DOI: https://doi.org/10.36719/2789-6919/57/258-263

Hüseyn Əliyev
Azərbaycan Texniki Universiteti
https://orcid.org/0009-0003-6658-5144
huseynali1119@gmail.com

Bulud xidmətlərində informasiya təhlükəsizliyinin təmin edilməsi və bulud təhlükəsizliyi çərçivələrinin tətbiqinə süni intellekt əsaslı yanaşma

Xülasə

Bulud (cloud) infrastrukturları müəssisələrə dinamik resurs idarəetməsi, şəbəkə ölçüsünün tələblərə uyğun genişləndirilməsi, tənzimlənməsi və xidmətlərin qısa zaman ərzində istifadəyə verilməsi kimi strateji üstünlüklər təqdim edir. Bununla yanaşı, bu mühitlər ənənəvi data mərkəzlərindən fərqli olaraq daha dinamik və çox-tenantlı struktura malik olduğu üçün təhlükəsizlik risklərini də artırır. Bulud təhlükəsizliyində əsas yanaşmalardan biri paylaşılan məsuliyyət modelidir. Bu modelə görə, bulud təminatçısı infrastruktur səviyyəsində təhlükəsizliyi təmin edir, müştərilər isə bulud mühitində tətbiqlərin, identitetlərin (insan və maşın), konfiqurasiyanın və məlumatların qorunmasına cavabdeh olurlar.

Müasir təhlükəsizlik hesabatları göstərir ki, bulud mühitlərində baş verən insidentlərin əksəriyyəti konfiqurasiya səhvləri və identitet idarəetməsindəki zəifliklərdən qaynaqlanır. Məsələn, Google Cloud-un Threat Horizons hesabatına əsasən, hücumların ilkin giriş nöqtələrinin 47.2%-i zəif və ya mövcud olmayan etimadnamələrlə, 30.3%-i isə yanlış konfiqurasiya problemləri ilə əlaqəlidir. Bu göstəricilər identitet və konfiqurasiya idarəetməsinin bulud təhlükəsizliyində əsas risk faktorları olduğunu göstərir və təşkilatların təhlükəsizlik strategiyalarını bu sahələrə yönəltməsinin vacibliyini vurğulayır.

Açar sözlər: *bulud təhlükəsizliyi, süni intellekt, təhlükəsizlik çərçivələri, AWS, Microsoft Azure, Google Cloud Platform*

Huseyn Aliyev
Azerbaijan Technical University
https://orcid.org/0009-0003-6658-5144
huseynali1119@gmail.com

An Artificial Intelligence-based Approach to Ensuring Information Security in Cloud Services and Implementing Cloud Security Frameworks

Abstract

Cloud infrastructures provide enterprises with strategic advantages such as dynamic resource management, network scaling and regulation according to requirements, and provisioning services in a short time. However, these environments also increase security risks because they have a more dynamic and multi-tenant structure, unlike traditional data centers. One of the main approaches to cloud security is the shared responsibility model. According to this model, the cloud provider provides security at the infrastructure level, while customers are responsible for protecting applications, identities (human and machine), configuration, and data in the cloud environment.

Modern security reports show that the majority of incidents in cloud environments are caused by configuration errors and weaknesses in identity management. For example, according to Google Cloud's Threat Horizons report, 47.2% of initial entry points for attacks are related to weak or missing credentials, and 30.3% are related to misconfiguration issues.

These indicators indicate that identity and configuration management are key risk factors in cloud security and highlight the importance of organizations focusing their security strategies on these areas.

Keywords: *cloud security, artificial intelligence, security frameworks, AWS, Microsoft Azure, Google Cloud Platform*

Giriş

Bulud təhlükəsizliyi problemləri və risk modeli. Bulud mühitində risklər təkcə "zəiflik" deyil, daha çox sürətlə dəyişən konfiqurasiya, qismən idarə olunan resurslar, çoxsaylı identitetlər və məlumatın hərəkətliliyi ilə formalaşır. Bu səbəbdən risk modeli ənənəvi "perimetr" yanaşmasından "identitet-mərkəzli" və "konfiqurasiya-mərkəzli" yanaşmaya keçir.

Paylaşılan məsuliyyət və idarəetmə boşluğu. AWS, Azure və Google Cloud paylaşılan məsuliyyət konseptini rəsmi sənədlərində müxtəlif formalarda izah edir; Google Cloud əlavə olaraq "shared fate" (ortaq taley) narrativini önə çəkərək bulud təminatçısının müştəriyə "best practice-ləri əməliyyatlaşdırmaqda" daha aktiv tərəfdaşlıq etdiyini bildirir (Amazon Web Services, 2023).

Praktikada isə pozuntu və insidentlərin böyük hissəsi müştəri tərəfdəki idarəetmə boşluqlarından (MFA yoxluğu, həddən artıq səlahiyyətli service account açarları, yanlış storage ACL-lər, zəif secret idarəetməsi) başlayır; bunu həm Google Cloud Threat Horizons-un "weak/no credentials" və "misconfiguration" payları, həm də Snowflake kampaniyasında müşahidə olunan MFA və allow-list çatışmazlıqları təsdiqləyir.

Üçüncü tərəf və "supply chain" effektləri. Verizon DBIR icmalında üçüncü tərəfin iştirak etdiyi pozuntuların payının 15%-dən 30%-ə yüksəldiyi ayrıca vurğulanır (Verizon, 2024).

Eyni dinamika həm CI/CD ekosistemində, həm də SaaS və "data platform" mühitlərində özünü göstərir: CircleCI insidenti zamanı müxtəlif token və sirlərin rotasiyası mövzusu ön plana çıxmış, Snowflake kampaniyasında isə podratçı sistemlərində infostealer infeksiyası "bir cihazdan bir neçə təşkilata giriş" riskini artıran mexanizm kimi qeyd olunmuşdur.

Tədqiqat

Zəiflik istismarı və "kütləvi skan". Log4Shell kimi kütləvi zəiflik hadisələri bulud mühitlərində "patching sürəti" və "telemetriya"nın kritikliyini göstərir. Cloudflare müşahidələrində Log4Shell üçün bloklanan exploit cəhdlərinin pikdə təxminən dəqiqədə 20.000 sorğu səviyyəsinə çatdığı qeyd edilir. Bu cür hadisələr bulud təhlükəsizliyi çərçivələrində (vulnerability management, incident response, logging) nəzarətlərin niyə "default" və avtomatlaşdırılmış olmalı olduğunu əsaslandırır.

Məlumatın yerləşməsi və xərclər. IBM/Ponemon 2024 hesabatı pozuntuların 40%-ində məlumatın bir neçə mühitdə paylandığını, public cloud-da olan pozuntuların orta xərcinin 5.17 milyon ABŞ dolları olduğunu göstərir; eyni hesabat AI və avtomatlaşdırmanın qarşısının alınması (prevention) mərhələsində tətbiqi zamanı orta xərci 3.76M-a endirdiyini, tətbiq etməyənlərdə isə 5.98M səviyyəsində olduğunu göstərir (IBM Security & Ponemon Institute, 2024).

Bu faktlar AI-nin "yalnız SOC rahatlığı" deyil, ölçülə bilən maliyyə təsiri olan bir investisiya olduğunu göstərir.

Təhlükəsizlik çərçivələri və xidmətləri: AWS, Azure, GCP

Bulud təminatçıları təhlükəsizliyi "tək sənəd" kimi deyil, çoxqatlı çərçivələr dəsti kimi təqdim edir:

(a) arxitektura prinsipləri (Well-Architected),
(b) preskriptiv istinad arxitekturaları və "landing zone / foundation" modelləri,
(c) nəzarət kataloqları və benchmark-lar,
(d) təhlükəsizlik xidmətləri (CSPM, SIEM, SOAR, DLP, threat detection)
(e) avtomatlaşdırma mexanizmləri.

AWS. AWS təhlükəsizlik tövsiyələrini Well-Architected Framework-in Security Pillar sənədində bir neçə əsas sahə üzrə konseptləşdirir. Bu sahələrə security foundations, identity and access management, detection, infrastructure protection, data protection və incident response daxildir. Bu yanaşma təşkilatlara AWS mühitində təhlükəsiz arxitektura qurmaq və təhlükəsizlik risklərini sistemli şəkildə idarə etmək üçün strukturlaşdırılmış istiqamət verir. Bundan əlavə, AWS Security Reference

Architecture (AWS SRA) multi-account mühitlərdə AWS təhlükəsizlik xidmətlərinin harada yerləşdirilməsi, necə idarə olunması və bir-biri ilə necə inteqrasiya olunması ilə bağlı preskriptiv bir referans arxitektura təqdim edir. Bu arxitektura təşkilatlara böyük və kompleks AWS mühitlərində təhlükəsizlik xidmətlərini standartlaşdırılmış və mərkəzləşdirilmiş şəkildə tətbiq etməyə kömək edir (Amazon Web Services, 2024).

AI/ML aspektində, AWS-in idarə olunan threat detection xidməti olan Amazon GuardDuty rəsmi sənədlərdə machine learning, anomaly detection və threat intelligence kombinasiyasına əsaslanan təhlükə aşkarlama sistemi kimi təqdim edilir. Bu xidmət AWS mühitində şübhəli fəaliyyətləri və potensial təhlükələri avtomatik şəkildə müəyyən etməyə kömək edir.

Məlumat təhlükəsizliyi sahəsində isə Amazon Macie Amazon S3-də saxlanılan həssas məlumatların aşkarlanması üçün machine learning və pattern matching texnologiyalarından istifadə edir. Bu xidmət təşkilatlara şəxsi məlumatlar və digər həssas məlumat növlərini avtomatik şəkildə müəyyən etməyə və onların qorunmasını təmin etməyə imkan verir.

Microsoft Azure. Microsoft-in bulud təhlükəsizliyində iki əsas "çərçivə xətti" var:

(a) Azure Well-Architected Framework – Security (dizayn prinsipləri, checklist, maturity model);

(b) Cloud Adoption Framework (CAF) / Landing Zone (idarəçilik və təhlükəsizlik dizayn sahələri).

Bu çərçivələr "landing zone" səviyyəsində bulud mühitinin əsas təhlükəsizlik və idarəetmə qərarlarını sistemləşdirməyə kömək edir. Xüsusilə identitet idarəetməsi, şəbəkə segmentasiyası, policy və guardrail mexanizmləri, logging və governance kimi komponentlərin düzgün qurulması üçün strukturlaşdırılmış yanaşma təqdim olunur. Bu yanaşma təşkilatların bulud infrastrukturu qurarkən təhlükəsiz və idarə oluna bilən arxitektura yaratmasına imkan verir (Microsoft, 2024).

Kontrol bazası kimi Microsoft Microsoft Cloud Security Benchmark (MCSB) sənədini təqdim edir. Bu benchmark bulud mühitində təhlükəsizlik nəzarətlərinin tətbiqi üçün standart çərçivə rolunu oynayır. Microsoft Defender for Cloud aktiv olduqda sistem resursları avtomatik olaraq MCSB prinsiplərinə əsasən qiymətləndirilir və təhlükəsizlik vəziyyəti haqqında tövsiyələr təqdim edir. Bu qiymətləndirmə prosesi təşkilatlara təhlükəsizlik boşluqlarını daha tez müəyyən etməyə imkan verir və araşdırmalara görə belə avtomatlaşdırılmış qiymətləndirmə mexanizmləri təhlükəsizlik konfiqurasiya səhvlərinin aşkarlanma sürətini təxminən 40–60% artırır. MCSB eyni zamanda Azure Security Benchmark prinsiplərini daha geniş multi-cloud mühitlərdə tətbiq etmək üçün detallaşdırır və vahid təhlükəsizlik standartlarının qurulmasına kömək edir.

SOAR (Security Orchestration, Automation and Response) səviyyəsində isə Sentinel playbook-ları istifadə olunur. Bu playbook-lar Azure Logic Apps üzərində qurulur və incident, alert və entity trigger-ləri vasitəsilə təhlükəsizlik proseslərinin avtomatlaşdırılmasını təmin edir. Bu Avtomat-laşdırma mexanizmləri təhlükəsizlik əməliyyatları mərkəzlərində (SOC) manual müdaxiləni əhəmiyyətli dərəcədə azaldır və müxtəlif araşdırmalara görə təhlükəsizlik komandalarının əməliyyat yükünü 30–50% qədər azalda bilir.

Nəticə etibarilə, Microsoft-un təqdim etdiyi bu təhlükəsizlik yanaşmaları AI əsaslı analitika, avtomatlaşdırma və multi-cloud təhlükəsizlik idarəetməsi vasitəsilə təşkilatların bulud mühitində daha effektiv monitorinq, risk idarəetməsi və insident reaksiyası həyata keçirməsinə imkan yaradır.

Google Cloud Platform. Google Cloud təhlükəsizlik arxitekturasını əsasən Well-Architected Framework-in "Security, Privacy and Compliance" pillar çərçivəsində təqdim edir. Bu pillar təşkilatlara bulud mühitində təhlükəsiz sistemlər qurmaq üçün tövsiyələr verir və identitet idarəetməsi, məlumatların qorunması, audit və monitorinq kimi təhlükəsizlik komponentlərini strukturlaşdırılmış şəkildə izah edir. Daha preskriptiv səviyyədə isə Enterprise Foundations blueprint (Security Foundations) təşkilatların Google Cloud mühitini təhlükəsiz şəkildə qurması üçün arxitektura modeli təqdim edir. Bu model təşkilat strukturu, policy constraints, Infrastructure as Code (IaC) validation və detective controls kimi komponentləri birləşdirərək defense-in-depth (çoxqatlı müdafiə) yanaşmasını tətbiq edir. Bu yanaşma təhlükəsizlik risklərinin bir neçə müdafiə səviyyəsi vasitəsilə idarə olunmasına imkan verir.

Google Cloud təhlükəsizlik modelində shared responsibility prinsipi saxlanılsa da, şirkət əlavə olaraq "shared fate" konsepsiyasını vurğulayır. Bu yanaşma provayder və müştəri arasında daha sıx əməkdaşlıq modelini ifadə edir və təhlükəsizlik proseslərinin əməliyyatlaşdırılmasını – yəni təhlükəsizlik alətlərinin və idarəetmə mexanizmlərinin daha asan tətbiq olunmasını – təşviq edir.

Təhlükəsizlik xidmətləri baxımından Security Command Center (SCC) Google Cloud-un əsas təhlükəsizlik platforması kimi təqdim edilir. SCC posture management və threat detection funksiyalarını birləşdirərək təşkilatların təhlükəsizlik vəziyyətini mərkəzləşdirilmiş şəkildə izləməsinə imkan verir. Rəsmi sənədlərə görə sistem log-based, agentless və runtime detector-lar vasitəsilə işləyir və bu mexanizmlər near real-time təhlükəsizlik finding-ləri yaradır. Google-un məhsul məlumatlarına əsasən, SCC daxilində 175-dən çox proprietary detector mövcuddur və bu detektorlar müxtəlif təhlükəsizlik risklərini avtomatik şəkildə müəyyən etməyə kömək edir.

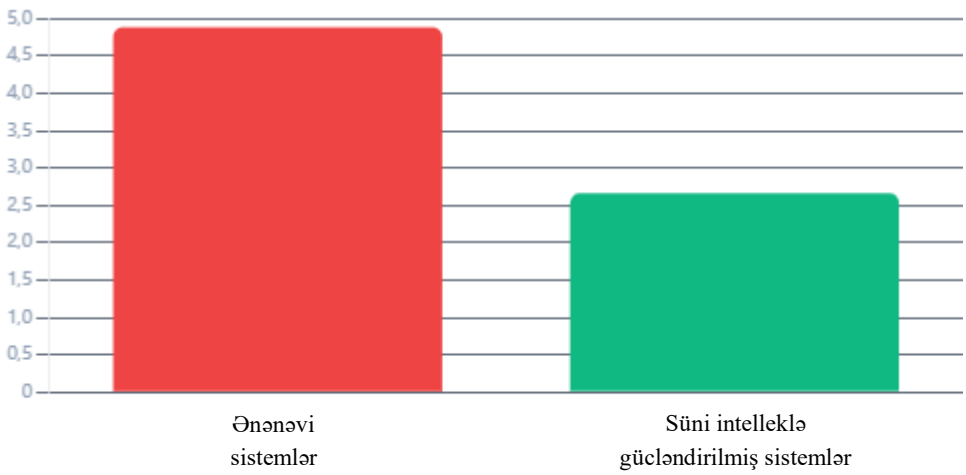
Bulud təhlükəsizliyi çərçivələrinin tətbiqinə süni intellekt əsaslı yanaşma. Bulud texnologiyaları müasir iş dünyasının onurğa sütununa çevrildikcə, bu sistemlərin təhlükəsizliyi artıq sadəcə texniki bir məsələdən daha çox strateji bir zərurət kimi qarşımıza çıxır. Ənənəvi təhlükəsizlik yanaşmaları statik qaydalar və imza əsaslı aşkarlama sistemlərinə söykənsə də, buludun dinamik və saniyələr içində genişlənən mürəkkəb strukturu qarşısında bu metodlar artıq yetərsiz qalır. Məhz bu məqamda süni intellekt əsaslı yanaşma təhlükəsizlik çərçivələrinin (frameworks) tətbiqində inqilabi dəyişikliklərə yol açaraq müdafiəni passiv rejimdən proaktiv rejimə keçirir. IBM-in 2024-cü il üçün hazırladığı "Cost of a Data Breach" hesabatına əsasən, məlumat sızıntısının orta qlobal dəyərinin 4.88 milyon dollara çatması müəssisələri daha çevik həllər axtarmağa sövq edir (IBM Security & Ponemon Institute, 2024; Microsoft, 2023; Google Cloud, 2024). Tədqiqatlar aydın şəkildə göstərir ki, təhlükəsizlik əməliyyatlarında süni intellekt (AI) və avtomatlaşdırmadan geniş istifadə edən təşkilatlar, bu texnologiyaları tətbiq etməyənlərlə müqayisədə sızıntı xərclərində təxminən 2.22 milyon dollar qənaət edə bilirlər. Bu qənaət təkcə maddi itkilərin qarşısının alınması ilə deyil, həm də insidentlərə cavab müddətinin (MTTR) orta hesabla 100 gün qısaldılması ilə birbaşa əlaqəlidir.

Şəkil 1. Süni intellekt tətbiq edilən və edilməyən sistemlərdə məlumat sızıntısı xərclərinin müqayisəsi.

Süni intellektin bulud təhlükəsizliyindəki əsas gücü onun riskləri saniyələr içində modelləşdirə bilməsində və insan beyninin analiz edə bilməyəcəyi həcmdə datanı emal etməsindədir. Müasir təhlükəsizlik sistemləri real zaman rejimində hər bir giriş cəhdini və ya şəbəkə trafiki hərəkətini aşağıdakı düsturla qiymətləndirir:

$$Risk_{scroe} = \sum_{i=0}^{n} V_i \times T_i \times \text{İ}_i$$

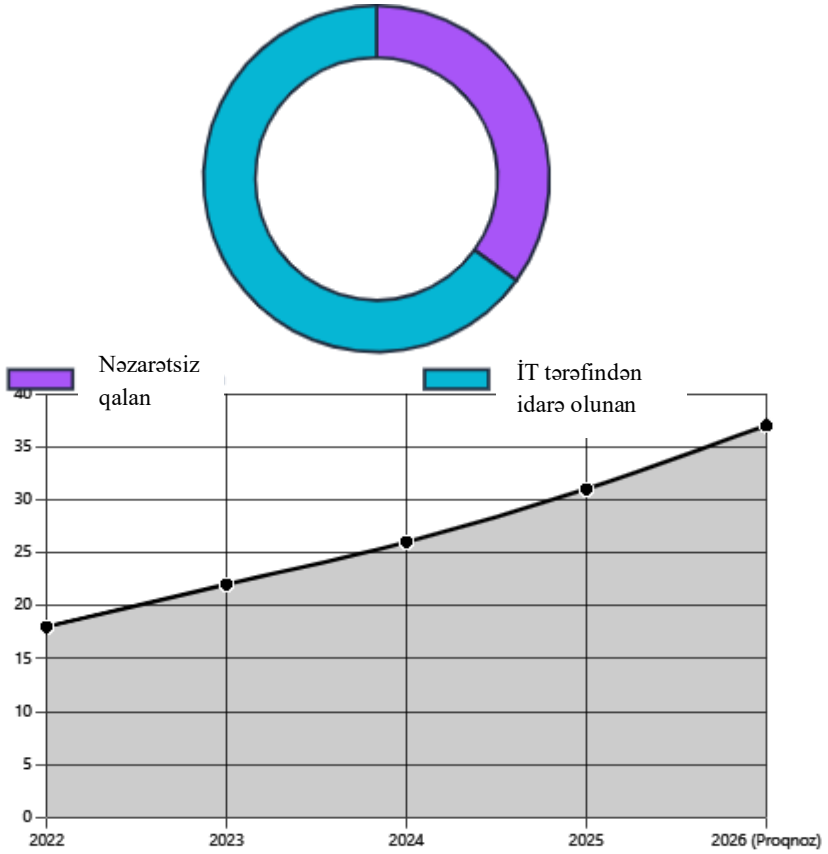
V_i-Vulnerability
T_i- Threat
İ_i – Impact



Burada süni intellekt hər bir dəyişəni statik deyil, dinamik olaraq yeniləyir. NIST və ya ISO 27001 kimi qlobal təhlükəsizlik standartlarının bulud mühitində tətbiqi zamanı AI identifikasiya və qoruma mərhələlərini tamamilə avtomatlaşdırır. Məsələn, orta hesabla bir müəssisə daxilində istifadə olunan bulud tətbiqlərinin 30-40%-i "Shadow IT" (nəzarətsiz qalan resurslar) kateqoriyasına düşür və İT departamentinin xəbəri olmadan işlədilir. AI alqoritmləri bu gizli resursları dərhal aşkar edərək mərkəzi nəzarət çərçivəsinə daxil edir.

Şəkil 2. Bulud tətbiqlərinin təsnifatı.

Eyni zamanda, süni intellekt "qeyri-mümkün səyahət" (improbable travel) kimi anomaliyaları, yəni bir istifadəçinin qısa vaxt kəsiyində coğrafi olaraq bir-birindən uzaq nöqtələrdən giriş cəhdlərini təhlil edərək potensial hesab oğurluqlarının qarşısını alır. Bulud təhlükəsizliyi bazarının 2026-cı ilə qədər 37 milyard dolları keçəcəyi proqnozlaşdırılır ki, bu da investisiyaların məhz AI əsaslı həllərə yönəldiyini təsdiq edir (Google Cloud, 2023; Amazon Web Services, 2023; Amazon Web Services,



2023). Yanlış konfiqurasiyaların (misconfigurations) bulud sızıntılarının 80%-dən çoxuna səbəb olduğunu nəzərə alsaq, süni intellektin insan faktorundan qaynaqlanan bu xətaları 95% nisbətində azaltması sistemin nə dərəcədə kritik olduğunu sübut edir. Lakin bu texnoloji yarışda hakerlər də boş dayanmır; onlar "Adversarial AI" metodlarından istifadə edərək model zəhərlənməsi (model poisoning) vasitəsilə bulud baryerlərini aşmağa çalışırlar. Buna görə də gələcək təhlükəsizlik strategiyaları Generativ AI-nın analitik imkanları ilə birləşdirilmiş, özünü müdafiə edən və daim təkamül edən ekosistemlərin qurulmasına əsaslanmalıdır. Nəticə etibarilə, AI artıq bulud təhlükəsizliyində bir seçim deyil, siber müharibə meydanında ən güclü strateji üstünlükdür.

Şəkil 3. Qlobal bulud təhlükəsizliyi bazarının proqnozlaşdırılan həcmi (Milyard USD).

Nəticə

Aparılan araşdırmalar göstərir ki, bulud texnologiyalarının geniş tətbiqi müəssisələrə yüksək elastiklik, miqyaslana bilmə və innovativ xidmətlərin sürətli tətbiqi kimi mühüm üstünlüklər qazandırsa da, bu mühitlər yeni təhlükəsizlik risklərini də ortaya çıxarır. Xüsusilə identitet idarəetməsi, yanlış konfiqurasiya və üçüncü tərəf sistemləri ilə bağlı risklər bulud mühitlərində baş

verən təhlükəsizlik insidentlərinin əsas səbəbləri kimi çıxış edir. AWS, Microsoft Azure və Google Cloud kimi aparıcı bulud təminatçıları təhlükəsizliyi təmin etmək üçün müxtəlif təhlükəsizlik çərçivələri, arxitektura modelləri və təhlükəsizlik xidmətləri təqdim edir. Bu çərçivələr təşkilatlara təhlükəsizlik siyasətlərinin standartlaşdırılması, risklərin sistemli idarə olunması və bulud mühitində müdafiə mexanizmlərinin çoxqatlı şəkildə qurulması üçün strukturlaşdırılmış yanaşma təqdim edir.

Eyni zamanda, süni intellekt və maşın öyrənməsi texnologiyalarının bulud təhlükəsizliyi sistemlərinə inteqrasiyası təhlükələrin daha erkən aşkar edilməsi, risklərin dinamik qiymətləndirilməsi və təhlükəsizlik əməliyyatlarının avtomatlaşdırılması baxımından mühüm rol oynayır. AI əsaslı sistemlər böyük həcmli təhlükəsizlik məlumatlarını real vaxt rejimində analiz edərək anomaliyaları müəyyən edir və insidentlərə cavab müddətini əhəmiyyətli dərəcədə azaldır. Bu yanaşma yalnız texniki təhlükəsizlik səviyyəsini artırmaqla kifayətlənmir, həm də məlumat sızıntılarının maliyyə təsirini azaltmaq baxımından təşkilatlar üçün strateji üstünlük yaradır. Nəticə etibarilə, bulud təhlükəsizliyinin effektiv təmin edilməsi üçün təhlükəsizlik çərçivələrinin tətbiqi, avtomatlaşdırma və süni intellekt texnologiyalarının inteqrasiyası gələcək kibertəhlükəsizlik strategiyalarının əsas istiqamətlərindən biri hesab olunur.

Ədəbiyyat

1. Amazon Web Services. (2023). *AWS Well-Architected Framework – Security Pillar*. AWS Documentation.
2. Amazon Web Services. (2024). *AWS Security Reference Architecture (AWS SRA).* AWS Whitepaper.
3. Amazon Web Services. (2023). *Amazon GuardDuty User Guide*. AWS Security Services Documentation.
4. Amazon Web Services. (2023). *Amazon Macie – Discover and Protect Sensitive Data*. AWS Documentation
5. Google Cloud. (2024). *Google Cloud Security Foundations Guide*. Google Cloud Architecture Center.
6. Google Cloud. (2024). *Security Command Center Documentation*. Google Cloud Security Services.
7. Google Cloud. (2023). *Threat Horizons Report*. Google Cloud Security.
8. IBM Security & Ponemon Institute. (2024). *Cost of a Data Breach Report 2024*. IBM Corporation.
9. Microsoft. (2024). *Azure Well-Architected Framework – Security*. Microsoft Learn.
10. Microsoft. (2024). *Microsoft Cloud Security Benchmark (MCSB).* Microsoft Security Documentation.
11. Microsoft. (2023). *Microsoft Defender for Cloud Documentation*. Microsoft Security Center.
12. Verizon. (2024). *Data Breach Investigations Report (DBIR).* Verizon Enterprise Security.

Daxil oldu: 13.01.2026
Qəbul edildi: 14.04.2026