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: “ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ З ВИКОРИСТАННЯМ SIEM”

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

_____ Олександр МАРЦЕНЮК

(Підпис) *Ім’я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Олександр МАРЦЕНЮК

Керівник:
к.в.н., доц. Юрій ЯКИМЕНКО

Рецензент:
д.т.н., проф. Олександр ТУРОВСЬКИЙ

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 Марценюку Олександру Вячеславовичу

(прізвище, ім’я, по батькові здобувача)

1. Тема кваліфікаційної роботи: “Підвищення ефективності системи управління інформаційною безпекою з використанням SIEM”

керівник кваліфікаційної роботи Юрій ЯКИМЕНКО, к.в.н.,доц.

(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: *інформаційна безпека підприємства, методи та засоби управління інформаційною безпекою, нормативні документи, стандарти, міжнародні стандарти.*
4. Перелік питань, які потрібно розробити:
   1. Розглянути обґрунтування застосування SIEM для підвищення ефективності управління інформаційною безпекою.
   2. Сформувати підходи і процеси у підвищенні ефективності системи управління інформаційною безпекою організації з використанням SIEM.
   3. Дослідити та розробити рекомендації для підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM.
   4. Перелік ілюстративного матеріалу: *презентація*
5. Дата видачі завдання “26” вересня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: ”26” вересня 2023 р..

№ з/п	Етапи роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	26.09.2023	виконано
2.	Збір та аналіз літератури.	03.10.2023	виконано
3.	Розділ 1. Теоретичне обґрунтування застосування SIEM для підвищення ефективності управління інформаційною безпекою	17.10.2023	виконано
4.	Розділ 2. Аналіз підходів і процесів у підвищенні ефективності інформаційної безпеки організації	31.10.2023	виконано
5.	Розділ 3. Дослідження та розробка рекомендацій для підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM	14.11.2023	виконано
6.	Формулювання висновків за результатами проведеного дослідження	01.12.2023	виконано
7.	Оформлення роботи	08.12.2023	виконано
8.	Оформлення презентації	15.12.2023	виконано
9.	Отримання рецензії на роботу	23.12.2023	виконано
10.	Захист в ДЕК	16.01.2024	виконано

Здобувач вищої освіти _____ Олександр МАРЦЕНЮК_
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Юрій ЯКИМЕНКО_
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

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

Направляється здобувач Марценюк О.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "Підвищення ефективності системи управління інформаційною безпекою з використанням SIEM".
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **МАРЦЕНЮК ОЛЕКСАНДР** у кваліфікаційній роботі дослідив сучасні процеси і підходи до підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM в Україні, визначив основні переваги і недоліки використання SIEM рішень на підприємствах та розробив рекомендації для організацій (підприємств), які прагнуть покращити свої заходи кібербезпеки завдяки ефективному використанню інструментів SIEM. **МАРЦЕНЮК ОЛЕКСАНДР** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на науково-практичній конференції «Актуальні проблеми кібербезпеки».
Це дозволяє оцінити виконану кваліфікаційну роботу здобувача **МАРЦЕНЮКА Олександра** на оцінку "відмінно" та присвоїти їй кваліфікацію Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи ___ Юрій ЯКИМЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___"_____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач **МАРЦЕНЮК О.В.** допускається до захисту даної роботи в Державній екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти Марценюка Олександра Вячеславовича
на тему “ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ З ВИКОРИСТАННЯМ SIEM ”

Актуальність

Інформація завжди була як найважливішим об'єктом, так і засобом боротьби між людьми. Неможливо заперечувати факти здійснення інформаційного впливу на широку аудиторію протягом усіх етапів історичного розвитку, хоча в різні періоди інтенсивність застосування тих чи інших способів впливу, як і досконалість його організації, значною мірою відрізнялися.

Тому процес підвищення ефективності системи управління інформаційною безпекою з використанням SIEM має бути побудований з урахуванням потреби запобігати і протидіяти загрозам, що виникають внаслідок застосування методів інформаційного протиборства, захищати потенційно важливу інформацію, інфраструктуру та персонал як стратегічний ресурс підприємства.

Позитивні сторони

В ході виконання роботи було проведено всебічне дослідження систем управління інформацією та подіями. Робота спрямовувалася на оцінку ефективності системи управління інцидентами інформаційної безпеки, з використанням програми Splunk Enterprise Security для збору та аналізу даних. У рамках першого розділу було проведено глибоке дослідження процесу інтеграції SIEM-систем та аналіз щодо впливу SIEM на безпеку даних та інформаційну безпеку організації У другому розділі було детально розглянуто роль та значення SIEM-систем у сучасних умовах цифрової економіки. Проаналізовано ринок вендорів які розробляють SIEM-системи, наведені їх переваги та недоліки. З використанням програми Splunk Enterprise Security, було проведено детальний аналіз ефективності SIEM. Отримані дані демонструють значне покращення в таких ключових областях, як час виявлення інцидентів та швидкість реагування, а також зменшення помилкових спрацьовувань. У третьому розділі були наведені можливі шляхів впровадження рекомендацій та їх практична реалізація. Також була надана оцінка рекомендацій з точки зору практичної реалізованості та впливу на безпеку даних.

Недоліки

У роботі також доцільно було б визначити заходи застосування штучного інтелекту при плануванні, але вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує оцінки «відмінно», а її автор Марценюк Олександр Вячеславович заслуговує присвоєння кваліфікації «Магістр кібербезпеки за спеціалізацією Управління інформаційною безпекою».

Рецензент:
д.т.н, професор

_____ Олександр ТУРОВСЬКИЙ
підпис *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 81 стор., 23 рис., 60 джерел.

Метою роботи є вивчення процесів і підходів до підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM.

Об'єктом дослідження є процеси у підвищенні ефективності системи управління інформаційною безпекою організації з використанням SIEM.

Предмет дослідження - підходи до підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи технологічного аналізу та теорії інформаційної безпеки, теорії інформаційного протиборства та конкуренції між суб'єктами підприємницької діяльності.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті підвищення ефективності використання системи управління інформаційною безпекою.

Короткий зміст роботи. Як результат у роботі проведено аналіз рекомендацій що до підвищення ефективності системи управління інформаційною безпекою з використанням SIEM; досліджено особливості управління інформаційною безпекою підприємства в умовах використання SIEM; проведено аналіз ринку SIEM рішень, їх переваги та недоліки.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті протидії загрозам, пов'язаним із веденням інформаційного протиборства.

КЛЮЧОВІ СЛОВА : ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, SIEM.

ABSTRACT

The text part of the qualification work for the master's degree: 81 pages, 23 figures, 60 sources.

The purpose of the work is to study the processes and approaches to improving the efficiency of an organisation's information security management system using SIEM.

The object of research is the processes of improving the efficiency of an organisation's information security management system using SIEM.

The subject of research is approaches to improving the efficiency of an organisation's information security management system using SIEM.

Research methods. To solve the above scientific task, the methods of technological analysis and theory of information security, theory of information confrontation and competition between business entities were used in the work.

Scientific novelty of the results. The developed approaches can be used in the planning and implementation of the enterprise information security management system in the context of improving the efficiency of the information security management system.

Summary of the work. As a result, the paper analyses the recommendations for improving the efficiency of the information security management system using SIEM; investigates the features of enterprise information security management in the context of using SIEM; analyses the market of SIEM solutions, their advantages and disadvantages.

Scope of application. The developed approaches can be used in the planning and implementation of the enterprise information security management system in the context of counteracting threats associated with information warfare.

KEYWORDS : ENTERPRISE INFORMATION SECURITY, , INFORMATION SECURITY MANAGEMENT SYSTEM, SIEM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

CMDB - Configuration Management Database

CPPA - California Privacy Protection Act

EDR - Endpoint Detection and Response

GDPR - General Data Protection Regulation

HIPAA - Health Insurance Portability and Accountability Act

IDS - Intrusion Detection System

IPS - Intrusion Prevention System

ISO - Міжнародна організація зі стандартизації

KPI - Key Performance Indicator

LGPD - Lei Geral de Proteção de Dados - Загальний закон про захист даних (Бразилія)

NIST - National Institute of Standards and Technology

SaaS - Software as a Service

SEI - Software Engineering Institute

SEM - Security event management

SIEM - Security information event management

SOAR - Security Orchestration, Automation, and Response

SPL - Splunk Processing Language

TIP - Threat Intelligence Platform

СУІБ - система управління інформацією безпекою

ВСТУП

Актуальність теми. Інформація завжди була як найважливішим об'єктом, так і засобом боротьби між людьми. Неможливо заперечувати факти здійснення інформаційного впливу на широку аудиторію протягом усіх етапів історичного розвитку, хоча в різні періоди інтенсивність застосування тих чи інших способів впливу, як і досконалість його організації, значною мірою відрізнялися.

Тому процес підвищення ефективності системи управління інформаційною безпекою з використанням SIEM має бути побудований з урахуванням потреби запобігати і протидіяти загрозам, що виникають внаслідок застосування методів інформаційного протиборства, захищати потенційно важливу інформацію, інфраструктуру та персонал як стратегічний ресурс підприємства.

З огляду на зазначене, тема кваліфікаційної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки суб'єктів підприємницької діяльності.

Мета роботи полягає у вивченні процесів і підходів до підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM.

Об'єкт дослідження - процеси у підвищенні ефективності системи управління інформаційною безпекою організації з використанням SIEM.

Предмет дослідження – підходи до підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM.

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

Розглянути обґрунтування застосування SIEM для підвищення ефективності управління інформаційною безпекою.

Сформувати підходи і процеси у підвищенні ефективності системи управління інформаційною безпекою організації з використанням SIEM.

Дослідити та розробити рекомендації для підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи технологічного аналізу та теорії інформаційної безпеки, теорії інформаційного протиборства та конкуренції між суб'єктами підприємницької діяльності.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою підприємства у контексті підвищення ефективності використання системи управління інформаційною безпекою.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і рекомендацій підвищення ефективності, покращення інфраструктури та персоналу підприємства у відповідності до цілей бізнесу, корпоративних можливостей та ресурсів в умовах інформаційного протиборства.

Апробація результатів кваліфікаційної роботи було оприлюднено на науково-практичній конференції:

Марценюк О.В. SIEM системи (security information and event management) – що це і навіщо потрібно?. Актуальні проблеми кібербезпеки : Всеукр. науково-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 321–323.

РОЗДІЛ 1.
ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ ЗАСТОСУВАННЯ SIEM ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

1.1 Опис теоретичних підходів до інтеграції SIEM в інфраструктуру організації

Інтеграція систем управління інформаційною безпекою (SIEM) в інфраструктуру організації є важливим етапом для забезпечення цілісності та безпеки даних. Існує кілька теоретичних підходів до цієї інтеграції, які можуть бути використані для оптимізації процесів моніторингу та аналізу подій в організації.

Інтеграція SIEM з системами виявлення вторгнень (IDS) та системами запобігання вторгнень (IPS) є важливим етапом для підвищення ефективності та повноти моніторингу та захисту мережі організації.

Системи виявлення вторгнень (IDS) призначені для виявлення незвичайної або підозрілої активності в мережі, такої як незаконне використання акаунтів, спроби несанкціонованого доступу, атаки з використанням вразливостей тощо. Інтеграція SIEM з IDS дозволяє об'єднати дані про виявлені загрози з іншими джерелами інформації, такими як журнали подій, що дозволяє отримати більш повне уявлення про потенційні загрози та події в мережі.

Системи запобігання вторгнень (IPS) використовуються для блокування або відхилення шкідливої активності в реальному часі. Інтеграція SIEM з IPS дозволяє автоматично реагувати на виявлені загрози, наприклад, шляхом відключення атакуючого обладнання або встановлення правил фільтрації трафіку для блокування шкідливих пакетів.

Ця інтеграція також дозволяє забезпечити більш повне відслідковування подій та відповідних заходів, що були вжиті для запобігання або виявлення загроз. Вона також сприяє покращенню аналізу та реагування на інциденти,

оскільки об'єднує дані з різних джерел для отримання повного зображення про стан безпеки мережі.

Інтеграція SIEM з іншими системами моніторингу, такими як системи управління журналами подій (Log Management Systems) та системи аналізу великих даних (Big Data Analytics), грає важливу роль у покращенні здатності організації виявляти та реагувати на потенційні загрози безпеки.

Системи управління журналами подій (LMS) відіграють ключову роль у зборі, збереженні та аналізі журналів подій з різних джерел, таких як мережеві пристрої, сервери, додатки тощо. Інтеграція SIEM з LMS дозволяє об'єднати дані про події з різних джерел в єдину систему, що сприяє покращенню виявлення аномалій та загроз у мережі. Крім того, це дозволяє зберігати дані відповідно до регулятивних вимог та забезпечує можливість подальшого аналізу для виявлення шаблонів та трендів у безпеці.

Системи аналізу великих даних (Big Data Analytics) дозволяють обробляти та аналізувати великі обсяги даних для виявлення складних зв'язків та патернів. Інтеграція SIEM з Big Data Analytics дозволяє використовувати потужні алгоритми аналізу для виявлення навіть найбільш складних загроз та аномалій у мережі. Це може включати виявлення нових видів загроз, аналіз поведінки користувачів та виявлення витоків даних.

Така інтеграція дозволяє організаціям отримати більш повне та глибоке розуміння стану безпеки своєї мережі, а також забезпечує можливість вчасно реагувати на загрози та інциденти. Вона також допомагає виявляти та усувати проблеми безпеки на ранніх етапах, що дозволяє запобігти серйозним наслідкам для організації.

Інтеграція SIEM з іншими системами управління безпекою, такими як системи управління інцидентами (Incident Management Systems) та системи автоматизації відгуку на інциденти (Security Orchestration, Automation, and Response - SOAR), є важливим аспектом забезпечення безпеки в сучасних організаціях.

Системи управління інцидентами (IMS) дозволяють організаціям ефективно виявляти, реєструвати та вирішувати безпекові інциденти. Інтеграція SIEM з IMS дозволяє автоматично передавати дані про потенційні загрози та події безпеки з SIEM до системи управління інцидентами для подальшого аналізу та реагування. Це сприяє швидкому виявленню та вирішенню інцидентів, що дозволяє зменшити час реагування на потенційні загрози.

Системи автоматизації відгуку на інциденти (SOAR) поєднують в собі автоматизацію, оркестрацію та відгук на безпекові події. Інтеграція SIEM з SOAR дозволяє автоматизувати процеси відгуку на інциденти, включаючи виявлення, аналіз та реагування на загрози. Це допомагає зменшити навантаження на персонал та забезпечує швидке та послідовне реагування на безпекові події.

Загалом, інтеграція SIEM з системами управління інцидентами та системами автоматизації відгуку на інциденти допомагає організаціям підвищити ефективність виявлення, аналізу та реагування на безпекові загрози, зменшити час реагування на інциденти та забезпечити більш повний та автоматизований процес безпеки. [47]

Успішне впровадження SIEM вимагає ретельного планування, виконання та постійного аналізу, щоб гарантувати, що система відповідає потребам організації у сфері безпеки та відповідності вимогам. Нижче ми розглянемо ключові етапи цього процесу:

Встановлення вимог. Перш ніж впроваджувати рішення SIEM, дуже важливо визначити конкретні вимоги організації до безпеки та відповідності. Це включає в себе

- Регуляторний ландшафт: Вивчіть відповідні галузеві нормативні акти (наприклад, GDPR, HIPAA, PCI-DSS) і внутрішні політики, які визначають вимоги до безпеки і відповідності вашої організації.
- Джерела даних: Визначте всі джерела даних, які підлягають моніторингу, такі як брандмауери, системи виявлення вторгнень, засоби захисту

кінцевих точок, системи автентифікації та журнали додатків. Визначте їхні пріоритети на основі їхньої критичності та рівнів ризику.

- Бажані результати: Чітко сформулювати цілі впровадження рішення SIEM, такі як скорочення часу реагування на інциденти, забезпечення відповідності конкретним нормам або пріоритети сценаріїв використання, такі як отримання інформації про поведінку користувачів.

Планування впровадження. Після того, як вимоги встановлені, слід розробити детальний план впровадження. Цей план повинен охоплювати

- Вибір SIEM: Оцініть різні рішення SIEM на ринку на основі таких факторів, як функціональність, масштабованість, простота використання, можливості інтеграції та вартість. Розгляньте можливість проведення перевірки концепції, щоб допомогти прийняти обґрунтоване рішення.
- Масштаб і терміни проекту: Окресліть обсяг проекту впровадження SIEM, включаючи кількість джерел даних, необхідних інтеграцій та налаштувань. Встановіть реалістичний графік з проміжними етапами для кожного етапу проекту.
- Залучення зацікавлених сторін: Залучіть ключові зацікавлені сторони з команд IT, безпеки та комплаєнсу, щоб забезпечити співпрацю, комунікацію та узгодження цілей. Призначте членам команди конкретні ролі та обов'язки.
- План навчання: Розробіть навчальну програму для навчання членів команди ефективному використанню та управлінню системою SIEM. Вона повинна охоплювати такі теми, як системне адміністрування, реагування на інциденти, звітування та усунення несправностей.

Розгортання та огляд. Етап розгортання передбачає встановлення, налаштування та інтеграцію рішення SIEM з IT-інфраструктурою організації. Основні завдання включають

- Встановлення SIEM: Налаштування рішення SIEM шляхом встановлення необхідного програмного або апаратного забезпечення, а також необхідних агентів або роз'ємів на відповідних пристроях.
- Конфігурація: Визначте правила нормалізації даних і кореляції, щоб гарантувати, що події з різних джерел будуть точно проаналізовані і співвіднесені. Створюйте кастомні правила, сповіщення та інформаційні панелі відповідно до потреб вашої організації.
- Політики безпеки та робочі процеси: Розробляйте та впроваджуйте політики безпеки для управління використанням SIEM-системи. Створіть робочі процеси для обробки оповіщень та інцидентів, включаючи процедури ескалації та канали зв'язку.
- Тестування: Проведіть ретельне тестування системи SIEM, щоб перевірити її функціональність, ефективність і точність у виявленні загроз, генеруванні оповіщень і наданні контексту для реагування на інциденти.
- Аналіз і доопрацювання: Зберіть відгуки від зацікавлених сторін і кінцевих користувачів, щоб визначити сфери для вдосконалення. Доопрацюйте конфігурацію системи, правила та оповіщення, щоб усунути будь-які прогалини або проблеми, виявлені під час етапу тестування та аналізу.

Після впровадження. Після розгортання і початкового огляду система SIEM повинна постійно контролюватися, підтримуватися і оптимізуватися. Це включає в себе

- Оновлення політик і правил: Регулярно переглядайте та оновлюйте політики безпеки, правила та оповіщення, щоб забезпечити їхню актуальність та ефективність в умовах еволюції загроз та зміни бізнес-вимог.
- Оптимізація продуктивності: Відстежуйте продуктивність і використання ресурсів SIEM-системи та вносьте необхідні корективи для забезпечення оптимальної ефективності.
- Розвідка загроз: Інтегруйте рішення SIEM із зовнішніми каналами розвідки загроз, щоб бути в курсі останніх загроз, вразливостей і тенденцій.

- Постійне навчання та підтримка: Забезпечте безперервне навчання, документацію та підтримку членів команди, щоб вони могли ефективно керувати та використовувати систему SIEM.
- Періодичні огляди та аудити: Проводьте регулярні огляди та аудити системи SIEM, щоб оцінити її ефективність, відповідність вимогам та узгодженість з потребами організації у сфері безпеки та комплаєнсу. Використовуйте ці висновки для прийняття рішень на основі даних для подальшої оптимізації та вдосконалення. [3]

Основні проблеми при інтеграції SIEM в основних напрямках представлені на рис.1.1

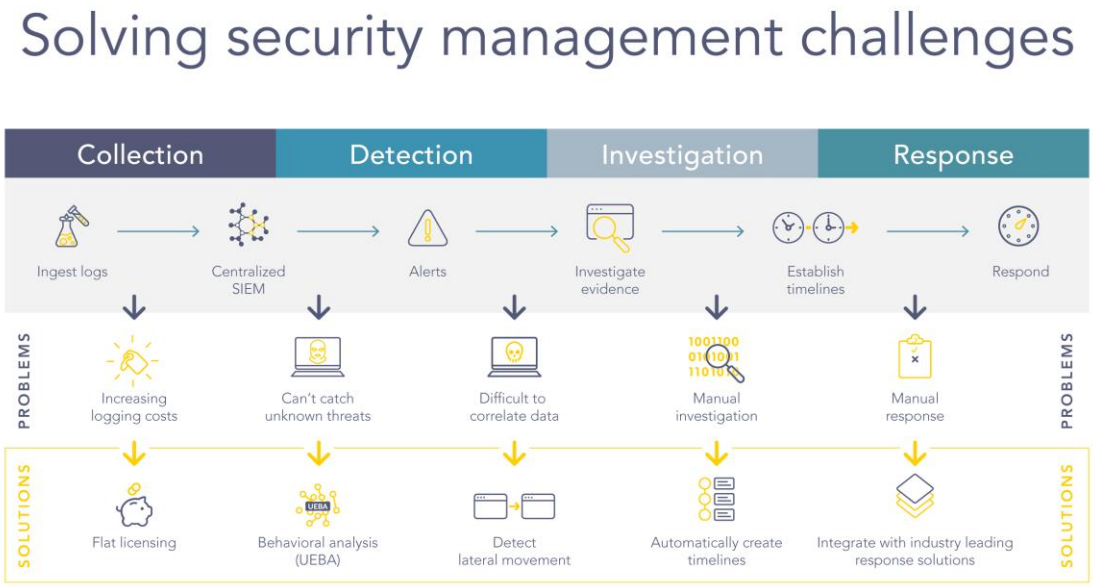

Рис.1.1. Основні проблеми при інтеграції SIEM [20]

1. Складність конфігурації. На етапі впровадження конфігурація SIEM-системи для задоволення конкретних потреб організації може бути дуже складною. Визначення джерел даних для інтеграції, встановлення правил кореляції та точне налаштування порогових значень сповіщень вимагають ретельної уваги до деталей.

Помилки в конфігурації можуть призвести до хибних спрацьовувань або пропущених загроз, що підкреслює важливість кваліфікованого персоналу на

цьому вирішальному етапі. Організації повинні інвестувати час і знання, щоб переконатися, що система SIEM точно налаштована для реагування на їхні унікальні вимоги до кібербезпеки.

2. Перешкоди інтеграції. Інструменти SIEM є компонентами інфраструктури кібербезпеки організації. Їх безперешкодна інтеграція з існуючими інструментами та системами безпеки може стати серйозним викликом. Відсутність сумісності може перешкоджати здатності SIEM надавати цілісне уявлення про події безпеки.

Процес інтеграції включає в себе оцінку існуючої інфраструктури організації, забезпечення безперебійного потоку даних між системами і створення необхідних протоколів для обміну даними. Це кропіткий процес, який вимагає ретельного планування та виконання.

3. Обмеження ресурсів. Впровадження рішень SIEM є ресурсоємним. Воно вимагає значних інвестицій у вигляді часу, грошей і кваліфікованого персоналу. Невеликі організації з обмеженим бюджетом можуть мати труднощі з виділенням необхідних ресурсів для успішного розгортання SIEM.

Цей виклик часто вимагає від організацій визначення пріоритетів своїх потреб у сфері кібербезпеки, зосередження уваги на найбільш важливих сферах в рамках своїх ресурсних обмежень для досягнення ефективного впровадження SIEM.

4. Приховані витрати. Хоча SIEM обіцяє посилення безпеки, приховані витрати можуть з'явитися, коли обсяг даних перевищить очікування.

У міру зростання організацій витрати на обробку і зберігання величезних обсягів даних журналів SIEM можуть застати їх зненацька. Ці приховані витрати можуть вплинути на бюджет і порушити процес впровадження SIEM.

5. Виклики при впровадженні даних. Забезпечення належної інтеграції всіх відповідних джерел даних в систему SIEM може бути значним тягарем при впровадженні. Різні системи і додатки можуть мати різні формати журналів і структури даних, що робить процес нормалізації і стандартизації даних критично важливим завданням.

Без належного введення даних ефективність SIEM у виявленні загроз може бути скомпрометована. Організаціям необхідно розробити стратегії для ефективної інтеграції та управління різноманітними джерелами даних, щоб максимізувати цінність свого рішення SIEM.

6. Обмеження масштабованості. Організаціям, особливо тим, які переживають швидке зростання, потрібні рішення SIEM, які можуть масштабуватися разом з ними. Забезпечення здатності SIEM-системи обробляти зростаючі обсяги даних журналів і подій має вирішальне значення для довгострокового успіху.

У міру того, як ваша організація розширюється, вимоги до SIEM-системи також будуть зростати. Без належної масштабованості SIEM може не встигати за потоком даних, що потенційно може призвести до проблем з продуктивністю та неповного захоплення подій.

Планування масштабованості на етапі впровадження має важливе значення для пристосування до майбутнього зростання і підтримки ефективності системи.

7. Правила зберігання та дотримання нормативних вимог. SIEM-системи генерують величезні обсяги даних, і збереження цих даних для цілей дотримання нормативних вимог і проведення розслідувань може бути складним завданням. Організації повинні знайти баланс між політикою збереження даних і витратами на їх зберігання.

Вимоги нормативно-правових актів часто диктують конкретні періоди зберігання даних, тому важливо, щоб рішення SIEM могло ефективно керувати зберіганням даних.

Впровадження надійних механізмів архівації та очищення даних необхідне для дотримання нормативних вимог та уникнення непотрібних витрат на зберігання. Крім того, організації повинні встановити чіткі політики щодо зберігання та видалення даних, щоб забезпечити відповідність нормативним вимогам.

Поради щодо успішного впровадження SIEM

Щоб забезпечити більш плавне проходження процесу впровадження SIEM і вирішити ці проблеми, розглянемо наступні стратегії:

- Визначте чіткі цілі: Почніть з визначення чітких і конкретних цілей для розгортання SIEM, що допоможе зберегти фокус і уникнути розширення масштабу.
- Інвестуйте в навчання: Виділіть ресурси для забезпечення комплексного навчання вашої команди, включаючи сертифікацію та безперервне навчання, щоб гарантувати, що вони мають необхідні навички для ефективного управління системою SIEM.
- Плануйте масштабованість: При виборі рішення SIEM враховуйте траєкторію зростання вашої організації, щоб переконатися, що воно має масштабованість для обробки зростаючих обсягів даних журналів і подій в міру розширення вашої організації.
- Розробіть політику зберігання даних: Створіть і впровадьте чіткі політики зберігання даних, які відповідають нормативним вимогам вашої організації, впроваджуючи відповідні рішення для архівації та зберігання даних, щоб забезпечити відповідність нормативним вимогам при ефективному управлінні даними.
- Визначте пріоритет інтеграції: Зробіть інтеграцію пріоритетом, переконавшись, що ваше рішення SIEM безперешкодно інтегрується з існуючим набором інструментів безпеки. Ви можете вивчити переваги впровадження уніфікованого рішення для забезпечення безпеки, яке поєднує можливості SIEM з іншими інструментами безпеки для більш раціонального підходу до кібербезпеки.
- Розгляньте керовані послуги SIEM: Дізнайтеся про переваги аутсорсингу управління SIEM у надійного стороннього постачальника керованих послуг безпеки (MSSP) [53]

1.2 Аналіз теоретичної бази щодо впливу SIEM на безпеку даних та інформаційну безпеку організації

У чому цінність і функції SIEM?

Рис. 1.2. Функції SIEM [30]

У більшості організацій SIEM мають 3 важливі функції: (1) виявлення загроз, (2) розслідування та (3) час для реагування. SIEM були розроблені для збору, зберігання, аналізу, розслідування та звітування щодо журналів та інших даних для реагування на інциденти, криміналістики та дотримання нормативних вимог. До появи SIEM журнали та інші дані часто збиралися вручну, а журнали з різних технологій, включаючи сервери, брандмауери, антивіруси, спам-фільтри тощо, потрібно було збирати, нормалізувати та аналізувати.

Навіть у невеликих організаціях може бути понад 300 програмних і апаратних продуктів, що створюють журнали, а на великих підприємствах їх, швидше за все, тисячі. Таким чином, як ви можете собі уявити, це був надзвичайно повільний і монотонний процес, який коштував дорого і був сповнений помилок. Тепер, після отримання та нормалізації журналів, SIEM зазвичай мають можливість аналізувати дані про події в режимі реального часу,

щоб забезпечити раннє виявлення цілеспрямованих атак, складних загроз та витоків даних.

Отже, давайте зведемо це до кількох речень, щоб надати чітке визначення SIEM.

SIEM збирає дані журналів з різноманітного мережевого обладнання та програмного забезпечення і аналізує їх у режимі реального часу. Мета SIEM - співвіднести події та виявити аномалії або моделі поведінки, такі як трафік з підозрілих IP-адрес або незвичне витікання даних, що може свідчити про злом.

Більшість SIEM мають різноманітні функції та можливості, включаючи

1. Базовий моніторинг безпеки - базовий збір, нормалізація, кореляція та аналіз журналів. Це основний обов'язок SIEM.

2. Виявлення інцидентів безпеки - другою основною функцією SIEM є автоматизоване сповіщення команд безпеки про аномалії або порушення політик за допомогою чіткої інформації.

3. Розширене виявлення загроз - SIEM інтегрує канали розвідки, які надають дані про поточні загрози, які SIEM використовує для виявлення загроз.

4. Сповіщення та оповіщення - SIEM можна налаштувати так, щоб оповіщати аналітиків безпеки про порушення політик або виявлення загроз.

5. Криміналістика та реагування на інциденти - SIEM мають можливість зберігати журнали, щоб при виникненні порушення або інциденту команди ІК та цифрові криміналісти могли провести аналіз першопричини.

6. Інформація про відповідність - SIEM все частіше використовуються для демонстрації відповідності, забезпечуючи аудит і звітність щодо даних для входу в систему, інформації про користувачів, IP-адреси та потоку даних.

Як SIEM допомагає в моніторингу та управлінні журналами?

Давайте зробимо крок назад і пройдемося по деякій короткій інформації, яку ми представили в попередній статті блогу під назвою «Моніторинг та управління журналами». Ефективне управління журналами має важливе значення для безпеки організації. Моніторинг, документування та аналіз системних подій є ключовим компонентом IT-безпеки. Програмне забезпечення

для управління журналами або SIEM автоматизує багато процесів, пов’язаних з цим. SIEM виконує дві наступні задачі, які до появи сучасних SIEM виконувалися індивідуально:

- SIM – управління інформацією про безпеку – довгострокове зберігання, а також аналіз і звітність даних журналів. Це було і залишається складним і трудомістким завданням, якщо ви повинні створювати власні з’єднання з IDS/IPS, брандмауерами, DLP-рішеннями, серверами додатків і багатьма іншими ресурсами, що генерують журнали у вашому IT-середовищі. Більшість SIEM сьогодні мають деякі роз’єми з коробки.
- SEM – менеджер подій безпеки – моніторинг в режимі реального часу, кореляція подій, сповіщення та подання консолі. Це ключова перевага SIEM, тому що хороший SIEM перетворює дані в аналітику, а відмінний SIEM, налаштований правильно, перетворює аналітику в візуальні інформаційні панелі, які допомагають аналітикам виявляти аномалії і загрози.

Отже, якщо повернутися до того, про що ми говорили в попередній публікації блогу, SIEM поєднує в собі SIM і SEM і забезпечує аналіз оповіщень про загрози безпеки, що генеруються мережевим обладнанням і додатками, в режимі реального часу. Вони використовують або обробляють наступне:

- Агрегація даних: SIEM агрегує дані з багатьох джерел, включаючи мережу, систему безпеки, сервери, бази даних, додатки. Вони надають можливість консолідувати відстежувані дані, щоб аналітики могли відстежувати і аналізувати дані в «єдиному вікні».
- Кореляція: SIEM шукає спільні атрибути і пов’язує події безпеки між собою, щоб зрозуміти сенс інформації. Технологія надає можливість виконувати різноманітні методи кореляції для інтеграції різних джерел.
- Сповіщення: SIEM налаштовані так, щоб сповіщати аналітиків про такі події, як виявлення вторгнень, контроль доступу або контроль відповідності. SIEM далекі від досконалості, і їх часто звинувачують у тому, що вони неточні і викликають у аналітиків «втому від оповіщення».

- Інформаційні панелі: SIEM надають інформаційні панелі, які дозволяють наносити дані на діаграми і легше виявляти закономірності даних.
- Зберігання: SIEM можуть використовувати зберігання історичних даних, щоб полегшити кореляцію даних з часом і забезпечити зберігання, необхідне для дотримання вимог нормативних вимог.
- Технічний аналіз: Оскільки SIEM можуть зберігати дані, і оскільки порушення зазвичай не виявляються в режимі реального часу, архівні журнали мають вирішальне значення для судового розслідування, щоб провести розтин порушення і зрозуміти його першопричину.

Вигоди та переваги SIEM включають:

1. Допомога зрозуміти загрози безпеці. Очевидно, що причина, по якій компаніям потрібні SIEM-системи для моніторингу журналів і повідомлень про підозрілі події, полягає в тому, що більшість організацій генерують занадто багато даних про події, щоб будь-яка людина змогла розібратися в них. [56]

2. Співвідносити дані для надання IOC. Гаразд, це трохи схоже на перевагу №1, однак, крім простого збору, нормалізації та аналізу журналів, SIEM-системи можуть поглинати канали розвідки загроз, і багато хто зараз інтегрує машинне навчання, щоб зрозуміти, що є справжнім індикатором компрометації (IOC), а що ні. [60]

3. Представлення даних. SIEM мають можливість представляти дані різними способами, в тому числі у вигляді готових звітів і звітів, що налаштовуються. Перевага полягає в тому, що аналітики можуть візуально виявляти тенденції, аномалії, сплески трафіку і багато іншого. Звіти та інформаційні панелі можуть слугувати наріжним каменем для визначення того, де і як заглибитися в будь-яку підозрілу активність.

4. Допомога в дотриманні нормативних вимог. Нарешті, з прийняттям GDPR, CCPA, HIPAA, PCI-DSS та багатьох інших законодавчих актів, SIEM-системи можуть створювати звіти про те, як організації захищають PII, хто і звідки отримує доступ до даних.

Висновок і допомога третьої сторони

На даний момент SIEM - це перевірена технологія, якщо вона правильно розгорнута, впроваджена та налаштована. Однак, початкові витрати, навчання, робоча сила і складність часто є непосильними для команд безпеки. MSSP або постачальники керованих послуг чудово справляються з управлінням SIEM для багатьох організацій. Переваги починаються з можливості орендувати, а не купувати технологію SIEM; величезна економія початкових витрат.

"SIEM-як-послуга", як її зазвичай називають MSSP, також забезпечує безперебійне впровадження і постійне обслуговування, так що аналітики можуть негайно використовувати технологію для захисту організації, її клієнтів і співробітників, замість того, щоб витрачати час на впровадження і розгортання.

Ми трохи заглибилися в розповідь, і, безумовно, в цій статті можна посперечатися про SIEM, в тому числі про витрати і переваги, які були представлені. Ми хотіли б почути ваші відгуки і, звичайно, дякуємо вам за те, що прочитали цю статтю. [12]

Як SIEM знижує ризики?

У сучасному динамічному ландшафті кібербезпеки організації стикаються з безліччю загроз, які можуть скомпрометувати їхні конфіденційні дані та порушити роботу. Щоб ефективно знизити ці ризики, організаціям потрібне комплексне рішення для забезпечення безпеки, яке забезпечує видимість IT-середовища в режимі реального часу і дозволяє проактивно виявляти загрози та реагувати на них. Саме тут в гру вступає управління інформацією та подіями безпеки (SIEM).

Розуміння зниження ризиків за допомогою SIEM:

SIEM слугує життєво важливим компонентом стратегії захисту кібербезпеки організації, дозволяючи ідентифікувати, аналізувати та пом'якшувати потенційні інциденти безпеки.

Агрегуючи та корелюючи дані з різних джерел, таких як мережеві пристрої, сервери, додатки та інструменти безпеки, SIEM дозволяє організаціям отримати цілісне уявлення про своє IT-середовище та виявити підозрілі дії або аномалії, які можуть свідчити про загрозу безпеці.

Проактивне виявлення загроз:

SIEM діє як проактивний механізм захисту, безперервно відстежуючи та аналізуючи події безпеки в режимі реального часу.

Вона використовує інтелектуальні алгоритми і методи машинного навчання для виявлення закономірностей і виявлення потенційних загроз, таких як спроби несанкціонованого доступу, зараження шкідливим програмним забезпеченням або ненормальна поведінка користувачів.

Виявляючи ці загрози на ранній стадії, SIEM дозволяє організаціям швидко реагувати на них, зменшуючи вікно вразливості та мінімізуючи потенційний вплив інцидентів безпеки.

Покращене реагування на інциденти:

На додаток до виявлення загроз, SIEM значно розширює можливості реагування на інциденти.

Коли відбувається інцидент безпеки, SIEM надає цінну інформацію та контекст для тих, хто реагує на інциденти, що дозволяє їм більш ефективно розслідувати та розуміти природу та серйозність інциденту.

Завдяки сповіщенням у режимі реального часу та автоматизованим робочим процесам реагування на інциденти, SIEM допомагає оптимізувати процеси реагування на інциденти, сприяючи швидшому локалізації, пом'якшенню та усуненню наслідків інциденту.

Таке швидке реагування зменшує загальний вплив і тривалість інцидентів безпеки, тим самим мінімізуючи потенційні фінансові та репутаційні збитки.

Покращений комплаєнс та аудит:

SIEM відіграє життєво важливу роль у дотриманні нормативних вимог. Централізуючи та аналізуючи журнали різних систем і додатків, SIEM надає організаціям аудиторський слід, забезпечуючи відповідність галузевим стандартам і нормам.

Це дозволяє організаціям продемонструвати дотримання правил захисту даних, таких як GDPR, HIPAA та PCI DSS, шляхом моніторингу та звітування про події безпеки, дії користувачів та контроль доступу.

Ця можливість не тільки допомагає уникнути потенційних юридичних наслідків, але й підвищує довіру клієнтів та їхню впевненість у прихильності організації до конфіденційності та безпеки даних.

Безперервний моніторинг та розвідка загроз:

SIEM надає організаціям можливості безперервного моніторингу, забезпечуючи проактивну позицію безпеки.

Збираючи та аналізуючи події безпеки в режимі реального часу, SIEM дозволяє організаціям виявляти та оперативно реагувати на нові загрози.

Крім того, SIEM інтегрується із зовнішніми джерелами розвідки загроз, що дозволяє організаціям отримувати доступ до актуальної інформації про нові вектори атак, вразливості та сигнатури шкідливого програмного забезпечення.

Ця інформація про загрози дає організаціям можливість проактивно коригувати свої заходи безпеки та захисту, знижуючи ризик стати жертвою новітніх кіберзагроз. [38]

Висновок до розділу. SIEM відіграє важливу роль у зниженні ризиків і зміцненні загальної системи кібербезпеки організації. Забезпечуючи проактивне виявлення загроз, поліпшені можливості реагування на інциденти, підтримку відповідності нормативним вимогам і доступ до розвідданих про загрози в режимі реального часу, SIEM дозволяє організаціям випереджати кіберзагрози, що розвиваються.

Впровадження SIEM як частини комплексної стратегії кібербезпеки дозволяє організаціям мінімізувати ризики, захистити конфіденційні дані, підтримувати нормативно-правову відповідність та забезпечити безперервність бізнесу. Оскільки кіберзагрози продовжують розвиватися, SIEM залишається найважливішим інструментом зниження ризиків і захисту активів організації.

РОЗДІЛ 2.
АНАЛІЗ ПІДХОДІВ І ПРОЦЕСІВ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

2.1 Аналіз стану системи управління інформаційною безпекою

Стан системи управління інформаційною безпекою аналізуються за стандартами та методологіями згідно яких ця система впроваджувалась

Розглянемо декілька методів впровадження системи управління інформаційною безпекою (СУІБ)

Створення та функціонування СУІБ може відбувається за класичним циклом **PDCA**. PDCA розшифровується як PLAN, DO, CHECK, ACT

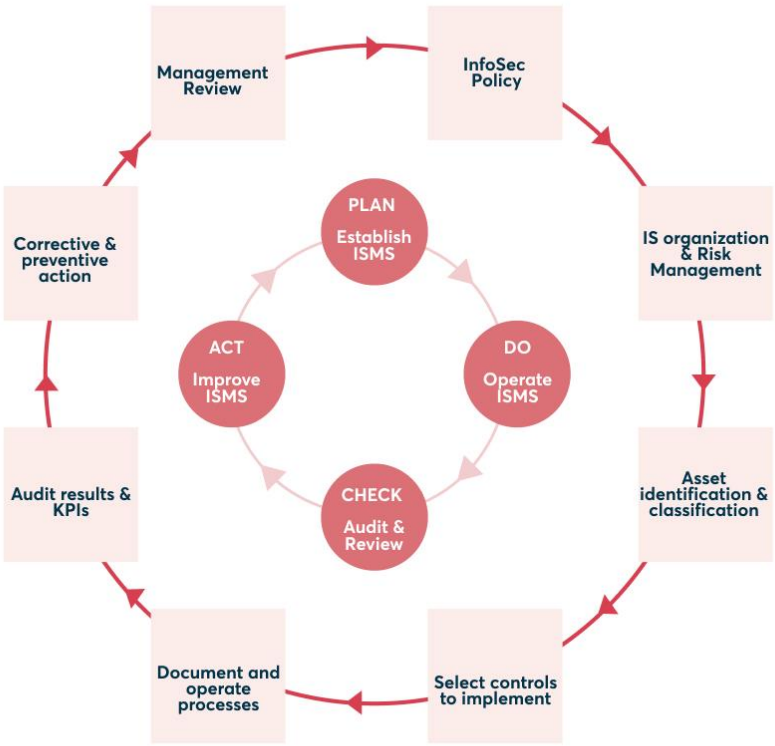

Рис. 2.1. Цикл PDCA [57]

Кроки, які необхідно виконати в деталях, є наступними:

1. Створити політику СУІБ. Чому ми, як компанія, хочемо створити СУІБ? Яких цілей ми розраховуємо досягти за її допомогою? Як ми впроваджуємо таку систему організаційно? Хто бере на себе роль відповідального за інформаційну безпеку (ISO)? Які ресурси він/вона має? Які заходи необхідно вжити?

2. Ідентифікація та класифікація активів. Які активи/інформацію ми хочемо захистити? Наскільки чутливими є ці активи? Приклад з автомобілями: Зображення прототипу автомобіля, який ще не був побудований, потребують набагато більшого захисту, ніж зображення тестової моделі під час дорожніх випробувань, тобто автомобіля незадовго до його виходу на ринок.

3. Створити організаційну структуру СУІБ та структуру управління ризиками. Які інструменти ми хочемо використовувати? Які фінансові та людські ресурси має ISO? Які структури необхідно створити?

4. Розробити механізми контролю. Як ми перевіримо, чи є СУІБ ефективною і чи захищає активи нашої компанії так, як ми хочемо?

5. Впроваджувати СУІБ. Які процеси ми застосовуємо в повсякденному житті? Як ми їх інтегруємо та документуємо?

6. Перевіряйте результати та KPI. Це питання слід ставити регулярно: Яких результатів досягає наша СУІБ та які ключові показники ефективності (КПЕ) ми отримуємо на їх основі?

7. Вносити корективи та вживати запобіжних заходів. В яких сферах нам потрібно вдосконалюватися на основі отриманих результатів? Як ми можемо протидіяти ризикам превентивно?

8. Аналіз з боку керівництва. Чи відповідають цілі та загальна спрямованість СУІБ все ще актуальним, або ж необхідна корекція курсу з боку керівництва? Це слід аналізувати щонайменше раз на рік. [56]

Також можна використовувати рекомендаціїї наведені в ISO 27001

Стандарти ISO 27001, а також ISO 27002 пропонують рекомендації щодо створення СУІБ на основі найкращих практик. Нижче наведено контрольний список найкращих практик, які слід врахувати перед тим, як інвестувати в СУІБ:

- **Розуміння потреб бізнесу**. Перш ніж впроваджувати СУІБ, організаціям важливо отримати уявлення про бізнес-операції, інструменти та системи управління інформаційною безпекою з висоти пташиного польоту, щоб зрозуміти бізнес-вимоги та вимоги до безпеки. Це також допомагає вивчити, як стандарт ISO 27001 може допомогти в захисті даних, і визначити осіб, які відповідатимуть за впровадження СУІБ.
- **Створіть політику інформаційної безпеки.** Наявність політики інформаційної безпеки перед створенням СУІБ є корисною, оскільки вона може допомогти організації виявити слабкі місця політики. Політика безпеки, як правило, повинна надавати загальний огляд поточних засобів контролю безпеки в організації.
- **Контролюйте доступ до даних.** Компанії повинні стежити за своєю політикою контролю доступу, щоб гарантувати, що тільки уповноважені особи отримують доступ до конфіденційної інформації. Цей моніторинг повинен відстежувати, хто, коли і звідки отримує доступ до даних. Окрім моніторингу доступу до даних, компанії також повинні відстежувати входи та автентифікацію і зберігати їх для подальшого розслідування.
- **Проводьте тренінги з підвищення обізнаності про безпеку.** Усі працівники повинні регулярно проходити тренінги з безпеки. Під час тренінгу користувачі повинні ознайомитися з мінливим ландшафтом загроз, типовими вразливостями даних в інформаційних системах, а також методами пом'якшення та запобігання загрозам для захисту даних від компрометації.
- **Захистіть пристрої.** Захистіть усі пристрої організації від фізичного пошкодження та несанкціонованого втручання, вживаючи заходів безпеки для запобігання спробам злому. Такі інструменти, як Google Workspace

та Office 365, мають бути встановлені на всіх пристроях, оскільки вони мають вбудовані засоби захисту пристроїв.

- **Шифруйте дані.** Шифрування запобігає несанкціонованому доступу і є найкращою формою захисту від загроз безпеці. Усі дані організації повинні бути зашифровані перед налаштуванням СУІБ, оскільки це допоможе запобігти будь-яким несанкціонованим спробам саботажу критично важливих даних.
- **Резервне копіювання даних.** Резервне копіювання відіграє ключову роль у запобіганні втрати даних і повинно бути частиною політики безпеки компанії до створення СУІБ. Окрім регулярного резервного копіювання, слід спланувати місце та частоту резервного копіювання. Організації також повинні розробити план забезпечення безпеки резервних копій, який повинен застосовуватися як до локальних, так і до хмарних резервних копій.
- **Провести внутрішній аудит безпеки.** Перед впровадженням СУІБ слід провести внутрішній аудит безпеки. Внутрішній аудит - це чудовий спосіб для організацій отримати контроль над своїми системами безпеки, програмним забезпеченням та пристроями, оскільки він дозволяє виявити та виправити прогалини в безпеці до впровадження СУІБ. [60, 27]

ISO 27001 можна назвати золотим стандартом для систем управління інформаційною безпекою. Інші стандарти, такі як згадані нижче, можуть розглядатися залежно від галузі, ринку та національного законодавства.

Cyber Essentials Scheme - Програма Cyber Essentials Scheme, запроваджена Національним центром кібербезпеки Великобританії, є ефективною схемою, що підтримується урядом і допомагає захистити вашу організацію від низки найпоширеніших кібератак.

Стандарт NIST - Стандарт NIST (Національний інститут стандартів і технологій) 800-53 є важливим для співпраці з державними інформаційними системами США. Загалом, керівництво NIST надає набір стандартів для

рекомендованих засобів контролю безпеки для інформаційних систем у федеральних агентствах. [6, 31, 1]

SOC 1 і SOC 2 - міжнародні стандарти контролю організації обслуговування SOC 1 і SOC 2 також можуть мати відношення до фінансової звітності компанії. Звіти SOC 1 зосереджені на контролі фінансової звітності, тоді як звіти SOC 2 зосереджені на операційному контролі та контролі за дотриманням законодавства в сервісних організаціях. [8, 9]

CPPA - Каліфорнійський закон про конфіденційність споживачів (CCPA) захищає конфіденційність жителів Каліфорнії. Індивідуальні дані, такі як активність в Інтернеті, файли cookie, IP-адреси та біометричні дані, регулюються CCPA, так само як і "побутові дані", зібрані пристроями Інтернету речей у будинку, наприклад. Відповідно до CCPA, споживачі мають право знати, які персональні дані збираються або продаються і з якою метою, а також на розкриття інформації про минулі транзакції, починаючи з 1 січня 2019 року. (дата прийняття закону). [9]

HIPAA - Правила конфіденційності HIPAA захищають медичні записи та іншу особисту інформацію. Він поширюється на плани медичного страхування, інформаційні центри та постачальників, які здійснюють електронні транзакції. Правило встановлює обмеження та умови щодо використання та розкриття захищеної медичної інформації без згоди особи.

LGPD - LGPD, Загальний закон про захист даних Бразилії, є реакцією країни на Загальний регламент про захист даних ЄС (GDPR). В принципі, LGPD зобов'язує вас обробляти персональні дані бразильських громадян лише для законних, точних, чітких і задекларованих цілей. [56, 19]

2.2 Вибір та впровадження SIEM-рішення

В цьому розділі слід розглянути лідерів на ринку SIEM рішень. Однією з лідерів у сфері інформаційних технологій на ринку є провідна світова дослідницька і консалтингова компанія Gartner .

Магічний квадрант Gartner для управління інформацією та подіями безпеки (SIEM) преставленні на рис.2.2.

Рис. 2.2. Магічний квадрант Gartner для управління інформацією та подіями безпеки (SIEM) 2022 [28]

Рис. 2.3. Компанії представлені в магічному квадранті

Компаніями-вендорами SIEM рішень [див.рис. 2.3] згідно цього магічного квадрату є:

Devo. Компанія Devo є претендентом у цьому магічному квадранті. Її SIEM-продукт, додаток Security Operations, поставляється як SaaS-пропозиція. Клієнтська база SIEM Devo в основному знаходиться в Північній Америці, за нею йдуть Європа і Близький Схід, і складається з малих, середніх і корпоративних організацій. На початку 2022 року Devo отримала статус "в процесі" за стандартом Федеральної програми управління ризиками та авторизацією (FedRAMP) і планує досягти повної авторизації пізніше в цьому році. Ліцензування, включаючи додаткові можливості (TIP через MISP, гаряче зберігання, Entity Analytics і Devo Flow), базується на обсязі даних, що надходять.

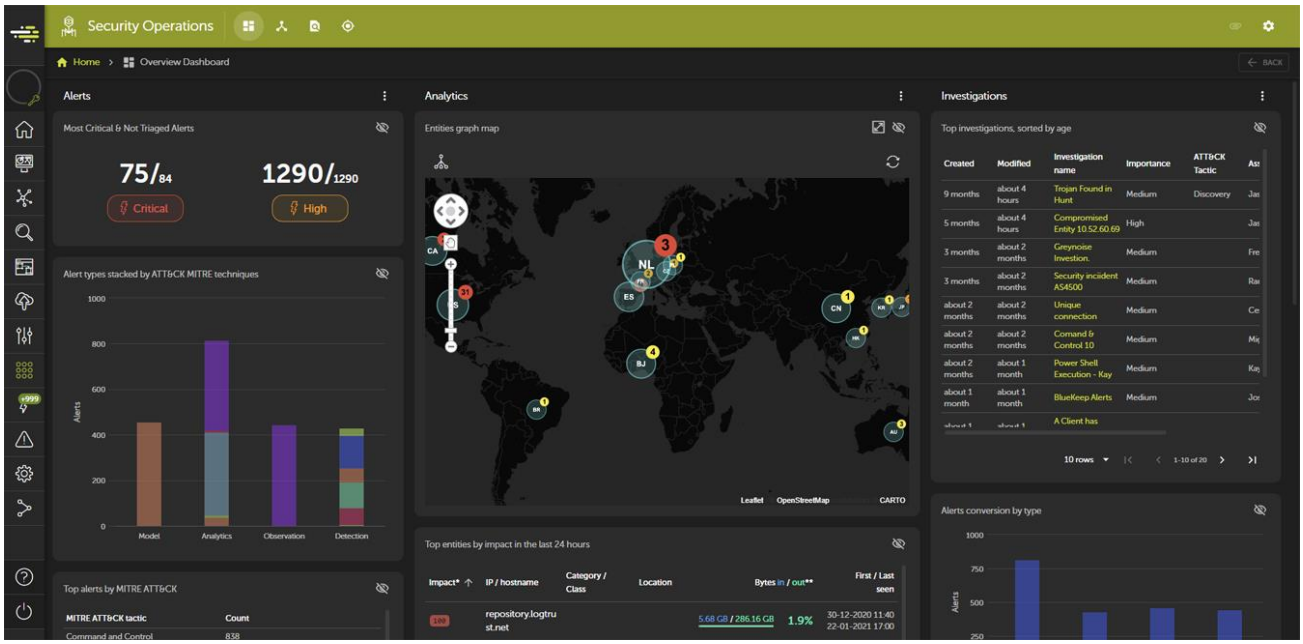

Рис. 2.4. Security Operations [52]

Сильні сторони

- IT-спостережливість у поєднанні з безпекою: Devo надає можливості IT-спостереження та безпеки в одному інтерфейсі і забезпечує чіткі часові рамки, а також суміжні подання для спільної роботи команд безпеки та IT-відділу.
- Доступність даних: Інструмент SIEM від Devo дозволяє користувачам швидко і легко відправляти дані в рішення через його API в будь-який момент, коли всі ці дані індексуються. Таким чином, клієнти можуть отримати доступ до даних будь-коли і будь-де і використовувати їх так, як їм потрібно.
- Вбудовані функції TIP: Devo надає функцію TIP через MISP без додаткової плати, яка використовує безліч загальнодоступних каналів і надсилає дані до інструменту SIEM для збагачення та покращення виявлення.

Застереження

- Бракує власної функціональності SOAR: Рішення SIEM від Devo інтегрується з багатьма відомими постачальниками SOAR на ринку; однак, в даний час воно не пропонує компоненти реагування SOAR.

- Обмежена видимість на ринку SIEM: Незважаючи на те, що Devo збільшила свої продажі і розширила маркетингові кампанії, вона не настільки відома на ринку SIEM, як деякі з її конкурентів.
- Обмежена підтримка служби безпеки: Зовнішня підтримка SIEM-рішення Devo від постачальників MSSP/MDR обмежена в порівнянні з іншими постачальниками SIEM на ринку. Клієнти, які потребують керованих або спільно керованих послуг SIEM, повинні переконатися, що обраний ними постачальник може підтримувати SIEM Devo і створювати додатковий користувацький контент для поліпшення правил, що надаються Devo.[52]

Elastic. Компанія Elastic є провидцем у цьому магічному квадранті. Її рішення Elastic Security в основному зосереджене на аналітиці безпеки та функціях корпоративного пошуку в поєднанні з агентом безпеки Elastic Endpoint, який входить до складу рішення SIEM. Більшість клієнтів Elastic Security знаходяться в Північній Америці та Європі, з рівним співвідношенням малих, середніх і корпоративних клієнтів. Приріст нових клієнтів наразі вищий серед малих організацій. У 2021 році Elastic завершила придбання компанії Cmd і build security, щоб запропонувати функціональність платформи захисту хмарних робочих навантажень в рамках Elastic Agent, що входить до складу Elastic Security. Ліцензування базується на хмарних ресурсах, таких як обчислювальні потужності та сховища для підтримки клієнтського середовища.

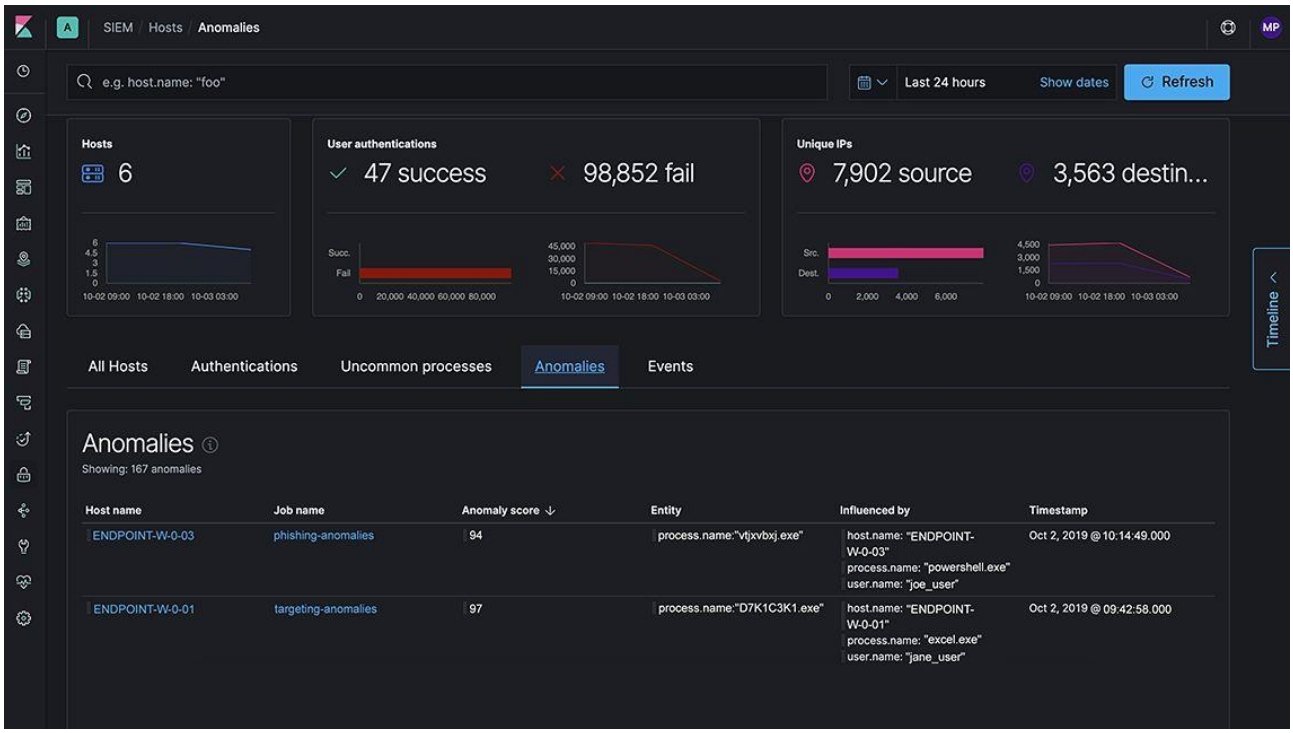

Рис. 2.5. Elastic Security [18]

Переваги

- Кастомізована візуалізація: Elastic відомий своїми інформаційними панелями, що легко налаштовуються, і створенням преференційних представлень даних для цілей аналізу. Користувачі можуть використовувати комбіновану IT-функцію спостереження та безпеки в одному поданні для унікальних часових шкал та суміжних видів активності.
- Функції пошуку: Elastic Security використовує свої популярні можливості пошуку і мову запитів, яка також використовується в якості внутрішньої системи пошуку і запитів іншими постачальниками SIEM, щоб полегшити завдання операцій з безпеки, такі як полювання на загрози. Здатність Elastic аналізувати та індексувати практично будь-яку частину журналу дає операторам безпеки необмежені можливості для пошуку та фрагментації будь-яких даних, які були проіндексовані.
- Інтеграція для спільної роботи та сповіщень: Elastic використовує Дії та Коннектори для інтеграції з різними інструментами спільної роботи, системами продажу квитків та інструментами сповіщень. Покупці, які шукають

SIEM, що може інтегруватися з обраним ними інструментом для спільної роботи з інцидентами, побачать, що Elastic Security підтримує інтеграцію з багатьма популярними рішеннями сторонніх розробників.

Застереження

- Власні сучасні функції SIEM: Elastic Security не пропонує вбудований SOAR у своєму рішенні SIEM, покладаючись на партнерську інтеграцію з іншими постачальниками SOAR і пропонуючи деякі дії реагування за допомогою Elastic Agent. У рішенні відсутня функція TIP, яка з'являється у все більшій кількості конкуруючих рішень.
- Підтримка сторонніх EDR: Elastic Security підтримує збір даних від основних постачальників EDR. Однак двонаправлену підтримку постачальників EDR, що не належать до Elastic, необхідно налаштовувати за допомогою стандартного REST-коннектора Elastic.
- Звітність про відповідність вимогам: Elastic Security не пропонує підтримку сповіщень та звітів про відповідність стандартам. Покупцям потрібно буде знайти альтернативні рішення для звітування про відповідність стандартам.[18]

Exabeam. Exabeam є лідером у цьому магічному квадранті. Рішення SaaS SIEM від Exabeam, відоме як Exabeam Fusion SIEM, доступне як основний продукт або в комплекті з корпоративними версіями. Ці продукти також доступні для гібридної хмари. Корпоративна версія включає в себе Advanced Analytics, Threat Hunter, Entity Analytics і Case Manager. Додаткове хмарне сховище даних (Cloud Archive) і система реагування на інциденти (SOAR) доступні як доповнення. Більшість клієнтів Exabeam знаходяться в Північній Америці, з наступною за величиною концентрацією в Європі. Більшість клієнтів є великими підприємствами, проте кількість клієнтів середнього та малого бізнесу зростає. Ліцензування є строковим і залежить від обсягів поглинутих даних.

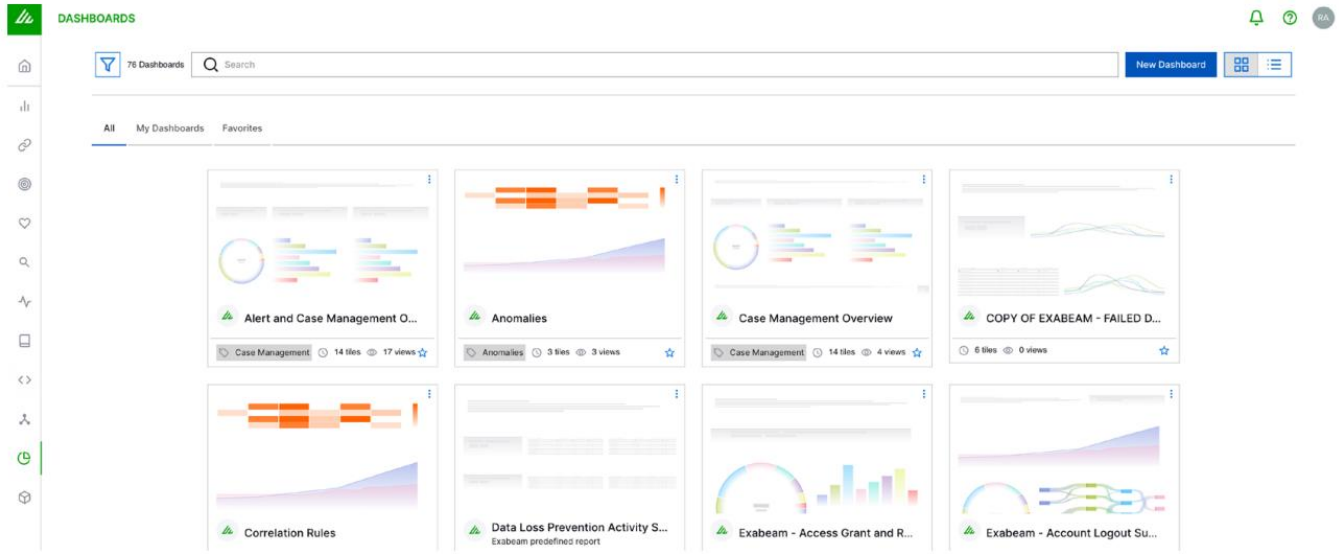

Рис. 2.6. Exabeam Fusion SIEM [43]

Сильні сторони

- Довгострокове зберігання журналів з можливістю пошуку: Поєднання хмарного архіву Exabeam (для зберігання даних до 10 років), пошуку за нормалізованими подіями, аномаліями, індикаторами компрометації та часовою шкалою подій журналу з автоматизованим збагаченням дозволяє здійснювати пошук і розслідування, підтримуючи багатий контекст протягом тривалих періодів часу.
- Доступ до даних третіх сторін в реальному часі: Exabeam Fusion SIEM здатний відображати і обробляти дані в реальному часі від сторонніх систем (наприклад, потоки даних про загрози), що дозволяє SIEM працювати більш децентралізовано для певних сценаріїв використання. Децентралізація даних забезпечує більш економічно ефективне розгортання з більш актуальними даними, що, як очікується, буде ключовим трендом для SIEM протягом наступних 18 місяців.
- Ефективна пріоритизація оповіщень: Динамічний скоринг дозволяє клієнтам виявляти важливі виявлення з оповіщень сторонніх розробників (на додаток до власних оповіщень Exabeam), використовуючи контекстуалізацію та аналітичні моделі в режимі реального часу. Це дозволяє аналітикам безпеки

отримати пріоритетне уявлення про всі оповіщення, що генеруються в усьому стеку технологій безпеки.

Застереження

- Відсутність власних компонентів екосистеми: Exabeam покладається на сторонні EDR і NDR. Відсутність власних можливостей відстає від деяких конкурентів на ринку і знижує здатність реагувати на загрози без додаткових інвестицій в сумісні набори інструментів.
- Заплутані повідомлення щодо Fusion XDR та Fusion SIEM: Exabeam у своєму маркетингу охоплює два ринкові сегменти, а відсутність узгодженості в назвах продуктів та їх функціональності викликає суперечки у кінцевих користувачів.
- Тривалий час адаптації: Для налаштування Exabeam SIEM потрібна більша кількість днів професійних послуг, ніж для інших SaaS SIEM на ринку. Це збільшує вартість і складність для кінцевих користувачів. Доступно багато "пакетів" професійних послуг.[43]

Fortinet. Компанія Fortinet є претендентом у цьому магічному квадранті. Її SIEM-рішення - FortiSIEM. Воно має глобальну присутність і клієнтів у всіх основних регіонах світу, але особливо в Північній Америці та Європі. Цей продукт включає в себе розширені агенти (для UEBA на базі Windows). FortiSIEM інтегрується з FortiSOAR, FortiAnalyzer та іншими елементами набору продуктів безпеки Fortinet. Ціна базується на пристроях для SOAR, EPS та кількості агентів для SIEM. FortiSIEM доступний у вигляді віртуального або фізичного пристрою. Ліцензування базується на пристроях, пов'язаних з 10 подіями в секунду на пристрій. Доступні безстрокові та передплачені ліцензії.

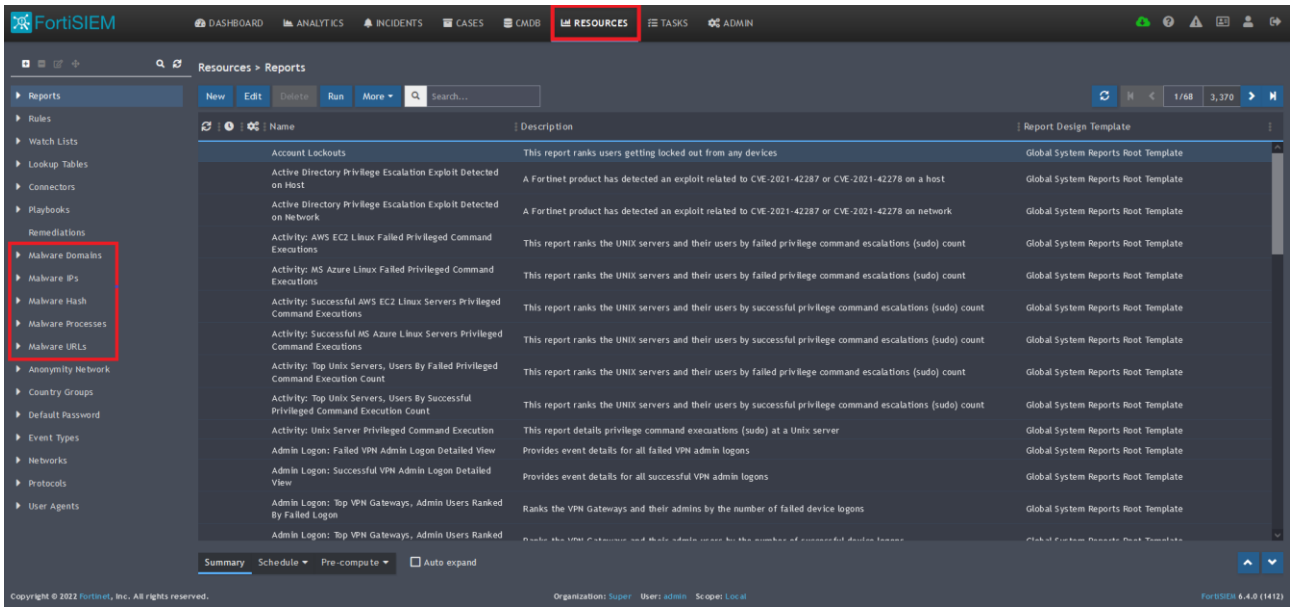

Рис. 2.7. FortiSIEM [44]

Сильні сторони

- Підтримка постачальників послуг і складних організацій: Fortinet FortiSIEM пропонує вбудовану багатокористувацьку підтримку для складних організацій і постачальників послуг, а також різноманітні функції, характерні для них. Він також пропонує модель на основі споживання для керованих постачальників послуг безпеки (MSSP) з необмеженим EPS.
- Вбудовані можливості видимості активів: Fortinet FortiSIEM має потужні засоби виявлення активів і вбудовану базу даних управління конфігурацією (CMDB). Це забезпечує централізовану видимість активів, виявлених за допомогою активного сканування і пасивної перевірки журналів.
- Інтеграція з більш широкою екосистемою Fortinet: Fortinet пропонує різноманітну екосистему продуктів для забезпечення безпеки та мережевих продуктів, інтегрованих за допомогою Fortinet Security Fabric. Потенційні та існуючі клієнти Fortinet, які шукають єдиного постачальника рішень для моніторингу, виявлення та реагування на загрози, повинні звернути увагу на Fortinet.

Застереження

- Відсутність прямої стратегії "як послуга": Fortinet покладається на партнерів, які пропонують послуги хостингу для FortiSIEM як засіб надання покупцям послуг, подібних до SaaS. Кінцеві користувачі можуть розгорнути рішення у власній публічній або приватній хмарі, або у вигляді гібридної хмарної моделі.
- Обмежене покриття для моніторингу хмарних середовищ: Покриття хмарної безпеки FortiSIEM не таке широке, як у інших конкурентів. Йому не вистачає підтримки декількох служб інфраструктури та платформ публічної хмари (CIPS), а єдиними підтримуваними брокерами безпеки хмарного доступу (CASB) є власний продукт Fortinet FortiCASB і Oracle CASB.
- Опції аналітики поведінки користувачів та організацій: UEBA доступний у двох варіантах: преміум-пропозиція та більш обмежена версія для FortiSIEM. Обидва варіанти вимагають розгортання агента і не мають функцій, які доступні у конкурентів, наприклад, можливість створювати динамічні однорангові групи. Однак, дорожня карта Fortinet вказує на те, що ці прогалини будуть усунені.[44]

Gurucul. Gurucul - провидець у цьому магічному квадранті. Її SIEM називається Analytics-Driven SIEM і являє собою модульне рішення, широко орієнтоване на SIEM, UEBA, аналітику ідентичності, аналітику шахрайства, SOAR і аналіз мережевого трафіку. Gurucul пропонує пакетні можливості TDIR через свою Платформу аналітики безпеки та операцій. Компанія присутня на ринку переважно в Північній Америці, а її клієнтський профіль в переважній більшості базується на великих корпоративних організаціях. Gurucul має надійну дорожню карту, що охоплює інтеграцію з соціальними мережами, інтеграцію з оцінкою стану безпеки, а також покращену інтеграцію з аналітикою загроз та послугами захисту від цифрових ризиків. Ліцензування базується на відстежуваних активах і доступне як передплата або безстрокове.

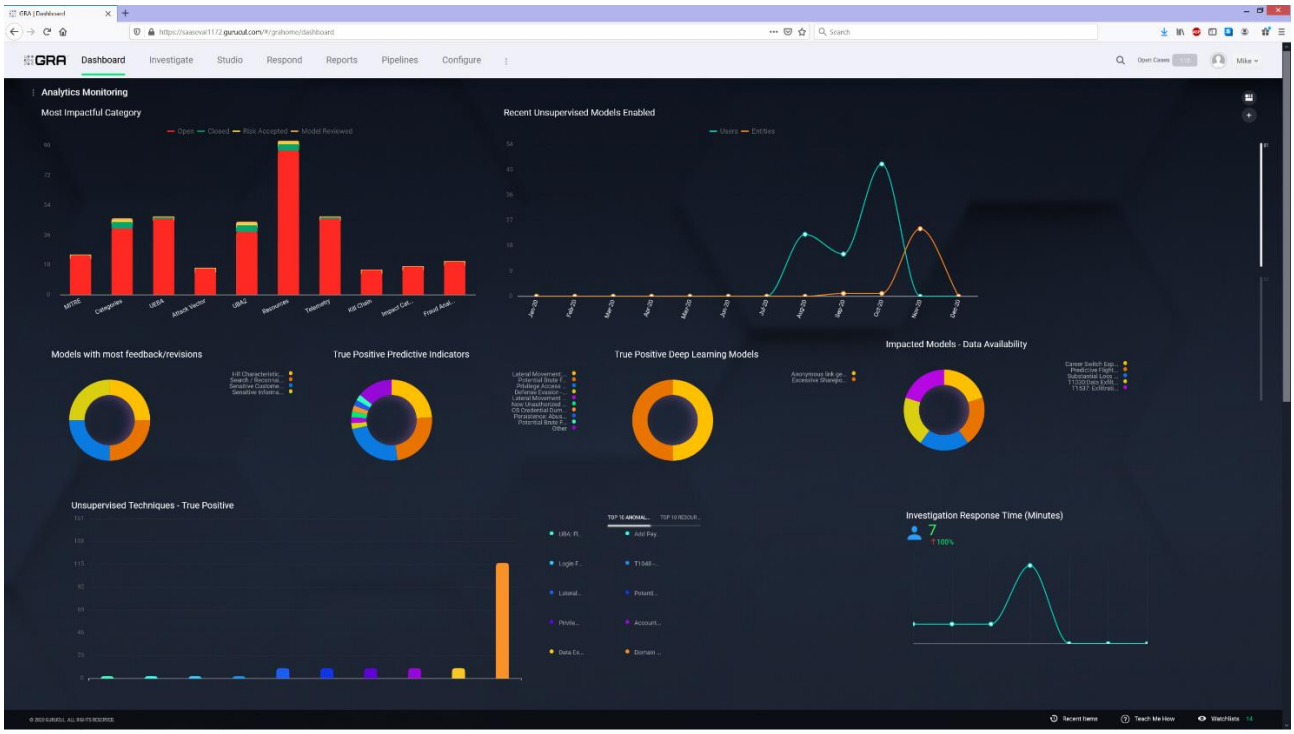

Рис. 2.8. Analytics-Driven SIEM [32]

Сильні сторони

- Підтримка архітектури та озер даних: Gurucul підтримує модель озера даних та/або сховища, що дозволяє уникнути необхідності реплікації даних в інше сховище для забезпечення безпеки. Gurucul пропонує широкий спектр варіантів архітектури для підтримки SaaS і моделей, що розгортаються клієнтом.
- Спільні моделі машинного навчання та контент про загрози: Відкриті виявлення в бібліотеці виявлення загроз Gurucul доступні всім користувачам для зворотного зв'язку та обміну, що дозволяє налаштовувати і ділитися ідеями щодо варіацій алгоритмів і контенту загроз для модифікації виявлених загроз.
- Прогнозоване ціноутворення: Gurucul встановлює ціни на свої рішення на основі активів, що зменшує занепокоєння щодо надмірного обсягу або швидкості передачі даних, а також не має обмежень на зберігання даних. Він пропонує модульну структуру, що дозволяє покупцям вибирати лише ті функції, які їм потрібні для їхнього конкретного середовища.

Застереження

- Обмежені функції розвідки загроз: Gurucul не пропонує таку саму платформу/функції управління аналітикою загроз, як деякі конкуренти. Покупці, яким потрібні функції розвідки загроз (наприклад, аналіз посилань, створення власних тегів та управління індикаторами), не знайдуть цих функцій у Gurucul.
- Присутність на ринку та реалізація: Gurucul залишається відносно невідомим на ринку SIEM, незважаючи на посилені маркетингові зусилля. Покупці SIEM часто не знайомі з Gurucul або його рішеннями, а також відчувається нестача керованих служб безпеки, які підтримують спільно керовані розгортання Gurucul в порівнянні з іншими постачальниками SIEM.
- Орієнтація на велике середовище: Переважна більшість клієнтів Gurucul - це великі підприємства, які часто мають великі і зрілі команди безпеки, необхідні для використання складних SIEM, таких як SIEM, керовані аналітикою. Gurucul пропонує багатогранне рішення, що вимагає більш просунутого досвіду аналізу даних і операцій з безпеки.

Huawei. Huawei є нішевим гравцем у цьому магічному квадранті. Її SIEM-рішення називається HiSec Insight і включає в себе Huawei Cloud Security Brain. Існує безліч додаткових модулів і супутніх технологій для специфічних вимог до функцій або архітектури. Клієнти SIEM в основному зосереджені в Китаї, хоча менша кількість клієнтів знаходиться на Близькому Сході, в Африці та Латинській Америці. Клієнтська база компанії майже рівномірно розподілена між великими та середніми підприємствами, але є й невеликі клієнти. Ціни на локальні розгортання базуються на швидкості передачі даних (EPS) та обсязі (гігабайти на день), з додатковою оплатою за зберігання журналів та додаткові модулі. Розгортання SaaS базується на кількості придбаних еластичних хмарних серверів.

Переваги

- Поведінкова аналітика: Аналітика є сферою інвестицій компанії Huawei. Її аналітика поведінки користувачів забезпечує динамічне виявлення на основі однорангових груп. Рейтинг ризиків для організацій на основі машинного

навчання відображає такі фактори, як вартість активів, пов'язані з ними виявлення на основі правил і дані про вразливості.

- Широка екосистема продуктів: Huawei пропонує низку інтегрованих можливостей, включаючи виявлення та реагування на мережеві загрози, ізольоване середовище, обман, аналіз поведінки користувачів, оркестровку та реагування, а також розвідку загроз.
- Гнучкість щодо форм-факторів: Продукти Huawei доступні в різних форм-факторах, які можна комбінувати за потреби. До них відносяться програмне забезпечення, фізичні та віртуальні пристрої. Також є варіанти розміщення в публічній або приватній хмарній інфраструктурі Huawei.

Застереження

- Обмежена підтримка моніторингу хмарної інфраструктури: Моніторинг хмарних інфраструктур обмежений власною хмарою Huawei. Жодні інші хмарні сервіси не підтримуються з коробки.
- Відсутність підтримки моніторингу SaaS: Моніторинг популярних SaaS-додатків "з коробки" не передбачений. Платформа Huawei не має інтеграції з Microsoft 365, Google Workspace або додатками Workday, Salesforce чи Box.
- Обмежена доступність: зосередженість Huawei на Китаї, ринках, що розвиваються в Азії та Тихоокеанському регіоні, а також на Близькому Сході та Африці означає, що її продукт мало доступний для покупців SIEM в інших країнах. Huawei не має найближчих планів щодо виходу на ринки Північної Америки та Європи.[32]

IBM. IBM є лідером у цьому магічному квадранті. Її продукт IBM QRadar може бути розгорнутий за допомогою локального програмного забезпечення, в публічній/приватній хмарі або гібридній хмарі, або поставлятися в хмарному форматі як QRadar on Cloud (QROC). Клієнтська база SIEM IBM охоплює Північну Америку, Європу, Азійсько-Тихоокеанський регіон, Близький Схід та Латинську Америку, більшість з них - середні та корпоративні клієнти. На додаток до QRadar, IBM пропонує інші продукти для забезпечення безпеки, такі як QRadar Network Insights, QRadar Vulnerability Manager, QRadar XDR Connect,

QRadar SOAR (формально Resilient) і Cloud Pak for Security (CP4S). Ліцензування QRadar SIEM базується на кількості подій в секунду (EPS) та/або потоків в хвилину (FPM). Необмежене серверне ліцензування є альтернативним варіантом тільки для хмарних екземплярів.

Рис. 2.9. IBM QRadar [23]

Переваги

- Потужна аналітика та кастомізація: QRadar має велику кількість готового контенту та аналітичних можливостей. Клієнти також надали позитивні відгуки про здатність QRadar створювати і налаштовувати додатки та інформаційні панелі.
- Великий бізнес у сфері безпеки та присутність: IBM має глобальну присутність (через прямі та партнерські канали), необхідну для надання своїх продуктів, підтримки та послуг у кожному великому географічному регіоні. Крім того, компанія має достатню кількість співробітників, які розуміють специфічні регіональні норми та розмовляють кількома мовами, щоб підтримувати індивідуальні проекти та конфігурації.
- Різноманітні пропозиції продуктів для забезпечення безпеки: IBM пропонує широкий спектр додаткових і тісно інтегрованих додаткових

технологій, а також послуг, які доповнюють і підтримують QRadar. До них відносяться мережева безпека, управління вразливостями, розвідка загроз, захист даних, послуги UEBA, SOAR і MSSs/MDR.

Застереження

- Правила кореляції та аналітика є аналогічними: QROC не робить різниці між правилами кореляції та аналітикою; отже, існують різні ступені складності, від простих до просунутих, щодо нестандартного контенту, що ускладнює порівняння.
- Cloud Pak уповільнює інновації SIEM: Інновації в QRadar SIEM були повільними, оскільки IBM переносить ресурси на платформу Cloud Pak for Security і можливості безпеки наступного покоління.
- Реалізації потребують вдосконалення: Судячи з відгуків, клієнти повідомляють, що початкове розгортання може бути складним процесом. Йому також може бракувати гнучкості з точки зору підключення нових джерел даних.[23]

Logpoint. Logpoint є нішевим гравцем у цьому магічному квадранті. Її SIEM-рішення поєднується з функціоналом SOAR і переважно використовується клієнтами у форматі SaaS або хмарних сервісів. Найбільша концентрація покупців - це малі та середні компанії, що базуються в Європі. Logpoint має помітну пропозицію для моніторингу та реагування на загрози для платформ SAP. Ліцензування базується на кількості "вузлів", за якими здійснюється моніторинг. Компонент SOAR вимірюється за кількістю користувачів, а ліцензія на одного користувача входить до складу продукту SIEM. Можливості UEBA ліцензуються окремо.

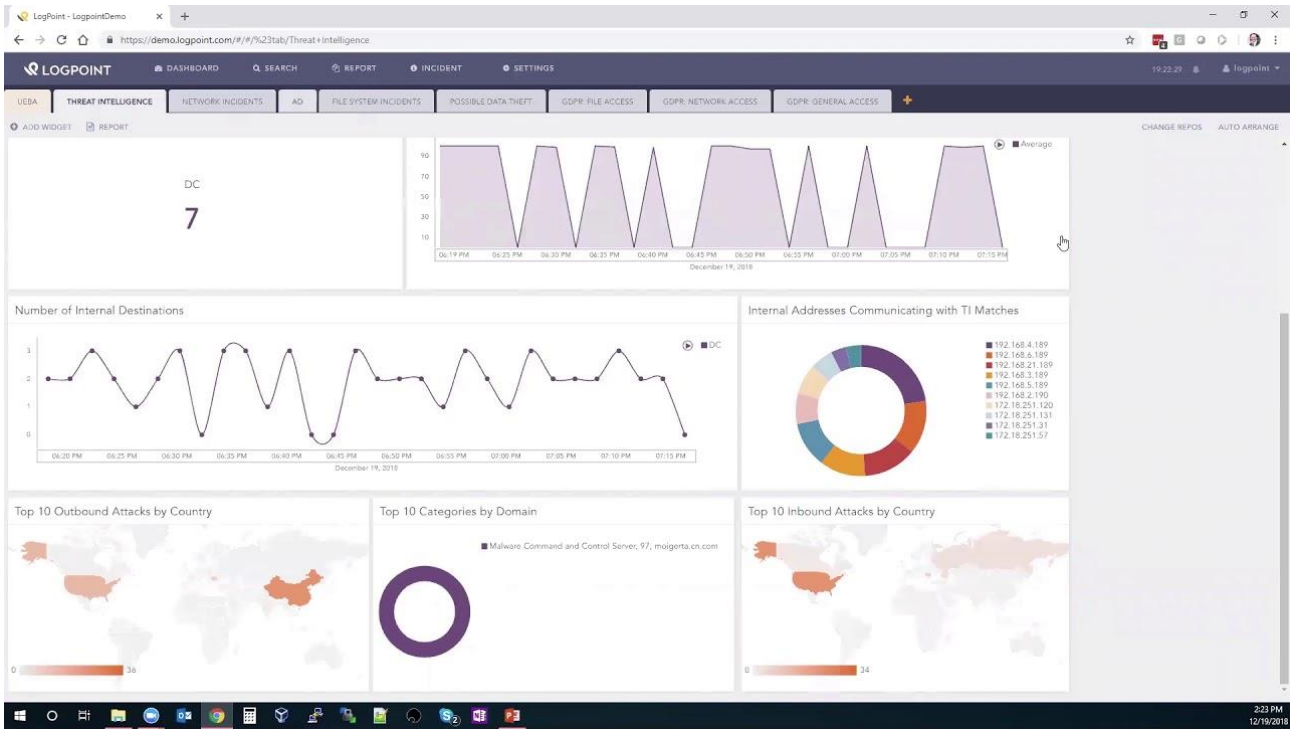

Рис. 2.10. Logpoint [58]

Сильні сторони

- Просте, зрозуміле ціноутворення: Logpoint пропонує модель ціноутворення, яка є однією з найпростіших для розуміння на ринку. Багаторівневе ціноутворення, засноване на кількості "вузлів" (або активів), що надсилають журнали до рішення, доступне для основного елемента SIEM продукту, в той час як комплектний SOAR оцінюється за кількістю користувачів (однокористувацька ліцензія включена до продукту SIEM).
- Моніторинг сторонніх SaaS додатків: Акцент на сторонніх SaaS-платформах, безумовно, є частиною стратегії Logpoint, зі значними можливостями для SAP і Salesforce, а також хорошою підтримкою Microsoft 365. Також доступні інтеграції для сервісів Amazon S3 і ServiceNow.
- Підтримка сервісів: Пропозиція Logpoint SIEM + SOAR включає в себе додаткові сервісні пропозиції для підтримки оперативного моніторингу SIEM, а також проектування і розробки сценаріїв SOAR. Вони доступні за додаткову плату за підписку безпосередньо в Logpoint.

Застереження

- Відсутня функція самостійного створення UEBA: Logpoint підтримує ряд наборів інструментів, які мають можливість надавати аналітичний контент, і хоча доступна велика кількість готових аналітичних даних, досвідчені користувачі не зможуть самостійно створювати нові аналітичні дані про поведінку користувачів і організацій.
- Єдина модель ціноутворення сховища SaaS SIEM: Logpoint включає 90 днів індексованого зберігання логів у своєму SaaS-продукті. Наступні 90 днів "холодного" зберігання є платними, і покупці, які потребують більш тривалих періодів зберігання, повинні купувати з кроком в 90 днів. Потенційні покупці повинні запитати про вартість більш тривалого зберігання. Доступне вивантаження на сторонні склади.
- Орієнтований на Європу: Logpoint переважно обслуговує клієнтів в одному регіоні - Європі. Продажі в Північній Америці очевидні, а інфраструктура і сили продажів присутні в регіоні і зростають. Покупці повинні переконатися в тому, що вони можуть розраховувати на необхідний рівень міжнародної підтримки. [58]

LogRhythm. LogRhythm - претендент у цьому магічному квадранті. Її SIEM-рішенням є LogRhythm SIEM Platform, яка включає в себе кілька додаткових компонентів для надання аналітики кінцевих точок, мережі та поведінки користувачів. Переважна більшість клієнтів SIEM знаходяться в Північній Америці та Європі, решта - в Азійсько-Тихоокеанському регіоні, на Близькому Сході, в Африці та Латинській Америці. Клієнтська база компанії орієнтована на підприємства середнього та малого бізнесу, хоча великі підприємства також придбали LogRhythm SIEM. Існує хмарний варіант, але більшість клієнтів розгорнули SIEM локально. Ліцензування доступне на безстроковій основі (з оплатою за середню кількість повідомлень в секунду або в день) або на основі підписки (з оплатою за кількістю співробітників).

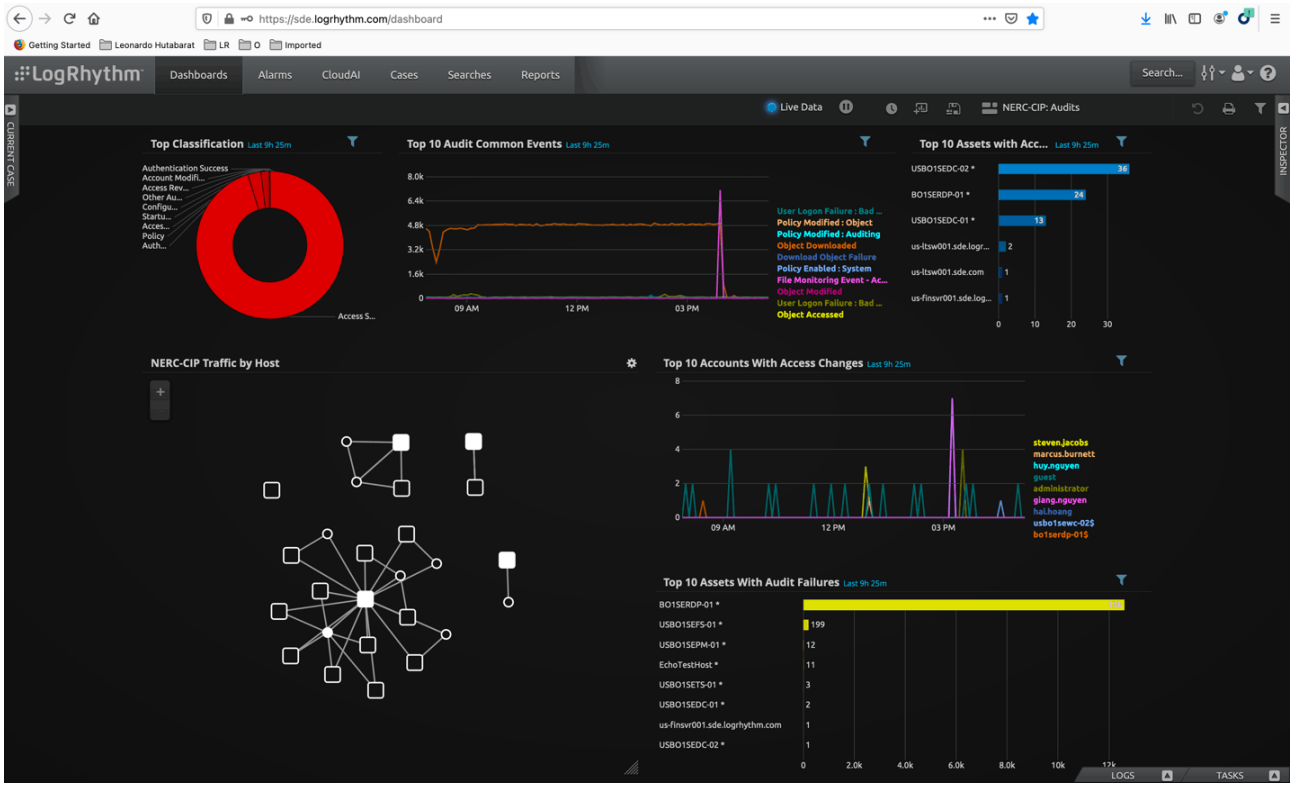

Рис. 2.11. LogRhythm SIEM Platform [42]

Переваги

- Широка мережа реселерів: LogRhythm має сильну команду партнерів-реселерів у кожному великому регіоні світу. Ця сильна сторона віддзеркалюється широкою підтримкою з боку постачальників керованих послуг, які допомагають покупцям зі скромними ресурсами керувати та контролювати SIEM.
- Пілотні варіанти та варіанти перевірки концепції (POC): Покупці можуть скористатися кількома типами пілотних програм і програм перевірки концепції, починаючи від підготовчих семінарів і закінчуючи хостинговими тест-драйвовими вправами на основі сценаріїв і опціями "спробуй і купи".
- Розслідування та управління справами: LogRhythm надає зрілі та вдосконалені можливості розслідування та управління справами, які збирають контекст і дозволяють користувачам створювати доказову базу для вирішення справи.

Застереження

- Обмежені хмарні можливості: Нещодавні придбання LogRhythm і дорожня карта продукту демонструють прогрес у ранній розробці можливостей SaaS SIEM, але в цьому відношенні постачальник відстає від багатьох конкурентів. Хмарна пропозиція SIEM надає розділені інтерфейси, що вимагають від користувачів перемикання між двома середовищами. Функції адміністрування використовують застарілу консоль адміністрування LogRhythm для створення парсерів і правил, а також для управління каналами розвідки загроз. Інтерфейс інформаційної панелі та сповіщень більш наближений до того, що користувачі вважають хмарним.
- Магазин додатків є складним: Магазин додатків LogRhythms пропонується в рамках застарілого додатку База знань адміністративної консолі. Він має лише базові функції і не схожий на сучасний магазин додатків SaaS, де користувачі можуть використовувати ключові інтеграції API, щоб легко підключати точкові рішення або джерела даних (як у випадку з конкуруючими рішеннями).
- Перехід до хмари: Перед LogRhythm стоїть завдання розробити нову хмарну SIEM і представити її можливості покупцям, одночасно підтримуючи свою застарілу SIEM і виконуючи свої плани з міграції клієнтів на нову архітектуру SaaS. [42]

ManageEngine. ManageEngine є нішевим гравцем у цьому магічному квадранті. Її рішення Log360 SIEM є хмарним і розгорнуте у власному центрі обробки даних Zoho Corporation. Основними покупцями Log360 є середні та корпоративні клієнти, переважно з Північної Америки, Європи, Близького Сходу та Азійсько-Тихоокеанського регіону. На додаток до інструменту SIEM, Log360 включає інші продукти безпеки, такі як Firewall Analyzer, EventlLog Analyzer, ADAudit Plus, Vulnerability Manager Plus, Cloud Security Plus, DataSecurity Plus і FileAnalysis. Ліцензування SaaS базується на обсязі даних, що зберігаються в хмарі протягом певного періоду. Ліцензування локальної версії базується на кількості джерел журналів. Сюди входять такі пристрої, як робочі станції, сервери Windows та інші мережеві пристрої. Такі можливості, як аналіз

поведінки користувачів і організацій (UEBA), розширений аналіз загроз і аудит додатків, доступні як доповнення.

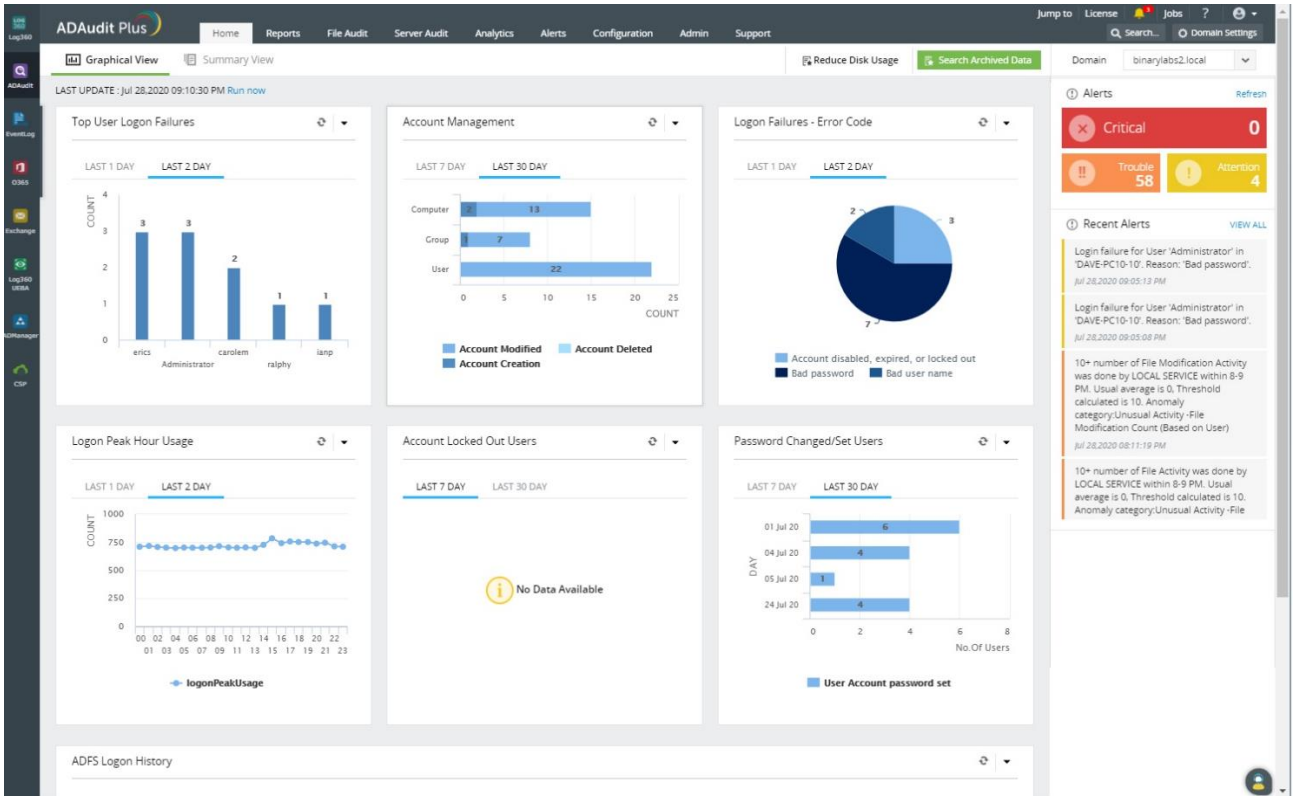

Рис. 2.12. Log360 SIEM [39]

Сильні сторони

- Можливості хмарної безпеки: ManageEngine тепер пропонує можливості CASB, до яких можна отримати доступ через Log360 Cloud. Це забезпечує збагачення рішення Log360 SIEM, а також можливість виявляти несанкціоновані хмарні додатки і зупиняти використання будь-яких заборонених додатків.
- Простота впровадження та експлуатації: Відгуки експертів Gartner про здатність ManageEngine легко розгортати і використовувати SIEM-інструмент в цілому позитивні.
- Вбудовані функції конфіденційності та захисту даних: ManageEngine надає можливості шифрування, маскування та приховування даних, які відповідають вимогам щодо конфіденційності та захисту даних Загального регламенту про захист даних (GDPR).

Застереження

- Бракує розширених можливостей: ManageEngine не має більш розширених можливостей, які, швидше за все, будуть потрібні більш зрілим організаціям, таких як розширена аналітика (наприклад, контрольований ML і аналітика глибокого навчання) і власний SOAR.
- Обмежена інтеграція зі сторонніми рішеннями: Продукт Log360 від ManageEngine має обмежену двосторонню інтеграцію зі сторонніми інструментами безпеки, такими як EDR, NDR і SOAR.
- Обмеження користувацького інтерфейсу: Хоча Log360 підтримує інтеграцію з провідними інструментами ITSM і має власну функцію чату, він не відображає інформацію зі сторонніх систем і не може обмінюватися контентом (наприклад, звітами) між користувачами. [39]

Micro Focus. Micro Focus є провидцем у цьому магічному квадранті. Її продукт ArcSight в основному зосереджений на функціональності SIEM, UEBA, SOAR і TIP. Операції ArcSight географічно диверсифіковані (за винятком Латинської Америки), а клієнтський профіль компанії - переважно середній бізнес. Локальні розгортання значно переважають хмарні, що значною мірою пов'язано з нещодавньою появою хмарної опції. Micro Focus інвестувала значні кошти в портфель продуктів безпеки CyberRes, який включає в себе захист даних, управління доступом до ідентифікаційних даних (IAM), безпеку додатків і операцій безпеки. Першим основним продуктом з портфоліо CyberRes є Galaxy, хмарне рішення для розвідки загроз, яке інтегрується з робочим процесом ArcSight. Ліцензування базується на EPS для SIEM та на організацію для UEBA.

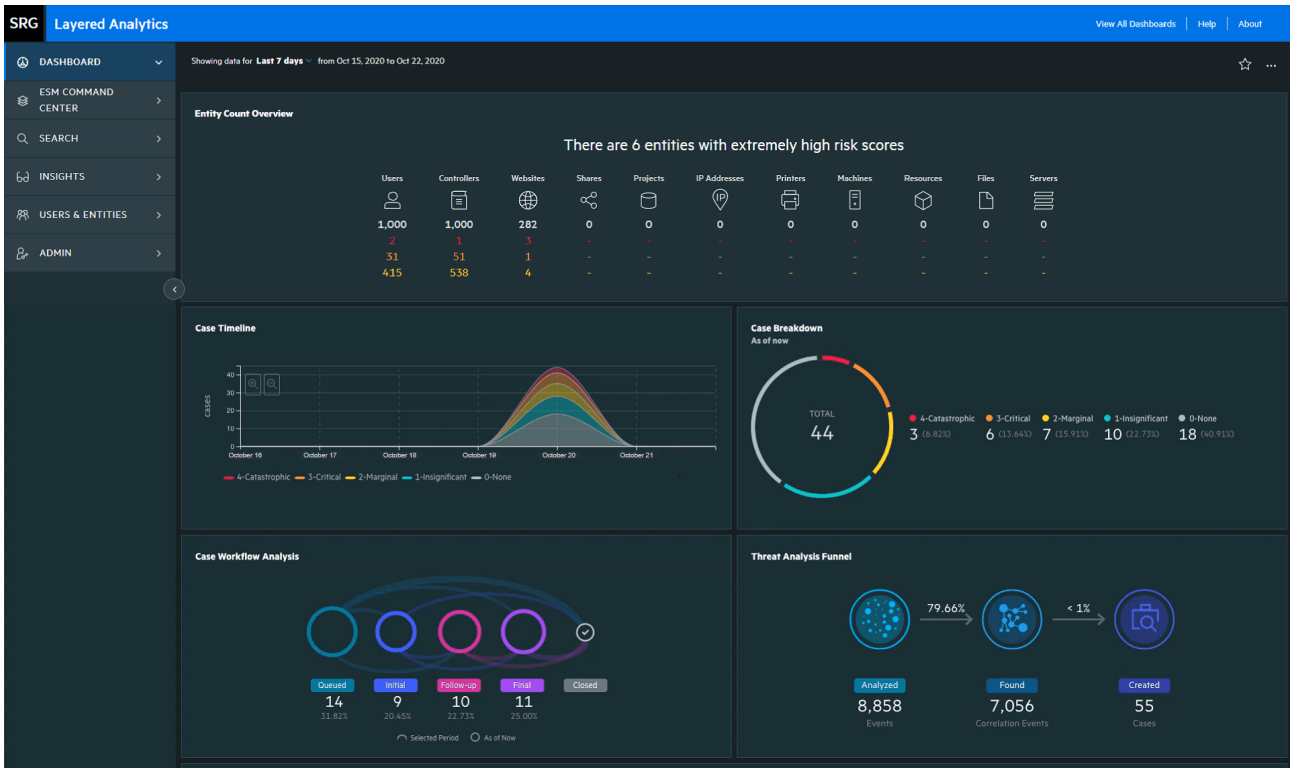

Рис. 2.13. ArcSight [41]

Сильні сторони

- Платформа розвідки загроз (TIP): Базове рішення Galaxy Threat Acceleration Plus (GTAP) Basic TIP входить до складу ArcSight SIEM. Воно надає аналітику з відкритим вихідним кодом MISP всім покупцям ArcSight без додаткових витрат і може бути оновлене до версії GTAP Plus, яка надає преміум-канали аналітики загроз CyberRes. Це рішення SaaS TIP забезпечує графічне представлення та аналіз зв'язків між показниками.
- SOAR входить до складу SIEM: ArcSight SIEM включає SOAR без додаткової плати, але поки що це не функція на основі SaaS. Користувачі можуть використовувати графічне полотно для створення робочих процесів з безліччю варіантів конфігурації, представлених у вигляді випадаючих списків. Інженери з автоматизації також можуть використовувати інтерфейс розробки на основі коду для створення більш складних сценаріїв. Всі автоматизовані дії реагування записуються в файл управління справами.
- ArcSight Fusion UI: Fusion UI надає оновлений інтерфейс з відчуттям SaaS, що свідчить про відхід від історичного консольного інтерфейсу ArcSight.

Fusion забезпечує сучасні часові рамки і графічне представлення даних, щоб показати шаблони активності користувача або організації. Аналітики можуть використовувати повзунок для фільтрації подій на основі ризиків, щоб звузити активність в розслідуванні.

Застереження

- Розділений інтерфейс між ArcSight Console і SaaS: Користувачі виявлять, що все ще існує потреба звертатися до функціонального, але застарілого інтерфейсу ArcSight Console для управління, навіть в архітектурі SaaS. FlexConnector, Quick Flex, FlexAgent, Correlation Condition Editor (CCE) - це приклади, де все ще потрібна стара консоль ArcSight, а не оновлений інтерфейс Fusion UI.
- Налаштування/створення аналітики вимагає зовнішніх інструментів: ArcSight не надає користувацького інтерфейсу для підтримки власних моделей машинного навчання. Замість цього користувачі використовують сторонні інструменти науки про дані (такі як SPSS, SAS або R) для експорту моделей у стандартному форматі PMML. Потім ці моделі можна імпортувати в ArcSight. Хоча це знімає тягар необхідності вивчення специфічного для ArcSight аналітичного інтерфейсу і робочого процесу, використання зовнішніх інструментів може бути не настільки інтуїтивно зрозумілим або зручним для деяких покупців.
- Варіанти перегляду пов'язаних подій: Micro Focus продемонструвала лише два варіанти перегляду подій, пов'язаних з виявленим інцидентом в ArcSight. Основний метод - через власний інтерфейс управління інцидентами (SOAR) ArcSight, а другий - через завантаження PDF-файлу. Деякі покупці можуть захотіти отримати додаткові опції, які допоможуть у розслідуванні інцидентів. Покупцям доведеться звернутися до Micro Focus за додатковими рекомендаціями та опціями. [41]

Корпорація Майкрософт. Microsoft є лідером у цьому магічному квадранті. Її продукт SIEM, Microsoft Sentinel, постачається лише як SaaS через центри обробки даних Microsoft Azure. Microsoft має велику і різноманітну

клієнтську базу, обслуговуючи як великих, так і малих клієнтів, і пропонуючи SIEM-продукт в різних умовах на міжнародному рівні. Ліцензування ґрунтується на обсязі отриманих даних, зарезервованих потужностях або оплаті за фактом. Однак багато корпоративних рівнів Microsoft для Microsoft 365 включають кредит на використання Sentinel і Defender. Розширене сховище даних, додаткові можливості екосистеми Microsoft (наприклад, Defender для кінцевих точок і Defender для Інтернету речей) доступні за додаткову плату.

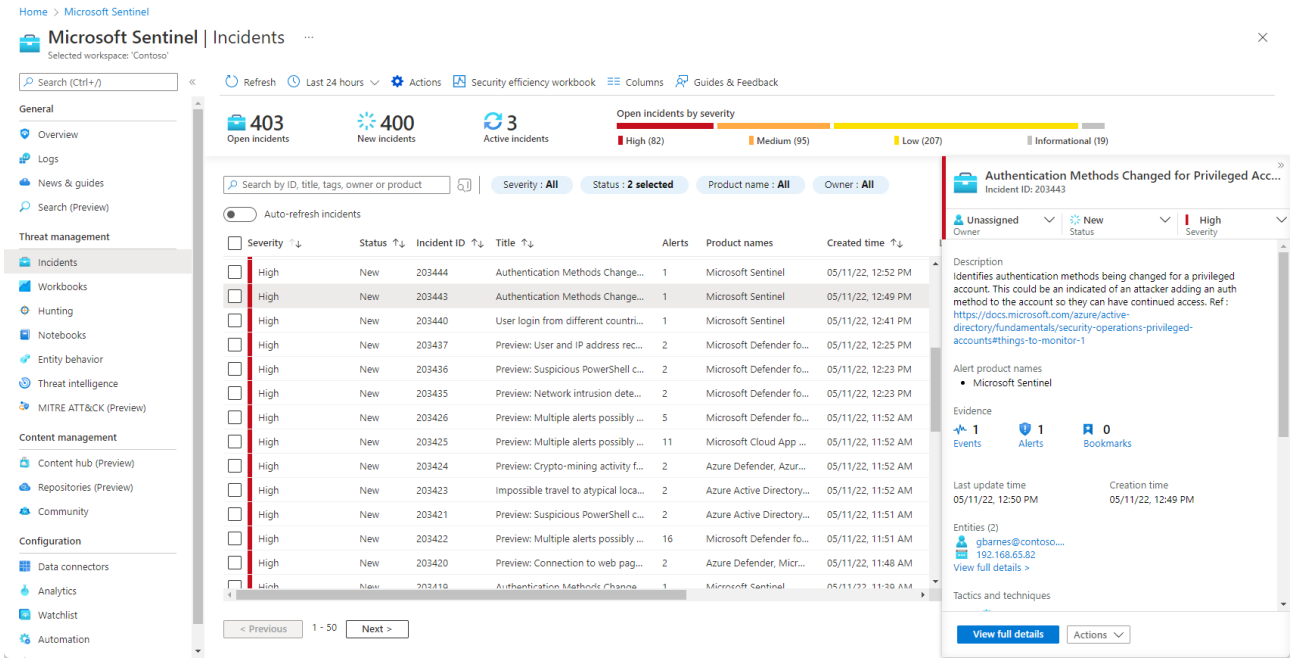

Рис. 2.14. Microsoft Sentinel [17]

Переваги

- Багата екосистема високоінтегрованих продуктів для захисту: Корпорація Майкрософт пропонує велику кількість високоінтегрованих екосистемних продуктів у таких сферах, як CASB, ідентичність, безпека кінцевих точок, мережі та OT. Крім того, ряд її традиційних IT-можливостей мають двосторонню інтеграцію. Покупці, які інвестують в широкий набір продуктів Microsoft - як безпекових, так і не безпекових - можуть розраховувати на відмінну видимість безпеки на всій своїй території.
- Швидко розвивається дорожня карта: Клієнти, які інвестують у Microsoft Sentinel, вже спостерігають значне та постійне збільшення

функціональності, зручності використання та зростання спільнот кінцевих користувачів протягом періоду інвестування.

- Багаторівневі та гібридні операції: Можливість послідовно налаштовувати, керувати та контролювати кілька об'єднаних екземплярів Sentinel за допомогою функції "Lighthouse" приносить користь як користувачам зі складними середовищами, так і тим, хто використовує Sentinel і бажає перейти на модель керованих послуг або безпосередньо з Microsoft, або з одним із зростаючої кількості партнерів з керованих послуг, представлених на ринку.

Застереження

- Важко зрозуміти справжню вартість: Хоча в ціноутворенні використовується проста модель поглинання даних і є варіанти оплати за фактом використання, клієнти повідомляють, що ціна непередбачувана і складна для розуміння в поєднанні з іншими ліцензіями Microsoft. Покупці, які розглядають Sentinel, повинні враховувати вартість переміщення даних з локальних і сторонніх хмарних активів, а також ціну SIEM.
- Можливість непрямої прив'язки до постачальника: Інтеграцію продуктів Microsoft в Sentinel легко реалізувати, однак, складно порівняти власну функціональність і ціни Microsoft з інтеграціями сторонніх розробників. Покупці повинні ретельно планувати вибір інструментів SOC і переконатися, що їхня залежність від одного постачальника не вплине на їхню здатність досягати поставлених цілей.
- Обмежена кількість готового контенту: У порівнянні з багатьма іншими продуктами SIEM, в Sentinel відсутні деякі нестандартні функції, в тому числі звітність про дотримання нормативних вимог. Однак клієнти мають гнучкість у створенні власного аналітичного контенту, що є менш поширеним на ринку. Оцінюючи справжню вартість, покупці повинні враховувати додаткові витрати на професійні послуги, необхідні для забезпечення їхніх потреб.[17]

Rapid7. Компанія Rapid7 є претендентом на перемогу в цьому магічному квадранті. Її SIEM-рішення InsightIDR працює на хмарній платформі Insight. Інші доступні продукти включають InsightVM (управління вразливостями),

InsightAppSec, InsightConnect (SOAR), InsightCloudSec (управління хмарною безпекою) і Threat Command (аналіз загроз). Клієнти InsightIDR SIEM в основному зосереджені в США, за ними йдуть Європа та АТР. Ліцензування базується на строковій ліцензії з простою моделлю ціноутворення, яка базується на кількості активів, що контролюються.

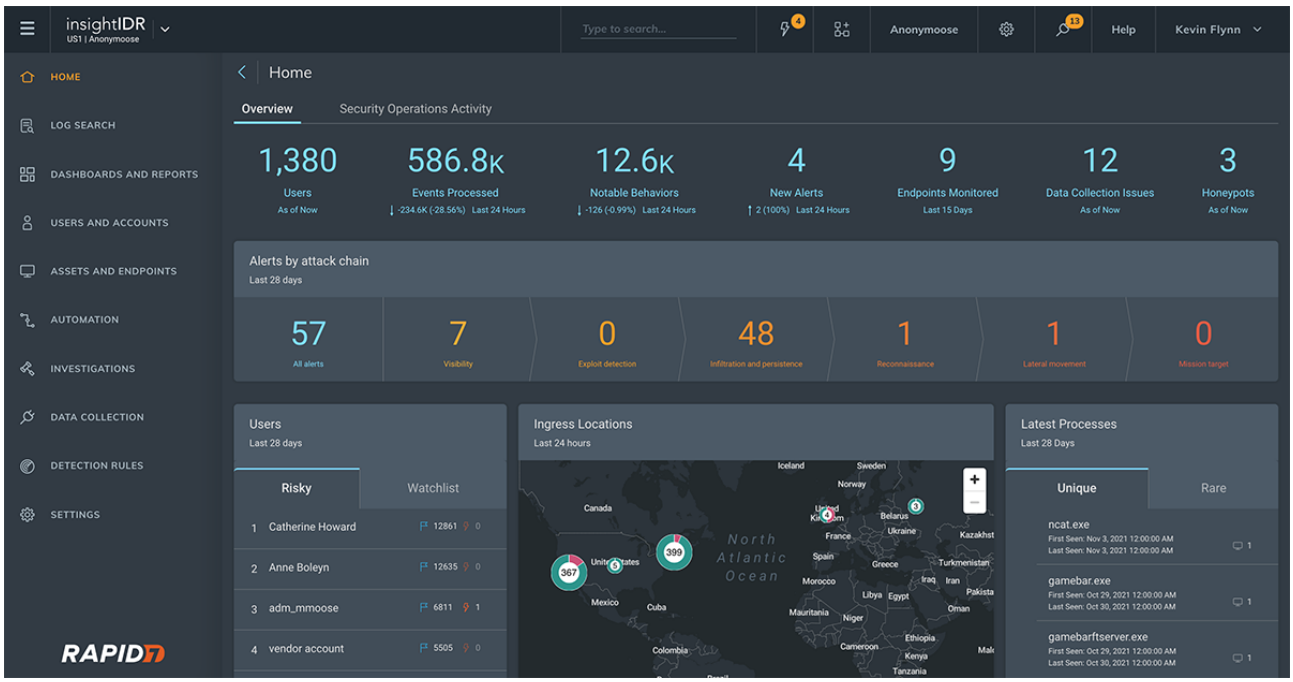

Рис. 2.15. InsightIDR [26]

Сильні сторони

- Широкий спектр інтегрованих можливостей: Rapid7 пропонує базову SIEM з безліччю функцій безпеки, включаючи InsightVM, яка пропонує управління вразливостями; і InsightIDR, яка має можливості EDR, UEBA і NDR. Всі ці можливості тісно інтегровані одна з одною для забезпечення єдиного досвіду для операторів SOC.
- Економічна ефективність: Rapid7 є одним з найбільш економічно ефективних рішень, оцінених в рамках цього дослідження, з середньою ціною на його основний SaaS SIEM, набагато нижчою, ніж в середньому на ринку.
- Керована служба виявлення та реагування: Ця послуга доступна безпосередньо від Rapid7 за додаткову плату. Це єдине джерело для клієнтів, які

хочуть отримати доступ до продукту SIEM і потребують сервісної підтримки для моніторингу та розслідування.

Застереження

- Немає сумісності зі сторонніми сховищами даних: Продукт SIEM від Rapid7 практично не підтримує виклик даних зі сторонніх сховищ. Це може призвести до додаткових витрат і посилення регуляторних вимог. Покупці з великими вимогами до зберігання даних або специфічними потребами щодо регіонального розміщення даних повинні переконатися, що Rapid7 може задовольнити їхні вимоги в цих областях.
- Підтримка інтеграції сторонніх систем автоматизації: Rapid7 не має комерційно доступних інтеграцій для сторонніх SOAR/платформ автоматизації. Покупці, які вже інвестували в ці інструменти, повинні врахувати накладні витрати на підтримку інтеграції або спільного використання продуктів як частини свого набору технологій для операцій з безпеки.
- Відсутність підтримки приховування даних: Рішення Rapid7 не може підтримувати обфускацію даних, а це означає, що дані, які зберігаються на платформі, можуть не відповідати деяким стандартам конфіденційності або локальним вимогам відповідності. Покупець повинен звернутися до професійних сервісних команд Rapid7 - або, можливо, до сторонніх рішень - якщо у нього є потреба в затушовуванні даних журналів. [26]

Securonix. Securonix є лідером у цьому магічному квадранті. Її SIEM-рішення Next-Gen SIEM включає в себе Next-Gen SIEM, Security Data Lake, UEBA, SOAR, NDR, аналітику загроз, аналітику поведінки супротивника і кілька спеціальних додатків (наприклад, для охорони здоров'я і SAP). Більшість клієнтів Securonix знаходяться в Північній Америці, далі йдуть Європа, Азія/Тихоокеанський регіон, Близький Схід і Африка, а також Латинська Америка. Клієнтами компанії є переважно великі підприємства, але її продукти також приваблюють деяких клієнтів середнього розміру. Менших клієнтів здебільшого обслуговують партнери з керованого обслуговування. Ліцензування

базується на ідентифікації та EPS. Більшість покупців обирають строкові ліцензії, але доступні й безстрокові ліцензії.

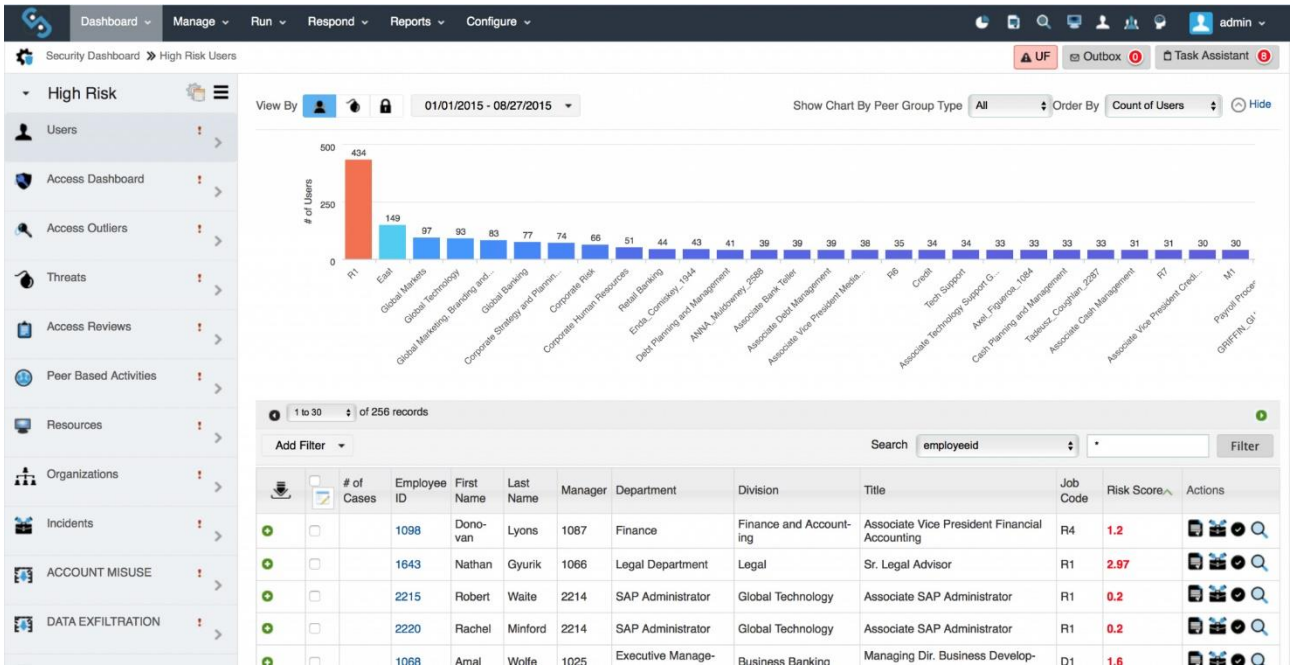

Рис. 2.16. Securonix Next-Gen SIEM [55]

Переваги

- Доступ до сторонніх озер даних: Securonix SIEM може запитувати і відображати дані в реальному часі зі сторонніх систем, таких як озера даних, що дозволяє платформі працювати більш децентралізовано. Децентралізація даних забезпечує більш економічно ефективне розгортання з більш актуальними даними і, як очікується, стане ключовим трендом для SIEM протягом наступних 18 місяців.
- Включно з доступом до аналітики загроз: Securonix надає набір інтеграцій з розвідкою загроз для додаткового збагачення без додаткової оплати. Компанія публікує цю інформацію у відкритому доступі для використання.
- Розслідування та управління справами: Securonix надає вдосконалені можливості для розслідування та управління справами, які збирають контекст і надають доступ до контексту і співпраці в рамках платформи.

Застереження

- Перекриття в маркетингових повідомленнях Open XDR і Next-Gen SIEM: Securonix охоплює два ринкових сегменти в своєму маркетингу, тому переконайтеся, що ви розумієте, що вам потрібно від продукту, коли купуєте його.
- Нетрадиційні моделі ціноутворення: Securonix використовує модель, яка враховує як прибуток на акцію, так і індивідуальність. Користувачі повинні оцінити вимоги до EPS, щоб уникнути несподіваного збільшення вартості. Користувачі можуть зіткнутися з непослідовністю та непередбачуваністю необхідної кількості подій, а отже, і вартості.
- Додатковий пакет аналітики: Securonix пропонує комплексний набір преміум-додатків для аналітики, які оплачуються окремо для кожного користувача і окремо для кожного додатка. При оцінці вам необхідно розуміти, які можливості аналітичного додатку вже включені, а які необхідно додати для правильної оцінки. Хоча вартість придбання всієї функціональності подібна до вартості однієї аналітичної надбудови від інших постачальників SIEM, складно порівнювати пропозиції, порівнювати з ринком і планувати, які можливості необхідні. [55]

Splunk. Splunk є лідером у цьому магічному квадранті. Його SIEM - це Enterprise Security (Splunk ES) і є доповненням до рішення Splunk Enterprise. Важливо відзначити, що Gartner не оцінює і не розглядає основне рішення Splunk Enterprise як SIEM. Більшість покупців Splunk ES знаходяться в Північній Америці. Основними покупцями Splunk ES є великі корпоративні організації. Напрямок Splunk ES полягає в тому, щоб запропонувати більше збагачення подій і артефактів через свій користувальницький інтерфейс, а також сприяти доставці більшої кількості контенту. Ліцензування доступне у вигляді обсягу на день або хмарних робочих навантажень (так звані "Віртуальні обчислення Splunk").

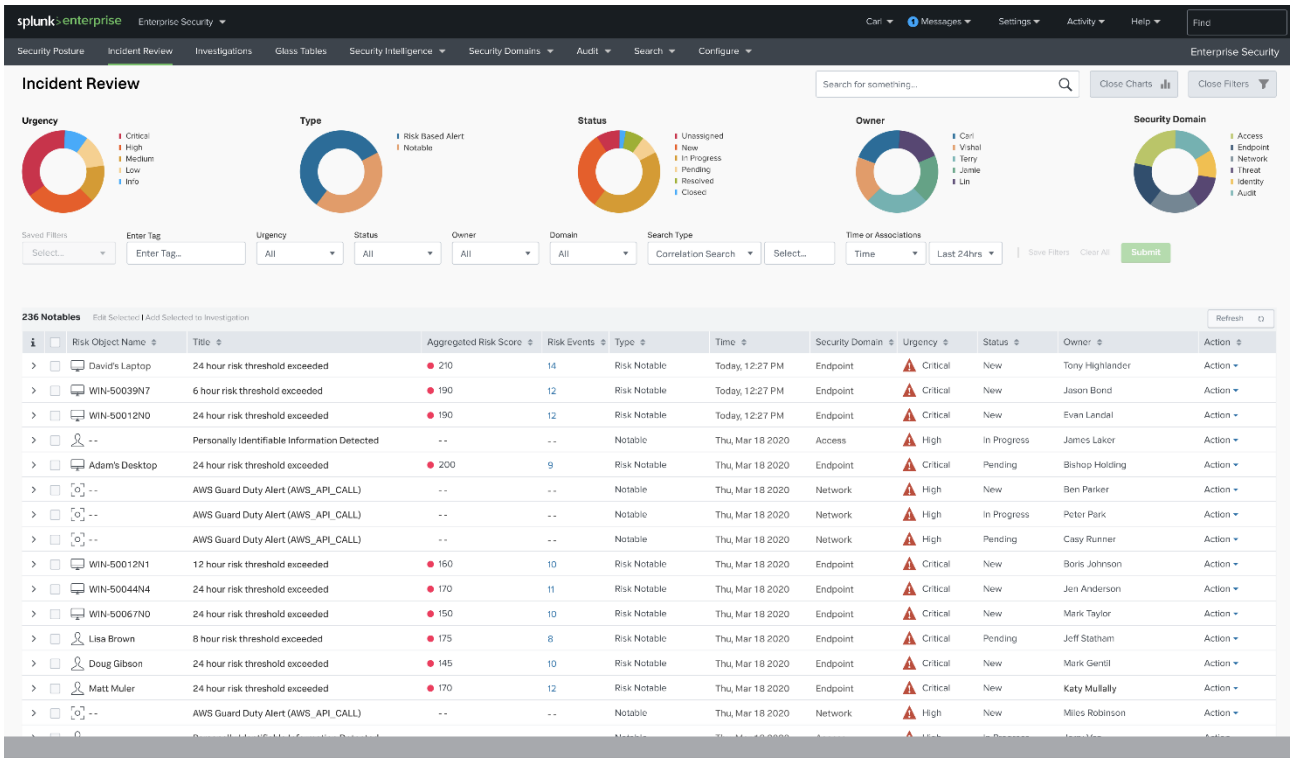

Рис. 2.17. Splunk Enterprise Security [49]

Переваги

- Пакетні функції безпеки: Модель SaaS Splunk ES включає можливості TIP і UEBA без додаткових витрат. Раніше Splunk використовував модульну модель продукту для продажу своїх пропозицій, але зараз ми пакуємо критичні компоненти в Splunk ES, щоб надати більш комплексне рішення для забезпечення безпеки.

- Спостережливість IT в поєднанні з безпекою: Незмінною перевагою Splunk є його здатність надавати IT-спостережливість і аналітику користувачам, які не мають відношення до безпеки, одночасно надаючи командам безпеки функціональність об'єднаних операцій з безпеки через Splunk ES. Splunk збільшує злиття даних про навколишнє середовище з даними про безпеку, щоб надати користувачам збагачене уявлення про їхнє середовище.

- Користувацький досвід роботи з операціями безпеки: Покупці Splunk постійно повідомляють про позитивний користувацький досвід роботи з продуктом ES завдяки функціональності потужних запитів, можливостям API,

налаштованим інформаційним панелям і аналітиці, заснованій на науці про дані, що надається "з коробки".

Застереження

- Ціноутворення: Покупці все ще повідомляють про занепокоєння витратами на Splunk, а нові ціни на віртуальні обчислення Splunk (SVC) не принесли обіцяного полегшення. Зростаючі вимоги до ведення журналів змушують існуючих клієнтів Splunk і нових покупців шукати дешевші альтернативи, щоб компенсувати величезні витрати на поглинання і зберігання даних.
- Складність та експертиза: Покупці висловлюють занепокоєння щодо складності Splunk ES, а існуючі користувачі повідомляють про проблеми з управлінням даними в рамках рішення. Існують також реальні проблеми з навчанням, утриманням і наймом експертів Splunk ES на ринку через високу конкуренцію між власниками Splunk ES за обмежений пул талантів.
- Експертиза регіональних продажів: Більшість спеціалістів з продажу Splunk працює в Північній Америці, а менший відсоток - за межами цього регіону. Недостатнє розуміння вимог та обмежень місцевого ринку може призвести до поганого досвіду з точки зору продажів та підтримки.[49]

Sumo Logic. Sumo Logic є провидцем у цьому магічному квадранті. Її SIEM-продукт, Cloud SIEM, поставляється тільки як SaaS-рішення. Клієнтська база Sumo Logic складається з малих, середніх та корпоративних клієнтів, більшість з яких знаходяться в Північній Америці. За останній рік компанія збільшила свою присутність в Європі та Азійсько-Тихоокеанському регіоні. У 2021 році Sumo Logic придбала компанію DFLabs, яка забезпечує додаткові процеси обробки інцидентів, автоматизовані дії за плейбуком та збагачення за рахунок зовнішніх джерел інформації з такою ж ефективністю, як і окрема пропозиція SOAR. Ліцензування здійснюється на основі передплати (з ціноутворенням на основі споживання даних) або на основі кредитів (з кредитами, які використовуються для забезпечення конкретного використання

ресурсів, наприклад, для епізодичного пошуку або безперервної аналітики), з варіантами багаторівневості та пакунків.

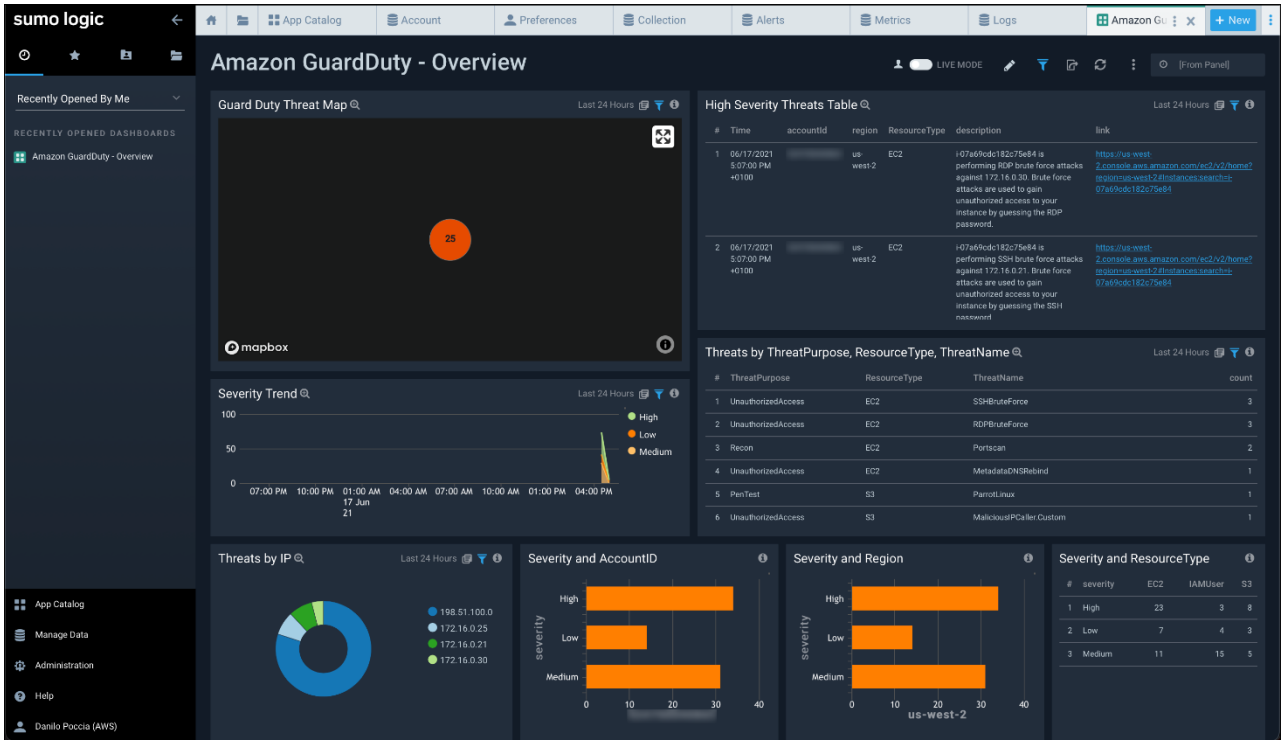

Рис. 2.18. Sumo Logic Cloud SIEM [25]

Переваги

- Об'єднання SecOps і DevOps: Використання Sumo Logic може виходити за рамки операцій з безпеки і поширюватися на розробку та експлуатацію, що є надбанням компанії, а також демократизує дані для декількох бізнес-підрозділів.
- Безкоштовні комерційні готові TI: Sumo Logic надає розвіддані про загрози через CrowdStrike для додаткового збагачення без додаткової оплати.
- Інтегрована функціональність SOAR: Можливості DFLabs SOAR тепер інтегровані в SIEM після придбання, що скорочує трудомісткі завдання SecOps, а також час, необхідний для розгортання SOAR і подальшої інтеграції, щоб зробити його функціональним.

Застереження

- Розширена аналітика: Sumo Logic не має широких можливостей розширеної аналітики, таких як UEBA, в порівнянні з іншими SIEM-конкурентами на ринку.
- Досвід пошуку: Рецензенти Gartner's Peer Insights висловили занепокоєння щодо можливостей пошуку в Sumo Logic, зокрема, щодо впливу на продуктивність при пошуку великих наборів та/або старих даних.

Обмежена видимість: Незважаючи на те, що компанія Sumo Logic стала більш помітною серед постачальників MSSP/MDR з точки зору реселерів та/або керованої підтримки SIEM, її думка щодо SIEM серед кінцевих клієнтів Gartner залишається низькою. [28]

Після детального аналізу рекомендацій від Gartne, в подальшому будемо описувати використання Splunk Enterprise Security.

2.3 Моніторинг і аналіз подій з використанням SIEM

Приступити до опису використання Splunk Enterprise Security можна після проведення моніторингу і аналізу подій з використанням SIEM. Для цього необхідно виконувати визначені дії.

По-перше, потрібно налаштувати джерела даних, щоб вони надсилали свої журнали до Splunk SIEM. Це можуть бути журнали, створені серверами, додатками, мережевими пристроями, пристроями безпеки тощо. Splunk підтримує різні методи збору даних, такі як збір на основі агентів, перенаправлення системних журналів, моніторинг файлів і API.

Рис. 2.19. Приклад схеми отримання даних від різних джерел [59]

Після отримання журналів Splunk індексує їх і зберігає в зручному для пошуку форматі. Splunk перетворює необроблені дані журналів у структуровані події, що полегшує їх аналіз і пошук. Процес індексування організовує дані на основі атрибутів подій, таких як часові мітки, джерела та хости.

Splunk пропонує інструменти візуалізації для створення інтерактивних інформаційних панелей і звітів на основі результатів пошуку. Можна створювати діаграми, графіки і таблиці для візуалізації тенденцій, аномалій і закономірностей. Таке візуальне представлення допомагає зрозуміти дані і виявити інциденти безпеки або операційні проблеми. Звіти можуть бути автоматизовані і заплановані для регулярного розповсюдження.

Використання дашбордів є найзручнішим способом обробки великої кількості даних. Дашборди можна гнучко налаштовувати під свої операційні свої потреби.

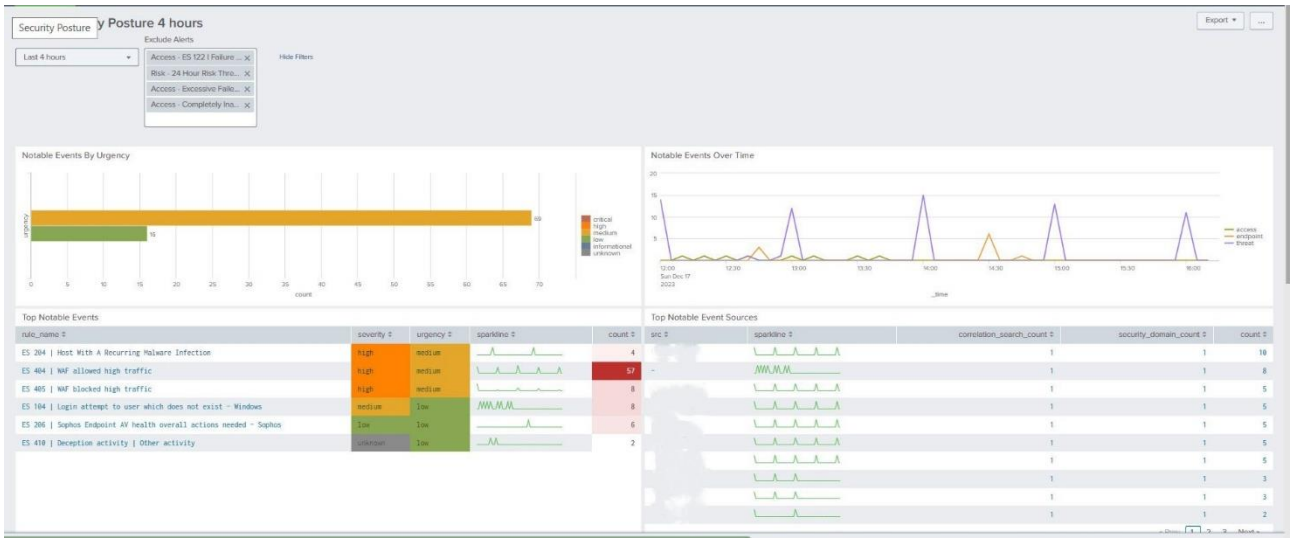

Рис. 2.20. Приклад дашборду в Splunk Enterprise Security

В кожну з подій які показані на рисунку 1.18 можна «провалитись» і отримати більше детальну інформацію по події. Також можна відмітити подію как оброблену або призначити її на вашого колегу для подальшого розслідування

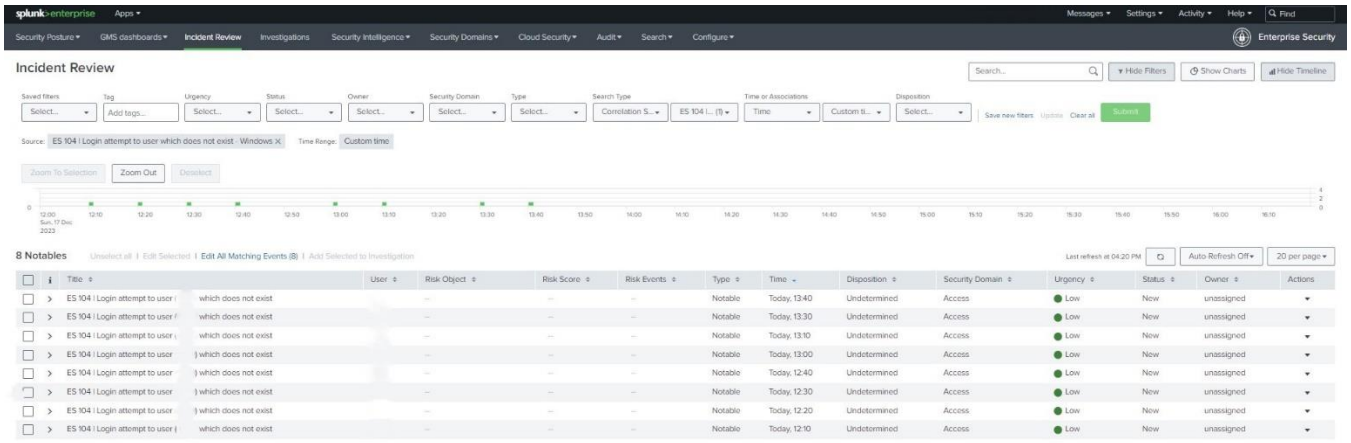

Рис. 2.21. Приклад більш детальної інформації про подію

Splunk надає потужну мову пошуку і запитів (SPL - Splunk Processing Language), яка дозволяє вам досліджувати і отримувати дані. Ви можете використовувати запити SPL для пошуку конкретних подій, фільтрувати дані на основі критеріїв і застосовувати функції та оператори для вилучення необхідної

інформації. Цей крок дозволяє розслідувати конкретні інциденти або збирати інформацію із зібраних журналів.

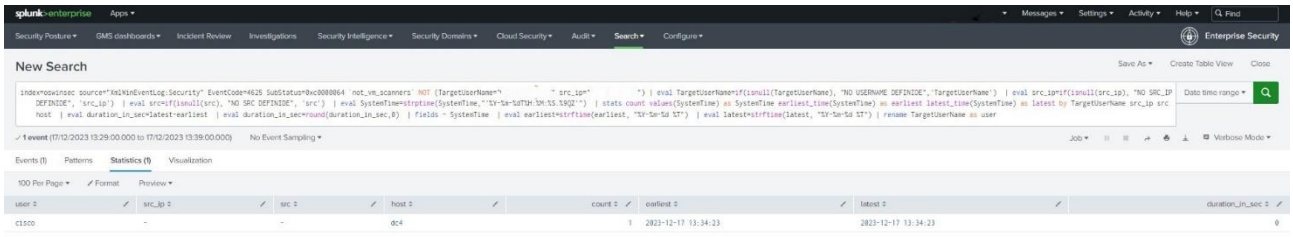

Рис. 2.21 Приклад пошукового запиту

Ось один з прикладів пошукового запиту «Спроба входу в акаунт якого не існує»

index=oswinsec source="XmlWinEventLog:Security" EventCode=4625

| eval TargetUserName=if(isnull(TargetUserName), "NO USERNAME DEFINIDE",'TargetUserName')

| eval src_ip=if(isnull(src_ip), "NO SRC_IP DEFINIDE", 'src_ip')

| eval src=if(isnull(src), "NO SRC DEFINIDE", 'src')

| eval SystemTime=strptime(SystemTime,"'%Y-%m-%dT%H:%M:%S.%9QZ'")

| stats count values(SystemTime) as SystemTime earliest_time(SystemTime) as earliest latest_time(SystemTime) as latest by TargetUserName src_ip src host

| eval duration_in_sec=latest-earliest

| eval duration_in_sec=round(duration_in_sec,0)

| fields - SystemTime

| eval earliest=strftime(earliest, "%Y-%m-%d %T")

| eval latest=strftime(latest, "%Y-%m-%d %T")

| rename TargetUserName as user

2.4 Реагування на інциденти безпеки та підвищення ефективності інформаційної безпеки

При реагуванні на інциденти безпеки важливу роль відіграве такий показник як швидкість. Необхідно якомога швидше виявити інцидент і почати реагування. Це допоможе мінімізувати його вплив.

Виходячи з особистого досвіду швидкість можна визначити на практиці - порівняння витраченого часу з виявлення і реагування на інцидент двох співробітників. При цьому один - Працівник А користується SIEM системою, другий- Працівник Б, який не користується нею. Для цього в системі управління організовується подія інформаційної безпеки і після чого- спостерігається незвичайна активність входу в систему і дії співробітників компанії, в тому числі і Працівників А і Б.

Працівник А: SIEM негайно виявить незвичайну кількість невдалих спроб входу і повідомляє про це повідомленням на пошту або у дашборді за яким слідкує Працівник А.

Реагування на інцидент: за допомогою SIEM команда безпеки починає розслідування протягом кількох хвилин.

Аналіз: SIEM дозволяє швидко розуміти інцидент завдяки хронології подій. Також SIEM дозволяє бачити картину в цілому та наприклад відразу перевірити через пошук чи якість інші підозрілі активності пов’язані з цим користувачем

Автоматизація: Автоматичне реагування включає блокування підозрілих IP-адрес.

Працівник Б під час регулярного перегляду системних журналів IT-адміністратор помітив, що кількість невдалих спроб входу в систему зросла.

Реагування на інцидент: Адміністратор вручну збирає відповідні журнали з багатьох серверів і пристроїв. Цей процес займає багато часу, оскільки потрібно спілкуватися з різними командами та орієнтуватися в різних системах.

Аналіз: Зіставлення журналів і відновлення хронології подій займає більше часу, якщо немає централізованої системи.

Здійснення вручну заходів безпеки, таких як блокування IP-адрес, займає більше часу, але не має автоматизованої відповіді.

Загальний час реагування без SIEM: від кількох годин до кількох днів

Як показує результат проведенного порівняння витраченого часу з виявлення і реагування на інцидент двох співробітників, загальний час реагування без SIEM є більшим, чим з використанням SIEM, і порівнює від кількох годин до кількох днів

Висновки до другого розділу. Отже, стратегічне впровадження та управління системою управління інформаційною безпекою (СУІБ) мають вирішальне значення для захисту активів організації в сучасному цифровому ландшафті. Прийняття циклу PDCA забезпечує структурований підхід для постійного вдосконалення інформаційної безпеки. Такі ключові кроки, як розробка надійної політики безпеки, класифікація активів і створення ефективної організаційної структури, закладають основу для стійкої СУІБ.

Фундаментальними кроками є розробка чіткої політики безпеки, сувора ідентифікація та класифікація активів, а також створення ефективної організаційної структури СУІБ та управління ризиками. Ці кроки гарантують, що основні цілі інформаційної безпеки будуть глибоко інтегровані в організаційну структуру.

Був підвищений акцент на найкращих практиках, включаючи контроль доступу до даних, регулярне навчання з безпеки, захист пристроїв, шифрування даних і послідовні стратегії резервного копіювання, зміцнюючих систему безпеки. Інтеграція цих практик з глобальними стандартами, такими як ISO 27001, NIST 800-53, звіти SOC, CCPA і HIPAA, забезпечує відповідність вимогам і задовольняє специфічні потреби безпеки в різних секторах.

Роль SIEM-рішень у підвищенні ефективності СУІБ неможливо переоцінити. Ці рішення забезпечують аналіз і моніторинг у режимі реального

часу, що є життєво важливим для виявлення, запобігання та реагування на інциденти безпеки.

По суті, комплексний підхід, описаний в цьому розділі, не тільки захищає інформаційні активи, але й відповідає міжнародним стандартам, гарантуючи, що організації будуть добре підготовлені до протистояння новим викликам у сфері інформаційної безпеки. Завдяки добре впровадженій СУІБ організації можуть досягти балансу між захистом своїх цінних інформаційних активів і підтримкою операційної ефективності у все більш взаємопов'язаному світі.

В розділі було розглянуто процеси моніторингу і підхід до аналізу подій з використанням SIEM. Результатами є проведення порівняння працівників які користуються та не користуються SIEM системами

Досліджений перелік SIEM-рішень які є лідерами на рику та дані переваги і недолі цих інструментів

Показано місце та роль реагування на інциденти безпеки у підвищенні ефективності інформаційної безпеки з використанням SIEM систем

РОЗДІЛ 3.
ДОСЛІДЖЕННЯ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ SIEM

3.1 Визначення можливих шляхів впровадження рекомендацій та їх практична реалізація

Впровадження рекомендацій має вирішальне значення для покращення IT-стану організацій. Однак, перш ніж обирати інструменти, важливо оцінити досвід існуючих команд та можливості інтеграції . Це допоможе визначити найбільш підходящі рішення, які можна практично реалізувати. Для забезпечення практичної реалізації найкращих у своєму класі інструментів рекомендується проводити виробничу оцінку . Установам необхідно знайти комбінації постачальників/рішень, які відповідають їхній поточній IT-позиції . Це може допомогти уникнути інвестицій в інструменти, які не сумісні з існуючою структурою. Крім того, організаціям необхідно запровадити найкращі практики для забезпечення послідовності у впровадженні IT в рамках всієї установи. Ці кращі практики повинні вирішувати поточні проблеми і залишати простір для вдосконалення в майбутньому, оскільки технології та бізнес-потреби розвиваються . Дотримуючись цих рекомендацій та впроваджуючи їх на практиці, організації можуть забезпечити стабільне та ефективне IT-середовище.

Для підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM необхідно визначити можливі шляхи впровадження рекомендацій. Ці шляхи можна розділити на два основні типи:

Технологічні шляхи. Вони пов'язані з впровадженням нових технологій або вдосконаленням існуючих. Наприклад, це може бути впровадження нового

SIEM-продукту, розширення функціональності існуючого SIEM-продукту або впровадження додаткових інструментів і сервісів для підтримки SIEM.

На практиці це може бути нове кореляційне правило яке б замінювало або об’єднувало декілька старих для полегшення обробки та зменшення кількості оброблених фолспозитивних подій.

Також це може бути встановлення адоннів для SIEM систем за для більш детальної та простішої інтеграції інших систем захисту які представленні в компанії.

Процесуальні шляхи. Вони пов'язані зі зміною процесів управління інформаційною безпекою. Наприклад, це може бути впровадження нових процедур виявлення та реагування на інциденти за для більш швидкого реагування.

Написання інструкцій з реагування на ті чи інші інциденти, що також сприяє підвищенню BCP(План забезпечення безперервності бізнесу) . В такому випадку менш підготовлені спеціалісти або колеги які дотично можуть виконувати роль SOC аналітика зможуть ефективно реагувати на інциденти.

Вдосконалення процедур управління конфіденційністю або вдосконалення процедур навчання та підвищення обізнаності співробітників про інформаційну безпеку. Навчання співробітників також є важливою складовою ефективного використання SIEM систем

3.2 Оцінка рекомендацій з точки зору практичної реалізованості та впливу на безпеку даних

При оцінці рекомендацій з точки зору практичної реалізовності та впливу на безпеку даних необхідно враховувати наступні аспекти:

Практична реалізованість. Рекомендації повинні бути такими, щоб їх можна було практично реалізувати в рамках існуючої системи управління інформаційною безпекою організації. Оцінка практичної реалізовності повинна

включати в себе аналіз існуючої системи управління інформаційною безпекою, визначення необхідних ресурсів і оцінку можливих ризиків.

Наприклад, якщо організація має обмежені ресурси, то вона може не мати можливості впровадити нові технологічні рішення, такі як впровадження нового SIEM-продукту або розширення функціональності існуючого SIEM-продукту. У цьому випадку організація може зосередитися на впровадженні процедурних змін, таких як вдосконалення процедур виявлення та реагування на інциденти або вдосконалення процедур навчання та підвищення обізнаності співробітників про інформаційну безпеку.

Вплив на безпеку даних. Рекомендації повинні мати позитивний вплив на безпеку даних. Оцінка впливу на безпеку даних повинна включати в себе аналіз потенційних ризиків та переваг впровадження рекомендацій.

Наприклад, впровадження нового SIEM-продукту може призвести до підвищення ефективності виявлення загроз, але також може призвести до збільшення складності управління SIEM. У цьому випадку необхідно оцінити, чи переважують потенційні переваги потенційні ризики.

Приклади оцінки рекомендацій

Розглянемо наступні рекомендації для підвищення ефективності системи управління інформаційною безпекою організації з використанням SIEM:

Рекомендація 1: Впровадити новий SIEM-продукт, який підтримує більш широкий спектр джерел даних і має більш розвинену функціональність виявлення загроз.

Оцінка практичної реалізовності: Рекомендація є практично реалізовною, оскільки на ринку представлено широкий спектр SIEM-продуктів з різними характеристиками. Однак, впровадження нового SIEM-продукту може бути пов'язано з певними витратами і ризиками.

Оцінка впливу на безпеку даних: Рекомендація може мати позитивний вплив на безпеку даних, оскільки новий SIEM-продукт може забезпечити більш ефективне виявлення загроз. Однак, необхідно оцінити, чи переважують потенційні переваги потенційні ризики.

Рекомендація 2: Вдосконалити процедури виявлення та реагування на інциденти, включивши в них автоматизовані сценарії реагування.

Оцінка практичної реалізовності: Рекомендація є практично реалізовною, оскільки існує ряд інструментів і сервісів, які можуть бути використані для автоматизації завдань виявлення та реагування на інциденти. Однак, впровадження автоматизованих сценаріїв реагування може бути пов'язано з певними витратами і ризиками.

Оцінка впливу на безпеку даних: Рекомендація може мати позитивний вплив на безпеку даних, оскільки вона може допомогти організації швидко і ефективно реагувати на інциденти.

Рекомендація 3: Навчити співробітників організації про використання SIEM і про виявлення та реагування на інциденти.

Оцінка практичної реалізовності: Рекомендація є практично реалізовною, оскільки її можна реалізувати за допомогою внутрішніх ресурсів або за допомогою сторонніх постачальників послуг.

Оцінка впливу на безпеку даних: Рекомендація може мати позитивний вплив на безпеку даних, оскільки вона може допомогти співробітникам організації розуміти важливість інформаційної безпеки і вживати заходів для її забезпечення.

Рекомендація 4: Створення нового кореляційного правило яке б замінювало або об’єднувало декілька старих

З точки зору практичної реалізовності, створення нового кореляційного правила не вимагає значних ресурсів чи зусиль. Для цього необхідно лише провести аналіз існуючих кореляційних правил, визначити, які з них можна об’єднати або замінити, і розробити нове правило.

З точки зору впливу на безпеку даних, нова кореляційне правило може мати наступні переваги:

Полегшення обробки подій. Новий кореляційне правило може бути спрощено таким чином, щоб його було легше розуміти та використовувати. Це може допомогти операторам безпеки швидше і ефективніше реагувати на події.

Зменшення кількості фолспозитивних подій. Об’єднання або заміна декількох старих кореляційних правил може допомогти зменшити кількість фолспозитивних подій. Це пов’язано з тим, що нове правило буде більш точним і менш сприйнятливим до помилок.

Однак, необхідно враховувати, що нова кореляційне правило може мати і деякі недоліки. Наприклад, воно може бути менш ефективним у виявленні деяких видів загроз, ніж декілька старих правил. Тому перед впровадженням нового правила необхідно провести ретельний аналіз його ефективності.

Рекомендація 5: Встановлення адоннів для SIEM систем

Встановлення адоннів не вимагає значних ресурсів чи зусиль з точки зору практичної реалізації. Щоб досягти цього, вам потрібно просто завантажити та встановити відповідні аддони.

Аддони можуть мати наступні переваги з точки зору впливу на безпеку даних:

Розширення можливостей SIEM-системи. Аддони можуть додати нові можливості до системи SIEM, наприклад виявлення нових типів загроз, автоматизацію завдань або покращення інтерфейсу користувача.

Збільшення продуктивності SIEM-систем. Наприклад, аддони можуть підвищити ефективність SIEM-систем організації шляхом зменшення кількості фолспозитивних подій або підвищення точності виявлення загроз.

Тим не менш, важливо пам’ятати, що аддони можуть мати деякі недоліки. Наприклад, вони можуть не працювати з існуючою системою SIEM або мати помилки. Отже, перед встановленням адоннів необхідно провести ретельний аналіз їх безпеки та сумісності.

Рекомендація 6: Написання інструкцій з реагування на ті чи інші інциденти

Написання інструкцій не вимагає значних зусиль чи ресурсів з точки зору практичної реалізації. Щоб досягти цього, необхідно лише проаналізувати поточні процедури реагування на інциденти, визначити, які з них потребують документування, і створити відповідні вказівки.

Інструкції з реагування на інциденти можуть бути корисними з точки зору безпеки даних:

Покращення ефективності реагування на надзвичайні ситуації. Інструкції можуть допомогти організаціям швидко та ефективно реагувати на інциденти, надаючи працівникам знання та ресурси, необхідні для цього.

Зменшення ймовірності помилок Інструкції можуть допомогти працівникам уникнути помилок під час реагування на інциденти.

Покращення ефективності спілкування під час реагування на інциденти Інструкції можуть допомогти організаціям забезпечити ефективну комунікацію під час реагування на інциденти між різними підрозділами.

Але слід пам’ятати, що інструкції з реагування на інциденти можуть мати недоліки. Наприклад, вони можуть бути надто заплутаними або складними, або вони можуть не враховувати всі потенційні сценарії інцидентів. Отже, перед написанням інструкцій потрібно провести ретельний аналіз потреб організації.

Загалом, рекомендація щодо створення інструкцій з реагування на інциденти є хорошою ідеєю, оскільки вона може допомогти організації зробити свою роботу ефективнішою.

Ось кілька конкретних рекомендацій щодо створення інструкцій з реагування на інциденти:

- Інструкції повинні бути зрозумілими та простими. Вони повинні бути написані таким чином, щоб вони були легко зрозумілими та ефективними.
- Інструкції повинні бути змінені відповідно до потреб конкретної організації. Вони повинні розглянути всі можливі випадки, які можуть статися в організації.
- Інструкції повинні регулярно переглядати та доопрацьовувати. Це потрібно, щоб вони завжди відповідали потребам організації.

Висновки до третього розділу. В цьому розділі були надані шляхи впровадження рекомендацій та їх практична реалізація. Впровадження інструментів SIEM є одночасно корисним і складним способом зміцнення інформаційної безпеки організації. Як було показано в роботі, комплексний підхід до кібербезпеки забезпечується поєднанням технологічних досягнень SIEM з процедурними вдосконаленнями. Можна створити надійний механізм захисту від кіберзагроз, ретельно обираючи та налаштовуючи рішення SIEM відповідно до потреб організації, а також доповнюючи цю технологію добре розробленими процедурами та навчанням співробітників. Таке стратегічне впровадження не лише зміцнює поточну систему безпеки організації, але й готує її до майбутніх проблем у постійно змінюваному цифровому світі.

Успіх цих проектів залежить від того, наскільки добре організація розуміє можливості та обмеження технології SIEM, а також наскільки вона готова змінюватися та розвиватися. Оскільки загрози стають все більш складними, ми також повинні вдосконалювати наші методи захисту. Ці рекомендації служать дорожньою картою для організацій, які прагнуть покращити свої заходи кібербезпеки. Зрештою, ефективне використання інструментів SIEM - це більше, ніж просто технологія; це створення культури знань і реагування на загрози, які поширюються на всі рівня організації. Така проактивна поведінка дозволяє компанії залишатися обережною, стійкою та на крок попереду в боротьбі з кіберзагрозами.

Також були надана оцінка рекомендацій з точки зору практичної реалізованості та впливу на безпеку даних. Завдяки глибокому розумінню переваг і недоліків технології SIEM, а також готовності організації змінюватися та розвиватися, ці проекти можуть бути успішними. путівник для організацій, які прагнуть покращити свої кібербезпекові заходи.

ВИСНОВКИ

Інтеграція та ефективне розгортання систем управління інформацією та подіями безпеки (SIEM) відіграють вирішальну роль в удосконаленні управління інформаційною безпекою в організаціях. У цьому документі детально розглядаються різні аспекти SIEM, підкреслюється його цінність у виявленні, розслідуванні та управлінні часом реагування на загрози. Системи SIEM, за своєю суттю, агрегують і аналізують дані журналів з різноманітного мережевого обладнання та програмного забезпечення, забезпечуючи аналіз даних про події в реальному часі для попередження цілеспрямованих атак, складних загроз і витоків даних.

Однією з ключових переваг SIEM є здатність об'єднувати аналітику загроз і можливості машинного навчання, що дозволяє організаціям проактивно виявляти і пом'якшувати наслідки інцидентів безпеки. Така проактивна позиція має вирішальне значення в сучасному ландшафті кібербезпеки, де загрози не тільки різноманітні, але й все більш витончені.

Інтеграція SIEM з системами виявлення вторгнень (IDS), системами запобігання вторгненням (IPS), системами управління журналами (LMS), аналітикою великих даних та іншими системами управління безпекою, такими як системи управління інцидентами (IMS) та інструменти оркестрування, автоматизації та реагування на інциденти (SOAR), підкреслює їх багатогранну корисність. Така інтеграція забезпечує більш комплексний механізм моніторингу, аналізу та реагування, підвищуючи здатність організації виявляти аномалії та загрози, автоматизувати процеси реагування на інциденти та значно скоротити час реагування.

Однак розгортання SIEM-систем не позбавлене певних труднощів. До них відносяться складність конфігурації, труднощі інтеграції з існуючими інструментами безпеки, обмеження ресурсів, приховані витрати, проблеми з впровадженням даних, обмеження масштабованості, а також дотримання нормативних правил зберігання даних і дотримання нормативних вимог.

Вирішення цих проблем вимагає чіткої постановки цілей, ретельного планування, ретельного впровадження та постійної оптимізації SIEM-системи.

Таким чином, SIEM-системи є незамінними в сучасній стратегії кібербезпеки, пропонуючи комплексний підхід до виявлення загроз, реагування на інциденти, дотримання нормативних вимог і безперервний моніторинг розвідданих про загрози. Їх роль у зниженні ризиків, захисті конфіденційних даних, забезпеченні нормативно-правової відповідності та підтримці безперервності бізнесу є незаперечною. Оскільки кіберзагрози продовжують розвиватися, SIEM залишається життєво важливим інструментом для зниження ризиків і захисту активів організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Відомості про вбудовану ініціативу щодо відповідності вимогам стандарту NIST SP 800-53, ред. 4. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/ru-ru/azure/governance/policy/samples/nist-sp-800-53-r4.

2. Корченко О.Г. Аудит управління інцидентами інформаційної безпеки. навч. посібник. НАСБУ, 2017. с.147

3. Марценюк О.В. SIEM системи (security information and event management) – що це і навіщо потрібно?. Актуальні проблеми кібербезпеки : Всеукр. науково-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 321–323.

4. Нові виклики для інформаційної безпеки підприємства: як мінімізувати потенційні ризики. ESET - офіційний сайт. Антивірусні програми Iсет в Україні | ESET. URL: https://eset.ua/ua/blog/view/67/novyye-vyzovy-dlya-informatsionnoybezopasnosti-predpriyatiya-kak-minimizirovat-potentsialnyye-riski.

5. Управління інцидентами інформаційної безпеки | Управління інцидентами ІБ - SearchInform. Інформаційна безпека підприємства. Захист конфіденційної інформації компанії від витоку - SearchInform. URL: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/upravlenie-intsidentami-informatsionnoj-bezopasnosti/.

6. Що таке ніст 800-53? - визначення з техопедії - Безпека 2023. Icy Science. URL: https://uk.theastrologypage.com/nist-800-53.

7. ADEYANJU S. THE BENEFITS OF SPLUNK SIEM. *riversafe.co.uk*. URL: https://riversafe.co.uk/resources/tech-blog/the-benefits-of-splunk-siem/.

8. American Institute of Certified Public Accountants. (2021). Service Organization Controls (SOC) 1: Reporting on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting. New York, NY: AICPA.

9. American Institute of Certified Public Accountants. (2022). SOC 2: Service Organization Controls (SOC) 2 Report Type 1 and Type 2. New York, NY: AICPA.

10. artiusha. На сторожі безпеки: IBM QRadar SIEM. Хабр. URL: https://habr.com/ru/companies/muk/articles/325330/.

11. Automated Incident Response Explained. AT&T Cybersecurity | Managed Security Services for Network, XDR & more. URL: https://cybersecurity.att.com/blogs/security-essentials/automated-incident-response-in-action-7-killer-use-cases.

12. Bond R. The Benefits of Using a SIEM to Improve IT Security. *LinkedIn*. URL: https://www.linkedin.com/pulse/benefits-using-siem-improve-security-robert-bond/?trk=article-ssr-frontend-pulse_more-articles_related-content-card.

13. Cloud SIEM | Sumo Logic. Sumo Logic. URL: https://www.sumologic.com/solutions/cloud-siem/.

14. Complaint Form - California Privacy Protection Agency (CPPA). California Privacy Protection Agency (CPPA). URL: https://cppa.ca.gov/webapplications/complaint.

15. Cybersecurity and Privacy Reference Tool | CSRC. NIST Computer Security Resource Center | CSRC. URL: https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home.

16. Dess G. G. Strategic management. New York : McGraw-Hill, 2018. с. 73.

17. Einav E. Introducing a Unified Security Operations Platform with Microsoft Sentinel and Defender XDR. *TECHCOMMUNITY.MICROSOFT.COM*. URL: https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/introducing-a-unified-security-operations-platform-with/ba-p/3983341.

18. Elastic Observability [8.11] | Elastic. Elasticsearch Platform – Find real-time answers at scale | Elastic. URL: https://www.elastic.co/guide/en/observability/current/index.html.

19. European Parliament and the Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119/1.

20. Gillis A. S., Rosencrance L. What is SIEM? | A Definition from TechTarget.com. *Security*.
URL: https://www.techtarget.com/searchsecurity/definition/security-information-and-event-management-SIEM

21. Guide to Information Security Management | Smartsheet. Smartsheet. URL: https://www.smartsheet.com/content/information-security-management.

22. Huawei Listed Again in the Gartner SIEM Magic Quadrant in 2022-HUAWEI CLOUD. Huawei Cloud. URL: https://www.huaweicloud.com/intl/en-us/news/20221116143452362.html.

23. IBM Documentation. IBM in Deutschland, Österreich und der Schweiz | IBM. URL: https://www.ibm.com/docs/ru/qsip/7.5?topic=started-qradar-overview.

24. Information security management - definition & overview | Sumo Logic. Sumo Logic. URL: https://www.sumologic.com/glossary/information-security-management/.

25. Information security management - definition & overview | Sumo Logic. Sumo Logic. URL: https://www.sumologic.com/glossary/information-security-management/.

26. InsightIDR - XDR & SIEM Platform - Rapid7. Rapid7. URL: https://www.rapid7.com/products/insightidr/.

27. ISO/IEC 27002:2023 «Information technology. Security techniques. Code of practice for information security controls».

28. Magic Quadrant for Security Information and Event Management. *Gartner | Delivering Actionable, Objective Insight to Executives and Their Teams*. URL: https://www.gartner.com/doc/reprints?id=1-2BDC4CDW&ct=221010&st=sb.

29. Maximizing Cybersecurity: A Comprehensive Guide to Using Splunk as a SIEM | SubRosa. *Cybersecurity Testing & Advisory Services | SubRosa*. URL: https://subrosacyber.com/blog/using-splunk-as-a-siem.

30. Mills T. Cloud Artistry: Building a Custom SIEM Environment with Microsoft Azure. Medium. URL: https://medium.com/@vermillionmills/cloud-artistry-building-a-custom-siem-environment-with-microsoft-azure-b0c33c7fd5dd.

31. National Institute of Standards and Technology. (2023). Special Publication 800-53 Revision 5: Security Controls for Information Systems and Organizations. Gaithersburg, MD: U.S. Department of Commerce.

32. Next-Gen SIEM. Gurucul. URL: https://gurucul.com/products/gurucul-siem.

33. PayOnline. Що таке PCI DSS і як відбувається перевірка на відповідність стандарту? Хабр. URL: https://habr.com/ru/companies/payonline/articles/303330/.

34. Performance reference for Splunk Enterprise Security - Splunk Documentation. *Documentation - Splunk Documentation*. URL: https://docs.splunk.com/Documentation/ES/7.2.0/Install/DeploymentPlanning.

35. Preparing for Security Event Management. URL: http://www.windowsecurity.com/uplarticle/NetworkSecurity/360is-prep-sem.pdf.

36. Preparing for Security Event Management. windowsecurity. URL: https://www.windowsecurity.com/uplarticle/NetworkSecurity/360is-prep-sem.pdf.

37. Product Portfolio - Exabeam. Exabeam. URL: https://www.exabeam.com/product/.

38. Raghunathan A. How Does SIEM Reduce Risk? Unveiling the Power of Security Information and Event Management. *LinkedIn*. URL: https://www.linkedin.com/pulse/how-does-siem-reduce-risk-unveiling-power-security-raghunathan/.

39. Security Information and Event Management (SIEM) Solutions - ManageEngine. ManageEngine: IT security, operations & service management. URL:

https://www.manageengine.com/security-information-event-management.html?pos=MEhome&loc=SolMenu&cat=KS.

40. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *PubMed Central (PMC)*. URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8309804/.

41. Security Information and Event Management Tool | SIEM Software | OpenText | CyberRes. Micro Focus is now OpenText. URL: https://www.microfocus.com/en-us/cyberres/secops/arcsight-esm.

42. SIEM | Security Information and Event Management | LogRhythm. LogRhythm. URL: https://logrhythm.com/solutions/security/siem/.

43. SIEM Implementation in 4 Steps. *Exabeam*. URL: https://www.exabeam.com/explainers/siem/siem-implementation-in-4-steps/.

44. SIEM Solutions & Tools | Get Best Enterprise SIEM Software | FortiSIEM. Fortinet. URL: https://www.fortinet.com/products/siem/fortisiem.

45. SIEM Tools: How They Enhance Federal Cybersecurity. *Technology Solutions That Drive Government*. URL: https://fedtechmagazine.com/article/2020/01/siem-tools-how-they-enhance-federal-cybersecurity-perfcon.

46. SIEM. Logpoint. URL: https://www.logpoint.com/en/product/siem/.

47. SIEM: Security Information & Event Management Explained. *Splunk-Blogs*. URL: https://www.splunk.com/en_us/blog/learn/siem-security-information-event-management.html.

48. Splunk Enterprise | Splunk. Splunk. URL: https://www.splunk.com/en_us/products/splunk-enterprise.html.

49. Splunk Enterprise Security | Splunk. *Splunk*. URL: https://www.splunk.com/en_us/products/enterprise-security.html.

50. Splunk Search Command of the Week: Where Command – Kinney Group. Kinney Group – Splunk is a Journey. We Know the Way. URL: https://kinneygroup.com/blog/splunk-where-command/.

51. Splunk SIEM Review & Alternatives. *Comparitech*. URL: https://www.comparitech.com/net-admin/splunk-siem-review-alternatives/.

52. The 2023 Buyer's Guide to Next-Gen SIEM : Електронна книга. Cambridge : Devo, 2022. 17 p. URL: https://www.devo.com/wp-content/uploads/2023/06/The-Buyers-Guide-to-Next-Gen-SIEM-eBook-2023.pdf.

53. Top Challenges in Implementing SIEM Solutions | Logsign Blog. *Logsign*. URL: https://www.logsign.com/blog/top-challenges-in-implementing-siem-solutions/.

54. Understanding Splunk SIEM: A Comprehensive Guide to Your Cybersecurity Needs | SubRosa. *Cybersecurity Testing & Advisory Services | SubRosa*. URL: https://subrosacyber.com/blog/what-is-splunk-siem.

55. Unified Defense SIEM. Securonix. URL: https://www.securonix.com/products/unified-defense-siem/.

56. What is Information Security Management System (ISMS)?. *Data Privacy & Information Security - DataGuard*. URL: https://www.dataguard.co.uk/blog/what-is-information-security-management-system.

57. What is ISO 27001? Key Information at a Glance. Data Privacy & Information Security - DataGuard. URL: https://www.dataguard.co.uk/knowledge/iso-27001/.

58. What is SIEM? A complete guide to Security Information and Event Management. Logpoint. URL: https://www.logpoint.com/en/what-is-siem/.

59. What is Splunk used for? | Splunk SIEM | Splunk Meaning 2022. Comodo. URL: https://www.comodo.com/is-splunk-a-siem.php.

60. Yasar K. What is Information Security Management System (ISMS)?. *WhatIs.com*.
URL: https://www.techtarget.com/whatis/definition/information-security-management-system-ISMS.