УДК 004

С.Главнов, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОЇ SIEM ДЛЯ АНАЛІЗУ ЗАГРОЗ БЕЗПЕЦІ КОРПОРАТИВНОЇ ІТ-ІНФРАСТРУКТУРИ

У статті розроблено програмне забезпечення, яке призначено для системи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. Метою розробки є дослідження та принципи побудови системи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. Об’єктом дослідження є процес мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. Предметом дослідження є методи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

SIEM, аналізу загроз безпеці, корпоративна ІТ-інфраструктура

Постановка проблеми. Мережі вашої організації є основною інфраструктурою для ваших інформаційно-технологічних (ІТ) систем, операційних технологій (ОТ) та промислових систем управління (ІКС). Тому важливо забезпечити безпеку вашої мережевої інфраструктури, щоб захистити вашу організацію від порушень, вторгнень та інших кіберзагроз. Мережеве ведення журналу та моніторинг подій безпеки допоможуть вам:

- захистіть свою мережеву інфраструктуру;
- визначити індикатори компрометації (IoCs);
- своєчасно вживати коригувальних заходів;
- мінімізувати вплив у разі виникнення інциденту безпеки.

Рішення SIEM об'єднує функції моніторингу та ведення журналу. Термін SIEM вперше був введений Gartner у 2005 році для опису комбінації наступних підходів:

- управління інформацією безпеки (SIM), що стосується діяльності, пов'язаної зі збором даних, таких як файли журналів, з кількох джерел у централізоване сховище;
- управління подіями безпеки (SEM), що стосується діяльності, пов'язаної з моніторингом та аналізом конкретних подій безпеки в режимі реального часу, які можуть бути тривожними сигналами.

Традиційно, SIEM-рішення здебільшого пропонували захист для локальних середовищ з обмеженими джерелами даних та можливостями. SIEM-рішення еволюціонували, і SIEM наступного покоління пропонують більше можливостей для боротьби з передовими кіберзагрозами та обробки величезних обсягів даних. Зараз доступно багато хмарних SIEM-рішень, які можуть захищати активи як локально, так і в хмарі.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевої siem для аналізу загроз безпеці корпоративної іт-інфраструктури.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи мережевої SIEM для аналізу загроз безпеці корпоративної ІТ-інфраструктури.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

– Дослідження системи мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

– Програмна реалізація системи мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

Об'єктом дослідження є процес мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

Предметом дослідження є методи мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

Методи дослідження базуються на методах захисту інформації у мережі, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Рішення SIEM наступного покоління включають такі технології для виявлення складних загроз та горизонтального переміщення, а також для автоматизації реагування на інциденти:

Аналіз поведінки користувачів та об'єктів

Аналітика поведінки користувачів та об'єктів (UEBA) використовує алгоритми та машинне навчання для виявлення аномальних моделей поведінки користувачів та пристроїв (наприклад, маршрутизаторів, серверів та кінцевих точок) у мережі. UEBA дозволяє вашій організації виявляти ширший спектр кіберзагроз, таких як атаки методом перебору, розподілені атаки відмови в обслуговуванні (DDoS).) та внутрішні загрози.

Оркестрація безпеки та автоматизоване реагування

Оркестрація безпеки та автоматизація реагування (SOAR) допомагають координувати та автоматизувати реагування на виявлені загрози за допомогою автоматизованих сценаріїв або робочих процесів. Вони також використовують штучний інтелект.(Штучний інтелект) вивчає моделі поведінки, щоб передбачати подібні загрози до їх виникнення.

Переваги SIEM-рішень

Рішення SIEM може допомогти керувати ризиками кібербезпеки вашої організації, підтримуючи виявлення загроз, дотримання вимог та управління інцидентами безпеки. Рішення SIEM дозволяють вашій команді безпеки:

– керувати безперервним надходженням даних журналів з багатьох різних джерел:

o допомагає зменшити вартість окремих інструментів, що використовуються різними групами у вашій організації;

o централізує дані журналів в одному сховищі;

– співвідносити та аналізувати великі обсяги даних, щоб мати змогу проактивно виявляти потенційні загрози, оскільки вони залишають сліди в різних джерелах журналів;

– автоматизувати завдання безпеки, щоб зменшити навантаження аналітиків безпеки шляхом автоматизації повторюваних завдань;

– отримувати автоматичні сповіщення та відповідні дії за допомогою автоматичного тригера на основі конкретних випадків використання для забезпечення швидкого реагування на інциденти;

– отримуйте дані в режимі реального часу по всій організації, щоб допомогти вашій організації швидко виявляти та усувати сліпі зони вразливостей у вашій мережі;

– пошук історичних даних журналів для різних мережевих вузлів та періодів часу для підтримки аналізу першопричин та виявлення інцидентів після того, як стався витік;

– генерувати звіти для аудиторів, щоб продемонструвати дотримання нормативних вимог та виявляти потенційні порушення на ранній стадії, щоб їх можна було усунути;

– переглядати інформаційні панелі управління, які відображають дані про події в інформаційних діаграмах, щоб побачити закономірності незвичайної діяльності:

o допомагає вашій організації визначити пріоритети ресурсів для першочергового вирішення найважливіших загроз.

Рішення SIEM дозволяють вашій організації автоматизувати впровадження, оцінку та постійний моніторинг засобів контролю безпеки. Згідно зі спеціальною публікацією (SP) 800-137 Національного інституту технологічних стандартів (NIST), технології SIEM можуть допомогти організаціям автоматизувати багато специфічних засобів контролю безпеки. Ці технічні, операційні та управлінські засоби контролю безпеки описані в документі Кіберцентру «Управління ризиками безпеки IT : підхід життєвого циклу» (ITSG-33).

– Технічні засоби контролю безпеки:
o AC-5 Розподіл обов'язків;
o AU-2 Події, що підлягають аудиту;
o AU-6 Аудиторський огляд, аналіз та звітність;
o Скорочення аудиту AU-7 та створення звітів.
– Контроль операційної безпеки:
o Моніторинг інцидентів IR-5;
o PE-6 Моніторинг фізичного доступу;
o Моніторинг інформаційної системи SI-4.
– Контроль безпеки управління:
o Оцінювання безпеки CA-2;
o Безперервний моніторинг CA-7;
o Оцінка ризиків RA-3;
o Сканування вразливостей RA-5.

Хмарні SIEM-рішення

У сфері кібербезпеки перехід до хмарних SIEM-рішень змінює те, як організації керують своїми даними та взаємодіють з ними. У звіті Gartner за 2023 рік було оцінено, що до кінця року 90% SIEM-рішень пропонуватимуть можливості виключно в хмарі. На відміну від традиційних локальних SIEM-рішень, які вимагають спеціалізованого апаратного та програмного забезпечення у власній інфраструктурі організації, хмарне SIEM-рішення розміщується на серверах, що обслуговуються стороннім постачальником хмарних послуг (CSP).

Хмарні SIEM-рішення дозволяють вашій організації перекласти більшу частину управління інфраструктурою на постачальника послуг зв'язку (CSP) та зосередитися на використанні вашої системи для досягнення ваших цілей безпеки. На практиці це означає, що журнали даних з мережевих пристроїв та систем вашої організації збираються, передаються в хмару та безпечно зберігаються на серверах CSP.

Після цього ваша організація може взаємодіяти з вашими даними через веб-інтерфейсабо інтерфейс прикладного програмування (API), що надається постачальником послуг криптографії (CSP). Цей API зазвичай містить набір інструментів для аналізу даних, візуалізації та звітності. Це дозволяє вашій організації виконувати складну аналітику для виявлення, розслідування та реагування на інциденти безпеки.

Хмарні SIEM-рішення часто оснащені можливостями машинного навчання та штучного інтелекту для кращого виявлення аномалій та потенційних загроз. Це відбувається в режимі реального часу та у великих масштабах, надаючи організаціям потужний, гнучкий та ефективний інструмент для управління своєю кібербезпекою.

Типи хмарних пропозицій

Існує два типи пропозицій для хмарних SIEM-рішень: керовані та некеровані.

Керований

Це ближче до моделі «SIEM як послуга», де постачальник SIEM-рішення відповідає за хмарну інфраструктуру та її обслуговування. Постачальник SIEM-рішення також надає клієнту послуги моніторингу інцидентів у режимі реального часу та виявлення загроз. Клієнт зазвичай має менше контролю над управлінням життєвим циклом SIEM-рішення, оскільки це

є відповідальністю постачальника. Хоча керовані рішення можуть бути дорожчими, вони знімають з клієнта тягар впровадження та обслуговування SIEM-рішення.

Некерований

Клієнт відповідає за створення, підтримку, усунення несправностей та управління життєвим циклом усіх компонентів SIEM-рішення. Третя сторона може надавати додаткову допомогу, але загалом клієнт несе відповідальність за доступність SIEM-рішення.та стабільність. Некеровані рішення можуть бути підходящим варіантом для організацій з високочутливими активами, яким потрібен повний контроль над своїм SIEM-рішенням.

Переваги хмарних SIEM-рішень

Хмарні SIEM-рішення можуть забезпечити вашій організації кілька переваг.

Масштабованість та гнучкість

У міру зростання вашої організації або коливань попиту, хмарні рішення можуть адаптуватися до ваших потреб. Така масштабованість також означає, що ви платите лише за те, що використовуєте, що може бути економічно вигідним вибором для багатьох компаній.

Зменшення операційних накладних витрат

Завдяки локальному рішенню SIEM ваша організація відповідає за обслуговування апаратного та програмного забезпечення, що може бути ресурсомістким. Хмарні рішення SIEM перекладають значну частину цієї відповідальності на постачальника послуг зв'язку (CSP). Це дозволяє вашій команді безпеки зосередитися на стратегічних завданнях, а не на обслуговуванні.

Аналітика

Хмарні SIEM-рішення часто включають комерційну готову аналітику (COTS), специфічну для CSP. Ця аналітика розроблена для оптимальної роботи в інфраструктурі постачальника послуг, потенційно пропонуючи покращені можливості виявлення загроз та аналізу даних. Наявність цієї аналітики може покращити можливості вашої організації щодо кіберзахисту, використовуючи спеціалізовані знання та ресурси постачальника.

Недоліки хмарних SIEM-рішень

Хоча хмарні SIEM-рішення можуть запропонувати багато переваг вашій організації, вам слід знати про потенційні недоліки.

Проблеми конфіденційності даних

Коли ви використовуєте хмарне SIEM-рішення, ваші дані зберігаються на серверах постачальника послуг зв'язку (CSP). Перш ніж переходити на хмарне рішення, переконайтеся, що ви повністю розумієте та знайомі з методами обробки та зберігання даних вашого постачальника.

Зафіксованість постачальника

Перехід на хмарне SIEM-рішення може призвести до прив’язки до постачальника, тобто до ситуації, коли важко або дорого перейти до іншого постачальника або повернутися до локального рішення. Багато хмарних сервісів є власністю CSP, що може ускладнити перенесення даних. Перш ніж вибрати хмарне SIEM-рішення, переконайтеся, що ви розумієте умови надання послуг, зокрема, що передбачає зміна постачальників.

Вартість

Хмарні SIEM-рішення можуть забезпечити економію коштів, особливо з точки зору обслуговування та інфраструктури, але вони також можуть збільшити витрати. Це особливо актуально, якщо ваша організація використовує багато даних, оскільки багато CSP стягують плату залежно від обсягу оброблених даних.

Безпечне розгортання та експлуатація SIEM-рішень є життєво важливими. SIEM-рішення слід розглядати як систему вищої цінності, таку як адміністративний контроль або контроль доступу системи. Через свою роль у моніторингу та виявленні інцидентів безпеки, слід приділяти особливу увагу забезпеченню безпеки як продукту, так і постачальника. У разі виникнення вразливості нульового дня, а також через чутливість даних та рівень доступу до рішення SIEM, Кіберцентр вважає за потрібне розробляти архітектуру SIEM на основі рішень кількох постачальників, а не бути прив’язаним до одного. Такий підхід покращує

загальний рівень безпеки, зменшуючи ризики, пов’язані з вразливостями, характерними для певних постачальників.

Неправильно впроваджене SIEM-рішення може призвести до більшої кількості хибнопозитивних результатів, виявлення більшої кількості «аномальних» подій та генерування додаткових, некорисних сповіщень. Це може створювати навантаження на ресурси вашої команди кібербезпеки. Впроваджуючи наведені нижче найкращі практики, ваша організація може отримати максимальну користь від вашого SIEM-рішення.

Загальні рекомендації

– Визначення варіантів використання для моніторингу, оповіщення та аудиту:

o З цих випадків використання визначте джерела журналів, які потрібно отримати та проаналізувати.

– Розгляньте можливість проведення перевірки концепції (POC), щоб оцінити, чи підходить SIEM-рішення для вашого середовища:

o Налаштуйте POC у тестовому середовищі, яке базується на чітко визначених сценаріях користувачів і є репрезентативною підмножиною вашої інфраструктури та даних.

– Визначте свої найважливіші ресурси, такі як дані та пристрої, і налаштуйте SIEM-рішення для їх моніторингу.

– Налаштуйте відповідний моніторинг джерел журналів та сповіщення, щоб отримувати сповіщення про проблеми зі збиранням журналів.

– Оцініть, скільки даних ви хочете зібрати, щоб отримати повне уявлення про вашу мережу.

– Як мінімум, вам слід збирати дані журналу про:

o транзакції авторизації (успішні та невдалі спроби);

o зміни привілеїв користувачів, включаючи зміни облікових записів користувачів (зокрема створення та видалення), зміни членства в групах та механізмів автентифікації (паролі та багатофакторна конфігурація), а також додавання або видалення привілейованого доступу;

o помилки програми;

o процеси згоди, такі як умови та положення;

o дії, що виконуються всіма користувачами з правами адміністратора;

o реєстрація нових пристроїв в інфраструктурі, включаючи будь-які мобільні телефони та персональні пристрої, що дозволяють використовувати власні пристрої.

– Запобігайте збору конфіденційних даних вашим SIEM-рішенням, таких як:

o фінансова інформація (наприклад, банківські записи або дані кредитної картки);

o персональну інформацію (наприклад, ідентифікаційний номер, виданий урядом);

o паролі та ключі шифрування;

– Зрозумійте вимоги до дотримання вимог вашого бізнесу та налаштуйте SIEM-рішення відповідно до них.

– Регулярно перевіряйте та тестуйте своє SIEM-рішення, щоб переконатися, що воно правильно налаштоване на основі впроваджених заходів безпеки та політик.

– Розробіть план реагування на інциденти, щоб ваша організація була готова належним чином впоратися з подією, коли трапляється інцидент безпеки:

o Для отримання додаткової інформації зверніться до нашої публікації «Розробка плану реагування на інциденти» (ITSAP.40.003).

– Синхронізуйте всі мережеві пристрої з центральним сервером часу, щоб гарантувати, що записані журнали аудиту використовують одне й те саме джерело часу;

o Налаштуйте щонайменше 3 сервери часу для полегшення обслуговування та усунення несправностей.

– Підпишіться на зовнішні канали загроз і створюйте сповіщення на основі даних, що надсилаються, регулярно оновлюйте логіку виявлення для виявлення нових загроз:

o Кіберцентр надає IoC організаціям, включаючи партнерів у канадській критичній інфраструктурі, через автоматизовану систему під назвою AVENTAIL, яку можна інтегрувати безпосередньо у вашу SIEM.

Дані журналу якості

Щоб ваша організація отримувала найкориснішу інформацію про діяльність у вашій мережі, переконайтеся, що високоякісні дані журналів надходять до вашого інструменту SIEM.

Виберіть відповідні методи збору журналів

Рішення SIEM можуть збирати та зберігати журнали безпеки з різних джерел. Визначте, який метод збору журналів підходить для потреб вашої організації.

– Потік журналів: Пристрої генерують журнали та надсилають їх безперервним потоком до колектора журналів рішення SIEM. Це забезпечує рішення SIEM інформацією в режимі реального часу.

– Надсилання журналів: Пристрій автоматично збирає журнали та надсилає (завантажує) їх безперервно або через регулярні проміжки часу до колектора журналів рішення SIEM. Колектор журналів налаштовано на прийом журналів у певному форматі та за певним протоколом (syslog, FTP тощо).

– Збір журналів: Як і при надсиланні журналів, цей метод використовує збирач журналів рішення SIEM для ініціювання підключення та запиту журналів. Цей метод часто використовується для збору журналів на рівні операційної системи за допомогою програмного агента.

Перегляд та оновлення аналізаторів журналів

Різні системи генерують журнали в різних форматах. Деякі формати журналів мають чітко визначену структуру та їх легко використовувати в SIEM-рішеннях, тоді як інші формати журналів менш узгоджені та складніші для аналізу та обробки в SIEM-рішеннях. Переконайтеся, що вибране вами SIEM-рішення може зрозуміти отримані журнали.

Формати журналів також можуть змінюватися з часом (наприклад, після оновлень програмного забезпечення), що може призвести до того, що SIEM не зможе аналізувати та індексувати журнали з певного джерела. Регулярно переглядайте аналізатори журналів та оновлюйте їх за потреби.

Правильне керування сховищем журналів

Дані журналів, отримані рішенням SIEM, зберігаються відповідно до налаштованих політик зберігання. Журнали можна надсилати до сховища для архівування або до механізму кореляції рішення SIEM, де вони будуть проаналізовані та зіставлені з іншими журналами. Така кореляція може надати важливу інформацію вашій IT- команді.

Залежно від обраного вами рішення SIEM, журнали можуть зберігатися або в отриманому вигляді, або у стиснутому форматі. Оскільки пошук стиснутих журналів займає більше часу, деякі рішення SIEM зберігають останні журнали в нестиснутому форматі. Після певного часу журнали стискаються, щоб зменшити використання пам’яті.

SIEM-рішення можуть отримувати тисячі журналів щосекунди, тому зберігання нестиснених журналів протягом тривалого періоду може призвести до високих витрат на зберігання. Якщо SIEM-рішення зберігає журнали в хмарі, витрати на зберігання також можуть значно зрости.

Видалення журналів після того, як вони більше не мають цінності, допоможе зменшити витрати на зберігання та продуктивність. Журнали, обсяг яких перевищує політику зберігання, можна відкинути або зберігати в дешевших рішеннях.

Зберігання даних журналу

Політики зберігання журналів можуть допомогти контролювати потреби в сховищі. Розробляючи політику зберігання журналів вашої організації, ретельно обміркуйте, як довго слід зберігати журнали безпеки. Як загальне правило, ми рекомендуємо зберігати важливі журнали вашої організації щонайменше 6 місяців. Для більш критичних журналів розгляньте період зберігання 13 місяців.

Термін зберігання залежатиме від вашого:

– галузеві стандарти організації;
– нормативні акти та закони;
– конкретні проблеми кібербезпеки, унікальні для вашого бізнес-середовища;
– витрати на зберігання та доступність;

Багато компрометацій виявляються через довгий час після того, як стався витік. Згідно з публікацією IBM «Вартість звіту про витік даних за 2023 рік», середній час виявлення витоку становив 204 дні. Якщо у вашій організації стався витік, ваші журнали є важливим доказом, який допоможе вам виявити та розслідувати інцидент. Ретельно розробляйте політику зберігання журналів та періодично переглядайте її, щоб перевірити, чи потрібні коригування та чи зберігаються ваші журнали протягом належного часу.

Активація індексації найчастіше шуканих полів

Журнали з різних типів джерел містять різну інформацію та використовують різні формати. Рішення SIEM використовують аналізатори журналів для розуміння форматів журналів та інформації, яку вони містять. Це може включати сам журнал, інформацію про дату та час, а також розташування імені користувача або імені машини в потоці журналів. Ці поля можна індексувати, що призведе до швидшого пошуку.

Індексування журналів пришвидшує пошук, але вимагає додаткових ресурсів сховища та центрального процесора (CPU), що може вплинути на продуктивність рішення SIEM. Ми рекомендуємо індексувати лише ті поля, які часто шукаються.

Рішення SIEM повинно надавати інформацію про пошукові запити, зокрема, які поля шукаються та чи індексуються ці поля. Використовуючи цю інформацію, адміністратор SIEM може активувати або деактивувати індексацію залежно від того, як часто виконується пошук у полях.

Нормалізувати дані журналу

Нормалізація журналів важлива для кореляції подій та розслідування інцидентів. Рішення SIEM може отримувати журнали в різних форматах. Наприклад, ваша мережа може мати пристрої в різних часових поясах, деякі журнали можуть використовувати 12-годинний формат, а інші – 24-годинний, або журнали Active Directory (AD) можуть містити імена користувачів, тоді як хмарні журнали відображають адресу електронної пошти користувача як його ім'я користувача.

Рішення SIEM повинно мати можливість нормалізувати якомога більше полів, щоб обмежити кількість рядків пошуку, що вказують на одного й того ж користувача або ресурс. Під час розслідування інцидентів пошук подій, що відбулися протягом певного періоду, повинен повертати журнали з усіх пристроїв, незалежно від часового поясу, на який налаштовано рішення SIEM.

Налаштування правил кореляції та порогових значень

Кореляція подій стосується аналізу подій у бізнес-контекстах та встановлення зв'язків між ними на основі набору попередньо визначених правил. Ці правила дозволяють вашому SIEM-рішенню визначати, які підозрілі дії слід розглядати як потенційні загрози безпеці. Для точного виявлення інцидентів механізм кореляції SIEM-рішення має бути налаштований належним чином. Налаштуйте правила кореляції та встановіть порогові значення на основі конкретних випадків використання або бізнес-потреб вашої організації. Ви можете почати зі стандартних правил конфігурації SIEM-рішення та деактивувати й активувати параметри відповідно до того, що ви хочете корелювати.

Архітектура нульової довіри

Термін «нульова довіра» (ZT) являє собою систему безпеки для захисту інфраструктури та даних. Центральний принцип ZT полягає в тому, що жоден суб'єкт (додаток, користувач чи пристрій) в інформаційній системі не є довіреним за замовчуванням. Довіра має оцінюватися та перевірятися щоразу, коли суб'єкт запитує доступ до нового ресурсу. Ступінь наданого доступу динамічно коригується залежно від рівня довіри, встановленого з суб'єктом. ZT передбачає прийняття нового підходу до безпеки, завжди

припускаючи порушення та зосереджуючись на захисті ресурсів (наприклад, послуг та даних). Архітектура нульової довіри (ZTA) – це корпоративний підхід до проектування систем, у яких безпека базується на принципах ZT. У стандарті NIST SP 1800-35B «Впровадження архітектури нульової довіри» описано приклади рішень для впровадження ZTA. Ці рішення припускають, що технологія SIEM є однією з базових функцій кібербезпеки організації, можливості якої поступово додаються в міру розвитку ZTA. Рішення SIEM підтримують впровадження ZTA, оскільки зібрані ними дані можуть бути використані в механізмі політик ZTA для прийняття рішень щодо динамічного доступу.

Великі організації та підприємства стикаються з постійно мінливим ландшафтом кіберзагроз. Щоб пом'якшити атаки з боку передових зловмисників, ваша організація повинна інвестувати в інструменти безпеки, які надають аналітику активності у вашій мережі в режимі реального часу. Інструменти кібербезпеки, такі як рішення SIEM, можуть забезпечити вам єдиний інтерфейс для отримання цієї аналітики. Рішення SIEM може допомогти вашій організації виявляти, аналізувати та реагувати на кіберзагрози, перш ніж вони порушать вашу бізнес-операцію. Як і у випадку з будь-яким важливим IT- рішенням, вам слід зважити всю інформацію, представлену в цій публікації, з урахуванням конкретних потреб та обставин вашої організації, щоб визначити, чи є рішення SIEM найкращим для вас.

Інтеграція сканера уразливостей з SIEM дозволяє сполучити кілька методів виявлення погроз і значно підвищити ймовірність своєчасного виявлення. Приміром, SIEM може виявити аномалію через baseline, але без інформації про те, що на активі є уразливість, SIEM не зможе сказати, із чим саме ця аномалія зв'язана. При наявності відомостей від сканера уразливості, SIEM зможе зробити вивід про те, що виробляється експлуатація уразливості. Маючи інформацію про уразливість, а також про критичність активів від сканера уразливостей, система SIEM здатна пріоритизувати інциденти по їхній критичності. Це дозволить у першу чергу реагувати на значимі інциденти, важливі для бізнесу

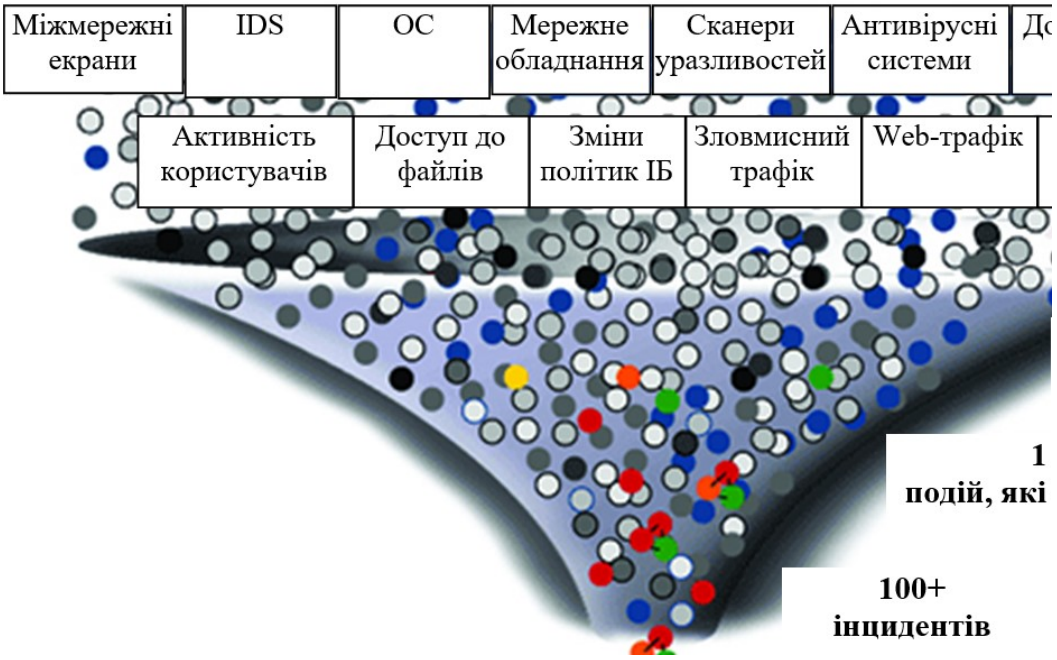

Рисунок 1 – Структурна схема системи

Сканер уразливостей є відмінним постачальником інвентаризаційної інформації для SIEM, наприклад, про версії програмного забезпечення і його конфігурацій. Ця інформація може використовуватися при виявленні інциденту, при з'ясуванні причин його виникнення. Використання убудованого в SIEM механізму перевірки відповідності внутрішнім політикам і високорівневим стандартам без інтеграції зі сканером уразливостей не дає повноцінної картини, тому що використовується дуже мала частка технічних вимог.

Жоден джерело не надасть більше детальної й повної інформації про наявність уразливості й про можливість її експлуатації (з урахуванням топологічної структури мережі й конфігурацій) краще, ніж сканер уразливостей. Уразливість може бути присутнім, але бути при цьому неексплуатований (закритий мережний порт, зупинена служба, на активному мережному встаткуванні організована VLAN або правилами міжмережного екрана заблокований трафік на даний порт). Інформація про це може істотно знизити залишкові ризики, допоможе витрачати кошти на дійсно необхідні засоби захисту, а також виключити помилкові інциденти.

Процес керування конфігураціями, що так складно реалізувати, стає простим при використанні зв'язування SIEM і сканера уразливостей. Ви можете аналізувати, що змінилося, ким і коли були зроблені зміни, а також можете автоматично оцінити, на що вони вплинули. Для цього необхідно лише скласти найпростіші правила кореляції в SIEM і налаштувати параметри переданої інформації від сканера; всю іншу логіку здійснить сама система SIEM. Природно, що чим більше ефективних джерел інформації в SIEM, тим більше ймовірність виявлення погрози на ранній стадії її виникнення. Ви можете використовувати SIEM або сканер уразливостей окремо. Але описане зв'язування значно мінімізує ризики.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

– Досліджена система мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури. Розроблені алгоритми дозволяють успішно вирішувати завдання мережевої SIEM для аналізу загроз безпеці корпоративної IT-інфраструктури. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». II Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
2. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
3. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція “Інформаційна безпека та комп’ютерні технології” до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
4. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп’ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв’язку, 2023, вип. 2(72), С. 170-178.
5. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
6. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
7. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
8. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до

диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
9. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
10. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
11. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
12. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
13. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.
14. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
15. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
16. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
17. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
18. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
19. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
20. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84.
21. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
22. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171.
23. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
24. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
25. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
26. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
27. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
28. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
29. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
30. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019.