ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.056 doi.org/10.33298/2226-8553.2023.2.40.21

Кочегаров В. С, Богом'я В. І.

ОПЕРАЦІЙНИЙ ЦЕНТР БЕЗПЕКИ (SOC)

«Операційні центри безпеки (SOC) є втіленням сучасної стратегії кібербезпеки», пропонуючи цілісний підхід до управління загрозами за умови їх належного розгортання. Поєднання людського досвіду, процедурних рамок, технологічної інфраструктури та дотримання нормативних вимог є основою ефективного впровадження SOC. Їх основна мета - проактивне виявлення, перехоплення та пом'якшення потенційних кібер-ризиків, таким чином зміцнюючи загальний стан безпеки організації. В академічному дискурсі операції SOC часто розглядаються через призму "Люди, процеси та технології" (People, Processes, and Technology, PPT), що слугує концептуальною основою для розуміння та оптимізації різних аспектів управління інформаційними технологіями. SOC слугує організаційним ядром стратегії безпеки організації, об'єднуючи процеси, технології та персонал для посилення та регулювання заходів з безпеки. Ефективність SOC залежить від кількох ключових факторів, зокрема, від розподілу ролей та обов'язків в рамках SOC, вдосконалення механізмів виявлення та аналізу для перетворення необроблених даних на дієві розвідувальні дані, а також від надійного управління та протоколів відповідності для забезпечення відповідності регуляторним вимогам та внутрішнім стандартам. Стандарти і рекомендації, аудити безпеки, оцінки зрілості і метрики є невід'ємними компонентами роботи SOC, що сприяють постійному вдосконаленню і підвищенню стійкості до нових кіберзагроз.

***Ключові слова**:* Операційні центри безпеки (SOC), Виявлення загроз нейтралізація загроз, операційні процедури, технологічні інструменти, управління інфраструктура безпеки, реагування на інциденти, люди, процеси та технології (PPT).

Вступ. Операційні центри безпеки (SOC) пропонують комплексний підхід до виявлення та нейтралізації загроз за умови ефективного впровадження. Вони включають в себе поєднання людського досвіду, операційних процедур, технологічних інструментів, а також дотримання стандартів управління та відповідності, щоб проактивно виявляти, перехоплювати та пом'якшувати потенційні ризики до їхнього прояву.

SOC слугує основою інфраструктури безпеки організації. Замість того, щоб сприйматися як окрема одиниця, вона є багатогранною структурою, призначеною для посилення загального стану безпеки організації. Її основна роль полягає у виявленні, аналізі та реагуванні на загрози та інциденти кібербезпеки шляхом використання людських ресурсів, встановлених процедур і передових технологій.

В академічному дискурсі операції SOC зазвичай описуються за допомогою концепції "Люди, процеси і технології" (People, Processes, and Technology, PPT). Ця концепція, на яку часто посилаються в дослідженнях, слугує концептуальною моделлю для розуміння та оптимізації різних аспектів управління інформаційними технологіями, починаючи від обробки знань і закінчуючи взаємовідносинами з клієнтами.

Операційний центр безпеки (SOC) представляє собою організаційний вимір стратегії безпеки компанії, об'єднуючи процеси, технології та персонал для посилення та контролю загального стану безпеки. Ця мета, як правило, виходить за межі можливостей окремого підрозділу або системи, що вимагає складної структури. Підвищуючи обізнаність про ситуацію, зменшуючи визнані ризики і сприяючи дотриманню нормативних вимог, SOC відіграє ключову

роль. Більше того, вона забезпечує управління та дотримання вимог як загальну основу, в межах якої діють окремі особи, а також адаптуються процеси і технології.

Архітектура. SOC можуть приймати різні структурні конфігурації, а саме централізовані, розподілені або децентралізовані моделі на високому та концептуальному рівнях. У централізованій архітектурі всі дані, що надходять з різних місць або дочірніх компаній, передаються до єдиного центрального SOC для подальшої обробки. І навпаки, розподілена SOC функціонує подібно до єдиної системи, що охоплює кілька дочірніх компаній, надаючи користувачам безперебійний досвід, що нагадує взаємодію з єдиним суб'єктом. Завдяки розподіленій системі всі компоненти можуть отримувати доступ, обробляти, об'єднувати і надавати інформацію та послуги з безпеки іншим компонентам, сприяючи справедливому розподілу робочого навантаження і даних. Третьою поширеною архітектурною основою SOC є децентралізована система, яка об'єднує елементи вищезгаданих проектів. Децентралізована SOC складається з декількох SOC, кожна з яких потенційно має обмежені можливості, під керівництвом одного або декількох центральних SOC, що є переходом від більш централізованої SOC до децентралізованої архітектури.

Кожна операційна модель має свій власний набір переваг і недоліків, що підкреслює важливість прийняття рішень на ранній стадії. Зміна структури SOC після конфігурації тягне за собою значні витрати часу та ресурсів. Таким чином, ретельне вивчення наслідків вибору конкретної операційної моделі є обов'язковим:

1. Корпоративна стратегія: Оцінка загальної бізнес- та IT-стратегії має вирішальне значення для визначення найбільш підходящої операційної моделі. Визначення стратегії SOC передує вибору відповідної операційної моделі.
2. Галузевий вплив: Галузь, в якій працює компанія, суттєво впливає на необхідну величину SOC.
3. Масштаб: Розмір компанії також відіграє ключову роль у процесі прийняття рішень, оскільки менші підприємства можуть зіткнутися з проблемами у створенні та підтримці SOC самостійно або не потребувати жорстко визначеної структури SOC.
4. Фінансові міркування: Важливо порівняти витрати, пов'язані з внутрішнім впровадженням та підтримкою SOC, з витратами на аутсорсинг операцій з безпеки. Хоча на початковому етапі створення власної SOC може вимагати більших витрат, з часом це може виявитися більш економічно ефективним. Витрати, пов'язані з пошуком, набором і навчанням персоналу СЗІ, мають значну вагу, особливо в умовах зростаючого дефіциту кваліфікованих кадрів і підвищеного ринкового попиту.
5. Час: Створення СОК вимагає значних витрат часу. Тому важливим є узгодження з планами та графіками організації. Крім того, час, необхідний для створення SOC, слід зіставити з часом, необхідним для його аутсорсингу.
6. Відповідність нормативним вимогам: Різні галузі підпадають під дію різних нормативно-правових актів, які необхідно враховувати. Певні нормативні акти можуть вимагати створення власного SOC, тоді як інші можуть обмежувати аутсорсингові операції SOC або визначати затверджених постачальників, які відповідають відповідним нормам.
7. Занепокоєння щодо конфіденційності: Необхідно також дотримуватися правил конфіденційності, особливо щодо обробки персональних даних.
8. Доступність: Необхідно враховувати вимоги доступності, типовою метою якої є цілодобова доступність SOC протягом усього року.
9. Підтримка керівництва: Забезпечення підтримки з боку керівництва має вирішальне значення під час створення спеціального SOC. Відсутність зацікавленості керівництва та нездатність ефективно донести переваги SOC до вищого керівництва може перешкоджати виділенню необхідних ресурсів для команди.
10. Інтеграція: Внутрішні можливості SOC потребують інтеграції з іншими IT-відділами, в той час як зовнішній SOC вимагає безперешкодної інтеграції з обраним постачальником для забезпечення доступу до всіх необхідних даних.

11. Занепокоєння щодо безпеки даних: SOC зазвичай слугує центральним вузлом для обробки значного обсягу конфіденційних даних. Внутрішні ЦОД повинні надавати пріоритет заходам безпеки, тоді як зовнішні ЦОД повинні ретельно обирати надійних постачальників, здатних захистити дані від крадіжки інтелектуальної власності та ненавмисної втрати.

12. Придбання експертизи: Набуття досвіду вимагає як часу, так і фінансових інвестицій. Досвід роботи з SOC не є легкодоступним. Отже, набір та утримання кваліфікованого персоналу є першочерговим завданням для внутрішніх SOC. І навпаки, зовнішні провайдери послуг SOC часто вже володіють необхідним досвідом. Зокрема, в контексті SOC, знайомство з різними організаціями може надати провайдерам SOC перевагу в знаннях. Тим не менш, компанії повинні визнати, що аутсорсинг зменшує збереження внутрішніх знань.

Спеціалізуючий персонал. Ця структура передбачає розмежування процесів для оптимізації операцій, впровадження відповідних технологій для підвищення ефективності та підбір персоналу з необхідними навичками для нагляду за цими процесами. Таким чином, ця структура дає змогу всебічно визначити СУЯ та її складові елементи.

Документація полегшує розмежування різних ролей та обов'язків, що є невід'ємною частиною управління SOC. Крім того, в літературі підкреслюється важливість стратегій набору персоналу та різноманітних підходів до утримання персоналу. Крім того, підкреслюється важливість навчальних ініціатив та інформаційних програм, а також визначення процедур міжвідомчої співпраці та комунікації в рамках SOC.

1) **Ролі та обов'язки**

Як і будь-який інший організаційний підрозділ, СРЦ виконує різні ролі та обов'язки, специфіка яких залежить від його масштабу та сфери діяльності. Залежно від розміру, необхідні різні команди, що складаються з різної кількості людей. Основні ролі, які зазвичай виконують у SOC, включають аналітиків різного рівня кваліфікації, а також спеціалізованих менеджерів. На основі визначених завдань виділяють три окремі ролі з відповідними обов'язками.

- Рівень 1 (спеціаліст з сортування): Аналітики рівня 1 відіграють центральну роль у первинній обробці даних, збираючи первинну інформацію та перевіряючи тривоги і сповіщення. Їхні основні завдання включають перевірку, оцінку або коригування рівнів серйозності тривог, доповнюючи їх релевантними даними. Кожне попередження проходить ретельну перевірку на предмет його достовірності або потенційного хибнопозитивного статусу. Крім того, аналітикам рівня 1 доручено виявляти інші події з високим рівнем ризику та потенційні інциденти, яким потім надається пріоритет на основі рівня їхньої критичності. Якщо будь-які нові проблеми залишаються невирішеними на цьому рівні, вони передаються на розгляд аналітикам рівня 2. Крім того, фахівці з сортування часто здійснюють нагляд за управлінням та конфігурацією інструментів моніторингу.
- Рівень 2 (Реагування на інциденти): На рівні 2 аналітики зосереджуються на ретельному вивченні найбільш критичних інцидентів безпеки, виявлених фахівцями з сортування, проводячи ретельну оцінку, використовуючи дані про загрози, такі як індикатори компрометації та оновлені правила. Їхні обов'язки поширюються на розуміння масштабу атаки та розуміння систем, які постраждали. На цьому рівні необроблені дані телеметрії атаки, зібрані на рівні 1, перетворюються на дієву інформацію про загрози. Фахівці з реагування на інциденти мають розробити та впровадити стратегії локалізації та відновлення після інцидентів. Якщо аналітик рівня 2 стикається зі значними труднощами в ідентифікації або пом'якшенні наслідків атаки, він може звернутися за допомогою до додаткових аналітиків рівня 2 або ескалувати інцидент до рівня 3.
- Рівень 3 (пошук загроз): Аналітики рівня 3 - це найдосвідченіші фахівці в SOC. Їхнє завдання полягає в управлінні серйозними інцидентами, які їм передають фахівці з реагування на інциденти. Крім того, вони контролюють або безпосередньо проводять оцінку вразливостей і тести на проникнення, щоб виявити потенційні вектори атаки. Їх основний обов'язок полягає у проактивному виявленні потенційних загроз, вразливостей безпеки та прогалин, які можуть бути неочевидними. Накопичуючи досвід щодо потенційних системних загроз, вони також надають рекомендації щодо оптимізації розгорнутих інструментів моніторингу безпеки. Крім

того, цей рівень відповідає за аналіз критичних сповіщень про загрози, розвідданих про загрози та інших даних про безпеку, наданих аналітиками рівнів 1 і 2.

- Керівник Операційного центру безпеки (SOC): Менеджери SOC відповідають за нагляд за командою операційної безпеки. Хоча вони надають технічні рекомендації, коли це необхідно, їхня основна відповідальність полягає в ефективному управлінні командою. Це включає в себе такі завдання, як підбір, навчання та оцінювання роботи членів команди, а також встановлення процесів, оцінювання звітів про інциденти, розробка та виконання планів комунікації в кризових ситуаціях, якщо це необхідно. Вони також здійснюють нагляд за фінансовими аспектами SOC, допомагають в аудиті безпеки та звітують перед директором з інформаційної безпеки (CISO) або іншими відповідними керівниками вищого рівня.

У менших за розміром SOC ролі передбачають ширші обов'язки, хоча вони, як правило, стають більш спеціалізованими в міру розширення SOC. Наприклад, у невеликому SOC з обмеженою кількістю аналітиків кожен з них повинен володіти кількома навичками, щоб вирішувати всі завдання, що виникають через обмеженість робочої сили. І навпаки, у більшому SOC ролі можуть бути більш чітко розподілені; наприклад, деякі аналітики можуть спеціалізуватися на моніторингу мережі, в той час як інші можуть стати експертами в конкретних аспектах функціональності Windows або Linux. Такий підхід має багато переваг, зокрема покращене та швидке реагування на загрози та ефективніший розподіл завдань.

2) **Виявлення та аналіз**

Велика кількість даних, накопичених на попередніх етапах, може виявитися складною навіть для досвідчених експертів і дослідників у сфері безпеки. Перетворення цих даних на практичні висновки досягається за допомогою аналізу даних, який, по суті, передбачає інтерпретацію зібраної інформації. Що стосується автоматизованого аналізу та виявлення, то існуюча література переважно заглиблюється в конкретні методи і технології аналізу та виявлення. Однак лише кілька статей розглядають цю тему з більш широкої, процедурної точки зору. Шляхом об'єднання існуючих процесів та впорядкування окремих кроків, описаних у літературі, було визначено низку процедурних кроків. Результатом є структурований процес, що складається з різних етапів:

- Виявлення: Інциденти виявляються або за допомогою людського спостереження, або за допомогою автоматизованих процесів, що вимагає визначення того, чи свідчать зібрані дані про порушення безпеки.
- Аналіз: Застосовуються різні методи аналізу, включаючи кореляцію джерела і цілі, структурний аналіз, функціональний аналіз і поведінковий аналіз. Автори пояснюють мету кореляції як здатність розчленовувати складні послідовності, генеруючи спрощені, консолідовані та точні події.
- Пріоритизація/сортування сповіщень: Пріоритезація оповіщень, яку також називають сортуванням, є життєво важливою ланкою у стримуванні, ліквідації та відновленні. Вона виконує дві основні задачі: по-перше, гарантує, що найбільш критичні інциденти отримають пріоритет, а по-друге, розподіляє інциденти для подальшого опрацювання на основі наявних ресурсів.

Управління та дотримання вимог. IT-управління контролює ефективне та результативне використання IT-систем шляхом встановлення стратегічних директив, формулювання стандартів, політик і процедур, а також їх впровадження. Комплаєнс, з іншого боку, гарантує, що організації дотримуються як зовнішніх правил, таких як галузеві стандарти та законодавчі вимоги, так і внутрішніх правил, включаючи політики та процедури компанії. Крім того, комплаєнс слугує важливим механізмом зворотного зв'язку для управління безпекою, демонструючи, як управлінські директиви перетворюються на практичне застосування.

1) **Стандарти та настанови**

Багато організацій наразі намагаються прийняти рішення щодо необхідності та особливостей впровадження СУБ. Однак бракує всеосяжних стандартів SOC або галузевих

керівних принципів, які б допомогли в цьому процесі прийняття рішень. Тим не менш, SOC може сприяти дотриманню певних нормативних вимог, тим самим забезпечуючи впевненість у дотриманні регуляторних норм.

Стандарти:

- ISO/IEC 27001
- NIST Cybersecurity Framework (CSF)
- NIST Special Publication 800-53
- MITRE ATT&CK Framework
- PCI DSS (Payment Card Industry Data Security Standard)
- ITIL (Information Technology Infrastructure Library)
- SANS Institute's Critical Security Controls (CSCs)
- GDPR (General Data Protection Regulation)

2) **Аудит безпеки та оцінка зрілості**

Регулярний аудит засобів контролю в рамках SOC є дуже важливим. HACA наводить приклад внутрішнього аудиту, проведеного в SOC, та його результати. Зовнішні оцінки незалежними сторонами зазвичай не проводяться через відсутність загальноприйнятих стандартів і керівних принципів. Тим не менш, в літературі існують методології для оцінки поточного рівня зрілості можливостей SOC та її загальної ефективності. Різні загальні моделі зрілості були порівняні і зведені до п'яти стадій зрілості спроможностей: неіснуюча, початкова, повторювана, визначений процес, проаналізований і оновлений, а також постійно оптимізований.

3) **Метрики**

Метрики слугують числовими орієнтирами, які використовуються для моніторингу та оцінки стану процесу або системи. Вони відіграють ключову роль у підтримці прийняття стратегічних рішень, забезпеченні якості та полегшенні тактичного контролю. У багатосайтових мережах метрики використовуються для оцінки стану безпеки окремих сайтів в режимі реального часу, що дозволяє виявляти потенційні загрози по всій мережі. Водночас зусилля з підвищення стійкості мережі передбачають оцінку програмного забезпечення для моделювання через призму показників відмовостійкості.

Висновок. Центри управління безпекою (SOC) відіграють життєво важливу роль у зміцненні стратегії кіберзахисту організації. Надаючи централізований центр для моніторингу, виявлення, аналізу та реагування на інциденти кібербезпеки, SOC дають змогу компаніям краще захищати свої цифрові активи та конфіденційну інформацію.

Однак створення ефективного SOC вимагає ретельного планування, впровадження та інтеграції в наявну інфраструктуру організації. Це передбачає визначення чітких цілей, розробку надійних політик і процедур, впровадження передових інструментів і технологій моніторингу, а також збір кваліфікованої команди фахівців з кібербезпеки.

Успіх SOC залежить від його здатності розвиватися й адаптуватися до загроз, що виникають, і мінливих вимог бізнесу. Регулярні оцінки та оцінювання допомагають визначити області для поліпшення, а постійне навчання та обмін знаннями гарантують, що персонал SOC буде в курсі останніх тенденцій і методів кібербезпеки.

При правильному впровадженні SOC значно розширюють можливості компанії запобігати кібератакам, зменшувати фінансові втрати і захищати від крадіжки особистих даних і витоку даних. Вони слугують механізмом превентивного захисту, даючи змогу організаціям виявляти і нейтралізувати загрози до того, як вони переростуть у повномасштабні інциденти безпеки.

На закінчення, хоча SOC відіграють важливу роль у посиленні захисту від кібербезпеки, їхня ефективність залежить від ретельного планування, реалізації та постійного вдосконалення. Віддаючи пріоритет інвестиціям у можливості SOC і формуючи культуру обізнаності та пильності в галузі кібербезпеки, компанії можуть краще захистити себе від постійно мінливого ландшафту кіберзагроз.

ЛІТЕРАТУРА

1. Security Operations Center: A Systematic Study and Open Challenges [Електронний ресурс] / M.Vielberth, F. Böhm, I. Fichtinger, G. Pernul // IEEE – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/9296846.
2. Security information and event management [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Security_information_and_event_management.
3. Information security operations center [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Information_security_operations_center.
4. Security operations center [Електронний ресурс] – Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Security_operations_center.
5. What is a Security Operations Centre? [Електронний ресурс] – Режим доступу до ресурсу: https://cmage.crest-approved.org/soc-critical-function.pdf.

6. Ayhan E. Modeling a Security Operations Center [Електронний ресурс] / E. Ayhan, M. Tannous – Режим доступу до ресурсу: https://www.diva-portal.org/smash/get/diva2:1703746/FULLTEXT01.pdf.

7. Wang J. Anatomy of a Security Operations Center [Електронний ресурс] / John Wang – Режим доступу до ресурсу: https://ntrs.nasa.gov/api/citations/20110011188/downloads/20110011188.pdf.

Kocheharov V. S. Bohomia V. I.

SECURITY OPERATIONS CENTRE (SOC)

«Security Operations Centres (SOCs) are the epitome of a modern cybersecurity strategy», offering a holistic approach to threat management when properly deployed. The combination of human expertise, procedural frameworks, technological infrastructure and regulatory compliance is the basis for effective SOC implementation. Their main goal is to proactively detect, intercept and mitigate potential cyber risks, thereby strengthening the overall security posture of an organisation. In academic discourse, SOC operations are often viewed through the lens of the People, Processes, and Technology (PPT) concept, which serves as a conceptual framework for understanding and optimising various aspects of information technology management. The SOC serves as the organisational core of an organisation's security strategy, bringing together processes, technology and personnel to enhance and manage security measures. The effectiveness of an SOC depends on several key factors, including the assignment of roles and responsibilities within the SOC, improved detection and analysis mechanisms to turn raw data into actionable information, and robust governance and compliance protocols to ensure compliance with regulatory requirements and internal standards. Standards and guidelines, security audits, maturity assessments and metrics are integral components of the SOC's work to drive continuous improvement and resilience.

Keywords*:* Security Operations Centres (SOCs) Threat detection Threat neutralisation Operational procedures Technological tools Management Security infrastructure Incident response People, processes and technology (PPT)