UOT 33:005
DOI:10.30546/3006-0346.2024.2.80.1356

# KİBERTƏHLÜKƏSİZLİYİN GÜCLƏNDİRİLMƏSİ: TƏHLÜKƏNİN AŞKARLANMASINDA İNTERAKTİV VİZUALLAŞDIRMANIN GÜCÜ

**ALLAHŞÜKÜR ƏHMƏDZADƏ**
*Azərbaycan Dövlət Neft və Sənaye Universiteti, doktorant*

*E-mail: a.ahmadzada1998@gmail.com*

## Giriş

Kibertəhlükəsizlik kompüter sistemlərinin, şəbəkələrin, cihazların, məlumatların və istifadəçilərin icazəsiz girişdən, zədələnmədən və ya kiberhücumlar nəticəsində yaranan zərərdən qorunmasını nəzərdə tutan termindir. Kiberhücumlar müxtəlif məqsədlərə nail olmaq üçün informasiya texnologiyaları (İT) sistemləri və ya şəbəkələrindəki zəifliklərdən istifadə edən zərərli fəaliyyətlərdir, məsələn, həssas məlumatların oğurlanması, xidmətlərin pozulması, pul tələb edilməsi və ya nüfuzuna xələl gətirmək. Kibertəhlükəsizlik konsepsiyası üç əsas prinsipə əsaslanır: məxfilik, bütövlük və əlçatanlıq. Məxfilik o deməkdir ki, yalnız səlahiyyətli şəxslər onlara lazım olan məlumat və ya resurslara daxil ola bilər. Dürüstlük o deməkdir ki, məlumat və ya resurslar icazəsiz şəxslər tərəfindən dəyişdirilməyib və ya pozulmayıb. Mövcudluq o deməkdir ki, verilənlər və ya resurslar lazım olduqda əlçatan və funksionaldır.

Kibertəhlükəsizlik kiberhücumların qarşısını almaq, aşkar etmək və onlara cavab vermək məqsədi daşıyan texniki, təşkilati və insan amillərinin məcmusunu əhatə edir. Texniki amillərə İT sistemlərini və şəbəkələrini kibertəhlükələrdən qorumaq üçün aparat, proqram təminatı və şəbəkə alətləri və üsullarından istifadə daxildir. Təşkilati amillərə İT sistemlərinin və şəbəkələrinin necə idarə olunduğunu və təhlükəsizliyini tənzimləyən siyasətlər, prosedurlar və standartlar daxildir. İnsan faktorlarına İT sistemlərinin və şəbəkələrinin istifadəçilərinin və idarəçilərinin bacarıqları, bilikləri və davranışları daxildir.

## Əsas mövzu

İnteraktiv vizuallaşdırma kibertəhlükəsizliyi gücləndirmək üçün güclü texnikadır, çünki o, kibertəhlükələri daha effektiv şəkildə aşkar etməyə və qarşısını almağa kömək edə bilər. İnteraktiv vizuallaşdırma istifadəçilərə verilənlərlə qarşılıqlı əlaqədə olmaq və onu müxtəlif perspektivlərdən araşdırmaq imkanı verən qrafiklər, xəritələr və ya diaqramlar kimi verilənlərin qrafik təsvirlərinin istifadəsini nəzərdə tutur. İnteraktiv vizuallaşdırma kibertəhlükəsizlik üçün bir sıra üstünlüklər təmin edə bilər. İnteraktiv vizuallaşdırma kibertəhlükəsizlik üzrə analitiklərə və peşəkarlara şəbəkə fəaliyyətini və statusunu izləmək, anomaliyaları və nümunələri müəyyən etmək, kiber insidentlərin kontekstini və təsirini anlamağa kömək edə bilər. Məsələn, interaktiv qrafik vizualizasiyasından istifadə edərək, analitiklər şəbəkədə baş verən hadisələri bir baxışda görə bilər və zərərli trafikin mənbəyini və təyinat yerini izləyə bilərlər. Zaman qrafikinin vizuallaşdırılmasından istifadə edərək, analitiklər bulud mənzərələri üzrə xəbərdarlıqları başa düşə və zərərli hücumları aşkar edə bilərlər.

İnteraktiv vizuallaşdırma kibertəhlükəsizlik üzrə analitiklərə və peşəkarlara gördükləri məlumat əsasında məlumatlı və vaxtında qərarlar qəbul etməyə kömək edə bilər. Məsələn, interaktiv idarə panellərindən istifadə edərək, analitiklər real vaxt rejimində KPI-lərə, tarixi məlumatlara və fəaliyyətlərini istiqamətləndirə biləcək performans göstəricilərinə daxil ola bilərlər. İnteraktiv xəritələrdən istifadə edərək, analitiklər kiberhücumların coğrafi mənşəyini və yayılmasını müəyyən edə və müvafiq olaraq onların cavabını prioritetləşdirə bilərlər.

İnteraktiv vizuallaşdırmalar təhlükəsizlik analitiklərinə istifadəçi dostu və intuitiv şəkildə şəbəkə trafik qeydləri və ya sistem qeydləri kimi böyük verilənlər dəstlərini araşdırmaq imkanı verir. Bu, ənənəvi mətn əsaslı təhlil vasitəsilə ayırd etmək çətin ola biləcək nümunələri və meyilləri aşkar edə bilər. Vizuallaşdırmalar xam qeydləri təhlil edərkən dərhal aşkar olunmayan verilənlərdə nümunələri aşkar edə bilər. Məsələn, şəbəkə trafikini vizuallaşdırmaqla təhlükəsizlik analitikləri qeyri-müntəzəm zirvələri aşkar edə, meyilləri müəyyən edə və hücumun göstəricisi ola biləcək şübhəli nümunələri tanıya bilərlər. İnteraktiv vizuallaşdırmalar müəyyən hadisələrin əhəmiyyətini başa düşməyi asanlaşdıraraq, verilənlərə kontekst verə bilər. Məsələn, sistem qeydlərinin qrafik təsviri müxtəlif jurnal qeydləri arasındakı əlaqəni göstərə və analitiklərə hücumun gedişatını anlamağa kömək edə bilər. Məlumatlardakı anomaliyalar çox vaxt təhlükəsizlik təhdidinin ilkin göstəriciləri olur. İnte-

raktiv vizuallaşdırmalar real vaxt məlumatlarında kənar göstəriciləri və ya qeyri-qanunilikləri vurğulaya bilər ki, bu da analitiklərə potensial problemləri daha tez müəyyən etməyə və cavab verməyə başlamağa imkan verir. Vizuallaşdırma alətləri təhlükəsizlik qruplarına təhdidlərin zamanla necə inkişaf etdiyini anlamağa kömək edərək tarixi məlumat meyllərini göstərə bilər. Bu uzunmüddətli perspektiv proaktiv təhlükəsizlik tədbirlərinin hazırlanmasına kömək edə bilər. İnteraktiv vizuallaşdırmalar müxtəlif mənbələrdən məlumatları birləşdirə və vahid şəkildə göstərə bilər. Bu korrelyasiya analitiklərə zahirən əlaqəli olmayan hadisələr arasında əlaqələri tanımağa kömək edə və potensial olaraq əlaqələndirilmiş hücumları aşkar edə bilər. İstifadəçi davranışının vizuallaşdırılması tipik fəaliyyət nümunələrini izləyə və kənarlaşmaları vurğulaya bilər. Bu, oğurlanmış hesabları və ya daxili təhdidləri müəyyən etmək üçün dəyərlidir. Şəbəkə trafikinin coğrafi vizuallaşdırılması, xüsusən də paylanmış xidmətdən imtina (DDoS) hücumları və ya məkana əsaslanan təhdidlər halında hücumların mənşəyini təyin etməyə kömək edə bilər. Şəbəkə və ya sistem daxilində asılılıqların vizuallaşdırılması uğursuzluq və ya istismarın kritik nöqtələrini aşkar edə bilər. Məsələn, asılılıq xəritəsi müxtəlif serverlərin və ya xidmətlərin bir-biri ilə necə əlaqəli olduğunu göstərə bilər və analitiklərə potensial zəif əlaqələri müəyyən etməyə imkan verir. Vizual təqdimatlar texniki olmayan işçilərə təhlükəsizlik anlayışlarının izahını sadələşdirə bilər. Təlim materialları və maarifləndirmə proqramları işçiləri potensial təhlükələri tanımaq üçün öyrətmək üçün tez-tez vizualizasiyadan istifadə edir. Təhlükəsizlik qrupları müxtəlif hücum ssenarilərini simulyasiya etmək üçün interaktiv vizualizasiyalardan istifadə edə bilər ki, bu da onlara potensial təsirləri qiymətləndirməyə və cavab planlarını əvvəlcədən hazırlamağa imkan verir. Analitiklər öz xüsusi ehtiyaclarına uyğunlaşdırılmış fərdi tablolar yarada bilərlər. Bu, onlara öz öhdəliklərinə ən uyğun olan məlumatlara və vizuallaşdırmalara diqqət yetirməyə imkan verir.

İnteraktiv idarə panelləri şəbəkə və ya sistemin vəziyyəti haqqında real vaxt məlumatları göstərə bilər. Analitiklər qeyri-adi fəaliyyəti tez aşkar edə və dərhal cavab verə bilərlər. Bu vizualizasiyalara trafikin istilik xəritələri, müdaxilənin aşkarlanması sistemi xəbərdarlığı və sistem performans göstəriciləri daxil ola bilər. İnteraktiv idarə panelləri vasitəsilə real vaxt rejimində monitorinq kibertəhlükəsizlik təhdidinin aşkarlanmasının mühüm aspektidir. İnteraktiv idarə panelləri şəbəkə və ya sistemin vəziyyəti haqqında real vaxt yeniləmələrini təmin edir. Təhlükəsizlik analitikləri qeyri-adi və ya şübhəli fəaliyyətləri baş verən kimi tez aşkar edib onlara cavab verə bilər, bu da təhdidləri aşkar etmək və azaltmaq üçün lazım olan vaxtı azaldır. Trafik istilik xəritələri şəbəkənin müxtəlif hissələri arasında axan məlumatların həcmini göstərməklə şəbəkə trafikini vizuallaşdırır. Trafikdə qəfil sıçrayışlar və ya qeyri-adi nümunələr asanlıqla müəyyən edilə bilər ki, bu da paylanmış xidmətdən imtina (DDoS) hücumunu və ya digər anomaliyaları göstərə bilər. Intrusion Detection System (IDS) Alerts xəbərdarlıqları potensial təhlükələri aşkar etmək üçün vacibdir. İnteraktiv idarə panelləri bu xəbərdarlıqları real vaxt rejimində göstərə bilər ki, bu da analitiklərə şübhəli fəaliyyətləri araşdırmaq və onlara operativ reaksiya vermək imkanı verir. Onlar xəbərdarlıqları süzgəcdən keçirə və onların ciddiliyinə və uyğunluğuna əsasən prioritetləşdirə bilərlər. Sistemin performans göstəricilərinin real vaxt rejimində monitorinqi təhlükəsizlik insidentinin göstəricisi ola biləcək performansın azalması və ya resursdan həddən artıq istifadəni müəyyən etməyə kömək edə bilər. Bu ölçülərə CPU istifadəsi, yaddaş istifadəsi, şəbəkə bant genişliyi və disk fəaliyyəti daxil ola bilər. Real vaxt rejimində monitorinq istifadəçi fəaliyyətlərini, məsələn, giriş və giriş qeydlərini göstərə bilər. Qeyri-adi istifadəçi davranışı və ya icazəsiz giriş cəhdləri dərhal müəyyən edilə və istifadəçi hesablarının təhlükəsizliyini təmin etmək üçün dərhal tədbirlər görülə bilər. İnteraktiv idarə panelləri uğursuz giriş cəhdlərinin qəfil artması və ya həssas məlumatlara giriş kimi əvvəlcədən müəyyən edilmiş şərtlər yerinə yetirildikdə xəbərdarlıqlar və bildirişlər yarada bilər. Bu xəbərdarlıqlar analitiklərə real vaxt rejimində çatdırıla bilər və bu, sürətli cavabları təmin edir. İnteraktiv idarə panelləri real vaxt rejimində yenilənmək üçün nəzərdə tutulmuşdur, ona görə də təhlükəsizlik analitikləri həmişə ən aktual məlumatlarla işləyirlər. Bu, potensial zərəri minimuma endirməklə, hər hansı davam edən təhlükələrin dərhal müəyyən edilməsini təmin edir. Analitiklər konkret hadisələri daha dərindən başa düşmək üçün real vaxt məlumatlarını araşdıra bilərlər. Bu, onlara anomaliyaların kök səbəbini araşdırmaq və daha effektiv cavab vermək imkanı verir.

Vizuallaşdırma vasitələri təhlükəsizlik qruplarına şəbəkə əlaqələri, istifadəçi davranışı və digər məlu-

matları başa düşülən formatda göstərməklə potensial təhlükələri müəyyən etməyə kömək edə bilər. Şübhəli nümunələr araşdırma üçün vurğulana bilər. İnteraktiv vizuallaşdırma anomaliya aşkarlama modellərini yaratmaq üçün istifadə edilə bilər. Normal davranışdan sapmalar aşkar edildikdə, bu modellər xəbərdarlıqları işə sala və ya anomaliyaların vizual təsvirlərini yarada bilər, analitiklərə mənbəni və təsiri dəqiq müəyyənləşdirməyə kömək edir. İnsident zamanı vizuallaşdırmalar hadisələrin və görülən tədbirlərin qrafikini təqdim edərək analitiklərə hücumun əhatə dairəsini, onun gedişatını və cavab səylərinin effektivliyini anlamağa kömək edə bilər. Vizuallaşdırmalar şəbəkə üzrə istifadəçi davranışını izləməyə və təhlil etməyə kömək edə bilər. Bu, daxili təhdidləri və ya oğurlanmış hesabları müəyyən etmək üçün vacibdir. İnteraktiv vizuallaşdırmalar təhlükə kəşfiyyatını daha əlçatan və təsirli edə bilər. Təhlükəsizlik qrupları ortaya çıxan təhdidlər və zəifliklər haqqında məlumatları vizual cəlbedici formatda paylaşa bilər. Vizuallaşdırmalar fişinq hücumları və sosial mühəndislik taktikaları ilə bağlı nümunələri müəyyən etməyə, məsələn, e-poçt trafikinin vizuallaşdırılması şübhəli göndərici domenlərini və ya qeyri-adi e-poçt fəaliyyətini vurğulaya bilər. İnteraktiv vizualizasiyalar şəbəkədəki aktivlərlə məlum zəiflikləri xəritələşdirməklə sistemdəki zəiflikləri müəyyən etməyə kömək edə bilər. Bu, yamaq idarəetmə səylərini prioritetləşdirməyə kömək edir. Təhlükənin aşkarlanmasını artırmaq üçün maşın öyrənməsi alqoritmləri interaktiv vizualizasiyalara daxil edilə bilər. Məsələn, klasterləşdirmə alqoritmləri oxşar hadisələri birlikdə qruplaşdıra bilər ki, bu da nümunələri müəyyən etməyi asanlaşdırır.

Təhlükənin aşkarlanması üçün istifadə edilən bəzi interaktiv vizuallaşdırma üsulları bunlardır:

Piksel əsaslı vizuallaşdırma məlumatın əsas vahidi kimi piksellərdən istifadə edir və verilənlərin müxtəlif atributlarını və ya dəyərlərini təmsil etmək üçün müxtəlif rəng və ya formalar təyin edir. Piksel əsaslı vizuallaşdırma böyük həcmdə məlumatı yığcam və genişlənə bilən şəkildə göstərməyə və verilənlərdəki gizli nümunələri və klasterləri aşkar etməyə kömək edir. Piksel əsaslı vizuallaşdırma, xüsusən də böyük verilənlər bazası ilə işləyərkən məlumatların nümayişi və təhlili üçün dəyərli bir yanaşmadır. Bu texnika məlumat ötürmək üçün hər birinə xüsusi rəng, forma və ya digər atributlar təyin edilmiş fərdi piksellərdən istifadə edir. Piksel əsaslı vizuallaşdırma böyük verilənlər dəstlərinin kompakt formatda sıxılmasına imkan verir. Hər bir piksel məlumat nöqtəsini təmsil edir, beləliklə, tək bir şəkil böyük miqdarda məlumatı əhatə edə bilər, idarə etməyi və paylaşmağı asanlaşdırır. Bu üsul yüksək dərəcədə miqyaslana bilir, çünki piksellərin sayı müxtəlif ölçülü verilənlər toplusunu yerləşdirmək üçün tənzimlənə bilər. Böyük verilənlər dəstləri hələ də ardıcıl və mənalı şəkildə göstərilə bilər ki, bu da istifadəçilərə məlumatları effektiv şəkildə araşdırmaq imkanı verir. Piksellər üçün müxtəlif rənglərin, formaların və ya atributların istifadəsi istifadəçilərə verilənlər daxilində nümunələri və klasterləri aşkar etməyə imkan verir. Məlumatları bu şəkildə vizuallaşdırmaqla, kənar göstəricilər və meyillər tez müəyyən etmək olar. Piksel əsaslı vizuallaşdırmalar istifadəçilərə məlumatları daha intuitiv və interaktiv şəkildə araşdırmaq imkanı verir. Vizuallaşdırmanı böyütmək və kiçiltmək və ya sürüşdürmək daha incə təfərrüatları və kontekstləri aşkarlaya bilər, məlumatların araşdırılmasına kömək edir.

Qrafik təsviri hostlar, bağlantılar, protokollar və ya hücumlar kimi verilənlərdəki obyektləri və əlaqələri təmsil etmək üçün qovşaqlardan və kənarlardan istifadə edir. Qrafik təsvir şəbəkənin strukturunu və dinamikasını göstərməyə, zərərli trafikin mənbəyini və təyinatını izləməyə kömək edir. Qrafik təsvir, xüsusilə kibertəhlükəsizlik sahəsində mürəkkəb məlumatları təhlil etmək və vizuallaşdırmaq üçün güclü bir yoldur. Obyektləri və əlaqələri təmsil etmək üçün qovşaqlardan və kənarlardan istifadə etməklə, qrafik vizuallaşdırma şəbəkələrin strukturunu, dinamikasını və modellərini anlamağa kömək edə bilər və onu təhlükəsizlik təhdidlərinin müəyyən edilməsi və azaldılması üçün dəyərli alətə çevirir. Qrafik təsvirlər şəbəkə topologiyalarını göstərmək üçün əladır. Hər bir qovşaq cihazı və ya hostu, kənarlar isə aralarındakı əlaqələri və ya rabitə yollarını təmsil edə bilər. Bu vizuallaşdırma təhlükəsizlik analitiklərinə şəbəkənin strukturunu, o cümlədən onun iyerarxiyasını və qarşılıqlı əlaqəsini anlamağa kömək edir. Qrafiklər potensial hücum yollarını modelləşdirmək və təhlil etmək üçün istifadə edilə bilər. Qovşaqlar şəbəkə aktivlərini və ya zəifliklərini, kənarlar isə təcavüzkarın bu aktivləri pozmaq üçün keçə biləcəyi yolları təmsil edir. Bu, ən kritik zəiflikləri və təcavüzkarların istifadə edə biləcəyi potensial marşrutları müəyyən etməyə kömək edir. Qrafiklər zərərli proqramın şəbəkə daxilində necə yayıldığını təsvir edə bilər. Qovşaqlar yoluxmuş cihazları, kənarlar isə zərərli proqramın ötürülməsini təmsil edir. Bu, zərərli kodun axınını

izləməyə və infeksiya mənbələrini müəyyən etməyə kömək edir. Qrafiklər məlum təhdidlər, kompromis göstəriciləri (IoC) və təsirlənmiş sistemlər arasında əlaqələri göstərə bilər. Bu, təhdidlərin yayılmasını izləməyə və cavab tədbirlərini əlaqələndirməyə kömək edir. Qrafiklər istifadəçi davranış nümunələrini və şəbəkə daxilində istifadəçilər və qurumlar arasında münasibətləri təsvir edə bilər. Bu, qeyri-adi istifadəçi fəaliyyətlərini və potensial daxili təhdidləri müəyyən etmək üçün dəyərlidir. Kibertəhlükəsizlik kontekstində sosial şəbəkə təhlili kiberhücumlarda və ya zərərli fəaliyyətlərdə iştirak edən şəxslər və ya qurumlar arasında əlaqələr və əlaqələri müəyyən etmək üçün istifadə edilə bilər. Qrafiklərdən hadisəyə cavab planının gedişatını izləmək üçün istifadə edilə bilər. Düyünlər tapşırıqları, kənarlar isə asılılıqları və ya tərəqqini göstərir. Bu, bütün tələb olunan tədbirlərin tamamlanmasını və hadisənin effektiv şəkildə qarşısının alınmasını təmin edir.

Koordinasiya edilmiş çoxtərəfli görünüşlər xəritələr, vaxt qrafikləri, tablolar və ya cədvəllər kimi bir-biri ilə əlaqəli və sinxronlaşdırılan çoxsaylı vizuallaşdırma növlərini istifadə edir. Koordinasiya edilmiş çoxtərəfli görünüşlər məlumatlar üzrə çoxsaylı perspektivlər və təfərrüat səviyyələrini təmin etməyə və məlumatların interaktiv kəşfiyyatını və müqayisəsini dəstəkləməyə kömək edir. Əlaqəli və sinxronlaşdırılmış vizualizasiyalar kimi tanınan əlaqələndirilmiş çox görünüşlər məlumatların təhlili və kəşfiyyatına güclü yanaşmadır. Bu texnika xəritələr, vaxt qrafikləri, tablolar, cədvəllər və s. kimi çoxsaylı vizuallaşdırma növlərindən istifadə etməyi və bu vizuallaşdırmaların bir-biri ilə əlaqəli olmasını və ahəngdar şəkildə işləməsini təmin etməyi əhatə edir. Koordinasiya edilmiş çoxtərəfli görünüşlər daha dərin fikirlər əldə etmək, verilənləri müqayisə etmək və interaktiv məlumat kəşfiyyatını dəstəkləmək baxımından çoxsaylı faydalar təmin edir.

Koordinasiya edilmiş çoxlu görünüşlər istifadəçilərə məlumatları eyni vaxtda müxtəlif bucaqlardan araşdırmaq imkanı verir. Hər bir vizuallaşdırma növü fərqli perspektiv təmin edir və mürəkkəb məlumatları müxtəlif bucaqlardan nəzərdən keçirərək başa düşməyi asanlaşdırır. Məlumatların təqdim edilməsinin bir çox üsullarını təmin etməklə, əlaqələndirilmiş çoxtərəfli görünüşlər istifadəçilərə təqdim olunan məlumatı daha əhatəli başa düşməyə kömək edir. İstifadəçilər məlumatları daha bütöv şəkildə tədqiq edə, bir görünüşdən istifadə edərkən əldən çıxa biləcək nümunələri və ya əlaqələri potensial olaraq aşkar edə bilərlər. Müxtəlif təfərrüat səviyyələrində məlumatları göstərmək üçün müxtəlif vizuallaşdırmalardan istifadə edilə bilər. İstifadəçilər yüksək səviyyəli icmal və ya konkret məlumat nöqtələrinin daha ətraflı araşdırılmasından asılı olmayaraq, öz xüsusi ehtiyacları üçün ən uyğun vizuallaşdırmanı seçə bilərlər.

Koordinasiya edilmiş çoxlu görünüşlər mahiyyətcə interaktivdir. İstifadəçilər məlumatlar arasında gəzə, filtrlər tətbiq edə, xüsusi məlumat nöqtələrini böyüdə və daha çox məlumat əldə edə bilərlər. Bu dinamik kəşfiyyat daha dəqiq və təsirli anlayışlara səbəb ola bilər. Bu vizuallaşdırmalar verilənlərin müxtəlif aspektləri arasında birbaşa müqayisəyə imkan verir. Məsələn, koordinasiya edilmiş çox görünüşlü sistem istifadəçilərə qrafikadakı tendensiyaları xəritədəki coğrafi məlumatlarla müqayisə etməyə imkan verə bilər ki, bu da nümunənin tanınması və təhlilini asanlaşdırır. Zaman qrafikləri və hadisələrin ardıcıllığı müvəqqəti təhlili dəstəkləmək üçün digər vizuallaşdırmalarla sinxronlaşdırıla bilər və istifadəçilərə hadisələrin zamanla necə cərəyan etdiyini anlamağa kömək edir.

Məlumatların məkan paylanmasını və onun digər atributlarla əlaqəsini anlamaq üçün xəritələr və coğrafi vizuallaşdırmalar digər görünüşlərlə əlaqələndirilə bilər. Müxtəlif mənbələrdən və ya məlumat domenlərindən məlumatların birləşdirilmiş görünüşünü təklif edən hərtərəfli idarə panelləri yaratmaq üçün koordinasiya edilmiş çoxtərəfli görünüşlər tez-tez istifadə olunur. Bu tablolar monitorinq, qərar qəbuletmə və situasiya haqqında məlumatlılıq üçün xüsusilə faydalıdır. İstifadəçilər məlumatları bir görünüşdə seçə bilərlər və seçim avtomatik olaraq digər əlaqəli görünüşlərdə əks olunur. Məsələn, xəritədə bir bölgənin seçilməsi cədvəldəki məlumatları süzgəcdən keçirə və ya yalnız həmin regionda hadisələri göstərmək üçün qrafiki yeniləyə bilər. Koordinasiya edilmiş çoxlu görünüşlər bir baxış vasitəsilə aydın görünməyən korrelyasiya və münasibətləri aşkar etməyə imkan verir. Məsələn, səpələnmə qrafiki iki dəyişən arasındakı əlaqələri aşkar edə bilər, müvafiq istilik xəritəsi isə əlavə nümunələri vurğulaya bilər. Bu vizuallaşdırmalar müxtəlif mənbələrdən və formatlardan verilənlərin vahid, informativ ekrana inteqrasiyasını asanlaşdırır. Bu, məlumatların müxtəlif mənbələrdən əldə oluna biləcəyi kibertəhlükəsizlik kimi sahələrdə məlumatların birləşdirilməsi üçün xüsusilə dəyərlidir.

**Nəticə**

İnteraktiv vizuallaşdırma təhdid analitiklərinə zərərli fəaliyyəti göstərə biləcək nümunələri və anomaliyaları müəyyən etməkdə kömək etməklə kibertəhlükəsizliyi gücləndirə bilən güclü vasitədir. Mürəkkəb məlumat dəstlərini asan başa düşülən və qarşılıqlı əlaqədə olan şəkildə vizuallaşdırmaqla analitiklər başqa cür əldə etmək çətin və ya qeyri-mümkün olan fikirlər əldə edə bilərlər.

Analitiklər şübhəli nümunələr və ya anomaliyaların axtarışında böyük həcmli məlumatları araşdırmaq üçün interaktiv vizuallaşdırmalardan istifadə edə bilərlər. Məsələn, onlar fəaliyyətdə qeyri-adi sıçrayışları və ya məlum zərərli IP ünvanları ilə əlaqə modellərini müəyyən etmək üçün şəbəkə trafiki məlumatlarını vizuallaşdıra bilərlər. Təhlükəsizlik hadisəsi baş verdikdə, analitiklər zərərin dərəcəsini tez başa düşmək və əsas səbəbi müəyyən etmək üçün interaktiv vizuallaşdırmalardan istifadə edə bilərlər. Məsələn, onlar təhlükəyə məruz qalmış hesabları müəyyən etmək və ya şəbəkə vasitəsilə zərərli proqramların hərəkətini izləmək üçün istifadəçi giriş məlumatlarını vizuallaşdıra bilərlər. İnteraktiv vizuallaşdırmalar təşkilatın sistemlərində və şəbəkələrində təhlükəsizlik zəifliklərini müəyyən etmək və qiymətləndirmək üçün istifadə edilə bilər. Məsələn, analitiklər kritik təhlükəsizlik imkanları olmayan və ya köhnəlmiş proqram təminatı ilə işləyən sistemləri müəyyən etmək üçün aktivlərin inventar məlumatlarını vizuallaşdıra bilərlər.

İnteraktiv vizuallaşdırma sürətlə inkişaf edən bir sahədir və hər zaman yeni və innovativ alətlər hazırlanır. Bu alətlər daha əlçatan və sərfəli olduqca, çox güman ki, interaktiv vizuallaşdırma kibertəhlükəsizlikdə getdikcə daha mühüm rol oynayacaq.

Google-da təhlükəsizlik analitikləri şübhəli şəbəkə fəaliyyətini araşdırmaq üçün interaktiv vizualizasiyalardan istifadə edirlər. Onlar trafik axınlarında qeyri-adi nümunələri tez və asanlıqla müəyyən edə bilirlər ki, bu da onlara təhlükələri daha tez müəyyən etməyə və onlara cavab verməyə kömək edə bilər. ABŞ Müdafiə Nazirliyi təhdid tendensiyalarını izləmək və təhlil etmək üçün interaktiv vizualizasiyalardan istifadə edir. Bu, onlara yaranan təhlükələri müəyyən etməyə və əks tədbirləri inkişaf etdirməyə kömək edir. Maliyyə institutları fırıldaqçılığı aşkar etmək və qarşısını almaq üçün interaktiv vizuallaşdırmalardan istifadə edir. Onlar fırıldaq fəaliyyəti göstərə biləcək şübhəli nümunələri müəyyən etmək üçün əməliyyat məlumatlarını vizuallaşdıra bilərlər.

**ƏDƏBİYYAT SİYAHISI:**

*1. Kim D. (2018), "The Shellcoder's Handbook: Discovering and Exploiting Security Holes", Indianapolis, "Wiley Publishing", 561 p.*

*2. Parno B., Perrig A. "Challenges in Securing Vehicular Networks" // "Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV)", 2015, 18(10), 20-33 p.*

*3. Pfleeger C., Pfleeger S., Margulies J. (2014), "Security in Computing", Boston, "Pearson", 588 p.*

*4. Radack S., DeBar H. (2017), "Computer Security Basics", Sebastopol, "O'Reilly Media", 389 p.*

*5. Rogers M. (2019), "Network Security Fundamentals", Indianapolis, "Wiley Publishing", 409 p.*

*6. Schneier B. (2016), "Secrets and Lies: Digital Security in a Networked World", New York, "Wiley Publishing", 450 p.*

*7. Simson Garfinkel, S. (2020), "Web Security, Privacy & Commerce", Sebastopol, "O'Reilly Media", 570 p.*

*8. Stallings W. (2017), "Cryptography and Network Security: Principles and Practice", Boston, "Pearson", 517 p.*

**XÜLASƏ**

Təhlükələrin aşkarlanmasında interaktiv vizuallaşdırmanın gücü istifadəçilərə verilənlərlə qarşılıqlı əlaqədə olmağa və onu müxtəlif perspektivlərdən araşdırmağa imkan verən qrafiklər, xəritələr və ya diaqramlar kimi məlumatların təsvirlərindən istifadə etmək qabiliyyətidir. İnteraktiv vizuallaşdırma kibertəhlükəsizlik üzrə analitiklərə və peşəkarlara şəbəkə fəaliyyətini və vəziyyətini izləmək, anomaliyaları və nümunələri müəyyən etmək, kiber insidentlərin kontekstini və təsirini anlamağa kömək edə bilər. İnteraktiv vizuallaşdırma həmçinin istifadəçilərə kibertəhlükəsizlik anlayışları və təcrübələri haqqında daha çox məlumat əldə etməyə, həmçinin bu sahəyə maarifləndirmə və marağını artırmağa kömək edə bilər. Təhlükənin aşkarlanması üçün istifadə edilən interaktiv vizuallaşdırma üsullarından bəziləri piksel əsaslı vizuallaşdırma, qrafik təsviri və əlaqələndirilmiş çoxlu görünüşlərdir. Piksel əsaslı vizuallaşdırma məlumatın əsas vahidi kimi piksellərdən istifadə edir və verilənlərin müxtəlif atributlarını və ya dəyərlərini təmsil etmək üçün müxtəlif rənglər və ya formalar təyin edir. Qrafik təsviri hostlar, əlaqələr, protokollar və ya hücumlar kimi verilənlərdəki obyektləri və

əlaqələri təmsil etmək üçün qovşaqlardan və kənarlardan istifadə edir. Koordinasiya edilmiş çoxtərəfli görünüşlər xəritələr, vaxt qrafikləri, idarə panelləri və ya cədvəllər kimi bir-biri ilə əlaqəli və sinxronlaşdırılan çoxsaylı vizuallaşdırma növlərini istifadə edir.

**Açar sözlər:** *Kibertəhükəsizlik, interaktiv vizuallaşdırma, təhlükə, kiber hücüm.*

## ENHANCING CYBER SECURITY: THE POWER OF INTERACTIVE VISUALIZATION IN THREAT DETECTION

**Ahmadzade Allahshukur Nariman**
***Azerbaijan State Oil and Industry University, PhD student***

### SUMMARY

The power of interactive visualization in threat detection is the ability to use graphical representations of data, such as charts, graphs, maps, or diagrams, that allow users to interact with the data and explore it from different perspectives. Interactive visualization can help cybersecurity analysts and professionals to monitor the network activity and status, identify anomalies and patterns, and understand the context and impact of cyber incidents. Interactive visualization can also help users to learn more about cybersecurity concepts and practices, as well as to raise their awareness and interest in this field. Some of the interactive visualization techniques that are used for threat detection are pixel-based visualization, graph representation, and coordinated multi-views. Pixel-based visualization uses pixels as the basic unit of information, and assigns different colors or shapes to represent different attributes or values of the data. Graph representation uses nodes and edges to represent entities and relationships in the data, such as hosts, connections, protocols, or attacks. Coordinated multi-views uses multiple types of visualizations that are linked and synchronized with each other, such as maps, timelines, dashboards, or tables.

**Key words:** *Cyber security, interactive visualization, threat, cyber attack.*

## ПОВЫШЕНИЕ КИБЕРБЕЗОПАСНОСТИ: ВОЗМОЖНОСТИ ИНТЕРАКТИВНОЙ ВИЗУАЛИЗАЦИИ В ОБНАРУЖЕНИИ УГРОЗ

**Ахмадзаде Аллахшукюр Нариман,**
***Аспирант Азербайджанский Государственный Университет Нефти и Промышленности***

### РЕЗЮМЕ

Сила интерактивной визуализации при обнаружении угроз заключается в возможности использовать графические представления данных, такие как диаграммы, графики, карты или диаграммы, которые позволяют пользователям взаимодействовать с данными и исследовать их с разных точек зрения. Интерактивная визуализация может помочь аналитикам и специалистам по кибербезопасности отслеживать активность и состояние сети, выявлять аномалии и закономерности, а также понимать контекст и влияние киберинцидентов. Интерактивная визуализация также может помочь пользователям узнать больше о концепциях и методах кибербезопасности, а также повысить их осведомленность и интерес к этой области. Некоторые из методов интерактивной визуализации, которые используются для обнаружения угроз, — это пиксельная визуализация, графическое представление и скоординированные множественные представления. Пиксельная визуализация использует пиксели в качестве основной единицы информации и назначает разные цвета или формы для представления различных атрибутов или значений данных. Представление в виде графа использует узлы и ребра для представления сущностей и связей в данных, таких как узлы, соединения, протоколы или атаки. Скоординированные мультипредставления используют несколько типов визуализаций, которые связаны и синхронизированы друг с другом, например карты, временные шкалы, информационные панели или таблицы.

**Ключевые слова:** *Кибербезопасность, интерактивная визуализация, угроза, кибератака.*