МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____2022 р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, професор
_____ С.В. Легомінова
«___»_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
другого магістерського рівня вищої освіти
на тему:

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ SIEM ТА SOAR СИСТЕМ НА ПІДПРИЄМСТВІ

СТУДЕНТ: Стешенко Олександр Михайлович _____
(підпис)

КЕРІВНИК: к.в.н., доцент Якименко Юрій Михайлович _____
(підпис)

НОРМОКОНТРОЛЕР: _____
(підпис)

Київ – 2022

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Спеціальність 125 Кібербезпека
Спеціалізація Управління інформаційною безпекою
Другого магістерського рівня вищої освіти

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
_____ С.В.Легомінова

“___”_____2022 р.

ЗАВДАННЯ
на кваліфікаційну роботу

студента **Стешенка Олександра Михайловича**

Тема РОБОТИ “ Розробка рекомендацій щодо впровадження SIEM та SOAR систем на підприємстві”, затверджена наказом по університету від “ ” 2022 р. №

Термін здачі студентом оформленої роботи «08» 12 2022 р.

1. **Об'єкт дослідження:** процеси щодо впровадження і експлуатації SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки.
2. **Предмет дослідження:** методи та засоби впровадження та експлуатації SIEM та SOAR систем на підприємстві.
3. **Мета дослідження:** вивчення процесів впровадження SIEM та SOAR систем і їх ролей в управлінні інцидентами інформаційної безпеки на підприємстві.
4. **Перелік питань, які мають бути розроблені:**

4.1 провести аналіз процесів впровадження SIEM та SOAR систем на підприємстві;
4.2 дослідити методичні підходи щодо використання SIEM та SOAR систем на підприємстві;
4.3 визначити методи та засоби впровадження та експлуатації SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки;
4.4 провести дослідження та розробити рекомендації щодо впровадження SIEM та SOAR систем на підприємстві.

5. **Дата видачі завдання «**26» вересня 2022 р.

Науковий керівник _____ Ю.М.Якименко
(підпис)

Завдання прийнято до виконання _____ О.М. Стешенко
(підпис)

КАЛЕНДАРНИЙ ПЛАН
виконання кваліфікаційної роботи
студентом Стешенком Олександром Михайловичем
Дата видачі завдання: «26» вересня 2022 р.

№ з/п	Етапи роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	26.09.2022	
2.	Збір та аналіз літератури.	03.10.2022	
3.	Розділ 1. Аналіз процесів впровадження SIEM та SOAR систем на підприємстві	17.10.2022	
4.	Розділ 2. Методичні підходи щодо використання SIEM та SOAR систем на підприємстві	31.10.2022	
5.	Розділ 3. Дослідження і розробка рекомендацій щодо впровадження SIEM та SOAR систем на підприємстві	14.11.2022	
6.	Формулювання висновків за результатами проведеного дослідження	01.12.2022	
7.	Оформлення роботи	08.12.2022	
8.	Оформлення презентації	15.12.2022	
9.	Отримання рецензії на роботу.	23.12.2022	
10.	Захист в ДЕК	___01.2023	

Студент О.М. Стешенко
(підпис)

Науковий керівник Ю.М. Якименко
(підпис)

РЕФЕРАТ

Текстова частина магістерської роботи: 70 сторінок, 8 рисунків, 29 джерел.

Об'єкт дослідження – процеси щодо впровадження і експлуатації SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки.

Предмет дослідження – методи та засоби впровадження та експлуатації SIEM та SOAR систем на підприємстві.

Мета роботи – вивчення процесів впровадження SIEM та SOAR систем і їх ролей в управлінні інцидентами інформаційної безпеки на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

В роботі проведено аналіз процесів впровадження SIEM та SOAR систем на підприємстві.

Досліджено методичні підходи щодо використання SIEM та SOAR систем на підприємстві.

Визначено методи та засоби впровадження та експлуатації SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки

Досліджено процес впровадження SIEM та SOAR систем на підприємстві.

На основі досліджень проведених в роботі розроблено рекомендації щодо впровадження SIEM та SOAR систем на підприємстві.

Галузь використання – центри та відділи забезпечення кібербезпеки.

Ключові слова: АВТОМАТИЗАЦІЯ, КОРЕЛЯЦІЯ, ПОЛІТИКИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ПЛАН УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, СТАНДАРТНІ РОБОЧІ ПРОЦЕДУРИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, УГОДА ПРО РІВЕНЬ ОБСЛУГОВУВАННЯ, CSIRT, SIEM СИСТЕМА, SOAR СИСТЕМА, SOC

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

ГРІІБ – група реагування на інциденти інформаційної безпеки

ІБ – інформаційна безпека

ІТ -інформаційні технології

КГШР – комп'ютерна група швидкого реагування

ОЗ – обліковий запис

ОС – операційна система

ПК – персональний комп'ютер

СРП – стандартні робочі процедури

СУІБ - система управління інформаційною безпекою

СУІІБ – система управління інцидентами інформаційної безпеки

ЦП – центральний процесор

ШІ – штучний інтелект

ACL – Access Control List (список контролю доступу)

API – application programming interface (інтерфейс прикладного програмування)

AV – AntiVirus (антивірусна програма)

CERT – Computer Emergency Response Team (комп'ютерна група реагування на надзвичайні ситуації)

CSIRC – Computer Security Incident Response Capability (здатність реагування на інциденти комп'ютерної безпеки)

CSIRT – Computer Security Incident Response Team (група реагування на інциденти інформаційної безпеки)

DDoS – Distributed Denial of Service (розподілена атака на відмову в обслуговуванні)

DoS – Denial of Service (відмова в обслуговуванні)

IDS – Intrusion Detection System (система виявлення вторгнень)

MSS – Managed Security Service (керований сервіс безпеки)

MSSP – Managed Security Service Providers (постачальник керованих послуг безпеки)

MTTD – Mean time to detect (середній час виявлення)

MTTI – Mean time to investigate (середній час на розслідування)

MTTT – Mean time to triage (середній час сортування)

MTTQ – Mean time to qualify (середній час відповідності вимогам)

MTTR – Mean time to respond (середній час відповіді)

NDA – Non-disclosure Agreement (угода про нерозголошення)

POC – Proof of concept (перевірка концепції)

SIEM – Security information and event management (система управління інформацією про безпеку та подіями)

SLA – Service-level agreement (угода про рівень послуг)

SOAR – Security Orchestration, Automation, and Response (система оркестровки безпеки, автоматизації та реагування)

SOC – Security Operations Center (центр операційної безпеки)

ВСТУП

Актуальність дослідження. Реагування на непередбачувану або несанкціоновану подію або збій у роботі служби та повернення служби до її робочого стану здійснюється за допомогою управління інцидентами інформаційної безпеки. Найважливішим аспектом будь-якої події є її швидке вирішення, тому так важливо кодифікувати процес і слідувати йому.

Автоматизоване керування інцидентами інформаційної безпеки — це практика автоматизованого реагування на інциденти ІБ, щоб переконатися, що ключові події ідентифікуються та розглядаються найбільш ефективним і надійним способом.

Час має важливе значення, коли справа доходить до управління інцидентами. Отже, швидкість є головною перевагою автоматизованого керування інцидентами. Роботи, що потребують багато часу, можна виконувати значно швидше завдяки автоматизації.

Об'єкт дослідження – процеси щодо впровадження і експлуатації SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки.

Предмет дослідження – методи та засоби впровадження та експлуатації SIEM та SOAR систем на підприємстві.

Мета роботи – вивчення процесів впровадження SIEM та SOAR систем і їх ролей в управлінні інцидентами інформаційної безпеки на підприємстві.

Завдання магістерської роботи:

провести аналіз процесів впровадження SIEM та SOAR систем на підприємстві;

дослідити методичні підходи щодо використання SIEM та SOAR систем на підприємстві;

визначити методи та засоби впровадження та експлуатації SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки;

провести дослідження та розробити рекомендації щодо впровадження SIEM та SOAR систем на підприємстві.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: рекомендації щодо щодо впровадження SIEM та SOAR систем на підприємстві можуть бути використані у центрах та відділах кібербезпеки.

1 АНАЛІЗ ПРОЦЕСІВ ВПРОВАДЖЕННЯ SIEM ТА SOAR СИСТЕМ НА ПІДПРИЄМСТВІ

1.1 Організація побудови, впровадження та експлуатації системи управління інцидентами інформаційної безпеки

Типові політики інформаційної безпеки або захисні заходи інформаційної безпеки не можуть повністю гарантувати захист інформації, інформаційних систем, сервісів чи мереж. Після впровадження захисних заходів, ймовірно, залишаться слабкі місця, які можуть зробити забезпечення інформаційної безпеки неефективним, і, отже, лишається вірогідність виникнення інцидентів інформаційної безпеки. Інциденти інформаційної безпеки можуть надавати прямий чи опосередкований негативний вплив на бізнес-діяльність організації. Крім того, будуть неминуче виявлятимуться нові, раніше не ідентифіковані загрози. Недостатня підготовка конкретної організації до обробки таких інцидентів робить практичну реакцію на інциденти малоефективною і це потенційно збільшує ступінь негативного впливу на бізнес.

Таким чином, для будь-якої організації, що серйозно відноситься до інформаційної безпеки, важливо застосовувати структурний та плановий підхід до:

- виявлення, оповіщення про інциденти інформаційної безпеки та їх оцінку;
- реагування на інциденти інформаційної безпеки, включаючи активізацію відповідних захисних заходів для запобігання, зменшення наслідків та (або) відновлення після негативних впливів (наприклад, у сферах підтримки та планування безперервності бізнесу);
- отримання уроків з інцидентів інформаційної безпеки, запровадження превентивних захисних заходів та поліпшення загального підходу до менеджменту інцидентів інформаційної безпеки.

З метою виконання вищезазначених задач в організації має впроваджуватись система управління інцидентами інформаційної безпеки і створюватись група реагування на інциденти інформаційної безпеки.

Запровадження системи управління інформаційною безпекою є стратегічно важливим рішенням для організації. На створення та впровадження системи управління інформаційною безпекою організації впливають потреби та цілі організації, вимоги безпеки, організаційні процеси, що застосовуються, а також розмір і структура організації. Очікується, що всі ці фактори впливу змінюватимуться з часом[1].

Система управління інформаційною безпекою зберігає конфіденційність, цілісність і доступність інформації, застосовуючи процес управління ризиками, і дає впевненість зацікавленим сторонам, що ризики управляються належним чином.

Важливо, щоб система управління інформаційною безпекою була повністю інтегрована в процеси організації та загальну структуру управління, а також необхідно щоб інформаційна безпека враховувалась при розробці процесів, інформаційних систем і засобів контролю. Очікується, що впровадження системи управління інформаційною безпекою буде масштабовано відповідно до потреб організації.

Інцидент ІБ – одна (або серія) небажана та несподівана подія, яка може порушити безпеку інформаційних активів організації, негативно впливати на пов'язані з цими активами бізнес-процеси та системи і, як наслідок, завдати шкоди організації.

Система управління інцидентами інформаційної безпеки є базовою частиною загальної системи управління інформаційною безпекою (СУІБ) і дозволяє виявляти, враховувати, реагувати й аналізувати події та інциденти інформаційної безпеки.

Для опису процесу формування СУІБ використовується класична модель безперервного удосконалення процесів (рис. 1.1), що отримала назву від циклу

Шухарта-Демінга - модель PDCA (Plan - Плануй, Do - Виконуй, Check - Перевіряй, Act - Дій).

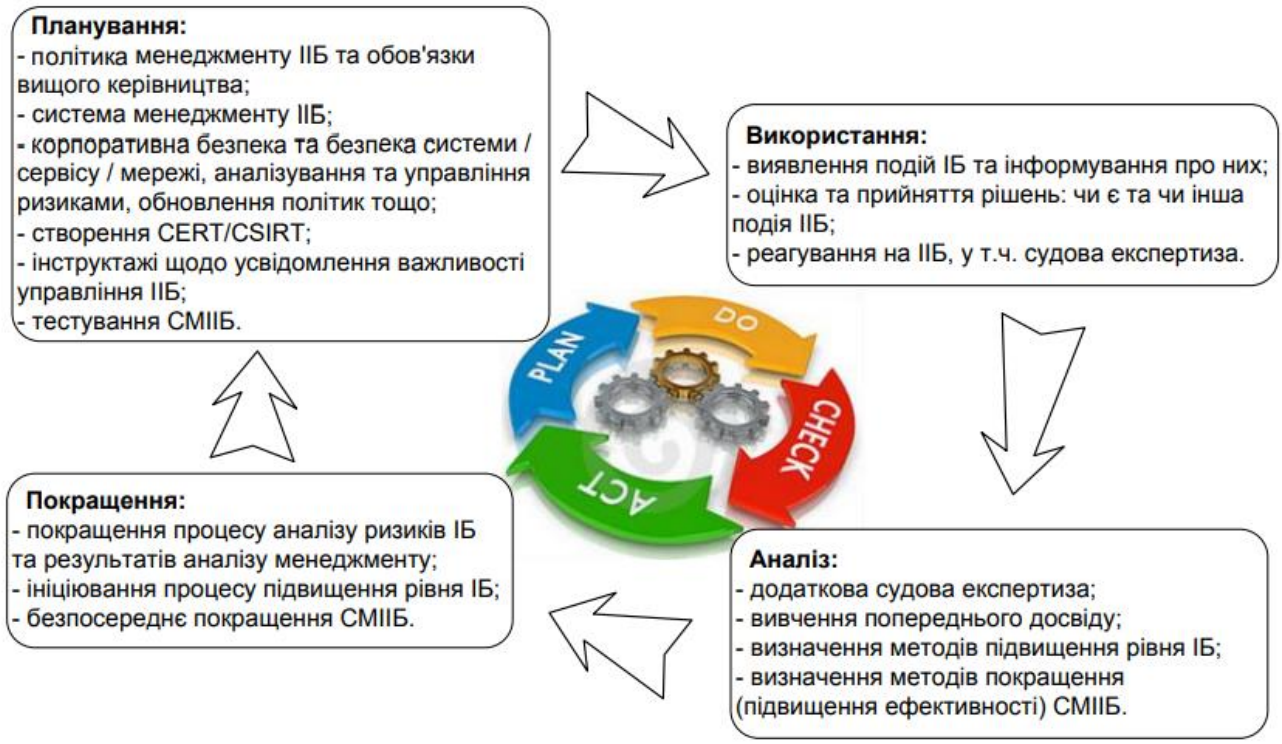

Рис. 1.1. Етапи формування СУІІБ відповідно до моделі PDCA[30]

Стандарт ISO/IEC 27001 описує модель PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою[2].

Для того, щоб процедура УІІБ було ефективною, всі ці етапи моделі PDCA повинні безперервно і послідовно повторюватися. Через певний час (як правило, через півроку або рік) необхідно знову переглянути перелік подій, названих інцидентами, форму звіту та ін., впровадити оновлену процедуру, перевірити її функціонування і ефективність, реалізувати запобіжні заходи. Таким чином, цикл моделі PDCA буде безперервно повторюватися і гарантувати чітке функціонування процедури управління інцидентами і, головне, її постійне удосконалення.

Детальні дії, процедури та інформація мають бути пов’язані з наступним[4]:

• планування та підготовка:

- стандартизований підхід до категоризації та класифікації подій/інцидентів інформаційної безпеки, щоб забезпечити послідовні результати. У будь-якому випадку рішення має ґрунтуватися на фактичних або

прогнозованих несприятливих впливах на бізнес-операції організації та відповідних рекомендаціях;

- база даних інформаційної безпеки, структурована для обміну інформацією, ймовірно, забезпечить можливість обмінюватися звітами/сповіщеннями, порівнювати результати, покращувати інформацію про попередження та забезпечувати більш точне уявлення про загрози та вразливі місця інформаційних систем. Фактичний формат і використання бази даних залежатиме від вимог організації. Наприклад, дуже невелика організація може використовувати документи, тоді як складна організація може використовувати більш складні технології, такі як реляційні бази даних і інструменти прикладних програм;

- вказівки щодо прийняття рішення про те, чи потрібна ескалація під час кожного відповідного процесу, і для кого, а також пов’язані процедури. На основі вказівок, наданих у плані управління інцидентами інформаційної безпеки, будь-хто, хто оцінює подію, інцидент або вразливість інформаційної безпеки, повинен знати, за яких обставин необхідно передавати питання на ескалацію та кому це слід передавати. Крім того, бувають непередбачені обставини, коли це може знадобитися. Наприклад, незначний інцидент інформаційної безпеки може перерости у значну або кризову ситуацію, якщо не впоратися належним чином, або незначний інцидент інформаційної безпеки, який не буде розглянуто протягом тижня, може стати серйозним інцидентом інформаційної безпеки;

- процедури, яких слід дотримуватися, щоб гарантувати, що всі дії з управління інцидентами інформаційної безпеки належним чином реєструються, а аналіз журналу проводиться призначеним персоналом;

- процедури та механізми для забезпечення підтримки режиму контролю змін, що охоплює відстеження подій інформаційної безпеки, інцидентів і вразливостей, а також оновлення звітів про інформаційну безпеку та оновлення самого плану;

- процедури аналізу доказів інформаційної безпеки;

- процедури та інструкції щодо використання систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS), гарантуючи, що відповідні правові та нормативні аспекти були враховані. Рекомендації повинні включати обговорення переваг і недоліків здійснення заходів відстеження зловмисників;

- керівництво та процедури, пов’язані з технічними та організаційними механізмами, які створені, впроваджені та експлуатуються з метою запобігання виникненню інцидентів інформаційної безпеки та зменшення їх вірогідності, а також для вирішення інцидентів інформаційної безпеки, коли вони виникають;

- матеріали для програми інформування та навчання з питань інформаційної безпеки, інцидентів і управління вразливістю;

- процедури та специфікації тестування плану управління інцидентами інформаційної безпеки;

- план організаційної структури управління інцидентами інформаційної безпеки;

- положення та обов'язки CSIRT в цілому та окремих членів;

- важлива контактна інформація;

- процедури та вказівки щодо обміну інформацією, узгоджені з офісом організації зі зв’язків з громадськістю, юридичним відділом і вищим керівництвом або відповідними відділами;

• Виявлення та повідомлення:

- вимоги до планування та підготовки до виявлення та звітування повинні дозволяти та підтримувати розробку та функціонування процесів пошуку або прийняття інформації про інциденти інформаційної безпеки;

- необхідно визначити критерії прийняття звіту про інцидент на основі повноти звіту та перевірки однієї чи кількох подій інформаційної безпеки. Щоб підтримати подальше прийняття рішень, мінімальні критерії для прийняття будь-якого попередження про виявлення події або звіту вручну повинні бути визначені до процесу планування та повинні включати принаймні ідентифікацію зачепленого середовища або активу, заяву про одну або більше підозрілих або підтверджених подій або кваліфікований тип події та отриманий час. Щоб

підтримувати прийняття рішень, процес планування повинен включати метод повернення виявлення або звітів, які містять недостатню інформацію;

- результати звітування або сповіщення мають бути визначені в контексті організації, політики реагування на інциденти та призначення технічних і управлінських ролей. Формат звітів і сповіщень має відповідати шкалі класифікації інцидентів або узгодженому пов’язаному показнику.

Основні моменти на етапі «Планування та підготовка» включають наступне[3]:

— політика управління інцидентами інформаційної безпеки та зобов’язання вищого керівництва;

— політики інформаційної безпеки, в тому числі ті, що стосуються управління ризиками, оновлені як на корпоративному рівні, так і на рівні системи, сервісу та мережі;

— план управління інцидентами інформаційної безпеки;

— створення групи реагування на інциденти (CSIRT);

— визначені зв'язки з внутрішніми та зовнішніми організаціями;

— технічне та інше забезпечення (включаючи організаційне та операційне);

— брифінги та тренінги щодо управління інцидентами інформаційної безпеки;

— тестування плану управління інцидентами інформаційної безпеки.

Політика управління інцидентами інформаційної безпеки організації повинна забезпечувати офіційно задокументовані принципи та наміри, які використовуються для керування прийняттям рішень, і забезпечувати послідовне та відповідне впровадження процесів, процедур тощо щодо цієї політики[4].

Будь-яка політика управління інцидентами інформаційної безпеки повинна бути частиною стратегії інформаційної безпеки для організації. Вона також має підтримувати існуючу місію організації та відповідати вже існуючим політикам і процедурам.

Організація повинна запровадити політику управління інцидентами інформаційної безпеки, яка визначає процеси, відповідальних осіб,

повноваження та лінії звітування (зокрема, основну контактну точку для повідомлення про підозрілі інциденти) у разі виникнення інциденту інформаційної безпеки. Політику слід регулярно переглядати, щоб переконатися, що вона відображає найновішу організаційну структуру, процеси та технології, які можуть вплинути на реагування на інциденти. Політика також повинна окреслювати будь-які ініціативи з підвищення обізнаності та навчання в організації, пов’язані з реагуванням на інциденти.

Організація повинна задокументувати свою політику щодо управління подіями, інцидентами та вразливими місцями інформаційної безпеки як окремий документ, як частину загальної політики системи управління інформаційною безпекою (згідно ISO/IEC 27001:2013) або як частину своєї Політики інформаційної безпеки (згідно ISO/IEC 27002:2013). Розмір, структура та бізнес-характер організації, а також рівень її системи управління інцидентами інформаційної безпеки є вирішальними факторами, які визначають, який із цих варіантів прийняти. Організація повинна спрямовувати свою політику управління інцидентами інформаційної безпеки на кожну особу, яка має законний доступ до її інформаційних систем і відповідних місць.

Успішна політика управління інцидентами інформаційної безпеки повинна бути створена та впроваджена як процес на рівні підприємства.

Організація повинна гарантувати, що її політика щодо управління інцидентами інформаційної безпеки схвалена членом вищого керівництва за зобов’язаннями всього вищого керівництва.

Політика управління інцидентами інформаційної безпеки повинна бути доступною для кожного співробітника та підрядника, а також повинна розглядатися на інструктажах і тренінгах з інформаційної безпеки.

Політика управління інцидентами інформаційної безпеки має бути високого рівня. Детальна інформація та покрокові інструкції повинні бути включені в серію документів, які складають план управління інцидентами інформаційної безпеки.

Організація повинна включити вміст управління інцидентами інформаційної безпеки у свої політики інформаційної безпеки на корпоративному рівні, а також на рівнях конкретної системи, сервісу та мережі та пов’язати цей вміст із політикою управління інцидентами.

Організація повинна оновлювати та підтримувати свою корпоративну інформаційну безпеку та політику управління ризиками, а також політику інформаційної безпеки конкретної системи, служби чи мережі разом, щоб гарантувати, що вони залишаються послідовними та актуальними. Ці політики корпоративного рівня мають прямо посилатися на політику управління інцидентами інформаційної безпеки та відповідні плани.

Політика корпоративного рівня повинна містити вимогу щодо встановлення відповідних механізмів перевірки. Ці механізми перевірки повинні гарантувати, що інформація, отримана від виявлення, моніторингу та вирішення інцидентів інформаційної безпеки, а також від роботи з повідомленими вразливими місцями інформаційної безпеки, використовується як вхідні дані для процесу, розробленого для підтримки постійної ефективності політик.

Метою плану управління інцидентами інформаційної безпеки є документування дій і процедур для роботи з подіями, інцидентами та вразливими місцями інформаційної безпеки та повідомлення про них[4]. План випливає з політики управління інцидентами інформаційної безпеки та ґрунтується на ній.

Загалом планова документація повинна охоплювати численні документи, включаючи форми, процедури, організаційні елементи та інструменти підтримки для виявлення та звітування, оцінки та прийняття рішень, пов’язаних із реагуванням на інциденти інформаційної безпеки та винесення уроків з них.

План управління інцидентами інформаційної безпеки починає діяти щоразу, коли виявляється подія інформаційної безпеки або повідомляється про вразливість інформаційної безпеки.

Планування та підготовка плану реагування на інциденти має здійснюватися власником процесу з чіткою метою або набором цілей для

реагування на інциденти в межах визначеного обсягу на основі політики управління інцидентами інформаційної безпеки.

Терміни та визначення повинні бути нормалізовані між членами CSIRT та партнерськими організаціями. Це включає в себе назви та ідентифікатори для організацій і команд, інформаційних активів, бізнес-процесів тощо. Якщо термінологія складна або схильна до неправильного тлумачення, план управління інцидентами повинен містити стандартні терміни та визначення в глосарії.

Ролі та відносини із зовнішніми CSIRT та іншими організаціями реагування, а також структури та межі реагування мають бути визначені власником процесу управління інцидентами.

Відповідальності залучених сторін можуть збігатися і повинні бути скориговані консенсусом у процесі планування управління інцидентами. Якщо межі прийняття рішення щодо реагування на інциденти збігаються, план має визначити відповідальну сторону.

Залучені сторони та зовнішні CSIRT часто мають різні показники. Учасники планування повинні оцінити доступні показники, надані їхніми відповідними сторонами або зовнішніми організаціями, і погодитися консенсусом щодо певного набору(ів) існуючих показників або погодитися зв’язати різні показники за допомогою оборотного відображення. Незалежно від підходу, план має вибрати або зв’язати кількісні показники так, щоб їх обсяги були ідентичними, а також вибрати або зв’язати якісні показники з остаточною еквівалентністю.

План також має враховувати будь-яких сторонніх користувачів, а також інциденти інформаційної безпеки та пов’язані з ними вразливості, про які повідомляють сторонні організації та організації, що надають інформацію про інциденти та вразливості державної та комерційної інформаційної безпеки.

Якщо очікується, що залучені сторони братимуть активну участь у обробці інцидентів інформаційної безпеки, слід чітко розподілити ролі та обов’язки та повідомити про них усіх.

Розподіл ролей має супроводжуватися узгодженим протоколом передачі інциденту, щоб обмін інформацією відбувався належним чином. Якщо це доцільно та можливо, передача інциденту та обмін інформацією мають бути автоматизовані, щоб прискорити процес. Такий сценарій може виникнути, якщо деякі можливості організації або CSIRT передано третій стороні.

Зміст плану управління інцидентами інформаційної безпеки має надавати огляд, а також визначати детальні заходи. Як зазначалося вище, планова документація повинна охоплювати декілька документів, включаючи форми, процедури, організаційні елементи та інструменти підтримки.

Метою створення ГРІІБ є забезпечення організації відповідним персоналом оцінки, реагування на інциденти ІБ та отримання уроків з них, а також необхідної координації, менеджменту, зворотного зв'язку та процесу передачі інформації. Члени ГРІІБ можуть брати участь у зниженні фізичної та фінансової шкоди, а також шкоди для репутації організації, пов'язаної з інцидентами ІБ[5].

Склад та кількість персоналу, а також структура ГРІІБ повинні відповідати масштабу та структуру організації. ГРІІБ може бути ізольованою командою або відділом, персоналом цієї групи може виконувати інші обов'язки, і навіть залучати співробітників із різних підрозділів організації. У багатьох випадках ГРІІБ може бути діючою групою, яку очолює старший керівник. Вищому керівнику надають допомогу фахівці з конкретних питань, наприклад, відображення атак шкідливих програм, які залучаються залежно від типу інциденту. Залежно від чисельного складу організації співробітники ГРІІБ можуть виконувати кілька функцій всередині ГРІІБ. У ГРІІБ можуть також залучатися службовці з різних підрозділів організації (наприклад, бізнес-операцій, IT/телекомунікацій, аудиту, відділу кадрів та маркетингу).

Члени групи повинні бути доступні для контакту так, щоб їхні імена та імена осіб, які їх заміняли, а також подробиці про контакт з ними були доступними всередині організації. Наприклад, у документації системи менеджменту інцидентів ІБ мають бути чітко зазначені необхідні деталі,

включаючи будь-які документи щодо процедур та форми звітів, але не в положеннях політики.

Необхідно підтримувати єдину структуру планів безперервності бізнесу, щоб забезпечити послідовність усіх планів, узгоджено відповідати вимогам інформаційної безпеки та визначити пріоритети для тестування та обслуговування[12].

Кожен план безперервності бізнесу повинен описувати підхід до безперервності, наприклад, підхід до забезпечення доступності та безпеки інформації або інформаційної системи. У кожному плані також має бути визначено план ескалації та умови його активації, а також осіб, відповідальних за виконання кожного компонента плану.

Плани безперервності бізнесу слід перевіряти та регулярно оновлювати, щоб переконатися, що вони актуальні та ефективні.

Тестування плану безперервності бізнесу має гарантувати, що всі члени групи відновлення та інший відповідний персонал знають про плани та свою відповідальність за безперервність бізнесу та інформаційну безпеку, а також знають свою роль під час запуску плану.

У графіку тестування для плану забезпечення безперервності бізнесу має бути зазначено, як і коли кожен елемент плану має бути перевірений.

Необхідно використовувати різноманітні методи, щоб забезпечити впевненість у тому, що план працюватиме у реальному житті. Вони повинні включати:

- тестування різних сценаріїв (обговорення механізмів відновлення бізнесу на прикладах переривань процесів);

- моделювання (зокрема, для навчання людей їхнім ролям після надзвичайних ситуацій);

- тестування технічного відновлення (забезпечення ефективного відновлення інформаційних систем);

- тестування відновлення на альтернативному місці (запуск бізнес-процесів паралельно з операціями відновлення поза основних ресурсів);

- випробування обладнання та послуг постачальника (переконання, що послуги та продукти, що надаються сторонніми компаніями, відповідатимуть договірним зобов’язанням);

- тестування в умовах максимально наближених до реальних (перевірка того, що організація, персонал, обладнання, приміщення та процеси можуть впоратися з перервами).

Ці методи можуть бути використані будь-якою організацією. Їх слід застосовувати у спосіб, який відповідає конкретному плану відновлення. Результати випробувань повинні бути зафіксовані та, якщо необхідно, вжиті заходи для покращення планів.

Слід покласти відповідальність за регулярні перегляди кожного плану безперервності бізнесу. Виявлення змін у бізнес-угодах, які ще не відображені в планах безперервності бізнесу, повинно супроводжуватися відповідним оновленням плану. Цей офіційний процес контролю за змінами має гарантувати, що оновлені плани розповсюджуються та підкріплюються регулярними переглядами повного плану.

Прикладами змін, у яких слід розглянути оновлення планів безперервності бізнесу, є придбання нового обладнання, модернізація систем і зміни в:

- кадровому складі;
- адресах або номерах телефонів;
- бізнес-стратегії;
- розташуванні ресурсів;
- законодавстві;
- підрядниках, постачальниках та ключових клієнтах;
- запровадженні нових або видаленні старих процесів;
- ризиках (операційних і фінансових).

1.2. Процеси під час впровадження та експлуатації SIEM систем

SIEM (Security information and event management) у комп'ютерній безпеці є програмними продуктами, які об'єднують управління інформаційною безпекою SIM (англ. Security information management) та управління подіями безпеки SEM (англ. Security event management). Технологія SIEM забезпечує аналіз в реальному часі подій (тривог) безпеки, отриманих від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для журналювання даних і генерації звітів в цілях сумісності з іншими бізнес-даними[6].

Системи безпеки та управління подіями (SIEM) широко розгортаються як потужний інструмент для запобігання, виявлення та реагування на кібератаки. Рішення SIEM перетворилися на комплексні системи, які забезпечують широку видимість для виявлення областей високого ризику та проактивно зосереджені на стратегіях пом’якшення, спрямовані на зменшення витрат і часу на реагування на інциденти[7].

Зараз системи SIEM і пов’язані з ними рішення повільно зближуються з інструментами аналізу великих даних. Ризики кібербезпеки надзвичайно зросли за останні роки, головним чином через активізацію державних кібервійськ і кіберзлочинців. Зловмисники стали більш досвідченими та небезпечними, а їх належне та своєчасне виявлення стало справжнім викликом. Прикладами поточних інцидентів кібербезпеки є: атаки програм-вимагачів; зловмисне програмне забезпечення, яке впливає на здатність підприємства вести бізнес і операції; фішингові кампанії, спрямовані на керівників, помічників керівників, інженерів SCADA, IT-адміністраторів або інших привілейованих користувачів; інциденти зламу ділової електронної пошти, включаючи захоплення облікового запису або видавання себе за керівників; витік даних і крадіжки; соціальна інженерія для збору конфіденційної інформації від персоналу.

Згідно з нещодавнім звітом NIST, рішення з кібербезпеки в промислових системах управління повинні забезпечувати виявлення поведінкових відхилень у режимі реального часу, забезпечувати швидке управління інцидентами та дозволяти інтелектуальну візуалізацію мережі та всіх її взаємопов’язаних вузлів.

Системи безпеки інформації та керування подіями (SIEM) розглядають вищезазначені можливості як вбудовані функції.

Система управління інформацією про безпеку та подіями (SIEM) є відносно новою у сфері інформаційних технологій (IT). Ранні компоненти систем SIEM почали з’являтися в різних формах 10–20 років тому, але вони лише почали добре інтегруватися, знаходячи свою опору в організаціях. Система SIEM — це комплексний набір технологій, розроблених для забезпечення бачення та чіткості корпоративної IT-системи в цілому, що також приносить користь аналітикам безпеки та IT-адміністраторам. Це потужне доповнення до IT-інфраструктури практично кожного малого, середнього чи великого підприємства, департаменту чи державного органу[8].

Фахівці з безпеки та аналітики використовують систему SIEM для моніторингу, виявлення, документування та іноді реагування на порушення безпеки. Деякі з цих подій безпеки очевидні, як-от навмисні та зловмисні атаки типу «відмова в обслуговуванні» (DoS) і спалахи вірусів. Система SIEM також може ідентифікувати більш невловимі події безпеки. Багато подій настільки непомітні або настільки приховані тисячами подій за секунду, що без допомоги потужної та точно налаштованої системи SIEM вони залишилися б абсолютно непоміченими. Ці більш невловимі події безпеки включають порушення політики, спроби неавторизованого доступу та спроби висококваліфікованого та цілеспрямованого зловмисника, який методично та непомітно проникає у IT-середовище.

Головне завдання аналітиків із безпеки, які використовують систему SIEM, — зменшити кількість хибно-позитивних сповіщень, які є копицею сіна у загальновідомій концепції «голка в стозі сіна». Менш складні системи безпеки, такі як система виявлення вторгнень (IDS), відомі (або, точніше, сумно відомі) тим, що сповіщають про багато хибно-позитивних (False Positive) подій. Ці численні хибно-позитивні сповіщення витрачають час і енергію аналітика безпеки та часто притупляють зосереджену увагу аналітика, що значно підвищує

шанси не помітити рідкісніше та важливіше справді-позитивне (True Positive) попередження.

Багато пристроїв, як-от IDS, зменшують хибно-позитивні сповіщення, застосовуючи загальне «ігнорування» до певних подій або позначаючи джерело чи трафік як «дружні». Ці дозволи подій і трафіку далекі від тонкого налаштування; вони досить часто занадто широкі та створюють канали, які можуть дозволити зловмисникам вільно та непомічено проникнути у IT-системи. Завдяки більш складній SIEM системі зменшення хибно-позитивних сповіщень досягається шляхом ретельного створення фільтрів і корельованих правил подій, які часто називають вмістом SIEM, щоб ідентифікувати та попереджати лише про ті високопріоритетні події безпеки, належним чином перевіряючи та точно ігноруючи більшість хибно-позитивних подій.

Хоча SIEM розроблено та націлено на аспекти безпеки IT-системи, персонал мережевих операцій та IT-адміністратори можуть використовувати SIEM у своїй рутинній та менш насиченій подіями «операційній» ролі. IT-операції можуть використовувати SIEM для виявлення різних типів операційних проблем у мережі, як-от вимкнені сервери та несправні чи неправильно налаштовані системи, програми та пристрої. SIEM можна використовувати для моніторингу звичайних потреб IT-системи, наприклад, додаткових вимог до потужності, проблем з навчанням користувачів і роботі програм із помилками, які можуть потребувати виправлення, оновлення або заміни.

На додаток до цих переваг і можливостей внутрішньої IT-безпеки та мережевих операцій, є аспекти потужної SIEM системи, які почали досліджувати лише нещодавно. Мислячи поза межами власної IT-інфраструктури та повертаючи погляди на SIEM в іншому напрямку, відділи маркетингу, власники бізнесу та навіть уряди можуть відстежувати та отримувати сповіщення майже в реальному часі про важливу зовнішню діяльність, яка може вказувати на значні зміни у конкурентів та на ринку. Системи SIEM можуть бути налаштовані назовні на стрічки новин, пошукові системи і запити до бібліотек та сповіщати про зміни в тенденціях і збільшення специфічних або тематичних типів запитів.

Використовуючи SIEM для збору інформації про ринок, бізнес або політику, можливо ідентифікувати та кількісно оцінити зовнішні сили, які включають незначні та значні зміни на внутрішньому ринку, зовнішніх ринках, глобальній економіці та навіть діючих політичних силах. Використовуючи систему SIEM, можливо отримати інформацію про невидимі в іншому випадку дії конкурентів або іноземних урядів.

Процес впровадження складається з декількох послідовних етапів [9]:

- оцінка масштабу та інфраструктури;

- прийняття рішення про спосіб впровадження;

- формування та затвердження технічного завдання;

- установка та базове налаштування SIEM-системи, тобто необхідно налаштувати SIEM-сервер, прописати логи, виконати специфічні налаштування відносно мережі підприємства;

- налаштування джерел подій;

- написання можливих додаткових правил реагування на інциденти, тому що “з коробки” SIEM-система не буде працювати належним чином;

- тестова експлуатація і накопичення статистики. В загальному слід відвести на цей пункт декілька місяців;

- корегування та доповнення правил кореляції. Нерідко виконується паралельно з попереднім етапом;

- завершення тестової експлуатації. Слід залишити декілька днів на фінальні корективи;

- підготовка до об'єднання SIEM-систем з системами, які знаходяться на підприємстві.

На сьогодення проблеми впровадження виникають на перших етапах, так як вони вимагають найбільшої уваги з урахуванням всіх необхідних параметрів режиму їх функціонування і мають обмеження на технічне забезпечення, а також налаштування в SIEM-системі великої кількості конфігураційних атрибутів. Первинне налаштування проекту являє собою набір дій по налаштуванню

конфігураційних файлів системи. Складність побудови дієвої SIEM-системи пов’язана з необхідністю збору та аналізу подій різних типів, тому потребує:

- високої кваліфікації фахових спеціалістів по налаштуванню коректної конфігурації;

- виділення нестандартних апаратних платформ, що може обмежити впровадження SIEM-системи у вже існуючу інформаційну структуру підприємства;

- окрім цього, також достатньо високі вимоги до технічних характеристик апаратних платформ, на яких розгортаються SIEM-системи. Це може призводити до того, що первинна цінна проекту буде збільшуватись;

- велика трудомісткість розробки технічної документації на багатокомплексну SIEM-систему і, відповідно, потенційна наявність значної кількості помилок може збільшити терміни впровадження системи.

До основних проблем при інтегруванні SIEM-системи в інформаційну структуру підприємства відносяться:

• оцінка масштабу. Від масштабу інформаційної структури підприємства, в яку інтегруватиметься SIEM-система, залежить подальше планування, впровадження та зростання проекту. Коректна оцінка масштабу впливає на вибір рішення, архітектурні вимоги, необхідну кількість співробітників. Перед впровадженням SIEM-системи на підприємство, слід оцінити [10]:

- об'єм даних, які оброблятиме система протягом місяця (вимірюються в гігабайтах в місяць);

- кількість джерел, що надсилатимуть дані в систему;

- кількість співробітників, які працюватимуть з системою;

• надлишкова інформація. Від кількості логів безпеки залежить навантаження на SIEM-систему. SIEM отримує інформацію з великої кількості різних джерел, до прикладу таких як:

- IDS

- IPS

- Журнали аудиту

- Брандмауери
- Комутатори
- Маршрутизатори
- Сканери уразливості
- Антивіруси

Наприклад, одна з найважливіших задач для IDS - отримання високого проценту істинно позитивних подій. Істинно позитивні події - коли відбувся негативний інцидент і IDS система виявила це. Цей процент досягається за рахунок потоку хибно позитивних спрацювань, де хибно позитивні спрацювання – коли система генерує попередження, але активність насправді не була зловмисною. Якщо передача інформації від IDS до SIEM-системи буде налаштована не досить коректно, то надсилатиметься надлишкова кількість подій, яка призведе до переповнення зайвою інформацією, що не потребує уваги. Це в свою чергу збільшить час роботи аналітика на обробку подій, які слід було ігнорувати. Систему слід налаштовувати таким чином, щоб вона була орієнтована на попередньо запланований результат;

• кваліфікація співробітників. Для успішного впровадження і роботи SIEM-системи співробітники повинні бути компетентні та мати підготовку до роботи з SIEM. SIEM-системи самі по собі працювати не можуть. Вони потребують постійного доналаштування і регулярного обслуговування для правильного реагування на події, які виникають в системі, та коректної обробки вхідних даних. Окрім цього, є необхідність в людській участі для розслідування інцидентів і усування проблем, що виникатимуть в процесі експлуатації[11];

• час необхідний на впровадження. Початкове налаштування SIEM в більшості випадків не викликає складнощів. На те щоб підключити і налаштувати отримання інформації від перших джерел даних зазвичай виділяється пару місяців і, на перший погляд, це забезпечує великі успіхи в досягненні цілей впровадження SIEM-системи. Однак, забезпечення системи необхідними для роботи даними, її тонке налаштування, редагування вбудованих і написання власних конфігураційних файлів та повна інтеграція в роботу може

зайняти рік або навіть більше. Як правило, чим надійніше SIEM-система, тим більше часу повинен витратити аналітик на її вивчення через те, що потрібен час на освоєння інструменту.

1.3 Процеси під час впровадження та експлуатації SOAR систем

Ландшафт кібербезпеки постійно розвивається. Кожне покращення безпеки призводить до покращення зловмисного програмного забезпечення, яке підриває цю безпеку. Сучасне зловмисне програмне забезпечення обходить традиційні профілактичні технології, рухається вбік несподіваними шляхами, перебуває в стані очікування протягом тривалого часу та може вживати контрзаходів проти легких або простих процесів виявлення. Сучасні зловмисники використовують широкий спектр методів для викрадання даних, порушення роботи служб, шахрайства або просто викрадення ресурсів. Що довше організації виявляють зловмисне програмне забезпечення, то більше часу мають зловмисники, щоб досягти своїх цілей і отримати доступ до цільових систем[12].

У відповідь на сучасні загрози кібербезпеці багато компаній створюють центр операційної безпеки (SOC) - організацію, відповідальну за управління безпекою компанії. SOC складається з команди, яка може бути місцевою, розподіленою, включати кілька фахівців або кілька департаментів.

Просте створення SOC підвищує кібербезпеку до рівня, який підвищує видимість і контроль за ситуацією. Зрештою, легше фінансувати SOC, ніж підтримувати одного аналітика, який намагається виконувати «додаткову роботу».

Ефективний SOC працює цілодобово та має аналітиків, які володіють інструментами та процесами, необхідними для реагування на загрози. Постійний моніторинг і аналіз мережевої активності допомагають гарантувати своєчасне виявлення та локалізацію інцидентів безпеки, таким чином зменшуючи ризик викрадання даних.

Оперативний процес усунення загроз у SOC складається з наступного:

- система управління інформацією про безпеку та подіями (SIEM) збирає, аналізує та збагачує дані журналу судової експертизи;

- SIEM виконує машинну аналітику для пошуку потенційних проблем, які кваліфікуються як подія безпеки;

- коли SIEM виявляє подію безпеки, він створює сповіщення для аналізу та реагування;

- фахівець із безпеки сортує сигнали тривоги, додаючи контекст, оцінюючи ризик і визначаючи вплив;

- аналітик безпеки вирішує сигнали тривоги, усуваючи проблему;

- аналітик безпеки переглядає та змінює засоби контролю безпеки, якщо це необхідно, щоб запобігти повторенню тієї самої події.

Ефективний, дієвий та добре керований SOC вимірює та зменшує такі показники, як показано на рисунку 1.2:

- Mean time to triage (MTTT): MTTT – це середній час, необхідний для аналізу даних безпеки та створення сповіщення;

- Mean time to detect (MTTD): MTTD – це середній проміжок часу, який потрібен SOC для виявлення потенційного інциденту безпеки. Чим швидше SOC виявить атаку, тим швидше SOC зможе її пом’якшити;

- Mean time to qualify (MTTQ): MTTQ — це середній проміжок часу, який потрібен SOC, щоб визначити, що сповіщення системи безпеки є справді позитивним (а не помилковим) і потребує розслідування;

- Mean time to investigate (MTTI): MTTI – це середня кількість часу, який потрібен SOC для вивчення та розуміння загрози, щоб визначити, як найкраще її пом’якшити;

- Mean time to respond (MTTR): MTTR — це середній час, який потрібен SOC для припинення атаки. Здатність SOC своєчасно зупиняти атаку допомагає зменшити ризик безпеки.

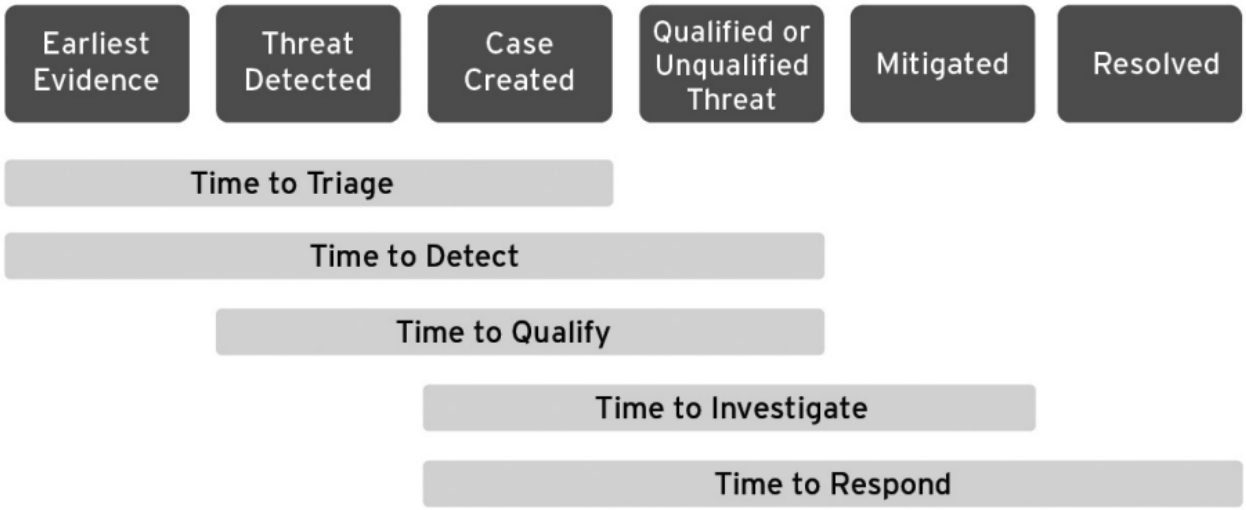

Рис. 1.2. Етапи процесу забезпечення безпеки[12]

Добре керований SOC також демонструє такі характеристики:

- ефективні робочі процеси реагування на інциденти. Процеси та процедури окреслюються напередодні інциденту з чітко визначеними завданнями. Також визначено обов'язки членів команди, тому завдання можна розподіляти швидко й точно;

- повторювані процеси та процедури. Робочі процеси реагування на інциденти узгоджені. Аналітики безпеки та групи реагування на інциденти дотримуються тих самих кроків для подібних інцидентів;

- оптимізована автоматизація. Якомога більше нудних ручних завдань автоматизовано, що дозволяє аналітикам працювати ефективніше та зосереджуватися на більш складних завданнях;

- послідовна звітність. Звіти про показники, описані раніше, дозволяють командам і керівництву SOC контролювати ефективність SOC і вимірювати покращення.

Хоча було б непогано, якби SOC не стикалися з проблемами, описаними раніше, факт полягає в тому, що ці проблеми ніколи повністю не зникають. По-перше, керівники з безпеки завжди будуть боротися з обмеженнями ресурсів. Організація навряд чи здійснить організаційну перебудову лише для того, щоб задовольнити потреби SOC. Тим не менш, без виконання певних умов неможливо побудувати ефективний SOC. Керівникам безпеки потрібно прагматично подумати про те, що необхідно для його створення:

- необхідність створювати визначені робочі процеси для навчання та скерування аналітиків. Визначені робочі процеси направляють аналітиків через послідовний, повторюваний процес під час реагування на загрозу кібербезпеці. Ця структура гарантує, що аналітики не пропустять жодного кроку, і допомагає масштабувати SOC, дозволяючи новим аналітикам і аналітикам рівня 1 виконувати ті самі процеси, що й більш просунуті аналітики;

- необхідність запроваджувати автоматизацію, щоб зменшити зусилля, необхідні для ручного додавання контексту, аналізу та реагування на загрози. Ручні завдання низького рівня, які відривають аналітиків від роботи вищого рівня, необхідно автоматизувати. Навіть процеси з діями, які повинні бути затверджені перед їх виконанням, повинні бути максимально автоматизовані. Зменшивши ручну роботу, аналітики можуть зосередитися на реагуванні на складні інциденти, що потребують поглиблених навичок і креативності;

- необхідність використовувати керування справами (case management), щоб відстежувати дії, заходи та потреби. Управління справами дозволяє організаціям значно підвищити зрілість і ефективність своїх операцій безпеки та заходів з реагування на інциденти. Матеріали справ служать централізованим місцем для взаємодії, а також архівом усієї інформації, пов’язаної з попередніми розслідуваннями. Це полегшує аналітикам створення та відстеження заходів щодо виправлення та відновлення під час розслідування загроз. Таким чином, управління справами допомагає командам у їхніх зусиллях щодо відповідності нормативним вимогам, оскільки мандати щодо відповідності все частіше вимагають відстеження реагування на виникаючи інциденти. Нарешті, оптимізуючи розслідування, управління справами допомагає командам швидше вирішувати інциденти;

- необхідність використовувати керування заявками (ticket management), щоб допомогти прискорити пом’якшення загроз і реагування на інциденти. Аналітики та спеціалісти з реагування на інциденти можуть легко надсилати запити в службу IT-підтримки для постановлення завдань, які є частиною робочого процесу реагування;

- необхідність відстежувати показники, щоб оцінити ефективність. Існує вдалий вислів, що описує дану необхідність: «Якщо ви не можете виміряти це, ви не можете покращити». SOC потребує фіксації показників і звітів про MTTD і MTTR, щоб допомогти командам працювати ефективніше та зменшити ризик, створений загрозами безпеці, які вже є в мережі.

Усі ці питання можливо досить ефективно вирішити за допомогою застосування системи оркестровки безпеки, автоматизації та реагування (англ. SOAR - Security Orchestration, Automation, and Response).

SOAR - це технологія, яка дозволяє компаніям збирати дані про загрози та попередження, а також дозволяє аналітикам реагувати на загрози за менший час і автоматизувати повторювані завдання[13].

SOAR — це термін, розроблений Gartner , який використовується для опису трьох відмінних можливостей програмного забезпечення. Оркестровка, як термін, охоплює управління загрозами та вразливостями, що включає всі технології, які допомагають у вирішенні кіберзагроз. Автоматизація відноситься до автоматизації безпеки, яка описує процес використання прогресивної автоматизації та машинного навчання для автоматизації окремих сфер безпеки. Термін реагування означає реагування на інцидент безпеки, яке детально вимірює те, як організація реагує на загрози, щоб використовувати цю інформацію для стратегічного підвищення ефективності операцій з підвищення безпеки (SecOps). Ці три елементи разом складають комплексну технологію, відому як SOAR.

SOC, які борються з обмеженнями ресурсів і намагаються зменшити час реагування, можуть отримати вигоду від оркестровки безпеки, автоматизації та реагування (SOAR). Технології SOAR збирають дані безпеки та сповіщення з безлічі джерел, ідентифікують сповіщення, які вимагають відповіді, і керують вимірюваними, стандартизованими робочими процесами для ефективного реагування.

SOAR робить роботу аналітика з безпеки легшою та ефективнішою завдяки автоматизації робочих процесів і прискоренню процесів кваліфікації

загроз, дослідження та реагування. SOAR часто інтегрується з іншими технологіями, щоб забезпечити контекст подій, який дозволяє аналітикам швидше визначити масштаб і першопричину інциденту або порушення. Завдяки ефективності та інтеграції можливості SOAR сприяють якіснішому реагуванню на інциденти та оптимізують робоче навантаження аналітиків за рахунок зменшення ручних завдань і підвищення узгодженості процесу. SOAR також надає основу для показників для оцінки SOC і забезпечує постійне навчання та вдосконалення.

Ключова відмінність SOAR та SIEM систем полягає в тому, що SOAR починається там, де закінчується SIEM. Платформа SOAR характеризується як середовище, у якому розгорнуто SOAR, і зміни, які вона завдає конкретній екосистемі безпеки.

Платформа SOAR зазвичай включається в SOC, щоб підвищити ефективність роботи спеціалістів із безпеки, які працюють у SOC. SOAR використовує автоматизацію та оркестровку, щоб допомогти організаціям точно визначити реальні кіберзагрози, усунути помилкові спрацьовування та реагувати на реальну небезпеку, значно покращивши час реагування на інцидент.

З іншого боку, SIEM — це сучасний агрегатор даних, який використовується виключно для збору інформації щодо сповіщень. На відміну від SOAR, який базується на механізмі машинного навчання, щоб постійно бути в курсі найсучасніших кіберзагроз, SIEM потребує частих ручних налаштувань від кібераналітика, щоб підтримувати свій сучасний статус.

Іншими словами, SOAR не тільки збирає дані, але й використовує свій механізм машинного навчання, щоб самотужки реагувати на загрози та використовувати автоматизацію для повного виконання завдань із низьким рівнем ризику (наприклад, документування процесу аналізу попередження) без необхідності людської взаємодії. SIEM відрізняється від SOAR у тому сенсі, що SIEM надає дані про загрозу, не сприяючи рекомендованим напрямкам дій, зрештою вимагаючи від спеціалістів із безпеки виконувати роботу з оцінки кожного окремого сповіщення вручну.

У рамках певної платформи SOAR дозволяє командам SOC виявляти, оцінювати та усувати кіберінциденти, водночас зменшуючи потребу в людському втручанні в процес, надаючи автоматизований аналіз і використовуючи машинне навчання та ШІ. Тоді як SIEM потребує постійних налаштувань і оновлень, щоб мати змогу розрізняти звичайні та підозрілі сповіщення.

Ось чому за допомогою SOAR аналітики мають більше часу, щоб зосередитися на призначеннях з вищим пріоритетом, замість того, щоб перевіряти вручну кожне сповіщення, що надходить у режимі реального часу, як у випадку з тими SOC, які покладаються на SIEM.

Користь, що набувають організації при використанні SOAR:

- вирішується проблема втоми від сповіщень: багато організацій щодня отримують тисячі сповіщень, і SOC часто не мають робочої сили, щоб належним чином оцінити кожне з них. Величезний обсяг сповіщень неминуче призводить до перевантаження роботи для аналітиків, які не в змозі встигати за нескінченним потоком сповіщень. Використовуючи автоматизацію безпеки, SOAR замінює аналітиків, піклуючись про сповіщення з низьким рівнем ризику, які складають понад 60% усіх сповіщень;

- вирішується проблема нестачі навичок: кількість щоденних сповіщень зростає, і, на жаль, кількість кваліфікованих фахівців із безпеки зменшується. Однак SOAR безпосередньо вирішує цю проблему, підвищуючи продуктивність SOC у десятки разів, що дозволяє командам SOC досягати більшого, роблячи менше;

- значне зменшення часу реагування на інциденти: групи SOC, які не покладаються на найсучасніші технології та не працюють із найкваліфікованішими аналітиками, часто надто повільно аналізують сповіщення. SOAR дозволяє фахівцям із безпеки зменшити час реагування на кіберзагрози до 80% за допомогою повністю або напівавтоматичних реакцій.

Причина зростання популярності та попиту на SOAR полягає в тому, що SOAR вирішує проблеми, які не можна вирішити за допомогою старих технологій.

SOAR діє як комплексне рішення, одночасно зміцнюючи різні аспекти SOC. І у 2019 році Gartner вважав, що порівняно з 5% у 2019 році, у 2022 році понад 30% усіх SOC із понад 5 членами покладатимуться на SOAR як на своє основне технологічне рішення, яке об’єднує всі аспекти їхньої платформи безпеки[14].

Висновки до першого розділу

У розділі було розглянуто організацію побудови, впровадження та експлуатації системи управління інцидентами інформаційної безпеки. Було здійснено опис CSIRT, політик та плану управління інцидентами інформаційної безпеки.

Також, було здійснено опис процесів під час впровадження та експлуатації SIEM та SOAR систем.

Крім того, було здійснено опис функцій, що виконують SIEM та SOAR системи, та процесів, які SIEM та SOAR системи автоматизують.

2 МЕТОДИЧНІ ПІДХОДИ ЩОДО ВИКОРИСТАННЯ SIEM ТА SOAR СИСТЕМ НА ПІДПРИЄМСТВІ

2.1 Досвід використання методичних підходів щодо управління інцидентами інформаційної безпеки

Організація ефективного реагування на інциденти комп'ютерної безпеки (CSIRC) включає кілька основних рішень та дій. Одним із перших міркувань має бути створення специфічного для організації визначення терміну «інцидент» таким чином, щоб обсяг терміну був зрозумілим. Організація повинна вирішити які послуги має надавати група реагування на інциденти, продумати, які структури та моделі команди можуть надавати ці послуги, а також вибрати та запровадити одну або кілька груп реагування на інциденти. Створення плану реагування на інциденти, політики та процедури є важливою частиною створення команди, щоб реагування на інцидент виконувалося ефективно та послідовно. Це необхідно робити таким чином, щоб команда мала повноваження робити те, що потрібно зробити. План, політика та процедури повинні відображати взаємодію команди з іншими командами всередині організації, а також із сторонніми сторонами, такими як правоохоронні органи, ЗМІ та інші CSIRC[5].

Згідно NIST.SP.800-61r2 управління інцидентами інформаційної безпеки складається з п'яти окремих фаз[5]:

• планування та підготовка, що включає:

- політику управління інцидентами інформаційної безпеки та затвердження вищим керівництвом;
- політику інформаційної безпеки, в тому числі пов'язану з управлінням ризиками, оновлену як на корпоративному рівні, так і на рівні системи, сервісу та мережі;
- план управління інцидентами інформаційної безпеки;
- створення ГРІБ;
- відносини та зв'язки з внутрішніми та зовнішніми організаціями;

- технічну та іншу підтримку (включаючи організаційну та операційну підтримку);

- брифінги та тренінги з управління інцидентами інформаційної безпеки;

- тестування плану управління інцидентами інформаційної безпеки;

• виявлення та звітування, що включає:

- збір інформації про ситуацію з місцевого середовища, зовнішніх джерел даних та актуальних новин;

- моніторинг систем і мереж, виявлення та сповіщення про аномальну, підозрілу або зловмисну діяльність;

- збір звітів про події інформаційної безпеки від установ, постачальників, інших ГРІБ або організацій безпеки та автоматизованих датчиків;

- формування звітів про події інформаційної безпеки;

• оцінка та рішення, що включає:

- оцінка інформаційної безпеки та визначення інцидентів інформаційної безпеки;

• реагування, що включає:

- визначення наявності інцидентів інформаційної безпеки, що знаходяться у стадії розслідування та дослідження;

- стримування та викорінення інцидентів інформаційної безпеки;

- відновлення після інцидентів інформаційної безпеки;

- вирішення та закриття інцидентів інформаційної безпеки;

- а також, активні дії, що включають подальше дослідження, якщо це необхідно;

• вивчені уроки, що включають:

- визначення отриманих уроків;

- визначення та внесення покращень до інформаційної безпеки;

- визначення та вдосконалення оцінки ризиків інформаційної безпеки та результатів аналізу керівництва;

- визначення та вдосконалення плану управління інцидентами інформаційної безпеки;

- оцінка продуктивності та ефективності ГРІБ.

Атаки часто ставлять під загрозу особисті та ділові дані, тому дуже важливо швидко і ефективно реагувати на порушення безпеки. Концепція реагування на інциденти комп'ютерної безпеки стала широко прийматись та впроваджуватись. Однією з переваг можливості реагування на інцидент є те, що вона підтримує систематичне реагування на інциденти (тобто дотримання методології послідовної обробки інцидентів), щоб було вжито відповідних дій. Реагування на інциденти допомагає персоналу звести до мінімуму втрати або крадіжку інформації та порушення роботи послуг, викликані інцидентами. Ще одна перевага реагувань на інциденти – це здатність використовувати інформацію, отриману під час обробки інцидентів, для кращої підготовки до обробки майбутніх інцидентів і для забезпечення більшого захисту систем і даних. Можливість реагування на інцидент також допомагає належним чином вирішувати юридичні питання, які можуть виникнути під час інцидентів. Крім ділових причин для створення можливостей реагування на інциденти, організації повинні дотримуватися закону, нормативних актів і політики, спрямованої на скоординований, ефективний захист від загрози інформаційній безпеці.

Процедури реагування на інциденти інформаційної безпеки повинні ґрунтуватися на політиці та плані реагування на інциденти. Стандартні робочі процедури (СРП) – це окреслення конкретних технічних процесів, методів, контрольних списків і форм, які використовуються CSIRT. СРП мають бути достатньо вичерпними та детальними, щоб гарантувати, що пріоритети організації відображаються в операціях реагування. Крім того, наступні стандартизовані відповіді повинні звести до мінімуму помилки, особливо ті, які можуть бути викликані обробкою інцидентів, що призвели до виникнення стресових ситуації. СРП слід перевірити, щоб підтвердити їх точність і корисність, а потім розповсюдити всім членам команди. Необхідно забезпечити

навчання користувачів СРП; документи СРП можна використовувати як інструкції.

Група реагування на інцидент (ГРІІБ) має бути доступна для всіх, хто виявляє або підозрює інцидент. Один або кілька членів команди, залежно від величини інциденту та наявності персоналу, задіяні у вирішенні інциденту. Обробники інцидентів аналізують дані про інцидент, визначають вплив інциденту та діють належним чином, щоб обмежити пошкодження та відновити нормальні послуги. Успіх групи реагування на інцидент залежить від участі та співпраці осіб по всій організації.

Керівник ГРІІБ повинен:

- мати делеговані повноваження негайного прийняття рішення про те, яких заходів вжити щодо інциденту;

- як правило, мати окрему лінію для оповіщення вищого керівництва, яка має бути ізольованою від звичайних бізнес-операцій;

- забезпечувати необхідний рівень знань та майстерності для всіх членів ГРІІБ, а також підтримання цього рівня;

- доручати розслідування кожного інциденту найбільш компетентному члену групи.

Організаціям часто потрібно спілкуватися із сторонніми особами щодо інциденту (рис. 2.1), і вони повинні це робити тому, що часто це доречно. Наприклад, зв’язатися з правоохоронними органами, надіслати запити ЗМІ та розшукати зовнішнього експерта. Іншим прикладом є обговорення інцидентів з іншими залученими сторонами, такими як постачальники Інтернет послуг (ISP), постачальники уразливого програмного забезпечення або інші групи реагування на інциденти.

Організації також можуть активно ділитися відповідною інформацією про індикатори інцидентів з колегами для покращення виявлення та аналізу інцидентів. Групі реагування на інцидент слід обговорити обмін інформацією зі службою зі зв’язків з громадськістю, юридичним відділом та керівництвом організації до того, як станеться інцидент і встановити політику та процедури

щодо обміну інформацією. В іншому випадку конфіденційна інформація про інциденти може бути надана неуповноваженим сторонам, що потенційно може призвести до додаткових збоїв і фінансових втрат. Команда повинна задокументувати всі контакти та спілкування із зовнішніми сторонами для розподілення відповідальності та доказових цілей.

Рис. 2.1. Зв'язок із сторонніми організаціями [5]

Також, згідно ISO/IEC 27002:2005 управління інцидентами інформаційної безпеки потребує наступних дій[15]:

• повідомлення про події та недоліки інформаційної безпеки:

- звітування про події інформаційної безпеки. Усі співробітники, підрядники та сторонні користувачі повинні знати про свою відповідальність та повідомляти про будь-які події інформаційної безпеки якомога швидше. Вони також повинні знати про порядок повідомлення про події інформаційної безпеки та контактну інформацію;

- повідомлення про недоліки безпеки. Усі працівники, підрядники та треті сторони, користувачі інформаційних систем і послуг, повинні зазначати та повідомляти про будь-які спостережувані або підозрювані недоліки безпеки в системах або службах;

• управління інцидентами інформаційної безпеки та вдосконалення:

- обов'язки та процедури. Необхідно встановити обов’язки та процедури керівництва для забезпечення швидкого, ефективного та впорядкованого реагування на інциденти інформаційної безпеки;

- навчання на основі інцидентів інформаційної безпеки. Мають існувати механізми, які дозволятимуть кількісно оцінювати типи, обсяги та вартість інцидентів інформаційної безпеки та здійснювати моніторинг. Інформацію, отриману в результаті оцінки інцидентів інформаційної безпеки, слід використовувати для виявлення повторюваних інцидентів або інцидентів із сильним впливом;

- збір доказів. Необхідно розробити внутрішні процедури та дотримуватися їх під час збору та представлення доказів для цілей дисциплінарних стягнень, що застосовуються в організації.

2.2 Характеристика існуючих автоматизованих SIEM та SOAR систем в управлінні інформаційною безпекою

SIEM допомагає вирішити цілий ряд завдань. Серед них: своєчасне виявлення спрямованих атак і непередбачених порушень важливої інформаційної безпеки зі сторони користувачів, оцінка захищеності критичних систем і ресурсів, ведення слідчих інцидентів і багато іншого[16].

При цьому в SIEM-системах є ряд обмежень. Вони, наприклад, не вміють класифікувати дані, досить часто погано працюють з електронною поштою, мають сліпу зону у відношенні власних подій. Але разом з цим вони є важливою частиною захисної системи підприємства. Тема розвитку SIEM-систем не стоїть на місці. Наприклад, у деяких сучасних продуктах є аналітичні функції, тобто

вони не просто видають звіти та вказують на потенційні проблеми, але й уміють самі аналізувати події та приймати рішення щодо інформування про них або інших подіях.

У будь-якому випадку при виборі конкретного продукту слід орієнтуватися на безліч умов, серед яких можна виділити централізований збір, обробку та зберігання інформації, повідомлення про інциденти та аналіз даних (кореляція), а також ширину охоплення корпоративної мережі.

Нижче наведено порівняльний опис деяких серед найбільш розповсюджених на ринку SIEM-систем.

• IBM QRadar Security Intelligence

SIEM-платформа від технологічного гіганта IBM є однією з найбільш просунутих на ринку: навіть у квадрант лідерів Gartner вона коштує вище конкурентів, при цьому потрапляє туди вже 10 років поспіль. Продукт складається з кількох інтегрованих між собою систем, які разом забезпечують максимальний охоплення вихідних у мережі подій, а безліч функцій працюють прямо «з коробки». Інструмент дозволяє зібрати дані з різноманітних джерел, наприклад, операційних систем, пристроїв безпеки, бази даних, програм та багатьох інших.

QRadar Security Intelligence дозволяє сортувати події за пріоритетністю та виділяти ті, які не є найбільшою загрозою безпеки. Це відбувається завдяки функціям аналізу аномальної поведінки об’єктів (користувачів, обладнання, служб і процесів у корпоративній мережі). У цьому числі визначаються дії, пов'язані зі зверненням до підозрілої IP-адреси або запитам від неї. Насправді всі подозрілі дії надають докладні звіти, що, наприклад, дає можливість виявити підозрілі дії в неробочий час. Подібний підхід у комбінації з функціями моніторингу користувачів і наглядним представленням мережі на рівні програм дозволяє боротися з загрозами інсайдерів. Крім того, при звичайних кібератаках інформація надходить дуже швидко і дозволяє запобігти їх до того, як вони досягнуті цілий і несуть істотного збитку.

Одна з головних особливостей IBM QRadar Security Intelligence — виявлення та розстановка пріоритетів на основі ризиків із використанням розширеного аналізу та кореляції між активами, користувачами, мережевою активністю, що мають уразливості, аналізом загроз тощо. IBM Qradar може зв'язувати події в одному ланцюжку, створюючи для кожного інциденту окремий процес.

Завдяки тому, що інформація збирається і виводиться на екран в одному місці, адміністратор може бачити всі пов’язані дії, які були виявлені системою. Нові пов'язані події додаються в ланцюжок, так що аналітики не повинні переключатися між кількома повідомленнями. А для більш глибокого розслідування спеціальний інструмент IBM QRadar Incident Forensics може відновити всі мережеві пакети, пов’язані з інцидентом, і спробувати відтворити дії злочинця.

• Splunk Enterprise Security

Одна з провідних у галузі платформ, відмінною рисою якої є широкий перелік джерел інформації, з якою вона працює. Splunk Enterprise Security збирає журнали подій із традиційних компонентів мережі (сервери, пристрої безпеки, шлюзи, бази даних тощо), мобільних пристроїв (смартфони, ноутбуки, планшети), веб-сервісів та розподілених джерел. Інформація що збирається: дані про дії користувачів, журнали, результати діагностики та ін. Це дозволяє проводити зручний пошук і аналіз в автоматичному і ручному режимі. Рішення має безліч вбудованих попереджень, які на основі зібраної інформації попереджають про наявні загрози та завчасно повідомляють про потенційні проблеми.

• AlienVault Unified Security Platform

Компанія AlienVault об'єдналася з AT&T Business під брендом AT&T Security. Цей інструмент, як і більшість інших платформ з огляду, має більш широку функціональність, ніж традиційний SIEM. Так, в AlienVault USM є різноманітні модулі, що підтримують контроль активів, повне захоплення пакетів тощо. Платформа також має можливість проводити тестування мережі на

наявність вразливостей, причому це може бути як разова перевірка, так і неперервний моніторинг. У останньому випадку повідомлення про наявність нової вразливості походять практично одночасно з її проявами.

Серед інших можливостей платформи — перевірка оцінки вразливості інфраструктури, яка показує, рівень захисту, а його параметри відповідають стандартам безпеки. Платформа також уміє визначати атаки на мережу і вчасно сповіщати про них. У такому разі адміністратори отримують детальну інформацію про те звідки йде вторгнення, які частини мережі зазнали атаки та які методи використовують зловмисники, а також, що необхідно пзробити для відновлення в першу чергу. Крім того система вміє визначати інсайдерські атаки зсередини мережі та повідомляти про них.

• Fortinet FortiSIEM

Комплексне та масштабне рішення від Fortinet є частиною платформи Fortinet Security Fabric. Рішення поставляється у вигляді фізичних пристроїв, але може використовуватися також на базі хмарної інфраструктури або в якості віртуального пристрою. Засіб забезпечує широке охоплення джерел інформації — підтримуються понад 400 пристроїв інших виробників. Серед них кінцеві точки, пристрої інтернет-речей, додатки, засоби безпеки та багато іншого.

Платформа вміє збирати і обробляти інформацію з кінцевих точок, в тому числі про цілістність файлів, зміни в реєстрі і про встановленя програм і інших подозрілих подіях. FortiSIEM має засоби глибокого аналізу, серед яких пошук подій у реальному часі, а також минулих подій, пошук за атрибутами та ключовими словами, динамічно змінювані списки відстеження, які використовуються для виявлення критичних порушень та багато іншого.

Виходячи з досліджень Gartner «Emerging Technology Analysis: SOAR Solutions»[17], ринок SOAR зараз знаходиться на стадії розвитку. При цьому в прогнозному аналізі «Forecast Analysis: SOAR, Worldwide» Gartner оцінює, що ринок SOAR буде зростати.

Згідно з дослідженнями Gartner «Market Guide for Security Orchestration, Automation and Response Solutions», на світовому ринку можна виділити кілька популярних пропозицій SOAR-систем[31].

• Cisco SecureX

Cisco SecureX надає більше можливостей для взаємодії з іншими рішеннями, ніж звичайні SOAR або SIEM-платформи, дозволяючи налаштувати різноманітні сценарії аналізу і реагування. Cisco SecureX являє собою відкриту багатовендорну платформу.

Cisco SecureX вдало використовує можливості всіх рішень Cisco з інформаційної безпеки для забезпечення інформування про загрози, а також надає аналітику та автоматизує робочі процеси, прискорюючи та полегшуючи виявлення і протидію кібератакам. Продукт являє собою хмарну платформу, що полегшує роботу з продуктами компанії Cisco у сфері інформаційної безпеки та зменшує проблему надлишкової складності систем, що стала однією з головних для директорів з кібербезпеки.

• Cortex XSOAR

Як стверджує виробник, Cortex XSOAR – перша «eXtended SOAR» - система, яка забезпечує одночасно й управління заявками, і контроль KPI та SLA, і автоматизацію дій аналітиків з одночасним підвищенням рівня їх кваліфікації, а також має можливості спільного розслідування інцидентів у режимі реального часу, проактивний пошук загроз (Threat Hunting) і зв'язок з найсвіжішими світовими даними щодо кіберзагроз (Threat Intelligence). Cortex XSOAR отримує повідомлення та індикатори компрометації з різних джерел подій, наповнює свої бази знань і запускає в автоматичному режимі процеси для реагування на інциденти. Cortex XSOAR уміє інтегруватися з майже 500 рішеннями та продуктами від сторонніх вендорів, і ця цифра зростає. Відкрита торговельна площадка (marketplace) модулів інтеграції ще більше розширює спектр можливостей системи.

• FortiSOAR

Основним призначенням FortiSOAR є узгодження роботи (оркестровки) систем кібербезпеки та управління реагуванням на інциденти в режимі реального часу. За допомогою гнучких сценаріїв система не просто збирає інформацію про індикатори компрометації, а ще може збагачувати її відомостями із зовнішніх джерел, після чого може керувати пристроями для припинення кібератаки. Це звільняє аналітиків SOC від виконання стандартних операцій і дозволяє сконцентруватися на аналізі дійсно важливих інцидентів.

Завдяки функціям аналізу вхідних повідомлень і керування отриманими даними фахівці з безпеки отримують більш повне уявлення про загрози. Продумана архітектура, що припускає як одиночну корпоративну, так і багатоклієнтську мультитенантну моделі використання, передбачає різні варіанти масштабування в різних режимах роботи. FortiSOAR містить візуальний редактор автоматичних сценаріїв реагування і велику кількість готових вбудованих плейбуків, які можна використовувати «з коробки» і які не вимагають глибоких навичок програмування. Також система забезпечує ефективне адміністрування режимів доступу на основі ролей, завдяки чому організації клієнтів SOC можуть управляти конфіденційними даними відповідно до рекомендованих політик і пропозицій.

• IBM Resilient SOAR

IBM Resilient SOAR – платформа координації подій та автоматизації процесів реагування на інциденти. Вона може швидко і легко інтегруватися з наявними засобами захисту та IT інфраструктурою. Рішення дозволяє негайно опрацьовувати попередження з безпеки, а також надає цінну аналітичну інформацію про інцидент, забезпечуючи адаптивне реагування на складні кібератаки. Новітнє доповнення Dynamic Playbooks – дає можливість гнучкого інтелектуального реагування на складні атаки з автоматичним аналізом та оновленням інцидентів в режимі реального часу.

Основні функції платформи: управління реагуванням на події ІБ (компонент Security Module), координація та автоматизація реагування (Action Module), управління повідомленнями про несанкціонований доступ до

обмежених ресурсів (Privacy Module). Крім уже згаданого інтелектуального реагування за допомогою Dynamic Playbooks, доступні візуалізація в модулі Incident Visualization, спрощення складних процесів з Visual Workflows, а також можливість тренування аналітиків за допомогою компонента Resilient Simulations.

• Splunk Phantom

Модель додатка Phantom вміє підтримувати сотні інструментів і тисячі унікальних API, дозволяючи координувати складні робочі процеси команди SOC. Потужна візуалізація дозволяє зосередитися на меті розслідування, а платформа переводить це в команди, адаптовані під інструмент.

Phantom дає можливість працювати ефективніше, виконуючи ряд дій – від детектування подій до відправки до карантину джерел підозрілої поведінки у інфраструктурі безпеки за лічені секунди, у порівнянні з годинами чи навіть днями, якщо це все виконується вручну. Доступна можливість автоматизації стандартних робочих процесів завдяки написанню сценаріїв дій за допомогою візуального редактора (уміння програмування не обов'язкове) або інтегрованого середовища розробки Python.

2.3 Підходи щодо використання SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки

SIEM-системи складаються з двох рішень[6]:

- SIM (Security information management) – це управління інформаційною безпекою. Комплекс рішень, які спрямовані на створення та підтримку стабільної роботи системи, яка повинна забезпечити зберігання важливої інформації, доступ до неї, а також проводити облік даних.

- SEM (Security event managemen) – це управління подіями безпеки. Забезпечує збір даних про загрози та впровадження засобів захисту, а також забезпечує реалізацію рішень необхідних для прийняття конкретних заходів по пріоритизації, розслідуванню та усуненню загроз.

Зазвичай вважається, що система керування інформацією та подіями безпеки (SIEM) надає наступний набір послуг[8]:

- керування журналами (Log Management);
- відповідність вимогам та нормам (IT Regulatory Compliance);
- кореляція подій (Event correlation);
- активна відповідь (Active response);
- безпека кінцевої точки (Endpoint security).

• Керування журналами (Log Management)

Керування журналами в системі SIEM починається з налаштування вузлів в IT-системі, зокрема найбільш важливих або критичних вузлів, для надсилання відповідних системних подій і подій додатків (журналів, логів (logs)) до централізованої бази даних, якою керує програма SIEM. Ця програма бази даних SIEM спочатку аналізує та нормалізує дані, надіслані численними та дуже різними типами вузлів IT-системи. Тоді SIEM зазвичай надає послуги зберігання журналів, організації, пошуку та архівування, щоб задовольнити вимоги до керування журналами, які можуть мати підприємства. Ці послуги часто потрібні підприємствам для дотримання нормативних вимог. Ця подача даних у компонент керування журналами системи SIEM дає змогу додатково використовувати аналіз майже в реальному часі та інтелектуальний аналіз даних щодо працездатності та стану безпеки всіх IT-систем, які передають свої дані в систему SIEM. Чим більше вузлів надходить у систему SIEM, тим повнішим і точнішим є бачення IT-системи в цілому.

Системи або можуть мати вбудовані клієнтські служби типу системного журналу, встановлені для експортування журналів, наприклад, на маршрутизаторах та інших мережевих пристроях, або можливо знадобитися інсталювати клієнтське програмне забезпечення сторонніх розробників на мережевих вузлах для експорту журналів, наприклад Winlogd або Snare. Постачальник SIEM також може надати колекцію спеціальних агентів для встановлення на певних типах вузлів для виконання цієї функції експорту.

• Відповідність вимогам та нормам (IT Regulatory Compliance)

Коли всі події з важливих і критичних систем реєструються, можливо створювати фільтри або правила та таймери для аудиту (моніторингу за стандартом) і перевірки згідно відповідності вимогам або виявлення порушень згідно відповідності вимогам, які висуваються до організації. Правила, які перевіряються за журналами, які надсилаються в систему, можуть включати моніторинг частоти зміни пароля, виявлення та визначення операційних систем (ОС) або програмних оновлень, які не вдається встановити, а також частоту аудиту оновлень антивірусного, антишпигунського програмного забезпечення та IDS відповідно до вимог. Хоча можливо створити власну колекцію фільтрів або правил, щоб допомогти у відповідності до вимог, багато постачальників SIEM включають готові колекції правил, спеціально розроблених для задоволення вимог до різних законів і нормативних актів, яких підприємства повинні дотримуватися. Зазвичай це упаковані додаткові компоненти, які надаються клієнтам SIEM за окрему плату постачальниками або навіть торговими посередниками післяпродажного обслуговування.

Практично всі системи SIEM включають повнофункціональні системи звітності, багато з яких мають готові та настроювані звіти. Ці звіти часто потрібні підприємствам, щоб надати докази самостійного аудиту та підтвердити рівень відповідності вимогам.

• Кореляція подій (Event correlation)

Кореляція подій забезпечує більш високий рівень аналізу в обробці подій. За допомогою кореляції подій система враховує різні умови перед тим, як запустити тривогу. Наприклад, причини, через які сервер працює зі 100-відсотковим використанням ЦП, можуть бути досить різними. Це може вказувати на наявність проблеми, яку потрібно виправити, а може і не вказувати. Це може бути несправна програма, яка заблокувала сервер. Або можливо система перевантажена легітимною діяльністю, і це вказує на те, що одну або кілька служб або програм слід розподілити між додатковими серверами, як у кластері. Можливо, сервер досягає повної потужності через хробак, який виконує на

систему атаку типу «відмова в обслуговуванні» (DoS). Також це може бути просто тимчасова легітимна активність сервера.

• Активна відповідь (Active response)

Коли всі системи, що надсилають події в SIEM, налаштовані, правила та фільтри визначені, а також застосовані правила кореляції, можна робити вибір між ручним вживанням заходів і реагуванням на інцидент для всіх перевірених подій безпеки або налаштуванням SIEM на автоматичну й активну реакцію на певні типи корельованих подій? Автоматичне застосування SIEM коригувальних дій щодо передбачуваних загроз або неправильних конфігурацій, знимає багато завдань з аналітика безпеки та IT-відділу. Багато систем SIEM можуть виконувати активну відповідь, наприклад, додаючи фільтри IP-адрес і портів до списку контролю доступу (ACL) на маршрутизаторі чи брандмауері. Ініційована, автоматизована та активна реакція SIEM на передбачувану загрозу відбувається набагато швидше, ніж просто сповіщення про подію аналітика.

• Безпека кінцевої точки (Endpoint security)

Більшість SIEM систем можуть контролювати безпеку кінцевих точок, щоб централізовано перевіряти «справність» безпеки системи. Багато SIEM систем можуть відстежувати, чи працює брандмауер на ПК чи сервері, і можуть визначити, коли востаннє оновлювалися бази AV і чи є зараження шпигунським програмним забезпеченням. Деякі системи SIEM можуть навіть керувати безпекою кінцевих точок, фактично вносячи коригування та покращуючи безпеку вузла у віддаленій системі, наприклад, налаштовуючи брандмауери та оновлюючи та відстежуючи продукти AV, антишпигунського програмного забезпечення та спаму на вузлах у системі. Крім того, деякі системи SIEM можуть прийняти та інсталювати оновлення або в режимі активної відповіді налаштувати ACL на некоректно налаштованому особистому брандмауері.

У SIEM-системі наявна розподілена архітектура, яка передбачає більш високий рівень ефективності та дозволяє системі масштабуватися. Різноманітні компоненти SIEM-системи представлені на різних платформах, і декілька компонентів можуть взаємодіяти один з одним для досягнення конкретної мети.

Процес обробки інформації націлений на використання в різних організаційних моделях SOC. Ціль SIEM-проекту – це збір великої кількості даних та їх обробка, для того, щоб аналітики мали змогу використовувати цю інформацію для роботи.

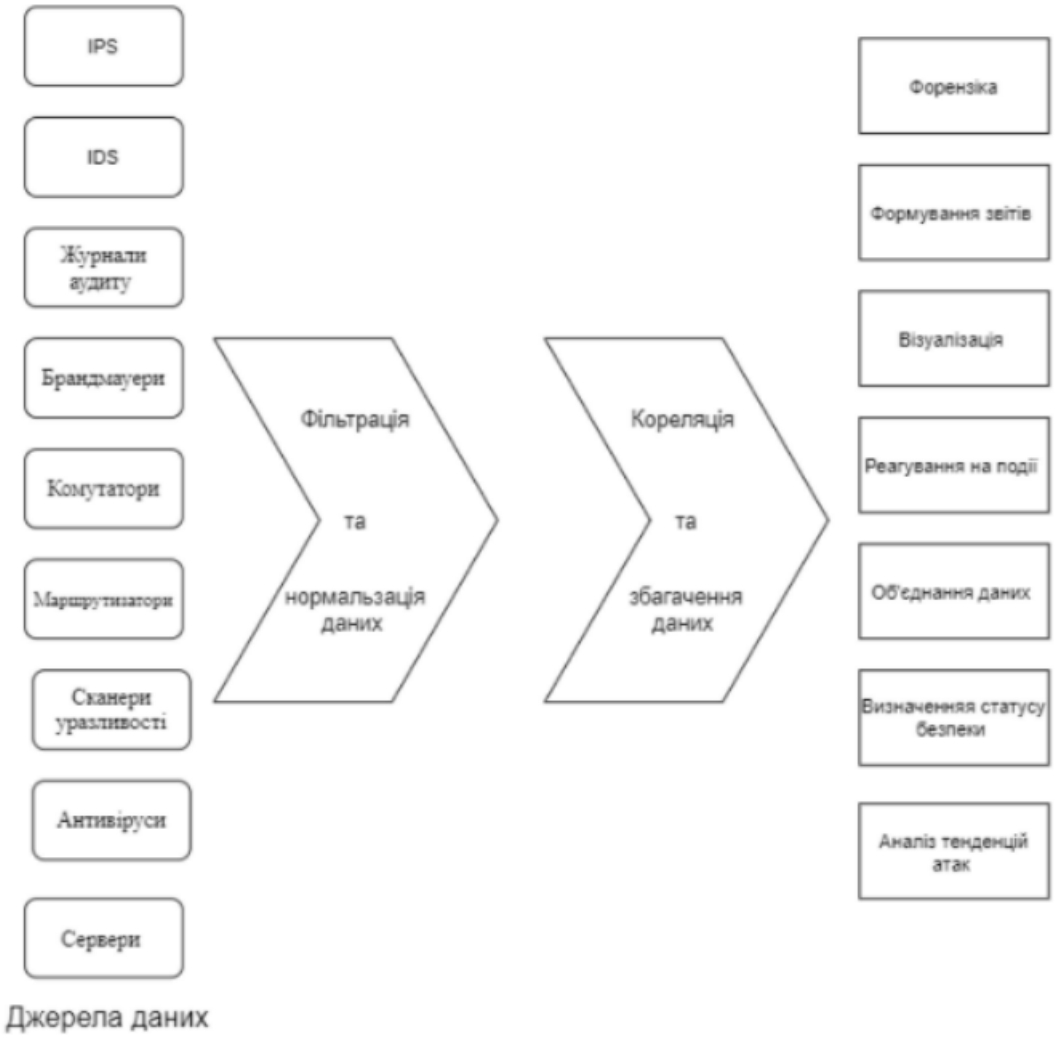

Рис. 2.2. Архітектура SIEM-систем [11]

Завдяки архітектурі (рис. 2.2) та набору функцій SIEM-система має декілька варіантів розвитку [10] :

- відслідковування автентифікацій і виявлення компрометації облікових записів користувачів і адміністраторів;

- відслідковування випадків зараження. Виявлення шкідливих програм з використанням вихідних журналів файєрвола і журналів веб-проксі, а також внутрішніх журналів підключення і мережевих потоків;

- моніторинг підозрілого вихідного трафіку і переданих по мережі даних з

використанням журналів файєрвола, журналів веб-проксі і NetFlow. Виявлення крадіжки даних і інших підозрілих зовнішніх з'єднань;

- відстеження системних змін і інших адміністративних дій у внутрішніх системах і їх відповідності застосованій дозвільній політиці;

- відстеження атак на веб-додатки та їх наслідків з використанням журналів веб-сервера, WAF (Web Application Firewall, екран для захисту веб-додатків) і програмних подій. Виявлення спроб компрометації вебдодатків шляхом аналізу різних звітів;

- аналіз інцидентів, відстеження та зберігання даних журналу аудиту.

Функціональні можливості рішень класу SOAR[18]:

• Збір даних про потенційні інциденти. SOAR-системи здатні агрегувати та обробляти ІБ-сигнали з безлічі джерел, до яких входять:

- SIEM-рішення;

- Антивіруси та інше програмне забезпечення для захисту кінцевих точок;

- DLP продукти;

- Платформи для аналізу погроз (Threat Intelligence);

- Система для аналізу поведінки користувачів (UEBA-рішення);

- Міжмережеві екрани;

- Служби каталогів ОС.

• Аналіз інциденту. За допомогою автоматичних сценаріїв або в ручному режимі рішення класу SOAR доповнюють інформацію про кіберінцидент даних із зовнішніх баз, записів про аналогічні події та інших джерел. Також на цьому етапі формується перелік порушених інцидентом об'єктів та пристроїв.

• Ідентифікація та класифікація загроз. На підставі комплексного аналізу отриманих даних SOAR оцінює стан інфраструктури, виділяє потенційно небезпечні події, групує їх за рівнем ризику та інформує про них фахівців. При необхідності система ізолює заражені пристрої, щоб не допустити подальшого поширення атаки, або вживає інших заходів, що відповідають політиці компанії. Реагування на інцидент. На основі інформації про інцидент SOAR виконує набір дій, необхідних для усунення загрози або мінімізації її наслідків. Це можуть бути

команди іншим ІБ-продуктам, дистанційне видалення шкідливих об'єктів, відновлення ключів реєстру та інші дії.

• Візуалізація даних та формування звітності. Більшість рішень класу SOAR здатні представляти зведену інформацію про кіберінцидентів по підрозділах компанії, кінцевих точках, програмних продуктів або конкретних співробітників. Звітність про поточний рівень безпеки організації формується як наочних діаграм чи інформерів, оновлюваних як реального часу.

За статистикою SOAR покращує час реагування на інцидент середньостатистичної команди SOC на 80% за рахунок наступного:

- відповідь на загрози протягом декількох хвилин замість годин: SOAR використовує свої можливості автоматизації, щоб розбиратися в суті вхідних сповіщень. Великі компанії щодня бомбардують тисячами загроз, і без SOAR відповідь на кожне з цих сповіщень може зайняти години, дні, а іноді навіть тижні;

- SOAR представляє швидке візуальне представлення з усіма відповідними характеристиками попередження, і враховуючи, що SOAR здатний відрізнити звичайні попередження від підозрілих, SOAR сповіщатиме аналітиків лише у випадку безпрецедентно складної проблеми, яку SOAR не може вирішити за допомогою наявної інформації. І понад 60% усіх сповіщень у кінцевому підсумку виявляються або хибними спрацьовуваннями, або загрозами з низьким рівнем ризику. SOAR дозволяє аналітикам реагувати на загрози, які дійсно мають значення, за лічені хвилини;

- замість того, щоб відображати нескінченні дані, SOAR автоматично представляє найбільш релевантну інформацію про загрозу, дозволяючи аналітикам приймати добре обґрунтовані рішення на основі агрегованої інформації, яку SOAR надає за допомогою настроюваних інформаційних панелей.

І принадність цього полягає в тому, що SOAR запам’ятає алгоритм дій, вжитих для усунення складних загроз, і таким чином розширить свої знання та стане більш компетентним, щоб принаймні надати рекомендовані алгоритми дій, коли подібна загроза з’явиться в майбутньому. Це суть прогресивної автоматизації.

Дуже важливо розуміти, що SOAR не замінює SIEM. Реальність така, що SOAR і SIEM — це дві дуже різні технології, і хоча SOAR у деяких сферах перевершує SIEM, зрештою, є причина, чому так багато компаній використовують SIEM.

Функція SIEM полягає у зборі та агрегуванні інформації про безпеку. Однак, коли SIEM зберігає агреговані дані, її роботу виконано. А щоб мати змогу відтворювати поведінку SOAR і розрізняти звичайні та підозрілі сповіщення, SIEM потребує постійного налаштування, яке виконують аналітики та інженери безпеки. Але хоча SOAR має перевагу в цій області та може автономно розрізняти звичайні та потенційно шкідливі сповіщення, SIEM краще генерує великі обсяги даних щодо сповіщень безпеки.

Отже, замість того, щоб вибирати між SIEM і SOAR, розумніше було б поєднати сильні сторони цих двох дуже різних технологій і використати їхні переваги, об’єднавши їх в єдину платформу SOC. Працюючи разом, SOAR зможе своєчасно та ефективно реагувати на кожне сповіщення, створене SIEM.

2.3.1 Методи та засоби впровадження та експлуатації SIEM систем

Перш ніж впроваджувати SIEM-систему необхідно переконатися в тому, що реалізовано наступні передумови [11]:

- у SOC вже є альтернативні інструменти збору логів. Але потреби в аналітиці та кореляції даних більше, ніж пропонують існуючі інструменти;

- SOC виконує значну частину своїх функцій з аналізу подій в режимі реального часу;

- SOC вже виділив крім IDS / IPS ще декілька потоків даних, які потребують передачі в SIEM в режимі реального часу;

- SOC бере участь в процесі регулярного управління і налаштування датчиків, для чого є навчений персонал. Тим самим SOC демонструє, що він готовий взяти на себе управління SIEM.

SIEM- проекти мають доволі складну схему обслуговування і їх остаточна ціна зазвичай залежить від:

- кількості джерел даних;

- об’єму даних, які оброблюватиме система;

- кількості користувачів, що обслуговуватимуть систему.

Ретельне панування має ключове значення перед запровадженням SIEM-систем, тому що SOC повинен запланувати щорічні виплати в рамках загальної вартості підтримки. Розмір щорічної плати за обслуговування та підтримку складає від 20-30% від початкової вартості придбання.

При роботі з SIEM-системою необхідно чітко розуміти головні вимоги до неї. Тому насамперед слід розглянути ключові параметри архітектури та функціоналу SIEM-систем.

Ключові характеристики SIEM-систем:

• пакет розгортання. Пакети розгортання існують декількох типів:

1. Коллектори - пакети в вигляді ПЗ, які встановлюються на кінцевий пристрій в єдиній точці збору, наприклад, на сервері бази даних IDS. Вони мають можливості конфігурації параметрів, що дозволяють адміністраторам робити оптимізацію ресурсів: ЦП, пам’ять, об’єм дискового простору і багатопотоковість.

2.Менеджери (головний вузол) – пакети у вигляді ПЗ (у вигляді встановлюваного ПЗ або у вигляді віртуального пристрою) та апаратного пристрою. Менеджер повинен мати багатопотоковість, щоб підтримувати паралельне виконання запитів і ефективну кореляцію подій;

• зберігання даних. Теоретично продукти SIEM здатні зберігати події, зібрані за багато років і навіть десятиліть. Але тривалість зберігання зазвичай обмежується періодом роботи з моменту першої ітерації. У деяких випадках SOC може створити нову інсталяцію SIEM, щоб почати з чистого аркуша. Це може стати джерелом проблем, оскільки SOC буде міняти багато поколінь продуктів SIEM, одночасно продовжуючи прагнути до довгострокового зберігання даних

аудиту. У міру розвитку і зростання стабільності продуктів, оновлене ПЗ краще підтримує зберігання даних про події і призначені для користувача дані;

• кількість пристроїв. SIEM повинна мати можливість отримувати та обробляти дані з десятків або навіть сотень тисяч кінцевих пристроїв по різних каналах передачі даних. SIEM також повинна мати можливість розпізнавати декілька потоків даних з однієї і тієї ж кінцевої точки. Добре спроектоване ПЗ агента має справлятися з багатьма пристроями (можливо, до десяткыв тисяч), чий сумарний потік подій може підтримувати більше тисячі подій в секунду;

• кількість подій. Правильна реалізація можливостей SIEM-системи зазвичай обробляє події, що надходять зі швидкістю на рівні тисяч подій в секунду, що складає десятки або сотні мільйонів подій в день. Це має бути оптимальна цифра для SIEM.

Перед впровадженням SIEM-проекту в інфраструктуру підприємства слід визначити, які пристрої будуть слугувати джерелами даних та актуалізувати окремі правила кореляції, для того щоб аналітики не губили потрібну інформацію серед нескінченного потоку подій. Для цього слід починати з інвентаризації ІБ-активів організації, за допомогою, наприклад, використання сканерів вразливостей. Це допомагає за відносно короткий проміжок часу зібрати всю потрібну інформацію про наявні компоненти інфраструктури компанії та про наявні на них вразливості, а також допоможе в майбутньому відстежувати стан мережі. Коли вся необхідна інформація зібрана, слід її приорітизувати, тобто визначитись зі ступенем критичності для кожної окремної події та вирішити, які дані слід збирати, оброблювати та зберігати. До SIEM-систем потрібно підключати найбільш важливі та критичні джерела.

Коли SOC купує SIEM, важливо звернути увагу на функції, які підтверджують, що продукт був сконструйований як SIEM корпоративного рівня з самого початку створення, а не як разовий або домашній проект, який згодом переріс в комерційну пропозицію. Багато продуктів класу SIEM, що представлені на сьогоднішньому ринку, були спочатку спроектовані з вужчим набором функцій і варіантів використання в порівнянні з тим, про що вони пропонують зараз.

Хороший продукт SIEM повинен бути сконструйований з надійним механізмом кореляції і масштабованими можливостями прийому даних.

Початкове налаштування SIEM досить просте, його можна виконати за кілька днів. Щоб забезпечити швидкий старт, через кілька тижнів або місяців можна підключити і налаштувати перші канали отримання даних і почати створення контенту. Однак забезпечення системи потрібними даними, її налаштування, створення відповідних функцій з надання послуг для клієнтських організацій і повна інтеграція в роботу займає біля року - за політичних і технологічних причин, а не через технічні причини. У багатьох випадках отримання надійних і стійких каналів журналів аудиту може бути політично складним процесом.

Слід також пам’ятати, що кожний аналітик на своєму робочому місці в SOC по-різному використовує дані і функції SIEM. Лінія 1 буде зацікавлена в отриманні та сортуванні даних в реальному часі і конкретних сценаріях реагування, під які вони можуть написати інструкції. Лінія 2 скоріш за все буде зацікавлена в зборі якомога більшої кількості деталей про кожен конкретний потенційний інцидент, тобто вони будуть виконувати запити різноманітних форм протягом тривалих періодів часу. Ті, хто відповідають за виявлення та попередження атак або за відстеження тенденцій, ймовірно, будуть створювати довгі ресурсоємні запити для агрегації результатів з різних джерел даних. Менеджери будуть зацікавлені в спостереженні за координацією роботи і метриками, які надає інструмент, щоб переконатися, що відповідні підрозділи SOC виконують інструкції, відстежують аномальну активність, коли система її вловлює, і не допускають простою системи.

Розподіл механізмів по рівням ієрархії зображений на рисунку 2.3. При переході до механізмів більш високого рівня показаної моделі, кількість оброблюваних подій зменшується, а складність їх обробки збільшується.

Рис. 2.3. Ієрархія механізмів [19]

• Одним із головних механізмів, які використовує SIEM, є механізм збору та агрегації логів. Ця інформація надходить з безлічі різних джерел - мережеве обладнання, засоби захисту інформації, додатки, СУБД. Інформація потрапляє в SIEM або на пряму з відслідковуємих систем, або через парсинг лог-файлів. У більшості випадків інформація про ту чи іншу подію містить позначку про час (timestamp), код події, а також набір довільних полів даних, частина яких зустрічається дуже часто (IP адреса джерела події, ім'я користувача і т.і.). Налаштувавши в правилах формат парсингу логів і призначення полів даних, можливо налаштувати логи для використання в SIEM системі. Після обробки інформація стає доступна оператору, який може її використовувати для розслідування інцидентів, статистичного аналізу роботи IT систем або аудиту.

• Кореляція подій. При підключені великої кількості джерел подій постає питання аналізу цих подій. Обробка даних вручну не кращий варіант, тому для моніторингу системи використовують так звану кореляцію подій, що забезпечує автоматизований аналіз подій, які надходять до системи, та повідомляє оператора безпеки про загрозу тільки за необхідності. Виділяють два способи кореляції:

1. Кореляція на базі правил (Rule based correlation). В даному випадку при впровадженні системи описується певна послідовність логічних дій, які характеризують дії зловмисника. Наприклад, велика кількість спроб входу в систему, що подібна процесу підбору пароля, яка закінчується успішним входом в цю систему. Перевагою цього способу є висока точність виявлення зловмисних дій. До недоліків можна віднести необхідність періодичного оновлення правил кореляції задля додавання виключень і неможливість реагувати на послідовність подій, що не зафіксована в правилах.

2. Кореляція без використання правил (Rule-lesscorrelation). Використовує ризик орієнтований підхід подібний банківським скорінговим системам. В рамках цього підходу всі події мають певний рейтинг, і, коли рівень рейтингу послідовності подій з певним параметром (вихідної IP адреси, цільової IP адреси, користувача і т.і.) перевищує попередньо встановлений, відбувається оповіщення оператора. Перевагою цього способу є відсутність залежності від написання правил і можливість виявлення нових векторів атак. До недоліків відноситься більш високий рівень хибних спрацювань, тому що існує ймовірність того, що дії виконуються легітимним користувачем. Також можна виділити кореляцію на основі статистичного аналізу подій, коли працюючи системи створюють стандартний профіль подій (наприклад, велика кількість успішних авторизації в Active Directory вранці в будній день). Таким чином, подія, що не відповідає стандартній поведінці (наприклад, авторизація вночі або спроба віддаленого доступу з території іншої держави) також може означати ймовірність інциденту ІБ.

• Розслідування інцидентів. Так як SIEM-система є центром агрегації всіх даних, обсяг подій, що вимагають більш глибокого аналізу, в ній завжди вище, ніж в інших засобах ІБ. У зв'язку з цим, SIEM-системи зазвичай мають у своєму розпорядженні вбудований механізм процесу побудови та розслідування інцидентів ІБ. Наприклад, в разі появи інциденту, пов'язаного з роботою мережного обладнання, буде створено інцидент і призначено відповідального співробітника.

• Нормалізація. Приведення форматів записів журналів подій, зібраних з різних джерел, до єдиного внутрішнього формату SIEM-системи, який потім буде використовуватися для їх зберігання і подальшої обробки.

• Фільтрація подій безпеки. Полягає у видаленні надлишкових подій з надходячих до системи потоків даних.

• Класифікація. Дозволяє на основі атрибутів подій безпеки визначити їх приналежність певним класам.

• Пріоритезація. Визначає рівень значимості і критичності подій безпеки на підставі правил, визначених у системі.

• Аналіз подій. Включає процедури моделювання виникнення подій, атак і їх наслідків, аналізу наявних вразливостей і ступеню захищеності системи, визначення параметрів потенційних порушників безпеки, оцінки ризику, прогнозування майбутніх подій та інцидентів.

• Прийняття рішень. Визначає розроблення та застосування заходів по зміні конфігураційних правил засобів захисту з метою запобігання потенційним атакам або для відновлення безпеки інфраструктури.

• Візуалізація. Передбачає подання у графічному вигляді даних, що дають характеристику результатів аналізу подій безпеки і стану захищеності системи та її елементів.

Функціональна модель SIEM-систем (рис. 2.4) об’єднує такі функціональні підсистеми як [19]:

- збір даних;
- попередня обробка даних;
- зберігання;
- аналіз;
- представлення в зрозумілому вигляді.

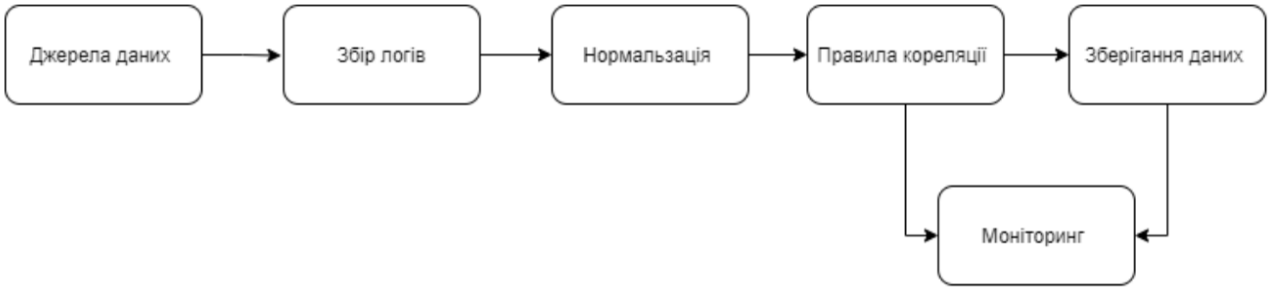

Рис. 2.4. Загальна послідовність обробки подій SIEM-системою [20]

2.3.2 Методи та засоби впровадження та експлуатації SOAR систем

Одним з нових акронімів у сфері ІБ, що нещодавно з'явилися, є SOAR (Security Orchestration, Automation and Response). Термін Orchestration (оркестровка) означає об'єднання різних наборів даних і технології безпеки для спільної роботи. Automation (автоматизація) скорочує час вирішення інциденту за рахунок мінімізації участі людини в повторюваних завданнях процесу реагування. Response (реагування) знаходиться в основі терміну SOAR і поєднує автоматично оркестровані елементи різних технологій для вирішення інцидентів[21].

Зломисники використовують для проникнення в корпоративну мережу автоматизовані інструменти, які діють швидко і точно. Водночас засоби захисту типу SIEM-систем, IPS та IDS можуть в автоматичному режимі запобігти тільки заздалегідь відомим атакам. Для протидії новим та невідомим атакам необхідна участь людини. Але поки оператор буде розбиратися в тому, що відбулося, хакер може встигнути підвищити привілеї, закріпитися в системі та знищити сліди свого проникнення. Саме тому для організації та автоматизації процесу розслідування і реагування використовуються SOAR.

Саме тлумачення терміну SOAR визначає набір функцій технології: оркестровка для взаємодії із засобами захисту та іншими IT-системами підприємства, автоматизація шляхом заздалегідь налаштованих сценаріїв реагування (Playbook) на виявлені інциденти і реагування на них за допомогою

оркестровки. Також не варто забувати про систему управління та оцінки ефективності роботи SOC. Слід зазначити, що SOAR є наступним етапом розвитку технології SIEM. Однак остання має обмеження і виконує лише моніторингові функції та підготавлює звіти, залишаючи реагування на зовнішні рішення. Фактично кінцевим результатом діяльності SIEM є звіт про інциденти з можливими рекомендаціями щодо реагування. В той же час SOAR може не тільки надавати рекомендації, а й автоматично реагувати на події. Таким чином, SOAR має наступні функціональні можливості:

- оркестровка. В межах розслідування для збору додаткових даних і формування контексту аналітику необхідно взаємодіяти з різними засобами та системами моніторингу. Подібна «ручна» робота має два недоліки: по-перше, сильно уповільнює процес розслідування, по-друге – вона досить однотипна та нудна. Це є однією з головних причин високої плинності аналітиків першої лінії. Оркестровка дозволяє інтегруватися з різними системами для збору даних і керування ними, скорочуючи час на перемикання між консолями та інтерфейсами. Наприклад, при виявленні потенційної атаки, коли спрацювала віртуальна пастка, згідно плейбуку запускаються додаткові перевірки показників компрометації, включаються системи більш суворого сегментування корпоративної мережі або пошук сигнатур шкідливих кодів;

- автоматизація. SOAR-рішення дозволяє описати та автоматизувати виконувані в рамках розслідування рутинні дії за допомогою заздалегідь підготовлених сценаріїв реагування (Playbook). Таким чином, система дозволяє автоматизувати однотипні дії, які раніше аналітики виконували вручну, тим самим відчутно скорочуючи час на розслідування і збір необхідних даних для винесення рішень. Також варто відзначити, що не всі операції можна автоматизувати повністю і система повинна мати можливість дозволити зупинити процес і чекати подальших дій від оператора. Наприклад, після автоматичного збору даних про зараження кінцевої точки аналітик проводить аналіз достатності наявних доказів і приймає рішення про блокування скомпрометованого облікового запису або перенесення зараженого вузла мережі

в ізольований сегмент. План реагування повинен дозволяти будувати складні сценарії реагування з різними шляхами розвитку і розгалуженнями (у залежності від результату проведеного аналізу);

- реагування. Завдяки оркестрації SOAR-рішення має можливість автоматичного реагування та застосування певних дій щодо виявлених інцидентів. І хоча не завжди можливо в автоматичному режимі розв’язати проблему, це дозволяє переналаштувати засоби захисту в більш «жорсткі» режими роботи, оперативно виконати збір необхідної статистики та обмежити потенційно небезпечні операції. Наприклад, після заражень шифрувальником WannaCry актуальною функціональністю систем захисту стало оперативне реагування на зараження, щоб мінімізувати поширення елементів шкідливих кодів, – від швидкості реакції на агресивне зараження може сильно залежати отриманий кінцевий збиток. При застосуванні автоматичного реагування за допомогою показників компрометації можливо виявити заражені пристрої та відключити їх від основної мережі, щоб блокувати подальше поширення шкідливого коду.

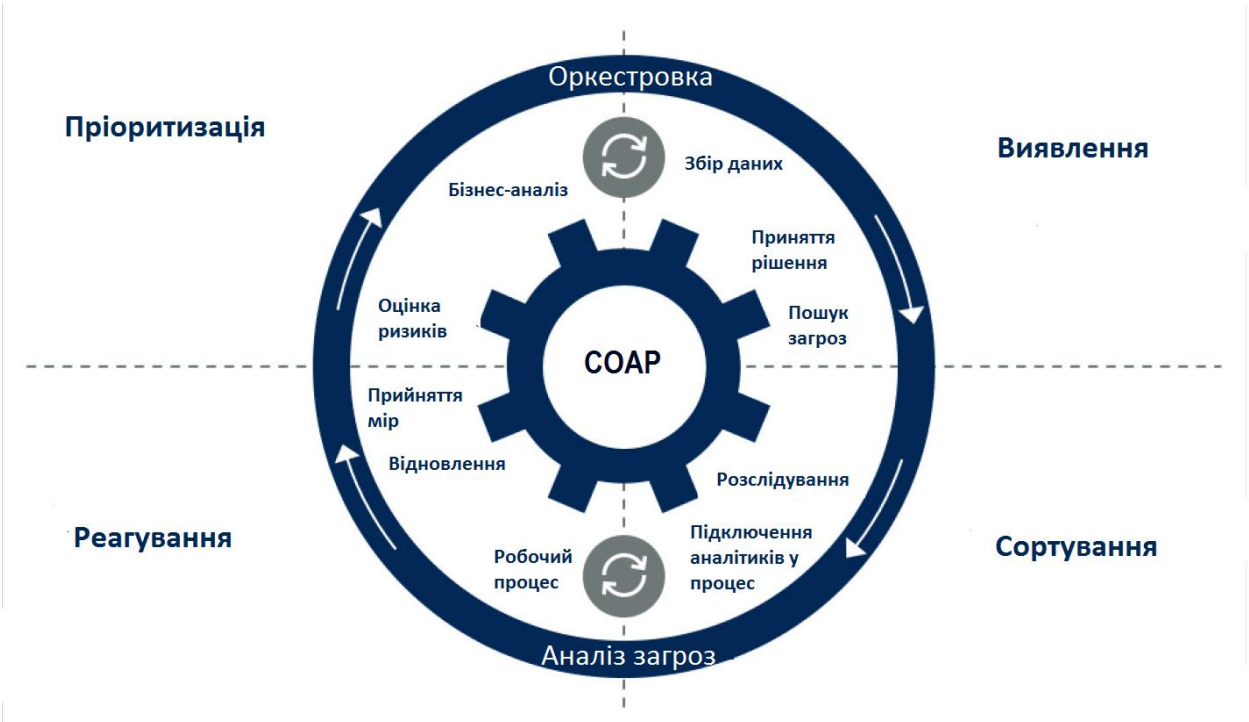

Рис. 2.5. Основні функції систем SOAR [31]

Також варто відзначити інші важливі функції SOAR-систем (рис. 2.5): оцінку ефективності роботи відділу ІБ, управління інцидентами ІБ, інтеграцію з різними постачальниками (так зване, Threat Intelligence). Таким чином, SOAR-рішення може стати єдиною точкою для ефективного управління інцидентами ІБ в компанії.

Також варто зазначити, що досить велика частина функціоналу SOAR належить до класу SIEM. Тому рішення SOAR може частково охоплювати функціонал SIEM як елементу первинного збору та обробки відомостей про події та інциденти, або інтегруватися з зовнішніми SIEM-системами для отримання характеристик зловмисної діяльності [22].

В той же час величезною перевагою SOAR над SIEM є повна автоматизація процесів управління інформаційною безпекою: починаючи від визначення та призначення пріоритетності та закінчуючи ситуативним реагуванням на інциденти. На відміну від простого аналізу логів подій, що застосовується у SIEM, рішення SOAR увібрали в себе цілий набір різноманітних технологій, що забезпечують безперервну діяльність сервісних центрів і служб моніторингу. Використання SOAR-систем дозволяє розробляти інтеграцію відомостей про загрози для системи безпеки, використовуючи інформацію, що надходить з різних джерел. Це досягається за допомогою трьох основних модулів SOAR-систем.

• Security Incident Response (ідентифікація інцидентів). Цей модуль спрощує проведення ідентифікації інцидентів. Також модуль займається імпортуванням інформації з підключених рішень ІБ і відповідає за актуалізацію процесів реагування на інцидент.

• Vulnerability Response (ідентифікація вразливостей). Модуль використовується для того, щоб розставити пріоритетність вразливостей, яка допомагає визначати схильність до загроз критичних для бізнесу систем. Завдяки цьому модулю проводиться:

- аналіз залежностей;

- оцінка впливу дій співробітників на бізнес-процеси, а також вплив вимушених простоїв;

- внесення необхідних змін;

- перевірка виконаних змін.

• Threat Intelligence (розпізнавання загроз). Модуль необхідний для виявлення індикаторів компрометації та відстеження загроз на більш глибоких рівнях. Його перевага в підтримці різноманітних стандартів, що служать для обміну відомостями про відомі ризики. До того ж цей модуль дає можливість підключати настроювані джерела та проводити обмін інформацією зі сторонніми системами моніторингу загроз[23].

Відповідно до завчасно налаштованого сценарію SOAR-система може самостійно відреагувати на ті чи інші події, що відбуваються в мережі. Це досить вагома перевага цього роду систем у порівнянні з іншими. Але для повноцінної роботи вимагається мати максимально повну та докладну базу даних подій, що взагалі відбуваються у спостережуваній мережі.

Завдяки оркестрації SOAR автоматично може проаналізувати всі отримані дані та прорахувати взаємозв’язок між багатьма несанкціонованими подіями, що для аналітика-людини через великий потік інформації може виявитись неможливим.

SOAR-системи апріорі є модульними, тому їх впровадження відбувається поступово, крок за кроком, з нарощуванням функціонального набору. Насамперед необхідно визначити, які завдання планується вирішувати на момент впровадження SOAR. Якщо йдеться лише про реагування на вірусні інциденти, то при інтеграції потрібно лише збагатити систему даними для антивірусу. По мірі наростання інцидентної бази, наприклад за рахунок доповнення її мережевими інцидентами, з'являтимуться інші засоби інтеграції та нові модулі. При впровадженні необхідно також брати до уваги рівень гетерогенності інфраструктури. Від цього залежатиме не тільки обсяг робіт, що виконуються, а й тривалість процесу впровадження SOAR. При впровадженні необхідно забезпечити такий функціонал, щоб SOAR «із коробки» одразу допомогла

отримати корисні результати. SOAR - це за визначенням конструктор, його функціональність поступово наростає з урахуванням вимог конкретного замовника. На думку спеціалістів, на повноцінне впровадження SOAR-системи іде в середньому щонайменше півроку. Досягти результату швидше не вийде: основні затримки виникатимуть на стороні замовника. "То немає одних даних, то інших ...". На думку інших спеціалістів, названий термін у півроку дуже занижений. Дуже багато залежить від інфраструктури. В інфраструктурі великого підприємства впровадження може затягтися на рік-півтора.

Проблеми впровадження[24].

Gartner зазначає, що основною перешкодою на шляху впровадження безпеки SOAR залишається відсутність чи низька зрілість процесів та процедур у командах SOC. Ось чому дуже важливо звернутися за порадою до фахівця під час планування впровадження SOAR.

Додаткові підводні камені, пов'язані з використанням SOAR:

- нереалістичні очікування. SOAR – не панацея від усіх проблем безпеки. Організації наражаються на ризик при впровадженні SOAR, якщо їм не вдається встановити чітко визначені сценарії використання та реалістичні цілі;

- надмірна залежність від автоматизації. Життєво важливо не покладатися просто на інструкції та процеси, які спочатку налаштовані в SOAR. Компаніям необхідно переконатися, що вони застосовують новітні знання з безпеки, щоб їх SOAR завжди був готовий ефективно реагувати на нові типи загроз;

- неясні метрики. Організації ризикують не отримати бажаних результатів від SOAR через свою нездатність чітко визначити параметри успіху. Важливо розуміти, що необхідно автоматизувати.

Висновки до другого розділу

У розділі було розглянуто стандартні робочі процедури при використанні методичних підходів щодо управління інцидентами інформаційної безпеки. Було

проаналізовано характеристики існуючих автоматизованих SIEM та SOAR систем в управлінні інформаційною безпекою.

Також було проаналізовано підходи щодо використання SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки та виокремлено варіанти розвитку систем. Було досліджено взаємозамінність та взаємодоповнення SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки.

Було визначено методи та засоби впровадження та експлуатації SIEM та SOAR систем.

Крім того, було розглянуто переваги, які отримує SOC при використанні SIEM та SOAR систем.

3 ДОСЛІДЖЕННЯ І РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ SIEM ТА SOAR СИСТЕМ НА ПІДПРИЄМСТВІ

3.1 Опис підприємства та постановка задачі на проведення дослідження на прикладі

Прагнення цифрової трансформації та хмарних сервісів для підвищення ефективності, підвищення гнучкості та скорочення витрат швидко та значно розширило поверхню атаки для більшості організацій[25]. Кіберзловмисники користуються цими тенденціями, оскільки співробітники стають все більш мобільними та віддаленими, отримуючи доступ до додатків, систем, служб та даних як локально, так і у хмарі з-за меж корпоративної мережі. Швидке збільшення кількості людей, які працюють вдома, прискорило цю тенденцію та посилило ризик.

Прагнучи захистити конфіденційні дані відповідно до зростаючого числа правил захисту даних у всьому світі, а також захистити інтелектуальну власність та іншу конфіденційну комерційну інформацію, більшість організацій вклали значні кошти в інструменти моніторингу безпеки на підприємстві та у хмарі.

Однак для багатьох організацій це спричинило щоденну лавину попереджень системи безпеки. Більшості цих організацій, особливо малим та середнім підприємствам, важко чи неможливо розслідувати та аналізувати кожне попередження.

Ще одним ключовим фактором стала нестача навичок кібербезпеки, що стосується організації всіх розмірів. SOCaaS дозволяє використовувати переваги центру управління безпекою (SOC) або додаткових ресурсів SOC без необхідності шукати та утримувати людей із необхідними навичками. SOCaaS також забезпечує можливість швидкого нарощування ємності та з набагато меншими витратами, ніж підтримка додаткових потужностей власними силами.

Перед обличчям все більш складного та швидко мінливого середовища бізнесу, IT та кіберзагроз зростає попит на SOCaaS, оскільки більшість організацій бачать цінність запропонованих переваг, які включають:

- безперервний та всебічний централізований моніторинг та аналіз корпоративних систем на предмет підозрілої активності за фіксованою та передбачуваною щомісячною або річною вартістю;

- поліпшення часу та методів реагування на інциденти;

- швидше виявлення подій безпеки, таких як компрометація та стримування загроз;

- дозвіл всіх попереджень для максимальної віддачі від існуючих систем;

- зниження витрат та впливу інцидентів безпеки на бізнес.

SOC-as-a-Service - це отримання послуг від вже наявного центру моніторингу і реагування одного з наявних провайдерів послуг ІБ на ринку. Зазвичай це - найпростіший і найменш витратний варіант реалізації SOC.

Провайдерів послуг ІБ можна розділити на два типи:

- послуги гібридного SOC. Коли центр моніторингу організований на базі інфраструктури замовника, а послуги моніторинга та аналітики виконує постачальник послуги;

- хмарний SOC. Цей варіант найкраще підійде для невеликих організацій, що не мають можливості для придбання та обслуговування власного SIEM-рішення, або для високотехнологічних компаній, у яких немає власного SOC, але які потребують швидкого результату і які готові використовувати в роботі аутсорсинг.

Отже, «віртуальний SOC», це коли прямі обов'язки фахівця з кіберзахисту покладаються на наявний персонал (адміністратори мережі, системні адміністратори тощо), виділеного приміщення може і не бути, а під SOC розуміються скоріше лише процеси забезпечення безпеки. Гібридний варіант - це коли якась частина функцій захисту забезпечується на місцях, а все інше передаються на аутсорсинг в комерційний SOC.

Комерційні SOC також мають назву «провайдери керованого сервісу безпеки» (Managed Security Service, MSS). Gartner визначає MSS як моніторинг або управління функціями IT-безпеки, що надаються за допомогою загальних служб з віддалених SOC, а не через персонал безпосередньо на місці[26].

MSS повинен відповідати трьом основним вимогам:

- цілодобовий віддалений моніторинг подій і джерел даних, що мають відношення до ІБ;

- забезпечення захисту відбувається віддалено з SOC, а не співробітниками на місці (і це має бути реалізовано як комерційно доступний сервіс, а не послуга для єдиного споживача);

- адміністрування та управління технічними засобами IT-безпеки.

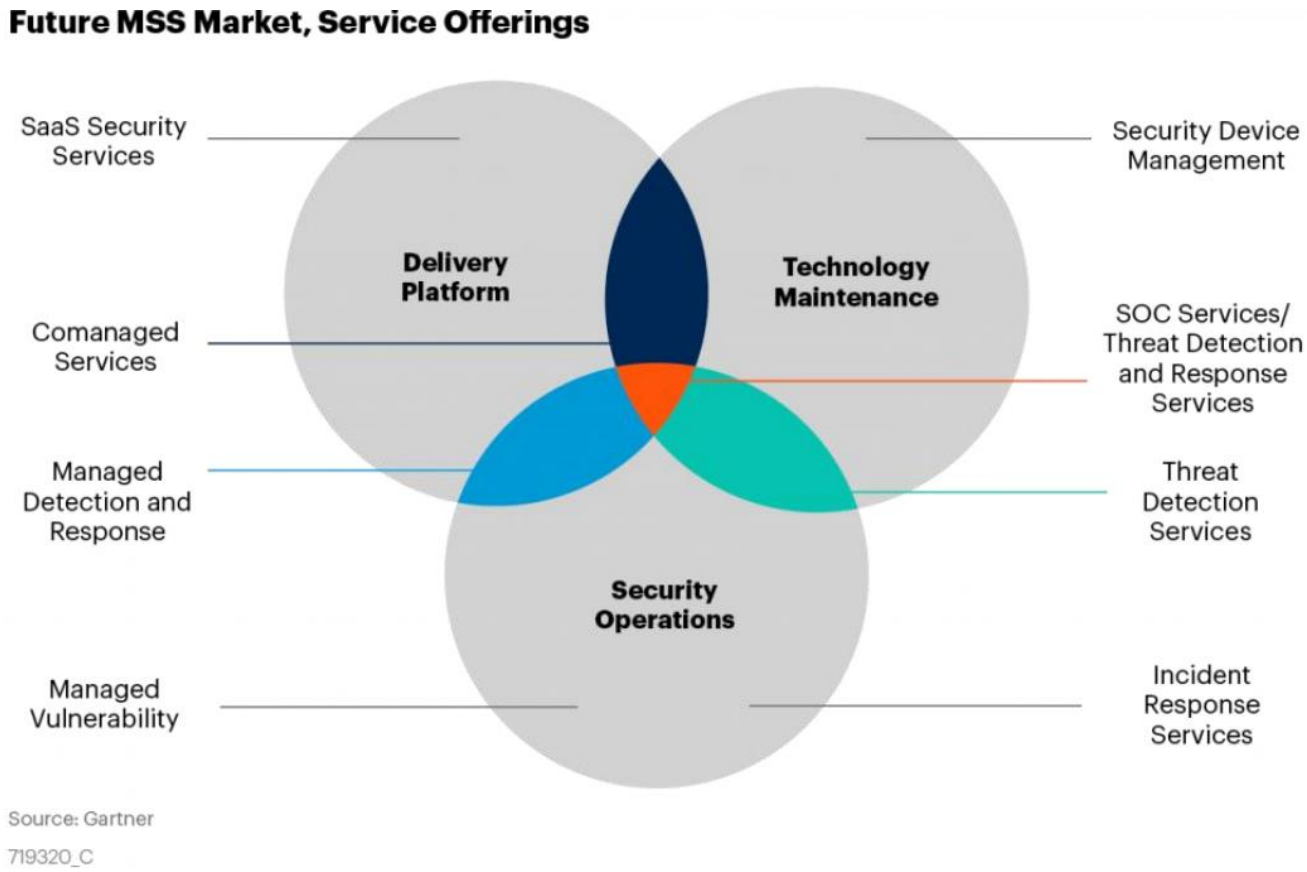

Рис. 3.1. Складові ринку MSS [27]

Крім моніторингу подій інформаційної безпеки, SOC може надавати інші послуги. Наприклад, управління міжмережевими екранами, системами IDS / IPS і іншими пристроями ІБ, реагування на інциденти ІБ (віддалено або з виїздом на

місце), оцінку вразливостей мережі та систем з супутніми діями (сканування, аналіз і вироблення рекомендацій). По мірі того як компанії все більше, і більше впроваджують хмарні технології систем безпеки, разом з тим розширюється і охоплення послуг віддаленого моніторингу.

Ринок MSS складається з трьох основних функціональних областей (рис. 3.1):

- платформи доставлення (Delivery Platforms) - Saas, хмарні або локально розміщені;

- технічне обслуговування (Technology Maintenance) - доставлення контенту та підтримка технологій;

- операції із забезпечення безпеки (Security Operations) – сервіс реагування на інциденти ІБ та сканери вразливостей[27].

Для проведення дослідження на прикладі запропоновано розглянути процес впровадження та експлуатації в організації системи управління інцидентами інформаційної безпеки з використанням SIEM та SOAR-систем за участі організації-надавача послуг SOC-as-a-Service – комерційного SOC.

На першому етапі, згідно методичних підходів щодо впровадження СУІБ, має бути розроблення та впровадження в організації політик та плану управління інцидентами ІБ та визначення стандартних робочих процедур.

Розроблення та впровадження політик УІБ відбувається безпосередньо всередині організації. Розроблення плану УІБ покладається на провайдера послуг SOC. Взаємовідносини сторін, їх відповідальність однієї перед іншою, а також стандартні робочі процедури УІБ описуються в укладених між сторонами SLA[28] (угоді про надання послуг) та NDA[29] (угоді про нерозголошення).

На цьому етапі має бути складений повний перелік послуг, що надаватиме SOC, включаючи:

- період часу моніторингу аналітиками подій, що відбуваються в мережі організації;

- час реагування на виникаючі події та інциденти ІБ в залежності від рівня критичності;

- послуги з встановлення, налаштування, розгортання та обслуговування апаратних та програмних засобів, що необхідні для виконання запропонованих послуг;

- необхідність та періодичність проведення аудіту ІБ, включаючи сканування на вразливості, що потребує певних додаткових дозволів.

Також має бути розроблена та затверджена мережева архітектура та вимоги до неї, що включають:

• програмні та апаратні компоненти, що застосовуватимуться для досягнення цілей, вимоги до них (включаючи апаратні вимоги, версії використовуємого ПЗ, IP-адресацію тощо);

• порядок взаємодії мережевих інженерів для налаштування доступу до цільових ресурсів з обох сторін (налаштування VPN, RDP, FTP та інших доступів);

• має бути складений перелік критичних ресурсів організації, що потребують особливої уваги. Це можуть бути як критично важливі сервери, так і облікові записи користувачів з підвищеними привілеями:

• має бути складений перелік ресурсів організації до яких SOC повинен мати доступ, в тому числі:

- цілодобовий доступ для виконання своїх безпосередніх обов’язків;

- ресурси з обмеженим доступом. Використання можливе за підтвердженої необхідності відповідальними особами;

• необхідність створення додаткових облікових записів для фахівців SOC з відповідними дозволами;

• інші питання, що можуть відношення до впровадження СУІБ.

3.2 Дослідження оптимізації процесів впровадження та експлуатації SIEM та SOAR систем

Необхідно зауважити, що в наведеному прикладі перед впровадженням SIEM та SOAR систем в організації, має бути повністю оговорена та налаштована взаємодія посадових осіб та інженерів организації та SOC. Також має бути налаштована мережева взаємодія та надані усі необхідні права та доступи.

В досліджуваному прикладі організація потребує послуг фахівців задля забезпечення процесу моніторингу та реагування на інциденти ІБ. Також необхідні додаткові інструменти обробки подій та реагування на інциденти через велику кількість необробленої інформації, що надходить від вже запроваджених:

- систем виявлення та запобігання атак (IDS/IPS);
- системи виявлення / запобігання вторгнень на хостах (HIDS / HIPS);
- мережевих екранів;
- журналів ОС, додатків і мережевих пристроїв, таких як журнали вебсервера, журнали веб-проксі, журнали DNS і попередження антивіруса (AV).

Після того як налаштовано мережеву взаємодію між організацією та SOC, можливо починати впровадження SIEM-системи з технічної частини, що включає в себе:

- підготовка фізичних чи віртуальних машин до розгортання кластеру SIEM;
- розгортання складових компонентів серверу SIEM-системи;
- встановлення на цільових системах агентів (сенсорів) SIEM-системи для збору логів;
- налаштування мережевої взаємодії серверу та агентів.

Після розгортання та налаштування сервер SIEM готовий для опрацювання подій в тестовому режимі. На цьому етапі вже є можливість увімкнути правила, що налаштовані “з коробки”. Предналаштовані дашборди відображають стан агентів, кількість подій, кількість підключених пристроїв. Таким чином вже починається накопичення статистики.

Подальше впровадження передбачає додаткове корегування та доповнення правил кореляції. Ця процедура починається з самого початку введення системи в експлуатацію і продовжується постійно впродовж її функціонування. Змінюються умови обробки подій, мережева інфраструктура, відключаються ОЗ звільнених працівників і створюються нові ОЗ для нових працівників. Все це робить середу спостереження динамічно змінюваною і потребує постійного перегляду контролів.

Після завершення цього етапу організація вже набуває вигоду через те, що їй вже не треба обробляти тисячі і тисячі подій. SIEM-система вже корелює та агрегує цю величезну кількість подій у відносно невелику кількість сповіщень безпеки.

Водночас по мірі того, як розширюється інфраструктура організації, або організація зацікавлена в моніторингу все більшої кількості своїх ресурсів, буде збільшуватись кількість агентів, що надсилатимуть інформацію про події на сервер. Це також є безперервним процесом і може тривати від початку тестування системи і до нескінченності, обмежуючись лише можливостями SIEM-системи щодо кількості підтримуваних пристроїв. Тож це питання також відіграє важливу роль при обранні SIEM-системи та розробленні плану УІІБ.

Як приклад щодо поліпшення процесу управління інцидентами інформаційної безпеки після впровадження SIEM-системи можна навести контроль за подіями невдалої аутентифікації користувачів. При опрацюванні інформації без кореляції та агрегації є вірогідність стикнутися з необхідністю обробки величезної кількості таких подій, надсилаємих, наприклад, контролером домену. І серед мільйонів помилок аутентифікації користувачів може не бути такої події, де дійсно б був якийсь злий намір. Однак, після запровадження SIEM-системи є можливість налаштувати правила таким чином, щоб події групувалися за ОЗ користувача і в консолі аналітик бачитиме вже не мільйони розрізнених подій, а десятки ОЗ користувачів з помилковою аутентифікацією.

Проте поліпшення процесу спостереження дуже опосередковано впливає на швидкість реагування. Без заперечень аналітик буде швидше обробляти події невдалої автентифікації, однак, все одно це потребує досить багато часу та уваги для аналізу і реакції. Тож на цьому етапі вже можливо впроваджувати SOAR-систему.

Впровадження SOAR-систем так само починається з встановлення програмного забезпечення на сервер. Проте, на відміну від розгортання SIEM-систем, SOAR-система не потребує розповсюдження агентів. Взаємодія з підключеними системами відбувається за рахунок використання API

(інтерфейс прикладного програмування). Для цього у системі налаштовуються необхідні конектори для взаємодії з кожною цільовою системою.

Після встановлення та перевірки мережевої взаємодії, можна налаштувати конектори до SIEM-системи для отримання від неї алертів в режимі реального часу, а також конектори до інших систем, що необхідні для забезпечення інформаційної безпеки підприємства (контролери домену, мережеві пристрої, IDS/IPS тощо). Слід взяти до уваги, що конектори до пристроїв, які будуть застосовуватись в процесах виконання автоматизованих SOAR-системою дій, мають підтримувати зв’язок в обох напрямках від і до системи (на відміну від SIEM, яка досить часто лише отримує інформацію). Це необхідно для того, щоб SOAR-система могла виконати команду на віддаленому пристрої за допомогою API.

Після налаштування всіх конекторів до пристроїв, необхідних для виконання оговорених послуг з забезпечення інформаційної безпеки, можна запускати тестування системи. На цьому етапі вже можливо починати розробляти та застосовувати плейбуки з обробки подій та реагування на інциденти ІБ.

Якщо взяти попередній приклад з невдалою автентифікацією та продовжити далі розглядати його, можна побачити в повному обсязі всю користь, що організація отримує від впровадження SOAR-системи.

Приблизний сценарій реагування (плейбуку) може мати наступний вигляд:

• після отримання алерту від SIEM, SOAR-система виокремлює з нього інформацію щодо:

- ОЗ користувача;

- підтипу події невдалої автентифікації (substatus для event_id 4625);

- IP-адреси, з якої здійснювалося підключення;

- інше, необхідне для розслідування та реагування;

• в системі створюється інцидент і починається його розслідування, що включає:

- перевірку IP-адреси на належність до зловмисної активності (збагачення за допомогою конекторів до баз знань VirusTotal тощо);

- перевірку ОЗ користувача (активний, вимкнений, заблочений, останній вдалий/невдалий вхід тощо за допомогою конектору до контролеру домену);

- опрацювання підтипу події (якщо у пароля користувача закінчився строк дії буде відображено substatus:0xC0000071 і це свідчить про те, що скоріш за все дії виконувалися легітимним користувачем, і він просто забув про зміну паролю. Але все одно така подія потребує уваги аналітика);

- інші передбачені плейбуком збагачення;

• далі в залежності від отриманої інформації можливі наступні варіанти дій:

- інцидент збагачується інформацією, отримує низький рівень пріоритету та очікує обробки аналітиком (в разі, якщо це схоже на дії легітимного користувача і не зафіксовано успішного входу цього ОЗ);

- інцидент збагачується інформацією, отримує середній рівень пріоритету та очікує обробки аналітиком, при цьому ОЗ користувача блокується (в разі, якщо це не схоже на дії легітимного користувача);

- інцидент збагачується інформацією, отримує високий рівень пріоритету та сповіщає аналітика про необхідність термінового реагування, при цьому ОЗ користувача блокується (в разі, якщо це не схоже на дії легітимного користувача, а IP-адреса, з якої відслідковувалися спроби входу, належить до зкомпроментованих);

- інцидент збагачується інформацією, отримує найвищий рівень пріоритету та сповіщає аналітика про необхідність негайного реагування, при цьому ОЗ користувача блокується (в разі, якщо це не схоже на дії легітимного користувача, зафіксовано вдалий вхід під цим ОЗ, а IP-адреса, з якої відслідковувалися спроби входу, належить до зкомпроментованих);

• SOAR-система надсилає сповіщення про інцидент аналітику;

• SOAR-система інформує користувача, під ОЗ якого були зафіксовані спроби невдалої автентифікації, за допомогою конектора до месенжера або Exchange.

Після завершення всіх попередніх дій з впровадження та налаштування SIEM та SOAR-систем можна починати їх експлуатувати як складову частину

системи управління інцидентами ІБ, постійно оновлюючи діючі та впроваджуючи нові функції, що вони надають.

3.3 Рекомендації щодо оптимізації впровадження SIEM та SOAR систем на прикладі

Процес оптимізації впровадження SIEM та SOAR систем можливо реалізовувати впродовж всього життєвого циклу існування систем, починаючи з процесу їх встановлення і закінчуючи регулярним переглядом та коригуванням плейбуків.

На етапі розгортання SIEM системи перше, що можна оптимізувати це розташування серверів. Якщо розгортати сервери SIEM безпосередньо в інфраструктурі організації, а не в мережі SOC, це дозволить зменшити навантаження на мережеві пристрої для передачі логів між підмережами замовника та SOC. Оскільки зазвичай між організаціями створюється та підіймається VPN-тунель, увесь трафік буде йти через один пристрій з кожного боку і його пропускної здатності може не вистачити для отримання постійного потоку даних. Якщо ж встановити сервер SIEM в одній мережі з пристроями, що моніторяться, це значно спростить процес збору та передачі логів від агентів до сервера і звільнить канал між організаціями для передачі вже корельованої та агрегованої інформації.

По-друге, на етапі розповсюдження агентів на пристрої можна створити автоматизовані скрипти, що значно прискорить процес створення кластеру. При наймні не треба буде на кожній системі щоразу вводити вручну одні й ті самі команди, а необхідно буде лише запустити скрипт. Крім того, ще можливо застосувати певні політики на контролері домену щодо розповсюдження і запуску таких скриптів. Звичайно це не збавить від необхідності встановлення особисто на кожен цільовий мережевий пристрій, але процес встановлення на робочі станції працівників може пройти значно швидше.

На етапі впровадження SOAR системи величезним плюсом буде використання мультитенантних систем. Мультитенантність - це можливість ізольовано обслуговувати користувачів із різних організацій (тобто незалежних передплатників SaaS) у рамках одного сервісу (однієї інсталяції чи розгортання). Це дозволить SOC не обмежуватись одним замовником, а знаходити нових і надавати послуги все більшому і більшому числу клієнтів. Для організації це в свою чергу дозволить не купувати цілу SOAR систему, а придбати у SOC лише частину ресурсів (тенант), яка буде обробляти лише цю організацію і матиме повний функціонал, однак буде значно дешевше. Крім того, розміщення SOAR на ресурсах SOC дозволить використати ресурси, на яких система мала розгортатися, для інших потреб.

Найбільшої оптимізації використання SIEM системи можливо досягнути за рахунок написання самописних правил кореляції, що контролюють лише обмежені певними умовами події. Це дозволить зменшити кількість хибно-позитивних спрацювань до прийнятного рівня, що, в свою чергу, вивільнить аналітиків для роботи з дійсно важливими подіями і інцидентами. В той же час необхідно розуміти, що відключення або тонке налаштування правил, що контролюють більш широкий діапазон подій, може призвести до виникнення хибно-негативних подій коли реальне порушення ІБ пройде непоміченим. Для того, щоб уникнути цього, необхідно щоб правила кореляції створював та редагував досвідчений кваліфікований спеціаліст.

Якщо продовжити розглядати приклад порушення ІБ з невдалою автентифікацією, можна наочно продемонструвати роботу правил кореляції в дії. Події невдалої автентифікації постійно надсилаються до SIEM системи, що призводить до формування відповідних попереджень, якщо увімкнено правило відслідковування таких подій. За умови, що користувач не має менеджера паролів та вводить щоразу свій пароль вручну, не буде дивним, що він періодично помилятиметься і вводитиме не вірний символ. Це призведе до формування події, а потім і сповіщення про порушення ІБ. Це буде явне хибно-позитивне спрацювання. Однак, можливо налаштувати правило кореляції таким чином, щоб

воно створювало попередження лише в разі виникнення інциденту, в даному випадку спробі підбору пароля. Для цього достатньо лише додати умову, щоб правило спрацьовувало не на кожну подію невірної автентифікації, а, наприклад, на десять невірних спроб протягом десяти хвилин. В такому разі при створенні алерту вірогідність того, що система зафіксувала спробу брутфорсу значно зростає.

Подібним прикладом оптимізації процесів з боку SOAR системи може слугувати створення більш складних та функціональних сценаріїв реагування (плейбуків). Варто пам’ятати, що розроблення плейбуків у SOAR системі, як і у випадку з правилами кореляції у SIEM, потребує досвідчених кваліфікованих фахівців. Функціональні можливості SOAR системи значно вищі за можливості SIEM, тож наскільки більше SOAR може принести користі при правильному використанні, настільки ж більше вона може нанести шкоди.

Ще одним прикладом оптимізації експлуатації SIEM та SOAR систем може слугувати створення кастомних дашбордів для моніторинга мережевої активності, кількості подій та інцидентів, контролю за дотриманням вимог щодо процесу реагування тощо.

Висновки до третього розділу

В даному розділі було розглянуто процес впровадження та експлуатації SIEM та SOAR систем як частини системи управління інцидентами інформаційної безпеки в організації.

На прикладі формування та оброблення типового інциденту ІБ було досліджено оптимізацію процесів впровадження SIEM та SOAR систем.

За результатами дослідження було розроблено наступні рекомендації щодо оптимізації процесів впровадження та експлуатації SIEM та SOAR систем:

- при впровадженні SIEM та SOAR систем необхідно враховувати технічні можливості ресурсів організації, за можливості більшу частину інструментів

моніторингу необхідно розгортати в тій самій підмережі яку необхідно моніторити;

- процес розгортання та налаштування можливо автоматизувати за допомогою самописних скриптів, що допомагають значно зекономити час;

- при обранні SOAR систем перевагу слід надати мультитенантним рішенням через їх гнучкість та універсальність;

- написання більш складних та вузьконаправлених для кожної конкретної цілі відстеження правил кореляції для SIEM систем та створення більш складних та багатофункціональних плейбуків для SOAR систем значно підвищує ефективність роботи SOC в цілому та якість і швидкість обробки інцидентів ІБ кожним аналітиком окремо. При цьому слід пам’ятати, що розроблення плейбуків у SOAR системі, як і у випадку з правилами кореляції у SIEM, потребує досвідчених кваліфікованих фахівців;

- для SIEM та SOAR систем існує можливість створення інформаційних дашбордів, що можуть повністю задовільнити потреби у візуалізації кількості подій та інцидентів, стану мережі, якості роботи SOC в цілому тощо.

ВИСНОВКИ

За результатами роботи:

1. Було розглянуто організацію побудови, впровадження та експлуатації системи управління інцидентами інформаційної безпеки. Було здійснено опис CSIRT, політик та плану управління інцидентами інформаційної безпеки. Також, було здійснено опис процесів під час впровадження та експлуатації SIEM та SOAR систем. Крім того, було здійснено опис функцій, що виконують SIEM та SOAR системи, та процесів, які SIEM та SOAR системи автоматизують.

2. Також було розглянуто стандартні робочі процедури при використанні методичних підходів щодо управління інцидентами інформаційної безпеки. Було проаналізовано характеристики існуючих автоматизованих SIEM та SOAR систем в управлінні інформаційною безпекою. Також було проаналізовано підходи щодо використання SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки та виокремлено варіанти розвитку систем. Було досліджено взаємозамінність та взаємодоповнення SIEM та SOAR систем в управлінні інцидентами інформаційної безпеки. Було визначено методи та засоби впровадження та експлуатації SIEM та SOAR систем. Крім того, було розглянуто переваги, які отримує SOC при використанні SIEM та SOAR систем.

3. На прикладі формування та оброблення типового інциденту ІБ було досліджено оптимізацію процесів впровадження SIEM та SOAR систем.

4. За результатами дослідження було розроблено наступні рекомендації щодо оптимізації процесів впровадження та експлуатації SIEM та SOAR систем:

- при впровадженні SIEM та SOAR систем необхідно враховувати технічні можливості ресурсів організації, за можливості більшу частину інструментів моніторингу необхідно розгортати в тій самій підмережі яку необхідно моніторити;

- процес розгортання та налаштування можливо автоматизувати за допомогою самописних скриптів, що допомагають значно зекономити час;

- при обранні SOAR систем перевагу слід надати мультитенантним рішенням через їх гнучкість та універсальність;

- написання більш складних та вузьконаправлених для кожної конкретної цілі відстеження правил кореляції для SIEM систем та створення більш складних та багатофункціональних плейбуків для SOAR систем значно підвищує ефективність роботи SOC в цілому та якість і швидкість обробки інцидентів ІБ кожним аналітиком окремо. При цьому слід пам’ятати, що розроблення плейбуків у SOAR системі, як і у випадку з правилами кореляції у SIEM, потребує досвідчених кваліфікованих фахівців;

- для SIEM та SOAR систем існує можливість створення інформаційних дашбордів, що можуть повністю задовільнити потреби у візуалізації кількості подій та інцидентів, стану мережі, якості роботи SOC в цілому тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ISO/IEC 27001:2013 Information security management. URL: https://www.iso.org/obp/ui/#iso:std:iso–iec:27001:ed–2:v1:en
2. Аудит та управління інцидентами інформаційної безпеки : навч. посіб. / [Корченко О.Г., Гнатюк С.О., Казмірчук С.В. та ін.]. К. : Центр навч.-наук. та наук.-пр. видань НА СБ України, 2014. – 190 с.
3. ISO/IEC 27035-2:2016 Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response
4. ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management
5. NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide. April 23, 2021
6. SIEM [Електроний ресурс] / [Автори Вікіпедії]. – Версія SIEM // Вікіпедія: Вільна енциклопедія. – Сан–Франциско: Фонд Вікімедіа, 2012. – URL: https://uk.wikipedia.org/wiki/SIEM– Загл. с титул. екрана. – Опис на основі версії, датованої 13 травня 2022 01:20UTC.
7. González-Granadillo, G.; González-Zarzosa, S.; Diaz, R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. — Sensors 2021, 21, 4759– URL: https://doi.org/10.3390/s21144759
8. David R. Miller, Shon Harris. Security information and event management (SIEM) implementation. — New York: McGraw-Hill, 2019. — 430 pages — ISBN 9780071701082, 0071701087.
9. SIEM: ответы на часто задаваемые вопросы [Електронний ресурс] – 2013. – URL: https://habr.com/ru/post/172389/

10. Overcoming Common Causes for SIEM Solution Deployment Failures 2017. – URL: https://www.gartner.com/en/documents/3732517/overcoming-common-causes-forsiem-solution-deployment-fa

11. What is a Security Operations Center (SOC)? [Електронний ресурс] – URL: https://digitalguardian.com/blog/what-security-operations-center-soc

12. Crystal Bedell. Definitive Guide to SOAR. — CyberEdge Press, 2019. — ISBN:1948939029, 9781948939027

13. Davor Karafiloski. SOAR guide: The fundamentals of Security Orchestration, Automation and Response. — Sumo Logic, September 17, 2020 URL: https://www.sumologic.com/blog/soar-guide-the-fundamentals-of-security-orchestration-automation-and-response/

14. Gartner Releases 2019 Market Guide for SOAR Solutions. URL: https://securityintelligence.com/posts/gartner-releases-2019-market-guide-for-soar-solutions/

15. ISO/IEC 27002:2005 Information technology — Security techniques — Code of practice for information security management

16. Обзор решений SIEM (Security information and event management) вопросы. URL: https://habr.com/ru/company/roi4cio/blog/528770/

17. Gartner Research. Emerging Technology Analysis: SOAR Solutions 2018. URL: https://www.gartner.com/en/documents/3895089

18. SOAR (Security Orchestration, Automation and Response)– URL: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/

19. The Definition of SOC-cess? SANS 2018 Security Operations Center Survey (https://www.sans.org/reading-room/whitepapers/analyst/definition-soc-cess-2018-security-operations-center-survey-38570)– URL: https://www.sans.org/reading-room/whitepapers/analyst/membership/38570

20. Ванерке Р. М. SOAR: автоматизация реагирования. URL: http://itsec.ru/articles2/Oborandteh/soar-avtomatizatsiya-reagirovaniya

21. Сусліна А. Обзор решений UBA, SIEM и SOAR: в чем различие? 2018. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/UBA-SIEM-SOAR

22. Как повысить производительность центров безопасности на порядок и еще +2 раза? URL: https://softprom.com/ru/kak-uvelichit-proizvoditelnost-tsentrov-bezopasnosti-na-poryadok-i-esche-2-raza-

23. Why your business needs SOC as a service: URL: https://www.computerweekly.com/opinion/Why-your-business-needs-SOC-as-a-service

24. Managed Security Services (MSS), Worldwide Reviews and Ratings– URL: https://www.gartner.com/reviews/market/managed-security-services-worldwide

25. The Managed Security Services Landscape Is Changing URL: https://blogs.gartner.com/pete-shoard/the-managedsecurity-services-landscape-is-changing/

26. Service-level agreement Wikipedia URL: https://en.wikipedia.org/wiki/Service-level_agreement

27. Non-disclosure agreement. URL: https://en.wikipedia.org/wiki/Non-disclosure_agreement

28. Deming Cycle (PDCA) – Importance in Agile. URL: https://www.techagilist.com/agile/deming-cycle/