МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: “ПРОДУКТИ ТА ТЕХНОЛОГІЇ В АРХІТЕКТУРІ SOC ОРГАНІЗАЦІЇ”

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

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

_____ Максим ДОВІРАК

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Максим ДОВІРАК

Керівник:
д.е.н., професор Світлана ЛЕГОМІНОВА

Рецензент:
д.т.н., професор Галина ГАЙДУР

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека
Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
“___”_____2023 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Довіраку Максиму Ігоровичу
(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Продукти та технології в архітектурі SOC організації”
керівник кваліфікаційної роботи Світлана ЛЕГОМІНОВА, д.е.н., професор
(Ім’я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від “19“ жовтня 2023 р. №145
2. Строк подання кваліфікаційної роботи “18” грудня 2023 р
3. Вихідні дані до кваліфікаційної роботи: *архітектура SOC, операційний центр безпеки, система управління та збору подій інформаційної безпеки, сучасні кіберзагрози*
4. Перелік питань, які потрібно розробити:
   1. Аналіз типових архітектур операційних команд безпеки та загроз, які стоять перед ними.
   2. Практичне використання сучасних продуктів SOC та розробка автоматизації реагування на інциденти.
   3. Розробка рекомендацій щодо реалізації сучасного SOC організації зі врахуванням викликів сьогодення
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання “02” жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”02” жовтня 2023 р.

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	виконано
2.	Збір та аналіз літератури.	23.10.2023	виконано
3.	Аналіз типових архітектур команд реагування на кіберінциденти та кіберзагроз.	27.10.2023	виконано
4.	Дослідження та практична реалізація сучасного продукту SOC Palo Alto XSIAM. Побудова плану реагування на інциденти та автоматизація реагування на них.	10.11.2023	виконано
5.	Визначення методів побудови SOC та побудова рекомендацій щодо його реалізації.	15.11.2023	виконано
6.	Формування висновків за результатами проведеного дослідження.	22.11.2023	виконано
7.	Оформлення роботи.	04.12.2023	виконано
8.	Оформлення презентації.	14.12.2023	виконано
9.	Отримання рецензії на роботу.	18.12.2023	виконано
10.	Захист в ДЕК.	16.01.2024	виконано

Здобувач вищої освіти _____ Максим ДОВІРАК
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Довірак М.І. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: " Продукти та технології в архітектурі SOC організації"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ДОВІРАК Максим** у кваліфікаційній роботі дослідив сучасні та типові архітектури центрів моніторингу та реагування на кіберінциденти та запропонував сучасний підхід щодо побудови центру безпеки на основі програмного продукту Palo Alto XSIAM. Відповідно, студент продемонстрував реалізацію архітектури SOC із використанням сучасних технологій штучного інтелекту, автоматизованим аналізом та реагуванням на кіберінциденти, збору подій інформаційної безпеки. Розглянуто основні типові помилки в архітектурах SOC та рекомендації по їх усуненню.
Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача **ДОВІРАКА Максима** на оцінку "відмінно" та присвоїти їй кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Довірак М.І. допускається до захисту даної роботи в Державній екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

Здобувач вищої освіти Довірак Максим Ігорович
на тему “Продукти та технології в архітектурі SOC організації”

Актуальність Швидке зростання кількості та складності атак вимагає постійного вдосконалення інфраструктури для виявлення, реагування та запобігання інцидентам безпеки. SOC відіграє ключову роль у цьому процесі, і технології повинні бути адаптовані до різноманітних викликів сучасного кіберпростору, включаючи розширення атак на різні рівні та різноманітні форми загроз. Зростання регуляторних вимог і перехід до хмарних та гібридних середовищ також визначають необхідність вдосконалення продуктів для ефективного захисту інформації. Усе це підкреслює важливість постійного розвитку продуктів та технологій для забезпечення безпеки та надійності SOC у сучасному цифровому ландшафті.

Позитивні сторони

1. У роботі досліджено основні типи архітектур Security Operation Center та методи його побудови в організаціях. Детально розібрані продукти та технології, які застосовуються для забезпечення роботи команд реагування на кіберінциденти. Наведені основні типи загроз та методи протидії від них. Практично реалізована архітектура команди безпеки на основі програмного продукту Palo Alto XSIAM.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки.
3. За результатами дослідження запропонована сучасна архітектура SOC в якій основну роль відіграє автоматизація типових процесів аналітиків центру безпеки, реалізація архітектури системи безпеки в хмарі та управління системами безпеки організації за методом “все в одному”.

Недоліки

1. Доцільно було б приділити більше уваги сучасним загрозам, які стоять перед командами безпеки, та яким чином сучасна архітектура SOC може ефективно їм протистояти.

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

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач Довірак Максим Ігорович заслуговує присвоєння кваліфікації “Магістр кібербезпеки за освітньо-професійною програмою “Управління інформаційною безпекою”.

Рецензент:
д.т.н., професор _____ Галина ГАЙДУР
(підпис)

РЕФЕРАТ

Кваліфікаційна робота присвячена аналізу продуктів та технологій в архітектурі SOC компанії. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел, що містить 36 найменувань. Загальний обсяг роботи становить 85 аркушів, з яких 3 аркуші займає перелік посилань.

Метою роботи є дослідження та аналіз взаємодії між технологіями та продуктами в архітектурі Security Operation Center.

Об'єктом дослідження є архітектура операційного центра безпеки.

Предметом дослідження – технології та продукти, які можуть бути застосовані для побудови ефективного та сучасного центру операційної безпеки організації.

Методи дослідження. Для вирішення завдань кваліфікаційної роботи застосовано метод аналізу та синтезу, компаративний аналіз технічної документації різних програмних комплексів, які використовуються в центрах операційної безпеки в організаціях малих, середніх та крупних розмірів, структурно-функціональний аналіз. А також підходи власного спостереження процесів та досвід, набутий в міжнародній компанії на посаді головний інженер центру операційної безпеки.

Короткий зміст роботи. Як результат у роботі проведено аналіз типових архітектур центрів моніторингу та реагування на кіберіцниденти: практично реалізовано сучасну архітектуру команди реагування на кіберінциденти за допомогою програмного продукту Palo Alto XSIAM із врахування захисту внутрішнього та зовнішнього периметрів мережі, а також використання інструментів автоматизації для реагування на загрози; результати проаналізованої інформації та практичних напрацювань застосовані для написання рекомендацій щодо реалізації сучасного центру SOC.

Галузь застосування. Розроблені рекомендації можуть бути використані під час аудиту центру операційної безпеки на підприємстві для розуміння

ефективності його роботи, а також для побудови сучасного ефективного SOC організації.

Ключові слова: ОПЕРАЦІЙНИЙ ЦЕНТР РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ, СИСТЕМА УПРАВЛІННЯ ПОДІЯМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, АВТОМАТИЗАЦІЯ РЕАГУВАННЯ НА ІНЦИДЕНТИ, АРХІТЕКТУРА SOC

ABSTRACT

The qualification work is dedicated to the analysis of products and technologies in the SOC architecture of the company. The text part of the qualification work for obtatining a master's degree: introduction, 3 sections, conclusions, and a list of used sources, which includes 36 references. The total volume of the work is 85 pages, with 3 pages allocated for the reference list.

The purpose of the work is to research and analyze the interaction between technologies and products in the architecture of a Security Operation Center.

Object of research is the architecture of the Security Operations Center.

Subject of research is the technologies and products that can be applied to build an effective and modern operational security center for an organization.

Research methods. To resolve the tasks of the qualification work, methods of analysis and synthesis, comparative analysis of technical documentation of various software complexes used in security operations centers of organizations of small, medium, and large sizes, as well as structural-functional analysis, have been applied. Additionally, approaches based on personal observations of processes and experience gained in an international company in the position of Lead Engineer of the Security Operations Center were used.

Brief content of research. As a result of the work, an analysis of typical architectures of security operation center for cybersecurity incidents was conducted. The modern architecture of a cybersecurity incident response team was practically implemented using the Palo Alto XSIAM software product, taking into account the protection of both internal and external network perimeters, along with the utilization of automation tools for threat response. The results of the analyzed information and practical developments were applied to formulate recommendations for the implementation of a modern Security Operations Center (SOC).

Field of research. The developed recommendations can be utilized during the audit of the Security Operations Center at the enterprise to assess its effectiveness and for constructing a modern and efficient SOC for the organization.

KEYWORDS: SECURITY OPERATION CENTER, AUTOMATED INCIDENT RESPONSE, SECURITY INFORMATION AND EVENT MANAGEMENT, MODERN SECURITY OPERATION CENTER ARCHITECTURE

ЗМІСТ

ВСТУП 12

РОЗДІЛ 1 ТИПОВА АРХІТЕКТУРА КОМАНДИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРЗАГРОЗИ 14

1.1 Необхідність та методи побудови Security Operation Center в організації 14

1.2 Огляд поточного стану архітектури SOC в компаніях 16

1.3 Загальна характеристика кіберінцидентів та кіберзагроз 24

1.4 Етапи побудови архітектури Security Operation Center 31

Висновки до першого розділу 36

РОЗДІЛ 2 38

РЕАЛІЗАЦІЯ СУЧАСНОЇ АРХІТЕКТУРИ SOC ЗА ДОПОМОГОЮ ПРОГРАМНОГО ПРОДУКТУ PALO ALTO XSIAM 38

2.1 Загальна характеристика та призначення Palo Alto XSIAM 38

2.2 Практична реалізація захисту внутрішнього периметру за допомогою Palo Alto XSIAM 40

2.2.1 Реагування на інциденти та їх автоматизація 52

2.3 Практична реалізація захисту зовнішнього периметру за допомогою Palo Alto XPANSE 58

Висновки до другого розділу 62

РОЗДІЛ 3 ПОБУДОВА СУЧАСНОЇ АРХІТЕКТУРИ SOC 64

3.1 Тенденції подальшого розвитку архітектур SOC 64

3.2 Рекомендації щодо побудови сучасної архітектури SOC 68

3.3 Рекомендації щодо вирішення типових проблем SOC 76

Висновки до третього розділу 78

ВИСНОВКИ 80

ПЕРЕЛІК ПОСИЛАНЬ 82

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІБ	-	інформаційна безпека
ІТ	-	інформаційна технологія
SOC	-	Security Operation Center, центр операційної безпеки
EDR	-	Endpoint Detection and Response, захисту кінцевих точок та реагування
XDR	-	Extended Detection and Response, розширене виявлення загроз та реагування
SIEM	-	Security Information and Event Management, управління інформаційною безпекою та подіями безпеки
MDM	-	Mobile Device Management, управління мобільними пристроями
ITSM	-	Information Technology Service Management, управління сервісами інформаційних технологій

ВСТУП

Актуальність теми. Кібербезпека організації стала одним з ключовим факторів для ефективного ведення бізнесу, що спонукало до залучення інвестицій для розвитку технологій та інструментів захисту інформації. Власне безпека в кіберпросторі є пріоритетом для сучасного інформаційного суспільства через зростання кіберзагроз, їх складністю та наслідками. Тому організації потребують напрацювань ефективних механізмів для захисту власних інформаційних систем, активів, мереж, процесів та пристроїв.

SOC – це один з найефективніших шляхів для захисту організації через те, що це відокремлений підрозділ в середині компанії, який займається моніторингом, аналізом та реагуванням на кіберінциденти в режимі реального часу.

Архітектура SOC визначає його структуру, функції, ролі, обов’язки, інструменти, технології, процеси, показники, стандарти та інші аспекти, які впливають на його ефективність та оптимальність. Побудова архітектури не є простим завданням через те, що її неможливо скопіювати чи перенести з однієї організації в іншу. Через велику сукупність різних факторів, які притаманні тій чи іншій організації, побудова центру операційної безпеки повинна включати потреби бізнесу в захисті без впливу на інші підрозділи компанії. Для багатьох організацій це може стати викликом у зв’язку з тим, що зміни вразливих інструментів чи процесів може зупинити критично-важливі процеси, які впливають на продуктивність інших підрозділів компанії та отримання прибутку в цілому.

З огляду на зазначене тема дослідження архітектури SOC компанії дозволяє виявити її сильні та слабкі сторони, а також дозволяє розробити практичні рекомендації щодо її вдосконалення, що є актуальним для багатьох організацій для ефективної адаптації до змінних умов кіберсередовища.

Мета роботи полягає у дослідженні та аналізі взаємодії між технологіями та продуктами в архітектурі центру операційної безпеки.

Об’єктом дослідження – є архітектура операційного центра безпеки.

Предметом дослідження – технології та продукти, які можуть бути застосовані для побудови ефективного та сучасного центру операційної безпеки організації. Для досягнення цієї мети в роботі поставлено до виконання наступні завдання:

1. Провести аналіз типових архітектур центрів реагування на кіберінциденти та кіберзагроз.
2. Реалізувати сучасну архітектуру центру реагування на кіберінциденти на основі програмного рішення Palo Alto XSIAM.
3. На основі проаналізованої інформації побудувати рекомендації щодо побудови сучасної архітектури SOC.

Методи дослідження. Для вирішення завдань кваліфікаційної роботи застосовано метод аналізу та синтезу, компаративний аналіз технічної документації різних програмних комплексів, які використовуються в центрах операційної безпеки в організаціях малих, середніх та крупних розмірів, структурно-функціональний аналіз. А також підходи власного спостереження процесів та досвід, набутий в міжнародній компанії на посаді головний інженер центру операційної безпеки.

Наукова новизна одержаних результатів. За результатами дослідження сформульована та запропонована до реалізації сучасна архітектура SOC організації. Запропоновані підходи до реалізації команди операційної безпеки, які дозволяють автоматизувати реагування на кіберзагрози, економити ресурси організації в довгостроковій перспективі, дозволяють ефективно захистити організацію від сучасних різних типів загроз.

Практичне значення одержаних результатів. Застосування напрацювань дають змогу здійснити побудову сучасного центру реагування на кіберзагрози, надають практичні рекомендації щодо вирішення проблем типового SOC організації, демонструють можливості по автоматизації реагування на кіберінциденти.

РОЗДІЛ 1
ТИПОВА АРХІТЕКТУРА КОМАНДИ РЕАГУВАННЯ НА КІБЕРІНЦИДЕНТИ ТА КІБЕРЗАГРОЗИ

1.1 Необхідність та методи побудови Security Operation Center в організації

SOC (Security Operation Center) стрімко розвивається за останні декілька років та демонструє високу ефективність у забезпеченні інформаційної та кібербезпеки в організації. Це доволі непроста інвестиція для багатьох організацій через те, що результат команди операційної безпеки вирахувати складніше за інші підрозділи. Якщо для будь-яких інших сфер бізнесу, інвестиції чи капіталовкладення можна обґрунтувати зростанням прибутку, відкриттям нових напрямів ведення бізнесу, технологічних проривів чи автоматизацією процесів для залучення меншої кількості людей та зменшення видатків, що переважають над прибутком, то з центром операційної безпеки це зробити складніше. Програмні комплекси у багатьох випадках є не простими, і потребують досвідченого персоналу для його налаштування та інтеграції в наявну інфраструктуру. А в свою чергу, досвідчений персонал для SOC на ринку праці знайти не так і просто, а із врахуванням реалій сьогодення, для багатьох зміна робочого місця може бути неможливим або надто ризиковим.

Для організацій різного розміру та масштабу стоїть декілька основних викликів, які необхідно вирішити перед тим, як починати інтеграцію команди реагування на кіберінциденти [1]. Серед основних, можна виділити наступні:

1. Стратегія забезпечення кібербезпеки складається з частини людей, яка відповідає за SOC в основному складається з технічного персоналу, завдання яких інтегрувати програмні комплекси, процеси та рішення для забезпечення моніторингу та реагування на кіберінциденти. Для вирішення та виконання цього завдання, необхідно побудувати чітку картину, до якої мети прагне керівництво компанії перед тим як інвестувати в кібербезпеку. В загальних практиках, за

стратегію відповідає CISO (Chief Information Security Officer) – директор з інформаційної безпеки компанії, який визначає політику, стратегію та стандарти інформаційної та кібербезпеки організації.

2. Аудит інфраструктури дає чітке розуміння реальної ситуації в інфраструктурі компанії є ключовим для визначення стратегії, а в майбутньому побудови ефективного SOC. Зовнішній та внутрішній аудит дозволяє зрозуміти, які ризики існують в організації, який периметр є менш захищений та критичніший для роботи компанії.

3. Оцінка ризиків з побудови кіберзахисту часто є розмінною монетою між простотою та зручністю виконання поставлених задач для персонала, які дещо можуть бути ускладнені або зробити денну роботу менш зручною. Заборона на використання персональних девайсів для виконання робочих задач, двоетапна автентифікація, перелік дозволеного програмного забезпечення, відсутність прав адміністратора, використання складних паролів та їх безпечне зберігання в менеджерах паролів, стандарти конфігурацій, тощо – все це створює незручності для повсякденної роботи для простого користувача, але в рази збільшує загальну захищеність організації. Ці загальні практики не просто реалізувати в організації, яка звикла так працювати останні роки чи десятиліття, саме тому оцінка ризиків повинна включати ці фактори.

4. Бюджет та інвестиції для бізнесу – це критичне питання, відповідь на яке одразу отримати складно. Для кожної організації зменшення витрат при отриманні кращого результату є “ідеальними” умовами. Але часто це зробити складно або неможливо. Це добре зрозуміло ринку, тому за останні десятиліття ринок послуг у сфері кібербезпеки зріз в рази та дозволяє організаціям любих розмірів, масштабів, сфери діяльності, потреб та бюджету вибрати для себе кращий варіант.

5. Ринок кібербезпеки пропонує різні методи інтеграції SOC, а всього існує декілька основних архітектур. Внутрішня інтеграція (Internal SOC) – дозволяє компанії самостійно розробити, впроваджувати та підтримувати свою систему кібербезпеки і дає повний контроль над процесами та інструментами,

але взамін потребує висококваліфікованого персоналу. Зовнішня інтеграція (SOC-as-Service / External SOC) – залучення сторонніх постачальників послуг, які надають готові рішення та платформи, консультації та підтримку у забезпеченні кібербезпеки. Цей варіант швидший та простіший в реалізації, але потребує довіри до стороннього постачальника, координації між компаніями, та витрат на сторонні послуги. Ну і гібридна інтеграція Hybrid SOC – що дає змогу поєднати зовнішні та внутрішні ресурси, персонал та інструменти. Цей варіант дає можливість компанії вибирати найкращі рішення, платформи чи програмні комплекси з урахуванням своїх специфічних потреб та цілей та в той же час отримувати консультації з-зовні для власного персоналу [2].

Якщо організація має чітке бачення результатів власних інвестицій та стратегію побудови кібербезпеки, команда операційної безпеки може значно зміцнити захищеність організації та ефективно виконувати власні функції щоденно в різних режимах роботи, наприклад тільки бізнес-години чи то навіть в режимі 24 на 7.

1.2 Огляд поточного стану архітектури SOC в компаніях

Кожна організація, як людський організм є унікальною, з власними методами ведення бізнесу та баченням власного майбутнього. В індустрії кібербезпеки, команди SOC застосовують неписані стандарти, яким чином функціонує та які інструменти застосовує. Як будь-який інший департамент, типові команди операційної безпеки складаються з декількох рівнів та можуть містити від декількох до десятків людей в залежності від потреб організації.

Компанія, яка веде власний SOC, в переважній більшості буде складатися з трьох основних рівнів. Перший – це рівень операторів аналітиків, завдання яких проведення моніторингу інфраструктури, реагування та ескалювання кіберінцидентів, згідно до інструкцій (Playbook), політик та практик компанії. Переважно, до складу аналітиків першої лінії входять люди з меншим досвідом, завдання яких закривати операційну роботу команди. Другий рівень – це

аналітики, які займаються аналізом кіберінцидентів, написанням правил детектування кіберзагроз та написання інструкцій щодо реагування на кіберінциденти (Playbook). Третій рівень – переважно складається з досвідчених членів команди, завдання яких усунення наслідків кіберінцидентів, консультація інших департаментів по запитам кіберінцидентів, інтеграція моніторингу на інфраструктуру, аналіз шкідливого коду. В залежності від організації, ті чи інші обо'язки можуть передаватися між рівнями або навіть бути об'єднані в один рівень задля кращої ефективності в роботі. До прикладу, сфокусуватися тільки на двох, де перший буде займатися комплексно запитами щодо аналітики та реагування на інциденти, а другий – налаштуванням систем чи аналізом шкідливого коду. Тут не існує кращого чи гіршого варіанту, а все впиратиметься в кількості запитів та об'ємом роботи, яка стоїть перед SOC командою.

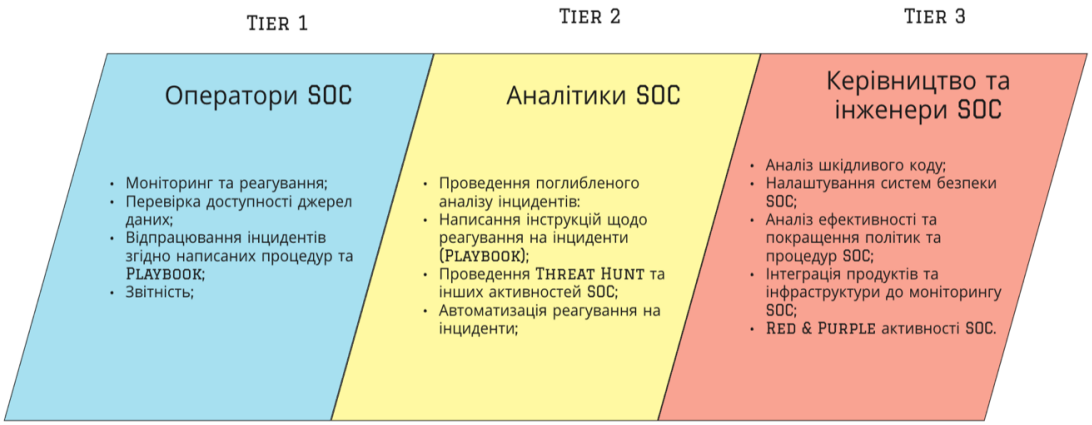


Рис. 1.1. Типові рівні центру операційної безпеки організації

Звичайно, що будь-яка кібер команда не обійдеться без програмних комплексів, якими вона здатна виконувати власні завдання. Ринок насичений різними продуктами та стартапами, які здатні підійти для організації будь-якого розміру та типу. Основним інструментом аналітики вважається SIEM (System Information and Event Management), яка надає команді SOC можливість централізовано збирати події, корелювати їх між собою та застосовувати для

виявлення кіберзагроз. Основною перевагою цього продукту є можливість інтеграцій. В своїй більшості будь-яке програмне рішення здатне інтегруватися з SIEM, що дає змогу не бути обмеженим в збиранні подій для моніторингу інфраструктури. Така система може бути розгорнута як в хмарних середовищах (SaaS Based) так і на ресурсах компанії (On-Prem). Також, варто не забувати, що існують інструменти з відкритим кодом, які можна використовуватися задля моніторингу домашньої інфраструктури чи для проведення власних досліджень. SIEM не обмежує тільки можливостями моніторингу, а також надає можливість будувати аналітичні звіти та панелі, які можуть бути використані операторами для більш ефективного виявлення інцидентів чи аномалій. Дані системи почали розробляти ще з 2005 року, і відповіді на запитання “Що таке SIEM?” зазнали багатьох змін. Зміни в тактиках проведення кібератак створили потребу в швидкому виявленні різноманітних загроз, проте традиційні рішення SIEM не можуть збирати та аналізувати значні обсяги даних з різних джерел. До прикладу, інтеграція хмарного середовища з SIEM системою, може бути зовсім неефективним у зв’язку з відсутністю необхідного рівня інтеграції у програмному рішенні, або унеможливлює створення нових правил виявлення кіберзагроз через відсутність необхідних функціональних спроможностей. У зв’язку з експоненційним зростанням обсягу даних, ті хто вибирають рішення SIEM, що базується на кількості вхідних подій, стикаються із зростаючими витратами та відсутністю передбачуваності ціноутворення. Таким чином, багато з них обмежуються вхідними логами лише з безпеки, щоб не перевищити бюджет, та створює прогалини у видимості для команди реагування [3].

SIEM відіграє важливу роль у відстеженні, виявленні та сповіщенні про події або інциденти в галузі IT. Він забезпечує комплексний та централізований погляд на стан безпеки IT-інфраструктури та надає фахівцям з кібербезпеки уявлення про події в їхньому IT-середовищі. У травні 2005 року Gartner поклали край дискусіям про те, що вибрати - SIM чи SEM, коли вони опублікували свою роботу “Покращення безпеки IT за допомогою відправлення вразливостей” [4]. Вони передбачили поєднання обох технологій і придумали термін SIEM -

рішення, яке могло б обробляти сирий журнал та робити це в реальному часі. Їх рекомендацією було розглядати виробників широкого спектру для інтегрованого продукту, який збирав дані про безпеку та аналізував їх на момент для виявлення патернів, які призводять до проблем з безпекою. І історія, схоже, повторювалася, коли в кінці 2021 року в одному зі своїх звітів Gartner передбачили, що консолідація платформ стане нормою. Згідно з їхніми прогнозами, “до 2025 року 80% підприємств приймуть стратегію єдиної платформи для доступу до вебу, хмарових служб та приватних додатків від одного постачальника на платформі безпеки (SSE)” [4]. Та ж сама логіка застосована до створення зіткнутих платформ, які допомагали клієнтам інтегрувати свій технічний стек та мінімізувати кількість засобів безпеки.

Наступним важливим кроком для команди кібербезпеки є захист інфраструктури, почати варто з кінцевих точок. Єдиним ефективним інструментом для цього є EDR (Endpoint Detection & Response). Оскільки такий інструмент дає можливість виявляти та блокувати кібератаки на рівні кінцевих точок, такі як комп’ютери, смартфони, планшети, віртуальні машини, тощо. EDR збирає та аналізує дані про поведінку та стан кінцевих точок, використовуючи різні методи, такі як антивірус, брандмауери, машинне навчання, штучний інтелект чи аналіз поведінки. Такий програмний комплекс дозволяє виявляти складні цільові атаки, які можуть уникнути традиційних засобів захисту та надає можливість відновлювати кінцеві точки після інцидентів або ізольовувати їх в мережі в один клік. EDR також інтегрується з іншими технологіями та інструментами, що можуть використовуватися в SOC, такими як SIEM чи SOAR. Таке рішення здатне забезпечити проактивний та оперативний захист від кіберзагроз, а також підвищити кіберстійкість та кіберготовність організації.

Проте з часом стало зрозуміло, що в EDR присутні певні обмеження з обізнаністю, а фокус тільки на кінцевих точках є недостатнім. До прикладу, зловмисник може використати тактику обходу EDR та проникнути в середину мережі за допомогою облікового запису користувача та активно використовувати скомпрометований обліковий запис для доступу до

конфіденційних даних компанії, що з точки EDR буде вважатися легітимною та нормальною активністю користувача. Для цього було розроблено технологію XDR (Extended Detection & Response), яка поєднує одразу дві основні компоненти: захист кінцевих точок та інтеграція з інфраструктурою, збирання журналів з інших систем до однієї консолі. Можна сказати, що це певний еволюційний крок у сфері кібербезпеки, який розширює поняття Endpoint Protection [5]. Якщо робити пряме порівняння, то основні відмінності між XDR та EDR включають:

- EDR фокусується на виявленні та реагуванні на загрози на рівні кінцевих точок. Зазвичай, працює відокремлено від інших програмних рішень та може вимагати інтеграції з SIEM чи SOAR. Також він занадто обмежений в кореляції подій між іншими системами, що є критично важливим для аналітики. До прикладу, уявімо інцидент, при якому була успішна компрометація хосту та поперечне пересування в інфраструктурі Lateral Movement. З точки зору аналітики EDR в оператора є можливість проаналізувати активність виключно на хості без будь-якої обізнаності, що відбувалось в інфраструктурі крім нього.
- XDR розширює це покриття на інші компоненти мережі та інфраструктури, створює більш повний погляд на ситуацію та обізнаність [6]. Такий продукт спроєктований для інтеграції з різними джерелами даних, і забезпечує більш широкий аналітичний огляд для виявлення та реагування на загрози. Узагальнюючи, XDR значно розширює поняття EDR та навіть запозичує деякі елементи з SIEM та SOAR, пропонує більш широкий погляд на безпеку та інтегрованість з різними джерелами даних для покращення захищеності кінцевих точок.

Наступним важливим елементом моніторингу в команді операційної безпеки є користувачі, а найбільш поширений метод атак на інфраструктуру починається з соціальної інженерії та фішингу. Поштові шлюзи є вразливими до нових методів соціальної інженерії такі як зловмисні QR-коди, сканування яких призведе до обходу мультифакторної автентифікації користувача. Шлюзи вимагають ретельної конфігурації та правильного і своєчасного моніторингу.

Команда реагування на інциденти має розуміти, як сконфігурований поштовий шлюз та правила безпеки на ньому і звичайно важливу роль відіграє конфігурація поштового серверу. Саме через його некоректну конфігурацію в зловмисників є можливість реалізації атак типу “людина-в-середині” (Man-in-the-middle), а з точки зору користувача це виглядатиме як типовий лист з посиланням від співробітника компанії, що не є підозрілим. Події з поштових шлюзів однозначно необхідно інтегрувати з іншими інструментами безпеки для повної обізнаності оператору про дії користувача, як на кінцевій точці, так і на власному клієнті пошти. Успішна інтеграція двох продуктів дозволяє відслідковувати цілий ланцюжок атак, починаючи від збереження та відкриття підозрілого файлу з пошти (Initial Access), до його виконання (Execution), поперечного пересування в інфраструктурі (Lateral Movement) та ексфільтрації даних (Exfiltration).

Обізнаність в інфраструктурі є елементом успіху команди реагування на інциденти. Знання про мережу, кількість кінцевих точок, критичних елементів, ассетів, тощо, дозволяє операторам своєчасно реагувати та приймати рішення при активних інцидентах. Для обізнаності в інфраструктурі та її стану використовують сканер вразливості. Переважно під управління сканером вразливості виділяють окремих операторів, які сфокусовані над регулярним оновленням даних про мережу, скануванням кінцевих точок, конфігурацією профілів сканування, аналізу та побудовою плану усунення вразливостей. За допомогою сканеру вразливостей в команди операційної безпеки є розуміння про найуразливіші елементи в інфраструктурі та своєчасному усуненню нових критичних вразливостей. В свою чергу, враховуючи тенденцію переходу до хмарних технологій та хмарної інфраструктури, сканера вразливостей стають менш ефективними через відсутність можливості виявлення помилок в конфігурації хмарних середовищах, можливості інвентаризації всередині хмар, тощо.

Операційні команди часто працюють одночасно з великою кількістю подій, тому ефективний кейс менеджмент є важливим компонентом на рівні з програмними рішеннями для забезпечення кібербезпеки. Задля ефективної

комунікації між департаментами та управлінням інцидентами із врахуванням кращих практик для вирішення цього завдання використовують ITSM (IT Service Management) – це інструмент до управління та надання послуг IT, який визначає ролі та завдання необхідні для кожного етапу виконання завдання, проєктування та вдосконалення IT-послуг. За допомогою нього можна покращити процеси надання IT-послуг, а також вирішення кіберінцидентів. Основною перевагою такого продукту є чітка градація обов'язків та прав на вирішення того чи іншого інциденту, що мінімізує ризики втрати критичних подій в інфраструктурі. Операційний центр має змогу конфігурувати час на реагування на інциденти, що в майбутньому дасть змогу відслідковувати ефективність роботи команди за критеріями, такі як тип інцидентів, зони покриття, відповідальність, які кроки були здійснені задля усунення проблеми та відповідального оператора за інцидент. Також користувачі та персонал організації має змогу створити запит до команди операційної безпеки у випадку виявлення підозрілої активності. Таким чином в інструменті ITSM, SOC має єдине бачення про інциденти та запити та може ефективно оперувати ними відповідно до пріоритетності. Це значно прискорює роботу команди і дає змогу централізовано вирішувати кіберінциденти та будувати статистику, наприклад які сегменти мережі найбільше генерують інциденти та яким чином можна виправити таку ситуацію.

Основним елементом в архітектурі SOC є процеси [7]. Можна виділити декілька основних процесів, які побудовані в центрах операційної безпеки. Варто розпочати з управлінням подіями інформаційної безпеки, яке реалізовується за допомогою програмного комплексу SIEM і дає обізнаність про події в IT-інфраструктурі. На основі збирання подій, команда операційної безпеки має можливість побудувати аналітичні звіти в режимі реального часу і в декілька кроків відповісти на типові запитання, які можуть виникати під час моніторингу: кількість активних робочих станцій, кількість користувачів та кількість невдалих автентифікацій, перелік країн з яких здійснюються автентифікації користувачів, перелік найбільш активних активів компанії, кількість запобігань вторгнень

(IDS/IPS), кількість отриманих подій, кількість відкритих інцидентів, тощо. Цей перелік можна розширювати в залежності від потреб підрозділу організації.

Наступним важливим кроком є реагування на кіберінциденти та розроблений план реагування на них. Incident Response здійснюється за допомогою інструкцій операторами SOC, та можуть бути автоматизовані, до прикладу програмними рішеннями як SOAR, які у випадку виявлені сигнатури розробленої в інструкції (плейбук), виконує реагування в режимі реального часу без участі аналітика. Варто зазначити, що плейбуки варто розробляти під конкретний тип кіберзагроз розроблені аналітиками, щоб мінімізувати ризики неправильного аналізу чи помилкового закриття реального інциденту. План щодо реагування на інциденти та оркестрація – два суміжні процеси, які варто розробити командам операційної безпеки. Оркестрація – це використання автоматизованих інструментів для виконання рутинних завдань та автоматизація робочих процесів для ефективного реагування на інциденти. В свою чергу, план щодо реагування на інцидент може бути автоматизований, для прикладу ізоляція кінцевої точки у випадку виявлення комунікації з ботнет мережею. Управління інцидентами та сповіщеннями (Incident & Alert Management) визначає тип інцидентів, їх пріоритетність, статус вирішення та час на вирішення того чи іншого кейсу [8].

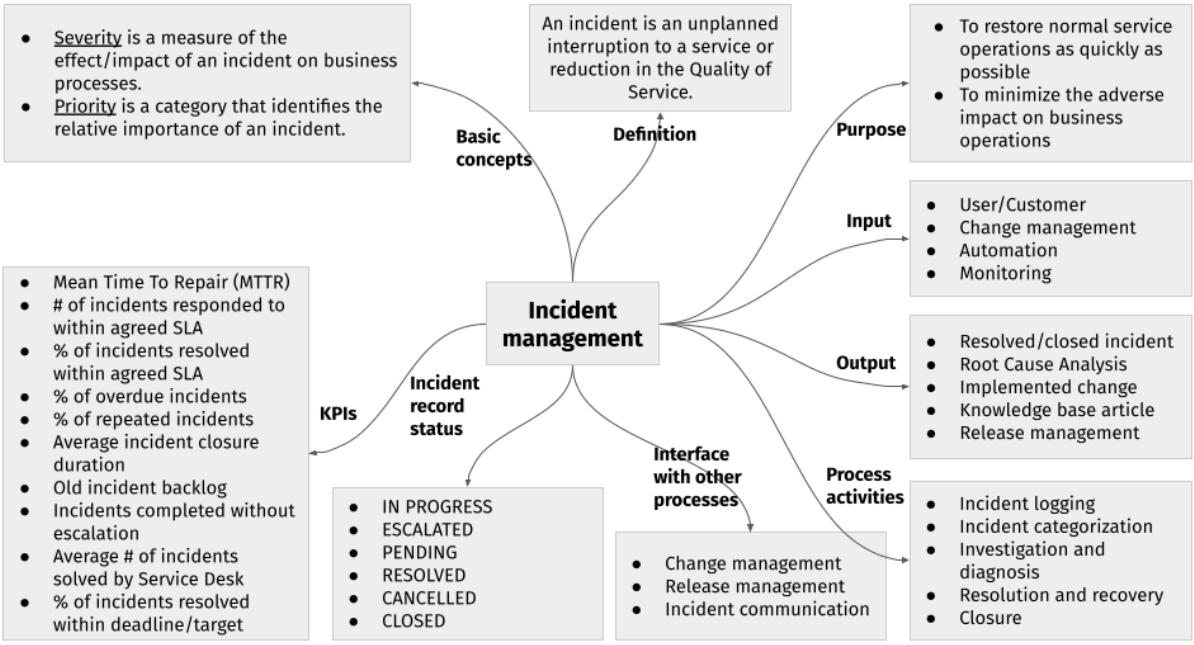


Рис. 1.2. Управління інцидентами та його критеріями

Лідер операційної команди безпеки, повинен визначити перелік та тип кіберінцидентів, якими оперує SOC, а також які статуси використовуються під час їх вирішення, наприклад False Positive, True Positive Benign, Confirmed Security Incident, Inconclusive, тощо. Правильне управління кейсами SOC дає змогу аналізувати найбільш активні вектори атак на інфраструктуру та планувати подальше покращення програмних комплексів щоб зменшити кількість інцидентів інформаційної безпеки або ж мінімізувати вплив зловмисників на інфраструктуру. Останнім основним критерієм можна визначити звітність, яку варто вести лідеру команди операційної безпеки. Розробка звітності дасть змогу відслідковувати ефективність персоналу та їх помилки, дасть змогу демонструвати керівництву компанії обізнаність та статус кібербезпеки в організації, будувати та планувати покращення безпеки інфраструктури та залучати більше інвестицій для проведення пасивних так і активних дій задля покращення безпеки.

1.3 Загальна характеристика кіберінцидентів та кіберзагроз

Кіберінциденти та кіберзагрози становлять серйозну загрозу для сучасного інформаційного суспільства. Задля їх протидії та зменшення впливу на організацію, команди операційної безпеки реалізовують комплексні заходи та методи до їх протидії. Для початку варто розглянути відмінності між кіберінцидентами та кіберзагрозами.

Кіберінцидент - це непередбачена подія або серія подій в кіберпросторі, яка може призвести до порушення конфіденційності, цілісності чи доступності інформації, а також до шкоди комп'ютерним системам чи мережам [9].

Кіберзагроза - це будь-який потенційний вектор атаки, який може викликати кіберінцидент, загрожуючи інформаційній безпеці, економіці чи навіть національній безпеці [9].

Кіберінциденти можуть приймати різні форми та мати різні характеристики. Розпочати варто з обсягу. Від окремих ізольованих випадків до масштабних атак, які можуть впливати на великі території. Типи атак - кіберінциденти можуть включати в себе різноманітні атаки, такі як витік чутливої інформації, атаки на доступність мережі, чи використання вразливостей програмного забезпечення. Ступінь складності - від простих, здійснюваних аматорами, до складних та високотехнологічних атак, що вимагають великого рівня експертизи. Залежно від джерел, кіберзагрози можуть бути класифіковані на різні категорії. Наприклад, в Україні, основними видами кіберзагроз вважаються:

Кіберзлочинність – це протиправне втручання в роботу кібернетичних систем, створення та використання в злочинних цілях певної кібернетичної (комп’ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп’ютерних) систем. [9]

Кібертероризм та кібершпигунство - це активності, спрямовані на застосування сили або шантажу для досягнення політичних, економічних або соціальних цілей через кіберпростори. [8]

Кібервійна – це застосування кібертехнологій для проведення військових дій, включаючи кібершпигунство, кібервійну, кібертероризм та кіберспам [9].

Можна впевнено сказати, що українській кіберсектор є найгарячішою точкою конфлікту в кіберпросторі. Посилаючись на звіти від Microsoft [10], на Україну спрямовані чисельні атаки на критичну інфраструктуру, цивільне населення, комерційні компанії, енергетичні об’єкти, які одночасно можуть координуватися з військовими діями. Так, до прикладу восени 2022 року, під час масованих ракетних обстрілів на енергетичні об’єкти нашої держави, проросійські актори здійснювали кібератаки на критичну інфраструктуру, які здійснювались паралельно з військовими операціями [11].

Центри операційної безпеки акумулюють величезну кількість подій в режимі реального часу і кожен кіберінцидент має власну класифікацію та тип. Вважається, що найкращими практиками є класифікація інцидентів відповідно до матриці MITRE. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) [12] - це засіб, що використовується в галузі кібербезпеки для опису дій, тактик та технік, які використовують кіберзлочинці та інші загрози для проникнення в інформаційні системи. Цей фреймворк розроблений MITRE Corporation і надає широкий огляд загроз та методів їхнього виявлення. Основні компоненти MITRE ATT&CK [12]:

- Тактики (Tactics): Описують загальні цілі атак та стратегії, які використовуються зловмисниками. Приклади тактик включають “Execution” (виконання коду), “Persistence”" (збереження доступу) і “Privilege Escalation” (підняття привілеїв).
- Техніки (Techniques): Конкретні методи чи способи використання тактик для досягнення конкретних цілей. Наприклад, “Spearphishing Attachment” (цілеспрямований фішинг з використанням вкладеного файлу) або “Exploit Public-Facing Application” (експлуатація публічних веб-додатків).
- Матриці (Matrics): Специфічні таблиці, які відображають відносини між тактиками та техніками. Наприклад, MATRIXTM для Enterprise та MATRIXTM для Mobile охоплюють атаки в корпоративних та мобільних середовищах відповідно.

- Групи та Загрози (Groups and Threats): MITRE ATT&CK включає інформацію про конкретні групи зловмисників та загрози, їхні методи та тактики. Це дозволяє організаціям зрозуміти, які конкретні загрози можуть становити небезпеку їхнім системам.

- Миттєві Тактики та Техніки (PRE-ATT&CK): Охоплює етапи атаки, що передують основному вторгненню, такі як розвідка, виявлення слабкостей і підготовчі дії.

Ефективне використання матриці дає кращу обізнаність про інцидент операторам SOC, а найголовніше планувати ефективні методи протидії кібератакам. Компанії, які спеціалізуються над аналізом кіберзагроз та акторів, використовують матрицю MITRE для пошуку патернів, почерку акторів, які в свою чергу дають можливість ідентифікувати організатора атаки.

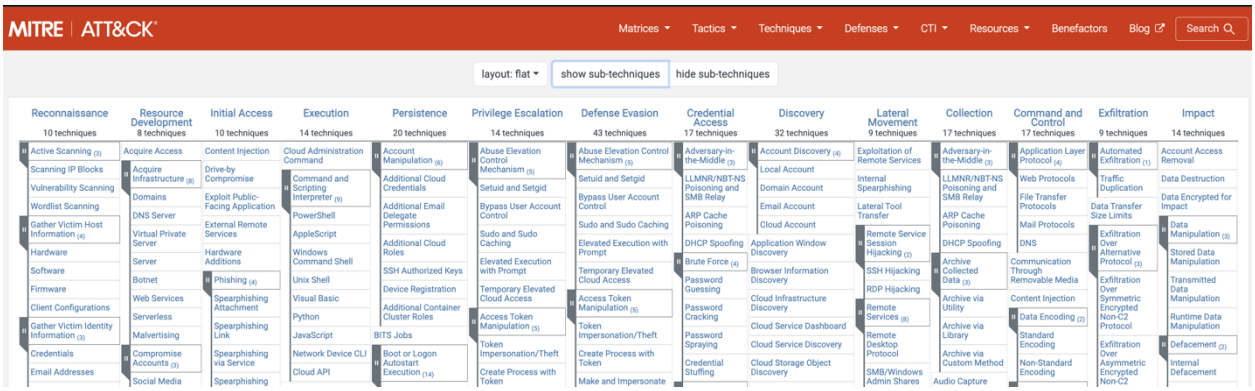


Рис. 1.3. Матриця MITRE

Згідно з останнім звітом “Verizon 2020 Data Breach Report: Money Still Makes the Cyber-Crime World Go Round” [13] з кіберзлочинності, 86% атак фінансово мотивовані: зловмисники або безпосередньо вимагають гроші у жертви, або виконують сторонній замовлення, наприклад, конкурентів чи інших недоброзичливців. Найбільшою мірою сьогодні схильні до атак оператори зв’язку, фінансові організації, ритейл-мережі і промисловий сектор. Крім того все більше привертає уваги кіберзлочинців малий і середній бізнес. Це пояснюється тим, що конкуренція в ньому досить висока, а можливості кіберзахисту і оцінки ризиків часто обмежені. Посилює проблему масовий

перехід на віддалену роботу, через що периметр мережі організації поширився на будинки співробітників і їх особисті пристрої. Отже, враховуючи всі ці фактори, можна виділити наступні типові кіберзагрози на даний час, з якими оператори SOC найчастіше стикаються: програми-вимагачі, цільові кібератаки, DDoS-атаки, інсайдерські загрози та фішинг.

Віруси-вимагачі шифрують дані на комп'ютері користувача і вимагають викуп за можливість відновити доступ до них. Зазвичай пропонується здійснити викуп криптовалютою. Проникнувши в корпоративну мережу, віруси-вимагачі здатні блокувати відразу велику кількість комп'ютерів. Найбільш схильні до атак з метою вимагання телекомунікаційні компанії, інтернет-провайдери, освітні установи, урядові і технологічні організації. У кіберзлочинності спостерігається тенденція до спеціалізації і співпраці. Об'єднуючи зусилля, зловмисні актори успішно справляються з системами захисту великих організацій, розділяючи виручку. Для повноцінного захисту від вимагачів потрібно не тільки сучасне програмне забезпечення, а й системна профілактика, що включає оцінку ризиків, фаерволи та коректну сегментацію мережі, створення резервних копій, розробка різних сценаріїв та плейбуків реагування на інциденти. Пасивні методи захисту є також ефективними для протидії проти вірусів-вимагачів. Для багатьох компаній курси з кібербезпеки та правила кібергігієни стають нормою і обов'язковим етапом, які тісно інтегровані в кодекс та політики організації. Таким чином, створюється контроль та регулярне нагадування про те, що жоден інструмент з кібербезпеки не здатен захистити організацію, як окрема особа і відповідальність щодо безпеки лежить на кожному з її членів. Загальна обізнаність створює ефективний метод протидії, а можлива нетипова поведінка в мережі, буде ескальована до команди операційної безпеки задля додаткової перевірки.

В останні роки кіберзлочинці перейшли до більш цілеспрямованих атак, зосереджуючись на конкретних галузях з їх характерними уразливими місцями. Зростання частки цілеспрямованих атак зумовлений низкою причин. По-перше, зловмисники жадають не витрачати час на компанії, які не гарантують їм

грошовий прибуток. По-друге, щорічно з’являються нові групи зловмисників, які спеціалізуються на атаках класу APT (Advanced Persistent Threat – різновид складних кібератак з метою отримання несанкційованого доступу до інформаційних систем жертви та встановлення прихованого доступу до неї з метою використання або контролю в майбутньому). Цільова атака полягає в тому, що спочатку зловмисники шукають спосіб потрапити в корпоративну мережу: збирають інформацію, шукають уразливості організації (не тільки цифрові, але й фізичні), вивчають розклад, маршрути, слабкості, цікавлять співробітників та інше. Потім здійснюється власне проникнення: зловмисники можуть надіслати на конкретного співробітника фішинговий лист, вкрасти телефон співробітника для вилучення будь-яких корпоративних паролів, втертися в довіру компанії під виглядом підрядника або проникнути в офіс в якості кур’єра. Метою на цьому етапі є приховане встановлення програмного забезпечення на корпоративній техніці. На останньому кроці діючи вже з середини компанії, зловмисники підбираються до інформації, яка їх цікавить і викрадають її в обхід засобів захисту. Потім, як правило, зловмисники замітають сліди, щоб атака не була виявлена. В цільової атаці можуть використовуватися будь-які інші кіберзлочинні методи – фішинг, вимагання та інше. Запобігання цільових атак – складне завдання. Однак сучасні засоби захисту при їх правильному і комплексному використанні дозволяють зрозуміти, що відбувається якась неавторизована активність [14].

DDoS-атака – це атака на будь-яку обчислювальну систему (наприклад, сервер) з метою вичерпати її апаратний ресурс шляхом величезної кількості одночасних звернень до неї. Коли система не справляється з обробкою цих звернень, відбувається відмова в обслуговуванні (Denial of Service) і система виходить з ладу. DDoS-атаки становлять небезпеку в першу чергу для компаній, діяльність яких безпосередньо пов’язана з інтернетом (електронна комерція), а також для операторів зв’язку. Останнім часом зловмисники використовують для своїх ботів пристрої інтернету речей (IoT), тобто, наприклад, побутові прилади з підключенням до інтернету: принтери, розумні колонки, кондиціонери, системи

освітлення в розумному будинку та інше. Виробники IoT-пристроїв, як і користувачі цих пристроїв, найчастіше не приділяють уваги їх безпеки, тому заразити IoT-пристрій відносно просто. Для боротьби з DDoS-атаками застосовують DDoS-фільтри, що дозволяють вибірково відсікати зайві звернення до сервера, що йдуть від ботів. Профілактика DDoS-атак включає розумну мінімізацію контактів системи з іншими пристроями: доступ до системи повинен бути закритий для портів, протоколів і додатків, взаємодія з якими не передбачено [14].

І звичайно фішинг - це вид шахрайства, метою якого є виманювання у довірливих або неуважних користувачів мережі персональних даних. Найчастіше приманкою є електронний лист, здатний зацікавити одержувача, а гачком – закладений в цей лист шкідливий виконуваний файл або гіперпосилання на нього. На даний час, це може бути посилання на свіжу статистику по темі, що стосується Covid, або якусь іншу актуальну інформацію, яка цікава багатьом користувачам [14]. Небезпека фішингу в тому, що головний елемент в ньому не технічний, а психологічний. Зловмисники знають, що людину обдурити легше, ніж машину. Сучасні засоби захисту дозволяють в автоматичному режимі у всіх файлах, які передаються поштою або через інтернет, аналізувати посилання в процесі відкриття і переривати цей процес, якщо фіксують запуск виконуваних файлів.

Команда операційної безпеки здатна працювати з різними векторами атак, чи це типове зловмисне програмне забезпечення з поганою репутацією чи то навіть комплексна APT-атака на об’єкт критичної інфраструктури. Постійний та регулярний моніторинг мінімізує ризики комплексної атаки на об’єкт, так як постійне відслідковування активності в мережі та користувачів дозволяє виявляти аномалії чи нетипову активність. Це і є основною перевагою SOC – постійна обізнаність про IT-інфраструктуру та фокус над подіями та виявлення інцидентів.

1.4 Етапи побудови архітектури Security Operation Center

Людство на протязі свого існування використовує планування як єдиний ефективний метод досягнення цілей. Не є виключенням і побудова команди реагування на кіберінциденти, тому організації вимушені розпочати його побудову виключно з попереднім плануванням та його розбиттям на етапи або фази. Ці кроки дозволяють уникнути проблем під час експлуатації SOC, а концептуальні необдумані архітектурні рішення можуть загрожувати правильній роботі команди реагування на кіберінциденти. Отже, загальними кращими практиками під час побудови Security Operation Center є розбиття цього процесу на чотири фази: планування, дизайн, побудова та експлуатація [15].

Етап *планування* починається з оцінки існуючих можливостей безпеки для людей, процесів і технологій. Цей підхід дозволяє встановити базову лінію, яку можна порівняти з цілями для майбутнього SOC. Ця стратегія потрібна як новим SOC, так і існуючим SOC, які хочуть покращити свої можливості. Можна визначити основні критерії для планування:

- Визначення та ідентифікація бізнес-цілей SOC та IT.
- Визначення можливості, які необхідно оцінити, на основі цілей SOC.
- Зібрати інформацію про людей, процеси та технологічні можливості.
- Проаналізувати зібрану інформацію та призначити рівні зрілості оціненим можливостям.
- Представлення, обговорення та формалізація результатів в конкретні кроки та строки.

Ідея планування полягає в тому, щоб спочатку визначити бізнес-цілі організації, щоб усе, що буде розроблено, мало значення для керівництва, яке спонсорує SOC. Наступним кроком є перелік можливостей, які відповідають бізнес-цілям, визначеним на першому кроці. Можливості включають наявних людей, процеси та технології. Для кожної можливості встановлюються рівні зрілості, які, у свою чергу, узгоджуються з бізнес-ціллю, щоб можна було визначити пріоритетність прогалин для розробки плану створення майбутнього

SOC. Цей план обговорюється та зрештою закріплюється всіма сторонами, відповідальними за розробку SOC.

Другою частиною етапу планування є розробка вашої стратегії SOC, яка складається з таких елементів: головна місія SOC, стратегічні цілі SOC, область контролю SOC, модель роботи SOC, послуги SOC, дорожня карта розвитку можливостей SOC, ключові показники ефективності SOC (KPI) і метрики.

Неадекватна або неточна оцінка можливостей SOC призведе до слабкої стратегії SOC, яка не відповідає цілям організації. Не варто пропускати та поспішати на етапі оцінювання та варто переконатися, що завершені всі пункти стратегії, перш ніж переходити до наступного етапу.

На етапі планування має бути визначена модель роботи майбутнього SOC: фізична, віртуальна чи гібридна. На етапі планування також буде визначено тип послуг, які надаватиме SOC, вказано, чи відповідає SOC за всю мережу чи частину мережі, а також деталі цих послуг [15].

Після завершення етапу планування наступним кроком є дизайн SOC. Етапи дизайну та будівництва майже нерозривно пов’язані, і вибір технології є основною частиною обох етапів для майбутнього SOC. Одним із важливих напрямків є те, як SOC збиратиме дані. Зазвичай це завдання виконується за допомогою централізованого інструменту збору даних, такого як рішення для керування інформацією та подіями безпеки (SIEM). Інші інструменти безпеки, такі як фаерволи, фільтри трафіку та контенту, системи виявлення/запобігання вторгненням тощо, експортуватимуть події до SIEM, дозволяючи аналітикам SOC оцінювати всі події, щоб отримати ширшу картину поточного стану безпеки організації. Існує багато різновидів технологій безпеки; однак найкраща практика полягає в тому, щоб переконатися, що обраний підхід використовує багаторівневі можливості, щоб, якщо захід захисту не виявив нападу, був доступний інший засіб, щоб запобігти атаці. Наявність брандмауерів кількох постачальників, розташованих один до одного, не забезпечує значної додаткової безпеки, оскільки всі брандмауери, ймовірно, матимуть однакові відкриті порти. Наявність як системи запобігання вторгненням (IPS), так і антивірусного

програмного забезпечення – це добре, але обидві технології базуються на сигнатурах і, ймовірно, виявлятимуть подібні загрози. Кращим підходом було б використання багатошарових можливостей захисту/виявлення, таких як: фільтр вмісту, який може виявляти шкідливі веб-джерела, IPS для виявлення атак, захист кінцевих точок або розширена його версія (EDR/XDR), яка шукає невідомі загрози, пропущені IPS, інструмент (наприклад, NetFlow), який створює базову лінію мережі, а потім відстежує в ній незвичайні тенденції даних.

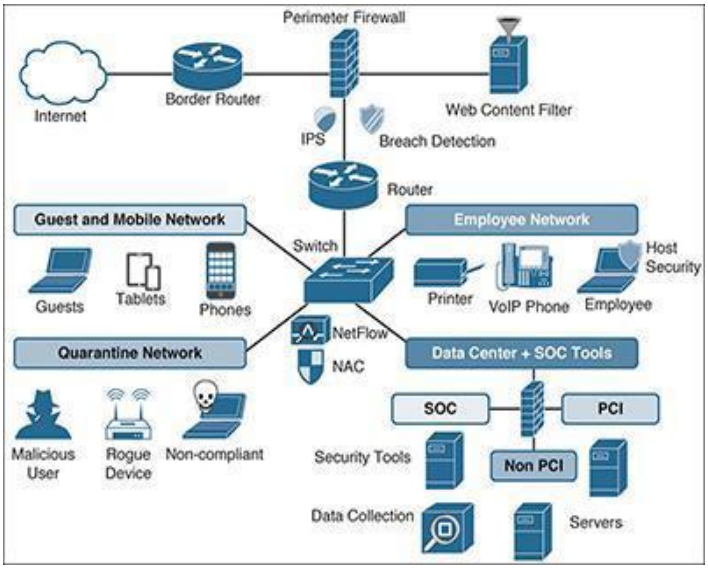


Рис. 1.4. Контроль периметру SOC організації

Захист безпеки має поширюватися на всі ділянки мережі. Якщо не забезпечити однаковий рівень безпеки для різних частин вашої мережі, найменш захищена область, швидше за все, стане ціллю зловмисників для атаки. Деякі області проектування, які слід включити, включають безпеку краю мережі, мобільних пристроїв, робочих столів користувачів, філій і центру обробки даних.

Щоб визначити та захистити найслабшу ланку в організації, SOC має включати можливості керування вразливими місцями. Обсяг цих послуг має бути визначений у плануванні послуг SOC. Технологія, необхідна для життєвого циклу керування вразливістю, може включати інструменти оцінки, які ідентифікують і кваліфікують уразливості такі як Nessus, OpenVAS або Metasploit, а також різні підходи до розрахунку рівня ризику, пов’язаного із

загрозою, щоб визначити, як пом’якшити її, передати, прийняти або уникнути вразливості. Також важливо мати автоматизований інструмент інвентаризації та оцінки, щоб SOC знав про всі існуючі активи та їхній поточний ризик для організації. Без цієї інформації SOC може не оцінити деякі активи, що може наражати організацію на невідомий ризик.

Після завершення проектування останньою сферою, яку слід розглянути перед переходом до етапу експлуатації, є оцінка людей. Це може бути найскладнішою частиною цього кроку, оскільки сьогоднішній ринок праці продовжує мати більше робочих місць, ніж кваліфікованих людей, які можуть їх заповнити. Ця ситуація також ускладнює утримання талантів, оскільки робота SOC може бути дуже складною та повторюваною, і часто вимагає тривалого робочого дня. Ефективний процес і процедури можуть допомогти підтримувати стабільність послуг, коли посадові ролі змінюються; однак надмірна залученість у процес і процедури може негативно вплинути на роботу SOC, відокремлюючи найкращих виконавців.

Коли SOC побудовано, настав час переходити до фази експлуатації, також відомої як фаза “ввійти в дію” [15]. Вкрай важливо, щоб новий SOC подолав деякі ключові проблеми до дати запуску. По-перше, важливо підтвердити, що SOC все ще має виконавче спонсорство. У багатьох випадках проходить великий проміжок часу між початковим погодженням керівництва щодо створення SOC до моменту, коли SOC фактично готовий до роботи. Процеси будуть складними, оскільки деякі з них будуть новими та потребуватимуть перевірки. Технології потрібно перевірити, щоб переконатися, що все працює належним чином. Може знадобитися навчання для членів команди, які відповідають за використання та підтримку рішень. Перехід через кожен крок від будівництва до експлуатації SOC вимагає добре керованого плану переходу. Успішні плани переходу, як правило, мають деякі спільні фактори успіху. Перше, чи критерії успіху чіткі та зрозумілі. Простий контрольний перелік критеріїв успіху слід узгодити зі спонсорами як частину дизайну, і цей перелік має стати основою для управління очікуваннями та виконанням. Наступним важливим кроком є те чи ресурси

детальні та добре структуровані. Це може стосуватися людей, часу або грошей. Має бути чітко визначено, як і коли очікується кожен ресурс протягом проекту чи програми. Вимоги до навичок, технологій, результатів і змісту чіткі та досяжні. Команда має бути достатньо навченою до дати запуску, щоб виконувати роботу. Можна виконати прості перевірки, щоб переконатися, що мета була успішно досягнута. Необхідно розробити простий контрольний список, який чітко визначає, як будуть оцінюватися результати кожної діяльності, завдання або етапу. Після того, як SOC запрацює, завершальним етапом є перевірка того, наскільки успішно він працює, а також визначення областей для покращення. Перевірка SOC компанії не дуже відрізняється від перевірки будь-якої іншої важливої та дорогої бізнес-функції. Наступний п'ятиетапний метод добре працює для розробки звіту, який можна використовувати для оновлення керівництва щодо поточного стану SOC. Це може включати всі аспекти SOC як частину всебічного огляду, але часто корисніше обмежити обсяг і зосередитися на окремих сферах. Необхідне чітке визначення учасників, щоб розуміти, хто буде виступати і брати участь в огляді. Конкретні учасники можуть залежати від обсягу перевірки. Встановлення чіткої методології дуже важливо в цьому процесі. Організації необхідна чітка методологія, щоб керувати будь-яким переглядом, а також очікувані результати та результати на основі заздалегідь визначеного шаблону. Необхідно вирішити, як часто виконувати такі перевірки. Певні типи оглядів можуть або мають відбуватися частіше. Наприклад, рекомендується виконувати часті огляди після інциденту протягом перших 72 годин після нього, щоб люди, які були залучені, не забули певні події, пов'язані з інцидентом. Пріоритезація результатів та дій як і в будь-які сфері, які потребують покращення, і пов'язані з ними дії мають бути визначені за пріоритетністю, виконані та виконані, щоб гарантувати внесення необхідних змін. SOC має продовжувати працювати над покращенням ключових показників ефективності (KPI) для можливостей, які відповідають бізнес-цілям, щоб судити про те, чи послуги працюють на очікуваному рівні. Керівники SOC повинні націлюватися на KPI для кожної категорії можливостей, створених на етапі

проектування, пов’язаних із конкретними часовими рамками, такими як щоквартальні перевірки. Недосягнення цілей може вказувати на потребу в більшій кількості людей, процесів, покращення технологій або їх зміна.

З усіма цими вимогами легко зрозуміти, чому SOC може не виконати своїх початкових обіцянок. Жоден SOC не є ідеальним, але здоровий SOC може розвиватися на краще. Зусилля щодо підтримки, перегляду та вдосконалення вашого SOC є основоположними для його довгострокової життєздатності. Варто пам'ятати, що SOC – це подорож, а не пункт призначення.

Висновки до першого розділу

За результатами аналізу проведеного в першому розділі, було досліджено доцільність та необхідність створення власного центру моніторингу та реагування на кіберінциденти в організації. Враховані основні ризики та виклики під час його побудови і визначено основні моделі архітектур команди SOC: зовнішнє управління, повністю інтегровані в структуру організації та гібридна модель. Також проведений аналіз поточних типових архітектур SOC в організаціях. Компанія, яка веде власний SOC, в переважній більшості буде складатися з трьох основних рівнів. Перший – це рівень операторів аналітиків, завдання яких проведення моніторингу інфраструктури, реагування та ескалювання кіберінцидентів, згідно до інструкцій (Playbook), політик та практик компанії. Другий рівень – це аналітики, які займаються аналізом кіберінцидентів, написанням правил детектування кіберзагроз та написання інструкцій щодо реагування на кіберінциденти (Playbook). Третій рівень – переважно складається з досвідчених членів команди, завдання яких усунення наслідків інцидентів, консультація інших департаментів на запити забезпечення кібербезпеки, інтеграція моніторингу інфраструктур, аналіз шкідливого коду. Критичними для команд реагування на кіберзагрози є інструменти, тому розглянуто основні типи програмних комплексів, які застосовані для моніторингу та захисту організації: SIEM, EDR, XDR, ITSM, SOAR, фаерволи та

поштові шлюзи. Визначена відмінність та методи застосування кожного із них, які в цілому складають основу архітектури безпеки. Наведені основні напрями та загрози від яких команда SOC повинна захищати організацію. Центри операційної безпеки акумулюють величезну кількість подій в режимі реального часу і кожен кіберінцидент має власну класифікацію та тип. Вважається, що найкращими практиками є класифікація інцидентів відповідно до матриці MITRE. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge). Серед основних загроз зазначено програми-вимагачі, які все частіше стають не тільки фінансово вмотивовані, але і мета яких деструктивний характер, тобто знищення IT інфраструктури організації задля зупинки критично-важливих процесів організації. Команда операційної безпеки здатна працювати з різними векторами атак, чи це типове зловмисне програмне забезпечення з поганою репутацією чи то навіть комплексна APT-атака на об’єкт критичної інфраструктури. Постійний та регулярний моніторинг мінімізує ризики комплексної атаки на об’єкт, тому що, постійне відслідковування активності в мережі та користувачів дозволяє виявляти аномалії чи нетипову активність до того як зловмисники розпочнуть активні дії. Це і є основною перевагою SOC – постійна обізнаність про IT-інфраструктуру, фокус над подіями та виявлення інцидентів. Визначені основні етапи під час побудови операційного центру з кібербезпеки: планування, дизайн, побудова та експлуатація.

РОЗДІЛ 2
РЕАЛІЗАЦІЯ СУЧАСНОЇ АРХІТЕКТУРИ SOC ЗА ДОПОМОГОЮ ПРОГРАМНОГО ПРОДУКТУ PALO ALTO XSIAM

2.1 Загальна характеристика та призначення Palo Alto XSIAM

Враховуючи потреби та вимоги кожної організації можуть плануватися та реалізовуватися різні типи команд реагування на комп'ютерні інциденти: гібридна, зовнішня та внутрішня SOC команда. Ринок кібербезпеки збільшується разом із пропозиціями програмних продуктів, тому бачення "все в одному" набирає все більше популярності задля простоти та швидкості обізнаності про події та інциденти організації. Поки найкраще це вдається реалізувати за допомогою систем SIEM, які можуть працювати з іншими IT рішеннями і дають можливість операторам бачити єдину картину про події з інтегрованими системами, даючи можливість економити час для аналізу та обізнаність під час інциденту. Можна спостерігати як потреби SOC змінюються з часом, але дизайн SIEM та SOC ні. Більшість ключових елементів архітектури були модернізовані, до прикладу типовий антивірус перейшов до технології EDR та XDR, перехід захисту мережі від типових фаерволів до Zero Trust та SASE, перенесення інфраструктури до хмарного середовища. На відміну від цього, занадто багато SOC команд застрягли з 20-річною моделлю, де SIEM та її правила є серцем і ключем всіх операцій та безпеки команди. Звичайно, що з сучасними загрозами це є недостатньо, тому сучасний центр операцій повинен будуватися на новій архітектурі включаючи наступні елементи:

- Широкий вибір інтеграцій, автоматизації, аналізу та сортування даних.
- Уніфіковані робочі процеси, які дозволяє аналітиками бути продуктивними незалежно від кількості активних операторів SOC.

- Вбудований штучний інтелект і автоматичне реагування, які можуть блокувати атаки з мінімальною допомогою аналітика. Ввести щось нове та змінити парадигму підходу до реалізації SOC спробувала компанія Palo Alto з програмним рішення XSIAM, яке ще називають SIEM нової генерації, об’єднуючи в собі сучасні технології, захист кінцевих точок та автоматизацію реагування на інциденти. Cortex XSIAM - (extended security intelligence and automation management) - об’єднує найкращі в своєму класі функції, включаючи кінцеву точку виявлення та реагування (EDR), розширене виявлення та відповідь (XDR), оркестровка безпеки, автоматизація та реагування (SOAR), управління зовнішнім периметром та атак на неї (ASM), аналіз поведінка користувача та суб'єкта (UEBA), платформа аналізу загроз (TIP), і безпеки управління інформацією та подіями (SIEM). Використання спеціальної моделі даних безпеки та застосування машинного навчання XSIAM автоматизує інтеграцію даних, аналіз і сортування для відповіді більшість сповіщень. Це дає змогу зосередитися на інцидентах, які вимагають втручання людини. Модель даних постійно оновлюється за допомогою Palo Alto Networks дані про загрози, зібрані в усьому світі серед десятків тисяч клієнтів. XSIAM використовує дизайн на основі ML для інтеграції масивних обсягів даних безпеки, об’єднувати сповіщення в інциденти для автоматизованого аналізу та сортування та автоматично реагувати на більшість інцидентів. XSIAM уже перевірено у виробництві, живлячи власний SOC Palo Alto Networks перетворюючи трильйон подій на місяць у кілька аналітичних інцидентів на день. Враховуючи всі ці фактори, на ринку все більше і популярніші рішення “SOC-In-A-Box”. В сучасному ланшафті загроз організації, які стурбовані лише припиненням відомих типів атак, матимуть величезні прогалини у своїй безпеці використовуючи типові SIEM рішення. Це тому, що всі SIEM, так чи інакше, залежать від написання правил для набору даних, щоб спробувати ідентифікувати шаблони чи патерни загроз.

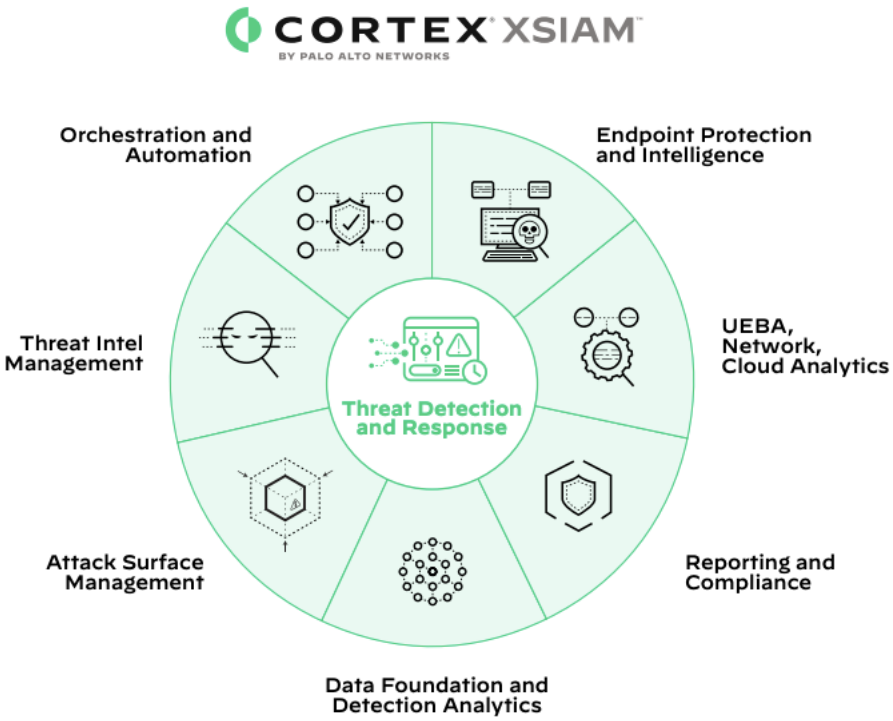


Рис. 2.1. Огляд архітектури Cortex XSIAM

Основною перевагою рішення є вбудовані правила детекцій різного типу інцидентів з врахуванням матриці MITRE, які регулярно оновлюються командою реагування на інциденти Palo Alto UNIT42. Оперуючи величезну кількість подій клієнтів та власної інфраструктури, їх команди має змогу побудувати унікальні виявлення, як на типові атаки, так і на атаки типу “нульового дня”

2.2 Практична реалізація захисту внутрішнього периметру за допомогою Palo Alto XSIAM

Система нового покоління Cortex XSIAM складається з декількох основних компонентів: агент для захисту кінцевих точок та збору подій, поведінковий аналіз, оркестрація та автоматизація, звітність та візуалізація. Деякі модулі є опціональні та потребують додаткового ліцензування від вендора. Туди входять: контроль та захист атак зовнішнього периметру компанії (Attack Surface Management) та розвідка, централізований збір знань про загрози (Threat Intelligence). По суті, така архітектура об’єднує декілька програмних рішень в

одну консоль, що в результаті дає організації “SOC в одній коробці”, зменшує час та ресурси для налаштування та інтеграції різних рішень в мережі. Не менш важливим є те, що таке рішення розгортається виключно в хмарах, що економить час та ресурси організації на підтримку та оновлення продукту. Рішення в хмарі дає змогу реалізації повного бачення про інфраструктуру організації не тільки з середини але із з-зовні. Початок захисту внутрішнього периметру мережі варто розпочати із захистом кінцевих точок, туди можуть входити: персональні комп’ютери користувачів, віртуальні та фізичні сервери, мобільні пристрої. Для покриття захисту кінцевих точок за допомогою XSIAM, використовується досить популярне рішення Cortex XDR, розробленою компанією Palo Alto.

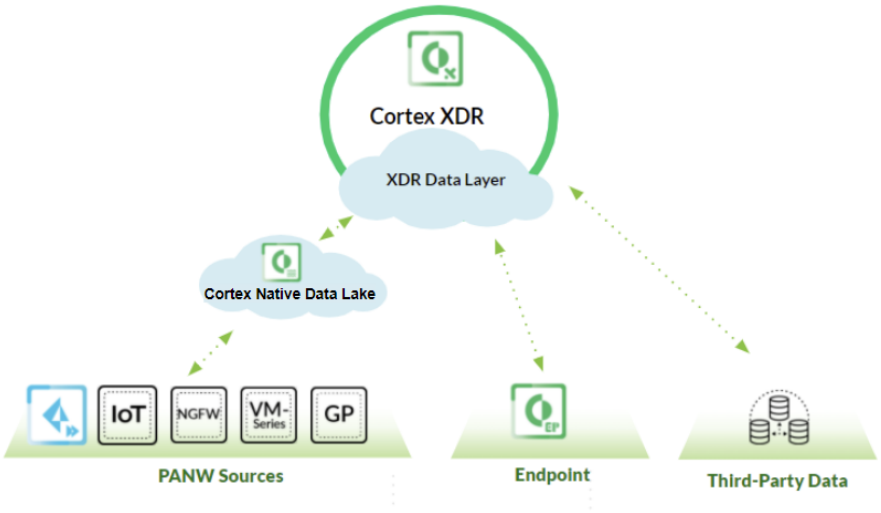


Рис. 2.2. Архітектура Cortex XDR

Cortex XDR забезпечує повну видимість інфраструктури на всіх рівнях у вигляді даних та подій в реальному часі. Додаток надає єдиний інтерфейс, за допомогою якого необхідно досліджувати та сортувати сповіщення, вживати заходів щодо виправлення та визначати політики для виявлення зловмисної діяльності в майбутньому. Наступним компонентом агенту є механізм аналітики. Механізм аналітики Cortex XDR — це служба безпеки, яка використовує мережеві дані для автоматичного виявлення загроз після вторгнення та звітування про них. Механізм аналітики робить це шляхом

виявлення належної (нормальної) поведінки у вашій мережі, щоб він міг помітити погану (аномальну) поведінку. Брандмауери нового покоління Palo Alto Networks — локальні або віртуальні брандмауери, які забезпечують дотримання політик безпеки мережі. У вас є змога налаштувати політику брандмауера для конкретної кінцевої точки в залежності від типу та критичності кінцевої точки. Зовнішні брандмауери та сповіщення — Cortex XDR може отримувати журнали трафіку від зовнішніх постачальників брандмауерів, наприклад Check Point, і використовувати механізм аналітики для аналізу цих журналів і попередження про аномальну поведінку. Щоб отримати додатковий контекст у інцидентах. Також агенти захищають кінцеві точки від відомих і невідомих шкідливих програм, зловмисної поведінки та методів. Для цього агент виконує власний аналіз локально на кінцевій точці, але також використовують дані про загрози WildFire.

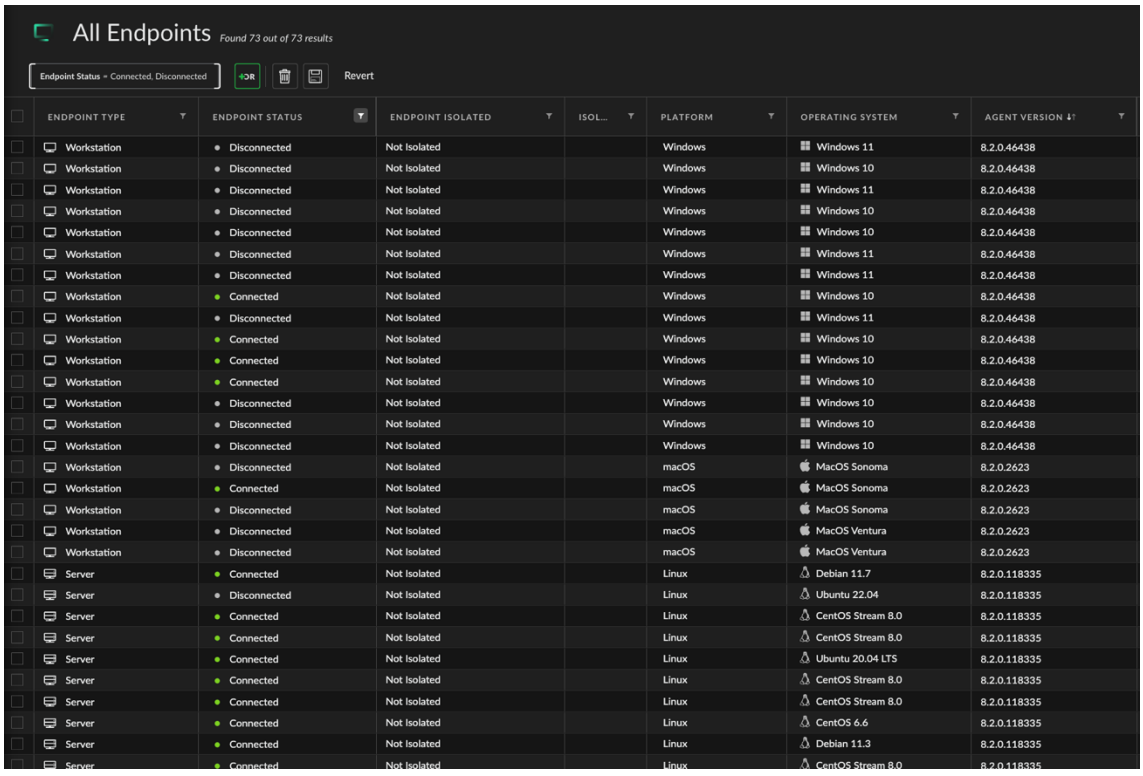


Рис. 2.3. Інвентаризація кінцевих точок в інтерфейсі Palo Alto XSIAM

Після встановлення агента на кінцевій точці, наступним важливим етапом є налаштування політик кінцевих точок. Політики безпеки розробляється

інженерами SOC та складаються з двох основних компонентів: політика конфігурації та політика попередження загроз кінцевих точок. Політика захисту включає в себе набір профілів, які в свою чергу визначають набір правил безпеки для захисту. Всього існує декілька профілів, які необхідно визначати для кожної операційної системи: шкідливе програмне забезпечення (malware), експлойт (exploit), налаштування агенту (agent settings), обмеження (restrictions) та виключення (exceptions).

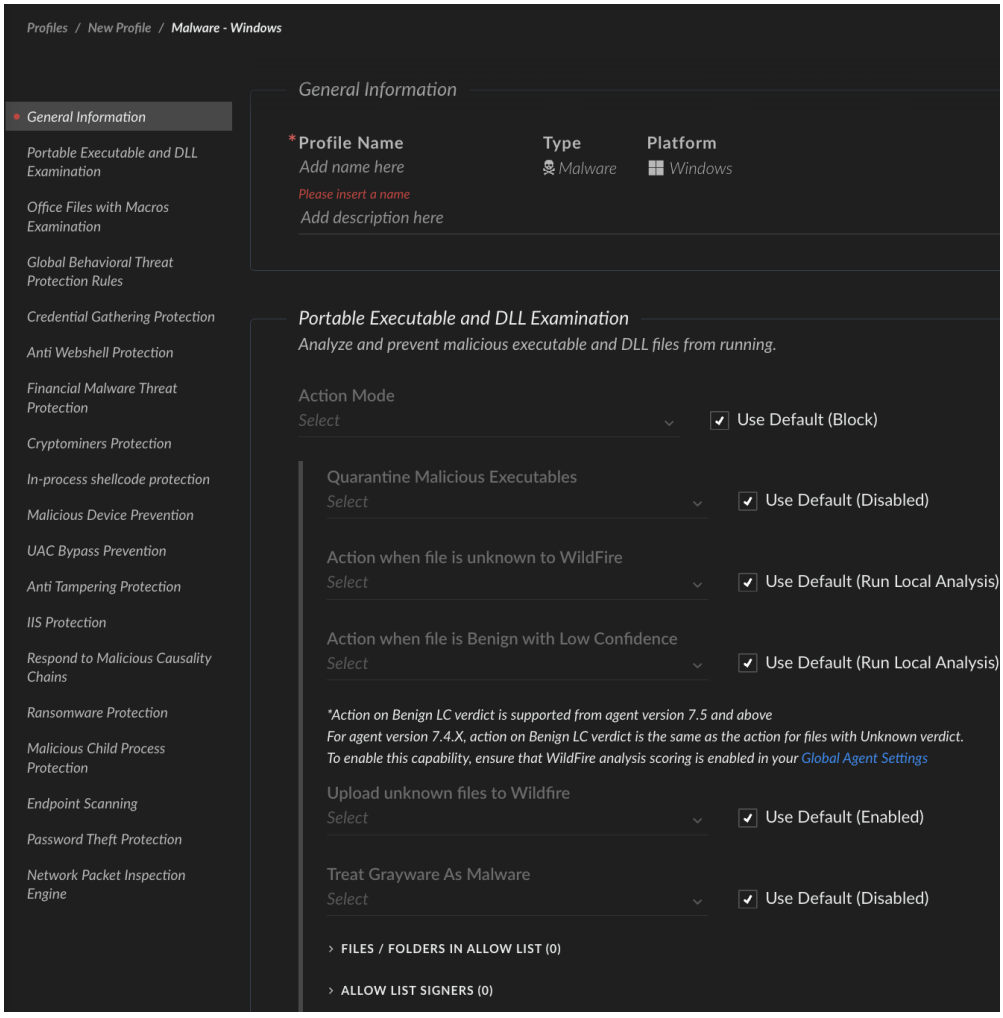


Рис. 2.4. Налаштування профілю захисту від шкідливого програмного забезпечення

Конфігурація профілю здійснюється, щоб досягнути двох основних цілей. Перше - безпека та ефективний захист кінцевих точок. Друге – забезпечення захисту без втручання в продуктивність системи та без загрози зупинення

робочих процесів. Найкращою практикою в такому випадку є розбиття пристроїв по групам, до прикладу сервери, комп'ютери користувачів, сервери розробки, обчислювальні сервери, мобільні пристрої, тощо. Кожна така група повинна містити правила ідентифікації за якими можна визначити, до якої пристрій відноситься. Сюди входить мережева адреса, ідентифікатор (hostname), тип операційної системи. До прикладу розглянемо конфігурацію профілю захисту від шкідливого програмного забезпечення. Профіль містить декілька основних компонентів. Перший, це є аналіз портативних виконуваних файлів та динамічних бібліотек Windows (DLL). Зловмисники можуть виконувати власний шкідливий код, замінюючи порядок пошуку бібліотек Windows. Системи на базі Windows використовують загальний метод для пошуку необхідних бібліотек DLL для завантаження в програму. Є багато способів, якими зловмисники можуть використати завантаження DLL. Найбільш типові є розміщення файлів бібліотеки динамічних посилань (DLL) троянів в каталозі, у якому здійснюватиметься пошук перед місцем розташуванням легітимної бібліотеки, запитуваної програмою, що змушує операційну систему завантажити шкідливу або модифіковану бібліотеку. Динамічні бібліотеки можна постійно генерувати та вшивати в легітимне програмне забезпечення, тому репутація такого файлу завжди буде «чистою». Другий компонент є захист від інфікованих файлів Office та макросів. Досвід під час російсько-української війни демонструє, що це є один з наймасовіший метод інфекції кінцевих точок державних установ чи критичної інфраструктури. Такі файли можуть бути поширені за допомогою фішингових листів та розповсюдженні за допомогою технік соціальної інженерії. Третій компонент використовує штучний інтелект та призначений для виявлення нетипової експлуатації операційної системи, на приклад під час Zero-Day атак. Його завдання є запобігання складним атакам, які використовують вбудовані виконувані файли операційної системи і звичайні утиліти адміністрування, постійно відстежуючи діяльність кінцевих точок на наявність зловмисних ланцюжків причин. До профілю також входять: захист кешу зберігання паролів ОС (LSASS), запобігання веб-шелів, виявлення програм-вимагачів, виявлення

криптомайнерів, захист процесів від модифікації, захист від обходу контролю облікових записів (UAC) та підняття привілеїв, інспекція та контроль трафіку. Також слід не забувати, що агент має здатність логувати поведінку користувача, його трафік, а також події на основі Active Directory, що в свою чергу надає повну обізнаність під час інциденту про користувача та кінцеву точку. Політика безпеки з профілями захисту може застосовуються на певну групу активів задля впевненості, що легітимні процеси чи компоненти не будуть виявлені як підозрілі чи зловмисні. Щоб попередити такі ризики, групи створюються для кожної з категорій пристроїв в мережі, наприклад сервери, ноутбуки, персональні пристрої, тощо. Наступний тип політики є конфігурація пристроїв, яку на даний момент підтримують дві операційні системи Windows та macOS.

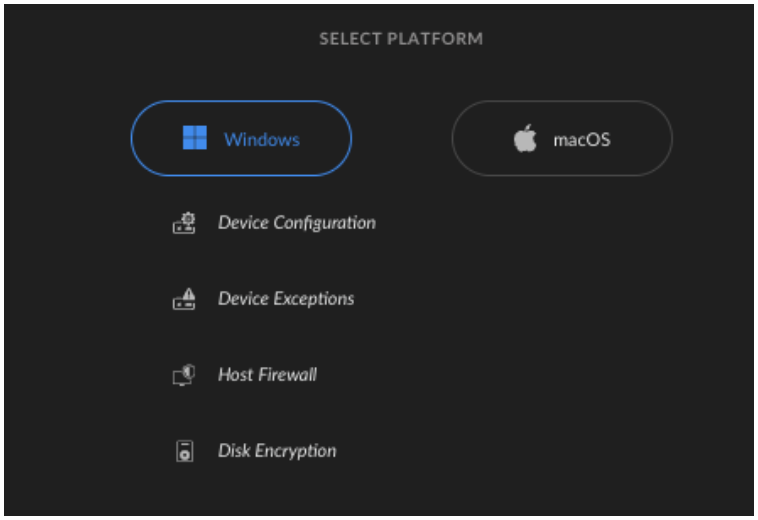


Рис. 2.5. Набір правил в політиці конфігурації

Слід не забувати, що конфігурація кожної системи є одним з ключових елементів безпеки. Виявлені недоліки конфігурації можуть бути використані для обходу систем захисту. У випадку з агентом Cortex, сюди входить: конфігурація пристрою, виключень, фаервол кінцевої точки та шифрування диску.

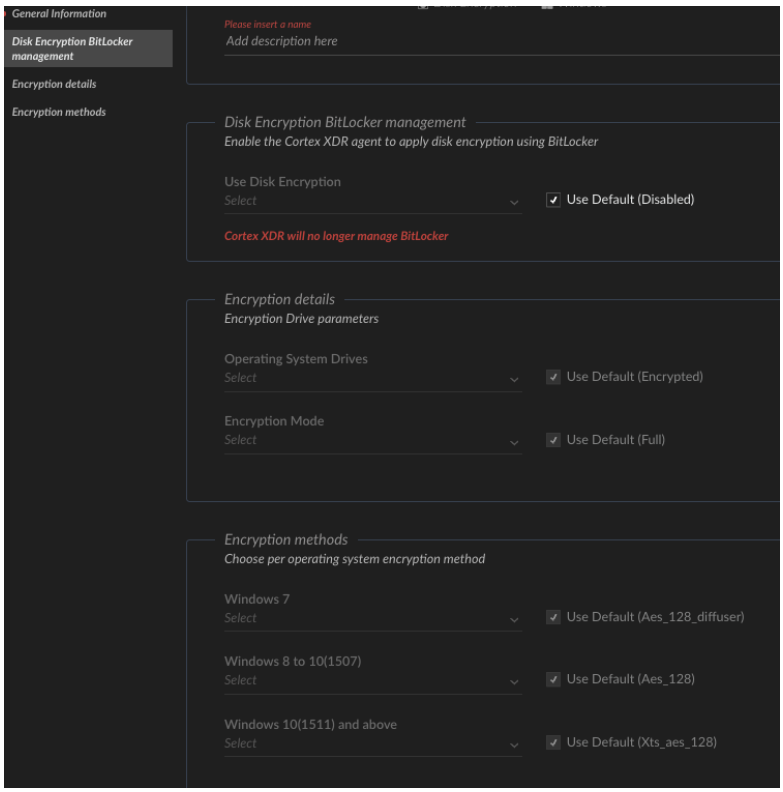


Рис. 2.6. Налаштування профілю шифрування диску кінцевої точки

Шифрування диску є важливим критерієм для організації задля забезпечення конфіденційності збереження даних у випадку втрати користувачем корпоративного пристрою. Агент здатен виявити відсутність шифрування диску та увімкнути його, якщо такий профіль буде застосований. Ще однією корисною функцією може бути блокування зовнішніх USB пристроїв чи дисків. Це мінімізує ризик інфекції шкідливим програмним забезпеченням кінцеву точку чи зловмисного апаратного забезпечення для відслідковування дій користувача.

Після застосування профілів та політик кінцевої точки, в команди SOC з’являється можливість централізовано збирати події про стан кінцевої точки, перелік активних користувачів на ній, встановлених додатків, активних процесів, тощо. На основі цих даних та активних інцидентів будується оцінка ризиків кінцевої точки.

Рис. 2.7. Оцінка ризиків кінцевої точки користувача

Враховуючи такі фактори як: департамент та групи користувача може визначатися критичність кінцевої точки. Якщо користувач відноситься до фінансового департаменту, у разі виявлення інциденту на такій кінцевій точці, ризик значно буде збільшено не тільки для користувача, але і для всієї групи. Таку аналітику команда SOC може використовувати задля вдосконалення профілів чи політик безпеки.

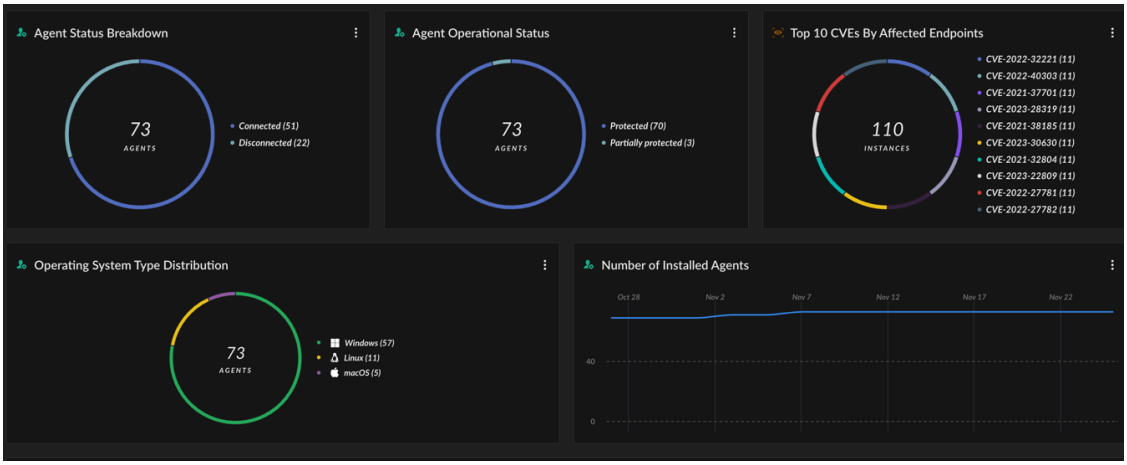


Рис. 2.8. Аналітична панель контролю кінцевих точок

В інструменті XSIAM та використовуючи пошук XQL, аналітики команди безпеки можуть реалізовувати власні панелі безпеки. Такі аналітичні дашборди можуть оновлюватися в режимі реального часу та економити час аналізу шкідливих або потенційно шкідливих (аномальних) подій в мережі. Щоб

успішно виконати таке завдання організації необхідно реалізувати централізований збір подій безпеки до єдиної консолі. У функціоналі XSIAM для цього є не тільки агенти, але і сервер збору подій Broker Virtual Machine.

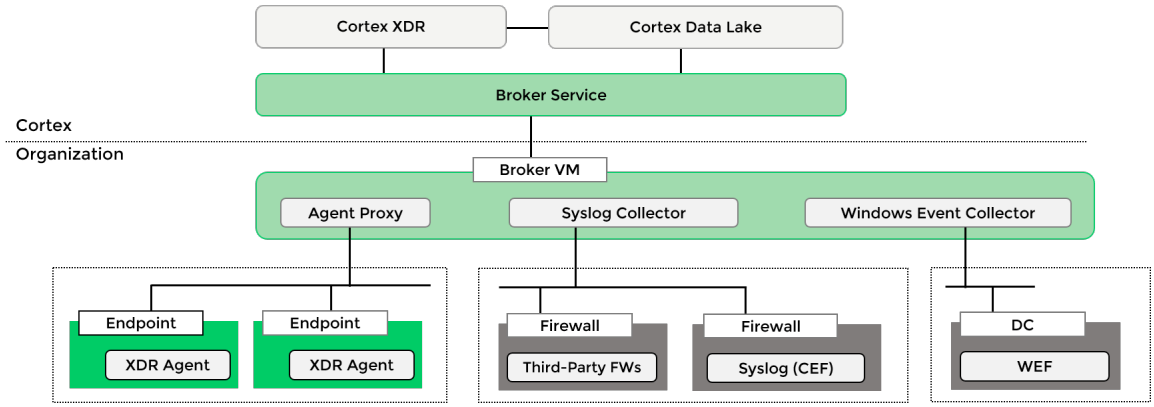


Рис. 2.9. Схема роботи Broker Service

Як і в типовому SIEM його завдання є централізований збір та передача подій до консолі. До прикладу, з фаерволів мережі достатньо виконати конфігурації syslog та передавати дані в зручному для вас форматі, до прикладу LEEF чи CEF, а вже на стороні панелі XSIAM за допомогою інструментів агрегації та кореляції відформатувати дані, щоб сама система їх розуміла та застосовувала в правилах виявлення. В разі інтеграції хмарного середовища, достатньо використовувати прямі інтеграції з консолею за допомогою API без будь-яких рішень посередині між ними. Використовуючи ці дані, можна реалізувати такі кейси як контроль про надходження подій до системи, виявлення аномалій в автентифікації на системах, виявлення сенситивних даних у відкритому вигляді на пристрої, підозрілий трафік мережі та нетипові DNS запити.

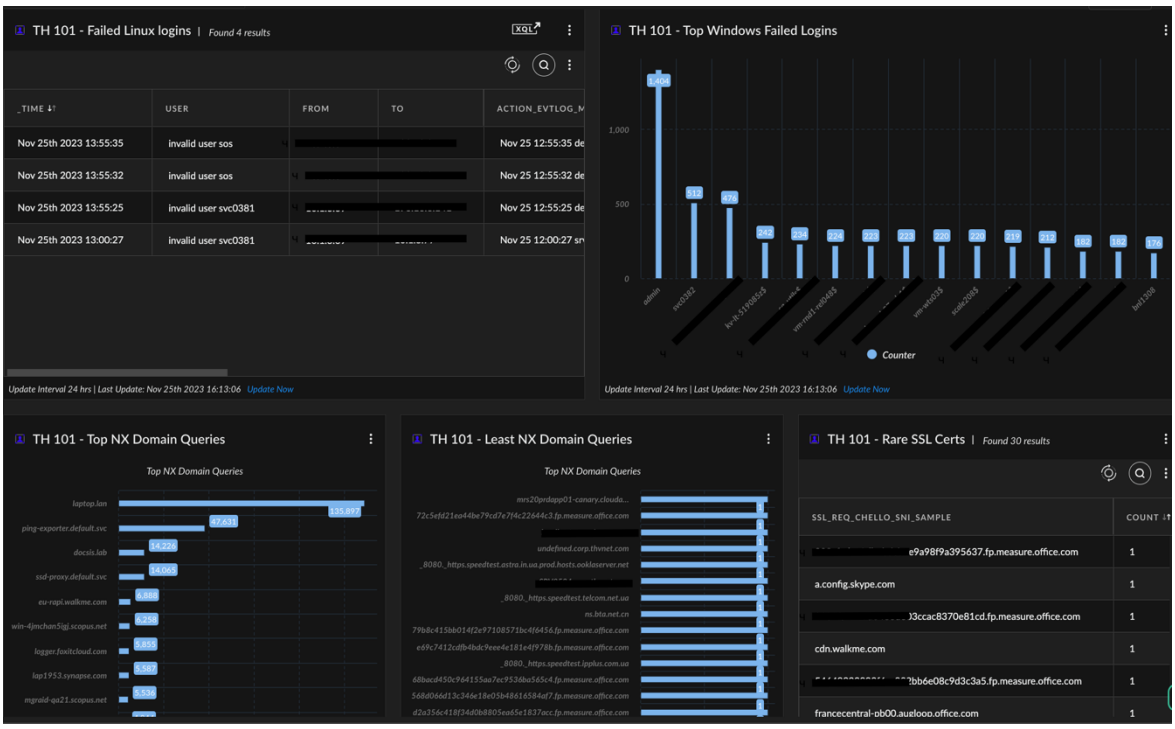


Рис. 2.10. Приклад реалізації аналітичної панелі з інформацією про невдалі автентифікації з систем та підозрілого трафіку

Наступним кроком під час інтеграції джерел даних є хмарні середовища та платформи з відкритими API. Одна з переваг XSIAM величезна кількість підтримуваних платформ, що дає безлімітні можливості для інженерів команд безпеки, а якщо певна система офіційно не підтримується, продукт пропонує варіанти інтеграції та написання власних інтеграцій власноруч. Найкращі аналітики безпеки, незалежно від їхніх технологій і навичок, просто не можуть переглянути нескінченний потік даних рядка за рядком, щоб виявити зловмисну діяльність. Застосовуючи Broker та XSIAM, система збирає й упорядковує всі дані, що надходять із різних джерел у вашій мережі, і пропонує вашій команді SOC статистичні дані, щоб вони могли швидко виконувати важливі дії, наприклад: виявляти внутрішні та зовнішні атаки, реагувати на них, спрощення керування загрозами, отримання видимості у всій організації та розвідку безпеки, централізація завдання SOC з моніторингу, реагування на інциденти, керування журналами, звітування про відповідність і забезпечення виконання політики. За лічені секунди, система може проаналізувати величезні пакети даних безпеки, що надходять із тисяч джерел, щоб виявити незвичну поведінку

та зловмисну активність і автоматично зупинити їх. Щоб використовувати такий масив даних ефективно, оператори та інженери повинні вивчити XQL (Cortex Query Language). Мова запитів Cortex (XQL) дозволяє запитувати інформацію, що міститься в широкому спектрі джерел даних у Cortex XDR, для ретельного аналізу кінцевих точок і мережевих подій. Для виконання запитів потрібен набір даних або джерело даних. Якщо не вказано інше, запит виконується з набором даних xdr_data, який містить усю необроблену інформацію журналу, яку збирає Cortex XDR. XQL подібний до інших мов запитів і використовує деякі з тих самих функцій, які можна знайти в багатьох реалізаціях SQL, але це не SQL. XQL формує запити поетапно. Кожен етап виконує певну операцію запиту та відокремлюється вертикальною рискою. Щоб допомогти аналітику створити ефективний запит XQL із належним синтаксисом, поле запиту в інтерфейсі користувача надає пропозиції та визначення під час введення. Це універсальний інструмент для управління даними системи, створення аналітичних панелей та звітностей.

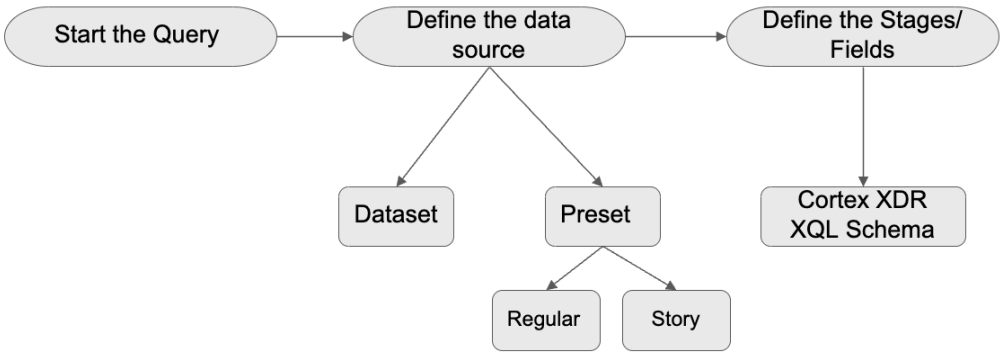


Рис. 2.11. Схема роботи XQL

Досвідчені аналітики використовують пошук не тільки для аналізу подій але для виявлення поводів (lead). У контексті системи, lead – це частина контексту подій інформаційних систем, до першого контакту з потенційною загрозою, яку можна отримати з декількох джерел. Якщо типові сповіщення (alerts) сигналізують про потенційний інцидент, контекст, що веде до цієї події необхідно виявити самотужки. Якщо в аналітика є критерії та контексти, які

визначають про потенційну небезпеку, повід можна перетворити в сповіщення. На практиці можна розглянути наступний приклад. Оператору SOC, необхідно виявити активність в мережі, яка могла б відноситися до певної тактики, техніки чи процедурі (TTPs) згідно фреймворку MITRE. Підхід, який може використати аналітик, може включати: полювання на загрози виконується самостійно, окремо одне від одного за типом кейсу, розпочати варто з побудови гіпотези, що свідчить про активність зловмисного актора в мережі, створення XQL запиту до визначеної гіпотези, перевірка результату, наступних кроків по усуненню та побудова сповіщення на основі правила виявлення та запобіганню загроз. Приклад гіпотези, системний адміністратор чи привілейованих користувач, отримує доступ до критичних систем використовуючи текстовий файл у відкритому вигляді, через емулятор терміналу Putty чи Windows CMD. Ціль пошуку виявити зберігання паролів до привілейованих облікових записів у відкритому вигляді.

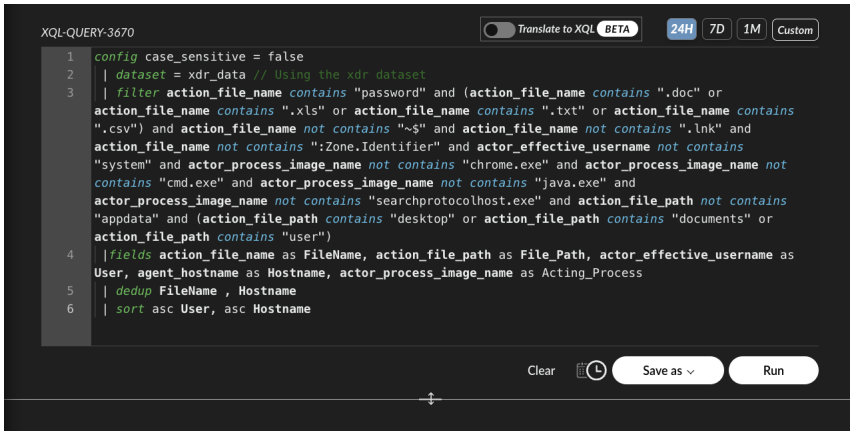


Рис. 2.12. Реалізація XQL запиту для виявлення паролів у відкритому вигляді

У вікні результату, аналітик має змогу перевірити знайдені артефакти, створити на основі пошуку правило виявлення із сповіщенням, перетворити запит у аналітичну панель з регулярним оновленням або створення звіту.

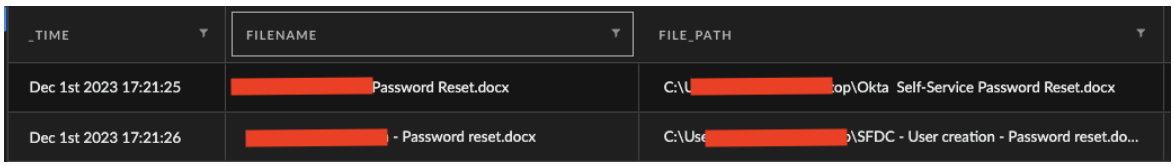


Рис. 2.13. Приклад виявлення файлу з паролями на кінцевій точці користувача

2.2.1 Реагування на інциденти та їх автоматизація

Відкрите сповіщення або набір відкритих алертів можуть свідчити про інцидент інформаційної безпеки, на який SOC має відреагувати, враховуючи власні процедури та інструкції. В типових SOC, це набір правил з якими кожен оператор повинен ознайомитися перед початком зміни. Перевага XSIAM є реалізація автоматизацій, і мається на увазі не лише прискорення взаємодії між продуктами безпеки, наприклад автоматичне ізолювання кінцевої точки, але і повна автоматизація кроків, процедур та процесів аналітиків. XSIAM може рекомендувати нові інструкції або відповідні дії на основі машинного навчання, тим самим роблячи автоматизацію робочого процесу більш потужною.

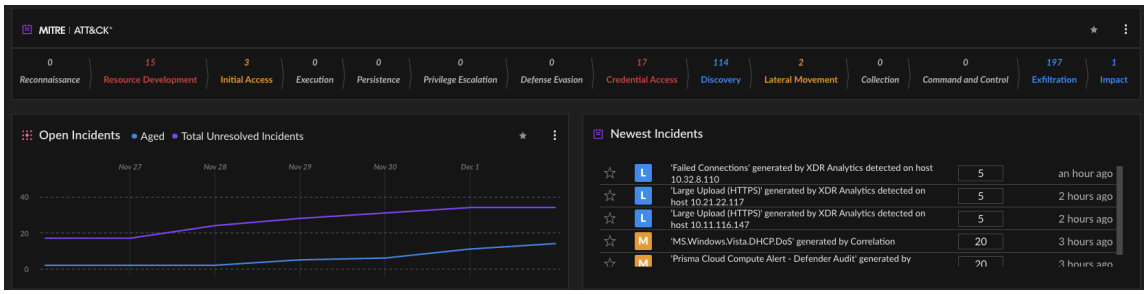


Рис. 2.2.1. Приклад аналітичної панелі з відкритими інцидентами

В продукті XSIAM інтегрований модуль XSOAR, який вже зарекомендував себе на ринку, як один з найпотужніших інструментів автоматизації та оркестрацій подій інформаційної безпеки у світі. Весь вміст Cortex XSOAR організовано в пакетах. Пакети — це набір готових інструментів для інженерів безпеки для інтеграції продуктів різних вендорів до єдиної екосистеми. Пакети вмісту створюються не тільки Palo Alto Networks, але і технологічними

партнерами, консалтинговими компаніями, MSSP чи клієнтами, що прискорює інтеграцію будь-якого продукту в саму систему, створюючи величезну бібліотеку готовий автоматизацій для нового клієнта. Пакети вмісту можуть містити різноманітні компоненти, такі як інтеграції, автоматизація, плейбуки, типи інцидентів, віджети тощо.

Cortex XSOAR — це система оркестровки та автоматизації, яка використовується для об'єднання всіх різних типів джерел даних для єдиного бачення і побудови реагування на інциденти. Одним з основним ворогом команди моніторингу є хибні або дублюючі спрацювання. Саме тому у більшості випадків головною автоматизацією є виявлення хибних або легітимних спрацювань в системі, а також об'єднання інцидентів за спільними критеріями до одного. Це дає змогу аналітикам зосередитися на невеликій кількості інцидентів, які потребують подальшого реагування

Розглянемо практичну реалізацію інструкції (плейбуку) для реагування на інцидент. Згенеровано інцидент щодо масованої невдалої автентифікації з хосту до різних кінцевих точок всередині мережі. Команда SOC може реалізувати одразу декілька автоматизацій, наприклад: збагачення інформації про IP адресу, збагачення інформації про користувача, автоматичне ізолювання пристрою з мережі, автоматичне блокування IP адреси чи автоматичне блокування користувача.

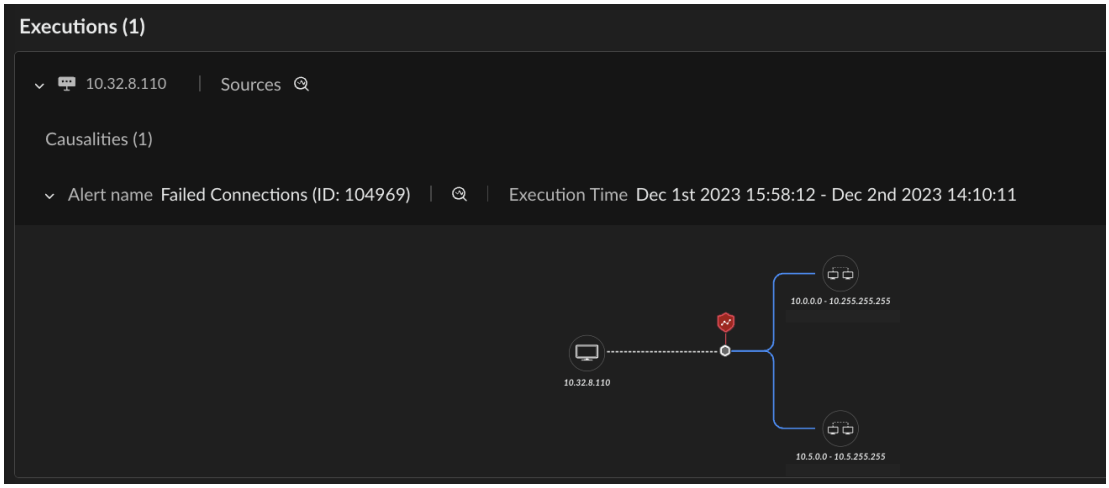


Рис. 2.2.2. Візуалізація інциденту

Для інциденту край важливо збагачення інформації з різних джерел, і правильне налаштування його плейбуків. Це дає аналітику за лічені секунди отримати інформацію, на пошук якої без інструменту автоматизації піде десятки хвилин.

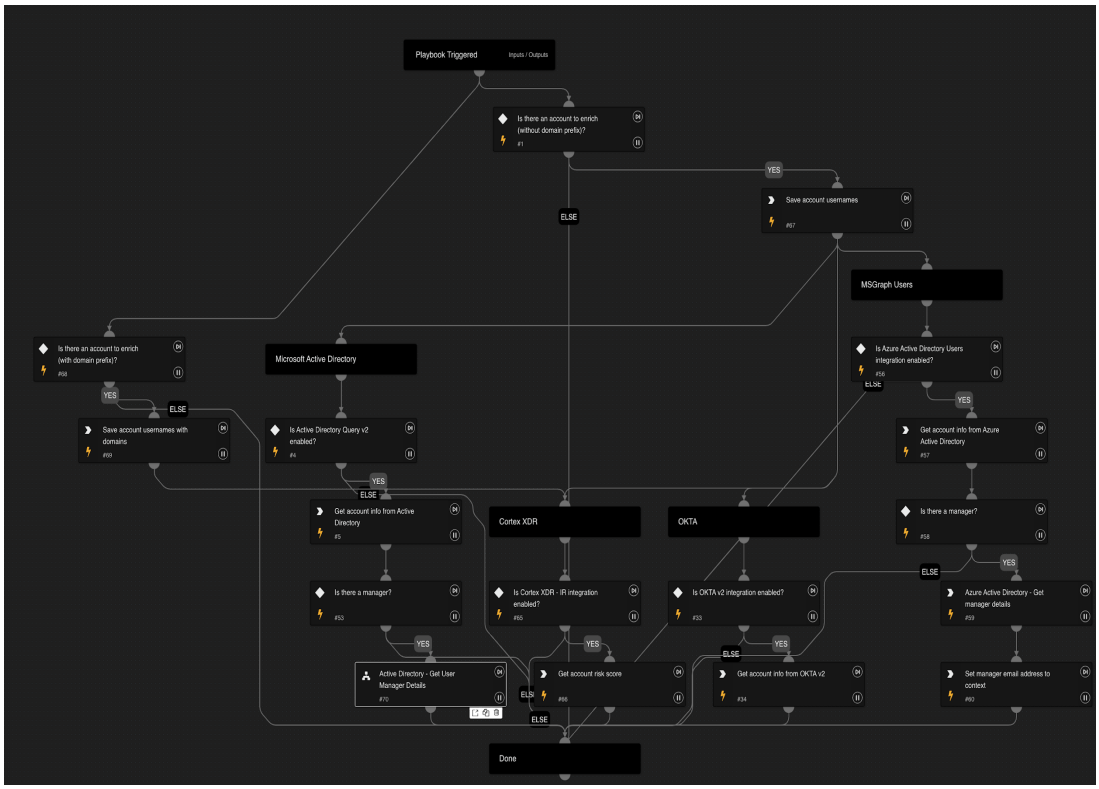


Рис. 2.2.3. Схема плейбуку для автоматизації збагачення інформації про користувача

В розробленому прикладі бере участь одразу декілька інформаційних систем: Microsoft Active Directory, Microsoft Azure, Okta та Cortex XDR. Розпочинається виконання з кроку один, це виявлення облікового запису в контексті інциденту. Для деяких систем, префікс з назвою домену організації може заважати для ідентифікації. Тому, розроблено два кроки: перший – обліковий запис з префіксом домену, другий – префікс відсутній. Під час виконання першого кроку, автоматизація запитує Azure AD та Microsoft AD чи є такий обліковий запис в системі, його контактні дані, контакти менеджера та департамент. Також, даний крок отримує повну назву облікового запису, та

створює крок три – звернення до Okta із запитом про активність облікового запису, статусом мультифакторної автентифікації користувача. Це допоможе зрозуміти, чи не було використано деактивований обліковий запис. Під час виконання другого кроку, Cortex перевіряє наявність облікового запису та відповідної кінцевої точки з неї, передаючи цю інформацію аналітику з оцінкою ризику. В інженера безпеки є інструмент для тестування сценаріїв та скриптів, тому розглянемо тестування ідентифікації користувача через Active Directory.

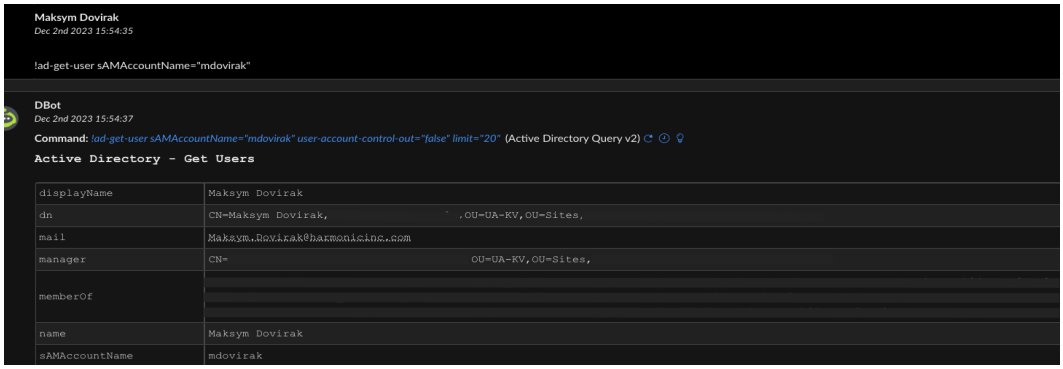


Рис. 2.2.4. Приклад перевірки ідентифікації користувача mdovirak

В комплексі інструмент дає можливість економити час та ресурси команди реагування на кіберінциденти та розробку більш складніших сценаріїв реагування. На прикладі це можна побачити під час автоматичного виявлення підозрілої активності в мережі організації.

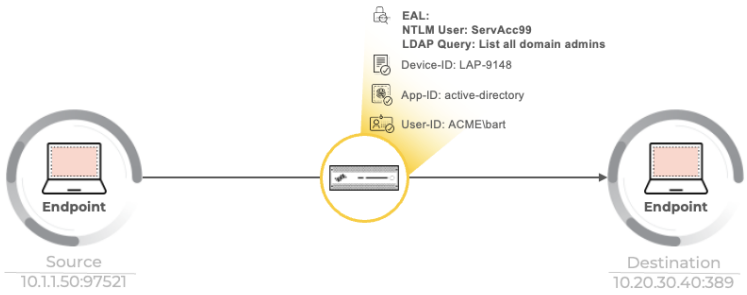


Рис. 2.2.5. Схема взаємодії між хостами в мережі організації

Під час виявлення події, система розпочинає ідентифікацію ініціатора, протокол за яким ця взаємодія відбулась, назва мережі, назва пристрою,

обліковий запис. Це може відбуватися не тільки з подій від мережевих пристроїв, але і на пряму з Cortex XDR, так як агенти мають можливість відслідковувати трафік користувача в режимі реального часу.

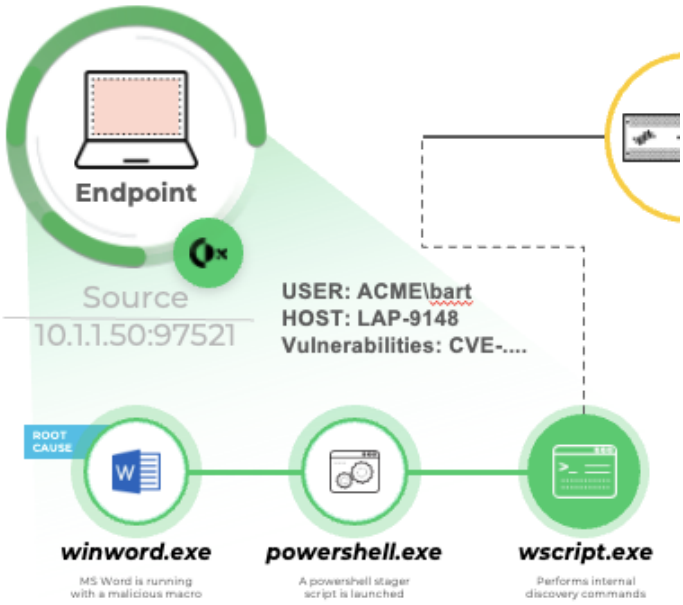


Рис. 2.2.6. Схема ідентифікації зловмисних процесів

Після успішної ідентифікації трафіку та інформації про взаємодію між хостами в мережі, агент надає повну інформацію про хронологію підозрілої активності для оператора SOC. До прикладу, ініціація підозрілого запиту було здійснено через wscript.exe, який в свою чергу був ініційований через powershell.exe згенерований процесом winword.exe. Подібна подія говорить, що хост був скомпрометований вразливим макросом в документі Word, який до прикладу міг бути відправлений електронним листом або скопійований з менш захищених носіїв інформації.

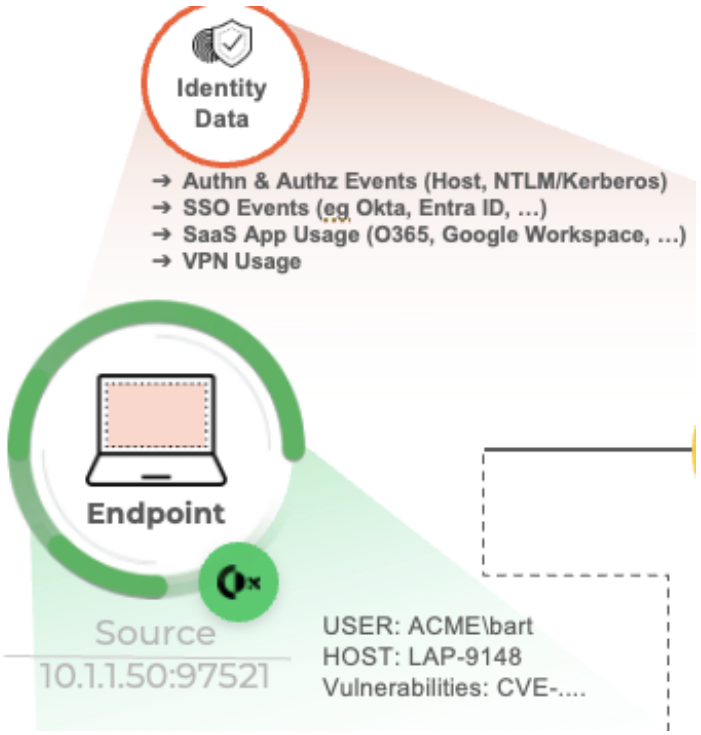


Рис. 2.2.7. Схема ідентифікації власника системи

В систему XSIAM інтегровані системи обліку користувачів та доступу, тому автоматизація автоматично намагається визначити та надати оператору інформацію більше деталей про користувача, його роль та якими сервісами він користується. Така обізнаність є критичною під час ідентифікації інциденту.

Як результатом комплексної автоматизації спрацьовує одразу декілька модулів захисту. Перший - це виявлення аномальної активності (behavioral threat prevention), а саме ініціація скрипта через файл Word.Exe, що вважається, як не типовим. Другим – це запобігання загрозі (threat prevention) на основі аналізу трафіку з мережі. Мережевий запит, який був ініційований зловмисним файлом успішно заблоковано в середині мережі організації, а отримувач залишився в безпеці. Третій модуль який спрацює є поведінкові індикатори компрометації (BIOC), які додають більше контексту про подію під час атаки. До прикладу, який зміст містив підозрілий макрос під час ініціації. Це дає можливість аналітикам проаналізувати кроки атакуючого, його техніки та інструменти. Таких спрацювань може буде декілька, або ж атакуючий може спробувати інші спроби компрометації кінцевої точки на різних хостах. Використовуючи

автоматизацію, всі вони будуть об’єднані до одного інциденту та розглянуті, як єдиний цілісний інцидент, приорітетність якого буде збільшена використовуючи механізми машинного навчання.

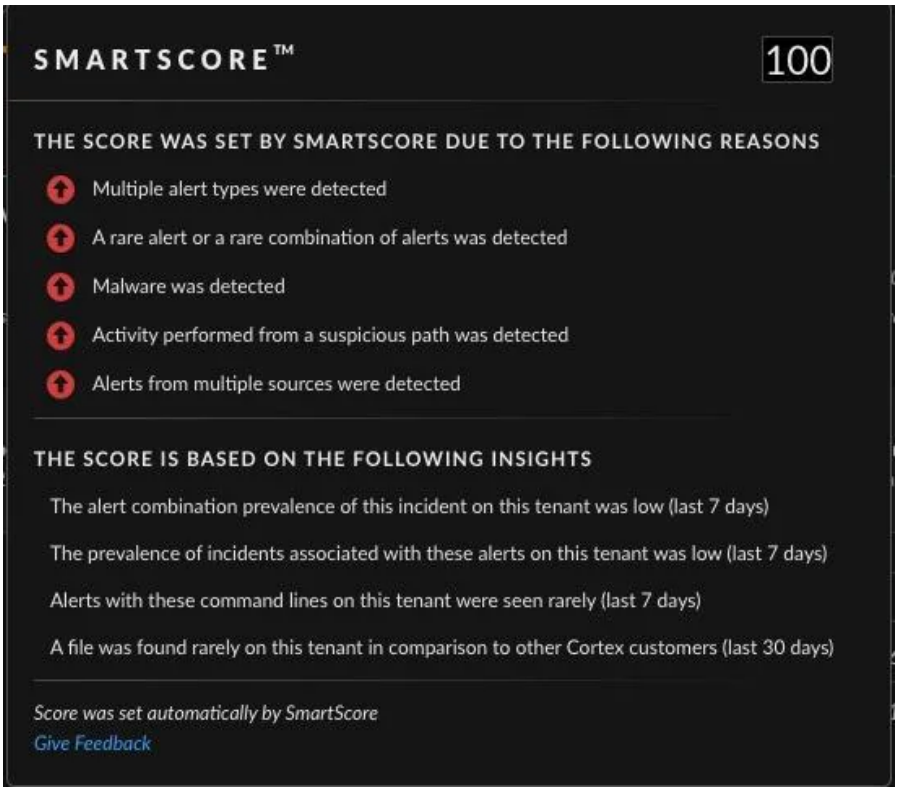


Рис. 2.2.7. Приорітизація інциденту із використанням машинного навчання

2.3 Практична реалізація захисту зовнішнього периметру за допомогою Palo Alto XPANSE

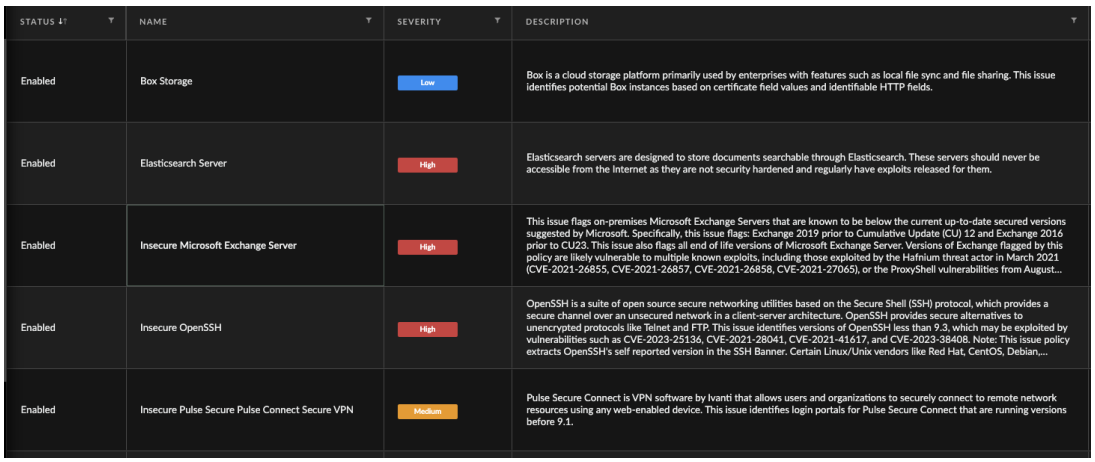
Периметр мережі — це захищений кордон між приватною та локально керованою стороною мережі, часто внутрішньою мережею компанії, та загальнодоступною стороною мережі. Розглянемо типові компоненти внутрішнього периметру мережі. Маршрутизатори служать дорожніми знаками мереж. Вони спрямовують трафік у мережу та в ній. Граничний маршрутизатор — це останній маршрутизатор під контролем організації перед тим, як трафік з’явиться в ненадійній мережі, наприклад Інтернеті. Фаервол – це пристрій, який

має набір правил, які визначають, який трафік він дозволяє або забороняє проходити через нього. Фаервол зазвичай починає роботу там, де зупиняється прикордонний маршрутизатор, і набагато ретельніше фільтрує трафік. Система виявлення вторгнень також є важливим компонентом та інтегрована в фаервол. По суті, її функція створення тривог для вашої мережі, яка використовується для виявлення підозрілої активності та сповіщення про неї. Цю систему можна створити з одного пристрою або набору датчиків, розміщених у стратегічних точках мережі. Важливим компонентом також є демілітаризовані зони та екрановані підмережі DMZ. Екранована підмережа відносяться до невеликих мереж, що містять загальнодоступні служби, підключені безпосередньо до брандмауера або іншого пристрою фільтрації та пропонують захист за допомогою брандмауера. В свою чергу, може здаватися, що зовнішній периметр захистити просто і достатньо використати типовий брандмауером чи фаерволом для веб-додатків, але це не так. В організації з великою кількістю публічних ресурсів хмарних середовищ як Amazon, Azure, Oracle OCI, питання контролю “що саме доступно до мережі” та хто за це відповідний стає гостріше. Зазвичай команда SOC не може знати точну інформацію про активи в хмарних середовищах чи дата-центрах, так як їх використання, до прикладу може бути тимчасове. Тут і створюється багато різних ризиків, такі як розгортання віртуальної машини для тестування, яка не була добре захищена, та про яку забули розробники. В той час, вона може мати доступ до внутрішній ресурсів, а атакуючий може експлуатувати відкриті вразливості для отримання доступу до неї. В такому випадку, команда реагування буде необізнана про потенційну шкідливу активність, потенційно відкриті вразливості та проаналізувати ризики, які є всередині мережі через такі доступи.

Частину цієї проблеми може вирішити Attack Surface Management (ASM) – керування поверхневими атаками або управління поверхнею атак. Такі типи продуктів почали активно розвиватися разом із впровадженням хмарних технологій. Інструмент дає можливість команді SOC централізувати видимість щодо всіх цифрових активів у відкритому периметрі мережі, та оцінити

потенційні атаки, які неавторизований користувач або зловмисник може експлуатувати. Ключові цілі управління поверхнею атак є виявлення вразливостей і такий продукт допомагає організації зменшити потенційний вплив в їх IT-інфраструктурі, програмах, мережах та інших цифрових активах постійно відслідковуючи та скануючи хости. Зменшення ризику, розуміння поверхні атаки та активне керування нею дозволяє організаціям зменшити загальний ризик кібератак. Усуваючи вразливості та обмежуючи точки впливу, служби безпеки можуть мінімізувати ймовірність успішних кібератак. Багато галузей промисловості та організацій підпадають під дію нормативних стандартів відповідності, які вимагають від них підтримувати певний рівень безпеки. Attack Surface Management допомагає досягти та підтримувати відповідність, гарантуючи наявність заходів безпеки для захисту конфіденційних даних, тобто дає розуміння в реальному часі на відповідність до аудиту кібербезпеки. У разі інциденту безпеки, продукт ASM дає краще розуміння поверхні атаки та дозволяє швидше та ефективніше реагувати на інциденти для команди SOC. Команди безпеки можуть реагувати швидше й точніше, коли мають чітке уявлення про цифровий ландшафт своєї організації. ASM також сприяє кращому управлінню цифровими активами, забезпечуючи регулярне сканування зовнішнього периметру організації. Керування поверхнею атаки не є одноразовою діяльністю і передбачає регулярний моніторинг та реагування. Цей проактивний підхід допомагає організаціям випереджати нові загрози та відповідним чином адаптувати свої заходи безпеки.

Одним із опціональним модулем в XSIAM є Attack Surface Management XPANSE розроблений компанією Palo Alto, що дає можливість сканування зовнішній периметр компанії, ідентифікувати активи в режимі реального часу та давати аналітикам безпеки повну картину про організацію. Після початку сканування, в консолі управління аналітик має змогу активувати правила виявлення і розпочати проактивний моніторинг своїх публічно доступних ресурсів.



STATUS	NAME	SEVERITY	DESCRIPTION
Enabled	Box Storage	Low	Box is a cloud storage platform primarily used by enterprises with features such as local file sync and file sharing. This issue identifies potential Box instances based on certificate field values and identifiable HTTP fields.
Enabled	Elasticsearch Server	High	Elasticsearch servers are designed to store documents searchable through Elasticsearch. These servers should never be accessible from the Internet as they are not security hardened and regularly have exploits released for them.
Enabled	Insecure Microsoft Exchange Server	High	This issue flags on-premises Microsoft Exchange Servers that are known to be below the current up-to-date secured versions suggested by Microsoft. Specifically, this issue flags: Exchange 2019 prior to Cumulative Update (CU) 12 and Exchange 2016 prior to CU23. This issue also flags all end of life versions of Microsoft Exchange Server. Versions of Exchange flagged by this policy are likely vulnerable to multiple known exploits, including those exploited by the Hafnium threat actor in March 2021 (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), or the ProxyShell vulnerabilities from August...
Enabled	Insecure OpenSSH	High	OpenSSH is a suite of open source secure networking utilities based on the Secure Shell (SSH) protocol, which provides a secure channel over an unsecured network in a client-server architecture. OpenSSH provides secure alternatives to unencrypted protocols like Telnet and FTP. This issue identifies versions of OpenSSH less than 9.3, which may be exploited by vulnerabilities such as CVE-2023-25136, CVE-2021-28041, CVE-2021-41617, and CVE-2023-38408. Note: This issue policy extracts OpenSSH's self reported version in the SSH Banner. Certain Linux/Unix vendors like Red Hat, CentOS, Debian,...
Enabled	Insecure Pulse Secure Pulse Connect Secure VPN	Medium	Pulse Secure Connect is VPN software by Ivanti that allows users and organizations to securely connect to remote network resources using any web-enabled device. This issue identifies login portals for Pulse Secure Connect that are running versions before 9.1.

Рис. 2.3.1. Управління правилами атак та виявлення вразливостей зовнішнього периметру

Cortex Xpanse сканує ваші відомі та невідомі активи для виявлення веб-сайтів, які належать вашій організації. Потім Web ASM переглядає ці окремі веб-сторінки для виявлення та класифікації різних веб-технологій, використовуваних для побудови конкретного веб-активу. Як тільки цей постійно оновлюваний веб-інвентар створений для вашої організації, Web ASM виконує аналіз найкращих практик з безпеки для виявлення неправильних конфігурацій та потенційних вразливостей. Потім Web ASM збагачує інциденти додатковим бізнес-контекстом, щоб допомогти вашим командам з безпеки вирішувати проблеми швидше та в масштабі.

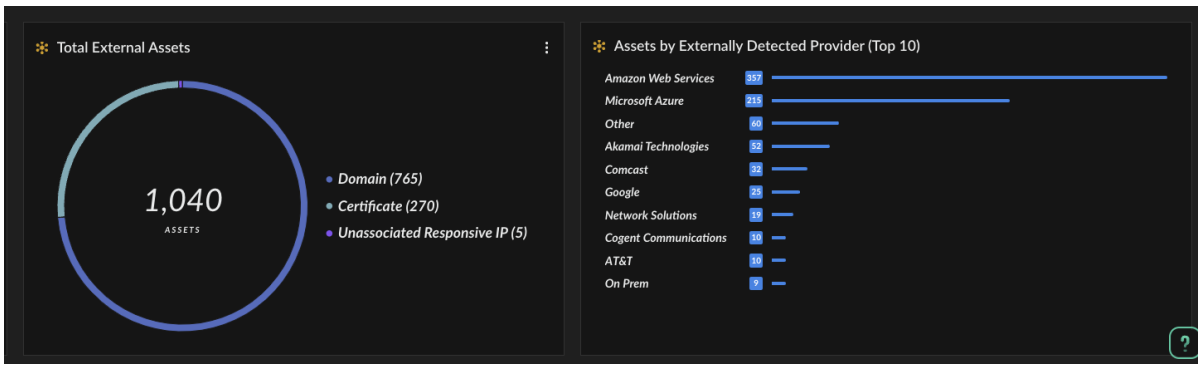


Рис. 2.3.2. Візуалізація публічного периметру організації

Система вміє сама ідентифікувати активи організації на основі домену та мереж, які були налаштовані в конфігурації XSIAM, що значно економить

ресурси команди. Для деяких організацій, одразу окремий департамент, може займатися виключно реалізацією цього напряму, в той час як XPANSE автоматизує цей процес для SOC команди.

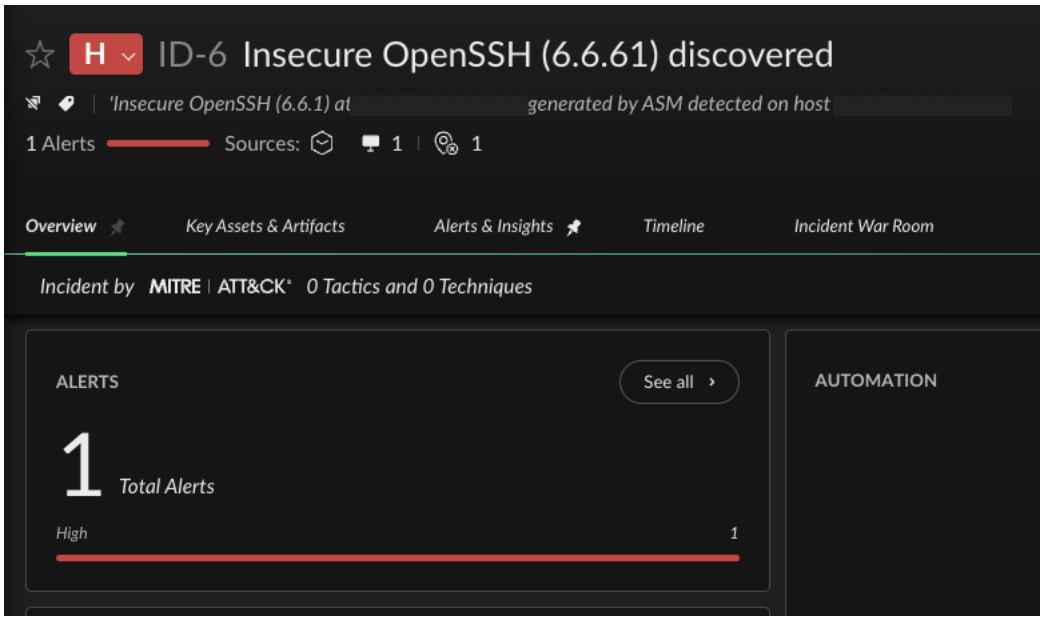


Рис. 2.3.3. Приклад виявлення вразливого SSH

Xpanse допомагає командам корпоративної безпеки зменшити їхню поверхню атак, виявляючи ризики та викритості їхньої глобальної інтернет-поверхні атак. Дані Xpanse про активи, викритості та поведінку можуть бути інтегровані у існуючі інструменти управління інформаційною безпекою (SIEM) та засоби управління вразливостями, щоб забезпечити можливість виявлення нових викритостей, змін конфігурацій та ризикованих чи виходящих за рамки політики комунікацій для подальшого попередження та виправлення.

Висновки до другого розділу

В другому розділі було проведено практичну роботу із побудови сучасної архітектури SOC на основі програмного рішення Palo Alto XSIAM, яке часто називають системою збору та аналізу подій інформаційної безпеки (SIEM) нової генерації. Занадто багато SOC команд застрягли з 20-річною моделлю, де SIEM

та її правила є серцем і ключем всіх операцій та безпеки команди. Cortex XSIAM - (Extended Security Intelligence and Automation Management) - об’єднує найкращі в своєму класі функції, включаючи кінцеву точку виявлення та реагування (EDR), розширене виявлення та відповідь (XDR), оркестровка безпеки, автоматизація та реагування (SOAR), управління зовнішнім периметром та атак на неї (ASM), аналіз поведінка користувача та суб'єкта (UEBA), платформа аналізу загроз (TIP), і безпеки управління інформацією та подіями (SIEM). На ринку все більше і популярніші рішення “SOC-In-A-Box”. В сучасному ланшафті загроз організації, які стурбовані лише припиненням відомих типів атак, матимуть величезні прогалини у своїй безпеці використовуючи типові SIEM рішення. Це тому, що всі SIEM, так чи інакше, залежать від написання правил для набору даних, щоб спробувати ідентифікувати шаблони чи патерни загроз. Основною перевагою рішення є вбудовані правила детекцій різного типу інцидентів з врахуванням матриці MITRE, які регулярно оновлюються командою реагування на інциденти Palo Alto UNIT42. Оперуючи величезну кількість подій клієнтів та власної інфраструктури, їх команди має змогу побудувати унікальні виявлення, як на типові атаки, так і на атаки типу “нульового дня”. Було продемонстровано конфігурацію профілів безпеки кінцевих точок та продемонстровано, що інструмент підтримує не тільки про безпеку робочих станцій користувачів, але і про смартфони. За допомогою власної мови запитів XQL, продемонстровані аналітичні панелі, які можуть використовувати команди SOC для пришвидшення власних операцій, побудови аналітичних звітів чи власних правил виявлення. Продемонстровано переваги Palo Alto XSOAR – система оркестраціїї та автоматизації інцидентів кібербезпеки. На практиці, розглянуто автоматизацію розширення контексту під час інциденту за допомогою даних з Azure, IDP Okta та Active Directory, що без цієї автоматизації забирає в оператора команди безпеки значно велику кількість часу. В додаток до цього, розглянуто детальний аналіз автоматичного аналізу підозрілої мережевої активності між хостами в локальній мережі та яким чином XSIAM агрегує ці дані між собою.

РОЗДІЛ 3
ПОБУДОВА СУЧАСНОЇ АРХІТЕКТУРИ SOC

3.1 Тенденції подальшого розвитку архітектур SOC

Легко припустити, що пандемія COVID-19 найбільше вплинула на центр безпеки будь-якої компанії і традиційні підходи до кібербезпеки. Проте деякі тенденції SOC уже сформували майбутнє, і я пандемія прискорила ці процеси. Слід чесно сказати, що COVID-19 сильно вплинув на те, що ми вважали нормальним у кібербезпеці, від існуючих процесів до операційної інфраструктури. До пандемії більшість компаній із власними SOC ніколи не думали, що їм доведеться керувати своїми SOC віддалено. Тепер ці компанії орієнтуються на рішення безпеки, які дозволяють цілодобово віддалено керувати життєво важливими процесами операціями безпеки. Можна виділити декілька основних векторів та тенденцій розвитку Security Operation Center [30].

Тенденція перша – це ведення SOC зовнішніми постачальниками або в гібридному форматі. Ще до COVID-19 компанії зіткнулися з браком висококваліфікованих спеціалістів у сфері безпеки та досвіду, необхідних для ефективного управління SOC. У 2019 році суттєва нестача навичок існувала практично в кожному регіоні та галузі та вплинула на організації будь-якого розміру. Що створює розрив талантів? По-перше, IT-інфраструктури стають дедалі складнішими. Компанії значною мірою покладаються на цифрову комерцію, розумні пристрої, хмарні технології та мобільну робочу силу як частину своїх стандартних операцій, а інструменти безпеки, необхідні для моніторингу та захисту всього цього, стають не тільки дорожчими, але і складнішими в експлуатації та більш комплексні. Для багатьох компаній зростаюча складність зробила вартість аутсорсингу SOC MSSP або визначення того, як оптимізувати та полегшити внутрішню роботу, не лише привабливою,

але й необхідною. Ще до цього враховуючи труднощі пошуку найкращих спеціалістів і підтримки оновлень системи, і легко зрозуміти, чому кваліфікований постачальник, який може запропонувати цілодобовий нагляд і гарантію відповідності, представляє шлях найменшого опору. Правильний партнер або рішення може зрештою коштувати менше, ніж внутрішні ресурси.

Другою тенденцією, яку варто виділити є оркестровка безпеки, автоматизація та реагування SOAR. В SOC є зростання популярності оркестровки безпеки, автоматизації та реагування SOAR. Інструменти оркестрації та автоматизації розроблені, щоб допомогти організаціям автоматизувати та оптимізувати свої процеси реагування на безпеку. Використовуючи інструменти SOAR, організації можуть швидко й ефективно реагувати на потенційні загрози безпеці, такі як атаки зловмисного програмного забезпечення або витік даних. Одним із ключових способів, за допомогою яких інструменти SOAR можуть автоматизувати дії реагування на безпеку, є надання централізованої платформи для координації та керування різними етапами реагування на інцидент безпеки. Наприклад, інструменти SOAR можуть автоматично збирати та аналізувати дані з багатьох джерел. Прикладами таких джерел є мережеві пристрої, сервери та програми. Дані з цих джерел накопичуються та використовуються для виявлення потенційних загроз безпеці та визначення відповідної реакції на конкретну загрозу чи інцидент безпеки. Після виявлення потенційної загрози інструменти SOAR можуть автоматизувати виконання дій у відповідь, таких як ізоляція хостів або встановлення правил блокування на брандмауері. Організації можуть швидко стримати та пом’якшити вплив інциденту безпеки та запобігти його поширенню на інші частини свого IT-середовища. Таким чином, інструменти SOAR надають організаціям можливість автоматизувати та прискорити процеси реагування на безпеку, дозволяючи командам ефективніше виявляти потенційні загрози безпеці та реагувати на них. SOAR можна використовувати в поєднанні з інформацією про безпеку та керування подіями. Ці два підходи не суперечать один одному, а доповнюють один одного. SIEM відіграє важливу роль у сфері безпеки SOC, фільтрації та

виявленні інцидентів. SOAR виводить безпеку SOC на новий рівень, пропонуючи належне усунення реальних загроз.

Третім трендом не тільки для команд безпеки але і для всієї сфери кібербезпеки є застосування штучного інтелекту та машинного навчання. У той час як традиційний моніторинг безпеки зазвичай зосереджується на виявленні відомих загроз, інструменти на основі штучного інтелекту можуть допомогти організаціям ідентифікувати та реагувати на нові та нові загрози, які, можливо, не були виявлені раніше. Наприклад, алгоритми машинного навчання можуть аналізувати великі обсяги даних безпеки, щоб ідентифікувати шаблони та аномалії, які можуть вказувати на наявність потенційної загрози. Це може дозволити організаціям завчасно виявляти і реагувати на інциденти безпеки задовго до того, як ці загрози завдадуть значної фінансової, операційної чи репутаційної шкоди. До прикладу, вже зараз компанія Microsoft інтегрує в свої продукти безпеки штучний інтелект Microsoft Security Copilot — це потужний інструмент, який може допомогти організаціям випередити потенційні загрози безпеці. Security Copilot Microsoft [31] працює на основі моделі OpenAI ChatGPT-4, однієї з найдосконаліших доступних моделей штучного інтелекту. Microsoft Copilot Security використовує систему навчання «замкнутого циклу», що означає, що вона постійно навчається та вдосконалюється. Використовуючи замкнутий цикл навчання, Microsoft може з часом зробити штучний інтелект більш ефективним. Security Copilot вже зараз займається проактивним виявленням загроз. Copilot Security використовує величезні обсяги даних і штучний інтелект для виявлення потенційних загроз до того, як вони можуть завдати шкоди. Цей проактивний підхід гарантує, що організації завжди на крок попереду зловмисників. У разі порушення безпеки Copilot Security надає інструменти швидкого реагування та стратегії для пом’якшення наслідків і запобігання подальшому вторгненню. Це допомагає організаціям мінімізувати шкоду, спричинену інцидентами безпеки. За допомогою комплексних інструментів звітності організації отримують глибше розуміння стану безпеки. Це допомагає їм приймати обґрунтовані рішення щодо покращення заходів безпеки. Також

варто зазначити Copilot Security легко інтегрується з іншими продуктами Microsoft, забезпечуючи єдиний підхід до безпеки на всіх платформах. Це полегшує організаціям керування своїми заходами безпеки в одному місці. У своїй основі Copilot Security використовує передові моделі штучного інтелекту для постійного навчання та адаптації до середовища загроз, що постійно змінюється. Це гарантує, що організації завжди оновлюються з найновішими заходами безпеки [31].

Як показує практика, якщо гіганти індустрії інтегрують та інвестують в такі технології, це означає збільшення конкуренції між вендорами, які розроблять рішення з безпеки, а в свою чергу, все більше продуктів безпеки, будуть мати інтегровані функції штучного інтелекту. Тобто, така функція вже не буде опціональною чи унікальною, а стане обов'язковою для інженерів безпеки, а може навіть ключовою під час побудови стратегії безпеки організації.

Також, варто зазначити важливий тренд на інструменти оцінки атак з-зовні, які напевне найближчим часом, на рівні із іншими типовими продуктами, як захист кінцевих точок, мають стати ключовими для архітектури команд безпеки. Віддалена робота змусила організації перейти від захищених локальних середовищ, до хмарних і так чи інакше все більше ресурсів організації стають доступнішими через мережу інтернет. Для зловмисника – це ключ до інфраструктури компанії, враховуючи, що більшість систем обслуговуються IT командами, які не завжди дотримуються регулярних оновлень безпеки. До прикладу, вразливість нульового дня для мережевого шлюзу, який використовують співробітники для віддаленого підключення до інфраструктури організації, може стати ціллю номер один для операторів шифрувальників, тому під час пандемії, саме такі типи атак були наймасовіші за всю історію. Контроль периметру та своєчасне виявлення вразливостей організації, які доступні через мережу інтернет, дозволяє командам SOC своєчасно виявляти потенційні ризики та усувати їх. Основною перевагою таких рішень є виявлення помилок спричинені людським фактором або недбайливе ставлення до власної

кібергігієни IT спеціалістами. До прикладу відкриття зовнішнього доступу до комп’ютера організації через RDP.

Загалом, останні тенденції в моніторингу безпеки мають один спільний знаменник: вони відображають зсув до більш проактивних і передових підходів до виявлення загроз і реагування на них. Використовуючи досвід і вдосконалені інструменти, надані службами MDR у поєднанні з SOAR, і застосовуючи штучний інтелект для виявлення невідомих загроз, організації можуть краще захистити себе від небезпек, які таїть у собі ландшафт загроз, що постійно змінюється.

3.2 Рекомендації щодо побудови сучасної архітектури SOC

Побудова центру операцій безпеки передбачає ретельне планування та координацію людей, процесів і технологій. Що стосується людей, SOC вимагає команди кваліфікованих аналітиків та інженерів, здатних контролювати, виявляти та реагувати на загрози безпеці. До цієї команди мають входити люди з різними знаннями, від молодших до старших аналітиків, спеціалістів з реагування на інциденти та менеджера для нагляду за операціями. Команда повинна бути здатна реагувати на загрози 24 години на добу, 7 днів на тиждень і регулярно проходити навчання, щоб бути в курсі останніх загроз і методів безпеки. Процеси в SOC повинні бути стандартизовані для забезпечення послідовності та ефективності. Це включає процедури моніторингу, реагування на інциденти, виправлення та звітування. Ці процеси мають бути задокументовані та зберігатися для довідки команди. SOC також має мати стандартні процедури для ідентифікації, виявлення та відокремлення складних загроз від простих, а також для захисту даних і реагування на цільові загрози.

Варто чітко розуміти, команда реагування на кіберінциденти не є службою підтримки IT. Основним завданням служби підтримки IT є допомога співробітникам підприємства та забезпечення основних потреб інших

спеціалістів компанії. Для забезпечення ефективності підприємство має встановити чітку місію та статут SOC та визначити його функціональні атрибути. Команда безпеки призначена для захисту всього підприємства, і він повинен бути стратегічно пов’язаний з бізнес-цілями підприємства. Також, центр повинен мати повний доступ до інфраструктури підприємства, розуміти класифікацію критичних даних і мати перевірені технологічні рішення.

Таблиця 3.1

Критичні атрибути ефективності та викликів команд реагування

Критичні атрибути ефективності	Функціонування на всіх рівнях організації	Інтеграція з бізнес-цілями організації	Має увагу від правління директорів організації	Повна видимість над цифровими активами організації	Компетентний колектив
Критичні функціональні обов’язки	Моніторинг в режимі реального часу	Перевірка та реагування на інциденти	Стримування та усунення загроз	Звітність та KPI	Постійне вдосконалення та максимальна автоматизація
Критичні викликів	Ведення постійної операційної діяльності	Невідповідність корпоративній культурі	Ізольованість команди та процесів	Недостатнє фінансування	Передача критичних процесів на аутсорс

Визначення важливих атрибутів SOC найкраще досягається за допомогою підходу зверху вниз, коли місія агрегується, а статут базується на меті якнайкраще служити цілям і культурі підприємства. Низькорівневий підхід використовує цілісний погляд на критичні атрибути SOC, щоб точно відобразити управління кіберпідприємством [21].

Найбільш відповідним підходом до побудови надійної моделі SOC є участь міжфункціональних зацікавлених сторін на підприємстві. Виконання і щоденні операції є представниками методу «знизу вгору». Підхід «знизу вгору»

забезпечує дотримання вимог безпеки SOC, використання найкращих практик і повне використання переваг кіберпродуктів. Створення команди безпеки на підприємстві є дорогою справою. Це вимагає значних капіталовкладень в інфраструктуру та кіберпродукти, розробка політики та процедур, і зобов'язання наймати, навчати та утримувати висококваліфікованих технічних аналітиків. Ефективний SOC має працювати 24 години на добу, сім днів на тиждень, 365 днів на рік із персоналом, здатним реагувати на серйозні загрози та запобігати їм [20].

Як правило, кібербезпека підприємства не повинна передаватися сторонньому постачальнику керованих послуг безпеки. Ідеально, щоб підприємство взяло на себе суттєву відповідальність за функцію SOC і мало пряму частку в операційній власності. Звичайно, це залежить від спроможності підприємства зробити необхідні початкові інвестиції та зобов'язання щодо поточних операційних витрат. Малим підприємствам може знадобитися передати більшість функцій SOC MSSP. Підприємства середнього розміру часто вбудовують різні можливості SOC у власні функції кібербезпеки та передають деякі інші функції SOC третім сторонам, щоб зменшити витрати. Наприклад, підприємства середнього розміру можуть передати аутсорсингові тестування на проникнення, сканування вразливостей, оцінку безпеки та кібернавчання співробітників. Іншою можливістю для аутсорсингу є моніторинг інцидентів у другу або третю зміну та звітування з тимчасовими кібервиправленнями, поки основна команда SOC працює в першу зміну.

Ефективна команда безпеки передбачає контроль над функціонуванням і управлінням моніторингом безпеки підприємства, кіберзахистом, кібервиправленням і кіберзвітністю KPI. Має бути набір додатків та інструментів, які підтримують ідентифікацію, виявлення, захист від кіберзагроз і реагування на них, а також відновлення бізнес-операцій після події. Крім того, важливо, щоб SOC звітував про свої KPI відповідно до стандартів і рамок, таких як міжнародна організація стандартизації (ISO) ISO 27001/27002, Національний інститут стандартів і технологій США (NIST), спеціальна публікація (SP) 800-53, чи стандарт безпеки даних індустрії платіжних карток (PCI DSS) [28]. На основі

сучасних технологій, як Palo Alto XSIAM організації різного типу та розміру, мають можливість переглянути існуючі процеси, які будувалися довкола побудови багаторівненого SOC та уніфікувати критично-важливі процеси, а для компаній, які розглядають створення власного операційного центру, відкривається можливість побудувати його економлячи ресурси та час.

Розглянемо до прикладу сучасну схему архітектури команди реагування на кіберінциденти.

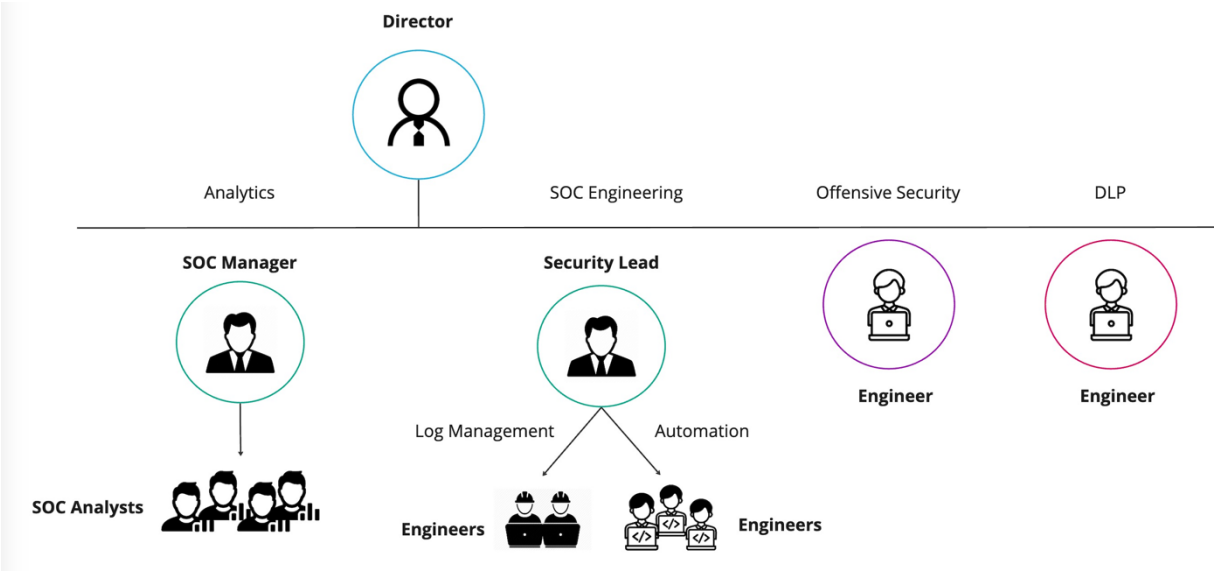


Рис. 3.2.1 Приклад сучасної архітектури SOC

Подібна архітектура не є багаторівневою, а процеси уніфіковані за типом задач такі як: аналітика, команда інжинірингу куди входить інтеграції джерел даних та автоматизації, відокремлений підрозділ наступальної безпеки, куди можуть входити спеціалісти по тестуванню на проникнення (пентестери) чи фахівці “червоної команди”, а також відокремленою є категорія спеціалістів відповідальних за інструменти контролю витоку даних. Така структура є більш ефективною для організації, процеси стають простішими для розуміння. Взяти до прикладу команду аналітиків, які в типовому SOC на даний момент можуть складатися з трьох рівнів. Основна відмінність між рівнями – це складність виконання поставлені перед ними завдання. Що стосується вищих рівнів, задачі можуть стосуватися аналізу шкідливого коду, які варто відокремити від типового

SOC. Такі спеціалісти можуть надати підтримку команді безпеки, як відокремлений підрозділ, завдання якого насичувати систему моніторингу різними типами індикаторами компрометації, або написання аналітичних звітів на основі яких можна побудувати нові контролі безпеки. Для великих організацій, де існує трьохрівневі команди аналітики, до кожного з них прив'язується відповідальний керівник, що може створювати дублікацію обов'язків. В свою чергу, сучасна архітектура пропонує об'єднати аналітику, як цільний підрозділ завдання якого виконання різного типу завдань пов'язаних з аналізом та реагування на інциденти. Відповідальна особа за команду аналітики повинна розробляти та пропонувати завдання відповідно до компетенції свого підрозділу і такі задачі можуть стосуватися як проактивного пошуку вразливостей, що переважно виконує другий або третій рівень аналітики команди безпеки, так і перевірку коректності виявлення, що типово виконує перший рівень.

Команда інженерів є важливою складовою любої архітектури команди безпеки. З кращих практик його інженерів відносять до третього рівня, як відповідальний персонал за роботу систем збору даних, кінцевих точок, правильності роботи кореляційних правил, тощо. В такому випадку, третій рівень означає, що він здатен виконувати різні задачі любого рівня, як аналітики так і проактивного виявлення вразливостей чи їх скануванню. Це створює значне навантаження на персонал, а також вимагає хорошої технічної підготовки. В сучасній архітектурі пропонується розділити команду інженерів на два рівня, відповідальні за джерела даних та інтеграції, другий автоматизація. Налаштування джерел даних, написання інструкцій щодо підготовки інтеграції, збір та аналітика даних, написання парсингу для читання подій інформаційної безпеки, створення кореляційний правил, звітів та дашбордів, налаштування інструментів захисту кінцевих точок, тощо, все це відноситься до інженерів операційної безпеки. Не варто інтегрувати такий величезний перелік різного типу і складності завдань, як третій рівень команди безпеки. До автоматизації можуть відноситися інженери, завдання яких забезпечити та облегшити роботу

команді безпеки загалом, шляхом автоматизацій рутинних процесів та задач, реагування на інциденти чи написання сторонніх інтеграцій, які офіційно не підтримуються вендорами.

Наступними в сучасній архітектурі, які не є обов'язковими але яких варто враховувати під час побудови професійного центру безпеки є спеціалісти з атак на інфраструктуру. За допомогою них в SOC є унікальна можливість перевірити, яким чином відпрацьовують системи захисту та взаємодія команди під час кібератаки. Це може бути регулярний рутинний процес, мета якого виявлення недоліків чи помилок конфігурації команд безпеки чи то його вразливих зон. Такі звіти важливі для керівників організації для повного розуміння, як і при яких умов спрацьовує захист, а також яким чином можливо його обійти. Адміністратори рішень по виявленню та протидії витокам виділені в окрему категорію спеціалістів. Для організацій великих розмірів з великим обсягами даних, такий тип інструменту може «вбити» операційність та швидкодію команд безпеки, так як DLP більш схильний до помилкових спрацювань, які потребують постійного доопрацювання. Правила виявлення можуть бути комплексними і потребують ретельного вивчення та тестування перед включенням для користувачів та систем. Щоб залишити SOC ефективним, під ці задачі варто розглянути окрему людину, яка буде відповідальна за такий продукт, і в свою чергу, яка інтегрує в команду безпеки моніторинг критичних подій та спрацювань з DLP.

Щоб сучасна архітектура SOC працювала ефективно, варто розглянути технічні аспекти архітектури команд реагування на кіберінцидети.

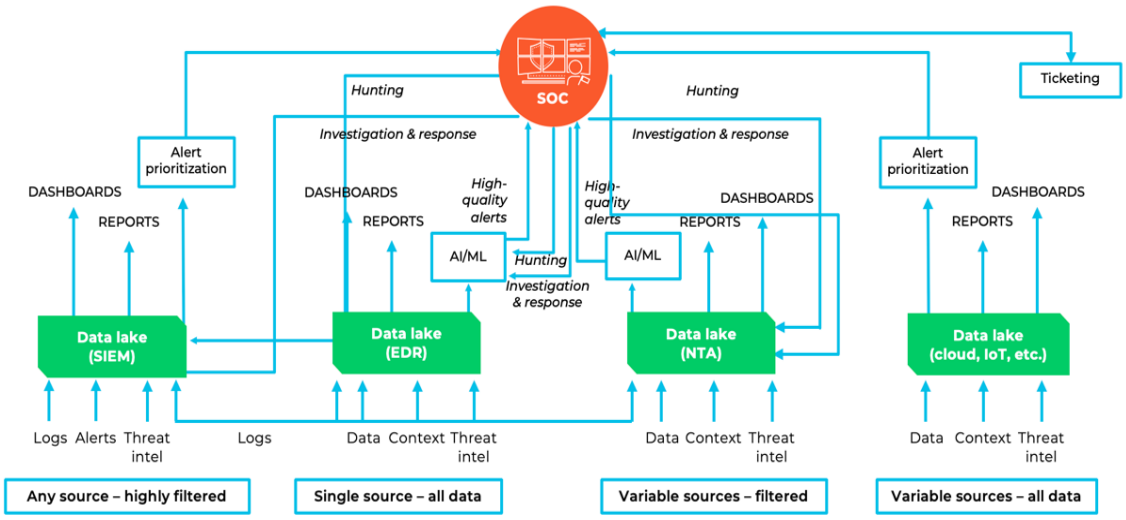


Рис. 3.2.2 Організація моніторингу інфраструктури

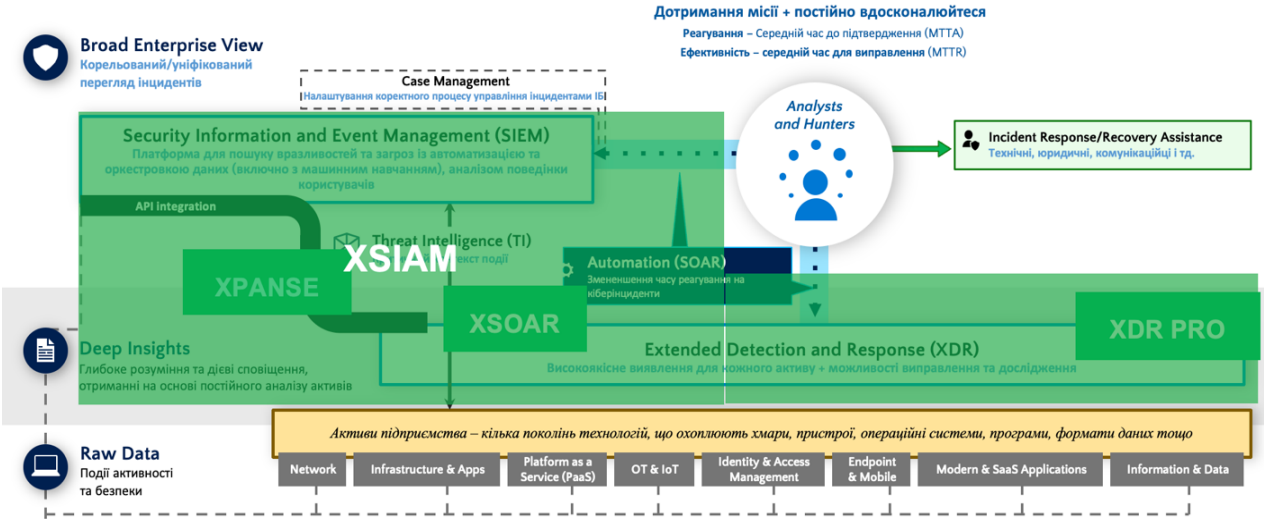


Рис. 3.2.3. Архітектура сучасної команди SOC

В сучасній архітектурі на основі програмного продукту Palo Alto XSIAM, за допомогою централізованого збору подій, оркестрації та автоматизації, розширеного виявлення та захисту кінцевих точок, штучного інтелекту та машинного навчання значно прискорює роботу та загальні показники ефективності. Потрібно зауважити, що в будь-якій іншій типові архітектурі, кожен окремий елемент захисту, по суті є окремим програмним продуктом, не пов’язаних між собою та різних вендорів, що потребує додаткових ресурсів для його підтримки, оновлень, тощо. Показники можна порівняти з типовими SIEM.

Таблиця 3.2

Порівняльна характеристика економії часу під час використання SIEM

Тип задачі	**SIEM**	**XSIAM**	**Приблизний показник економії часу**
Створення правил виявлення загроз Постійний процес створення, та впровадженян правил	120 год/тиж безперервно	20 год/тиж безперервно Більша частина правил пишеться XSIAM Research Team	100год/тиж
Виправлення правил виявлення	80 год/тиж безперервно	8 год/тиж безперервно Більша частина правил оптимізовується XSIAM Research Team	72 год/тиж
Обслуговування системи	15 год/тиж безперервно	15 год/тиж безперервно	-
Кореляція даних	20 год/тиж безперервно	5 год/тиж безперервно	15 год/тиж
Аналітика	год/тиж потребує додаткові пакети для побудови аналітичної моделі	-год/тиж Автоматично навчається на моделі ML	

Рис. 3.2.4. Приблизна економія часу аналітиків під час автоматизації

3.3 Рекомендації щодо вирішення типових проблем SOC

Нерозумно намагатися сконструювати літак під час польоту, він вийде з ладу. Подібним чином керівництво підприємства може запобігти збою, уникнувши таких підводних каменів під час створення та експлуатації команди реагування на кіберінциденти. Ніколи не варто припускати, що існує 100-відсоткове безпечне середовище. Успішні операції безпеки можливі лише тоді, коли підприємства постійно вдосконалюють власні підходи для забезпечення інформаційної та кібербезпеки.

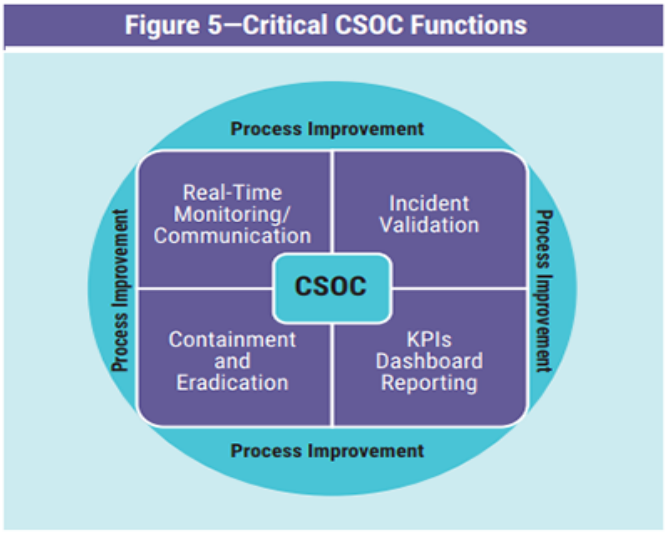


Рис. 3.3.1. Критичні функції SOC

Важливо визначити пріоритети ассетів, ізолювати критичні мережі, посилити внутрішній контроль, запровадити моніторинг у реальному часі та сповіщення про інциденти, а також проводити аудити з безпеки не тільки організації але і SOC. Не варто передавати весь SOC аутсорсингу [32]. Це означає передачу всієї відповідальності за безпеку підприємства на аутсорсинг. Таким чином неможливо передати звітність іншій компанії, так як відповідальність та звітність належить самому підприємству. Частковий аутсорсинг деяких функцій SOC є прийнятним, але найважливіші функції мають залишатися внутрішніми,

наскільки це можливо. Намагатися убезпечити все означає не убезпечити нічого. Кожен день приносить нові кіберзагрози у вигляді програм-вимагачів, шкідливих програм, фішингу, соціальної інженерії та витоку даних. Інвестиції в команди, інструменти та додатки з кібербезпеки не є абсолютною відповіддю. Необхідно знайти баланс між інвестиціями в навчання співробітників, кіберінструментами та політиками, а також процедурами, щоб гарантувати, що підприємство знаходиться в оптимальній позиції для реагування на кіберзагрози. Техніка не може замінити людей. Програми штучного інтелекту не можуть замінити людський інтелект. Практично кажучи, штучний інтелект у сфері кібербезпеки ще недостатньо зрілий. Заміна людей технологіями призведе до відмови від людського боку середовища, культури та бізнесу підприємства. Зараз підприємства повинні покладатися на кваліфікований персонал для перевірки та застосування коригувальних дій. Використання занадто великої кількості продуктів безпеки може переповнити технологічну екосистему та призвести до конфліктних продуктів. Аналітики безпеки повинні бути навчені визначати основні причини проблем і викорінювати їх. KPI мають фіксувати тенденції кіберзагроз, наприклад, шляхом визначення змінних тенденцій за 12 місяців. Немає простої відповіді на централізоване та децентралізоване планування та виконання. Це залежить від розміру підприємства. Прийняття рішень – це мистецтво, а не наука. Немає жодного математичного рівняння, яке б дало точні кількісні результати. Творче мислення та компетентне управління необхідні для визначення відповідного ступеня централізації та децентралізації управління, планування та виконання SOC. Одна команда чи один ресурс не може зробити все. SOC буде найбільш ефективним за наявності спеціалізованих груп і розподілу обов’язків. Повинні бути різні команди, які зосереджуються на моніторингу та звітності в реальному часі, перевірки інцидентів, їх локалізації та ліквідації, централізована звітність та інформаційна панель KPI, безперервне вдосконалення процесів і технологій. Наскільки це можливо, заздалегідь необхідно скласти посібники з реагування на інциденти. Процеси SOC повинні бути задокументовані та поширені, а системні аналітики мають бути навчені

дотримуватися відповідних процедур. SOC не може працювати у вакуумі. Його ефективність залежить від отримання вхідних даних і співпраці з різними зацікавленими сторонами, такими як директор з інформаційної безпеки організації (CISO), розробники, служба підтримки IT, користувачі, постачальники рішень і галузеві консорціуми [33].

Висновки до третього розділу

Третій розділ присвячений написанню рекомендацій та аналізом щодо подальшого розвитку архітектур Security Operation Center. Тенденція перша – це ведення SOC зовнішніми постачальниками або в гібридному форматі. Ще до COVID-19 компанії зіткнулися з браком висококваліфікованих спеціалістів у сфері безпеки та досвіду, необхідних для ефективного управління SOC. У 2019 році суттєва нестача навичок існувала практично в кожному регіоні та галузі та вплинула на організації будь-якого розміру. В свою чергу, це робить SOC доступнішим більшому колу організацій, як малого так і великих розмірів. Другою тенденцією, яку варто виділити є оркестровка безпеки, автоматизація та реагування SOAR. В SOC є зростання популярності оркестровки безпеки, автоматизації та реагування SOAR. Інструменти оркестрації та автоматизації розроблені, щоб допомогти організаціям автоматизувати та оптимізувати свої процеси реагування на безпеку. Використовуючи інструменти SOAR, організації можуть швидко й ефективно реагувати на потенційні загрози безпеці, такі як атаки зловмисного програмного забезпечення або витік даних. Одним із ключових способів, за допомогою яких інструменти SOAR можуть автоматизувати дії реагування на безпеку, є надання централізованої платформи для координації та керування різними етапами реагування на інцидент безпеки. Наприклад, інструменти SOAR можуть автоматично збирати та аналізувати дані з багатьох джерел. Прикладами таких джерел є мережеві пристрої, сервери та програми. Третім трендом не тільки для команд безпеки але і для всієї сфери кібербезпеки є застосування штучного інтелекту та машинного навчання. У той

час як традиційний моніторинг безпеки зазвичай зосереджується на виявленні відомих загроз, інструменти на основі штучного інтелекту можуть допомогти організаціям ідентифікувати та реагувати на нові та нові загрози, які, можливо, не були виявлені раніше. Наприклад, алгоритми машинного навчання можуть аналізувати великі обсяги даних безпеки, щоб ідентифікувати шаблони та аномалії, які можуть вказувати на наявність потенційної загрози. Це може дозволити організаціям завчасно виявляти і реагувати на інциденти безпеки задовго до того, як ці загрози завдадуть значної фінансової, операційної чи репутаційної шкоди. Розглянуто питання дотримання ефективності команди безпеки, тому це передбачає контроль над функціонуванням і управлінням моніторингом безпеки підприємства, кіберзахистом, кібервиправленням і кіберзвітністю KPI. Має бути набір додатків та інструментів, які підтримують ідентифікацію, виявлення, захист від кіберзагроз і реагування на них, а також відновлення бізнес-операцій після події. Крім того, важливо, щоб SOC звітував про свої KPI відповідно до стандартів і рамок, таких як міжнародна організація стандартизації (ISO) ISO 27001/27002, національний інститут стандартів і технологій США (NIST), спеціальна публікація (SP) 800-53. На основі сучасних технологій, як Palo Alto XSIAM організації мають можливість переглянути існуючі процеси, які будувалися довкола побудови багаторівненого SOC та уніфікувати критично-важливі процеси, а для компаній, які розглядають створення власного операційного центру, відкривається можливість побудувати його економлячи ресурси та час. Намагатися убезпечити все означає не убезпечити нічого. Кожен день приносить нові кіберзагрози у вигляді програм-вимагачів, шкідливих програм, фішингу, соціальної інженерії та витоку даних. Інвестиції в команди, інструменти та додатки з кібербезпеки не є абсолютною відповіддю. Необхідно знайти баланс між інвестиціями в навчання співробітників, кіберінструментами та політиками, а також процедурами, щоб гарантувати, що підприємство знаходиться в оптимальній позиції для реагування на кіберзагрози.

ВИСНОВКИ

У кваліфікаційній роботі було проведено всебічний аналіз продуктів, технологій та архітектури команд операційної безпеки. За результатами аналізу проведеного в першому розділі, було досліджено доцільність та необхідність створення власного центру моніторингу та реагування на кіберінциденти в організації. Враховані основні ризики та виклики під час його побудови і визначено основні моделі архітектур команди SOC: зовнішнє управління, повністю інтегровані в структуру організації та гібридна модель. Також проведений аналіз поточних типових архітектур SOC в організаціях. Центри операційної безпеки акумулюють величезну кількість подій в режимі реального часу і кожен кіберінцидент має власну класифікацію та тип. Серед основних загроз зазначено програми-вимагачі, які все частіше стають не тільки фінансово вмотивовані, але і мета яких деструктивний характер, тобто знищення IT інфраструктури організації задля зупинки критично-важливих процесів організації.

В другому розділі було проведено практичну роботу із побудови сучасної архітектури SOC на основі програмного рішення Palo Alto XSIAM, яке часто називають системою збору та аналізу подій інформаційної безпеки нової генерації.. Основною перевагою рішення є вбудовані правила детекції різного типу загроз з врахуванням матриці MITRE, які регулярно оновлюються командою реагування на інциденти Palo Alto UNIT42. Було продемонстровано конфігурацію профілів безпеки кінцевих точок та продемонстровано, що інструмент підтримує не тільки про безпеку робочих станцій користувачів, але і про смартфони. Продемонстровано переваги Palo Alto XSOAR – система оркестрації та автоматизації інцидентів кібербезпеки. На практиці, розглянуто автоматизацію розширення контексту під час інциденту за допомогою даних з Azure, IDP Okta та Active Directory.

Третій розділ присвячений написанню рекомендацій та аналізом щодо подальшого розвитку архітектур Security Operation Center. Визначені основні тендеції розвитку центрів безпеки. Тенденція перша – це ведення SOC

зовнішніми постачальниками або в гібридному форматі. Другою - це є оркестровка безпеки, автоматизація та реагування SOAR. В SOC є зростання популярності оркестровки безпеки, автоматизації та реагування SOAR. Інструменти оркестрації та автоматизації розроблені, щоб допомогти організаціям автоматизувати та оптимізувати свої процеси реагування на безпеку. Використовуючи інструменти SOAR, організації можуть швидко й ефективно реагувати на потенційні загрози безпеці, такі як атаки зловмисного програмного забезпечення або витік даних. Одним із ключових способів, за допомогою яких інструменти SOAR можуть автоматизувати дії реагування на безпеку, є надання централізованої платформи для координації та керування різними етапами реагування на інцидент безпеки. Третім трендом не тільки для команд безпеки але і для всієї сфери кібербезпеки є застосування штучного інтелекту та машинного навчання. У той час як традиційний моніторинг безпеки зазвичай зосереджується на виявленні відомих загроз, інструменти на основі штучного інтелекту можуть допомогти організаціям ідентифікувати та реагувати на нові та нові загрози, які, можливо, не були виявлені раніше. Наприклад, алгоритми машинного навчання можуть аналізувати великі обсяги даних безпеки, щоб ідентифікувати шаблони та аномалії, які можуть вказувати на наявність потенційної загрози. Це може дозволити організаціям завчасно виявляти і реагувати на інциденти безпеки задовго до того, як ці загрози завдадуть значної фінансової, операційної чи репутаційної шкоди.

Висновки та рекомендації, представлені в цій роботі, можуть служити важливим ресурсом для компаній, які прагнуть автоматизувати власні процеси SOC та отримати бачення “все в одному”.

ПЕРЕЛІК ПОСИЛАНЬ

1. The Top SOC Analyst Challenges. Swimlane. URL: https://swimlane.com/blog/top-soc-analyst-challenges/

2. 4 Key Challenges for Next-Get Security Operations Centers. TechBeacon. URL: https://techbeacon.com/security/4-key-challenges-next-gen-security-operations-centers

3. Best Security Information and Event Management (SIEM) Software Reviews 2023 | Gartner Peer Insights. Gartner. URL: https://www.gartner.com/reviews/market/security-information-event-management.

4. Кібербезпека бізнесу в умовах нестабільності. PwC. URL: https://www.pwc.com/ua/uk/publications/2022/cybersecurity-uncertainty-state.html

5. What is EDR in Cyber Security? Excitium. URL: https://www.xcitium.com/edr-in-cyber-security/

6. What is Extended Detection and Response (XDR). Palo Alto Networks. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-extended-detection-response-XDR

7. SOC Proccesses, Operations, Challenges and Best Practices. Sapphire. URL: https://www.sapphire.net/security/soc-processes/

8. Mojaloop Business Opertaions Documentation. URL: https://docs.mojaloop.io/mojaloop-business-docs/HubOperations/TechOps/incident-management.html

9. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України. URL: https://goal-int.org/klasifikatsiya-kiberzagroz-ta-yih-legitimatsiya-u-normativno-pravovih-aktah-ukrayini/

10. Ongoing Russian cyberattacks targeting Ukraine - Microsoft On the Issues. Microsoft On the Issues. URL: https://blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyberattacks-ukraine-cadet-blizzard/

11. Russian spies behind cyber attack on Ukraine power grid in 2022. Reuters. URL:https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/

12. MITRE ATT&CK®. MITRE ATT&CK. URL: https://attack.mitre.org/

13. Vision 2020 Data Breach Report: Money Still makes the Cyber-Crime World Go Round. Verizon. URL: https://www.verizon.com/a bout/news/verizon-2020- data-breach-investigations-report

14. Top 7 types of attacks in security operation center (SOC) you must know. CyberNX. URL: https://www.cybernx.com/b-top-7-types-of-attacks-in-security-operation-center-soc-you-must-know

15. Security Operation Center. Building, Operation and Maintaining your SOC.URL: https://ptgmedia.pearsoncmg.com/images/9780134052014/samplepages/9780134052014.pdf

16. What is Cortex XSIAM? Palo Alto Network. URL: https://www.paloaltonetworks.com/cyberpedia/what-is-extended-security-intelligence-and-automation-management-xsiam

17. Palo Alto Networks Introduces the Autonomous Security Platform, Cortex XSIAM to reimagine SIEM and SOC Analytics. Palo Alto. URL: https://www.paloaltonetworks.com/company/press/2022/palo-alto-networks-introduces-the-autonomous-security-platform--cortex-xsiam--to-reimagine-siem-and-soc-analytics

18. Why does your organization need Cortex XDR? Xcitium. URL: https://www.xcitium.com/cortex-xdr/

19. Attack Surface Management XPANSE. Palo Alto. URL: https://www.paloaltonetworks.com/cortex/cortex-xpanse

20. Cortex XSOAR – Redefing Security Orchestration, Automation and Response. Palo Alto Network. URL: https://www.exclusive-networks.com/uk/wp-content/uploads/sites/28/2021/07/cortex-xsoar-DATASHEET.pdf

21. Evaluating SOC automation benefits and limitations. Techtarget. URL: https://www.techtarget.com/searchsecurity/tip/Evaluating-SOC-automation-benefits-and-limitations

22. Why you should adopt automation in your SOC. Mindflow. URL: https://mindflow.io/soc-automation/

23. Low-code Security automations benefits for your SecOps. Swimlane. URL: https://swimlane.com/blog/low-code-security-automation-benefits-for-secops/

24. SOC Automation: Preventing Analyst Burnout. Forta. URL: https://www.fortra.com/blog/soc-automation-preventing-analyst-burnout

25. Palo Alto Networks Launches XSIAM 2.0: The Key Updates. CRN. URL: https://www.crn.com/news/security/palo-alto-networks-launches-xsiam-2-0-the-key-updates

26. Can Palo Alto Networks XSIAM Disrupt SIEM Security Software Market? MSSP Alert. URL: https://www.msspalert.com/news/palo-alto-networks-seeks-to-disrupt-siem-security-market

27. Palo Alto Networks Ushers in the Next-Generation Security Operation Center with General Availability of Cortex XSIAM. CDSAonline. URL: https://www.cdsaonline.org/post/?u=2022/10/12/palo-alto-networks-releases-cortex-xsiam-to-automate-the-soc-venturebeat

28. Palo Alto Networks Introduces the Autonomous Security Platform, Cortex XSIAM. DarkReading. URL: https://www.darkreading.com/cybersecurity-operations/palo-alto-networks-introduces-the-autonomous-security-platform-cortex-xsiam

29. Palo Alto Networks adds new AI-related security features to its Cortex line. Siliconangle. URL: https://siliconangle.com/2023/11/13/palo-alto-networks-adds-new-ai-related-security-features-cortex-line/

30. 3 SOC Trends Shaping the Future of Security. URL: https://blog.ariacybersecurity.com/blog/3-soc-trends-shaping-the-future-of-security

31. Operationalizing Microsoft Security Copilot to Reivent SOC Productivity. Microsoft. URL: https://techcommunity.microsoft.com/t5/microsoft-

defender-xdr-blog/operationalizing-microsoft-security-copilot-to-reinvent-soc/ba-p/3944877

32. Best Practices for Setting Up a Cybersecurity Operation Center. ISACA. URL: https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/best-practices-for-setting-up-a-cybersecurity-operations-center

33. Guideline to develop and maintain the security operation center (SOC) | Infosec. Infosec Resources - IT Security Training & Resources by Infosec. URL: https://resources.infosecinstitute.com/topics/general-security/guideline-to-develop-and-maintain-the-security-operation-center-soc/

34. Five challenges SOC teams face everyday. DNIF. URL: https://www.dnif.it/en/blog/five-challenges-soc-teams-face-everyday