УДК 004.056.53

АНАЛІЗ СИСТЕМ УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Юшко А.В.[1)] , Шевчук Р.П.[2)]
Західноукраїнський національний університет
[1)]аспірант;[2)] к.т.н., доцент

I. Постановка проблеми

Глобальність та багатовекторність бізнес-процесів сучасних організацій вимагають ефективного реагування на сучасні виклики та загрози їх безпеці. Для вирішення цієї задачі в даний час широко використовуються інформаційні системи класу SIEM (Security information and event management). Основним завданням цих систем є здатність збирати, агрегувати, фільтрувати, зберігати, нормалізувати, корелювати та візуалізовувати дані, які характеризують стан безпеки на основі контекстної, поведінкової і часової аналітики [1].

Питання вибору системи управління подіями інформаційної безпеки є достатньо складною задачею, оскільки її вирішення визначається рядом чинників, зокрема наявністю власних правил кореляції та їх керуванням, підходами щодо ескалації інцидентів, засобами оповіщення про інциденти, інтеграцією із сторонніми системами інформаційної безпеки, можливістю створення власних моделей визначення критичності вразливостей та активів та іншими. Тому дана робота присвячена аналізу відомих інформаційні системи класу SIEM.

II. Мета дослідження

Метою дослідження є аналіз відомих інформаційних систем класу SIEM та визначення їх основних характеристик.

III. Типова схема інформаційних системи класу SIEM

Інформаційні системи класу SIEM є комплексним рішенням спрямованим на керування процесами прикладного і системного програмного забезпечення, які застосовуються засобами обчислювальної техніки. Вони забезпечують виконання функцій активного та пасивного моніторингу стану програмно-апаратного середовища обчислювальних засобів та здатні виявляти:

- мережеві атаки по внутрішньому і зовнішньому периметрах;
- вірусні епідемії або окремі вірусні зараження, не видалені віруси, трояни;
- спроби несанкціонованого доступу до конфіденційної інформації;
- помилки та збої в роботі інформаційної системи;
- вразливості;
- помилки конфігурацій в засобах захисту і інформаційних системах.

Важливо відмітити, що SIEM системи в якості самостійного рішення не призначені і не можуть запобігати порушенням подій інформаційної безпеки, аєуніверсальними згідно своєї бізнес логіки.

До основних джерел інформації для інформаційних систем типу SIEM можна віднести:

- Access Control, Authentication.
- DLP-системи.
- DS \ IPS.
- Антивірусне програмне забезпечення.
- Журнали подій серверів і робочих станцій.
- Міжмережеві екрани.
- GRC-системи.
- Netflow та системи обліку трафіку.
- Системи інвентаризації та asset-management.
- Системи веб-фільтрації.

Основними складовими SIEM-системи є (рисунок 1):

- агенти – встановлюються на інформаційну систему і передають дані з неї на сервер, до складу агентів можуть включатися модулі для перетворення даних;
- сервер-колектор – збирає події від безлічі джерел;
- сервер-корелятор – збирає і обробляє інформацію від колекторів і агентів;
- сервер баз даних – зберігає журнали подій.

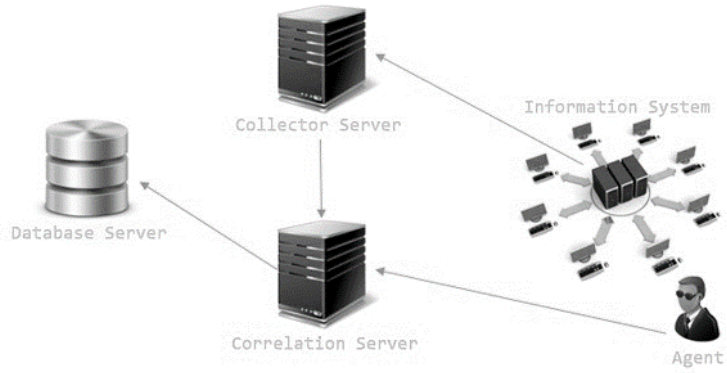

Рисунок 1 –Типова схема інформаційних системи класу SIEM

Схема взаємодії компонент SIEM-систем в загальному вигляді завжди містить модуль кореляції інформації та подій безпеки, який є одним із основних елементів застосовуваних механізмів безпеки. Робота компонентів кореляції спрямована на виявлення атак, шкідливої активності і порушень політики безпеки. Даний компонент виконує як функції кореляції подій, так і їх перед- пост обробку в залежності від конкретної реалізації системи[2].

IV. Порівняльний аналіз інформаційних системи класу SIEM

У роботі виділено основні характеристики SIEM-систем та проведений аналіз частини представлених на ринку систем відповідно до виділених характеристик (таблиця 1).

Таблиця № 1

Порівняльна таблиця SIEM систем

Характеристика/ Вендор	FortiSIEM	AlienVault OSSIM	McAfee ESM	QRadar SIEM	RSA NetWitness	Splunk
1	2	3	4	5	6	7
Шляхи ескалації інциденту	Автоматична ескалація при формуванні інциденту за часом (прострочені кейси і за абсолютним значенням - дні, години), додатково - відправка повідомлень	немає	Ручна ескалація або за допомогою налаштування автоматичного сповіщення	Ескалація вручну	Ескалація вручну або сповіщення	Автомат. система ескалації на SOAR та інші засоби Ручна ескалація через WorkflowActions в карточці інциденту
Оповіщення про інцидент	email, консоль, інструменти оповіщення відповідно до налаштованої політики	email	SMTP, SMS	SMTP, скрипти	SMTP, скрипти	email, месенджери, скрипти, інтеграція зі стороніми сервісами
Інтеграція з системами Service Desk	API, встановлені: ConnectWise, ServiceNow, SalesForce	API, email, SNMP	API, email	API, email, SNMP	Так (Syslog)	Так (API, email, SNMP)
Автореєстрація вразливостей (інтеграція зі сканерами)	API, інтеграція з будь-якими зовнішніми інструментами при наявності	Сканер вразливостей	Інтеграція по API з декількома сканерами	Інтеграція з більше ніж 20 сканерами. Підтримка AXIS	немає	Інтеграція зсканерами по відкритим протоколам

1	2	3	4	5	6	7
Налаштування власної моделі визначення критичності уразливості	Так	Ні	Так	Немає	Немає	Так
Можливість виділення помилкових спрацьовувань	Так	Ні	В ручному режимі	В ручному режимі	В ручному режимі	В ручному режимі
Визначення критичності активу	Так	Так	В ручному режимі	На рівні мережного об'єкта	Немає	Система вбудованих довідників
Наявність встановлених правил кореляції	Більше 650	82	Більше 180	Більше 140	Більше 130	Більше 550
Наявність встановлених графічних панелей (Dashboards)	Більше 150	5	11	7	11	57
Наявність встановлених звітів	Більше 2800	11	Більше 100	Більше 110	Більше 80	462
Можливість формування звітів у вигляді документів, формати експорту звітів у вигляді документів	PDF, HTML, CSV	PDF	PDF, HTML, CSV	PDF, HTML, RTF, XML, XLS	PDF, CSV	Raw, PDF, CSV, XML, JSON
Формування та надання звітів за розкладом / за критерієм	Так	Ні	Так	Так	Так	Так
Можливість збільшення потужності компонентів системи	Так	Ні	Так	Так	Так	Так
Можливість відновлення бази даних після збоїв	Так	В ручному режимі	Так	Так	В ручному режимі	Так
Управління правилами кореляції	Так	Так	Так	Так	Так	Так

Висновок

У роботі виділено основні характеристики SIEM-систем та проведений аналіз частини представлених на ринку систем відповідно до виділених характеристик. Одержані результати можна використати при виборі оптимальної системи управління подіями інформаційної безпеки.

Список використаних джерел

1. MITRE. Ten Strategies of a World-Class Cybersecurity Operations Center. Carson Zimmerman – The MITRE Corporation, 2014. – 346 p. [Електронний ресурс] – Режим доступу: https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf.
2. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2. // Труды СПИИРАН. 2016. Вып. 47. С. 5-27.