AZƏRBAYCAN RESPUBLİKASI ELM VƏ TƏHSİL NAZİRLİYİ
AZƏRBAYCAN TEXNİKİ UNİVERSİTETİ

Əlyazması hüququnda

İBRAHİMLİ QOŞQAR RÖVŞƏN oğlu
ƏMƏNOV ELVİN MALİK oğlu
UMAROV SƏMƏD İSLAM oğlu

Şəbəkə trafikinin analizi sisteminin işlənməsi

mövzusunda
MAGİSTRLİK DİSSERTASİYASI

İxtisas: 060509 - " Kompüter elmləri"

İxtisaslaşma: "Dövlət informasiya sistemlərinin təhlükəsizliyi"

Elmi rəhbər: **tex.f.d, dosent Fərhad Yusifov**

Kibertəhlükəsizlik" kafedrasının
müdiri **t.e.d., dos. Yadigar İmamverdiyev**

BAKI - 2023

MÜNDƏRİCAT

GİRİŞ 5

I FƏSİL Şəbəkə trafikinin monitorinqi və analizi sahəsində beynəlxalq təcrübənin araşdırılması 7

1.1 Şəbəkə trafikinin monitorinqi sahəsində mövcud vəziyyət, problemlər və həllər 7

1.2 Şəbəkə trafikinin monitorinq və analizi vasitələrinin təsnifatı 11

1.3 Şəbəkə təhlükəsizliyinin analizi metodlarının müqayisəli təhlili 19

II FƏSİL Şəbəkə trafikinin təhlükəsizliyinin monitorinqi üçün konseptual modelin işlənməsi 25

2.1 Kiberhücumların aşkarlanması və qarşısının alınması sistemlərinin analizi 25

2.2 Şəbəkə trafikinin analizi sistemin arxitekturası və dizaynı 32

2.3 Şəbəkə trafikinin analizi üçün konseptual modelin işlənməsi 37

III FƏSİL Şəbəkə trafikinin analizi sisteminin işlənməsi 40

3.1. Şəbəkə trafikinin analizi sisteminin arxitekturası 40

3.2. Şəbəkə trafikində paketlər arasında vaxt intervalının təhlili.....48

3.3. Şəbəkə trafikinin analizi sisteminin yaradılması və eksperimentin keçirilməsi.....53

Nəticə 63

İstifadə olunmuş ədəbiyyatların siyahısı 64

XÜLASƏ 66

SUMMARY 67

РЕЗЮМЕ 68

İXTİSARLARIN SİYAHISI

KŞ – Kompüter Şəbəkəsi

SEM - Security Event Management

(Təhlükəsizlik insidentlərinin menecmenti)

SIM - Security Information Management **(Təhlükəsizlik informasiyalarının menecmenti)**

SIEM - Security Information Event Management **(İnformasiyaların və hadisələrin idarəedilməsinin təhlükəsizliyi)**

PCI DSS - Payment Card Industry Security Standard **(Ödəniş kartları sənayesinin təhlükəsizlik standartı)**

NPM – Network Packet Manager **(Şəbəkə paket meneceri)**

TCP - Transmission Control Protocol **(Transmissiya İdarəetmə Protokolu)**

IP – Internet Protokol **(İnternet protokolu)**

ACK - Base Transceiver Station **(Baza stansiyası)**

RTP – Real-time Transport Protocol **(Real vaxtda Nəqliyyat Protokolu)**

NIST - National Institute of Standards and Technology

(**Milli Standartlar və Texnologiya İnstitutu**)

RNC - Radio Network Controller **(3G şəbəkəsində baza stansiyalarının idarəedicisi)**

FDMA - Frequency Division Multiple Access **(Kanalların tezliyə görə bölünməsi)**

CERT - Computer Emergency Response Team (**Kompüterdə Təcili Yardım Qrupu)**

NCİRC - NATO Computer Incident Response Capability **(NATO-nun kompüter insidentlərinə cavab vermə qabiliyyəti)**

US-CERT - United States Computer Emergency Response Team **(Amerika Birləşmiş Ştatları Kompüter Təcili Cavablama Qrupu)**

NİSCC (UK-CERT) - United Kingdom Computer Emergency Response Team **(Birləşmiş Krallıq Kompüter Təcili Cavablama Qrupu)**

CERTBw - Computer Emergency Response Team **(Almaniya Kompüter Təcili Yardım Qrupu)**

CERT-Difesa - Italy Computer Emergency Response Team **(İtaliya Kompüter Təcili Yardım Qrupu)**

AusCERT - Australia Computer Emergency Response Team **(Avstraliya Kompüter Təcili Yardım Qrupu)**

NASA - National Aeronautics and Space Administration **(Milli Aeronavtika və Kosmos İdarəsi)**

GİRİŞ

Mövzunun aktuallığı. Dünyada telekommunikasiya informasiya texnologiyalarının sürətlə inkişafı kompüter şəbəkələrinin sürətlə böyüməsinə gətirib çıxarır. Rabitə və şəbəkə infrastrukturunun ölçüsü və mürəkkəbliyi artdıqca, şəbəkə mühitinə tam nəzarət və şəbəkə mühiti haqqında anlayışa malik olmaq təşkilatlar üçün həyati əhəmiyyət kəsb edir.

Telekommunikasiya texnologiyaları və şəbəkələrinin sürətlə inkişafı ilə yanaşı bu şəbəkələrin təhlküəsizliyinə olan təhdidlər də günü – gündən artır. İnkişafda olan sənaye tələblərini yerinə yetirmək üçün müasir təhlükəsizlik tədbirlərinin görülməsi vacibdir.Təəssüf ki, kibertəhlükəsizlik müdafiəsində əhəmiyyətli artımlara baxmayaraq, şəbəyəkiberhücumlar və məlumatların sızdırılması bütün dünyada hələ də böyük fəsadlarla özünü göstərir. ABŞ-ın "İdentity Theft Resource Center" şirkətinin məlumatına görə 2022-ci ildə məlumat sızıntısı ötən ilə nisbətən 14 faiz artmışdır.Ən son artım, 2020-ci ilə nisbətən məlumat sızıntısının 2021-ci ildəki 68 faiz artması ilə əlaqədardır ki, bu da 2017-ci ildə müəyyən edilmiş əvvəlki rekordu 23 faiz üstələmişdir.ABŞ-ın tanınmış kibertəhlükəsizlik həlləri şirkəti olan "Fortinet"-in məlumatına əsasən son ildə baş verən kiberhücumlar təkcə təşkilatlar deyil, dövlət strukturlarına da yönəlmişdir. 2022-ci ilin avqust ayında Rusiya haktivist qrupu tərəfindən 7.25 milyon bot istifadə edərək Ukrayna dövlətinin nüvə enrjisi şirkətinə DDoS (xidmətdən imtina) hücumu həyata keçirmişdir. Digər məlumata əsasən 2022-ci ilin avqust ayında Finlandiya parlamentinin veb saytı DdoS hücumuna məruz qalmışdır.

Dünya miqyasında telekommunikasiya və kompüter şəbəkələrinə yönəlmiş elə hücumlar şəbəkə və sistemlərin monitorinqinin və təhlükəsizliyinin artırılmasının vacibliyinin göstəricisidir.

Tədqiqatın məqsəd və vəzifələri. Tədqiqat işinin məqsədi kompüter şəbəkələrində trafikin analiz olunması üsullarının tədqiqidir. Bu məqsədə çatmaq üçün aşağıdakı əsas vəzifələrin icrası nəzərdə tutulmuşdur:

- Kompüter şəbəkələrinin quruluşu və təsnifatını öyrənmək;

- Şəbəkə avadanlıqlarının işləmə prinsipinin və onların təhlküəsizliyinin təmin edilməsi prosesinin tədqiqi;
- Şəbəkə təhlükəsizliyi sistemlərinin quruluşunun və təsnifatının öyrənilməsi;
- Şəbəkə axınının izlənilməsi və idarə edilməsi üsullarının tədqiqi;
- Şəbəkə trafikinin analizi sisteminin işlənməsi.

İşin elmi yeniliyi. Əsası python üzərində qurulan və bir-neçə proqramlaşdırma dilindən istifadə olunmaqla yaratdığım SIEM bizə həm lokal həm də qlobal tipli internet şəbəkəsinə malik olan strukturda internet şəbəkəsindən istifadənin limitlənməsi, qanunauyğunsuzluqların,kənardan (outbound) və ya daxildən (inbound) hücumların, tanınmayan və mənbəyi məlum olmayan internet paketlərinin təyini, bloklanmasını həyata keçirir. SIEM yaradılarkən dünyada və ölkəmizdə istifadə olunan modellərə diqqət yetirilmiş və aparılan tədqiqatlar və statistikalar barədə eyni zamanda ölkəmizdə olan internet şəbəkəsində tətbiqi imkanları barəsində çoxsaylı təhlillər aparılmışdır.

Tədqiqatın həqiqiliyi. Dissertasiya işi zamanı aparılan tədqiqatlar, həmçinin aparılmış testlər nəticəsində alınan nəticələr internet şəbəkəsində bilərəkdən buraxılmış səhvləri tapmağa nail olmuşdur, əldə olunan hesabatlar struktur quruluşu ilə üst-üstü düşür.

İşin təcrübi əhəmiyyəti. Aparılmış tədqiqatların, hesabatların alınmış nəticələrinin analizi göstərir ki, tədqiqatlar nəticəsində əldə edilmiş nəticələr və müvafiq analizlər, nəzəri cəhətdən əsaslandırmaq üçün elmi material kimi qiymətləndirilə bilər.

İşin strukturu və həcmi. Dissertasiya işi girişdən, 3 fəsildən, nəticədən, 27 sayda ədəbiyyat siyahısından ibarətdir. İşin əsas hissəsi 66 səhifə mətndən, 26 şəkildən və 4 cədvəldən ibarətdir. İşin ümumi həcmi 60 səhifədir.

I FƏSİL. ŞƏBƏKƏ TRAFİKİNİN MONİTORİNQİ VƏ ANALİZİ SAHƏSİNDƏ BEYNƏLXALQ TƏCRÜBƏNİN ARAŞDIRILMASI

1.1 Şəbəkə trafikinin monitorinqi sahəsində mövcud vəziyyət, problemlər və həllər

Bütün dünya ölkələrində fəaliyyət göstərən kompüter şəbəkələri hər hansı bir inkişaf səviyyəsindən asılı olmayaraq, bir tək kiberfəzada - İnternetdə birləşdirilir. Beynəlxalq kompüter şəbəkələri istifadəçilər üçün məhdud olmayan (şəffaf) olduğundan, cinayətkarlar, terrorçular, hakerlər və s. məqsədli şəxslər üçün kiberfəzada məlumat təhlükəsizliyi məsələsi Amerika Birləşmiş Ştatları və inkişaf etmiş Avropa ölkələri daxil olmaqla, beynəlxalq dünyada terrorizm ilə eyni problemlər səviyyəsində qiymətləndirilir. Bu mənada, yeni məlumat texnologiyalarının istifadə edildiyi bütün əsas infrastrukturların kibertəhlükəsizliyini qorumaq xüsusi önəm daşıyır. Bu ölkələrdə yeni məlumat texnologiyaları, o cümlədən kompüter şəbəkələri daxil olmaqla, dövlət (hərbi-siyasi) qurumlarının, özəl təşkilatların, maliyyə və bank sistemlərinin, təhsil, sağlamlıq, mədəniyyət, ticarət, istehsal prosesləri və s. sahələrdə geniş istifadə olunur.

Müasir şəbəkə trafikinin analizi sistemləri inkişaf etməsinə onların effektivliyinə və səmərəliliyinə təsir edən bir sıra qlobal problemlərlə üzləşir. Bu qlobal problemlər aşağıdakılardır:

- **Şəbəkə sürətlərinin artırılması**. Müasir şəbəkələrdə məlumat mübadiləsi sürəti artmağa davam etdikcə, şəbəkə trafikinin analizi sistemləri yüksək məlumat mübadiləsi sürəti ilə ayaqlaşmaq üçün mübarizə aparır. Şəbəkə trafikinin real vaxt rejimində işlənməsi və təhlili daha çətinləşir, yüksək ötürmə qabiliyyətini idarə etmək üçün xüsusi avadanlıq və optimallaşdırılmış alqoritmlər tələb olunur.
- **Şifrələnmiş trafik.** HTTPS kimi şifrələmə protokollarının geniş şəkildə tətbiqi şəbəkə trafikinin təhlili üçün əhəmiyyətli problem yaradır. Şifrələnmiş trafik paketlərin məzmununun yoxlanılması və təhlilinin qarşısını alır, potensial təhlükəsizlik təhdidlərinin müəyyən edilməsini və ya OSİ modelinin tətbiq səviyyəsində davranışa nəzarəti çətinləşdirir.
- **Şəbəkə mürəkkəbliyi.** Müasir şəbəkələr müxtəlif cihazlardan, protokollardan və

texnologiyalardan ibarət mürəkkəb və heterogen şəbəkələrdir. Bulud əsaslı xidmətlər, virtuallaşdırılmış mühitlər və ya əşyaların interneti (İoT- İnternet of Things) kimi müxtəlif mənbələrdən trafikin idarə edilməsi və təhlili bu mürəkkəbliyi effektiv şəkildə idarə edə biləcək qabaqcıl texnika və alətlər tələb edir.

- **Qabaqcıl təhdidlər və yayınma texnikaları.** Kiber təhlükələr şəbəkə trafikinin təhlili sistemlərindən yan keçmək üçün yayınma üsullarından istifadə edərək daha da təkmilləşir. Bədniyyətli şəxslər fəaliyyətlərini gizlətmək və aşkarlanmaqdan yayınmaq üçün şifrələmə, tunelləşdirmə və ya digər yayınma üsullarından istifadə edirlər. Şəbəkə təhlili sistemləri bu təhlükələrlə mübarizə aparmaq üçün davamlı olaraq uyğunlaşmalı və qabaqcıl aşkarlama mexanizmlərindən istifadə etməlidir.
- **Big Data problemləri.** Şəbəkə məlumatlarının eksponensial artımı emal edilməli, saxlanmalı və təhlil edilməli olan böyük miqdarda məlumat yaradır. Şəbəkə trafikinin analizi sistemləri böyük həcmli trafik məlumatlarından effektiv və istifadəyə yararlı məlumat çıxarmaq üçün məlumatların saxlanması, genişlənmə qabiliyyəti və məlumatların səmərəli işlənməsi üsulları kimi problemlərin həlli üsulunu təyin etməlidirlər.
- **Məxfilik və hüquqi məsələlər.** Şəbəkə trafikinin analizi potensial həssas məlumatların toplanması və təhlilini həyata keçirir ki, bu da öz növbəsində məxfilik və hüquqi narahatlıqların artmasına gətirib çıxarır. Təhlil apararkən məlumatların qorunması qaydalarına riayət olunmasının təmin edilməsi və istifadəçi məxfiliyinin qorunması şəbəkə trafikinin təhlili sistemləri üçün əhəmiyyətli problemlər yaradır.
- **Real vaxt rejimində analiz.** Təhlükəsizlik insidentinə reaksiya və ya şəbəkə performansının monitorinqi kimi bir çox şəbəkə analizindən istifadə halları hadisələri dərhal müəyyən etmək və onlara cavab vermək üçün real vaxt rejimli analiz tələb edir. Real vaxt rejimində analizə nail olmaq və vaxtında praktik və dəqiq nəticələr almaq məlumatların səmərəli işlənməsi və təhlili alqoritmləri tələb edir.

Bu problemlərin həlli şəbəkə trafikinin analizi sistemlərinin imkanlarını təkmilləşdirmək üçün davamlı tədqiqat və təkmilləşdirmə səylərini tələb edir. Bura maşın öyrənməsi və süni intellekt texnologiyalarında irəliləyişlər, şifrələmə texnologiyaları ilə

daha yaxşı inteqrasiya və genişmiqyaslı və səmərəli məlumat emalı sistemlərinin inkişafı daxildir. Bundan əlavə, tədqiqatçılar, sənaye mütəxəssisləri və siyasətçilər arasında əməkdaşlıq şəbəkə trafikinin analizi ilə bağlı məxfilik və hüquqi problemləri həll etmək üçün vacibdir.

Ümumi hallarda, ölkə sərhədləri içində məlumat təhlükəsizliyini təmin etmək üçün lazımi tədbirləri həyata keçirərək, kiberfəzada məlumat təhlükəsizliyini təmin etmək mümkün deyil. Beləliklə, məlumat təhlükəsizliyi məsələləri həll edilməmiş digər ölkələrin kompüter şəbəkələrinə, hətta ən sərt təhlükəsizlik tədbirləri olan digər ölkələrin kompüter şəbəkələrinə İnternet vasitəsilə daxil olmaq, hətta cinayətkar və terrorçu hərəkətləri daxil olmaqla bədniyyətli hərəkətləri həyata keçirmək mümkündür.

ABŞ, Böyük Britaniya, Almaniya, İtaliya, İsveç və s. kimi məlumat texnologiyalarının inkişaf etdiyi çoxsaylı ölkələrdə məlumat təhlükəsizliyi kompüter və telekommunikasiya şəbəkələrində yalnız bu şəbəkələri dəstəkləyən təşkilat və qurumların səviyyəsində deyil, dövlət səviyyəsində də aparılır. Bu ölkələrdə, məlumat təhlükəsizliyi milli strategiya kimi qəbul edilmişdir və bu strategiyaya uyğun olaraq kibertəhlükəsizlik tənzimləməsi işi həyata keçirilir. Böyük Britaniyada hüquq mühafizə orqanlarının fəaliyyətinin əlaqələndirilməsini, araşdırmalar və təhqiqatların aparılmasını, koordinasiya və məsləhətlər təmin etmək üçün Milli mərkəz yaradılmışdır. Struktur baxımından bu mərkəz dörd şöbədən ibarətdir:

– Təhqiqat şöbəsi - yüksək texnologiyadan istifadə edən təşkilatlı qruplar tərəfindən törədilən ağır cinayətləri araşdırır. Araşdırma bəzi hallarda digər hüquq mühafizə orqanları ilə birgə aparıla bilər.

– Axtarış şöbəsi - kibertəhlükəsizliklə əlaqəli cinayətkarları axtarır.

– Taktiki və Texniki yardım şöbəsi - yerli və beynəlxalq hüquq mühafizə orqanlarına, qurumlara və təşkilatlara, dövlət və biznes nümayəndələrinə məsləhət və yardım göstərir.

– Əşyavi-dəlillər (rəqəmli) şöbəsi - yüksək texnologiyalı sahədə törədilən cinayətlərin araşdırılmasında hüquqi yardım təmin edir.

Bundan başqa, bir çox ölkədə, məlumat təhlükəsizliyi strategiyasının həyata keçirilməsi, dövlət və hökumət orqanlarında, hərbi, maliyyə, bank, təhsil və digər müəssisələrdə məlumat sistemləri, kompüter və telekommunikasiya şəbəkələrinin, kiberfəzada təhlükəsizliyinin qorunması dövlət səviyyəsində təşkil olunur, koordinasiya mərkəzləri yaradılır, müvafiq qurumlar, onların qarşısının alınmasında işləyərək, koordinasiya edərək və vaxtında kömək təmin edərək fəaliyyət göstərir. İnkişaf etmiş ölkələrin təcrübəsinə əsasən, ölkə ərazisindəki məlumat təhlükəsizliyi təcili (kritik) vəziyyətlərinə reaksiya verən, adətən milli qanunvericilik tərəfindən təyin olunan məlumat təhlükəsizliyini təmin etmə ilə əlaqədar təsis edilmiş və fəaliyyət göstərən qurumlara daxil olan koordinasiya mərkəzləri - CERT (Computer Emergency Response Team) təşkilatları mövcuddur.

CERT mərkəzləri, ölkənin qanunvericilik tərəfindən verilmiş səlahiyyətlər çərçivəsində məlumat təhlükəsizliyi sahəsində əsasən aşağıdakı funksiyaları icra edir:

– ölkə ərazisində mövcud olan kompüter şəbəkələrinə ümumi texniki nəzarət edilməsi və onların monitorinqinin aparılması;

– kompüter şəbəkələrində "zəif yerlər"in və məxfi informasiyanın mümkün sızması hallarının, eləcə də şəbəkələrə kənardan icazəsiz daxilolma (müdaxilə) imkanlarının aşkar olunması məqsədilə müntəzəm araşdırmaların aparılması;

– baş verə biləcək hadisələrin proqnozlaşdırılması və onların vaxtında qarşısının alınması üzrə tövsiyələrin verilməsi;

– baş vermiş hadisələrin aradan qaldırılması, kompüter şəbəkələrinin təhlükəsiz fəaliyyətinin bərpası və müvafiq texniki yardımın göstərilməsi;

– kibertəhlükəsizliyin təmin edilməsi üzrə təşkilati və texniki qərarların qəbul edilməsi;

– informasiya təhlükəsizliyi sahəsində qanunvericilik bazasının yaradılması, bu məqsədlə əlaqədar dövlət və hökumət orqanları ilə birgə işin təşkili;

– digər ölkələrdə fəaliyyət göstərən CERT mərkəzləri ilə işgüzar əlaqələrin yaradılması və saxlanması;

– informasiya təhlükəsizliyi, o cümlədən kibernetik təhlükəsizlik sahəsində mütəxəssislərin hazırlanması, zəruri kadr və maddi-texniki potensialın inkişaf etdirilməsi.

Bir çox inkişaf etmiş ölkələrdə güc nazirliklərinin və ya digər dövlət orqanlarının tərkibində CERT mərkəzləri və ya analoji təşkilatlar artıq fəaliyyət göstərir:

– NCİRC (NATO-CERT) – NATO-nun Kompüter fövqəladə hallarına reaksiya vermə potensialının inkişafı üzrə koordinasiya mərkəzi;

– US-CERT – ABŞ-ın Daxili təhlükəsizlik idarəsinin Kompüter şəbəkələrinin milli təhlükəsizliyi şöbəsi nəzdində;

– NİSCC (UK CERT) – Böyük Britaniya Milli infrastrukturun koordinasiya mərkəzi;

– CERTBw – Kompüter fövqəladə hallarına reaksiya qrupu, Almaniya Bundeswehr;

– CERT-Difesa – Kompüter fövqəladə hallarına reaksiya qrupu, İtaliya Müdafiə Nazirliyi;

– AusCERT – Avstraliya Kompüter fövqəladə hallarına reaksiya qrupu;

Azərbaycan Respublikasının 2005-2008-ci illər üçün Kommunikasiya və İnformasiya Texnologiyalarının İnkişafı Dövlət Proqramı (“Elektron Azərbaycan”) çərçivəsində, Azərbaycan Respublikasının Prezidenti tərəfindən oktyabr 2005-ci ildə təsdiqlənmişdir, “İnformasiya təhlükəsizliyi üzrə Milli” yaratmaq planlaşdırılır.

1.2 Şəbəkə trafikinin monitorinq və analizi vasitələrinin təsnifatı

Şəbəkə monitorinqinin məqsədi və məsələləri

Şəbəkə monitorinq texnologiyaları vasitəsilə KŞ-də kompüterlərin (hostlar) və şəbəkə xidmətlərinin daimi fəaliyyətini və əlçatanlığını təmin edə bilərsiniz. Bu texnologiyalar, e-poçt və mobil telefonları da daxil olmaqla, şəbəkə administratorunu şəbəkədə mövcud olan problemlər, dayanıqlılıq problemləri və təhlükələrlə bağlı xəbərdar edə bilər.

Şəbəkə monitorinqinin vəzifəsi, kompüter şəbəkəsinin qorunması üçün tələb olunan məlumatların toplanmasıdır. Bu monitorun məqsədi, şəbəkə və şəbəkə idarəetmə tətbiq-

ləri üçün məlumatların toplanmasıdır. Kompüter şəbəkəsinin ən yaxşı konfiqurasiyası serverlər və istifadəçi kompüterlərə etibarlı proqramların quraşdırılmasıdır. Həmçinin onun vəziyyətinə avtomatik və davamlı nəzarət etmək vacibdir. Müasir kompüter şəbəkəsinin ölçüsündən dolayı, onu bir neçə hissəyə bölürlər və şəbəkə təchizatının əksəriyyəti bu müxtəlif sahələr (segmentlər) arasında yayılır. Tətbiqetmə idarəetmə alətləri əsasən doğrudan bağlı terminalları olmadığından, bu cihazların vəziyyətini izləmək üçün xüsusi şəbəkə nəzarəti texnologiyaları və alətləri hazırlanmışdır.

Şəbəkə monitorinqi kompüter şəbəkəsinin idarəetməsi üçün müxtəlif şəbəkə komponentlərindən vacib məlumatların toplanması və istifadə edilməsi üçün istifadə olunur. Bu məqsədlə əlaqədar olaraq aşağıdakı sahələr monitorinq olunur:

- şəbəkə məhsuldarlığının monitorinqi;
- şəbəkə səhvlərinin monitorinqi;
- şəbəkədən istifadənin monitorinqi.

Bu monitoriqlər funksional kompüter şəbəkəsində OSI (Open Systems Interconnect) tərəfindən təklif edilən standartlar olaraq qeyd edilir. Bu standartlar beş funksionalla bağlıdır. Şəbəkə monitorinqinin məqsədi ilə heç bir əlaqəsi olmayan iki əsas məsələ, şəbəkə konfiqurasiya idarəetməsi və təhlükəsizliyin idarə olunmasıdır.

Şəbəkə performansı monitorinqi vasitəsilə kompüter şəbəkəsinin performansı qiymətləndirilir. Əsasən, bu yolla monitorinqin üç məsələsi var. Birincisi, şəbəkə performansının izlənməsindən əldə edilən məlumatlar əsasən kompüter şəbəkəsinin genişlənməsi üçün hazırlıq məqsədi ilə istifadə edilir və şəbəkəni istifadə edərkən mövcud problemləri müəyyən edir. İkinci olaraq, şəbəkə performansı monitorinqinin müddəti şəbəkə performans modelinin təyin edilməsi üçün kifayət qədər uzun olmalıdır. Üçüncüsü, ən yaxşı nəticəni əldə etmək üçün uyğun qiymətləndirmə metodunu seçmək mühüm rol oynayır.

Kompüter şəbəkəsində, qiymətləndirilməsi vacib olan çoxlu sayda parametrlər vardır. Bununla birlikdə, bu şəbəkənin iqtisadi səmərəliliyi və vacibliyidə nəzərə alınmalıdır. Şəbəkə göstəriciləri, şəbəkənin xüsusiyyətlərini təyin edən bir neçə qiymət-

ləndirilmiş şəbəkə məlumatları toplusudur. (Cədvəl 1.1, şəbəkə göstəricilərinin bir neçə nümunəsi göstərilmişdir.)

Kompüter şəbəkəsində baş verən səhvləri aşkar etmək üçün şəbəkə səhvlərinin monitorinqini izləmək lazımdır. Əsasən şəbəkə səhvləri izləməsi fərqli şəbəkə səviyyələrində həyata keçirilir, çünki problem şəbəkənin müxtəlif səviyyələrində yarana bilər. Bu səbəbdən, problem hansı şəbəkə səviyyəsində yarandığını müəyyənləşdirmək vacibdir. İkincisi, şəbəkə səhvlərinin monitorinqi uzun müddətə qəbul edilmiş normal şəbəkə xarakteristikalarının olmasını tələb edir. Kompüter şəbəkəsində həmişə səhvlər var, lakin səhvlərin mövcudluğu həmişə problem olduğu anlamına gəlmir. Bu səhvlərin bir hissəsin olması həmişə gözlənilir. Məsələn, bir şəbəkənin kommunikasiya kanallarındakı gürültü məlumatların ötürülməsində səhvlərə səbəb ola bilər. Kompüter şəbəkəsində problem, səhvlərin sayı dramatik şəkildə artdığı və normal işləməsinin pozulduğu halda ortaya çıxır.

Cədvəl 1.1. Şəbəkə göstəricilərinin siyahısı

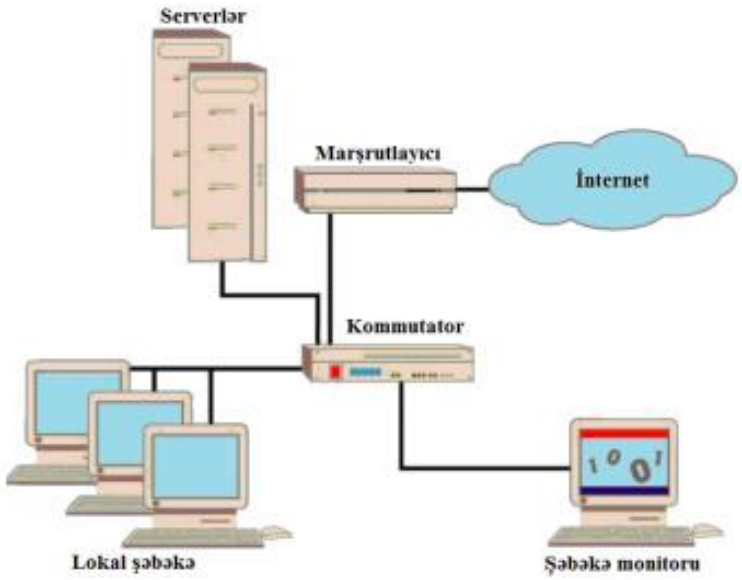
Şəbəkə göstəriciləri	Xarakteristikası
Əlaqə kanallarının uyğunluğu	Şəbəkə əlaqələrinin faktiki müddəti və şəbəkədəki istifadəçilərin mövcudluğu
Qovşaqların uyğunluğu	Səhv olmadan hostlardan istifadə edən istifadəçilərin faktiki müddəti
Təcridetmə əmsalı	Şəbəkəyə giriş əldə edə bilməyən istifadəçilərin sayı
Cavab müddəti	Siqnalın göndərilmə və cavabın qəbul edilmə müddəti

İstifadəçilərin şəbəkəni necə istifadə etdiyini müəyyən etmək üçün şəbəkə istifadəsi nəzarəti edilə bilər. Bu nəzarət istifadəçilərin bir kompüter şəbəkəsinin hansı şəbəkə vasitələrindən və necə istifadə etdiklərini qeyd edir. Bu məlumatlar istifadəçilərin şəbəkə istifadəsi profilini müəyyənləşdirmələrinə və gələcək fəaliyyətlərini proqnozlaşdırmağa imkan verir.

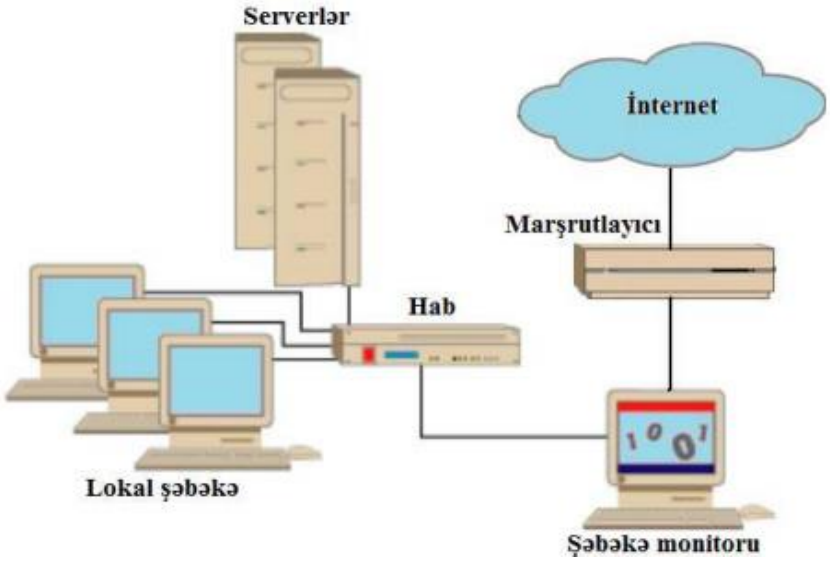
Konfiqurasiya idarəetməsinin məqsədi, kompüter şəbəkəsinin hər iki hissəsinin – aparat və proqram tənzimləməsinin qeydini saxlamaqdır. Bu, hər bir şəbəkə qurğusunda işləyən proqramın versiyasını və hər qurğunun proqram tənzimləməsini daxil edir.Şəbəkə resurslarının hesabatı, iki geniş sahəni əhatə edir: şəbəkə aktivlərinin idarəedilməsi və keyfiyyət idarəedilməsi. Şəbəkə aktivlərinin idarəedilməsi, şəbəkədə hansı kompüterlərin olduğunu, kimə məxsus olduğunu, kim istifadə edir və harada yerləşdiyini müəyyənləşdirir. Səhv idarəetməsinin məqsədi, kompüter şəbəkəsinin problemləri və səhvləri aşkar etməkdir. Belə səhvlər qeyd edilməlidir və uyğun həyacan siqnalı qaldırılmalıdır. Bu sahə, problemləri müəyyənləşdirmək, səhvlərin səbəbini müəyyənləşdirmək və uyğun addımın atılmasını təmin etməkdə vacibdir. Şəbəkə monitorinqi problemlərin həllinə kömək edən proqram və aparat vasitələri, əlaqə avadanlıqlarına yerləşdirilmiş monitorinq alətləri və şəbəkə idarəetmə sistemi agentləri ilə həll edilir. Monitorinq tapıntılarının qiymətləndirilməsi məsələsinin həllinə mütəxəssis sistemlərinin istifadəsi vacibdir, həmçinin bir çox şəbəkə mütəxəssislərinin praktiki təcrübəsini özündə cəmləşdirən mürəkkəb ekspert sistemlərindən istifadə etmək tələb olunur.

Kompüter şəbəkəsini nəzarət etmək üçün, serveri adətən kommutatorun nəzarət portuna qoşulur (Şəkil 1.1).

Əgər bir kompüter şəbəkəsi bir neçə kommutator istifadə edirsə, nəzarət serveri hər kommutatorun nəzarət portuna qoşulmalıdır. Bu halda, virtual kanal və ya real kabel vasitəsi ilə bağlantı qurulur.Əgər kommutatorların nəzarət portuna giriş yoxdursa, monitorinq serveri kompüter şəbəkəsinin internetə qoşulduğu nöqtədə quraşdırıla bilər. Bu halda, monitorinq serveri iki şəbəkə arasında ötürülən bütün trafiki izləyir (Şəkil 1.2).

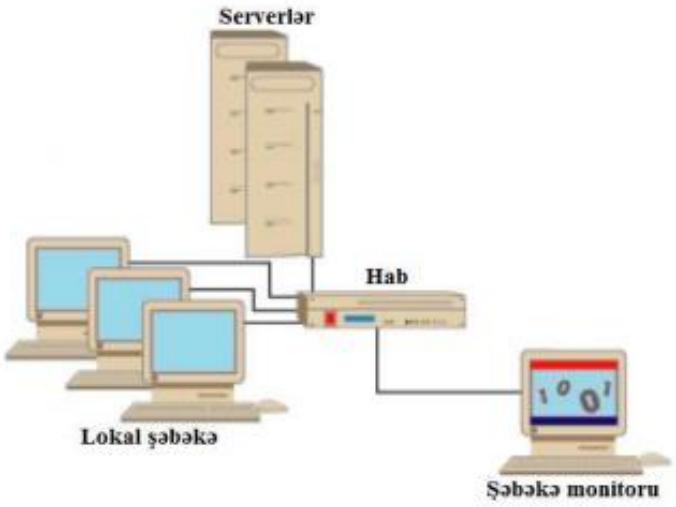


Şəkil 1.1. Serveri kommutatorun monitorinq portuna qoşulma sxemi



Şəkil 1.2. Monitorinq serverinin kompüter şəbəkəsi ilə İnternet arasında yerləşdirilməsi sxemi

Bu halda, xüsusi monitorinq serverlə bağlı problemlər şəbəkədə dayanmalara səbəb ola bilər. Həmçinin, xüsusi monitorinq serverinin imkanları tələb olunan şəbəkə ötürmə genişliyindən qısa gələrsə, "butulka boğazı" problemləri yarana bilər. Bu məsələni həll etmək üçün ən yaxşı yol, sadə bir habdan istifadə edərək xüsusi monitorinq serveri daxili şəbəkəyə qoşmaqdır (Şəkil 1.3).



Şəkil 1.3. Monitorinq serverinin haba qoşulması sxemi

Bu halda, habın sıradan çıxmasından dolayı şəbəkə təhlükə altındadır. Ancaq, mərkəzlər ruterlərdən daha etibarlıdır və onların sıradan çıxması halında funksional olanları ilə dəyişmək daha asandır.

Şəbəkə monitorinqi üsullar

Kompüter şəbəkələrini nəzarət etdikdə monitorinq məlumatlarının toplanması əsasən iki üsulla həyata keçirilir - aktiv və passiv monitorinq üsulları və onların müqayisəsi Cədvəl 1.2-də göstərilmişdir.

Aktiv şəbəkə monitorinqi - şəbəkəyə əlavə test paketlərinin yerləşdirilməsi nəticəsində toplanan məlumatların analizində əsaslanır. Bunlar əsasən ping (şəbəkələrlə əlaqəni yoxlamaq üçün kompüter proqramı), traceroute (şəbəkələrdəki məlumatları izləyən yolun təyin edilməsi üçün kompüter vasitəsi), pathchar (şəbəkə çökməsi ehtimalı, gecikmələr və s. təyin etmək üçün kompüter proqramı), ICMP (Internet Control Message Protocol - Şəbəkələrarası Məlumat İdarəetmə Protokolu) əsaslanır.

Passiv şəbəkə monitorinqi aktiv şəbəkə trafikindən toplanmış məlumatların (loq-faylların) analizində əsaslanır. Bu əsasən polling (cihazların hazırlıq səviyyəsini sorğulama), event reporting (hadisələrin hesabatı), sniffing (şəbəkə trafikinə passiv eşidilmə), SNMP (Simple Network Management Protocol - Sadə Şəbəkə İdarəetmə Protokolu), RMON (Remote Network Monitoring - Kompyuter Şəbəkələrinin

Monitorinq Protokolu), NetFlow (Şəbəkə trafikinin qeydiyyatı üçün nəzərdə tutulan şəbəkə protokolu) vasitəsilə həyata keçirilir [2].

Cədvəl 1.2. Şəbəkə nəzarət metodlarının müqayisəsi

	Aktiv monitorinq	Passiv monitorinq
Forması	Çoxnöqtəli	Bir və ya çoxnöqtəli
Verilənlərin həcmi	Çoxnöqtəli	Böyükdür
Yerinə yetirilməsi	Əlavə trafik	Proqram, proqram-aparat təminatı
Məqsədi	Ləngimə, paketlərin itməsi, iş qabiliyyəti	Səmərəlilik, trafikin parametrləri, meyllər və aşkarlama
CPU tələblər	Orta aşağı	Yüksək

Şəbəkə monitorinqi zamanı trafikin toplanması və analiz edilməsi prosesi aşağıdakı addımlardan ibarətdir:

- Şəbəkə paketləri nəzarət nöqtəsində əldə edilir (adətən, serverdə, marşrutlayıcıda və yaxud şəbəkənin istənilən nöqtəsində yerləşən kompyuter vasitəsi ilə əldə edilir);
- Paketlərin seçilməsi və filtrə edilməsi, protokollar, şəbəkə xidmətləri, portlar və s. kimi elementlərdən istifadə edilərək həyata keçirilir;
- Paketlər klassifikasiya edilir və axın yazıları kimi təsvir edilir;
- Seçilmiş və süzülmüş axınlar istifadə edilir. Seçim mərhələsi ya təkrarlanır, ya da hər ikisi birdəfədən çox tətbiq edilə bilər;
- Axın yazıları tətbiqi proqramlarda emal edilir (hücumların analizi, DoS-un monitorinqi, vizuallaşdırma (FlowScan), toplama (TCPdump), əks etdirmə və s.).

Şəbəkə monitorinqi vasitələri

Bugün bir çox fərqli şəbəkə monitorinq alətləri mövcuddur ki, şəbəkə administratorlarına geniş bir seçim imkanı təqdim edir. Lakin, monitorinq alətlərinin çeşidliliyi seçim prosesini çox çətinləşdirir. Şəbəkə administratorlarının KŞ-də effektiv şəbəkə monitorinq və analiz alətlərinə ehtiyacı duyurlar. Hazırda, şəbəkə monitorinq alətləri

SNMP protokolu, WMI (Windows Management Instrumentation), sniffer və Netflow şəbəkə monitorinqi və analiz metodlarını istifadə edir.Kompüter şəbəkəsini düzgün və effektiv şəkildə monitorinq etmək üçün, əvvəlcə monitorinq alətini seçmək lazımdır. Mövcud olan monitorinq alətləri funksiyalarına əsasən müxtəlif siniflərə bölünə bilər:

- Yoxlama aparan monitorinq alətləri kompüter şəbəkəsinin problemlərini aşmaq və təmir etmək üçün hazırlanmışdır. Bu vasitələr interaktivdir və qısa müddətdə işləyir (məsələn, ping proqramı göstərilə bilər). Ping, əlaqəni yoxlamaq üçün seçilmiş hostlara test trafiki göndəri;
- Protokol analizatorları şəbəkədəki hər paketi yoxlayır və bütün əlaqələr haqqında məlumat toplayır (məsələn, mənbə və təyinat IP ünvanlarını, protokol məlumatlarını və hətta tətbiq səviyyəsi məlumatlarını toplayır);
- Meylləri aşkarlayan monitorinq alətləri - uzun bir müddət arxa fon üzərində monitorinq aparır və nəticəni, əsasən qrafik formada göstərir. Reallaşdırılmış monitorinq alətləri meylləri aşkarlayan monitorinq alətləri ilə eyni şəkildə monitorinq aparır və problem aşkar edildikdə təzə vəziyyətdə şəbəkə administratorunu məlumatlandırır;
- Log fayllarının təhlil edilməsi ilə məşğul olan log analizatorları müxtəlif tətbiqlərin log-fayllarını təhlil edir və problemlər aşkar edildikdə şəbəkə administratoruna bildiriş göndərir;
- Müdaxilələrin aşkarlanması vasitələri - qeyri-müəyyən hadisələr və ya hücum təşəbbüsləri aşkar edildikdə uyğun tədbirlər görür (əsasən giriş qadağası və ya administratora bildirişi göndərilir və s.);
- Etalon testləşdirmə vasitələri - şəbəkə xidmətlərinin və ya şəbəkə bağlantılarının performansını ölçməyə imkan verir;
- Kabel sistemlərinin diaqnostikası və sertifikasyası üçün avadanlıqlar.

Cədvəl 1.3, məlumat toplama və analiz metodlarına, analiz sahəsinə (ISO/OSI modeli), arxitekturuna və istifadəçi interfeysinə əsaslanan bəzi şəbəkə monitorinq alətlərini müqayisə edir.

Cədvəl 1.3. Şəbəkə monitorinqi vasitələrinin müqayisəsi

Vasitələr	**Verilənlərin əldə edilməsi üsulu**	**Verilənlərin analizi üsulu**	**Analiz sahəsi (ISO/OSI modeli)**	**Paylanmış arxitektura**	**İstifadəçi iterfeysi**
Tcpdump	Libpcap	real zamanda	7-ci səviyyə	yox	Text
Ntop	Libpcap	seriya	7-ci səviyyə	yox	Web
Ethereal	Libpcap	real zamanda, seriya	7-ci səviyyə	yox	X-Windows
MRTG	snmp agent	seriya	2-ci səviyyə	hə	Web
WebTraf Mon	libpcap	real zamanda, seriya	7-ci səviyyə	yox	Web

1.3 Şəbəkə təhlükəsizliyinin analizi metodlarının müqayisəli təhlili

Şəbəkə təhlükəsizliyinin monitorinqinin əsas funksiyaları

Şəbəkə təhlükəsizliyi monitorinqi, müasir tələbləri ödəyən və şəbəkə haqqında məlumatların toplanması, analizi və nəticələri haqqında məlumatları əlaqədar şəxslərə və ya sistemlərə yönləndirən proqram və avadanlıq sistemlərindən ibarət mürəkkəb bir sistemdir. Monitorinq sistemi bir çox funksiyaları yerinə yetirir ki, bu da şəbəkənin effektivliyinin artırılmasına kömək edir.

Şəbəkə təhlükəsizliyi monitorinqinin əsas vəzifələri aşağıdakı kimi izah edilə bilər:

İnternet trafikinin izlənilməsi və qeydə alınması. Bu proses trafikin izlənilməsi ilə başlayır, cari sessiyaların qeydə alınması, istifadə olunan trafikin miqdarının ölçülüb hesablanması, İnternet trafikinin istifadəsinin nəzarət edilməsi, paketlərin tarixə görə qeydə alınması.

İnternetə qoşulmuş sistemlərin təhlükəsizliyini real vaxtda nəzarət. Sistemlərin təhdid edə biləcəyi dərəcə onların imkanlarına bağlıdır. Bu sistemləri təhlükə dərəcəsinə görə siniflərə bölmək və nəzarət səviyyəsinin xüsusiyyətlərini rahat bir formada düzəltmək lazımdır.

İnternet istifadəçilərinin təhlükəsizliyi, məxfiliyi və qorunması. İnformasiya təhlükəsizliyini təhdid edə biləcək bəzi pis niyyətli fəaliyyət növləri: xidmətlərə hücumlar, artırılmış imtiyazlara sahib olmaq üçün hücumlar, məxfi informasiyanın qəbulu və təhlükəli proqramların yüklənməsi, həm şəbəkənin, həm də onun istifadəçilərinin təhlükəsizliyi və məxfiliyi nəzərdən çox təhlükəlidir.

Sistem çürüklüklərinin müəyyənləşdirilməsi. Sistemlərində məlumat təhlükəsizliyi çürüklər ola bilər. Bunlar verilənlər bazalarında, konfiqurasiyada, idarəçilikdə və yazılım mənbə kodunda ola bilər. Bu çatışmazlıqlar şəbəkənin məlumat təhlükəsizlik vəziyyətini təsir edir.

Əməliyyatların davamlılığı. Əsas məqsəd İnternet trafikinin keyfiyyətini pisləşdirən amilləri aradan qaldırmaq və onun yalnız zəruri məqsədlər üçün istifadə olunmasını təmin etməkdir.

Riskin qiymətləndirilməsi. Şəbəkə təhlükəsizliyi idarəetmənin əsasını riskin qiymətləndirilməsi və idarəetmə prosesi təşkil edir. Analizin doğruluğu və ətraflılığı, risk faktorlarının qiymətləndirilməsi və qərar verilmə mekanizminin tətbiqi, hər hansı bir təşkilatda bu prosedurun effektivliyinin necə təyin edildiyini müəyyənləşdirmək üçün önəmli rol oynayır.

Şəbəkə təhlükəsizliyinin monitorinqinin problemləri

Əksər hallarda, böyük və orta ölçülü işlər ümumiyyətlə mürəkkəb infrastruktur və çeşitli təşkilat strukturlarına malik olurlar, bu isə onları çox sayda platforma ehtiyac duyurmağa məcbur edir. Təhlükəsizlik texnologiyalarının təhlili nəticəsində görünür ki, müxtəlif şəbəkələrin məlumat təhlükəsizliyi bütöv, tam birləşdirilmiş bir həll ilə təmin edilə bilməz. Şəbəkə təhlükəsizliyi monitorinq sistemləri ilə bağlı problemləri aşağıdakı kateqoriyalara qruplaşdırmaq ən məqsədəuyğun olanıdır:

1. *Effektivlik*. Əksər hallarda, hücum aşkar etmə sistemləri bütün məlum təhlükələri axtarmağa çalışırlar, bu isə çox sayda yanlış məlumat verməyə səbəb olur.

2. *Performans.* Həqiqi istifadə şərtlərində şəbəkə təhlükəsizliyi monitorinqinin effektivliyini qiymətləndirmək çətindir. Əlavə olaraq, şəbəkə təhlükəsizliyi monitorinqini qiymətləndirmək üçün ümumi təlimatlar yoxdur.

3. *Vizualizasiya.* Çeşidlilik və məlumatın miqdarının çox olması səbəbindən, məlumat analizi effektiv vizualizasiya texnikalarının yaradılmasını tələb edən çətin bir əməliyyatdır.

4. *Modernizasiya*. Köhnə şəbəkə təhlükəsizliyi monitorinq texnologiyalarının yenilənənlərlə əvəzlənməsi çətin bir işdir. Bütün sistem yeni altsistemlərlə əlaqə qurmaq məcburiyyətindədir və zaman-zaman ümumi uyğunluğu təmin etmək mümkün olmaz.

5. *Hərəkətlilik.* Hazırda mövcud olan şəbəkə təhlükəsizlik monitorinqlərinin çoxu müəyyən avadanlıqlar ilə istifadə üçün hazırlanır və onları eyni təhlükəsizlik tədbirlərini tələb edən digər sistemlərə uyğunlaşdırmaq çətin olur.

Şəbəkə trafikinin klassifikasiyası metodları

İnternetin geniş yayılması, protokollərin və tətbiqlərin artması nəticəsində trafik kateqoriyalanması sahəsindəki araşdırmalar da önəmli bir hal almışdır. TCP/IP axınınn xüsusiyyətlərinin başa düşülməsi internet trafikinin izlənməsi, təhlükəsizlik pozuntularının aşkar edilməsi və daha bir çox tapşırıq üçün əsas məsələdir.

İyerarxiyalı və mürəkkəb trafik identifikasiyası üçün trafik kateqoriyalanması texnikalarının təsnifatı tədqiq edilməkdədir [3]. Xidmət, tətbiq, protokol və funksiya olmaq üzrə dörd kateqoriyalanma kriteriyası, mürəkkəb identifikasiyanı asanlaşdırmaq üçün tövsiyə olunur. Tövsiyə olunan təsnifat taksonomiyası, artan və ya azalan iyerarxiyalı strukturların nəticələrini də nəzərə alır.

Trafik kateqoriyalanması son zamanlarda "Machine learning" texnikalarının geniş istifadəsini görmüşdür. Ən yaxın qonşular metodu əsasında klassifikasiya cox yaxşı nəticə nümayiş etdirir. Ancaq təlim məlumatlarının azlığı hallarında nəticənin doğruluğu çətinlik çəkə bilər. Bu kimi halların qarşısını almaq üçün, kateqoriyalanma mərhələsi boyunca məlumatların əlaqələndirilməsi vacibdir [4].

Verilənlər bazasına və brauzerə olan yaxın əlaqələri səbəbindən, veb sistemlər xüsusilə hücumlara qarşı çox həssas olurlar. Onlayn sistemləri təsir edən bu təhlükəsizlik riskləri kateqoriyalanır və xüsusiyyətləri məlum edilir [5]. Analiz üçün əvvəlcədən nə olduğu, hansı növ olduğu və hansı vaxt baş verdiyi müəyyən edilir. Sonra, "Machine learning" texnikalarından istifadə edərək təhlükəsizlik hadisələri kateqoriyalanır və iki qrupa ayrılır: hücumlar və boşluqların skanlanması.

İnternet trafik kateqoriyalanmasının doğruluğunu artırmağa yönlənən çeşitli metodlar mövcuddur, ancaq bunlar alt səviyyədə kateqoriyalanma üçün çox doğru hesablanmır. Çeşitli intellektual analitik texnikaları istifadə edərək onlayn internet trafik kateqoriyalanması təklif olunmuşdur. Bu texnikaların əsas məqsədi yanlış məlumatları müəyyən etmək və beləliklə yanlış müsbət qiymətləndirilmə prosesindən imtina etməkdir. Verilənlər düzgün şəkildə İnternet trafik axınınan toplanır və bu yolla ətraf mühitin bütünlüyünü qiymətləndirmək və işləmə vaxtını qısaltmaq mümkündür. Əgər şəbəkə mühiti nəza-rət altında olarsa, HTTP trafik kateqoriyalanması "paralel neyron şəbəkəsi kateqoriyası strukturu"na əsaslanacaq. Bu strategiyanın effektivliyi, bu trafik kateqoriyalanması zamanı əldə olunan məlumatlara əsaslanaraq 85-91% arasında ölçülür.

Şəbəkə trafikinin klasterizasiyası metodları

Fərqli statistik xüsusiyyətlərə əsaslanaraq, "Machine learning" texnikası şəbəkə məlumatlarında anormal axışları müəyyənləşdirmək üçün sıx istifadə olunur. Ənənəvi qruplaşdırma, təbii məlumat işləmə və qeyri-müəyyən axınların aşkar edilməsi üçün daha az çevikdir. Qeyri-müəyyən axışları müəyyənləşdirmək üçün bir çox qruplaşdırma yanaşması mövcuddur. Qruplaşdırma texnikalarından istifadə edərək, hər bir axış sessiyasını digər sessiyalarla olan fərqləri və oxşarlıqları əsasında uyğun qruplara ayırmaq mümkündür. Bu kateqoriyalara təyin olunan simvollar onların təsvirləri kimi xidmət edir. Daha sonra şəbəkə axışının növü bu simvollardan istifadə edərək müəyyən olunur. Funksiyalar üçün ən mühüm olan problemlərdən biri şəbəkə axışlarının sürətli və doğru aşkarlanması, xidmət keyfiyyətinin idarə olunması, şəbəkə təhlükəsizlik monitorinqi kimi məsələlərdir. Lakin son zamanlarda P2P-dən istifadə daha yayılmışdır. Həmçinin, bir

neçə portdan istifadə edərək hər hansı bir cihazı, faydalı trafik və ya şifrlənmiş trafik kimi sübut edən təcavüzkar trafik yaradırlar. Bu halda, “Port mapping” və ya “payload analysis” kimi ənənəvi üsullar faydasızdır. Alternativ bir strategiya isə şəbəkəyə çatmaq üçün bir neçə TCP paketinin davranışını təhlil və kateqoriyalandırmaqdır [6].

Simsiz şəbəkələrin təhlükəsizliyinə olan ehtiyacın artması, bu şəbəkələrin təhlükəsizlik məsələlərinə böyük diqqət çəkməkdədir. Naqilli şəbəkələrdə qeyri-müəyyən axış analizində istifadə olunan metodlar, simsiz şəbəkələr üçün uyğun deyildir. 802.11 simsiz şəbəkələrdə boşluqları aşkar etmək və simsiz şəbəkələrin təhlükəsizliyini modelləşdirilməsi üçün şəbəkə axışlarının ölçülməsi lazımdır. DDoS hücumlarının aşkarlanması, şəbəkələrin təhlükəsizliyində önəmli bir rol oynayır. Aşağıdakı adaptiv qruplaşdırma metodundan DDoS hücumlarını xarakterləşdirmək üçün istifadə edilir:

1. Şəbəkə trafik analizində birinci ilkin dəyişənlər seçilir;
2. Verilənin qruplaşma strukturunu müəyyənləşdirmək üçün dəyişdirilmiş qlobal alqoritm əsas qruplaşma alqoritmi kimi istifadə edilir;
3. Xətti korrelyasiya əmsalı əlamətləri ranqlaşdırmaq üçün istifadə olunur;
4. Ranqlaşdırılmış məlumatlar klasterlərin yenidən hesablanması üçün istifadə olunur

Bu adaptiv yanaşma, çeşitli DDoS hücum nümunələrinə görə xüsusiyyət vektorunda tələb olunan dəyişiklikləri etməklə qrupların keyfiyyətini və alqoritmanın effektivliyini artırmağa imkan verir.

Botnet, istifadəçinin bilmədiyi halda bir kompüteri virus vasitəsilə uzaqdan nəzarət etmək və onu şəbəkəyə qoşmaq üçün istifadə olunan bir infrastrukturadır. Belə zərərli texnologiya zombiləşmiş kompüterlərin ordusunun yaradılmasına uyğun məkan yaradır. Zərərli bir botnet şəbəkəsini idarə etmək üçün əmr və nəzarət prinsipindən istifadə edilir. Operatorun protokolu və kodlaması normal axışlardan fərqli olan şəbəkə axışlarını monitorinq edərək müəyyən edilə bilər [7]. Botnetlər üçün əmr və nəzarət kanallarını aşkar etmək üçün iyerarxiya qruplaşdırma istifadə olunur. Bu, botnetlərin idarə edilməsi üçün tələb olunan məlumat mübadiləsini müəyyənləşdirir. Bu yanaşma, istifadəçinin

kompüterinin botnet şəbəkəsinin bir hissəsi olduğunda onun xarici nəzarətdən qorunmasının effektiv bir vasitəsi olaraq nəzərə alına bilər.

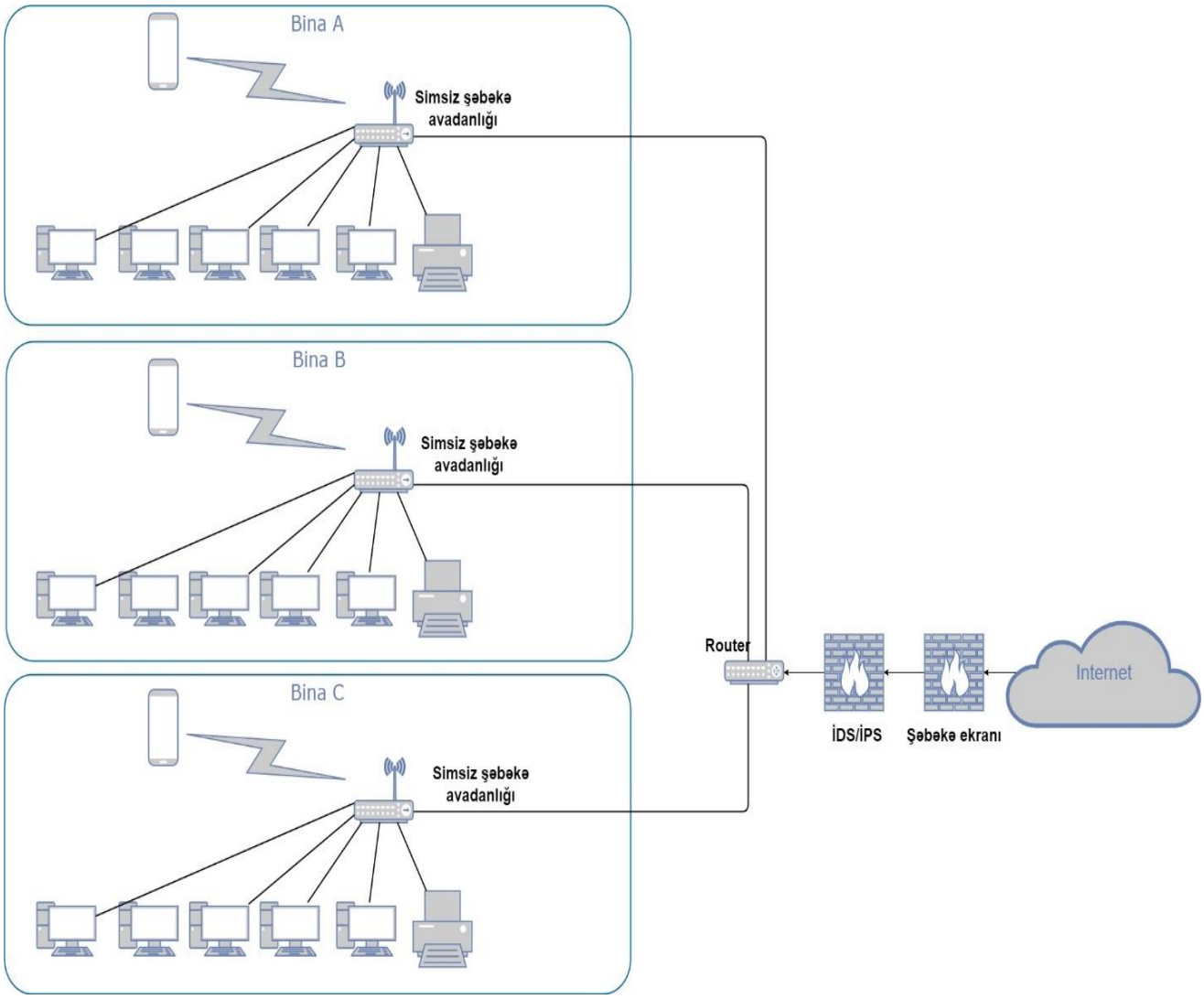
II FƏSİL. ŞƏBƏKƏ TRAFİKİNİN TƏHLÜKƏSİZLİYİNİN MONİTORİNQİ ÜÇÜN KONSEPTUAL MODELİN İŞLƏNMƏSİ

2.1. Kiberhücumların aşkarlanması və qarşısının alınması sistemlərinin analizi

Kiberhücumların aşkarlanması sistemləri təşkilatlarda kiberhücumların müəyyən edilməsində və müvafiq məlumatlandırma tədbirlərinin görülməsində mühüm rol oynayır. Kiberhücumların aşkarlanması üçün bir neçə yanaşma mövcuddur. İmza əsaslı aşkarlama, anomaliya əsaslı aşkarlama və davranış əsaslı aşkarlamanı buna misal göstərmək olar. İmza əsaslı aşkarlama sistemləri müəyyən verilənlər bazasında mövcud olan hücum indikatorları ilə şəbəkəyə daxil olan trafikin, kodun müqayisəli təhlili əsasında qərar verir. Anomaliya əsaslı aşkarlama normal sistem davranışından kənar davranışları müəyyən edir. Davranışa əsaslanan aşkarlama isə süni intellektin köməyi ilə formasından asılı olmayaraq hər -hansı zərərli fəaliyyət nümunələrini müəyyən edir. Bu üsulların birləşməsindən yaranan hibrid sistemlər kiberhücumların hərtərəfli aşkarlanma-sını təmin edir. Bundan əlavə, maşın öyrənməsi və süni intellekt üsullarının inteqrasiyası bu sistemlərə zamanla uyğunlaşmaq və öz-özünü təkmilləşdirmək imkanı verir.

Kiberhücumların qarşısının alınması sistemləri təşkilatları kiberhücumlardan fəal şəkildə qorumaq üçün nəzərdə tutulmuşdur ki, onlar təşkilata yönəlmiş kiberhücumları və təhdidləri təşkilatın infrastrukturuna, biznes proseslərə, fəaliyyətinə zərər vurmazdan əvvəl bloklamağa və ya azaltmağa imkan verir. Bu cür sistemlərə şəbəkə ekranları, müdaxilənin aşkarlanması və qarşısının alınması sistemləri (IDPS - İntrusion Detection and Prevention System), son nöqtə qorunma sistemləri (EDR - Endpoint Detection and Response), veb tətbiqlər üçün şəbəkə ekranları (WAF - Web application Firewall) və təhlükəsizlik hadisələrin idarə edilməsi (SIEM - Security Information and Event Management) sistemləri daxildir [9]. Şəbəkə ekranları daxili şəbəkələ və xarici təhlükələr arasında maneə rolunu oynayır. Lakin elə hallar ola bilər ki, şəbəkə ekranı bu cür təhlükələri aşkar edə bilməsin. Bunun üçün şəbəkə ekranından əlavə olaraq müdaxilənin aşkarlanması və qarşısının alınması sistemləri quraşdırılır ki, bu da öz növbəsində şəbəkədə baş verən şüb-

həli hadisələrin aşkarlanması və qarşısının alınması funksiyasını yerinə yetirir (Şəkil 2.1) [9].



Şəkil 2.1. Şəbəkə ekranı və müdaxilənin aşkarlanması və qarşısının alınması sistemi quraşdırılmış şəbəkə sxemi

IDPS sistemləri baş vermiş təhlükəsizlik hadisələri və insidentlərinin haqqında qeydlərini saxlayır. Bu qeydlər hadisədən sonrakı təhlil, araşdırmalar və uyğunluq tələbləri üçün çox vacibdir. IDPS aşkar edilmiş təhdidlər, onların təsiri və sistemin effektivliyi haqqında məlumat verən hesabatlar yaradır. Hesabatlar baş vermiş hücumlar haqqında məlumatları, tendensiyaları və təhlükəsizliyin təkmilləşdirilməsi üçün tövsiyələr kimi məlumatları ehtiva edir [9].

IDPS sistemləri effektivliyin artırılması məqsədi ilə digər təhlükəsizlik sistemləri ilə inteqrasiya edə bilər. Onlar şəbəkə ekranları, antivirus proqramı, təhlükəsizlik hadisələrinin idarə edilməsi (SIEM) sistemləri ilə məlumat mübadiləsi edə bilərlər [9]. Bu alətlər arasında əlaqə baş verən və ya verə biləcək təhlükənin aşkarlanmasını asanlaşdırır.

Günə artan kibertəhlükəsizlik təhdidləri kibertəhlükəsizlik hücumlarının aşkarlanması və qarşısının alınması sistemlərinin daim yenilənəsini və ən son təhdidlərə cavab verməsini tələb edir. Müdaxilələrin aşkarlanması və qarşısının alınması sistemlərinin effektiv çalışması üçün zərərli proseslərin, kodların və s. Potensial təhlükə daşıya biləcək proqram vasitələrinin indikator bazası yenilənməlidir. Bundan əlavə olaraq müdaxilələrin aşkarlanması və qarşısının alınması sistemlərinin də daxili təhlükəsizlik boşluğunun olma ehtimalını nəzərə alsaq, bu sistemlərdə davamlı olaraq təhlükəsizlik yoxlanışı keçirilməsi və monitoring edilməsi vacibdir.

Son nöqtə qoruma sistemləri şəbəkəyə qoşulmuş fərdi kompüterlər, mobil cihazlar və s. kimi fərdi cihazlarını qoruyur. Veb tətbiqlər üçün şəbəkə ekranı veb əsaslı proqramları hücumlardan qoruyur. Təhlükəsizlik hadisələrinin idarəetmə sistemləri potensial kibertəhlükələri aşkar etmək və onların qarşısının alınması üçün təhlükəsizlik hadisələri haqqında məlumatlarını toplayır və təhlil edərək mühəndisə məlumat verir. Kiberhücumların qarşısının alınması sistemləri kibertəhlükələrdən müdafiənin əsas hissəsini təmin etsə də, sürətlə inkişaf edən kiberhücum texnikalarına uyğunlaşmaq və bu texnikaların sistem performansına potensial təsir göstərmək kimi problemləri ilə üzləşə bilərlər.

Veb tətbiqlər üçün şəbəkə ekranı veb tətbiqlərə daxil olan HTTP/HTTPS sorğularını yoxlamaq üçün sorğu filtrləmə üsullarından istifadə edir [13]. Onlar potensial təhlükəsizlik boşluqlarını və ya zərərli sorğuları müəyyən etmək üçün başlıqlar, parametrlər, kukilər kimi müxtəlif elementlərin təhlilini aparırlar. Sorğuları əvvəlcədən müəyyən edilmiş qaydalarla müqayisə edərək, Veb şəbəkə ekranı(WAF) sorğuya icazə verə və ya bloklaya bilər [13].

Açıq Veb Tətbiqinin Təhlükəsizliyi Layihəsi (OWASP) ən vacib 10 veb tətbiqi təhlükəsizlik risklərinin siyahısını dərc edir. WAF sistemləri bu riskləri effektiv şəkildə həll etmək üçün nəzərdə tutulmuşdur [14]. Onlar inyeksiya hücumları (SQL, Əməliyyat sistemi və s.), saytlararası skriptlər (XSS), saytlararası sorğu saxtakarlığı (CSRF) və OWASP Top 10 tərəfindən müəyyən edilmiş digər zəifliklərdən qorunmaq üçün xüsusi əks tədbirlər həyata keçirirlər [14].

WAF müsbət təhlükəsizlik modeli ilə konfiqurasiya edilə bilər, burada o, yalnız müəyyən edilmiş qaydalar toplusuna əsaslanaraq yalnız icazə verilən sorğuları daxili veb tətbiqə yönləndirir. Bu yanaşma bloklanmalı sorğuları deyil, icazə verilməli sorğuları müəyyən edərək bütün digər sorğuları bloklayır [13].

Kiberhücumların aşkarlanması və qarşısının alınması sistemlərindən biri də təhlükəsizlik hadisələrinin idarəetmə sistemidir (SİEM) [10]. Bu, təşkilatın İT infrastrukturunda baş verən təhlükəsizlik hadisələrinin real vaxt rejimində monitorinqini, korrelyasiyasını, təhlilini və hesabatını təmin edən proqram həllidir [10]. SIEM sistemləri potensial təhlükəsizlik insidentlərini aşkar etmək və onlara reaksiya vermək və tənzimləyici tələblərə riayət etmək üçün nəzərdə tutulmuşdur [11].

Təhlükəsizlik hadisələrinin idarə etmə sisteminin(SİEM) işləmə prinsipi aşağıdakılardan ibarətdir:

1. **Məlumat yığımı.** SIEM şəbəkə cihazları (məsələn, şəbəkə ekranları, marşrutlaşdırıcılar), serverlər,kompüterlər, təhlükəsizlik cihazları (məsələn, müdaxilənin aşkarlanması sistemləri), proqramlar və əməliyyat sistemləri və verilənlər bazaları və s mənbələrdən onların daxilində baş verən hadisələr haqqında məlumat toplayır. Bu məlumatlar SIEM sistemində toplanır və mərkəzləşdirilmiş qaydada idarə edilir.
2. **Hadisələrin idarə edilməsi.** Toplanmış məlumatlar normallaşdırılır, təhlil edilir və müvafiq məlumatları çıxarmaq üçün filtrlənir və qeydlər şəklində saxlanılır. Müxtəlif mənbələrdən olan qeydlər ümumi formatda standartlaşdırılaraq hadisələrin təhlilini və əlaqələndirilməsini asanlaşdırır. Normallaşdırılmış qeydlər daha sonra emal üçün

mərkəzləşdirilmiş hadisələrin idarə edilməsi sistemində və ya verilənlər bazasında saxlanılır.

3. **Real vaxt rejimində monitorinq.** SIEM sistemləri real vaxt rejimində daxil olan hadisə məlumatlarını davamlı olaraq izləyir. Onlar potensial təhlükəsizlik insidentlərini və ya siyasət pozuntularını müəyyən etmək üçün hadisələri əvvəlcədən müəyyən edilmiş qaydalara uyğun olaraq təhlil edirlər.

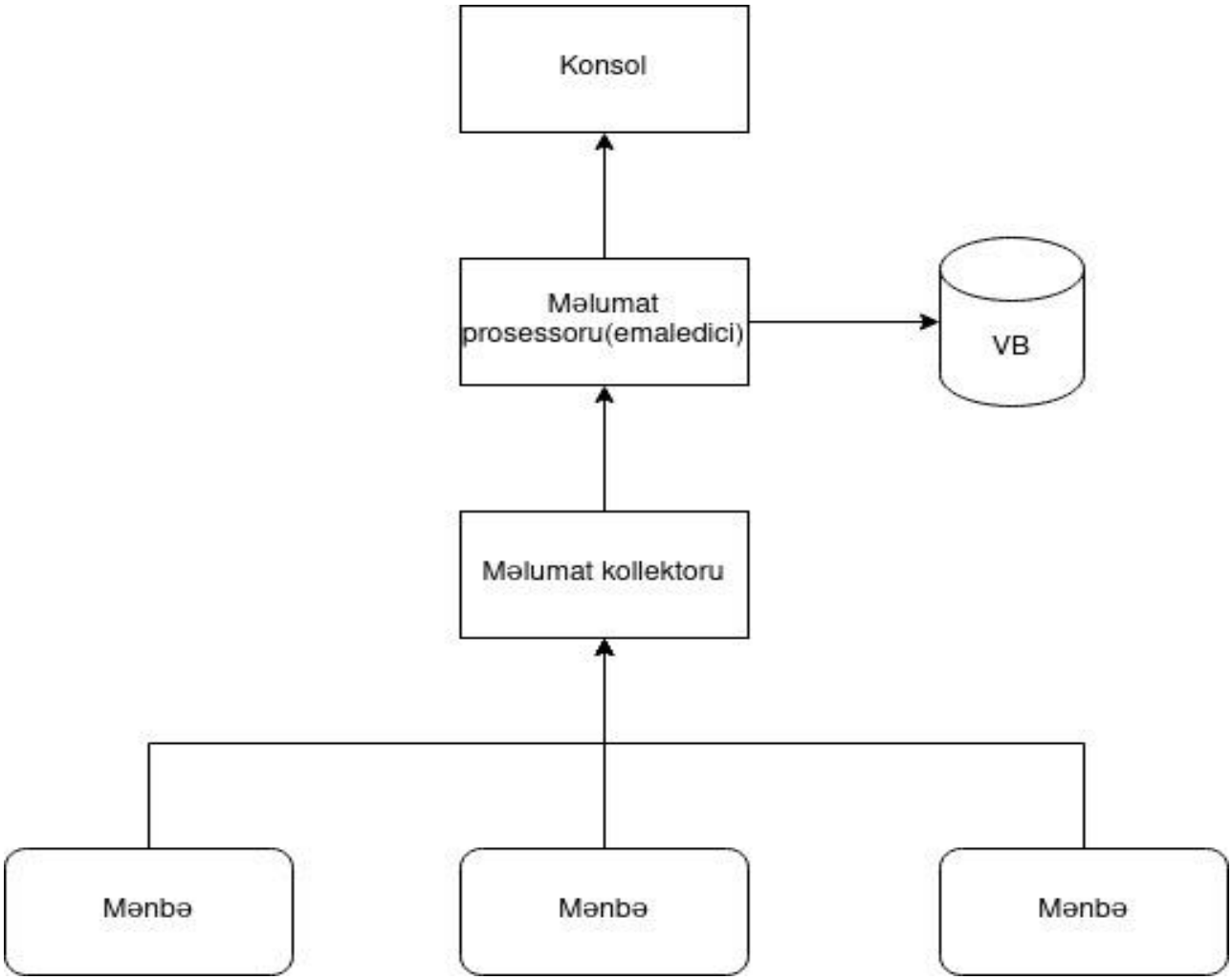
4. **Hadisələrin korrelyasiyası.** SIEM sistemləri müxtəlif mənbələrdən gələn hadisələri təhlil edərək və hadisələrin əlaqələndirilməsini təmin edərək korrelyasiya prosesini həyata keçirir. Məsələn, bir neçə uğursuz giriş cəhdlərinin ardınca baş verən uğurlu giriş brute-force hücumunun göstəricisi ola bilər. Korrelyasiya alqoritmləri SIEM sistemlərinə təhlükəsizlik hadisəsi haqqında daha əhatəli məlumatlandırmanı təmin etmək üçün hadisələri birləşdirməyə kömək edir.

5. **Xəbərdarlığın yaradılması:** Potensial təhlükəsizlik hadisəsi aşkar edildikdə, SIEM sistemi xəbərdarlıqlar və ya bildirişlər yaradır. Bu xəbərdarlıqlar e-poçt, SMS və ya mərkəzləşdirilmiş idarə paneli kimi müxtəlif kanallar vasitəsilə təhlükəsizlik analitiklərinə və ya idarəçilərə göndərilə bilər. Xəbərdarlıqlar hadisə, onun kritikliyi və hadisəyə effektiv cavab vermək üçün hər hansı əlavə kontekstual məlumatlar haqqında məlumat verir.

6. **Insidentlərə cavab**: SIEM sistemləri təhlükəsizlik qruplarına aşkar edilmiş insidentlər haqqında ətraflı məlumat verməklə insidentlərə cavab verməyi asanlaşdırır. Sistem analitiklərə hadisələri araşdırmaq, kriminalistika təhlili aparmaq və təhlükəni azaltmaq üçün müvafiq tədbirlər görmək imkanı verir. SIEM həmçinin insidentlərə cavab proseslərini avtomatlaşdırmaq üçün digər təhlükəsizlik alətləri ilə inteqrasiya edə bilər.

7. **Hesabat və Uyğunluq:** SIEM sistemləri təhlükəsizlik hadisələri və insidentləri əsasında uyğunluq hesabatları və digər xüsusi hesabatlar yaratmaq üçün imkanlar təklif edir. Bu hesabatlar təşkilatlara tənzimləyici standartlara uyğunluğu nümayiş etdirməyə kömək edir və onların təhlükəsizlik vəziyyəti haqqında fikirlər təqdim edir. SIEM

sistemləri həmçinin qeydlərin saxlanması və arxivləşdirilməsi funksiyasını həyata keçirə bilər. Şəkil 2.2-də SİEM sisteminin sxemi verilmişdir.



Şəkil 2.2. SİEM sisteminin sxemi

Şəkildə göründüyü kimi şəbəkə cihazları, kompüterlər, serverlər, əməliyyat sistemləri, proqramlar və s. mənbələr hadisələr haqqında qeydləri məlumat kollektoruna göndərir. Daha sonra məlumat kollektoru bu məlumatları normallaşdırılması və emal edilməsi üçün məlumat prosessoruna göndərir. Prosessorda emal edilmiş və normallaşdırılmış hadisə qeydləri daha sonra konsol vasitəsi ilə vizuallaşdırılır. Əlavə olaraq məlumat prosessorunda emal edilən bütün hadisə qeydləri verilənlər bazasında saxlanılır [11].

Təşkilatınızın nə qədər böyük və ya kiçik olmasından asılı olmayaraq, informasiya təhlükəsizliyi risklərini izləmək və azaltmaq üçün qabaqlayıcı addımlar atmaq vacibdir.

SIEM həlləri müəssisələrə müxtəlif yollarla fayda verir və təhlükəsizlik iş axınının sadələşdirilməsində mühüm komponentə çevrilib. SİEM həlləri infrastrukltur üzrə potensial təhdidləri və zəiflikləri müəyyən etməyə, təhlükəsizlik insidentlərinə reaksiya müddətinin əhəmiyyətli dərəcədə azaldılmasını təmin edir [10].

Bugünkü yeni nəsil SIEM həlləri güclü Təhlükəsizlik Orkestrasiyası, Avtomatlaşdırma və Cavab (SOAR- Security Orchestration, Automation and Response) imkanları ilə inteqrasiya edərək, informasiya təhlükəsizliyinin idarə olunmasında vaxta və resurslara qənaət edir [10]. Dərin maşın öyrənmə alqoritmlərindən istifadə etməklə şəbəkə davranışına avtomatik uyğunlaşan bu sistemlər daha az müddət ərzində mürəkkəb insidentlərin identifikasiyasını apara və insidentlərə cavab verə bilirlər.

Kibertəhlükəsizlik mühitinin nə qədər qısa müddətdə dəyişdiyini nəzərə alaraq, təşkilatlar həm məlum, həm də naməlum təhlükəsizlik təhdidlərini aşkarlaya və onlara cavab verə bilən həllərə etibar etməlidirlər. İnteqrasiya edilmiş süni intellekt texnologiyalarından istifadə etməklə SİEM sistemləri aşağıdakı kiberhücumların qarşısının alınmasını təmin edir [11]:

Daxili təhdidlər(insider) - Şirkət şəbəkələrinə və rəqəmsal aktivlərə icazəli girişi olan şəxslərdən yaranan təhlükəsizlik boşluqları və ya hücumlar [11].

Fişinq hücumları – Etibarlı şəxs, qurum və s. kimi maskalanan sosial mühəndislik hücumları, tez-tez istifadəçi məlumatlarını, giriş məlumatlarını, maliyyə məlumatlarını və ya digər həssas biznes məlumatlarını oğurlamaq üçün istifadə olunur [11].

SQL inyeksiya hücumları – Veb saytın və ya proqram təminatının boşluğundan istifadə edərək təhlükəsizlik tədbirlərini yan keçmək və SQL verilənlər bazasında qeydlər əlavə etmək, dəyişdirmək və ya silmək üçün nəzərdə tutulmuşdur [11].

DDoS Hücumları – Eyni anda çoxsaylı sorğular göndərməklə veb-saytların, sistemlərin və ya serverlərin yararsız hala salınması hücumu [11].

Məlumat sızıntısı – Şəbəkə cihazlarında, sistemlərdə sadə parolların istifadəsi kimi amillərin nəticəsi olaraq təşkilat məlumatlarının sızdırılması hücumlarıdır [11].

Kiberhücumların aşkarlanması və qarşısının alınması sistemləri daim dəyişən kiberhücumlara qarşı düzgün və vaxtında reaksiya vermək üçün daim inkişaf edir. Bir sıra inkişaf edən tendensiyalar bu sistemlərin gələcəyini formalaşdırır. Böyük verilənlərin (Big Data) analitikasının inteqrasiyası təşkilatlara mürəkkəb hücumları aşkar etmək üçün böyük həcmdə məlumatların emalı və korrelyasiyası imkanı verir. İstifadəçi və təşkilat davranışı analitikası (UEBA) sistemi maşın öyrənməsi alqoritmlərindən istifadə edərək mövcud kiberücumları göstərə biləcək anormal davranışı müəyyən etmək qabiliyyətinə malikdir [15]. Bulud əsaslı kiberhücumların aşkarlama və qarşısının alınması sistemləri bulud mühitlərində fəaliyyət göstərən təşkilatlar üçün genişlənən və çevik təhlükəsizlik həlləri təqdim edir. Kibercinayəkarları çaşdırmaq və hücumların qarşısını almaq məqsədi ilə süni hədəflərdən və tələlərdən istifadə etmək mümkündür. Bundan əlavə, süni intellekt və maşın öyrənməsindəki irəliləyişlər kiberhücumların aşkarlanması və qarşısının alınması sistemlərinin dəqiqliyini və səmərəliliyini artırır. Bununla belə, yaranan bu tendensiyalar məxfilik problemləri və bacarıqlı kibertəhlükəsizlik mütəxəssislərinə ehtiyac kimi yeni problemlər də gətirir.

Kiberhücumun aşkarlanması və qarşısının alınması sistemlərini seçərkən müxtəlif amillər nəzərə alınmalıdır. Bunlara təşkilatın informasiya təhlükəsizliyi ehtiyacları, performans göstəriciləri və qiymətləndirmə meyarları, büdcə və miqyaslılıq göstəriciləri, mövcud infrastrukturla inteqrasiya və qarşılıqlı fəaliyyət, uyğunluq tələbləri daxildir. Hərtərəfli qiymətləndirmələr aparmaqla təşkilatlar dayanıqlı kibertəhlükəsizlik mühiti yarada bilərlər.

2.2. **Şəbəkə trafikinin analizi sistemin arxitekturası və dizaynı**

Şəbəkə trafikinin təhlili sisteminin layihələndirilməsi bir neçə əsas komponenti və mülahizələri əhatə edir. Şəbəkə traffikinin analizi sisteminin qurulması və təkmilləşdirilməsi üçün müəyyən proseslər ardıcıllığına riayət edilməsi tələb edilir.

Düzgün və effektiv nəticənin alınmasını təmin etmək üçün ilkin olaraq məqsəd və tələblər müəyyən edilməlidir. Hansı növ şəbəkə trafikinə nəzarət olunacağı, tələb olunan

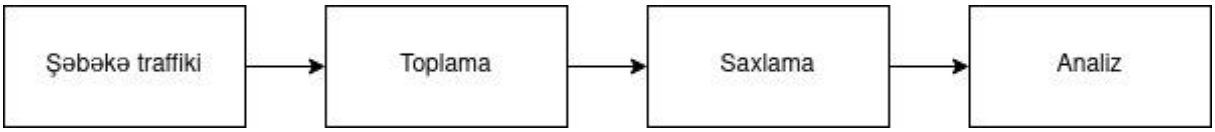
təfərrüat səviyyəsi və ya hər hansı xüsusi təhlükəsizlik tələbləri müəyyən edilməlidir. Şəbəkə trafikinin analizi sisteminin əsas məqsəd və tələbləri müəyyən edildikdən sonra növbəti mərhələdə məlumat yığımı prosesi aparılmalıdır. Bunun üçün şəbəkə ekranları, sviçlər, marşrutlaşdırıcılar və s. mənbələrdən məlumat yığılması mexanizmi qurulmalıdır. Bu mexanizmlərə portun əks etdirilməsi, şəbəkə paketlərinin skanı və ya axın əsaslı məlumat toplanması(məsələn, NetFlow, sFlow, IPFIX və s.) [8] mexanizmlərini misal göstərmək olar[9]. Məlumat yığılması prosesi aparıldıqdan sonra toplanmış məlumatın emalı və saxlanılması prosesi aparılmalıdır. Məlumatın həcmindən asılı olaraq onların saxlanılması üçün ayrılmış saxlanc serverləri və ya bulud həlləri istifadə etmək mümükündür.

Müxtəlif mənbələrdən toplu şəkildə yığılmış məlumatların kontenti pərakəndə olduğundan onların standartlaşdırılması və oxunaqlı vəziyyətə gətirilməsi tələb olunur. Bu səbəbdən şəbəkə trafiki məlumatlarını təhlil edən və müvafiq məlumatların çıxarılmasını təmin edən alətlərin hazırlanması tələb olunur. Bu prosesə şəbəkə protokollarının növünün təyin edilməsi, paket başlığının dekodlaşdırılmasını, mənbə və təyinat İP ünvanları, port nömrələri, vaxt ştampları və düzgün təhlil üçün lazım olan hər hansı digər məlumatların çıxarılması aiddir.

Məlumatlar standartlaşdırılma və filtrasiya prosesini keçdirkdən sonra trafikin analizi texnikaları müəyyənləşdirilməlidir. Şəbələ trafiki haqqında məlumat əldə etmək və anomaliyaları və ya təhlükəsilik təhdidlərini müəyyən etmək üçün bir sıra trafik təhlili üsulları tətbiq edilməlidir. Buraya statistik analiz, anomaliyaların aşkarlanması alqoritmləri, maşın öyrənmə modelləri və trafikin vizuallaşdırılması üsulları daxil ola bilər.Trafik analizi prosesinin yekununda trafikin analizinin nəticələri xəbərdarlıq və ya hesabatlarla bildirilməlidir. Şəbəkədə şübhəli və ya qeyri - normal davranışlar barədə idarəçilərə və ya təhlükəsizlik işçilərinə məlumat verilməsi üçün xəbərdarlıq mexanizmləri qurulmalıdır və təhlükəsizlik insidentləri, performans göstəriciləri barədə hesabat təqdim edilməlidir.Analizin daha rahat və effektiv aparılması üçün vizualizasiya və istifadəçi interfeysinin olması vacibdir. Məlumata intuitiv giriş, real vaxt rejimində

monitorinq və ətraflı araşdırma imkanlarını təmin etmək üçün interaktiv idarə panelləri, qrafiklər, diaqramlar və axtarış funksiyalarından istifadə edilməsi zəruridir.Şəbəkə trafikinin analizi sisteminin daimi və dayanıqlı fəaliyyətinin təmin edilməsi üçün genişmiqyaslılıq və performans göstəricilərinin tənzimlənməsi vacibdir. Genişmiqyaslı şəbəkə trafikinin analizi zamanı gecikmələrin və ya dayanmaların azaldılması üçün yük balanslaşdırılması, ayrılmış emaletmə kimi mexanizmlərdən istifadə edilməlidir.Şəbəkə trafikinin analizi sisteminin özünün də müxtəlif təhdidlərə və təhlükələrə məruz qala biləcəyi ehtimalını nəzərə alsaq, bu sistemin təhlükəsizliyinin təmin edilməsi üçün ayrıca təhlükəsizlik tədbirləri görülməlidir. Əlavə olaraq davamlı şəkildə yeniləmələr həyata keçirilməlidir.İstifadə edəcəyimiz şəbəkə trafikinin analizi sistemi üçün qeyd edilmiş proseslər nəzərə alınmışdır. Şəbəkə trafikinin analizi sisteminin məqsədi şəbəkə cihazlarından hadisə qeydlərini toplamaqla, onların analiz edilməsi və şəbəkədə baş verən şübhəli halların və anomaliyaların müəyyən edilməsi və onların qarşısının alınmasıdır.

Trafikin analizi sistemi şəbəkə trafikini qəbul edir, özündə saxlayır və analiz edir. Prosesin mərhələləri şəkil 2.3-də verilmişdir.



Şəkil 2.3. Şəbəkə trafikinin analizi prosesi

Trafikin toplanması prosesi sniffinq üsulu ilə həyata keçirilir. Sniffinq real-vaxt rejimində şəbəkə trafikinin toplanması və analizi prosesidir [16]. Bura şəbəkədən keçən məlumat paketlərinin tutulması və araşdırılması daxildir. Sniffinq üsulu adətən sistem inzibatçıları, şəbəkə inzibatçıları, təhlükəsizlik mühəndisləri tərəfindən şəbəkə davranışını təhlil edilməsi, şəbəkədə yaranmış problemlərin analizi və həll edilməsi və şəbəkə trafiki haqqında məlumat toplamaq üçün istifadə edilir [16]. Sniffinq üsulu ilə şəbəkə paketlərinin toplanması üçün snifferlərdən istifadə edilir. Snifferlər proqram təminatı və

ya qurğu ola bilər. Snifferlər kompüterlərə quraşdırıla, ayrıca qurğu kimi çalışa və ya şəbəkə infrastrukturunun elementlərinə (məsələn, sviçlərə, marşrutlaşdırıcılara və s.) quraşdırıla bilərlər [16]. Paketlər toplandıqdan sonra paket analizi proqram təminatından istifadə edilməklə analiz olunurlar. Proqram təminatı tutulmuş paketləri dekodlaşdıraraq onların daxilindəki informasiyanı (İP ünvanı, port nömrəsi, protokol növü və s.) çıxarır.

Sniffinq OSİ modelinin müxtəlif səviyyələrində aparıla bilər:

1. **Şəbəkə səviyyəsi.** Şəbəkə səviyyəsində çalışan snifferlər yalnız İP ünvanları, marşrutlama haqqında məlumatları, şəbəkə səviyyəsinə uyğun protokollar haqqında məlumatları analiz edə bilirlər.
2. **Nəqliyyat səviyyəsi.** Bu səviyyədə çalışan snifferlər nəqliyyat səviyyəsi protokollarını(TCP/UDP), sessiya məlumatlarını, port nömrələrini analiz edə bilirlər.
3. **Tətbiqi səviyyə.** Bu səviyyədə çalışan snifferlər HTTP, FTP, DNS, SMTP və s. kimi tətbiqi səviyyə protokollarını təhlil edərək daha dərin analizin aparılmasını təmin edirlər.

Sniffer vasitəsi ilə şəbəkə traffiki toplandıqdan sonra saxlama və analiz mərhələsindən keçir. Toplanılmış məlumat PCAP formatında saxlanılır [17]. PCAP (Packet Capture) şəbəkə paketlərini saxlamaq üçün geniş istifadə olunan fayl formatıdır. Bu format tutulan şəbəkə paketlərinin müvafiq metadata ilə birlikdə saxlanmasına imkan verən standart formatdır. PCAP faylları ümumiyyətlə şəbəkə təhlili, problemlərin aradan qaldırılması, protokolların düzəldilməsi və təhlükəsizlik araşdırmaları üçün istifadə olunur [18]. PCAP faylları ikili fayllardır, yəni məlumatları oxunaqlı formatda deyil, ikili formatda saxlayır. Bu ikili format böyük həcmdə şəbəkə paketi məlumatlarını səmərəli saxlamağa imkan verir [17]. PCAP fayllar paketlərin saxlanılmasını paket verilənləri və metadatanı özündə birləşdirən strukturda təşkil edir. Paket verilənləri hər bir tutulan paketin faktiki məzmununu, metadata isə vaxtştampları, paket uzunluqları, interfeys detalları və protokol məlumatı kimi məlumatları ehtiva edir. PCAP faylları snifferə daxil olan hər bir paket üçün dəqiq vaxt ştamplarını saxlayır [18]. Bu vaxt ştampları hər bir

paketin nə vaxt snifferə daxil olduğu barədə məlumat verir, paket vaxtı və şəbəkə trafikinin dəqiq təhlilinə imkan verir.

Paket məlumatlarının PCAP formatında saxlanılmasının üstünlükləri aşağıdakılardır [18]:

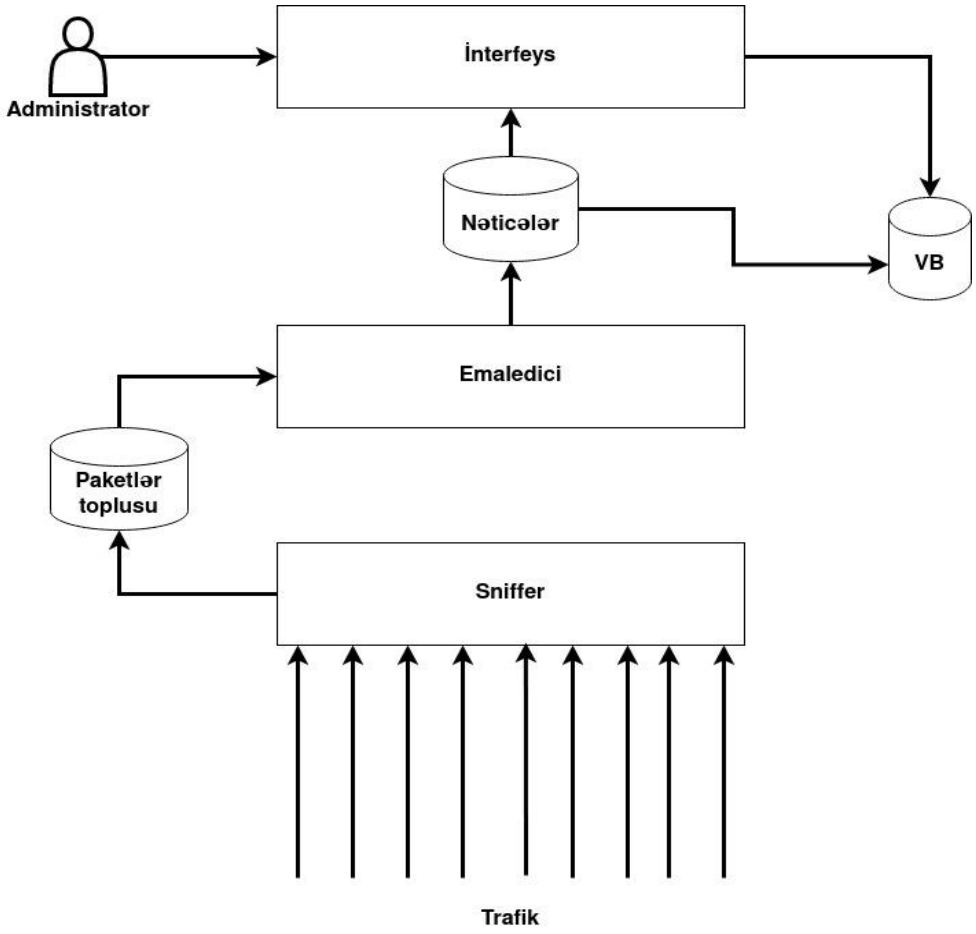
– PCAP faylları bir çox şəbəkə interfeysindən paket toplanmasını idarə edə bilər. Bu xüsusiyyət, trafikin müxtəlif mənbələrdən toplandığı hallarda və mürəkkəb şəbəkə mühitlərində xüsusilə faydalıdır.

– PCAP faylları TCP, UDP, ICMP, HTTP, FTP, DNS və s. daxil olmaqla geniş şəbəkə protokollarından paketləri saxlaya bilər. Bu xüsusiyyət müxtəlif şəbəkə protokollarının hərtərəfli təhlilinə imkan verir.

– PCAP formatı çoxsaylı şəbəkə analiz alətləri və proqram təminatı ilə dəstəklənir. Bu geniş alət dəstəyi PCAP fayllarını müxtəlif platformalarda və mühitlərdə, xüsusən də işləyib hazırladığımız şəbəkə trafikinin analizi sistemində asanlıqla paylaşıla bilən və əlçatan edir.

PCAP faylları, xüsusilə uzun müddət ərzində yüksək həcmli şəbəkə trafikini topladıqda olduqca böyük həcmli ola bilər. Bu səbəbdən PCAP fayllarını toplayarkən və saxlayarkən yaddaş tələblərini və disk sahəsinin mövcudluğunu nəzərə almaq vacibdir. İşlənməsi nəzərdə tutulan şəbəkə trafikinin analizi sisteminin ümumi sxemi 2.4-cü şəkildə verilmişdir.

Burada şəbəkə cihazlarından keçən traffik ilkin olaraq sniffer tərəfindən toplanır. Növbəti mərhələdə toplanılan paketlər toplusu emalediciyə ötürülür. Emaledici tərəfindən bu cür paketlər dekodlaşdırılır və tərkibindəki məlumatlar (protokol məlumatları, port, ip ünvan və s.) çıxarılaraq filtrlənir. Daha onra alınmış nəticənin bir nüsxəsi istifadəçi interfeysinə ötürülür, digər hissəsi isə verilənlər bazasında saxlanılır.



Şəkil 2.4. Şəbəkə trafikinin analizi sisteminin ümumi sxemi

2.3. Şəbəkə trafikinin analizi üçün konseptual modelin işlənməsi.

Şəbəkə traffikinin analizi sisteminin işlənməsi üçün python proqramlaşdırma dilindən istifadə edilmişdir. Python sadəliyi, oxunaqlılığı və çox yönlü olması ilə tanınan məşhur yüksək səviyyəli proqramlaşdırma dilidir. Şəbəkə proqramlaşdırması və məlumatların təhlili daxil olmaqla, müxtəlif sahələrdə populyarlıq qazanmışdır ki, bu da onu şəbəkə trafikinin analizi layihələri üçün ideal həllə çevirir. Şəbəkə trafikinin analizi sisteminin işlənməsi üçün Python istifadə etməyin bəzi əsas üstünlükləri aşağıdakılardır [19]:

- **İstifadəsinin asanlığı.** Python proqramlaşdırma dilinin oxunulması və yazılması sadə olan sintaksisi mövcuddur ki, bu da onu daha əlverişli edir və sürətli işləməyə şərait

yaradır. Onun sadəliyi şəbəkə trafikinin analizi sisteminin qurulmasını daha tez həyata keçirməyə və ona texniki dəstəyin göstərilməsini asanlaşdırmağa imkan verir [19].

- **Geniş kitabxana ekosistemi.** Geniş Kitabxana Ekosistemi: Python şəbəkə proqramlaşdırmasını və məlumatların təhlilini asanlaşdıran geniş kitabxana və modul kolleksiyasına malikdir. Scapy, pyshark və NetFlow/IPFIX kimi kitabxanalar şəbəkə paketlərini və paket axını məlumatlarını toplamaq, təhlil etmək üçün güclü imkanlar təqdim edir.
- **Müxtəlif platformalara uyğunluq.** Python çarpaz platforma dilidir, yəni Windows, macOS və Linux daxil olmaqla bir çox əməliyyat sistemlərində işləyir. Bu çoxfunksiyalılıq, şəbəkə trafikinin analizi sistemimizin kod hissəsində əhəmiyyətli dəyişikliklər etmədən müxtəlif platformalarda asanlıqla yerləşdirilməsinə imkan verir.
- **Çoxsaylı protokolları dəstəkləmə.** Python geniş sayda şəbəkə protokollarını dəstəkləyir, bu da öz növbəsində şəbəkə trafikinin analizi sisteminin OSİ modelinin müxtəlif səviyyələrində paketləri toplamaq, parçalamaq və təhlil etmək üçün uyğun edir. Scapy kimi kitabxanalar paketlərdən hər hansı xüsusi informasiyanı çıxarmağa və mürəkkəb şəbəkə təhlili tapşırıqlarını yerinə yetirməyə imkan verir [19].
- **Məlumatların təhlili və vizuallaşdırılması.** Python NumPy, Pandas, Matplotlib və Plotly kimi məlumatların təhlili və vizuallaşdırılması üçün zəngin kitabxana ekosistemi təklif edir. Bu kitabxanalar bizə şəbəkə trafiki məlumatlarını səmərəli şəkildə manipulyasiya etməyə və təhlil etməyə, daha asan təhlil üçün vizuallaşdırmalar yaratmağa və tapıntılarımızı aydın və cəlbedici şəkildə təqdim etməyə imkan verir [19].
- **İnteqrasiya imkanları.** Python digər dillər və texnologiyalarla mükəmməl inteqrasiya edilə bilir, bu da onu şəbəkə trafikinin analizi sistemini mövcud sistemlərlə inteqrasiya etmək və ya daha böyük layihələrə daxil etmək üçün ideal edir. O, mövcud kod və kitabxanalardan istifadə etməyə imkan verən C/C++, Java və digər proqramlaşdırma dilləri ilə qarşılıqlı əlaqəni dəstəkləyir [19].
- **Genişmiqyaslılıq və performans.** Python performansı və genişlənmə qabiliyyətini artırmaq üçün paralel prosessinq və ya multiprosessinq kimi üsullar təklif edir. Bundan əlavə, Python aşağı səviyyəli kitabxanalar və sistemlərlə asanlıqla interfeys

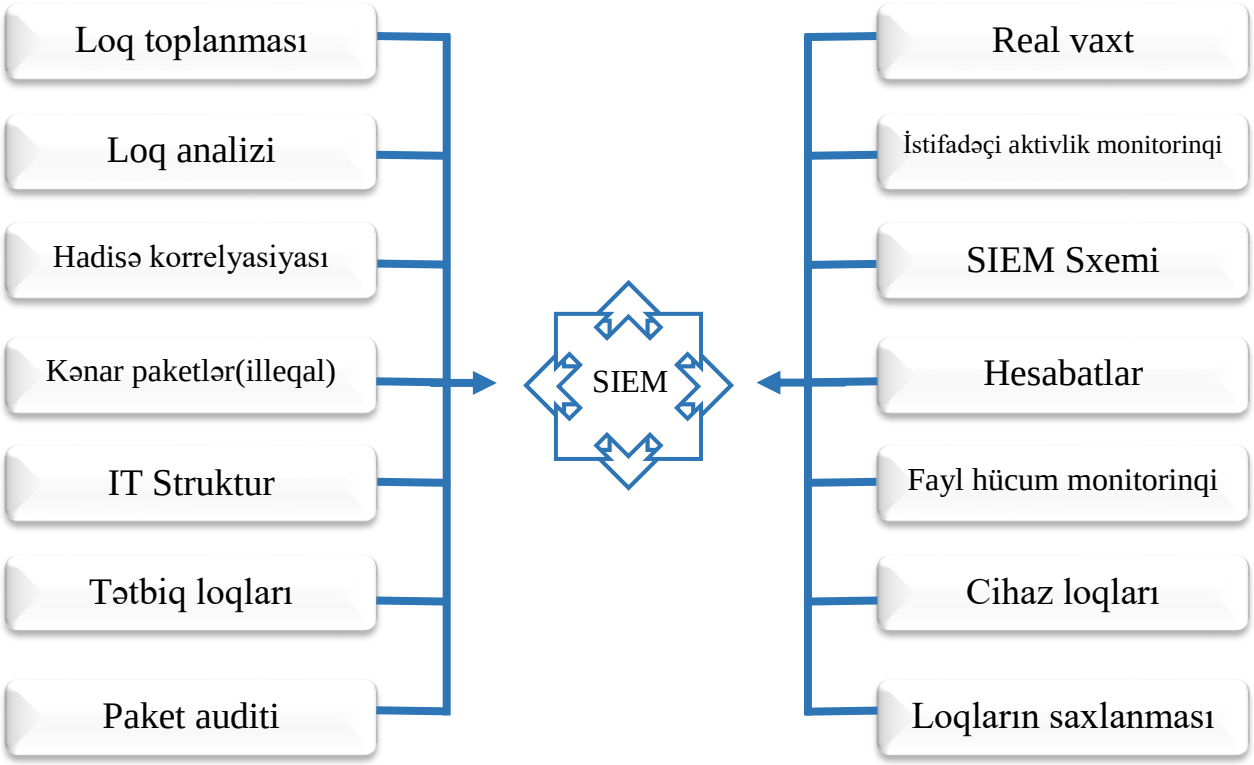
yarada bilər ki, bu da hesablama baxımından intensiv tapşırıqlar üçün optimallaşdırılmış koddan istifadə etməyə imkan verir [19].

Şəbəkə trafikinin analizi sistemində ilkin olaraq loq faylları toplanaraq PCAP formatında saxlanılır. İlkin yoxlama mərhələsində paket qəbul edilmiş şəbəkə cihazına qoşulmanın mümkün olub olmadığı periodik olaraq yoxlanılır. Qoşulma zamanı ilkin olaraq monitorinq tarixi təyin edilir və paketlərin toplanması prosesi başlayır. Əgər şəbəkə trafikinin analizi sisteminin cihazla əlaqəsi kəsilərsə qeyri aktiv zaman aralığı avtomatik olaraq hesablanır və təqdim edilir.Cihazlardan toplanmış paketlər təhlili üçün emalediciyə ötürülür. Emaledici yığılmış məlumat toplusundan təyin etdiyimiz informasiyanı filtrləyərək normallaşdırır. Bundan sonra alınmış nəticə istifadəçi interfeysində əksini tapır. Alınmış nəticələr əlavə olaraq verilənlər bazasında toplanır.Məlumat bazasında toplanmış informasiya əlverişli işlənməsi məqsədilə indekslənir. Şəbəkə trafikinin analizi sistemində indeksləşdirmə səmərəli axtarış və təhlili təmin etmək üçün şəbəkə trafiki məlumatlarının təşkili və strukturlaşdırılması prosesidir. İndeksləşdirmə böyük həcmli şəbəkə trafikinin sorğulanmasını və təhlilini sürətləndirməkdə həlledici rol oynayır və analitiklərə toplanmış məlumat yığınından müvafiq məlumatı tez tapmağa və çıxarmağa imkan verir. İndexlər paketlərdən çıxarılmış məlumat əsasında yaradılır. İndeksləşdirmə üçün seçilmiş sahələr təhlilin tələblərindən və məqsədlərindən asılıdır. Ümumi olaraq indeksləşdirilmiş sahələrə mənbə və təyinat IP ünvanları, port nömrələri, protokollar, vaxtştampları daxildir. Bu indeksləşdirilmiş sahələr təhlil zamanı əsas axtarış parametrləri kimi istifadə edilir. Şəbəkə trafikinin təhlili sistemlərində indeksləşdirmədən istifadə etməklə analitiklər böyük həcmdə şəbəkə trafiki məlumatlarını daha səmərəli şəkildə idarə edə və təhlil edə bilərlər. İndeksləşdirmə müvafiq şəbəkə trafik qeydlərinin sürətli axtarışına və təhlilinə imkan verir, şəbəkə problemlərinin aradan qaldırılması, təhlükəsizlik insidentinin araşdırılması, performans təhlili və uyğunluğun monitorinqi kimi vəzifələri asanlaşdırır.

III FƏSİL. ŞƏBƏKƏ TRAFİKİNİN ANALİZİ SİSTEMİNİN İŞLƏNMƏSİ

3.1. Şəbəkə trafikinin analizi sisteminin arxitekturası

Təhlükəsizlik məlumatı və hadisələrin idarə edilməsi (SIEM) təhlükəsizlik məlumatlılığını artırmağa və təhlükəsizlik təhdidlərini və risklərini müəyyən etməyə kömək edən təhlükəsizlik həllidir. O, müxtəlif təhlükəsizlik cihazlarından məlumat toplayır, bu məlumatları izləyir və təhlil edir və sonra nəticələri ondan istifadə edən biznesə uyğun şəkildə təqdim edir [27].



Şəkil 3.1. Təhlükəsizlik Məlumatı və Hadisə İdarəetmə (SIEM)

SIEM təhlükəsizlik məlumatının idarə edilməsi (SIM) və təhlükəsizlik hadisələrinin idarə edilməsinin (SEM) birləşməsidir. O, təşkilatları potensial hücumlar, informasiya təhlükəsizliyi insidentləri və ya hətta uyğunluq problemləri barədə xəbərdar edir. SIEM həlləri canlı məlumatları və tarixi təhlükəsizlik hadisəsi məlumatlarını çəkməklə təhlükənin aşkarlanması və təhlükəsizlik insidentinin idarə edilməsini gücləndirməklə hadisələrin real vaxt rejimində monitorinqini və təhlilini təklif edir.SIEM-in əsas

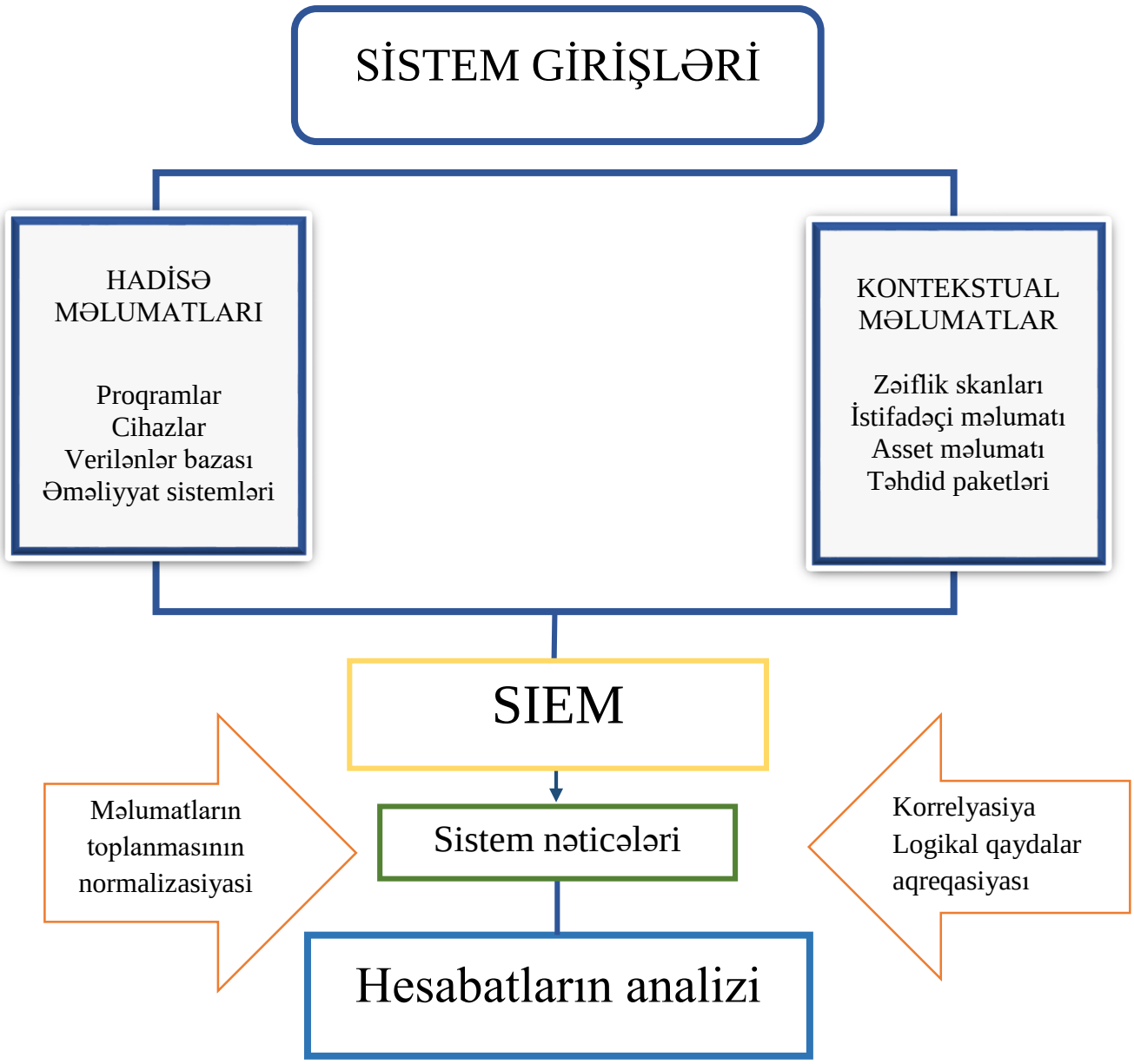
funksionallığına uyğunluq və ya audit məqsədləri üçün təhlükəsizlik məlumatlarının saxlanması, qeydi, toplanması və idarə edilməsi, o cümlədən qeydlər, məlumatların toplanması, təhlükəsizlik monitorinqi və istifadəçi icrasına nəzarət kimi məhdudiyyətlər daxildir.

SIEM necə işləyir?

Təşkilatlar ev kompüterləri kimi sistemlərinin yaratdığı proqramlar, cihazlar və ya hər hansı qeydləri izləmək, idarə etmək və onlarla yenidən qarşılıqlı əlaqə yaratmaq üçün SIEM proqram təminatından istifadə edə bilər. Bu, həssas hərəkətlərə güvənməkdənsə, hər hansı bir təhlükəsizlik problemi baş verməzdən əvvəl onları xəbərdar etmək bacarığına malikdir [24].

SIEM proqramı müxtəlif proqramlar, şəbəkə cihazları və hostlar, şəbəkələr, firewalllar və antivirus hadisələri kimi təhlükəsizlik sistemləri tərəfindən hazırlanmış məlumatların toplanmasına kömək edir. Sonra bütün məlumatları bir mərkəzi yerdə birləşdirir.

Məsələn, SIEM təhlükəni müəyyən etdikdə, xəbərdarlıq yaradır və hücumu müvafiq maraqlı tərəflərə bildirir və qeyd edir. SIEM-in fərdi idarə panelləri də yanlış pozitivlərin araşdırılmasına sərf olunan vaxtı azaltmağa kömək edir.SIEM əsasən təhlükənin aşkarlanması, qarşısının alınması və idarə edilməsinə aiddir. SIEM platformasının məqsədi real vaxt rejimində situasiya məlumatlılığını təmin etməkdir. Bu, təşkilata hücumları vaxtında aşkar etməyə və onlara cavab verməyə imkan verir. Onun arxitekturası SIEM-in düzgün işləməsi üçün mühüm rol oynayır. Əsasən, SIEM işə salınmazdan əvvəl onun quraşdırılmasına və texnoloji aspektlərinə kifayət qədər diqqət yetirilməlidir.Gəlin SIEM arxitekturasının əsas komponentlərini anlayaq və bu sistemin funksiyaları haqqında fikir sahibi olaq.



Şəkil 3.2. Logların idarəedilməsi

SIEM, işçilərin performansı, şirkətin maliyyə vəziyyəti, müştəri modelləri və s. kimi istifadəçi dostu məlumatların geniş spektrini təmin etmək üçün məlumatları ağıllı şəkildə toplayır. Bu komponent məlumatların toplanmasına, məlumatların idarə edilməsinə və əvvəlki məlumatların saxlanmasına cavabdehdir. Yuxarıdakı şəkildə göstərildiyi kimi, SIEM həm hadisə məlumatlarını, həm də quraşdırılmış xidmətlərdən, cihazlardan, şəbəkə protokollarından, saxlama protokollarından və axın protokollarından məlumatlar daxil olmaqla, kontekstual məlumatları toplayır.

Normalizasiya qanunları

Yuxarıdakı rəqəm SIEM-in normallaşdırmanın vacib olduğu hadisə və kontekstual məlumatları giriş kimi qəbul etdiyini də açıq şəkildə göstərir. Burada vacib olan odur ki, hadisə məlumatlarının lazımi təhlükəsizlik anlayışlarına çevrilməsi prosesi toplanmış məlumatlardan uyğun olmayan və ya arzuolunmaz məlumatları süzgəcdən keçirmək və silməklə həyata keçirilə bilər. Burada əsas məqsəd faydasız və lazımsız məlumatlardan xilas olmaq və gələcək təhlil üçün yalnız müvafiq məlumatları saxlamaqdır.

Giriş resursları

SIEM təşkilatında qeydlərin necə yerləşdirildiyi barədə aydın bir konsepsiyaya sahib olmaq üçün daxili jurnalların toplanması, birləşdirilməsi və təhlili prosesinə baxmaq lazımdır. Bu qeydlər şəbəkə proqramları, təhlükəsizlik sistemləri və ya bulud əsaslı sistemlər kimi müxtəlif sistemlərdən çıxarıla bilər. Əsasən, bu komponent məlumat mənbələrinə və harada köçürüldüyünə diqqət yetirir.

SIEM hostinqi və hesabatı

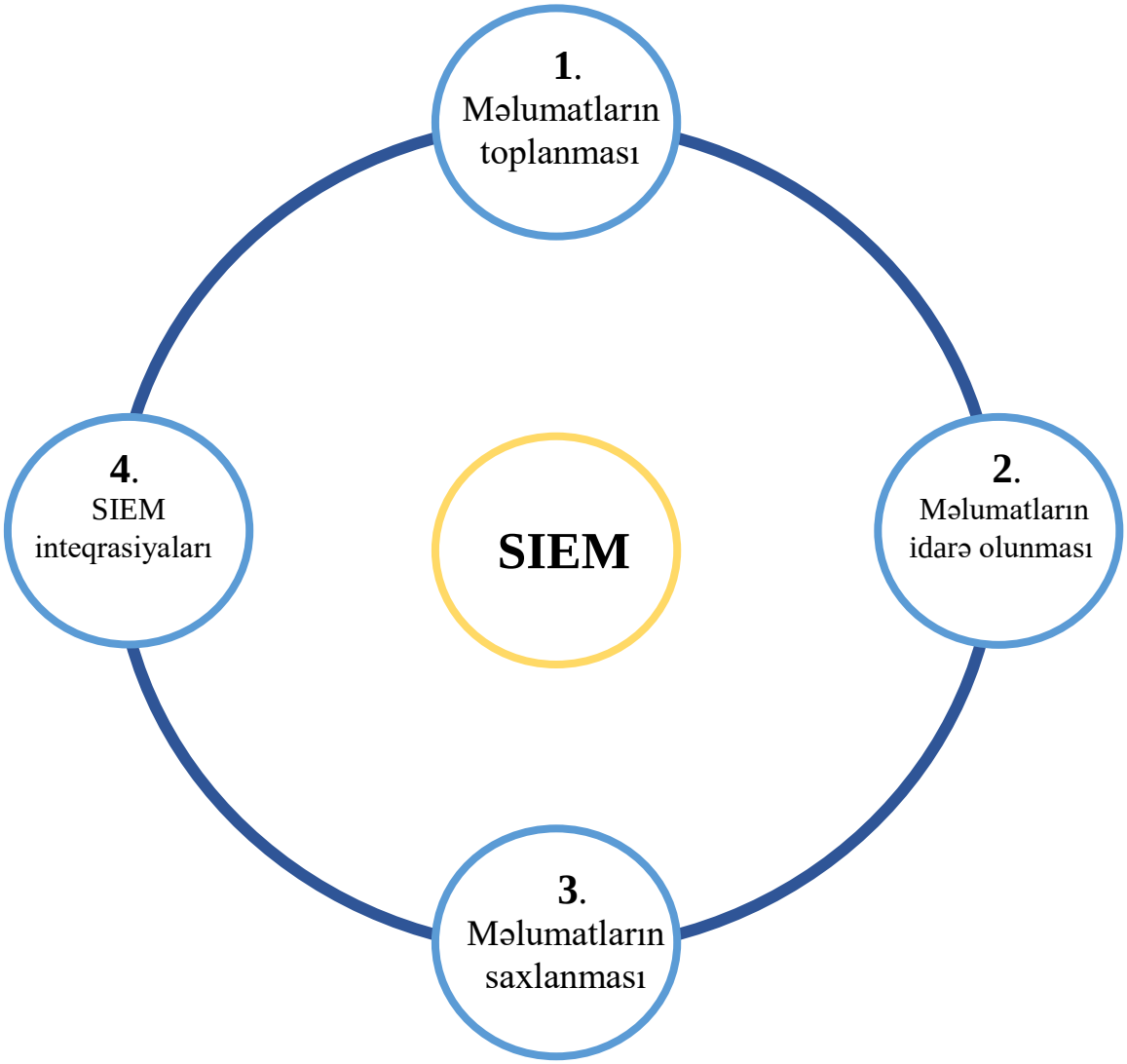
SIEM-i yerləşdirmək üçün öz-özünə host, bulud-host və hibrid-host kimi müxtəlif modellər mövcuddur. SIEM mövcud qeydlər əsasında qeyri-müntəzəm və ya zərərli fəaliyyəti aşkarlayır və hesabat verir.

Real vaxt rejimində monitorinq

Məlumatların şəbəkə təhlükəsizliyinin pozulması bu gün müəssisələrin ən böyük narahatlıqlarından biridir. SIEM real vaxt rejimində monitorinq həllini təmin edir ki, bu da təkcə zərərli hücumları aşkar etməyə kömək etmir, həm də onların mənşəyini müəyyənləşdirir, təhlükələri proqnozlaşdırır və potensial məlumat sızmasının qarşısını almaq üçün tədbirlər görür.Təhlükəsizlik Məlumatı və Hadisələrin İdarə Edilməsinin Əməliyyat Prosesi (SIEM) Təhlükəsizlik məlumatı və insidentlərin idarə edilməsi arxitekturasının ayrılmaz hissəsi effektiv kiber təhlükənin azaldılması strategiyasının yaradılmasının arxasında duran əməliyyat prosesidir. Bununla belə, bütün bu məlumatlar həddən artıq çox ola bilər və onu sadələşdirməyin bir yolu olmalıdır.

Düzgün əməliyyat təlimatları

SIEM-ə tam müəssisə təhlükəsizliyi məlumatlarının idarə edilməsi arxitekturasının fəal hissəsi olmağa imkan verə bilər. SIEM alətləri müxtəlif mənbələrdən toplanmış böyük həcmdə məlumatı götürür və onları biznesi qorumağa kömək edən hərəkətli kəşfiyyatda birləşdirir. SIEM arxitekturası və əməliyyat prosesləri arasında qüsursuz inteqrasiya sistemin işini yaxşılaşdırmaqda mühüm rol oynayır.



Şəkil 3.3. SIEM-in əməliyyat prosesində iştirak edən addımlar

SIEM-in əməliyyat prosesində iştirak edən addımları anlayaq:

1. Məlumatların toplanması

SIEM alətləri təşkilatın İT sistemindəki mənbələrdən qeydləri, müxtəlif növ məlumatları və hadisələri toplayır. SIEM bu cihazlardan məlumatları topladıqdan sonra onu standartlaşdırmaq və asan təhlil və nəzərdən keçirməyə imkan verəcək formatda saxlamağa cavabdehdir.

SIEM məlumatları iki yolla toplaya bilər:

1. Avtomatik məlumatların toplanması: Buraya cihazda quraşdırılmış agent və log fayllarını yaddaşdan (syslog formatı) və ya hadisə axını protokolundan əldə etmək üçün birbaşa keçidlər daxildir, onların hamısını asanlıqla əldə edilə bilən bir yerdə saxlayır ki, təşkilat şəbəkə üzərində tam görünürlük əldə edə bilsin.
2. Aktivlərin xarakteristikası: Təşkilatın informasiya texnologiyaları infrastrukturunu kateqoriyalara ayırarkən, şəbəkəni bəzi əsas oxşarlıqlara və ya funksiyalara malik olan daha kiçik aktiv qruplarına ayırmaq və ya parçalamaq çox vacibdir. İT aktiv kateqoriyalarına bəzi nümunələr cihazlar, şəbəkələr və proqramlardır. Bu, şəbəkə fəaliyyətini izləməyə və yüksək riskli aktivləri müəyyən etməyə kömək edir.

Cədvəl 4. SIEM məlumatlarının tipik mənbələri

Proqramlar	**Təhlükəsizlik Hadisələri**	**Şəbəkə loqları**	**Cihazlar**
Veb proqramlar	Firewall trafiki	Simsiz giriş nöqtələri	Mobil cihazlar
SaaS proqramları	Son nöqtə təhlükəsizliyi (antivirus və antimalware alətləri)	Virtual şəbəkələr	Fərdi noutbuklar və ya masaüstü kompüterlər
Intranet proqramları	Veb tətbiq filtrləri	Routerlər, Sviçlər	İnsanlar arasında paylaşılan iş stansiyaları

2. Məlumatların idarə olunması

Məlumatların toplanması prosesi başa çatdıqdan sonra məlumatların idarə edilməsi prosesi başlayır. Məlumat düzgün saxlandıqda təhlükəsizlik məlumatlarını və hadisələrin idarə edilməsi funksiyalarını tam təkmilləşdirə bilər.

- Saxlama: SIEM alətləri böyük həcmdə məlumat toplamağa qadirdir. Bu məlumatlar yerli, buludda və ya hər ikisində saxlanıla bilər. Ən əsası, hər hansı məlumat itkisinin qarşısını almaq üçün saxlama yerləri möhkəm şəkildə qorunmalıdır.
- Layered: Məlumatların daxil edilməsi müvafiqlik və əhəmiyyətə əsaslanmalıdır. Məsələn, canlı təhlükəsizlik monitorinqi üçün istifadə olunan qaynar məlumatlar yüksək performanslı saxlama altında yerləşdirilməlidir. Digər tərəfdən, dərhal istifadə edilə bilməyən soyuq məlumatlar ucuz saxlama mühitinə yerləşdirilməlidir.
- Təsnifat: Təsnifat SIEM alətlərinin performansını və imkanlarını təkmilləşdirməyə kömək edir. Təhlil, araşdırmalara və kəşflərə imkan vermək üçün məlumatları optimallaşdırmaq və indeksləşdirmək, təhdid risklərini təsnif etmək üçün təhdid kəşfiyyatından istifadə etməklə, yanlış pozitivlərin şansını azaltmaq üçün aşkarlama alqoritmləri ilə işləmək və standartlaşdırılmış məlumat iş axınları üçün siyasətlər qurmaqla həyata keçirilə bilər.

3. Məlumatların saxlanması

Təhlükəsizlik məlumatı və hadisələrin idarə edilməsi alətləri təşkilatda lazımsız yerə məlumatların saxlanmasını azaltmaq üçün müəyyən dərəcədə çeşidləmə və filtrasiya tələb edən böyük həcmdə məlumat daşıyır. Bu, həm də kritik məlumatların qorunmasına kömək edir.

Bundan əlavə, PCI, DSS və HIPAA tərəfindən təmin edilən uyğunluq tələbləri kritik qeydləri 1 ildən 7 ilədək saxlamağa məcbur edir. Məlumatların saxlanması ilə bağlı ağıllı olmaq, gələcək üçün o qədər də tipik olmayan istifadəçi davranışı və təhlükəsizlik nümunələrindəki meylləri təhlil etməyə kömək edə bilər.SIEM jurnal həcmini minimuma endirmək üçün aşağıdakı üsullardan istifadə edir:

- Syslog serverləri: Syslog çevik giriş standartıdır ki, bu da təşkilata standartlaşdırılmış formatda saxlayarkən böyük həcmdə məlumatları saxlamağa imkan verir. Syslog böyük həcmdə məlumatları sıxışdırır və qabaqcıl sorğu alətlərindən istifadə edərək bu qeydləri asanlıqla axtarmağa imkan verir.
- Jurnalın silinməsi cədvəli: SIEM saxlama siyasətinin tələb etdiyindən daha uzun müddət saxlanılan jurnal məlumatlarını avtomatik silir. Giriş fayllarına adətən birbaşa Syslog formatında yaddaşdan daxil olmaq olar.
- Qeydiyyatın filtrasiyası: Təşkilatın SIEM proqramı uyğunluq tələblərinə cavab vermək və ya məhkəmə-tibbi analiz məqsədləri üçün həmişə lazım olmayan qeydləri süzgəcdən keçirə bilər. SIEM administratorları logları mənbə, növ, vaxt və ya digər müəyyən edilmiş qaydalara görə süzgəcdən keçirə bilərlər. Həmçinin, log filtrindən istifadə emal olunan məlumatların miqdarını əhəmiyyətli dərəcədə azalda bilər.

Hər hadisə üçün saxlanılan məlumatların miqdarını azaltmaq üçün qeydlər ümumiləşdirilə bilər, lakin hadisələrin sayı, unikal IP-lər və s. üçün ümumiləşdirilməlidir. Bu kimi vacib bitləri saxlayır

4. SIEM inteqrasiyaları

Təhlükəsizlik məlumatı və insidentlərin idarə edilməsi proseslərini digər kibertəhlükəsizlik alətləri ilə birləşdirərək, sinerji bütün şirkət üçün daha yüksək qorunma təmin edir. Bunun səbəbi, təhlükəsizlik təhdidlərini aşkar edərkən, onların qarşısının alınmasında və baş verdikləri zaman ehtiva edən müxtəlif proqram alətləri ilə inteqrasiya edən SIEM tərəfindən idarə olunan platformadan istifadə etməsidir.

Bu həllin ən yaxşı tərəfi, məlumatlarının SIEM platformasında təhlükəsiz şəkildə yaradıla bildiyi müddətcə komandanın hansı proqramdan istifadə edəcəyini seçməməsidir. SIEM inteqrasiyası üçün bir neçə varianta misal olaraq şəxsiyyət və giriş idarəetmə proqramı, yamaq idarəetmə alətləri, bulud təhlükəsizliyi alətləri və üçüncü tərəf risk idarəetmə alətləri daxildir.

3.2. Şəbəkə trafikində paketlər arasında vaxt intervalının təhlili

Hansı alətdən istifadə etməyinizdən asılı olmayaraq, şəbəkə performans göstəricilərinin (məsələn, gecikmə, paket itkisi və ya ötürmə qabiliyyəti) necə hesablana biləcəyinin əsaslarını başa düşmək vacibdir. Bu hesablama Wireshark və ya hər hansı digər paket analizatoru ilə əl ilə həyata keçirilə bilər və ya seçdiyiniz şəbəkə performansının idarə edilməsi (NPM) həlli ilə avtomatlaşdırıla bilər. Tətbiqlərin əsas hissəsi TCP protokolları üzərində işləyir. TCP şəbəkə performansını qiymətləndirmək üçün istifadə edilə bilən müəyyən sayda mexanizmlər təklif edir.

Aşağıdakı diaqram TCP sessiyasında atılan ardıcıl addımları (bir seansda bayraqların olması ilə xarakterizə olunur) və müxtəlif əsas şəbəkə performans göstəricilərinə uyğun gələn vaxt intervallarını izah edir:

Şəbəkədə bandwith adında termin vardır ki,hansı Azəraycan dilinə tərcümədə -Bant genişliyi olaraq tərcümə olunur.Bant genişliyi müəyyən bir müddət ərzində simsiz və ya simli rabitə kanalı vasitəsilə ötürə biləcəyimiz maksimum məlumat miqdarını təmsil edir. Eynilə, şəbəkə ötürmə qabiliyyəti şəbəkədə vaxt vahidinə ötürülən məlumatların faktiki miqdarıdır. Buna görə də, faktiki şəbəkə ötürmə qabiliyyəti həmişə şəbəkə bant genişliyindən azdır. Ümumiyyətlə, bir keçid əhəmiyyətli bant genişliyinə malikdirsə, vahid başına məlumat ötürülməsi yüksək olacaqdır. Bundan əlavə, bant genişliyi şəbəkə sürəti ilə eyni deyil. Buna görə də, şəbəkə sürətini məlumat ötürülməsini emal etdiyimiz sürət kimi təyin edə bilərik. Digər tərəfdən, şəbəkə bant genişliyi rabitə kanalının tutumu ilə bağlıdır. Rabitə bağlantısı trafiklə dolu olduqda, onu düzəltməyin ən asan yolu şəbəkə bant genişliyini artırmaqdır. Bununla belə, şəbəkə administratorları və mühəndisləri şəbəkədə bant genişliyi istifadəsini optimallaşdırmaq və monitorinq etmək üçün məsuliyyət daşıyırlar. Şəbəkə bant genişliyi məhdud resursdur.

Buna görə də, bu, əlaqə üçün istifadə olunan yerlərdən və şəbəkə cihazlarından asılıdır. Bundan əlavə, biz şəbəkə bant genişliyini bit, kilobit və meqabitlə ölçürük. 4K video qabiliyyətinə malik televizorlar və video konfrans proqramları kimi müasir cihazlar yüksək şəbəkə bant genişliyindən istifadə edir.

Kompüter şəbəkələrindəki mənbədən təyinat yerinə çatmaq üçün paketin çəkdiyi vaxta təsir edən müxtəlif amillər var. Bundan əlavə, paket zamanı gecikmələr müxtəlif amillər, o cümlədən paket itkisi, şifrələmə, məsafə səbəbindən baş verir. Emal gecikməsi, növbə gecikməsi, ötürmə gecikməsi və yayılma gecikməsi daxil olmaqla, şəbəkələşmədə müxtəlif gecikmələr var:

Bağlantı vaxtı - bu metrik ilkin TCP sessiyasında SYN və ACK arasındakı vaxt intervalına uyğundur: SYN, SYNACK və ACK paketlərindən ibarət 3 tərəfli əl sıxma prosesi başlıca göstəricidir [25].

Qoşulma vaxtı şəbəkə gecikməsinin ilkin göstəricisidir, çünki bu paketlər sistem və server müştəriləri tərəfindən prioritet olaraq idarə olunur.

Gediş-gəliş vaxtı – təqdimetmə mexanizmi həm də tutma nöqtənizdən (müştəri tərəfində, ortada və ya server tərəfində yerləşə bilər) müştəri və ya serverə gedən şəbəkənin gecikmə müddətini ölçməyə kömək edə bilər. Gediş-dönüş vaxtı faydalı yükü olan paket və onun müvafiq təsdiq paketi arasındakı vaxt intervalı kimi ölçülür. Gediş-dönüş vaxtı, gediş-gəliş şəbəkəsinin gecikməsinin yaxşı göstəricisidir.

Paket İtki Göstəriciləri - təyinat yerinə çatmamış paketi necə müəyyən etmək olar?

Bu kimi hallarda loq fayllarda itkiyə dair heç bir yararlı məlumat tapmaq mümkün deyil.İki üsul mövcuddur ya hər iki tərəfdən trafiki çəkirsiniz və hansı paketlərin çatışmadığına görə paketi müqayisə edirsiniz, ya da təkrar ötürmələr kimi paket itkisi göstəricilərinə etibar edirsiniz.

Təkrar ötürmələr paket qarşı tərəfə çatmadığı və qəbul edilmədiyi və ya təsdiqin ilkin göndərənə çatması çox vaxt apardığı zaman baş verir. Sadalanan hər bir hal şəbəkə ötürülməsinin keyfiyyətinə ciddi təsir göstərir.

Yenidən ötürmə dərəcələri - bu göstərici göndərilən ilkin paketlərin sayı ilə müqayisədə təkrar ötürülən paketlərin sayına uyğundur. Bu sürət paket itkisinin aydın göstəricisidir. Yenidən ötürülmə gecikməsi - bu metrik ilkin göndərilən paketlə ilk təsdiqlənmiş təkrar ötürmə arasındakı vaxt intervalına uyğundur. Məlumatların ötürülməsində təkrar ötürülmə/paket itkisi səbəbindən itirilmiş vaxtı təmsil edir [25].

Tranzaksiya gecikməsi D_P. marşrutlaşdırıcılar tərəfindən paket başlıqlarının işlənməsi nəticəsində yaranan gecikmədir. Routerlərdən gecikmə bit xətalarının yoxlanılması, paketin göndərilməsi üçün növbəti məlumatın tapılması və şifrələmə nəticəsində yaranır. Paketin qarşılaşa biləcəyi gecikmənin ikinci növü növbə gecikməsidir D_Q. İstinad növbələrində sərf olunan vaxt. Növbə gecikməsi məlumatların marşrutlaşdırıcının buferində gözlədiyi vaxtın miqdarıdır. Şəbəkə sıx olarsa, həddindən artıq növbə gecikməsi ola bilər.

Transmissiya gecikməsi D_T bütün mövcud məlumatların ötürücü mühitdə və ya kabeldə ötürülməsi vaxtıdır. Bitlərin sayını $\{N_B\}$ötürmə sürətinə $\{T_R\}$ bölmək yolu ilə ötürmə gecikməsini (saniyələrlə) hesablaya bilərik:

$$D_T = \frac{\{N_B\}}{\{T_R\}}$$

Paketin məlumat ötürülməsi zamanı qarşılaşa biləcəyi digər gecikmə yayılma gecikməsidir D_{PR}). Bu, bir paketin ötürmə mühitindən keçməsi üçün lazım olan vaxtdır. Bu, paketin məsafəsindən (D) və sürətindən (S) asılıdır. Beləliklə, yayılma gecikməsi:

$$D_{PR} = \frac{D}{S}$$

Şəbəkə gecikməsi N_L məlumat ötürülməsi zamanı paketin qarşılaşa biləcəyi bütün mümkün gecikmələrin cəmidir. Biz adətən şəbəkə gecikməsini gediş-gəliş vaxtı (RTT) kimi ifadə edirik və onu millisaniyələrlə (ms) ölçürük. Şəbəkə gecikməsinə emal, növbə, ötürmə və yayılma gecikmələri daxildir. Şəbəkə gecikməsini hesablamaq üçün formula qeyt etdiyim kimidir :

$$N_L = \ D_P + D_Q + D_T + D_{PR}$$

Şəbəkələrdən və proqramlardan asılı olaraq məqbul şəbəkə gecikməsi dəyişir. Məsələn, video konfranslar, VoIP zəngləri, video axını kimi proqramların səmərəli işləməsi üçün aşağı şəbəkə gecikməsi olmalıdır. Yüksək şəbəkə gecikməsi bu proqramların işinə əhəmiyyətli dərəcədə təsir göstərə bilər. Digər tərəfdən, e-poçt kimi proqramlar var ki, biz tətbiqin işinə çox təsir etmədən yüksək gecikməyə icazə verə bilərik.

Gediş-gəliş vaxtı (RTT) mesajın mənbədən təyinat yerinə çatması və sonra təyinat yerindən mənbəyə qayıtması üçün tələb olunan vaxtdır. Şəbəkə ping vaxtı gediş-gəliş vaxtı ilə çox oxşardır. Gediş-gəliş vaxtı şəbəkə gecikməsi ilə bağlıdır. Hər iki istiqamətdə asimmetrik gecikmələr ola biləcəyi üçün bu, şəbəkə gecikməsindən iki dəfə çox deyil. Həmçinin təyinat yerində əlavə emal vaxtı gediş-gəliş vaxtına daxildir. Biz şəbəkə ötürmə qabiliyyətini TP TCP qəbul pəncərəsindən (W) və gecikmə ilə əlaqəli şəbəkənin gediş-gəliş vaxtından (RTT) istifadə edərək hesablaya bilərik:

$$TP \leq \frac{W}{RTT}$$

Hesablama nümunələri:

Gecikmə və bant genişliyi məlumatından istifadə edərək paket vaxtını hesablayaq. Ev sahibi və keçidi nəzərdən keçirin. Fərz edək ki, ötürmə sürəti 1 Mbit/s və yayılma gecikməsi 70 ms-dir. Sıfır növbə və emal gecikməsini nəzərə alsaq, 1KB məlumat paketini ötürmək nə qədər vaxt aparacaq? Gəlin öyrənək:

1 Mbps ötürülmə
70 ms gecikmə

Burada əvvəllər müzakirə edilən şəbəkə gecikmə N_L düsturundan istifadə edə bilərik:

$$N_L = D_T + D_{PR} + D_P + D_Q$$

Bundan əlavə, biz əvvəlki bölmədə ötürmə gecikməsi və yayılma gecikməsi düsturunu müzakirə etdik. Beləliklə, şəbəkə gecikmə N_L düsturunu yenidən nəzərdən keçirək:

$$N_L = \frac{N_B}{T_R} + \frac{D}{S} + D_P + D_Q$$

Verilənləri yerinə qoyub hesablayaq :

$$N_L = \frac{N_B}{T_R} + \frac{D}{S} + D_P + D_Q = \frac{1000*8}{1000000} + \frac{70}{1000} + 0 + 0 = 0.0008 + 0.07 = 0.078sec\text{=}58\text{ms}$$

Beləliklə hamının yazılarda,internet paketlərində gördüyü ms-in nə olduğunu açıqladıq. Host və keçid arasında 1 KB məlumat paketlərini ötürmək üçün ümumi paket ötürmə vaxtı (\mathbf{T}) 78 ms olacaq.

Məhsuldarlığa əsaslanan paket vaxtının hesablanması Məhsuldarlıq Ötürmə qabiliyyəti irəli və geri göndərilən məlumatların miqdarına uyğundur. Müştəridən serverə və əksinə göndərilən baytları saymaq ötürmə qabiliyyətini qiymətləndirmək üçün kifayətdir. Məlumat ötürmə vaxtı Bu metrik sorğunun müştəridən serverə və ya serverdən müştəriyə cavabın ötürülməsi üçün tələb olunan vaxta uyğundur. Bu dəyər hər bir istifadəçinin yaşadığı ümumi cavab müddətinə güclü təsir göstərir. Serverin emal vaxtı, serverin cavab müddəti metrik sorğunun sonuncu paketi ilə cavabın ilk paketi arasındakı vaxt intervalına uyğundur. Bu, hər bir TCP əməliyyatı üçün server emal vaxtını təmsil edir.

IP bağlantısında faktiki ötürmə qabiliyyətinin hesablanmasına praktik yanaşmanı müzakirə edək. IP bağlantısı məlumat ötürmə sürətini yavaşlatan müxtəlif amillər üçün hesablanmış dəyərləri tənzimləyir. Buna görə də, əvvəllər müzakirə etdiyimiz məlumatların ötürülməsi zamanı müxtəlif gecikmələri nəzərdən keçirəcəyik. Qoşulma sürəti nəzərə alınmaqla müəyyən miqdarda məlumat ötürmək üçün vaxtın hesablanması üçün detalları müzakirə edək. Əvvəlcə minimum nəzəri vaxtı əldə etmək üçün ötürüləcək bitlərin sayını keçid sürətinə bölmək lazımdır. TCP kodlaşdırma əlavə xərcləri üçün təxminən 40% əlavə edirik. Bundan əlavə, bu nümunədə şəbəkə sıxlığının 22,5%-ni əlavə edirik. Güman edirik ki, məlumat ötürülməsi şifrələnmişdir. Buna görə 12,5% əməliyyat gecikməsi əlavə edirik.

İndi sual budur ki, 70 GB məlumat ötürülməsi üçün 20 Mbps bağlantıdan istifadə edərək A nöqtəsi ilə B nöqtəsi arasında məlumat ötürmək nə qədər vaxt aparacaq? Birincisi, heç bir əlavə xərci nəzərə almadan paketin ümumi ötürmə müddətini (T) hesablayaq:

$$T = \frac{(70 * 8 * 10^9)}{20 * 10^6} = \frac{560 * 1000}{20} = 28000\ sec$$

TCP yükü 40%-ə təyin edildikdən sonra emal müddəti:

$$T = 28000 * 1.4 = 39200\ sec$$

Sonra şəbəkə sıxlığının 22,5%-ni əlavə etdik. Beləliklə, trafik üçün əlavə 22,5% təyin etdikdən sonra paketin köçürmə vaxtı:

$$T = 39200 * 1.225 = 48020\ sec$$

Şifrələnmiş məlumat üçün 12,5% təyin etdikdən sonra paket ötürmə müddəti:

$$T = 48020 * 1.225 = 54022.5\ sec$$

Beləliklə, ümumi vaxt: $T = 54022.5\,\text{sec} = 900.375\ mins = 15\ saat$

Beləliklə A nöqtəsindən B nöqtəsinə 20 Mbps sürəti ilə 70Gb həcmli faylı 15 saata göndərə bilərik.

3.3 Şəbəkə trafikinin analizi sisteminin yaradılması və eksperimentin keçirilməsi

Şəbəkə trafikinin analizi sistemini yaradarkən, yəni SIEM topologiyasını qurarkən ilk öncə nəzərə almalı olduğumuz məqamlardan biri SIEM-in hansı mühitdə işləyəcəyidir. Mühit dedikdə ortalama paket axını miqdarı,internet şəbəkəsinin gücü,növü və bu kimi xarakteristikalardır. Növbəti mərhələdə hansı ƏS üzərində konfiqurasiya aparılacağı qərarlaşdırılmalıdır. Biz hibrid şəkildə həm Linux həm də Windows əməliyyat sistemlərində paralel olaraq konfiqurasiyalar aparmışıq. İndi isə Python dilində daha inkişaf etmiş funksiyalar istifadə etmək üçün bizə Kitabxana(Library) adlanan lib fayllar lazımdır. SIEM strukturunu qurarkən bizə lazım olacaq kitabxanalar : Flask, Socket, Request, Time, Scapy, Fpdf, Pandas, SSL, DateTime, Pickle, Smtplib Pythonda library yükləmək üçün aşağıda göstərilən terminal əmrindən istifadə olunur [21].

```
PS C:\Users\ibrahimliqr\Downloads\file\file> pip install pandas
Collecting pandas
  Downloading pandas-2.0.1-cp311-cp311-win_amd64.whl (10.6 MB)
     ---------------------------------------- 10.6/10.6 MB 6.1 MB/s eta 0:00:00
Collecting python-dateutil>=2.8.2 (from pandas)
  Downloading python_dateutil-2.8.2-py2.py3-none-any.whl (247 kB)
     ---------------------------------------- 247.7/247.7 kB 3.0 MB/s eta 0:00:00
Collecting pytz>=2020.1 (from pandas)
  Downloading pytz-2023.3-py2.py3-none-any.whl (502 kB)
     ---------------------------------------- 502.3/502.3 kB 4.5 MB/s eta 0:00:00
Collecting tzdata>=2022.1 (from pandas)
  Downloading tzdata-2023.3-py2.py3-none-any.whl (341 kB)
     ---------------------------------------- 341.8/341.8 kB 4.3 MB/s eta 0:00:00
Collecting numpy>=1.21.0 (from pandas)
  Downloading numpy-1.24.3-cp311-cp311-win_amd64.whl (14.8 MB)
     ---------------------------------------- 14.8/14.8 MB 6.4 MB/s eta 0:00:00
Collecting six>=1.5 (from python-dateutil>=2.8.2->pandas)
  Downloading six-1.16.0-py2.py3-none-any.whl (11 kB)
Installing collected packages: pytz, tzdata, six, numpy, python-dateutil, pandas
```

Şəkil 3.4 Library fayllarının yüklənməsi

Göstərilən üsulla bütün lazım olan kitabxanaları yüklədikdən sonra, import əmri ilə kitabxanalardan bizə lazım olan funksiyaları import(idxal) etməliyik.

```
from scapy.all import sniff
from fpdf import FPDF
import pandas as pd
```

Şəkil 3.5 Funksiyaların kitabxanadan import edilməsi

Yaratdığımız şəbəkə monitorinqi alətində şəbəkənin public internetsiz qalma vaxtı, açıq portlar, paketlər arası intervalın təyini, gələn paketlərin və muraciət olunan ip-lərin leqallıq yoxlanışı, yaranan problemlər zaman mail və mobil nömrəyə mesajın göndərilməsi kimi funksiyalar yer alacaqdır.

Portları skanlamaq, yəni açıq portları təyin etmək üçün ilk öncə “port_scanner” adı altında funksiya təyin edirik. Portların sayları ən sadə serverdə və ya evdə işlətdiyimiz kompüterdə belə minlərlə ola bilər,məhz buna görə də,skanlama üçün seçilən intervalda yoxlama funksionallığı tərəfimizdən əlavə edilib.

```python
@app.route('/port_scanner', methods=['POST'])
def port_scanner():
    target = request.form['target']
    start_port = int(request.form['start_port'])
    end_port = int(request.form['end_port'])

    try:
        ip = socket.gethostbyname(target)
    except socket.gaierror:
        return render_template('index.html', error="Invalid target")

    open_ports = []
    for port in range(start_port, end_port + 1):
        try:
            sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
            result_code = sock.connect_ex((ip, port))
            if result_code == 0:
                open_ports.append(port)
            sock.close()
        except socket.error:
            return render_template('index.html', error="Qeyd edilən ip ünvanına qoşulmaq mümkün deyil")

    return render_template('port_scanner.html', target=target, open_ports=open_ports)
```

Şəkil 3.6 Port skanlama funksiyası

İstifadə müddəti bitmiş, yeni versiyaya yüksəldilməmiş hər bir avadanlığın əməliyyat sistemi, server hətta mobil cihazlar belə təhlükəsizlik protokollarında boşluqlar kimi qeydə alınır, çünki hər bir yenilənmə zamanı təhlükəsizlik səviyyəsi 1 pillə yuxarı qaldırılır. Bu kimi halların qarşısının alınması üçün daimi nəzarət mütləqdir,lakin bunu əl ilə ayrı-ayrılıqda yoxlamaq həm vaxt itkisinə həm də çoxsaylı risk insidentlərinə səbəb ola bilər. Şəbəkə monitorinq alətimiz bunu avtomatik olaraq həyata keçirir və nəticələri bizə report şəklində təqdim etmək qabiliyyətinə malikdir. Təhlükəsizlik yoxlanışı funksiyasının quruluşu aşağıdakı şəkildə göstərilmişdir [19].

```python
@app.route('/vulnerability_check', methods=['POST'])
def vulnerability_check():
    target = request.form['target']

    # Təhlükəsizlik yoxlanışları istəyimizdən asılı olaraq digər mənbələr vasitəsilə də yoxlanıla bilər.

    try:
        response = requests.get(f"http://{target}/", timeout=5)
        if response.status_code == 200 and "Köhnə əməliyyat sistemli server" in response.text:
            vulnerability_result = f"{target} is running an outdated web server!"
        else:
            vulnerability_result = f"{target} qeyd edilən ip təhlükəsizdir."
    except requests.exceptions.RequestException:
        return render_template('index.html', error=f"Qeyd edilən : {target} ünvanına qoşulmaq mümkün olmadı. Yoxlanış baş tutmadı")

    return render_template('vulnerability_check.html', target=target, result=vulnerability_result)
```

Şəkil 3.7 Təhlükəsizlik yoxlanışı

Paketlər arasında vaxt intervalının təyini dedikdə ilk baxışdan insanda çaşqınlıq yaradır,lakin informasiya təhlükəsizliyi üçün önəmli mövzulardan biridir. Paketlər arası vaxt intervalının təyini bizə hücum aktının,virusun, serverdə olan kənar şəxsin hərəkətlərini bəlli edir. Əməliyyat sistemlərində arxa fonda işləyən servislər adətən standart qanunauyğunluqla testlər, yoxlamalar keçirir və EV-də qeydlər aparırlar. Misal üçün hamının istifadə etdiyi "ZOOM" proqramı istifadə olunarkən 1 saniyədə 15 internet paketi göndərərək internet şəbəkəsinə qoşulub-qoşulmadığını yoxlayır. Bunu hər-hansı virus da edə bilər, lakin paketlərin arasındakı vaxt intervalı fərqli olacağından prosesin digər mənbədən icra olunduğu üzə çıxacaq. Paketləri analiz etmək üçün müraciət edilən nöqtənin ip ünvanını proqramda qeyd etməyimiz kifayətdir. Paketlərin analizi funk-siyasının kod nümunəsi aşağıdakı şəkildə göstərilmişdir.

```python
@app.route('/packet_analysis')
def packet_analysis():
    global previous_time
    previous_time = None
    sniff(prn=analyze_packet_time_interval, count=10)
    return "Paket analizi sonlanmışdır"

def analyze_packet_time_interval(packet):
    global previous_time
    if previous_time is None:
        previous_time = time.time()
        return
    current_time = time.time()
    time_interval = current_time - previous_time
    print(f"Paketlər arasında vaxt intervalı: {time_interval} saniyədir")
    previous_time = current_time

    return render_template('packet_analysis.html', time_interval=time_interval)
```

Şəkil 3.8 İnternet paketlərinin analizi

Bu hissəyə qədər serverlərin qoşulu olduğu şəbəkədə nəzarəti həyata keçirməyə müvəffəq olduq. Lakin bu ən yaxşı hal ssenarisidir. Yazdığımız kod hissəsində ilişmə olarsa və ya hansısa fiziki problemə görə qoşulma baş tutmazsa biz bunu yalnız terminal hissəsindən görə bilərik. Terminal hissəsinə nəzarət isə adi proqram istifadəçiləri tərəfindən nəzər yetirilməyən bir hissədir, məhz buna görə də, elektron poçt və ya hansısa

mesajlaşma proqramı vasitəsilə məlumat almaq ,yarana biləcək problemlərə vaxtında cavab verməyimizə köməklik göstərəcəkdir. Bu tipli SIEM topologiyalarında adətən SMS mesajlarından istifadə olunur, lakin biz burada SMS yox “Telegram” və elektron poçt olaraq “Gmail” platformasından istifadə edəcəyik. Çünki hal-hazırda test apardığımız resurslar SMS funksionallığından istifadə etməyə imkan vermir.

Mail göndərilməsi üçün mail serverə ehtiyac duyulur, lakin bizim resurslar limitli olduğuna görə gmail platformasında olan mail ünvanından istifadə edirik. Elektron poçt vasitəsilə məktub göndərmək üçün “smtplib” kitabxanasından istifadə edirik və kod bloku şəkildəki kimidir.

```
from telethon.sync import TelegramClient
from telethon.tl.types import InputPeerUser, InputPeerChannel
from telethon import TelegramClient, sync, events

api_id = 'API_idin'  #
api_hash = 'API_hashing'
token = 'Tokende bot'
message = "Mesaj gonderilir..."
phone = '+994517774139'
client = TelegramClient('sessiya', api_idin, api_hashing)

client.connect()

if not client.is_user_authorized():
    client.send_code_request(phone)

    client.sign_in(phone, input('Kodu daxil edin: '))
try:


    receiver = InputPeerUser('user_id', 'user_hash')


    client.send_message(receiverin, messagean, parse_mode='html')
except Exception as e:

 print(e);

client.disconnect()
```

Şəkil 3.9 İnternet paketlərinin analizi

Eyni qayda ilə API-lərdən istifadə edərək Telegram vasitəsilə mesaj göndərə bilərik, burada Telegramın python üçün hazırladığı API-lərdən istifadə edirik. Konfiqurasiya aşağıda göstərildiyi kimidir.

Eyni qayda ilə API-lərdən istifadə edərək Telegram vasitəsilə mesaj göndərə bilər.

```
def email_alert(subject, body, to):

    msg = EmailMessage()
    msg.set_content(body)

    # UPDATE THESE LINES TO YOUR INFO
    gmail_user = 'qoshqar.ibrahimli@gmail.com'
    gmail_password = 'parolum '
    msg['Subject'] = subject
    msg['From'] = "qoshqar.ibrahimli@gmail.com"
    msg['To'] = to

    to = 'qoshqar.core@gmail.com'


    # Buranı öz mail serverimiz ilə dəyişə bilərik.
    s = smtplib.SMTP('smtp.gmail.com', 587)
    s.ehlo()
    s.starttls()
    s.login(gmail_user, gmail_password)
    s.send_message(msg)
    s.quit()
```

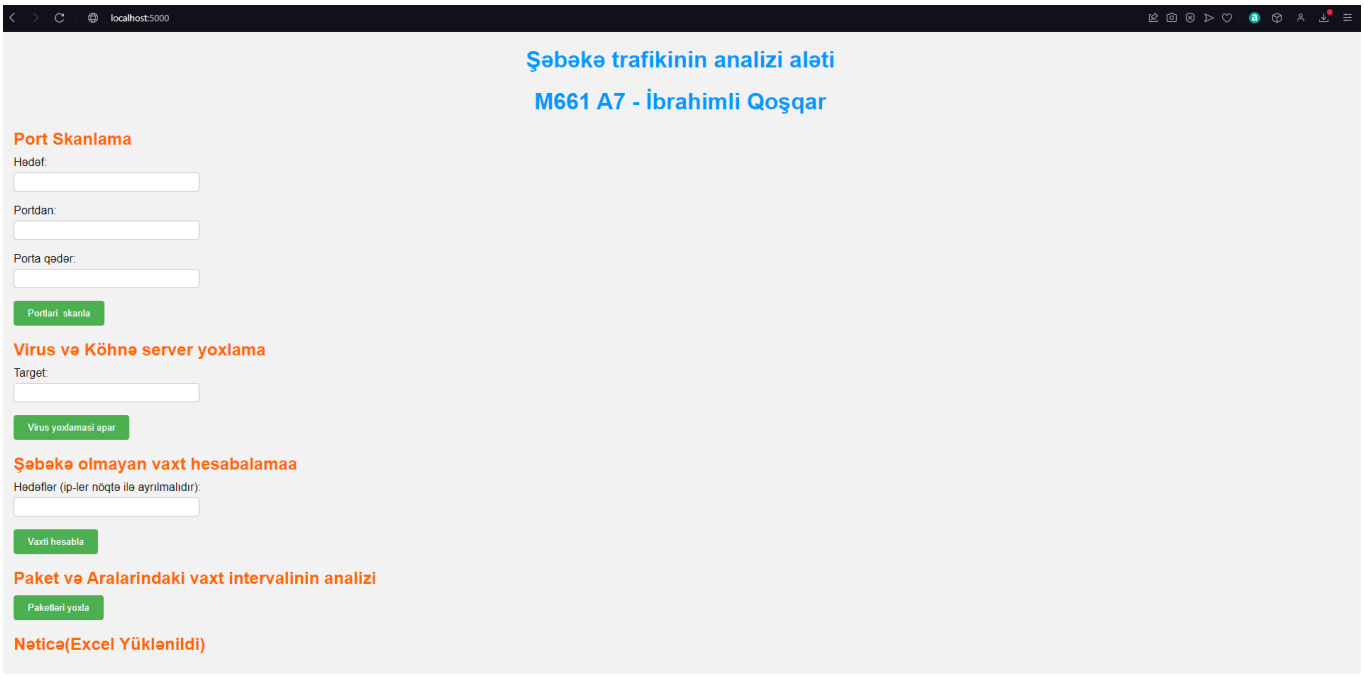
Şəkil 3.10 Telegram ilə mesaj göndərmə bloku

İndi isə yazdığım şəbəkə monitorinq alətinin test mərhələsinə keçid edə bilərik.

Test etmək üçün əvvəlcə Python dilində yazdığımız proqramı Visual Studio Code mühitində işə salırıq.

```
PS C:\Users\ibrahimliqr\Downloads\file\file> & "C:/Program Files (x86)/Microsoft VS Code/python/python.exe" c:/Users/ibrahimliqr/Downloads/file/file/scan01.py
WARNING: No libpcap provider available ! pcap won't be used
 * Serving Flask app 'scan01'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
```

Şəkildən də göründüyü kimi proqramımız problemsiz olaraq emal olundu. Proqramda əlçatanlığın əldə olunması üçün sadə HTML kodları ilə həm də veb-interfeys yaradılmışdır. Veb-interfeys lokal şəbəkə üzərində 5000 portu ilə paylaşılmışdır.



Testləri həyata keçirərkən heçbir işləyən sistemə zərər verməmək üçün virtual serverlər və ƏS-lər istifadə olunmuşdur. Virtual serverler VmWare üzərində hazır ISO-lar vasitəsilə yaradılmış və Bridge mode vasitəsilə lokal şəbəkəyə qoşulmuşdur. Port skanlama və subdomain testləri zərər verməyən test növü olduğundan bunu universitetimizin saytı üzərində test edə bilərik.

Hədəf nöqtəsi hissəsinə “aztu.edu.az” qeyd etdikdən sonra Portları skanlama düyməsini click edirik və artıq excel formasında reportumuz kompüterimə yüklənir. Alınan excelin nəticəsi aşağıdakı kimidir :

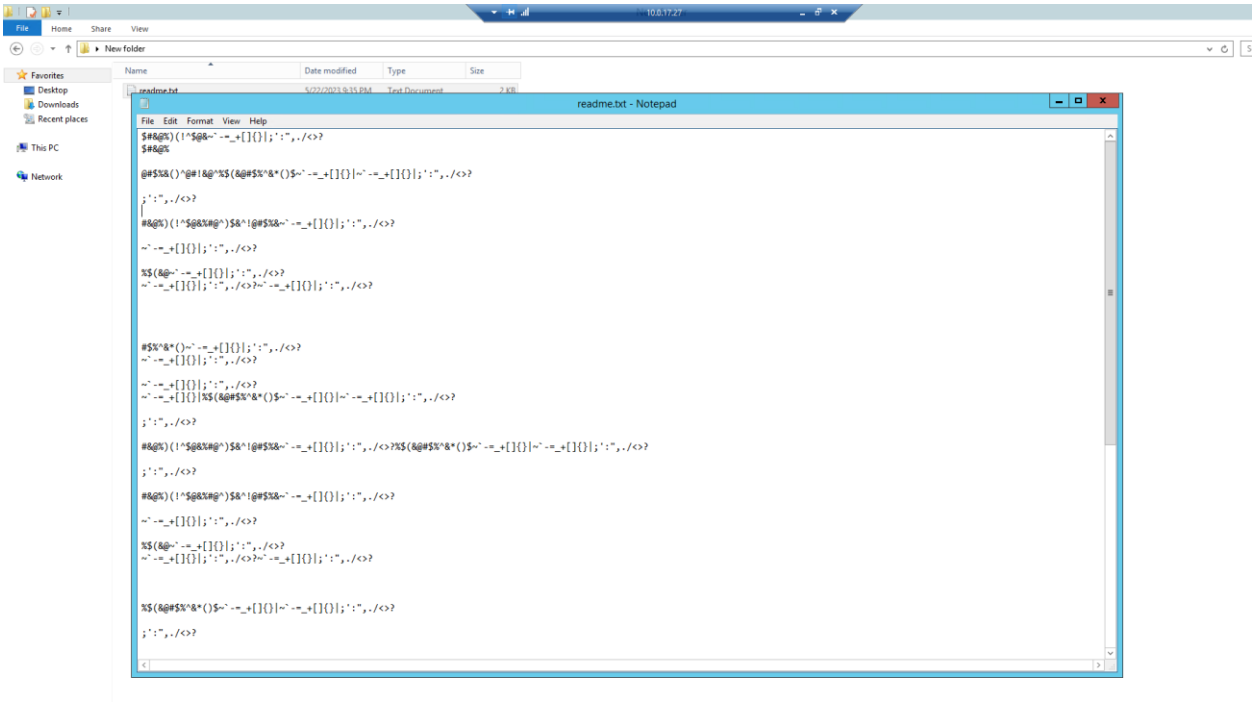
	A	B	C	D	E	F	G	H
1								
2	Result by http://localhost:5000 auth : Goshgar Ibrahimli							
3	Domain	Ports						
4	443	Closed						
5	80	Open						
6	55	Open						
7								
8								

Aztu.edu.az veb-saytının yoxlanışı zamanı 55,80,443 portları yoxlanıldı.

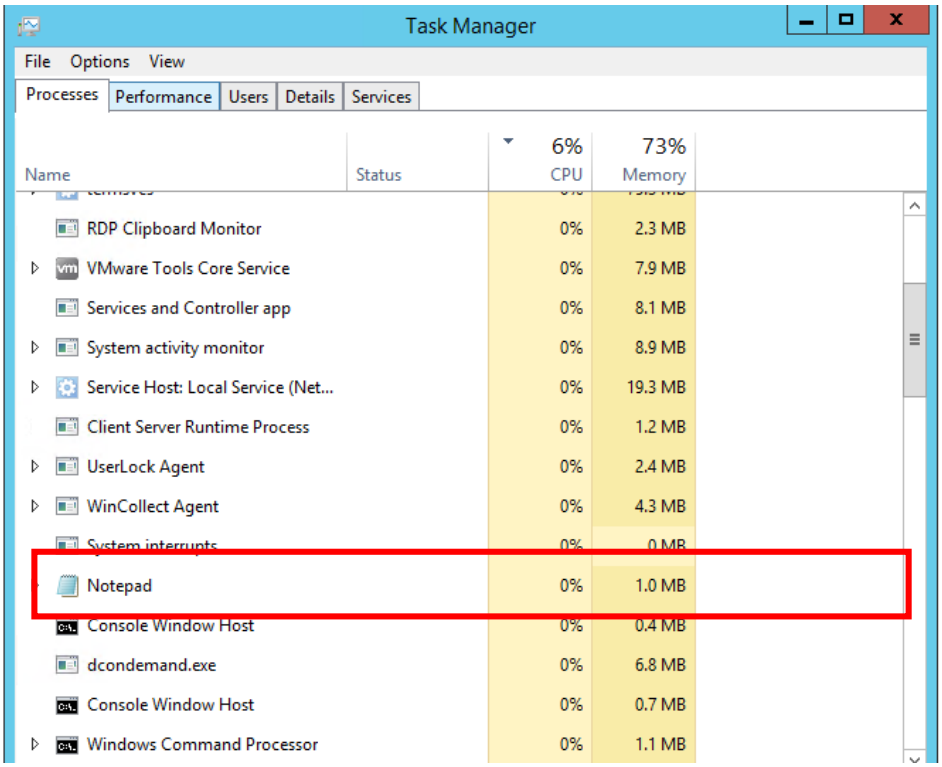
80 portunun nginx servisi üçün, 50 portunun isə domain səviyyəsində açıq olduğunu görürük. 80 Portu ilə kiber hücum etmək mümkündür. Məhz buna görə də, telegram vasitəsilə bizə bildiriş göndəriləcəkdir.

Sadə testlər bitdiyinə və funksionallığın tam işlədiyinə əmin olduğumuza görə artıq server səviyyəsində testlərə keçid edə bilərik. Server səviyyəsində testləri həyata keçirmək üçün yuxarıda da qeyd etdiyimiz kimi virtual maşınlardan istifadə etmişik. İlk olaraq lokal şəbəkə üzərində Windows 10 əməliyyat sisteminə malik olan virtual kompüterdən ikinci bir kompüterə içərisində “Nimda” adlanan virus olan .txt sonluqlu fayl göndərilir. Virusun işə düşməsi üçün faylı açıb oxumaq kifayətdir. Bu zaman virus kompüterdən xaotik olaraq müxtəlif ip-lərə müraciətlər edir. Bu prosesin izlənilməsi üçün hazırldığımız monitorinq sisteminin skripti Linux əməliyyat sistemli cihazda şəbəkəyə qoşulu vəziyyətdə işə salınmalıdır.

Linux əməliyyat sistemində işə saldığımız monitorinq alətində bütün subnet üzrə yoxlama aparmaq üçün şəkildə qeyd edildiyi kimi subneti daxil edib, virus yoxlaması apar düyməsini click etməyimiz kifayətdir.



readme.txt faylı virus olduğuna görə daxilində olan məlumatlar şifrələnmiş formada qarşımıza çıxır və faylı save etdiyimiz andan etibarən fayla daxil olub çıxış etməyimizə baxmayaraq arxa fonda işləməyə başlayır.



Bu zaman monitorinq alətimiz əvvəlcə şəbəkədə göndərilən bu faylın hash kodunu çıxararaq virus total-da yoxlayır, daha sonra çoxsaylı fərqli ip ünvanlara müraciət olduğunu görərək virus-total nəticəsini və müraciət olunan ip cədvəlini log olaraq bizə bildirir. Proqramı Kibana adlı loq vizuallaşdırıcı terminallar ilə əlaqələndirərək daha aydın nəticələr almaq mümkündür, hal-hazırda işlədiyimiz sistem kiçik çaplı olduğuna görə biz nəticələri .csv yəni excel formatında görürük.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Result by httpl//localhost:5000 auth Goshgar Ibrahimli											
2	Period : Period : 19/05/2023 19:01:28 to 19/05/2023 19:12:40											
3	Domain Name : test											
4	Annotation : Showing reports for Virus											
5	Number of Records : 23											
6	Object Name(s) : All											
7	Business Hour Setting : All											
8												
9	User Name	Caller User Name	Modified Time	Domain Controller	Domain	Percentage	Event Number	Event Typ	Event Cod	Record number		
10	kali@goshgarsu	ScriptUser	19/05/2023 19:01:28	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	374811901		
11	kali@goshgarsu	ScriptUser	19/05/2023 19:01:29	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	374809990		
12	kali@goshgarsu	ScriptUser	19/05/2023 19:01:30	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	278650250		
13	kali@goshgarsu	ScriptUser	19/05/2023 19:01:31	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	383834796		
14	kali@goshgarsu	ScriptUser	19/05/2023 19:01:32	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	383832365		
15	kali@goshgarsu	ScriptUser	19/05/2023 19:01:33	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	383830382		
16	kali@goshgarsu	ScriptUser	19/05/2023 19:01:34	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	338345474		
17	kali@goshgarsu	ScriptUser	19/05/2023 19:01:35	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	338345477		
18	kali@goshgarsu	ScriptUser	19/05/2023 19:01:36	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	338345480		
19	kali@goshgarsu	ScriptUser	19/05/2023 19:01:37	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	338345484		
20	kali@goshgarsu	ScriptUser	19/05/2023 19:01:38	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	338345492		
21	kali@goshgarsu	ScriptUser	19/05/2023 19:01:39	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	338345446		
22	kali@goshgarsu	ScriptUser	19/05/2023 19:01:40	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	338345452		
23	kali@goshgarsu	ScriptUser	19/05/2023 19:12:33	test.magistr.az	TEST	Totally virus or unnamed pack	4725	Success	8	338345455		
24												
25												
26												

NƏTİCƏ

Şəbəkə trafikinin analizi sahəsində dünyada mövcud vəziyyət, problemlər analiz edilmişdir. Dünya üzrə şəbəkə trafikinin analizi sahəsində mövcud problemlərin və boşluqların aradan qaldırılması üsulları tədqiq edilmişdir.

Şəbəkə trafikinin analizi sistemlərinin təsnifatının, onların struktur və iş prinsipinin dərin tədqiqi aparılmış və təqdim edilmişdir.

Mövcud şəbəkə təhlükəsizliyinin analizi metodlarının müqayisəli təhlili aparılmışdır. Şəbəkə trafikinin monitorinqinin effektivlik, performans, vizualizasiya, modernizasiya, hərəkətlilik problemləri analiz edilmiş və bu problemlərin aradan qaldırılması üçün görülməli tədbirlər tədqiq edilmişdir.

Təhlil edilmiş məlumatlar, tərtib edilmiş arxitektur model əsasında şəbəkə trafikinin analizi sisteminin konseptual modeli hazırlanmışdır. Hazırlanmış yeni konseptual model strukturların, qurumların və təşkilatların şəbəkə trafikinin analizi sahəsində üzləşdiyi məlumat mübadiləsi sürətinin artırılması, şifrələnmiş trafik, şəbəkənin mürəkkəbliyi, qabaqcıl təhdidlər və təhlükəsizlik sistemlərindən yayınma texnikaları, real-vaxt rejimindi analiz, Big Data problemləri, məxfilik və hüquqi problemləri aradan qaldırır.

Şəbəkə trafikinin monitorinqi sisteminin işlənməsi zamanı korrelyasiya alqoritmləri, normallaşdırma, məlumatların emalı, saxlanması və ötürülməsi üsulları effektiv şəkildə tətbiq edilmişdir.

Təklif edilmiş arxitektur və konseptual modelə əsasən şəbəkə trafikinin monitorinqi sistemi işlənib hazırlanmışdır və effektivlik testləri aparılmışdır. Apardığımız testlər nəticəsində həqiqətən də yaratdığımız şəbəkə monitorinq alətinin (SIEM) doğru portları müəyyən etdiyi və monitorinq zamanı şəbəkədə olan virusları və kənardan olan müraciətləri müəyyən etdiyi görülmüşdür.

Əldə edilmiş nəticələr, şəbəkə trafikinin analizi sisteminin şəbəkədə istifadəsi zamanı şirkətin, qurumun, strukturun informasiya təhlükəsizliyinin təmin olunmasına böyük töhvələr verir və şəbəkədə olan resurs istifadəsinə böyük təsir göstərə bilir.

İSTİFADƏ EDİLMİŞ ƏDƏBİYYAT SİYAHISI

1. Wilson Cyprus, Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. 2018
2. Corporation. Netflow services and applications, http://www.cisco.com/
3. Ross J. Anderson , "Security Engineering: A Guide to Building Dependable Distributed Systems" ,2020.
4. Tommaso Melodia, Antonio Iera. Computer Networks, 2022
5. Goseva-Popstojanova K., Anastasovski G., Dimitrijevikj A., Pantev R., Miller B. Characterization and classification of malicious Web traffic // Computers & Security, 2014, vol. 42, pp. 92-115.
6. Bing-Jhih Yaoa, Shaw-Hwa Hwanga, Cheng-Yu Yeh. Mathematical Model of Network Address Translation Port Mapping, 2014
7. Behrouz A. Forouzan. Data Communications and Networking, Fifth Edition TMH, 2013.
8. John Sherwood, Andrew Clark, David Lynas ,Enterprise Security Architecture – A Business-Driven Approach. 2013
9. Ramya Mohanakrishnan. What Is Intrusion Detection and Prevention System? Definition, Examples, Techniques, and Best Practices, 2022.
10. James F. Kurose , Keith W. Ross. "Computer Networking: A Top-Down Approach",2021.
11. Zach Codings, Computer Programming and Cyber Security for Beginners, December 4,2019
12. Min Xiao and Mei Guo. Computer Network Security and Preventive Measures in the Age of Big Data, 2020.
13. Simon Applebauma, Tarek Gaberb , Ali Ahmed. Signature-based and Machine-Learning-based Web Application Firewalls: A Short Survey, 2021 pp. 360-361
14. Robert Grimmick. Network Flow Monitoring Explained: NetFlow vs sFlow vs

IPFIX. 2021.

15. Saurav P.J “ A Brief Survey on Next Generation Firewall Systems over Traditional Firewall Systems” International Journal of Scientific & Engineering Research Volume 11, Issue 1, January-2020

16. Erik Hjelmvik. What is a PCAP file? Netresec Journal, Oct 27, 2022

17. Shivam Arora. Why Learn Python? Reasons and Benefits of Learning Python, 2023.

18. Andrew Clark, David Lynas ,Enterprise Security Architecture – A Business-Driven Approach. John Sherwood, 2013

19. CompTIA Security+ Review Guide Exam SYO-601 Fifth Edition, November 12, 2020, səh 579

20. Jazib Frahim ,Cisco ASA, All in one firewall, IPS and VPN Adaptive Security appliance, 2020

21. Wendell J. Odom “Cisco cyberops associate cbrops 200-201” , Dec 29, 2020 pp.24-28, 384-385.

22. Justin Seitz ,"Black Hat Python: Python Programming for Hackers and Pentesters" ,2014

23. Ramiz Şıxəliyev. Müasir kompüter şəbəkələrinin təhlükəsizlik trendləri haqqında, 2015. 42.pdf (ict.az)

24. В.Олифер, Н.Олифер. Компьютерные сети, принципы, технологии, протоколы. Москва, 2017.

25. Alexander S. Gillis, Security Information and Event Management (SIEM) , December 14, 2020

XÜLASƏ

Dissertasiya işi şəbəkə trafiki və şəbəkə trafikinin analizi sistemlərinə dair hərtərəfli tədqiqatı təqdim edir. Tədqiqat şəbəkə trafikinin analizi sistemlərinin nəzəri əsasları, praktikada tətbiq edilməsi və Python proqramlaşdırma dilindən istifadə edərək yeni şəbəkə trafikinin analizi sisteminin yaradılmasına yönəlmişdir . Aparılan tədqiqat şəbəkə trafikinin analizi sistemlərinin problemlərinin həll edilməsində və avtomatlaşdırılmış analizin aparılmasının təmin edilməsi üsullarını araşdırır. 1-ci fəsil şəbəkə trafikinin monitorinqi və analizi vasitələri haqqında məlumat verir, şəbəkə təhlükəsizliyinin analizi metodlarının müqayisəli təhlilini aparır, şəbəkə trafikinin monitorinqi sahəsində mövcud problemlər və həllər barədə məlumat verir. 2-ci fəsildə davranış əsaslı və imza əsaslı kiberhücumların aşkarlanması və qarşısının alınması sistemlərinin müxtəlif növlərinin analizi aparılır. Bundan əlavə işləyib hazırladığımız şəbəkə trafikinin analizi sisteminin konseptual modeli, arxitekturası və dizaynı tərtib edilmişdir. 3-cü fəsildə Python proqramlaşdırma dilindən istifa də edərək şəbəkə trafikinin analizi sistemi hazırlanmış, test edilmişdir. Testlər zamanı şəbəkə trafikində paketlər arasında vaxt intervalı təhlil edilmişdir. Dissertasiyada təqdim edilmiş proqram təminatı və nümunələr şəbəkə trafikinin daha dərindən başa düşməyə və trafikin analizi üsullarının inkişafına kömək edir.

SUMMARY

The dissertation presents a comprehensive study of network traffic and network traffic analysis systems. The research focuses on the theoretical foundations of network traffic analysis systems, their application in practice, and the creation of a new network traffic analysis system using the Python programming language. Conducted research examines methods for troubleshooting network traffic analysis systems and providing automated analysis. Chapter 1 provides information on network traffic monitoring and analysis tools, conducts a comparative analysis of network security analysis methods, and provides information on existing problems and solutions in the field of network traffic monitoring. Chapter 2 analyzes different types of behavior-based and signature-based cyber attack detection and prevention systems. In addition, the conceptual model, architecture and design of the network traffic analysis system developed by us have been drawn up. In Chapter 3, a network traffic analysis system was developed and tested using the Python programming language. During the tests, the time interval between packets in the network traffic was analyzed. The software and examples presented in the thesis contribute to a deeper understanding of network traffic and the development of traffic analysis methods.

РЕЗЮМЕ

В диссертации представлено всестороннее исследование сетевого трафика и систем анализа сетевого трафика. Основное внимание в исследовании уделяется теоретическим основам систем анализа сетевого трафика, их применению на практике и созданию новой системы анализа сетевого трафика с использованием языка программирования Python. В проведенном исследовании рассматриваются методы устранения неполадок в системах анализа сетевого трафика и обеспечения автоматизированного анализа. Глава 1 содержит информацию об инструментах мониторинга и анализа сетевого трафика, проводит сравнительный анализ методов анализа сетевой безопасности, а также предоставляет информацию о существующих проблемах и решениях в области мониторинга сетевого трафика. В главе 2 анализируются различные типы систем обнаружения и предотвращения кибератак на основе поведения и сигнатур. Кроме того, составлена разработанная нами концептуальная модель, архитектура и дизайн системы анализа сетевого трафика. В главе 3 была разработана и протестирована система анализа сетевого трафика с использованием языка программирования Python. В ходе тестов анализировался временной интервал между пакетами в сетевом трафике. Программное обеспечение и примеры, представленные в диссертации, способствуют более глубокому пониманию сетевого трафика и развитию методов анализа трафика.