КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.903
УДК 004.056

Тишик Іван Ярославович
кандидат технічних наук, доцент кафедри захисту інформації
Національний університет «Львівська політехніка», Львів, Україна
ORCID ID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

ПІДХОДИ ЩОДО ВДОСКОНАЛЕННЯ СИСТЕМ МОНІТОРИНГУ КІБЕРЗАГРОЗ У КОРПОРАТИВНИХ МЕРЕЖАХ

Анотація. У роботі досліджено теоретичні основи та практичні аспекти впровадження систем моніторингу кіберзагроз у корпоративних інформаційних системах. Проаналізовано їхню роль у забезпеченні інформаційної безпеки організації, розглянуто сучасні підходи до виявлення загроз і актуальні тенденції розвитку систем моніторингу кіберзагроз у корпоративних мережах. Особливу увагу приділено ролі моніторингу як ключового елементу корпоративної безпеки, що забезпечує постійний контроль за мережевою активністю, інформаційними системами та кінцевими пристроями. Такий підхід дає змогу своєчасно виявляти потенційні загрози та оперативно реагувати на них. Застосування сучасних аналітичних інструментів і технологій дозволяє ідентифікувати аномальні дії та підозрілі патерни, які можуть свідчити про спроби несанкціонованого доступу, інфікування шкідливим програмним забезпеченням або реалізацію внутрішніх загроз. Постійне спостереження за станом інформаційної інфраструктури сприяє своєчасному виявленню вразливостей і усуненню ризиків до того, як вони спричинять витік даних, призведуть до фінансових втрат або заподіють шкоду для репутації. Проаналізовано недоліки традиційних засобів кіберзахисту, які часто виявляються неефективними при розпізнаванні складних, динамічних загроз. З огляду на це запропоновано сучасні підходи до моніторингу та реагування на кіберінциденти, що включають використання новітніх інструментів та алгоритмів виявлення несанкціонованих втручань. Представлені рішення спрямовані на підвищення ефективності кіберзахисту в умовах зростаючої складності ландшафту кіберзагроз. Систематичне документування і аналіз подій безпеки дозволяють формувати достовірний звіт аудиту про поточний стан інформаційної системи, що є важливим під час розслідування інцидентів. Основну увагу приділено технічній реалізації систем моніторингу, інтеграції алгоритмів машинного навчання, використанню віртуальних середовищ для моделювання атак та побудові архітектури захищених корпоративних мереж. Також запропоновано практичні рекомендації щодо підвищення ефективності моніторингу загроз, зокрема шляхом впровадження автоматизації та штучного інтелекту.

Ключові слова: кіберзагроза; кіберзахист; пристрої інтернет речей; хмарний сервіс; проактивний моніторинг; машинне навчання

ВСТУП

Стрімкий розвиток цифрових технологій суттєво трансформував функціонування бізнесу та об’єктів критичної інфраструктури, відкривши нові можливості для підвищення ефективності й упровадження інновацій. Проте цифровізація також спричинила ускладнення їх структури та зростання кіберзагроз. Особливо вразливими в цьому контексті стали корпоративні мережі, оскільки в основному вони забезпечують зберігання й обробку критичної для організації інформації. Це зумовило потребу у впровадженні надійних механізмів кіберзахисту, що, у свою чергу, активізувало розвиток систем моніторингу кіберзагроз, здатних виявляти та нейтралізувати загрози в реальному часі.

У сучасному світі, де цифрові мережі стають невід’ємною частиною існування людства, їх безпека стає першочерговою проблемою багатьох корпорацій. Інтернет

відкрив перед бізнесом безліч можливостей для збільшення прибутковості своєї діяльності. Однак у світі, де цифрова безпека набуває все більшого значення, виявлення та швидке реагування на кіберзагрози має важливе значення. Традиційні методи виявилися неадекватними з точки зору боротьби з динамічним і складним характером сучасних кіберзагроз. Виявлення кіберзагроз є процесом розпізнавання потенційних небезпек і вразливостей у комп'ютерній системі, мережі або цифровому середовищі. Цей процес передбачає використання різних методів, інструментів і методологій для виявлення зловмисних дій, які можуть поставити під загрозу конфіденційність, цілісність або доступність інформації. Основна мета — виявити загрози до того, як вони можуть завдати шкоди або призвести до витоку даних.

Моніторинг є ключовим елементом системи кібербезпеки, що передбачає безперервне спостереження за мережевим трафіком, системними логами та діями користувачів з метою виявлення аномальних шаблонів, які можуть свідчити про наявність кіберзагроз. Системи моніторингу відіграють критичну роль у сучасному кіберзахисті, оскільки дозволяють оперативно виявляти загрози, реагувати на них та мінімізувати потенційні наслідки ще до того, як буде завдано шкоди. Такий моніторинг охоплює широкий спектр заходів, зокрема виявлення інцидентів у реальному часі, обробку даних з журналів подій, а також використання інтелектуальних алгоритмів для виявлення відхилень та загроз у поведінці мережі.

Сучасний кіберпростір характеризується широким спектром небезпек — від традиційного шкідливого програмного забезпечення до складних і тривалих атак типу APT (Advanced Persistent Threats) та програм-вимагачів. Додаткову складність становить стрімке впровадження технологій, таких як хмарні сервіси, пристрої Інтернету речей (IoT) та віртуалізовані середовища, що значно розширюють потенційну поверхню атак. У зв’язку з цим зростає актуальність створення гнучких і технологічно просунутих систем моніторингу, здатних інтегрувати інструменти штучного інтелекту, машинного навчання та автоматизованого аналізу загроз.

Постановка проблеми. З огляду на сказане, постає потреба в удосконаленні засобів кібербезпеки, що зумовлено стрімким зростанням кількості та складності кіберзагроз. Однією з головних проблем є запізніле виявлення атак, що дозволяє зловмисникам завдати значної шкоди до моменту реагування. Крім того, відсутність інтеграції між окремими засобами безпеки та неефективне використання ресурсів унеможливлюють формування цілісної системи захисту. Такі недоліки не лише знижують ефективність реагування на інциденти, але й підвищують ризики порушення цілісності, конфіденційності та доступності критичних даних. Це створює необхідність у розробці практичних підходів до модернізації систем кіберзахисту, які б дозволили підвищити загальний рівень захищеності корпоративних мереж.

Метою роботи є дослідження сучасних підходів та практик щодо вдосконалення систем моніторингу кіберзагроз у корпоративних мережах із акцентом на впровадження новітніх технологій. Основну увагу зосереджено на використанні штучного інтелекту для підвищення ефективності реагування на інциденти, а також на інтеграції різнорідних засобів безпеки з метою створення цілісної системи управління кіберзагрозами.

Аналіз останніх досліджень і публікацій. Багато дослідників у своїх працях акцентують увагу на важливості проактивного моніторингу загроз як наріжного каменю ефективних стратегій кібербезпеки. У дослідженнях часто підкреслюється необхідність безперервного моніторингу мережевої інфраструктури для виявлення загроз у режимі реального часу, що скорочує час реагування на інциденти [1]–[3]. Нині сформована концепція інтеграції технологій машинного навчання та штучного інтелекту з метою

підвищення ефективності виявлення загроз. Такі підходи розглядаються деякими авторами як засіб для точнішого виявлення аномалій та зменшення кількості помилкових спрацювань [4], [5]. Ряд авторів у своїх працях наголошують на необхідності прийняття організаціями цілісного підходу до кібербезпеки, який охоплює як технологічні рішення, так і організаційну політику [6]–[10]. Часто виникають розбіжності щодо ефективності методів виявлення несанкціонованих дій у системі на основі сигнатур у порівнянні з методами виявлення на основі аномалій [11], [12]. У той час як деякі дослідники відстоюють здатність останніх виявляти нові загрози, інші вказують на надійність і швидкість підходів, заснованих на сигнатурних аналізаторах.

Ряд досліджень підкреслює зростаючий тиск на організації щодо дотримання національних та міжнародних норм у сфері захисту даних та кібербезпеки. Наприклад, у працях [9]–[11] наголошується на необхідності дотримання організаціями конкретних стандартів, які складають нормативну основу кібербезпеки. Ці стандарти визначають ролі та обов'язки органів державної влади та приватних суб'єктів у забезпеченні захисту критичної інфраструктури організацій та їх інформаційних систем. Як наслідок зростання кіберзагроз, компанії все частіше впроваджують SIEM–системи для посилення безпеки своєї мережевої інфраструктури [11]. Ці системи збирають та аналізують дані про стан безпеки мережевої інфраструктури з різних її джерел, надаючи інформацію про потенційні загрози в режимі реального часу, що дозволяє завчасно виявляти потенційні інциденти, оперативно реагувати на них та підвищувати загальний рівень кіберстійкості організації. Важливими інструментами для захисту корпоративних мереж залишаються технології IDS та IPS, які широко використовуються для моніторингу мережевого трафіку на предмет підозрілої діяльності, що також надає можливість виявляти та реагувати на загрози в режимі реального часу. На цей час ці технології широко застосовуються організаціями для захисту своєї критичної інфраструктури від дедалі складніших кіберзагроз.

У праці [13] здійснено глибокий огляд систем управління інформаційною безпекою та найкращих практик, які можуть бути застосовані в організаціях будь–якого розміру. Тут розглянуті такі важливі компоненти захисту мережевої інфраструктури, як розробка політики інформаційної безпеки, навчання з питань безпеки та впровадження технічних засобів контролю. Автор у своїй праці наголошує на важливості узгодження практик безпеки з бізнес–цілями для створення стійкої системи інформаційної безпеки для будь-якої організації.

Таким чином, забезпечення безпеки інформаційних систем характеризується динамічною взаємодією між теоретичними основами та технологічними досягненнями. Постійний розвиток як наукових знань, так і технологічних безпекових інструментів має важливе значення для організацій, які прагнуть підвищити свою стійкість до різноманітних кіберзагроз.

РЕКОМЕНДАЦІЇ ЩОДО ОПТИМІЗАЦІЇ СИСТЕМ МОНІТОРИНГУ КІБЕРЗАГРОЗ

Оцінка поточних практик моніторингу в корпоративних мережах виявляє критичні вразливості, які перешкоджають ефективному виявленню та реагуванню на загрози. Однією з найактуальніших проблем є недостатнє охоплення нових векторів загроз, таких як пристрої Інтернету речей (IoT) та хмарні середовища. Пристрої Інтернету речей, завдяки своїй різноманітній функціональності та обмеженим вбудованим засобам безпеки, все частіше стають привабливою мішенню для зловмисників. Багато організацій не поширюють інструменти моніторингу на ці кінцеві точки, створюючи «сліпі зони»,

які можуть бути використані для несанкціонованого доступу або витоку даних. Аналогічно, динамічний і розподілений характер хмарних середовищ створює проблеми для традиційних систем моніторингу, які часто намагаються адаптуватися до складнощів мультихмарних або гібридних хмарних архітектур. Неправильні конфігурації, відсутність видимості та розподілу відповідальності за безпеку між організаціями та постачальниками хмарних послуг ще більше посилюють ризики.

Іншою важливою проблемою є неефективність кореляції даних з різних джерел, що підриває здатність виявляти загрози в режимі реального часу. Корпоративні мережі генерують величезні обсяги даних з різних кінцевих точок, додатків і систем, але відсутність безшовної інтеграції та централізованого аналізу перешкоджає ефективному виявленню загроз. Без розширеної кореляції даних команди безпеки можуть зіткнутися з фрагментарними уявленнями, що призводить до затримок у реагуванні та підвищує ймовірність успішних порушень. Така затримка особливо небезпечна у випадку складних атак, таких як експлойти нульового дня, які вимагають швидких і рішучих дій. Ці виклики підкреслюють нагальну потребу в модернізації практик моніторингу, які включають передові технології, такі як машинне навчання та штучний інтелект, що забезпечить всебічне охоплення та аналіз в режимі реального часу. Усуваючи прогалини в моніторингу Інтернету речей і хмарних технологій та покращуючи кореляцію даних, організації можуть підвищити здатність виявляти і зменшувати ймовірність виникнення загроз.

Проблеми з масштабуванням систем моніторингу корпоративних мереж є критичною перешкодою для підтримки надійної кібербезпеки в міру зростання організацій і ускладнення їх інфраструктури. Одна з ключових труднощів полягає в адаптації існуючих систем моніторингу організації при розширені її мережевої інфраструктури, що часто призводить до появи нових кінцевих точок, сервісів і користувачів в мережі. Застарілі системи, побудовані зі статичними конфігураціями і обмеженою масштабованістю, намагаються безперешкодно інтегрувати з новими технологіями або платформами. Відсутність адаптивності створює прогалини в моніторингу, роблячи розширені ділянки мережі вразливими до нових загроз. Крім того, експоненціальне зростання обсягів даних, що генеруються великими мережами, створює проблеми з ефективним управлінням та аналізом цих даних без шкоди для точності виявлення. Висока пропускна здатність кінцевих точок, пристроїв Інтернету речей, хмарних додатків і мережевого трафіку може перевантажити інструменти моніторингу, що призводить до погіршення їх продуктивності та збільшення часових затримок у виявленні загроз. Вимоги до обробки даних великомасштабної аналітики часто потребують значних обчислювальних ресурсів, які можуть бути недоступні в існуючій інфраструктурі.

Традиційні системи моніторингу, включаючи застарілі рішення для управління інформацією та подіями безпеки (SIEM), не здатні ефективно захоплювати та аналізувати специфічний трафік, який генерується пристроями Інтернету речей, а також динамічний, багатокористувацький трафік хмарних середовищ. Нові дослідження показують, що інтеграція спеціалізованих інструментів моніторингу, таких як системи виявлення загроз для IoT і хмарні платформи безпеки (наприклад, AWS GuardDuty, Azure Security Center), може запропонувати нові, більш ефективні способи подолання цього розриву. Крім того, дослідження розподіленого виявлення аномалій з використанням федеративного машинного навчання для периферійних пристроїв і хмарних систем показують, перспективність виявлення загроз без шкоди для продуктивності і конфіденційності.

Amazon GuardDuty поєднує машинне навчання (ML) та інтегровану аналітику загроз від AWS (Amazon Web Services) і провідних сторонніх постачальників для захисту акаунтів, робочих навантажень і даних AWS. Основна функція AWS GuardDuty полягає

ISSN 2663 - 4023

у забезпеченні безперервного виявлення та моніторингу загроз для середовищ AWS. Він аналізує журнали AWS CloudTrail, журнали VPC Flow Logs та DNS, щоб виявити зловмисну активність, таку як незвичні виклики API, скомпрометовані екземпляри та несанкціонований доступ до даних (рис. 1). GuardDuty використовує машинне навчання, розпізнавання аномалій та аналітику для виявлення потенційних загроз, пропонуючи організаціям розуміння стану їхньої безпеки в режимі реального часу і дозволяючи їм оперативно реагувати на інциденти безпеки. Він допомагає зменшити складність виявлення загроз у хмарних середовищах, надаючи автоматизовані сповіщення та дієві ідеї для команд безпеки.

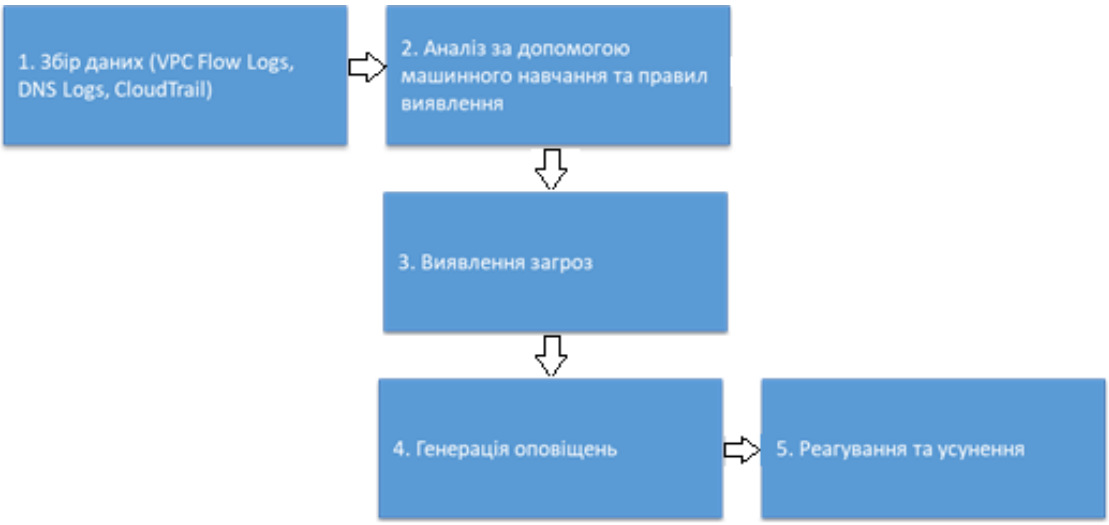

Рис. 1. Етапи роботи Amazon GuardDuty

З метою підвищення ефективності виявлення загроз та автоматизації реагування на інциденти AWS GuardDuty доцільно інтегрувати зі службою AWS Lambda, що дозволить командам безпеки швидко усунути загрози, не вдаючись до ручного втручання. Така інтеграція гарантує, що мережеве середовище AWS не тільки відстежуватиметься на наявність загроз, але й надасть можливість вживати негайних автоматизованих заходів для блокування зловмисної активності, скорочуючи час між виявленням і реагуванням.

Для виявлення несанкціонованого доступу за допомогою AWS GuardDuty, наприклад, у разі спроби підключення віддаленого хоста з підозрілою IP-адресою до ресурсів організації, доцільно реалізувати AWS Lambda-функцію, яка автоматично блокуватиме такі IP-адреси. Це може здійснюватися шляхом динамічної зміни правил груп безпеки (Security Groups) або мережевих списків контролю доступу (NACL). Lambda-функцію необхідно налаштувати на автоматичний виклик щоразу, коли GuardDuty створює знахідку, що відповідає визначеним критеріям (наприклад, спроба доступу з невідомої або підозрілої IP-адреси до корпоративних ресурсів у хмарі AWS). Лямбда-функція, написана на Python, може виглядати так:

```
import boto3
ec2 = boto3.client('ec2')
def lambda_handler(event, context):
#Витяг зловмисної IP-адреси з висновків GuardDuty
ip_address = even ['detail'] ['findings'] [0] ['servi ce'] ['action'] ['networkConnectionAction'] ['remoteIpDet ails'] ['ipAddressV4']
```

```
#Блокування шкідливої IP-адресу, оновивши групу безпеки
response = ec2.revoke_security_group_ingress
(
GroupId='sg-03e238a39827553ae',
#Замініть на ідентифікатор вашої групи безпеки
CidrIp=ip_address + '/32', IpProtocol='tcp', FromPort=80,
ToPort=80
)
return response
```

Lambda-функцію можна прив’язати до правила Amazon CloudWatch Events, яке автоматично запускатиме її щоразу, коли GuardDuty зафіксує підозрілу активність. Такий підхід забезпечує повну автоматизацію реакції на події, дозволяючи виконувати заходи реагування без ручного втручання та скорочуючи час усунення інцидентів.

AWS GuardDuty використовується багатьма світовими компаніями, особливо тими, що мають масштабні хмарні інфраструктури. Платформа особливо популярна серед організацій, які повністю або частково мігрували в хмару, або тих, що працюють у мультихмарних середовищах. Великі технологічні компанії, фінансові установи та транснаціональні корпорації часто використовують сервіс для виявлення та моніторингу загроз завдяки їх масштабованості, сповіщенням у режимі реального часу та інтеграції з іншими службами безпеки.

Однією з основних проблем моніторингу кіберзагроз є складність співставлення даних з різних, часто розрізнених джерел. У багатьох організаціях дані про безпеку збираються з кінцевих точок, мережевих пристроїв, брандмауерів, систем виявлення вторгнень (IDS) і додатків. Однак без належної кореляції ці джерела часто працюють ізольовано, що призводить до запізнілого виявлення нових загроз або їх ігнорування. Зі зростанням складності та різноманітності джерел даних у корпоративних мережах (включаючи датчики Інтернету речей, хмарні API та мобільні кінцеві точки) традиційні методи кореляції стають все менш ефективними. Багато систем все ще покладаються на механізми кореляції на основі правил, яким важко аналізувати великі обсяги високошвидкісних потоків даних, що призводить до помилкових спрацьовувань, та затримок у виявленні загроз.

Механізми кореляції на основі правил широко використовуються в сучасних корпоративних мережах як частина систем управління інформацією та подіями безпеки (SIEM) для оптимізації процесів виявлення загроз і реагування на них. Ці механізми функціонують, аналізуючи дані про безпеку відповідно до попередньо визначених правил, щоб виявити шаблони або комбінації подій, які вказують на потенційні загрози. Такі платформи, як Splunk, IBM QRadar та Elastic Security, використовують кореляцію на основі правил для забезпечення моніторингу та оповіщення в режимі реального часу, що робить їх важливими інструментами для підприємств, які керують складними ландшафтами безпеки. Splunk надає гнучку платформу для визначення правил кореляції, використовуючи мову обробки пошуку (SPL). Наприклад, нижче наведений сценарій, який включає в себе кореляцію невдалих спроб входу на різних пристроях для виявлення атак типу brute force:

```
index=security_logs sourcetype=auth_logs action=failure #Пошук невдалої спроби входу у джерелі auth_logs в індексі security_logs
| stats count by src_ip, user #Підсумовується кількість невдалих спроб входу для кожного IP джерела (src_ip) і користувача
```

| where count > 5 *#Фільтрування результатів запитів, які менше 5*
| table src_ip, user, count *#Формування результатів відображення підозрілої IP-адреси, користувача та кількості невдалих спроб*

Після того, як ви отримали запит, який ідентифікує потенційні загрози, такі як повторні невдалі спроби входу, ви можете зробити наступний крок, щоб зробити ваш моніторинг проактивним, створивши оповіщення. Для цього потрібно зберегти запит, налаштувати умови для запуску оповіщення та визначити спосіб отримання сповіщення.

Наступним кроком, після одержання запиту виявлення потенційних загроз (наприклад, повторні невдалі спроби входу), є перехід до проактивного моніторингу шляхом створення оповіщення. Для цього необхідно зберегти запит, визначити умови спрацювання та обрати спосіб доставки сповіщень.

Ще однією платформою, яка може бути використана для кореляції подій на основі правил в гетерогенних корпоративних мережах, є IBM QRadar — потужний інструмент, призначений для управління інформацією та подіями безпеки SIEM. QRadar широко відомий своєю здатністю виконувати глибоку кореляцію подій безпеки з різних джерел даних і можливостями інтеграції для автоматизованого реагування на інциденти. Наприклад, коли персонал організації хоче виявити і відреагувати на атаку типу «груба сила» в системі, зокрема, відстежити більше п'яти невдалих спроб входу з однієї IP-адреси протягом 10-хвилинного періоду, потрібно визначитися з логікою відповідного правила. Налаштувати таке правило в QRadar можна наступним чином: визначити умови події, створити власне правило в QRadar, задати відповідні параметри для фільтрів подій, налаштувати запуск правила «коли подія відповідає наступному фільтру». Для фіксації шаблону перебору, потрібно налаштувати поріг спрацьовування: якщо п'ять або більше подій відбуваються з однієї IP-адреси джерела протягом 10 хвилин.

Після того, як логіка правила визначена, необхідно організувати дії при його спрацюванні. Можна налаштувати QRadar на генерування сигналу про порушення як централізоване оповіщення, що робить його видимим для команди безпеки. Крім того, можна надіслати сповіщення, наприклад, на електронну пошту, або виконати автоматичну дію, запустивши скрипт. Для розширеного реагування на інциденти QRadar дозволяє інтегрувати автоматизацію за допомогою сценаріїв. Наприклад, наступний скрипт, написаний на Python, використовується для блокування підозрілої IP-адреси, взаємодіючи з API зовнішнього брандмауера. Проста функція Python для цієї мети може виглядати наступним чином:

```
import requests
def block_ip(ip_address):
# Приклад блокування IP через API брандмауера
firewall_api = "https://firewall.example.com/block" payload = {"ip": ip_address}
headers = {"Authorization": "Bearer <Your_API_Token>"} response = requests.post(firewall_api, json=payload,
headers=headers)
return response.status_code
# Приклад використання malicious_ip = "192.168.1.1" block_ip(malicious_ip)
```

Цей скрипт можна налаштувати на автоматичний запуск при спрацьовуванні правила користувача, що ефективно блокуватиму шкідливу IP-адресу в режимі реального часу. Скрипт взаємодіє з API брандмауера для додавання IP-адреси до списку

блокування, забезпечуючи швидке усунення виявленої загрози. Здатність QRadar безперешкодно виконувати такі сценарії, які запускаються в результаті виявлення порушень, робить його дуже адаптивним і проактивним рішенням для сучасних операцій з безпеки. Після налаштування правила та автоматизації важливо протестувати конфігурацію. Для цього необхідно згенерувати логи, які відповідають умовам правила, наприклад, кілька невдалих спроб входу з певної IP-адреси протягом певного періоду часу. Потім перевірити функціональність правила, спостерігаючи, чи правильно QRadar генерує порушення і чи виконується пов'язаний з ним скрипт для блокування IP-адреси. Цей наскрізний тест гарантує, що конвеєр моніторингу та реагування функціонує належним чином, забезпечуючи надійний захист від атак типу bruteforce та подібних загроз. Використовуючи можливості QRadar, організації можуть впроваджувати точні правила кореляції та інтегрувати автоматизовані відповіді, щоб посилити свою систему безпеки і скоротити час реагування на нові загрози.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У роботі проаналізовано теоретичні засади, опрацьовано технологічні рішення та дано практичні рекомендації щодо вдосконалення систем моніторингу кіберзагроз в гетерогенних корпоративних мережах з акцентом на використання сучасних інструментів та методів у контексті нових безпекових викликів. Встановлено, що застосування платформи AWS GuardDuty дозволяє організації створити ефективне та масштабоване рішення для моніторингу кіберзагроз, безперервно оцінювати її середовище на наявність аномалій і потенційних ризиків безпеці. У поєднанні з засобами автоматизації, такими як AWS Lambda, організації можуть значно скоротити час реагування та запобігти ескалації інцидентів безпеки. Здійснено порівняння та оцінювання провідних платформ моніторингу кіберзагроз, таких як Splunk та IBM QRadar, з виділенням їх сильних сторін та застосовуваності для конкретних випадків використання. Були надані практичні рекомендації щодо розгортання цих інструментів у корпоративному середовищі, які забезпечують відповідність механізмам кореляції на основі правил. Запропоновані у роботі рішення дають можливість організаціям підвищити рівень безпеки своєї мережевої інфраструктури, знизити ризики виникнення інцидентів та забезпечити відповідність міжнародним стандартам. Впровадження цих рекомендацій відіграватиме вирішальну роль у покращенні стану кібербезпеки, захисті критично важливих активів та підвищенні стійкості до загроз, що постійно еволюціонують.

Напрямки подальших досліджень можуть бути спрямовані на підвищення ефективності виявлення загроз шляхом їх аналізу з використанням штучного інтелекту та машинного навчання, що корінним чином змінить ландшафт кібербезпеки, дозволяючи організаціям ефективніше виявляти несанкціоновані втручання, зменшувати ризики їх появи та в цілому вдосконалити існуючі системи моніторингу кіберзагроз у корпоративних мережах.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Shan, A., & Myeong, S. (2024). Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application. *Sensors*, *24*(15), 4888. https://doi.org/10.3390/s24154888
2. Arash, M., Khanh, L., Hamed, A., & al. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, *232*, December 2024. https://doi.org/10.1016/j.jnca.2024.104004

3. Ali, S., & Seunghwan, M. (2024). Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application. *Sensors (Basel)*, *24*(15), 4888. https://doi.org/10.3390/s24154888
4. Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2020). Adversarial machine learning attacks and defense methods in the cybersecurity domain. *arXiv*. https://doi.org/10.48550/arXiv.2007.02407
5. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA threat landscape 2024: July 2023 to June 2024*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
6. Alotaibi, S., & Furnell, S. (2024). Emerging trends in cybersecurity: A holistic view on current challenges and integrative solutions. *Blockchain Healthcare Today*, *7*. https://doi.org/10.30953/bhty.v7.302
7. Alexei, A., et al. (2022). The holistic approach to cybersecurity in academia. In *CEEeGov '22: Proceedings of the Central and Eastern European eDem and eGov Days* (pp. 106–111). ACM. https://doi.org/10.1145/3551504.3551516
8. Haselmann, T., & Davy, J. (2023). Information security policies compliance in a global setting. *Computers & Security*. https://doi.org/10.1016/j.cose.2023.102944
9. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29
10. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/88435.htm
11. Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1–6.
12. Aldweesh, A., Moustafa, N., & Slay, J. (2021). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy and open issues. *Journal of Network and Computer Applications*, *178*, 102983. https://doi.org/10.1016/j.jnca.2020.102983
13. Khokh, V. D., Meleshko, Ye. V., & Smirnov, O. A. (2017). Research of methods for auditing information security management systems. *Systems of Control, Navigation and Communication: Collection of Scientific Papers*, *1*(41), 38–42.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Ivan Tyshyk
Ph.D, Associate Professor, Associate Professor at the Department of Information Security
National University "Lviv Polytechnic", Lviv, Ukraine
ORCID ID: 0000-0003-1465-5342
ivan.y.tyshyk@lpnu.ua

APPROACHES TO ENHANCING CYBER THREAT MONITORING SYSTEMS IN CORPORATE NETWORKS

Abstract. The paper explores the theoretical foundations and practical aspects of implementing cyber threat monitoring systems in corporate information systems. It analyzes their role in ensuring organizational information security and examines modern approaches to threat detection, along with current trends in the development of cyber threat monitoring systems within corporate networks. Special attention is given to the role of monitoring as a key component of corporate security, providing continuous oversight of network activity, information systems, and endpoint devices. This approach enables timely identification of potential threats and rapid response to emerging incidents. The use of advanced analytical tools and technologies facilitates the detection of anomalous behavior and suspicious patterns that may indicate attempts at unauthorized access, malware infections, or the manifestation of insider threats. Continuous monitoring of the state of the information infrastructure contributes to the early detection of vulnerabilities and mitigation of risks before they result in data breaches, financial losses, or reputational damage. The study highlights the limitations of traditional cybersecurity tools, which often prove inadequate in detecting complex and dynamic threats. In response, modern approaches to monitoring and incident response are proposed, incorporating the use of cutting-edge tools and intrusion detection algorithms. The proposed solutions aim to enhance the efficiency of cybersecurity efforts in the context of an increasingly complex cyber threat landscape. Systematic documentation and analysis of security events enable the generation of reliable audit reports on the current state of the information system, which are essential for incident investigations. The primary focus is placed on the technical implementation of monitoring systems, the integration of machine learning algorithms, the use of virtual environments for attack simulation, and the design of secure corporate network architectures. Additionally, practical recommendations are provided to improve threat monitoring effectiveness, particularly through the adoption of automation and artificial intelligence.

Keywords: cyber threat; cybersecurity; Internet of Things; cloud service; proactive monitoring; machine learning.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Shan, A., & Myeong, S. (2024). Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application. *Sensors*, *24*(15), 4888. https://doi.org/10.3390/s24154888
2. Arash, M., Khanh, L., Hamed, A., & al. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, *232*, December 2024. https://doi.org/10.1016/j.jnca.2024.104004
3. Ali, S., & Seunghwan, M. (2024). Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application. *Sensors (Basel)*, *24*(15), 4888. https://doi.org/10.3390/s24154888
4. Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2020). Adversarial machine learning attacks and defense methods in the cybersecurity domain. *arXiv*. https://doi.org/10.48550/arXiv.2007.02407
5. European Union Agency for Cybersecurity (ENISA). (2024). *ENISA threat landscape 2024: July 2023 to June 2024*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
6. Alotaibi, S., & Furnell, S. (2024). Emerging trends in cybersecurity: A holistic view on current challenges and integrative solutions. *Blockchain Healthcare Today*, *7*. https://doi.org/10.30953/bhty.v7.302
7. Alexei, A., et al. (2022). The holistic approach to cybersecurity in academia. In *CEEeGov '22: Proceedings of the Central and Eastern European eDem and eGov Days* (pp. 106–111). ACM. https://doi.org/10.1145/3551504.3551516

8. Haselmann, T., & Davy, J. (2023). Information security policies compliance in a global setting. *Computers & Security*. https://doi.org/10.1016/j.cose.2023.102944
9. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. https://doi.org/10.6028/NIST.CSWP.29
10. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/88435.htm
11. Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management*, *22*(1), 1–6.
12. Aldweesh, A., Moustafa, N., & Slay, J. (2021). Deep learning approaches for anomaly-based intrusion detection systems: A survey, taxonomy and open issues. *Journal of Network and Computer Applications*, *178*, 102983. https://doi.org/10.1016/j.jnca.2020.102983
13. Khokh, V. D., Meleshko, Ye. V., & Smirnov, O. A. (2017). Research of methods for auditing information security management systems. *Systems of Control, Navigation and Communication: Collection of Scientific Papers*, *1*(41), 38–42.