Міністерство освіти і науки України
Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту

Кафедра кібербезпеки інформаційних систем, мереж і технологій

До захисту допущено
Кафедрою КІСМіТ протокол №____ від «___» грудня 2025 р.

завідувач кафедри Марина ЄСІНА
(підпис) *(ім'я, прізвище)*
«___» грудня 2025 р.

Кваліфікаційна робота

здобувача другого (магістерського) рівня вищої освіти

«Обґрунтування та рекомендації щодо розробки методики захисту корпоративних мереж від сучасних кібератак»

Спеціальність (спеціалізація) 125 «Кібербезпека та захист інформації»

Освітня програма «Безпека інформаційних і комунікаційних систем»

Виконавець Дар'я ДЕГНЕРА

Науковий керівник Марина Єсіна

Харків – 2025

РЕФЕРАТ

Пояснювальна записка до дипломної роботи містить 60 сторінок, 14 рисунків, та 50 джерел за переліком посилань.

Метою дипломної роботи є обґрунтування та формування рекомендацій щодо розробки сучасної методики захисту корпоративних мереж від актуальних кібератак, із урахуванням практичних аспектів функціонування мережевої безпеки та необхідності підвищення кіберстійкості організацій.

У роботі застосовано методи аналізу сучасних кіберзагроз, порівняння фреймворків безпеки, мережеве сканування вразливостей, оцінку конфігурацій, аудит привілейованих облікових записів, аналіз активів та логічної сегментації мережі. Важливим елементом дослідження стала практична частина щодо використання SIEM-системи, яка включала аналіз потоків подій, налаштування збору записів журналів, їх нормалізації, категоризації та моніторингу для виявлення потенційно небезпечної активності.

У результаті роботи розроблено комплексну методику пошуку вразливостей корпоративних мереж, яка поєднує технічні й організаційні підходи до виявлення загроз. Новизна методики полягає в інтеграції практичних рекомендацій із використання SIEM для підвищення ефективності моніторингу, виявлення інцидентів та оптимізації процесів безпеки без необхідності створення спеціальних кореляційних правил. У роботі розглянуто принципи якісного збору даних, підготовки журналів, побудови інформативних подань та організації роботи оператора безпеки.

Запропоновані рекомендації можуть бути використані в IT-відділах, підрозділах інформаційної безпеки та SOC для вдосконалення процесів моніторингу, покращення якості обробки подій і скорочення часу реагування на інциденти. Методика може бути адаптована відповідно до вимог міжнародних стандартів (NIST CSF, ISO/IEC 27001).

Значущість роботи полягає у формуванні практичного підходу до управління мережею та інформаційною безпекою, що дозволяє підвищити рівень виявлення загроз, мінімізувати ризики компрометації та підсилити загальну кіберстійкість компаній. У висновках підтверджено ефективність методики та її застосовність у корпоративних мережах різної складності.

Ключові слова: КІБЕРБЕЗПЕКА, КОРПОРАТИВНІ МЕРЕЖІ, ЗАХИСТ МЕРЕЖІ, ВРАЗЛИВОСТІ, SIEM, ЖУРНАЛИ ПОДІЙ, МОНІТОРИНГ БЕЗПЕКИ, АУДИТ ДОСТУПУ, МЕРЕЖЕВИЙ АНАЛІЗ.

ABSTRACT

The explanatory note to the thesis contains 60 pages, 14 figures and 50 references.

The aim of this thesis is to justify and develop recommendations for creating a modern methodology for protecting corporate networks from current cyberattacks, considering practical aspects of network security and the need to enhance organizational cyber resilience.

The research applies cyber-threat analysis, comparison of security frameworks, network vulnerability scanning, configuration assessment, asset and segmentation analysis, and privileged account auditing. A key element of the practical part includes the use of a SIEM system, focusing on log collection, normalization, categorization, event flow analysis, and monitoring to identify potentially suspicious activity, without developing or applying correlation rules.

As a result, a comprehensive vulnerability assessment methodology for corporate networks has been developed. Its novelty lies in integrating practical SIEM-based monitoring recommendations to improve incident detection, enhance the quality of collected security data, and optimize operator workflows, without the need for building custom correlation logic. The thesis outlines approaches to structured log management, creation of informative dashboards, and organization of effective monitoring processes.

The proposed methodology can be applied in IT departments, security teams, and Security Operations Centers to improve event monitoring, increase visibility of network activity, and accelerate incident response. It can also be aligned with international standards such as NIST CSF and ISO/IEC 27001.

The significance of the work lies in strengthening practical approaches to monitoring corporate networks, reducing risks of compromise, and improving overall cybersecurity posture. The conclusions confirm the effectiveness of the methodology and its applicability in diverse corporate environments.

Keywords: CYBERSECURITY, CORPORATE NETWORKS, NETWORK PROTECTION, VULNERABILITIES, SIEM, EVENT LOGGING, SECURITY MONITORING, ACCESS AUDIT, NETWORK ANALYSIS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

APT – Advanced Persistent Threat, Атака з розширеною постійною загрозою

ARP – Address Resolution Protocol, Протокол визначення адрес

ATT&CK – Adversarial Tactics, Techniques and Common Knowledge, Тактики, техніки й загальні відомості про дії противника

BYOD – Bring Your Own Device, Використання власних пристроїв

CALDERA – MITRE CALDERA Adversary Emulation Platform, Платформа емуляції дій противника MITRE CALDERA

CASB – Cloud Access Security Broker, Проксі безпеки доступу до хмари

CIA – Confidentiality, Integrity, Availability, Конфіденційність, цілісність, доступність

CIS – Center for Internet Security, Центр Інтернет-безпеки

CISCO – Cisco Systems, Сіско Системз

CK – Cybersecurity Knowledge Base, База знань з кібербезпеки

CSF – Cybersecurity Framework, Рамкова модель кібербезпеки

CVE – Common Vulnerabilities and Exposures, Загальні вразливості та експозиції

DB – Database, База даних

DNS – Domain Name System, Система доменних імен

DDoS – Distributed Denial of Service, Розподілена відмова в обслуговуванні

DHCP – Dynamic Host Configuration Protocol, Динамічний протокол конфігурації вузлів

DMZ – Demilitarized Zone, Демілітаризована зона

DoS – Denial of Service, Відмова в обслуговуванні

EDR – Endpoint Detection and Response, Виявлення та реагування на кінцевих точках

FTP – File Transfer Protocol, Протокол передачі файлів

HTTP – HyperText Transfer Protocol, Гіпертекстовий протокол передачі даних

HTTPS – HyperText Transfer Protocol Secure, Захищений гіпертекстовий протокол передачі даних

IDS – Intrusion Detection System, Система виявлення вторгнень

IPS – Intrusion Prevention System, Система запобігання вторгненням

IP – Internet Protocol, Інтернет-протокол

MITRE – MITRE Corporation, Корпорація MITRE

MITM – Man-in-the-Middle, Атака «людина посередині»

MSSP – Managed Security Service Provider, Провайдер керованих послуг безпеки

NIST – National Institute of Standards and Technology, Національний інститут стандартів і технологій США

NIST SP 800-53 – Security and Privacy Controls, Контролі безпеки та приватності

NIST CSF 2.0 – NIST Cybersecurity Framework version 2.0, Рамкова модель кібербезпеки NIST версії 2.0

OSINT – Open Source Intelligence, Розвідка з відкритих джерел

PKI – Public Key Infrastructure, Інфраструктура відкритих ключів

RDP – Remote Desktop Protocol, Протокол віддаленого робочого стола

SIEM – Security Information and Event Management, Управління інформацією та подіями безпеки

SOAR – Security Orchestration, Automation and Response, Оркестрація, автоматизація та реагування на інциденти безпеки

SOC – Security Operations Center, Центр операцій безпеки

SQL – Structured Query Language, Мова структурованих запитів

TCP – Transmission Control Protocol, Протокол керування передаванням

UDP – User Datagram Protocol, Протокол користувацьких датаграм

VLAN – Virtual Local Area Network, Віртуальна локальна мережа

VPN – Virtual Private Network, Віртуальна приватна мережа

XDR – Extended Detection and Response, Розширене виявлення та реагування

ZTA – Zero Trust Architecture, Архітектура нульової довіри

ZTNA – Zero Trust Network Access, Мережевий доступ у моделі нульової довіри

ВСТУП

Сучасний етап розвитку цифрових технологій характеризується стрімким зростанням масштабів використання корпоративних мереж, які стали невід'ємною частиною функціонування більшості організацій. Широке впровадження хмарних сервісів, розподілених інформаційних систем, мобільного доступу та віддаленої роботи значно розширює можливості бізнесу, проте одночасно створює нові загрози, що робить питання забезпечення кібербезпеки критично важливим. Кібератаки стають дедалі складнішими, цілеспрямованими та автоматизованими, а зловмисники активно використовують інтелектуальні інструменти, соціальну інженерію, вразливості у програмному забезпеченні та помилки конфігурацій для досягнення своїх цілей. У таких умовах корпоративні мережі залишаються одним із основних об'єктів атак, що потребує розробки, удосконалення та впровадження надійних методик захисту.

В останні роки кіберзагрози набули системного характеру: кібератаки здійснюються не лише з метою порушення роботи ресурсів чи викрадення даних, але й як засіб економічного та політичного впливу. Зростає кількість інцидентів, пов'язаних із компрометацією облікових записів, використанням шкідливого програмного забезпечення, проникненням до внутрішніх сегментів мережі, підміною трафіку, атак на інфраструктуру Active Directory та експлуатацією zero-day вразливостей. Разом із тим, підвищилася частота атак типу ransomware, які паралізують роботу компаній і завдають суттєвих фінансових збитків. Усе це свідчить про те, що традиційні підходи до захисту корпоративних мереж поступово втрачають ефективність і потребують модернізації.

Для протидії сучасним загрозам організації мають застосовувати багаторівневі, гнучкі та адаптивні системи безпеки, побудовані на комплексному підході. Важливо враховувати не тільки технічні аспекти – такі як мережеві фаєрволи, системи виявлення вторгнень чи засоби сегментації, – але й

організаційні, зокрема підготовку персоналу, створення політик безпеки, аудит конфігурацій та регулярний моніторинг інцидентів. Ефективний захист корпоративної мережі потребує інтеграції сучасних технологій, таких як Zero Trust, багатофакторна автентифікація, поведінкова аналітика та автоматизовані засоби виявлення аномалій. Важливим елементом також є побудова правильної архітектури, що передбачає мінімізацію довіри, ізоляцію критичних активів та постійний контроль доступу.

Однією з ключових проблем, яка актуалізує необхідність цього дослідження, є розрив між реальними потребами корпоративного сектору та рівнем впроваджених засобів кіберзахисту. Багато компаній не мають системного підходу до виявлення вразливостей, а використання застарілих методик, відсутність регулярного тестування безпеки та недостатній рівень обізнаності співробітників значно підвищують ризик успішної атаки. Крім того, у процесі цифрової трансформації організації розширюють мережеву інфраструктуру, додаючи нові точки доступу, що також збільшує площину атаки. У таких умовах важливо мати структуровану, науково обґрунтовану методику захисту корпоративних мереж, яка враховує сучасні загрози, особливості архітектури та специфіку бізнес-процесів.

Наукова значущість роботи полягає в аналізі сучасних кібератак та визначенні підходів, які дозволяють ефективно протидіяти цим загрозам у корпоративному середовищі. Дослідження охоплює не лише технічні аспекти, але й методологічні: побудову процесів забезпечення кібербезпеки, моделювання загроз, впровадження систем моніторингу, формування набору рекомендацій щодо підвищення стійкості мережі. Практична цінність полягає в розробці пропозицій щодо удосконалення мережевої безпеки, які можуть бути інтегровані в реальну інфраструктуру будь-якої організації незалежно від її масштабу та сфери діяльності. Об’єктом дослідження є корпоративні мережі як сукупність апаратних, програмних та організаційних компонентів, що забезпечують обмін інформацією всередині організації. Предметом дослідження виступають методи, підходи та технології, спрямовані на захист таких мереж від сучасних кібератак. Метою

роботи є обґрунтування та формування рекомендацій щодо розробки методики захисту корпоративних мереж, яка відповідатиме актуальним вимогам безпеки та зможе забезпечити надійний захист від актуальних загроз.

Методи дослідження включають аналіз наукових праць, стандартів, міжнародних рекомендацій, огляд сучасних інструментів безпеки, порівняльний аналіз методів захисту та моделювання загроз. Використано комплексний підхід, який дозволяє всебічно оцінити чинники ризику, визначити актуальні проблеми та сформувати оптимальні рекомендації.

Структура роботи складається зі вступу, трьох розділів, висновків та списку використаних джерел. У першому розділі розглядаються основні види сучасних кібератак та їх класифікація. Другий розділ присвячено аналізу існуючих методів захисту корпоративних мереж. У третьому розділі формуються рекомендації щодо розробки методики захисту, а також описуються практичні підходи до її впровадження.

Таким чином, тема дослідження є актуальною та важливою у контексті сучасних викликів кібербезпеки. Дипломна робота спрямована на створення теоретичного та практичного підґрунтя для розробки ефективної методики захисту корпоративних мереж, яка здатна забезпечити високий рівень стійкості до загроз і сприятиме підвищенню загальної кібербезпеки організації.

1 ОГЛЯД, ДОСЛІДЖЕННЯ ТА АНАЛІЗ ТИПІВ СУЧАСНИХ КІБЕРАТАК

1.1 Класифікації кібератак

Кібератака – це навмисна зловмисна спроба особи чи групи осіб порушити конфіденційність, цілісність чи доступ до інформаційних систем іншої особи чи групи осіб [3].

У сучасних матеріалах з вивчення кібербезпеки, кібератаки можна класифікувати за різними ознаками.

1) Класифікація за вектором атаки:

Вектор атаки – це шлях, завдяки якому атакуюча особа може отримати доступ до хоста. Вектор атаки включає вразливості, так як для успішної атаки часто використовуються декілька вразливостей [4].

- Неправильна конфігурація – Атакуючий використовує помилки в конфігурації для отримання доступу до хосту або мережі хостів та потім задіює інші атаки. Дуже часто початкові налаштування є легкою ціллю для атакуючого.
- Недоліки ядра – Атакуючий використовує помилки ядра для отримання адміністративного доступу в системі та використовує потім вразливості в самій операційній системі.
- Переповнення буферу – Переповнення буфера виникає, коли фрагмент коду не перевіряє належним чином відповідну довжину вхідних даних, а вхідне значення не відповідає розміру, який очікує програма. Атака може використати вразливість переповнення буфера, що призведе до можливого використання виконання довільного коду, часто з привілеями на адміністративному рівні, під час роботи програми [5].
- Недостатня перевірка вхідних даних – Програма не може коректно перевірити дані, які користувач пересилає програмі [5]. Таким чином зловмисник може використати різні ін’єкції, змусивши свій код працювати на сервері.

- Символічні посилання – Це файл, що звертається до іншого файлу. Атакуючий може використати цю вразливість, щоб вказати на цільовий файл, для якого процес операційної системи має дозволи на запис [5].
- Умова гонки – виникає тоді, коли програма ініціює операцію, а відповідний об’єкт змінюють між двома послідовними звертаннями. Така ситуація дає можливість зловмиснику тимчасово отримати вищі привілеї під час виконання програми або процесу [5].
- Неправильні права доступу до файлу або каталогу – помилкова конфігурація дозволів, через яку користувачі або процеси отримують невідповідні права. Експлуатація цієї вразливості відкриває шлях до різних видів атак [5].
- Соціальна інженерія – методика отримання інформації про жертву або комп’ютерну систему шляхом маніпуляції соціальними взаємодіями. Такі прийоми часто дають швидкий доступ до даних, які в нормальних умовах були б недосяжні для атакуючого.

2) За мотивом:

- Фінансова вигода – Атакуючий хоче отримати грошову вигоду.
- Шпигунство – Збір секретної інформації.
- Підривна діяльність – Спроба вивести з ладу роботу компанії.
- Помста – Колишні чи теперішні працівники компанії можуть спробувати вчинити кіберзлочин для помсти.
- Політичні чи ідеологічні – Атакуючі хочуть мати вплив на політичну ситуацію.
- Бажання слави – Бажання атакуючих показати свої навички або почути про себе в медіапросторі.
- Етичні – Замотивовані моральними принципами можуть зробити витік неетичних практик, які використовуються в компанії.
- Шантаж – Маніпуляції для отримання виконання умов, інакше зловмисник оприлюднить інформацію [7].

3) За типом зловмисника:

- Script Kiddie – Користувачі без серйозних навиків хакінгу, які використовують готові скрипти з Інтернету.
- Хактивісти – Хакери з ідеологічними цілями, які таким чином намагаються мати вплив на соціум, владу.
- Організована злочинність – Згруповані хакери, які працюють заради фінансової вигоди.
- Держава – Хакери, що діють від імені уряду.
- Внутрішня загроза – Працівник компанії, який зловживає своїм доступом заради фінансів або помсти.
- Конкуренти – Конкуренти, які хочуть дестабілізувати роботу компанії.
- Тіньове IT – Працівники, які не навмисно можуть створити вразливості [7].

4) За об’єктом:

- Людина/кінцевий користувач – Хакер має ціль отримати доступ до особистої інформації людини або зробити іншу атаку від її імені.
- Програмні застосунки – Хакер має мету викрасти дані компанії, отримати контроль над програмним застосунком чи інше.
- Кінцева точка – Хакер має ціль отримати контроль над робочою станцією або сервером, розповсюдити свій код по всій мережі чи зашифрувати дані.
- Мережа та інфраструктура – Хакер має ціль проникнути в мережу компанії для викрадення інформації або переривання нормальної роботи компанії.
- Дані – Хакер має ціль порушити CIA даних, тобто конфіденційність, цілісність чи доступність.
- IoT – Хакер може мати на меті компрометацію промислових систем, або використати IoT як точку входу для подальшої атаки.
- Промислова інфраструктура – Хакер має на меті порушення роботи промислової інфраструктури.

- Фізичні носії – Хакер може використати фізичні носії як точку входу для проведення подальшої атаки [8].
- Хмари – Хакер отримати несанкціонований доступ до хмари компанії.

5) За складністю:

- Масові – Хакери використовують вже відомі вразливості та готові інструменти, щоб атакувати найвразливіші пристрої.
- Спрямовані – Хакери вже більш підготовлені, проводять попереднє дослідження, продумують атаки під конкретну особу чи компанію.
- Тривалі цільові атаки (APT) – Найбільш кваліфіковані групи хакерів, часто спонсоровані державою, тому такі атаки є найбільш складними. Також проводять найкращу підготовку для проведення атаки, можуть довго перебувати в системі для викрадення інформації [9].

1.2 Типи кібератак

Детальніше розглянемо існуючі типи кібератак:

- Шкідливе програмне забезпечення(Ransomware):
- Програми-вимагачі – програмне забезпечення, яке проникає в систему, шифрує дані користувача і вимагає викуп для відновлення доступу до даних. Навіть після внесення грошей на рахунок хакера, дані, частіше за все, не повертаються. Так як для повернення даних, зловмиснику потрібно залишити більший цифровий слід, що є небезпечним для нього.
- Троян (Trojan) – Програма, яка маскується під корисний для користувача софт. Тому користувач може завантажити потрібний інсталятор для гри з неофіційного сайту, а отримати шкідливе програмне забезпечення, яке дасть зловмиснику доступ до системи.
- Хробак (Worm) – Програмне забезпечення, що використовує вразливості або слабкі облікові дані, розповсюджується по мережі і не потребує взаємодії з користувачем.

- Шпигунське програмне забезпечення (Spyware) – Програмне забезпечення, що має на меті збір особистих даних користувача без його згоди, таким чином порушивши конфіденційність.
- Непотрібне ПЗ (Bloatware) – Неефективне та небажане програмне забезпечення, яке не приносить користі, але знижує продуктивність системи.
- Вірус (Virus) – Шкідливий код, який приєднується до іншого програмного забезпечення і виконується та поширюється під час їхнього запуску. Може пошкодити та модифікувати системні файли чи дані користувача [7].
- Реєстратор натискання клавіатури (Keylogger) – Записує кожне натискання клавіші, таким чином краде конфіденційну інформацію користувача. Наприклад, може бути використаний для викрадення паролів для подальших атак.
- Логічна бомба (Logic bomb) – Шкідливе програмне забезпечення, яке активується при певній дії користувача та починає виконувати шкідливі дії.
- Руткіт (Rootkit) – Шкідливе програмне забезпечення, яке використовується злочинцями для отримання контролю над системою [7].

1) Мережеві атаки:

- DoS (Denial of Service attacks) – Зловмисник переповнює запитами мережу або сервер, таким чином виводячи з ладу систему, яка не може обробити такий потік інформації. Наприклад, зловмисник робить багато запитів на з’єднання до серверу, сервер не може їх обробити і стає недоступним також і для легітимних користувачів. У випадку DoS атака проводиться з одного пристрою.
- DDoS (Distributed Denial of Service) – Зловмисник використовує групу завчасно скомпрометованих пристроїв для проведення Denial of Service атаки, таким чином робить атаку сильнішою. Використовується частіше, ніж звичайна Denial of Service атака, так як сучасні сервери в спромозі впоратися з одним атакуючим пристроєм.
  - Приклади DoS та DDoS атак: UDP Flood, SYN Flood, HTTP Flood, Smurf Attack.

- MitM (Man-in-the-middle attacks) – Зловмисник знаходиться посередині передачі даних. Таким чином має можливість для перехоплення чи підміни даних між клієнтом і сервером.
  - Приклади MitM атак: ARP Spoofing, HTTPS Spoofing, Session Hijacking.
- Спуфінг (Spoofing attacks) – Атака, при якій зловмисник маскується під іншого користувача та може підробляти дані, відправлені від нього. Наприклад, зловмисник вводить свої пакети через Інтернет через підробну IP-адресу відправника. Таким чином в іншого пристрою в системі не буде сумнівів для передачі секретної інформації зловмиснику [10].
  - Приклади спуфінг атак: IP Spoofing – зловмисник підробляє IP-адресу відправника; ARP Spoofing-зловмисник підробляє повідомлення протоколу ARP.
- Сніфінг атаки (Sniffing attacks) – Пасивні атаки, направлені на перехоплення мережевого трафіку.
- Атака повторного відтворення (Replay attacks) – Зловмисник перехоплює повідомлення і відправляє його повторно отримувачу, щоб видати себе за початкового відправника. Таким чином зловмисник проходить автентифікацію [11].
- Атаки на систему доменних імен (DNS attacks) – Атаки націлені на використання вразливостей DNS для переривання нормальної роботи системи, переправки користувачів на зловмисні сайти або для викрадення секретної інформації.
- Приклади атак на систему доменних імен: DNS spoofing, DNS tunneling, DNS amplification [10].

У результаті аналізу сучасних типів кібератак було встановлено, що спектр можливих загроз постійно розширюється та ускладнюється, а використовувані інструменти та техніки атакуючих стають дедалі витонченішими. Це підкреслює необхідність комплексного підходу до кібербезпеки, включаючи як технічні способи захисту, так і моніторинг поведінкових індикаторів. Можна зробити

висновок, що лише постійне оновлення систем захисту та розвиток методологій виявлення загроз дозволять ефективно протидіяти різним типам атак.

2 ДОСЛІДЖЕННЯ ТА АНАЛІЗ МЕТОДІВ ВИКОРИСТАННЯ ВРАЗЛИВОСТЕЙ

2.1 Огляд інструментів і технік, що використовуються для здійснення атак на корпоративні мережі

Для кращого розуміння кіберзловмисників та детального розбору кібератак на етапи у 2011 році компанія Lockheed Martin розробила одну із основних моделей кібербезпеки – Cyber Kill Chain. Таким чином ми можемо розглянути дії зловмисника на кожному етапі, проаналізувати інструменти, які він застосовує та продумати протидію.

Розглянемо Cyber Kill Chain поетапно:

1) Розвідка: На цьому етапі зловмисник намагається дізнатися як можна більше про систему жертви: від пошт працівників компанії до WHOIS-запитів.

Техніки збору інформації: збір інформації за допомогою відкритих джерел (OSINT), підбір адрес, сканування мережі, перегляд інформації працівників в соціальних мережах, збір поштових адрес працівників, визначення публічних сервісів компанії.

Інструменти та сервіси: використання таких засобів як Censys, Shodan, Maltego, SpiderFoot аналіз DNS-записів та субдоменів, WHOIS-запитів [12].

2) Озброєння:

На цьому етапі зловмисник продумує вектор атаки та створює шкідливе програмне забезпечення, яке буде використовувати вразливості. Також на цьому етапі зловмисник може продумати back door для постійного доступу до системи [13].

Техніки: створення експлойту, підготовка документу з макросами, створення payload.

Інструменти: для створення payload часто використовується Metasploit, msfvenom, Cobalt Strike.

3) Доставка:

На цьому етапі зловмисник завантажує розроблений payload системі жертви, через продумані на попередньому етапі вектори атак. Для цього зловмисник може використовувати різні види соціальної інженерії та фішинг.

Техніки: фішинг та різні підвиди фішингу, remote services exploit, фізичний переносник, malvertising.

Інструменти: різні засоби для створення фішингових повідомлень, соціальна інженерія, зламані веб-платформи.

4) Експлуатація:

На цьому етапі шкідливий код виконується на комп'ютері жертви, використовуючи вразливості системи жертви.

Техніки: експлуатація вразливостей програмного забезпечення, експлуатація SQL-ін'єкцій, експлуатація макросів, використання слабких облікових даних.

Інструменти: Metasploit, Exploit DB, sqlmap, Burp Suit.

5) Встановлення:

Шкідливе програмне забезпечення буде встановлено для подальшого контролю над системою жертви.

Техніки: використання бекдорів, руткітів.

Інструменти: Cobalt Strike, Empire, Sliver, Covenant, LOLBins [14].

6) Командування та контроль:

На цьому етапі зловмисник встановлює зв'язок між системою жертви та сервером зловмисника.

Техніки: встановлення каналів зв'язку, шифрування і поліморфізм трафіку, використання потрібних часових інтервалів для з'єднання.

Інструменти: Cobalt Strile, Metasploit Meterpterer, Sliver, Empire, lodine, Mythic.

7) Дії щодо цілі:

Етап, на якому зловмисник може реалізувати свою фінальну ціль, заради якої була пророблена вся його робота.

Техніки: горизонтальне переміщення, вертикальне переміщення, збір даних, шифрування, саботаж.

Інструменти: BloodHound, AdFind, PowerView, PsExec, RDP, CrackMapExec, Impacket, Mimikatz, PowerUp, Juicy Potato [14].

2.2 Дослідження найбільш поширених вразливостей корпоративних мереж

CVE – це база даних відомих вразливостей та дефектів безпеки, яка присвоює кожній властивості власний унікальний ідентифікатор.

Багато компаній працюють над аналізом вразливостей, які були популярні у хакерів за останні роки. Таким чином, прочитавши ці статті, можемо зробити узагальнений огляд найпоширеніших вразливостей корпоративних мереж.

1) Використання застарілого або неоновленого програмного забезпечення.

Багато компанії використовують застарілі версії програмного забезпечення, які не підтримують оновлень. Більшість сервісів пов’язані з відповідними версіями програмного забезпечення, тому оновлення до актуальних версій є просто неможливим. Це призводить до того, що зловмисники навіть без особливих знань можуть просканувати систему на вразливість та задіяти вже відомий експлойт, знайдений в Інтернеті.

2) Слабка або неправильна автентифікація:

Під цим може матися на увазі використання занадто простих, дефолтних паролів або відсутність багатофакторної автентифікації. Таким чином, зловмисники використовуючи інструменти такі як Hydra, Meduza чи Mimikatz можуть легко використати дану вразливість для компрометації облікових записів.

3) Неправильне керування доступом:

Під цим мається на увазі отримання користувачем доступу, який користувач не мав отримати. Таким чином користувач може мати доступ до секретної від нього інформації або нелігітимних для нього функцій, які в невмілих руках легко можуть зашкодити компанії.

4) Вразливості веб-додатків:

Всі компанії зараз мають сайти у публічному доступу, тому часто зловмисники бачать в цьому потенційну точку входу в корпоративну мережу. Саме тому намагаються виявити та поексплуатувати вразливості веб-додатків.

5) Відкриті порти та служби:

Незахищені, нефільтровані та просто відкриті порти можна часто побачити в периметрі компаній. Сканування мережі є одним із базових та початкові етапів злому, тому дана вразливість також є критичною для закриття та регулярної перевірки.

6) Недостатня сегментація мережі:

Багато організацій не мають сегментації мережі, яка б допомогла б розділити публічні та приватні сервери, тестові та продуктивні сервери від звичайних робочих станцій користувачів. Це в свою чергу дає можливість зловмиснику легко рухатись по мережі і мати доступ з однієї точки мережі в іншу. Також це набагато ускладнює своєчасне реагування на інциденти кібербезпеки.

7) Якби спеціалісти з кібербезпеки не намагались покращити безпеку мережі через технічні засоби та використання новітніх інструментів – найбільш небезпечною вразливістю будь-якої корпоративної мережі досі залишається людина. Звичайні працівники компанії можуть стати точкою входу в компанію для призвести до злому всієї мережі.

На основі проведеного аналізу методів використання вразливостей можна зробити висновок, що найбільш критичними елементами мережевої інфраструктури залишаються кінцеві точки, відкриті сервіси та слабкі конфігурації мережі. Інформація, класифікована з позиції Cyber Kill Chain, показала, що системне виявлення вразливостей на ранніх стадіях дозволяє значно знизити ризик успішної атаки. Особливу увагу потрібно приділяти регулярному оновленню ПЗ та впровадженню багаторівневого механізму контролю доступу.

3 ДОСЛІДЖЕННЯ ТА ОЦІНКА ІСНУЮЧИХ МЕТОДИК ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

3.1 NIST Cybersecurity Framework 2.0

NIST Cybersecurity Framework (CSF) версії 2.0 [15, 16] є однією з найбільш поширених та адаптивних методологій управління кіберризиками, яка застосовується для створення, оцінювання та постійного вдосконалення програм кіберзахисту в організаціях різного масштабу, від малого бізнесу до великих корпорацій.

Фреймворк базується на орієнтації на ризик-менеджмент, дозволяючи організаціям формувати заходи захисту пропорційно до актуальних бізнес-ризиків та критичності активів. CSF 2.0 надає таксономію результатів (outcomes) – чітко структуровані цілі безпеки, що значно полегшують процес планування, моніторингу та контролю.

Ядром CSF є функціональна модель, яка логічно поділяє діяльність із безпеки на шість ключових, взаємопов'язаних функцій:

- Govern (G): Керування ризиками та пріоритезація рішень на рівні керівництва.
- Identify (I): Визначення активів, ризиків, регуляторних вимог та ресурсів.
- Protect (P): Розробка та впровадження захисних механізмів.
- Detect (D): Виявлення кіберподій та інцидентів.
- Respond (R): Вжиття заходів щодо усунення наслідків виявлених інцидентів.
- Recover (C): Діяльність із відновлення систем та послуг після інциденту.

Системі CSF притаманна висока гнучкість і масштабованість. Вона не є сукупністю жорстко визначених технічних контролів, а скоріше «каркасом»

(framework), який інтегрується з іншими провідними стандартами та практиками (наприклад, ISO/IEC 27001, CIS Controls, NIST SP 800-53), а також із внутрішніми корпоративними політиками. Фреймворк також включає Профілі (Profiles) та Рівні зрілості (Tiers), які дають змогу оцінити поточний стан кіберзахисту та визначити еволюційні шляхи розвитку системи безпеки [15, 16].

Застосування NIST CSF 2.0 має низку суттєвих переваг:

1) Гнучкість та інтероперабельність: Універсальність фреймворку дозволяє його використання в широкому спектрі організацій та спрощує узгодження різних стандартів безпеки (ISO, SOC 2).

2) Орієнтація на бізнес-пріоритети: CSF 2.0 явно пов'язує кіберзахист із бізнес-процесами та ризиками, полегшуючи комунікацію між технічним персоналом та C-level керівництвом.

3) Чітка методологія: Шестифункціональна структура забезпечує логічний та зрозумілий підхід до організації безпеки, підтримуючи можливість пріоритезації контролів.

4) Оцінка зрілості: Вбудовані механізми (Tiers) дають інструментарій для оцінки поточного стану кіберзрілості та планування її вдосконалення.

Недоліки даної методології:

1) Абстрактність контролів: CSF визначає, що потрібно досягти (outcomes), але не надає конкретних технічних інструкцій (як досягти). Це вимагає обов'язкового доповнення фреймворку більш деталізованими стандартами (наприклад, NIST SP 800-53 або CIS Controls).

2) Ресурсоємність впровадження: Хоча CSF є гнучким, його повноцінне впровадження вимагає значних управлінських компетенцій, уваги менеджменту та ресурсів, що може бути викликом для невеликих організацій.

3) Відсутність офіційної сертифікації: На відміну від ISO 27001, NIST CSF не передбачає надання офіційного сертифіката відповідності, що може бути невідповідним для компаній, яким потрібне документальне підтвердження безпеки для ринку чи регуляторів.

4) Потреба в галузевій адаптації: Універсальність CSF може призводити до надто загального формулювання деяких результатів, що вимагає додаткової локалізації та уточнення для специфічних секторів (фінанси, охорона здоров'я тощо) з метою забезпечення точного вимірювання рівня виконання [15, 16].

3.2 Zero Trust Architecture

Модель Zero Trust Architecture (ZTA) являє собою концепцію кіберзахисту, яка ґрунтується на принципі повної відсутності апріорної довіри до будь-якого користувача, пристрою чи сервісу. На відміну від традиційних периметрових підходів, ZTA вимагає постійної верифікації кожного запиту на доступ, незалежно від того, з якого сегмента мережі він надходить. Цей підхід забезпечує більш високий рівень контролю та стійкості до сучасних загроз [17-19].

Переваги Zero Trust Architecture:

1) Відповідність сучасним розподіленим та хмарним середовищам. Zero Trust ефективно застосовується у хмарних, контейнерних та гібридних інфраструктурах, де традиційний мережевий периметр або відсутній, або є недостатньо надійним.

2) Зниження ризику бокового переміщення зловмисника. Застосування мікросегментації та суворий контроль міжсегментного доступу значно обмежує можливість lateral movement, ускладнюючи розвиток атаки після первинного проникнення.

3) Реалізація принципу найменших привілеїв. Модель забезпечує надання доступу лише у межах необхідного функціоналу та часто на обмежений часовий період, що зменшує ймовірність несанкціонованого використання облікових даних.

4) Динамічна та контекстна перевірка доступу. Рішення щодо надання доступу приймаються з урахуванням численних факторів: автентичності користувача, стану пристрою, геолокації, поведінкових характеристик та поточного рівня ризику. Перевірка триває протягом усієї сесії.

5) Підтримка регуляторної відповідності. Деталізоване журналювання, контроль доступу та прозорість операцій полегшують відповідність вимогам галузевих та державних стандартів кібербезпеки та захисту персональних даних [17-19].

Недоліки Zero Trust Architecture:

1) Складність впровадження та необхідність архітектурних змін. Перехід до моделі Zero Trust потребує перегляду мережевої топології, процесів автентифікації та управління ідентичністю, що є трудомістким і тривалим процесом, особливо для організацій із застарілою інфраструктурою.

2) Висока вартість реалізації. Повноцінне впровадження ZTA вимагає інвестицій у системи багатофакторної автентифікації, рішення IAM, інструменти мікросегментації та засоби постійного моніторингу політик доступу.

3) Можливі проблеми з продуктивністю. Постійна перевірка кожного запиту може створювати додаткове навантаження на мережеві ресурси та сервіси керування політиками, що може впливати на швидкодію системи за відсутності оптимізації.

4) Підвищені вимоги до кваліфікації персоналу. Ефективна експлуатація Zero Trust потребує глибоких знань у сфері доступу, мікросегментації та динамічного аналізу ризиків, що вимагає додаткової підготовки або залучення спеціалізованих фахівців [17-19].

3.3 Модель MITRE ATT&CK

Модель MITRE ATT&CK є відкритою базою знань, яка систематизує тактики, техніки та процедури (TTPs), що застосовуються зловмисниками на різних етапах атаки. Ця матриця описує реальні поведінкові патерни супротивників та широко використовується у сферах аналізу загроз, побудови систем виявлення та оцінювання ефективності засобів захисту [20-22].

Переваги MITRE ATT&CK:

1) Повна та структурована база тактик і технік супротивників. Модель пропонує детальний опис дій зловмисників, класифікованих за тактиками та техніками, що дозволяє організаціям краще розуміти можливі вектори атак, їх логіку та послідовність.

2) Підтримка процесів виявлення загроз та аналітики. ATT&CK активно застосовується для оцінювання здатності систем до виявлення різних сценаріїв атак, що робить її важливим інструментом під час побудови й оптимізації SOC, threat hunting та кореляції подій.

3) Підвищення ефективності тестування контролів. Модель використовується як основа для перевірки ефективності систем безпеки через ATT&CK-based testing, зокрема за допомогою таких інструментів, як Atomic Red Team або CALDERA.

4) Поширеність та відкритість. MITRE ATT&CK є загальнодоступним ресурсом, постійно оновлюється та підтримується професійною спільнотою й дослідниками, що забезпечує високу якість і актуальність даних.

5) Покращення комунікації між командами. Наявність загальної термінології дозволяє уніфікувати опис інцидентів, звітів та технічних обговорень, що полегшує взаємодію аналітиків, розробників, команди SOC та керівництва [20-22].

Недоліки MITRE ATT&CK:

1) Висока деталізація та складність для початківців. Великий обсяг технік і варіантів реалізації може бути складним для організацій, які лише починають впроваджувати структурований підхід до аналізу загроз.

2) Фокус на пост-експлуатаційному етапі. Значна частина моделі описує дії зловмисників після отримання початкового доступу, що може залишати поза увагою ранні фази атаки, які потребують інших моделей (наприклад, PRE-ATT&CK або Cyber Kill Chain).

3) Відсутність прямих рекомендацій щодо захисту. ATT&CK не надає конкретних інструкцій щодо впровадження контрзаходів, а лише описує можливі

дії супротивника. Організації мають самостійно визначати, які контролі використовувати.

4) Необхідність постійного оновлення кореляційних правил. Через високий темп появи нових технік аналітикам потрібно регулярно переглядати та вдосконалювати правила виявлення, що збільшує навантаження на SOC.

5) Потенційні витрати на інтеграцію. Хоч ресурс і безкоштовний, повноцінне його застосування вимагає налаштування систем моніторингу, SIEM, SOAR та проведення тестування, що може вимагати додаткових ресурсів [20-22].

3.4 SASE та SSE

Архітектури SASE (Secure Access Service Edge) та SSE (Security Service Edge) представляють собою сучасний підхід до поєднання мережевих і безпекових функцій у єдину хмарну платформу. Концепція SASE включає інтеграцію SD-WAN, Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), Firewall-as-a-Service (FWaaS) та інших сервісів, що забезпечують захист як віддалених офісів, так і мобільних користувачів. SSE, у свою чергу, фокусується виключно на безпекових складових SASE. Підхід активно просувається та описується у звітах аналітичної компанії Gartner [23-25].

Переваги архітектур SASE / SSE

1) Єдина платформа для мережі та безпеки. Консолідація SD-WAN і хмарних засобів кіберзахисту в одному рішенні спрощує управління, зменшує фрагментацію інструментів та підвищує ефективність адміністрування.

2) Оптимізований доступ для віддалених і мобільних користувачів. Завдяки розподіленій хмарній інфраструктурі SASE забезпечує швидкий та захищений доступ до корпоративних ресурсів незалежно від місця підключення, що особливо актуально в умовах розподіленої роботи.

3) Застосування принципів Zero Trust. Архітектура передбачає контекстну автентифікацію, постійну перевірку доступу та мінімальні привілеї, що дозволяє значно підвищити рівень безпеки.

4) Зниження складності інфраструктури. Об’єднання мережевих функцій і засобів безпеки в єдиному сервісі зменшує кількість окремих пристроїв, локальних шлюзів і продуктів, що потребують обслуговування.

5) Масштабованість і гнучкість. Хмарна модель дозволяє організаціям швидко адаптувати інфраструктуру відповідно до потреб бізнесу та кількості користувачів, не потребуючи значних капітальних витрат [23-25].

Недоліки архітектур SASE / SSE

1) Залежність від постачальника та хмарної платформи. Інтеграція великої кількості функцій у одного провайдера може створювати vendor lock-in та збільшувати ризики у разі перебоїв у роботі сервісу.

2) Вимоги до якісного та стабільного Інтернет-з’єднання. Оскільки безпекові сервіси виконуються у хмарі, загальна ефективність залежить від пропускної здатності та стабільності мережі.

3) Висока початкова вартість впровадження. Координація переходу з традиційної архітектури на SASE або SSE може потребувати помітних фінансових та часових ресурсів.

4) Необхідність перебудови процесів і політик. Перехід до моделі SASE передбачає перегляд політик доступу, маршрутизації, а також інтеграцію IAM і ZTNA, що потребує значної організаційної роботи.

5) Потенційні складності з інтеграцією існуючих рішень. Інфраструктури, які вже використовують різні продукти SD-WAN, CASB або NGFW, можуть зіткнутися з викликами при їх уніфікації в одну платформу [23-25].

3.5 EDR / XDR / NDR: багаторівневе виявлення загроз

Системи EDR (Endpoint Detection and Response), XDR (Extended Detection and Response) та NDR (Network Detection and Response) забезпечують багаторівневий захист корпоративної інфраструктури, збираючи телеметрію та аналізуючи активність на різних рівнях:

- EDR – захист кінцевих точок (ПК, серверів, мобільних пристроїв), включає збір детальних журналів, аналіз поведінки процесів та користувачів, виявлення шкідливих програм і аномалій у діяльності систем.
- XDR – інтегрує дані з EDR, NDR, хмарних сервісів та інших джерел, корелює події для більш точного виявлення складних атак, забезпечує централізоване реагування.
- NDR – аналізує мережевий трафік, виявляє аномалії, атаки на протоколи, внутрішню активність зловмисників, що не проявляється на кінцевих точках [26-28].

Переваги:

1) Проактивне виявлення загроз: дозволяє виявляти складні та приховані атаки, які не відстежуються традиційними антивірусними рішеннями.

2) Інтеграція з Threat Intelligence: платформи можуть підключати дані розвідки загроз для підвищення точності виявлення.

3) Автоматизоване реагування: можливість блокування або ізоляції заражених об’єктів до серйозних наслідків.

4) Централізований моніторинг: XDR забезпечує огляд усіх активностей в корпоративній інфраструктурі.

5) Підвищення ефективності SOC: аналітики отримують структуровану інформацію для швидшого реагування [26-28].

Недоліки:

1) Високі вимоги до ресурсів: великі обсяги телеметрії потребують потужних серверів та сховищ даних.

2) Необхідність кваліфікованого персоналу: ефективне налаштування та аналіз даних вимагає високої експертизи.

3) Можливість помилкових спрацювань: false positives особливо ймовірні при некоректній інтеграції XDR/NDR.

4) Вартість ліцензій та підтримки: впровадження таких систем потребує значних фінансових вкладень.

5) Складність інтеграції: особливо в середовищах з різнорідними платформами та застосунками [26-28].

3.6 SIEM та SOAR: централізований збір та автоматизація безпеки

SIEM (Security Information and Event Management) та SOAR (Security Orchestration, Automation and Response) є ключовими технологіями для ефективного управління безпекою в сучасних організаціях.

- SIEM забезпечує збір, нормалізацію та кореляцію журналів із різних джерел – серверів, мережевих пристроїв, кінцевих точок і хмарних сервісів. Він дозволяє систематизувати події безпеки, проводити їх аналіз у реальному часі та формувати централізовану базу даних для подальшого редагування.
- SOAR автоматизує процеси реагування на інциденти та оркеструє роботу Security Operations Center (SOC). Це дозволяє створювати стандартизовані робочі процеси (playbooks), інтегрувати різні системи безпеки та швидко реагувати на виявлені загрози [29-32].

Переваги:

1) Централізований моніторинг та аналітика: SIEM дозволяє бачити всю активність в інфраструктурі в одному місці, що підвищує точність виявлення загроз.

2) Автоматизація реагування: SOAR зменшує ручну роботу аналітиків, забезпечує швидке блокування атак та виконання процедур ізоляції або сповіщення.

3) Стандартизація процесів SOC: дозволяє створювати повторювані сценарії реагування на різні типи інцидентів.

4) Підвищення ефективності персоналу: аналітики зосереджуються на складних завданнях, тоді як рутинні дії виконуються автоматично.

5) Покращене регуляторне дотримання: системи ведуть журналювання та аудит, що полегшує виконання вимог стандартів безпеки та законодавства [29-32].

Недоліки:

1) Висока складність впровадження: інтеграція різнорідних джерел журналів та систем реагування потребує значних ресурсів.

2) Вартість ліцензій та обслуговування: повноцінне використання SIEM + SOAR потребує фінансових вкладень у програмне забезпечення та навчання персоналу.

3) Потреба в постійному оновленні: правила кореляції і сценарії реагування потрібно регулярно оновлювати під нові загрози.

4) Ризик перевантаження тривогами: без тонкої настройки SIEM може генерувати численні хибні спрацьовування, що знижує ефективність SOC.

5) Складність оцінки ефективності: необхідність моніторингу продуктивності та результативності автоматизованих процесів.[29-32].

3.7 Традиційні мережеві контролі: NGFW, IDS/IPS, VLAN, VPN

Традиційні мережеві засоби захисту залишаються основою безпеки корпоративних мереж і виконують функції фільтрації, контролю доступу та виявлення атак:

- NGFW (Next-Generation Firewall) забезпечує комплексний контроль трафіку на основі застосунків, користувачів та контексту, поєднуючи традиційний брандмауер з функціями IDS/IPS, антивірусного сканування та інтеграції з Threat Intelligence.
- IDS/IPS (Intrusion Detection/Prevention System) аналізують мережевий трафік для виявлення відомих і нових атак, а IPS здатна блокувати підозрілі з’єднання в реальному часі.
- VLAN / міжсегментація дозволяє логічно розділяти мережу на ізольовані сегменти, обмежуючи пересування користувачів і потенційних зловмисників всередині мережі.
- VPN (Virtual Private Network) забезпечує захищене шифроване з’єднання для віддалених користувачів та офісів. У рамках Zero Trust підходу VPN

часто доповнюють або замінюють ZTNA (Zero Trust Network Access) для гнучкого контролю доступу [33-35].

Переваги:

1) Базовий захист мережевого периметра: NGFW та IDS/IPS ефективно блокують відомі загрози та фільтрують трафік.

2) Сегментація та контроль доступу: VLAN та міжсегментація обмежують lateral movement зловмисників і мінімізують вплив потенційних інцидентів.

3) Простота адміністрування: добре відпрацьовані технології з великою кількістю документації та досвіду у фахівців.

4) Надійне шифрування віддалених з'єднань: VPN забезпечує конфіденційність даних при доступі з зовнішніх мереж.

5) Інтеграція з іншими системами безпеки: NGFW і IDS/IPS можна поєднувати з SIEM, SOAR, NAC для створення багаторівневого захисту [33-35].

Недоліки:

1) Обмежена ефективність у хмарних або мобільних середовищах: традиційні периметрові технології не завжди адаптовані до динамічних та розподілених систем.

2) Складність швидкої адаптації: зміни політик і оновлення правил потребують часу, особливо при нових загрозах.

3) Необхідність постійного моніторингу: для ефективного функціонування NGFW і IDS/IPS потрібен постійний аудит та налаштування.

4) Витрати на підтримку та оновлення: ліцензії, апаратні ресурси та навчання персоналу збільшують загальні витрати.

5) VPN може не відповідати принципам Zero Trust: потребує інтеграції з ZTNA для гнучкого контролю доступу та динамічної авторизації [33-35].

3.8 NAC (Network Access Control): контроль доступу пристроїв

Network Access Control (NAC) забезпечує контроль доступу пристроїв до корпоративної мережі, включаючи керовані та некеровані ПК, мобільні пристрої, IoT-пристрої та BYOD (Bring Your Own Device). NAC виконує автентифікацію, оцінку відповідності політикам безпеки та обмежує доступ пристроїв, які не відповідають встановленим вимогам [36-40].

Основні функції NAC:

- Автентифікація пристроїв: перевірка, чи відповідає пристрій політикам безпеки організації перед підключенням.
- Оцінка стану безпеки: перевірка оновлень, антивірусного захисту, конфігурацій та інших параметрів безпеки.
- Рольовий доступ: надання доступу до ресурсів відповідно до типу пристрою та ролі користувача.
- Ізоляція або обмеження доступу: блокування або перенаправлення пристроїв, які не відповідають політикам, на карантинну VLAN або мережу з обмеженим доступом [36-40].

Переваги:

1) Захист мережі на рівні доступу: обмежує ризики від неконтрольованих або потенційно небезпечних пристроїв.
2) Підтримка BYOD та IoT: дозволяє безпечно інтегрувати різні типи пристроїв.
3) Гнучкі політики доступу: можна застосовувати правила на основі ролей, стану пристрою та часу доступу.
4) Централізоване управління: адміністратори мають повний контроль над пристроями та їх підключенням до мережі [36-40].
5) Сумісність із сучасними рішеннями безпеки: NAC легко інтегрується з SIEM, SOAR та системами багаторівневого захисту.

Недоліки:

1) Складність впровадження у великій мережі: потрібне детальне планування та інтеграція з існуючою інфраструктурою.

2) Вартість ліцензій і підтримки: особливо для масштабних організацій з великою кількістю пристроїв.

3) Проблеми сумісності з деякими IoT-пристроями: старі або нестандартні пристрої можуть не підтримувати повноцінну автентифікацію.

4) Необхідність постійного оновлення політик: зміни у конфігурації мережі або нові загрози потребують регулярного перегляду правил NAC.

5) Вплив на користувацький досвід: обмеження доступу або додаткові процедури автентифікації можуть створювати незручності для користувачів [36-40].

Висновки: розгляд існуючих підходів до захисту корпоративних мереж, включаючи NIST CSF, Zero Trust, MITRE ATT&CK, SASE/SSE, EDR/XDR/NDR, SIEM/SOAR та традиційні засоби захисту, дозволяє стверджувати, що найефективніший підхід полягає у комбінуванні цих рішень у єдину систему. Жоден із методів не забезпечує абсолютного рівня безпеки сам по собі, проте їх інтеграція дозволяє створити стійку та адаптивну архітектуру захисту, що здатна протидіяти як відомим, так і невідомим загрозам.

4 РОЗРОБКА РЕКОМЕНДАЦІЙ ІЗ ВПРОВАДЖЕННЯ МЕТОДИКИ ЗАХИСТУ

4.1 Формування політик і процедур безпеки

Першочерговим етапом у впровадженні системи кіберзахисту є створення набору політик і процедур, які регламентують дії персоналу, порядок доступу до інформаційних ресурсів та вимоги до технічних налаштувань. До основних документів, які повинні бути розроблені, належать [41]:

1) Політика доступу та управління обліковими записами, що визначає ролі, права доступу, процедури створення, модифікації та видалення облікових записів.

2) Парольна політика, що включає вимоги до складності, довжини, регулярності зміни паролів та застосування менеджерів паролів.

3) Політика використання мережі та корпоративних ресурсів, яка регламентує доступ до Інтернету, використання електронної пошти, роботу з файлами та підключення зовнішніх пристроїв.

4) Політика BYOD (Bring Your Own Device) – актуальна для організацій, що дозволяють співробітникам використовувати власні пристрої для роботи.

5) Політика управління інцидентами безпеки – містить порядок ідентифікації, класифікації, реагування та документування інцидентів.

6) Політика управління оновленнями та патчами, що визначає регламент перевірки оновлень, відповідальних осіб і порядок впровадження.

Також обов’язковими є вимоги до сегментації мережі, використання VPN або ZTNA, контролю доступу на рівні пристроїв (NAC) та правил роботи з критичною інфраструктурою. Документи повинні проходити регулярний перегляд (щонайменше раз на рік) та оновлюватися відповідно до змін у загрозах або бізнес-процесах [41].

4.2 Технічні заходи захисту мережі

1) Захист периметра

Захист периметра корпоративної мережі базується на застосуванні міжмережевих екранів нового покоління (NGFW), які забезпечують глибоку перевірку пакетів (DPI), фільтрацію трафіку за категоріями, функції IDS/IPS, геоблокінг та інтегрований DDoS-захист. Для підвищення рівня безпеки необхідно реалізувати принцип deny by default, що передбачає дозволення лише заздалегідь визначеного трафіку, який відповідає політикам доступу. Важливо також обмежити доступ до адміністративних інтерфейсів за допомогою ACL, VPN або ZTNA, уникаючи їх відкритості в мережу та мінімізуючи ризик несанкціонованої експлуатації.

2) Сегментація мережі

Сегментація мережі спрямована на обмеження можливостей зловмисника переміщуватися інфраструктурою у разі компрометації одного елемента. Логічне розмежування ресурсів за допомогою VLAN, мережевих зон довіри та окремих сегментів для користувачів, серверів і службових систем дозволяє контролювати маршрутизацію та ізолювати критичні компоненти. Додатково рекомендується застосовувати micro-segmentation на рівні гіпервізора або застосунків, що забезпечує детальний контроль взаємодії між окремими вузлами та мінімізує ризики lateral movement у середовищах із високими вимогами до конфіденційності.

3) Захист і контроль доступу

Ефективний контроль доступу потребує застосування багатофакторної автентифікації (MFA) для всіх ключових сервісів, включаючи VPN, ZTNA, корпоративну пошту, AD та хмарні платформи. Підхід Zero Trust Network Access дозволяє створювати гнучкі правила доступу на основі контекстної оцінки: стану пристрою, поведінки користувача, географічного розташування та рівня ризику. Забезпечення контролю привілейованих облікових записів через рішення PAM

дає можливість ізолювати адміністративні сесії, вести повний аудит дій та мінімізувати наслідки компрометації облікових записів з розширеними правами.

4) Захист кінцевих точок

Робочі станції, сервери та мобільні пристрої є основними точками входу для атак, тому впровадження рішень класу EDR/XDR є обов'язковим. Такі системи забезпечують виявлення поведінкових аномалій, блокування шкідливого ПЗ у реальному часі та автоматизоване реагування на інциденти. Додатковими заходами виступають повне шифрування дисків, контроль доступу до USB-портів, централізоване управління політиками безпеки та автоматизоване розгортання оновлень операційних систем і прикладного ПЗ, що зменшує ризик експлуатації відомих вразливостей.

5) Захист хмарної інфраструктури

У разі використання хмарних сервісів організація має забезпечувати відповідний рівень безпеки за допомогою інструментів CSPM, CWPP і CASB. Рішення CSPM здійснюють моніторинг та аудит конфігурацій, забезпечуючи відповідність найкращим практикам. CWPP захищає робочі навантаження у хмарі й контейнерних середовищах, а CASB контролює доступ користувачів до SaaS-платформ та виявляє нетипову активність. Управління доступом у хмарному середовищі повинно ґрунтуватися на принципі найменших привілеїв, із регулярним переглядом ролей та аналізом журналів подій IAM.

6) Резервне копіювання та відновлення

Резервне копіювання є критичним елементом забезпечення стійкості до інцидентів. Рекомендується впровадження правила 3-2-1: три копії даних, дві з яких зберігаються на різних типах носіїв, а одна – у віддаленому або офлайн-середовищі. Перевага надається використанню immutable backup, які неможливо змінити навіть у разі компрометації системи. Важливо не лише створювати резервні копії, а й регулярно тестувати процедури відновлення, щоб гарантувати працездатність механізмів у разі атаки типу ransomware чи іншого критичного інциденту.

4.3 Підвищення обізнаності співробітників

1) Навчання персоналу [42]

Необхідно розробити комплексну освітню програму, яка охоплює основи кібергігієни, навички розпізнавання фішингових атак, безпечне використання електронної пошти, мобільних пристроїв та USB-носіїв, правила безпечної роботи з корпоративними ресурсами за межами офісу, а також ознайомлення зі внутрішніми політиками та процедурами компанії. Навчання може проводитися у форматах e-learning, практичних занять або інтерактивних вікторин, що забезпечує активну участь співробітників та ефективне закріплення отриманих знань.

2) Регулярні тренування та симуляції

Персонал повинен регулярно проходити фішингові тести та table-top exercises для відпрацювання реагування на інциденти. Симуляції кібератак у форматі red team або purple team assessments дозволяють перевіряти готовність організації до реальних загроз і вдосконалювати процедури реагування.

3) Політики поведінки співробітників

Співробітники мають знати порядок повідомлення про інциденти, дотримуватися заборони використання особистих пристроїв без дозволу та правил створення і зберігання паролів. Також важливо дотримуватися правил поводження з конфіденційною інформацією та корпоративними ресурсами.

4) Комунікація всередині організації

Регулярна комунікація включає розсилки про нові загрози, доступні інструкції та чек-листи для співробітників. Це сприяє підтриманню високого рівня обізнаності, формуванню культури безпеки та зменшенню ризику помилкових дій персоналу.

4.4 Інструменти для моніторингу та аудиту

1) Моніторинг безпеки [43]

Для виявлення аномалій і загроз використовуються SIEM-системи, такі як Splunk, Wazuh, Elastic Security, QRadar та Azure Sentinel. Вони забезпечують кореляцію логів, автоматизацію розслідувань (SOAR) та підтримку правил на основі MITRE ATT&CK. Для моніторингу мережевого трафіку застосовуються NDR-рішення (Darktrace, Vectra AI, Corelight/Zeek), а для захисту кінцевих точок – EDR/XDR (CrowdStrike, SentinelOne, Defender for Endpoint).

Рекомендації щодо створення візуалізацій:

Для цього потрібно зайти в інтерфейс Wazuh (рис. 4.1):

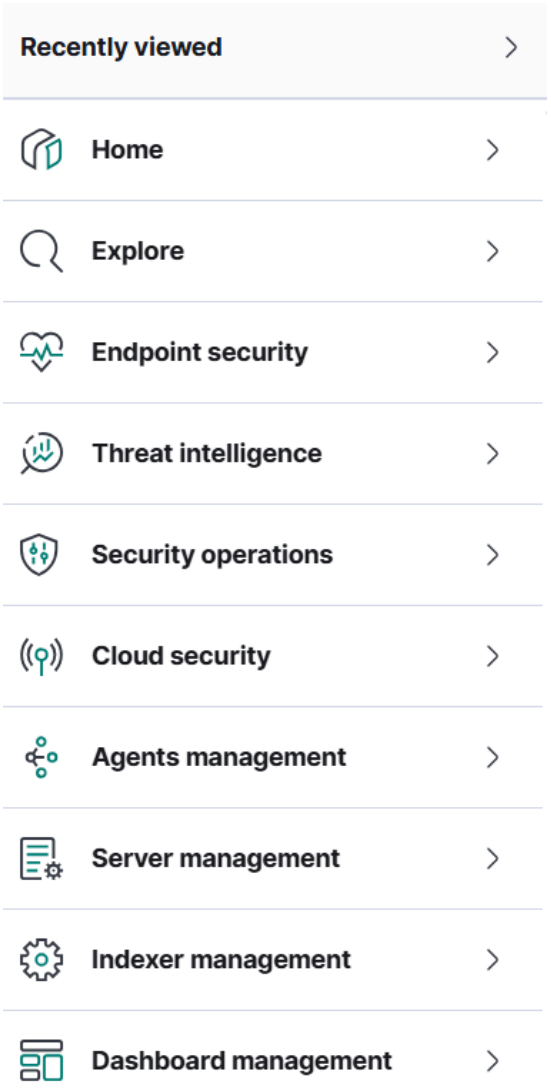

Рисунок 4.1 – Веб-інтерфейс системи Wazuh

Огляд інтерфейсу для створення Dashboard (рис. 4.2 - рис. 4.7):

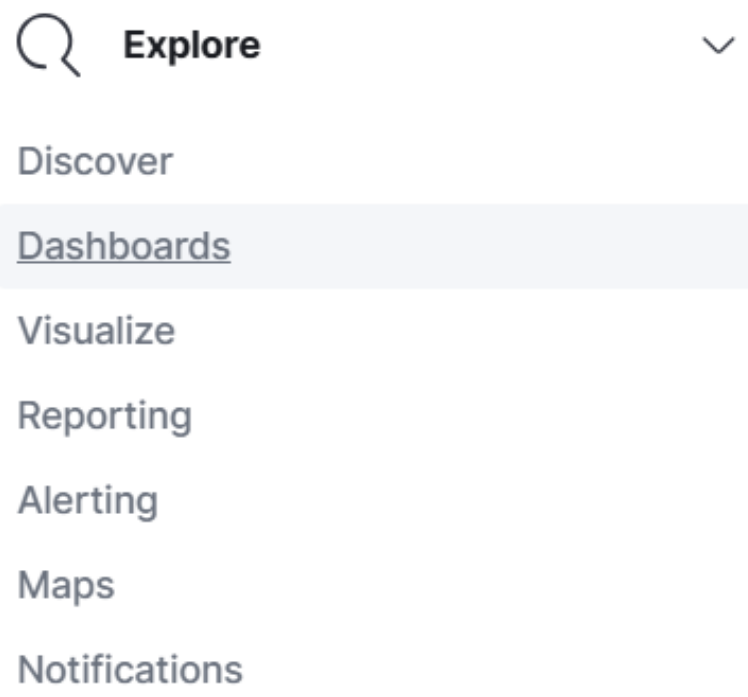

Рисунок 4.2 – Пункт Explore

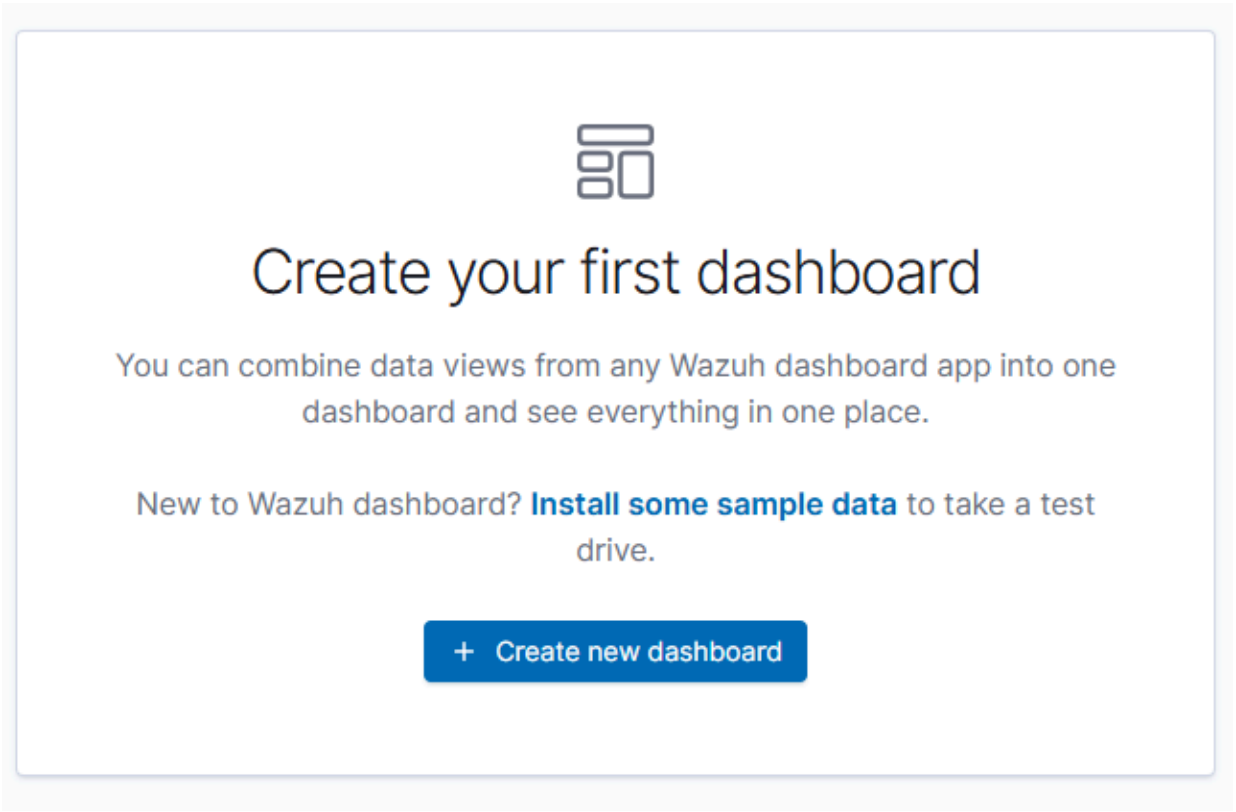

Рисунок 4.3 – Етап створення дашборду

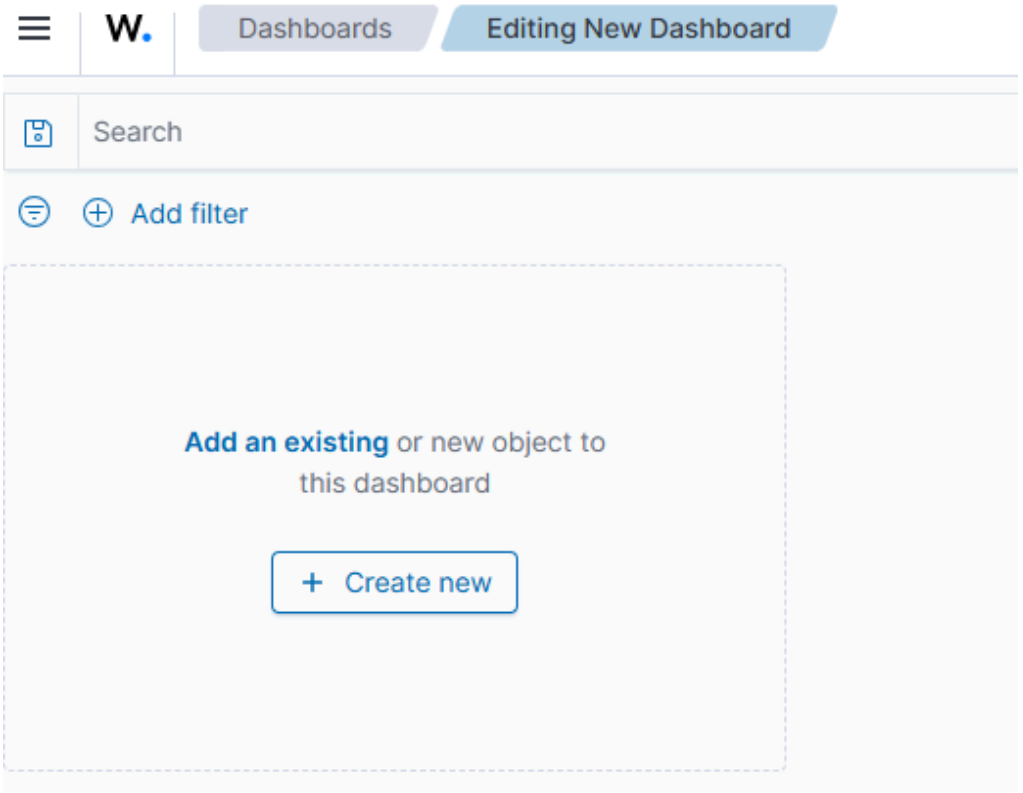

Рисунок 4.4 – Етап створення дашборду

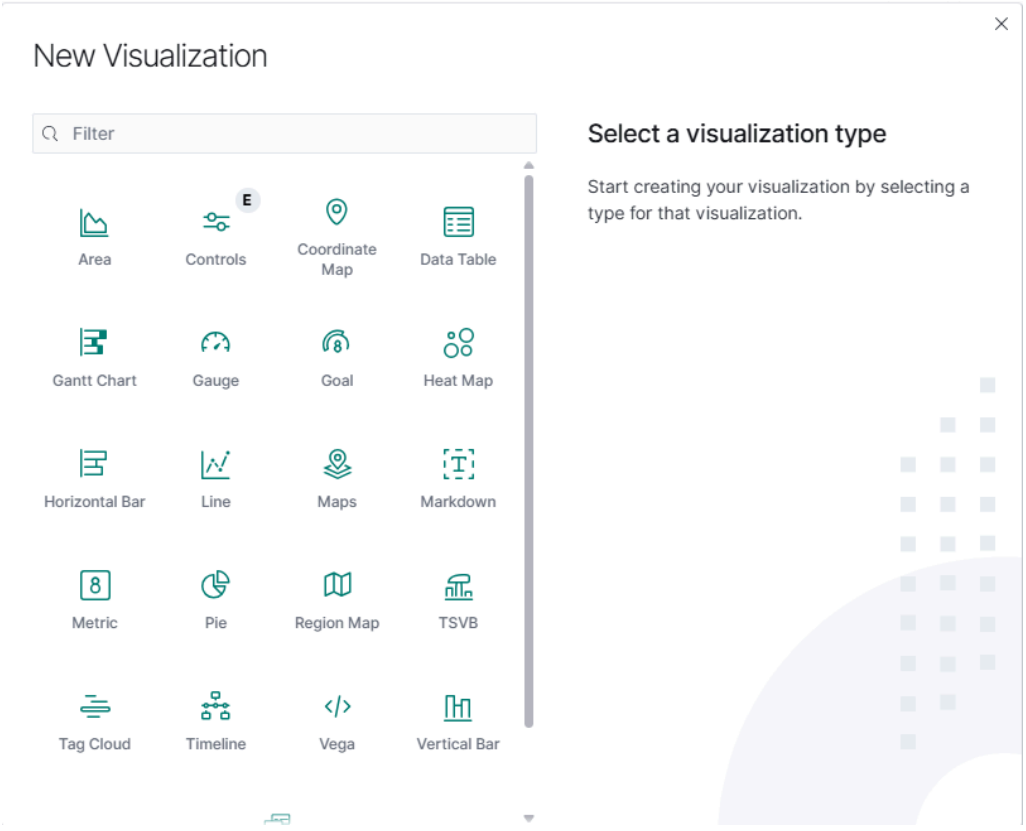

Рисунок 4.5 – Огляд інтерфейсу для вибору потрібної візуалізації

Рисунок 4.6 – Огляд інтерфейсу для вибору потрібного джерела

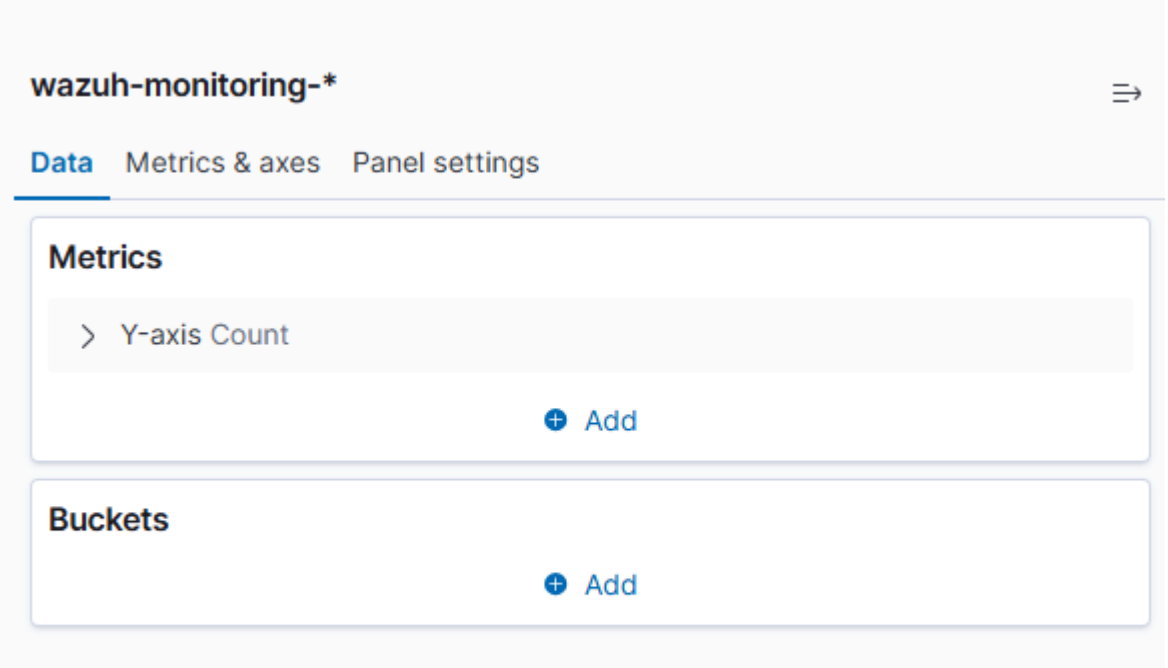

Рисунок 4.7 – Огляд інтерфейсу для налаштування графіку візуалізації

l. Тривоги за рівнями серйозності (Severity Levels) [43]

Візуалізація рівнів серйозності використовується для оцінювання загального стану безпеки та пріорітезації подій. Вона дозволяє швидко визначити, чи є у системі критичні інциденти, наскільки інтенсивно генеруються події різного рівня небезпеки та як змінюється ситуація в динаміці. Це важливий інструмент для оперативного аналізу стану інформаційної безпеки й оцінки навантаження на SOC.

Для побудови цієї візуалізації відкривається модуль побудови графіків у Kibana або OpenSearch та обирається діаграма, яка найкраще відображає розподіл подій, наприклад, bar chart чи pie chart. Після цього вказується індекс wazuh-alerts-*, де зберігаються всі тривоги. У полі групування обирається атрибут rule.level, який і містить числову оцінку серйозності події. Графік оновлюється автоматично й демонструє, які рівні загроз домінують у системі. За необхідності додається часовий фільтр або додаткові умови, які дозволяють аналізувати конкретні типи інцидентів чи окремі групи хостів.

II. Типи загроз / категорії правил (Rule Groups)

Ця візуалізація дозволяє визначити, які види загроз найчастіше виникають у системі. Завдяки аналізу груп правил можна бачити, які напрями атак домінують – спроби автентифікації, зміни в системних файлах, мережеві аномалії чи діяльність шкідливих процесів. Це допомагає прогнозувати ризики та виявляти сфери, де найбільше потрібні додаткові заходи захисту.

Візуалізація створюється у Kibana/OpenSearch, де вибирається індекс wazuh-alerts-*. Для групування подій використовується поле rule.groups, що містить категорії тривог. Система будує графік, який показує розподіл за різними групами загроз. У разі потреби додаються фільтри для конкретного компонента, наприклад, syscheck, rootcheck або authentication, що дозволяє виділити певну область безпеки та виконати глибший аналіз.

III. Статус агентів (Active / Disconnected / Never Connected)

Ця візуалізація необхідна для контролю працездатності всієї інфраструктури Wazuh. Вона дозволяє визначити, які агенти активно передають дані, які тимчасово недоступні, а які ніколи не встановлювали зв’язок із сервером. Такий огляд дає змогу оперативно виявляти проблеми з мережевим доступом, конфігурацією клієнтів або некоректною інсталяцією.

Для створення графіка відкривається модуль візуалізації, де обирається індекс wazuh-monitoring-*, що містить інформацію про стан агентів. У налаштуваннях вибирається поле agent.status, яке автоматично формує категорії

Active, Disconnected та Never Connected. Після побудови графік відображає поточний стан агентів, а також може бути обмежений часовими рамками, якщо виникає потреба відслідковувати їх динаміку.

IV. Геолокація IP-адрес

Візуалізація геолокації IP-адрес у Wazuh використовується для аналізу просторового походження підозрілих мережевих подій. Вона дозволяє визначати регіони, з яких надходять SSH-атаки, спроби підбору паролів, сканування портів чи інші аномалії в трафіку. Такий підхід допомагає швидко виявляти нетипові джерела активності, оцінювати масштаб атак і виявляти географічні закономірності загроз, що є корисним для оперативного реагування та побудови моделі поведінки зловмисників.

Налаштування геолокаційної візуалізації починається з відкриття модуля карт у Kibana або OpenSearch та вибору типу Coordinate Map чи Maps. Система повинна мати поле з координатами типу geo_point, тому перед побудовою перевіряється, чи IP-адреси зберігаються у вигляді поля на кшталт srcip.location. Якщо координат немає, використовується ingest pipeline з процесором GeoIP, який автоматично додає широту та довготу на основі IP-адреси. Після цього обирається індекс wazuh-alerts-*, у якому зберігаються події безпеки, а у налаштуваннях шару карти задається поле, що містить геолокаційні дані.

Коли карта готова, до неї застосовуються фільтри, щоб концентруватися на конкретних типах загроз. Для аналізу SSH-активності додається умова rule.groups: ssh, а для дослідження виключно невдалих спроб входу – rule.groups: authentication_failed. Після цього карта відображає лише ті географічні точки, що стосуються вибраних подій, забезпечуючи наочну оцінку джерел атак та їх інтенсивності.

V. Спроби автентифікації (успішні та невдалі)

Дана візуалізація забезпечує детальний аналіз спроб входу в систему, допомагаючи виявляти атаки типу brute-force, несанкціонований доступ та аномальні входи з нетипових джерел. Завдяки поділу на успішні та невдалі спроби

можна оцінити, чи мають зловмисники успіх і які механізми безпеки спрацьовують найчастіше.

Створення візуалізації здійснюється на основі індексу wazuh-alerts-*, де в якості часової осі використовується поле @timestamp. Для класифікації результатів входу застосовується поле event.action або data.ssh.event, залежно від джерела журналу. За допомогою цього поля дані поділяються на невдалі та успішні авторизації, що стає основою графічного відображення. За потреби додаються фільтри, як-от rule.groups: authentication або rule.groups: ssh, які дозволяють виділити лише події автентифікації.

VI. Контроль цілісності файлів (Syscheck File Changes)

Візуалізація змін системних файлів дає змогу контролювати потенційно небезпечну активність у файловій системі. Події syscheck свідчать про модифікації, створення або видалення файлів, що може вказувати на діяльність шкідливого ПЗ, ескалацію привілеїв або несанкціоноване адміністрування. Це один із ключових індикаторів компрометації системи.

На етапі налаштування обирається індекс wazuh-alerts-*. Візуалізація базується на полі syscheck.event, у якому міститься тип дії над файлом. Система автоматично формує категорії modified, added, removed. Додавання часової шкали дозволяє бачити інтенсивність змін, а застосування фільтра rule.groups: syscheck дає можливість виділити тільки події контролю цілісності.

VII. Вразливості за хостами (Vulnerability Detector)

Це візуалізація, яка дає змогу оцінити рівень ризику в інфраструктури, показуючи кількість знайдених вразливостей на кожному хості та їхній рівень критичності. Такий аналіз допомагає визначити, які системи потребують першочергового патчування та які вузли є найбільш вразливими до атак.

Налаштування виконується на індексі wazuh-alerts-*, де відбираються події, що містять дані про вразливості. Для цього застосовується фільтр rule.groups: vulnerability-detector. У візуалізації використовуються поля vulnerability.severity та agent.name, які дозволяють будувати графічний розподіл критичності

вразливостей по хостах. Це дає змогу легко визначити найбільш небезпечні системи.

VIII. Мережеві події (NIDS / Firewall / Suricata)

Мережеві візуалізації дають змогу оцінювати структуру та інтенсивність мережевих подій. Вони дозволяють визначати найактивніші порти, протоколи, джерела та типи атак у мережі, що надзвичайно важливо для аналізу DDoS, port-scanning та інших мережевих загроз.

Візуалізація створюється на основі wazuh-alerts-*, де використовуються поля network.protocol, srcport, dstport та IP-адреси. Вибір відповідного поля визначає напрям аналізу: протоколи – для класифікації трафіку, порти – для виявлення сканувань, IP-адреси – для виявлення джерел атак. За необхідності додається фільтр rule.groups: firewall або rule.groups: ids.

IX. Топ джерел інцидентів (Top Alert Sources)

Візуалізація показує, які хости генерують найбільшу кількість попереджень. Це дозволяє виявляти системи, що перебувають під атакою, або ті, де є проблеми з конфігурацією та виникає надмірна кількість тривог. Такий аналіз також допомагає оптимізувати ресурсне навантаження SOC.

Використовується індекс wazuh-alerts-* та поле agent.name, яке групує події за хостами. Візуалізація автоматично сортує хости за кількістю тривог. За потреби накладаються фільтри, що дозволяють аналізувати лише певний тип загроз, наприклад, rule.level або rule.groups.

X. Динаміка тривог у часі (Alerts Over Time)

Це універсальна візуалізація, яка показує загальну активність системи безпеки протягом часу. Вона дозволяє визначити піки атак, оцінити стабільність роботи сервера, а також виявляти зміни у поведінці системи після встановлення оновлень або змін конфігурацій.

У цій візуалізації використовується поле @timestamp, яке задає часову шкалу. Після вибору індексу wazuh-alerts-* система будує лінійний графік, що відображає кількість подій у вибрані проміжки часу. Для глибшого аналізу можна

застосувати додаткові фільтри, які відокремлюють певні категорії подій або рівні серйозності.

2) Рекомендації щодо створення сповіщень (тривог) [44]

Огляд інтерфейсу для створення сповіщень (рис. 4.8-4.14):

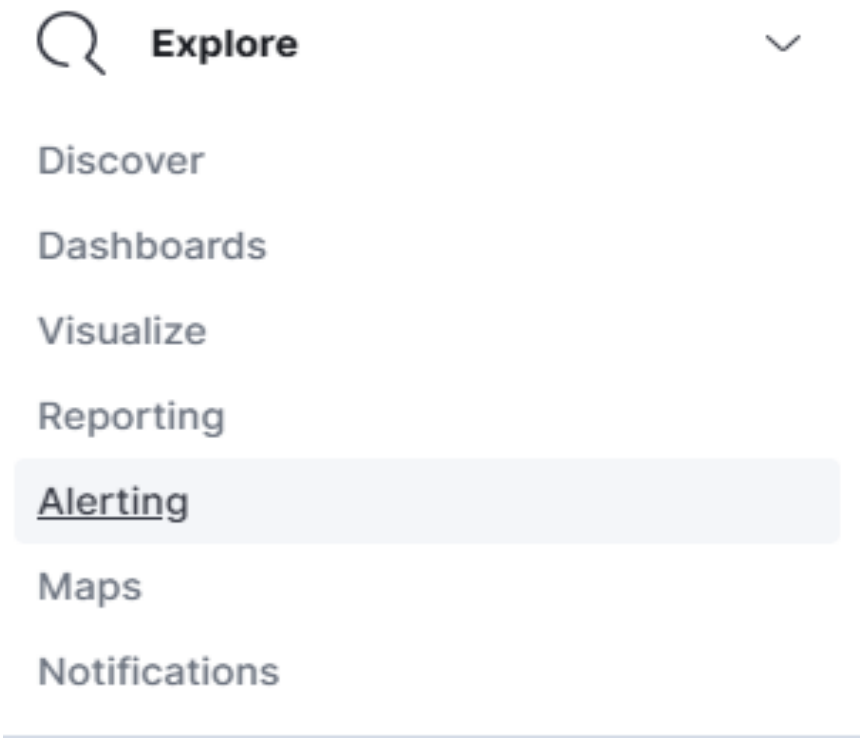

Рисунок 4.8 – Огляд інтерфейсу для створення сповіщень

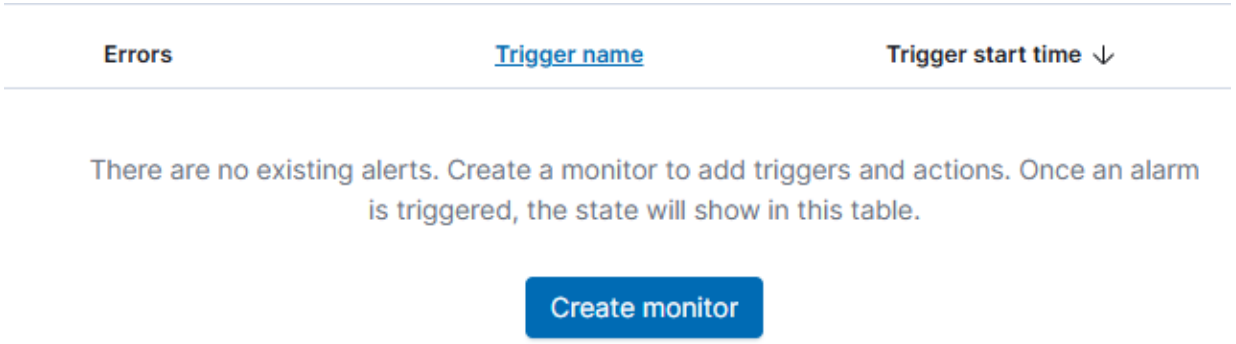

Рисунок 4.9 – Огляд інтерфейсу для створення монітору

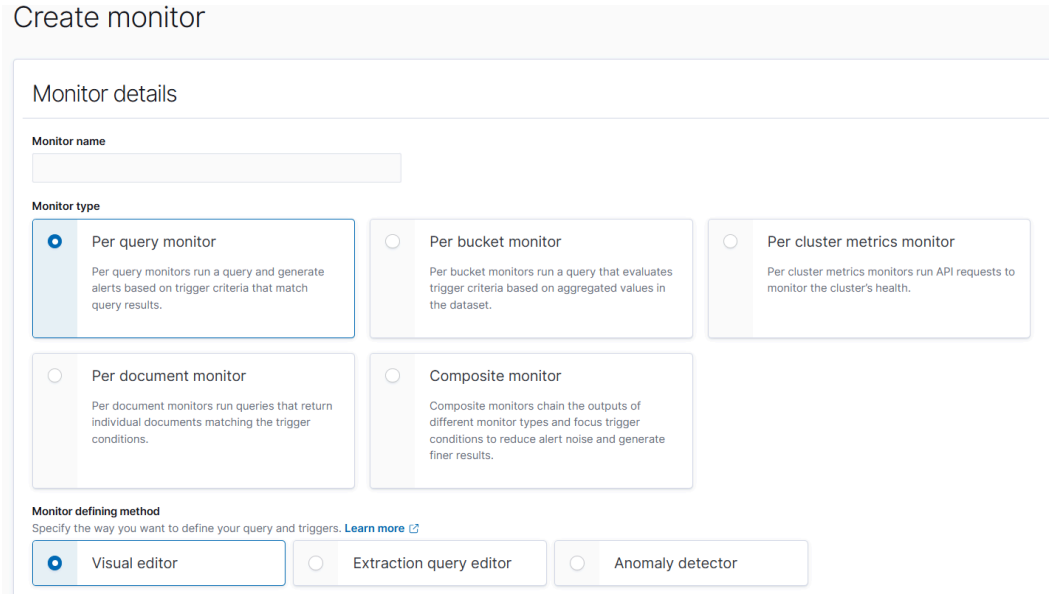

Рисунок 4.10 – Огляд інтерфейсу для створення монітору

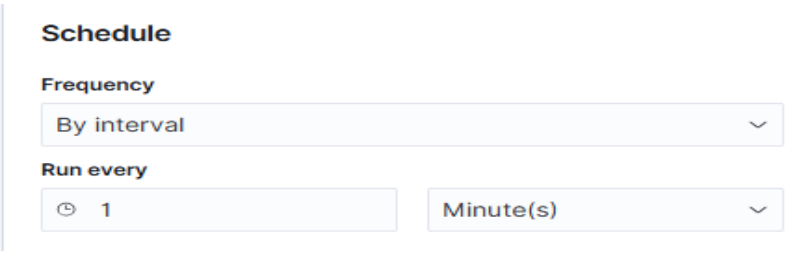

Рисунок 4.11 – Огляд інтерфейсу для створення графіку

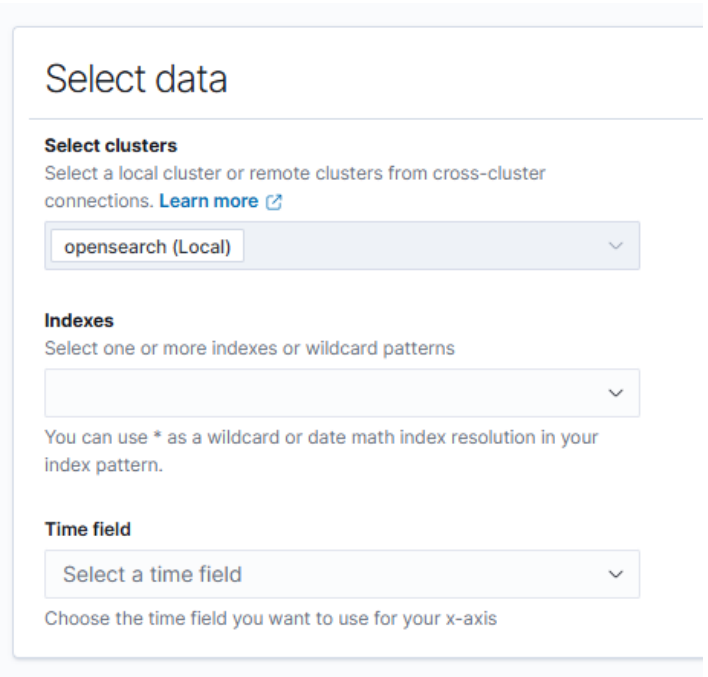

Рисунок 4.12 – Вибір інформації для створення сповіщення

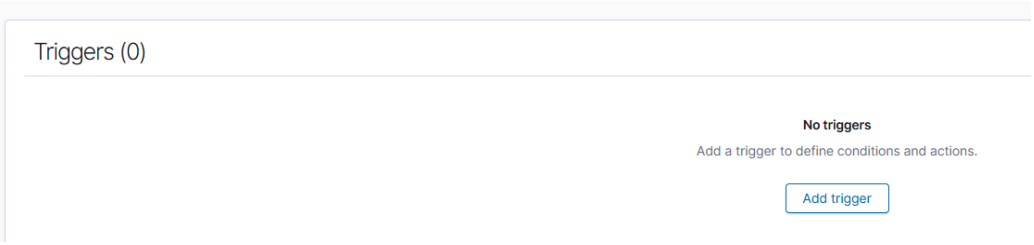

Рисунок 4.13 – Огляд інтерфейсу для створення тригеру

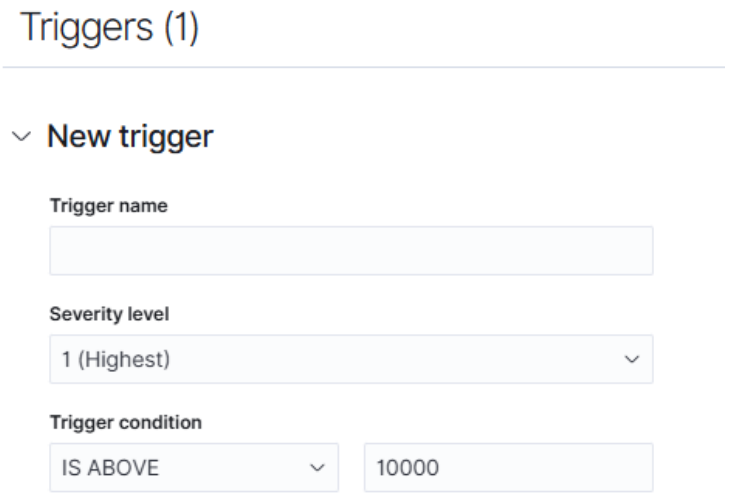

Рисунок 4.14 – Огляд інтерфейсу для створення тригеру

I. Тривога на масові невдалі спроби автентифікації (SSH-брутфорс) [44]. Тривога використовується для виявлення масових невдалих спроб входу через SSH, що є характерною ознакою атаки перебору паролів і може призвести до компрометації серверів. Події цього типу класифікуються у групі authentication_failed.

Створення тривоги виконується у модулі Alerting, де задається тип Per Query Monitor з інтервалом опитування у одну хвилину та джерелом даних wazuh-alerts-. У візуальному редакторі формується фільтр rule.groups: "authentication_failed", який дозволяє відокремити події невдалих входів через SSH. Тригер налаштовується з порогом count() > 10, що означає, що у разі фіксації понад десяти невдалих спроб автентифікації протягом одного циклу моніторингова система надсилатиме сповіщення.

II. Тривога на сканування портів

Така тривога дозволяє виявити спроби сканування портів, які є типовою фазою підготовки атаки та свідчать про збирання інформації щодо відкритих сервісів. Події цього типу найчастіше належать до групи network_scan.

Тривога створюється у Per Query Monitor з джерелом wazuh-alerts-. У редакторі формується фільтр rule.groups: "network_scan", який може бути доповнений статистичним критерієм, наприклад, data.srcip:* AND NOT rule.groups:authentication_failed для виявлення великої кількості різних портів у короткий час. Критерій спрацювання визначається умовою count() > 50, що дозволяє зафіксувати агресивні сканування на ранньому етапі.

III. Тривога на підозрілу активність sudo

Ця тривога дає змогу контролювати спроби ескалації привілеїв через sudo, включно з виконанням атипових команд або численними невдалими спробами. Події цього типу належать до групи sudo.

Монітор створюється з інтервалом перевірки в одну хвилину на основі індексу wazuh-alerts-. У редакторі формується фільтр rule.groups: "sudo", після чого визначається критерій спрацювання. Для аномально високої частоти використовується умова count() > 5, а для фіксації невдалих спроб – пошук подій із описом *authentication error*. У повідомленні містяться ім’я користувача, виконана команда та агент, що дозволяє оцінити ризик ситуації.

IV. Тривога на зміну критичних системних файлів

Тривога призначена для виявлення несанкціонованих змін у ключових конфігураційних файлах, таких як /etc/passwd, /etc/shadow або SSH-конфігурації. Події відносяться до групи syscheck.

У модулі Alerting створюється Per Query Monitor з інтервалом 2-5 хвилин, оскільки подібні зміни трапляються порівняно рідко. Джерелом даних є індекс wazuh-alerts-, а у редакторі формується фільтр rule.groups: "syscheck" з уточненням шляхів file.path: "/etc/*" або конкретних файлів. Тригер визначається умовою count() > 0, оскільки будь-яка зміна критичного файлу потребує негайної уваги.

V. Тривога на підозрілі зміни у списку користувачів і груп

Така тривога дає змогу виявляти маніпуляції з обліковими записами – створення нових користувачів, зміну груп або модифікацію пов’язаних системних файлів. Події можуть бути класифіковані як syscheck або users.

Для створення монітора використовується індекс wazuh-alerts-. У запиті задаються фільтри як для змін у файлах /etc/passwd, /etc/group, /etc/shadow, так і для подій групи users. Тригер count() > 0 дозволяє реагувати на будь-яке втручання у структуру облікових записів, незалежно від масштабу зміни.

VI. Тривога на запуск підозрілих процесів

Призначена для виявлення аномальних процесів, що можуть вказувати на запуск шкідливого ПЗ, скриптів із тимчасових директорій або мережевих утиліт, що використовуються у атаках.

Створюється монітор з індексом wazuh-alerts- і фільтром rule.groups: "process_creation". Уточнюється перелік підозрілих процесів, зокрема "nc", "ncat", "curl", "wget", "bash", "sh", "*miner*", /tmp/*. Тривога спрацьовує за умовою count()>0, а повідомлення містить ім’я процесу, користувача та контекст виконання.

VII. Тривога на зміну конфігурації SSH

Виявляє модифікації у файлі sshd_config, які можуть свідчити про спробу послабити політику доступу та створити несанкціонований бекдор.

Монітор створюється на основі подій syscheck із фільтром file.path: "/etc/ssh/sshd_config". Умова спрацювання count() > 0 дозволяє реагувати на будь-яку зміну параметрів SSH, що може бути ознакою компрометації.

VIII. Тривога на різке зростання мережевої активності

Дозволяє ідентифікувати аномальні піки трафіку, включно з можливими DDoS-атаками, ексфільтрацією даних або роботою ботнет-клієнтів.

Створення монітора здійснюється на основі подій групи network_activity. У тригері задається статистичний поріг, наприклад, count() > 200, що дозволяє

виявляти різкі зміни у мережевому навантаженні. Повідомлення включає IP-джерело та рекомендації щодо перевірки стану мережі.

IX. Тривога на підозрілі зовнішні з’єднання

Фіксує outbound-трафік до небажаних або аномальних зовнішніх IP-адрес, що може вказувати на зв’язок із C2-сервером або викрадення даних.

У запиті формується фільтр event.module: "network" AND network.direction: "outbound", який дозволяє контролювати вихідні з’єднання. Тривога спрацьовує при будь-якій події (count() > 0), якщо IP не входить до дозволеного списку.

X. Тривога на зміну привілеїв користувачів

Призначений для виявлення фактів ескалації прав доступу або модифікації ролей користувачів, що може свідчити про спроби зловмисника отримати контроль над системою.

У фільтрі використовується група user_management, доповнена ознаками зміни привілеїв. Тригер із умовою count() > 0 дозволяє фіксувати кожен випадок модифікації доступу. Повідомлення містить деталі зміни привілеїв та ідентифікатор агента.

XI. Тривога на виконання команд у нестандартний час

Дозволяє виявляти команди, що виконуються поза робочими годинами, що може бути ознакою автоматизованих скриптів або дій зловмисника після компрометації.

Формується фільтр подій rule.groups: "command_execution", доповнений часовою умовою NOT @timestamp BETWEEN "08:00" AND "19:00". Тривога спрацьовує при фіксації будь-якої такої події за умовою count() > 0.

XII. Тривога на виявлення Indicators of Compromise (IoC)

Спрямована на фіксацію шкідливих IP-адрес, доменів, гешів файлів та інших індикаторів, які свідчать про можливу компрометацію системи.

У модулі Alerting задається фільтр rule.groups: "ioc" або data.threat.indicator:*. Тригер count() > 0 забезпечує негайне реагування при появі

індикатора у журналах. Використання інтегрованих списків Threat Intelligence підвищує точність виявлення.

3) Управління вразливостями [45-47]

Регулярний аудит безпеки здійснюється за допомогою сканерів вразливостей, таких як Nessus, OpenVAS та Qualys. Для перевірки конфігурацій застосовуються інструменти CIS-CAT та Lynis, а автоматизоване тестування залежностей виконується за допомогою Snyk або OWASP Dependency Check. Це дозволяє своєчасно виявляти і усувати ризики в інфраструктурі та програмному забезпеченні.

Практичні рекомендації щодо проведення сканування вразливостей за допомогою OpenVAS:

Сканування вразливостей є одним із ключових процесів забезпечення кіберзахисту корпоративної мережі. OpenVAS (Greenbone OpenVAS Scanner) – це відкритий високоточний інструмент, що виконує пошук вразливостей, неправильно налаштованих сервісів та слабко захищених компонентів мережевої інфраструктури. Нижче наведено комплекс практичних рекомендацій для ефективного впровадження та використання OpenVAS у організації.

- Підготовка до сканування [48-50]

Підготовчий етап передбачає обов’язкове оновлення бази вразливостей Network Vulnerability Tests, що забезпечує актуальність перевірок та виявлення нових CVE. На цьому етапі також формується повний інвентар активів, який має охоплювати всі сервери, робочі станції, мережеве обладнання, IoT-пристрої, віртуальні та хмарні ресурси. Для критичних систем визначається рівень впливу сканування, оскільки розширений аналіз може тимчасово впливати на продуктивність. Крім того, доцільно створити окремі профілі сканування: швидкі базові перевірки, стандартні комплексні тести, глибокі сканування для висококритичних вузлів та автентифіковані перевірки для максимально точного результату.

- Виконання сканування OpenVAS [48-50]

Під час виконання сканування пріоритет надається автентифікованому аналізу, оскільки він дозволяє виявляти внутрішні недоліки, включно з неправильними конфігураціями системи, слабкими параметрами ядра, небезпечними версіями бібліотек та відсутністю важливих оновлень. Без цього частина вразливостей залишається непоміченою. У великих мережах важливо оптимізувати навантаження, контролюючи кількість одночасних цілей та інтенсивність тестів. Сканування слід виконувати з урахуванням критичності активів: критичні сервери перевіряють щотижнево, інші – один раз на 2-4 тижні, робочі станції – щомісяця, а зовнішні сервіси DMZ – щотижня або після змін конфігурації. Кожен запуск має бути задокументований із зазначенням цілей, дати, профілю та відповідальних осіб.

- Аналіз та інтерпретація результатів [48-50]

Аналіз результатів базується на пріоритезації вразливостей відповідно до CVSS та важливості активу для бізнес-процесів. Критичні проблеми потребують негайного виправлення, високі – протягом кількох днів, середні – протягом кількох тижнів, а низькі – планового усунення. Обов'язковою частиною є верифікація можливих хибнопозитивних результатів, оскільки деякі знайдені вразливості можуть вимагати додаткової перевірки за допомогою інших інструментів. Виявлені проблеми групуються за категоріями, такими як оновлення ОС і ПЗ, конфігураційні помилки, небезпечні порти та протоколи, слабкі криптографічні параметри або публічні службові інтерфейси. OpenVAS надає рекомендації щодо усунення через функцію Remediation Notes, які потрібно включати до звітів.

- Інтеграція результатів OpenVAS із SIEM-системою

Результати сканувань доцільно інтегрувати в SIEM через syslog або API, що дає можливість аналізувати динаміку вразливостей та співставляти їх із подіями безпеки в реальному часі. На основі цих даних формується дашборд "Vulnerability Management Overview", який може відображати кількість вразливостей за рівнями CVSS, середній час їх усунення, активи зі стійкими проблемами та перелік найпоширеніших вразливостей. Інтеграція також дозволяє корелювати знайдені

слабкі місця з атакувальною активністю: наприклад, якщо інструмент виявив відкрите RDP із застарілою криптографією, SIEM може автоматично контролювати підозрілі спроби підключення до цього сервісу.

- Процес усунення вразливостей

Після аналізу формується план виправлень, який визначає строки усунення та відповідальних осіб. Після впровадження змін проводиться повторне сканування, що має виконуватися протягом 24-48 годин для підтвердження ефективності виправлень. Усі зміни підлягають документуванню із зазначенням суті вразливості, використаних засобів усунення, дат та підтвердження результату повторним аналізом [45, 46].

4) Аудит та контроль відповідності [32]

Організація повинна проводити періодичні пентести (1-2 рази на рік) та аудит мережевих конфігурацій (щоквартально). Важливо, щоб політики та процедури відповідали стандартам ISO 27001 або CIS Controls та вимогам локального законодавства, таким як GDPR, NIS2 або ДСТУ. Це гарантує системний контроль і підтримання високого рівня інформаційної безпеки.

Висновки: рекомендації, сформульовані у цьому розділі, підтверджують, що ефективна методика захисту корпоративних мереж повинна включати як формалізовані політики та процедури, так і впровадження технічних інструментів, що відповідають сучасним вимогам. Важливим чинником залишається людський фактор, що вимагає регулярного навчання персоналу та підвищення їх обізнаності. Таким чином, запропонована методика забезпечує комплексний і гнучкий підхід до мережевої безпеки, адаптований до умов постійного розвитку кіберзагроз.

ВИСНОВКИ

Захист корпоративних мереж є одним із ключових завдань сучасної кібербезпеки, і проведене дослідження дозволяє узагальнити отримані результати, сформувати цілісну картину актуальних загроз і методик їх виявлення та сформувати рекомендації щодо побудови ефективної системи безпеки.

По-перше, досліджено сучасний стан кіберзагроз і встановлено, що атаки на корпоративні мережі еволюціонували від масових поверхневих атак до цілеспрямованих багаторівневих операцій, які реалізуються спеціалізованими групами хакерів. Особливо небезпечними є APT-атаки, ransomware, експлуатація zero-day-вразливостей та соціальна інженерія. Розмаїття векторів атак, включаючи протокольні, програмні, мережеві та людські фактори, свідчить про те, що універсального та простого способу захисту не існує.

По-друге, аналіз інструментів, що використовуються зловмисниками для реалізації атак, показує, що на кожному етапі Cyber Kill Chain атакуючі використовують різні техніки та набори інструментів. Це означає, що системи захисту повинні бути багатофункціональними та здатними протидіяти як на етапі розвідки, так і на фінальних стадіях атаки. Необхідне впровадження засобів виявлення підозрілої активності, механізмів контролю автентифікації, обмеження прав доступу та активного моніторингу подій.

По-третє, огляд існуючих методик захисту показав, що найбільш ефективним підходом є поєднання кількох фреймворків і моделей захисту. NIST CSF 2.0 надає фундамент для управління ризиками на стратегічному рівні. Zero Trust змінює філософію доступу в мережі, ліквідуючи концепцію “довірених” зон. MITRE ATT&CK дає можливість побудувати ефективний механізм виявлення атак на основі реальних сценаріїв. SASE, SSE, EDR/XDR, SIEM, SOAR і традиційні мережеві контролі створюють багаторівневу систему активного моніторингу та блокування загроз.

Особливо важливим результатом дослідження стало усвідомлення того, що технічні засоби не можуть бути ефективними без організаційної зрілості та належного рівня обізнаності співробітників. Соціальна інженерія залишається одним із найефективніших методів проникнення в корпоративні системи. Тому навчання персоналу, регулярні тренінги, тестування на фішинг, симуляції атак та формування безпекової культури є невід'ємними складовими системи захисту.

У межах роботи розроблено та обґрунтовано власну методику пошуку вразливостей, що має низку важливих переваг. Вона включає регулярне мережеве сканування, динамічну оцінку конфігурацій, аналіз активів, сегментацію, перевірку довірених зон, контроль відкритих портів, аудит привілейованих облікових записів та тестування кінцевих точок за допомогою EDR/XDR. Окремо було включено компонент оцінки людського фактору, що дозволяє оцінювати поведінкові ризики та рівень безпекової грамотності персоналу.

Проведене тестування запропонованої методики підтвердило її ефективність та практичну цінність. Вона дозволяє не лише виявити вразливості у мережевій архітектурі, але й сформувати рекомендації щодо їх усунення, що сприяє зниженню ймовірності успішної атаки. Методика може бути адаптована до особливостей конкретних організацій і масштабована відповідно до кількості користувачів, сервісів і рівня критичності ресурсів.

Отримані результати показують, що безпека корпоративних мереж повинна розглядатися як безперервний процес, а не одноразова дія. Оскільки ландшафт загроз постійно змінюється, необхідним є регулярний аудит захисту, оновлення систем, впровадження нових методів виявлення атак та оперативне реагування на інциденти. Рекомендовано перехід від традиційної реактивної безпеки до моделі превентивного та проактивного захисту, який передбачає виявлення аномалій у поведінці користувачів, аналіз трафіку та прогнозування ризиків.

Таким чином, наукова та практична цінність роботи полягає у формуванні комплексного підходу до захисту корпоративних мереж, що включає технічні, організаційні та поведінкові аспекти. Створена методика дозволяє будувати

адаптивну систему безпеки, яка здатна своєчасно реагувати на загрози та забезпечувати стійкість мереж до кіберінцидентів. Проведене дослідження не лише поглиблює розуміння механізмів атак і засобів захисту, але й формує основу для подальших наукових і прикладних розробок у сфері кібербезпеки, що має важливе значення в умовах сучасної цифрової трансформації бізнесу та зростання взаємозалежності інформаційних систем.

Висновок: розробка сучасних методик захисту корпоративних мереж має базуватися на комплексному погляді на проблему безпеки, поєднуючи технологічні інновації, процесне управління ризиками та людський фактор. Ефективне впровадження запропонованих рекомендацій дозволить організаціям значно підвищити рівень кіберзахисту та знизити ризик успішних атак у мінливому середовищі кіберзагроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Cisco Networking Academy. Cybersecurity. [Електронний ресурс]. – Режим доступу: https://www.netacad.com/cybersecurity.

2. DATAMI. Типи кібератак. [Електронний ресурс]. – Режим доступу:https://datami.ee/ua/blog/types-of-cyberattacks-4-classifications-of-cyber-threats/.

3. Cisco. What is a Cyberattack? [Електронний ресурс]. – Режим доступу: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-cyberattack.html.

4. Cloudflare. Attack Vector. [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/security/glossary/attack-vector/.

5. AVOIDIT: A Cyber Attack Taxonomy. – Режим доступу: https://nsarchive.gwu.edu/sites/default/files/documents/4530310/Chris-Simmons-Charles-Ellis-Sajjan-Shiva.pdf.

6. Scarfone, K., Souppaya, M., et al. Technical Guide to Information Security Testing and Assessment. NIST, Sept. 2008. [Електронний ресурс]. – Режим доступу: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152164.

7. CTO Help. Exam Objectives Sec2. [Електронний ресурс]. – Режим доступу: https://www.cto-help.com/secplus/ExamObjectivesSec2.html.

8. NIST. Computer Security Incident Handling Guide, Special Publication 800-61r2. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

9. Syteca. Opportunistic Insiders. [Електронний ресурс]. – Режим доступу: https://www.syteca.com/en/blog/opportunistic-insiders.

10. Pentera. Defending Against Computer Network Attacks. [Електронний ресурс]. – Режим доступу: https://pentera.io/glossary/defending-against-computer-network-attacks/.

11. Chainlink Education Hub. Replay Attack. [Електронний ресурс]. – Режим доступу: https://chain.link/education-hub/replay-attack.

12. Itorakul. Cyber Kill Chain. [Електронний ресурс]. – Режим доступу: https://itorakul.com.ua/cyber-kill-chain/.

13. CrowdStrike. Cyber Kill Chain. [Електронний ресурс]. – Режим доступу: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/cyber-kill-chain/.

14. MITRE. ATT&CK Techniques: T1033. [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/techniques/T1033/.

15. NIST. Cybersecurity White Paper. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

16. NIST. Zero Trust Architecture, Special Publication 800-207. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf.

17. ANSSI. Views on the Zero Trust model. – Режим доступу: https://cyber.gouv.fr/sites/default/files/document/Anssi%20views%20on%20the%20Zero%20Trust%20model_0.pdf.

18. Palo Alto Networks. What is a Zero Trust Architecture? [Електронний ресурс]. – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture.

19. MITRE ATT&CK Framework. [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/.

20. MITRE. ATT&CK Design and Philosophy, March 2020. – Режим доступу: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

21. MITRE ATT&CK Resources. [Електронний ресурс]. – Режим доступу: https://attack.mitre.org/resources/.

22. NetworkWorld. Digital Transformation with SD-WAN, SASE and SSE. [Електронний ресурс]. – Режим доступу: https://www.networkworld.com/article/971198/digital-transformation-with-sd-wan-sase-and-sse.html.

23. Gartner. Secure Access Service Edge (SASE) Glossary. [Електронний ресурс]. – Режим доступу: https://www.gartner.com/en/information-technology/glossary/secure-access-service-edge-sase.

24. Palo Alto Networks. EDR vs XDR. [Електронний ресурс]. – Режим доступу: https://www.paloaltonetworks.com/cyberpedia/what-is-edr-vs-xdr.

25. Corelight. NDR, EDR, XDR Glossary. [Електронний ресурс]. – Режим доступу: https://corelight.com/resources/glossary/ndr-edr-xdr.

26. SentinelOne. EDR vs NDR vs XDR. [Електронний ресурс]. – Режим доступу: https://www.sentinelone.com/cybersecurity-101/endpoint-security/edr-vs-ndr-vs-xdr/.

27. Microsoft. What is SOAR? [Електронний ресурс]. – Режим доступу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-soar.

28. SecurityScorecard. SIEM vs SOAR. [Електронний ресурс]. – Режим доступу: https://securityscorecard.com/blog/siem-vs-soar/.

29. Swimlane. SOAR Capabilities eBook. – Режим доступу: https://swimlane.com/assets/uploads/documents/SOAR_Capabilities_e_book___Swimlane.pdf.

30. LogManager. SIEM vs SOAR [Електронний ресурс]. – Режим доступу: https://logmanager.com/blog/security/siem-vs-soar/.

31. Держспецзв'язку України. Рекомендації щодо забезпечення кіберзахисту. – Режим доступу: https://mtu.gov.ua/files/%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D1%96%D1%97_%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA%D0%B0.pdf.

32. ISO/IEC 27001:2022. [Електронний ресурс]. – Режим доступу: https://learn.microsoft.com/fr-fr/azure/compliance/offerings/offering-iso-27001.

33. NIST SP 800-53 Revision 5. [Електронний ресурс]. – Режим доступу: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

34. CIS Controls v8. [Електронний ресурс]. – Режим доступу: https://www.cisecurity.org/insights/white-papers/cis-controls-v8.

35. Palo Alto Networks. NGFW Overview. [Електронний ресурс]. – Режим доступу: https://www.scribd.com/presentation/886757899/Palo-Alto-NGFW-Spotlight-2025.

36. Fortinet. ZTNA vs VPN. [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/ztna-vs-vpn.

37. CrowdStrike. EDR/XDR Overview. [Електронний ресурс]. – Режим доступу: https://www.exabeam.com/explainers/crowdstrike/crowdstrike-xdr-solution-overview-pricing-pros-and-cons/.

38. Veeam. Microsoft 365 Backup 3-2-1. [Електронний ресурс]. – Режим доступу: https://www.veeam.com/blog/microsoft-365-backup-3-2-1-veeam-data-cloud.html.

39. SentinelOne. Cloud Security Comparison. [Електронний ресурс]. – Режим доступу: https://www.sentinelone.com/cybersecurity-101/cloud-security/casb-vs-cspm-vs-cwpp/.

40. KnowBe4. Security Awareness Training Overview. [Електронний ресурс]. – Режим доступу: https://www.knowbe4.com/products/security-awareness-training/pricing.

41. SHI. Security Awareness Best Practices. [Електронний ресурс]. – Режим доступу: https://blog.shi.com/cybersecurity/security-awareness-training-best-practices/.

42. Wazuh Official Documentation. XDR Capabilities. [Електронний ресурс]. – Режим доступу: https://wazuh.com/platform/xdr/.

43. Wazuh/OpenSearch Documentation. Custom Dashboard. [Електронний ресурс]. – Режим доступу: https://medium.com/@gibinkjohnofficial/creating-custom-wazuh-dashboard-dl-series-7-9d4cf73e316f.

44. Wazuh Documentation. Alert Management. [Електронний ресурс]. – Режим доступу: https://documentation.wazuh.com/current/user-manual/manager/alert-management.html.

45. Greenbone Networks (OpenVAS). System Architecture. [Електронний ресурс]. – Режим доступу: https://greenbone.github.io/docs/latest/background.html.

46. Tenable Nessus. CVSS vs VPR. [Електронний ресурс]. – Режим доступу: https://docs.tenable.com/nessus/Content/RiskMetrics.htm.

47. MITRE ATT&CK Navigator. [Електронний ресурс]. – Режим доступу: https://mitre-attack.github.io/attack-navigator/.

48. OpenVAS – full-featured vulnerability scanner. [Електронний ресурс]. – Режим доступу: https://openvas.org/.

49. Greenbone Documentation. Офіційна документація та мануали. [Електронний ресурс]. – Режим доступу: https://docs.greenbone.net/.

50. HackerTarget. OpenVAS Installation and Setup Guide. [Електронний ресурс]. – Режим доступу: https://hackertarget.com/install-openvas/.