Bouchard M., 2015). Təhdid kəşfiyyatı vasitəsilə təşkilatlar hal-hazırda mövcud olan və ya inkişaf etməyə davam edən təhdid və ya risk barəsində məlumat əldə edirlər. Təhdid risklərinə təhdid aktoru tərəfindən sistemə icazəsiz giriş, məlumatlardan icazəsiz istifadə, gizli məlumatların açıqlanması, sistemdə icazəsiz dəyişikliklər və qanuni istifadəçi üçün girişin bloklanması proseslərini misal göstərmək olar. CTI vasitəsilə “False Positive”-lərin (və ya “False

Negative”-lərin) minimuma endirilməsi də kibertəhdiddən müdafiə üsulunun effektivliyini artırır.

Qabaqcıl rəqib taktikalarını, texnikalarını və prosedurlarını (ing. Tactics, Techniques, and Prosedures) öyrənmək CTI-ın aparıcı xassələrindən biridir. TTP-lər məqsədə çatmaq üçün təhdid aktorunun istifadə etdiyi metodlara istinad edir (Lekidis A., 2023):

- **“Taktika”** termini təhdid aktoru tərəfindən həyata keçirilən hərəkətlərin məqsədinin strateji izahını bildirir.
- **“Texnika”** termini təhdid aktoru tərəfindən həyata keçirilən faktiki hərəkətlərin taktika kontekstində daha ətraflı izahını bildirir.
- **“Prosedur”** termini təhdid aktorunun müəyyən bir yanaşmanı yerinə yetirmək məqsədilə istifadə etdiyi daha detallı təlimatları texnika kontekstində bildirir (Johnson C., Badger M. & Waltermire D., 2016).

TTP sistemdəki anomaliyaları aşkarlamağa, təhdid aktorlarını müəyyən etməyə və bəzən hücum baş verməmişdən əvvəl təhdidlərin qarşısını almağa yardım edə bilər. O, xüsusi hücumu planlaşdırmaq və idarə etmək üçün təhdid aktoru tərəfindən istifadə olunur. Təhdid aktorları rəqəmsal cihazlara və ya sistemlərə qəsdən zərər vuran bədniyyətli insanlar və ya təşkilatlardır. Əsasən təhdid aktoru qismində təşkilat rəqibləri və zərərverici bədniyyətlilər olur. Onlar fişinq, ransomware və zərərli proqram hücumları kimi bir neçə növ kiberhücum həyata keçirmək məqsədilə kompüter sistemləri, şəbəkələri və proqram təminatındakı boşluqlardan istifadə edirlər (Lee M., 2023).

Kibertəhdid kəşfiyyatı seçilmiş metodlardan asılı olaraq taktiki, operativ və strateji olmaqla üç növə ayrılır (Nova K., 2022):

- **Taktiki kibertəhdid kəşfiyyatı:** Taktiki kibertəhdid kəşfiyyatı rəqiblərin hücum etmək üçün istifadə etdikləri ən son taktika, texnika, və prosedurlar haqqında xüsusi informasiyaları araşdırır. Bu kəşfiyyat növü uzunmüddətli perspektivlərə fokuslanmır. Taktiki kibertəhdid kəşfiyyatı “nə” və “necə” suallarından yola çıxaraq ani təhdidlərə və xüsusi insidentlərə fokuslanır. O, hücumların necə həyata keçirildiyini müəyyən etməyə yardımçı olur. Bu kəşfiyyat növü təhdidlərə cavab

vermək üçün hərəkətə keçə bilən təlimat verir. Belə ki, təhdid aktoru öz TTP-sini həyata keçirir və bununla da onun hücumlarının təfərrüatı məlum olur. Bununla da onların hansı yolu izlədiyi müəyyənləşdirildikdən sonra səbəb olduqları təhdidlərin qarşısının alınması üçün müəyyən tədbirlər hazırlamaq mümkün olur. Taktiki CTI növündən istifadə edilərkən domen adları, URL-lər, fayl adları, IP ünvanları, heşlər və başqa mənbələr istifadə edilir.

- **Operativ kibertəhdid kəşfiyyatı:** Operativ kibertəhdid kəşfiyyatı "necə" və "nə vaxt" suallarından yola çıxaraq şirkət və ya təşkilatlara davam edən təhdidlər, rəqib taktikaları, hücumun vaxtı və təbiəti haqqında məlumat təqdim edərək təhlükəsizlik tədbirlərini aktiv şəkildə uyğunlaşdırmağa dəstək göstərir. Operativ kəşfiyyat menecerləri bu kəşfiyyat növü vasitəsilə təşkilatlarını qısa və orta müddətdə cari və potensial təhdidlərdən qorumağa imkan əldə edirlər. Sözügedən kəşfiyyat növündən istifadə edilərək təhdid aktorlarının rabitə kanallarının araşdırılması və gələn hücumların əvvəlcədən təxmin edilməsi məqsədilə sosial media, dark veb, çatlar və digər bu kimi şəxsi və ictimai mənbələrindən istifadə olunur.
- **Strateji kibertəhdid kəşfiyyatı:** Strateji kəşfiyyat yeni və yaranmaqda olan təhdid növlərinə və təşkilat üçün risk yarada biləcək rəqiblərə diqqət yetirir. Yəni yeni yaranan təhdidlərin motivasiyalarını vurğulamaq üçün istifadə olunur. Strateji CTI-lar "kim" və "niyə" suallarından yola çıxaraq hücumların arxasında duran niyyətləri və səbəbləri ortaya qoyur. O, xüsusilə kibertəhdidlərin arxasında duran şəxsi səbəbləri və onların hədəflərini müəyyənləşdirməyə çalışır. Strateji kibertəhdid kəşfiyyatı uzunmüddətli tendensiyalar, yaranan təhdidlər və kiber landşaftı formalaşdıran amillər haqqında daha geniş anlayış təklif edir.

Kibertəhdidlərin risk faktorlarını azaltmaq və qarşısını almaq məqsədilə onları anlamaq, analiz etmək və qabaqcıl tədbirlər görmək üçün beş metoddan istifadə olunur (Hassan N. A., Hijazi R., 2018):

- **TIP**: Təhdid Kəşfiyyatı Platformaları (TIP-lər) xarici təhdid məlumatlarını avtomatlaşdırılmış şəkildə toplayan, birləşdirən və analiz edən alətlərdir.

- **SIEM**: Təhlükəsizlik məlumatı və hadisələrin idarə edilməsi vasitələri olan SIEM alətləri sistem qeydləri, hadisə məlumatları və digər kontekst mənbələri daxil olmaqla daxili təhdid məlumatlarını toplayır və analiz edir.
- **Threat Intelligence Feeds**: Təhdid Kəşfiyyatı Lentləri xüsusi olaraq cari kibertəhdidlərərə fokuslanan real vaxt məlumat axınıdır. Onlara IP ünvanları, domenlər və zərərli proqram imzaları kimi maraq sahələri üzrə yeniləmələr daxildir (Brown S., Gommers J. & Serrano O., 2015).
- **Sandboxing Tools**: Sandboxing alətləri təşkilatların əsas sistemlərinə heç bir təhdid yaratmadan potensial təhlükəli məlumatları, proqramları və ya boşluqları analiz etmək və bəzən onlara daxil olmaq üçün təhlükəsiz mühit təmin edir.
- **OSINT tools**: Açıq mənbə kəşfiyyatı alətləri sosial media, bloqlar, açıq xəbər saytları və açıq müzakirə forumları kimi açıq mənbələrdən məlumat toplamaq üçün istifadə olunur. OSINT tool-lar haqqında 3.1-ci hissədə ətraflı məlumat verilmişdir.

CTI mənbələri, demək olar ki, kibertəhlükəsizlik mühitinin özü kimi müxtəlifdir. Buna baxmayaraq, CTI-nin bəzi ümumiləşdirilmiş tanınmış mənbələri var (Abu M. S., Selamat S. R. & Yusof R., 2018):

- **Daxili məlumatlar:** təşkilatın öz məlumat bazalarından, şəbəkə qeydlərindən, insident cavablarından və digər daxili mənbələrindən topladığı məlumatlar aid edilir.
- **Açıq mənbə kəşfiyyatı (OSINT):** ictimaiyyətə açıq olan və ictimai sahənin bir hissəsi hesab edilən mənbələrdən məlumat tapılır.
- **Qapalı mənbə kəşfiyyatı (CSINT):** daha geniş ictimaiyyət üçün əlçatmaz məlumatlardır.
- **Məlumat mübadiləsi və təhlil mərkəzləri (ISACs):** müvafiq təhdid məlumatlarını toplayan, analiz edən və əməkdaşlar arasında ötürən təşkilatlardır (Imamverdiyev, Y., 2018).
- **Hökumət tövsiyələri:** ABŞ-da FBI, Böyük Britaniyadakı Milli Kibertəhlükəsizlik Mərkəzi və ya Avropa İttifaqının Kibertəhlükəsizlik

Agentliyi olan ENISA kimi agentliklər tərəfindən yayılan məlumatlara istinad edilir (Əliquliyev R., İmamverdiyev Y., 2012).

- **Deep and dark veb kəşfiyyatı:** cinayətlər və fəaliyyətlər haqqında anlayışlar təklif edən şifrələnmiş və anonim məlumatlar aid edilir. Bu kəşfiyyat qaçılmaz hücumlar barədə erkən xəbərdarlıqla yanaşı təhdid aktorlarının səbəbləri və üsulları haqqında qiymətli biliklər verir (Basheer R., Alkhatib B., 2021).

Açıq Mənbə Kəşfiyyatı (Open Source İntelligence - OSINT) Platformaları ictimaiyyətə potensial kibertəhdidləri müəyyən etmək üçün açıq mənbələrdən məlumatları toplamağa və analiz etməyə imkan yaradır. Bu platformalar ortaya çıxan təhdidlər və düşmən taktikası haqqında kəşfiyyat məlumatları toplamaq üçün sosial media platformalarından, veb saytlardan, bloqlardan, forumlardan və digər onlayn mənbələrdən istifadə edir (Roberts A., 2021). Nəticədə təşkilatlara öz sistem boşluqları barəsində qeydlərə nəzarət etməyə imkan yaradır.

Açıq mənbə təhdid kəşfiyyatı ictimaiyyətdən və açıq mənbələrdən məlumat toplayır (Breeden J., 2023). Həmin mənbələrə misal olaraq aşağıdakılar göstərilə bilər (Quinlan S., Nguyen C. K., 2023):

- Media (qəzetlər, jurnallar, radio, televiziya və s.)
- İnternet (bloqlar, qaranlıq veb, veb saytlar, YouTube, Twitter, Facebook və s.)
- İctimai Hökumət Məlumatları (hökumət hesabatları, çıxışları, konfransları və s.)
- Peşəkar və Akademik Nəşrlər (jurnal, akademik məqalələr, dissertasiya və s.)
- Kommersiya məlumatları (kommersiya təsvirləri, maliyyə və sənaye qiymətləndirmələri və s.)
- Kommersiya nəşrlərində dərc olunmayan sübutlar (hesabatlar, patentlər, və s.).

Əlavə olaraq OSINT-in kəşfiyyatın tələblərindən asılı olaraq dəyişən 2 növü mövcuddur:

- **Aktiv OSINT:** məlumat əldə etmək üçün hədəflə birbaşa qarşılıqlı əlaqəni nəzərdə tutur. Bu, sosial media, e-poçt və ya hətta şəxsi əlaqə vasitəsilə həyata keçirilə bilər. Aktiv OSINT-in hədəf tərəfindən aşkar olunma ehtimalı daha yüksəkdir, lakin o, passiv OSINT-ə nəzərən daha faydalı məlumat verə bilər. Bu növ əsasən aşağıdakı hallarda istifadə olunur:

    - Kibercinayətkar və ya təhdid aktoru araşdırması
    - Bir təşkilatın şəbəkəsinə və ya təhlükəsizlik sistemlərinə pentestinq
    - Rəqib müəssisə və ya fiziki şəxsə aid məlumatların əldə edilməsi
- **Passiv OSINT:** hədəflə birbaşa iştirak tələb etmir. Bunun əvəzinə o, internet saytları, sosial media hesabları və axtarış motorları daxil olmaqla, ictimaiyyət üçün açıq olan mənbələrdən məlumatları toplayır. Passiv OSINT-in hədəf tərəfindən aşkar olunma ehtimalı azdır, lakin mənalı məlumat əldə etmək üçün daha çox vaxt və cəhd tələb oluna bilər. Bu növ isə əsasən aşağıdakı hallarda istifadə edilir:
    - Potensial işçinin keçmişinə dair hərtərəfli araşdırma aparmaq
    - Korporasiya və ya təşkilat haqqında araşdırma aparmaq
    - Trendləri və ya təhdidləri müəyyən etmək üçün sosial media monitorinqi

Aktiv OSINT mümkün qədər çox məlumat toplamaq üçün ideal strategiya ola bilər. Məqsəd gizli qalmaqdırsa, passiv OSINT ən yaxşı seçimdir. Hər iki növ OSINT həm müsbət, həm də mənfi məqsədlərə xidmət edə bilər. Məsələn, cinayətkarlar OSINT-dən istifadə edərkən mümkün hədəflər haqqında məlumat əldə etmək məqsədi daşıya bilərlər, hüquq-mühafizə orqanları isə cinayətləri araşdırmağı hədəfləyə bilərlər. OSINT-dən etik və düzgün istifadə etmək çox vacibdir.

Ümumi olaraq, CTI təhdid aktorları, onların istifadə etdiyi hücum alətləri, təhdid infrastrukturları və kəşfiyyat metodları haqqında məlumat verir. O, əsasən hücum növlərinin müəyyən edilməsinə, proseslərə qoyulan tələblərin təyin olunmasına, prioritetləşdirilməsinə, təhdid aktorunun istifadə etdiyi TTP-lərin müəyyən olunmasına, müdaxilələrin aşkarlanması sistemlərinin tətbiqinə və müdafiə strategiyalarının hazırlanmasına imkan verir. CTI təşkilatın bütün təhdidlərini anlamaq və onların təsirini minimuma endirmək üçün istifadə edilən əsas vasitədir. O, təşkilat üçün təhlükəsizliyə təhdid ola biləcək indiki, keçmiş və gələcək potensial hücumlar haqqında analiz edilmiş məlumatları, hücumların həyata keçirilməsində tez-tez istifadə olunan fayllar, IP ünvanları, domen adları və URL-lər kimi dərin informasiyaları təqdim edir.

1.2. Təhdid kəşfiyyatı proseslərinin mərhələləri

Texnologiyanın yüksək dərəcədə inkişaf etdiyi indiki dövrdə təşkilatlar öz sistemlərini, məlumatlarını və əməliyyatlarını təhlükə altına sala biləcək çoxsaylı təhdidlərlə üzləşirlər. PWC audit, konsaltinq və vergi xidmətləri şirkətinin 2021-ci il sorğusu baş icraçı menecerlər olan CEO-ların 95%-nin cavablarına əsasən kibertəhdidlərin şirkətin inkişafı üçün əsas təhlükə olduğunu göstərdi. Bu faiz 2020-ci ildəki 61%-dən demək olar ki, 1.5 dəfə çoxdur (PwC, 2021). CTI təşkilatlara kiberhücumları proqnozlaşdırmaq, təhdidləri müəyyən etmək, qiymətləndirmək və onlara cavab vermək üçün lazımi anlayışlar təqdim edərək, onlara qarşı müdafiənin mühüm elementi kimi seçilir. CTI-ın əsas proses mərhələləri əsasən 6 hissədən ibarətdir (Chantzios T. K., Paris D., 2019):

1. **İstiqamətləndirmə:** İlk mərhələdə kəşfiyyatın tələbləri müəyyən edilməli və razılaşdırılmalıdır. Kəşfiyyatın məqsədi, istifadə edəcəyi CTI növü (taktiki, operativ və ya strateji), əldə olunan məlumatların təqdim ediləcəyi format və məlumatın tələb olunduğu müddət əvvəlcədən təyin olunmalıdır. İstiqamətləndirmə mərhələsi CTI üçün hədəfləri müəyyən edir.
2. **Məlumatların toplanması:** CTI-ın 2-ci addımında həm daxili, həm də xarici mənbələrdən lazımlı xam məlumatların toplanması prosesi baş verir. Xarici məlumat bazalarına OSINT mənbələri, dark veb monitorinqi, TIP-lər, təhlükəsizlik təchizatçıları, hüquq-mühafizə orqanları və dövlət qurumları daxil olmaqla müxtəlif mənbələrdən məlumatların toplanması daxildir. Daxili məlumat bazalarına isə şəbəkə trafiki, daxili qeydlər və sistem xəbərdarlıqları aiddir.
3. **Məlumatların emalı**: 3-cü addım olan emal mərhələsində məlumatlar toplandıqdan sonra təşkilat tərəfindən istifadə edilə bilən formata çevrilir. Qeyd etmək lazımdır ki, bütün toplanmış məlumatlar ya manual, ya da avtomatik şəkildə emal edilməlir. Bu mərhələ aşağıdakı prosesləri ehtiva edir:
    - təsadüfən toplanmış qarışıq məlumatların filterizasiya prosesi olan süzgəcdən keçirilməsini
    - analiz mərhələsini asanlaşdırmaq üçün məlumatların strukturlaşdırılmasını
    - kontekstual informasiyalarla məlumatların zənginləşdirilməsini

- analiz mərhələsində istifadəsi təsdiq olunmuş oxşar məlumatların bir yerdə qruplaşdırılmasını

4. **Məlumatların analizi**: CTI-ın 4-cü addımı olan analiz mərhələsində emal edilmiş xam məlumat potensial təhdidləri göstərən nümunələri, tendensiyaları və kompromis göstəricilərini (IoC) müəyyən etmək üçün analiz edilir və əlaqələndirilir. Bundan əlavə, mərhələnin əsas tələblərinə təhdidlərin mahiyyətini anlamaq, təşkilata təsirini qiymətləndirmək və potensial riskləri və ya anomaliyaları müəyyən etmək aiddir. Məlumat analizini həyata keçirərkən müxtəlif standartlar nəzərə alınaraq maşın öyrənmə (ML) alqoritmlərindən, statistik analizlərdən və TIP-lərdən istifadə edilir (Preuveneers D., Joosen W., 2021). Əlavə olaraq, bu mərhələ vasitəsilə mənbələr təhdidlərin və boşluqların azaldılmasına yönləndirilə bilir.
5. **Məlumatların yayılması:** 5-ci addım olan bu mərhələdə analiz edilmiş kəşfiyyat məlumatları kibertəhdidlərə cavabı asanlaşdırmaq və əsaslandırılmış qərarların qəbul edilməsini təmin etmək üçün maraqlı tərəflər arasında paylaşıla bilər. Təhdid kəşfiyyatında təhlükəsizlik qrupları, insidentlərə cavab verən qruplar, rəhbərlər və tərəfdaşlar maraqlı olan tərəflərə misal olaraq göstərilə bilər. Təşkilatlar ortaya çıxan təhdidlər barəsində məlumatların mübadiləsini həyata keçirtmək məqsədilə müxtəlif təhdid kəşfiyyatı məlumatlarını paylaşan icmalarda, xüsusi Məlumat Paylaşma və Təhlil Mərkəzlərində (ISACs) və nüfuzlu dövlət qurumlarında iştirak edə bilirlər.
6. **Əks-əlaqə:** Son mərhələdə isə kəşfiyyat hesabatı ilə bağlı rəy əldə edildikdən sonra təhdid kəşfiyyatının məqsədə uyğunluğunu, aktuallığını və effektivliyini qiymətləndirmək mümkün olur. Əlavə olaraq, maraqlı tərəflər CTI mərhələlərində müəyyən dəyişikliklər istəsə, bununla bağlı əks-əlaqə vasitəsilə düzəlişlər edə bilərlər. Əks-əlaqə mərhələsinin ən vacib aspektlərindən biri də CTI-ın effektivliyini ölçmək məqsədilə performans göstəricilərinin yaradılmasıdır. Təşkilatlar davamlı inkişaf edən təhdidlərə cavab planlarını hazırlamaq, təhlükəsizlik nəzarətini həyata keçirmək, kiber insidentlərə effektiv cavab vermək

və təhlükəsizlik məlumatlılığını artırmaq üçün əks-əlaqədən istifadə edərək kəşfiyyatı təkmilləşdirməlidirlər (Samtani S., Abate M. Benjamin V., 2020).

Şəkil 1. Kibertəhdid kəşfiyyatının 6 əsas proses mərhələləri

Müasir dövrdə təhdid kəşfiyyatı prosesləri vasitəsilə kibertəhdidlərin fəal şəkildə müəyyənləşdirilməsi, analizi və təhdiddən müdafiə üsullarının həyata keçirilməsi mümkündür. Bunun əsas səbəbi isə təhdid kəşfiyyatının mərhələlərinin xətti proses deyil, daim təkmilləşdirmə və yeni təhdidlərə uyğunlaşma tələb edən təkrarlanan dövr olmasıdır. CTI-ın əsas istifadə məqsədləri aşağıda göstərilmişdir (Patel I., 2021):

- **Təhdidin erkən aşkarlanması:** CTI təşkilatlara hücumların qarşısını almaq üçün qabaqlayıcı tədbirlər görməyə imkan verməklə, yaranan təhdidlərin ilkin mərhələdə aşkar olunmasına imkan verir.
- **Təkmilləşdirilmiş Təhlükəsizlik Metodu:** Təşkilatlar CTI-dan istifadə etməklə öz təhlükəsizlik müdafiələrini gücləndirə, infrastrukturlarındakı boşluqları müəyyənləşdirə və riskləri azaltmaq üçün məqsədyönlü təhlükəsizlik tədbirləri həyata keçirə bilərlər.
- **Kontekstual Anlaşma:** CTI təhdidlərin motivasiyaları, TTP-ləri daxil olmaqla, təhdidlər haqqında daha dərin məlumatları təmin edir, və təşkilatlara təhdidlərlə effektiv mübarizə aparmaq üçün strateji qərarlar qəbul etməyə imkan yaradır.
- **Vaxtında operativ reaksiya:** Təşkilatlar vaxtında və avtomatik yerinə yetirilən təhdid kəşfiyyatı vasitəsilə inkişaf edən təhdidlərə operativ reaksiya verə, kiberhücumların təsirini azalda, və sistemin dayanma müddətini minimuma endirə bilərlər.
- **Risklərin İdarə Edilməsi:** CTI təşkilatlara təhlükəsizlik risklərini müəyyən etməyə, prioritetləşdirməyə və idarə etməyə kömək edir, onlara resursları səmərəli

şəkildə bölüşdürməyə, və aktivlərini qorumaq üçün kritik boşluqların aradan qaldırılmasına şərait yaradır.

CTI məlumatları açıq mənbə kəşfiyyatı olan OSINT, qapalı mənbə kəşfiyyatı olan CSINT, texniki kəşfiyyat olan TECHINT və insan kəşfiyyatı olan HUMINT daxil olmaqla müxtəlif mənbələrdən əldə edilə bilir (Ivanjko T., Dokman T., 2019). Təhlükəsizlik Əməliyyatları Mərkəzi (SOC) CTI vasitəsilə qərar qəbul etmək və cavab vermək imkanlarını artıra biləcək dəyərli anlayışlar təmin edə bilər (Crodis C., 2019) Əlavə olaraq SOC kontekstində CTI-ın əsas istifadə məqsədləri aşağıda göstərilmişdir:

- **Təkmilləşdirilmiş situasiya məlumatlılığı:** CTI müvafiq təhdid aktorları, kampaniyalar, TTP-lər, IoC-lar və hücum vektorları haqqında məlumat verməklə kibertəhdid mühiti haqqında hərtərəfli və vahid fikir əldə etməkdə SOC-a kömək edir. Bu, SOC-a ən əhəmiyyətli və təxirəsalınmaz təhdidləri müəyyən etməyə, onların cavab tədbirlərini prioritetləşdirməyə və resursları müvafiq şəkildə bölüşdürməyə imkan verir (Tserpes K., Gallicchio C. & Bravos G., 2023).
- **Təkmilləşdirilmiş təhdid aşkarlanması və qarşısının alınması:** SOC CTI-dən təsirli və müasir kəşfiyyat məlumatları əldə etməklə hücumları aşkar etmək və dayandırmaqda daha effektiv olur. Əlavə olaraq CTI təhlükəsizlik divarları (ing. Firewall), müdaxilənin aşkarlanaraq qarşısının alınması sistemləri olan IDPS, təhlükəsizlik məlumatı və hadisələrin idarə edilməsi olan SIEM, və son nöqtə mühafizə platformaları olan EPP kimi təhlükəsizlik alətləri və ya sistemlərini təkmilləşdirmək üçün istifadə edir (Alguliyev R., Nabiyev B. & Dashdamirova K., 2023).
- **Daha sürətli və effektiv cavab:** SOC CTI-nin köməyi ilə təhdidə cavab prosesini sürətləndirə və təkmilləşdirə bilir ki, bu da ona nəzarət, aradan qaldırma və bərpa kimi insidentlərə cavab tapşırıqlarında kömək edə biləcək müvafiq məlumat verir.
- **Proaktiv və Strateji Müdafiə:** CTI gələcək təhdidləri proqnozlaşdırmağa və onlara qarşı strateji müdafiə taktikası hazırlamağa kömək edə bilən kəşfiyyat üsulu verməklə SOC-a reaktiv və taktiki müdafiə mövqeyindən proaktiv və strateji mövqeyə keçməyə kömək edir. Əlavə olaraq, CTI SOC-a təhlükəsizlik proseslərindəki boşluqları tapıb düzəltməyə kömək etməklə yanaşı təşkilatın

məqsədlərinə uyğun olan daha güclü təhlükəsizlik planı quraraq onu həyata keçirməyə kömək edə bilər (CREST, 2019).

Ümumilikdə təşkilatlar istər açıq, istərsə də qapalı CTI sistemlərinin üstünlüklərindən istifadə edərək sərfəli şəkildə qiymətli təhdid kəşfiyyatı məlumatlarını əldə edə, təhdidin aşkarlanması metodlarını təkmilləşdirə və inkişaf etməkdə olan kibertəhdidlərə qarşı təhlükəsizlik vəziyyətlərini gücləndirə bilərlər.

1.3. Təhdid kəşfiyyatının standartları

Bilindiyi üzrə kibertəhdidlər daimi olaraq inkişaf edir. Bu proses fərdlər, təşkilatlar və dövlətlər üçün əhəmiyyətli problemlərə səbəb olur. CTI sadalanan maraqlı tərəflərə bu təhdidlərin başa düşülməsində, mümkün qədər azaldılmasında və effektiv cavablandırılmasında dəstək olur (Li Q., Yang Z., Liu B. & Jiang Z., 2017). Təhdid kəşfiyyat məlumatlarının toplanmasını, analizini, yayılmasını və mübadilə edilməsini asanlaşdırmaq üçün bəzi standartlar mövcuddur. Tədqiqatın bu bölməsi CTI standartları, onların əhəmiyyəti və onlar haqqında əsas məlumatlar barəsində geniş izah verir. Kibertəhdid kəşfiyyatı məlumatlarının mübadilə strukturunun standartlaşdırılması və birgə fəaliyyət göstərməsinin asanlaşdırılması üçün bəzi standartlar yaradılmışdır. Ən çox tanınan və istifadə olunan CTI standartlarına nümunə olaraq aşağıdakılar göstərilə bilər:

I. **STIX (Strukturlaşdırılmış Təhdid Məlumatının İfadəsi):**
   STIX strukturlaşdırılmış informasiya standartlarının təkmilləşdirilməsi təşkilatının (OASIS) CTI Texniki Komitəsi (CTI-TC) tərəfindən yaradılmış açıq mənbəli kəşfiyyat standartıdır (Barnum S., 2014). STIX standartı kompromis göstəriciləri olan IoC-lar, təhdid aktorlarının strategiyaları və TTP-ləri daxil olmaqla kibertəhdidlər barəsində məlumatı göstərmək məqsədilə strukturlaşdırılmış dil təklif edir. Bu standart qeyd olunan ümumi dil və formatdan istifadə edərək fərqli təhlükəsizlik təşkilatları arasında kibertəhdid məlumatlarının paylaşılması və analizini asanlaşdırır (Briliyant O., Tirsa N. & Hasditama M., 2021).
II. **TAXII (Göstərici məlumatlarının etibarlı avtomatlaşdırılmış mübadiləsi):**
   Kibertəhdid məlumatlarının avtomatlaşdırılmış mübadiləsini dəstəkləmək üçün OASIS CTI-TC tərəfindən hazırlanan digər standart TAXII-dir. TAXII vasitəsilə

etibarlı tərəflər arasında CTI məlumatlarının ötürülməsi və yönləndirilməsi üçün protokollar və xüsusiyyətlər müəyyənləşdirilir. Təşkilatlar TAXII standartına uyğun həlləri tətbiq edərək IoC-ları, təhdid hesabatlarını və digər CTI bazalarını etibarlı tərəfdaşlar və dövlət qurumlarıyla paylaşmaq məqsədilə təhlükəsiz və genişlənə bilən kanallar qura bilərlər (Dimitriadis A., Lontzetidis E., 2021).

III. CybOX (Kiber Müşahidə Edilə bilən İfadə):

CybOX, kiber hadisələrin və ya fəaliyyətlərin ölçülə bilən xüsusiyyətləri olan kiber müşahidə olunanları təmsil edən digər bir standartdır. CybOX şəbəkə göstəriciləri, reyestr açarları və fayl heşləri kimi texniki detalları göstərmək məqsədilə standartlaşdırılmış format təqdim edərək STIX standart dilini tamamlamaq üçün yaradılmışdır. Təşkilatlar CybOX-u CTI sistemlərinə əlavə edərək təhdid kəşfiyyatı məlumatlarının ardıcıllığına, bir-birləri ilə qarşılıqlı əlaqəsinə və zənginliyinə töhfə verə bilər. CybOX-un yaradılmasında məqsəd dəqiq avtomatlaşdırılmış paylaşma, xəritələşdirmə, aşkarlama və analiz üsullarının imkanlarını asanlaşdırmaqdır (Crisey E., Back G. & Barnum S., 2015).

IV. IODEF (İnsident Obyektinin Təsviri Mübadilə Formatı):

İnsident Obyektinin Təsviri Mübadilə Formatı olan IODEF standartı internet mühəndisliyi işçi qrupu olan IETF tərəfindən təhlükəsizlik insidentləri barəsində strukturlaşdırılmış məlumat mübadiləsi üçün hazırlanmışdır. IODEF standartı fəaliyyətin təsnifatı, təsirin qiymətləndirilməsi və cavab tədbirləri kimi nüansları da ehtiva etməklə insident hesabatlarının təsvir edilməsi məqsədilə XML əsaslı məlumat formatı təqdim edir. Təşkilatlar tərəfindən IODEF standartı qəbul edilərək hadisələrin idarə olunması prosesləri, məlumat mübadiləsi və xarici maraqlı tərəflərlə əməkdaşlıq effektiv şəkildə artırıla bilər (Mkuzangwe N., Khan Z., 2020).

Təşkilatlar və ümumillikdə kibertəhlükəsizlik ictimaiyyəti kibertəhlükəsizlik standartlarının qəbulu vasitəsilə bəzi üstünlüklər əldə edir. Yuxarıda ətraflı məlumat verilən STIX, TAXII, CybOX və IODEF kimi standartlar CTI məlumatlarını mübadilə etməyə görə ümumiləşdirilmiş protokollar təmin edərək qarşılıqlı strategiyalara kömək edir. Əlavə olaraq, təşkilatlar standartlaşdırılmış CTI həllərini tətbiq edərək təhdid kəşfiyyatının məlumatlarının toplanmasını, analizini və yayılmasını avtomatlaşdıra,

manual işi azalda və real vaxt rejimində cavablamanı sürətləndirə bilir (Abu M., Selamat S., Ariffin A. & Yusof R., 2018). CTI standartları həmçinin fərqli təşkilatlar, sektorlar, hətta coğrafi bölgələr arasında əməkdaşlığı və məlumatların mübadiləsini asanlaşdıraraq mübadilə əsasında toplanmış bütün təhdidlərdən kollektiv müdafiə imkanı yaradır. Yekun olaraq standartlaşdırılmış CTI strategiyaları kəşfiyyat məlumatlarının təqdim edilməsində ardıcıllıq və dəqiqliyi təmin edərək bölüşdürülən kəşfiyyatın faydalılığını və etibarlılığını artırır.

Nəticə olaraq kibertəhdidlər inkişaf etməyə davam etdiyi müddətdə, müəyyən edilmiş CTI standartlarından istifadə yeni təhdidlərə qarşı adaptiv və davamlı müdafiə imkanlarının yaradılmasında mühüm rol oynayacaq.

1.4. Təhdid kəşfiyyatı platformalarının analizi

Təhdid kəşfiyyatı platformaları (TIP) potensial təhdidləri və boşluqları müəyyənləşdirmək məqsədilə böyük həcmdə məlumatları birləşdirərək, əlaqələndirərək və analiz edərək müasir kibertəhlükəsizlik əməliyyatlarında əhəmiyyətli rol oynayır. Təşkilatların böyük bir qismi təhdid aşkarlama və monitorinq sistemlərinin, əsasən də SIEM-lərin boşluqlarını və məhdudiyyətlərini aradan qaldırmaq məqsədilə TIP-lərə etibar etməyə başladılar (Əliquliyev R., İmamverdiyev Y., 2012). Onlar müxtəlif kənar mənbələrdən həm strukturlaşdırılmış, həm də strukturlaşdırılmamış məlumatların əldə edilməsinə cavabdehdirlər. TIP-lər həmçinin məlumatların süzülməsi, yığılması, normallaşdırılması, aşkarlanması, analizi və zənginləşdirilməsi kimi bir sıra mürəkkəb tapşırıqları yerinə yetirirlər. Əlavə olaraq onlar alınan yeni məlumatları SIEM-lərə də ötürürlər. Lakin Sauerwein də qeyd etdiyi kimi, platformaların tətbiqi və istifadəsi hələ başlanğıc mərhələsindədir və hələ də həll edilməli olan bir sıra məsələlər var. Məsələn, qabaqcıl analiz imkanları və xarici mənbələrin dinamik etibarının qiymətləndirilməsi üçün hələ də insan faktoruna ehtiyac var (Sauerwein C., 2017).

Məlumatların toplanması, saxlanması, mübadiləsi və xarici qurumlarla inteqrasiyası üçün TIP əvəzolumaz üsullardan biridir. Onların əsas üstünlüyü birgə müdafiə strategiyasını təşviq etmək qabiliyyətidir. İndiki bir-biri ilə əlaqəli rəqəmsal

ekosistemdə bir təşkilata yönəlmiş kiberhücum bütün sənaye və coğrafiyalar üzrə çoxsaylı təşkilalara təsir edərək domino effekti yarada bilər. Təşkilatlar etibarlı şəbəkə olan TIP daxilində CTI mübadiləsi apararaq paylaşılan nümunələri, IoC-ları aşkar etmək və təhdid aktorları tərəfindən istifadə olunan strategiyaları inkişaf etdirmək üçün əməkdaşlıq edə bilirlər. Bu ortaq biliklərdən istifadə etməklə iştirakçılar təhlükəsizlik protokollarını tənzimləyirlər, və təhdidlərin potensial təsirini genişmiqyaslı fəlakətlərə çevrilməzdən əvvəl minimuma endirmə şansı əldə edirlər (Faiella M., Granadillo G., 2019).

Tarixən kibertəhlükəsizlik sahəsində məlumat mübadiləsininin aparılmasına məlumatların məxfiliyi, mülkiyyət hüquqları və qanunvericilik məhdudiyyətləri ilə bağlı narahatlıqlar mane olub. Buna baxmayaraq, bu platformalar hal-hazırda müvafiq qanuni və tənzimləyici təlimatlara əməl edərək istifadəçilərin məlumat mübadiləsi üçün təhlükəsiz və mütəşəkkil məkan təklif edir. Qeyd olunduğu kimi, CTI platformaları üstünlüklərinə baxmayaraq bir sıra problem və mülahizələrlə qarşılaşır. Əsas məsələ gizli məlumatların açıqlanması ilə fərdi məxfilik və mülkiyyət maraqlarının qorunması arasında balans yaratmaqdır. Problemləri aradan qaldırmaq və platforma üzvləri arasında inam yaratmaq üçün 3 əsas göstəriciyə malik olmaq çox vacibdir (Özeren S., 2024):

- effektiv idarəetmə strukturları
- gizli məlumatların anonimləşdirilməsi üsulları
- məlumat mübadiləsi üçün standartlaşdırılmış normalar

Kibertəhlüəsizlik üzrə redaktor Jenna Phipps-in apardığı araşdırmalara əsasən 2024-cü ilin ilk rübü ərzində təşkilatların istifadəsinə yararlı müxtəlif göstəricilər üzrə 5 ən yaxşı təhdid kəşfiyyatı platformalarını müəyyən etmişdir (Phipps J., 2024). Sözügedən platformalar bunlardır:

1) **ThreatConnect**

ThreatConnect təşkilatlara kibertəhlükəsizlik təhdidlərini aşkarlamaq, idarə etmək və azaltmaqda kömək etmək məqsədilə nəzərdə tutulmuş kibertəhlükəsizlik platformasıdır. ThreatConnect platforması təhdidləri effektiv şəkildə izləmək və prioritetləşdirmək üçün təhdid kəşfiyyatının toplanması, analizi və paylaşılması, eləcə

də fərdiləşdirilə bilən idarə panelləri və hesabat alətləri kimi xüsusiyyətləri təklif edir (Aggarwal D., Gautam S., 2017). Onun yerləşdirilmə çevikliyi, geniş CTI imkanları və bir çox üçüncü tərəf birləşdiriciləri onu təşkilatlar üçün əvəzolunmaz platforma edir. Qabaqcıl funksiyalara təhdid qrafiki və MITRE ATT&CK arxitekturasının xəritələşdirilməsi də daxildir. MITRE ATT&CK arxitekturası hücumları kateqoriyalara ayırmaq, hücumun mənbəyini və məqsədlərini müəyyən etmək və təşkilatın zəiflik səviyyəsini qiymətləndirmək üçün yaradılmış strategiya və metodların deposudur (Sytrom B., Applebaum A. & Miller D., 2018). ThreatConnect geniş imkanlara və təhlükəsizlik əlaqələrinə ehtiyacı olan müəssisələr üçün uyğundur. Təhlükəsizlik əməliyyatları mərkəzlərindəki SOC komandalar platformanın təqdim etdiyi riskləri avtomatlaşdıraraq sıralaya bilər (Keim Y., Mohapatra A., 2022). ThreatConnect platformasının müsbət və mənfi cəhətləri aşağıda qeyd olunmuşdur:

Cədvəl 1. ThreatConnect platformasının müsbət və mənfi cəhətləri

Müsbət cəhətlər	Mənfi cəhətlər
➢Korporativ səviyyəli CTI platforması xüsusiyyətlərinin bolluğunu təklif edir. ➢Qabaqcıl təhlükəsizlik platformaları ilə mükəmməl inteqrasiya edir, qarşılıqlı fəaliyyət qabiliyyətini artırır və təhdidlərin idarə edilməsini asanlaşdırır. ➢Təşkilat infrastrukturlarının ehtiyaclarını ödəmək üçün fərdi həll yolu variantları təklif edir.	➢Müştəri xidmətləri haqqında ətraflı məlumatın olmaması istehlakçıların suallarına cavab vermək və ya problemlərini tez həll etməyə mane ola bilər. ➢Pulsuz sınaq seçiminin olmaması platformanın uyğunluğunu və effektivliyini qiymətləndirmək imkanlarını məhdudlaşdırır. ➢Qiymət şəffaflığının olmaması təşkilatlara problem yaradaraq qərarların qəbul edilməsinə və büdcə planlaşdırılmasına mane ola bilər.

Nəticə olaraq, ən yaxşı TIP-lərdən biri kimi qiymətləndirilən ThreatConnect mürəkkəb məlumatları başa düşülən, faydalı fikirlərə çevirmək üçün analitika, avtomatlaşdırma, kəşfiyyat və risk kəmiyyətini birləşdirən hərtərəfli platforma təqdim edir. ThreatConnect API istifadəçilərə HTTP sorğularından istifadə edərək proqramlı şəkildə ThreatConnect məlumatlarına daxil olmaq və JavaScript Obyekt Notasiyası olan JSON istifadə edərək strukturlaşdırılmış cavablar almaq imkanı verir. Bu, analitik

prosesi optimallaşdırmaq və məlumatlardan fərdi seçimlərə uyğun istifadə etmək üçün digər məhsulların inteqrasiyasına imkan verir (Keim Y., Mohapatra A., 2022). Platformadan faydalanan istifadəçilərin sayı alınmış üzvlük planından asılıdır. Lakin, bu planın sayında məlumatı yalnız oxuyan və şərh yazan istifadəçilər üçün məhdudiyyəti yoxdur.

2) Rapid7 Threat Command:

Rapid7 Threat Command birbaşa təşkilatlara və fərdlərə yönəlmiş təhdidləri aşkar edən və dayandıran yüksək texnologiyalı CTI platformasıdır. Bu platforma ağıllı seçimlər etməklə və surface, deep, dark vebdəki minlərlə mənbəyə nəzər salmaqla təhlükəsizliyi qorumaq üçün cəld hərəkət etməyə imkan yaradır. Onun ən vacib xüsusiyyətlərindən bəziləri IoC prioritetləri, təhdidin şiddət dərəcəsini hesablama və açıq mənbəli kəşfiyyat bazalarına qoşulma qabiliyyətidir (Preuveneers D., Joosen W., 2021). Threat Command platforması şəbəkə hesabatları, xəbərdarlıq hesabatları, icraçı qeydləri və oğurlanmış parol hesabatları kimi müxtəlif növ hesabatlar hazırlamağa imkan verir. Bununla yanaşı Threat Command InsightIDR, Rapid7-nin SIEM-i, EDR və insidentlərə cavab platforması ilə inteqrasiya edir. Threat Command platformasının müsbət və mənfi cəhətləri aşağıda qeyd olunmuşdur:

Cədvəl 2. Rapid7 platformasının müsbət və mənfi cəhətləri

Müsbət cəhətlər	Mənfi cəhətlər
• 1-ci dərəcəli problemlər üçün 24/7 dəstək verir, mühüm hadisələr üçün operativ kömək və həlli təmin edir. • InsightIDR həlli və digər TIP-lərlə birləşərək kibertəhlükəsizlik ekosistemində uyğunluğu təkmilləşdirir. • İstifadəçilər platformanın imkanlarından uğurla istifadəyə imkan verən geniş çeşiddə təlim videoları və materialları əldə edə bilirlər.	• Peşəkar texniki hesab menecerinin olmaması platformanın təşkilat üçün daha yaxşı servis etməsinə mane ola bilər. • Pulsuz sınaq seçiminin olmaması platformanın uyğunluğunu və effektivliyini qiymətləndirmək imkanlarını məhdudlaşdırır. • Təhdidləri təsnif edən bəzi funksiyalar çatışmaması təhdidlərin səhv təhlil edilməsinə və onlara yanlış cavab verilməsinə səbəb ola bilər.

Nəticə olaraq, Rapid7 Threat Command təhdid kəşfiyyatını avtomatlaşdırılmış təhlükəsizlik prosesinə çevirərək proaktiv müdafiəni təmin edir və bununla da riskin azaldılması üçün həyat dövrünü avtomatlaşdırır.

3) Anomali ThreatStream:

Anomali ThreatStream yeni təhdidləri tapmaq, təhlükəsizlik xətalarını aşkarlamaqda və təhlükəsizlik qruplarına riskləri dərk edərək azaltmaqda kömək edən CTI platformasıdır. ThreatStream Anomali 100-dən çox açıq mənbə lentinə sahibdir. Bu, təhdid məlumatlarını görmək istəyən təşkilatlar üçün çox yaxşı platformadır. ThreatStream saytda və Cloud mühitində proqram təminatı kimi quraşdırıla bilər (Strom B.E., Appebaum A. & Miller D.P., 2020). Anomali ThreatStream platforması ML-dən istifadə edərək təhdidləri ciddiliyinə görə qiymətləndirə və sıralaya bilir. ThreatStream bir sıra firewall, SIEM və EDR həlləri ilə inteqrasiya edərək hücumun bloklanmasını avtomatlaşdırır. ThreatStream təşkilatlara Anomalinin öz lentlərini, çoxlu açıq mənbəli lentlər və ödənişli lentlər kimi bir sıra seçimlər təqdim edir. ThreatStream platformasının müsbət və mənfi cəhətləri aşağıda qeyd olunmuşdur:

Cədvəl 3. Anomali ThreatStream platformasının müsbət və mənfi cəhətləri

Müsbət cəhətlər	Mənfi cəhətlər
➢Bir sıra sistem tərəfdaşları ilə işləyərək təhdid məlumatlarını və ümumi mühafizəni yaxşılaşdırmaq üçün istifadə olunan resurslar yaradır. ➢Fərqli mənbəli lentlərlə işləyir, təhdid məlumatlarına müxtəlif mənbələr əlavə edir və təhdidləri təhlil edib cavab verməyə imkan verir. ➢İstifadəçilərə platformadan yaxşı istifadə etmək və təhdid kəşfiyyatı əməliyyatlarını təkmilləşdirmək üçün ThreatStream üzrə təlim təklif edir.	➢Təhdid xəbərdarlıqlarının idarə edilməsi funksiyası aydın olmadığı üçün istifadəçilərin platforma daxilində təhlükəsizlik məsələlərini çətinləşdirə bilər. ➢Müştəri xidmətləri məlumatının aydın olmaması istehlakçıların suallarına cavab verməyə və problemlərini tez həll etməyə mane ola bilər. ➢Pulsuz sınaq seçiminin olmaması platformanın uyğunluğunu və effektivliyini qiymətləndirmək imkanlarını məhdudlaşdırır.

Anomali şirkəti 2013-cü ildə yaradılıb və o vaxtdan etibarən 250-dən çox işçi qüvvəsi toplayıb və yarandığı gündən bəri ümumi investisiyası 96,3 milyon dollardan

çox təşkil edib. Anomali öz saytında xidmət qiymətlərini dərc etməsə də, Amazon Veb Servislər bazarı göstəricilərinə əsasən 3500 işçili bir təşkilat üçün Anomali Threatstream-ə illik abunə haqqı 150.000 dollara başa gəlir (AWS Marketplace, 2024).

4) Mandiant Advantages

Google Cloud idarə olunan müdafiə və hücum səthinin idarə edilməsinə əlavə olaraq təhdid məlumatı verən kibertəhlükəsizlik platforması Mandiant Advantage-ə sahibdir. Bu platforma, idarə paneli, təhdid aktoru, zəiflik məlumatları və OSINT göstəriciləri daxil olmaqla məhdud funksiyaları olan pulsuz versiya təklif edir. Mandiant Advantage böyük təşkilatlar üçün yaxşı seçimdir. Həmçinin, kiçik və orta bizneslər də bu məşhur platformanı çox istifadə edirlər, çünki ödəniş etmədən limitli funksiyalarla olsa belə əsas təhdid kəşfiyyatı imkanlarına sahib ola bilirlər. Mandiant Advantage kiçik təşkilatlar üçün uyğun olan və fundamental CTI imkanlarını təklif edən təqdirə layiq TIP-dir (Phipps J., 2024) Lakin, təhdid aşkarlama standartları və sandbox inteqrasiyaları kimi bəzi mürəkkəb xüsusiyyətlərə malik deyil. Mandiant Advantage platformasının müsbət və mənfi cəhətləri aşağıda qeyd olunmuşdur:

Cədvəl 4. Mandiant Advantages platformasının müsbət və mənfi cəhətləri

Müsbət cəhətlər	Mənfi cəhətlər
➢Pulsuz versiya təqdim edir və təşkilatlara heç bir ilkin pul öhdəliyi olmadan kritik funksiyalaradan istifadə etmək imkanı verir. ➢İstifadəçilər hər hansı texniki problem və ya sorğuların operativ yardım və həllinə zəmanət verən 24/7 dəstəkdən istifadə edə bilərlər. ➢Təşkilatın təhlükəsizlik arxitekturasında təhdidlərin idarə edilməsinə imkan verən Firewall, EDR və SIEM interfeysləri ilə inteqrasiya təklif edir.	➢Bəzi mürəkkəb imkanlarının olmaması onun mürəkkəb təhlükəsizlik tələbləri və ya xüsusi uyğunluq tələbləri olan təşkilatlar üçün həyat qabiliyyətini məhdudlaşdıra bilər. ➢API olmaması fərdiləşdirmə və inteqrasiya cəhdlərinə mane ola bilər, dəyişən təhlükəsizlik tələblərinə cavab verməkdə platformanın çevikliyini və miqyasını məhdudlaşdıra bilər.

5) Recorded Future:

Recorded Future tərəfindən təqdim edilən Təhdid Kəşfiyyatı Bulud Platforması, kəşfiyyat qrafikindən istifadə edərək sistemi analiz etmək məqsədilə təhdid məlumatlarını toplayır və təşkil edir. Əlavə platforma funksiyalarına MITER

ATT&CK çərçivəsi ilə xəritələşdirmə və təhdid reytinqi daxildir. Recorded Future, bir çox imkanları özündə birləşdirən pulsuz brauzer plug-in təmin etdiyinə görə təşkilatlar üçün sərfəli seçimdir. Əlavə olaraq, bu platforma icra dəstəyi üçün ödəniş etməyi seçən təşkilatlar üçün ixtisaslaşmış texniki hesabat meneceri təklif edir.

Recorded Future tərəfindən təqdim edilən Detection Rule API istifadəçilərə Snort, Sigma və YARA təhdid aşkarlama qaydalarını əldə etməyə imkan verir. Əlavə olaraq, platforma daxilində olan risk siyahıları təhlükəsizlik insidentlərini əlaqələndirmək üçün istifadə edilə bilər və hər biri üçün reytinqləri olan bir sıra təhdidləri ehtiva edir. Recorded Future's Threat Monitor platforması vasitəsilə sosial media və dark veb də daxil olmaqla müxtəlif mənbələrdən təhdid məlumatları alınır. Həmin məlumatlar real vaxt rejimində e-poçt xəbərdarlıqları yaratmaq üçün istifadə olunur. Recorded Future platformasının müsbət və mənfi cəhətləri aşağıda qeyd olunmuşdur:

Cədvəl 5. Recorded Future platformasının müsbət və mənfi cəhətləri

Müsbət cəhətlər	Mənfi cəhətlər
➢ Veb-brauzerlərdə onlayn təhlükəsizliyi təkmilləşdirmək üçün pulsuz brauzer proqramı təqdim edir. ➢ Fərdi təhlükəsizlik tələblərini platformanın xüsusiyyətlərini əlavə etməyə və dəyişdirməyə imkan verən API mövcuddur. ➢ Təşkilatlara mümkün risklər haqqında daha çox məlumat vermək üçün şübhəli hərəkətlərə dəqiq baxmaq imkanı verən dərin təhlil üçün biznes test aləti təklif edir.	➢ İnsidentlərə cavab vermək imkanları yoxdur ki, bu da təşkilatların real vaxt rejimində təhlükəsizlik məsələlərinin idarə edilməsinə mane ola bilər. ➢ İstehlakçıların texniki yardım almasına kömək ola biləcək telefon və ya canlı söhbət dəstəyi yoxdur. ➢ Hesabat vermə qabiliyyəti qeyri-müəyyəndir. Bu da istifadəçilərin təhlükəsizlik hadisələri, təhdidlər və platformadan istifadə ilə bağlı tam məlumatları toplamaq və təhlil etmək imkanlarını məhdudlaşdıra bilər.

Recorded Future, təhlükəsizlik qruplarına riski azaltmaq üçün unikal ML ilə idarə olunan tam CTI sistemi verə bilən yeganə şirkətdir. Amazon Veb Servislər bazarına istinadən, bu platforma vasitəsilə təhdidləri 10 dəfə tez tapmaq, baş verməmişdən əvvəl 22% daha çox təhdidləri aşkar etmək və təhdidlərdən 63% daha tez xilas olmaq mümkündür (AWS Marketplace, 2024).

Kibertəhlükəsizlik sferasında çox sayda TIP-ləri mövcuddur. Lakin adıçəkilən platformalar bəzi unikal güclü tərəflərinə görə digər qeyd olunmayan platformalardan fərqlənir. Həmin güclü tərəflər aşağıda qeyd olunmuşdur:

- **ThreatConnect** platforması müxtəlif funksiyalar və birləşdiriciləri özündə birləşdirən çevik həll axtaran təşkilatlar üçün ən yaxşı seçimdir.
- **Rapid7 Threat Command** platforması çox ciddi təhlükəsizlik ehtiyacları olan insanlar üçün əvəzolunmazdır, çünki bu ehtiyaclara cavab verən bir çox güclü xüsusiyyətlərə malikdir.
- **Anomali ThreatStream** platforması təşkilat daxili və bulud əsaslı həllərin mükəmməl birləşməsini təklif edərək, hibrid tətbiqi araşdıran təşkilatlara yol göstərir.
- **Mandiant Advantage** platforması pula qənaət etmək istəyən insanlar üçün ən yaxşı seçimdir, çünki aylıq ödəniş tələb etmədən bir çox təhlükəsizlik funksiyaları təklif edir.
- **Recorded Future** platforması xüsusi ehtiyacları olan kiçik komandalar üçün ən yaxşı seçimdir, çünki o, kiçik müəssisələrin ehtiyaclarına uyğun hazırlanmış həllər təklif edir.

CTI platformaları bazarı öz daxilində çox rəqabətlidir. Əsas oyunçular olan tanınmış platformalar həmişə texnologiyalarınını təkmilləşdirməyə və bazarda iştiraklarını artırmağa çalışırlar. Yaxın bir neçə il ərzində bazarın çox böyüməsi ehtimalı var. Bunun səbəbi, onlayn təhdidlərin getdikcə artması və insanların daha təkmilləşdirilmiş təhlükəsizlik strategiyalarına ehtiyacı olmasıdır (İmamverdiyev Y., Muradova G., 2019) Şimali Amerika, Asiya-Sakit Okean, Avropa, ABŞ və Çin də daxil olmaqla çoxsaylı bölgələrin qlobal TIP bazarında əhəmiyyətli genişlənməyə şahid olacağı gözlənilir. Qabaqcıl kibertəhlükəsizlik həllərinin artan tendensiyası və əhəmiyyətli sənaye iştirakçılarının olması səbəbindən bazarda Şimali Amerikanın, xüsusən də ABŞ-ın üstünlük təşkil edərək bazarın təxminən 40%-ni təşkil edəcəyi gözlənilir. Avropanın təxminən 25% bazar payına sahib olacağı proqnozlaşdırılır, Asiya-Sakit Okean və Çinin isə müvafiq olaraq bazar payının 20% və 15% olacağı gözlənilir (Sukshi R., 2017).

Yekun olaraq, göründüyü kimi TIP-lər müasir kibertəhlükəsizlik əməliyyatlarının ayrılmaz tərkib hissəsidir və təşkilatlara yaranan təhdidləri proaktiv şəkildə aşkar edərək onlara cavab vermək imkanı təklif edir. Məlumatların toplanması, avtomatlaşdırılması, fərdiləşdirilməsi, istifadəçi təcrübəsi, miqyaslılıq, uyğunluq, inteqrasiya və qiymət kimi amillər nəzərə alınaraq, təşkilatlar tərəfindən öz unikal tələblərinə ən yaxşı uyğun gələn və ümumi təhlükəsizlik vəziyyətini yaxşılaşdıran TIP-lər seçilə bilər. Daim dəyişən kibertəhdid risklərini effektiv şəkildə idarə etmək və daha təhlükəsiz rəqəmsal gələcəyi təmin etmək məqsədilə bu platformalara davamlı investisiyalar etmək və əməkdaşlığa üstünlük vermək əhəmiyyətlidir.

1.5. Tədqiqat məsələsinin qoyuluşu

Elmi tədqiqatların sistemləşdirilməsi və təhlili prosesi vasitəsilə bu dissertasiya işində aşağıdakı tədqiqat məsələləri qoyulmuşdur:

- Tədqiqat mövzusu çərçivəsində əvvəlki illərdə əhəmiyyətli tədqiqat nəşrlərinin qısa şəkildə analizi;
- Açıq mənbələrdən toplanan məlumatlar əsasında AlienVault OTX, CTI4SOC, DOCGuard, MISP Threat Sharing, OpenCTI kimi sistemlərində açıq kodlu təhdid kəşfiyyatının aparılması, bu platformaları müqayisəli şəkildə təhlil edib, hər birinin xüsusiyyətlərinin aşkara çıxarılması;
- Praktiki məsələlərə diqqət ayıraraq informasiya təhlükəsizliyinin təmin olunması üçün təhdid informasiya mənbələrinin müəyyən edilməsi;
- Python dilində məlumat axtarış botu vasitəsilə veb tətbiqin layihələndirilməsi və işlənməsi məsələlərinin icra edilməsi;
- Veb tətbiqin funksionallığının və OSINT platformalarında yoxlanışının eksperimentlərinin aparılması.

II FƏSİL. AÇIQ KODLU TƏHDİD KƏŞFİYYATI SİSTEMLƏRİNİN ANALİZİ.

Açıq mənbə təhdid kəşfiyyatı platformaları təhdidlərin aşkarlanması, analizi və onlara cavab tədbirlərini asanlaşdırmaq məqsədilə açıq kodlu kəşfiyyatı qabaqcıl analitika və avtomatlaşdırma imkanları ilə birləşdirən hərtərəfli platformalardır. Bu platformalar vasitəsilə təşkilatlar müxtəlif təhdid məlumat mənbələrini qəbul edə, normalara uyğun hala sala və əlaqələndirə bilir. Bundan əlavə, təhlükəsizlik qrupları həmin platformalarla kibertəhdidləri göstərən nümunələri əldə edir və anomaliyaları aşkar etmək məqsədilə səlahiyyət ala bilir (Faiella M., Granadillo G., Azevedo R. & Zarzosa S., 2019). OSINT platformalarına nümunə olaraq AlienVault OTX, zərərli proqram məlumat paylaşma platforması olan MISP (ing. Malware Information Sharing Platform), CTI4SOC, DOCGuard və OpenCTI platformaları daxildir.

2.1. AlienVault OTX

Open Threat Exchange (OTX) dünyanın ilk açıq mənbəli təhdid kəşfiyyat platforması kimi tanınır. 2016-cı ildə istifadəyə verilmiş AlienVault isə OTX-in yenilənmiş versiyasıdır. O, Intel və Hewlett Packard ilə əməkdaşlıq edir. AlienVault tədqiqatçılar və təhlükəsizlik mütəxəssisləri üçün dünya miqyasında şəbəkə təklif edir. Onun vasitəsilə istifadəçilər fəal şəkildə müzakirələrdə iştirak edə, araşdırma apara və təhdid məlumatlarını mübadilə edə bilərlər. OTX icması “Pulse”-lar (az. nəbz) əsasında fəaliyyət göstərir. Pulse-lar təhdid xülasəsindən, təhdid məlumat hesabatından və IoC-lardan ibarətdir (CREST, 2019).

AlienVault, təhdid kəşfiyyat keyfiyyətini daha da artırmaq üçün AlienVault OTX-ni təqdim etdi. Qlobal miqyasda ən böyük təhdid informasiyası paylaşan icmalardan biri olan OTX 140 ölkədən 53.000-dən çox insanı bir araya topladı. Bu iştirakçılar birlikdə gündəlik olaraq 10 milyondan çox IoC təqdim edirlər. Bundan əlavə, icma üzvləri hər gün orta hesabla 10 yeni “Pulse” təqdim edirlər. “Pulse”-lar icma üzvləri tərəfindən təqdim olunan təhdid analizi brifinqləridir.

İstifadəçilərə təhdid məlumatlarını anonim şəkildə daxil etmək və paylaşmaq imkanı verən AlienVault-un vahid təhlükəsizlik idarəetməsi olan USM sistemindən və

OSSIM məhsul quraşdırmalarından gündə yüz minlərlə məlumat gəlir. Daha çox əməkdaşlıq keyfiyyətin və şəffaflığın artması ilə nəticələnir. Əlavə olaraq, AlienVault OTX platformasında olan təhdidlərin fəal müzakirəsi aktı təşkilatlar tərəfindən yeni təhdid məlumatlarının yoxlanılmasının və onlardan müdafiənin həyata keçirilməsinin sürətini artırır. Təhdid məlumatı OTX qrupuna "Pulse" şəklində göndərilir və qəbul edilir. "Pulse"-da ən azı bir, adətən isə birdən daha çox IoC olur. IoC şəbəkədə və ya son nöqtədə aşkarlanan təhdidkar hücum üçün yolu təmsil etmək ehtimalı yüksək olan elementdir. Cədvəl 6 IoC növlərinin hərtərəfli siyahısını təqdim edir (Crec A., 2019).

Cədvəl 6. IoC növlərinin cədvəli

IoC Tipi	Təsviri
CIDR	Sinifsiz domenlərarası marşrutlaşdırma. Zərərli fəaliyyət və ya hücumda şübhəli bilinən şəbəkədə bir sıra IP ünvanlarını müəyyən edir.
CVE	Boşluqların ümumi tezaurusu
domain	Hostinqdə və ya zərərli fəaliyyətdə şübhəli bilinən veb sayt və ya server üçün domen adı. Domenlər bir sıra host adlarını da əhatə edə bilər.
email	Zərərli fəaliyyətlə əlaqəli e-poçt ünvanı.
FileHash (MD5, SHA1, SHA256, IMPHASH)	Şübhəli hesab edilən faylın məzmununun dəyişdirildiyini və ya pozulduğunu aşkarlamaq üçün istifadə edilən fayl üçün heş hesablaması.
filepath	Zərərli fəaliyyətdə şübhəli bilinən resursun fayl sistemində unikal yeri.
hostname	Zərərli fəaliyyətdə şübhəli bilinən bir domen daxilində yerləşən server üçün host adı.
filepath	Zərərli fəaliyyətdə şübhəli bilinən resursun fayl sistemində unikal yeri.
IPv4, IPv6	Zərərli fəaliyyətdə şübhəli bilinən onlayn server və ya digər cihaz üçün mənbə/təyinat kimi istifadə edilən IP ünvanı.
Mutex	Birdən çox proqram başlığına eyni resursu paylaşmağa imkan verən qarşılıqlı istisna obyekti. Mutekslər zərərli proqramlar tərəfindən sistemin yoluxmuş olub-olmadığını aşkar edən mexanizm kimi istifadə olunur.
URI	Zərərli fəaliyyətdə şübhəli bilinən onlayn yerləşdirilən faylın açıq yolunu təsvir edən vahid resurs identifikatoru (URI).
URL	Şübhəli zərərli fəaliyyətlə əlaqəli fayl və ya resursun onlayn yerini ümumiləşdirən vahid resurs yerləri (URL).

AlienVault OTX dünya üzrə bütün təhdid tədqiqatçılarına və təhlükəsizlik ekspertlərinə şəbəkəyə məhdudiyyətsiz giriş imkanı verir. Sistem icma tərəfindən təmin edilən təhdid məlumatlarını əlçatan edir, birgə tədqiqatı asanlaşdırır və istənilən mənbədən gələn təhdid məlumatları ilə təhlükəsizlik infrastrukturunu təkmilləşdirmə prosesini avtomatlaşdırır. OTX təhlükəsizlik cəmiyyətindəki şəxslərə fəal

müzakirələrdə iştirak etməyə, araşdırma aparmağa və təhdidlər, tendensiyalar, yanaşmalar haqqında ən müasir məlumat mübadiləsi aparmağa imkan verir.

AlienVault OTX həm təhdidləri paylaşan platformadır, həm də AlienVault Labs təhdid tədqiqat qrupu tərəfindən bildirilmiş ən yeni təhdidlər haqqında çoxlu məlumata malikdir. AlienVault USM texnologiyası təhdid məlumatlarını beş kritik təhlükəsizlik imkanları ilə birləşdirərək daha da effektiv edir (Abrahim K., Cherqi O., Hammouchi H., Ghogho M. & Benbrahim H., 2021):

- aktivlərin identifikasiyası
- zəifliyin qiymətləndirilməsi
- müdaxilənin aşkarlanması
- davranış monitorinqi
- SIEM

Bu beş mühüm təhlükəsizlik nəzarəti ilə AlienVault USM-in ən yeni təhdidlərlə yenilənməsi mümkün olur. Platformanın hesabatlarına istinadən hazırda 140 ölkədən 200 000 iştirakçı tərəfindən iyirmi milyondan çox təhdid göstəricisi təqdim edilir. AlienVault Labs komandası OTX məlumatlarından istifadə edərək və onu AlienVault bilikləri ilə artıraraq USM platformasında səkkiz əlaqələndirilmiş qayda dəstini təqdim edir (Özeren S., 2024).

1) **Korrelyasiya Direktivləri:** USM şəbəkə boyunca fərqli hadisələri əlaqələndirməklə davranış nümunələrini effektiv təhdid məlumatına çevirən əvvəlcədən müəyyən edilmiş 3000-dən çox qayda göndərir.
2) **Şəbəkə IDS İmzaları:** şəbəkədəki ən yeni zərərli trafiki müəyyənləşdirir.
3) **Host IDS İmzaları:** sistemlərə hücum edən ən yeni təhdidləri müəyyən edir.
4) **Aktiv Kəşf İmzaları:** ən son əməliyyat sistemlərini, tətbiqləri və cihaz məlumatlarını müəyyənləşdirir.
5) **Boşluğun Qiymətləndirilməsi İmzaları:** sistemdə son boşluqları aşkar edir.
6) **Hesabat Modulları:** idarəetmə və auditor ehtiyaclarını ödəmək üçün ətraf mühit haqqında mühüm məlumatların yeni perspektivlərini əldə edir.
7) **Dinamik İnsident Cavab Şablonları:** hər bir həyəcan siqnalına necə reaksiya vermək barədə fərdi tövsiyələr təmin edir.

8) **Yeni Dəstəklənən Məlumat Mənbəsi Pluginləri:** köhnə təhlükəsizlik cihazlarından və tətbiqlərdən məlumatları inteqrasiya etməklə monitorinq izini artırır.

Bu qayda dəsti və USM-də quraşdırılmış təhlükəsizlik nəzarətləri birləşərək mövcud olan ən yaxşı təhdid aşkarlaması strategiyasını təklif edir. Yeni təhdidləri tədqiq etmək və onları tapmaq üçün sistemləri manual şəkildə qurmağa görə vaxt itirməyə ehtiyac qalmır. AlienVault, istifadəçilərə təqdim olunan məlumatların hərtərəfli nəzərdən keçirilməsini, təsdiqlənməsini və struktur cəhətdən tamamlanmasını təmin edərək, CTI-a vahid yanaşma tətbiq edir. Hər bir istifidəçi hər gün zərərli IP ünvanları və URL-ləri, domen adları, zərərli proqram nümunələri və şübhəli faylları əhatə edən təxminən on milyon IoC toplayır. AlienVault bu məlumatları bütün dünyada açıq təhdid kəşfiyyatını paylaşan ilk icma olan OTX platformasında birləşdirir. Məlumat bir çox kanallar vasitəsilə əldə edilir. OTX mənbələrindən bəziləri aşağıdakılardır:

- Xarici təhdid kəşfiyyatçıları – AntiVirus proqramları (McAfee, Virus Total, Emerging Threats kimi)
- Açıq və ictimai mənbələr (məsələn, dövlət qurumları, təşkilat rəhbərləri, akademik institutlar, SANS İnternet Fırtınası Mərkəzi və Zərərli Proqram Domen Siyahısı)
- Ən son hücum üsullarını və alətlərini ələ keçirmək üçün qurulan yüksək təsirli tələlər vasitəsilə əldə olunan məlumatlar (Məsələn, OTX sistemin istismar dəstlərinə səbəb olaraq qurbanı təqlid edən veb səhifələri fəal şəkildə axtarır.)
- OTX "Pulses" şəklində icma tərəfindən verilən təhdid məlumatları (OTX icmasının təhdid məlumatlarını paylaşma üsulu)
- OSSIM və USM istifadəçilərinin təqdim etdikləri sərbəst şəkildə anonimləşdirilmiş məlumatlar

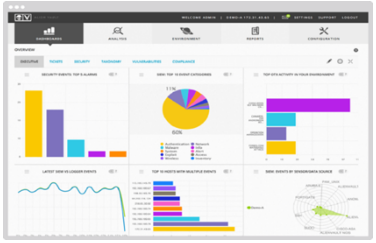
Növbəti addım olaraq avtomatlaşdırılmış sistemlər OTX-də toplanmış IoC-ların doğruluğunu və ciddiliyini analiz etmək üçün ML-dən istifadə edir. Sistemlər bunlardır:

- Töhfə Sistemi (Malware üçün)
- URL Sistemi (şübhəli URL-lər üçün)

- IP Reputasiya Sistemi (şübhəli IP ünvanları üçün)

Növbəti addımda, xüsusi risk göstəricilərini yoxlamaq və təsdiqləmək üçün AlienVault Labs Təhlükəsizlik Tədqiqat Qrupu tərəfindən hazırlanan və idarə olunan təhdidin qiymətləndirilməsi alətlərindən istifadə edilir. Bu alətlər ML-dən istifadə etməklə yanaşı Malware analizatoru, DNS Analizatoru, veb analizatoru və Botnet monitorunu ehtiva edir.

AlienVault tətbiqini daha ətraflı izah etmək üçün onun Malware hücumu ilə üzləşdikdə strategiyasını göstərmək olar. İlk addım olaraq platforma veb analizatordan istifadə edərək, bir domenin zərərli proqram yaydığını müəyyən edir. Daha sonra, o, şübhəli URL-ə qoşulur, onu analiz edir və sonra faylı işə salır. Fayl zərərli olarsa, platforma domen və serveri zərərli kimi qeyd edəcək. Zərərli proqram nümunələrini aşkar və analiz etmək üçün qabaqcıl sandboxing metodlarından da istifadə edilir. AlienVault Labs Təhlükəsizlik Tədqiqat Qrupu daha sonra bu risklər üzrə keyfiyyət və kəmiyyət araşdırmaları aparır. Məsələn, zərərli proqram nümunəsini analiz etmək və ya təkrarlanan davranış nümunələrini müəyyənləşdirmək üçün konkret rəqiblər və onların infrastrukturu üzərində hərtərəfli araşdırmalar aparmaq məqsədilə tərs mühəndislik üsullarından istifadə edilir. AlienVault bu ciddi prosedura riayət etməklə əsas göstəricilərin imkanlarını üstələyir. O, istifadəçiləri dəqiq və hərtərəfli CTI ilə təmin edir. Zərərli proqramların analizi, davranış analizi, hadisə nümunələri və şəbəkə imzaları haqqında hərtərəfli anlayışlar təqdim etməklə istifadəçilərin yaranan təhdidlər və lazımi əks tədbirlər haqqında tam anlayışa malik olması təmin edilir. AlienVault Labs Təhlükəsizlik Tədqiqat Qrupu dünyanın ən yaxşı təhlükəsizlik ekspertləri tərəfindən toplanan kəşfiyyat məlumatlarının həm avtomatik, həm də manual analizindən istifadə etməklə təşkilatlara dəqiq, faydalı və etibarlı təhdid məlumatı verir.



Şəkil 2. AlienVault OTX platformasının ümumi görüntüsü

2.2. CTI4SOC

SOCRadar Threat Intelligence mürəkkəb rəqəmsal risklərə qarşı effektiv müdafiə platformasıdır. O, məlumat topladığı mənbələr və güclü CTI xidməti vasitəsilə mövcud kibertəhlükəsizlik infrastrukturlarında proaktiv müdafiəçi kimi fəaliyyət göstərir. Bu platforma süni intellekt (AI) texnologiyasından istifadə edərək deep veb, dark veb, PasteBin saytları, BotMarket, Github və sosial media mənbələrindən topladığı məlumatları kəşfiyyat mənbəyinə çevirir (Trifonov R., Nakov O. & Mladenov V., 2018). Təhlükəsizlik əməliyyatları mərkəzinin (SOC) funksiyalarına bunlar aiddir:

- kibertəhdidləri araşdırmaq;
- kibertəhdidləri aşkarlamaq;
- kibertəhdidlərə nəzarət etmək;
- kibertəhdidlərin qarşısını almaq.

SOC komandaları təşkilatın virtual mülkiyyəti, kadr məlumatları, təşkilat sistemləri və brend bütövlüyü kimi aktivlərinin davamlı monitorinqini və qorunmasını təmin edir. Bununla da, onlar təşkilatın CTI strategiyasını həyata keçirir. SOC komandalarının işçilərinin sayı təşkilatın və sənayenin ölçüsündən asılıdır. SOC elə bir platformadır ki, onun vasitəsilə təhdidlərin qarşısının alınması, aşkarlanması, analizi və davamlı olaraq izlənməsi mümkündür. SOC vasitəsilə şəbəkə gecə-gündüz izlənilir və potensial təhdid göstəricilərinə aid iz görünəndə dərhal qarşısı alınır. SOC analitikləri şübhəli bir izlə qarşılaşanda daha dərin araşdırma üçün daha çox məlumat toplamağa fokuslanırlar. SOC analitiki araşdırma mərhələsində təhdidin xarakterini və onun infrastruktura nüfuz dərəcini aşkarlamaq məqsədilə şübhəli fəaliyyəti analiz edir. Bu platforma hücumların necə baş verdiyini və onlara necə effektiv cavab veriləcəyini müəyyənləşdirərək həyata keçirmə planı qurur. Əgər təhdid halı baş verərsə, SOC son nöqtələri təcrid etmək, zərərli prosesləri dayandırmaq və onların icrasının qarşısını almaq proseslərini həyata keçirərək cavab verir. O, təhdidin mümkün zərərləri dayandırıldıqdan sonra itirilmiş və ya pozulmuş məlumatları bərpa etmək üçün fəaliyyət göstərir. Yəni, SOC platforması şəbəkəni təhdid baş verməzdən əvvəl olduğu vəziyyətə qaytarmağa çalışır.

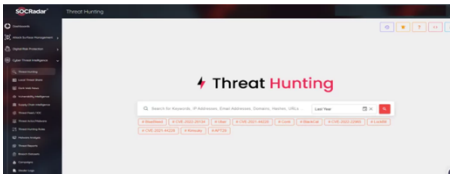
CTI4SOC platforması SOCRadar-ın yeni müstəqil CTI həll qoludur. O, SOC analitiklərinin işini asanlaşdırmaq məqsədilə yaradılmış yeni nəsil təhdid kəşfiyyatı platformasıdır. SOC komandaları CTI4SOC-un tərkibində olan 12 funksional modulunu effektiv və istifadəyə daha uyğun hesab etdikləri üçün, bu yeni nəsil platformadan yararlanmağı üstün hesab edirlər. CTI4SOC-un geniş monitorinq imkanları potensial dark veb və səthi veb (ing. surface web) təhdidlərini CTI mərhələsində aşkarlamağa imkan verir. O, adi CTI platformasından fərqli olaraq mütəmadi olaraq sosial medianı, telegram kanallarını və yeni yaranan kommunikasiya kanallarını izləyir və təhdid məlumatları toplayır. CTI4SOC platformasında IoC-un axtarışı və zənginləşdirilməsi zərərli fəaliyyətləri və onlarla əlaqəli təhdid aktorlarını müəyyələşdirməyə yardımçı olur. CTI4SOC kibertəhdidləri ilə bağlı nəticələri istifadəçi üçün rahat şəkildə göstərən interfeysə sahibdir.

CTI4SOC həmçinin MITER ATT&CK çərçivəsi ilə qarşılıqlı fəaliyyət göstərir. Nəticə olaraq, bu qarşılıqlı fəaliyyət vasitəsilə təhdid subyektlərinin məqsədləri, strategiyaları, TTP-ləri və yanaşmaları haqqında hərtərəfli məlumat əldə edilərək riskləri effektiv şəkildə qiymətləndirmək mümkün olur. SOC analitikləri tərəfindən təhdid subyektlərinin TTP-lərinin, motivasiyalarının və davranış modellərinin öyrənilməsi onlara perspektiv formalaşdırmağa dəstək olaraq kəşfiyyat prosesinə kömək edir.

SOCRadar Threat Hunting modulu SOC analitikləri üçün araşdırma prosesi zamanı əvəzolunmaz vasitədir. CTI komandaları zərərli proqram (ing. Malware), IP və domen kimi kritik məlumatların axtarışı vasitəsilə kəşfiyyat görüşlərini zənginləşdirə bilirlər. CTI4SOC platforması API ilə işləmək üçün hazırlanmış bir platformadır və potensial hücum zamanı mövcud məlumatları genişləndirmək məqsədilə istifadə edilə bilər (Paakala S., 2021). CTI4SOC şəbəkədə IP ünvanları, fayl heşləri və ya domen adları kimi böyük məlumatlarında daxil olduğu milyonlarla IoC-a malik olmaqla CTI üçün istifadə edilə bilər. SOC analitikləri IoC-lardan istifadə etməklə hansı xəbərdarlıqların müəyyən edilmiş təhdidlərlə əlaqəli olduğunu səmərəli şəkildə ayırd edə bilirlər. Bununla da, onlara araşdırmalarını həmin konkret hallar üzərində cəmləşdirməyə imkan yaradırlar. Məsələ ondadır ki, IoC-un özü SOC analitikləri üçün

təhdidin mahiyyətini və onun mümkün nəticələrini anlamağa görə kifayət qədər kontekst təmin etməyə bilər. IoC-un təkmilləşdirilməsi onun əlavə kontekst və təfərrüatlarla genişləndirilməsini nəzərdə tutur. Məsələn, məsul olan təhdid aktorunun müəyyən edilməsi, əlaqəli zərərli proqram təminatının dəqiqləşdirilməsi və ya hücumun mümkün nəticələrinin qiymətləndirilməsi kim kontekstlər əlavə edilə bilər (Oherqi C., Hammouchi H., Ghogho M. & Benbrahim H., 2021). Bu əlavə kontekstlərin təmin edilməsindən sonra SOC analitikləri araşdırmalarını prioritetləşdirə, mümkün risklərə daha səmərəli cavab verə və ətraf mühitin mühafizəsi ilə bağlı daha məlumatlı mühakimə yürüdə bilərlər. IoC-lar CTI4SOC vasitəsilə genişləndirilə bilir. CTI4SOC müxtəlif məlumat mənbələrini əlaqələndirməklə, analitiklərə təhdid mühiti haqqında hərtərəfli və dəqiq anlayış təqdim edə bilər. Aşağıda qeyd olunan bəzi modullar SOC analitiklərinə işlərini səmərəli yerinə yetirməyə yardımçı olur:

1) **Hücuma səbəb ola biləcək boşluq kəşfiyyatı:** SOC analitiklərini vəzifələrini effektiv şəkildə prioritetləşdirmək, yaranan təhdidləri müəyyən etmək, insidentlərə reaksiyanı artırmaq, potensial riskləri aşkar etmək və izləmək, uyğunluq və tənzimləmə öhdəliklərini yerinə yetirmək üçün vacib məlumatlarla təchiz edir. Bundan əlavə, o, SOCRadar Zəiflik Risk Skoru olan SVRS istifadə edərək hücum riskini azaltmaq üçün həll edilməli olan boşluqlar haqqında praktiki məlumat təqdim etməklə bərpa prosesinə kömək edə bilər.
2) **Dark veb xəbərləri:** SOC analitiklərinə hərtərəfli məlumat təqdim edir. Bu da həmin analitiklərə oğurlanmış etimadnamələri müəyyənləşdirməyə, mürəkkəb hücumları aşkarlamağa, daxili təhdidləri tanımağa, uyğunluq və tənzimləmə öhdəliklərini yerinə yetirməyə və insidentlərə cavab vermək imkanlarını təkmilləşdirməyə imkan yaradır. Bundan əlavə, o, təhdidlərin mənşəyi və istifadə olunan üsullar haqqında praktiki biliklər verməklə hücumdan sonra əvvəlki vəziyyətə bərpa prosesinə kömək edə bilər (Basheer R., Alkhatib B., 2021).



Şəkil 3. SOC Radar platformasının CTI keçidinin Threat Hunting modulunun ümumi görüntüsü

2.3. DOCGuard

DocGuard açıq təhdid kəşfiyyatı platforması faylların və e-poçtların içərisində gizlənən zərərli proqram təminatını (ing. Malware) müəyyən etmək üçün sistem təhlükəsizliyində bir sıra metodologiya və texnologiyalardan istifadə edir. Bu sistem struktur analiz adlanan yeni növ statistik analiz həyata keçirir. O, həmçinin zərərli proqramları effektiv aşkar etmək üçün şlüzlərdəki (ing. Gateway) boşluqları aradan qaldırır. Bundan əlavə, DocGuard struktur analizindən istifadə edərək sətirlərin daxilində IoC-ları müəyyən etməklə zərərli proqram təminatının yerini dəqiq müəyyən etmək qabiliyyətinə malikdir. O, həmçinin sənəd şifrələməsi və simli kodlaşdırma şəklində şifrələmə hücumlarını aşkar edə bilər. DocGuard rəqəmsal faylları, URL-ləri, e-poçtları məlumatların pozulması, viruslar və icazəsiz giriş daxil olmaqla bir sıra təhdidlərdən qorumaq üçün nəzərdə tutulmuş çoxfunksiyalı sənəd təhlükəsizliyi sistemidir (Turhan A., 2024). Qeyd edilə bilər ki, bu sistemin aparıcı məqsədlərinə daxildir:

- sənədlərə daxil edilmiş təhdidlərin müəyyənləşdirilməsi və analiz edilməsi;
- sənədlərin tamlığının təmin edilməsi;
- icazəsiz girişin qarşısının alınması;
- gizli məlumatların qorunması.

Zərərli proqram, kompüter sistemlərinin strukturuna müdaxilə etmək, zərər vermək və ya icazəsiz daxil olmaq üçün xüsusi olaraq yaradılmış proqram təminatının geniş yayılmış növüdür. Zərərli proqram təminatının tipik formalarına viruslar, soxulcanlar, troyanlar, ransomware, casus proqramları və zərərli reklam proqramları daxildir. Həmin proqramların yayılmasının əsas üsulları e-poçt qoşmaları, zərərli virusa yoluxmuş veb saytlar və USB yaddaş kartlarıdır. Onları müəyyən etmək, qeyri-adi fəaliyyətləri aşkar etmək və imzaları tanımaq üçün antivirus proqramı, şəbəkə monitorinq alətləri və davranış analizi üsullarından tez-tez istifadə olunur. Aşağıda zərərli proqram təminatını aşkarlamaq məqsədilə DocGuard sisteminin işləmə prinsipləri haqqında məlumat verilir:

I. Sənəd və ya elektron poçtun təhlili və skan edilməsi:

DocGuard anomaliyaları, zərərli proqram imzalarını və şübhəli faylları analiz etmək üçün etibarlı sənəd təhlili və skan üsullarından istifadə edə bilər. Qeyd edilə bilər ki, bu sistemə sənəd və e-poçt metadatası, başlıqların və məzmunun araşdırılması daxildir. DocGuardın zərərli proqram aşkarlama alətləri və antivirus proqramları ilə inteqrasiyası ona fərqli geniş spektrli zərərli proqram variantlarını: virusları, troyanları və soxulcanları müəyyən etmək üçün skan prosesini əhəmiyyətli dərəcədə təkmilləşdirmədə imkan yarada bilər. Bu analiz növünə bəzən imza əsaslı aşkarlama da deyilir. DocGuard imza əsaslı aşkarlamadan istifadə edərək adətən sənədlərdə görünən zərərli proqram imzalarını aşkarlayır. Belə ki, sistem məlum zərərli proqram imzalarının verilənlər bazası ilə sənəd heşlərini və ya nümunələrini müqayisə edərək zərərli proqramı müəyyənləşdirə bilir.

II. Davranış analizi:

DocGuard, skan analizinə (və ya digər adla imza əsaslı aşkarlama) əlavə olaraq zərərli proqram təminatını aşkar etmək üçün davranış analizi yanaşmalarından istifadə edir. Bu yanaşmalar zərərli proqram təminatının fəaliyyətini və davranışlarını analiz etməyi əhatə edir. Sözügedən analiz növü təcrid olunmuş mühitlərdə işləyərək sənədlərin və ya elektron poçtların davranışlarınının izlənilməsi və zərərli proqramların aşkarlanmasını özündə ehtiva edir. DocGuard, imzalara əsaslanan aşkarlama yanaşmalarından yayına bilən zərərli proqramların və təhdidlərin əvvəllər aşkarlanmamış əlamətlərini tapmaq imkanına malikdir.

III. Evristik analiz:

DocGuard sadalanan analizlərdən fərqli olaraq evristik analizdən istifadə etmək yolu ilə zərərli proqram təminatlarının xarakteristikası və davranışlarını prioritet götürərək onları müəyyən edə bilər. Bu analizin alqoritmlərini əsas götürərək sənədlərdəki şübhə doğuran məqamlar (şübhəli makrolar, qarışıq kod və ya qeyri-adi sənəd strukturları) müəyyənləşdirilə bilər. DocGuard evristik analizin həyata keçirilməsi metodu ilə zərərli proqramları, sıfır gün istismarlarını və müəyyən edilə bilməyən digər qabaqcıl təhdidləri aşkarlaya bilər.

IV. Maşın Öyrənməsi (ML) və Süni İntellekt (AI):

Doc Guard ML və AI alqoritmlərinin inteqrasiyasından istifadə etməklə keçmiş buna bənzər situasiyaları öyrənə və hal-hazırda inkişafda olan təhdidlərə adaptasiya imkanı yaratmaqla zərərli proqramların müəyyən edilməsini asanlaşdıra bilər.

DocGuard rəqəmsal imza və kriptoqrafik heş metodlarının istifadəsi vasitəsilə sənədin tamlığını yoxlaya bilir. Bu sistem, sənədlərin əldə olunmuş hesabatlarının daxilində dəyişiklik olmadığından və ya olmayacağından əmin olmaq məqsədilə əvvəldən məlum olan datalarla müqayisə edir. DocGuard faylın tamlığını daimi olaraq izləyərək icazəsiz dəyişiklikləri və ya sistemə müdaxilə cəhdlərini müəyyənləşdirə, nəticədə potensial təhlükəsizlik pozuntuları haqqında sistem administratorlarına məlumat verə bilər (Öztürk E., 2023).

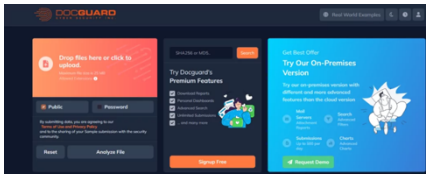
Təşkilatlar DocGuard-ı açıq təhdid kəşfiyyatı resursları və verilənlər bazası ilə inteqrasiya etməklə zərərli proqram təminatını müəyyənləşdirmək qabiliyyətini artıra bilər. Bu platforma təhlükəli veb saytlar, zərərli proqramlar və yeni təhdidlər haqqında ən son məlumatlardan istifadə etməklə zərərli faylları aktiv şəkildə müəyyən etmək və qarşısını almaq qabiliyyətinə malikdir. DocGuard sənədlər və IoC-lər, eləcə də təhlükəsizlik pozuntusunun açıq əlamətləri kimi xidmət edən zərərli davranışlar arasında əlaqə yaratmaq üçün CTI-lar ilə problemsiz əlaqə yaradır. Nəticə etibarilə, zərərli proqram təhdidlərinin identifikasiyası və onlara cavab tədbirləri gücləndirilir və asanlaşdırılır.

Bütün kəşfiyyat platformaları kimi DocGuard da daim inkişafda olan zərərli proqram təhdidlərini qabaqlamaq üçün davamlı monitorinq və müntəzəm yenilənmələr həyata keçirir. Zərərli proqram imzaları, eviristik aşkarlama qaydaları və yeni təhdid kəşfiyyatı anlayışlarına əsaslanan ML modelləri davamlı olaraq yenilənməlidir. Əlavə olaraq DocGuard vasitəsilə təhdidlərin aşkarlanıb qarşısının alınması üçün real vaxt rejimində databazalara, e-poçt qoşmalarına və fayl paylaşma platformalarına nəzarət edilməlidir. Bu sistem OSINT resurslarından əldə olunan məlumatlar və müxtəlif təhlükəsizlik insidentləri ilə üzləşmə əsasında təhlükəsizlik tədbirlərini müntəzəm olaraq inkişaf etdirir. Belə ki, o təhdid müəyyənləşdirmə alqoritmlərini təkmilləşdirir, təhdidlərə cavab vermək imkanlarını artırır və inkişaf edən təhdidlərə uyğunlaşaraq effektiv sənəd təhlükəsizliyini qoruyur. Əlavə olaraq, DocGuard sistemindən istifadə

edən şəxslər və ya təşkilatlar bu sistemin sənəd təhlükəsizliyindəki avantajları barəsində maariflənmək, potensial təhdidləri tanımaq və təhlükəsizlik hadisələrinə real vaxt rejimində effektiv cavab vermək məqsədilə təlim və maarifləndirmə proqramlarına investisiya edirlər. Doc Guard sənədlərə giriş qaydalarını, yəni kimin sənədə daxil ola, dəyişdirə və ya paylaşa biləcəyini tənzimləmək məqsədilə girişə nəzarət mexanizmlərini həyata keçirir. Bu sistem istifadəçi autentifikasiyası, avtorizasiya siyasətləri və rol əsaslı giriş nəzarətlərini tətbiq edərək icazəsiz girişin qarşısını almağa zəmin yaradır. Bundan başqa, DocGuard sistemi sadəcə səlahiyyətli şəxslərin və ya təşkilatların gizli sənədlərə çıxışının təmin edilməsi məqsədilə şəxsiyyət idarəetmə sistemləri ilə inteqrasiya edir.

Sözügedən platforma etibarlı tərəfdaşlar və ya təşkilatlarla təhdid kəşfiyyatı strategiyasını paylaşaraq təhdidlərə qarşı kollektiv müdafiəni gücləndirə bilir. Nəticə olaraq, bu sistem OSINT paylaşma platformalarına böyük fayda verir, yaranan təhdidlər barəsində məlumat mübadiləsi aparır və təhdidin mümkün azaldılması strategiyaları əsasında əməkdaşlıq həyata keçirir. DocGuard təhlükəsizlik hadisəsi ilə üzləşdikdə isə onun qarşısını almaq, aradan qaldırmaq və bərpa etmək məqsədilə zərərli proqrama yoluxmuş faylları təcrid edərək hadisələrə cavab prosedurlarına başlayır.

Yekun olaraq, ümumilikdə DocGuard sisteminin tətbiqi deyildikdə sənədlərə və ya elektron poçtlara daxil edilmiş zərərli proqram təminatının aşkarlanması və mümkün qədər azaldılması üçün sənədlərin təhlili üsulları (skan analizi, davranış analizi, evristik analiz, maşın öyrənməsi), təhdid kəşfiyyatının inteqrasiyası, sənəd bütövlüyünün yoxlanılması, giriş nəzarəti, sistemə müntəzəm monitorinq və daimi yenilənmələr nəzərdə tutulur. Son olaraq, DocGuard innovativ və real vaxt rejimli təhdid müəyyənləşdirmə strategiyalarını tətbiq edərək və yaranan yeni təhdidlərdən məlumatlı olaraq sistemin istifadə olunduğu təşkilatları zərərli proqram təhdidlərinin yayılmasından yüksək səviyyədə qoruya bilir.



Şəkil 4. DOCGuard platformasının ümumi görüntüsü

2.4. MISP Threat Sharing

MISP (Malware Information Sharing Platform) zərərli proqram təminatları haqqında məlumatların paylaşılması üçün olan OSINT platformasıdır. Bu platforma kibertəhlükəsizlik mütəxəssisləri, şirkət və təşkilatlar arasında təhdidlər haqqında məlumatların paylaşılmasını asanlaşdırmaq üçün nəzərdə tutulmuşdur. Onun vasitəsilə əməkdaşlıq şəraitində təhdid aktorları, zərərli proqram nümunələri və digər müvafiq təhdidlər haqqında olan məlumatları toplamaq, saxlamaq və paylaşmaq imkanı əldə edilir. MISP IoC-ləri paylaşaraq daha effektiv CTI üçün zəmin yaradır (MISP, 2024).

MISP, təhdidlər barəsində məlumatın korrelyasiyasını və paylaşılmasını asanlaşdırmaq üçün təşkilatlara hücumlarla bağlı həm texniki, həm də qeyri-texniki məlumatları saxlamağa imkan verən və istifadəçi interfeysi olan verilənlər bazasını ehtiva edir. MISP vasitəsilə məlumatlar OpenIoC, mətn, CSV, MISP XML və JSON formatlarında ixrac edilə bilər. Bu məlumatlar müdaxilənin aşkarlanması və qarşısının alınması üçün istifadə olunur. MISP layihəsini genişlətdirdikcə yalnız zərərli proqram göstəricilərini deyil, həm də anomaliyalar və sistemdəki boşluqlarla bağlı məlumatları da əhatə edir. Bu platforma həmçinin istifadəçilərə digər MISP istifadəçiləri və ya icmalar ilə təhdid məlumatlarını paylaşmağa imkan verən güclü xüsusiyyətlərə malikdir. MISP yalnız kibertəhlükəsizlik IoC-larını və zərərli proqramların analizini saxlamaq və paylaşmaq üçün istifadə olunmur. O, həm də informasiya və kommunikasiya texnologiyaları olan İKT infrastrukturlarına, təşkilatlara və ya fərdlərə qarşı hücumların, anomaliyaların və ya təhdidlərin aşkarlanması və qarşısının alınması üçün IoC-lərdən və məlumatlardan istifadə edilmə xüsusiyyətlərini birləşdirir (Mahmudova R., Daşdəmirova K., 2021).

Bu platformanın layihəsi 2011-ci ilin iyununda Kristof Vandeplasın e-poçt və ya PDF sənədlərində IoC-ların həddən artıq paylaşılmasından məyus olması ilə başladı. Belə ki, o, bu problemi həll etmək üçün CakePHP dən istifadə etmiş və CyDefSIG olan Kiber Müdafiə İmzaları adlı öz konsepsiyasını yaratmışdır. O, 2011-ci ilin iyul ayının ortalarında iş yeri olan Belçika Müdafiə Nazirliyində şəxsi layihəsini təqdim edərək pozitiv rəylər almışdır. Belçika Müdafiə Nazirliyi öz şəxsi serverində CyDefSIG-ə giriş

icazəsi verdikdən sonra 2011-ci ilin avqust ayının ortalarından etibarən rəsmi olaraq CyDefSIG-dən istifadə etməyə başlamışdır. 2012-ci ildən etibarən isə Şimali Atlantika müqaviləsi təşkilatı olan NATO bu layihə barəsində araşdırma apararaq onun açıq kodlu bir layihə olmasını üstünlük kimi qiymətləndirmişdir. Daha sonra NATO-nun təhlükəsizlik işçisi olan Aleks Vandurme CyDefSIG-i təkmilləşdirib əlavə funksiyalar artıraraq MISP: Zərərli Proqram Məlumat Paylaşma Layihəsi-ni irəli sürmüşdür. 2013-cü ilin yanvar ayında isə MISP istifadəyə verilmişdir. Bununla da digər təşkilatlar da MISP platformasını qəbul etməyə başladılar, və onu CERT dünyasında təbliğ etdilər. MISP-in tərtibatçısı olan Andras İklody hal-hazırda Lüksemburq Kompüter İnsidentlərinə Müdaxilə Mərkəzi olan CIRCL üçün işləyir. MISP Thread Sharing platforması bir çox xüsusiyyətlərinə görə seçilir. Onlardan bəziləri aşağıdakılardır:

- **Səmərəli IoC və göstəricilər bazasının olması:** MISP-in zərərli proqram nümunələri, insidentlər və kəşfiyyat haqqında texniki və qeyri-texniki məlumatları saxlamağa imkan verən səmərəli IoC və göstəricilər bazası mövcuddur.
- **Göstəricilər arasında əlaqənin avtomatik tapılması**: MISP zərərli proqramların, hücumların və ya IoC-ların arasında əlaqənin avtomatik tapılmasını təmin edir.
- **Mürəkkəb obyektləri sadələşdirən model:** CTI-ı, insidentləri və ya əlaqəli elementləri ifadə etmək üçün mürəkkəb obyektlərin ifadə oluna və birləşdirilə bilinəcəyi çevik olan sadə məlumat modeli təqdim edir.
- **Daxili paylaşma funksiyası**: Müxtəlif paylama modellərindən istifadə edərək məlumat mübadiləsini asanlaşdırmaq üçün daxili paylaşma funksiyası mövcuddur. MISP digər MISP-lərlə hadisələri və atributları avtomatik sinxronizasiya edə bilir. O, qabaqcıl filtrləmə funksiyaları çevik paylaşma qrupu tutumu və atribut səviyyəsində paylama mexanizmləri daxil olmaqla, hər bir təşkilatın paylaşma siyasətinə cavab vermək üçün istifadə edilə bilir.
- **Intuitiv istifadəçi interfeysinin mövcud olması**: MISP tərəfindən istifadəçilər üçün göstəricilər yaratmaq, yeniləmək və əməkdaşlıq etmək üçün intuitiv istifadəçi interfeysi istifadə edilir**.** Hadisələr və onların korrelyasiyaları arasında problem olmadan çalışan qrafik interfeysi var. Obyektlər və göstəricilər arasında əlaqələr yaratmaq və onlara baxmaq üçün isə hadisə qrafiki funksionallığından istifadə edilir.

Analitiklərə IoC-lardan müdafiyəyə yardımçı olmaq məqsədilə qabaqcıl filtrləmə funksiyaları və xəbərdarlıq siyahısı təqdim olunur.

- **Məlumatların strukturlaşdırılmış formatda saxlanması**: CTI boyunca kibertəhlükəsizlik göstəricilərinin geniş dəstəyi ilə məlumatların strukturlaşdırılmış formatda saxlanmasını dəstəkləyir. O, müxtəlif məqsədlər üçün verilənlər bazasından avtomatlaşdırılmış istifadəyə imkan yaradır.
- **İxrac:** Digər sistemlərlə inteqrasiya etmək üçün IDS, OpenIoC, CSV, MISP XML və ya JSON kimi ixraca imkan yaradır.
- **İdxal:** Toplu idxal, sərbəst mətn idxalı, OpenIoC, GFI sandbox, ThreatConnect CSV və ya MISP XML formatında məlumatların idxalını təmin edir.
- **Pulsuz mətn idxal aləti:** Strukturlaşdırılmamış hesabatların MISP platformasına inteqrasiyasına dəstək olmaq məqsədilə çevik pulsuz mətn idxal aləti mövcuddur.
- **Əməkdaşlıq etmək üçün uyğun sistem olması:** MISP platforması IoC siyahısına əlavələr və ya fərdi istəyə uyğun dəyişikliklər təklif etməyə imkan yaradır. Bununla da o, digər mənbələrlə əməkdaşlıq etmək üçün uyğun sistem hazırlaya bilir.
- **Məlumat mübadiləsi:** MISP platforması istifadə edilməklə digər tərəflərlə və etibar edilən qruplarla avtomatik mübadilə və sinxronizasiya mümkün edilir.
- **MISP-i təşkilat məlumatları ilə inteqrasiya etmək üçün çevik API:** MISP platforması təhdid göstəricilərini əldə etmək, əlavə etmək və ya yeniləmək, zərərli proqram nümunələrini idarə etmək və ya təhdid izlərini müəyyənləşdirmək məqsədilə çevik Python Kitabxanası olan PyMISP ilə birləşdirilmişdir.
- **Tənzimlənən sistematika**: Təşkilat sxemlərinə uyğun olaraq təhdidləri təsnif etmək və etiketləmək üçün tənzimlənən sistematikadan istifadə edir.
- **Kəşfiyyat lüğətləri**: MISP qalaktikası adlanan və MISP-dəki göstəricilərlə asanlıqla əlaqələndirilə bilən mövcud təhdid aktorları, zərərli proqram, uzaqdan giriş troyanı RAT, ransomware və ya MITRE ATT&CK ilə birləşdirilmiş kəşfiyyat lüğətləri var.
- **Python-da genişləndirmə modulları**: MISP platforması təşkilatların istifadəsində genişləndirmək və ya artıq mövcud olan MISP modullarını aktivləşdirmək məqsədilə Python-da təkmilləşdirmə modulları istifadə olunur.

- **Müşahidə dəstəyi**: Paylaşılan göstəricilərlə bağlı təşkilatlara müşahidə dəstəyi var. Müşahidə prosesi MISP istifadəçi interfeysi, API, TAXII və ya STIX standartları vasitəsilə həyata keçirilə bilir.
- **STIX dəstəyi**: STIX dəstəyi XML və JSON məlumatlarının idxalını və ixracını təmin edir (Barnum S., 2014).
- **Bildirişlərin inteqrasiya olunmuş şifrələməsi və imzalanması:** İstifadəçi seçimlərindən asılı olaraq yüksək gizlilik proqramı olan PGP və/və ya təhlükəsiz /çoxməqsədli internet poçt genişlənmələri olan S/MIME vasitəsilə bildirişlərin inteqrasiya edilmiş şifrələnməsi və imzalanması mümkündür.
- **MISP daxilində real vaxt rejimində kanal:** Sıfır Mesaj Növbəsi olan ZeroMQ-da və ya Kafka-da bütün dəyişiklikləri, göstəriciləri və müşahidələri avtomatik almaq məqsədilə MISP daxilində real vaxt rejimində işləyən kanal mövcuddur.
- **Vizuallaşdırma və Hesabat:** MISP platforması istifadəçilərinə CTI məlumatlarını vizuallaşdırmaq və effektiv vəziyyətdə çatdırmaqda yardımçı olmaq məqsədilə hesabat imkanları təqdim olunur və nəticədə onlara qərar qəbul etməkdə dəstək olur.

Ümumilikdə, MISP təşkilatlara kibertəhlükəsizlik təhdidlərini daha effektiv şəkildə aşkarlamaq məqsədilə digər sistemlərlə əməkdaşlıq edən və müdafiə mexanizmlərini təkmilləşdirməyə imkan yaradan CTI platformasıdır. MISP platformasının açıq mənbəli olması və aktiv məlumat paylaşma icmasına sahib olması onu kibertəhlükəsizlik icması üçün dəyərli aktivə çevirir.

Şəkil 5. MISP platformasının ümumi görüntüsü

2.5. OpenCTI

OpenCTI, təşkilatlara CTI məlumatlarını effektiv şəkildə analiz və idarə etməyə dəstək olan açıq mənbəli TIP-dir. OpenCTI açıq mənbə platforması olaraq onun mənbə kodunu hər kəsin yoxlaması, səhvlik gördükdə dəyişdirilməsini təklif etməsi və paylaşması üçün sərbəstdir. Nəticədə, bu TIP xüsusi təşkilati ehtiyaclara əsasən fərdiləşməni təmin edir. OpenCTI müxtəlif mənbələrdən CTI məlumatlarını toplayıb təşkil və analiz edərək mərkəzləşdirilmiş platforma təmin edir. Təşkilatlar CTI-in mərkəzləşdirilməsilə yaranan təhdidlər haqqında hərtərəfli anlayış əldə edə və kibertəhlükəsizlik strategiyaları haqqında əsaslandırılmış qərarlar qəbul edə bilərlər (Chantzios T. K., Paris D., 2019). OpenCTI platformasının xüsusiyyətləri aşağıdakılardır:

1) **Məlumat qəbulu**: OpenCTI müxtəlif mənbələrdən (məsələn, açıq mənbəli lentlər, kommersiya lentləri, daxili qeydlər və insident hesabatlarından) CTI informasiyalarının qəbulunu təmin edir. OpenCTI IoC-lar, təhdid aktorları, zərərli proqram imzaları və digər göstəricilər haqqında geniş məlumat bazası ehtiva edir.
2) **Məlumatların zənginləşdirilməsi:** Platforma təhdid aktoru profilləri, hücum üsulları, atribusiya məlumatları və müvafiq CVE-lər (Ümumi Zəifliklər və Təsirlər) kimi kontekstual məlumatlar əlavə edərək CTI məlumatlarını zənginləşdirir. Bu zənginləşdirmə təhdidlərin anlaşıqlı olmasını asanlaşdırır və cavab tədbirlərinin prioritetləşdirməyə dəstək olur.
3) **Məlumatların korrelyasiyası:** OpenCTI təhdid nümunələrini və onlara meylliliyi aşkarlamaq məqsədilə müxtəlif məlumat mənbələrinin korrelyasiyasını təmin edir. Bu korrelyasiya vasitəsilə analitiklər bir-birindən fərqli görünən informasiya parçaları arasında nöqtələri birləşdirə və gizli təhdidləri müəyyənləşdirə bilirlər.
4) **İnteqrasiya imkanları:** OpenCTI təşkilatların tələblərinə uyğun platformanı SIEM-lər, təhlükəsizlik avtomatlaşdırması və cavab tədbirləri olan SOAR platformaları, CTI xəbərləri və digər təhdid analizi alətləri kimi təhlükəsizlik texnologiyaları ilə təchiz edərək geniş inteqrasiya imkanları təklif edir.

OpenCTI platformasının istifadə halları aşağıda qeyd olunmuşdur :

- **Təhdid Kəşfiyyatının İdarə Edilməsi:** OpenCTI məlumatlarının saxlanması və idarə edilməsi üçün mərkəzləşdirilmiş repozitor kimi xidmət edir. O, təşkilatların hərəkətə keçə bilən kəşfiyyat məlumatlarına daxil olmasını, analizini və paylaşılmasını asanlaşdırır.
- **İnsidentlərə Cavab:** Platforma təşkilatlara vaxtında və tələbə uyğun CTI təqdim edərək təhlükəsizlik insidentlərini aşkarlamaq, qarşısını almaq və aradan qaldırımaq proseslərini asanlaşdırmağa kömək edir.
- **Kibertəhdid Kəşfiyyatının Paylaşımı**: OpenCTI məlumatların etibarlı tərəfdaşlar və icmalar arasında paylaşılmasını asanlaşdırır. O, təşkilatlara real vaxt rejimində platforma ilə əməkdaşlığı və ümumi təhdidlərdən kollektiv şəkildə müdafiəni təklif edir.

OpenCTI platformasının üstünlükləri bunlardır:

I. **Hərtərəfli Təhdid Kəşfiyyatı:** OpenCTI bir çox mənbələrdən CTI məlumatlarını toplayaraq və əlaqələndirərək təşkilatlara təhdid mənzərəsini hərtərəfli başa düşməyə yardımçı olur.

II. **Təkmilləşdirilmiş Qərar Qəbuletmə:** OpenCTI təşkilatları kontekstləşdirilmiş CTI ilə təmin etməklə, kibertəhlükəsizlik strategiyaları və cavab tədbirləri haqqında təkmil qərarlar qəbul etməyə imkan yaradır.

III. **Xərc-effektivlik:** OpenCTI təşkilatlara bahalı lisenziya haqqı ödəmədən CTI məlumatlarını analiz və idarə etmək üçün sərfəli üsul təklif edir.

IV. **Fərdiləşdirmə və Çeviklik:** OpenCTI-nin fərdiləşdirilə bilən arxitekturası vaitəsilə təşkilatlar platformanı öz unikal tələblərinə və iş axınlarına uyğunlaşdıra bilir və xüsusi CTI ehtiyaclarını ödəyitlər.

V. **Yerləşdirmə Seçimləri:** OpenCTI təşkilati üstünlüklərdən və tələblərdən asılı olaraq sistemdə və ya Cloud bulud sistemində yerləşdirilə bilər. Platforma miqyasından asılı olmayaraq müxtəlif ölçülü təşkilatların ehtiyaclarını ödəyir.

VI. **Texniki Memarlıq:** OpenCTI ən yeni texnologiyalarla qurulub. O, modul arxitekturasına riayət etməklə çeviklik və genişlənmə imkanı yaradır. Platforma əsasən frontend üçün JavaScript və backend üçün Node.js istifadə edərək istifadəçi interfeysi yaradır.

VII. **Məlumat Standartları və Qarşılıqlı Fəaliyyətdən istifadə:** OpenCTI, digər TIP-lərlə qarşılıqlı əlaqəni təmin edən STIX və TAXII kimi sənaye standartlarına riayət edir. Platforma STIX formatlı CTI məlumatlarının qəbulunu və ixracını dəstəkləyir. O, STIX-i də dəstəkləyən üçüncü tərəf sistemləri ilə problemsiz inteqrasiyanı təmin edir.

VIII. **İcma və İnkişaf:** OpenCTI platforması onun inkişafı üçün əməkdaşlıq edən, bilik və təcrübələrini bölüşən və onun təkmilləşdirilməsinə töhfə verən istifadəçilər və tərtibatçılardan ibarət fəal və artan icma vasitəsilə inkişaf edir. Layihənin GitHub-da yerləşdirilməsi istifadəçilərə mənbə koduna daxil olmaq, problemləri bildirmək, yeni kod təkmilləşdirmələrinə dəstək olmaq və icma ilə əlaqə saxlamaq imkanı verir. Beləliklə, icma və əsas inkişaf qrupu müntəzəm yeniləmələr, səhv düzəlişləri və xüsusiyyət təkmilləşdirmələri təklif edərək OpenCTI-nin daim yenilənərək kibertəhdidlərə cavab verməsini təmin edir.

IX. **Təlim və Sənədləşdirmə:** OpenCTI istifadəçilərini hərtərəfli sənədlər, dərs vəsaitləri, təlim resursları, təlim sessiyaları, vebinarlar və seminarlarla təmin edərək onların platformanın imkanlarından səmərəli istifadəsinə kömək edir.

X. **Təhlükəsizlik və Məxfilik:** OpenCTI gizli informasiyaları qorumaq məqsədilə etibarlı giriş nəzarətlərini, şifrələmə mexanizmlərini və audit imkanlarını tətbiq edir. Platforma məlumatların anonimləşdirilməsi xüsusiyyətləri və ümumi məlumatların qorunması qaydaları olan GDPR vasitəsilə rol əsaslı giriş nəzarəti RBAC-ın və yalnız səlahiyyətli istifadəçilərin xüsusi məlumat dəstlərinə və funksionallıqlara daxil olmasını təmin edir.

Ümumilikdə, OpenCTI təhdid kəşfiyyatı məlumatlarını analiz və idarə etmək məqsədilə yaradılmış çox yönlü və güclü platformadır. O, təşkilatlara kibertəhlükəsizlik mövqeyini artırmaq və inkişaf edən təhdidlərdən müdafiə olunmaq məqsədilə lazım olan imkanları təklif edir.

Şəkil 6. OpenCTI platformasının ümumi görüntüsü

2.6. Açıq Təhdid Platformalarının müqayisə cədvəli

Davamlı olaraq dəyişən kibertəhlükəsizlik dünyasında təşkilatların yeni təhdidləri aşkarlaması, analiz etməsi və onlara reaksiya verməsi üçün effektiv təhdid kəşfiyyatı platformaları vacibdir. Bu fəsildə beş məşhur açıq mənbəli CTI platformalarının hərtərəfli müqayisəsi üçün müxtəlif metrikalar üzrə matriks göstərilmişdir. Bu platformalar haqqlarında ətraflı analiz verilmiş AlienVault OTX, CTI4SOC, DOCGuard, MISP Threat Sharing və OpenCTI platformalarıdır. Dərəcələrlə (yüksək/güclü, orta, zəif/aşağı) qiymətləndirmə metrikalarına daxildir: məlumat mənbələri, inteqrasiya, platforma istifadəçiləri tərəfindən töhfə; məlumat paylaşma mexanizmi; yenilənmə tezliyi; təhdid aşkarlama mexanizmi; url təhlili; avtomatlaşdırma; təhlükəsizlik tədbirləri; məlumat strukturunun quruluşu; istifadə rahatlığı; istifadə xərci və süni intellekt/maşın öyrənmədən istifadə. Matriks cədvəl 7-də göstərilmişdir:

Cədvəl 7. Təhdid platformalarının metrikalar üzrə müqayisə matriksi

Müqayisə Metrikaları		İzahat	AlienVault OTX	CTI4SOC	DOCGuard	MISP Threat Sharing	OpenCTI
1	**Platforma istifadəçiləri olan icma üzvləri haqqında məlumat**	İstifadəçi bazası və onların fəal iştirakı.	**Yüksək:** Gündəlik IoC-lərə töhfə verən 53,000+ üzv	**Orta:** Aktiv töhfələri olan orta istifadəçi bazası	**Aşağı:** Məhdud istifadəçi əlaqəsi və töhfələr	**Yüksək:** Güclü əlaqə ilə geniş qlobal icma	**Yüksək:** Forumlarda və GitHub-da tez-tez qarşılıqlı əlaqədə olan aktiv tərtibatçı və istifadəçi icması
2	**Platforma icması tərəfindən verilən töhfə**	Forumlar, sənədlər və birbaşa əməkdaşlıq da daxil olmaqla platforma icmasından dəstəyin mövcudluğu və keyfiyyəti.	**Yüksək:** Forumlar və əməkdaşlıq vasitəsilə güclü dəstək	**Orta:** Dəstəyi təmin edən daha kiçik, lakin aktiv istifadəçi bazası tərəfindən daxil edilən məlumatlar	**Aşağı:** Kiçik icma tərəfindən məhdud dəstək	**Yüksək:** Forumlar, sənədlər və qlobal iştirak vasitəsilə geniş dəstək	**Yüksək:** GitHub, forumlar və əməkdaşlıq layihələri vasitəsilə aktiv dəstək
3	**Məlumat Paylaşma Mexanizmi**	CTI məlumatların paylaşmaq üçün istifadə olunan metod, standart və protokollar.	**Yüksək:** Paylaşım üçün "Pulse"-lar istifadə edir; anonim təqdimatları dəstəkləyir	**Orta:** Çeviklik üçün xüsusi bəzi protokollar	**Aşağı:** Məhdud paylaşma mexanizmləri	**Yüksək:** Problemsiz paylaşım üçün STIX və TAXII standartları istifadə edilir	**Yüksək:** STIX və TAXII standartlarına əməl edilir, qarşılıqlı əlaqə təmin edilir

Müqayisə Metrikaları		İzahat	AlienVault OTX	CTI4SOC	DOCGuard	MISP Threat Sharing	OpenCTI
4	Standartlara Uyğunluq	STIX	**Güclü**	**Güclü**	**Orta**	**Güclü**	**Güclü**
		TAXII	**Güclü**	**Güclü**	**Orta**	**Güclü**	**Güclü**
		CybOX	**Orta**	**Zəif**	**Zəif**	**Zəif**	**Zəif**
		IODEF	**Orta**	**Zəif**	**Zəif**	**Zəif**	**Zəif**
5	İnteqrasiya	Digər təhlükəsizlik alətləri və platformaları ilə inteqrasiya etmək imkanı.	**Yüksək:** API vasitəsilə USM, OSSIM və müxtəlif üçüncü tərəf alətləri ilə inteqrasiya	**Orta:** Bəzi fərdi inteqrasiya imkanları	**Aşağı:** Daxili alətlərlə məhdudlaşır	**Yüksək:** Çoxsaylı TIP və SIEM sistemləri ilə inteqrasiyanı dəstəkləyir	**Yüksək:** Müxtəlif təhlükəsizlik alətləri ilə geniş inteqrasiya variantları
6	Daha detallı inteqrasiya və qarşılıqlı fəaliyyət məlumatları	API Access	**Yüksək səviyyədə**	**Yüksək səviyyədə**	**Aşağı səviyyədə**	**Yüksək səviyyədə**	**Yüksək səviyyədə**
		SIEM	**Yüksək səviyyədə**	**Orta səviyyədə**	**Aşağı səviyyədə**	**Yüksək səviyyədə**	**Yüksək səviyyədə**
		SOAR	**Orta səviyyədə**	**Orta səviyyədə**	**Aşağı səviyyədə**	**Orta səviyyədə**	**Yüksək səviyyədə**
7	Yenilənmə Tezliyi	Yeni CTI məlumatları əlavə edilməsi.	**Yüksək:** Yeni "Pulse"-lar ilə gündəlik yeniləmələr	**Orta:** Sabit yeniləmə axını	**Aşağı:** Nadir yeniləmələr	**Yüksək:** Avtomatlaşdırılmış paylaşma platforması və geniş istifadəçi bazasına görə tez-tez yeniləmələr	**Yüksək:** Platforma icmasından daimi yeniləmələr və töhfələr
8	Təhdid Aşkarlama Mexanizmi	Təhdidləri aşkarlamaq üçün istifadə olunan üsullar və alqoritmlər.	**Yüksək:** Əsasən icmalar arası paylaşma və "Pulse" bazaları	**Yüksək:** Fərdi aşkarlama üsulları	**Yüksək:** Təməl aşkarlama alqoritmləri	**Yüksək:** Aşkarlanma üçün IoC-ləri və təhdid nümunələrini analiz edir	**Təkmil:** Mürəkkəb aşkarlama alqoritmləri
9	URL Təhlili	Təhdidləri aşkarlamaq üçün URL-ləri analiz etmək imkanı	**Yüksək:** Əsas xüsusiyyətə aiddir	**Yüksək:** Əsas URL yoxlamaları	**Aşağı:** Əsasən sənəd, e-poçt və fayl təhdidlərinə yönəlib	**Yüksək:** Hərtərəfli URL analizi imkanları	**Yüksək:** Ətraflı URL analizi dəstəyi
10	Avtomatlaşma	Platformada proseslərin hansı dərəcədə avtomatlaşdığı	**Orta:** Məlumat mübadiləsinə diqqət yetirir	**Yüksək:** Məlumat toplanması və təhlili üçün avtomatlaşma	**Zəif:** Məhdud avtomatlaşma xüsusiyyətləri	**Yüksək:** Avtomatlaşmış qəbul, təhlil və paylaşma prosesləri	**Yüksək:** Qabaqcıl avtomatlaşma imkanları
11	Təhlükəsizlik tədbirləri	Məlumatların təhlekəsizliyi üçün görülən işlər	**Yüksək:** məlumatların şifrələnməsi	**Orta:** Orta səviyyəli təhlükəsizlik	**Yüksək:** sənəd qoruma xüsusiyyəti	**Yüksək:** icazə idarəetməsi	**Yüksək:** geniş tədbirlər

Müqayisə Metrikaları		İzahat	AlienVault OTX	CTI4SOC	DOCGuard	MISP Threat Sharing	OpenCTI
12	**Məlumat strukturunun quruluşu**	Platforma təhdid kəşfiyyatı məlumatlarını necə strukturlaşdırır və təşkil edir.	**Güclü:** Məlumatlar IoC-lər və kontekstlə "Pulslar" şəklində strukturlaşdırılıb	**Orta**: Aşkarlama və təhlil proseslərinə uyğunlaşdırılmışdır	**Orta**: Fayl əsaslı təhdidlərə fokuslanıb	**Yüksək:** Standartlaşdırma və qarşılıqlı fəaliyyət üçün STIX formatından istifadə edir	**Yüksək:** Strukturlaşdırılmış təhlükə kəşfiyyatını təmin edən STIX formatından da istifadə edir
13	**İstifadə rahatlığı**	Platforma interfeysinin istifadəsi	**Yüksək:** Sadə və intuitiv interfeys	**Yüksək:** Sadə interfeys	**Orta:** Orta səviyyəli istifadə rahatlığı	**Orta:** Orta səviyyəli istifadə rahatlığı, xüsusi konfiqurasiya tələbləri	**Yüksək:** Sadə istifadə interfeysi, geniş icma dəstəyi
14	**İstifadə Xərci**	İstifadəsində detallı pulsuz və pullu seqmentləri	**Pulsuz (məhdudiyyətlərlə)**	**Pulsuz (Sadə versiya və tələbələr üçün)**	**Pulsuz**	**Pulsuz**	**Pulsuz (məhdudiyyətlərlə)**
15	**Süni İntellekt və Maşın Öyrənmə**	AI və ML istifadəsi əsasında təhdid məlumatı toplama	**Orta səviyyədə**	**Yüksək səviyyədə**	**Zəif səviyyədə**	**Yüksək səviyyədə**	**Yüksək səviyyədə**
16	**Məlumat mənbələri və əhatə dairəsi**	Dark Veb Monitorinq	**Orta səviyyədə**	**Yüksək səviyyədə**	**Orta səviyyədə**	**Zəif səviyyədə**	**Yüksək səviyyədə**
		Deep Veb Monitorinq	**Orta səviyyədə**	**Yüksək səviyyədə**	**Orta səviyyədə**	**Zəif səviyyədə**	**Yüksək səviyyədə**
		Açıq mənbə Veb Monitorinqi	**Yüksək səviyyədə**	**Yüksək səviyyədə**	**Yüksək səviyyədə**	**Orta səviyyədə**	**Yüksək səviyyədə**
		Xarici Lentlərlə İnteqrasiya	**Yüksək səviyyədə**	**Yüksək səviyyədə**	**Orta səviyyədə**	**Yüksək səviyyədə**	**Yüksək səviyyədə**

III FƏSİL. TƏHDİD KƏŞFİYYAT SİSTEMİNİN İŞLƏNMƏSİ.

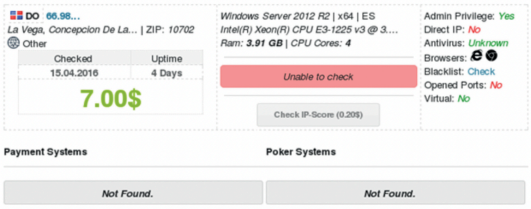
3.1. İnformasiya mənbələrinin siyahısının müəyyən edilməsi

Kibertəhdid kəşfiyyatı aparılarkən təşkilatların üzləşdiyi təhdidlər haqqında daha geniş və vahid anlayış təmin etmək məqsədilə fərqli mənbələrdən geniş istifadə edilir. Çünki əksər təşkilatların qarşılaşdığı kibertəhdidlərin əhatə dairəsi fərqlidir. Həmin təhdidləri yaradan təhdid aktorları haqqında müvafiq məlumatları əldə etmək üçün uyğun mənbələr seçilməlidir (Hassan N., Hijazi R., 2018). Kibertəhdid kəşfiyyatçıları tərəfindən məlumat toplanan mənbələrə aşağıdakılar daxildir:

- **Zərərli davranışla əlaqəli kompromis göstəriciləri (IoCs):** IoC-lar Zərərli proqram nümunələrinin, domen adlarının və IP ünvanlarınının heşləri bütün firewalları və hücum aşkarlama sistemlərini məlumatlandırmaq və yeniləmək üçün istifadə edilə bilər. Onlar həm də təhdid aktorlarının TTP-lərini anlamaq üçün məqsədə uyğundur. IoC-lar CTI-ın daha geniş sahəsinin bir qoludur.
- **İstifadəçidən alınan məlumatlar:** Təşkilatın infrastrukturu haqqında məlumatlar və onun SIEM alətindən və ya başqa log-larından əldə edilən məlumatlar digər mənbələrlə əlaqələndirilə bilər və ya təhdid ovu kimi proaktiv tədbirlər üçün istifadə edilə bilər.
- **Deep veb:** Bu mənbə gizli onlayn məzmuna sahibdir və kibercinayətkarların tez-tez ziyarət etdiyi eksklüziv haker forumlarını ehtiva edir. Kibercinayətkarlar onun vasitəsilə hücum üçün tanınmış alətlər və xidmətlər haqqında əhəmiyyətli biliklər ala bilərlər. Onlar həmçinin hansı boşluqların müzakirə olunduğunu aşkarlaya bilər, və nəticədə hansı hücum növündən istifadə edəcəklərini müəyyənləşdirə bilərlər. Şəkil 7-də göstərilən rus deep veb forumundan tərcümə edilmiş mesaj ordakı istismarlar haqqında dəyərli məlumat verir.

Şəkil 7: Rus deep veb forumundan tərcümə edilmiş mesaj

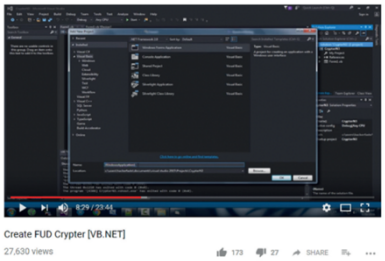
- **Dark veb:** Bu mənbə cinayətkarların qeyri-qanuni məhsul və xidmətlərin əldə edilməsi ilə məşğul olduğu Onion, Tor və ya görünməz internet layihəsi olan I2P kimi anonimlik mərkəzli şəbəkələrdə fəaliyyət göstərən bazarları və biznesləri əhatə edir. O, istifadəçilərə öz gizli məlumatlarının, giriş parollarının və əqli mülkiyyətə aid qiymətli məlumatlarının əlçatan olub-olmadığını və ya satışa çıxarılıb çıxarılmadığını aşkarlamağa imkan verir. Dark veb həm də fərdlərin və ya təşkilatların istifadə etdikləri infrastrukturun hədəfə alınma riskinin olub-olmadığını müəyyən etməyə yardımçı olur. Məsələn, şəkil 8-də göstərilən RemoteDesktop protokolu ilə dark veb şirkətlərinin zədələnmiş müştəri infrastrukturunu necə aşkarlana biləcəyi göstərilir.



Şəkil 8. RemoteDesktop protokolu ilə dark veb şirkətlərinin zədələnmiş müştəri infrastrukturunu necə aşkarlana biləcəyi göstərilir.

- **Mesajlaşma platformaları:** Təhdid iştirakçıları bu üsuldan ünsiyyət qurmaq və məlumat vermək üçün istifadə edirlər. Bəzi kibercinayətkarlar öz mal və xidmətlərini bir-birlərinə satmaq üçün birbaşa ünsiyyətə üstünlük verirlər. Kibercinayətkarlar öz fəaliyyətlərini planlaşdırmaq üçün adətən köhnəlmiş internetdə danışıq protokolu olan IRC və ICQ mesajlaşma sistemlərindən istifadə edərək gələcək metodlar və hədəflər haqqında fikirlərini bölüşürlər. Bu platformalardan istifadə olunaraq təhdid iştirakçıları və onların strategiyaları barəsində məlumat almaq olar.
- **Sosial media platformaları:** Bu platformalar hal-hazırda təhdid aktorlarının çoxu üçün əlçatandır. Əsasən imkanları məhdud olan təhdid aktorları sosial media vasitəsilə kiməsə zərər vurmağa çalışırlar. Bu sistem vasitəsilə onlar əvvəlcədən konkret seçdikləri hədəflərə çatmaq niyyətlərini bəyan edə bilirər. Təhdid aktorları potensial müştəriləri şirnikləndirmək üçün hüquq-mühafizə imkanları məhdud olan populyar şəbəkələrdən əvəzedici strategiya kimi istifadə

edə bilirlər. Əlavə olaraq, sosial media məlumatlarının toplanması istifadəçilərin gizliliyinin pozulması və daxili təhdidləri ehtiva edə bilər. Təhdid kəşfiyyatçılarını işlətdiyi üsullardan biri sosial media mənbələrindən istifadə edərək təhdid aktorlarını tələyə salıb onların strategiyalarını öyrənməkdir. Sosial media platformalarına misal olaraq Telegram, Discord, Twitter, Instagram, Facebook və LinkedIn göstərilə bilər. Əlavə olaraq hər bir sosial media platformasının özünə xas OSINT aləti mövcuddur. Məsələn, Instagram üçün Osintgram var ki, istənilən istifadəçinin nickname-i vasitəsilə Instagram hesabında analiz apara bilir. Facebook üçün Facebook Scanner, Linkedin üçün InSpy alətlərini misal göstərmək olar. Əlavə olaraq, kibercinayətkalar TTP-lərini sosial mediada, məsələn Şəkil 9-da göstərildiyi kimi YouTube-da paylaşa bilərlər.



Şəkil 9: Kibercinayətkaların TTP-lərini YouTube-da paylaşması

- **Human İntelligence:** Azərbaycanca insan zəkası olan CTI mənbəsini yuxarıda qeyd olunan mənbələrdən istifadə edərək insanlarla qarşılıqlı əlaqədə əldə etmək mümkündür. Lakin, açıq təhdid kəşfiyyatçıları bu addımı yalnız müəyyən edilmiş etik və hüquqi standartlara uyğun struktur daxilində həyata keçirməlidirlər. Provayderlər sosial mediadan və insan zəkasından məlumat toplama cəhdlərinin GDPR kimi qaydalara uyğun olmasını təmin etməlidirlər.
- **Zərərli proqram (Malware) analizi:** Bu strategiya vasitəsilə tədqiqatçılar sistemdə müştərinin gizli məlumatlarını hədəf alan IoC-ları müəyyən edə bilərlər. Analiz provayderlərə təhdid aktorlarının strategiyalarını, yanaşmalarını və proseslərini anlamağa kömək edir, təhdid kəşfiyyatçılarına isə daha effektiv reaksiya verməyə imkan yaradır. Sandboxing zərərli proqram analizi üçün yaxşı nümunə ola bilər. O, sınaq üçün təcrid olunmuş mühitdə kodu işə salaraq sistemə zərər vermədən analiz edir və mümkün təhdidləri göstərir. Ransomware şantaj

vasitəsilə fərd və ya təşkilatın şəxsi məlumatlarına girişini həmişəlik bloklayan kriptovirusoloji zərərli proqram olduğu üçün tədqiqatçılar bu proqramı da sözügedən strategiya vasitəsilə analiz edə bilirlər (Guri M., Puzis R. & Choo K., 2019).

- **Bot bazarları:** Bu mənbə hakerlərin zərərli bot proqramlarından istifadə etməklə qurbanların cihazlarından əldə etdikləri məlumatları satdıqları rəqəmsal platformalardır. Bot bazarında risk altında olan şəxsin rəqəmsal şəxsiyyəti daxil olmaqla bütün məlumatları paketlənir və satılır. Paketə istehlakçının giriş məlumatları, kukilər, rəqəmsal barmaq izləri və digər müvafiq məlumatlar daxildir (Imamverdiyev Y., Garayeva G., 2018). Təhdid kəşfiyyatçıları fərdlərin və ya təşkilatların bu sistemlərdə məlumatlarının olub olmadığını öyrənə bilərlər.
- **Kod anbarları**: Bu mənbə təhdid aktorları üçün əlçatan olan istismar edilə bilinəcək məlumatları aşkarlamağa və həmin boşluqlardan hansılarına üstünlük verilməli olduğunu göstərməyə yararlıdır. Buna görə də kibertəhdid kəşfiyyatçıları təhdid aktorlarından əvvəl mümkün boşluqları aşkarlayıb aradan qaldırmalıdırlar. Kod anbarlarına Github, Gitlab, GoogleCode və Bitbucket kimi bir sıra platformaları misal çəkmək olar.
- **Yerləşdirmə saytları (ing. Paste Sites)**: Bu mənbə istifadəçilərə kodları, skriptləri, faylları və ya hər hansı mətn məlumatlarını saxlamağa və paylaşmağa imkan verən veb saytdır. O, oğurlanmış giriş parolları, gizli kod bölmələri və sistemlərdəki təhlükəsizlik boşluqları kimi müxtəlif məlumatları ifşa edə bilər. Bu mənbəyə Pastebin.com, JustPaste.it və başqaları misal göstərilə bilər. Kibertəhdid tədqiqatçıları bu sistemləri daim nəzarətdə saxlayaraq boşluqları və zərərli faktları aradan qaldıra bilərlər.
- **Məlumat paylaşma platformaları**: Sözügedən platformalar istifadə məqsədlərinə görə açıq və ya qapalı, özəl və ya dövlət tərəfindən olmaqla müxtəlif bazaları birləşdirir. Onlar təhdid aktorlarının fəaliyyətləri haqqında daha ətraflı məlumatları birləşdirə bilir. Həmin platformalara nümunə olaraq aşağıdakı bazalar da misal kimi göstərilə bilər:

- Böyük Britaniya Milli Kibertəhlükəsizlik Mərkəzi olan NCSC-nin Kibertəhlükəsizlik Məlumat Paylaşma Tərəfdaşlığı olan CISP-i;
- Maliyyə Xidmətləri Məlumatının Paylaşılması və Təhlili Mərkəzi olan FS-ISAC;
- ABŞ Kompüter Fövqəladə Hallara Hazırlıq Komandası olan US-CERT-in Avtomatlaşdırılmış İndikator Paylaşımı olan AIS platforması;
- AlienVault OTX, DOCGuard, SOC Radar və s.

- **Bal küpəsi (Honeypot):** Bu mənbə şübhəli aktivlik barəsində informasiya toplamağı hədəfləyən hostdur. O, administratorundan başqa heç kəsə admin icazəsi verməyərək informasiya sistemlərinə olan icazəsiz cəhdləri aşkar edir, onları yayındır və ya onlara qarşı çıxır. Təhdid kəşfiyyatçıları bu üsuldan istifadə edərək təhdid məlumatlarını əldə edə bilərlər (Imamverdiyev Y., 2021).
- **İctimaiyyət üçün əlçatan Alətlər və Resurslar**:
  - **Shodan:** Şəbəkə təhlükəsizliyinə nəzarət edir və deep veb də axtarış aparır. O, istifadəçilərə ölkə, əməliyyat sistemi və şəbəkə növü üzrə şəbəkəyə qoşulmuş çoxlu sayda cihazları axtarmağa imkan yaradır və təhdid kəşfiyyatçılarına lazımlı məlumat verir.
  - **Maltego:** Kali Linux-a daxil olaraq rəqəmsal cəsusluq üçün güclü vasitədir. O, "transforms"dan istifadə edərək pulsuz və pullu xarici proqramlardan informasiyaları birləşdirir və analiz edir. Onun proqram təminatı araşdırmalar üçün faydalı olan IP-lər və domenlər təqdim edir (Breeden J, 2023).
  - **BinaryEdge:** ML və kibertəhlükəsizlikdən istifadə edərək ictimai internet məlumatlarını skan etmək, toplamaq və təsnif etmək üçün unikal platformadan istifadə edir. Proqram təminatı bütün İnternetə nəzarət edir və real vaxt rejimində fərd və ya təşkilatla bağlı təhdid məlumat axınları və hesabatlar yaradır.

Şəkil 10: Kibertəhdid kəşfiyyatçıları tərəfindən məlumat alınan mənbələrə nümunələri

- **Xəbərlər və KİV-lər:**

İctimai sənədlər və verilənlər bazaları açıq mənbə kəşfiyyatı olan OSINT üçün əldə olunmuş böyük miqdarda məlumatları özündə birləşdirir. Bunlara kibercinayətkarlıq tarixi və onların fəaliyyəti kimi geniş məlumatlar daxil ola bilər. Kibertəhlükəsizliklə bağlı təhdidlərin iri miqyaslı və sürətlə yayıldığı dövrdə kibertəhdid kəşfiyyatçıları kibertəhlükəsizliklə bağlı ən son xəbərləri əldə etməyə ehtiyac duyurlar (Pastor-Galindo J., Nespoli P., Mármol F. G. & Pérez G., 2020). OSINT üçün əhəmiyyəli olan cari və tarixi kibertəhlükəsizlik məlumatlarının daha tez əldə edilməsinə şərait yaratmaq məqsədilə açıq məlumatları süzgəcdən keçirən xüsusi axtarış motorları, onlayn xəbər saytları, KİV-lər, bloqlar və forumlar yaradılmışdır.

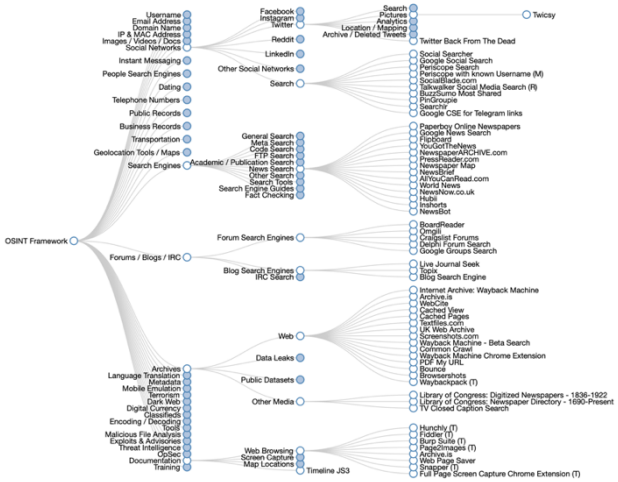
Bu texnologiyalar miqyasından asılı olmayaraq təşkilatlar və kəşfiyyat tədqiqatçıları üçün açıq mənbəli kəşfiyyat məlumatlarını əlçatan etmişdir. OSINT-in məlumat axtarış və ya xəbər bazalarını qurmaq üçün əsasən aşağıdakı üsullardan istifadə olunur (Nuaghari S. A., Jaisan A. & Karuppayah S., 2021):

- Veb saytlardan və axtarış motorlarından Web Scraping Bot vasitəsilə kibertəhlükəsizlik mövzusuna aid məlumatların toplanması;
- Xüsusi monitorinq alətlərindən istifadə etməklə sosial mediadakı kibertəhlükəsizliklə bağlı son məlumatların toplanması;
- Şübhəli şəkilləri və videoları analiz edən alətlər vasitəsilə təhlükəsizlik informasiyalarının toplanması.

Şəkil 11-də də göründüyü kimi OSINT çərçivəsində olan həm arxivdəki, həm də cari veb məlumat resusrları olduqca çoxdur. Onların bəzilərini bir mənbədə birləşdirərək istifadəçilərin və tədqiqatçıların kibertəhdidlər haqqında məlumat toplama prosesinə yardımçı olmaq olar (Nuaghari S., Jaisan A., Karuppayah S., 2021).

Bu dissertasiya işinin praktiki hissəsində Web Scraping Bot vasitəsilə veb internet resurslarından kibertəhlükəsizliklə bağlı məlumatların toplanıb xəbər saytı formatında cəmiyyətə açıq mənbə kimi təqdim edilməsi hədəflənir. Qeyd etmək lazımdır ki, ən son kibertəhlükəsizlik xəbərlərinin hamı üçün əlçatan olması həm OSINT tədqiqatçıları, həm də sadə insanlar üçün faydalı olacaq. Çünki, onlar bu sayt

vasitəsilə həyata keçmiş və ya cəhd olunmuş hücumlar barəsində məlumatlı olmaqla potensial təhdidlərin önünə keçmək üçün tədbir görə bilərlər.



Şəkil 11: OSINT çərçivəsində xəbər və veb məlumat resursları

3.2. Veb tətbiqin layihələndirilməsi və işlənməsi

Dissertasiya işinin praktiki hissəsini ehtiva edən layihənin həyata keçirilməsinin əsas məqsədi ilk növbədə xəbər veb saytlarından kibertəhlükəsizliklə bağlı xəbərlərin kəşfiyyatı üçün Python Requests modulu ile Web Scraping bot yaratmaqdır. Back-end hissəsi üçün Phyton Flask, front-end hissəsi üçün Angular Framework və məlumatların saxlanması hissəsi üçün SQLite databaza sistemindən istifadə edilən veb tətbiqin sözügedən botun yerləşdirilməsindən sonra işə salınması hədəflənmişdir. Daha ətraflı qeyd etsək kibertəhlükəsizliklə bağlı xəbər kəşfiyyatı edən veb saytın qurulması zamanı görülən əsas addımlar bunlardır:

1. Frontend üçün Angular
2. Backend üçün Python Flask
3. Web Scraping prosesi data üçün Python requests modulu ile bot
4. Məlumatların saxlanması üçün SQLite verilənlər bazası

3.2.1. Front-end development üçün istifadə olunan Angular haqqında məlumat və istifadə səbəbi

Angular front-end veb proqramları hazırlamaq üçün nəzərdə tutulmuş güclü proqramlaşdırma üsuludur. Bu layihədə istifadə edilən əsas proqramlaşdırma dili təkmilləşdirilmiş kod təşkilini təklif edən TypeScript-dir. Angular Framework Google tərəfindən hazırlanmışdır. Angular öz kodunu hər birinin öz HTML, CSS və TypeScript-yazılı nəzarətçisi olan bir-birindən asılı komponentlərdən istifadə edərək təşkil edir. Bundan əlavə, Angular komponentlərin qurulmasını asanlaşdırmaqla yanaşı, həmçinin xidmətlərin, direktivlərin və bir sıra digər xüsusiyyətlərin dizaynını gücləndirir. Hal-hazırda, Angular ən populyar front-end veb tətbiqi inkişaf çərçivələrindən (Framework) biri kimi qəbul edilir (Cincovic J., Delcev S. & Draskovic D., 2019). Əlavə olaraq, Angular Framework bu layihənin back-end development-i üçün istifadə olunan Python Flask Framework üçün ən yaxşı kombinasiyalardan biri kimi çıxış edir. Həm geniş və rahat istifadə imkanları, həm də back-end development ilə rahat əməkdaşdlığı baxımından bu layihədə front-end development üçün Angular Framework istifadə edilmişdir. Angular Framework üçün istifadə olunan kod Əlavə 1-də qeyd olunmuşdur.

3.2.2. Back-end development üçün istifadə olunan Python Flask haqqında məlumat və istifadə səbəbi

Python dili adətən təsvir və mətn emalı, əşyaların interneti olan IoT sistemləri ilə əlaqə, eləcə də geniş büdcə və riyazi imkanlara ehtiyacı olan proqramların inkişafı kimi tapşırıqlar üçün üstünlük təşkil edir (Əliquliyev R., Mahmudov R., 2016). Full Stack tərtibatı kontekstində, front-end üçün istifadə edilən Angular tez-tez Python və Flask proqramlaşdırma dilləri ilə birlikdə istifadə olunur. Tez-tez MySQL və SQLite kimi əlaqəli verilənlər bazaları ilə inteqrasiya olunur.

Python yüksək səviyyəli proqramlaşdırma dili kimi məşhurdur. Standart modul kitabxanası müxtəlif standart formatlar və protokollar üçün geniş imkan yaradır. Kitabxanadakı müxtəlif modullar bir neçə sahədə səmərəli işi asanlaşdırır. Bu dil elmi sahələrdə, xüsusən proqram təminatının qurulması və sınaqdan keçirilməsi sahələrində geniş istifadə olunur. Layihədə bu dilin Flask Framework-unu istifadə etməkdə əsas səbəblərdən biri də bu idi. Python məlumatları yaddaş, fayllar və ya verilənlər bazası kimi bir neçə formada saxlamaq imkanına malikdir (Adekunle T., 2023). Python Flask Framework-ü SQLite, MySQL, PostgreSQL, Microsoft SQL Server və Maria DB kimi bir neçə verilənlər bazası sistemini dəstəkləyir. Bu layihədə SQLite verilənlər bazası istifadə olunur. Flask Micro Framework kimi təsnif edilir çünki oun verilənlər bazası kimi daxili xüsusiyyəti yoxdur. Buna görə də qeyd edildiyi kimi müxtəlif xarici verilənlər bazası ilə əməkdaşlıq edərək tamamlanır. Bu Framework LinkedIn və Pinterest tərəfindən hazırlanmış proqramlarda da istifadə olunur (Singh M., Verma A., Parasher A., Chauhan N. & Budhiraja G., 2019).

Tətbiqin Angular front-end və Python back-end komponentləri arasında uğurlu əlaqə yaratmaq üçün flask və flask_cors paketləri tərəfindən təmin edilən sinifləri (ing. Class) quraşdırmaq vacibdir. Server Python skripti daxilində olan sorğuları emal edir. Sistem daxilində sinfin hansı funksiyanı işə salması lazım olduğu Angular Framework-dən ötürülən direktivlərlə müəyyən edilir. Daha sonra müvafiq sinif işə salınır. Əlavə 2-də, müəyyən müddət ərzində kiber xəbərlərə aid nəticələri səhifələmə üsulu ilə əldə edən və verilənlər bazası ilə əlaqələndirən prosedurun layihəyə aid olan hissəsi təqdim edilir. Python Flask Framework kiçik veb saytlar üçün idealdır və veb xidmətləri API

yaratmaq üçün çox uyğundur. Qeyd edilən məlumatlar nəzərə alınaraq layihədə back-end development üçün Python Flask Framework-ün SQLite databazası ilə birgə təklif etdiyi metoddan istifadə olunmuşdur.

3.2.3. Məlumatların saxlanması üçün SQLite verilənlər bazası haqqında məlumat

SQLite, quraşdırılmış sistemlər üçün nəzərdə tutulmuş kompakt verilənlər bazası sistemidir. Bir neçə cədvəl, indeks və görüntülərdən ibarət SQLite verilənlər bazası bir disk faylı daxilində saxlanılır. Əlavə olaraq bu databaza sistemi kiçik və orta miqyaslı proqramlar və ya veb saytlar üçün əvəz olunmazdır. Flask və SQLite birlikdə istifadə edildikdə, mürəkkəb verilənlər bazası serverinin yaradılması və ona nəzarət yükü olmadan kiçik verilənlər bazasına ehtiyacı olan onlayn proqramların və veb saytların qurulması üçün möhkəm və uyğunlaşa bilən həll təmin edir (Le Nhat T., Dung T., 2018). Bu səbəblərdən layihədə veb saytın back-end hissəsi Python Flask və SQLite əsasında yaradılmışdır. SQLite tez-tez Flask veb proqramları ilə birlikdə istifadə olunan səmərəli, müstəqil və fayl yönümlü verilənlər bazası idarəetmə sistemidir. SQLite-ı Flask ilə istifadə etmək üçün aşağıdakı tələblər ödənilməlidir:

1) **Python və Flask:** Flask-dan istifadə etmək üçün Python-a Flask kitabxanası quraşdırılmalıdır. Flask, əsasən SQLite verilənlər bazası istifadə edən onlayn proqramların və və veb saytların inkişafını asanlaşdıran Python veb çərçivəsidir.
2) **SQLite Kitabxanası:** SQLite kitabxanası Python-da əvvəlcədən quraşdırılmış modul kimi daxil edilir və SQLite-ın Flask ilə birlikdə istifadə edilmək üçün olan quraşdırma tələbini aradan qaldırır.
3) **SQLite Database:** Məlumatları saxlamaq üçün SQLite verilənlər bazası faylı tələb olunur. SQLite verilənlər bazaları strukturlaşdırılmış şəkildə məlumatları ehtiva edən və ya .db və ya .sqlite uzantısına malik olan fayllardır. Şəkil 12-də göründüyü kimi layihədəki fayl .db uzantısına malikdir.

Şəkil 12. SQLite verilənlər bazasının .db uzantısı ilə faylı

4) **Fundamental SQL biliyi:** Flask və SQLite verilənlər bazası birlikdə işlədildikdə layihəni həyata keçirməyi sadələşdirsə də, SQL (Strukturlaşdırılmış Sorğu Dili) haqqında ibtidai anlayışa malik olmaq əhəmiyyətlidir. SQLite verilənlər bazasında cədvəlin necə yaradılması, əlaqənin necə müəyyən edilməsi və proseslər başa düşülməlidir.

Layihədə API sorğularını yerinə yetirmək, məlumatları çıxarmaq və SQLite verilənlər bazasında saxlamaq üçün Flask çərçivəsindən istifadə edərək Python proqramı yaradılmışdır. Proqram, HTTP sorğularını API son nöqtəsinə ötürmək üçün sorğu kitabxanasından və qaytarılan məlumatı analiz etmək üçün json kitabxanasından istifadə edir. Çıxarılan məlumatlar SQLite verilənlər bazasından istifadə edilərək saxlanılır. Proqram verilənlər bazası ilə əlaqə yaratmaq və məlumatların saxlanması üçün cədvəllər yaratmaq üçün SQLite3 kitabxanasından istifadə edir.

Əlavə 3-dəki kod nümunəsi Scrapping və SQLite 3 kitabxanalarından istifadə edərək məlumat saxlama prosedurunun Python-da tətbiqini nümayiş etdirir. Layihədə mənbə veb saytından API sorğularını başlatmaq üçün “Requests” (az. sorğular) kitabxanasından istifadə edilir. Daha sonra çıxarılan məlumatları saxlamaq və saxlanma müddətini idarə etmək üçün SQLite verilənlər bazasından istifadə edilir. Scraping sinfi mənbə URL-dən, autentifikasiya üçün API açarından və istifadə olunacaq yerli SQLite verilənlər bazasının fayl adından (news_database.db) istifadə etməklə yaradılır. Yaradılan Web Scrapping Bot, SQLite verilənlər bazasına məlumatların davamlı surətdə çıxarılması və yüklənməsi üçün əsas alət kimi xidmət edir. scraping.scrape() funksiyasından istifadə edərək məlumatları veb-səhifədən çıxarır və sonra add_data(db_name, table_name, data) funksiyasından istifadə edərək verilənlər bazasına daxil edir. Şəkil 13-də göstərir ki, news_database.db faylında 7 başlıq altında məlumatlar toplanmışdır. Həmin başlıqlar bunlardır: id, title, description, news, p.time, category və source.

news

id	title	description	news	p_time	category	source
fe781623	Generative AI is a Looming Cybersecurity Threat	Researchers have not identified any AI-engineered cyberc	Generative AI poses a significant cybersecurity threat a	1715264159	Emerging Threa	https://www.cybersecuritydive.com/news/generative-ai-artificial-intelligence-cyber-threat/715531/?&web_view=true
f19397cc	Pktstat: Open-Source Ethernet Interface Traffic Monitor	Pktstat is an open-source tool that is a straightforward alt	Pktstat is an open-source tool that is a straightforward	1715264159	Security Produc	https://www.helpnetsecurity.com/2024/05/08/pktstat-open-source-ethernet-interface-traffic-monitor/?&web_view=true
77955c16	Security Tools Fail to Translate Risks for Executives	CISOs stress the importance of DevSecOps automation t	A report by Dynatrace highlights that CISOs face challe	1715264159	NA	https://www.helpnetsecurity.com/2024/05/08/ciscos-c-suite-challenges/?&web_view=true
52594294	Mirai Botnet Exploits Ivanti Connect Secure Flaws for Pi	In the attack chain observed by Juniper Threat Labs, CVE	The Mirai botnet, known for its ability to rapidly infect a	1715264159	NA	https://blogs.juniper.net/en-us/security/protecting-your-network-from-opportunistic-ivanti-pulse-secure-vulnerability-exploitation?&web_view=true
b0c676da	CISA Extends CIRCIA Rule Comment Period	The CISA will prolong the comment period for new regula	The Cybersecurity and Infrastructure Security Agency s	1715264159	Laws	https://www.scmagazine.com/brief/cisa-extends-circia-rule-comment-period?&web_view=true
cb0eeb7b	Findings Show MFA Bypass in Microsoft Azure Entra ID	Researchers at Pen Test Partners successfully bypassed	Multi-factor authentication (MFA) has become the back	1715264159	NA	https://www.hackread.com/mfa-bypass-microsoft-azure-entra-id-sso/?&web_view=true
bdfb2e47	Report: 97% of Organizations Hit by Ransomware Turn	According to a new Sophos report, 59% of those organiz	Sophos has released additional findings from its annua	1715264159	NA	https://www.helpnetsecurity.com/2024/05/08/ransomware-law-enforcement-help/?&web_view=true
05dbae3b	Fake E-commerce Network Scams $50M from America	According to a report by the German cybersecurity firm S	A crime ring dubbed BogusBazaar has scammed 850,(	1715264159	Identity Theft	https://www.theregister.com/2024/05/08/bogusbazaar_fraud_china/?&web_view=true
b07b9f13	Six Austrians Arrested in Multi-Million Euro Crypto Sche	Law enforcement agencies from Austria, Cyprus, and Cze	Law enforcement agencies from Austria, Cyprus and C	1715264159	Incident Respo	https://www.infosecurity-magazine.com/news/six-arrested-million-euro-crypto/?&web_view=true
03a5d55c	FBI Warns of Gift Card Fraud Ring Targeting Retail Com	The FBI has issued a warning about a hacking group nam	The FBI has issued a warning about a hacking group ru	1715264159	Threat Intel & Ir	https://www.bleepingcomputer.com/news/security/fbi-warns-of-gift-card-fraud-ring-targeting-retail-companies/?&web_view=true
7deec1d4	Poland Says it was Targeted by Russian Military Intelligc	Poland's CERT-PL said on Wednesday that it had observe	Russian state-sponsored hackers have targeted Polish	1715265108	NA	null
1300a162	How Workforce Reductions Affect Cybersecurity Posture	The Cobalt State of Pentesting Report highlights the chall	The Cobalt State of Pentesting Report highlights the cl	1712269682	NA	https://www.helpnetsecurity.com/2024/05/08/pentesting-cybersecurity-importance/?&web_view=true
a3dc6e65	Update: Boeing Confirms Attempted $200 Million Ransc	Boeing confirmed to CyberScoop that it is the unnamed r	The cybercriminals who targeted Boeing using the Lock	1712269682	Incident Respo	https://cyberscoop.com/boeing-confirms-attempted-200-million-ransomware-extortion-attempt/?&web_view=true

Şəkil 13. SQLite verilənlər bazasının news_database.db faylı

Xülasə, bu həll botdan istifadə edərək veb saytdan çıxarılan məlumatların avtomatlaşdırılmış halda birbaşa verilənlər bazasına əlavə olunmasını təmin edir. Belə bir prosesesin həyata keçirilməsi zamanı GDPR-a uyğun olaraq məlumatların məxfiliyi, məlumatların qorunması və məlumat təhlükəsizliyi aspektlərini nəzərə almaq çox vacibdir.

3.2.4. Veb saytlarda Kibertəhlükəsizliklə bağlı xəbərlərin kəşfiyyatı üçün Python Requests modulu ile Web Scraping edən bot qurulması

İnternet səhifələrindən məlumatların çıxarılması botunu qurmaq üçün Java, C# və ya Python kimi bir neçə kompüter proqramlaşdırma dilindən istifadə edilə bilər. Python Requests, internet səhifələrindən məlumatların çıxarılması üçün bir neçə dəstək paketi təklif edən obyekt yönümlü və yüksək səviyyəli açıq mənbəli proqramlaşdırma dilinin çərçivəsidir. Python Requests modulların və paketlərin istifadəsini asanlaşdırır, proqramların daha kiçik, təkrar istifadə edilə bilən komponentlərə bölünməsini təşkil edir.

Web scrapping prosesi onlayn veb saytlardan xüsusi məlumatların əldə edilməsi aktıdır. Bu yanaşma onlayn mənbələrlə məşğul olmaq, müvafiq məlumatların seçilməsi, verilənlərdən məlumatların çıxarılması və məlumatların lazımi formata çevrilməsi daxil olmaqla bir çox addımları əhatə edir. Web scrapping prosesi tez-tez bir çox alət və kitabxanadan istifadəni əhatə edir:

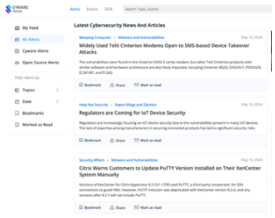
- **Chrome DevTools və ya FireBug Add-on:** HTML/XML sənədində müəyyən elementləri dəqiq müəyyən etmək üçün istifadə oluna bilər. Bu konsepsiyanın nümunəsi Python Beautifulsoup kitabxanasıdır. O, analiz edilmiş ağac strukturlarının naviqasiyası, axtarışı və dəyişdirilməsi üçün alətlər təqdim edir.
- **HTTP kitabxanaları:** Bu kitabxanalar serverlə əlaqəni və cavab sənədinin axtarışını təmin edir. Bu konsepsiyanın nümunəsi Python Requests kitabxanasıdır. O, HTTP sorğularını göndərmək və cavabları emal etmək üçün API təmin edir.

Bu layihədə veb resurlardan məlumat lazım olduğu üçün Python Requests istifadə olunaraq HTTP kitabaxanası olan urllib.parse-a müraciət edilir. Əlavə olaraq requests kitabxanası veb saytlardan məlumat çıxarmaq və məlumat əldə etmək üçün mühüm

vasitədir və o da bot yaratmaq üçün istifadə olunur. Python Requests HTTP sorğuları yaratmaq və HTTP cavablarını idarə etmək üçün sadə və istifadəçi dostu interfeys təklif edir. Bu texnologiyalar API istifadə edərək veb saytdan məlumatların toplanması prosesini avtomatlaşdırmaq üçün birlikdə istifadə edilə bilər. API-yə HTTP sorğusu göndərməklə, bot tələb olunan məlumatı çıxara bilər. Ümumiyyətlə, Python Requests modulundan istifadə veb saytdan məlumatların çıxarılmasının effektivliyini və dəqiqliyini xeyli artıra bilər. Web scrapping prosesi aşağıdakı addımlarda ümumiləşdirilə bilər:

I. Web scrapping əməliyyatı üçün istifadə ediləcək onlayn resursun URL-i müəyyən edilir.
II. Yarım strukturlaşdırılmış məlumatı əldə etmək üçün üstünlük verilən HTTP kitabxanadan istifadə edilməlidir. Bu layihədə urllib.parse kitabxanası istifadə edilmişdir. O, əlaqənin birləşdirilməsi, təkrar cəhdlər və fasilələr kimi qabaqcıl xüsusiyyətləri təmin edir.
III. Lazım olan məlumatları çıxarmazdan əvvəl, yarım strukturlaşdırılmış məlumatlar müəyyən edilir.
IV. Əldə edilmiş yarımstrukturlaşdırılmış məlumatları çıxarmaq və onu daha strukturlaşdırılmış formata çevirmək üçün web scrapping əməliyyatından istifadə edilir.
V. İstifadə edilməli olan məlumatlar veb saytdan çəkilir və Python Flask vasitəsilə SQLite databazasına əlavə edilir.

İnternetdəki məlumatlar web scrapping vasitiəsilə toplandıqdan sonra, onlar JSON faylında saxlanmalı və əgər məlumatların daim yenilənməsi tələb olunursa web scrapping botu hazırlanmalıdır. Web scrapping botu, bu layihədə CyWare.com və onun əsasında digər saytlardandan kibertəhlükəsizlik xəbərlərinin kəşfiyyatını apara bilən avtomatlaşdırılmış bir proqramdır. Web scrapping botundan istifadə edilərək, yuxarıdakı veb saytlardan məlumat çıxarılır və müvafiq olaraq angular.json və news_database.db faylları yaradılır. 14-cü şəkildə xəbərlərin çəkilməsi istənilən veb saytın nümunə səhifəsi göstərilir:



Şəkil 14. Mənbə saytlarının əsası olan CyWare veb saytının interfeysi

Web scrapping botunun hazırlanmasına başlamaq üçün ilk vəzifə ümumiləşdirilmiş URL-i (https://cyware.com/cyber-security-news-articles) müəyyən etməkdir. Bu URL öz tərkibində 30-dan çox kiber xəbər mənbəsini birləşdirir. Həmin URL-lərin siyahısı aşağıdakılardır (Cədvəl 8):

Cədvəl 8. Kibertəhlükəsizlik xəbərlərinə aid mənbə URL-lərin siyahısı

№	Mənbə URL-lərin siyahısı		
1	https://arstechnica.com/security/	17	https://helpnetsecurity.com/
2	https://bbc.com/innovation	18	https://krebsonsecurity.com/
3	https://bleepingcomputer.com/	19	https://nextgov.com/cybersecurity/
4	https://bleepingcomputer.com/	20	https://reuters.com/technology/cybersecurity/
5	https://blogs.juniper.net/en-us/security	21	https://scmedia.com/news/
6	https://broadcom.com/support/security-center/	22	https://securityaffairs.com
7	https://cnbc.com/technology/	23	https://securityaffairs.com/
8	https://csoonline.com	24	https://securityboulevard.com/
9	https://cyberscoop.com/	25	https://securityweek.com
10	https://cybersecuritydive.com	26	https://techcrunch.com/category/security/
11	https://darkreading.com/cybersecurity-operations/	27	https://technologyreview.com
12	https://download.cnet.com/security/	28	https://thehackernews.com
13	https://finsmes.com/	29	https://therecord.media/
14	https://forbes.com/cybersecurity/	30	https://theregister.com/
15	https://hackread.com/	31	https://wired.com/category/security/
16	https://helpnetsecurity.com	32	https://zdnet.com

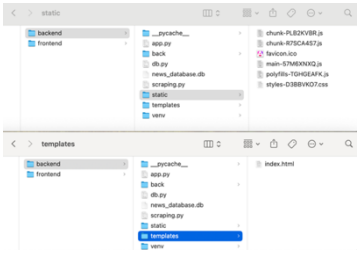
Tətbiqimizdə, təmin edilmiş URL sətirindən istifadə edərək URL-də göstərilən mənbənin şifrəsini açmaq üçün cavabdeh olan decode_url adlı metod yaradıldı. Əlavə 4-dəki kod nümunəsi Python Requests-də olan web scrapping prosedurunu göstərir. Veb resurslarını əldə etmək üçün requests modulundan istifadə edilir. Nümunə olaraq aşağıdakı hissə göstərilə bilər:

```
>>> import requests
def decode_url(url):
… return url.replace('\\u002F', '/')
```

```
>>>def  scrape(url='https://cyware.com/cyber-security-news-articles'):
response = requests.get(url)
```

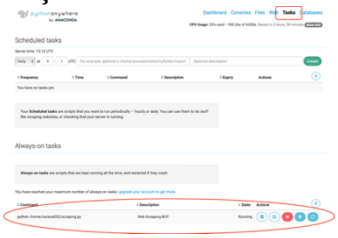
Yuxarıdakı kodda URL-i giriş kimi qəbul edən və resursu əldə etmək üçün requests modulundan istifadə edən scrape adlı metod var. Qeyd olunan proses web scrapping botunun hazır olması ilə nəticələnir.

Layihədə veb saytın işləməsi üçün yuxarıda sadalanan kodlar hər biri quruldu və sonda front-end faylları back-end qovluğuna statik və template qovluqlarının tərkibində daxil edildi. Şəkil 15-də yerləşdirmənin görüntüsü daha dəqiq verilmişdir.



Şəkil 15. Front-end fayllarının back-end qovluğuna statik və template qovluqlarının tərkibində daxil edilməsi

Veb Hostinq olaraq pythonanywhere.com flask veb hostinqi işlədilir, çünki pythonanywhere.com Web Scraping Botu yerləşdirmək üçün həmişə aktiv olan tapşırıqlar bölməsi mövcuddur. Həmin Bot hər 1 dəqiqədən bir ən son xəbərləri yoxlayır. Web Scraping Botunun Veb Hostinq-in Tasks bölməsində yerləşdirilmə görüntüsü Şəkil 16-da göstərilmişdir.



Şəkil 16. Web Scraping Botunun Veb Hostinq-in Tasks bölməsində yerləşdirilmə görüntüsü

Nəticə olaraq, layihənin həyata keçirilmə prosesinə web scrapping botunu hazırlamaq üçün Python Request modulundan istifadə, back-end üçün Phyton Flask ilə API təkmilləşdirmə, front-end üçün Angular JSON işlətmə və verilənlər bazasında məlumatların saxlanması üçün SQLite proqramından istifadə daxildir. Şəkil 17-də adıçəkilən kod fayllarının layihə veb saytının tərkibində olması görünür.

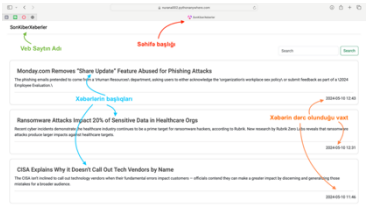
Şəkil 17. Layihə veb saytının tərkibində olan hazırlanmış kodlar

3.3. Eksperimentlərin aparılması

Dissertasiya işində hazırlanmış layihənin kibertəhlükəsizlik xəbərləri barəsində açıq kodlu kəşfiyyat aparmasının təmin olunması üçün təkmilləşdirilmiş texniki hazırlanma hissələri (kodların yazılması, hostinq serverde quraşdırılması, botun işə salınması və s.) 3.2. bölmədə ətraflı şəkildə izah olunmuşdur. Bu hissədə isə layihənin əsasını təşkil edən website-ın funksiyaları göstərilmişdir. Bundan əlavə veb saytın URL linki bəzi öyrənilən açıq kodlu təhdid kəşfiyyatı platformalarında yoxlanılmışdır.

A. İstənilən kibertəhdid kəşfiyyatçısı və istifadəçi tərəfindən istifadə olunan layihə veb saytının funksiyaları

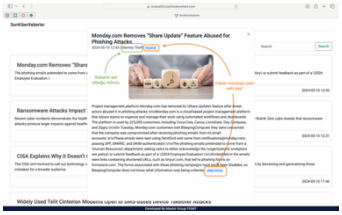
İlk növbədə veb saytın istifadəçi interfeysi (ing. User İnterface) ilə tanışlıq həyata keçirilir. Şəkil 18-də istifadəçi interfeysinin giriş səhifə detalları göstərilmişdir.



Şəkil 18. Layihə veb saytının giriş səhifəsi

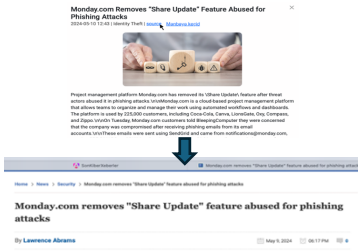
Giriş səhifəsindəki detallarda səhifə başlığının və veb sayt adının "SonKiberXeberler" olduğu görünür. Bundan əlavə xəbər başlıqları və həmin xəbərlərin dərc olunduğu vaxtlar da istifadəçilər üçün ən rahat interfeys formasında əlavə edilib.

İstifadəçi xəbərə daxil olduqda isə xəbərlər haqqında ətraflı məlumat, xəbərin götürüldüyü mənbə saytına keçid üçün link və xəbərin mövzusu barədə ətraflı məlumat ala bilirlər. Əlavə olaraq sadə istifadəçi interfeysi vasitəsilə əgər xəbərin mənbəsində xəbərə aid hər hansı bir şəkil qoyularsa, o şəkli də istifadəçilərin mövzu haqqında fikirlərini daha da yaxşılaşdırmaq üçün layihə veb saytına gətirir. Şəkil 19-da deyilən fikirlərin öz əksini tapdığı görülür.



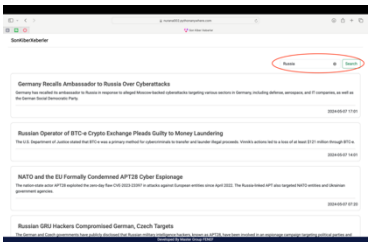
Şəkil 19. Layihə veb saytının xəbər başlığına daxil olduqdan sonra görüntüsü

Qeyd etmək lazımdır ki, xəbərin mənbə səhifəsinə keçidi Şəkil 20-də görmək mümkündür. Nümunədə göründüyü kimi “source” düyməsinin üzərinə toxunulmaqla xəbər mənbəsi olan https://www.bleepingcomputer.com/news/security/mondaycom-removes-share-update-feature-abused-for-phishing-attacks/?&web_view=true saytına keçid alınır.



Şəkil 20. Layihə veb saytının xəbər başlığınadan mənbə veb saytına daxil olunma görüntüsü

İstifadəçi interfeysinin giriş səhifəsində olan əlavə funksiyalardan biri də xəbər axtarış sisteminin olmasıdır. İstənilən kibertəhdid kəşfiyatçısı və ya sadə istifadəçi bu axtarış funksiyası vastəsilə məqsədinə uyğun mövzuda və ya başlıq altında bütün mümkün kibertəhlükəsizlik xəbərlərini əldə edə bilər. Aşağıdakı Şəkil 21-də nümunə kimi mövzu başlığı olaraq “Russia” ilə bağlı xəbərlər araşdırılmışdır. Nəticədə axtarılan mövzuya bağlı fərqli xəbər başlıqları əldə edilmişdir.



Şəkil 21. Layihə veb saytının xəbər axtarış sisteminində “Russia” ilə bağlı nəticələrin görüntüsü

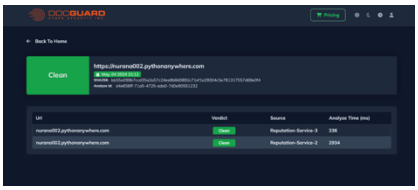
Əlavə olaraq, qeyd edilməlidir ki, layihə ilkin etapda sınaq layihəsi olduğu üçün xüsusi domen adı istifadə olunmayıb. Layihə veb saytına dünyanın istənilən yerindən limitsiz sayda və məhdudiyyətsiz olaraq qeyd olunan link vasitəsilə keçid edilə bilir: https://nurana002.pythonanywhere.com

B. Layihə veb saytının URL linkinin bəzi öyrənilən açıq kodlu təhdid kəşfiyyatı platformalarında yoxlanılması

II fəsildə haqqında ətraflı məlumat verilən OSINT platformalarının açıq mənbə funksiyasından istifadə edərək hazırlanmış veb sayt linkində hər hansı şübhəli

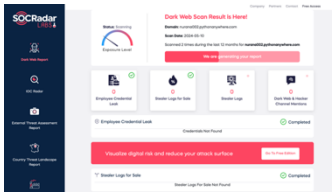
məqamın və ya təhdidin olub olmaması barəsində ətraflı məlumat almaq mümkündür. Buna görə də hazırlanan veb saytın linki URL yoxlanışı üçün mümkün olan DOCGuard, AlienVault və SOCRadar OSINT platformalarında yoxlanılmışdır. Yoxlanışın nəticələri vizual şəkildə aşağıda göstərilmişdir.

İlk növbədə layihə veb saytı DOCGuard platformasında yoxlanılmışdır. Nəticədə Şəkil 22-də görüldüyü kimi veb saytın daxilində heç bir təhdid faktoruna rast gəlinməmiş və səhifə yaşıl rənglə göstərilən “Clean” (az. təmiz) seqmentinə daxil edilmişdir.



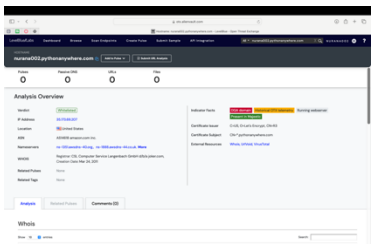
Şəkil 22. Layihə veb saytının DOCGuard platformasında yoxlanmasından sonra nəticə görüntüsü

Daha sonra SOCRadar platformasının tələbələr üçün olan versiyası SOCRadar Labs-da sözügedən veb sayt daxilində təhdid şübhəsinin olub olmadığını yoxlamaq məqsədilə sınaqdan keçirilmişdir. Nəticə olaraq 0 işçi boşluğu, 0 oğurluq loqları və dark veb tərəfindən 0 istifadə nəticələri əldə edilmişdir. Bu da veb saytın DOCGuard platformasında qeyd olunduğu kimi hələ ki heç bir təhdidlə üzləşmədiyini göstərir. Şəkil 23-də qeyd olunan məlumatlar barəsində vizual məlumat təqdim edilir.



Şəkil 23. Layihə veb saytının SOCRadar platformasında yoxlanmasından sonra nəticə görüntüsü

Son olaraq isə layihə əsasında hazırlanmış veb saytın Url linki AlienVault OTX platformasında istifadə olunaraq hər hansı təhdid izinin mövcudluğu barədə məlumat alınmağa çalışıldı. Yoxlanışda çıxan cavablara əsasən layihədə hal-hazırda 0 pulse, 0 zərərli DNS və 0 zərərli fayl aşkar edilmişdir. Şəkil 24-də də göstərildiyi kimi veb saytda heç bir təhdid izinin aşkarlanmaması nəticəsində sayt “Whitelisted” (ağ-siyahı) siyahısına əlavə edilmişdir.



Şəkil 24. Layihə veb saytının AlienVault OTX platformasında yoxlanmasından sonra nəticə görüntüsü

Qeyd etmək lazımdır ki, layihənin daha yeni yaradılması və sistemin yeni işə salınması da hələ ki onun bədniyyətlilərin hədəfindən kənar qalmağına səbəb ola bilər. Gələcək dövr ərzində layihə veb saytının təkmilləşdirilməsi və qeyd edilmiş OSINT platformalarında yenidən yoxlanılması planlaşdırılır.

NƏTİCƏ

Magistrlik dissertasiyasının mövzusu müvafiq tədqiqatların yoxlanılması ilə başlamış və bir çox məsələlər üzrə tədqiqat aparılaraq aşağıdakı nəticələrlə yekunlaşmışdır:

- Kibertəhdid kəşfiyyatının müxtəlif növləri, proses mərhələləri, standarları və bir sıra platformaları analiz edilmişdir;
- Açıq kodlu təhdid kəşfiyyatı sistemləri olan AlienVault OTX, CTI4SOC, DOCGuard, MISP Threat Sharing və OpenCTI platformaları geniş aspektdə araşdırılmışdır;
- Açıq kodlu təhdid kəşfiyyatında tədqiqat aparmaq üçün zəmin yaratmaq məqsədilə müxtəlif OSINT informasiya mənbələri haqqında araşdırmalar aparılmış və ən uyğun variant seçilmişdir.
- Veb tətbiqinin layihələndirilməsi və qurulması məqsədilə front-end hissəsində Angular Framework, back-end hissəsində Phyton Flask, Web Scraping prosesində Python requests modulu ile bot və məlumatların saxlanması üçün SQLite verilənlər bazası istifadə edilmişdir.
- Tədqiqatın praktiki hissəsinin əsas hədəfi olan və Web Scraping Bot istifadə edilərək yaradılan xəbər saytı vasitəsilə kibertəhlükəsizliklə bağlı məlumatlar əldə edilmiş və maraqlı tərəfləri lazımi məlumat və alətlərlə təmin edilmişdir.
- Hazırlanan layihənin veb sayt URL-i olan DOCGuard, AlienVault və SOCRadar OSINT platformalarında analiz edilmiş və heç bir təhdid faktoruna rastlanılmamışdır.

İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISI

1. Əliquliyev, R. M., İmamverdiyev, Y. N. (2012). İnformasiya təhlükəsizliyi insidentləri. Bakı,"İnformasiya Texnologiyaları" nəşriyyatı, 115-122; 166-177.

2. Əliquliyev, R. M., Mahmudov, R.Ş. (2016). İnternet cəmiyyətin inkişafının hərərkətverici qüvvəsi kimi. İnformasiya cəmiyyəti problemləri, №1, 35-45.

3. İmamverdiyev, Y. N. (2015), İnformasiya təhlükəsizliyi teminlərinin izahlı lüğəti. Bakı: "İnformasiya Texnologiyaları" nəşriyyatı.

4. İmamverdiyev Y. N., Muradova, G. (2017). Qlobal kibertəhlükəsizlik sənayesinin analizi. Proqram mühəndisliyinin aktual elmi-praktiki problemləri I respublika konfransı. https://doi.org/10.25045/NCSoftEng.2017.22

5. Mahmudova, R.Ş., Daşdəmirova, K.Q. (2021). İnformasiya cəmiyyəti mühitində bəzi informasiya təhlükəsizliyi problemlərinin analizi. İnformasiya cəmiyyəti problemləri, №2, 83-94. https://doi.org/10.25045/jpis.v12.i2.06

6. Abrahim, K., Cherqi, O., Hammouchi, H., Ghogho, M., & Benbrahim, H. (2021). Leveraging open threat exchange (OTX) to understand spatio-temporal trends of cyber threats. 2021 IEEE International Conference on Intelligence and Security Informatics (ISI), 1-6. https://doi.org/10.1109/ISI53945.2021.9624677

7. Abu, M. S., Selamat, S. R., Yusof, R., & Ariffin A. (2018). Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 371-379. http://doi.org/10.11591/ijeecs.v10.i1.pp371-379

8. Adekunle, G. T., (2023). Automating Data Retention From A Website Using An Application Programming Interface. Journal of Multidisciplinary Engineering Science and Research (JMESR), 2(5), 220-226. http://doi.org/10.14293/PR2199.000114.v1

9. Aggarwal, D., Gautam, S., (2017). Threat Intelligence: Let's Make Internet Secure. International Conference on Advanced Computing (ICAC-2017), 39-45.

10. Alguliyev, R., Nabiyev, B., & Dashdamirova, K. (2023). CTI Challenges and Perspectives as a Comprehensive Approach to Cyber Resilience. 5th International Conference on Problems of Cybernetics and Informatics (PCI), 1-5. https://doi.org/10.1109/PCI60110.2023.10325971

11. AWS Marketplace (2024). Recorded Future Intelligence Platform. https://aws.amazon.com/marketplace/

12. Barnum, S. (2014). Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIXTM). Journal of MITRE Corporation, 11(1), 1-22. http://doi.org/10.1007/978-3-642-27739-9_1716-1

13. Basheer, R., Alkhatib, B. (2021). Threats from the dark: a review over dark web investigation research for cyber threat intelligence. Journal of Computer Networks and Communications, 1-21. https://doi.org/10.1155/2021/1302999

14. Breeden, J. (2023). 15 top open-source intelligence tools. CSO Online Journal.

15. Briliyant, O. C., Tirsa, N. P., & Hasditama, M. A. (2021). Towards an automated dissemination process of cyber threat intelligence data using stix. 6th International Workshop on Big Data and Information Security (IWBIS), 109-114. http://doi.org/10.1109/CIC.2016.060

16. Brown, S., Gommers, J. & Serrano, O. (2015). From Cyber Security Information Sharing to Threat Management. 2nd ACM Work Inf Shar Collab Secur Conference, 43-49. http://doi.org/10.1145/2808128.2808133

17. Chantzios, T. K., Paris, D. (2019). The quest for the appropriate cyber-threat ıntelligence sharing platform. 8th International Conference on Data Science, Technology and Applications. http://doi.org/10.5220/0007978103690376

18. Cincovic, J., Delcev, S., & Draskovic, D. (2019). Architecture of web applications based on Angular Framework: A Case Study. methodology, 7(7).

19. CREST, (2019). What is Cyber Threat Intelligence and how is it used? CREST.

20. Crec, A. (2019). Leveraging OSINT to Improve Threat Intelligence Quality. Conference on Universidade de Lisboa.

21. Crisey, E., Back, G., & Barnum, S. (2015). Leveraging CybOX™ to standardize representation and exchange of digital forensic information. Journal of Digital Investigation, 12, 102-110. http://doi.org/10.1016/j.diin.2015.01.014

22. Crodis, C.(2019). A computing toolkit for building efficient autonomous applications leveraging humanistic intelligence: Teaching project. European Commission CORDIS.

23. Dimitriadis, A., Lontzetidis, E., & Mavridis, I. (2021). Evaluation and Enhancement of the Actionability of Publicly Available Cyber Threat Information in Digital Forensics. IEEE International Conference on Cyber Security and Resilience (CSR), 318-323. http://doi.org/10.1109/CSR51186.2021.9527934

24. Faiella, M., Granadillo, G., Medeiros, I., Azevedo, R., & Zarzosa, S. G. (2019). Enriching Threat Intelligence Platforms Capabilities. 6th International Joint Conference on e-Business and Telecommunications (ICETE), 37-48. http://doi.org/10.5220/0007830400370048

25. Friedman, J., Bouchard, M. (2015). Definitive guide to cyber threat intelligence: Using knowledge about adversaries to win the war against targeted attacks, CyberEdge Group.

26. Guri, M., Puzis, R., Choo, K. R., Rubinshtein, S., Kedma, G., & Elovici, Y. (2019). Using malware for the greater good: Mitigating data leakage. Journal of Network and Computer Applications, 140-145. https://doi.org/10.1016/j.jnca.2019.07.006

27. Hassan, N. A., Hijazi, R. (2018). Open source intelligence methods and tools: A Practical Guide to Online Intelligence. Apress. https://www.oreilly.com/library/view/open-source-intelligence/9781484232132/

28. Imamverdiyev, Y. N. (2018). A consensus ranking method for ınformatıon security threats of an e-government. Problems of information technology, 2, 30-40. https://doi.org/10.25045/jpit.v09.i2.04

29. Imamverdiyev, Y. N. (2021). Analysis of cybersecurity problems in process control systems. Problems of Information Technology, 2, 16-29.

30. Imamverdiyev, Y. N., Garayeva, G. B. (2018). Multi-level analysis of initiatives in countering botnets. Problems of information technology, 1, 32-40. http://doi.org/10.25045/jpit.v09.i1.04

31. Ivanjko, T., Dokman T. (2019). Open Source Intelligence (OSINT): issues and trends. 7th International Conference The Future of Information Sciences INFuture, 191-196. http://doi.org/10.17234/INFUTURE.2019.23

32. Johnson, C. S., Badger, M. L., Waltermire, D. A., Snyder, J., & Skorupka, C. (2016). Guide to Cyber Threat Information Sharing, National Institute of Standards and Technology Special Publication 800-150.

33. Keim, Y., Mohapatra, A. K. (2022). Cyber threat intelligence framework using advanced malware forensics. International Journal of Information Technology, 14(1), 521-530. http://doi.org/10.1007/s41870-019-00280-3

34. Le Nhat, T., Dung, T. (2018). Performance assessment of some data scraping tools for data science analysis. 11th UBT Annual International Conference On Computer Science And Engineering.

35. Lee, M. (2023). Computer security expert of Cyber threat intelligence. Wiley Publication, 49-53; 82-85.

36. Lekidis, A. (2023). Cyber-attack TTP analysis for EPES systems. 16th UBT Annual International Conference On Computer Science And Engineering. http://doi.org/10.48550/arXiv.2302.09164

37. Li, Q., Yang, Z., Liu, B., & Jiang, Z. Y. (2017). Framework of Cyber Attack Attribution Based on Threat Intelligence. International Conference on Interoperability in IoT International Conference on Safety and Security in IoT, 92-103. http://doi.org/10.1007/978-3-319-52727-7_11

38. MISP. (2024). MISP Open Source Threat Intelligence Platform and Open Standards For Threat Information Sharing. https://www.misp-project.org

39. Mkuzangwe, N., Khan, Z. (2020). Cyber-threat information-sharing standards: A review of evaluation literature. The African Journal of Information and Communication, 25, 1-12. http://doi.org/10.23962/10539/29191

40. Nova, K. (2022). Security and resilience in sustainable smart cities through cyber threat intelligence. International Journal of Information and Cybersecurity, 21-42.

41. Nuaghari, S. A., Jaisan, A., & Karuppayah, S. (2021). OSINT Explorer: A Tool Recommender Framework for OSINT Sources. International Conference on Advances in Cyber Security, 389-400. http://doi.org/10.1007/978-981-16-8059-5_24

42. Oherqi, C., Hammouchi, H., Ghogho, M., & Benbrahim, H. (2021). Leveraging Open Threat Exchange (OTX) to Understand Spatio-Temporal Trends of Cyber Threats: Covid-19 Case Study. IEEE International Conference on Intelligence and Security Informatics (ISI), 1-6. http://doi.org/10.1109/ISI53945.2021.9624677

43. Özeren, S. (2024). Open Source Cyber Threat Intelligence Platforms. Online Book of Picus Security. https://www.picussecurity.com/

44. Öztürk, E. (2023). Top 10 Best Free Cyber Threat Intelligence Sources and Tools in 2023. Cyber Intelligence SOCRadar. https://socradar.io/

45. Paakala, S. (2021). Integrating Open Threat Exchange data in a Security Operations Center. Conference of South-Eastern Finland University of Applied Sciences (XAMK), 9-16.

46. Pastor-Galindo, J., Nespoli, & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. Journal of IEEE Access, 8, 10282-10304. https://doi.org/10.1109/ACCESS.2020.2965257

47. Patel, I. V. (2021). The necessity of cyber threat intelligence / by Iksith Patel. Utica.

48. Phipps, J. (2024). 7 Top Threat Intelligence Platforms & Software in 2024. Journal of eSecurity Planet.

49. Preuveneers, D., Joosen, W. (2021). Sharing machine learning models as indicators of compromise for cyber threat intelligence. Journal of Cybersecurity and Privacy, 1(1), 140-163. https://doi.org/10.3390/jcp1010008

50. PwC (2021). PwC's 24th Annual Global CEO Survey: CEOs on their tech concerns. Report by PwC annual survey of CEO on IT or technology concerns.

51. Quinlan, S., Nguyen, C. K. (2023). A Brief History and Critique of Cybersecurity Attack Frameworks. Inaugural defense and security research symposium of the purdue military research institute. https://engineering.purdue.edu

52. Roberts, A., Cyber threat intelligence – what does it even mean? Cyber Threat Intelligence, 2021, pp. 17-36. http://doi.org/10.1007/978-1-4842-7220-6_2

53. Rose, R., Pillitteri, V., Graubart, R., & Mcquaid, R. (2021). Developing Cyber Resilient Systems: A Systems Security Engineering Approach. Special Publication National Institute of Standards and Technology NIST SP. https://doi.org/10.6028/NIST.SP.800-160v2r1

54. Samtani, S., Abate, M., Benjamin, V., & Li W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. Journal of International Cybercrime and Cyberdeviance, 135-154. http://doi.org/10.1007/978-3-319-90307-1_8-1

55. Sauerwein, C., Sillaber, C., Mussmann, A., & Breu, R. (2017). Threat intelligence sharing platforms: An exploratory study of software vendors and research perspectives. 13th Conference on Wirtschaftsinformatik, 837-851.

56. Seker, E. (2019). Cyber Threat Intelligence Understanding Fundamentals. Milli Təhlükəsizlik Və Hərbi Elmlər Elmi-Praktiki Jurnal, 75-78.

57. Singh, M., Verma, A., Parasher, A., Chauhan, N., & Budhiraja, G. (2019). Implementation of Database Using Python Flask Framework. International Journal of Engineering and Computer Science, 8(12), 24890-24893. https://doi.org/10.18535/ijecs/v8i12.4390

58. Strom, B., Appebaum, A., & Miller, D.P. (2020). MITRE Corporation: Design and Philosophy. MITRE Corporation.

59. Sukshi, R. (2017). Cyber Security Market 2018-2028 By Size, Share, Trends, Growth, Forecast. TechSci Research, 27-39. https://www.techsciresearch.com/report/cyber-security-market/4741.html

60. Sytrom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2018). Mitre Att&ck: Design and philosophy. In Technical report of The MITRE Corporation, 6-25.

61. Trifonov, R., Nakov, O., & Mladenov, V. (2018). Artificial intelligence in cyber threats intelligence. International conference on intelligent and innovative computing applications (ICONIC), 1-4. https://doi.org/10.1109/ICONIC.2018.8601235

62. Tserpes, K., Gallicchio, C., Bravos, & Veledar, O. (2023). Computing Toolkit for Building Efficient Autonomous appliCations Leveraging Humanistic IntelliGence. 3rd Workshop Conference on Flexible Resource and Application Management on the Edge (FRAME '23), 37–39. https://doi.org/10.1145/3589010.3594886

63. Turhan A. P. (2024), How to Use DOCGuard. Docguard Detect Malware Platform.

ƏLAVƏLƏR

Əlavə 1. Angular Framework (JSON)


```
{"$schema": "./node_modules/@angular/cli/lib/config/schema.json",
 "version": 1,
 "newProjectRoot": "projects",
 "projects": {
  "cyware": {
   "projectType": "application",
   "schematics": {},
   "root": "",
   "sourceRoot": "src",
   "prefix": "app",
   "architect": {
    "build": {
     "builder": "@angular-devkit/build-angular:application",
     "options": {
      "outputPath": "dist/cyware",
      "index": "src/index.html",
      "browser": "src/main.ts",
      "polyfills": [
       "zone.js"],
      "tsConfig": "tsconfig.app.json",
      "assets": [
       "src/favicon.ico",
       "src/assets"],
      "styles": [
       "@angular/material/prebuilt-themes/indigo-pink.css",
       "node_modules/bootstrap/dist/css/bootstrap.min.css",
       "src/styles.css"],
      "scripts": []},
     "configurations": {
      "production": {
       "budgets": [
        {"type": "initial",
         "maximumWarning": "500kb",
         "maximumError": "1mb"},
        {"type": "anyComponentStyle",
         "maximumWarning": "2kb",
         "maximumError": "4kb"}],
       "outputHashing": "all"},
      "development": {
       "optimization": false,
       "extractLicenses": false,
       "sourceMap": true}},
     "defaultConfiguration": "production"},
    "serve": {
     "builder": "@angular-devkit/build-angular:dev-server",
     "configurations": {
```

```
          "production": {
            "buildTarget": "cyware:build:production"},
          "development": {
            "buildTarget": "cyware:build:development"}},
        "defaultConfiguration": "development"},
      "extract-i18n": {
        "builder": "@angular-devkit/build-angular:extract-i18n",
        "options": {
          "buildTarget": "cyware:build"}},
      "test": {
        "builder": "@angular-devkit/build-angular:karma",
        "options": {
          "polyfills": [
            "zone.js",
            "zone.js/testing"],
          "tsConfig": "tsconfig.spec.json",
          "assets": [
            "src/favicon.ico",
            "src/assets"],
          "styles": [
            "@angular/material/prebuilt-themes/indigo-pink.css",
            "src/styles.css",
            "node_modules/bootstrap/dist/css/bootstrap.min.css"],
          "scripts": []}}}}},
  "cli": {"analytics": false}}
```

Əlavə 2. Python Flask App

```
from flask import Flask, request, jsonify, send_file, abort, render_template, send_from_directory
from flask_cors import CORS
import db
from datetime import datetime
import os

app = Flask(__name__, static_folder='static')
CORS(app)

def timestamp_to_datetime(timestamp):
    if isinstance(timestamp, int):
        dt_object = datetime.fromtimestamp(timestamp)
        formatted_datetime = dt_object.strftime('%Y-%m-%d %H:%M')
        return formatted_datetime
    else:
        return 'NA'

# Pagination function
def paginate_data(data, page, is_search):
    data.reverse()
    per_page = 5
    start_index = (page - 1) * per_page
    end_index = start_index + per_page
```

```
    if is_search:
        date_corrected = []
        for i in data[start_index:end_index]:
            i['p_time'] = timestamp_to_datetime(i['p_time'])
            date_corrected.append(i)
        return date_corrected, end_index < len(data)
    date_corrected = []
    for i in data[start_index:end_index]:
        i['p_time'] = timestamp_to_datetime(i['p_time'])
        date_corrected.append(i)
    return date_corrected, end_index < len(data)

# Endpoint for fetching paginated data
@app.route('/get_data', methods=['GET'])
def get_data():
    page = request.args.get('pag', 1, type=int)
    search_query = request.args.get('q', '')
    database_name = "news_database.db"
    table_name = "news"
    all_data = db.get_data(database_name, table_name)
    # Filter data based on search query
    if search_query:
        filtered_data = [record for record in all_data if search_query.lower() in
record['description'].lower() or search_query.lower() in record['news'].lower()]
    else:
        filtered_data = all_data
    if len(search_query) > 0:
        is_search = True
    else:
        is_search = False
    paginated_data, has_more = paginate_data(filtered_data, page, is_search)
    return jsonify({'data': paginated_data, 'has_more': has_more})

@app.route('/', defaults={'path': ''})
@app.route('/<path:path>')
def catch_all(path):
    if path != "" and os.path.exists(app.static_folder + '/' + path):
        return send_from_directory(app.static_folder, path)
    else:
        return render_template('index.html')

@app.route('/', methods=['GET'])
def index():
    return render_template('index.html')

if __name__ == '__main__':
    app.run(debug=True)
```

Əlavə 3. Python Flask + SQLite Database

```
import sqlite3
import scraping
```

```
# Function to create a new SQLite database
def create_database(db_name):
    conn = sqlite3.connect(db_name)
    conn.close()
# Function to create a table in the database
# Function to create a table in the database
def create_table(db_name, table_name):
    conn = sqlite3.connect(db_name)
    cursor = conn.cursor()
    try: cursor.execute(f'''CREATE TABLE {table_name} (
                    id TEXT PRIMARY KEY,
                    title TEXT,
                    description TEXT,
                    news TEXT,
                    p_time TIMESTAMP,
                    category TEXT,
                    image TEXT,
                    source TEXT)''')
    except sqlite3.OperationalError as e:
        print(f"Table '{table_name}' already exists.")
        # If the table already exists, drop it and recreate it
        cursor.execute(f'DROP TABLE {table_name}')
        cursor.execute(f'''CREATE TABLE {table_name} (
                    id TEXT PRIMARY KEY,
                    title TEXT,
                    description TEXT,
                    news TEXT,
                    p_time TIMESTAMP,
                    category TEXT,
                    image TEXT,
                    source TEXT)''')
    conn.commit()
    conn.close()

def clear_table(db_name, table_name):
    conn = sqlite3.connect(db_name)
    cursor = conn.cursor()
    cursor.execute(f'DELETE FROM {table_name}')
    conn.commit()
    conn.close()
# Function to add data to the database
def add_data(db_name, table_name, data):
    conn = sqlite3.connect(db_name)
    cursor = conn.cursor()
    existing_ids = {row[0] for row in cursor.execute(f'SELECT id FROM {table_name}')}
    for item in data:
        if item['id'] not in existing_ids:
            keys = ', '.join(item.keys())
            placeholders = ', '.join('?' * len(item))
            values = tuple(item.values())
            cursor.execute(f'INSERT INTO {table_name} ({keys}) VALUES ({placeholders})', values)
    conn.commit()
    conn.close()

def get_data(db_name, table_name):
    conn = sqlite3.connect(db_name)
    cursor = conn.cursor()
```

```
    cursor.execute(f'SELECT * FROM {table_name}')
    rows = cursor.fetchall()
    columns = [desc[0] for desc in cursor.description]
    data = []
    for row in rows:
        data.append(dict(zip(columns, row)))
    conn.close()
    return data
# Retrieve data from the database
# #clear_table(database_name, table_name)
## database_name = "news_database.db"
# table_name = "news"
# #create_table(database_name, table_name)
# #clear_table(database_name, table_name)
# add_data(database_name, table_name, scraping.scrape())
# data = get_data(database_name, table_name)
# print((data))
```

Əlavə 4. Python Requests module

```
import requests    import json    import re    import urllib.parse
import time    from bs4 import BeautifulSoup
def decode_url(url):
    return url.replace('\\u002F', '/')
def extract_data(start_str, end_str, input_str):
    pattern = re.compile(re.escape(start_str) + "(.*?)" + re.escape(end_str))
    match = pattern.search(input_str)
    if match:    return match.group(1).strip()
    else:    return None
def convert_to_dic(text):
    id = extract_data("id:", '",', text).replace('"', '')
    title = extract_data("title:", '",', text).replace('"', '')
    description = extract_data("desc1:", '",', text).replace('"', '')
    news = extract_data("text:", '",', text).replace('"', '')
    p_time = extract_data("p_time:", ',', text).replace('"', '')
    p_time = str(int(time.time()))
    try: category = extract_data("category:", ',', text).replace('"', '')
        if len(category) < 3:
            category = 'NA'
    except: category = 'NA'
    try: image = decode_url(extract_data("image:", '",', text).replace('"', ''))
    except: image = 'NA'
    return {"id": id,"title":title, "description": description, "news": news, "p_time":p_time,
"category": category, "image": image}
def get_source(dic, html_content):
    soup = BeautifulSoup(html_content, 'html.parser')
    source_container = soup.find('div', id=dic['id'])
    a_tag = source_container.find('div', class_='cy-panel__body').find('a', target='_blank')
    href = a_tag['href']
    dic['source'] = href
    return dic
def scrape(url='https://cyware.com/cyber-security-news-articles'):
    response = requests.get(url)
```

```
    #print(response.text)
    text = (response.text.split("results:")[1].split("}]")[0] + '}]')
    splitted_1 = text.split('},')
    final_texts = []
    final_texts.append(splitted_1[0][1:] + '}')
    final_texts.append(splitted_1[-1][:-2] + '}')
    for t in splitted_1[1:-1]:
        final_texts.append(t + '}')
    data = [convert_to_dic(d) for d in final_texts]
    data = [get_source(d, response.text) for d in data]
    return data
```

Source kodlar GitHub vasitəsilə linkdə yerləşdirilib:

https://github.com/nuraca/AzTU-Project.git

Açıq Kodlu Kibertəhdid Kəşfiyyatı Sisteminin İşlənməsi

XÜLASƏ

Diplom işi təhdid mühitinin dinamik xarakterini və təşkilatların qarşılaşdığı kibertəhdidlərin artan mürəkkəbliyini araşdırır. Bu təhdidlərin aradan qaldırılmasında kibertəhdid kəşfiyyatı olan CTI-ın əhəmiyyəti vurğulanır və mövzu barəsində olan mövcud tədqiqatları qiymətləndirir. Açıq mənbə təhdid kəşfiyyatının əhəmiyyətini vurğulanaraq, CTI-ın növləri, proses mərhələləri, standartları və platformaları daxil olmaqla, bir çox aspektlər araşdırılır.

Bundan əlavə, araşdırma təhdid məlumatlarının səmərəli şəkildə toplanması üçün təşkilatlar, əsasən kiçik və orta müəssisələr tərəfindən istifadə edilən açıq mənbəli kəşfiyyat sistemlərini araşdırır. Onlayn xəbər mənbələrindən kibertəhlükəsizliyə aid məlumatlarının toplanmasına və ictimaiyyətin istifadə edə biləcəyi veb-saytda nümayiş etdirilməsinə yönəlmiş layihənin işlənməsi də təsvir edilir. Layihənin əsas məqsədi kibertəhlükəsizliklə əlaqəli təhdidlərin qarşısının alınmasına kömək etmək üçün mövzu ilə bağlı ən son xəbərləri əlçatan etməkdir.

Layihə istifadəçi interfeysi üçün Angular çərçivədən, server tərəfi funksionallığı üçün Python Flask-dan istifadə edən veb tətbiqi qurmaq və xəbər saytlarından məlumat toplamaq üçün veb scrapping botunu tətbiq etməklə həyata keçirilir. Diplom işi güclü təhdid kəşfiyyatı platformasının yaradılmasında elmi və praktiki ehtiyacı vurğulayır. Araşdırma təhdid kəşfiyyatı mövzusunun təkmilləşdirilməsində həm nəzəri əsasların, həm də praktiki tətbiqlərin həyata keçirilməsi ilə bitir.

Açar sözlər: kibertəhdid kəşfiyyatı, açıq mənbəli kəşfiyyat, təhdid kəşfiyyat platformaları, standartlar, təhdid kəşfiyyat mənbələri, təhdid kəşfiyyat sistemi.

Development of an Open Source Cyber Threat Intelligence System

SUMMARY

The thesis examines the dynamic nature of the threat environment and the increasing complexity of cyber threats faced by organizations. It highlights the importance of cyber threat intelligence (CTI) in addressing these threats and evaluates existing research on the topic. Many aspects of CTI are explored, including types, process steps, standards, and platforms, emphasizing the importance of open source threat intelligence.

In addition, the study examines open source intelligence systems used by organizations, mainly small and medium enterprises, to efficiently collect threat intelligence. It also describes the development of a project aimed at gathering cybersecurity information from online news sources and displaying it on a publicly accessible website. The main goal of the project is to make available the latest news on the topic to help prevent threats related to cyber security.

The project is implemented by building a web application that uses the Angular framework for the user interface, Python Flask for the server-side functionality, and implementing a web scraping bot to collect data from news sites. The thesis highlights the scientific and practical need to create a robust threat intelligence platform. The study concludes with the implementation of both theoretical foundations and practical applications in improving the subject of threat intelligence.

Keywords: cyber threat intelligence, open source intelligence, threat intelligence platforms, standards, threat intelligence sources, threat intelligence system.

Разработка Системы Анализа Киберугроз С Открытым Исходным Кодом

РЕЗЮМЕ

В диссертации рассматривается динамичный характер среды угроз и растущая сложность киберугроз, с которыми сталкиваются организации. В нем подчеркивается важность разведки киберугроз (CTI) в борьбе с этими угрозами и оцениваются существующие исследования по этой теме. Исследуются многие аспекты CTI, включая типы, этапы процессов, стандарты и платформы, подчеркивая важность анализа угроз с открытым исходным кодом.

Кроме того, в исследовании рассматриваются системы разведки с открытым исходным кодом, используемые организациями, в основном малыми и средними предприятиями, для эффективного сбора информации об угрозах. В нем также описывается разработка проекта, направленного на сбор информации о кибербезопасности из новостных онлайн-источников и ее отображение на общедоступном веб-сайте. Основная цель проекта — сделать доступными последние новости по теме, чтобы помочь предотвратить угрозы, связанные с кибербезопасностью.

Проект реализуется путем создания веб-приложения, которое использует платформу Angular для пользовательского интерфейса, Python Flask для серверной функциональности и внедрения бота для сбора данных с новостных сайтов. В диссертации подчеркивается научная и практическая необходимость создания надежной платформы анализа угроз. Исследование завершается реализацией как теоретических основ, так и практических приложений для улучшения предмета разведки угроз.

Ключевые слова: разведка киберугроз, разведка из открытых источников, платформы разведки угроз, стандарты, источники разведки угроз, система разведки угроз.