УДК 004.056

ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ДЕРЖАВНОГО СЕКТОРУ НА ОСНОВІ SIEM-СИСТЕМ

DOI 10 36994 / 2788- 5518- 2022-02-04-14

Кошара А.В. *Державний університет інтелектуальних технологій і зв'язку, Київ, Україна. artemkosharaa@gmail.com*

Бакало Б.В. *. Відкритий міжнародний університет розвитку людини «Україна»,Київ,Україна. konstantin.bogdanbakalo@.gmail.com*

Анотація: *У статті розглядається актуальність експлуатації SIEM-систем задля організації захисту інформаційно-телекомунікаційних систем та оперативного виявлення кібератаки, своєчасне реагування на таку атаку для якісного розслідування інциденту кібератаки направленої на державні установи та оборонні підприємства держави. Наведено статистичні дані незалежних комерційних організацій та державного Держспецзв'язку, на тему найбільш вразливих категорій підприємств та найбільш ризикових векторів загроз. В статті викладено , що потреба в описаних системах обумовлена експоненційним зростанням кількості кіберзагроз, їх ускладненням і появою цілеспрямованих атак з використанням різних векторів проникнення. Цінність SIEM-системи полягає в тому, що вона збирає інформацію з різних систем та мережевих пристроїв, зберігає їх в одному місці та видає в доступному для аналізу вигляді, також система зберігає дані про всі події в мережі для розслідування інцидентів співробітниками відділу інформаційної безпеки. Тільки завдяки аналізу накопичених даних в SIEM, дозволяє визначити, стався інцидент вперше або подібні атаки були і в минулому. Проведено дослідження сучасних інструментів інформаційної безпеки, що входять до складу SIEM-систем, в розрізі моніторингу та реагування на інциденти інформаційної безпеки. Проведено огляд засобів SIEM-системи, що допомагають виявляти загрози інформаційної безпеки та оперативно реагувати на них. А саме: способи виявлення внутрішніх загроз, встановлення факту крадіжки даних, виявлення зловживання привілейованим доступом, виявлення компрометації довіреного пристрою, опис роботи та можливостей інструменту UBA, що базується на технології штучного інтелекту. Проведено огляд програмних складових (компонентів) SIEM-систем, з описом основних фунцій зазначених компонентів. Наведено рекомендації, щодо глибшого дослідження певних аспектів роботи SIEM-систем та систем наступного покоління – SOAR.*

Ключові слова: *кібербезпека, SIEM, атака, виявлення, реагування, держустанова, оборонний сектор.*

INCREASING SECURITY OF THE PUBLIC SECTOR BASED ON SIEM-SYSTEMS

Artem Koshara . *State University of Intellectual Technologies and Communication, Kyiv, Ukraine.artemkosharaa@gmail.com*

Bogdan Baralo. *Open International University of Human Development "Ukraine",Kyiv, Ukraine. bogdanbakalo@.gmail.com*

Abstract: *The article examines the relevance of using SIEM systems to organize the protection of information and telecommunication systems and the prompt detection of a cyber attack, timely response to such an attack for the qualitative investigation of an incident of a cyber attack directed at state institutions and defense enterprises of the state. Statistical data of independent commercial organizations*

and the state State Intelligence Service are given on the topic of the most vulnerable categories of enterprises and the most risky threat vectors. The article states that the need for the described systems is due to the exponential growth of the number of cyber threats, their complexity and the appearance of targeted attacks using various penetration vectors. The value of a SIEM system is that it collects information from various systems and network devices, stores it in one place and issues it in an accessible form for analysis, and the system also stores data about all events in the network for the investigation of incidents by employees of the information security department. Only thanks to the analysis of the accumulated data in SIEM, it is possible to determine whether the incident happened for the first time or whether similar attacks have occurred in the past. A study of modern information security tools, which are part of SIEM systems, was conducted in terms of monitoring and responding to information security incidents. An overview of the tools of the SIEM system, which help to detect threats to information security and promptly respond to them, was conducted. Namely: methods of detecting internal threats, establishing the fact of data theft, detecting the abuse of privileged access, detecting the compromise of a trusted device, describing the operation and capabilities of the UBA tool based on artificial intelligence technology. An overview of software components (components) of SIEM systems was conducted, with a description of the main functions of the specified components. Recommendations are given for a deeper study of certain aspects of the work of SIEM systems and systems of the next generation - SOAR.

Key words: *cyber security, SIEM, attack, detection, response, government agency, defense sector.*

Вступ

Більшість інформаційно-комунікаційних систем України сьогодні піддаються впливу різноманітних загроз інформаційної безпеки. Всього лише за перші 4 місяці повномасштабного воєнного вторгнення росії за даними Держспецзв'язку було проведено 796 кібератак на цифрову інфраструктуру України. Переважна більшість атак прийшлася саме на державний сектор: уряд і місцеві органи влади – 179 атак та сектор безпеки і оборони – 104 [1]. Загалом, загрози можуть надходити як ззовні, так і зсередини організації та можуть мати руйнівні наслідки. Атаки можуть повністю вивести з ладу системи або призвести до витоку конфіденційної, таємної інформації, що може суттєво вплинути на обороноздатність держави.

Для захисту держустанови та її локальної мережі тепер недостатньо звичайної антивірусної програми та міжмережевого екрану. Починаючи з другого десятиліття XXI століття, спектр потенційних загроз значно розширився, а число пристроїв, підключених до однієї комп'ютерної мережі, може становити більше декількох тисяч, при цьому знаходитися на різних континентах. Першим кроком до посилення стану захищеності мереж стало виявлення підозрілої активності, адже якщо загрозу було виявлено вчасно, то її нейтралізація та подальший захист від неї буде значно легшим кроком для підприємства, аніж усунення наслідків успішної для зловмисника кібератаки.

Вказані вище об'єми атак на дежрустанови підіймають наступні важливі питання: оперативне виявлення кібератаки, своєчасне реагування на таку атаку та зручний централізований засіб для аналізу подій інформаційної безпеки з IT-систем для якісного розслідування інциденту. Для покриття вищевказаних задач існують SIEM-системи.

Виконання досліджень

Системи Security Information and Event Management (управління інформацією та подіями безпеки), або скорочено SIEM - центральний елемент центру управління кібербезпекою (SOC) та є важливою частиною розвиненої системи захисту підприємства або державної організації. SIEM-системи збирають дані про інциденти від різних систем захисту, таких як фаєрволи, IPS, антивіруси. Також є можливість збирати дані з кінцевих пристроїв за допомогою агентів SIEM-системи. Системи управління інформацією та подіями безпеки дозволяють виявляти підозрілі і потенційно небезпечні ситуації. Крім того, ці системи скорочують затрати на інформаційну безпеку та ризики загроз безпеки, зменшуючи час на їх виявлення.

SIEM - система управління інформацією і подіями безпеки (англ. security information and event management) являє собою централізовану платформу реєстрації подій інформаційної безпеки, що дозволяє групам кібербезпеки аналізувати дані про події в режимі реального часу для раннього виявлення цільових кібератак і витоків даних. SIEM використовується як інструмент для збору, зберігання, дослідження і складання звітів за даними журналу для виявлення загроз, реагування на інциденти та для проведення

криміналістичної експертизи.

Потреба в зазначених системах обумовлена експоненційним зростанням кількості кіберзагроз, їх ускладненням і появою цілеспрямованих APT-атак, в тому числі з використанням різних векторів проникнення. SIEM може бути реалізована апаратно, або постачатися як програмне забезпечення (віртуальна машина), може бути розміщена, як в мережі замовника, так і віддалено - в хмарі. Цінність SIEM-системи полягає в тому, що вона збирає інформацію з різних систем та мережевих пристроїв, зберігаючи їх в одному місці та видає в доступному для аналізу вигляді, також система зберігає дані про всі події в мережі (успішна або неуспішна спроба введення паролю від облікового запису, активність вірусів, аномальний трафік, спроба підключення до кінцевого обладнання з використанням протоколів віддаленого доступу, тощо) для розслідування інцидентів співробітниками відділу інформаційної безпеки. Тільки SIEM здатна ефективно зафіксувати розвинену сталу загрозу (APT), при якій шкідливий код може бути присутнім в системах багато місяців до самого моменту активації. Завдяки аналізу накопичених даних SIEM дозволяє визначити, стався інцидент вперше або подібні атаки були і в минулому.

Щоб зрозуміти, наскільки важливу роль в забезпеченні інформаційної безпеки грають SIEM-системи, необхідно звернути увагу на масштаб інцидентів безпеки і задіяних в ньому даних. Велике підприємство здатне генерувати більше 25000 подій в секунду (EPS) і вимагати більше 50 ТБ для збереження даних. Здатність SIEM фільтрувати всі дані і визначати пріоритети найбільш критичних проблем інформаційної безпеки робить безпеку більш керованою. Ефективна SIEM-система виправдає витрати на неї за рахунок економії часу персоналу, навіть якщо сама система вимагає управління та налаштування. В процесі свого функціонування, кожен мережевий пристрій, додаток та кожна операційна система, записують усі події, що відбуваються з ними в журнали реєстру. Завдяки даним, що записані в журналах подій (логах), SIEM може проаналізувати поведінку системи чи користувача, провести оцінку ризиків, враховуючи критичність активів та порушенню на них директив кореляції та надати оцінку захищеності інфраструктури. Наприклад, можна визначити, які саме операції відбувалися в системі на момент порушення директиви кореляції.

В звіті Verizon «Data Breach Investigation Report» зазначено, що 60% основних порушень безпеки були пов'язані з інсайдерськими (внутрішніми) загрозами, інсайдерські загрози залишаються непоміченими протягом місяців (в 42% випадків) або років (38% випадків) [2]. Виявлення інсайдерських загроз є складним завданням - поведінка не викликає підозри в більшості інструментів безпеки, тому що зловмисник є легітимним користувачем. SIEM може виявити індикатори внутрішніх загроз за допомогою поведінкового аналізу, допомагаючи службам інформаційної безпеки виявляти і запобігати атакам завдяки SIEM-системам наступного покоління, які використовують технологію «user behavior analytics» (UBA). Технологія UBA використовує машинне навчання і поведінковий аналіз для визначення базових показників IT-користувачів і систем та інтелектуального виявлення аномалій, що виходять за рамки правил і статистичних кореляцій, які використовуються в SIEM.

Звіт RiskBased Security про порушення конфіденційності даних показав, що виявлено 3932 публічно зареєстрованих випадків витоку даних, в результаті яких було скомпрометовано більш 37 мільярдів записів. У порівнянні з 2019 роком кількість публічно заявлених порушень скоротилася на 48%. Однак загальна кількість скомпрометованих записів збільшилася на 141% і на сьогоднішній день є найбільшою кількістю записів, виявлених за один рік з моменту створення звітності RBS (RiskBased Security) в 2005 році. Було зафіксовано 676 порушень, в яких елементом атаки використовувалися програми-вимагачі, що на 100% більше, ніж в 2019 році [3]. Зростання числа програм-вимагачів в поєднанні з практикою витоку даних, вкрадених під час атаки являли собою головні теми 2022 року для обговорення центрів кіберзахисту, як підприємств різного масштабу, так і центрів кіберзахисту держав по всьому світу.

Сектор охорони здоров'я виявився найбільш постраждалим, на нього довелося 12,3% зареєстрованих порушень. Медичні служби, підприємства роздрібної торгівлі та державні установи зазнали найбільших збитків. Деякі з цих секторів більш привабливі для

кіберзлочинців, тому що вони містять фінансові та медичні дані. Але незважаючи на попередній тезис, всі підприємства що використовують комп’ютерні мережі, є потенційними мішенями для кібератак або корпоративного шпигунства.

International Data Corporation прогнозує, що з урахуванням того, що масштаби кіберзагрози будуть зростати, до 2022 року світові витрати на рішення для кібербезпеки сягатиме 133,7 млрд доларів [4]. Уряди по всьому світу відреагували на зростаючу кількість кіберзагроз, надавши рекомендації з надання допомоги організаціям, що впроваджують ефективні методи кібербезпеки. Наприклад, національний інститут стандартів і технологій (NIST) США створив «Cybersecurity Framework» для боротьби з поширенням шкідливого коду і допомоги в ранньому виявленні. Система виконує безперервний моніторинг всіх електронних ресурсів в режимі реального часу.

SIEM-система здатна «полювати на загрози». Це практика активного пошуку кіберзагроз в організації або мережі. Полювання на загрози може проводитися відразу після інциденту безпеки, але також і в превентивному режимі для виявлення нових або невідомих атак або порушень. Для пошуку загроз необхідний широкий доступ до даних безпеки з усієї організації, який може бути наданий SIEM.

Способи, якими SIEM-система допомогає в процесі пошуку загроз включають в себе: повіщення від систем безпеки, які надають контекст і дані, що допомагають розслідувати потенційний інцидент, виявлення аномалій в IT-системах за допомогою кореляції та поведінкової аналітики, пошук серед історичних даних шаблонів атак або сигнатур, аналогічних відомим атакам, поєднання аналітики загроз з даними безпеки для інтелектуального виявлення атак в IT-системах, створення попереджень, заснованих на відомих ризиках, що допомагають аналітикам інформаційної безпеки сформулювати гіпотезу і перевірити її, досліджуючи дані безпеки в SIEM, перевірка, чи було зафіксовано подібний інцидент раніше - пошук в даних інформаційної безпеки шаблонів, схожих на поточний або попередній інцидент безпеки.

Виявлення зловживання привілейованим доступом SIEM-системою: моніторинг і звітність про підозрілий доступ до конфіденційних даних, моніторинг активності зовнішніх постачальників і партнерів, що мають доступ до інформаційних систем організації, з метою виявлення аномальної поведінки або підвищення привілеїв, попередження про будь-якої активності припинених облікових записів користувачів або несподіваної активності в облікових записах, які зазвичай неактивні, попередження про аномальну активність, що може бути катастрофічною людською помилкою, наприклад, при видаленні великих обсягів даних, створення звітів про користувачів, які звертаються до систем або даних, які виходять за рамки їх звичайного профілю використання.

Виявлення компрометації довірених осіб SIEM-системою: виявлення аномальної активності, попередження про це і надання даних, необхідних для встановлення факту того, чи було скомпрометовано обліковий запис привілейованого користувача, створення базових показників активності серверів, виявлення відхилень від базових показників і оповіщення співробітників центру кібербезпеки, моніторинг трафіку, виявлення аномальних сплесків, використання незахищених протоколів передачі даних, антивірусний моніторинг - шкідливе програмне забезпечення є частою точкою входу для компрометації хоста. SIEM моніторить антивірусні системи захисту, розгорнуті на кінцевих пристроях та повідомляють про такі події, як відключення антивірусного захисту, видалення антивірусу.

Встановлення факту крадіжки даних SIEM-системою: виявлення мережевого трафіку до центрів управління та контролю, виявлення заражених систем, що передають дані неавторизованих сторонам, моніторинг мережевого трафіку по протоколах, які полегшують передачу великих обсягів даних, і попередження, коли передаються незвичайні обсяги або типи файлів, або коли мета невідома або є шкідливою, моніторинг використання веб-додатків організації або внутрішнього використання зовнішніх веб-додатків, що може включати завантаження або доступ браузера до конфіденційних даних, виявлення електронних листів, переадресованих або відправлених іншим особам, крім зазначеного одержувача, крадіжка даних зазвичай пов'язана зі спробами зловмисників підвищити привілеї або отримати доступ до інших IT-систем. SIEM-система може виявляти вказані вище дії шляхом зіставлення даних з декількох IT-систем, відстеження даних від

мобільних пристроїв співробітників і виявляти аномалії, які можуть вказувати на витік інформації через мобільний пристрій.

Виявлення внутрішніх загроз є складним завданням - поведінка не викликає підозри в більшості інструментів безпеки, тому що зловмисник є легітимним користувачем. SIEM може виявити індикатори внутрішніх загроз за допомогою поведінкового аналізу, допомагаючи службам інформаційної безпеки виявляти і запобігати таким загрозам завдяки технології «user behavior analytics» (UBA). Технологія UBA використовує машинне навчання і поведінковий аналіз для визначення базових показників IT-користувачів і систем та інтелектуального виявлення аномалій, що виходять за рамки правил і статистичних кореляцій.

Способи, якими SIEM-системи допомогають зупинити інсайдерські загрози: поведінковий аналіз для виявлення аномальної поведінки користувачів, вказуючих на компрометацію. Наприклад, вхід в систему в незвичайний час доби з незвичайною частотою або доступ до незвичайних даних або систем, SIEM виявляє, що користувачі змінюють або підвищують привілеї для критично важливих систем, SIEM співвідносять мережевий трафік з даними про загрози, щоб виявляти шкідливі програми, які взаємодіють із зовнішніми зловмисниками. Це ознака зламаного облікового запису користувача, поведінковий аналіз для аналізу подій інформаційної безпеки, таких як вставка флеш-накопичувачів USB, використання особистих поштових сервісів, несанкціонованого хмарного сховища або надмірного друку документів, виявлення і зупинення шифрування великих обсягів даних, адже це може вказувати на атаку програми-шифрувальника, інсайдери, які проводять атаку, можуть спробувати вимкнути облікові записи, машини і IP-адреси на шляху до мети. SIEM можуть виявити це поведінку, тому що мають широкий огляд IT-систем.

Типове рішення SIEM-системи включає в себе кілька функціональних компонентів, що зображені на рисунку 1: агент (сервіс, демон), що встановлюється на систему, яку необхідно моніторити, локально збирає журнали подій і за наявності заздалегідь налаштованого мережевого маршруту передає їх до SIEM-систему), лог-колектори, що призначені для попередньої акумуляції подій від безлічі джерел, кореляція, що опрацьовує інформацію від колекторів за встановленими правилами і алгоритмами кореляції, бази даних і сховища для зберігання, як опрацьованих, так і неопрацьованих журналів подій.

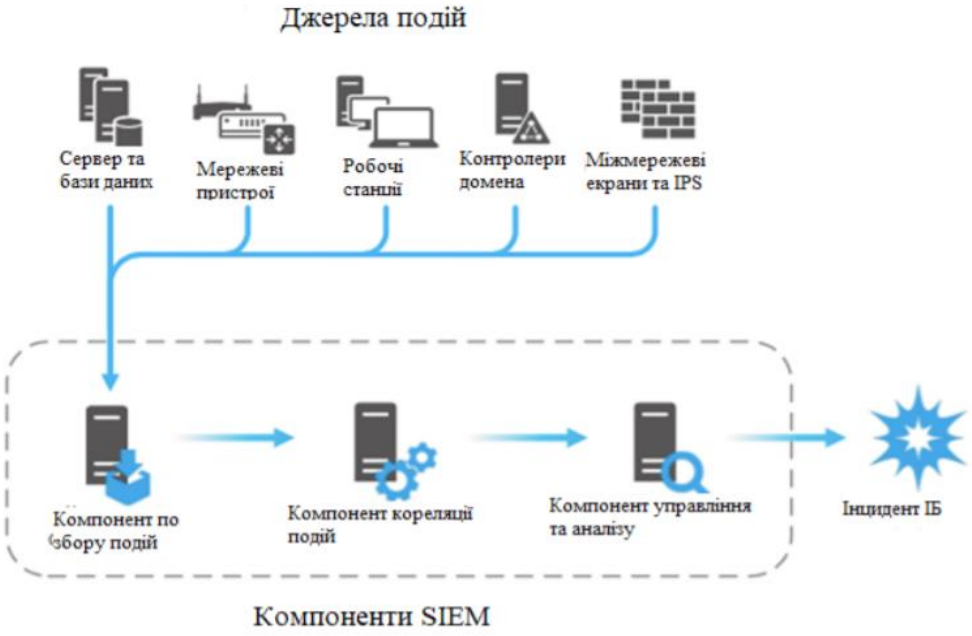

Рис. 1. Основні компоненти SIEM-системи

Висновки

SIEM-система є найнеобхіднішим сучасним інструментом кібербезпеки для державних установ та бізнесу, як в мирний, так особливо і в воєнний час. Адже в обставинах безперервних, як ракетних, так і кібератак, оперативне реагування є ключовою складовою убезпечення життя, як людського, так і життя оборонного сектору держави, а отже і держави вцілому. Наявність великої кількості описаних інструментів у складі SIEM-системи, дозволяє експлуатувати її у відповідності до особливостей діяльності підприємства та задач інформаційної безпеки, що перед ним стоять.

Перспектива подальших досліджень вбачається в ґрунтовнішому вивченні використання інструменту UBA, що базується на технології штучного інтелекту та у висвітленні актуальності експлуатації системи SOAR, як наступного кроку у розвитку автоматизованого реагування на інциденти кібербезпеки.

Література

1. Держспецзв'язку. Статистика кібератак за чотири місяці війни. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni
2. Verizon. 2022 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/
3. RiskBased Security Report. URL: https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report
4. International Data Corporation Report. URL: https://www.idc.com/getdoc.jspcontainerId=prUS46773220
5. Microsoft. What Is SIEM. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem
6. What Is SIEM, Why Is It Important and How Does It Work? URL: https://www.exabeam.com/explainers/siem/what-is-siem/
7. SIEM Architecture: Technology, Process and Data. URL: https://www.exabeam.com/explainers/siem/siem-architecture/
8. Everything You Need to Know about SIEM Architecture. URL: https://wisdomplexus.com/blogs/siem-architecture/

References

1. Derzhspeczv'yazku. Statistika kiberatak za chotiri misyaci vijni. [Statistics of cyberattacks for four months of the war]. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni
2. Verizon. 2022 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/
3. RiskBased Security Report. URL: https://pages.riskbasedsecurity.com/en/en/2020-yearend-data-breach-quickview-report
4. International Data Corporation Report. URL: https://www.idc.com/getdoc.jspcontainerId=prUS46773220
5. Microsoft. What Is SIEM. URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-siem
6. What Is SIEM, Why Is It Important and How Does It Work? URL: https://www.exabeam.com/explainers/siem/what-is-siem/
7. SIEM Architecture: Technology, Process and Data. URL: https://www.exabeam.com/explainers/siem/siem-architecture/
8. Everything You Need to Know about SIEM Architecture. URL: https://wisdomplexus.com/blogs/siem-architecture/