ENERGY SOAR

bako tech®

SOAR ДЛЯ ПОЧАТКІВЦІВ

Подолайте проблеми безпеки за допомогою рішень SOAR
(Security Orchestration, Automation, and Response)

www.energylogsoar.com

Що таке SOAR?

Висока частота атак, складність IT-мереж і відсутність кваліфікованих фахівців наражають багато компаній на ризик втрати даних, фінансових збитків і репутаційної шкоди. SOAR — це рішення, яке дозволяє автоматизувати процеси реагування на інциденти безпеки.

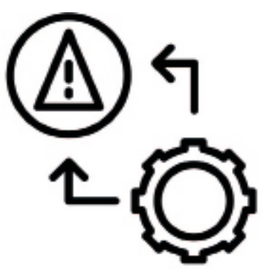
Абревіатура «SOAR» розшифровується як Security Orchestration, Automation, Response, і кожен компонент цієї платформи має певну роль у процесі реагування на інцидент безпеки:

Оркестрація (Orchestration)

Оркестрація в SOAR передбачає координацію дій та інтеграцію різних інструментів, систем і процесів для ефективного реагування на інциденти безпеки. Цей компонент дає змогу створювати автоматизовані процеси реагування на інциденти та покращує співпрацю між різними командами, залученими до роботи з кібервторгненнями.

Автоматизація (Automation)

Автоматизація є ключовим елементом SOAR, оскільки вона дозволяє легше та ефективніше реагувати на атаки. Завдяки автоматизації можна прискорити запуск відповідних процедур виявлення та ізолювання загроз, а також швидше надсилати повідомлення про інциденти. І це ще не повний список можливостей!



Реагування (Response)

Компонент реагування в SOAR передбачає оперативне вживання заходів для мінімізації збитків у результаті інциденту безпеки. Це охоплює ідентифікацію та класифікацію інцидентів, ізоляцію та нейтралізацію загроз, а також аналіз та документування інцидентів.

Коли вам варто задуматись над впровадженням SOAR?

Коли не вистачає відповідних ресурсів

Багато організацій борються з нестачею кваліфікованого персоналу, здатного ефективно реагувати на інциденти безпеки. SOAR автоматизує процеси реагування, заощаджуючи час і людські ресурси та одночасно забезпечуючи потужну реакцію на інциденти.

Коли стоїть гостра потреба дотримання нормативних вимог

Багато секторів економіки підпадають під суворі нормативні вимоги щодо кібербезпеки. SOAR дозволяє організаціям відповідати цим вимогам шляхом автоматизації процесів реагування на інциденти та звітування про результати.

Коли необхідно швидко реагувати на інциденти

У сучасному ландшафті відповідь на загрози має бути швидкою та ефективною. SOAR дбає про оперативне виявлення зловмисних дій та реагування на них, мінімізуючи збитки в результаті атак.

Коли є потреба у постійному вдосконаленні

Сучасні організації мусять постійно покращувати свої процедури та процеси у сфері кібербезпеки, щоб протистояти збільшеній кількості загроз. SOAR сприяє безперервному вдосконаленню процесів реагування на інциденти та покращує роботу команди з IT-безпеки. Він інтегрується з різними IT-системами та системами безпеки в організації, такими як SIEM, електронна пошта, хмарні середовища, системи продажу квитків, брандмауери тощо. Ця інтеграція дозволяє збирати інформацію з різних джерел, забезпечуючи комплексне управління інцидентами.

Архітектура

Сервери MISP і комерційні списки загроз займають провідне місце в архітектурі SOAR. З їхньою допомогою система отримує найактуальнішу інформацію про підозрілі IP- та URL-адреси, файли та IoC, сприяючи швидкому реагуванню на загрози.

SOAR також дозволяє виконувати певні автоматизовані дії на основі зібраної інформації. Він може проводити аналіз вкладень, блокувати хости, IP-адреси та файли пісочниці, а також сповіщати призначених осіб в організації.

Архітектура Energy SOAR складається з центральної точки, яка збирає всю інформацію, пов’язану з інцидентами безпеки та інтеграцією з різними системами. Використовуючи сервери MISP і комерційні списки загроз, SOAR може отримувати найновішу інформацію про небезпеки, забезпечуючи швидке реагування на інциденти.

Інтеграції

Energy SOAR запускає автоматизовані дії в IT-системах і системах безпеки через інтеграцію з їхнім API. Він налаштовує дії, які будуть виконуватися у відповідь на певні події чи інциденти, наприклад виявлення підозрілої активності чи атаки.

Коли SOAR виявляє загрозу або інцидент, він може ініціювати певні дії: наприклад, автоматично відправити всю систему в карантин або заблокувати IP-адресу в брандмауері. Він також може надсилати сповіщення іншим рішенням чи командам, інформуючи їх про інцидент і спонукаючи їх вжити заходів.

Варто зазначити, що SOAR зазвичай налаштований у такий спосіб, що дозволяє адміністраторам вибирати, які дії слід запускати за певних умов, відповідно до встановлених правил безпеки та політики організації.

Інтеграція з CSIRT

Інтеграція рішення класу SOAR із зовнішньою CSIRT (групою реагування на інциденти комп’ютерної безпеки) передбачає сприяння співпраці та обміну інформацією між компанією та зовнішнім постачальником послуг CSIRT.

SOAR може інтегруватися із зовнішньою CSIRT, пересилаючи інформацію, що пов’язана з інцидентом (наприклад, дані журналу) і результати аналізу, щоб отримати допомогу у розв’язанні проблеми. SOAR автоматично передає цю інформацію зовнішньому постачальнику послуг CSIRT, прискорюючи процес реагування на інциденти та підвищуючи його ефективність.

Інтеграція із зовнішнім CSIRT також дає змогу обмінюватися даними про тенденції та загрози кібербезпеки, допомагаючи компанії підвищити ефективність запобіжних заходів щодо майбутніх інцидентів.

Життєвий цикл SOAR в організації

Життєвий цикл SOAR — це безперервний процес, спрямований на забезпечення ефективного функціонування системи та задоволення вимог організації. Усі етапи цього циклу однаково важливі та вимагають належного планування й залучення організаційного персоналу.

Ключем до успіху впровадження SOAR є належне планування та узгодження з потребами організації, а також постійний розвиток і адаптація до мінливих вимог.

1 ПЛАНУВАННЯ

Визначаються цілі та вимоги організації, а також найпоширеніші типи інцидентів та процеси їх обробки в організації. Перевіряються можливості інтеграції з іншими рішеннями безпеки.

2 РЕАЛІЗАЦІЯ

На цьому етапі система налаштовується відповідно до вимог компанії, інтегрується з наявними рішеннями та інструментами. Для оптимізації операцій створюються автоматизовані процеси, а персонал, відповідальний за їх роботу, проходить спеціальне навчання.

3 ЕКСПЛУАТАЦІЯ ТА РОЗВИТОК

Як і будь-яке рішення безпеки у сфері IT, SOAR потребує постійного моніторингу, оцінки та розвитку. Це гнучке середовище, яке забезпечує безперервне зростання організації та автоматизацію все більш нових і передових процесів.

Створення робочих процесів

Користувачі можуть створити робочі процеси за допомогою редактора, який доступний в Energy SOAR. Редактор дозволяє додавати різні етапи до процесу, наприклад, дії, рішення, умови та інтеграції. Користувачі також можуть вказати, як саме слід запускати робочий процес: вручну, автоматично у відповідь на певні події або в певний час.

Кожен етап робочого процесу можна налаштувати для запуску певних дій в IT-системах та системах безпеки. Наприклад, коли SOAR виявляє загрозу, він може автоматично ініціювати робочий процес, який запускає автоматизовані дії в інших рішеннях (SIEM, IDS/IPS, антивірусах або системах керування подіями). Завдяки цій інтеграції, SOAR забезпечує автоматизацію процесів і покращує ефективність роботи у випадку інцидентів безпеки.

Як виглядає SOAR на практиці

Тож що являє собою покроковий процес роботи SOAR — від виявлення інциденту до реагування на нього?

1. Першим кроком є інтеграція SOAR з іншими системами безпеки — SIEM, IDS, IPS, EDR та електронною поштою. Він отримує дані про виявлені інциденти та автоматизує серію дій, які зазвичай потрібно виконувати вручну.

2. Після цього система виконує аналіз атрибутів отриманої події (спостережуваних), таких як IP-адреси, імена хостів, імена користувачів або URL-адреси. Кожному кейсу автоматично призначається рівень критичності та відповідні теги. Кейси можна призначати вручну або автоматично операторам, які отримують певні завдання для виконання. Кожен користувач має доступ до чіткого списку власних завдань, а весь процес розгляду справи фіксується в історії.

Якщо виконуються конкретні умови для певного типу кейса (наприклад, визначення відповідного правила кореляції), SOAR виконує весь процес обробки справи без залучення IT-фахівців. У таких випадках система не тільки збирає дані про інцидент, але й виконує завдання, які призводять до блокування IP-адреси на брандмауері або ізоляції комп’ютера в мережі.

За допомогою SOAR організація може швидко й ефективно реагувати на загрози безпеці, забезпечуючи захист даних і запобігання порушенням конфіденційності.

Варіанти використання

Аналіз електронної пошти

Якщо співробітник помітить, що отриманий електронний лист виглядає підозрілим або невідповідним, він може переслати його в SOAR, який проаналізує його зміст і структуру.

SOAR використовує різні механізми аналізу, такі як синтаксичний і семантичний, щоб ідентифікувати потенційно шкідливі елементи в повідомленні електронної пошти. Ці механізми дозволяють виявляти підозрілі посилання, вкладення та інші типові ознаки спроб фішингу. Система також може використовувати публічні або приватні списки загроз і бази даних, які містять інформацію про відомі спроби атак, що дозволяє порівнювати вміст повідомлення з цими загрозами.

Якщо SOAR визначає потенційну загрозу в повідомленні електронної пошти, він автоматично кваліфікує інцидент як потенційну фішингову атаку. Згодом система може виконати серію автоматизованих дій, щоб мінімізувати ризик. Можливі дії можуть передбачати блокування відправника повідомлення і його IP-адреси та пересилання підозрілого повідомлення до спеціалізованої групи аналізу безпеки інцидентів.

Під час виявлення фішингової атаки SOAR також має можливість сповістити відповідних осіб або команди в організації: команду безпеки, CSIRT або інші підрозділи інформаційної безпеки. Ці сповіщення дозволяють швидко реагувати на потенційні загрози.

Однією з ключових особливостей SOAR є можливість проводити подальший аналіз інцидентів. Команда безпеки або CSIRT може ретельно проаналізувати ситуацію, виявити потенційні загрози та вжити необхідних заходів для зменшення шкоди, завданої атакою.

Варіанти використання

Автоматичне блокування хостів / IP

Це один із найважливіших use cases, особливо в контексті захисту від атак зловмисного програмного забезпечення та злому мережі. Нижче наведено приклад того, як SOAR можна використовувати в цьому конкретному випадку.

Процес починається з виявлення потенційної загрози. SOAR, інтегрований з різними інструментами безпеки (системи виявлення та запобігання вторгненням (IDS/IPS), системи захисту від шкідливих програм або інструменти аналізу журналів), здатний ідентифікувати невідомі або підозрілі IP-адреси, які намагаються отримати доступ до мережі. Також SOAR може виявляти хости, що створюють підозрілий мережевий трафік.

Після виявлення загрози SOAR розпочинає аналіз. При цьому використовуються такі методи, як аналіз поведінки, аналіз тенденцій і порівняння із зовнішніми джерелами інформації про загрози, щоб оцінити, чи справді виявлена активність становить загрозу. Інцидент класифікується як загроза тільки після того, як SOAR підтверджує зловмисність дії. Інформація про цей інцидент зберігається в системі для подальшого аналізу.

Після класифікації інциденту SOAR виконує автоматичні дії, щоб заблокувати шкідливу IP-адресу або хост. Це може охоплювати налаштування мережевих брандмауерів для блокування трафіку, що надходить від визначеного джерела загрози, або блокування IP-адреси на рівні керування мережею.

Після блокування шкідливої IP-адреси або хоста SOAR автоматично сповіщає відповідних осіб про інцидент. Сповіщення можна передавати групі безпеки, CSIRT, IT-менеджерам або іншим відповідним сторонам. Повідомлення містить усю відповідну інформацію про інцидент, включно з подробицями вжитих дій.

Отримавши повідомлення, служба безпеки може провести подальший аналіз ситуації: наприклад, вжити додаткових заходів, таких як відстеження джерела атаки, посилення заходів безпеки мережі або навчання співробітників, щоб запобігти подібним інцидентам у майбутньому.

Нарешті, після закриття інциденту інформація про нього зберігається в SOAR для звітування та покращення. Цю інформацію можна використовувати для аналізу тенденцій, виявлення прогалин у безпеці, а також навчання команди.

Варіанти використання

Стеження за тенденціями аналізу загроз

Energy SOAR не тільки пропонує організаціям ефективне управління інцидентами безпеки, а й дозволяє досліджувати індикатори компрометації (IoC) та використовує поточні тенденції атак, щоб визначити, чи мали вони місце в компанії.

Приклад 1

У разі виявлення кампанії зловмисного програмного забезпечення, яка використовує певний домен для зв’язку HTTP, користувач SOAR може легко провести аналіз журналу DNS. Це допомагає перевірити, чи був зв’язок із цим доменом у системі. Якщо виявлено, що кінцева точка встановила такий зв’язок, є підозра на інфікування. Для мінімізації ризику подальшого розповсюдження загрози в SOAR можна вжити заходів, таких як карантин хоста або його повна ізоляція від мережі.

Приклад 2

Зловмисники часто використовують домени, схожі на популярні компанії, як-от «microsoft.com» (наприклад, «mlcrosoft.com»). У такому випадку інформація про поточні кампанії може з’явитися в списках Threat Intelligence. За допомогою SOAR можна проаналізувати журнали, щоб перевірити, чи не було підключення до цього підозрілого домену. Якщо такі з’єднання виявлено, можна вжити відповідних заходів для захисту організації від фішингу — наприклад, заблокувати доступ до цього домену або попередити користувачів про потенційну загрозу.

Отже, завдяки використанню можливостей SOAR для інтеграції зі списками розвідки про загрози та аналізу поточних тенденцій атак, рішення Energy SOAR дозволяє організаціям швидко реагувати на потенційні загрози.

Виявлення неавторизованих входів адміністраторів у неробочий час за допомогою SMS-підтвердження

Розглянемо приклад компанії XYZ, якій потрібно було захистити свою систему від несанкціонованого входу адміністратора в неробочий час. Мета полягала в тому, щоб реалізувати механізм перевірки входу за допомогою SMS-повідомлення з унікальним посиланням, яке адміністратор мав підтвердити протягом визначеного часу. В іншому випадку обліковий запис адміністратора буде автоматично заблоковано.

Процес реалізації

Виявлення неавторизованих спроб входу:

Energy SOAR був налаштований для моніторингу системних журналів і подій, пов’язаних із входом. У разі виявлення несанкціонованої спроби входу адміністратора в неробочий час система починає процедуру перевірки.

Генерація SMS-повідомлення:

SOAR автоматично генерує SMS-повідомлення, що містить унікальне посилання для підтвердження входу. Кожна спроба входу обмежена за часом (наприклад, 30 хвилин).

Надсилання SMS-повідомлення:

SOAR надсилає згенероване SMS-повідомлення з посиланням для підтвердження входу на зареєстрований мобільний пристрій, пов’язаний з обліковим записом адміністратора.

Підтвердження входу:

Адміністратор отримує SMS-повідомлення з посиланням для підтвердження входу на свій мобільний пристрій. Для підтвердження входу йому необхідно перейти за наданим посиланням.

Дії після підтвердження входу:

Після натискання посилання SOAR отримує підтвердження від адміністратора. Якщо підтвердження отримано протягом зазначеного часу (наприклад, 30 хвилин), вхід вважається авторизованим.

Блокування облікового запису в разі непідтвердження:

Якщо адміністратор не зможе підтвердити вхід протягом визначеного періоду часу, SOAR автоматично блокує обліковий запис адміністратора, мінімізуючи ризик несанкціонованого доступу та дій у системі.

Висновок

Завдяки процедурі перевірки входу адміністратора в позаробочий час за допомогою Energy SOAR, компанія XYZ отримала додатковий рівень захисту від неавторизованих входів.

Процес перевірки входу за допомогою SMS забезпечує додатковий рівень безпеки, мінімізуючи ризик несанкціонованого доступу. Реалізація описаної процедури може значно підвищити кібербезпеку організації, захищаючи дані та інфраструктуру від потенційних атак.

Energy SOAR — це одне з найбільш інноваційних рішень SOAR, доступних на ринку. Воно являє собою інтегровану платформу з IT-системами компанії, яка призначена для підвищення швидкості та ефективності реагування на інциденти безпеки. Energy SOAR є комплексним рішенням для управління інцидентами безпеки в організаціях, яке збирає всю інформацію щодо виявлених загроз.

BAKOTECH® — міжнародна компанія, яка посідає передові позиції у сфері фокусної Value Added IT-дистрибуції та постачає рішення провідних світових IT-виробників. Позиціонуючи себе як True Value-Added IT-дистриб'ютор, BAKOTECH надає професійну перед- та постпродажну, маркетингову, технічну підтримку для партнерів та кінцевих замовників.
Географічно компанія працює у 26 країнах на ринках Центральної та Східної Європи, Балкан, Балтії, Кавказу, Центральної Азії, з офісами в Празі, Кракові, Ризі, Києві, Баку та Нурсултані.

Якщо вам потрібна консультація щодо рішення, будь ласка, зв'яжіться з нами: els@bakotech.com

+380 67 100 0068
www.bakotech.com
www.energylogserver.com