МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ**

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ МОНІТОРИНГУ Й РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ (SOC) В ОРГАНІЗАЦІЇ»

на здобуття освітнього ступеня бакалавра
зі спеціальності 125 Кібербезпека
освітньої програми Управління інформаційною та кібернетичною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро ЮНАК
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав(ла): здобувач(ка) вищої освіти гр. УБД-41

Дмитро ЮНАК
Ім'я, ПРІЗВИЩЕ

Керівник: Дмитро РАБЧУН
Доцент Ім'я, ПРІЗВИЩЕ

Рецензент:
К.т.н., доцент Ім'я, ПРІЗВИЩЕ

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти бакалавр

Спеціальність 125 Кібербезпека

Освітня програма Управління інформаційною та кібернетичною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
“____”_____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Юнаку Дмитру Олеговичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи “Оцінка ефективності системи моніторингу й реагування на інциденти безпеки (SOC) в організації”,
керівник кваліфікаційної роботи РАБЧУН Дмитро, к.т.н., доцент ,
(ІПРІЗВИЩЕ, Ім’я,, науковий ступінь, вчене звання)

затверджені наказом Державного університету інформаційно-комунікаційних технологій від “__“ березня 2024 р. №__.

2. Строк подання кваліфікаційної роботи “20” травня 2024р.

3. Вихідні дані до кваліфікаційної роботи: *Оцінка ефективності системи моніторингу й реагування на інциденти безпеки (SOC) в організації, наукова та технічна література.*

4. Перелік питань, які мають бути розроблені:
4.1. Дослідити теоретичні аспекти системи моніторингу й реагування на інциденти безпеки SOC.
4.2. Визначити сутність SOC як комплексної системи, що включає процеси моніторингу, виявлення та реагування на інциденти інформаційної безпеки.
4.3. Проаналізувати ключові показники ефективності SOC, такі як швидкість виявлення інцидентів та час реагування на них.
4.4. Оцінити ключові показники ефективності SOC в організації.

5. Перелік ілюстративного матеріалу: *презентація PowerPoint*

6. Дата видачі завдання

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Етапи кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	18.03.2024	
2.	Збір та аналіз літератури.	29.03.2024	
3.	Аналіз особливостей управління інформаційною безпекою підприємства	08.04.2024	
4.	Дослідження основних характеристик технологій формування обізнаності й навчання персоналу.	22.04.2024	
5.	Вивчення інструментів та методів формування обізнаності й навчання персоналу з інформаційної безпеки	08.05.2024	
6.	Формулювання висновків за результатами проведеного дослідження.	20.05.2024	
7.	Оформлення роботи.	22.05.2024	
8.	Оформлення презентації.	03.06.2024	
9.	Отримання рецензії на роботу.	03.06.2024	
10.	Захист в ДЕК.	__.06.2024	

Здобувачка вищої освіти _____ Дмитро ЮНАК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ на здобуття освітнього ступеня бакалавра

Направляється здобувачка Юнак Д.О. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
освітньої програми Управління інформаційною та кібернетичною безпекою
(назва)
на тему: "Оцінка ефективності системи моніторингу й реагування на інциденти безпеки (SOC) в організації ".

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач ЮНАК Дмитро у кваліфікаційній роботі дослідив теоретичні аспекти системи моніторингу й реагування на інциденти безпеки SOC. Визначив сутність SOC, як комплексної системи, що включає процеси моніторингу, виявлення та реагування на інциденти інформаційної безпеки. Проаналізував основні компоненти SOC. Оцінив ключові показники ефективності SOC в організації. Визначив, що середній час реагування на інциденти та кількість помилкових спрацювань є основними аспектами, що потребують покращення. Надав ряд рекомендацій для підвищення ефективності SOC, зокрема підвищення рівня автоматизації процесів, регулярне навчання персоналу та вдосконалення процедур моніторингу та звітності.

Все це дозволяє оцінити кваліфікаційну роботу здобувача ЮНАКА Дмитра на оцінку "відмінно" та присвоїти йому кваліфікацію бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"____" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Юнак Д.О. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри
управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну бакалаврську роботу

здобувача вищої освіти ЮНАКА Дмитра
на тему «Оцінка ефективності системи моніторингу й реагування на інциденти безпеки (SOC) в організації»

Актуальність. В сучасному цифровому світі зростає загроза кібератак і порушень безпеки. Системи моніторингу й реагування на інциденти безпеки SOC грають ключову роль у виявленні та запобіганні таким загрозам. Оцінка ефективності SOC допомагає організаціям зрозуміти, наскільки добре їх системи працюють. Ця оцінка включає аналіз часу від виявлення до реагування на інциденти, відповідність стандартам безпеки, якість збору та аналізу даних, а також здатність операційного центру безпеки адаптуватися до нових загроз. Правильна оцінка допомагає підвищити ефективність SOC і зменшити ризики для організації.

З огляду на зазначене оцінка ефективності системи моніторингу й реагування на інциденти безпеки SOC в організації є актуальним науковим завданням.

Позитивні сторони.

1. У кваліфікаційній роботі досліджено теоретичні аспекти системи моніторингу й реагування на інциденти безпеки SOC. Визначено сутність SOC, як комплексної системи, проаналізовано ключові показники ефективності операційного центру безпеки та оцінено ключові показники ефективності SOC в організації.

2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків.

4. За результатами дослідження запропоновано рекомендації для підвищення ефективності SOC, зокрема підвищення рівня автоматизації процесів, регулярне навчання персоналу та вдосконалення процедур моніторингу та звітності.

Недоліки.

Доцільно було б приділити більше уваги вивченню і класифікації програмних інструментів для оцінки ключові показники ефективності SOC в організації

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки “відмінно”, а здобувач ЮНАК Дмитро заслуговує присвоєння кваліфікації бакалавра з кібербезпеки за освітньою програмою Управління інформаційною та кібернетичною безпекою.

Рецензент:
к.т.н., доцент _____ *підпис* Ім’я, ПРІЗВИЩЕ

РЕФЕРАТ

Кваліфікаційна робота присвячена дослідженню оцінювання ефективності системи моніторингу й реагування на інциденти безпеки SOC в організації. Робота складається зі вступу, трьох розділів, що містять 4 рисунків, висновки і список використаних джерел із 40 найменувань. Загальний обсяг роботи становить 71 аркуші, з яких 5 аркушів займають перелік умовних скорочень та список використаних джерел.

Метою роботи є оцінювання ефективності системи моніторингу й реагування на інциденти безпеки SOC в організації.

Об'єктом дослідження є засади формування ефективної системи моніторингу й реагування на інциденти безпеки.

Предмет дослідження — особливості оцінювання ефективності системи моніторингу й реагування на інциденти безпеки.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації, експертної оцінки.

Як результат у роботі досліджено теоретичні аспекти системи моніторингу й реагування на інциденти безпеки SOC. Визначено сутність SOC як комплексної системи, що включає процеси моніторингу, виявлення та реагування на інциденти інформаційної безпеки. Проаналізовано основні компоненти SOC: технології, процеси та людські ресурси. Проаналізовано ключові показники ефективності SOC, такі як швидкість виявлення інцидентів та час реагування на них. Проведено оцінку ефективності поточного стану SOC в організації та оцінено ключові показники ефективності SOC. Додатково було надано ряд рекомендацій для ефективності SOC, зокрема підвищення рівня автоматизації процесів, регулярне навчання персоналу та вдосконалення процедур моніторингу та звітності.

Галузь застосування. Розроблені підходи можуть бути використані при впроваджені та реалізації системи моніторингу й реагування на інциденти безпеки

SOC в організації.

Ключові слова: ОПЕРАЦІЙНИЙ ЦЕНТР БЕЗПЕКИ, ІНЦИДЕНТИ БЕЗПЕКИ, РЕАГУВАННЯ НА ІНЦИДЕНТИ, УПРАВЛІННЯ ІНЦИДЕНТАМИ, ВИЯВЛЕННЯ ЗАГРОЗ, БЕЗПЕРЕРВНИЙ МОНІТОРИНГ, ОЦІНКА ЕФЕКТИВНОСТІ, ІНТЕГРАЦІЯ СИСТЕМ БЕЗПЕКИ, НАВЧАННЯ ПЕРСОНАЛУ, ВЗАЄМОДІЯ З ІНШИМИ ПІДРОЗДІЛАМИ.

ABSTRACT

The qualification work is devoted to the study of evaluating the effectiveness of the SOC security monitoring and incident response system in an organization. The work consists of an introduction, three chapters containing 4 figures, conclusions and the list of references containing 40 items. The total volume of the work is 71 pages, of which 5 pages are occupied by the list of abbreviations and the list of references.

The purpose of the study is to assess the effectiveness of the security incident monitoring and response system SOC in an organization.

The object the study is the principles of forming an effective system for monitoring and responding to security incidents.

The subject of the study is the peculiarities of evaluating the effectiveness of the security incident monitoring and response system.

Research methods. To solve the above scientific task, the methods of analysis and synthesis, comparison, classification, and expert evaluation were used.

As a result, the theoretical aspects of the security incident monitoring and response system SOC are investigated. The essence of SOC as an integrated system that includes the processes of monitoring, detecting and responding to information security incidents is defined. The main components of SOC are analyzed: technologies, processes and human resources. The key performance indicators of the SOC, such as incident detection rate and response time, are analyzed. The effectiveness of the current state of SOC in the organization is assessed and the key performance indicators of SOC are evaluated. Additionally, a number of recommendations for SOC effectiveness were provided, including increasing the level of process automation, regular staff training, and improving monitoring and reporting procedures.

Field of application. The developed approaches can be used in the implementation and implementation of the SOC security incident monitoring and response system in an organization.

Keywords: SECURITY OPERATIONS CENTER, SECURITY INCIDENTS, INCIDENT RESPONSE, INCIDENT MANAGEMENT, THREAT DETECTION,

CONTINUOUS MONITORING, PERFORMANCE EVALUATION, SECURITY SYSTEMS INTEGRATION, PERSONNEL TRAINING, INTERACTION WITH OTHER DEPARTMENTS.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

СУІБ	Система управління інформаційною безпекою
УІІБ	Управління інцидентами інформаційної безпеки
CAASM	Cyber Asset Attack Surface Management
DFIR	Digital Forensics and Incident Response
EDR	Endpoint Detection and Response
KPI	Key Performance Indicators
MTTD	Mean Time To Detect
MTTR	Mean Time To Repair
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOP	Standard Operating Procedures
SOAR	Security Orchestration Automation and Response
PDCA	Plan-Do-Check-Act
TIP	Threat Intelligence Platforms
XDR	Extended Detection and Response

ВСТУП

Актуальність теми. В сучасному цифровому світі зростає загроза кібератак і порушень безпеки. Системи моніторингу й реагування на інциденти безпеки SOC грають ключову роль у виявленні та запобіганні таким загрозам. Оцінка ефективності операційного центру безпеки допомагає організаціям зрозуміти, наскільки добре їхні системи працюють. Ця оцінка включає аналіз часу від виявлення до реагування на інциденти, відповідність стандартам безпеки, якість збору та аналізу даних, а також здатність SOC адаптуватися до нових загроз. Правильна оцінка допомагає підвищити ефективність і зменшити ризики для організації.

З огляду на зазначене оцінювання ефективності системи моніторингу й реагування на інциденти безпеки SOC в організації є актуальним науковим завданням.

Метою роботи є оцінювання ефективності системи моніторингу й реагування на інциденти безпеки SOC в організації.

Об'єктом дослідження є засади формування ефективності системи моніторингу й реагування на інциденти безпеки.

Предмет дослідження — особливості оцінювання ефективності системи моніторингу й реагування на інциденти безпеки.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити теоретичні аспекти системи моніторингу й реагування на інциденти безпеки SOC.
2. Визначити сутність SOC як комплексної системи, що включає процеси моніторингу, виявлення та реагування на інциденти інформаційної безпеки.
3. Проаналізувати ключові показники ефективності SOC, такі як швидкість виявлення інцидентів та час реагування на них.
4. Оцінити ключові показники ефективності SOC в організації.

Методи дослідження. Для вирішення зазначеного вище наукового завдання в роботі використані методи аналізу та синтезу, порівняння, класифікації.

Практичне значення отриманих результатів. Застосування напрацювань дасть змогу здійснити оцінювання ефективності системи моніторингу й реагування на інциденти безпеки. Таким чином визначиться доцільність та необхідність впровадження SOC в організаціях.

Апробація результатів кваліфікаційної роботи відбулася на Всеукраїнській науково-практичній конференції «Стратегії кіберстійкості: управління ризиками та безперервність бізнесу» 28 лютого 2024 року.

РОЗДІЛ 1 ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМИ МОНІТОРИНГУ Й РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ SOC

1.1 Сутність системи моніторингу й реагування на інциденти безпеки SOC

Операційний центр безпеки (Security Operations Center, SOC) покращує ефективність організації в розпізнаванні, відповіді та запобіганні загрозам шляхом уніфікації та координації всіх технологічних та операційних аспектів кібербезпеки.

SOC або операційний центр інформаційної безпеки — це команда професіоналів з інформаційної безпеки, яка виконує моніторинг IT-інфраструктури організації у режимі 24/7. Її мета — виявлення, аналіз та реагування на інциденти безпеки в реальному часі. Функції SOC включають підтримку безпеки мереж, систем та програмного забезпечення, а також активний захист від кіберзагроз.

Поза офісом SOC часто входить до складу послуг з керованої безпеки, які надаються постачальниками таких послуг. Використання або аутсорсинг SOC дозволяє уніфікувати та координувати систему безпеки організації, що призводить до поліпшення захисних заходів, виявлення загроз та реагування на них. Також це сприяє відповідності організації галузевим та міжнародним стандартам безпеки даних та підвищує довіру клієнтів.

Діяльність та обов'язки SOC поділяються на три загальні категорії.

I. Підготовка, планування та профілактика

- Інвентаризація активів.

Операційний центр безпеки має забезпечувати повний перелік усього, що потрібно захистити, як всередині, так і поза центром обробки даних (наприклад, програми, бази даних, сервери, хмарні сервіси, кінцеві точки тощо), а також всіх інструментів, що використовуються для їхнього захисту (брандмауери, антивіруси, захист від шкідливих програм, програм вимагачів, програмне

забезпечення для моніторингу і т.д.). Більшість SOC використовують спеціальні рішення для виявлення активів з цією метою.

- Регулярне обслуговування та підготовка.

З метою максимізації ефективності наявних інструментів і заходів безпеки, SOC виконує запобіжне обслуговування, таке як встановлення виправлень і оновлень програмного забезпечення, постійне оновлення брандмауерів, списків дозволів та блокувань, а також політик і процедур безпеки.

Крім того, операційний центр безпеки може створювати резервні копії системи або допомагати у встановленні політик та процедур резервного копіювання для забезпечення безперервності бізнесу у випадку витоку даних, атаки з вимогою викупу або іншого кібербезпекового інциденту.

- Планування реагування на інциденти.

SOC відповідає за розробку плану реагування організації на інциденти. Цей план визначає заходи, ролі та обов'язки у випадку загрози або інциденту, а також критерії оцінки успішності реагування на події.

- Регулярне тестування.

Команда SOC проводить оцінку вразливостей — це комплексне дослідження, яке визначає ступінь вразливості кожного ресурсу перед потенційними або новими загрозами, а також пов'язані з цим витрати.

Крім того, вони виконують тести на проникнення, що імітують конкретні атаки на одну або декілька систем. На основі результатів цих тестів команда вносить корективи або доповнює програми, політики безпеки, найкращі практики та плани реагування на інциденти.

SOC завжди слідкує за останніми рішеннями і технологіями в галузі кібербезпеки, а також останніми даними про загрози, новинами та інформацією про кібератаки і хакерів, які їх здійснюють, що збираються з соціальних мереж, галузевих джерел та даркнету.

II. Моніторинг, виявлення і реагування

- Безперервний, цілодобовий моніторинг безпеки.

Операційний центр безпеки відповідає за постійний моніторинг всієї розширеної IT-інфраструктури, такої як додатки, сервери, системне програмне забезпечення, обчислювальні пристрої, хмарні робочі середовища та мережі в режимі 24/7/365, з метою виявлення ознак відомих вразливостей та будь-якої підозрілої активності.

Більшість SOC для моніторингу, виявлення та реагування використовують систему управління інформаційною безпекою та подіями інформаційної безпеки (SIEM).

SIEM відслідковує та агрегує сповіщення та телеметричні дані від програмного та апаратного забезпечення в мережі у реальному часі, а потім аналізує ці дані для виявлення потенційних загроз. Недавно деякі SOC також почали використовувати технологію розширеного виявлення та реагування (XDR), яка забезпечує більш детальну телеметрію та моніторинг, а також дозволяє автоматизувати виявлення інцидентів та реагування на них.

- Управління журналами.

Управління журналами — це збір та аналіз даних журналів, які генеруються кожною мережевою подією та є важливою складовою частиною моніторингу. Більшість IT-відділів збирають дані журналів, а саме аналіз визначає нормальну або базову активність і виявляє аномалії, які можуть вказувати на підозрілу активність. Багато хакерів розраховують на те, що компанії не завжди аналізують дані журналів, що може дозволити їхнім вірусам і шкідливим програмам працювати непомічено. Більшість рішень SIEM включають функцію керування журналами.

- Виявлення загроз.

Команда SOC відокремлює сигнали від шуму, тобто ознак реальних кіберзагроз і хакерських атак від помилкових викликів, потім сортує загрози за ступенем серйозності. Сучасні рішення SIEM включають штучний інтелект,

який автоматизує ці процеси та вдосконалюється на основі даних для кращого виявлення підозрілої активності.

- Реагування на інциденти.

Для зменшення наслідків загрози або реального інциденту, SOC застосовує низку заходів. Ці заходи можуть включати:

- Проведення розслідування, щоб встановити причини, що лежать в основі інциденту, включаючи технічні вразливості, які дозволили зловмисникам отримати доступ до системи, а також інші фактори, такі як слабка безпека паролів або недотримання політик безпеки.
- Відключення скомпрометованих кінцевих точок або їхнє відключення від мережі.
- Ізоляція скомпрометованих частин мережі або перенаправлення мережевого трафіку.
- Призупинення або завершення роботи скомпрометованих програм або процесів.
- Вилучення пошкоджених або заражених файлів.
- Запуск антивірусного або антишпіонського програмного забезпечення.
- Зміна паролів для внутрішніх та зовнішніх користувачів.

Багато рішень XDR дозволяють SOC автоматизувати і прискорити ці та інші методи реагування на інциденти.

III. Відновлення, доопрацювання та дотримання вимог

- Відновлення та усунення наслідків.

Після виявлення інциденту SOC негайно приймає заходи для припинення загрози і приступає до відновлення пошкоджених активів до їхнього попереднього стану (наприклад, очищення, відновлення та повторне підключення дисків, користувацьких пристроїв та інших кінцевих точок, відновлення мережевого трафіку, перезапуск додатків та процесів). У випадку витоку даних або атаки вірусу-вимагача, процес відновлення може також

включати перехід на резервні системи та скидання паролів і облікових даних для автентифікації.

- Аналіз і вдосконалення.

З метою запобігання повторенню інциденту SOC аналізує отриману під час інциденту інформацію для кращого усунення вразливостей, оновлення процесів і політик, вибору нових інструментів кібербезпеки або перегляду плану реагування на інцидент. На більш високому рівні команда SOC також вивчає, чи є інцидент частиною ширшої тенденції в сфері кібербезпеки, на яку необхідно реагувати.

- Виконання вимог щодо відповідності.

Операційний центр безпеки забезпечує відповідність всіх систем і процесів безпеки вимогам нормативних актів щодо захисту даних, таким як GDPR (General Data Protection Regulation), CCPA (California Consumer Privacy Act), PCI DSS (Payment Card Industry Data Security Standard) та HIPAA (Health Insurance Portability and Accountability Act). Після інциденту SOC переконується, що всі зацікавлені сторони, включаючи користувачів, регуляторів та правоохоронні органи будуть повідомлені згідно з нормативними вимогами і що необхідні дані будуть збережені для подальшого аналізу та аудиту.

SOC пропонує різноманітні переваги організаціям, включаючи:

- ✓ Шляхом активного моніторингу та швидкого реагування операційний центр безпеки сприяє запобіганню несанкціонованому доступу та зниженню ризику витоку даних, що забезпечує захист критичних систем та конфіденційних даних.
- ✓ Знижуючи кількість інцидентів безпеки та їхній вплив, SOC гарантує безперервність бізнес-операцій, що сприяє підтримці продуктивності, потоків доходів та задоволення клієнтів.
- ✓ Операційний центр безпеки допомагає організаціям відповідати нормативним вимогам у сфері кібербезпеки, впроваджуючи ефективні заходи безпеки та ведучи облік інцидентів і реагування на них.

- ✓ Інвестиції в проактивні заходи безпеки через SOC можуть забезпечити значну економію коштів шляхом запобігання витоку даних і кібератак, мінімізуючи фінансові втрати та ризики для репутації.
- ✓ Послуги операційного центру безпеки, спрямовані на підвищення рівня кібербезпеки, сприяють збільшенню довіри серед клієнтів та зацікавлених сторін.
- ✓ Швидке реагування SOC допомагає зменшити час простою та фінансові втрати, стримуючи загрози та швидко відновлюючи нормальну роботу.
- ✓ Аналізуючи події та тенденції у сфері безпеки, операційний центр безпеки виявляє потенційні вразливості організації та вживає проактивних заходів для їхнього усунення.
- ✓ Постійний моніторинг мереж і систем дозволяє SOC швидше виявляти та зменшувати загрози безпеки, що мінімізує потенційні збитки та витоки даних.

Слід зазначити, що операційний центр безпеки складається не лише з технічних систем, які надсилають аналітичні дані в реальному часі, а й з кваліфікованих експертів, здатних відрізнити справжні події від помилкових, а також визначити можливі взаємозв'язки між різними повідомленнями.

Головні ролі в команді SOC:

- Керівник SOC

Він відповідає за управління командою, контроль за всіма операціями з безпеки та представлення звітності перед CISO (керівником інформаційної безпеки) в організації.

- Інженери з безпеки

Ці фахівці забезпечують розробку та управління архітектурою безпеки організації. Вони займаються оцінкою, тестуванням, рекомендаціями, впровадженням і підтримкою інструментів та технологій безпеки. Крім того, вони співпрацюють з командами розробників або DevOps/DevSecOps, щоб

впевнитися, що архітектура безпеки організації включена в цикли розробки додатків.

- Аналітики безпеки

Ці спеціалісти, також відомі як дослідники безпеки або фахівці з реагування на інциденти, виявляють, розслідують і реагують на загрози або інциденти кібербезпеки. Вони визначають пріоритетність загроз, ідентифікують постраждалих користувачів та системи і вживають заходів для пом'якшення наслідків загроз або інцидентів.

- Мисливці за загрозами

Мисливці за загрозами, яких також називають експертними аналітиками безпеки або SOC-аналітиками, спеціалізуються на виявленні та стримуванні сучасних загроз, які уникають виявлення автоматизованими засобами захисту. Їх також називають експертами з безпеки або аналітиками SOC.

У складі команди SOC можуть бути інші фахівці, залежно від розміру організації або специфіки галузі. У великих компаніях може бути спеціаліст з реагування на інциденти, який координує комунікацію та організовує реагування на інциденти. Також деякі SOC можуть включати криміналістів, які спеціалізуються на зборі доказів з пристроїв, що пошкоджені або скомпрометовані в результаті кіберінциденту.

SOC щодня успішно протидіє новим викликам загроз інформаційної безпеки.

Дані загрози і рішення наведені в табл.1.1.

Таблиця 1.1.

Рішення загрозам інформаційної безпеки

Загрози інформаційної безпеки	**Рішення**
Мережевий захист є ключовим компонентом стратегії кібербезпеки організації. Він потребує особливої уваги, оскільки досвідчені зловмисники мають інструменти та ноу-хау, необхідні для того, щоб обійти	Впровадження інструментів, які мають функції виявлення аномалій та/або машинного навчання і можуть виявляти нові загрози.

традиційні засоби захисту, такі як брандмауери та засоби захисту кінцевих точок.	
Обсяг мережевого трафіку та даних, якими оперує середньостатистична організація, величезний. З таким астрономічним зростанням обсягу даних і трафіку зростають труднощі з аналізом всієї цієї інформації в режимі реального часу.	SOC покладаються на автоматизовані інструменти для фільтрації, аналізу, агрегування та кореляції інформації, щоб звести ручний аналіз до мінімуму.
У багатьох системах безпеки аномалії виникають з певною регулярністю. Якщо SOC покладається на нефільтровані сповіщення про аномалії, то дуже легко перевантажитися великою кількістю сповіщень. Багато сповіщень можуть не надавати контекст і дані, необхідні для розслідування, відволікаючи команди від реальних проблем.	Налаштування контент моніторингу та ранжування оповіщень, щоб розрізняти оповіщення з низьким рівнем точності та оповіщення з високим рівнем точності. Додаткове використання інструментів поведінкової аналітики, для переконання, що команда SOC в першу чергу зосереджується на найбільш незвичайних оповіщеннях.
Кінцеві точки та брандмауери не можуть ідентифікувати невідому загрозу за допомогою звичайних засобів виявлення на основі сигнатур.	SOC можуть вдосконалити свої рішення для виявлення загроз на основі сигнатур, правил і порогових значень, впровадивши поведінкову аналітику для виявлення незвичної поведінки.
Намагаючись відстежити кожну можливу загрозу, багато організацій купують кілька інструментів безпеки. Ці інструменти часто не пов'язані між собою, мають обмежену сферу застосування і не є достатньо досконалими для виявлення складних загроз.	Потрібно зосередитися на ефективних контрзаходах за допомогою централізованої платформи моніторингу та сповіщення.

1.2 Організація системи моніторингу й реагування на інциденти безпеки (SOC)

Зазвичай, керівник компанії, побачивши загрози в інформаційній безпеці або почувши історії про атаки на інші компанії, може вирішити впровадити операційний центр безпеки, що буде відслідковувати та реагувати на кіберзагрози. Цей підрозділ, який є постійним або навіть цілодобовим, може бути створений власноруч, або компанія може звернутися до зовнішнього SOC для отримання послуг забезпечення безпеки.

Внутрішній SOC — це частина компанії, яка складається з внутрішнього персоналу, зазвичай з фахівців в галузі IT та інформаційної безпеки. Однак такий SOC може собі дозволити лише велика корпорація через високі витрати і потребу у кваліфікованому персоналі.

Зовнішній SOC складається з експертів з інформаційної безпеки, які працюють на компанію, як зовнішні постачальники послуг. Такий підхід дозволяє компанії заощадити на власних співробітниках і повністю покладатися на фахівців зовнішнього SOC, які виконують свою роботу відповідно до умов договору обслуговування.

Для ефективного впровадження та функціонування центру оперативного реагування на інциденти безпеки, потрібно чітко визначити основні потреби організації, де планується використання SOC.

У більшості випадків, компанії проводять внутрішній аудит і виявляють наявні активи, які приносять найбільшу вигоду і потребують додаткового захисту від скоєння кібератак.

Важливо зазначити, що для доцільного використання SOC, організація має чітко сформулювати потреби і перед впровадженням оперативного центру реагування виконати наступні вимоги:

1. Оцінити наявний рівень загроз безпеці своїх ресурсів, провести пошуки та проаналізувати історію інцидентів інформаційної безпеки, надати відомості про наявні загрози у всьому периметрі організації та сформувати загальний рівень

ризиків для бізнесу.

2. Визначити обсяг важливих даних і ресурсів, які потребують постійного моніторингу та захисту.

3. Сформувати перелік бажаних технологічних рішень, систем моніторингу, рішень та інших інструментів безпеки для ефективного реагування на інциденти.

4. Найняти кваліфікований персонал, який здатний виявляти та реагувати на потенційні загрози. Команда має містити аналітиків безпеки, інженерів з безпеки мережі, аналітиків загроз, інцидент-менеджерів та інших спеціалізованих фахівців.

5. Оцінити бюджет, який організація може приділити для впровадження та підтримки SOC.

6. Визначитися зі своїми стратегічними цілями, щоб ефективно покрити свої потреби та досягти мети за допомогою оперативного центру реагування на інциденти.

Після з'ясування стратегії, потреб і специфіки організації, впровадження SOC є цілком доцільним та принесе максимальну користь.

1.3 Інструменти та технології, що використовуються в SOC

Від постановки цілей до впровадження ефективних процедур — кожен етап складний і лякаючий, особливо при ручному просіюванні журналів, відкладанні реагування на інциденти і вирішенні проблем з масштабуванням.

Використання інструментів SOC значно покращує загальний стан безпеки завдяки автоматизації, безперервному моніторингу, виявленню загроз у режимі реального часу та можливостям реагування на інциденти. На ринку представлено багато чудових варіантів, і вибір найкращого для організації залежить від конкретних потреб і бюджету.

Найкращі SOC-інструменти для бізнесу:

1. Платформи розвідки загроз (Threat intelligence platforms,TIP)

Основна перевага TIPs полягає в їхньому фокусі на обробці та візуалізації даних. Замість простого відображення сирої інформації, вони вдало поєднують та контекстуалізують дані, що дозволяє отримати глибше розуміння потенційних загроз. Ці рішення перетворюють складні дані на зрозумілі інформаційні панелі та звіти, що значно полегшує розуміння загальної картини загроз.

TIPs здатні збирати та узагальнювати дані щодо потенційних загроз із різноманітних джерел, включаючи:

- Розвідка з відкритих джерел (OSINT):

Новини, соціальні мережі та хакерські форуми дають цінну інформацію про тактику зловмисників та їхні розмови.

- Комерційні канали загроз:

Оновлення в реальному часі про відомі вразливості, сигнатури шкідливих програм і нові загрози.

- Дані про внутрішні загрози:

Інциденти безпеки компанії, журнали та спостереження.

Найкращими платформами для аналізу загроз є VirusTotal, Cisco Talos, Microsoft Defender Threat Intelligence, AlienVault Open Threat Exchange (OTX), AbuseIPDB та OpenTAXII.

2. Інструменти виявлення та реагування на кінцеві точки (EDR)

EDR (Endpoint Detection and Response) системи спостерігають за кінцевими точками, такими як персональні комп'ютери та сервери, з метою виявлення потенційно шкідливої активності. Крім того, їх можна використовувати для проведення розслідувань та реагування на інциденти. EDR мають важливі переваги порівняно з традиційним антивірусним програмним забезпеченням, і ось чому:

- Поведінковий аналіз:

Вони відстежують і аналізують поведінку файлів та програм, шукаючи підозрілі дії: несанкціонований доступ, модифікації реєстру або підозрілі мережеві з'єднання.

- Централізоване управління:

Можна легко керувати та контролювати EDR на всіх кінцевих точках з однієї центральної консолі, забезпечуючи цілісне уявлення про систему безпеки компанії.

Найкращими інструментами EDR є CrowdStrike Falcon Insight, SentinelOne Singularity Platform, Microsoft Defender, Elastic та Qradar EDR.

3. Інструменти розширеного виявлення та реагування (XDR)

XDR — це старший брат EDR. У той час як EDR фокусується на окремих кінцевих точках, таких як ноутбуки та сервери, XDR використовує більш широкий та інтегрований підхід. Ось що робить інструмент унікальним:

- Об'єднання даних з різних джерел:

EDR аналізує кінцеві точки, а XDR витягує дані з усього стеку безпеки і дає повну картину того, що відбувається у мережі, а не лише окремі біти та фрагменти.

- Кореляція подій:

Замість простого перегляду окремих сповіщень, XDR встановлює зв'язки між ними. Він виявляє закономірності та підозрілі дії, які можуть залишитися непоміченими, наприклад, зв'язок шкідливого програмного забезпечення з незнайомим сервером або незвичні спроби входу на різних пристроях.

- Автоматизація реагування:

XDR не лише реагує на загрози пасивно, а може автоматично виконувати попередньо визначені дії залежно від типу загрози, наприклад, ізолювати заражені пристрої або блокувати підозрілий мережевий трафік. Це зберігає час і перешкоджає зловмисникам завдати шкоди.

Найкращими інструментами XDR є CrowdStrike Falcon XDR, Palo Alto Networks Cortex XDR, Trend Micro Vision One, Cisco XDR та SentinelOne Singularity Platform.

4. Інструменти управління інформацією та подіями безпеки (SIEM)

SIEM пропонує централізовану систему для контролю та керування інформацією, що стосується безпеки, отриманої з різних джерел в IT-середовищі організації. Ця система збирає та аналізує дані з різних джерел безпеки, таких як брандмауери, системи виявлення вторгнень і рішення для захисту кінцевих точок.

Ці дані можна використовувати для виявлення непередбачуваних дій та потенційних загроз. Інструменти SIEM відіграють ключову роль у забезпеченні кібербезпеки, виконуючи такі функції:

- Збір логів.

Агрегування даних журналів з різних мережевих пристроїв, систем і додатків.

- Нормалізація та кореляція.

Виявлення закономірностей та аномалій шляхом мапування різноманітних даних у стандартний формат.

- Сповіщення.

Генерування сповіщень в режимі реального часу про підозрілі дії, що дозволяє оперативно проводити розслідування.

- Управління комплаєнсом.

Допомога у виконанні нормативних вимог за допомогою можливостей звітності та аудиту.

- Аналітика поведінки користувачів і організацій.

Дослідження поведінки користувачів та організацій для виявлення аномалій або ознак компроментації.

Найкращими інструментами SIEM є Splunk, IBM QRadar SIEM, LogRhythm SIEM, Securonix Unified Defense SIEM та Elastic SIEM.

5. Інструменти цифрової криміналістики та реагування на інциденти (DFIR)

DFIR, або Цифрове розслідування інцидентів та відновлення, охоплює область цифрової криміналістики, що спрямована на збір та аналіз електронних доказів. Це також включає реагування на інциденти, що передбачає системний підхід до керування та пом'якшення наслідків інцидентів безпеки в межах плану реагування на інциденти. Основний акцент порівняно з виявленням першопричин інцидентів полягає в оцінці ступеня компрометації та розробці стратегій для зменшення та усунення впливу на інформаційні системи та дані. Інструменти

DFIR володіють численними перевагами, серед яких:

- Автоматизований збір даних та розширений аналіз (аналіз пам'яті, виявлення шкідливого програмного забезпечення та дослідження першопричин)
- Цілісність доказів для суду завдяки безпечному зберіганню та відстеженню ланцюга постачання
- Проактивне полювання на загрози
- Координація реагування на інциденти
- Швидше локалізація та усунення загрози
- Скорочення часу на розслідування
- Підвищення рівня безпеки

Найкращими інструментами DFIR є OpenText EnCase Forensic, Autopsy, The Sleuth Kit, Wireshark, Mandiant's Redline, Exterro Forensic Security Toolkit (FTK), Cellebrite UFED (Universal Forensic Extraction Device) та Sysmon.

6. Сканери вразливостей

Сканери вразливостей призначені для виявлення відомих вразливостей програмного забезпечення, які можуть бути використані зловмисниками.

Основні переваги, які вони забезпечують:

- Краща видимість

Сканери забезпечують всебічний огляд вразливостей IT-інфраструктури, включаючи мережі, системи та програмне забезпечення.

- Покращене виявлення загроз та визначення пріоритетів

Вони аналізують ваше оточення на предмет наявності відомих вразливостей і готують докладні звіти про їхню серйозність, можливу експлуатацію та потенційний вплив.

- Покращене полювання на загрози та реагування на інциденти

Сканери вразливостей можуть інтегруватися з іншими інструментами безпеки, щоб надавати цінну інформацію для виявлення загроз та реагування на інциденти. Аналізуючи дані про вразливості разом з іншими подіями, пов'язаними з безпекою, команди SOC можуть виявити закономірності та зв'язки, які можуть залишитися непоміченими.

- Скорочення часу на виправлення:

Вони надають інформацію про те, як усунути виявлені вразливості, заощаджуючи командам SOC цінний час і зусилля.

- Покращена відповідність вимогам

Багато законодавчих актів і нормативних документів вимагають від організацій регулярно проводити перевірку своїх систем. Сканери вразливостей допомагають команді SOC продемонструвати відповідність вимогам, надаючи готові до аудиту звіти про виявлені слабкі місця та процес їх усунення.

- Економічна ефективність

Це вигідна інвестиція порівняно з потенційними витратами на успішну кібератаку.

Найкращими сканерами вразливостей є Tenable, Qualys, Greenbone та Rapid7 InsightVM.

7. Інструменти управління запасами активів

Управління активами включає постійний контроль та відстеження активів організації, охоплюючи як матеріальні, так і цифрові ресурси. Цей процес включає ідентифікацію, реєстрацію та оновлення даних про активи протягом їхнього життєвого циклу. Використання такого програмного забезпечення є важливим для оптимізації ресурсів, забезпечення відповідності та підвищення рівня безпеки.

Ефективне управління інвентаризацією активів має кілька переваг:

- Можливість швидко ідентифікувати уражені системи, відстежити шляхи атаки та зрозуміти потенційний масштаб порушення. Знання критичності активів та пов'язаних з ними вразливостей допоможе компніям визначити пріоритетність виправлень та заходів з мінімізації ризиків.
- Інструменти автоматизації можуть автоматично виявляти та оновлювати інформацію про активи, звільняючи час аналітиків для більш стратегічних завдань, таких як аналіз загроз та реагування на інциденти.
- Інформація, отримана з даних інвентаризації активів, може допомогти у розробці політики безпеки та оцінці ризиків.

- Добре проведена інвентаризація забезпечує задокументований облік активів компанії, що є корисним для внутрішнього аудиту та зовнішніх перевірок на відповідність вимогам.
- Виявляючи некеровані пристрої та несанкціоноване програмне забезпечення, можна мінімізувати ризики, пов'язані з тіньовими IT.
- ✓ Найкращими інструментами для управління інвентаризацією активів є Ivanti, Freshservice та Asset Panda.

8. Інструменти управління поверхнею атаки на кібер-активи (CAASM)

Інструменти CAASM надають можливість IT та відділу безпеки отримати повний огляд внутрішніх та зовнішніх активів. Вони легко інтегруються з існуючими інструментами та об'єднують дані. За допомогою даних рішень можливо:

- Отримати повну видимість, не залишаючи місця для прихованих вразливостей.
- Встановити масштаби вразливостей у всьому цифровому ландшафті.
- Проаналізувати та визначити пріоритетність загроз, зрозуміти їхню серйозність та потенційний вплив.
- Спрямувати ресурси на усунення найкритичніших загроз у першу чергу, щоб забезпечити максимальну ефективність.
- Вжити рішучих заходів для усунення вразливостей, впровадження засобів контролю безпеки та зменшення ризиків.
- Посилити кібербезпеку шляхом постійного моніторингу та аналізу поверхні атак і передбачення потенційних загроз до того, як вони відбудуться.
- Знизити ризики, пов'язані з тіньовими IT, виявляючи некеровані пристрої та несанкціоноване програмне забезпечення.
- ✓ Найкращими інструментами CAASM є Lansweeper, Axonius Platform, Armis Centrix та runZero.

1.4 Люди, як один з головних компонентів SOC

Розвиток персоналу, збереження співробітників та приваблення талантів є критичними складовими успішного SOC. Висококваліфікована та вмотивована команда відіграє ключову роль у забезпеченні надійної безпеки та ефективного реагування на інциденти.

Role	Description	Skills	Responsibilities
Tier 1 **Security Analyst**	**Triage Specialist** (Separating the wheat from the chaff)	Sysadmin skills (Linux/Mac/ Windows); programming skills (Python, Ruby, PHP, C, C#, Java, Perl, and more); security skills (CISSP, GCIA GCIH, GCFA, GCFE, etc.)	Reviews the latest alerts to determine relevancy and urgency. Creates new trouble tickets for alerts that signal an incident and require Tier 2 / Incident Response review. Runs vulnerability scans and reviews vulnerability assessment reports. Manages and configures security monitoring tools (IDS, correlation rules, etc.).
Tier 2 **Security Analyst**	**Incident Responder** (IT's version of the First Responder)	All of the above + natural ability, dogged curiosity to get to the root cause, and the ability to remain calm under pressure. Being a former white hat hacker is also a big plus.	Reviews trouble tickets generated by Tier 1 Analyst(s). Utilizes emerging threat intelligence (IOCs, updated rules, etc.) to identify affected systems and the scope of the attack. Reviews and collects asset data (configs, running processes, etc.) on these systems for further investigation. Determines and directs remediation and recovery efforts.
Tier 3 **Expert Security Analyst**	**Threat Hunter** (Hunts vs. defends)	All of the above + familiar with using data visualization tools and penetration testing tools.	Reviews asset discovery and vulnerability assessment data. Explores ways to identify stealthy threats that may have found their way inside your network, without your detection, using the latest threat intelligence. Conducts penetration tests on production systems to validate resiliency and identify areas of weakness to fix. Recommends how to optimize security monitoring tools based on threat-hunting discoveries.
Tier 4 **SOC Manager**	**Operations and Management** (Chief Operating Officer for the SOC)	All of the above + strong leadership and communication skills	Supervises the activity of the SOC team. Recruits, hires, trains, and assesses the staff. Manages the escalation process and reviews incident reports. Develops and executes crisis communication plan to CISO and other stakeholders. Runs compliance reports and supports the audit process. Measures SOC performance metrics and communicates the value of security operations to business leaders.

Рис.2.1. Основні ролі в SOC

Tier 1 (Triage Specialist) / Рівень 1 (Спеціаліст з сортування): Відповідальний за акумулювання необроблених даних та перевірку сигналізації і сповіщень. Їх потрібно оцінити, визначити або відрегулювати ступінь критичності сповіщень та збагатити їх відповідними даними. Кожне сповіщення перевіряється фахівцем з сортування для визначення його обґрунтованості або помилкового позитивного результату. Додатковим обов'язком на цьому рівні є виявлення інших подій високого ризику та потенційних інцидентів. Усі ці завдання мають бути пріоритетизовані відповідно до їхньої важливості. Якщо проблеми не можуть бути вирішені на даному рівні, вони передаються

аналітикам рівня 2. Крім того, спеціалісти з сортування часто керують та налаштовують засоби моніторингу.

Tier 2 (Incident Responder) / Рівень 2 (Реагування на інциденти): Аналітики переглядають більш серйозні інциденти безпеки, які потрапили в їхню компетенцію через ескалацію з рівня 1 і проводять більш детальну оцінку за допомогою аналізу загроз (індикатори компрометації, оновлені правила і т. д.). Вони повинні мати розуміння масштабу атаки та знати про вплив на уражені системи. Необроблені дані телеметрії про атаки, зібрані на рівні 1, перетворюються на конкретні дані про загрози на цьому рівні. У випадку, якщо виниклі проблеми не можуть бути вирішені на цьому рівні, вони передаються аналітикам рівня 3.

Tier 3 (Threat Hunter) / Рівень 3 (Мисливець за загрозами)

Аналітики на рівні 3 є найбільш досвідченою командою у SOC. Вони вирішують основні інциденти, що передаються їм від служб реагування на інциденти. Також вони проводять або керують оцінкою вразливостей та тестуванням на проникнення для виявлення потенційних векторів атаки. Їхнє головне завдання — проактивно виявляти можливі загрози, прогалини у безпеці і вразливості, які можуть залишатися невідомими. Вони також мають рекомендувати шляхи для оптимізації моніторингу безпеки. Крім того, будь-які критичні сповіщення про безпеку, аналізи загроз та інші дані про безпеку, які надаються аналітиками на рівнях 1 і 2, повинні бути перевірені на цьому рівні.

Керівник SOC / Менеджер SOC

Керівники SOC відповідають за керівництво командою забезпечення безпеки. Вони забезпечують технічне керівництво за необхідності, проте головне завдання — ефективне управління командою. Це включає процеси найму, навчання та оцінки членів команди, розробку процедур, аналіз звітів про інциденти, а також створення та впровадження планів комунікації у кризових ситуаціях. Вони також відповідають за фінансові аспекти SOC, підтримують аудити безпеки та подають звіти керівництву, такому як директор з інформаційної безпеки (CISO) або аналогічній вищій керівній посаді.

Technical roles / Технічні ролі

В сфері безпеки існує різноманіття додаткових спеціалістів, які співпрацюють з аналітиками SOC для забезпечення ефективної роботи центру. Однією з ключових ролей у цій групі є інженер безпеки (ІБ). Інженери безпеки відповідають за розробку, інтеграцію та підтримку інструментів SOC, а також визначення вимог до нових інструментів. Вони забезпечують адекватний рівень доступу до систем інструментів. Додатковими обов'язками є налаштування та встановлення брандмауерів і систем виявлення/попередження вторгнень. Крім цього, вони сприяють у написанні та оновленні правил виявлення для систем безпеки інформації та управління подіями (SIEM).

Висновки до розділу 1

В даному розділі ретельно розглянуто теоретичні засади системи моніторингу й реагування на інциденти безпеки SOC, що є важливим компонентом інформаційної безпеки сучасних організацій. Було досліджено основні поняття, принципи роботи SOC, а також важливі функції, які він виконує.

Можна зробити висновок, що ефективна система моніторингу та реагування на інциденти безпеки є критичною для забезпечення захисту інформаційних активів організації від різноманітних кіберзагроз. Добре налагоджений SOC дозволяє виявляти, аналізувати та вчасно реагувати на потенційні загрози, що дозволяє зменшити ризики і втрати.

Розділ 2 КЛЮЧОВІ ПОКАЗНИКИ ЕФЕКТИВНОСТІ СИСТЕМИ МОНІТОРИНГУ Й РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ SOC

2.1 Швидкість виявлення інцидентів

На сьогоднішній день наявні високі вимоги до безпеки даних та інформаційних ресурсів. У цьому контексті служби центрів операційної безпеки (SOC) стають першою лінією оборони від кіберзагроз. Усе більш зростаюча кількість кіберзагроз вимагає оперативної реакції та ефективного контролю для запобігання серйозним наслідкам для організацій та їхніх даних. Швидке виявлення інцидентів стає важливим фактором у забезпеченні безпеки та захисту інформації.

Швидке виявлення та реагування на інциденти в SOC має декілька ключових переваг. Перш за все, це дозволяє мінімізувати час, протягом якого зловмисники можуть шкодити системам та даним організації. Чим швидше виявлено та зупинено інцидент, тим менше можливостей для розповсюдження атаки та завдання шкоди.

Крім того, швидке реагування дозволяє зменшити витрати організації, пов'язані з відновленням після кібератаки. Чим швидше інцидент виявлено та припинено, тим менше часу і грошей потрібно на відновлення роботи систем та компенсацію збитків.

Швидкість виявлення інцидентів в SOC залежить від декількох ключових факторів, включаючи використання технологій, навичок персоналу та ефективність процесів.

Перший і один з найважливіших аспектів швидкого виявлення інцидентів в SOC — це використання передових технологій та інструментів. Сучасні системи моніторингу базуються на штучному інтелекті, машинному навчанні та аналізі великих обсягів даних. Ці системи здатні автоматично виявляти незвичайну або підозрілу активність в мережі та повідомляти про неї персоналу SOC для подальшого аналізу та реагування. Використання цих передових технологій

дозволяє значно зменшити час, потрібний для виявлення інцидентів, і вчасно реагувати на потенційні загрози.

Другим важливим аспектом є навички та кваліфікація персоналу SOC. Висококваліфіковані фахівці з кібербезпеки здатні швидко виявляти та аналізувати підозрілу активність, роблячи швидкі та обґрунтовані висновки щодо можливих загроз. Додатково, постійне навчання та підвищення кваліфікації персоналу дозволяє вони бути в курсі останніх тенденцій у світі кібербезпеки та ефективно використовувати нові технології та методи для виявлення інцидентів.

Ефективність процесів також відіграє важливу роль у швидкому виявленні інцидентів в SOC. Це включає ретельне планування та організацію робочих процесів, швидку передачу інформації між різними членами команди SOC та встановлення чітких процедур для реагування на інциденти. Ефективність процесів дозволяє мінімізувати час від виявлення інциденту до прийняття відповідних заходів для його усунення.

У підсумку, швидкість виявлення інцидентів в SOC є критично важливою для забезпечення безпеки та захисту даних та інформаційних ресурсів організації. Шляхом використання передових технологій, висококваліфікованого персоналу та ефективних процесів, SOC може швидко реагувати на кіберзагрози та запобігати серйозним наслідкам для бізнесу. Виявлення інцидентів в SOC — це не просто виклик, але і можливість підвищити рівень кібербезпеки та довіру в організації.

2.2 Час реагування на інциденти

Перед вирішенням, як реагувати на інцидент, необхідно чітко зрозуміти, що саме вважається інцидентом. У сфері IT існують три терміни, які іноді використовуються взаємозамінно, але мають різні значення.

Подія — це дія, яка, зазвичай, не має наслідків, наприклад, створення файлу, видалення папки або відкриття електронного листа. Сама за себе подія

рідко є ознакою порушення, але в поєднанні з іншими подіями може вказувати на загрозу.

Оповіщення — це сповіщення, що ініційоване певною подією, яка може або не може представляти загрозу.

Інцидент — це група взаємопов'язаних оповіщень, які люди або автоматичні засоби визнали як потенційну загрозу. Кожне оповіщення може не бути серйозною загрозою, але разом вони вказують на можливе порушення безпеки.

Реагування на інциденти — це набір дій, які виконує організація у випадку, якщо вона вважає, що IT-системи або дані можуть бути пошкоджені. Наприклад, фахівці з безпеки вживають заходи, якщо вони помічають недозволений доступ, виявляють шкідливі програми або помічають проблеми з безпекою.

Основна мета реагування — якомога швидше припинити кібератаку, відновити роботу системи, сповістити клієнтів або регулятивні органи згідно з вимогами законодавства та вивчити, як знизити ризик подібних порушень у майбутньому.

Реагування на інциденти зазвичай починається, коли команда безпеки отримує оповіщення від системи керування захистом інформації (SIEM). Члени команди повинні переконатися, що подія відповідає критеріям інциденту, і тоді вживаються заходи для ізоляції інфікованих систем та видалення загрози. У випадку серйозного інциденту або довгочасної реакції може знадобитися відновлення резервної копії даних, обговорення можливостей викупу або повідомлення клієнтам про можливі порушення безпеки їхніх даних.

Тому до процесу реагування зазвичай залучаються спеціалісти, які не належать до команди кібербезпеки. Експерти з конфіденційності, юристи та особи, що приймають стратегічні рішення в бізнесі, спільно визначають підхід організації до управління інцидентом та його вирішенням.

Під час реагування на інцидент команда повинна спільно й оперативно працювати з метою ефективного усунення загрози та відповіді на регуляторні вимоги. У подібних стресових ситуаціях легко збентежитися та допустити

помилки, що саме пояснює, чому багато компаній розробляють плани реагування на інциденти. Ці плани визначають ролі та обов'язки учасників інцидентного процесу та включають послідовні кроки, необхідні для належного вирішення ситуації, документування інциденту та інформування про нього.

Також важливо дотримуватися плану реагування на інциденти, адже значна кібератака впливає не лише на функціонування організації, але й на її репутацію перед клієнтами та громадськістю, і може мати юридичні наслідки. Швидкість реакції команди з безпеки на атаку та якість повідомлення керівництвом про інцидент впливають на загальні витрати організації.

Компанії, які приховують збитки від клієнтів та державних установ або не серйозно ставляться до загрози, можуть порушити законодавство. Ці помилки часто виникають через відсутність ретельно розробленого плану реагування. У стресових ситуаціях люди можуть приймати поспішні рішення під впливом паніки, що може заподіяти значну шкоду організації.

Чітко розроблений план дій дає працівникам визначеність у своїх діях на кожному етапі атаки, що убезпечує від необдуманих рішень. Після відновлення роботи організація може продемонструвати громадськості свою реакцію на інцидент, що підвищує довіру клієнтів та показує, що вона серйозно ставиться до безпеки та приймає необхідні заходи для запобігання подібним ситуаціям у майбутньому.

Розробка плану реагування на інциденти може здатися складним завданням, але це може значно знизити ризик того, що бізнес виявиться непідготовленим під час серйозного інциденту. Ось як можна почати роботу:

- Першим етапом у плані реагування на інцидент є чітке розуміння того, що саме потрібно захищати. Важливо задокументувати ключові дані компанії, включаючи їхнє розташування та значення для бізнесу.
- Під час напруженого інциденту, наявність чітких процедур допоможе швидко і ефективно вирішити проблему. Починаючи з визначення того, що саме вважається інцидентом, а потім скласти план дій, який команда

повинна виконати для виявлення, ізоляції та відновлення після інциденту, включаючи процедури документування прийнятих рішень та збір доказів.

- Необхідно створити план комунікацій, який позбавить команду від необхідності здогадуватися, коли і як повідомляти іншим всередині та поза організацією про те, що відбувається. Продумати різні сценарії, які допоможуть визначити, за яких обставин потрібно інформувати керівників, усю організацію, клієнтів, а також ЗМІ та інші зовнішні зацікавлені сторони.
- Зловмисники атакують співробітників на всіх рівнях організації, тому важливо, щоб усі розуміли план реагування та знали, що робити, якщо вони підозрюють, що стали жертвою атаки. Періодично потрібно проводити тестування співробітників, щоб переконатися, що вони вміють розпізнавати фішингові електронні листи і щоб їм було легко повідомити команду реагування на інциденти, якщо вони випадково натиснули шкідливе посилання або відкрили заражене вкладення.

Багато компаній використовують різні підходи до реагування на інциденти, але багато з них розраховують на організації, які спеціалізуються на стандартах безпеки, для керування цим процесом. Наприклад, SysAdmin Audit Network Security (SANS) пропонує шестикрокову систему реагування, яка допомагає компаніям ефективно вирішувати інциденти. Крім того, багато організацій використовують систему відновлення після інцидентів, розроблену Національним інститутом стандартизації та технологій (NIST).

Перед початком будь-якого інциденту важливо забезпечити підготовку. Це означає зниження вразливостей та встановлення політики та процедур безпеки ще до того, як станеться будь-який негативний випадок. Під час цього етапу організації проводять оцінку ризиків, щоб з'ясувати свої слабкі місця та визначити пріоритетність активів. Також важливо розробити та вдосконалити процедури безпеки, визначити ролі та обов'язки у команді, а також оновити системи для зменшення ризиків. Більшість організацій періодично повертаються до цього етапу, щоб покращувати свою політику, процедури та системи відповідно до здобутого досвіду або змін у технологіях.

Під час ідентифікації загроз команда забезпечення безпеки може отримувати значну кількість сповіщень за день, які вказують на потенційно підозрілу активність. Проте деякі з них можуть бути помилковими або не досягати рівня, щоб бути визнаними як інциденти. Після виявлення інциденту команда аналізує характер порушення та документує всі виявлені результати, зокрема, джерело порушення, тип атаки та мету зловмисника. На даному етапі важливо також інформувати зацікавлені сторони та повідомляти про подальші кроки, що плануються.

Наступним важливим завданням є швидка локалізація загрози. Чим довше зловмисники залишаються в системі, тим більше можуть вони завдати шкоди. Команда забезпечення безпеки працює над тим, щоб оперативно відокремити програми або системи, що постраждали від атаки, від інших частин мережі. Це допомагає уникнути доступу зловмисників до інших аспектів бізнесу.

Після успішної локалізації загрози, команда приступає до видалення зловмисника та всіх шкідливих програм з уражених систем і ресурсів. Це може включати виведення систем з мережі. Крім того, команда продовжує інформувати зацікавлені сторони про прогрес у вирішенні інциденту.

Наступний крок — початок процесу відновлення, що може зайняти декілька годин. Під час цього процесу вони відновлюють системи та дані з резервних копій і виконують контроль уражених областей, щоб переконатися, що зловмисники не зможуть повернутися.

Після завершення інциденту команда проводить аналіз події та визначає, які кроки можна зробити для поліпшення процесу реагування. Вивчення вчинків інциденту на цьому етапі допомагає команді зміцнити захист організації.

Оптимальний час реагування на інциденти в службі центру операційної безпеки SOC є ключовим елементом ефективного кіберзахисту організації. Цей час визначає, наскільки швидко SOC може виявити, аналізувати і вирішити потенційні загрози та інциденти, що можуть виникнути у мережі чи інформаційних системах.

Ідеальний час реагування в операційному центрі безпеки може коливатися залежно від різних факторів, таких як тип організації, специфіка її

діяльності, рівень загроз та відомостей про кібербезпеку. Однак, загалом оптимальний час реагування можна оцінити в години, або навіть хвилини, а не дні чи тижні.

Швидке виявлення та реагування на інциденти в SOC має декілька ключових переваг. Перш за все, це дозволяє мінімізувати час, протягом якого зловмисники можуть шкодити системам та даним організації. Чим швидше виявлено та зупинено інцидент, тим менше можливостей для розповсюдження атаки та завдання шкоди.

Крім того, швидке реагування дозволяє зменшити витрати організації, пов'язані з відновленням після кібератаки. Чим швидше інцидент виявлено та припинено, тим менше часу і грошей потрібно на відновлення роботи систем та компенсацію збитків.

Перш за все, важливо визначити, що розуміється під часом реагування на інциденти в SOC. Час реагування може бути розділений на кілька етапів, включаючи виявлення, аналіз та реагування на інцидент. Час виявлення оцінюється від моменту, коли відбулася подія, до моменту, коли вона була виявлена системою моніторингу або персоналом SOC. Час аналізу — це період, необхідний для перевірки, аналізу та оцінки інциденту, включаючи визначення його природи та масштабу. Час реагування — це час, необхідний для прийняття та впровадження заходів щодо усунення інциденту та мінімізації його впливу на систему чи організацію.

Звичайно, чим швидше виявлено інцидент, тим швидше можна реагувати на нього. Однак багато факторів може вплинути на час реагування на інциденти в SOC. Наприклад, складність та масштаб інциденту може вимагати більше часу для аналізу та реагування. Також важливо враховувати навички та досвід персоналу SOC, доступні ресурси та наявність автоматизованих систем моніторингу та реагування.

Швидке реагування на інциденти в SOC має кілька переваг. По-перше, це дозволяє мінімізувати можливість завдання шкоди системі та даним організації. Чим швидше виявлено та вирішено інцидент, тим менше часу будуть мати зловмисники для проведення атак та злому системи. Крім того, швидке

реагування допомагає зменшити витрати, пов'язані з відновленням після кібератаки та відшкодуванням збитків.

Для досягнення оптимального часу реагування на інциденти в SOC важливо використовувати передові технології моніторингу та аналізу, тренувати персонал для швидкого та ефективного реагування, а також встановлювати чіткі процедури для керування інцидентами. Швидке реагування на інциденти в SOC є ключовим елементом успішного кіберзахисту, що дозволяє організаціям ефективно захищати свої системи та дані від кіберзагроз.

2.3 Розробка ефективної процедури управління інцидентами ІБ згідно ISO/IEC 27035

Інциденти в галузі інформаційної безпеки (ІБ) часто не знаходяться на поверхні, а можуть пройти непомічено користувачами, але наслідки таких інцидентів можуть бути значними. Тому важливо, щоб жоден інцидент інформаційної безпеки не залишився непоміченим, а саме необхідно його ретельно розслідувати, визначати винних, а головне — вживати заходів для запобігання подібним ситуаціям у майбутньому. Отже, важливо мати чітку процедуру реєстрації та розслідування інцидентів безпеки, а також поінформувати користувачів про правила виявлення таких інцидентів.

Важливо розуміти, що реакція на інцидент інформаційної безпеки не призводить до виправлення збитків компанії (зазвичай, збитки вже заподіяні), але розслідування і впровадження проактивних та коригувальних заходів допомагають зменшити ймовірність повторення подібних ситуацій (і, отже, зменшують ризик подальших збитків). Також важливо підкреслити, що статистика інцидентів інформаційної безпеки має велике значення для компанії, як показник ефективності системи управління інформаційною безпекою. Аналіз цієї статистики повинен проводитися регулярно під час аудиту системи управління інформаційною безпекою.

Отже, для розробки ефективної процедури управління інцидентами інформаційної безпеки першочергово важливо, щоб цей процес був ініційований вищим керівництвом компанії. Як правило, розробка такої процедури відбувається в рамках загальної системи управління інформаційною безпекою, тому ключова підтримка керівництва у питаннях створення та функціонування такої системи є надзвичайно важливою. На даному етапі також важливо, щоб всі співробітники розуміли, що забезпечення інформаційної безпеки загалом і управління інцидентами інформаційної безпеки зокрема є основними цілями компанії.

На другому етапі проводиться розробка необхідних нормативних документів з управління інцидентами інформаційної безпеки (УІІБ). Зазвичай такі документи включають в себе наступне:

- Визначення понять інцидентів інформаційної безпеки та перелік подій, які можуть бути визнані інцидентами (в контексті конкретної компанії).
- Процедури оповіщення відповідальних осіб про виникнення інцидентів (з уточненням формату оповіщення та контактної інформації необхідних осіб).
- Порядок усунення наслідків та причин інцидентів інформаційної безпеки.
- Процедури розслідування інцидентів, включаючи визначення причин, винних та збір доказів.
- Механізми застосування дисциплінарних заходів.
- Впровадження необхідних коригувальних та профілактичних заходів.

Визначення подій, які можуть бути визнані інцидентами, є ключовим етапом у розробці процедури УІІБ. Це оскільки всі події, які не включені до цього переліку, розглядаються як нормальні (навіть якщо вони представляють загрозу інформаційній безпеці). До можливих інцидентів інформаційної безпеки в компанії можуть належати:

1) Відмова в обслуговуванні сервісів, інструментів обробки інформації та обладнання.

2) Порушення конфіденційності та цілісності важливої інформації.

3) Невиконання вимог інформаційної безпеки, встановлених у компанії (порушення правил обробки інформації).

4) Незаконне моніторингове використання інформаційних систем.

5) Виявлення шкідливих програм.

6) Компрометація інформаційних систем (наприклад, розголошення паролів користувача).

Інші можливі приклади інцидентів включають несанкціоновані зміни даних на веб-сайті компанії, залишення комп'ютера розблокованим без нагляду або надсилання конфіденційної інформації через корпоративну або особисту електронну пошту. Будь-яка подія, яка порушує правила, визначені в документах УІІБ, може бути визнана як інцидент. Це підкреслює важливість наявності чіткої документації, яка описує дозволені та заборонені дії в системі.

Для опису процесу формування СУІБ використовується класична модель безперервного удосконалення процесів, що отримала назву від циклу Шухарта-Демінга — модель PDCA (Плануй, Plan - Виконуй, Do - Перевіряй, Check - Дій, Act).

Рис. 2.2. Етапи формування СУІБ відповідно до моделі PDCA

Стандарт ISO/IEC 27001 використовує модель PDCA як основу для всіх процесів управління інформаційною безпекою. Це включає і процес управління інцидентами, який також відповідає моделі PDCA, згідно з стандартом ISO/IEC 27035.

Дана модель містить наступний функціонал:

1. Виявлення та реєстрація інциденту

Інцидент інформаційної безпеки може бути помічений або користувачем, або адміністратором системи. Зазвичай адміністратори знають, як діяти у випадку виявлення інцидентів, чого не можна сказати про користувачів. Для користувачів корисно розробити інструкцію, яка містить опис, як повідомити про виникнення інциденту, контактну інформацію відповідальних осіб та перелік дій, які користувач може виконати самостійно (або буде попереджений, що виконання будь-яких дій самостійно заборонено).

Звіт користувача про інцидент повинен включати детальний опис події, перелік співробітників, які брали участь у події, інформацію про того, хто виявив інцидент, а також дату й час реєстрації інциденту. Таким чином, кожен співробітник отримує інструкцію, яка роз’яснює, як діяти у випадку, наприклад,

якщо він продовжує працювати з документом і помічає, що в ньому були внесені зміни, які не відповідають реальності, і при цьому він не знає автора цих змін.

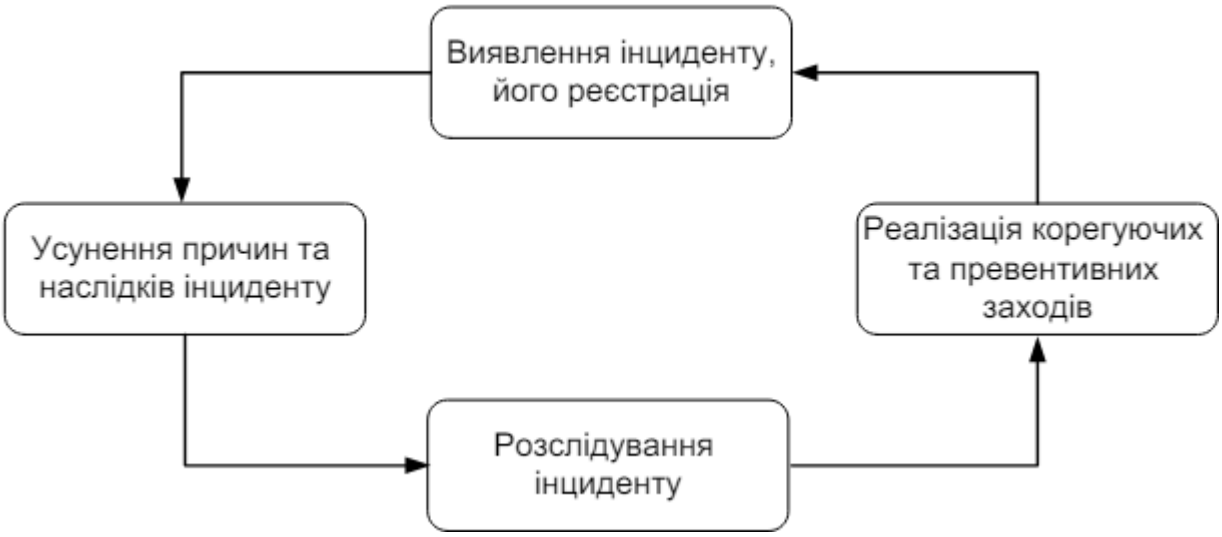

Рис. 2.3. Життєвий цикл процесу УІІБ

Також потрібно розробити інструкцію для співробітника, який відповідає за реєстрацію інцидентів. Коли співробітник виявляє інцидент, він зв'язується з відповідальним за реєстрацію інцидентів і виконує подальші дії. У малих компаніях співробітники можуть звертатися безпосередньо до фахівця, який може вирішити наслідки і причини інциденту (наприклад, системний адміністратор або адміністратор з безпеки). У великих компаніях, зазвичай, виокремлюється спеціалізований фахівець, який реєструє інциденти та передає інформацію відповідним фахівцям. Інструкція може включати правила та строки реєстрації інцидентів, список дій для співробітника, що виявив інцидент, та процедуру передачі інформації фахівцю, а також контроль за усуненням наслідків та причин інциденту.

2. Усунення причин, наслідків інциденту і його розслідування

Усунення причин та наслідків інциденту включає загальний опис заходів, які потрібно прийняти (конкретні дії для кожного випадку інциденту визначаються важко і не завжди ефективно), а також термін, протягом якого потрібно усунути наслідки та причини інциденту. Термін усунення залежить від важливості інциденту. Корисно класифікувати інциденти, визначати рівні їхньої

важливості та описувати для кожного рівня інциденту терміни усунення. Інструкція може містити опис заходів для усунення наслідків і причин інциденту, строки їхнього усунення та інформацію про відповідальність за недотримання інструкції.

3. Розслідування інциденту

Даний етап включає визначення винних, збір доказів та накладання відповідних дисциплінарних стягнень. У великих компаніях зазвичай утворюється комісія з розслідування інцидентів, до якої може входити співробітник, який реєструє інциденти. Інструкція повинна описувати заходи щодо розслідування інциденту, правила збору та зберігання доказів і правила накладання дисциплінарних стягнень.

4. Корегувальні та запобіжні заходи

Після усунення наслідків і відновлення нормального функціонування бізнес-процесів компанії, корисно провести заходи для запобігання повторенню інциденту. Для визначення необхідності таких заходів варто провести аналіз ризиків, під час якого визначається доцільність корекційних та запобіжних дій. У деяких випадках наслідки інциденту будуть незначними порівняно з корекційними та запобіжними діями, і тоді може бути доцільно не вживати подальших заходів після усунення наслідків інциденту.

Для того, щоб процедура УІІБ була ефективною, всі ці етапи моделі PDCA мають бути постійно і послідовно повторювані. Через певний період часу (зазвичай через півроку або рік) потрібно переглянути перелік подій, визначених як інциденти, форму звіту тощо, впровадити оновлену процедуру, перевірити її функціонування та ефективність, а також реалізувати запобіжні заходи. Таким чином, цикл моделі PDCA буде безперервно повторюватися, що забезпечить чітке функціонування процедури управління інцидентами та постійне її удосконалення.

Висновки до розділу 2

Можна зробити висновок, що безпека даних та інформаційних ресурсів стає пріоритетом служби центрів операційної безпеки. Швидке виявлення та реагування на інциденти SOC має ключове значення, оскільки це дозволяє знизити час, протягом якого зловмисники можуть нанести шкоду, а також зменшує витрати на відновлення після кібератаки. Використання передових технологій, висококваліфікованого персоналу та ефективних процесів дозволяє SOC швидко виявляти та реагувати на загрози і попереджувати серйозні наслідки для організацій. Додатково слід створити ефективну процедуру управління інцидентами ІБ та неухильно дотримуватися всіх встановелних пунктів відповідно до стандарту ISO/IEC 27035.

Таким чином, ефективне виявлення, реагування та створення процедур управління інцидентами в SOC не лише забезпечує безпеку даних, а й підвищує рівень довіри до організації в цифровому просторі.

Розділ 3 ОЦІНКА ЕФЕКТИВНОСТІ СИСТЕМИ МОНІТОРИНГУ Й РЕАГУВАННЯ НА ІНЦИДЕНТИ БЕЗПЕКИ SOC В ОРГАНІЗАЦІЇ

3.1. Аналіз поточного стану системи SOC в організації

Для успішної роботи системи SOC, оцінка поточних можливостей оперативного центру безпеки стає критично важливою. Для проведення цієї оцінки визначаються основні процеси та критерії, які характеризують ключові компоненти SOC. Оцінка здійснюється на основі різних аспектів, що враховують усі складові SOC.

Для компоненту «люди» проводяться оцінки за різними складовими. Наприклад, аналізується рівень усвідомленості вищого керівництва про важливість SOC, ступінь їх залучення та інвестування в цю область, а також наявність здатностей до звітування. Структурні аспекти також увійшли в оцінку, зокрема організаційна структура та взаємовідносини між різними ролями та департаментами, а також процес обміну інформацією всередині організації. Крім того, аналізується досвід персоналу, зокрема управління інцидентами, цифрове розслідування, виявлення вразливостей, управління журналюванням та робота з системою управління подіями та інцидентами (SIEM).

Для компоненту «процеси» проводяться оцінки за різними складовими. Наприклад, оцінюється формалізація процесу сортування за інцидентами та процеси класифікації і пріоритизації цих інцидентів. Також проаналізовано наявність процесів звітування по інцидентам, включаючи ідентифікацію необхідних типів звітів та їхню структуру. Оцінка також здійснюється стосовно процесів аналізу інцидентів безпеки та їх співставлення з класифікацією, а також процедур отримання та аналізу даних. Окремо розглядаються процеси закриття інцидентів, включаючи ліквідацію компрометацій та маркування їх як закритих. Додатково аналізується діяльність після інцидентів, включаючи процеси зберігання та обміну інформацією, а також обговорення серйозних інцидентів. У контексті виявлення вразливостей оцінюється наявність процесів виявлення,

отримання повідомлень про нові вразливості та оцінювання їхнього впливу. Додатково проводиться оцінка наявності процесів усунення та відслідковування вразливостей, включаючи поширення інформації серед власників та операторів.

Оцінка компонента «технології» включає аналіз різних аспектів. Наприклад, аналізується мережева інфраструктура, зокрема, її застосування та покриття, які використовуються для управління та моніторингу систем SOC. Додається оцінка доступності критичних систем та продуктивності мережі. Окрім цього, проводиться оцінка процесу збору, кореляції та аналізу подій, включаючи його планування, масштабованість та налаштованість систем для передачі подій. Додатково розглядається процес моніторингу, зокрема, аналіз перехоплених мережевих потоків і пакетів, а також здатність до звітування та виявлення проблем. У контексті безпеки, оцінюється відповідність контролів безпеки, правильність налаштування та застосування рольового контролю доступу. Також, проводиться аналіз управління журналами та виявлення вразливостей, включаючи наявність інструментів для виявлення вразливостей та їхню підтримку. Для вимірювання ефективності та оцінки рівня процесів управління може застосовуватися модель здатності процесу. Ця модель, що базується на стандартах COBIT (Control Objectives for Information and Related Technology) та SEI (Software Engineering Institute) включає:

- Рівень 0 описує стан, коли процес абсолютно відсутній і не визнаний.
- На рівні 1 процес характеризується як початковий, де він непередбачуваний, слабо контрольований і реактивний через відсутність стабільного середовища підтримки.
- На рівні 2 процес керується, він задокументований і підтверджений, але може бути недостатньо завершеним або непридатним для даного контексту організації.
- Рівень 3 відображає визначений процес, який повністю задокументований і відповідає контексту організації.
- На рівні 4 процес кількісно керований, його вимірюють і

контролюють, встановлені контролі для оцінки використання підтвердженого процесу.

- Рівень 5 відображає оптимізований процес з фокусом на постійному вдосконаленні, що досягається через регулярний перегляд та оновлення. Оцінки за цією моделлю представлені на шкалі від 0 до 5 і дозволяють виміряти поточні можливості та відстежувати прогрес щодо поставлених цілей. Оцінка здатностей SOC варто проводити, оцінюючи всі ключові компоненти — людей, процеси та технології.

Візуалізація оцінок в контексті кожного ключового компоненту може бути представлена у вигляді даного рисунку:

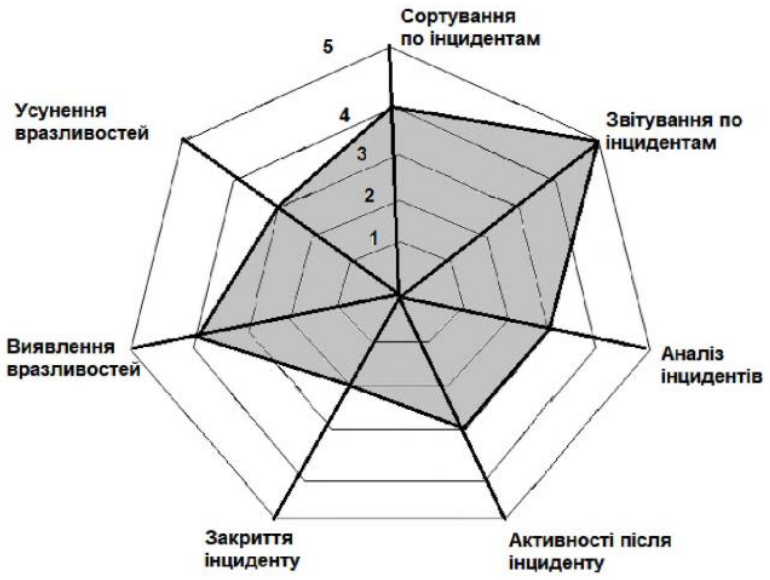

Рис.3.1.Оцінка здатності основних процесів SOC

3.2.Оцінка ключових показників ефективності SOC

Ландшафт загроз у нашому кіберпросторі, що постійно розвивається, продовжує розширюватися швидкими темпами. Зловмисники запускають складні атаки, які часто залишаються невиявленими одноточковими пристроями безпеки. Щоб захиститися від таких атак, організаціям необхідно впроваджувати комплексні програми безпеки, які охоплюють людей, процеси та технології.

Зрілі програми безпеки зосереджені на постійному вдосконаленні для успішного захисту від вхідних загроз.

У нинішніх умовах жодна організація не може стверджувати, що вона абсолютно захищена від кібератак. Кожна організація, незалежно від її розміру та галузі, є мішенню для інцидентів безпеки та витоку даних. Іноді зловмисники витрачають місяці на планування атаки, і їм достатньо лише одного разу, щоб порушити бізнес-операції. Однак, з іншого боку, очікується, що команда безпеки компанії повинна запобігати таким спробам 24x7. З іншого боку, організація не має жодного правдоподібного способу дізнатися кількість потенційних зловмисників, а кількість осіб у команді безпеки обмежена.

У цьому контексті організаціям стає складно вимірювати успіх своїх ініціатив у сфері безпеки. Хоча управлінські рішення, безумовно, спиратимуться на дані, а команди безпеки витрачають значну кількість часу на відстеження правильних показників. Вимірювання операцій безпеки, як якісне, так і кількісне, демонструє, наскільки добре функціонує програма безпеки. Ці результати можуть бути використані в подальшому для запиту додаткових бюджетних асигнувань на нові технології та інструменти.

Команди SOC часто стикаються з ситуаціями, коли клієнти впровадили найкращі заходи безпеки, але не відстежували належним чином свої операції з безпеки. Не можна заперечувати, що звітування про показники їхньої діяльності є дуже трудомістким процесом. За відсутності сумісності між різними інструментами безпеки та нестачі кваліфікованих кадрів проблема ще більше погіршується. Однак керівники служб безпеки та IT-директори повинні розуміти, що реєстрація показників діяльності постачальників послуг безпеки має важливе значення для загальної стратегії безпеки.

Перш ніж будувати план для практик безпеки організації, команда безпеки повинна мати чітке уявлення про те, які дані вони збирають і чому. Рекомендується підготувати довгострокові цілі на основі показників безпеки, які відповідають бізнес-вимогам організації. Ці цілі повинні вписуватися в загальну стратегію безпеки організації. Ще одним аспектом тут є правильне визначення

ролей та обов'язків осіб, відповідальних за програму збору показників безпеки у організації. Після того, як ця інформація буде задокументована і готова, команді безпеки буде зручніше користуватися підтримкою вищого керівництва.

Розглянемо ситуацію, коли команда безпеки звертається до вищого керівництва без будь-якої документації та чіткого розуміння того, що вони хочуть зробити. Швидше за все, вони отримають негативну відповідь. Якщо організація створює операційний центр безпеки (SOC), дуже важливо з самого початку фіксувати показники, щоб отримати вигоду в довгостроковій перспективі. Маючи належну документацію, команда безпеки може розраховувати на швидке схвалення з боку вищого керівництва та відповідну підтримку.

Коли починається підготовка до впровадження запропонованої програми з вимірювання показників безпеки, команда може зіткнутися з опором з боку окремих груп або осіб в самій службі безпеки. Деякі керівники можуть вважати, що інша команда, яка фіксуватиме їхні щодення завдання, створить додатковий тиск на їхню команду. Однак, програма збору показників безпеки повинна бути представлена як рішення для імпровізації операцій з безпеки, а не як організаційна програма для стеження за різними менеджерами та їхніми командами. Наявність чітко визначених ролей та обов'язків, які слід підготувати перед тим, як звертатися до вищого керівництва, допомагає зменшити подібні побоювання.

Ключовий показник ефективності (KPI) допомагає організації визначити, чи був бізнес-процес або мета успішними чи провальними. Вони надають практичну інформацію для осіб, які приймають рішення, і, зрештою, допомагають у процесі прийняття рішень. Як правило, KPI для операцій з безпеки спрямовані на виявлення позитивних і негативних тенденцій. Наприклад, одним з KPI може бути кількість хибних спрацювань інцидентів безпеки за останні шість місяців. Аналогічно, для адміністративних процесів KPI може бути кількість винятків, зроблених за попередні три місяці. Реєстрація KPI

може мати величезні переваги для операцій з безпеки, незалежно від того, чи є вони стратегічними або тактичними.

Чітко визначені ключові показники ефективності (KPI) можуть слугувати рушійною силою для постійного вдосконалення програми безпеки. KPI гарантують, що програма безпеки залишається ефективною, а прогалини усуваються до того, як вони можуть вплинути на безпеку. Щоб визначити відповідні показники безпеки, команда безпеки повинна почати з визначення різних операцій або функцій, які потрібно оцінити. Якщо організація має впроваджену систему СУІБ, наявний документ може допомогти їй у цьому. Для визначених операцій і функцій слід визначити різні показники безпеки або KPI, які допоможуть оцінити їхню ефективність.

Запис KPI вимагає певних витрат, як часових, так і грошових. Перш ніж остаточно скласти список KPI для відстеження, може бути корисним аналіз витрат і прибутку.

Кожен KPI повинен мати наступні SMART-характеристики:

- **Простота**: KPI має бути легко виміряти. Він не повинен бути складним, а мета його запису повинна бути задокументована і доведена до відома.
- **Вимірюваність**: ключові показники ефективності, які неможливо виміряти, не допоможуть в процесі прийняття рішень. Обрані KPI повинні бути вимірюваними, як якісно, так і кількісно. Процедура вимірювання ключових показників ефективності має бути послідовною і чітко визначеною.
- **Дієвими**: KPI обов’язково має сприяти процесу прийняття рішень в організації. Ключові показники ефективності, які не роблять жодного такого внеску, не мають жодної мети.
- **Релевантні**: KPI повинні бути пов'язані з операціями або функціями, які команда безпеки прагне оцінити.
- **Засновані на часі**: KPI має бути достатньо гнучкими, щоб демонструвати зміни в часі. З практичної точки зору, ідеальний показники ефективності може бути згрупований за різними часовими інтервалами.

Перейдемо до важливих показників для операцій з безпеки. Однією з найбільш очевидних метрик, яку слід реєструвати, є кількість загальних спрацювань та інцидентів, пов'язаних з безпекою.

Цей показник дасть відповіді на такі питання:

1. Чи збільшується або зменшується загальна кількість інцидентів безпеки?
2. Які типи інцидентів безпеки виявляються?
3. Скільки інцидентів безпеки з високим рівнем ризику було виявлено за останній місяць?

Цей показник допоможе визначити частку хибних спрацювань, середній час, необхідний для усунення інциденту, та середню кількість спрацювань на одного аналітика з безпеки. Якщо є велика кількість оповіщень про загрози безпеці. Якщо велика кількість спрацювань безпеки обробляється окремими членами команди, це дає змогу зрозуміти, що організації бракує людських ресурсів. Крім того, зібрана інформація з спрацювань та інцидентів допоможе виявити слабкі місця у технічній інфраструктурі компанії. Крім того, для оповіщень та інцидентів, спричинених помилками користувачів, можна спостерігати за членами команди, які потребують додаткового навчання з безпеки.

Якщо рішення SIEM є частиною операцій з безпеки, воно повністю впорядкує процес запису метрик для різних функцій і процесів. Крім того, можливості Security Orchestration, Automation and Response (SOAR) забезпечать команду безпеки інформацією про всю мережу в режимі реального часу, а також автоматизованими можливостями виявлення та реагування.

Використовуючи SIEM і SOAR, можливо додатково відстежувати такі метрики:

1. Кількість порушень, закритих аналітиком за день. Закриття спрацювань (автоматизоване проти ручного).
2. Кількість порушень, позначених як хибні. Перетворення спрацювань на інциденти безпеки.

3. Середній час, витрачений на виявлення інциденту безпеки. Типи порушень за певний період.

4. Порушеня за пристроєм-джерелом.

У великих організаціях, де команди безпеки мають кілька рівнів аналітиків, метрики безпеки можуть допомогти виявити цікаву інформацію про те, як аналітики взаємодіють один з одним. Уявімо, що в операційному центрі безпеки є три рівні аналітиків безпеки. Метрики безпеки можуть допомогти в розумінні:

- Типи оповіщень, ескалації на рівень 2 від аналітиків рівня 1.
- Час реакції аналітиків безпеки, відповідальних за реагування на інциденти безпеки.
- Час, необхідний для обробки порушень на кожному рівні.

Найчастіше використовувані сценарії.

- Найчастіші IP-адреси, користувачі та хости, залучені в оповіщеннях про загрози безпеці.

Перейдемо до важливих показників для бізнес-вимог.

Організація сподівається виконувати свої бізнес-операції без перебоїв. Вона приймає детальну систему управління ризиками, щоб мінімізувати ймовірність ризиків, з якими вона стикається. Організація може впровадити спеціальну систему управління безперервністю бізнесу для підтримки своїх ініціатив з управління ризиками. Хоча це правда, що кожна організація схильна до кібератак, управління ризиками може значно знизити витрати у випадку успішної кібератаки. Наприклад, якщо зловмисникам вдасться проникнути в мережу організації, перевірений і випробуваний план реагування на інциденти допоможе негайно розпочати процес реагування на інцидент. Як тільки інцидент буде ліквідовано, організація зможе відновити свою звичайну діяльність.

Якщо говорити з точки зору топ-менеджменту, то відповідним KPI може бути MTTD (середній час, необхідний для виявлення). MTTD — це час, необхідний команді безпеки для виявлення інциденту безпеки, коли він знаходиться в процесі або після того, як він стався. MTTR (середній час

реагування) — це час, необхідний вашій команді безпеки, щоб зменшити або усунути інцидент безпеки після його виявлення. Тенденції MTTD і MTTR за певний період можуть допомогти зрозуміти можливості команди безпеки щодо виявлення та реагування на інциденти. Ці дві метрики також можуть дати уявлення про тривалість, протягом якої зловмисники мали необмежений доступ до мережі організації. Протягом цього періоду зловмисники можуть виконувати різні дії, які можуть безпосередньо вплинути на стан безпеки вашої організації.

Для вищого керівництва знання про «втому від порушень» може допомогти у прийнятті рішення про необхідність інвестувати в додаткові людські ресурси для команди безпеки. Реагування на порушення одна за одною може призвести до втоми від них, і, як наслідок, загальна продуктивність команди безпеки знижується загальна продуктивність команди безпеки. Однак, якщо такі рішення, як SIEM і SOAR, є частиною операцій з безпеки організації, ймовірність втоми від оповіщення знижується. За допомогою автоматизації оповіщення з низьким рівнем ризику автоматично обробляються за допомогою сценаріїв. Сповіщення з високим рівнем ризику збагачуються контекстною інформацією і можуть бути призначені аналітикам безпеки для ручної перевірки.

Інші метрики для бізнес-вимог, які необхідно враховувати:

- ✓ Відсоток хибних спрацювань на інструмент безпеки
- ✓ Розподіл оповіщень та інцидентів за рівнями ризику
- ✓ Найпоширеніші джерела оповіщень та інцидентів безпеки
- ✓ Кількість інцидентів, які вплинули на бізнес-операції
- ✓ Продуктивність аналітиків безпеки на різних рівнях команди безпеки

Ручний збір даних для метрик може виявитися нудним процесом. Команда безпеки повинна вивчити різні можливості автоматизації збору, аналізу та представлення звітів. Після того, як показники безпеки почнуть збиратися, ви зможете створювати звіти, які демонструватимуть зміни, що відбулися з плином часу. Ці звіти можна надсилати вищому керівництву, щоб пояснити їм прогрес, а також наявні прогалини у вашій програмі безпеки. Подібні проблеми вирішуються за замовчуванням, коли організація покладається на рішення SIEM

і SOAR. Ці рішення мінімізують неузгодженість даних, спрощують процес звітування, забезпечують передбачуваність надання звітів і сприяють прийнятній практиці гігієни даних.

Підтримка базової лінії продемонструє зміни з часом, як позитивні, так і негативні. Команда безпеки повинна приділяти однакову увагу як негативним, так і позитивним змінам. Належна увага до негативних результатів допоможе заручитися підтримкою вищого керівництва в довгостроковій перспективі. Таким чином, замість того, щоб надмірно зосереджуватися на короткострокових результатах і позитивних змінах, ресурси повинні бути спрямовані на те, щоб звести до мінімуму випадки негативних змін.

Врешті-решт, показники безпеки нададуть детальне уявлення про ефективність вашої програми безпеки. Зі збільшенням рівня автоматизації збору даних підготовка звітів після аналізу даних займатиме менше часу. Якщо ви розглядаєте можливість часткового або повного аутсорсингу ваших операцій з безпеки стороннім постачальником послуг, ваша програма метрик повинна враховувати цю домовленість. Необхідно призначити контактну особу (KPI) для регулярного спілкування з вашим постачальником послуг і забезпечення належного обміну показниками для вимірювання операцій з безпеки. Рекомендується визначити очікувані рівні продуктивності у формі угоди про рівень обслуговування (SLA).

І останнє, але не менш важливе рішення SIEM в поєднанні з можливостями SOAR, безумовно, може в більшій мірі автоматизувати реагування на оповіщення про загрози безпеці. Ця автоматизація може бути як повністю, так і частково автоматизованою, що вимагає втручання людини. За допомогою цих рішень ручна робота, необхідна для управління оповіщеннями, значно скорочується. Крім того, коли ці рішення стають частиною операцій з безпеки організації, загальна ефективність їхніх програм безпеки зростає, а продуктивність команд постійно підвищується.

3.3 Рекомендації для покращення ефективності системи SOC

Навіть найсучасніші операційні центри безпеки можуть зіткнутися з труднощами у підвищенні ефективності SOC

Будь-який операційний центр безпеки — це нервовий центр зусиль організації з кібербезпеки. SOC — це напружене та динамічне середовище, де підготовка та запобігання є ключовими обов'язками команди безпеки.

Орієнтуючись на попередній розділ, де було визначено та оцінено основні показники ефективності SOC, можна надати рекомендації, які значно підвищать ефективність роботи операційного центру безпеки.

1. Оптимізація управління оповіщеннями.

Національний інститут стандартів і технологій (NIST) визначає «хибні спрацьовування» як сповіщення, які помилково вказують на наявність вразливості або зловмисної активності або неточно позначають нешкідливу активність як підозрілу. Згідно зі звітом Ponemon Institute, організації отримують в середньому 17 000 сповіщень про шкідливе програмне забезпечення щотижня, і лише 19% з них вважаються достовірними.

Втома від оповіщень є поширеною проблемою в SOC і ключ до її вирішення - оптимізація управління сповіщеннями:

- Впровадження розширеної аналітики. Необхідно використовувати можливості аналітичних інструментів для підвищення ефективності SOC, відфільтровуючи хибні спрацьовування та визначаючи пріоритети оповіщень на основі серйозності та ймовірності того, що вони є легітимною загрозою. Точний контроль меж дозволить уникнути хибних спрацьовувань і масового відключення облікових записів.
- Автоматизування реагування. Де це можливо, потрібно автоматизувати реагування на поширені типи сповіщень, щоб звільнити час аналітиків для більш складних завдань.

2. Покращення розвідки загроз

Як то кажуть, «дані без контексту — це шум», а хороша аналітика загроз

може значно підвищити ефективність і продуктивність SOC:

- Необхідно інвестувати в якісну аналітику загроз, щоб випереджати нові загрози. Використовуйте інструменти кібербезпеки на основі машинного навчання для запобігання атакам «нульового дня», щоб виявляти складні загрози, які традиційні заходи безпеки можуть пропустити. Сюди входять сучасні постійні загрози (APT), які є ключовими факторами для проактивної розвідки загроз.
- Налаштування аналітики. Важливо налаштувати дані про загрози відповідно до конкретних потреб і контексту вашої організації.

3. Інвестування в необхідні інструменти

Необхідні та правильно підібрані інструменти можуть значно підвищити ефективність SOC:

- Інтегровані платформи безпеки. Єдине вікно правди — це значна економія часу та клопоту. Використовуйте платформи, які інтегрують різні інструменти безпеки для єдиного бачення, і, якщо це можливо, використовуйте існуючі агенти EDR, щоб покращити видимість і зосередити зусилля, підвищити ефективність і досягти економії коштів за рахунок зменшення безладу.
- Інструменти автоматизації. Впровадження інструментів автоматизації кібербезпеки для виконання рутинних завдань, таких як:

✓ Виявлення загроз. Автоматично виявляє та позначає потенційні загрози безпеці на основі поведінкової аналітики та заздалегідь визначених правил.

✓ Керування оповіщеннями. Оптимізує процес управління оповіщеннями про загрози, зменшуючи кількість помилкових спрацьовувань і визначаючи пріоритетність критично важливих проблем.

✓ Реагування на інциденти. Автоматично запускає заздалегідь визначені дії реагування при виявленні загрози або аномалії, такі як ізоляція уражених систем або відкликання доступу.

✓ Застосування політик. Автоматично застосовує політики безпеки в мережі, забезпечуючи їх послідовне дотримання без ручного втручання.

✓ Звітність і відповідність вимогам. Створює регулярні звіти про стан безпеки та відповідність вимогам, полегшуючи управління та аудит.

✓ Моніторинг поведінки додатків. Постійно відстежує поведінку додатків на предмет відхилень від нормальних шаблонів, автоматизуючи процес виявлення аномалій.

✓ Оцінка ризиків. Автоматично оцінює та класифікує ризики на основі потенційного впливу, допомагаючи визначити пріоритети для їх усунення.

4. Регулярне навчання та розвиток навичок.

Дослідження ISC2 (International Information System Security Certification Consortium), присвячене кадровому забезпеченню кібербезпеки, показало, що глобальний дефіцит кадрів у сфері кібербезпеки становить 4,07 мільйона осіб, що підкреслює зростаючу потребу у підготовці кваліфікованих спеціалістів. Безперервне навчання має важливе значення для підтримання ефективності команд SOC:

- Регулярні навчальні програми. Потрібно проводити регулярні тренінги з новітніх тенденцій та технологій у сфері кібербезпеки.
- Розвиток навичок. Важливо заохочувати розвиток навичок у таких сферах, як реагування на інциденти, криміналістичний аналіз та полювання на загрози, а також виховуйте чемпіонів команди безпеки в таких напрямках, як тренінги з протидії ознакам фішингу та політики паролів компанії для всієї організації.

5. Впровадження багаторівневого підходу до реагування на інциденти

Згідно з Інститутом SANS (SysAdmin, Audit, Network, Security), багаторівневий підхід дозволяє краще розподіляти ресурси та експертизу в операціях SOC, а також забезпечує ефективну обробку інцидентів та оптимальне підвищення ефективності SOC:

- Рівень 1: Початковий аналіз та обробка загальних загроз.
- Рівень 2: Більш поглиблене розслідування складних загроз.
- Рівень 3: Поглиблене виявлення загроз та криміналістичний аналіз.

6. Зосередження на проактивному полюванні на загрози.

Згідно з нещодавнім звітом «Полювання на загрози» від Cybersecurity Insiders, 43% організацій стверджують, що полювання на загрози значно

покращило їхній захист:

- Регулярне полювання на загрози: Необхідно запланувати регулярні сесії для проактивного пошуку потенційних загроз. Такі заходи, як тренування «червоних команд», зміцнюють зв'язки, можуть бути цікавими і підвищують ефективність та швидкість реагування SOC.
- Інвестування в інструменти полювання на загрози: Використання вдосконалених інструментів для більш ефективного полювання на загрози. Ці інструменти аналізують мережеві та системні дані для виявлення аномалій, підозрілих шаблонів та індикаторів компрометації (IOC) на основі базової лінії затвердженої активності, допомагаючи упереджувати потенційні інциденти безпеки та запобігати атакам нульового дня до того, як вони переростуть у серйозні порушення.

7. Оптимізування комунікацій та співпраці.

Опитування McKinsey показало, що покращення комунікації та співпраці може підвищити продуктивність в організаціях на 20-25%, що робить ефективну комунікацію та співпрацю вирішальною:

- Інструменти для співпраці: Необхідно впроваджути інструменти, які сприяють легкій та швидкій комунікації між членами команди, навіть якщо це лише Teams, Discord або Slack.
- Міжвідомча співпраця: Рекомендовано сприяти співпраці з іншими відділами, такими як IT (Information Technology), HR (Human Resources) та юридичний. Це має вирішальне значення для команд безпеки, щоб забезпечити всебічну обізнаність про загрози, узгодити практики безпеки з цілями організації та сприяти єдиному підходу до кібербезпеки в межах всієї компанії.

8. Використання показники ефективності SOC

Експерт з безпеки Антон Чувакін з Gartner Insights неодноразово підкреслював важливість KPI для вимірювання та підвищення ефективності SOC, а вимірювання ефективності SOC є життєво важливим:

- Ключові показники ефективності (KPI): Важливо розробити KPI для вимірювання таких аспектів, як час відгуку, швидкість вирішення проблем і

навантаження на аналітика. Комунікація з командами SOC є важливимий аспектом, щоб дізнатися про такі показники:

✓ MTTD: Вимірює середній час, необхідний для виявлення загрози або інциденту безпеки.

✓ MTTR: Середній час, необхідний для реагування та усунення виявленого інциденту безпеки.

✓ Рівень вирішення інцидентів: Відсоток успішно вирішених інцидентів безпеки від загальної кількості зареєстрованих інцидентів. Точність сповіщень: Точність сповіщень про загрози у визначенні справжніх загроз порівняно з хибнопозитивними.

✓ Коефіцієнт успішності полювання на загрози: Вимірює ефективність проактивного полювання на загрози у виявленні прихованих загроз.

✓ Коефіцієнт дотримання нормативних вимог: Ступінь, до якого SOC дотримується нормативних стандартів і внутрішніх політик.

✓ Рівень обізнаності з питань безпеки: Оцінюється за допомогою регулярного тестування і вказує на ефективність програм навчання та підвищення обізнаності з питань безпеки.

✓ Час роботи/простою системи: Моніторинг часу роботи та простою критично важливих систем для оцінки впливу інцидентів безпеки.

✓ Оцінка задоволеності клієнтів: Відгуки внутрішніх та зовнішніх клієнтів про роботу та швидкість реагування SOC.

✓ Кількість інцидентів з плином часу: аналіз тенденцій кількості та серйозності інцидентів за певний період з метою виявлення закономірностей або сфер для покращення.

- Постійне вдосконалення: Рекомендовано використовувати ці показники для визначення сфер, які потребують вдосконалення.

9. Встановлення чітких процеси та SOP

Стандарт сертифікації ISO 27001 підкреслює важливість задокументованих процесів інформаційної безпеки для підвищення операційної ефективності, а чітко визначені процеси та стандартні операційні процедури (SOP, Standard

Operating Procedures) є ключовими:

- Задокументовані процеси: Переконайтеся, що всі процедури добре задокументовані та легко доступні. Це може включати в себе:
  - Протокол реагування на інциденти: Чіткі інструкції щодо виявлення, оцінки та реагування на інциденти кібербезпеки.
  - Процес сортування тривог: Кроки для оцінки та визначення пріоритетів для ефективного реагування на загрози безпеці.
  - Процедури ескалації: Визначені шляхи ескалації для різних типів інцидентів, включаючи те, кого і коли повідомляти.
  - Визначення ролей та відповідальності: Чіткий розподіл ролей та обов'язків в команді SOC.
  - План комунікації: Вказівки щодо внутрішньої та зовнішньої комунікації під час та після інцидентів безпеки.
  - Регулярний аудит безпеки: Процедури проведення періодичних аудитів безпеки та оцінки вразливостей.
  - Обробка даних та дотримання конфіденційності: Політика обробки конфіденційних даних, що забезпечує дотримання законів і правил про конфіденційність.
  - Практики безперервного моніторингу: Вказівки щодо постійного моніторингу мережі та систем організації.
  - Програми навчання та підвищення обізнаності: Регулярні тренінги та інструктажі для персоналу SOC щодо новітніх загроз та методів забезпечення безпеки.
  - Аналіз та звітність після інцидентів: Процедури проведення аналізу після інцидентів, документування отриманих уроків та звітування перед відповідними зацікавленими сторонами.
- Регулярні огляди: Регулярний перегляд та оновлення SOP з урахуванням нових загроз та технологій.

10. Пріоритет психічного здоров'я

Американський інститут стресу стверджує, що стрес на роботі є основним

джерелом проблем з психічним здоров'ям. Враховуючи сумнозвісний високооктановий характер роботи в команді SOC, не можна ігнорувати увагу до здоров'я команди, і лідери SOC повинні шукати рішення, як уникнути вигорання на роботі:

- Регулярні перерви: Важливо заохочувати регулярні перерви, щоб запобігти професійній втомі.
- Ресурси психічного здоров'я: Надавати доступ до ресурсів/підтримки психічного здоров'я та надихати культуру доступності.
- Заохочуйте баланс між роботою та особистим життям: Складайте справедливий графік роботи та сприяйте використанню права на відпустку, щоб співробітники могли встановити належні межі між роботою та особистим життям.

Підвищення ефективності операційного центру безпеки - це постійний виклик, який вимагає поєднання правильних інструментів, процесів, навичок і, що важливо, правильного підходу до добробуту команди. Реалізувавши ці кроки, організації можуть значно підвищити ефективність SOC, зробивши його кращим місцем для роботи та надійнішим захистом від кіберзагроз, що постійно змінюються.

Висновки до розділу 3

У даному розділі було проведено всебічний аналіз поточного стану системи Центру Оперативного Управління Безпекою (SOC) в організації, оцінено ключові показники ефективності SOC та надано рекомендації для покращення його ефективності.

Аналіз поточного стану показав, що існуюча система SOC має ряд сильних сторін, таких як наявність сучасного обладнання та кваліфікованого персоналу. Проте, виявлено й певні недоліки, включаючи недостатню автоматизацію деяких процесів та неефективне управління інцидентами, що може призводити до затримок у реагуванні на загрози.

Оцінка ключових показників ефективності SOC, зокрема середнього часу реагування на інциденти (MTTR), кількості помилкових спрацювань (false positives) та рівня задоволеності користувачів, вказала на необхідність вдосконалення певних аспектів діяльності SOC. Особлива увага була приділена показникам, що впливають на швидкість і точність виявлення та реагування на інциденти.

Для покращення ефективності системи SOC було запропоновано ряд рекомендацій. Серед них: підвищення рівня автоматизації за рахунок впровадження сучасних інструментів машинного навчання та штучного інтелекту, проведення регулярного навчання персоналу та оптимізація процесів обробки інцидентів. Також рекомендується вдосконалення процедур моніторингу та звітності для забезпечення більш прозорого та оперативного управління безпекою.

Впровадження запропонованих рекомендацій дозволить підвищити загальну ефективність системи SOC, що, в свою чергу, сприятиме кращому захисту інформаційних ресурсів організації від сучасних кіберзагроз.

ВИСНОВКИ

Кваліфікаційна робота присвячена дослідженню системи моніторингу й реагування на інциденти безпеки SOC, її теоретичних аспектів, ключових показників ефективності та практичної оцінки в конкретній організації. Проведене дослідження дозволило сформувати комплексне розуміння структури та функціонування SOC, а також розробити рекомендації для покращення її ефективності.

У першому розділі роботи були розглянуті теоретичні аспекти орпераційного центру безпеки, що включають сутність системи моніторингу й реагування на інциденти безпеки, організацію SOC, інструменти та технології, які використовуються в SOC, а також роль людей, як одного з головних компонентів цієї системи. Було визначено, що операційний центр безпеки є критично важливим елементом сучасної кібербезпеки, забезпечуючи постійний моніторинг, виявлення та реагування на інциденти безпеки.

Другий розділ присвячений ключовим показникам ефективності SOC, таким як швидкість виявлення інцидентів, час реагування на них, а також розробка ефективної процедури управління інцидентами інформаційної безпеки згідно зі стандартом ISO/IEC 27035. Було виявлено, що ефективність SOC значною мірою залежить від здатності швидко і точно ідентифікувати інциденти та оперативно на них реагувати, що потребує чітко налагоджених процесів та висококваліфікованих спеціалістів.

У третьому розділі було проведено оцінку ефективності операційного центру безпеки в організації. Аналіз поточного стану системи SOC дозволив виявити її сильні та слабкі сторони, а також оцінити ключові показники ефективності. На основі проведеного аналізу були розроблені рекомендації щодо покращення роботи SOC, включаючи впровадження нових технологій, оптимізацію процесів та підвищення кваліфікації персоналу.

1. Досліджено теоретичні аспекти системи моніторингу й реагування на інциденти безпеки SOC. Визначено сутність операційного центру як

комплексної системи, що включає процеси моніторингу, виявлення та реагування на інциденти інформаційної безпеки. Проаналізовано основні компоненти SOC: технології, процеси та людські ресурси.

2. Встановлено, що ефективна організація SOC базується на інтеграції сучасних технологій і методів управління безпекою. Виокремлено ключові інструменти та технології, що використовуються в операційному центрі безпеки, зокрема системи управління інформаційною безпекою та подіями інформаційної безпеки (SIEM), платформи для автоматизації й оркестрації безпеки (SOAR), а також засоби для аналізу загроз і виявлення аномалій.

3. Обґрунтовано, що людські ресурси є одним з головних компонентів SOC. Досліджено роль фахівців з безпеки, їхні компетенції та необхідність постійного навчання для підвищення рівня кваліфікації.

4. Проаналізовано ключові показники ефективності SOC, такі як швидкість виявлення інцидентів та час реагування на них. Визначено, що ці показники є критично важливими для оцінки ефективності системи та забезпечення оперативного реагування на загрози.

5. Розроблено ефективну процедуру управління інцидентами інформаційної безпеки згідно з ISO/IEC 27035, що включає етапи виявлення, аналізу, реагування та відновлення. Встановлено, що дотримання цієї процедури дозволяє забезпечити структурований підхід до управління інцидентами.

6. Проведено оцінку ефективності поточного стану SOC в організації. Виявлено сильні сторони, такі як використання сучасних технологій та наявність кваліфікованого персоналу, а також слабкі місця, включаючи недостатню автоматизацію процесів та недосконаліть управління інцидентами.

7. Оцінено ключові показники ефективності SOC в організації. Визначено, що середній час реагування на інциденти (MTTR) та кількість помилкових спрацювань є основними аспектами, що потребують покращення.

8. Рекомендовано впровадити ряд заходів для підвищення ефективності SOC, зокрема підвищення рівня автоматизації процесів, регулярне навчання персоналу та вдосконалення процедур моніторингу та звітності. Обґрунтовано,

що ці заходи дозволять підвищити швидкість і точність виявлення та реагування на інциденти.

Підсумовуючи, можна зробити висновок, що ефективна система моніторингу й реагування на інциденти безпеки є невід'ємною складовою захисту інформаційних ресурсів організації. Запропоновані у роботі рекомендації сприятимуть підвищенню рівня захищеності організації від кіберзагроз та забезпеченню стабільної роботи її інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Як побудувати та запустити центр безпеки (SOC) | Medium | URL: https://oleg-dubetcky.medium.com/%D1%8F%D0%BA-%D0%BF%D0%BE%D0%B1%D1%83%D0%B4%D1%83%D0%B2%D0%B0%D1%82%D0%B8-%D1%82%D0%B0-%D0%B7%D0%B0%D0%BF%D1%83%D1%81%D1%82%D0%B8%D1%82%D0%B8-%D1%86%D0%B5%D0%BD%D1%82%D1%80-%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8-soc-504266cefa53

2. Знайомство з процесами Security Operations Centre (SOC) та найкращі рекомендації для його ефективної роботи від Lepide | IITD | URL: https://iitd.com.ua/news/znajomstvo-z-procesami-security-operations-center-soc-ta-najkrashhi-rekomendacii-dlja-jogo-efektivnoi-roboti-vid-lepide/

3. 11 стратегій SOC від MITRE. Роадмап для вдумливої роботи українських CISO | Octava Defence | URL: https://octava.ua/11-strategij-soc-vid-mitre-roadmap-dlya-vdumlyvoyi-roboty-ukrayinskyh-ciso/

4. What is a security operations center (SOC)? | IBM | URL: https://www.ibm.com/topics/security-operations-center

5. What Is a Security Operations Center (SOC)? | Trellix | URL: https://www.trellix.com/securityawareness/operations/what-is-soc/

6. What is a security operations center (SOC)? | Microsoft | URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc

7. What is SOC? Types, Benefits and Security Challenges It Can Tackle | Infopulse | URL: https://www.infopulse.com/blog/soc-types-business-benefits

8. What are the key components of a security operations center? | Manage Engine | URL: https://www.manageengine.com/log-management/siem/components-of-security-operations-center-soc.html

9. Security Operations Center (SOC) Roles and Responsibilities | Check Point | URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/security-operations-center-soc-roles-and-responsibilities/

10. Challenges and best practices of security operations centers | Manage Engine | URL: https://www.manageengine.com/log-management/siem/challenges-and-best-practices-security-operations-center-soc.html

11. What are the tools and technologies used in SOCs? | Manage Engine | URL: https://www.manageengine.com/log-management/siem/soc-tools-technologies.html

12. Best SOC Tools to Strengthen Your Security Posture | Under Defense | URL: https://underdefense.com/blog/9-best-soc-tools-to-strengthen-your-security-posture/

13. Endpoint Detection and Response (EDR) Tools: How They Work and Solutions to Know | Cynet | URL: https://www.cynet.com/endpoint-protection-and-edr/top-6-edr-tools-compared/

14. What is EDR In Cyber Security? | Xcitium | URL: https://www.xcitium.com/edr-in-cyber-security/

15. Cybersecurity jargon busting: MDR, SOC, EDR, XDR, SOAR and SIEM | Airbus | URL: https://www.protect.airbus.com/blog/cybersecurity-jargon-busting-mdr-soc-edr-xdr-soar-and-siem/

16. What Is XDR? | Trellix | URL: https://www.trellix.com/security-awareness/endpoint/what-is-xdr/

17. XDR Security: How Will XDR Impact Your SOC? | BlueVoyant | URL: https://www.bluevoyant.com/knowledge-center/xdr-security

18. 3 Ways XDR Will Streamline Your SOC | Stellar Cyber | URL: https://stellarcyber.ai/learn/streamline-your-soc-with-xdr/

19. SOC and SIEM: The Role of SIEM Solutions in the SOC | exabeam | URL: https://www.exabeam.com/explainers/siem-security/the-soc-secops-and-siem/#:~:text=The%20SOC%20and%20Security%20Information%20and%20Event%20Management%20(SIEM)&text=The%20SIEM%20uses%20correlation%20and,contextual%20information%20to%20assist%20investigation.

20. The Top 11 SIEM Solutions | Expert Insights | URl: https://expertinsights.com/insights/the-top-siem-solutions/

21. What is SIEM? | Microsoft | URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem

22. What is security information and event management (SIEM)? | IBM | URL: https://www.ibm.com/topics/siem

23. Top 14 Vulnerability Scanners for Cybersecurity Professionals |Core Security| URL:https://www.coresecurity.com/blog/top-14-vulnerability-scannerscybersecurity-professionals

24. What is SOAR (security orchestration, automation and response)? | IBM | URL: https://www.ibm.com/topics/security-orchestration-automation-response

25. SOAR (security orchestration, automation and response) | TechTarget | URL: https://www.techtarget.com/searchsecurity/definition/SOAR

26. PDCA Cycle | ProductPlan | URL: https://www.productplan.com/glossary/pdca-cycle/

27. ISO/IEC 27035-1:2023— Information Security Management | ANSI | URL: https://blog.ansi.org/iso-iec-27035-1-2023-information-security-management/

28. MTTD vs MTTF vs MTBF vs MTTR | Alert Ops | URL: https://alertops.com/mttd-vs-mttf-vs-mtbf-vs-mttr/

29. MTTD (Mean Time to Detect): Defined and Explained | Plutora | URL: https://www.plutora.com/blog/mttd-mean-time-to-detect-defined-explained

30. Mean Time to Detect (MTTD) | Limble | URL: https://limblecmms.com/metrics/mean-time-to-detect/

31. What is mean time to repair (MTTR)? | IBM | URL: https://www.ibm.com/topics/mttr

32. Mean time to repair (MTTR) | Fiix | URL: https://fiixsoftware.com/maintenance-metrics/mean-time-to-repair-maintenance/

33. What is a KPI? | Qlik | URL: https://www.qlik.com/us/kpi#:~:text=KPIsKPI%20Examples-,What%20is%20a%20KPI%3F,the%20organization%20make%20better%20decisions.

34. KPIs: What Are Key Performance Indicators? Types and Examples | Investopedia | URL: https://www.investopedia.com/terms/k/kpi.asp

35. 6 Metrics & KPIs for measuring SOC success | Digital XRaid | URL: https://www.digitalxraid.com/6-soc-metrics-kpis/#:~:text=SOC%20metrics%20provide%20quantifiable%20data,your%20SOC%20meets%20predefined%20objectives.

36. Going beyond traditional metrics: 3 key strategies to measuring your SOC performance | NVISO Labs | URL: https://blog.nviso.eu/2021/05/26/going-beyond-traditional-metrics-3-key-strategies-to-measuring-your-soc-performance/

37. Eight Tips For Building An Effective SOC Strategy | Forbes | https://www.forbes.com/sites/forbestechcouncil/2023/07/27/eight-tips-for-building-an-effective-soc-strategy/?sh=5c465d3c6149

38. Ten Simple Steps to Improve SOC Efficiency | TrueFort | URL: https://truefort.com/improve-soc-efficiency/

39. How to improve the effectiveness of your SOC | Check Point | URL: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/how-to-improve-the-effectiveness-of-your-soc/

40. Boosting SOC Productivity in 2024: 5 Essential Tips for Security Operations Centers | Abnormal | URL: https://abnormalsecurity.com/blog/soc-productivity-tips-2024