ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення

API – Application Programming Interface

CTI – Cyber Threat intelligence

DLP – Data Loss Prevention

EDR – Endpoint Detection and Response

IDM – Identity Management

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

IoC – Indicators of Compromise

SIEM – Security Information and Event Management

SFSP – SOAR Framework Solution Pack

SOAR – Security Orchestration, Automation and Response

ВСТУП

Актуальність дослідження. Однією з головних проблем сьогодення для кібербезпеки організацій є невпинно зростаюча кількість кібератак. Так, згідно з даними джерела Statistica [1], починаючи з 2016 по 2022, кількість кібератак тільки в США зросла з 250000 до 480000 та, не беручи до уваги 2020 рік, коли значення досягло 540000 тисяч кібератак за рік через вплив COVID-19 та карантинних обмежень, не маючи тенденції до зменшення.

Враховуючи швидкість кількісного та якісного розвитку кібератак, їх адаптивність та комплексність, виявлення загроз в режимі реального часу стає все складнішою проблемою для спеціалістів з кібербезпеки. Вирішення цього питання вимагає від організацій не лише постійних інвестицій в сучасне обладнання та програмне забезпечення, а й покращення систем моніторингу, безперервного розвитку комплексних стратегій кібербезпеки, навчання та розширення штату з метою адаптації до нових та вже існуючих загроз.

Системи SOAR дозволяють організаціям не лише автоматизувати та керувати реакціями на кіберзагрози, підвищуючи ефективність спеціалістів з кібербезпеки, а й стандартизувати процес реакції на інциденти, забезпечуючи дотримання встановлених процедур, що зменшує вірогідність людської помилки та підвищує загальний рівень безпеки системи. Системи SOAR також підвищують рівень взаємодії команд кібербезпеки з IT-відділом, поліпшуючи обмін інформацією та координацію під час протидії кіберзагрозам.

Забезпечення ефективності систем SOAR досягається шляхом інтеграції з іншими інструментами безпеки організації, такими як SIEM, EDR, NDR, пристроями мережевої безпеки, системами керування загрозами та іншими. Це дозволяє автоматизувати процес збору даних про інциденти, аналізувати їх в режимі реального часу та вживати необхідних заходів без

зайвих затримок.

Отже, впровадження системи SOAR реалізує комплексний підхід до захисту організації від кіберзагроз, забезпечуючи інтеграцію різноманітних інструментів кібербезпеки, дозволяючи автоматизувати рутинні процеси та координувати реакції на інциденти. Як результат, SOAR надає можливість значно підвищити швидкість виявлення та нейтралізації загроз, зменшити час на реагування та знизити ризики.

Об'єкт дослідження – автоматизація процесів реагування на інциденти на базі рішення FortiSOAR.

Предмет дослідження – методи та засоби автоматизації процесів реагування на інциденти кібербезпеки в організаціях.

Мета роботи – розробити рекомендації щодо розгортання, конфігурації та впровадження системи автоматизація процесів реагування на інциденти FortiSOAR.

Наукові завдання:

дослідити сутність проблеми автоматизації процесів реагування на інциденти;

встановити сутність завдань автоматизації процесів реагування на інциденти;

проаналізувати існуючі підходи до автоматизації реагування на інциденти;

проаналізувати методи та засоби автоматизації реагування на інциденти на прикладі FortiSOAR;

розробити рекомендації щодо автоматизації процесів реагування на інциденти в інформаційній системі організації.

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

Практичне значення одержаних результатів: рекомендації щодо розгортання, конфігурації та впровадження системи автоматизація процесів

реагування на інциденти можуть бути використані у сфері кіберзахисту.

1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ РЕАГУВАННЯ НА ІНЦИДЕНТИ

1.1 Дослідження змісту реагування на інциденти в інформаційній системі організації

Ручні методи реагування на інциденти вимагають багато часу і значно зменшують ефективність обробки інцидентів. Кожен крок від перевірки алерту до вжиття відповідних заходів займає значну кількість часу. Аналітики повинні аналізувати кожне алерт, збирати додаткову інформацію та реагувати вручну [2]. Кожен інцидент може займати від кількох хвилин до навіть днів, що обмежує кількість подій, які можуть бути оброблені протягом робочого часу. В умовах великої кількості подій це призводить до накопичення незакритих інцидентів і створює додаткові ризики для безпеки організації.

Висока ймовірність помилок, властивих традиційним методам, також є важливою проблемою. Людський фактор, особливо втома, неуважність або відсутність кваліфікації, можуть призвести до неправильного визначення пріоритетів загроз або пропуску важливих деталей. Наприклад, неправильна класифікація інцидентів як false positive, може залишити реальні загрози непоміченими та невирішеними. Це збільшує ризик успішної атаки на інфраструктуру.

Через обмежену масштабованість ручних методів неможливо ефективно обробляти велику кількість інцидентів. Зі збільшенням кількості загроз потрібні додаткові ресурси: більше аналітиків і більше часу, що збільшує витрати організації. Це обмежує здатність швидко і ефективно реагувати на інциденти в рамках великої та розподіленої інфраструктури і створює вузькі місця в процесі забезпечення безпеки.

Неузгодженість і відсутність координації в процесі реагування вручну

також є суттєвими недоліками. Кожен аналітик може мати свій власний підхід до розслідування та реагування на інциденти, що призводить до невідповідності в діях. Відсутність координації між різними групами може призвести до дублювання зусиль або, навпаки, до пропуску ключових етапів у процесі реагування. Це створює додаткові ризики і знижує загальну ефективність захисту. Через численні обмеження, пов'язані з ручним реагуванням на кіберінциденти, Автоматизація все частіше потрібна для ефективного захисту організацій у сучасному динамічному середовищі кіберзагроз.

Давайте розглянемо приклад такого реагування на інцидент при виявленні індикатора шкідливого ПЗ. Процес ручного реагування на інцидент починається з отримання повідомлення про інцидент із SIEM. Використовуючи SIEM аналітик перевіряє існуючі IoC, щоб визначити, чи є IP-адреса шкідливою. Якщо адреса не знайдена серед відомих шкідливих програм, використовуються зовнішні CTI, такі як VirusTotal, RDAP, Anomali або OTX, для додаткової перевірки. Після збору всіх даних аналітик оцінює репутацію IP-адреси і приймає рішення про її шкідливості.

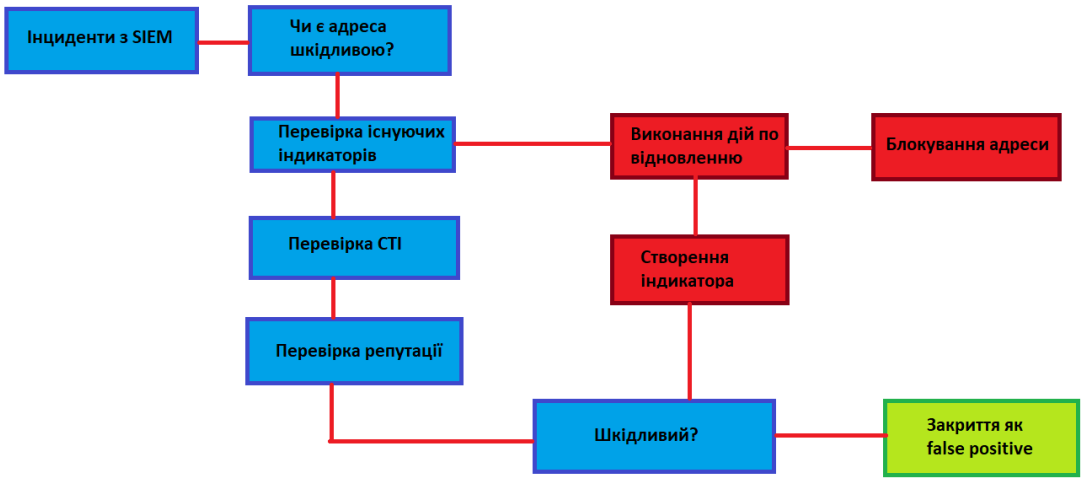

Рис. 1.1. Приклад алгоритму ручного реагування на інциденти

Якщо адреса визнана шкідливою, створюється індикатор і виконуються

дії з відновлення, такі як блокування IP-адреси на брандмауері. Якщо адреса не є шкідливою або виявлена як false positive, інцидент буде закритий з відповідною документацією.

Перехід на автоматизоване реагування на інциденти за допомогою інструменту SOAR має багато переваг, які роблять його найкращим вибором для організацій, які прагнуть підвищити свою стійкість до кіберзагроз.

SOAR значно прискорює реагування на кіберінциденти і звільняє час фахівців з кібербезпеки для вирішення більш складних завдань. Автоматизований процес SOAR менш схильний до людських помилок, що забезпечує чітке і безпомилкове реагування. SOAR також допомагає зменшити витрати, пов'язані з кіберінцидентами, скорочуючи час простою та мінімізуючи шкоду.

SOAR покращує координацію між командами, які беруть участь у реагуванні на інциденти, забезпечуючи чіткий та послідовний процес. SOAR збирає та обробляє великі обсяги даних про інциденти, щоб допомогти вам отримати чітке уявлення про те, що сталося з організацією, визначити першопричини та вдосконалити стратегію кібербезпеки. SOAR може ефективно масштабуватися для задоволення потреб організацій будь-якого розміру без істотного збільшення штату фахівців з кібербезпеки.

Впровадження SOAR допоможе організаціям значно поліпшити реагування на кіберінциденти, знизити ризики, пов'язані з кіберзагрозами, і підвищити загальну стійкість до кіберзлочинності.

1.2 Аналіз підходів до підвищення ефективності процесів реагування на інциденти

Головним інструментом, що поєднує в собі управління, автоматизацію та реагування на кіберінциденти є система SOAR (Security Orchestration, Automation and Response). SOAR допомагає організаціям більш ефективно та економно реагувати на кіберзагрози, автоматизуючи повсякденні завдання,

стандартизуючи процеси та забезпечуючи координацію між різними командами та системами.

SOAR пройшов довгий шлях від простих інструментів для автоматизації повсякденних завдань до потужної платформи для інтегрованого управління інцидентами. Спочатку SOAR допомагав команді SIRT швидше та ефективніше виконувати повсякденні завдання, такі як збір та аналіз даних. З часом SOAR розширив свої можливості, інтегруючись з іншими інструментами безпеки та додаючи потужні аналітичні можливості. Це зробило його централізованою платформою, яка поєднує в собі управління, автоматизацію, аналітику та реагування на інциденти, забезпечуючи комплексний підхід до кібербезпеки.

Таким чином, SOAR не є окремим інструмент, а радше платформа, яка інтегрується з різними інструментами та системами кібербезпеки. Це дозволяє SOAR поєднувати дані та дії з різних джерел, забезпечуючи більш чітке та послідовне реагування на кіберінциденти.

Виділяють три принципи, актуальні для будь-якої системи SOAR:

Оркестрація – це процес координації дій різних інструментів та систем кібербезпеки. SOAR автоматично запускає різні інструменти, включаючи сканери вразливості, системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) для збору даних та реагування на кіберінциденти.

Автоматизація – це автоматичне виконання рутинних завдань, пов'язаних з реагуванням на кіберінциденти. SOAR може автоматизувати такі завдання, як збір даних про інциденти, аналіз даних, ізоляція заражених систем, оновлення програмного забезпечення та звітування.

Реагування являє собою комплекс заходів, спрямованих на нейтралізацію кіберзагроз і мінімізацію їх наслідків. SOAR допомагає організаціям швидко та ефективно реагувати на кіберінциденти, автоматизуючи рутинні завдання та забезпечуючи координацію між різними командами.

Абсолютна більшість систем SOAR складаються з кількох основних компонентів:

Плейбуки – це набори інструкцій, які визначають, як SOAR реагує на різні типи кіберінцидентів. Плейбук містить детальні кроки, які необхідно вжити, дані про IoC та іншу важливу інформацію, необхідну для ефективного реагування. Плейбуки SOAR пропонують ряд важливих переваг організаціям, які прагнуть підвищити свою стійкість до кіберзагроз. Незалежно від того, який фахівець задіяний, вона забезпечує стандартизований і послідовний підхід до реагування на інциденти, зводячи до мінімуму ризик помилок і забезпечуючи ефективність дій. Плейбуки легко оновлюються, що дозволяє організаціям швидко адаптуватися до нових загроз та вразливостей. Крім того, вони можуть бути розроблені з урахуванням конкретних потреб і середовища організації, забезпечуючи найбільш ефективне реагування на інциденти, заощаджуючи час і ресурси.

Користувальницький інтерфейс (UI) дозволяє фахівцям з кібербезпеки взаємодіяти з SOAR, відстежувати хід реагування на інциденти, запускати програми та виконувати інші дії.

Центр управління координує дії різних інструментів та систем кібербезпеки відповідно до програми.

Механізми автоматизації виконують рутинні завдання, визначені в плейбуках, такі як збір даних, їх аналіз та звітування.

База даних загроз містить інформацію про відомі кіберзагрози, такі як IoC та методи атаки. SOAR може використовувати цю інформацію для покращення виявлення та реагування на інциденти.

Модуль інтеграції дозволяє інтегруватись з іншими засобами забезпечення безпеки, такими як антивірусні програми, системи IDS/IPS, брандмауери і SIEM.

Модуль аналітики надає SOAR можливості аналізу даних про інциденти, дозволяючи експертам з кібербезпеки виявляти тенденції, розуміти першопричини інцидентів і вдосконалювати стратегії реагування.

Модуль звітності генерує звіт про інцидент, що містить інформацію про тип інциденту, час виявлення, вжиті заходи реагування та результати.

Виходячи з вищевикладеного, SOAR пропонує широкий спектр функцій, які допомагають організаціям підвищити стійкість до кіберзагроз. Автоматизуючи рутинні завдання, організації можуть скоротити час простою та підвищити ефективність. Інтеграція з інструментами кібербезпеки допомагає організаціям краще координувати свої зусилля з кібербезпеки та підвищує видимість кіберзагроз. Аналіз даних про інциденти допомагає організаціям виявляти тенденції, розуміти основні причини інцидентів та вдосконалювати стратегії реагування.

1.3 Аналіз існуючих систем автоматизації процесів реагування на інциденти

Для визначення рівня ефективності системи FortiSOAR, вважаю необхідним в порівняти її з іншими системами SOAR, представленими на ринку. Цей процес передбачає ретельну оцінку різних факторів, що впливають на функціональність, надійність та загальну цінність платформи.

Давайте детальніше розглянемо ключові критерії порівняння системи SOAR та пояснимо їх важливість та спосіб оцінки:

Основними критеріями оцінки є функціональні можливості системи: автоматизація, інтеграція та аналіз. Важливо порівняти можливості створення та запуску плейбуків в різних системах, розглянути здатність роботи зі складними сценаріями, оцінити можливість інтеграції з іншими інструментами, протестувати автоматизоване реагування на різні типи інцидентів і подивитись, чи може платформа автоматично покращувати дані про інциденти і організовувати важливі дії інструментів. Потрібно проаналізувати інструменти кібербезпеки, IT-системи та бізнес-додатки, які можуть інтеграції, оцінити простоту та гнучкість інтеграції та перевірити, чи пропонує постачальник SOAR додаткові модулі інтеграції. Оцінити здатність

виявляти загрози, оцінювати ризики та приймати обґрунтовані рішення щодо кібербезпеки, дозволяючи системі реагувати на інциденти, передбачати та запобігати їм.

Додатковими критеріями є технічні характеристики обладнання – масштабованість, надійність і безпека. Незалежно від розміру організації, SOAR повинен бути масштабованим, щоб відповідати потребам організації, забезпечуючи обробку великих обсягів даних та інтеграцію з багатьма інструментами. Надійність SOAR має вирішальне значення для забезпечення безперервної доступності 24 години на добу, 365 днів на рік. Важливо перевірити, чи пропонує SOAR план резервного копіювання та аварійного відновлення. Безпека платформи також важлива для захисту конфіденційних даних про інциденти, тому слід ознайомитися з методами шифрування, функціями контролю доступу та політикою безпеки постачальника SOAR.

Наступним, але не найменш важливим критерієм є вартість продукту: ціноутворення, рівень підтримки, онлайн-ресурси та відкритість документів.

Для порівняння створено таблицю з лідерами ринку SOAR: FortiSOAR, Palo Alto Networks Cortex XSOAR та McAfee MVISION Orchestration.

Таблиця 1.1

Порівняння функціональних можливостей систем

Критерій	FortiSOAR	Cortex XSOAR	McAfee MVISION Orchestration
Автоматизація	Висока автоматизація з 3000+ діями для плейбуків та 350+ інтеграцій	Висока автоматизація з сотнями інтеграцій і гнучкістю сценаріїв	Середня автоматизація, потребує покращення інтеграцій
Інтеграція	Широкі інтеграційні можливості, проте потребує більше документації для деяких випадків	Сильні інтеграційні можливості, підтримка багатьох платформ	Потребує покращення інтеграцій з іншими платформами
Аналітика	Автоматичне виявлення загроз,	Модель на базі машинного	Обмежена аналітика, зосереджена на

	фільтрація хибно-позитивних	навчання для покращення захисту	підписах
Плейбуки	Візуальний конструктор плейбуків для ефективного створення та відлагодження	Автоматизовані плейбуки з аналізом та звітністю	Основні функції створення та виконання плейбуків
Простота використання	Інтуїтивний інтерфейс, потребує вдосконалення	Інтуїтивний і легко зрозумілий інтерфейс	Середня простота використання, потребує покращення

Таблиця 1.2.

Порівняння технічних характеристик систем

Критерій	FortiSOAR	Cortex XSOAR	McAfee MVISION Orchestration
Масштабованість	Підтримка мульти-оренди, гнучкі варіанти розгортання (VM, хмарні)	Висока масштабованість завдяки інтеграції з GCP	Обмежена масштабованість, потребує покращення
Надійність	Висока надійність завдяки резервуванню та кластеризації	Висока надійність, реалістичні аварійні плани	Середня надійність, потребує кращих планів відновлення
Безпека	Міцні функції контролю доступу, шифрування	Інтегрована керування загрозами в реальному часі	Обмежена безпека, потребує покращення інтеграції з іншими інструментами

Таблиця 1.3.

Порівняння підтримки користувачів

Критерій	FortiSOAR	Cortex XSOAR	McAfee MVISION Orchestration
Ціноутворення	Ліцензування та підписка, без плати за початкове налаштування	Без плати за початкове налаштування, може бути дорогим для великих обсягів	Включено в Microsoft підписки, зміни в залежності від обсягу даних

		даних	
Підтримка	Необхідність покращення підтримки клієнтів	Висока якість підтримки, з акцентом на стратегічні інновації	Середня підтримка, потребує кращої документації
Ресурси та документація	Необхідно більше документації для специфічних випадків	Гарна документація та спільнота користувачів	Обмежена документація, потребує покращення

На основі проаналізованих даних можемо зробити висновок, що FortiSOAR це одне з найкращих рішень на ринку, оскільки воно має інтуїтивно зрозумілий інтерфейс drag-and-drop, що робить його доступним для користувачів з різним рівнем досвіду, полегшує створення та управління плейбуками та сприяє швидкому реагуванню на інциденти. Надаючи вбудовану інтеграцію з більш ніж 350 інструментами кібербезпеки, IT-системами і бізнес-додатками, він автоматизує реагування на інциденти і збирає дані з різних джерел, щоб отримати чітке уявлення про ситуацію. Завдяки обробці великих обсягів даних про інциденти FortiSOAR може бути поширений на організації будь-якого розміру, від малих до великих підприємств. Різні моделі ліцензування, включаючи безкоштовну пробну версію, забезпечують економічність. Інші переваги включають автоматизоване реагування, що використовує понад 3000 готових вбудованих плейбуків, збагачення даних з більш ніж 100 джерел, оркестрацію інструментів кібербезпеки, аналітику з використанням машинного навчання, шифрування даних, управління доступом на основі ролей і цілодобову підтримку клієнтів.

2 АНАЛІЗ МЕТОДІВ АВТОМАТИЗАЦІЇ ПРОЦЕСІВ РЕАГУВАННЯ НА ІНЦИДЕНТИ ІЗ ЗАСТОСУВАННЯМ FORTISOAR

2.1 Призначення, рішення та архітектура FortiSOAR

FortiSOAR – це система управління інцидентами та координації дій (SOAR), розроблена компанією Fortinet, призначена для гнучкого впровадження в організаціях різного розміру і структури, від малого бізнесу до великих компаній з розподіленими підрозділами. Центральним компонентом системи є центральний сервер, який забезпечує автоматизацію процесів обробки даних, управління інцидентами і реагування. Центральний сервер взаємодіє з різними джерелами даних, включаючи системи управління безпекою, сервери журналів, системи ідентифікації та контролю доступу (IAM) та інші інструменти кібербезпеки. Потужна реляційна база даних забезпечує надійне зберігання всіх даних про інциденти, сценарії, журнали та інші пов'язані дані.

FortiSOAR підтримує розподілену архітектуру, яка дозволяє розгортати системи в різних географічних регіонах або підрозділах організації. Це забезпечує високу масштабованість і дозволяє обробляти великі обсяги даних з різних джерел без шкоди для продуктивності. Наприклад, великі компанії можуть розгорнути FortiSOAR у своїх регіональних офісах для забезпечення локальної обробки даних та швидкого реагування на інциденти. В федеративній архітектурі FortiSOAR розгортається за допомогою основних серверів (master node) та додаткових серверів (tenant node) у різних підрозділів або клієнтів. Це дозволяє обробляти дані локально, зберігаючи при цьому централізоване управління та координацію через головний сервер [8].

Висока доступність FortiSOAR забезпечується за рахунок кластеризації та реплікації даних. Система підтримує як активний/пасивний, так і

активний/активний режими, які забезпечують безперебійну роботу в разі виходу з ладу окремих компонентів. Наприклад, якщо один сервер виходить з ладу, інший сервер автоматично бере на себе його функції, щоб забезпечити безперервність обробки даних та реагування на інциденти. Завдяки стандартизованим API та конекторам ви можете легко інтегрувати свої системи в існуючу інфраструктуру безпеки вашої організації, гнучко інтегруючи їх з різними інструментами кібербезпеки та іншими системами [12].

Модульна архітектура FortiSOAR дозволяє організаціям додавати нові функції за допомогою модулів та плагінів. Це забезпечує гнучкість і можливість адаптації системи до змін в потребах організації. Наприклад, при появі нових типів загроз або впровадженні нових технологій організації можуть легко додати потрібні модулі для їх усунення, що дозволяє FortiSOAR ефективно реагувати на нові виклики і підтримувати високий рівень безпеки.

Практичний приклад демонструє ефективність архітектури FortiSOAR та її масштабованість. Великі міжнародні компанії використовують FortiSOAR для централізованого управління безпекою у всіх регіональних офісах. Система розгортається в кожному регіоні з використанням розподіленої архітектури, що дозволяє обробляти інциденти локально і швидко реагувати на загрози. Центральний сервер, що знаходиться в головному офісі, координує всю діяльність і забезпечує загальне управління політиками безпеки.

Постачальники послуг використовують FortiSOAR для надання послуг безпеки своїм клієнтам. Федеративна архітектура дозволяє постачальникам розгортати клієнтські вузли в інфраструктурі кожного клієнта для забезпечення локальної обробки даних та ізоляції. Головний сервер в центрі обробки даних провайдера координує дії і забезпечує централізоване управління політиками безпеки. Малі підприємства впроваджують FortiSOAR у своїх локальних мережах для автоматизації реагування на

інциденти та інтеграції з існуючими системами безпеки. Гнучка інтеграція та модульна архітектура дозволяють компаніям додавати нові функції по мірі зростання їх потреб і появи нових загроз.

Таким чином, архітектура та масштабованість FortiSOAR забезпечують високу продуктивність, надійність та гнучкість у впровадженні та використанні системи в різних організаціях. FortiSOAR дозволяє ефективно інтегруватися з існуючими інфраструктурами безпеки, масштабуватися відповідно до потреб організації та забезпечувати високу доступність і безперервність роботи.

Плейбуки FortiSOAR – це автоматизовані плани дій, які визначають, як ваша система реагує на різні типи кіберінцидентів. Вони складаються з назви, що описує призначення, детальної мети та сфери застосування, умов, що визначають час запуску playbook, та набір дій, які повинна виконати система. Дії включають збір додаткових даних про інциденти, ізоляцію заражених систем, нейтралізацію загроз, подання звітів експертам з кібербезпеки та запуск інших програм. Завершення визначає, що відбудеться після завершення всіх дій, таких як закриття інциденту, створення звіту або надсилання повідомлення. Використання Плейбуків забезпечує стандартизацію, ефективність, точність, оперативність і економію коштів. FortiSOAR надає зручний інтерфейс для створення та налаштування плейбуків, що дозволяє користувачам перетягувати дії, додавати умови, визначати тригери та налаштовувати інші параметри. Приклади використання плейбуків включають реагування на фішинг (ізоляція користувачів, сканування шкідливих програм, скидання паролів), витік даних (закриття облікових записів, повідомлення регуляторним органам, інформування жертв) та атаки (сканування мереж, ізоляція заражених систем, оновлення та усунення загроз).

Інтеграції FortiSOAR дозволяють системі обмінюватися даними та взаємодіяти з різними інструментами кібербезпеки та IT-системами всередині організації. Це покращує видимість, забезпечує єдине уявлення

всіх даних про кібербезпеку з різних джерел і дозволяє експертам швидко виявляти кіберзагрози і реагувати на них. Це також автоматизує повсякденні завдання та координує складні процеси реагування на інциденти, заощаджуючи час та ресурси. Інтеграція також підвищує ефективність реагування на кіберінциденти і знижує ризики за рахунок поліпшення видимості і автоматизації. Завдяки інтеграції з інструментами SIEM, антивірусами, брандмауерами, системами EDR і т.д., розширюються можливості системи і дозволяється FortiSOAR використовувати ці можливості для розширення своїх власних можливостей. FortiSOAR пропонує вбудовану інтеграцію з популярними інструментами кібербезпеки та IT-системами, інтеграцію, яка використовує API для створення користувацьких інтеграцій, інтеграцію з маркетплейсом та широку інтеграцію зі сторонніми постачальниками [12]. Приклади інтеграцій включають інтеграцію з SIEM для збору та аналізу даних про безпеку з різних джерел, інтеграцію з антивірусними програмами для автоматизації карантину та видалення шкідливих програм, інтеграцію з брандмауерами для блокування шкідливого трафіку та автоматизації реагування на мережеві атаки, збір даних про кінцеві точки, а також інтеграцію з системами EDR, які виявляють підозрілу активність і реагують на неї. до кіберзагроз на рівні кінцевих точок.

Консоль FortiSOAR – це веб-інтерфейс, який використовується для управління системою. Фахівцям з кібербезпеки надається широкий спектр можливостей, включаючи моніторинг інцидентів, розслідування інцидентів, управління плейбуками, агентами, користувачами та налаштування системи. У консолі є можливість переглядати активні та закриті інциденти, переглядати детальну інформацію, шукати дані про інциденти, аналізувати журнали, переглядати мережеву активність, створювати та редагувати плейбуки, керувати агентами, розгортати оновлення та нові плейбуки, створювати, редагувати, видаляти облікові записи користувачів, призначати ролі тощо. Є можливість керувати дозволами, інтеграціями, налаштовувати

звіти, сповіщення та журнали. Переваги використання консолі включають централізоване управління, простоту використання, гнучкість, масштабованість та безпеку. Інші функції консолі включають створення інформаційних панелей, генерацію звітів та налаштування сповіщень. Система також надає мобільний додаток, який дозволяє фахівцям з кібербезпеки отримувати доступ до важливої інформації та виконувати основні дії поза робочим місцем. Мобільний додаток забезпечує моніторинг інцидентів у режимі реального часу, отримання сповіщень про критичні події, затвердження або відхилення дій, передбачених сценарієм, спілкування з командами та перегляд даних про критичні інциденти [9]. Переваги використання мобільного додатка включають підвищену мобільність, обізнаність, швидку реакцію та ефективну співпрацю між членами вашої команди з кібербезпеки.

2.2 Порядок функціонування рішення FortiSOAR

FortiSOAR – це комплексна платформа для автоматизації та оркестрації реагування на інциденти, яка збирає, обробляє та аналізує дані з різних джерел, включаючи SIEM, IPS-системи та інші. Вона автоматично оцінює ризики, зіставляє дані і запускає програми швидкого реагування. Платформа розширює дані з глобальної бази даних про загрози, автоматично збільшує кількість складних інцидентів і інтегрується з існуючими інструментами кібербезпеки. FortiSOAR підтримує розподілену архітектуру, що забезпечує масштабованість і високу доступність за рахунок кластеризації, що забезпечує ефективну командну взаємодію та IT-безпеку.

Рис. 2.1. Спрощений принцип реакції на інциденти

Збір та Обробка Даних

FortiSOAR – це комплексна платформа для автоматизації та оркестрації реагування на інциденти, яка збирає, обробляє та аналізує дані з різних джерел, включаючи SIEM, IPS-системи та інші. Вона автоматично оцінює ризики, зіставляє дані і запускає програми швидкого реагування. Платформа розширює дані з глобальної бази даних про загрози, автоматично збільшує кількість складних інцидентів і інтегрується з існуючими інструментами кібербезпеки. FortiSOAR підтримує розподілену архітектуру, що забезпечує масштабованість і високу доступність за рахунок кластеризації, що забезпечує ефективну командну взаємодію та IT-безпеку.

FortiSOAR збирає та обробляє дані з різних джерел у режимі реального часу, надаючи повну картину подій в IT-інфраструктурі. Системи управління безпекою, такі як SIEM, забезпечують логи з брандмауерів, систем запобігання вторгненням (IPS), антивірусних програм та інших інструментів кібербезпеки. Це забезпечує велику базу даних для аналізу та зіставлення, що допомагає виявити потенційні загрози. Наприклад, у журналах брандмауера можуть відображатися підозрілі підключення, а в журналах антивірусної системи - виявлені шкідливі файли.

Отримавши попередження, FortiSOAR виконує початковий аналіз для оцінки його серйозності. Система автоматично зіставляє дані з різних джерел і виявляє зв'язки між подіями, які можуть бути непомітні при розгляді окремо. Наприклад, алерти від SIEM можуть поєднуватися з даними з IDS для виявлення складних атак на декількох рівнях інфраструктури. Автоматична оцінка ризиків для кожного оповіщення допомагає визначити пріоритетність загроз, приділяючи особливу увагу найбільш важливим інцидентам [14].

FortiSOAR також збагачує дані про загрози, додаючи контекстні та історичні дані з інших джерел. Це включає звернення до глобальних баз даних, таких як FortiGuard Labs, для отримання додаткової інформації про відомі загрози. Наприклад, якщо в попередженні вказано IP-адресу, пов'язану зі зловмисною активністю, FortiSOAR додає дані про попередні атаки з цієї адреси.

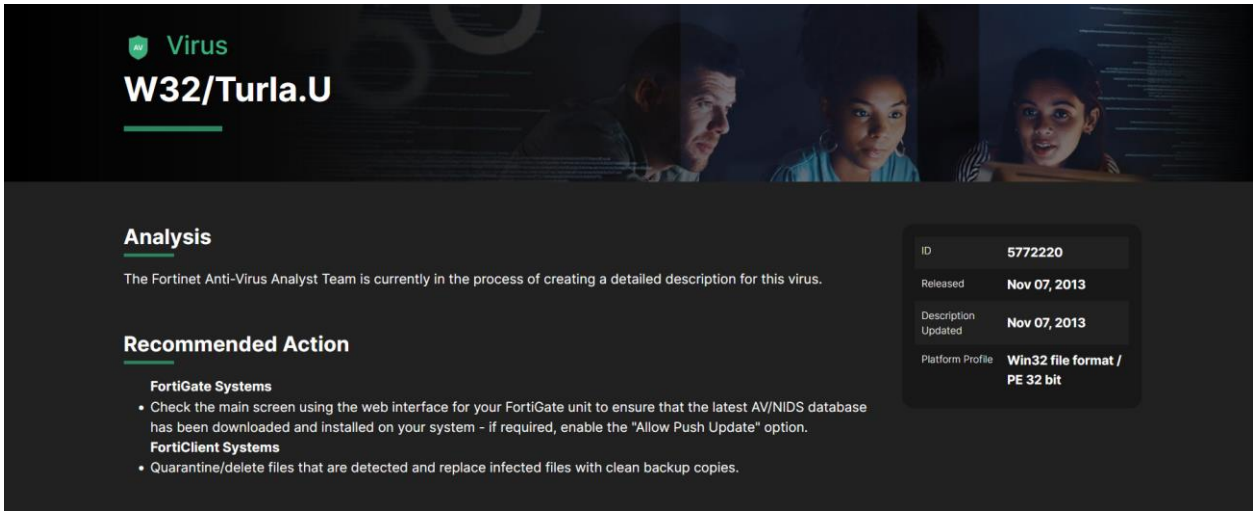

Рис. 2.2. Веб-версія FortiGuard Labs

Обробка даних у FortiSOAR включає автоматизоване прийняття рішень на основі зібраних та проаналізованих даних. Наприклад, якщо система виявляє підозрілу активність, вона може автоматично блокувати IP-адреси або ізолювати заражені пристрої, щоб запобігти поширенню загроз. Плейбуки, налаштовані в системі, перевіряють дані із зовнішніх джерел,

ескалюють інциденти, повідомляють про порушників та інші події, пов'язані з інцидентом, що забезпечує швидке та ефективне реагування на загрози та знижує ризик успішної атаки.

FortiSOAR може автоматично документувати всі виконані дії і результати та зберігати всю інформацію, необхідну для подальшого аналізу і вдосконалення процесу реагування [11]. Якщо інцидент вимагає додаткового розслідування, система направить відповідних експертів і надасть їм всю необхідну інформацію для прийняття рішення. Наприклад, якщо автоматичних заходів недостатньо для усунення інциденту, система може передати його аналітику високого рівня для більш глибокого аналізу та ручного втручання.

Таким чином, FortiSOAR забезпечує комплексний підхід до збору та обробки даних, автоматизує процеси та забезпечує швидке та ефективне реагування на загрози IT-інфраструктурі організації. Це може значно підвищити ефективність роботи команди, скоротити час обробки інцидентів і звести до мінімуму вплив людського фактора.

Автоматизація Реагування

FortiSOAR забезпечує комплексну автоматизацію реагування на інциденти, чим значно підвищує ефективність і швидкість обробки загроз в IT-інфраструктурі. Одним з основних компонентів автоматизації є плейблуки – попередньо налаштовані алгоритми дій, які система використовує для реагування на різні типи загроз. Наприклад, якщо FortiSOAR отримує попередження про підозрілу активність на мережевому рівні, система автоматично запускає алгоритм дій, який включає блокування підозрілих підключень, перевірку додаткових даних і повідомлення відповідальних осіб, що дозволяє негайно реагувати на інциденти і мінімізувати затримки, пов'язані з ручною обробкою.

Автоматичне оновлення даних – ще один важливий аспект роботи FortiSOAR. Система автоматично отримує доступ до глобальної бази даних загроз, таких як FortiGuard Labs та інші зовнішні API, щоб отримати

додатковий контекст для поточної загрози. Наприклад, якщо в алерті вказано IP-адресу, пов'язану зі шкідливою активністю, FortiSOAR автоматично перевіряє цю адресу на наявність її у списку відомих зловмисників, щоб більш точно оцінити ризик та прийняти обґрунтовані рішення щодо подальших дій [7].

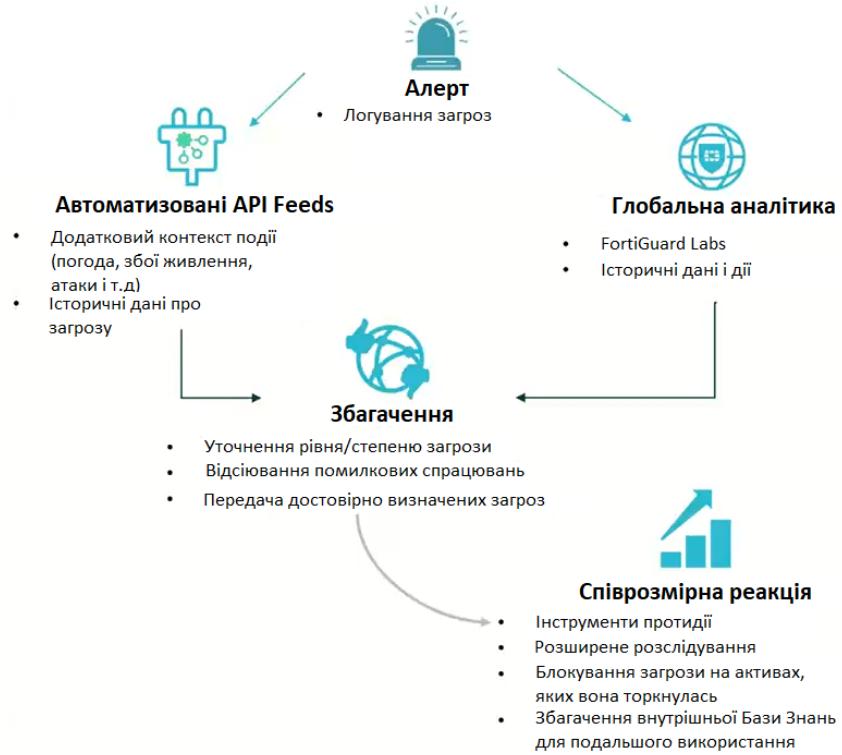

Рис. 2.3. Алгоритм обробки даних FortiSOAR

Якщо автоматичні заходи виявляться недостатніми, FortiSOAR може автоматично ескалувати інформацію про інцидент спеціалісту вищого рівня. Система передає всю зібрану інформацію, включаючи результати попередніх дій і додатковий контекст, що дозволяє фахівцям швидко розібратися в ситуації і вжити необхідних заходів. Наприклад, якщо інцидент вимагає ручного втручання, система повідомить відповідних аналітиків і надасть їм доступ до всієї інформації, необхідної для швидкого прийняття рішень.

Автоматичне прийняття рішень – ще одна важлива особливість FortiSOAR. Система дозволяє виконувати дії автоматично на основі зібраних даних і певних правил. Наприклад, при виявленні підозрілої активності

система автоматично блокує IP-адреси або ізолює заражені хости, щоб запобігти поширенню загроз [12]. Такий підхід значно скорочує час реагування на інциденти та мінімізує шкоду від атак.

Документування всіх виконаних дій та результатів є невід'ємною частиною автоматизації FortiSOAR. Система автоматично зберігає логи, створює звіти і веде історію всіх інцидентів. Це забезпечує повну прозорість і контроль над процесами безпеки, дозволяючи аналітикам зосередитися на більш складних завданнях. Наприклад, при виявленні нової загрози система документує всі вжиті заходи для її нейтралізації, і цей досвід може бути використаний для поліпшення реагування в майбутньому.

Таким чином, система автоматизації реагування FortiSOAR забезпечує швидке, ефективне і послідовне реагування на інциденти, знижує ризики і підвищує загальну безпеку IT-інфраструктури вашої організації. За допомогою цієї системи можливо миттєво реагувати на загрози, автоматично збагачувати свої дані, аналізувати складні інциденти і приймати обґрунтовані рішення на основі найсвіжішої інформації.

Ескалація та Співпраця у FortiSOAR

FortiSOAR забезпечує ефективну ескалацію інцидентів та співпрацю між командами, що має вирішальне значення для швидкого та ефективного реагування на загрози IT-інфраструктурі. Автоматична ескалація дозволяє системі передавати інциденти експертам вищого рівня, коли автоматизованих заходів недостатньо. Наприклад, якщо FortiSOAR виявить складну загрозу, яка вимагає ретельного розслідування, вона може автоматично надіслати повідомлення про інцидент аналітику, який має необхідні знання. Система передає всю зібрану інформацію, включаючи результати попередніх дій і ситуаційні дані, дозволяючи фахівцям швидко розібратися в ситуації і вжити необхідних заходів.

Аналітики також можуть вручну ескалувати інциденти, якщо виявлять, що загроза вимагає додаткового втручання або якщо потрібні додаткові ресурси. Наприклад, якщо аналітик виявить, що інцидент пов'язаний з новим

типом зловмисного програмного забезпечення, він може сформувати відповідну команду для поглибленого аналізу та розробки нових заходів захисту. FortiSOAR підтримує багаторівневу ескалацію і може передавати інциденти між аналітиками та менеджерами на різних рівнях. Наприклад, інцидент може бути спочатку оброблений аналітиком першого рівня, потім переведений на другий рівень для більш детального аналізу, а потім на третій рівень для прийняття стратегічних рішень.

Співпраця між командами FortiSOAR дозволяє різним експертам працювати в єдиному інтегрованому середовищі, обмінюватися інформацією та координувати дії для більш ефективного реагування на інциденти, наприклад, аналітики можуть використовувати єдину платформу для розслідування складних загроз та обміну інформацією для прийняття рішень. За допомогою FortiSOAR команди можуть обмінюватися всією необхідною інформацією про інцидент, включаючи ситуаційні дані, історію інцидентів, результати попередніх дій та інші важливі дані.

FortiSOAR підтримує гнучкий доступ на основі ролей, що дозволяє встановлювати права доступу до інформації та дій у системі відповідно до ролі користувача. Це забезпечує безпеку та конфіденційність даних, дозволяючи кожній команді чи експерту отримувати доступ лише до інформації, необхідної для виконання завдання. Наприклад, аналітики можуть отримати доступ до даних про інциденти, а менеджери - до звітів та статистики для прийняття стратегічних рішень. FortiSOAR також інтегрований з різними засобами комунікації, такими як електронна пошта, системи управління завданнями, які забезпечують ефективну координацію між командами.

Далі давайте розглянемо весь процес автоматичного реагування на інциденти, що забезпечується технологією FortiSOAR. Процес реагування на інциденти у FortiSOAR починається з отримання алертів з різних джерел, таких як FortiSIEM, та інформації про потенційні загрози через конектори [13]. Алерти агрегуються, сортуються та встановлюються пріоритети для

створення інцидентів, які потребують подальшого розслідування. Якщо автоматичних заходів недостатньо, справа передається фахівцям більш високого рівня для детального розслідування. Аналітики використовують FortiSOAR для збору додаткової інформації, аналізу контекстних даних та визначення характеру загрози. За результатами розслідування створюються завдання і запускається плейбук — попередньо налаштований алгоритм дій, який може включати блокування IP-адрес, ізоляцію заражених пристроїв, оновлення політик безпеки.

Плейбуки також включають дії з обробки та відновлення системи після інциденту. FortiSOAR автоматично виконує необхідні дії для нейтралізації загрози і відновлення нормального функціонування системи. Після виконання всіх дій кроки та результати документуються, зберігаються журнали та створюються звіти. Якщо загроза нейтралізована, інцидент закривається, а результати аналізуються для поліпшення процесу реагування. Це забезпечує швидке, ефективне та автоматизоване реагування на загрози, мінімізацію ризиків та забезпечення загальної безпеки IT-інфраструктури організації.

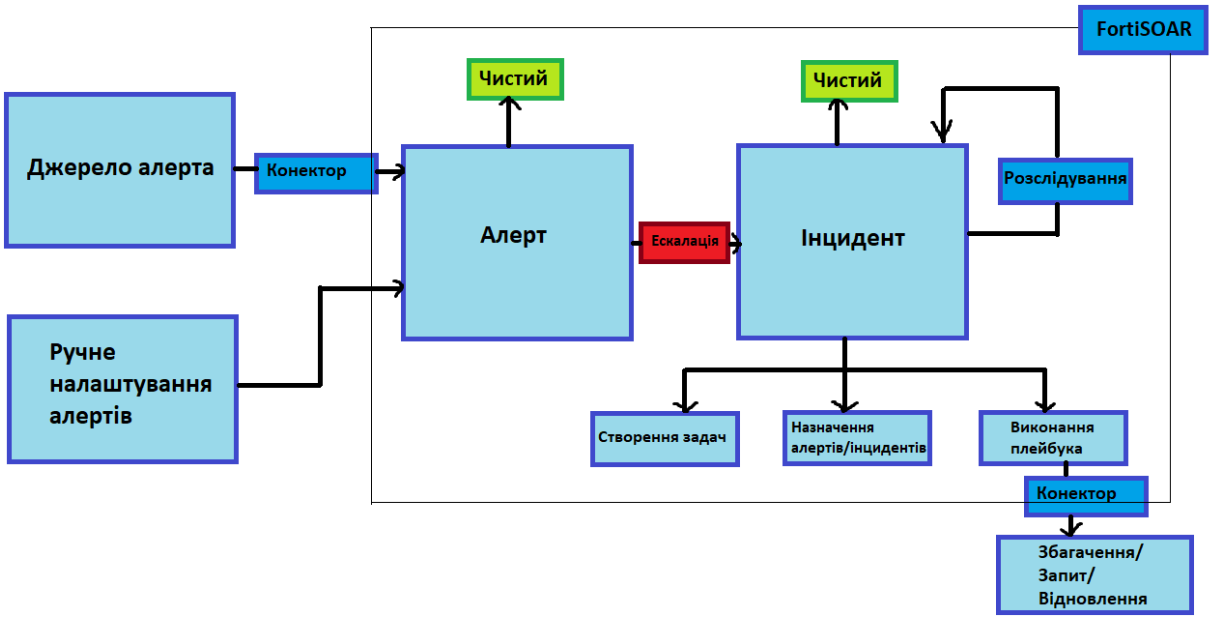

Рис. 2.4. Алгоритм обробки алертів FortiSOAR

2.3 Процес розгортання FortiSOAR на віртуальній інфраструктурі організації

Щоб ефективно впровадити FortiSOAR в інформаційну структуру організації, необхідно оцінити потреби для належного функціонуванні системи. У поточному прикладі, щоб проаналізувати процес розгортання FortiSOAR у віртуальній машині Vsphere, ми розглянемо технічні характеристики, необхідні для віртуальної машини. Інші вимоги універсальні як для фізичних, так і для віртуальних систем, а також для гібридних систем.

Рекомендовані характерстики для віртуальних машин включають 8 вільних vCPU, 32 ГБ оперативної пам'яті, 1 ТБ вільного місця на диску (рекомендується використовувати високопродуктивний SSD) і 1 віртуальний мережевий інтерфейс (vNIC). Використання дискового простору в значній мірі залежить від потреб, політик зберігання даних аудиту та робочих процесів. Для більш точного прогнозування використання бази даних є можливість використовувати команду csadm db --getsize, яка повертає розміри журналів робочих процесів, аудиту та основних даних.

Крім того, треба налаштувати мережеві параметри віртуальної машини та забезпечити доступність портів для вхідного і вихідного трафіку: 22 (управління по SSH), 25 (сервер ретрансляції електронної пошти SMTP) і 443 (користувальницький інтерфейс HTTPS).

Існують також особливі вимоги до інших компонентів FortiSOAR. Наприклад, для забезпечення захищеного обміну повідомленнями (Secure Message Exchange) рекомендовано використовувати VM з 8 вільними vCPU, 16 ГБ вільної RAM, 100 ГБ вільного місця на диску (рекомендується високопродуктивні SSD) та 1 vNIC. Для агентів FSR рекомендовано використовувати VM з 2 вільними vCPU, 4 ГБ вільної RAM та 10 ГБ вільного місця на диску, працюючих під управлінням Rocky Linux 9.3 або Red Hat Enterprise Linux Server release 9.3 [3].

Доступ до інтернету необхідний для оновлення обладнання FortiSOAR,

розгортання ліцензій та встановлення нових конвекторів. Потрібно додати наступний запис до списку дозволів брандмауера або проксі-сервера: для встановлення або оновлення до FortiSOAR або пізнішої версії – *.rockylinux.org, для оновлення FortiSOAR, встановлення з'єднувачів та доступу до бібліотеки віджетів – repo.fortisoar.fortinet.com, для залежностей з'єднувачів – pypi.python.org, для синхронізації даних ліцензії FortiSOAR – globalupdate.fortinet.net [3].

Для внутрішньої комунікації між сервісами на пристрої FortiSOAR необхідно забезпечити доступність наступних портів: Elasticsearch (9200 та 9300), RabbitMQ (5671, 5672, 4369, 15672, 25672), Cyops-Postman (7575), FSR-Workflow (8888), PostgreSQL (5432), Cyops-Auth (8443), Cyops-Integrations-Agent (9595), Cyops-Tomcat (8080), MQ TCP трафік (5671), Cyops-API (443) [3].

Підготувавши віртуальну машину, згідно з потребами, можемо підходити до розгортання системи.

Перед початком інтеграції з FortiSOAR необхідно завантажити образ віртуального пристрою FortiSOAR з порталу підтримки [6]. Після запуску образу SOAR у віртуальній машині потрібно переконатися, що віртуальна машина має доступ до repo.fortisoar.fortinet.com. Важливо звернути увагу, що інсталятор FortiSOAR обмежує доступ до SSH лише для користувачів root та csadmin, які є членами групи "wheel". Після встановлення користувачі, які не входять до цієї групи, не зможуть увійти до FortiSOAR, тому, тому додайте користувача, який не є root і може входити до FortiSOAR за допомогою SSH, до групи "wheel" перед початком інсталяції.

Після інсталяції FortiSOAR необхідно інсталювати також Secure Message Exchange. Для цього треба запустити команду tmux, щоб уникнути проблем з часом очікування сесії. Потім, завантажуємо інсталяційний файл за допомогою команди wget. Встановлення програми можна запустити введенням команди sh install-fortisoar-7.5.0.bin або після зміни прав доступу файла через chmod +x install-fortisoar-7.5.0.bin і виконання ./install-fortisoar-

7.5.0.bin. Після цього слід встановити SFSP, що можна зробити через Content Hub > Discover, шукаючи SOAR Framework і вибравши відповідний пакет для встановлення [3].

Після встановлення та запуску програми треба увійти у систему та змінити стандартний пароль. Після введення імені користувача "csadmin" та паролю "changeme", система попросить вас оновити ці дані. Після виконання цих дій з’явиться доступ до більш детальної настройки середовища FortiSOAR і управління ним.

І останній, але не менш важливий, етап встановлення всіх елементів – це встановлення агентів FortiSOAR (FSR), які використовуються для автоматизації реагування на інциденти безпеки та збору даних у різних точках мережі. Це дозволяє здійснювати моніторинг, виконання сценаріїв та інтеграцію з різними системами безпеки, що значно підвищує швидкість та ефективність реагування на загрози. Агенти FSR можна використовувати для виконання критичних функцій безпеки на серверах або робочих станціях, які потребують прямого моніторингу, або в IT-інфраструктурі вашої організації.

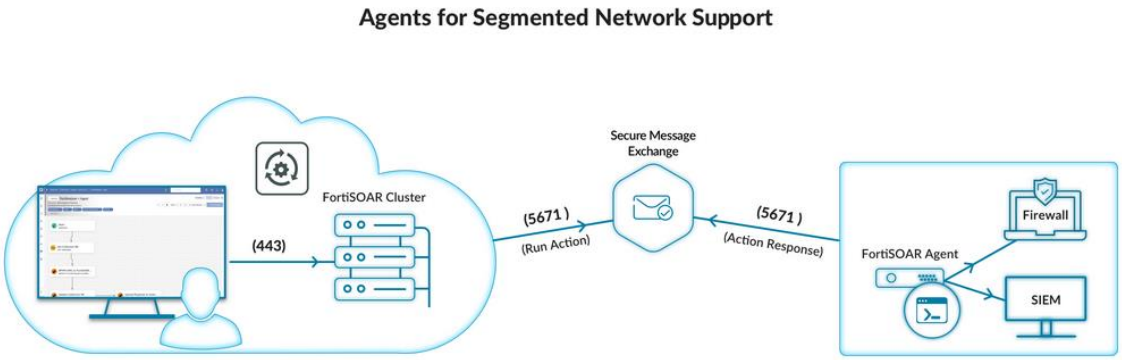

Рис. 2.5. Використання елементів FortiSOAR [3]

Процес встановлення FSR починається із завантаження відповідного інсталяційного пакету з сайту Fortinet. Розгортання FSR знаходиться останнім в списку, оскільки всі необхідні налаштування вже були виконані в попередніх пунктах. Інсталяційний скрипт запускається в терміналі з

правами адміністратора, і в процесі встановлення потрібно ввести параметри конфігурації, такі як налаштування мережі SOAR та дані автентифікації, налаштовані в попередньому абзаці. Після завершення інсталяції важливо перевірити підключення агента до сервера FortiSOAR і забезпечити автоматичний запуск під час старту системи.

Переглянемо базові налаштування FortiSOAR.

Майстер налаштування FortiSOAR запускається автоматично, коли користувач csadmin вперше входить через ssh і керує початковим налаштуванням системи. Процес починається з прийняття Ліцензійної угоди користувача Fortinet. Майстер надає інструкції на кожному етапі, щоб спростити процес налаштування системи.

Одним із перших кроків є зміна імені хосту та оновлення імені вузла MQ. Цей крок необов'язковий, але важливий для забезпечення, що ім'я хоста може бути розв'язане. Для статичних IP-адрес, якщо майстер не може визначити IP-адресу, ви можете налаштувати статичну IP-адресу, шлюз, мережеву маску та DNS-сервер вручну.

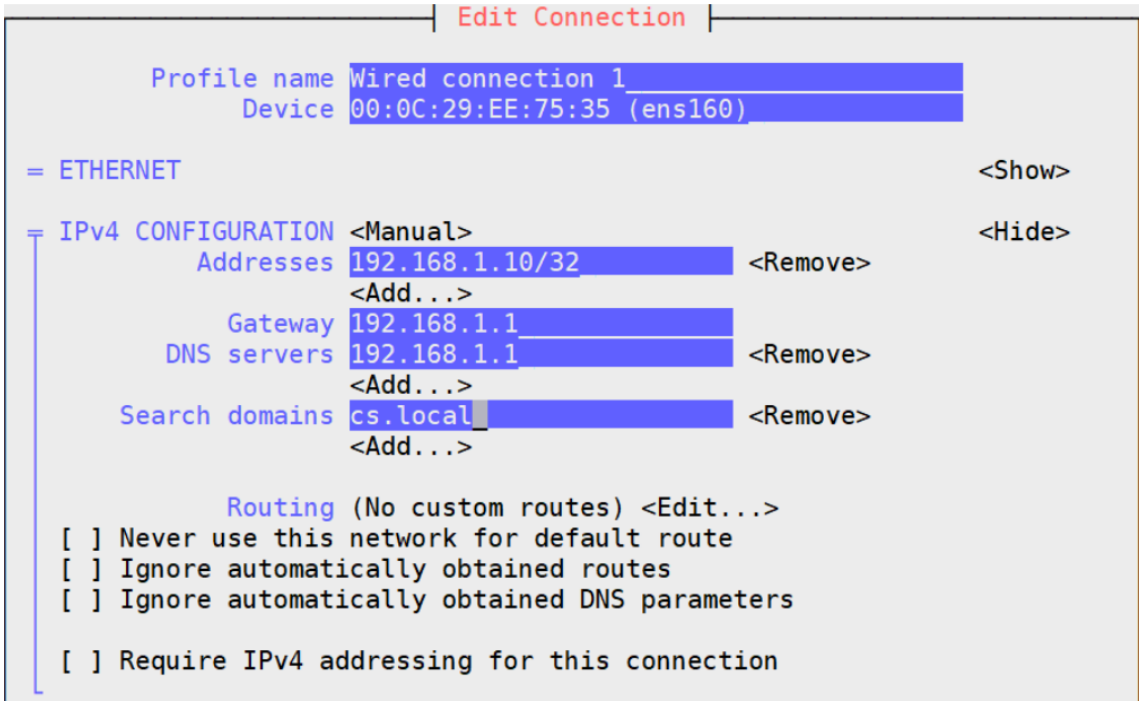

Рис. 2.6. Приклад конфігурації мережі [3]

Автоматичні процеси майстра включають оновлення мережевих конфігурацій, налаштування автентифікації між службами, генерацію сертифікатів та ключів пристрою, ініціалізацію пошукових індексів, встановлення бібліотек Python та стандартних віджетів. Важливо, що після завершення налаштувань користувач мусить повторно увійти в систему, щоб зміни вступили в силу.

Якщо під час налаштування виникає помилка, майстер відображає екран несправності з детальною інформацією про стан кожного кроку налаштування. Це полегшує виявлення та усунення несправностей. Якщо FortiSOAR не запускається навіть після вибору “Продовжити без виправлення помилок”, користувач може перезапустити служби або повторно запустити конфігурацію за допомогою команд CLI.

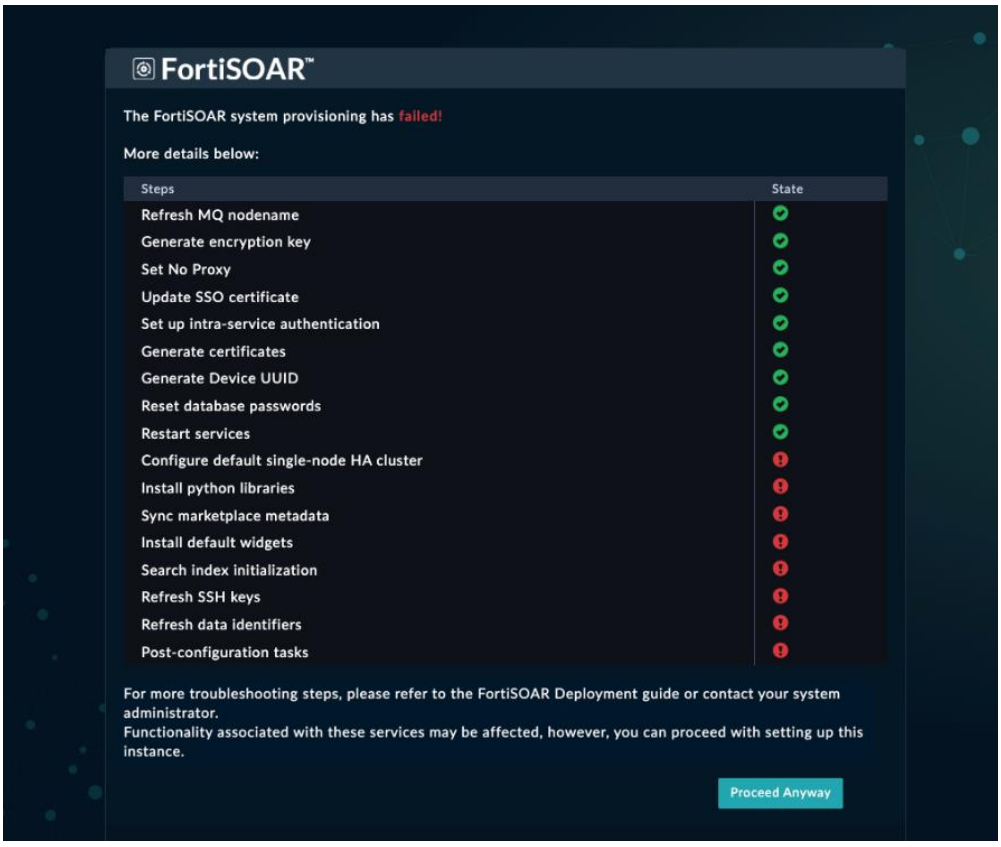

Рис. 2.7. Екран помилки [3]

Створення резервного користувача для FortiSOAR є ключовим кроком для забезпечення доступу до командного рядка (CLI), якщо основний

обліковий запис csadmin буде заблоковано або втрачено його пароль. Почніть із входу в систему як користувач csadmin і виконайте команду sudo su для отримання прав суперкористувача.

Далі створіть нового користувача командою adduser csadmin-bkp і встановіть для нього пароль через passwd csadmin-bkp, та запам'ятайте його. Завершальний крок – додавання користувача до групи wheel за допомогою usermod -aG wheel csadmin-bkp, що надає йому адміністративні права. Ці дії гарантують наявність резервного доступу до системи у випадку необхідності.

Останнім кроком для базових налаштувань є додавання Secure Message Exchange.

Щоб створити захищений канал обміну повідомленнями в системі FortiSOAR, важливо виконати певні кроки налаштування. Цей процес дозволяє розподіляти клієнтів через захищені канали обміну повідомленнями на основі географічного розташування, розміру або політики відповідності різним клієнтам.

Спочатку ви повинні увійти до FortiSOAR як адміністратор, оскільки роль адміністратора повинна включати дозволи на створення, оновлення та видалення в модулях Secure Message Exchange. Відкрийте сторінку системних налаштувань, вибравши іконку налаштувань у системному меню, та перейдіть до секції конфігурації агентів. Тут можна додати новий обмін повідомленнями, вибравши відповідний пункт меню.

На сторінці Secure Message Exchanges клікніть на "Add Secure Message Exchange". Зверніть увагу, що для налаштування клієнтів та обміну повідомленнями роль повинна мати принаймні дозволи на створення та читання відповідних модулів. Щоб змінити налаштування існуючої служби обміну повідомленнями, виберіть відповідний рядок та оновіть налаштування у діалоговому вікні редагування.

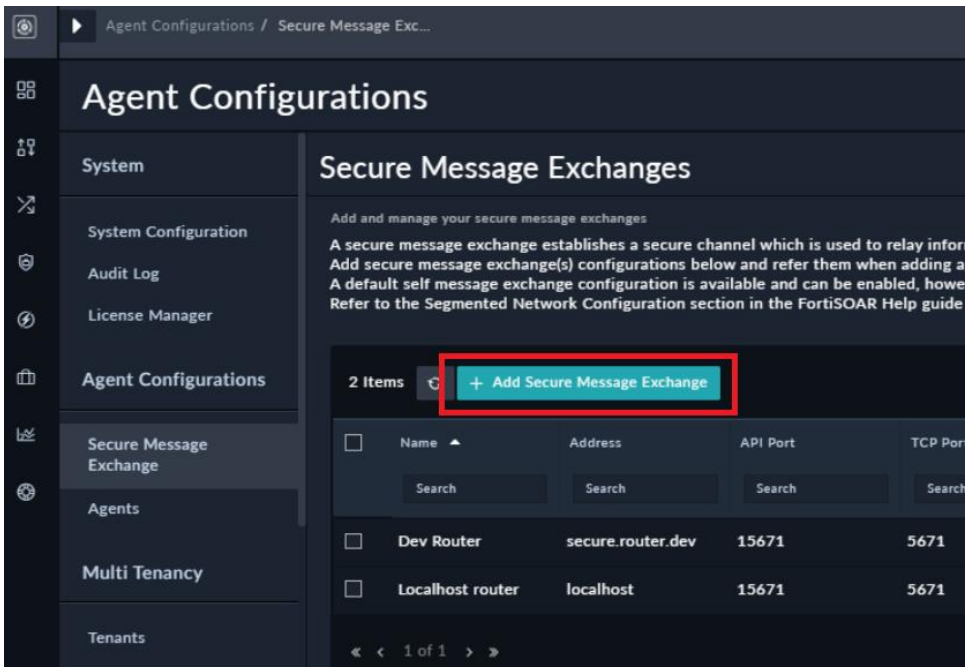

Рис. 2.8. Додавання Secure Message Exchanges [3]

Під час налаштування нового обміну повідомленнями необхідно вказати такі параметри: ім'я, повністю кваліфіковане ім'я хоста (FQHN), що відповідає імені, вказаному в сертифікаті SSL, ім'я користувача та пароль адміністратора, адресу SNI для обміну повідомленнями, порт управління RabbitMQ та порт TCP, які використовувались під час конфігурації, а також текст сертифікату CA у форматі pem. Зазначте також, що якщо сертифікат змінюється, новий сертифікат потрібно буде заново завантажити на майстер-вузол та внести зміни у маршрутизацію тенантів.

Для використання mTLS додайте пару клієнтських сертифікатів та ключів слухача подій обміну, якщо вимагається, що клієнти повинні представляти свої клієнтські сертифікати для верифікації. Після завершення всіх налаштувань збережіть конфігурацію, натиснувши кнопку "Save".

2.4 Процес інтеграції FortiSOAR з інструментами кібербезпеки

Інтеграція FortiSOAR з існуючою інфраструктурою безпеки є важливим кроком для забезпечення ефективної роботи вашої системи. Це дозволяє

організаціям об'єднувати різні інструменти та платформи кібербезпеки, що використовуються в єдиній екосистемі, для централізації та автоматизації процесу реагування на інциденти.

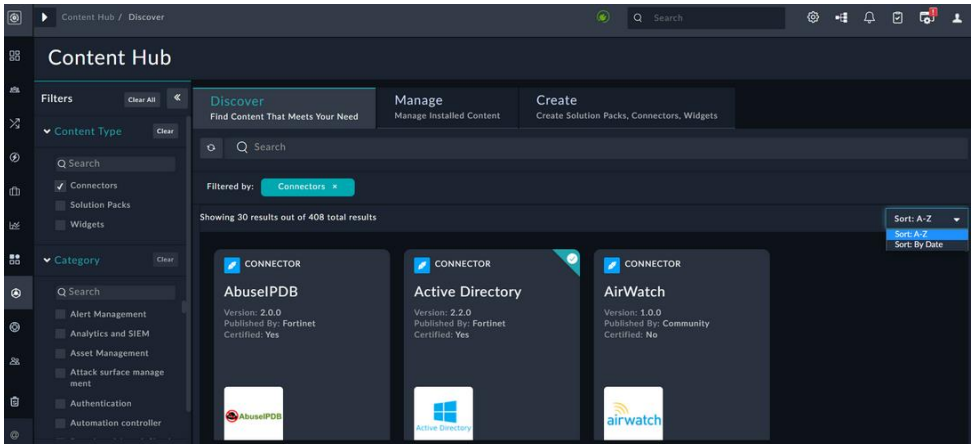

Рис. 2.9. Вікно управління конекторами [5]

Інтеграція FortiSOAR із системою SIEM є важливим етапом для ефективного управління інцидентами. Першим кроком є вибір системи SIEM, яка використовується, такі як Splunk, IBM QRadar, ArcSight, LogRhythm та McAfee Enterprise Security Manager. FortiSOAR підтримує інтеграцію з API і готові роз'єми, що спрощує підключення.

Для API-інтеграції потрібно налаштувати FortiSOAR на автоматичне витягування подій за допомогою API-запитів, забезпечивши належну аутентифікацію. Регулярні запити API можуть допомогти вам отримати актуальну інформацію про події безпеки. Використовуючи готові конектори, їх установка і настройка спрощують процес підключення і вимагають введення облікових даних і налаштувань безпеки [12].

Наступним кроком є налаштування збору даних. Визначте, які дані передаються від SIEM до FortiSOAR (події безпеки, системні журнали та пов'язані з ними інциденти). Встановіть правила кореляції в SIEM для виявлення складних загроз та автоматичного надсилання інцидентів у FortiSOAR для подальшого аналізу та реагування.

Після налаштування інтеграції створіть тестовий інцидент в SIEM і

протестуйте систему, підтвердивши відправку в FortiSOAR. Необхідно регулярно оновлювати SIEM і FortiSOAR для забезпечення сумісності та використання нових функцій.

Інтеграція FortiSOAR з SIEM-системами забезпечує централізований моніторинг і швидке реагування на інциденти.

Інтеграція FortiSOAR з антивірусними програмами є важливим аспектом забезпечення кібербезпеки кінцевих точок мережі. Цей процес може бути використаний для автоматизації виявлення шкідливих програм, їх аналізу та реагування на них, підвищення ефективності захисту та скорочення часу реагування на інциденти. Більшість найновіших антивірусних програм підтримують API, і FortiSOAR може отримувати інформацію про загрози в режимі реального часу. Для цього Вам потрібно налаштувати FortiSOAR на автоматичне отримання даних через запити API, забезпечуючи належну автентифікацію, наприклад, за допомогою ключа API.

За допомогою FortiSOAR можливо автоматизувати процес реагування на загрози, виявлені антивірусними програмами. Якщо зловмисне програмне забезпечення виявлено, FortiSOAR може автоматично виконувати такі дії, як видалення заражених файлів та ізоляція пристроїв. Також можна автоматично запускати додаткові перевірки для забезпечення повного усунення загрози. FortiSOAR може автоматично повідомляти відповідальних осіб про виявлення загрози та вжиття заходів, забезпечуючи швидке спілкування та координацію.

FortiSOAR забезпечує централізоване управління антивірусними програмами на різних кінцевих точках, що надає повний огляд безпеки та постійний моніторинг кінцевих точок в режимі реального часу для швидкого реагування на загрози і координації дій щодо забезпечення безпеки, а також інтегрує дані з різних антивірусних програм. Централізоване управління політиками антивірусного захисту забезпечує узгодженість і ефективність вжитих заходів.

Інтеграція FortiSOAR з антивірусною програмою дозволяє зіставляти

дані з різних джерел для виявлення складних загроз. FortiSOAR може корелювати дані з антивірусних програм з іншими джерелами, такими як брандмауери та системи управління вразливостями, для виявлення складних загроз. За допомогою FortiSOAR можливо автоматично вживати заходів при виявленні певних типів загроз, наприклад, блокувати відповідний трафік на брандмауері. Крім того, FortiSOAR може допомогти створювати звіти, проводити аналіз та виявляти тенденції та вразливості на основі даних антивірусної програми.

Після налаштування інтеграції потрібно протестувати систему. Рекомендується створити тестові інциденти в антивірусній програмі та перевірити, чи правильно вони надсилаються до FortiSOAR. Після інтеграції варто уважно стежити за роботою системи і вносити корективи для забезпечення стабільної роботи. Інтеграція FortiSOAR і антивірусних програм забезпечує автоматизовану, скоординовану і ефективний захист кінцевих точок, допомагаючи підвищити рівень кібербезпеки в організації.

Інтеграція FortiSOAR та брандмауера є ключовим фактором забезпечення кібербезпеки організації. Більшість сучасних брандмауерів підтримують API, які дозволяють FortiSOAR отримувати інформацію про підозрілий трафік та спроби несанкціонованого доступу в режимі реального часу. Варто налаштувати FortiSOAR на автоматичне отримання даних від брандмауера за допомогою запитів API, щоб забезпечити належну аутентифікацію з використанням, наприклад, ключів API. Якщо API недоступний, можливо налаштувати FortiSOAR для обробки лог-файлів брандмауера. Це дозволяє автоматично отримувати інформацію про подію з логів.

За допомогою FortiSOAR ви можете скоротити час відгуку, мінімізувати ризик вторгнення в мережу та автоматизувати процес реагування на мережеві загрози. Якщо виявлено підозрілу активність, FortiSOAR автоматично блокує підозрілі IP-адреси або сегменти мережі на брандмауері та встановлює правила автоматичного блокування на основі

таких критеріїв, як багаторазові спроби входу та виявлення шкідливого трафіку. FortiSOAR також може автоматично повідомляти відповідальну особу про важливі події і виконані дії, забезпечуючи швидкий зв'язок і координацію.

FortiSOAR забезпечує централізоване управління брандмауером, дозволяючи швидко реагувати на загрози та координувати безпеку. Постійно відстежуючи мережеві події в режимі реального часу та інтегруючи дані з різних брандмауерів, з’являється повне уявлення про мережеву безпеку. Використовуючи FortiSOAR для централізованого управління політикою брандмауера, забезпечується узгодженість та ефективність заходів безпеки.

Завдяки інтеграції FortiSOAR з брандмауерами можливо зіставляти дані з різних джерел для виявлення складних загроз. FortiSOAR може координувати дані брандмауера з іншими джерелами, такими як антивірусні програми та системи управління вразливістю, для виявлення складних загроз. За допомогою FortiSOAR стає реальною розробка сценаріїв реагування, які автоматично вживають заходів при виявленні певних типів загроз. Наприклад, якщо брандмауер виявляє підозрілу активність, FortiSOAR може запустити додаткову перевірку кінцевих точок. FortiSOAR також може допомогти виявити тенденції та вразливості та оптимізувати заходи безпеки, створюючи та аналізуючи звіти на основі даних брандмауера.

За допомогою *API FortiSOAR* платформа може бути інтегрована з різними інструментами кібербезпеки та IT-інфраструктури для централізованого управління інцидентами безпеки, автоматизації процесів та підвищення ефективності заходів захисту. Першим кроком є вивчення документації API, яка містить інформацію про кінцеві точки, методи автентифікації, формати запитів та відповідей та приклади використання.

Для безпечного підключення до API FortiSOAR необхідно налаштувати автентифікацію, використовуючи ключі API, маркери доступу або базову автентифікацію. Ключ API створюється в конфігурації FortiSOAR і додається до заголовка запиту. Маркери доступу можуть бути отримані за допомогою

процесу OAuth, який забезпечує більш безпечне управління доступом.

Запит API для взаємодії з FortiSOAR використовує методи GET, POST, PUT та DELETE для виконання різних операцій. Наприклад, метод GET може використовуватись для отримання даних, метод POST для створення нового об'єкта, метод PUT для оновлення існуючого об'єкта. Обробляйте відповіді API FortiSOAR для отримання та використання необхідної інформації.

Інтеграція з системами управління вразливостями дозволяє автоматично отримувати дані про вразливості і створювати завдання по їх усуненню. Наприклад, налаштування регулярних запитів API до системи управління вразливістю для отримання нових даних і створення завдання на їх усунення. Інтеграція з системою SIEM забезпечує збір і кореляцію подій безпеки. API SIEM використовується для автоматичного вилучення подій у FortiSOAR та створення інцидентів на основі корельованих подій.

Інтеграція з інструментами моніторингу мережі дозволяє виявляти аномалії трафіку та швидко реагувати на атаки. Варто налаштовувати FortiSOAR так, щоб він отримував дані про мережевий трафік через API інструменту моніторингу та автоматично виконував дії.

Після налаштування інтеграції рекомендується протестувати систему, щоб переконатися, що вона працює коректно. Варто запустити тестовий запит API, щоб переконатися, що конфігурація правильна. Після налаштування необхідно проводити моніторинг роботи системи і вносити корективи для забезпечення стабільної роботи. Регулярне оновлення FortiSOAR та інструментів інтеграції забезпечує сумісність та використання нових функцій.

Автоматизація процесу обміну даними між системами за допомогою FortiSOAR створює ефективну, скоординовану та швидку систему управління кібербезпекою. Це забезпечує постійний потік інформації, зменшує необхідність ручного втручання та підвищує швидкість реагування на інциденти. Першим кроком є визначення цілей та вимог інтеграції, таких

як виявлення загроз, управління вразливістю та автоматичне реагування на інциденти.

Вибір системи для інтеграції є важливим кроком. До них відносяться системи управління вразливостями, системи SIEM, антивірусні програми, брандмауери та системи моніторингу мережі. API FortiSOAR дозволяє здійснювати інтеграцію через відповідну аутентифікацію і налаштовувати запити API для отримання, оновлення, створення або видалення даних.

Створення конекторів і плейбуків є важливим аспектом автоматизації. Конектори дозволяють автоматично отримувати і передавати дані між FortiSOAR і іншими системами, а плейбук автоматизує повторювані завдання. Наприклад, сценарій автоматичного реагування на виявлення шкідливого ПЗ може бути використаний для ізоляції заражених пристроїв і виконання дій по блокуванню підозрілих IP-адрес [13].

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО АВТОМАТИЗАЦІЇ ПРОЦЕСІВ РЕАГУВАННЯ НА ІНЦИДЕНТИ З ВИКОРИСТАННЯМ РІШЕННЯ FORTISOAR

3.1 Алгоритми застосування рішення FortiSOAR

Для значного скорочення часу реагування на загрози, стандартизації процесу обробки інцидентів і зниження навантаження на аналітиків безпеки при використанні FortiSOAR рекомендується використання всіх можливих методів автоматизації.. Використання автоматизації забезпечує швидке реагування на інциденти і допомагає уникнути людських помилок.

Автоматизація процесу реагування скорочує час від виявлення інциденту до його усунення, що має вирішальне значення для мінімізації шкоди від загроз. Це також забезпечує послідовність реагування на інциденти та підвищує надійність та прозорість процесу. Крім того, автоматизація звільняє ресурси аналітиків, дозволяючи зосередитися на більш складних і стратегічних завданнях. Коли ви документуєте всі дії у відповідь на інцидент, автоматично створюється детальна документація, яка має вирішальне значення для аудиту та аналізу.

Автоматизація FortiSOAR базується на правилах, які активуються за допомогою певних тригерів, таких як сповіщення, події та дані моніторингу. В плейбуках використовується модуль дій, який виконує ряд дій з виявлення, оцінки, локалізації та вирішення інцидентів. Ці кроки включають збір додаткових даних, взаємодію з іншими системами та інструментами, надсилання сповіщень та автоматичну зміну конфігурації системи.

Приклади типових сценаріїв автоматизації реагування:

Виявлення шкідливого програмного забезпечення

Тригер*:* Антивірусна система виявляє шкідливе ПЗ на робочій станції.

Автоматичні дії:

збір додаткової інформації про інфіковану машину

ізоляція машини від мережі шляхом блокування всього трафіку

надсилання повідомлення команді безпеки з деталями про інцидент

відновлення та аналіз, видалення шкідливого ПЗ та відновлення системи

Виявлення підозрілої активності в мережі

Тригер: SIEM-система генерує алерт про підозрілу мережеву активність.

Автоматичні дії:

запит додаткових даних від SIEM-системи для підтвердження загрози

блокування IP-адреси джерела підозрілої активності на файрволі

створення інцидентного тікета для подальшого розслідування

надсилання сповіщення команді безпеки

Реагування на фішинговий емейл

Тригер: Система виявляє підозрілий емейл.

Автоматичні дії:

аналіз вмісту емейлу за допомогою інтегрованих сервісів

якщо емейл визначений як шкідливий, автоматичне блокування відправника у поштовій системі

надсилання попередження користувачу з рекомендаціями щодо подальших дій

Автоматизація типових сценаріїв реагування на інциденти в FortiSOAR забезпечує високу ефективність в боротьбі з загрозами, дозволяючи організаціям підтримувати високий рівень безпеки при одночасному зниженні навантаження на персонал.

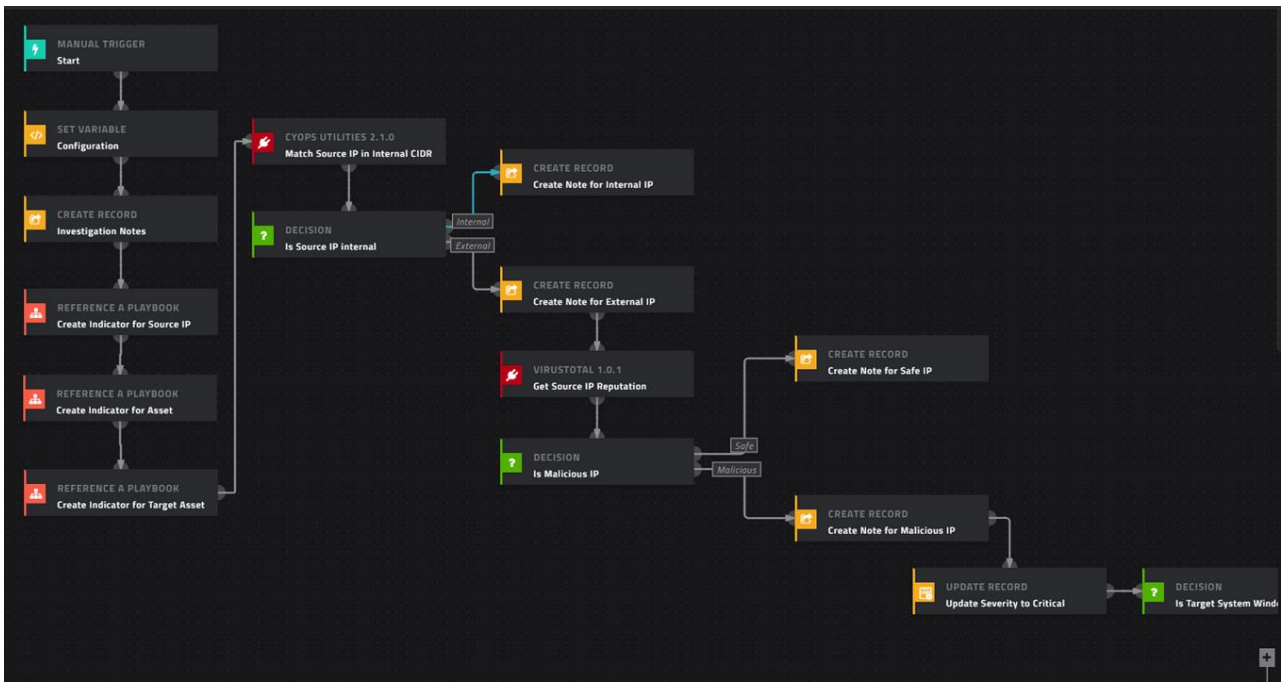

Рис. 3.1. Приклад створеного плейбуку, що відпрацьовує при отриманні трафіку зі зловмисної адреси [4]

Ще однією хорошою практикою вважається інтеграція більшості можливих інструментів організації. Таким чином, система отримує максимальний обсяг даних і значно підвищує якість обробки інцидентів.

Інтеграція сприяє ефективному обміну даними між різними системами, забезпечуючи швидке виявлення загроз і реагування на них. Це скорочує час між виявленням загроз та їх нейтралізацією, що важливо для зменшення потенційних збитків. Автоматизація рутинних процесів дозволяє фахівцям зосередитися на більш складних завданнях, що підвищує загальну продуктивність команди безпеки.

Основою інтеграції є використання API, які дозволяють FortiSOAR взаємодіяти з іншими системами, такими як SIEM, IDM, антивірусними рішеннями та іншими інструментами безпеки. Ці інтерфейси забезпечують стандартизований метод обміну даними, що дозволяє реалізовувати складні автоматизовані процеси.

SIEM системи (наприклад, Splunk або IBM QRadar): інтеграція з SIEM дозволяє автоматично обробляти оповіщення та події для забезпечення

швидкого реагування на інциденти.

IDM, такі як Microsoft Active Directory або Okta: ці системи дозволяють керувати користувачами та доступом. Це дуже важливо для контролю доступу в разі інциденту.

Антивірусні системи (наприклад, McAfee або Symantec): завдяки цій інтеграції FortiSOAR може отримувати повідомлення про виявлення вірусів і автоматично вживати заходів.

Системи управління інцидентами (наприклад, ServiceNow або Jira): автоматизовані процеси реєстрації, відстеження та вирішення інцидентів забезпечують ефективне управління інцидентами.

Інструменти моніторингу мережі (наприклад, SolarWinds або Nagios): надають інформацію про стан мережевої інфраструктури, яка може бути використана для реагування на інциденти.

Інтеграція FortiSOAR з цими та іншими інструментами забезпечує комплексний підхід до управління безпекою та підвищує загальну здатність організації реагувати на інциденти. Це сприяє створенню автоматизованої взаємопов'язаної екосистеми, яка оптимізує процеси забезпечення безпеки і підвищує ефективність реагування на загрози.

Важливим критерієм ефективної роботи з FortiSOAR є його використання для аналізу інцидентів. Аналітика SOAR є ключовим компонентом стратегії кібербезпеки організації, яка не тільки виявляє загрози, але й активно запобігає їм. За допомогою передових інструментів аналітики на платформі FortiSOAR ви можете всебічно аналізувати інформацію з різних джерел для ефективного реагування на інциденти.

Аналітика допомагає виявляти шкідливі дії на ранній стадії і знижує потенційний збиток від атак. Використовуючи дані для виявлення закономірностей і аномалій, які можуть вказувати на потенційні інциденти, організації можуть бути на крок попереду загроз. Це підвищує загальну швидкість реагування системи безпеки і забезпечує більш високий рівень захисту.

Система SOAR збирає та аналізує дані з різних джерел, включаючи журнали серверів, системи моніторингу мережі, антивірусні програми та системи виявлення вторгнень. Ці дані обробляються за допомогою алгоритмів машинного [10] навчання для виявлення аномалій, які можуть свідчити про кібератаку або внутрішні порушення. На основі цього аналізу генеруються автоматичні відповіді на інциденти, що значно зменшує час і збільшує якість реагування.

Рис. 3.2. Звіт реакції на інцидент, що використовується для аналітики

Приклади використання аналітичних даних FortiSOAR:

Виявлення шкідливого програмного забезпечення: FortiSOAR аналізує поведінку файлів і процесів у системі. При виявленні підозрілої активності, яка відповідає відомому шаблону вірусів або троянських програм, система запускає карантин і відправляє алерт відповідним командам.

Моніторинг аномалій в мережевому трафіку: Збираючи та аналізуючи

мережевий трафік, FortiSOAR може виявити нехарактерні підключення та спроби передачі даних на підозрілі сервери, що може вказувати на витік даних або зовнішнє управління.

Проактивне реагування на інциденти з фішингу: FortiSOAR використовує дані електронної пошти та веб-шлюзів для аналізу подібності запитів із відомими шаблонами фішингу для автоматичного блокування шкідливих посилань та відправників.

Виявлення незвичайної поведінки користувачів: Аналізуючи поведінку користувачів, FortiSOAR може виявляти несанкціонований доступ до критично важливих ресурсів або спроби внесення несподіваних змін в конфігурацію і швидко реагувати на потенційні внутрішні загрози.

Використовуючи аналітику в SOAR, можливо не тільки виявляти та реагувати на існуючі загрози, але й проактивно адаптувати стратегію безпеки, щоб запобігти майбутнім атакам та підтримувати високий рівень захисту інформаційних активів організації.

3.2 Рекомендації щодо автоматизації процесів реагування на інциденти в інформаційній системі організації

Щоб підвищити ефективність FortiSOAR і максимізувати віддачу від платформи, важливо впровадити стратегію, яка оптимізує її використання. Це включає в себе регулярне оновлення сценаріїв і правил, навчання команди і підвищення кваліфікації, а також регулярний моніторинг ефективності системи.

Регулярні оновлення сценаріїв і правил системи FortiSOAR є невід'ємною частиною управління кібербезпекою, забезпечуючи належне реагування на ландшафт загроз, що змінюються, і адаптацію до нових вимог і технологій. Це дозволяє оновлювати систему безпеки і підтримувати її ефективність в боротьбі з загрозами.

Важливо бути впевненим, що відповіді на інциденти є актуальними та

ефективними в умовах постійної мінливості тактики зловмисників та появи нових вразливостей в IT-інфраструктурі. Регулярні оновлення можуть допомогти зменшити ризик, пов'язаний зі старими правилами, які можуть пропускати нові атаки або викликати помилкові тривоги.

Оновлення сценаріїв та правил у FortiSOAR є систематичним процесом, що забезпечує адаптивність системи до нових загроз, технологій та змін бізнес-процесів. Ретельно спланований процес оновлення допомагає підтримувати високий рівень безпеки та ефективність реагування на інциденти.

Крок 1. Аналіз існуючої конфігурації. Він полягає у глибокому аналізі поточних сценаріїв і правил, що включає оцінку їх ефективності, вивчення даних про інциденти, що оброблялись, і збір зворотного зв'язку від операторів. Цей етап дозволяє визначити потреби для оновлень та вдосконалень.

Крок 2. Розробка оновлень. На основі зібраних даних формуються оновлення для плейбуків і правил. Розробка оновлень включає модифікацію вже створених правил для зменшення помилкових спрацьовувань, адаптацію сценаріїв до нових загроз та інтеграцію з новими технологічними рішеннями. Особливу увагу варто приділити тестуванню нових сценаріїв у контрольованих умовах.

Крок 3. Впровадження змін. Після розробки і тестування, змінені сценарії та правила запускаються в операційне середовище. Впровадження включає планування виходу в "живу" експлуатацію, щоб мінімізувати перебої у роботі системи та забезпечити гладке переведення на нові налаштування.

Крок 5. Моніторинг і корекція. Останнім етапом є постійний моніторинг впроваджених змін для оцінки їх впливу на загальну працеспроможність системи. Це включає слідкування за ефективністю нових правил і сценаріїв, а також швидке внесення змін у разі виявлення проблем або несподіваних наслідків оновлень.

Ефективне оновлення сценаріїв і правил FortiSOAR важливо для того, щоб завжди бути готовим до кіберзагроз. Нижче наведено детальні рекомендації щодо оптимізації процесу оновлення.

Планування регулярних переглядів правил та сценаріїв є важливим для визначення та внесення необхідні коректив у відповідь на загрози та зміни в бізнес-процесах. Рекомендується проводити перевірки щоквартально або при кожному великому інциденті.

Варто постійно оновлювати правила, активно відстежуючи новини про кібербезпеку, включаючи рекомендації постачальників та організацій, що займаються інформаційною безпекою (наприклад, CERT). Важливо швидко реагувати на нові вразливості та експлойти.

Нові правила і сценарії повинні бути ретельно протестовані в контрольованих умовах, перш ніж їх можна буде впроваджувати в продуктивне середовище. Тестування повинно гарантувати, що оновлення ефективно виявляє загрози без збільшення помилкових спрацьовувань.

Оновлення правил і сценаріїв повинно відображати зміни в технічних процесах і бізнес-стратегіях організації. Важливо враховувати нові програми, послуги чи технології, впроваджені в організації, та адаптувати свої сценарії для роботи з ними.

Щоб мати можливість проводити аудит і відстежувати впроваджені оновлення, важливо ретельно документувати всі зміни. Це включає запис про причини змін, опис процедури та результатів тестування, а також інформацію про вплив змін на систему.

Для зменшення ризику непорозумінь та спротиву з боку персоналу важливо забезпечити відкриту та ефективну комунікацію з усіма зацікавленими сторонами, включаючи керівництво, IT-відділ та кінцевих користувачів.

Навчання кібербезпеці та підвищення кваліфікації при роботі з FortiSOAR важливі для забезпечення ефективної командної роботи, швидкого виявлення загроз, зниження числа помилкових спрацьовувань і

адаптації до нових технологій. Регулярне навчання розширює можливості співробітників, дозволяє більш точно налаштовувати системи безпеки, допомагає ефективно використовувати нові інструменти і забезпечує дотримання нормативних вимог. Рекомендації включають в себе організацію регулярного перегляду, використання змішаних методів навчання, моніторинг зовнішніх джерел загроз і залучення адміністраторів для підтримки програм навчання, які допоможуть підготуватися до кіберзагроз високого рівня і максимально підвищити ефективність використання FortiSOAR.

Також для роботи системи життєво необхідний моніторинг її роботи. Це забезпечує її стабільність, безпеку та ефективність:

Забезпечення стабільності: Моніторинг допомагає виявляти технічні неполадки, що виникають в системі, і реагувати на них. Відстежуючи такі ресурси, як процесор, пам'ять та мережевий трафік, адміністратори можуть вжити заходів для оптимізації продуктивності та запобігання перевантаженню.

Виявлення збоїв: Регулярний моніторинг дозволяє швидко виявляти і усувати збої, зводити до мінімуму час простою і підвищувати безпеку даних.

Контроль виконання політик безпеки: Моніторинг здійснюється у відповідності з усіма політиками безпеки, що дозволяють відстежувати запуск і виконання сценаріїв реагування на інциденти, а також переглядати попередження і події.

Підтримка стандартів та аудитів: Моніторинг забезпечує ведення докладних журналів та записів, необхідних для проведення нормативних перевірок та дотримання стандартів безпеки, що сприяє готовності до інспекцій.

Оптимізація системи: Аналіз даних моніторингу використовується для поліпшення налаштувань і процесів за рахунок підвищення загальної продуктивності і результативності FortiSOAR.

Ефективний моніторинг системи FortiSOAR є ключовим для підтримки

її стабільності, безпеки та ефективності. Розробка стратегії моніторингу має включати наступні елементи:

Централізований моніторинг: Інструменти централізованого моніторингу, такі як Splunk та ELK Stack, дозволяють збирати та аналізувати дані FortiSOAR в одному місці. Це дозволяє використовувати інформаційні панелі для візуалізації продуктивності системи, виявлення аномалій та відстеження ключових показників продуктивності. Централізований збір даних також полегшує ведення журналу та аудит.

Рис. 3.3 Дашборди, що використовуються для моніторингу

Моніторинг в режимі реального часу: Налаштування системи моніторингу для надсилання автоматичних сповіщень при виявленні збоїв або аномалій важливо для швидкого реагування на інциденти. Інтеграція з комунікаційними платформами, такими як Slack та Microsoft Teams, дозволяє фахівцям із безпеки миттєво отримувати оновлення про потенційні проблеми.

Прогнозування і запобігання збоям: Впровадження методів машинного навчання для аналізу зібраних даних може допомогти передбачити потенційні збої та вразливості, перш ніж вони призведуть до серйозних проблем. Це включає моделювання поведінки системи для виявлення

нестандартних закономірностей, які можуть вказувати на майбутні проблеми.

Глибокий аналіз даних: Регулярний аналіз даних моніторингу може допомогти виявити тенденції та зміни у використанні системи, які можуть вказувати на необхідність технічного обслуговування або масштабування. Це також допоможе вдосконалити стратегію безпеки та оптимізувати ресурси.

Періодичний аудит та перегляд налаштувань: Заплановані перевірки налаштувань та політик безпеки допомагають забезпечити, що система залишається актуальною та відповідає сучасним вимогам безпеки. Перегляд конфігурацій на основі останніх рекомендацій з безпеки та технологічних оновлень є критично важливим для захисту від нових загроз.

Підтримка та оновлення: Регулярні оновлення програмного забезпечення FortiSOAR і його компонентів забезпечують захист від відомих вразливостей і використання новітніх функцій. Важливо стежити за випуском патчів і оновлень, щоб система була захищена і ефективна.

Застосовуючи ці стратегії, FortiSOAR підтримується в оптимальному стані і забезпечується високий рівень продуктивності, безпеки і адаптивності до мінливих умов сучасного кіберпростору.

Процес внесення коректив у роботу системи FortiSOAR, заснований на результаті моніторингу, включає кілька важливих кроків, які забезпечують покращення продуктивності та безпеки системи. Цей процес можна описати наступним чином:

Крок 1. Виявлення проблеми. Перший крок у внесенні коректив полягає у виявленні проблеми через систематичний моніторинг FortiSOAR. Моніторинг може виявити відхилення в продуктивності, помилки в журналах, безпекові інциденти або інші проблеми, що впливають на роботу системи.

Крок 2. Аналіз проблеми. Після ідентифікації проблеми необхідно провести детальний аналіз для з'ясування її причин. Аналіз може включати перевірку системних журналів, оцінку використання ресурсів або аудит налаштувань безпеки. Це допомагає зрозуміти кореневі причини проблеми та

планувати відповідні дії.

Крок 3. Розробка плану дій. На основі аналізу розробляється план дій для усунення виявленої проблеми. План може включати технічні коригування, такі як збільшення ресурсів, оновлення програмного забезпечення, зміни в конфігураціях або оновлення політик безпеки. Важливо також визначити критерії успіху та методи перевірки ефективності внесених змін.

Крок 4. Впровадження змін. Впровадження плану дій вимагає уважного підходу, зазвичай з використанням тестових середовищ для мінімізації впливу на роботу продакшн системи. Зміни слід вносити поетапно, з можливістю відкату у випадку непередбачених проблем. Всі зміни повинні бути документовані для забезпечення прозорості та відповідності регуляторним вимогам.

Крок 5. Моніторинг ефективності змін. Після впровадження змін важливо продовжувати моніторинг системи, щоб оцінити ефективність внесених коректив. Спостереження за продуктивністю та стабільністю системи допоможе виявити чи повністю усунута проблема та чи не виникли нові проблеми.

Крок 6. Зворотний зв'язок і адаптація. Останній крок полягає у зборі зворотного зв'язку від кінцевих користувачів та системних адміністраторів. На основі цього зворотного зв'язку можуть бути внесені подальші корективи для оптимізації роботи системи. Цей процес є неперервним, адже технологічне середовище та умови експлуатації постійно змінюються.

Виконання цих кроків забезпечує, що FortiSOAR не тільки відновлюється після існуючих проблем, але й адаптується до нових викликів, постійно покращуючи свою продуктивність та безпеку.

Інтегруючи FortiSOAR у стратегію кібербезпеки організації, можна значно підвищити загальний рівень інформаційної безпеки. За допомогою цієї платформи можливо автоматизувати виявлення інцидентів, їх аналіз і редагування, що робить процес управління безпекою більш швидким і

ефективним. FortiSOAR також пропонує глибоку інтеграцію з іншими інструментами безпеки, створюючи єдину ефективну систему реагування на загрози. Це не тільки підвищує рівень захисту, але і підвищує прозорість процесу забезпечення кібербезпеки, дозволяючи керівництву компанії краще розуміти поточні ризики і вживати відповідних заходів щодо їх мінімізації.

Централізоване управління інцидентами за допомогою FortiSOAR забезпечує єдину платформу для моніторингу, аналізу та реагування на інциденти в галузі кібербезпеки. Це дозволяє ефективніше координувати дії, скорочувати час реагування та підвищувати загальний рівень безпеки вашої організації. Збираючи дані з різних джерел, включаючи SIEM-системи, антивірусні програми, брандмауери і системи мережевого моніторингу, ми отримаємо повну картину подій, пов'язаних з безпекою.

FortiSOAR автоматизує процес обробки інцидентів, значно скорочуючи час реагування і підвищуючи ефективність. Використання API для автоматичного створення інцидентів на основі корельованих подій та плейбуків для автоматизації реагування допомагає швидко нейтралізувати загрози. Інструменти аналітики дозволяють детально досліджувати інциденти, такі як журнали подій та мережевий трафік, щоб допомогти визначити причину та наслідки загроз.

FortiSOAR забезпечує ефективну координацію та взаємодію між різними групами безпеки. Автоматичні сповіщення про нові інциденти та зміни в їх статусі забезпечують швидкий зв'язок, а спільна робота з розслідування інцидентів може допомогти швидше усунути загрози. Централізоване управління інцидентами включає в себе управління всім життєвим циклом інциденту від виявлення до завершення, забезпечуючи узгодженість статусу і виконуваних дій.

FortiSOAR також надає можливість автоматизувати створення звітів та аналіз даних про інциденти. Регулярні звіти можуть допомогти виявити тенденції, оцінити ефективність заходів безпеки та виявити потенційні вразливості. Постійні вдосконалення процесу управління інцидентами

включають регулярні перевірки та навчання співробітників, що допомагає підтримувати високий рівень кібербезпеки в організації.

Автоматизація процесу реагування на інциденти за допомогою FortiSOAR значно підвищує ефективність управління безпекою, скорочує час реагування на загрози і ризики для організації за рахунок автоматизації рутинних завдань, координації дій між різними системами і надання інструментів для поглибленого аналізу інцидентів. Детальний огляд основних аспектів автоматизації.

Створення плейбуків є ключовим елементом автоматизації процесів реагування на інциденти в системі FortiSOAR. Вони представляють собою набір заздалегідь визначених дій, які автоматично виконуються при виявленні інциденту або настанні певної події.

Крок 1. Визначення цілей та сценаріїв реагування. Необхідно провести аналіз ризиків та загроз, щоб встановити найбільш вірогідні та критичні загрози для організації. Визначення чітких цілей для кожного сценарію реагування допоможе забезпечити ефективне та швидке реагування на інциденти.

Крок 2. Розробка детальної послідовності дій для кожного сценарію реагування. Це включає визначення конкретних дій, які необхідно виконати, та їх порядок. Наприклад, для плейбуку виявлення шкідливого програмного забезпечення послідовність дій може включати ізоляцію пристрою, запуск антивірусного сканування та повідомлення команди безпеки. Важливо також визначити завдання, які можна автоматизувати, щоб зменшити потребу в ручному втручанні.

Крок 3. Налаштування тригерів та умов, за яких плейбуки активуються. Тригери можуть бути подіями або умовами, які автоматично запускають виконання плейбука, наприклад, виявлення шкідливого програмного забезпечення на кінцевій точці. Умови визначають, коли і за яких обставин плейбук повинен виконуватися, наприклад, тільки для високо ризикованого ПЗ.

Крок.4. Тестування. Це включає симуляцію інцидентів для перевірки послідовності дій плейбуків та аналіз результатів тестування для виявлення можливих недоліків. Після успішного тестування плейбуки можуть бути впроваджені в реальне середовище, де їх ефективність постійно моніториться.

Крок 5. Вдосконалення плейбуків. Регулярне оновлення плейбуків та проведення навчання для співробітників допоможе підтримувати високий рівень кібербезпеки в організації. Наприклад, додавайте нові дії або корегуйте існуючі на основі аналізу попередніх інцидентів і проводьте тренінги для команди SOC щодо нових плейбуків та оновлень.

Створення плейбуків є критичним аспектом автоматизації реагування на інциденти, що дозволяє стандартизувати процеси, зменшити час реагування та підвищити загальний рівень кібербезпеки організації.

Реагування на загрози за допомогою FortiSOAR дозволяє швидко та ефективно виявляти, аналізувати та нейтралізувати загрози. Інтеграція FortiSOAR з різними джерелами даних, такими як SIEM-системи, антивірусні програми та файрволи, забезпечує своєчасне виявлення загроз. Наприклад, FortiSOAR автоматично отримує події про спроби несанкціонованого доступу або дані про виявлення шкідливого ПЗ, що дозволяє оперативно реагувати на загрози.

Після виявлення загроз FortiSOAR аналізує та класифікує їх, щоб визначити пріоритети та подальші дії. Вбудовані інструменти аналітики дозволяють переглядати журнал подій і мережевий трафік, що допомагає визначити причину атаки. Правила автоматичної класифікації визначають пріоритетність загроз в залежності від ступеня їх серйозності для забезпечення ефективного використання ресурсів.

FortiSOAR автоматизує виконання дій з нейтралізації загроз за допомогою плейбуків. Наприклад, при виявленні шкідливого ПЗ FortiSOAR автоматично ізолює заражений пристрій, виконує антивірусну перевірку і блокує відповідну IP-адресу. Це скорочує час відгуку і підвищує

ефективність захисту. FortiSOAR також інформує відповідальних осіб про інциденти і виконуваних діях за допомогою автоматичних сповіщень для забезпечення оперативної комунікації.

Управління повним життєвим циклом інциденту від виявлення до закриття є ключовим аспектом FortiSOAR. Усі інциденти реєструються з детальною інформацією про подію, статус та відповідальну особу, надаючи можливість відстежувати стан інциденту. Крім того, FortiSOAR автоматизує звітність та аналіз даних про інциденти, виявляючи тенденції та допомагаючи оцінювати ефективність заходів безпеки шляхом створення звітів про виявлення загроз, контрзаходів та результатів.

Управління життєвим циклом інцидентів за допомогою FortiSOAR забезпечує послідовне та ефективне вирішення інцидентів безпеки від виявлення до закриття. Все починається з виявлення та реєстрації інцидентів. FortiSOAR інтегрується з різними джерелами даних, такими як SIEM-системи, антивірусні програми та брандмауери, для автоматичного виявлення інцидентів. Усі виявлені інциденти автоматично реєструються в системі з детальною інформацією про подію, такою як час, місце розташування, тип загрози та потенційний вплив.

Після реєстрації інцидентів необхідно класифікувати їх і розставити пріоритети. Інциденти класифікуються за типом загроз, такими як шкідливе програмне забезпечення, спроби несанкціонованого доступу та фішинг-атаки. Пріоритети визначаються на основі потенційного впливу інциденту на вашу організацію, що дозволяє зосередити ресурси на найбільш важливих загрозах. Використовуючи правила автоматичного визначення пріоритетів, ви можете ефективно розподіляти ресурси для реагування на інциденти.

Наступним кроком є детальний аналіз та розслідування інциденту. FortiSOAR збирає та зберігає докази, такі як журнали подій, мережевий трафік та файли, необхідні для розслідування інцидентів. Аналітичні інструменти FortiSOAR дозволяють розслідувати інциденти, включаючи аналіз журналів і мережевого трафіку, для визначення причини і методу атак.

Це допомагає виявити причину інциденту і оцінити його вплив.

Після аналізу вживаються заходи щодо нейтралізації загрози та запобігання подальшому поширенню атаки. Виконання плейбуків FortiSOAR дозволяє автоматизувати заздалегідь визначені дії, такі як ізоляція заражених пристроїв, блокування IP-адрес та видалення шкідливих файлів. Такі заходи допомагають швидко нейтралізувати загрозу та запобігти повторним атакам. Після нейтралізації загрози необхідно відновити нормальну роботу систем та мінімізувати вплив інциденту. Це включає відновлення систем та даних з резервних копій та перевірку їх цілісності для забезпечення нормальної роботи.

Після успішного завершення реагування та відновлення систем інцидент може бути закритий. Це включає документування всіх етапів реагування, аналізу та уроків, які були винесені. Документування допомагає в майбутньому покращити процеси та підвищити ефективність реагування. Оцінка ефективності реагування на інцидент та внесення необхідних змін до процесів і плейбуків дозволяють постійно вдосконалювати управління інцидентами.

FortiSOAR також надає автоматичні звіти та аналіз даних про інциденти. Періодичні автоматизовані звіти містять детальну інформацію про виявлені загрози, вжиті заходи та результати. Використання інструментів аналітики для виявлення тенденцій та оцінки ефективності заходів безпеки може допомогти виявити потенційні вразливості та оптимізувати захист. Управління життєвим циклом інцидентів за допомогою FortiSOAR забезпечує структурований, стандартизований і ефективний підхід до реагування на інциденти безпеки, значно підвищуючи рівень захисту організацій від кіберзагроз.

ВИСНОВКИ

В ході виконання бакалаврської роботи мною вдалось дослідити шляхи автоматизації процесів реагування на інциденти на базі рішення FortiSOAR. Основною метою дослідження було виявлення ефективних способів та інструментів автоматизації реагування на інциденти кібербезпеки та розробка рекомендацій щодо поліпшення кіберзахисту організації. Ця тема дуже актуальна в контексті постійного збільшення кількості та складності кіберзагроз.

Проведено аналіз актуального стану інструментів кібербезпеки та традиційних методів реагування на інциденти. Було встановлено, що метод ручного реагування на кіберінцидент вимагає великих витрат часу, схильний до людських помилок, що значно знижує його ефективність. Традиційний метод вимагає значного часу для перевірки кожного алерту та вжиття відповідних заходів. Це обмежує кількість інцидентів, які можуть бути оброблені протягом робочого дня, і створює додаткові ризики для безпеки вашої організації.

Досліджено методи та засоби автоматизації рутинних завдань за допомогою плейбуків та збагачення даних з зовнішніх джерел. Плейбуки FortiSOAR забезпечують стандартизацію та послідовність дій при реагуванні на інциденти, що мінімізує ризик помилок та забезпечує ефективність дій. Автоматичне збагачення даних дозволяє отримати додаткову контекстуальну інформацію про загрози, що сприяє більш точному оцінюванню ризиків та прийняттю обґрунтованих рішень щодо подальших дій.

Розглянуто порядок впровадження FortiSOAR на віртуальній інфраструктурі організації. Процес розгортання включає налаштування центрального сервера для обробки даних, інтеграцію з існуючими системами кібербезпеки та налаштування плейбуків для автоматизації реагування на інциденти.

Запропоновано рекомендації щодо налаштування та використання плейбуків для автоматизації реагування на інциденти. Рекомендації включають детальний опис кроків для створення та налаштування плейбуків, визначення умов для їх запуску та дій, які мають бути виконані системою.

Використання рекомендацій, які були розроблені мною, дозволять підвищити швидкість та ефективність реагування на кіберзагрози за рахунок автоматизації рутинних завдань. Автоматичне збагачення даних допоможе забезпечити більш точний аналіз та кореляцію даних, що сприятиме кращому виявленню загроз та прийняттю обґрунтованих рішень щодо їх нейтралізації. Це значно знизить час на обробку інцидентів та мінімізує вплив людського фактора. Використання плейбуків дозволить стандартизувати та послідовно виконувати дії при реагуванні на інциденти, забезпечуючи ефективність та зниження ризиків. Інтеграція з різними інструментами кібербезпеки покращить координацію між командами кібербезпеки, сприяючи швидшому та більш точному реагуванню на загрози.

Таким чином, автоматизація процесів реагування на кіберінциденти в інформаційній системі організації має забезпечити кібербезпеку інформаційних ресурсів організації в цілому.

ПЕРЕЛІК ПОСИЛАНЬ

1. Statistica / Annual number of cyberattacks in the United States from 2016 to 2022. URL: https://www.statista.com/forecasts/1448523/us-cyberattacks-annual

2. DNSSense / Manual Incident Response: An Impractical and Drawback-Ridden Approach. URL: https://www.dnssense.com/drawbacks-manual-incident-response

3. Fortinet / Deploying FortiSOAR. URL: https://docs.fortinet.com/document/fortisoar/7.4.3/deployment-guide/158469/deploying-fortisoar

4. SecureCyberDefense / SIEM/SOAR. URL: https://securecyberdefense.com/cybersecurity-services/siem-soar/

5. Fortinet / Introduction to connectors. URL: https://docs.fortinet.com/document/fortisoar/7.4.3/connectors-guide/929681/introduction-to-connectors

6. Fortinet / Support Fortinet. URL: https://support.fortinet.com

7. RTInsights / Data Enrichment: A Trend That's Only Going to Get Bigger. URL: https://www.rtinsights.com/data-enrichment-a-trend-thats-only-going-to-get-bigger/

8. Fortinet / Overview of Multi-tenancy support in FortiSOAR. URL: https://docs.fortinet.com/document/fortisoar/7.4.3/multi-tenancy-support-guide/121164/overview-of-multi-tenancy-support-in-fortisoar

9. Fortinet / Mobile Application for Android. URL: https://docs.fortinet.com/document/fortisoar/7.0.2/mobile-application-for-android/936371/overview#Overview

10. Fortinet Community / ML Capabilities In FortiSOAR. URL: https://community.fortinet.com/t5/FortiSOAR-Discussions/ML-Capabilities-In-FortiSOAR/m-p/220006

11. Fortinet / Reports in FortiSOAR. URL:

https://docs.fortinet.com/document/fortisoar/7.0.0/user-guide/292560/reports-in-fortisoar

12. Fortinet / API Guide. URL: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/8cef1011-c7b2-11ed-8e6d-fa163e15d75b/FortiSOAR-7.4.0-API_Guide.pdf

13. Fortinet / Connectors Guide. URL: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/095a3fa8-7969-11ee-a142-fa163e15d75b/FortiSOAR-7.4.3-Connectors_Guide.pdf

14. NIST SP 800-61 Rev. 2. Computer Security Incident Handling Guide, 6-9 c. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf