Моніторинг процесів функціонування інформаційно-комунікаційних систем

УДК 004.73:658.5

[1]*Валентина Ящук*

[1]Львівський державний університет безпеки життєдіяльності,[1]valentina.lender@gmail.com

Повномасштабне вторгнення росії в Україну спричинило значне зростання кібератак. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кіберінцидентів у 2022 році збільшилась на 38% порівняно з 2021 роком. Найпоширенішими типами кібератак сьогодні є DDoS-атаки (розподілені атаки відмови в обслуговуванні), фішингові атаки, атаки на вебсайти, шкідливе програмне забезпечення. Ручне реагування на кіберінциденти стає все більш складним і трудомістким, тому виникає необхідність автоматизації цих процесів за допомогою, наприклад, SIEM-систем.

Сучасні організації використовують складні інформаційні системи та мережі, які включають в себе різноманітні пристрої, додатки та протоколи. Управління інформаційною безпекою є складним і трудомістким завданням, яке вимагає постійного моніторингу та аналізу великої кількості даних. SIEM системи дозволяють автоматизувати багато завдань безпеки, що звільняє персонал для виконання інших важливих завдань. Зважаючи на це актуальність використання SIEM систем в менеджменті інформаційної безпеки є незаперечною.

Питаннями, які торкаються найрізноманітніших аспектів менеджменту інформаційної безпеки, займались багато дослідників сучасності, зокрема: Гончар В. І., Сіренко В. В., Зайцев О. В., Шрамко О. В. тощо. Разом з тим,. продовжує залишатись актуальною необхідність у подальших дослідженнях низки питань щодо моніторингу процесів функціонування інформаційно-комунікаційних систем. Проблеми, перераховані вище, їхня актуальність обумовили вибір теми, визначили мету й завдання.

Метою є визначення методичних підходів до автоматизація процесів менеджменту інформаційної безпеки з використання SIEM-систем, що є основою оптимізації. SIEM-система – це система управління інформаційною безпекою та розслідуванням інцидентів (Security Information and Event Management). Вона призначена для збору, консолідації, зберігання, аналізу та візуалізації даних безпеки з різних джерел, таких як мережеві пристрої, сервери, робочі станції, програмне забезпечення безпеки тощо. SIEM-системи використовуються для виявлення, реагування та розслідування інцидентів безпеки, а також для забезпечення відповідності вимогам безпеки.

Роботу SIEM-системи можна розділити на чотири основних етапи: збір даних; консолідація та зберігання даних; аналіз даних; розробка звітів та сповіщень. Окрім цих основних етапів, SIEM-система може виконувати також інші функції, такі як: менеджмент відповідей на інциденти – допомога в реагуванні на виявлені інциденти; аналіз поведінки користувачів – виявлення аномалій у поведінці користувачів; відстеження відповідності вимогам – забезпечення відповідності вимогам безпеки.

SIEM-системи збирають дані з різних джерел, таких як: мережеві пристрої, такі як брандмауери, маршрутизатори, комутатори тощо; сервери, такі як веб-сервери, файлові сервери, бази даних тощо; робочі станції, такі як комп'ютери, ноутбуки, планшети тощо; програмне забезпечення безпеки, таке як антивірусні програми, системи виявлення вторгнень (IDS), системи управління вразливостями тощо. SIEM-системи можуть збирати дані в різних форматах, таких як текстові файли, XML, JSON, CSV тощо. SIEM-система повинна мати можливість обробляти та перетворювати дані в єдиний формат для подальшого аналізу.

SIEM-системи можуть збирати дані кількома способами, такими як: пряме підключення – SIEM-система може підключатися безпосередньо до джерела даних і отримувати дані в реальному час; сервер повідомлень – SIEM-система може отримувати дані з сервера повідомлень, який збирає дані з різних джерел; автоматичне завантаження – SIEM-система може автоматично завантажувати дані з локальних або віддалених файлів; вибір методу збору даних залежить від конкретного джерела даних і потреб організації.

Основними функціями SIEM-систем є збір даних, обробка даних, фільтрація, кореляція, аналіз, виявлення аномалій, виявлення вторгнень, виявлення загроз, генегація рішень, повідомлення про загрози, автоматичне реагування. Сьогодні на світовому ринку представлено широкий спектр SIEM-систем, які пропонують різні функції та можливості. Наведемо деякі з найпопулярніших сучасних SIEM-систем: IBM QRadar: Комплексна SIEM-система, яка пропонує широкий спектр функцій, включаючи виявлення вторгнень, аналіз загроз, управління інцидентами та реагування на них; Splunk Enterprise Security: SIEM-система, яка спеціалізується на аналізі великих обсягів даних; Microsoft Sentinel: SIEM-система, яка інтегрована з іншими продуктами Microsoft, такими як Azure Monitor та Azure Security Center; Siemplify: SIEM-система, яка пропонує простий і зручний інтерфейс; LogRhythm: SIEM-система, яка пропонує широкий спектр функцій та можливостей для великих організацій.

Серед переваг використання SIEM-систем можна виділити підвищення ефективності менеджменту інформаційної безпеки; зменшення часу на реагування на кіберінциденти; підвищення рівня захисту інформації; зниження ризиків кібератак.

При виборі SIEM-системи слід враховувати такі фактори, як: розмір організації, типи даних, які потрібно збирати, функції та можливості, які потрібні. SIEM системи є ефективним інструментом для підвищення рівня інформаційної безпеки організації. Вони допомагають організаціям виявити потенційні загрози на ранніх стадіях, забезпечити відповідність вимогам безпеки, зменшити час реагування на інциденти безпеки та покращити ефективність управління інформаційною безпекою.

1. Miller D. Security Information and Event Management (SIEM) - Implementation Guide / David R. Miller. CRC Press, 2020.
2. Pitis Andrei. SIEM: Trends and Best Practices for Operations and Development / Andrei Pitis, Apress: 2020.