DOI: https://doi.org/10.36719/0860/87-93

Fərid Abdullazadə
Bakı Ali Neft Məktəbi
Magistr
https://orcid.org/0009-0002-0300-6347
faridabdullazadeh@yandex.com

SOC (Təhlükəsizlik Əməliyyatları Mərkəzi) xəbərdarlıqlarının idarə edilməsini təkmilləşdirmək üçün proses optimizasiyası və yeni süni intellekt texnologiyalarının birlikdə tətbiqi

Xülasə

Bildiyimiz kimi, müasir rəqəmsallaşma və kibertəhlükələrin sürətlə şaxələndiyi dövrdə informasiya aktivlərinin qorunması və insidentlərə vaxtında reaksiya verilməsi təşkilatların dayanıqlılığı üçün xüsusi aktuallıq kəsb edir. Bu kontekstdə Təhlükəsizlik Əməliyyatları Mərkəzlərində (SOC) formalaşan çoxsaylı xəbərdarlıqların idarə olunması əsas problemlərdən biri kimi çıxış edir, çünki yüksək həcmdə "səs-küylü" (yanlış müsbət) siqnallar, təkrarlanan hadisələr və məhdud analitik resursları operativliyi zəiflədir. Məqalədə SOC xəbərdarlıq idarəetməsinin təkmilləşdirilməsi üçün proseslərin optimallaşdırılması, iş axınlarının yenidən qurulması və standart əməliyyatların avtomatlaşdırılması ilə bağlı müasir yanaşmalar araşdırılır. Eyni zamanda, maşın öyrənməsi, təbii dil emalı (NLP), anomaliya aşkarlanması və böyük dil modelləri kimi yaranmaqda olan süni intellekt texnologiyalarının SIEM/EDR mənbələrindən daxil olan xəbərdarlıqların ilkin qiymətləndirməsində, prioritetləşdirilməsində və kontekstual təhlilində necə tətbiq olunduğu müzakirə olunur. Bundan əlavə, SOAR və orkestrasiya imkanlarının playbook əsaslı avtomatik yoxlamalar, kontekst toplanması və insident cavabının sürətləndirilməsi vasitəsilə analitik iş yükünə və əməliyyat göstəricilərinə (məsələn, MTTR-in azalması, yanlış siqnalların aşağı salınması, məhsuldarlığın artması) təsiri qeyd edilir. Xəbərdarlıq idarəetməsində proses optimizasiyası və AI texnologiyalarının tətbiqinin faydaları ilə yanaşı, məlumat keyfiyyəti və balanssızlığı, modelin zamanla zəifləməsi (model drift), izaholunma tələbləri, riskli qərarlarda insan nəzarətinin qorunması kimi çətinlik və məhdudiyyətlər də təhlil edilir. Ümumilikdə, məqalə SOC-da xəbərdarlıq axınının daha səmərəli idarə olunması üçün proses optimizasiyası ilə yeni AI texnologiyalarının sinerjisini vurğulayan, mərhələli tətbiq çərçivəsi və qiymətləndirmə meyarları əsasında təklif və tövsiyələr təqdim edən sistemli bir araşdırmadır.

Açar sözlər. *SOC, xəbərdarlıq idarəetməsi, proses optimizasiyası, SIEM, EDR, SOAR, maşın öyrənməsi, NLP, anomaliya aşkarlanması, böyük dil modelləri, MTTR .*

Combining Process Optimization and New AI Technologies to Improve SOC (Security Operations Center) Alert Management

Abstract

As we know, in the era of modern digitalization and the rapid diversification of cyber threats, protecting information assets and responding to incidents in a timely manner is of particular relevance for the resilience of organizations. In this context, managing the numerous alerts generated in Security Operations Centers (SOCs) is one of the main problems, since a high volume of "noisy" (false positive) signals, repetitive events, and limited analytical resources weaken operational efficiency. The article examines modern approaches to optimizing processes, reorganizing workflows, and automating standard operations to improve SOC alert management. At the same time, it discusses how emerging artificial intelligence technologies such as machine learning, natural language processing (NLP), anomaly detection, and large language models are applied in triaging, prioritizing,

and contextual analysis of alerts received from SIEM/EDR sources. Additionally, the impact of SOAR and orchestration capabilities on analytics workloads and operational metrics (e.g., reduced MTTR, reduced false positives, increased productivity) through playbook-based automated inspections, context collection, and accelerated incident response is noted. Along with the benefits of process optimization and AI technologies in alert management, challenges and limitations such as data quality and imbalance, model drift over time, requirements for validation, and maintaining human control over risky decisions are also analyzed. Overall, the paper is a systematic study that highlights the synergy of process optimization with new AI technologies for more efficient alert flow management in the SOC, and provides suggestions and recommendations based on a phased implementation framework and evaluation criteria.

Keywords: *SOC, alert management, process optimization, SIEM, EDR, SOAR, machine learning, NLP, anomaly detection, large language models, MTTR.*

Сочетание оптимизации процессов и новых технологий искусственного интеллекта для улучшения управления оповещениями в центре оперативного управления безопасностью (SOC).

Резюме

Как известно, в эпоху современной цифровизации и стремительной диверсификации киберугроз защита информационных активов и своевременное реагирование на инциденты имеют особое значение для устойчивости организаций. В этом контексте управление многочисленными оповещениями, генерируемыми в центрах оперативного управления безопасностью (ЦОС), является одной из главных проблем, поскольку большой объем «шумных» (ложноположительных) сигналов, повторяющиеся события и ограниченные аналитические ресурсы снижают операционную эффективность. В статье рассматриваются современные подходы к оптимизации процессов, реорганизации рабочих потоков и автоматизации стандартных операций для улучшения управления оповещениями в ЦОС. Одновременно обсуждается применение новых технологий искусственного интеллекта, таких как машинное обучение, обработка естественного языка (NLP), обнаружение аномалий и большие языковые модели, для сортировки, приоритизации и контекстного анализа оповещений, поступающих из источников SIEM/EDR. Кроме того, отмечается влияние SOAR и возможностей оркестровки на аналитические рабочие нагрузки и операционные показатели (например, сокращение MTTR, снижение количества ложных срабатываний, повышение производительности) за счет автоматизированных проверок на основе сценариев реагирования, сбора контекста и ускоренного реагирования на инциденты. Наряду с преимуществами оптимизации процессов и технологий ИИ в управлении оповещениями, анализируются также проблемы и ограничения, такие как качество и дисбаланс данных, дрейф модели с течением времени, требования к валидации и сохранение человеческого контроля над рискованными решениями. В целом, статья представляет собой систематическое исследование, которое подчеркивает синергию оптимизации процессов с новыми технологиями ИИ для более эффективного управления потоком оповещений в SOC и предлагает предложения и рекомендации, основанные на поэтапной структуре внедрения и критериях оценки.

Ключевые слова. *SOC, управление оповещениями, оптимизация процессов, SIEM, EDR, SOAR, машинное обучение, NLP, обнаружение аномалий, большие языковые модели, MTTR.*

Giriş

Müasir dövrdə rəqəmsal transformasiya prosesləri sürətləndikcə, kibertəhlükəsizlik infrastrukturunun əhəmiyyəti də buna mütənasib olaraq artmaqdadır. Hər gün milyonlarla cihaz, server, şəbəkə elementi və bulud xidmətlərindən yaranan loq axınları Təhlükəsizlik Əməliyyatları

Mərkəzlərinin (SOC) üzərinə böyük analiz yükü qoyur. Tədqiqatlar göstərir ki, tipik bir SOC analitiki gündəlik orta hesabla 1.000-dən çox xəbərdarlıqla üzləşir, bunların isə böyük əksəriyyəti yanlış müsbət (false positive) siqnallardır (1).

Bu vəziyyət bir sıra ciddi problemlərə yol açır: analitik yorğunluğu (alert fatigue), real təhdidlərin gecikmə ilə aşkar edilməsi, əməliyyat xərclərinin artması və kadr resurslarının qeyri-səmərəli istifadəsi. Belə şəraitdə ənənəvi, əl əməyinə dayanan xəbərdarlıq idarəetməsi yanaşmaları öz aktuallığını itirmiş, avtomatlaşdırma və süni intellekt texnologiyalarına əsaslanan yeni həllərin tətbiqi zəruri hala gəlmişdir.

Məqalənin məqsədi SOC-da xəbərdarlıq idarəetməsinin müasir çağırışlarını sistematik şəkildə analiz etmək, proses optimizasiyası metodlarını nəzərdən keçirmək, AI/ML texnologiyalarının bu sahədəki tətbiq imkanlarını qiymətləndirmək və praktiki tövsiyələr hazırlamaqdır. Araşdırma həm nəzəri, həm də tətbiqi aspektləri əhatə edir.

SOC-un Strukturu və Funksiyaları. Təhlükəsizlik Əməliyyatları Mərkəzi (SOC - Security Operations Center) bir təşkilatın kibertəhlükəsizlik hadisələrini real vaxt rejimində monitorinq edən, aşkar edən, araşdıran və onlara cavab verən ixtisaslaşmış bir bölmə və ya xidmətdir. SOC-un əsas funksional komponentləri aşağıdakılardır:

Hadisə aşkarlama və monitorinq: SIEM, IDS/IPS, EDR sistemlərindən toplanan məlumatların fasiləsiz izlənməsi;

İlkin qiymətləndirmə və prioritetləşdirmə: daxil olan xəbərdarlıqların həcm, ciddilik dərəcəsi və kontekstə görə sıralanması;

İnsident cavabı: aşkar edilmiş hadisələrin araşdırılması, aradan qaldırılması;

Kibertəhdid məlumatlarının inteqrasiyası: xarici təhdid məlumatlarının (threat intelligence feeds) daxili məlumatlara tətbiqi;

Hesabatlılıq və uyğunluq: müvafiq standartlar (ISO 27001, NIST, PCI DSS) çərçivəsində hesabatların hazırlanması.

SOC-lar adətən üç pilləli (Tier 1, Tier 2, Tier 3) iyerarxik model üzrə fəaliyyət göstərir. Tier 1 analitikləri ilkin qiymətləndirmə və rutin filtrləmənin, Tier 2 mütəxəssisləri daha dərin araşdırmaların, Tier 3 ekspertləri isə mürəkkəb insidentlərin idarəsinin və proaktiv axtarışın (threat hunting) üzərindədir (2).

Xəbərdarlıq İdarəetməsinin Əsas Problemləri. Müasir SOC mühitlərinin üzləşdiyi başlıca çağırışlar aşağıdakı kateqoriyalara bölünür:

Həcm problemi: Şəbəkə ölçüsündən asılı olaraq, bir SOC gündəlik on minlərlə xəbərdarlıq qəbul edə bilər. Bu həcmi insan resursları ilə effektiv şəkildə idarə etmək praktik olaraq mümkün deyil. Verizon 2023 DBIR hesabatına görə, orta ölçülü bir müəssisənin SOC-u aylıq 100.000-dən çox xəbərdarlıq qeydə alır.

Yanlış müsbət siqnalların yüksək nisbəti: Tədqiqatlar göstərir ki, SOC xəbərdarlıqlarının 40%-dən 90%-ə qədər hissəsi yanlış müsbət siqnallardır. Bu, analitiklərin əsl təhdidlərə konsentrasiya imkanını ciddi məhdudlaşdırır. Analitik yorğunluğu (alert fatigue) adlanan bu fenomen zamanla həqiqi insidentlərin də diqqətsiz qalmasına səbəb ola bilər (4).

Kontekst çatışmazlığı: Ayrı-ayrı xəbərdarlıqlar çox zaman lazımi kontekstdən məhrum şəkildə təqdim olunur. Analitik bir xəbərdarlığın kritik mi, yoxsa rutin bir hal mı olduğunu müəyyənləşdirmək üçün bir neçə sistemdən əlavə məlumat toplamaq məcburiyyətindədir.

Kadr çatışmazlığı: Kibertəhlükəsizlik sahəsindəki ixtisaslı mütəxəssislər üzrə qlobal miqyasda ciddi çatışmazlıq mövcuddur. ISC² hesabatına görə, 2023-cü ildə dünyada 3,4 milyon kibertəhlükəsizlik mütəxəssisinin çatışmazlığı qeydə alınmışdır (5).

Proses optimallaşdırması yanaşmaları

İş Axınlarının Yenidən Qurulması. SOC əməliyyatlarının səmərəliliyini artırmaq üçün proses optimizasiyası ilk atılacaq addımdır. Bu sahədə tətbiq olunan başlıca metodologiyalar aşağıdakılardır:

Lean metodologiyası SOC-larda aradan qaldırılmalı israfları (muda) müəyyənləşdirmək üçün geniş istifadə olunur. Bunlara dublikat araşdırmalar, standartlaşdırılmamış prosedurlar və gecikmiş kommunikasiya daxildir. Xəbərdarlıq mərhələsini standartlaşdırmaq, cavab playbook-larını

müəyyənləşdirmək və ilkin qiymətləndirmə meyarlarını aydın şəkildə təyin etmək proses optimizasiyasının əsasını təşkil edir (6).

Hadisə Prioritetləşdirmə Matrisi: Risk əsaslı prioritetləşdirmə üçün xəbərdarlıqlar iki ölçüt üzrə qiymətləndirilir - təsir potensialı (varlığın kritikliyi, məxfiliyin pozulması ehtimalı) və etibarlılıq (siqnalın doğruluğu, mənbənin keyfiyyəti). Bu matrisi avtomatik tətbiq etmək analitiklərin yalnız yüksək prioritetli hallara fokuslanmasını təmin edir.

Playbook Standartlaşdırması: Müxtəlif hadisə növləri üçün ətraflı addım-addım prosedurlar (playbook-lar) hazırlamaq həm cavab müddətini azaldır, həm də yeni analitiklərin adaptasiyasını sürətləndirir. Standartlaşdırılmış playbook-lar eyni zamanda SOAR sistemlərinin avtomatlaşdırma əsasını təşkil edir.

SOAR Texnologiyaları ilə Avtomatlaşdırma. SOAR (Security Orchestration, Automation and Response) platformaları SOC-da proses optimizasiyasının texniki sütununu təşkil edir. SOAR sistemlərinin əsas imkanları bunlardır:

Müxtəlif təhlükəsizlik alətlərinin (SIEM, EDR, firewall, threat intelligence platformaları) vahid interfeys altında birləşdirilməsi;

Tez-tez təkrarlanan araşdırma addımlarının (IP sorğusu, hash yoxlaması, istifadəçi tarixçəsinin çəkilməsi) avtomatik icrası;

Xəbərdarlıq kontekstinin zənginləşdirilməsi (enrichment) - xarici təhdid məlumatları ilə avtomatik korrelasiya;

Avtomatik cavab hərəkətlərinin icrası - şübhəli cihazın şəbəkədən kənarlaşdırılması, hesabın bloklanması;

İnsident sənədləşməsinin avtomatik yaradılması.

Tədqiqatlar göstərir ki, SOAR tətbiqi orta hesabla MTTR-i (Mean Time to Respond) 85%-ə qədər azalda, analitik iş yükünü isə 70%-ə qədər yüngülləşdirə bilər (7). Lakin SOAR-ın effektivliyi keyfiyyətli playbook-ların mövcudluğundan və sistemlər arası inteqrasiyanın düzgün qurulmasından birbaşa asılıdır.

Süni intellekt texnologiyalarının tətbiqi

Maşın Öyrənməsi Əsaslı Anomaliya Aşkarlanması. Maşın öyrənməsi (ML) SOC xəbərdarlıq idarəetməsini kökündən dəyişdirmə potensialına malik bir texnologiyadır. ML modellərinin bu sahədəki tətbiq istiqamətləri aşağıdakılardır:

UEBA (User and Entity Behavior Analytics): İstifadəçi və qurğuların normal davranış profilini öyrənən ML modelləri, bu profillərdən kənarlaşmaları (anomaliyaları) avtomatik aşkar edə bilir. Məsələn, bir istifadəçinin iş saatlarından kənarda giriş cəhdləri, qeyri-adi faylların yüklənməsi kimi anomaliyalar ML vasitəsilə daha yüksək dəqiqliklə müəyyənləşdirilir (8).

Korrelyasiya modelləri: Müxtəlif mənbələrdən (firewall, DNS, e-poçt, endpoint) gələn siqnalları bir-biri ilə əlaqələndirən ML modelləri ayrı-ayrılıqda şübhəsiz görünən hadisələrin birlikdə bir hücum zəncirini (kill chain) təşkil etdiyini müəyyən edə bilir. Bu yanaşma xüsusilə APT (Advanced Persistent Threat) kimi gizli hücumların aşkarlanmasında effektivdir.

Xəbərdarlıq prioritetləşdirməsi üçün ML: Tarixi insident məlumatları əsasında öyrədilmiş modellər yeni xəbərdarlıqların ciddilik dərəcəsini proqnozlaşdıra, yanlış müsbət olma ehtimalını qiymətləndirə bilər. Bu, analitiklərin diqqətini həqiqətən vacib hadisələrə yönəltməyə kömək edir.

Təbii Dil Emalı (NLP) Tətbiqləri. NLP texnologiyaları SOC-da bir neçə vacib funksiyaya xidmət edir:

Loq analizi: Strukturlaşdırılmamış loq məlumatlarından semantik anlam çıxarmaq, loqlardakı insan tərəfindən yazılmış mesajları və ya xəta kodlarını kontekstual olaraq başa düşmək NLP-nin əsas imkanlarındandır. Bu, xüsusilə böyük həcmli loq axınlarında anomal dil nümunələrinin aşkarlanmasında faydalıdır.

Threat intelligence emalı: Kibertəhdid hesabatları, OSINT mənbələri, dark web forumları kimi mətn məlumatlarından avtomatik olaraq mənalı kəşfiyyat məlumatlarının (IOC-lar, TTPS, zərərli proqram adları) çıxarılmasında NLP mühüm rol oynayır.

İnsident hesabatlarının avtomatik yaradılması: Araşdırma prosesini avtomatik izləyən NLP sistemləri insident sonunda ətraflı hesabatın avtomatik hazırlanmasını təmin edə bilər, bu isə analitiklərin sənədləşmə yükünü xeyli azaldır.

Böyük Dil Modelləri (LLM) ilə Yeni İmkanlar. GPT sinifli böyük dil modelləri (LLM) SOC əməliyyatlarına tamamilə yeni bir perspektiv gətirir. LLM-lərin bu sahədəki əsas tətbiqetmə istiqamətləri bunlardır:

Analitik köməkçisi: LLM-lər analitikə xəbərdarlığın təhlilini sadə dillə izah edə, şübhəli fəaliyyətin mümkün texnikalarını (MITRE ATT&CK çərçivəsinə uyğun olaraq) müəyyənləşdirə, növbəti araşdırma addımlarını tövsiyə edə bilər. Bu, xüsusilə Tier 1 analitikləri üçün böyük dəstək deməkdir.

Playbook generasiyası: LLM-lər yeni hadisə növləri üçün ilkin playbook-lar yarada, mövcud playbook-ları aktuallaşdıra bilər. Bu, SOC proseslərinin dinamik mühitə daha sürətli uyğunlaşmasını təmin edir.

SOC-xüsusi sorğu dili (query) generasiyası: Analitik natural dildə bir sual yazdıqda (məsələn, "son 24 saatda hansı daxili hostlar xarici C2 serverləri ilə əlaqə saxlayıb?"), LLM bunu avtomatik olaraq SIEM-in sorğu dilinə (SPL, KQL, Sigma) çevirə bilər (9).

Lakin LLM-lərin tətbiqində diqqət edilməli məqamlar da mövcuddur: hallüsinasiya (yanlış məlumat generasiyası) riski, məxfi məlumatların modelin mühitinə sızması təhlükəsi, habelə kritik təhlükəsizlik qərarlarında insan nəzarətinin qorunması zərurəti bunların başında gəlir.

Tətbiq çərçivəsi və qiymətləndirmə meyarları

Mərhələli Tətbiq Modeli. SOC-da xəbərdarlıq idarəetməsinin təkmilləşdirilməsi üçün mərhələli yanaşma tövsiyə olunur:

I mərhələ - Qiymətləndirmə (1-2 ay): Mövcud xəbərdarlıq həcminin, yanlış müsbət nisbətinin, MTTR-in və analitik iş yükünün ölçülməsi; əsas proses zəifliklərinin müəyyənləşdirilməsi; texniki borcun (technical debt) qiymətləndirilməsi.

II mərhələ - Proses optimizasiyası (2-4 ay): Xəbərdarlıq mərhələsinin meyarlarının standartlaşdırılması; hadisə kateqoriyaları üzrə playbook-ların hazırlanması; SOAR platformasının seçilməsi və birinci partiya inteqrasiyalarının qurulması; rutin, aşağı riskli xəbərdarlıqlar üçün avtomatik qaydaların müəyyənləşdirilməsi.

III mərhələ - AI/ML inteqrasiyası (4-8 ay): Tarixi məlumatlar əsasında anomaliya aşkarlama modelinin öyrədilməsi; UEBA imkanlarının aktivləşdirilməsi; LLM əsaslı analitik köməkçisinin pilot tətbiqi; NLP əsaslı threat intelligence toplamanın qurulması.

IV mərhələ - Optimizasiya və genişlənmə (davamlı): Model performansının daimi monitorinqi; model drift-nin aşkarlanması və modellərin yenilənməsi; yeni texnologiyaların izlənməsi; komanda bacarıqlarının inkişafı.

Əsas Performans Göstəriciləri (KPI). SOC xəbərdarlıq idarəetməsinin səmərəliliyini qiymətləndirmək üçün aşağıdakı əsas göstəricilər izlənməlidir:

- MTTR (Mean Time to Respond) - orta cavab müddəti; mümkün hədəf: 50-70% azalma;
- MTTD (Mean Time to Detect) - aşkarlama müddəti; mümkün hədəf: 40-60% azalma;
- Yanlış müsbət nisbəti - mümkün hədəf: 50-80% azalma;
- Analitik başına emal edilən xəbərdarlıq sayı - mümkün hədəf: 2-3 dəfə artım;
- Qaçırılmış insidentlər (missed detections) - mümkün hədəf: sıfıra yaxınlaşma;

Çətinliklər və məhdudiyyətlər. Proses optimizasiyası və AI texnologiyalarının SOC-a inteqrasiyası bir sıra ciddi çağırışları özü ilə gətirir:

Məlumat keyfiyyəti və balanssızlığı: ML modellərinin effektivliyi birbaşa öyrətmə məlumatlarının keyfiyyətinə bağlıdır. SOC mühitlərindəki məlumatlar çox zaman balanssız, natamam və ya düzgün etiketlənməmiş olur. Bu, modelin öyrənmə prosesini çətinləşdirir.

Model drift problemi: Kibertəhdid landşaftı daim dəyişir - yeni hücum texnikaları, sıfır günlük (zero-day) zəifliklər, yeni konfiqurasiyalar meydana çıxır. Sabit bir modelin zamanla dəqiqliyi aşağı düşür (model drift). Bu problemi həll etmək üçün daimi yenidən öyrəmə (retraining) prosesləri qurulmalıdır.

İzaholunma (explainability) tələbləri: Çoxlu parametrli "qara qutu" (black box) ML modellərinin verdiyi qərarları insan analitiklərinə izah etmək çox zaman çətin olur. Analitiklər yalnız bir skoru deyil, qərarın əsaslandığı konkret əlamətləri (features) görmək istəyir. XAI (Explainable AI) yanaşmaları bu problemi qismən həll etsə də, sahə hələ inkişaf mərhələsindədir (10).

İnsan nəzarətinin qorunması: Yüksək riskli qərarlarda (bir hostun şəbəkədən kənarlaşdırılması, hesabın bloklanması) tam avtomatlaşdırma yanlış müsbət halda ciddi əməliyyat problemlərinə yol açа bilər. Belə hallarda insan təsdiqini tələb edən hibrid model tövsiyə olunur.

Məxfilik və təhlükəsizlik: LLM-lərdən istifadə edərkən məxfi xəbərdarlıq məlumatlarının, IP ünvanların, istifadəçi adlarının xarici modellərə göndərilməsi məxfilik riski yaradır. Yerli (on-premise) yerləşdirilmiş modellər bu riski azaltsa da, hesablama xərclərini artırır.

Nəticə

Bu tədqiqat göstərir ki, SOC-da xəbərdarlıq idarəetməsinin təkmilləşdirilməsi heç bir tək bir texnologiya və ya metodik dəyişikliklə əldə edilə bilməz. Əsaslı nəticə o deməkdir ki, proses optimizasiyası ilə AI texnologiyalarının sinerjisi SOC-un əməliyyat yetkinliyini keyfiyyətcə yeni bir səviyyəyə çıxarmaq potensialına malikdir.

Tədqiqat əsasında aşağıdakı tövsiyələr irəli sürülür:

Birinci olaraq, hər hansı texniki investisiya etməzdən əvvəl mövcud proseslərin hərtərəfli auditini aparmaq; prosesin zəif halqalarını müəyyənləşdirmək; playbook-ları standartlaşdırmaq vacibdir. Texnologiya köhnə proseslərin üzərindən qurulanda ancaq onları avtomatlaşdırır.

İkinci olaraq, SOAR tətbiqini prioritet kimi müəyyənləşdirmək tövsiyə olunur. SOAR, öyrətmə məlumatlarına ehtiyac duymadan dərhal effekt verə bilən bir texnologiyadır. İlkin avtomatlaşdırma ssenarisi kimi aşağı riskli, yüksək həcmli xəbərdarlıq kateqoriyaları (məsələn, AV xəbərdarlıqları, rutin port skanetmə) seçilməlidir.

Üçüncü olaraq, ML modelləri üçün tarixi məlumatların etiketlənməsinə vaxtında başlamaq lazımdır. Analitiklər ilkin qiymətləndirmə qərarlarını qeydə aldıqca, bu məlumatlar gələcək modelin öyrəmə bazasını təşkil edəcək. Bu investisiya zamanla çox böyük müsbət təsir verəcəkdir.

Dördüncü olaraq, LLM tətbiqini pilotla başlamaq, daha sonra genişlətmək tövsiyə olunur. İlk mərhələdə LLM-ni yalnız analitikə köməkçi olaraq (copilot) tətbiq etmək, kritik qərarlarda həmişə insan nəzarətini qorumaq məsləhətdir.

Beşinci olaraq, süni intellekt sistemlərinin etibarlılığını və düzgünlüyünü daimi monitorinq etmək, model drift-ni aşkarlamaq üçün avtomatik alarmlar qurmaq vacibdir.

Nəticə olaraq, kibertəhlükəsizlik müdafiəsi texnoloji irəliləyişi əks etdirən hücum metodlarına qarşı durmaq üçün yalnız adaptiv, öyrənən və süni intellektlə gücləndirimiş SOC-lar effektiv ola bilər. Bu transformasiya nə qiymətsiz bir investisiyadır, nə də bir gecəlik bir dəyişiklik. Bu, müasir təşkilatların kibertəhlükəsizlik dayanıqlılığının vacib şərtidir.

Ədəbiyyat

1. Verizon. (2023). Data Breach Investigations Report. Verizon Business.
2. Muniz, J., McIntyre, G., AlFardan, N. (2015). Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press.
3. SANS Institute. (2023). 2023 SOC Survey. SANS Technology Institute.
4. Operant Networks. (2022). The Alert Fatigue Report: How Alert Overload is Impacting SOC Teams.
5. ISC². (2023). Cybersecurity Workforce Study. ISC² Research.
6. Panetta, K. (2019). Gartner Top 10 Security Projects for 2019. Gartner Inc.
7. Gartner. (2022). Market Guide for Security Orchestration, Automation and Response Solutions. Gartner Research.
8. Exabeam. (2023). State of the SOC Report 2023. Exabeam Inc.

9. Microsoft. (2023). Security Copilot: Empowering defenders at the speed of AI. Microsoft Security Blog.
10. Doshi-Velez, F., Kim, B. (2017). Towards a Rigorous Science of Interpretable Machine Learning. arXiv:1702.08608.
11. Behl, A., Behl, K. (2017). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.
12. Shackleford, D. (2015). Security Operations Centers: Building, Operating, and Maintaining Your SOC.