Təhlükəsizlik Əməliyyatları Mərkəzləri üçün Real Vaxt Hücum Vizuallaşdırma Sisteminin Dizaynı

Rəşad Əliyev[1], Sərfi Həbibova[2], Ülviyyə Məmmədova[3]
[1,2]Xəzər Universiteti, [3]YER xSP MMC, Bakı, Azərbaycan
[1]*rashad@aliev.info*, [2]*serfihebibova@gmail.com*, [3]*ulviyya.mammadova001@gmail.com*

***Xülasə*— Təşkilatların infrastrukturlarını hədəf alan kiberhücumlar həm miqyas, həm də mürəkkəblik baxımından artaraq vəziyyət barədə effektiv məlumatlılıq mexanizmlərinə artan tələbat yaradır. Təhlükəsizlik Məlumatı və Hadisə İdarəetmə (SIEM) sistemləri təhlükəsizlik hadisələrinin mərkəzləşdirilmiş aşkarlanmasına və təhlilinə imkan versə də, onların vizuallaşdırma imkanları əsasən mətn və idarəetmə panelinə əsaslanan təsvirlərlə məhdudlaşır. Mövcud qlobal kibertəhdid xəritələri yüksək səviyyəli anlayışlar təqdim edir, lakin təşkilata xas aktuallığa malik deyil. Bu məqalədə təhlükəsizlik xəbərdarlıqlarını (alert-ləri) coğrafi kibertəhlükə xəritəsinə çevirən real vaxt rejimində, SIEM-ə əsaslanan təhlükələrin vizuallaşdırılması yanaşması təklif olunur. Təklif olunan həll yolu real vaxt rejimində məlumatlılığı artırır.**

Açar sözlər*— *kibertəhlükəsizlik; təhlükəsizlik əməliyyatları mərkəzi; kibertəhdid; kiberhücumlar.

I. GİRİŞ

Rəqəmsal infrastrukturların sürətlə genişlənməsi və informasiya sistemlərinə artan etibar dünya miqyasında təşkilatlar üçün kibertəhlükəsizlik risklərini əhəmiyyətli dərəcədə artırıb. İnformasiya qaynaqları getdikcə bir-biri ilə əlaqəli və internetə məruz qaldıqca, serverləri, şəbəkələri və vacib xidmətləri hədəf alan kiberhücumlar həm tezlik, həm də mürəkkəblik baxımından inkişaf edib. İnformasiya cəmiyyətinin inkişafı kontekstində kibertəhlükəsizlik artıq yalnız texniki bir problem deyil, strateji və sosial-iqtisadi bir problem hesab olunur. İnformasiya təhlükəsizliyinin təmin edilməsi, xüsusən də bilik əsaslı iqtisadiyyata keçən ölkələr üçün davamlı rəqəmsal transformasiya və milli kiberdayanıqlılıq üçün əsas şərtdir [1].

Hadisələrin toplanması və aşkarlanmasındakı effektivliyinə baxmayaraq, bir sıra tədqiqatlar göstərir ki, SIEM sistemləri əsasən mətn qeydlərinə, cədvəl məlumatlarına və statik idarəetmə panellərinə əsaslanır ki, bu da analitiklərin yüksək xəbərdarlıq həcmləri altında mürəkkəb hücum ssenarilərini tez bir zamanda anlamaq qabiliyyətini məhdudlaşdıra bilər. Kiber vəziyyət barədə məlumatlılıq insidentlərə cavab və qərar qəbuletmə proseslərinin təkmilləşdirilməsində mühüm amil kimi müəyyən edilmişdir. Əvvəlki tədqiqatlar göstərir ki, kiber hadisələrin vizual təsvirləri analitiklərin hücum nümunələri, zaman trendləri və təhdid əlaqələri haqqında koqnitiv anlayışını əhəmiyyətli dərəcədə artıra bilər [2, 3]. Bununla belə, sistematik ədəbiyyat icmalı göstərir ki, mövcud vizuallaşdırma yanaşmaları çox vaxt real vaxt uyğunlaşma qabiliyyətinə malik deyil və məkan kontekstini, xüsusən də SIEM mühitlərində mənalı şəkildə daxil edə bilmir [4]. Coğrafi məkan məlumatlarının kibertəhlükəsizlik monitorinqinə inteqrasiyası, regional hücum konsentrasiyalarını və mənşəyə əsaslanan təhdid dinamikasını aşkar etmək potensialına baxmayaraq, az araşdırılmış bir sahə olaraq qalır.

Qlobal səviyyədə bir neçə kommersiya kibertəhlükəsizlik vendorları, ümumiləşdirilmiş kibertəhdid kəşfiyyatı məlumatlarına əsaslanaraq dünya miqyasında hücum fəaliyyətlərini vizuallaşdıran ictimai real vaxt kibertəhdid xəritələri təqdim edir. Kaspersky Cyber Threat Map [5], Radware Live Threat Map [6] və Check Point ThreatMap [7] kimi platformalar qlobal hücum trendləri və coğrafi paylanmalar haqqında yüksək səviyyəli məlumatlar təqdim edir. Bu həllər ümumi məlumatlılığa töhfə versə də, əsasən anonim və ümumiləşdirilmiş məlumatlar təqdim edir və bu da onların təşkilata xas monitorinq və əməliyyat reaksiyası üçün tətbiqini məhdudlaşdırır. Nəticə etibarilə, bu cür qlobal vizuallaşdırmalar müəyyən serverləri, təşkilatları və ya lokal infrastrukturları hədəf alan hücumları təhlil etmək üçün təhlükəsizlik xəbərdarlıqlarını real vaxt rejimində təhlükə xəritələrinə çevirən, vəziyyət barədə məlumatlılığı artıran, analitik səmərəliliyi artıran və SOC mühitlərində daha sürətli hadisələrə cavab verən bir yanaşmaya ehtiyac olduğunu vurğulayır.

II. PROBLEMİN TƏSVİRİ

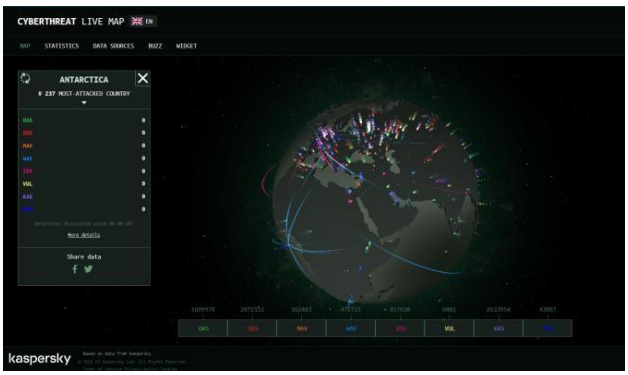
Şirkətlər və təşkilatlar informasiya texnologiyaları infrastrukturlarını qurduqları ilkin mərhələlərdə əsasən funksionallığa və xidmətlərin fasiləsizliyinə fokuslanırlar. Lakin zaman keçdikcə bu infrastrukturlar internetə açıq xidmətlərin artması və sistemlərin miqyasının genişlənməsi səbəbindən kiberhücumlar üçün cəlbedici hədəfə çevrilir. Bu mərhələdə hücumların qeydə alınması, təhlükəsizlik loqlarının toplanması, hadisələrin korrelyasiyası və insidentlərin vaxtında aradan qaldırılması üçün ixtisaslaşmış kibertəhlükəsizlik həllərinə ehtiyac yaranır. Bu ehtiyacın qarşılanması məqsədilə bir çox təşkilatlar təhlükəsizlik hadisələrinin mərkəzləşdirilmiş şəkildə toplanması və təhlili üçün SIEM sistemlərindən istifadə edirlər.

Aparılmış araşdırmalar göstərir ki, SIEM sistemləri hücumların aşkarlanması və hadisələrin korrelyasiyası baxımından effektiv olsa da, təqdim etdikləri vizuallaşdırma imkanları əsasən mətn əsaslı loqlar, cədvəllər və statik panellərlə (dashboard-larla) məhdudlaşır [8]. Fərqli SIEM platformalarının qiymətləndirilməsi üzrə aparılan tədqiqatlar da bu sistemlərin kontekstual vizuallaşdırmalar yaratmaqda

DOI: 10.25045/cyber.gov.2026.29

məhdud imkanlara malik olduğunu ortaya qoymuşdur [9]. Nəticə etibarilə, yüksək həcmli təhlükəsizlik hadisələri zamanı analitiklərin hücumların mənbəyi, növü və zaman üzrə paylanmasını operativ şəkildə qavraması çətinləşir.

Mövcud praktikada bir çox təşkilatlar aşkar etdikləri kiberhücumları yalnız daxili təhlükəsizlik komandaları səviyyəsində təhlil edir və ya müvafiq dövlət qurumlarına hesabat verməklə kifayətlənirlər. Qlobal səviyyədə isə bəzi kommersiya kibertəhlükəsizlik şirkətləri ümumiləşdirilmiş məlumatlara əsaslanan ictimai real vaxt kiberhücum xəritələri təqdim edirlər. Məsələn, Kaspersky Cyber Threat Map qlobal miqyasda müşahidə olunan zərərli fəaliyyətləri ölkələr üzrə vizuallaşdıraraq hücum növləri və intensivliyi haqqında ümumi təsəvvür yaradır (Şəkil 1).



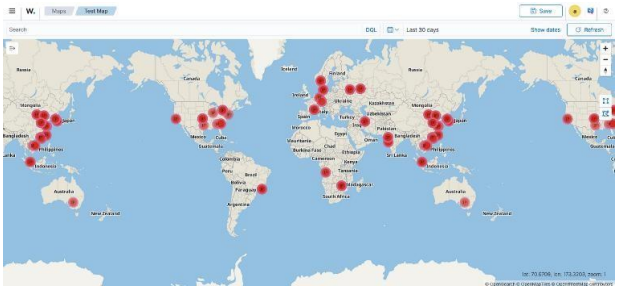
Şəkil 1. Kaspersky – Real Vaxt Hücum Xəritəsi

Oxşar şəkildə, Radware Live Threat Map dünya üzrə Distributed Denial-of-Service (DDoS) və digər şəbəkə əsaslı hücumları real vaxt rejimində nümayiş etdirir. Check Point ThreatMap platforması isə qlobal sensor şəbəkəsindən toplanan məlumatlara əsaslanaraq hücumların coğrafi paylanmasını və statistik göstəricilərini təqdim edir. Bundan əlavə, Fortinet Threat Map [10] və Cisco Talos Intelligence [11] kimi həllər də qlobal təhlükə mənzərəsini əks etdirən vizuallaşdırma platformaları təqdim edən tanınmış nümunələr sırasındadır. Bu tip platformalar qlobal təhdid mənzərəsini nümayiş etdirmək baxımından faydalı olsa da, konkret təşkilatlara və ya serverlərə yönəlmiş hücumları əks etdirmir və əməliyyat səviyyəsində SOC komandalarının ehtiyaclarını tam qarşılamır.

Mövcud real vaxt kiberhücum vizuallaşdırma alətləri əsasən qlobal və ümumi təhdid fəaliyyəti perspektivini təqdim edir. IDS (Intrusion Detection Systems) və SIEM platformaları təhlükəsizlik hadisələrini aşkar etmək və əlaqələndirmək üçün geniş imkanlar təqdim etsə də, bu məlumatın SOC analitiklərinə təqdim olunma üsulu çox vaxt statik qrafiklər və məhdud interaktiv panellərlə məhdudlaşır. Yüksək trafikli və çoxsaylı hücum ssenarilərində bu cür təqdimatlar ümumi təhdid mənzərəsini sürətlə anlamağı çətinləşdirir və hadisələrə effektiv reaksiyanı gecikdirə bilər. Halbuki SOC mühitlərində, xüsusilə aktiv hücumlar zamanı, analitiklər yalnız hansı növ hücumun baş verdiyini deyil, həm də hücumun haradan başladığını, nə qədər intensiv olduğunu və koordinasiyalı olub-olmadığını dərhal qavramalıdırlar.

HoneyMap [12], Norse Map [13], Radware Live Threat Map və Kaspersky Cyber Threat Map kimi geniş istifadə olunan platformalar qlobal səviyyədə paylanmış sensor şəbəkələrinə əsaslanır və dünya miqyasında hücumları vizuallaşdırmaq üçün nəzərdə tutulub. Bu sistemlər qlobal təhlükə şüurunun artırılması baxımından effektiv olsa da, müəyyən bir təşkilata və ya serverə yönəlmiş hücumları əks etdirmədiyindən, korporativ mühitdə insidentlərə operativ reaksiya üçün məhdud əməliyyat dəyərinə malikdir.

SIEM və SOC infrastrukturlarında təhlükə aşkarlanması üçün istifadə olunan monitorinq alətləri zəngin təhlükəsizlik telemetriyası toplasa da, onların vizuallaşdırma imkanları kifayət qədər inkişaf etməmişdir. Məsələn, Wazuh platforması [14] alertlərin coğrafi mənşəyini göstərən əsas geo-xəritə paneli təqdim etsə də, bu məlumatlar hadisələrin effektiv korrelyasiyası, zaman üzrə hücum davranışının təhlili və real vaxt qərarvermə üçün lazımi interaktivlik və kontekstual dərinlikdən məhrumdur (Şəkil 2).



Şəkil 2. Wazuh – Geo-xəritə

Bu məhdudiyyətlər əvvəlki tədqiqatlarda da əks olunmuşdur. Coğrafi məlumatların və Coğrafi İnformasiya Sistemləri (Geographic Information Systems - GIS) texnologiyalarının kibertəhlükəsizlik monitorinqinə inteqrasiyası həm akademik, həm də praktik ədəbiyyatda kifayət qədər araşdırılmamışdır [15]. Eyni zamanda, növbəti nəsil SIEM platformaları üzrə sənaye təhlilləri qabaqcıl analitika və avtomatlaşdırmanı vurğulasa da, real vaxtda və təşkilata xas coğrafi hücum vizuallaşdırılması ilə bağlı məhdud yanaşmalar təqdim edir [16].

Əlavə olaraq, xarici vizuallaşdırma servislərindən istifadə bir sıra praktiki problemlər yaradır. Bunlara lisenziya və abunəlik xərcləri, bulud əsaslı platformalardan asılılıq, həssas təhlükəsizlik məlumatlarının üçüncü tərəflərə ötürülməsi riski və lokal SOC mühitlərinin fərdiləşdirilməsi üçün məhdud imkanlar daxildir. Bu məhdudiyyətlər xüsusilə açıq mənbə təhlükəsizlik həllərindən istifadə edən təşkilatlar və akademik mühitlər üçün əhəmiyyətli problem yaradır.

Problem olaraq, qlobal səviyyəyə yönəlmiş mövcud təhdid vizuallaşdırma alətləri ilə SIEM mühitlərində fəaliyyət göstərən SOC komandalarının praktik ehtiyacları arasında aydın boşluq mövcuddur. Təşkilata yönəlmiş real vaxt hücum trafikini vizuallaşdıran canlı və kontekstual hücum xəritəsinin olmaması hücum nümunələrinin gec aşkarlanmasına və təhlükəsizlik qərarlarının effektivliyinin azalmasına səbəb olur.

III. ƏLAQƏLİ İŞLƏR

Təhlükəsizlik Əməliyyatları Mərkəzi və kibertəhlükəsizlik tədqiqatları getdikcə təhdidlərin aşkarlanmasını və cavab

verilməsini dəstəkləyən vizual analitika və real vaxt rejimində vəziyyətin fərqindəliliyi üzrə ehtiyacı vurğulayır. Bu sahədə əvvəlki işlər şəbəkə trafikinin izlənməsi, xəbərdarlıqların əlaqələndirilməsi, təhlükəsizlik datalarının vizuallaşdırılması və müxtəlif aşkarlama sistemlərinin inteqrasiya olunması üçün alətləri əhatə edirdi, ancaq bir çox həll SOC inteqrasiyası və real vaxt rejimində hücüm xəritələşdirməsindən çox aşkarlanmanın dəqiqliyi və ya abstrakt vizuallaşdırmaya fokuslanmışdır [17].

Bir neçə kommersiya və akademik səylər kiber təhdidərin vizual təsvirini araşdırmışdır. Əsas satıcılar (məsələn, Kaspersky, Norse) tərəfindən təmin olunan real vaxt hücum xəritələri qlobal kiber aktivliyi animasiya olunmuş data axını ilə göstərir, hücum nümunələri və mənbələri barədə geniş məlumat verir, lakin quruma əsaslanan xüsusi IDS/SIEM datasından çox aqreqasiya olunmuş xarici telemetriyaya əsaslanır [18]. Bu alətlər təhdidlərin tezliyi və miqyası haqqında məlumatlılığı artırır, ancaq lokal SOC infrstrukturu ilə birbaşa inteqrasiya eləmir və ya xüsusi hədəflərə edilən hücumlarla bağlı ətraflı məlumat vermir.

Lakin, bu tədqiqatlar çox vaxt təsviri xarakter daşıyır ya da xüsusi şəbəkə mühiti üçün müəyyən olunmuş hücum xəritəsi yaratmaq üçün canlı IDS və SIEM axınlarını inteqrasiya edən sistemlərdən çox ümümi vizuallaşdırma texnikalarına fokuslanmışdır.

IDS və SIEM platformalarının inteqrasiyası SOC mühitində hadisə korrelasiyasını və aşkarlanma dəqiqliyini artırmaq üçün geniş şəkildə araşdırılmışdır. Bir neçə araşdırma mərkəzləşdirilmiş monitorinqi və təhdid aşkarlanmasını inkişaf etdirmək üçün Suricata kimi şəbəkə əsaslı alətlərin Wazuh kimi SIEM platformaları ilə birləşdirən hibrid arxitekturalar irəli sürür [19]. Bu yanaşmalar zərərli aktivliyin müəyyənləşdirilməsində çoxqatlı aşkarlama və qayda əsaslı korrelasiyanın effektivliyini göstərir.

Bu cür inteqrasiyalar xəbərdarlıqların yaradılması, korrelasiyası və məlumatlandırma mexanizmlərinin inkişafını yaxşılaşdırsa da, onlar avtomatlaşdırılmış cavab və aşkarlama performansına yönəlib. Vizualizasiya çox zaman panellərlə və ya xəbərdarlıq məzmunu ilə məhdudlaşır. Situasiya məlumatlılığı üçün geolokasiya əsaslı və real vaxt rejimində animasiya vizuallaşdırılmalarını idarə etmək üçün inteqrasiya olunmuş IDS və SIEM datasının istifadəsi bu tədqiqatların əsas diqqət mərkəzi deyil.

Ədəbiyyatda kiber vəziyyət haqqıda məlumatlılığı yaxşılaşdırmağa yönəlmiş vizualizasiya üsulları geniş müzakirə olunmuşdur. SOC vizualizasiya haqqında olan tədqiqatlar koqnitiv yükün azaldılmasının və analistlərin böyük həcmli təhlükəsizlik datalarını şərh etmək bacarığının vacibliyini göstərir [20].

Son tədqiqatlar vəziyyət haqqında məlumatlılıq üçün immersiv və qabaqcıl vizualizasiya yanaşmalarını araşdırır, vizuallaşdırma texnikalarını qavrayış, anlama və proyeksiya məlumatlılıq səviyyələrinə görə kateqoriyalara ayırır [19]. Bu işlər vizualizasiya dizayn prinsipləri barəsində dəyərli məlumatla təmin etsə də, onlar real vaxt rejimində canlı şəbəkə trafikindən yaranan IDS xəbərdarlıqlarının qəbulu və coğrafi məkan xəritələşdirilməsindən çox istifadəçi qarşılıqlı əlaqəsi və interfeys anlayışlarına fokuslanırlar.

IV. PROBLEMİN HƏLLİ

Bu problemi həll etmək üçün server əsaslı və təşkilatlar üçün spesifik canlı təhdid xəritəsi (threat map) yanaşması təklif edilir. İnternet miqyasında ümumiləşdirilən və müxtəlif mənbələrdən toplanaraq hazırlanan qlobal təhdid xəritələrindən fərqli olaraq, təklif olunan yanaşma müəyyən serveri, təşkilatı və ya əvvəlcədən müəyyən edilmiş coğrafi ərazini hədəf alan real vaxt hücum hadisələrini vizuallaşdırmağa yönəlib. Qlobal xəritələr adətən ümumi kibertəhdidləri göstərmək üçün istifadə olunur və konkret bir təşkilatın təhdid profilini əks etdirmir. Lakin təklif olunan yanaşma yerli infrastrukturda müşahidə olunan təhlükəsizlik hadisələrinə əsaslanaraq daha kontekstual məlumat təqdim edir.

Təklif olunan yanaşmanın əsas ideyası SIEM mühitində (məsələn, Wazuh, Splunk, ELK və s.) yaradılan təhlükəsizlik xəbərdarlıqlarını real vaxt coğrafi təhdid xəritəsinin vizuallaşdırılmasına çevirməkdir. Sistem qlobal miqyasda toplanmış statistik məlumatlara deyil, birbaşa təşkilatın öz SIEM mühitindən gələn hadisələrə əsaslanır. Bu siqnallardan əldə olunan IP ünvanları, hücum növləri, vaxt nişanları və digər metadata geolokasiya mexanizmləri vasitəsilə coğrafi koordinatlara çevrilir və interaktiv xəritədə dinamik şəkildə göstərilir. Nəticədə, hər bir hücum cəhdi və ya şübhəli fəaliyyət mənbə ölkə səviyyəsində vizual olaraq izlənilə bilər.

Bu yanaşma müəyyən bir infrastruktur üzrə real vaxt hücum fəaliyyətinin fasiləsiz monitorinqini təmin edir və hücum növlərinin paylanması, xəbərdarlığın mənbəyi olan ölkəyə görə statistik bölünmə və zaman ərzində intensivlik dəyişiklikləri kimi göstəriciləri aydın şəkildə müşahidə etməyə imkan verir. Bundan əlavə, sistem vizual analitika vasitəsilə müəyyən zaman aralığında hücumların artma tendensiyasını, müəyyən coğrafi zonalardan yaranan anomaliyaları və ya konkret xidmətlərə yönəlmiş hədəfli fəaliyyətləri aşkar edə bilər. Beləliklə, təhdid xəritəsi yalnız estetik vizual element deyil, həm də analitik qərar qəbuletməni dəstəkləyən funksional təhlükəsizlik alətinə çevrilir.

Təklif olunan təhdid xəritəsi həm yerli SOC idarə panelinin bir hissəsi, həm də idarə olunan ictimai veb-interfeys kimi təqdim edilə bilər. SOC mühitində istifadə olunan versiya daha ətraflı texniki məlumat (məsələn, hücum növü, qayda (rule) ID-si, risk səviyyəsi, hədəf portu və s.) ehtiva edə bilər. Digər tərəfdən, ictimai versiya həssas məlumatları anonimləşdirilmiş və ümumiləşdirilmiş formada təqdim etməklə təşkilatın kibertəhlükəsizlik şəffaflığını və məlumatlılığını artırmağa xidmət edə bilər.

Bu yanaşma kibertəhlükəsizlik əməliyyatlarında vəziyyətə dair məlumatlılığı əhəmiyyətli dərəcədə yüksəldir. Vizual və kontekstual məlumatların birləşməsi analitiklərə hücum davranışlarını daha sürətli və intuitiv şəkildə qiymətləndirməyə imkan verir. Real vaxt xəritəsində müşahidə olunan intensivlik və coğrafi qruplaşma dəyişiklikləri qeyri-adi trafik nümunələrinin erkən aşkarlanmasına kömək edir. Nəticədə analitiklər müdaxilə prioritetlərini daha dəqiq müəyyən edə,

hadisəyə reaksiya prosesini sürətləndirə və qərarları birbaşa canlı əməliyyat məlumatlarına əsaslanaraq qəbul edə bilərlər.

Ümumilikdə, server əsaslı və təşkilatlar üçün spesifik təhdid xəritəsi yanaşması, qlobal vizuallaşdırma həllərindən fərqli olaraq, müəyyən bir təhdid səthinə uyğunlaşdırılmış əməliyyat və qərar yönümlü model təqdim edir və müasir SOC mühitlərində proaktiv müdafiə strategiyalarının formalaşmasına töhfə verir.

V. SİSTEMƏ ÜMUMİ BAXIŞ

Təklif olunan yanaşma dörd əsas mərhələdən ibarətdir: xəbərdarlıq toplanması, məlumatların zənginləşdirilməsi, hadisələrin aqreqasiyası və təhdid xəritəsinin vizuallaşdırılması. Hər mərhələ xam təhlükəsizlik xəbərdarlıqlarının SOC mühitləri üçün uyğun mənalı və şərh edilə bilən vizual təsvirlərə çevrilməsini töhfə təmin edir.

Xəbərdarlıqların (alert-lərin) Toplanması: Bu mərhələdə monitorinq mühitində yaradılan təhlükəsizlik xəbərdarlıqları toplanır. Bu xəbərdarlıqlar infrastrukturda yerləşdirilən aşkarlama mexanizmlərindən ötürülür və adətən mənbə IP ünvanı, zaman nişanı, hücum kateqoriyası və qayda təsviri kimi əsas atributları əhatə edir. Bu mərhələdə xəbərdarlıq məlumatlarının ardıcıllığının və bütövlüyünün təmin edilməsi sonrakı mərhələlərdə dəqiqliyi qorumaq üçün vacibdir.

Məlumatların zənginləşdirilməsi: Toplandıqdan sonra xəbərdarlıqlar effektiv vizuallaşdırma və şərh üçün tələb olunan əlavə kontekstual məlumatlarla zənginləşdirilir. Bu mərhələdə IP ünvanları geolokasiya üsullarından istifadə edərək müvafiq coğrafi yerlərinə xəritələşdirilir. Hücum növləri, ciddilik səviyyələri və ya kateqoriyaları ilə əlaqəli əlavə metaməlumatlar aydın istifadəni təmin etmək üçün normallaşdırılır. Bu zənginləşdirmə prosesi xam məlumatlarda birbaşa mövcud olmayan məkan və kontekstual ölçülər təmin etməklə xəbərdarlıqların analitik dəyərini artırır.

Təhdid Xəritəsinin Vizuallaşdırılması: Son mərhələdə birləşdirilmiş hadisələr canlı təhdid xəritəsi şəklində təqdim olunur. Vizuallaşdırma təbəqəsi real vaxt hücum fəaliyyətini interaktiv və coğrafi məkan formatında göstərir və istifadəçilərə hücum mənşəyini, paylanma tendensiyalarını və dominant hücum kateqoriyalarını müşahidə etməyə imkan verir. Bu mərhələ strukturlaşdırılmış təhlükəsizlik məlumatlarını vəziyyətlə bağlı məlumatılığı dəstəkləyən və davam edən təhdid fəaliyyətinin sürətli anlaşılmasını asanlaşdıran intuitiv vizual təsvirə çevirir.

NƏTİCƏ

Bu məqalədə SOC mühitlərində vəziyyətlə bağlı məlumatlılığın artırılmasına olan ehtiyacı və ənənəvi loq əsaslı monitorinq ilə xarici mənbəli təhdid vizuallaşdırma platformalarının məhdudiyyətlərini araşdırıldı. Müəyyən edilmiş boşluqlara əsasən, açıq mənbəli ekosistem daxilində müdaxilə aşkarlama və mərkəzləşdirilmiş monitorinq məlumatlarını birləşdirən lokal, real vaxt rejimində kiberhücum vizuallaşdırma sistemi üçün həll təklif edildi. Tədqiqat, hücum fəaliyyətinin daha aydın şərhini dəstəkləmək və SOC mühitlərində analitik iş axınlarını təkmilləşdirmək üçün təhlükəsizlik xəbərdarlıqlarını coğrafi vizualizasiyaya çevirməyin potensial faydalarını vurğulayır. Təklif olunan yanaşma, toplanan üçüncü tərəf məlumatlarına deyil, yerli olaraq yaradılan aşkarlama məlumatlarına diqqət yetirməklə, aktuallığı, kontekstual dəqiqliyi və təşkilati tələblərə uyğunlaşmanı vurğulayır.

Ümumiyyətlə, bu tədqiqat, xüsusən də səmərəli və yerli nəzarətdə olan təhlükəsizlik həllərinin strateji əhəmiyyət kəsb etdiyi mühitlərdə SOC əməliyyatları üçün praktik və əlçatan vizuallaşdırma strategiyaları ilə bağlı müzakirələrə töhfə verir.

ƏDƏBİYYAT

[1] R. M. Alguliyev, Y. N. Imamverdiyev, and R. Sh. Mahmudov, "Information security as a component of national security," *Problems of* Information Society, no. 1, pp. 3–25, 2020.

[2] S. Jajodia, A. K. Ghosh, V. Swarup, C. Wang, and X. S. Wang, Cyber Situational Awareness: Issues and Research. New York, NY, USA: Springer, 2010.

[3] A. T. Erbacher, K. L. Walker, and D. A. Frincke, "Intrusion and misuse detection in large-scale systems," IEEE Computer Graphics and Applications, vol. 22, no. 1, pp. 38–48, Jan.–Feb. 2002.

[4] M. Baykara and R. Daş, "A survey on cyber attack detection and visualization tools," *Journal of Information Security and Applications*, vol. 39, pp. 1–15, 2018.

[5] Kaspersky, "Kaspersky Cyber Threat Map." [Online]. Available:

[6] https://cybermap.kaspersky.com/ [Accessed:Feb. 11, 2026].

[7] Radware, "Radware Live Threat Map." [Online]. Available: https://livethreatmap.radware.com/ [Accessed: Feb. 11, 2026].

[8] Check Point Software Technologies, "ThreatMap." [Online]. Available: https://threatmap.checkpoint.com/ [Accessed: Feb. 11, 2026].

[9] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," Sensors, vol. 21, no. 14, Art. no. 4759, Jul. 2021, doi: 10.3390/s21144759.

[10] SANS Institute, An Evaluator's Guide to NextGen SIEM, SANS Institute, 2020.

[11] Fortinet, "FortiGuard Threat Map." [Online]. Available: https://fortiguard.fortinet.com/threat-map [Accessed: Feb. 11, 2026].

[12] Cisco, "Cisco Talos Intelligence." [Online]. Available: https://talosintelligence.com/ [Accessed: Feb. 11, 2026].

[13] HoneyMap, "HoneyMap Live Attack Map." [Online]. Available: https://www.honeymap.io/ [Accessed: Feb. 11, 2026].

[14] Norse, "Norse Attack Map." [Online]. Available:

https://norsecorp.com/map/ [Accessed: Feb.11, 2026].

[15] Wazuh Inc., Wazuh Documentation." [Online]. Available:

https://documentation.wazuh.com/ [Accessed: Feb. 11, 2026].

[16] Proc. European Conference on Cyber Warfare and Security, Vol. 21, No. 1, 2022.

[17] M. Rosenberg, B. Schneider, C. Scherb, and P. M. Asprion, "An adaptable approach for successful SIEM adoption in companies."

[18] R. A. Marty, "A survey of visualization systems for network security," in Proc. 2011 IEEE Workshop on Visualization for Cyber Security (VizSec), 2011.

[19] A. Z. A. Adrian, R. A. Megantara and F. A. Zami, "Hybrid Multilayer Architecture Integrating Suricata, Wazuh, and Cyber Threat Intelligence for Drive-by-Download Malvertising Detection," IEEE Access, 2025

[20] K. Päivärinta, "Visualization of SIEM log data using the MITRE ATT&CK framework," Bachelor's thesis, Theseus, 2025.

[21] H. Ahmad, F. Ullah and R. Jafri, "A Survey on Immersive Cyber Situational Awareness Systems," Cybersecurity, vol. 5, no. 2, Art. no. 33, 2025.

Design of a Real-Time Attack Visualization System for Security Operations Centers

Rashad Aliyev[1], Sarfi Habibova[2], Ulviyya Mammadova[3]

[1,2]Khazar University, [3]YER xSP MMC, Baku, Azerbaijan

Abstract— Cyberattacks which target organizational infrastructures are increasing in both scale and complexity, creating a growing need for effective situational awareness mechanisms. While Security Information and Event Management (SIEM) systems enable centralized detection and analysis of security events, their visualization abilities are very limited to text and dashboard-based representations. Existing global cyber threat maps provide high-level insights but lack specificity for organizations. This paper proposes a real-time, SIEM-based threat visualization approach that transforms security alerts into a geographic cyber threat map. The proposed solution increases awareness in real time.

Keywords— cybersecurity; security operation center; cyber threats; cyber attacks.