Розділ 14. Моніторинг процесів функціонування інформаційно-комунікаційних систем (ІКС)

14.1. Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу.

14.2. Система візуалізації та управління подіями (SIEM).

14.3. Аналіз подій

14.1. Джерела інформації про події та типи подій, що аналізуються в системах моніторінгу

До джерел інформації про події та типи подій, що аналізуються в системах моніторингу відносяться наступні:

– Журнали подій серверів та робочих станцій. Застосовуються для контролю доступу, забезпечення безперервності, дотримання політик інформаційної безпеки. Записуються тонкими і товстими клієнтами.

– Антивірусні програми. Генерують події про працездатність ПЗ, бази даних, зміну конфігурацій і політик, шкідливий код. Повідомляють про знаходження шкідливого програмного забезпечення або коду.

– Засоби антиексплойт захисту дозволяють виявляти та запобігати шкідливому впливу експлойтів, тобто. програм або набору команд, які використовують вразливість встановленого прикладного чи системного програмного забезпечення.

– «Пісочниці», або, по-науковому, засоби ізольованого виконання програм дозволяють запускати підозрілий файл в ізольованому віртуальному середовищі, яке спеціально призначене для пошуку аномалій або потенційно шкідливої поведінки досліджуваного файлу.

– DLP системи. Системи запобігання витоку (англ. Data Leak Prevention, DLP) – технології запобігання витоку конфіденційної інформації з інформаційної системи зовні, а також технічні пристрої (програмні або програмно-апаратні) для запобігання витоку. DLP-системи будуються на аналізі потоків даних, що перетинають периметр інформаційної системи, що захищається. При детектуванні в цьому потоці конфіденційної інформації спрацьовує активний компонент системи, і передача повідомлення (пакету, потоку, сесії) блокується. Відомості про спроби інсайдерських витоків, порушення прав доступу. Контролюють і не допускають несанкціоноване переміщення інформації за межі мережі.

– Системи контролю доступу, Access Control, Authentication. Застосовуються для моніторингу контролю доступу до інформаційних систем та використання привілеїв.

– IDS/IPS-системи. Система запобігання вторгнень (англ. Intrusion Prevention System, IPS) – програмна або апаратна система мережевої та комп'ютерної безпеки, що виявляє вторгнення або порушення безпеки і автоматично захищає від них. Системи IPS можна як розширення Систем

виявлення вторгнень (IDS), оскільки завдання відстеження атак залишається однаковою. Однак, вони відрізняються в тому, що IPS повинна відстежувати активність у реальному часі та швидко реалізовувати дії щодо запобігання атакам. Надають відомості про мережеві атаки, зміни конфігурації та доступ до пристроїв.

– Міжмережеві екрани. Відомості про атаки, шкідливе ПЗ, інциденти безпеки та інше.

– Мережеве активне обладнання. Використовується для контролю доступу, обліку мережевого трафіку.

– Системи веб-фільтрації. Надають дані про відвідування співробітниками підозрілих або заборонених веб-сайтів, контролює доступ до шкідливих сайтів.

– Сканери вразливостей. Дані про інвентаризацію активів, сервісів, програмного забезпечення, уразливостей, постачання інвентаризаційних даних та топологічної структури.

– Системи інвентаризації та asset-management. Поставляють дані для контролю активів в інфраструктурі та виявлення нових.

– Системи ресурсів-приманок для зловмисників (англ. honeypots і honeynets) є заздалегідь створеними «муляжами» інформаційних систем, схожими на реальні системи компанії, але не містять жодних цінних даних. Атакуючі, потрапивши в таку пастку, спробують застосувати свій інструментарій для проведення атаки, а в цей момент їхні дії ретельно журналюватимуться і потім вивчатимуть фахівці захисту інформації.

– Засоби управління портативними пристроями (MDM – Mobile Device Management) є програмами контролю та захисту портативних пристроїв співробітників організації. Встановивши такий засіб на свій пристрій, співробітник може отримати контрольований та безпечний віддалений доступ до IT-ресурсів організації, наприклад, підключивши собі на смартфон робочу пошту.

14.2. Система візуалізації та управління подіями (SIEM)

SIEM (Security information and event management) – об'єднання двох термінів, що позначають область застосування ПЗ: SIM (Security information management) – управління інформацією про безпеку, і SEM (Security event management) – управління подіями безпеки. Технологія SIEM забезпечує аналіз у реальному часі подій (тривог) безпеки, що виходять від мережевих пристроїв та додатків, і дозволяє реагувати на них до настання істотних збитків.

З зростаючим обсягом інформації, що обробляється та передається між різними інформаційними системами (ІС), організації та окремі користувачі все більше залежать від безперервності та коректності виконання цих процесів. Для реагування на загрози безпеці в ІС необхідно мати інструменти, що дозволяють **аналізувати в реальному часі події**, кількість яких тільки зростає. Одним із рішень даної проблеми є використання SIEM-систем.

Основним принципом системи SIEM є те, що дані про безпеку інформаційної системи збираються з різних джерел, і результат їх обробки надається в єдиному інтерфейсі, доступному для аналітиків безпеки, що полегшує вивчення характерних особливостей, що відповідають інцидентам безпеки.

SIEM є об'єднанням систем управління інформаційною безпекою(SIM) та управління подіями безпеки (SEM) в єдину систему управління безпекою. Сегмент SIM в основному відповідає за аналіз історичних даних, намагаючись покращити довгострокову ефективність системи та оптимізувати зберігання історичних даних. Сегмент SEM, навпаки, наголошує на вивантаженні з наявних даних певного обсягу інформації, за допомогою якого можуть бути негайно виявлені інциденти безпеки. У міру зростання потреб у додаткових можливостях безперервно розширюється та доповнюється функціональність цієї категорії продуктів.

Однією з головних цілей використання SIEM-систем є підвищення рівня інформаційної безпеки в існуючій архітектурі за рахунок забезпечення можливості маніпулювати інформацією про безпеку та здійснювати попереджувальне управління інцидентами та подіями безпеки в близькому до реального часу режимі.

Випереджальне управління інцидентами та подіями безпеки полягає у ухваленні рішень ще до того, як ситуація стане критичною. Таке управління може здійснюватися з використанням автоматичних механізмів, які прогнозують майбутні події на основі історичних даних, а також автоматичне підстроювання параметрів моніторингу подій до конкретного стану системи.

SIEM представлено програмами, приладами або послугами, і використовується також для журналування даних та генерації звітів з метою сумісності з іншими бізнес-даними.

Поняття *управління подіями інформаційної безпеки* (SIEM), введене Марком Ніколеттом та Амрітом Вільямсом з компанії Gartner у 2005 р., описує функціональність збору, аналізу та подання інформації від мережевих пристроїв та пристроїв безпеки, додатків ідентифікації (управління обліковими даними) та управління доступом, інструментів підтримки політики безпеки та відстеження вразливостей, операційних систем, баз даних та журналів додатків, а також відомостей про зовнішні загрози. Основна увага приділяється управлінню привілеями користувачів та служб, службами каталогів та іншим змінам конфігурації, а також забезпеченню аудиту та огляду журналів, реакціям на інциденти.

Розв'язувані завдання:

– збір, обробка та аналіз подій безпеки, що надходять до системи з багатьох джерел;

– виявлення в режимі реального часу атак та порушень критеріїв та політик безпеки ;

– оперативна оцінка захищеності інформаційних, телекомунікаційних та інших критично важливих ресурсів;

– аналіз та управління ризиками безпеки;
– проведення розслідувань інцидентів;
– прийняття ефективних рішень щодо захисту інформації;
– формування звітних документів

Архітектура

Зазвичай, SIEM-система розгортається над інформаційною системою, що захищається, і має архітектуру «джерела даних» – «сховище даних» – «сервер додатків».

SIEM-рішення являють собою інтегровані пристрої (all-in-one) або двотрикомпонентні комплекси. Розподілена архітектура найчастіше передбачає велику продуктивність і кращі можливості масштабування, а також дозволяє розгорнути SIEM-рішення в IT-інфраструктурах з кількома майданчиками.

Агенти виконують початкову обробку та фільтрацію, а також збирання подій безпеки.

Передача інформації від джерел даних може здійснюватися кількома способами:

– джерело ініціює передачу подій (наприклад, відправляє по syslog-протоколу);
– події з джерела забираються пасивно.

Розглянемо використання цих методів практично.

З першим варіантом все досить просто: на джерелі вказується IP-адреса пристрою, що здійснює збір подій (колектора), і події відправляються адресату.

Другий варіант включає агентний або безагентний збір інформації, причому в деяких SIEM-системах частини джерел доступні обидва способи.

Агентний спосіб передбачає використання спеціальної програми-агента, безагентний – налаштування джерела подій, такі як створення додаткових облікових записів, дозвіл віддаленого доступу та використання додаткових протоколів.

Зібрана та відфільтрована інформація про події безпеки надходить до сховища даних, де вона зберігається у внутрішньому форматі подання з метою подальшого використання та аналізу сервером додатків.

Сервер програм реалізує основні функції захисту інформації. Він аналізує інформацію, що зберігається в репозиторії, і перетворює її для вироблення попереджень або управлінських рішень щодо захисту інформації.

Виходячи з цього, в SIEM-системі виділяються такі **рівні її побудови**:

– збирання даних: здійснюється від джерел різних типів, наприклад, файлових серверів, міжмережевих екранів, антивірусних програм;

– керування даними: дані, що зберігаються в репозиторії, видаються за запитами моделей аналізу даних;

– аналіз даних: результатом є звіти у визначеній і довільній формі, оперативна кореляція даних про події, а також попередження, що видаються.

Функціонування SIEM

Для вирішення поставлених завдань SIEM-системи першого покоління застосовують нормалізацію, фільтрацію, класифікацію, агрегацію, кореляцію та пріоритезацію подій, а також генерацію звітів та попереджень.

У SIEM-системах нового покоління до них слід додати також аналіз подій, інцидентів та їх наслідків, а також прийняття рішень та візуалізацію.

Нормалізація наводить формати записів журналів, зібраних із різних джерел, до єдиного внутрішнього формату, який потім буде використовуватися для їх зберігання та подальшої обробки.

Фільтрація подій безпеки полягає у видаленні надлишкових подій з потоків, що надходять в систему.

Класифікація дозволяє для атрибутів подій безпеки визначити їхню належність певним класам.

Агрегація поєднує події, схожі за певними ознаками.

Кореляція виявляє взаємозв'язок між різнорідними подіями.

Пріоритезація визначає значущість та критичність подій безпеки на підставі правил, визначених у системі.

Аналіз подій, інцидентів та їх наслідків включає процедури моделювання подій, атак та їх наслідків, аналізу вразливостей та захищеності системи, визначення параметрів порушників, оцінки ризику, прогнозування подій та інцидентів.

Генерація звітів та попереджень означає формування, передачу, відображення чи друк результатів функціонування.

Візуалізація передбачає подання у графічному вигляді даних, що характеризують результати аналізу подій безпеки та стан системи, що захищається, та її елементів.

Функціональність:

- **Агрегація даних:** керування журналами даних; дані збираються з різних джерел: мережеві пристрої та послуги, датчики систем безпеки, сервери, бази даних, додатки; забезпечується консолідація даних із метою пошуку критичних подій.
- **Кореляція:** пошук загальних атрибутів, зв'язування подій у значні кластери. Технологія забезпечує застосування різних технічних прийомів для інтеграції даних із різних джерел перетворення вихідних даних на значну інформацію. Кореляція є типовою функцією підмножини Security Event Management.
- **Оповіщення:** автоматизований аналіз корелюючих подій та генерація сповіщень (тривог) про поточні проблеми. Оповіщення може виводитися на «приладову» панель самої програми, так і бути направлено в інші канали: e-mail, GSM-шлюз і т.п.
- **Засоби відображення** (інформаційні панелі): відображення діаграм, які допомагають ідентифікувати патерни, відмінні від стандартної поведінки.
- **Сумісність (трансформованість):** застосування додатків для автоматизації збору даних, формування звітності для адаптації даних, що

агрегуються, до існуючих процесів управління інформаційною безпекою та аудиту.

– **Зберігання даних:** застосування довгострокового сховища даних в історичному порядку для кореляції даних за часом та забезпечення трансформації. Довготривале зберігання даних є критичним для проведення комп'ютерно-технічних експертиз, оскільки розслідування мережного інциденту навряд чи проводитиметься в момент порушення.

– **Експертний аналіз:** можливість пошуку за безліччю журналів на різних вузлах; може виконуватися у межах програмно-технічної експертизи.

14.3. Аналіз подій SIEM

Перше завдання SIEM – отримати дані від джерела. Це може бути як «активне» джерело, яке вміє передавати дані в SIEM і йому достатньо вказати мережеву адресу приймача, так і «пасивний», до якого SIEM-система повинна звернутися сама.

Отримавши від джерела дані, SIEM-система перетворює їх на одноманітний, придатний для подальшого використання формат – це називається нормалізацією. Порівняємо це з великою компанією людей з різних країн: усі говорять своїми мовами, а SIEM-система всіх слухає і нормалізує, тобто. перекладає все англійською, щоб потім можна було переглянути всю розмову єдиною, зрозумілою мовою.

Далі SIEM-система виконує таксономію, тобто. класифікує вже нормалізовані повідомлення в залежності від їх змісту: яка подія говорить про успішну мережеву комунікацію, яка – про вхід користувача на ПК, а яка – про спрацювання антивіруса. Таким чином, ми отримуємо вже не просто набір записів, а послідовність подій з певним змістом та часом настання. Отже, ми вже можемо зрозуміти, в якій послідовності йшли події і який може бути зв'язок між ними.

Тут у гру входить основний механізм SIEM-систем: кореляція. Кореляція в SIEM – це співвідношення між собою подій, які відповідають тим чи іншим умовам (правилам кореляції). Приклад правила кореляції: якщо на двох і більше ПК протягом 5 хвилин спрацював антивірус, то це може свідчити про вірусну атаку на компанію. Більш складне правило: якщо протягом 24 годин були зафіксовані чиїсь спроби віддалено зайти на сервер, які зрештою увінчалися успіхом, а потім з цього сервера почалося копіювання даних на зовнішній файлообмінник, це може свідчити про те, що зловмисники підібрали пароль до облікового запису, зайшли всередину сервера та крадуть важливі дані. За підсумками спрацьовування правил кореляції у SIEM-системі формується інцидент інформаційної безпеки (у деяких системах, наприклад, у SIEM IBM QRadar інцидент називається Offense). При цьому фахівець з ІБ при роботі з SIEM повинен мати можливість швидкого пошуку по попереднім інцидентам і подіям, що зберігаються в SIEM-системі, на випадок, якщо йому знадобиться будь-які додаткові технічні подробиці для розслідування атаки.

Отже, **основні завдання SIEM-систем** такі:

1. Отримання журналів із різноманітних засобів захисту
2. Нормалізація отриманих даних
3. Таксономія нормалізованих даних
4. Кореляція класифікованих подій
5. Створення інциденту, надання інструментів щодо розслідування
6. Зберігання інформації про події та інциденти протягом тривалого часу (від 6 місяців)
7. Швидкий пошук за даними, що зберігаються в SIEM даних

Крім зазначеного функціоналу, SIEM-системи можуть також оснащуватися додатковими функціями, такими як управління ризиками та вразливістю, інвентаризація IT-активів, побудова звітів та діаграм тощо. Автоматизоване реагування на інцидент також можна налаштувати, для цього використовують системи IRP (Incident Response Platform, платформи реагування на інциденти інформаційної безпеки), які можуть без участі людини, наприклад, заблокувати зламаний обліковий запис або відключити інфікований ПК від мережі.

Підсумовуючи, ми можемо сказати, що системи SIEM необхідні компаніям для роботи з великим потоком різноманітних даних від різних джерел з метою виявлення потенційних інцидентів інформаційної безпеки та своєчасного реагування на них.

Користь від впровадження та застосування SIEM-системи полягає в тому, що вона значно прискорює процес обробки інцидентів ІБ та отримання необхідної інформації про події ІБ: аналітику не потрібно підключатися до кожного засобу захисту інформації, він бачить усі дані в єдиному консолідованому вигляді в одному зручному інтерфейс.

Якщо у компанії відповідно до законодавства є вимоги до зберігання всіх журналів аудиту (тобто логів) засобів захисту за певний часовий період, наприклад, не менше ніж за рік, використання SIEM-систем дозволяє виконати цю вимогу. Таким чином є можливість реалізувати SOC (Security Operations Center, або Центр забезпечення безпеки), ядром якого стане SIEM-система.

Зрозуміло, при впровадженні та налаштуванні SIEM-систем існують очевидні **труднощі** як організаційного, так і технічного характеру: крім купівлі самої SIEM-системи доведеться ще:

– налаштувати всі джерела даних на відправку даних у SIEM;
– створювати правила кореляції;
– усувати причини хибно-позитивних спрацьовувань;
– підтримувати SIEM-систему в актуальному стані;
– оперативно розслідувати інциденти інформаційної безпеки що згенеровані SIEM.

Але це є прийнятним, оскільки забезпечує безпеку даних, а значить – найціннішого, що часом є у компанії.

Перспективи розвитку SIEM-систем

Найбільш перспективними напрямками, які допоможуть SIEM-системам краще виявляти кіберінциденти та запобігати їх наслідкам, експерти назвали:

– розвиток експертизи в галузі управління системою;

– автоматизацію реагування на інциденти;

– розширення можливостей SIEM за рахунок технологій аналізу трафіку, аналізу того, що відбувається на кінцевих вузлах, моніторингу користувачів та сутностей;

– хмарних обчислень як джерела даних та надання SIEM за сервісною (as a service) моделлю.

Серед технологій, що впливають на розвиток SIEM-систем, фахівці відзначили розвиток експертизи в галузі управління системою. Останні 15 років про SIEM прийнято говорити як засіб для збору логів з різних систем і засобів кореляції, а аналіз зібраних масивів даних обмежується мапінгом правил кореляції по матриці MITRE ATT & CK.

Для підвищення якості моніторингу подій безпеки SIEM цього недостатньо, потрібні:

– правила нормалізації;

– способи налаштування джерел;

– пакети з правилами виявлення загроз;

– інструкції з активації джерел;

– опис правил детектування;

– рекомендації про те, що робити, якщо спрацювало правило.

Частка покриття цієї технології (глибина проникнення) становить 50-60%, якість реалізації – середня (3 бали).

Ще один тренд розвитку SIEM-систем – це автоматизація реагування на інциденти. Згідно з опитуванням, проведеним, 25% фахівців з ІБ проводять у SIEM-системі від двох до чотирьох годин щодня. До найбільш трудомістких завдань учасники опитування віднесли роботу з помилковими спрацьовуваннями (доналагодження правил кореляції) та розбір інцидентів: їх відзначили 58% та 52% респондентів відповідно. У 30% фахівців з ІБ багато часу забирають налаштування джерел даних та відстеження їх працездатності. Цей тренд дає поштовх розвитку SIEM-систем в область іншого класу продуктів – SOAR. Частка покриття технології становить 60-70%, а якість реалізації – 3.

Третій тренд пов'язаний з конвергенцією технологій аналізу трафіку (NTA-систем), логів (SIEM) і того, що відбувається на кінцевих вузлах (EDR). Без глибокого аналізу мережі та можливостей EDR моніторинг не буде повним. У найближчі три роки аналіз трафіку розглядатиметься як обов'язкова умова майбутнього SIEM, а аналіз подій на кінцевих вузлах – як функціональна можливість, що доповнює. Покриття технології 60-70%, якість реалізації – 2 бали.

Прагнення отримати на одному екрані єдину картину того, що відбувається в інфраструктурі, сприятиме додаванню до можливостей SIEM інструментів UEBA – поведінкового аналізу користувачів та сутностей (процесів, вузлів

мережі, мережевих активностей). Головна відмінність SIEM від UEBA в тому, що SIEM-система виступає як свого роду конструктор для збору логів, а рішення UEBA будує поведінкові моделі. Алгоритми пошуку та обробки аномалій можуть включати різні методи: статистичний аналіз, машинне навчання(machine learning), глибоке навчання (deep learning) та ін., які підказують оператору, які користувачі та сутності в мережі стали вести себе нетипово і чому ця поведінка для них нетипова. Це четверта технологія, покриття якої оцінюється в 70-80%, а якість реалізації на 4 бали.

П'яте напрямок розвитку SIEM-систем пов'язані з хмарами. Згідно з дослідженням, приблизно дві третини (64%) підприємств планують збільшити витрати на публічні хмарні платформи порівняно з попереднім роком. Такий підхід, з одного боку, змушує вендорів додавати найпопулярніші хмарні сервіси (AWS, Google Cloud Platform, Microsoft Azure) до списку підтримуваних SIEM джерел – за рахунок підключення конекторів до хмар а з іншого, навчитися і самим надавати SIEM за моделлю as a service – за допомогою додавання специфічних для хмарної інфраструктури способів розгортання, конфігурування та диригування SIEM (віртуальних, хмарних аплайнсів). За експертними оцінками, частка покриття цієї технології становить 60-70%, а якість реалізації – 3 бали.