УДК 004.056

Вадим ХМЕЛИК, Ренат ДАВЛЕТОВ

[1]Західноукраїнський національний університет

ДОСЛІДЖЕННЯ ПОБУДОВИ ОПЕРАЦІЙНОГО ЦЕНТРУ БЕЗПЕКИ

Вступ. Сучасні тенденції цифрової трансформації супроводжуються зростанням кількості та складності кіберзагроз, що вимагає від організацій переходу до проактивного моніторингу подій безпеки. Операційний центр безпеки (Security Operations Center, SOC) є ключовим елементом такої стратегії, забезпечуючи безперервне виявлення, аналіз і реагування на інциденти в реальному часі.

Використання інструментів із відкритим програмним кодом, зокрема Wazuh, Suricata, Zeek та MISP, дає змогу створювати ефективні та гнучкі SOC-рішення з мінімальними витратами. Дослідження побудови SOC на основі open-source технологій спрямоване на підвищення рівня кіберстійкості організацій та оптимізацію процесів управління інформаційною безпекою.

Мета дослідження полягає у аналізі принципів побудови SOC, визначенні його архітектури, основних компонентів та функціональних можливостей, а також у розробці підходів до впровадження SOC з використанням інструментів з відкритим програмним кодом.

1. Призначення операційного центру безпеки

SOC - це організаційна та технологічна структура, призначена для централізованого моніторингу, виявлення, аналізу та реагування на інциденти інформаційної безпеки в реальному часі [1, 2]. Основною метою SOC є забезпечення безперервного контролю за станом інформаційної інфраструктури, зменшення часу між виявленням загрози та реагуванням (показники Mean Time to Detect - MTTD та Mean Time to Respond - MTTR), а також підвищення рівня захищеності організації.

SOC функціонує як ядро системи управління інформаційною безпекою (ISMS), забезпечуючи взаємодію між технічними засобами захисту, аналітичними інструментами, базами знань про загрози (Threat Intelligence), а також персоналом, який здійснює моніторинг і реагування. Завдяки інтеграції різнорідних джерел даних - систем виявлення вторгнень (IDS/IPS), антивірусів, файрволів, систем контролю доступу, серверів логів тощо - SOC дозволяє створити єдину картину безпеки інформаційного середовища [3].

Основними завданнями SOC є:

– Моніторинг подій безпеки - збір, кореляція та аналіз журналів подій з усіх компонентів IT-інфраструктури за допомогою систем управління подіями безпеки (SIEM).

– Виявлення та класифікація інцидентів - ідентифікація аномалій, відхилень від базової поведінки або збігів із відомими сигнатурами атак.

– Оцінювання ризиків і пріоритезація - визначення критичності інцидентів відповідно до впливу на активи організації.

– Реагування на інциденти - ініціювання відповідних дій (ізоляція вузлів, блокування облікових записів, активація плейбуків реагування).

– Аналіз інцидентів - дослідження цифрових слідів для встановлення джерела атаки, методів проникнення та наслідків.

– Звітність і аудит - формування аналітичних звітів для оцінювання ефективності заходів безпеки та дотримання політик.

Залежно від масштабу та потреб організації SOC може бути реалізований у декількох формах [4]:

– Внутрішній SOC (Internal SOC) - функціонує в межах організації, забезпечуючи повний контроль над процесами безпеки.

– Керований SOC (Managed SOC) - частково або повністю делегований зовнішньому провайдеру, що забезпечує моніторинг та реагування як послугу (Security-as-a-Service).

– Гібридний SOC - поєднує внутрішні ресурси організації з можливостями зовнішніх аналітичних платформ.

У сучасних умовах SOC стає ключовим елементом концепції Zero Trust та Cyber Resilience, забезпечуючи безперервний моніторинг і адаптивну реакцію на нові вектори атак. Розвиток SOC спрямований у бік автоматизації процесів за допомогою технологій SOAR (Security Orchestration, Automation and Response), штучного інтелекту та машинного навчання, що дозволяє підвищити ефективність реагування та зменшити навантаження на аналітиків.

Використання інструментів з відкритим кодом (open source), таких як Wazuh, Suricata, Zeek, MISP, OpenSearch, Shuffle або TheHive, робить можливим створення повноцінного SOC навіть для організацій із обмеженим бюджетом. Такі рішення забезпечують високу гнучкість, прозорість і можливість кастомізації під специфічні вимоги безпеки.

Отже, SOC є стратегічним компонентом інформаційної безпеки, який забезпечує проактивний підхід до виявлення, аналізу та усунення загроз, а також підтримує процес безперервного вдосконалення системи захисту організації.

2. Архітектура та основні компоненти операційного центру безпеки

Архітектура SOC визначає організаційно-технічну структуру, взаємозв'язок компонентів та інформаційні потоки, необхідні для забезпечення повного циклу моніторингу, виявлення, аналізу та реагування на інциденти інформаційної безпеки. Ефективна архітектура SOC повинна забезпечувати централізовану обробку даних з різних джерел, інтеграцію з інфраструктурою організації та можливість масштабування відповідно до зростання обсягів інформації.

Концептуальна архітектура SOC (рисунок 1) демонструє взаємозв'язок між основними компонентами системи моніторингу, виявлення та реагування на інциденти безпеки [5]. Така архітектура визначає модель функціонування SOC у розрізі джерел даних, технологій, процесів та результатів їх взаємодії.

На схемі представлено ключові елементи SOC:

– вхідні джерела даних – системні журнали, мережевий трафік, події безпеки, системи автентифікації.

– інструменти збору та кореляції інформації – рішення SIEM, що агрегують і аналізують події з різних джерел.

– системи аналітики – модулі для виявлення аномалій, поведінкового аналізу та розслідування інцидентів.

– засоби реагування – автоматизовані механізми (SOAR) для ізоляції, блокування чи усунення загроз.

– моніторинг і звітність – панелі візуалізації, метрики продуктивності та оцінка ефективності заходів безпеки.

– вихідні результати – у вигляді сповіщень, дій з реагування та показників ефективності.

Це дозволяє забезпечити цілісне уявлення про структуру SOC і принципи взаємодії його компонентів.

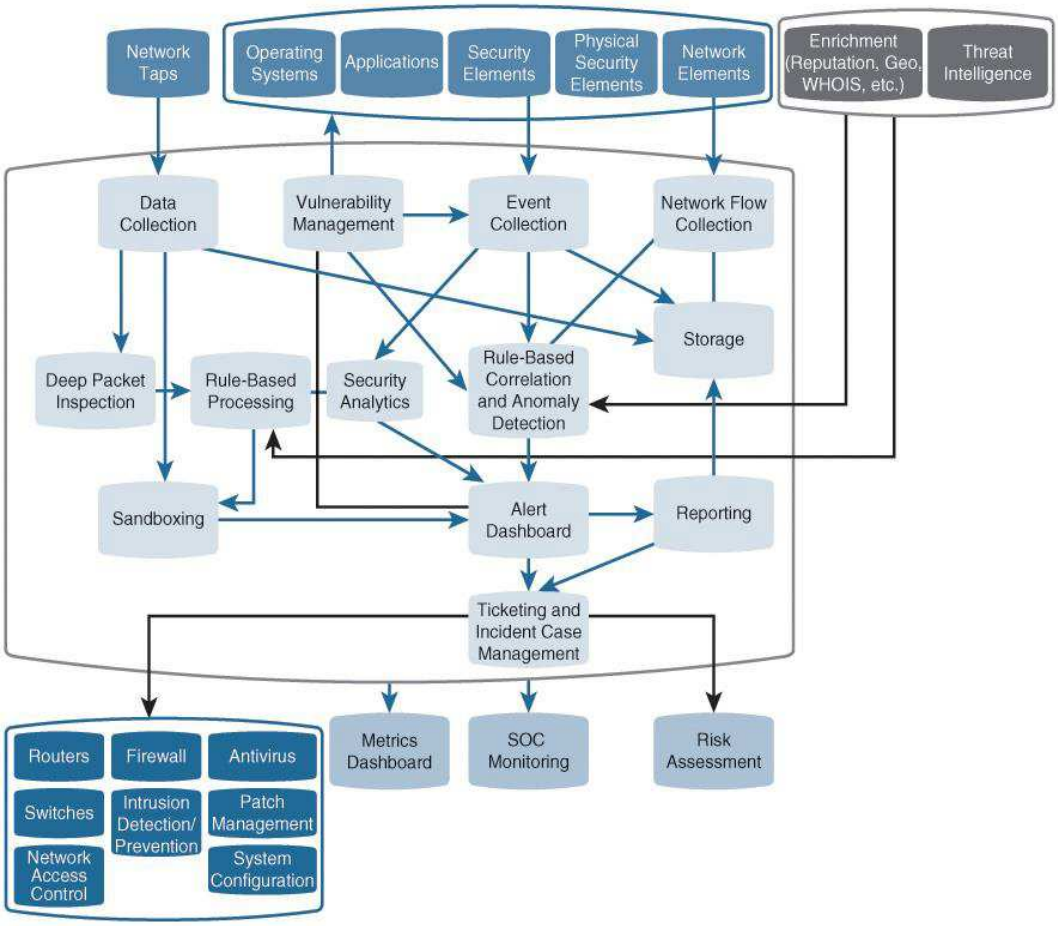

Рисунок 1 - Концептуальна архітектура SOC

Серед типових архітектурних моделей SOC можна виділити:

– монолітну (All-in-One) - усі функції (SIEM, IDS, FIM, SOAR) реалізовані в одному комплексному рішенні, наприклад, Security Onion або Wazuh All-in-One. Такий підхід зручний для малих організацій і навчальних середовищ.

– модульну (Distributed/Scalable) - окремі компоненти SOC (Wazuh, Suricata, Zeek, MISP, Shuffle) розміщені на різних вузлах і взаємодіють через API та черги повідомлень. Цей підхід забезпечує гнучкість, масштабованість та можливість розподіленої обробки даних.

Архітектура SOC являє собою багаторівневу інтегровану систему, яка поєднує апаратні, програмні та організаційні засоби для забезпечення комплексного захисту інформаційного середовища. Від ефективності взаємодії її компонентів залежить швидкість виявлення, точність аналізу та своєчасність реагування на кіберзагрози.

3. Сучасні підходи щодо розвитку SOC

Сучасний розвиток SOC передбачає використання комплексних методів і технологій для підвищення ефективності виявлення, аналізу та реагування на кіберзагрози. Впровадження SOC на базі open-source технологій передбачає поєднання кількох аспектів: вибір компонентів, інтеграцію між ними та налаштування процесів збору, аналізу і реагування на інциденти. Основні підходи включають:

– Вибір стеку технологій – визначаються інструменти для SIEM/XDR (Wazuh), мережевого моніторингу та виявлення вторгнень (Suricata, Zeek), управління інтелектом про загрози (MISP), автоматизації реагування (SOAR – Shuffle або StackStorm) та збору повного трафіку (Arkime).

– Модульний та інтегрований підхід – SOC може будуватися як єдина платформа (Security Onion) або як модульний стек із розподіленими сервісами, що дозволяє масштабувати інфраструктуру та додавати нові функції без повного переналаштування системи.

– Налаштування процесів збору та обробки даних включає підключення агентів на кінцевих точках (Windows, Linux), налаштування логування з мережевих сенсорів, інтеграцію фідів IOC у SIEM, створення правил детекції (Sigma, YARA, Suricata rules) та формування процедур реагування.

– Організація реагування – впровадження SOAR дозволяє автоматично обробляти сповіщення, виконувати сценарії ізоляції інфікованих систем, блокування загроз і створення кейсів інцидентів, що зменшує час реагування (MTTR) і підвищує ефективність SOC.

– Тестування та оцінка ефективності включає експерименти та сценарії атак, перевірку працездатності правил і кореляційних алгоритмів, а також збір метрик ефективності SOC для подальшого удосконалення.

Висновок. Побудова SOC базується на чіткій архітектурі, інтеграції основних компонентів та застосуванні стандартизованих процесів моніторингу й реагування. Реалізація SOC на базі open-source дозволить створювати гнучкі, масштабовані та адаптивні рішення, що сприятиме підвищенню кіберстійкості, оптимізації процесів управління інформаційною безпекою.

Перелік використаних джерел.

1. Security Operations Center (SOC). [Електронний ресурс].- Режим доступу: https://www.wallarm.com/what/security-operations-center-soc

2. What Is A Security Operations Center? [Електронний ресурс].- Режим доступу: https://purplesec.us/learn/security-operations-center-soc/

3. Security Operation Center (SOC). [Електронний ресурс].- Режим доступу: https://blogs.halodoc.io/security-operation-center-soc/

4. Building an Intelligent Security Operations Center. [Електронний ресурс].- Режим доступу: https://www.balbix.com/insights/introduction-to-security-operations-center/

5. Overview of Security Operations Center Technologies. [Електронний ресурс].- Режим доступу: https://www.ciscopress.com/articles/article.asp?p=2455014&seqNum=7