УДК 004.7

Л.А. Савицька[1], Т.І. Коробейнікова[2], О.П. Волос[1], М. Г. Тарновський[1]

МЕТОД ТА ЗАСІБ МОНІТОРИНГУ БЕЗПЕКИ В КОМП'ЮТЕРНІЙ МЕРЕЖІ ЗАСОБАМИ SIEM

[1]Вінницький національний технічний університет, Вінниця

[2]Національний університет «Львівська політехніка»

Анотація. Дана робота присвячена дослідженню, аналізу та вдосконаленню методів та засобів моніторингу безпеки в комп’ютерних мережах. У цій роботі засоби і методи моніторингу безпеки мережі розробляються на основі агентів системи SIEM (система управління інформацією про моніторинг мережі) з удосконаленням процесу нормування даних від журналів безпеки. Причому, для прискорення процесів реагування на загрози мережевої безпеки комп’ютерної мережі досліджується робота SIEM з точки зору тріади SIEM-EDR-NDR. Дослідження ґрунтуються на досвіді роботи іноземних компаній та вітчизняних банківських мереж.

У дослідженні розглядається взаємодія компонентів SIEM-EDR-NDR, утворюючи SOC-тріаду. SIEM використовується для централізованого аналізу даних, включаючи EDR і NDR, надаючи повну картину безпеки. EDR виявляє та реагує на загрози на кінцевих точках, а NDR доповнює його, розширюючи аналіз SIEM. Така комбінація забезпечує ефективне реагування на кібератаки, зменшуючи "час перебування" до виявлення.

Розглянуто формування завдань компонентів EDR у тріаді SIEM-EDR-NDR. Звернуто увагу на важливість захисту кінцевих пристроїв від всіх етапів атаки та визначено ефективні стратегії, такі як аналіз трафіку, контроль додатків та централізоване управління кібербезпекою. Наголошено на інтеграції EDR з існуючими засобами безпеки для створення комплексної системи.

У контексті SIEM висвітлено етапи обробки даних, починаючи від збору журналів і нормалізації до класифікації подій і кореляції. Підкреслено роль кореляції у формуванні інцидентів та проведенні розслідувань. Запропоновано удосконалену схему нормалізації з розширеною розгорткою агентів та ключовими етапами обробки даних в межах SIEM-системи.

Робота розглядає вдосконалення обробки журналів подій у SIEM для ефективного моніторингу мережевої безпеки та оперативного усунення загроз. Досягнута мета сприяє прискоренню процесів реагування на загрози завдяки інтеграції агентів SIEM в середовище, що дозволяє упорядковувати та класифікувати потоки інформації для оперативного усунення загроз..

Ключові слова: моніторинг, SIEM, EDR,NDR, тріаді SIEM-EDR-NDR, процес нормалізації журналів.

Abstract. This work focuses on researching, analyzing, and enhancing methods and tools for security monitoring in computer networks. The study develops security monitoring tools and methods based on SIEM agents, improving the data normalization process from security logs. The research explores SIEM's role in the SIEM-EDR-NDR triad perspective to accelerate responses to network security threats. The investigation is grounded in the experiences of foreign companies and domestic banking networks.

The interaction of SIEM-EDR-NDR components, forming a SOC triad, is examined. SIEM is utilized for centralized data analysis, including EDR and NDR, providing a comprehensive security overview. EDR detects and responds to threats on endpoints, complemented by NDR, extending SIEM analysis. This combination ensures effective response to cyberattacks, reducing "dwell time" until detection.

The formulation of tasks for EDR components in the SIEM-EDR-NDR triad is discussed. Emphasis is placed on the importance of protecting endpoints at all stages of an attack, and effective strategies, such as traffic analysis, application control, and centralized cybersecurity management, are identified. Integration of EDR with existing security tools to create a comprehensive system is highlighted.

Within the SIEM context, data processing stages, from log collection and normalization to event classification and correlation, are illuminated. The role of correlation in incident formation and investigation is underscored. An enhanced normalization scheme with an expanded agent deployment and key data processing stages within the SIEM system is proposed.

The work addresses the improvement of event log processing in SIEM for effective network security monitoring and timely threat mitigation. The achieved goal accelerates threat response processes through SIEM agent integration, facilitating the organization and classification of information flows for prompt threat mitigation.

Key words: testing, monitoring, SIEM, EDR,NDR, SIEM-EDR-NDR triad, log normalization process.

DOI: https://doi.org/10.31649/1999-9941-2023-58-3-22-32.

Вступ

Питання моніторингу безпеки в комп’ютерній мережі (КМ) стає все більш актуальним і важливим у всьому світі. Протягом лише 2021 року світова економіка зазнала значних втрат через кібератаки на загальну суму 6 трлн. доларів [1]. Україна не вийшла з-під цієї загрози, ба навіть зазнала її ще більше. За даними аналізу, проведеного компанією Microsoft у 2021 році, майже 20% світових кібератак спрямовані на Україну, що робить нашу країну другою за кількістю кібератак у світі, випереджаючи багатонаціональні корпорації [2]. Це великий виклик, оскільки з 2014 року Україна веде гібридну війну, включаючи і кібернетичний фронт.

З початком відкритої війни росії проти України в лютому 2022 року атаки ще більш загострилися. Лише впродовж перших 400 днів війни на Україну було скоєно понад 3000 потужних кібератак: DDoS атаки, атаки шкідливим програмним забезпеченням (ПЗ), ботнети, фішингові розсилки тощо [3].

Ураховуючи значні втрати моніторинг безпеки в КМ є одним із головних пріоритетів у системі національної безпеки. Отже, для відповіді на ці зростаючі загрози Україна вживає такі контрзаходи:

1) Працює Національний координаційний центр з безпеки [4], який курує заходи щодо кібербезпеки на національному рівні.

2) Працюють державний центр CERT-UA (Computer Emergency Response Team) та регіональні центри CSIRT (Computer Security Incident Response Team), які відповідають за забезпечення захисту інформації та комп’ютерних мереж від несанкціонованих доступів та кібератак [5].

3) Активно ведуть дії кібервійська [6], яка містять спецпідрозділи і фахівців для ведення операцій з кібербезпеки.

4) З метою нормативно-правового регулювання, у 2021 році прийнята нова Стратегія кібербезпеки України, яка має на меті створення безпечного кіберпростору та забезпечення безпеки в цьому важливому сегменті [7].

Актуальність

Всі ці заходи мають на меті забезпечити постійний моніторинг безпеки в КМ, аналіз вторгнень у мережу та виявлення атак в режимі real_time. Враховуючи нові виклики, що виникають у зв'язку з повною цифровою трансформацією країни, створюються можливості для досягнення цих завдань:

1) Розвиток новітніх організаційно-технічних моделей, що сприяють ефективному захисту комп’ютерних мереж та даних.

2) Впровадження інноваційних інструментів для оперативного виявлення та запобігання атак, і це допомагає реагувати на загрози вчасно та ефективно.

3) Підтримка досліджень і розробок у галузі кібербезпеки, спрямованих на розвиток новітніх IT-технологій та штучного інтелекту (ШІ).

Отже, тематика дослідження є актуальною, водночас існує реальна потреба у подальшому вдосконаленні методів і засобів для постійного і надійного моніторингу безпеки в комп’ютерних мережах.

Мета

Метою статті є прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів подій у методі інтеграції SIEM та її агентів в середовище. Запропонований підхід має потенціал упорядковувати і систематизувати хаотичні та розкидані дані про події у комп’ютерній мережі. Це дозволить конвертувати цю інформацію в зручний та легко зрозумілий формат, представленням у вигляді діаграм і графіків. Такий підхід сприяє оперативному виявленню можливих загроз та надає адміністраторам системи інструменти для їх швидкого усунення.

Задачі

1. дослідити новітній підхід щодо моніторингу безпеки в комп’ютерних мережах, зокрема, в парадигмі тріади SIEM-EDR-NDR;
2. дослідити новітній підхід щодо розробки неперервного ефективного моніторингу безпеки в комп’ютерних мережах у центрах SOC;
3. запропонувати альтернативний процесу обробки журналів подій.

Моніторинг безпеки в комп’ютерних мережах

Відповідно до стандарту ISO/IEC 27005 [8-9], рекомендується виконувати підготовку моніторингу безпеки в КМ за таким планом (рис. 1).

Рисунок 1 – Узагальнений план моніторингу безпеки в КМ

Дослідження потенційних загроз, дослідження можливих вразливостей активів та формування політик безпеки – це ті пункти плану, що становлять інтерес дослідження і де присутній моніторинг безпеки в КМ. За визначенням, активами вважаються всі ресурси, які мають цінність для компанії і вимагають захисту [9] (рис. 2). Серед таких активів можна відзначити: приміщення, в якому розміщена КМ; інформація, яку тут обробляють і зберігають; засоби комп’ютерних мереж: програмне, технічне обладнання (сервери, мережеві та кінцеві пристрої, засоби зв'язку і т. д.) [10].

Усі ці активи повинні бути ідентифіковані і обліковані. Фахівці проводять експертну оцінку відносної цінності цих активів (низька, середня, висока) з урахуванням можливих втрат або пошкоджень. На рисунку 2 показана схема дослідження активів під час моніторингу безпеки в інформаційній КМ.

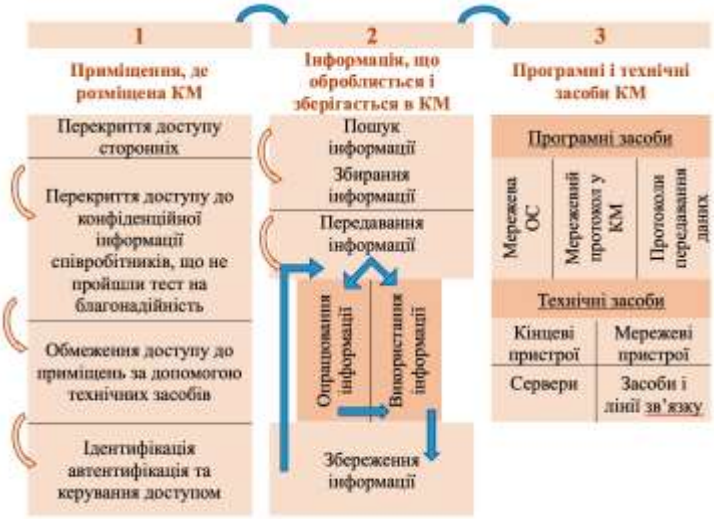

Рисунок 2 – Узагальнена схема дослідження активів під час моніторингу безпеки в КМ

Ккіберзагроза є потенційно небезпечним явищем чи фактором, що становить ризик для активів мережі та загалом для інформаційної безпеки (ІБ) компанії [9-14]. ІБ містить заходи, спрямовані на забезпечення захищеності від потенційних загроз. Загроза може завдати шкоди активам. Важливо ідентифікувати і випадкові, і навмисні загрози та визначити їх джерела. Типові загрози ІБ можуть бути класифіковані за різними ознаками: за аспектом, який вони спрямовані порушити; за місцем походження загроз; за рівнем впливу на КМ; за природою виникнення. За відношенням до аспектів, який можна порушити, загрози такі: загрози конфіденційності, цілісності, доступності:.За локалізацією джерела загроз, їх можна поділити на: внутрішні та зовнішні. За розмірами завданої шкоди, загрози поділяються на: загальні, локальні загрози та приватні загрози. За ступенем впливу на КМ, загрози поділяються на: пасивні загрози та активні загрози. За природою виникнення загрози, загрози можна розмежувати на природні (об'єктивні) та штучні (суб'єктивні) загрози. Джерелами загроз можуть бути суб'єкти (особи), об'єктивні прояви (конкуренти або злочинці).

Рисунок 3 – Схема загальної класифікації загроз під час моніторингу КМ

Джерела загроз призначені для отримання доступу до даних, їх модифікації і завдання прямої матеріальної шкоди. Необхідно позначити кожний актив у відповідності до видів загроз. Результатом аналітичної обробки цієї інформації є схема загальної класифікації загроз під час моніторингу інформаційної КМ (див. рис. 3).

Дослідження вразливостей активів є важливою частиною процесу моніторингу безпеки КМ. Уразливість в цьому контексті означає недолік або слабкість в активі або засобах захисту, яка може бути використана загрозами [112]. Різноманітність вразливостей покладає особливі вимоги на системи моніторингу безпеки в КМ. Поняття політики безпеки є ключовим в під час моніторингу безпеки КМ.

Після аналізу активів, потенційних загроз і вразливостей активів, формулюються політики інформаційної безпеки (ІБ).

Згідно зі стандартом ISO/IEC 27002 [5], політика ІБ є комплексом нормативних, організаційних та експлуатаційних документів, які охоплюють всі аспекти організації, керування та контролю ІБ та експлуатації засобів захисту. Отже, основною метою забезпечення ІБ є захист інформації від випадкових або навмисних втручань. Водночас ІБ також спрямована на забезпечення неперервності бізнес-процесів.

В таблиці 1 наведено принципи побудови системи ІБ.

Таблиця 1.1 – Принципи побудови системи інформаційної безпеки

Генеральний підхід	СЗ інформації повинна бути комплексною, охоплювати організаційні заходи, технічні та програмні засоби.
Системний підхід	Всі заходи і засоби захисту повинні бути пов’язані, узгоджені і забезпечувати цілісність системи.
Структурна ієрархія	Згідно із завданням тут повинен бути реалізований принцип поглибленого багаторівневого захисту .
Усеосяжність	Система захисту повинна охоплювати всі активи, всі вузли та кінцеві пристрої КМ, у тому числі BYOD.
Забезпечення надійності	Повинні бути створені такі механізми захисту, щоб вартість зламу її була дорожчою за інформацію, яку зловмисник прагне поцупити.
Контроль на всіх рівнях	Контроль повноважень будь-якого звернення до інформації повинен охоплювати всі рівні контролю: інформацію, ПЗ, апаратуру, персонал.
Цикл Демінга «PDCA»	Цикл моделі «PDCA» передбачає обов’язкові етапи: 1) Встановлення цілей та політик СЗ (Plan); 2) Реалізацію і впровадження СЗ (Do); 3) Оцінку, контроль, моніторинг і аналіз (Check); 4) Покращення (удосконалення і розвиток) СЗ (Act).

У таблиці 1 вказані основні загальноприйняті принципи побудови системи ІБ та використані такі скорочення: СЗ – система захисту; BYOD – Bring Your Own Device, особисті мобільні пристрої, яким дозволений доступ до КМ; PDCA – Plan-Do-Check-Act, модель безперервного поліпшення процесів.

Для виконання політик інформаційної безпеки на підприємстві реалізується відповідна низка заходів. Ці заходи включають в себе розробку і впровадження правил і процедур для забезпечення конфіденційності, цілісності і доступності інформації, встановлення відповідних технічних засобів захисту, навчання персоналу з питань інформаційної безпеки, а також постійний моніторинг і аналіз з метою виявлення і вирішення потенційних загроз

Моніторинг безпеки в комп’ютерних мережах в парадигмі тріади SIEM-EDR-NDR

Компоненти SIEM-EDR-NDR взаємодіють та вирішують завдання спільно, формуючи єдиний функціональний блок (SOC-тріаду) [15-19]. SIEM створює централізоване інформаційне вікно для аналітиків, щоб корелювати зібрані дані в середовищі, в т.ч. від EDR і NDR, та дозволяє командам забезпечення безпеки відокремлювати системні попередження та проводити аналіз потенційних загроз. SIEM забезпечує всебічний погляд на безпеку і використовує механізми з різних джерел, включаючи кінцеві точки, спеціальні програми, хмарні служби та інші джерела даних. Ці журнали збираються у різних форматах і піддаються аналізу для забезпечення їх кореляції та ефективного аналізу, що вказує на покращені можливості раннього виявлення і, отже, на досягнення головної мети SIEM – скорочення «часу перебування» до моменту виявлення.

EDR надає інформацію про зловмисну активність на кінцевих точках організації в рамках SOC-тріади. Виявляє, реагує на різні типи зловмисного ПЗ, а також забезпечує докладний огляд та повну видимість пристроїв у мережі. Можливості NDR доповнюють засоби EDR, усуваючи прогалини агентів EDR, і розширюють аналіз журналу SIEM, асоціюючи виявлені загрози з мережевою активністю та надаючи їм необхідний контекст.

Отже, комбінація цих рішень у складі SOC-тріади забезпечує неперевершену видимість та автоматичність реагування в умовах кібератаки.

Рисунок 4 – SOC-тріада

Тобто разом всі ці рішення, які схематично зображенні на рис. 4, забезпечують повну видимість та безпеку системи.

Новітній підхід щодо розробки неперервного ефективного моніторингу безпеки в комп’ютерних мережах у центрах SOC

Формування задач складових EDR у тріаді SIEM-EDR-NDR. Кожен кінцевий пристрій, який підключений до мережі, є «входом» до конфіденційної інформації. Тому важливо враховувати основні принципи розробки ефективної стратегії кіберзахисту кінцевих пристроїв у мережі:

Захист повинен виявляти і ліквідовувати всі етапи атаки. А саме, ефективний захист від вторгнень містить: засоби перевірки поштових додатків (електронна пошта залишається основним «засобом поширення зловмисних кодів» на пристроях користувачів); засоби захисту від завантаження небажаних. Тут працює технологія, яка аналізує весь вхідний та вихідний трафік і надає захист браузера, щоб блокувати такі загрози перед їх запуском на кінцевому пристрої; потужний захист самого кінцевого пристрою, із службами контролю та додатків, а також сам пристрій.

Механізм реагування та розслідування інцидентів має демонструвати конкретні результати, має мати можливість ізолювати кінцевий пристрій для ефективного вивчення інциденту, зупиняти поширення вірусів та відновлювати пристрій за допомогою його незараженої копії.

Система не повинна впливати на бізнес-процеси, тобто заходи безпеки не повинні заважати нормальному функціонуванню бізнес-процесів та швидкому обміну даними в мережі.

Централізоване управління кібербезпекою. Отже, політики адміністрування та сам протокол безпеки повинні включати заходи забезпечення безпеки всіх компонентів мережі підприємства, об'єднуючи всі кінцеві пристрої (BYOD). Кожен такий пристрій повинен відповідати вимогам доступу до мережі, що передбачає автоматизацію їхнього кіберзахисту.

Загалом, для дотримання політик безпеки кінцевих пристроїв ураховуючи зростання загроз, необхідно застосовувати: мережеві екрани для різних типів пристроїв; антивіруси для електронної пошти; моніторинг, фільтрацію та захист web-трафіку; управління безпекою та захисні рішення для MDM; контроль роботи додатків; шифрування; виявлення вторгнень.

EDR є інтегрованою системою безпеки кінцевої точки, об'єднує постійний моніторинг у реальному часі та збір даних із функціями автоматизованого реагування та аналізу на основі правил. Важливо відзначити, що EDR доповнюють, а не замінюють попередні засоби безпеки, інтегруються з ними для створення більш ефективної та комплексної системи захисту.

Інструментарій EDR складається із трьох основних компонентів:

1. Агенти збору даних. Моніторинг кінцевих точок та збір даних (процеси, підключення, обсяг активності та передача даних) і передавання цієї інформації у центральну БД.
2. Автоматизована відповідь. Заздалегідь налаштовані правила в рішенні EDR спроможні виявляти вхідні дані, що вказують на відомий тип порушення безпеки, та запускати автоматизовану реакцію, наприклад, вихід із системи кінцевого користувача чи висилання сповіщення співробітнику.
3. Аналіз та криміналістика. Аналіз в реальному часі та швидка діагностики загроз, застосуванння інструментів криміналістики для виявлення загроз чи проведення пост-аналізу атаки.

Безпека системи EDR забезпечує інтегроване централізоване середовище для збору, кореляції та аналізу даних кінцевих точок, а також для координації сповіщень і реагування на активні загрози (рис. 5). EDR операційно взаємодіють за допомогою агентів, які встановлюються на локальних пристроях. З метою полегшення управління ними вони централізовано об'єднуються через центральний хаб. Кілька

агентів приєднуються до цього централізованого хабу, і кожен постійно моніторить пристрій та надає інформацію для подальшого аналізу.

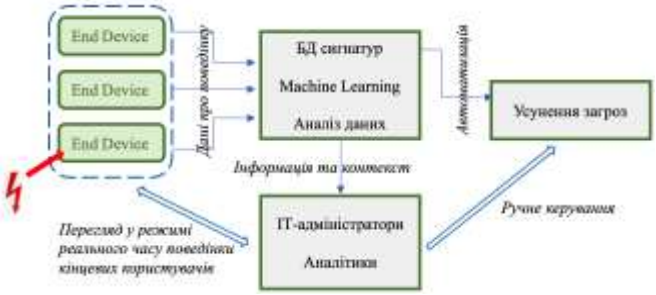

Рисунок 5 – Відома схема роботи EDR-систем

Дані, отримані з різних кінцевих точок, транслюються до централізованого хабу для проведення обробки та аналізу, часто використовуючи машинне навчання. Розроблені під час цього процесу статистичні моделі використовуються для часу аналізу вхідних даних з кінцевих точок та виявлення потенційних загроз.

У випадку виявлення загрози система EDR генерує сповіщення та надсилає його IT-адміністраторам чи команді кібербезпеки через інтерфейс користувача, які, здійснюють ізоляцію (переміщення в пісочницю) або вилучення шкідливих файлів, і так усувають потенційну загрозу. Саме так і пропонується вдосконалити схему відомого принципу функціонування EDR-системи (рис. 6).

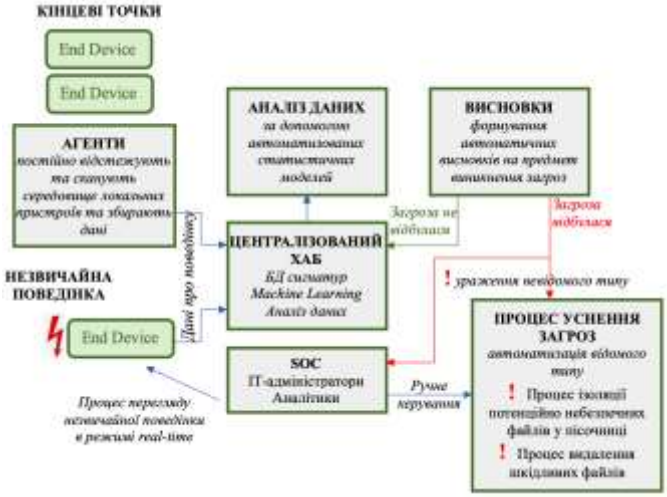

Рисунок 6 – Вдосконалений принцип роботи EDR-системи

Методи виявлення потенційних загроз в EDR:

- аналіз сигнатур – порівняння сигнатур мережевого трафіку із базою даних відомих сигнатур зловмисного програмного забезпечення;
- аналіз поведінки – поріг прийняття поведінки кінцевої точки порівнюється для виявлення випадків аномальної активності;
- аналіз пісочниці – потенційно небезпечні файли ізолюються в безпечному середовищі (пісочниці), і їхнє взаємодію спостерігається, уникаючи можливих негативних впливів на кінцеву точку;
- відповідність білого/чорного списків – дії кінцевих точок порівнюються із наперед визначеним списком IP-адрес у білому та чорному списках для контролю дозволеного/забороненого мережевого трафіку.

Формування задач складових NDR у тріаді SIEM-EDR-NDR. Як важливий елемент мережевої безпеки, система NDR (мережеве виявлення та реагування) містить технології мережевої безпеки для автоматизованого контролю, виявлення, аналізу та реагування на кіберзагрози.

Засоби NDR, які реалізовані для аналізу мережевого трафіку, включають IDS/IPS і розширений аналіз загроз, що надає змогу командам забезпечення безпеки спостерігати за мережевим трафіком в реальному часі та швидко реагувати на потенційні загрози.

У зв'язку з розширенням розподілених мереж, інструменти безпеки на основі сигнатур, такі як IDS/IPS, стають недостатніми для ефективного забезпечення безпеки підприємств. Рішення NDR використовують розширену поведінкову аналітику, машинне навчання та штучний інтелект для забезпечення додаткового рівня захисту в локальних і хмарних середовищах. Важливо відзначити, що рішення NDR не замінюють, а доповнюють попередні засоби моніторингу та аналізу мережі, утворюючи єдину повноцінну систему.

Рішення NDR можуть відстежувати транспортні потоки в обох напрямках (північ-південь та схід-захід, як внутрішні, так і зовнішні) за допомогою стратегічно розташованих датчиків.

Ефективні рішення NDR демонструють ряд переваг:

1. Розширена видимість загроз: групи безпеки можуть відслідковувати загрози, в т.ч. вторгнення та сторонні активності в мережі на локальному рівні та у хмарному середовищі.
2. Зменшення помилкових спрацьовувань: акцентування уваги на реальних вторгненнях.
3. Швидше запобігання або зупинка вторгнення: NDR використовує штучний інтелект і машинне навчання для роботи в режимі реального часу, розпізнавання та зупинки загроз зі швидкістю мережевого зв'язку.
4. Повна візуалізація атак: завдяки інформації про план вторгнень та детальному графіку загроз у мережі, служби безпеки можуть оперативно зрозуміти масштаб атаки та визначити пріоритетність ресурсів.

Рішення NDR постійно аналізують та корелюють значні обсяги мережевого трафіку та подій безпеки (Sec_Event_Logs) між різними активами та переходами. Інструменти NDR засновано на штучному інтелекті, який постійно самонавчається та адаптується для автоматичного виявлення еволюціонуючих та складних загроз. У випадку виявлення атаки рішення NDR забезпечують всебічний криміналістичний аналіз хронології атаки, починаючи від ініціювання проникнення та стороннім переміщеннями в мережі, а також автоматично запускають процеси для запобігання майбутнім атакам.

Альтернативний процес обробки журналів подій

Відомий процес нормалізації журналів подій. Процес нормалізації журналів подій відомий та продемонстрований на рисунку 7.

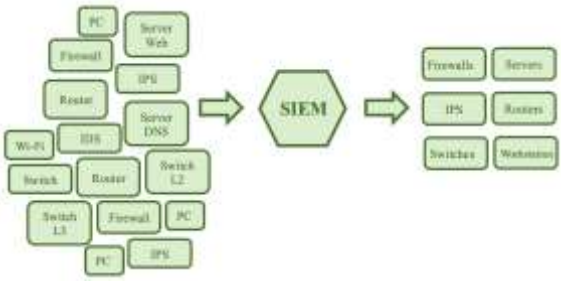

Рисунок 7 – Відомий процес нормалізації журналів подій

Система SIEM має здатність виконувати різноманітні функції: проводити таксономію (класифікацію отриманих даних за типами та категоріями) і здійснювати кореляцію (пов'язувати здавалося б розрізнені події між собою). Крім того, вона може надсилати повідомлення відповідальним особам про виявлені підозрілі події в журналах.

Функціонал SIEM на прикладі компанії середнього розміру (близько 1000 співробітників, їх робочі ПК, інформація та бізнес-системи зберігаються та працюють на серверах):

1. Антивірусні рішення, які призначені для уникнення активності шкідливого коду зловмисного ПЗ на кінцевих точках, у локальному та web-трафіку, а також в електронній пошті.
2. Засоби захисту від експлойтів, які здатні виявляти та запобігати негативному впливу встановленого прикладного чи системного ПЗ.
3. Системи управління та контролю обліковими записами, які реалізують централізоване керування обліковими записами користувачів та адміністраторів IT-систем.
4. Засоби захисту від витоку даних, які спрямовані на запобігання несанкціонованій передачі цінної інформації з порушенням установлених у компанії.
5. Мережеві брандмауери, які регулюють вхідний та вихідний мережевий трафік як в локальній, так і в інтернет-мережі.

6. Системи виявлення та/або запобігання мережевим вторгненням призначені для аналізу мережевого трафіку з метою виявлення ознак атаки на пристрої через мережу за допомогою експлойтів.
7. «Пісочниці» (засоби ізольованого виконання програм) дозволяють запускати сумнівний файл в ізольованому віртуальному середовищі, призначеному для виявлення аномалій.
8. Сканери вразливостей застосовуються для аналізу різних IT-систем, отримуючи дані про використовувані версії ПЗ для застосування відомих вразливостей, що застосовуються до зазначених версій.
9. Системи ресурсів-приманок для зловмисників (honeypots і honeynets) створюються як імітаційні системи інформаційних ресурсів, аналогічні реальним системам компанії, але не містять жодної цінної інформації. Атакуючі, потрапивши в таку пастку, намагаються використовувати свій інструментарій для атаки, і їхні дії ретельно журналюються та аналізуються фахівцями з безпеки інформації.
10. Засоби управління портативними пристроями (MDM – Mobile Device Management) – це програми контролю та захисту портативних пристроїв співробітників (BYOD). Встановивши такий інструмент, співробітник отримує можливість контрольованого та безпечного віддаленого доступу до IT-ресурсів організації, наприклад, підключивши робочу пошту на свій смартфон.

Вдосконалений процес нормалізації журналів подій. Розглянемо, як функціонує система SIEM, яка користь від її впровадження та які завдання вона виконує (рисунок 8).

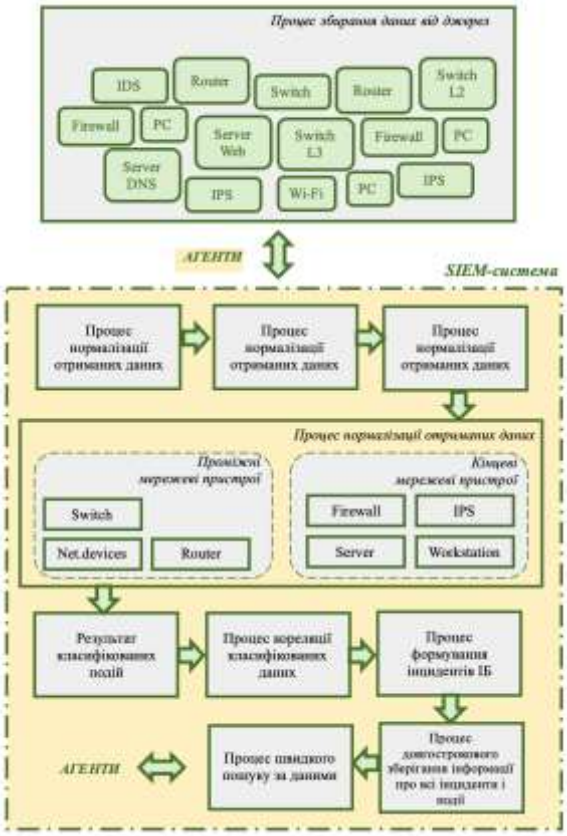

Рисунок 8 – Вдосконалений процес нормалізації журналів подій

Перше завдання SIEM – отримати дані від джерела. Це може бути як «активне» джерело, здатне передавати дані у SIEM, достатньо вказати мережеву адресу приймача (так званий менеджер), або «пасивне», до якого SIEM-система повинна самостійно звертатися (так званий агент). Отримавши дані від джерела, SIEM-система перетворює їх у єдиний, придатний для подальшого використання формат – це процес нормалізації. Далі SIEM-система виконує таксономію, класифікуючи вже нормалізовані повідомлення відповідно до їхнього змісту: яка подія вказує на успішну мережеву комунікацію, яка – на вхід користувача на ПК, а яка – на спрацювання антивіруса. Таким чином, отримуємо не лише набір записів, а послідовність подій (Sec_Event_Logs) із конкретним змістом та часом виникнення. Тепер ми

можемо зрозуміти, як взаємодіяли події та встановити можливий зв'язок між ними. В цьому контексті важливу роль відіграє основний механізм SIEM-системи – кореляція. Кореляція в SIEM – це встановлення взаємозв'язку між подіями, які відповідають конкретним умовам (правилам кореляції).

За результатами застосування правил кореляції у SIEM формується інцидент ІБ. В такому випадку фахівець, що працюєз SIEM, має ефективно знаходити серед попередніх інцидентів та подій, що зберігаються в системі SIEM. Отже, ключові завдання системи SIEM такі: 1. Збір журналів з усіх наявних засобів захисту; 2. Нормалізація отриманих даних; 3. Таксономія нормалізованих даних; 4. Кореляція класифікованих подій (Sec_Event_Logs); 5. Створення інциденту та забезпечення інструментів для проведення розслідування; 6. Збереження інформації про події та інциденти протягом значного періоду (принаймні 6 місяців); 7. Швидкий пошук за даними, які зберігаються в SIEM. Враховуючи ці аспекти, пропонується удосконалити схему відомого процесу нормалізації журналів подій.

Нова концепція схеми відрізняється від існуючих за такими параметрами: 1) вона була ретельно розглянута та уточнена, з докладно визначеними складовими процесу нормалізації журналів подій; 2) в ній визначено роль агентів між джерелом даних та SIEM-системою; 3) тут представлені ключові етапи обробки даних в межах SIEM-системи.

Висновки

Потреба у аналізі та удосконаленні методів та засобів неперервного моніторингу безпеки в комп’ютерних мережах засобами SIEM стала підставою для дослідження.

У даній роботі досягнута поставлена мета, яка дозволяє прискорення процесів реагування на загрози мережевої безпеки завдяки вдосконаленому процесу обробки журналів подій у методі інтеграції SIEM та її агентів в середовище. У підсумку це дозволяє упорядковувати та класифікувати хаотичні неосяжні потоки інформації про події в мережі та перетворити у зручну візуально прийнятну інформацію для оперативного усунення загроз адміністратором системи.

Список літератури

[1] Кібербезпека бізнесу в умовах нестабільності [Електронний ресурс] // PwC Україна. – 2022. – Режим доступу до ресурсу: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html
[2] Про Національний координаційний центр кібербезпеки [Електронний ресурс] // Верховна Рада України. – 2016. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/242/2016#Text
[3] Про CERT-UA [Електронний ресурс] // Державна служба спеціального зв’язку та захисту інформації України. – 2023. – Режим доступу до ресурсу: https://cert.gov.ua
[4] Військова кібербезпека [Електронний ресурс] // Міністерство оборони України. – 2023. – Режим доступу до ресурсу: https://www.mil.gov.ua/ukbs
[5] УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021 [Електронний ресурс] // Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України". – 2021. – Режим доступу до ресурсу: https://www.president.gov.ua/documents/4472021-40013
[6] What is the SOC visibility triad? [Електронний ресурс] // SOC visibility triad Режим доступу до ресурсу: https://www.nomios.be/en/resources/what-is-the-soc-visibility-triad/
[7] Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.
[8] Miller D. Security Information and Event Management (SIEM) - Implementation Guide / David R. Miller. CRC Press, 2020.
[9] Гребенюк А. М. Основи управління інформаційною безпекою [Ел. ресурс] / А. М. Гребенюк, Л. В. Рибальченко. – 2020. – Режим доступу: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf
[10] Pitis Andrei. SIEM: Trends and Best Practices for Operations and Development / Andrei Pitis, Apress: 2020.
[11] Top SIEM Use Cases for Correlation and SIEM Alerts Best Practices [Електронний ресурс] // DNSstuff. – 2020. – Режим доступу до ресурсу: https://www.dnsstuff.com/common-siem-alerts.
[12] Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, 2020 – 242p.
[13] Коробейнікова Т.І. Системний моніторинг мережевої безпеки в тріаді SIEM-EDR-NDR / Коробейнікова Т.І., Федорченко В. В. // International scientific journal «Grail of Science» – 2023. – №

27 (May, 2023). – С. 354–360. ISSN: 2710–3056. ISBN 979-8-88955-792-0.
[14] Коробейнікова Т.І. Системний моніторинг мережевої безпеки в тріаді SIEM-EDR-NDR / Коробейнікова Т.І., Федорченко В. В. // International periodical scientific journal «SWorldJournal» – 2023. – № 19 (part 1) (May, 2023). – С. 33–39. ISSN: 2663-5712. DOI: 10.30888/2663-5712.2023-19-01-029.
[15] Савицька Л.А., Коробейнікова Т.І. Удосконалений метод розробки API підвищеної швидкодії Інформаційні технології та комп`ютерна інженерія 2021: - №1 (50). - С. 31–35
[16] Савицька Л. А. Програмний модуль попереднього діагностування пацієнтів на основі нейронної мережі Кохонена [Текст] / Л. А. Савицька, Н. В. Добровольська, В. О. Кондратюк // Інформаційні технології та комп`ютерна інженерія. – 2023. – № 1. – С. 66-74.

Стаття надійшла: 20.11.2023 р.

References

[1] Kiberbezpeka biznesu v umovakh nestabil′nosti [Elektronnyy resurs] // PwC Ukrayina. – 2022. – Rezhym dostupu do resursu: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html
[2] Pro Natsional′nyy koordynatsiynyy tsentr kiberbezpeky [Elektronnyy resurs] // Verkhovna Rada Ukrayiny. – 2016. – Rezhym dostupu do resursu: https://zakon.rada.gov.ua/laws/show/242/2016#Text
[3] Pro CERT-UA [Elektronnyy resurs] // Derzhavna sluzhba spetsial′noho zv″yazku ta zakhystu informatsiyi Ukrayiny. – 2023. – Rezhym dostupu do resursu: https://cert.gov.ua
[4] Viys′kova kiberbezpeka [Elektronnyy resurs] // Ministerstvo oborony Ukrayiny. – 2023. – Rezhym dostupu do resursu: https://www.mil.gov.ua/ukbs
[5] UKAZ PREZYDENTA UKRAYINY №447/2021 [Elektronnyy resurs] // Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku "Pro Stratehiyu kiberbezpeky Ukrayiny". – 2021. – Rezhym dostupu do resursu: https://www.president.gov.ua/documents/4472021-40013
[6] What is the SOC visibility triad? [Elektronnyy resurs] // SOC visibility triad Rezhym dostupu do resursu: https://www.nomios.be/en/resources/what-is-the-soc-visibility-triad/
[7] Pobudova zakhyshchenykh merezh na bazi obladnannya kompaniyi Cisco. // Zakharchenko S.M., Troyanovs′ka T. I., Boyko O.V. Navchal′nyy posibnyk. Vinnytsya : VNTU, 2017. – 133 s.
[8] Miller D. Security Information and Event Management (SIEM) - Implementation Guide / David R. Miller. CRC Press, 2020.
[9] Hrebenyuk A. M. Osnovy upravlinnya informatsiynoyu bezpekoyu [El. resurs] / A. M. Hrebenyuk, L. V. Rybal′chenko. – 2020. – Rezhym dostupu: https://er.dduvs.in.ua/bitstream/123456789/5717/1/%D0%9F%D0%9E%D0%A1I%D0%91%D0%9D%D0%98%D0%9A%20%D0%9E%D0%A3I%D0%91%20.pdf
[10] Pitis Andrei. SIEM: Trends and Best Practices for Operations and Development / Andrei Pitis, Apress: 2020.
[11] Top SIEM Use Cases for Correlation and SIEM Alerts Best Practices [Elektronnyy resurs] // DNSstuff. – 2020. – Rezhym dostupu do resursu: https://www.dnsstuff.com/common-siem-alerts.
[12] Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats, 2020 – 242p.
[13] Korobeynikova T.I. Systemnyy monitorynh merezhevoyi bezpeky v triadi SIEM-EDR-NDR / Korobeynikova T.I., Fedorchenko V. V. // International scientific journal «Grail of Science» – 2023. – № 27 (May, 2023). – S. 354–360. ISSN: 2710–3056. ISBN 979-8-88955-792-0.
[14] Korobeynikova T.I. Cystemnyy monitorynh merezhevoyi bezpeky v triadi SIEM-EDR-NDR / Korobeynikova T.I., Fedorchenko V. V. // International periodical scientific journal «SWorldJournal» – 2023. – № 19 (part 1) (May, 2023). – S. 33–39. ISSN: 2663-5712. DOI: 10.30888/2663-5712.2023-19-01-029.
[15] Savyts′ka L.A., Korobeynikova T.I. Udoskonalenyy metod rozrobky ARI pidvyshchenoyi shvydkodiyi Informatsiyni tekhnolohiyi ta komp`yuterna inzheneriya 2021: - №1 (50). - S. 31–35
[16] Savyts′ka L. A. Prohramnyy modul′ poperedn′oho diahnostuvannya patsiyentiv na osnovi neyronnoyi merezhi Kokhonena [Tekst] / L. A. Savyts′ka, N. V. Dobrovol′s′ka, V. O. Kondratyuk // Informatsiyni tekhnolohiyi ta komp`yuterna inzheneriya. – 2023. – № 1. – S. 66-74.

Відомості про авторів

Савицька Людмила Анатоліївна – к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Savytska Liudmyla, PhD – associate professor of computing engineering department, Vinnytsya national technical university

Коробейнікова Тетяна Іванівна – к.т.н., доцент кафедри безпеки інформаційних технологій, Національний університет «Львівська політехніка», кафедра безпеки інформаційних технологій

Korobeinikova Tetiana – PhD, associate professor of information technology security department, National university “Lvivska Politechnika”

Волос Олександр Павлович – магістр кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Volos Oleksandr Pavlovych – magister of computing engineering department, Vinnytsya national technical university, department of the computer engineering

Тарновський Микола Геннадійович – к. т. н., доцент кафедри обчислювальної техніки, ВНТУ, кафедра обчислювальної техніки

Tarnovskyi Mykola, PhD, associate professor of computing engineering department, Vinnytsya national technical university

L. Savytska[1], T. Korobeinikova[2], O. Volos[1], M. Tarnovskyi[1]

METHOD AND MEANS OF SECURITY MONITORING IN A COMPUTER NETWORK BY SIEM MEANS

[1]Vinnytsya national technical university, Vinnytsya

[2]National university “Lvivska Politechnika”