УДК 004.056:004.77

ПРОЄКТУВАННЯ АВТОМАТИЗОВАНОЇ СИСТЕМИ МОНІТОРИНГУ ПОДІЙ БЕЗПЕКИ В ХМАРНІЙ СИСТЕМІ MICROSOFT AZURE

Бабенко М.В., к.т.н., доцент[1]; Бабенко Ю.М., доктор філософії[2], Тютюнніков М.В.[3]
[1]Дніпровський державний технічний університет; [2,3]Київський національний університет імені Тараса Шевченка
[1]Україна, Кам'янське; [2,3]Україна, Київ
[1]mvbab@ukr.net; [2]yurii.babenko@knu.ua; [3]maksimtutunnikov507@gmail.com

Анотація. *В даній роботі представлено проєкт та впровадження автоматизованої системи моніторингу подій безпеки у Microsoft Azure з використанням Microsoft Sentinel, Azure Monitor і Log Analytics. Запропоновано архітектуру збору, нормалізації, кореляції (KQL/UEBA) та SOAR-реагування (Logic Apps), включно з мапуванням інцидентів на MITRE ATT&CK. Експериментальна валідація на ATT&CK-емуляціях показала зменшення MTTD/MTTR і шуму FPR, а також контроль вартості логування.*

Ключові слова*: Microsoft Sentinel; Azure Monitor; Log Analytics; KQL; SOAR; UEBA; MITRE ATT&CK; Entra ID; автоматизований моніторинг.*

Вступна частина. Міграція сервісів у хмарні середовища створює багатоканальні потоки подій від ідентичностей, ресурсів та мережевих периметрів. У Microsoft Azure ключовими джерелами є Entra ID (ex Azure AD), Azure Activity, журнали ресурсів (Storage, Key Vault, SQL), Microsoft Defender та мережеві сервіси (Firewall, WAF). Ручний моніторинг або традиційні SIEM-рішення, спроєктовані для дата-центрів, погано масштабуються під еластичні навантаження та короткоживучі об'єкти хмари, що зумовлює перевантаження SOC і збільшення часу реагування [1-4].

Окрім технічної складності, існують нормативні вимоги до журналювання, зберігання, простежуваності та безперервного моніторингу, описані в ISO/IEC 27001 та настановах NIST щодо лог-менеджменту (NIST SP 800-92) [5] і ISCM (NIST SP 800-137) [6]. Водночас відкриті бази знань MITRE ATT&CK надають таксономію для зіставлення детекцій/інцидентів із тактиками й техніками зловмисників [7].

Мета дослідження – створити та оцінити автоматизовану систему моніторингу подій безпеки для Azure, яка забезпечує раннє виявлення, пріоритизацію та автоматизоване реагування на інциденти з мінімізацією хибних спрацювань і прозорим контролем вартості зберігання логів; забезпечити відповідність методичним вказівкам ISO/IEC 27001 і NIST.

Основна частина. Наявні практики часто обмежуються простими «плоскими» правилами або базовими алертами з окремих джерел, що ігнорує контекст користувача та активів, призводить до високого FPR і розмиття пріоритетів. Інші рішення не враховують вартісної моделі Azure та збирають надлишкові журнали без нормалізації, що збільшує TCO. Запропонований підхід робить акцент на кореляції подій на рівні ідентичності та активів, enrichment за watchlists/CMDB, а також на cost-aware логуванні.

В якості джерел даних виступають: Entra ID, Azure Activity, Defender for Cloud/Endpoint, M365, мережеві журнали, журнали ресурсів. Збір реалізовано через Diagnostic Settings та конектори, доставка – до Log Analytics за допомогою Data Collection Rules. Нормалізація та збагачення виконуються шляхом парсингу полів, уніфікації часових поясів і приєднання довідників (watchlists). Аналітичний шар побудовано у Microsoft

Sentinel: кореляції на KQL, UEBA для аномалій, scheduled rules для оперативних детекцій, hunting queries для проактивного пошуку. Реакція – через Logic Apps (SOAR) з гілкуванням за severity/ATT&CK та інтеграцією до ITSM [8].

У спроектованій автоматизованій системі моніторингу подій безпеки в хмарній системі Microsoft Azure в якості архітектури рішення використовується наступний потік даних: джерела → Diagnostic Settings/Event Hub → Log Analytics Workspace → правила кореляції/UEBA → інциденти → автоматизація (Automation Rules/Logic Apps) → ITSM. Рішення включає політики ретенції та архівації (дешевші шари зберігання), а також робочі книги (Workbooks) для візуалізації MTTD/MTTR, покриття ATT&CK і вартості за джерелами.

В якості прикладу проєктування детекцій наведемо сценарій «Impossible Travel»: кореляція послідовних успішних входів у короткому вікні з географічно несумісних регіонів для одного користувача; додається контекст довірених мереж, статус MFA, risk score користувача. Інші кейси: MFA fatigue (підрядні push-запити), token theft (анонімні/нехарактерні User-Agent), privilege escalation (role assignments), ексфільтрація зі сховищ.

Приклад спрощеного KQL-запиту для «Impossible Travel» (фрагмент):

```
SigninLogs
| where ResultType == 0
| project UserPrincipalName, TimeGenerated, IPAddress, Location
| order by UserPrincipalName asc, TimeGenerated asc
| serialize
| extend PrevTime=prev(TimeGenerated), PrevLoc=prev(Location)
| where UserPrincipalName == prev(UserPrincipalName) and datetime_diff('minute', TimeGenerated, PrevTime) between (0 .. 60)
| invoke geo_distance_km(Location, PrevLoc)
| where geo_distance_km > 1000
```

SOAR-плейбуки реалізують автоматичне закриття сесій, блокування IP, тимчасове призупинення облікового запису, створення тікету, повідомлення аналітику та запит додаткових артефактів через Graph/Defender API. Гілкування за severity, достовірністю та критичністю активу скорочує ручну працю Tier-1/2 і підвищує повторюваність процедур.

Для проведення експериментальної валідації було змодельовано декілька сценаріїв ATT&CK (Initial Access, Credential Access, Lateral Movement, Exfiltration) з відтворенням аномальних входів, MFA fatigue, нехарактерних User-Agent, змін ролей та операцій над сховищами. Порівнювали базову конфігурацію проти удосконаленої: спостерігалося зменшення MTTD з ~15 хв до ≤5 хв, MTTR – з ~120 хв до ~45–60 хв; TPR зріс на ~12–18%, FPR зменшився на ~20–30% за рахунок контекстуалізації та фільтрації шуму. Додатково оцінено вплив політик ретенції/архівації на бюджет логування.

Обмеження автоматизованої системи включають залежність від якості журналів джерел і можливі затримки інгесту; високі навантаження можуть вимагати перегляду DCR і квот. В перспективі подальшої роботи розглядається використання поведінкових моделей з урахуванням сезонності, автоматизований тестовий стенд для постійної валідації детекцій, а також розширення на мультихмарні середовища.

Висновки. Запропонована система перетворює розрізнені журнали Azure на керовані інциденти з прогнозованими витратами, зменшуючи MTTD/MTTR, знижуючи FPR і підвищуючи стійкість організації. Підхід узгоджується з ISO/IEC 27001, NIST SP 800-92/137

та структурований відповідно до MITRE ATT&CK, забезпечуючи як технічні, так і процесні вигоди для SOC та CISO.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] *Microsoft Sentinel documentation*. (б. д.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/en-us/azure/sentinel/

[2] Dakić, V., Morić, Z., Kapulica, A., & Regvart, D. (2024). Leveraging Microsoft sentinel and logic apps for automated cyber threat response. *Edelweiss Applied Science and Technology*, 8(6), 4319–4348. https://doi.org/10.55214/25768484.v8i6.2933

[3] Garudasu, S., Arulkumaran, R., Pagidi, R. K., Singh, S. P., Kumar, S., & Jain, S. (2024). Integrating Power Apps and Azure SQL for Real-Time Data Management and Reporting. *Journal of Quantum Science and Technology*, 1(3), 86–116. https://doi.org/10.63345/jqst.v1i3.110

[4] Sanugommula, H. (2024). Azure AKS CRUD Related Issues: Identification, Logging, Resolution, Examples, and Documentation. *Interantional Journal of Scientific Research in Engineering and Management*, 08(12), 1–5. https://doi.org/10.55041/ijsrem9545

[5] *SP 800-92, Guide to Computer Security Log Management*. (б. д.). NIST Computer Security Resource Center. https://csrc.nist.gov/pubs/sp/800/92/final

[6] *SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations*. (б. д.). NIST Computer Security Resource Center. https://csrc.nist.gov/pubs/sp/800/137/final

[7] *MITRE ATT&CK®*. (б. д.). MITRE ATT&CK® Enterprise Matrix. https://attack.mitre.org/

[8] *Azure Logic Apps documentation*. (б. д.). Microsoft Learn: Build skills that open doors in your career. https://learn.microsoft.com/uk-ua/azure/logic-apps/?view=azurenotificationhubs-1.0.7

Babenko Mykhailo[1], Babenko Yurii[2], Tiutiunnikov Maksym[3]

Automated Security Event Monitoring System in Microsoft Azure

Abstract. *The paper presents a reference architecture and practical implementation of an automated security event monitoring system for Microsoft Azure using Microsoft Sentinel, Azure Monitor, and Log Analytics. The solution enables cost-aware data collection via DCR, context-enriched KQL/UEBA detections mapped to MITRE ATT&CK, and SOAR playbooks implemented with Logic Apps. Evaluation with ATT&CK emulations demonstrates improved TPR, reduced FPR, and lower MTTD/MTTR.*

Keywords: *Microsoft Sentinel; Azure Monitor; Log Analytics; KQL; SOAR; UEBA; MITRE ATT&CK; Entra ID; automated monitoring.*