Підвищення кіберстійкості: Як платформа Logsign Unified SO випереджає SIEM, SOAR та XDR

logsign.bakotech.com logsign@bakotech.com

Які ключові відмінності між SIEM, SOAR, XDR та Logsign Unified SO Platform?

SIEM, SOAR, XDR та Logsign USO Platform — це технології кібербезпеки, які допомагають організаціям виявляти, розслідувати кіберзагрози та реагувати на них. Однак вони відрізняються за сферою застосування, можливостями та спрямованістю. Ось основні відмінності між ними:

SIEM

Рішення Security Information and Event Management (SIEM) збирають і аналізують дані, пов'язані з безпекою, з різних джерел, таких як мережеві пристрої, сервери та кінцеві точки. Інструменти SIEM зіставляють дані та генерують сповіщення у разі виявлення підозрілої активності. SIEM зосереджується на виявленні інцидентів безпеки та забезпеченні видимості подій безпеки в IT-середовищі організації.

SOAR

Рішення Security Orchestration, Automation and Response (SOAR) автоматизують та оптимізують процеси реагування на інциденти. Інструменти SOAR інтегруються з іншими технологіями безпеки, такими як SIEM та EDR, щоб допомогти командам безпеки керувати сповіщеннями, автоматизувати завдання реагування на інциденти, а також ефективніше розслідувати та розв’язувати інциденти безпеки.

XDR

Рішення Extended Detection and Response — це вдосконалена і більш розвинена версія EDR, яка розширює сферу виявлення та реагування за межі кінцевих точок, включно з іншими частинами IT-середовища, такими як хмарна інфраструктура та мережеві пристрої. Рішення XDR використо-вують аналітику та машинне навчання, щоб співвідносити дані про безпеку з різних продуктів безпеки та генерувати сповіщення у разі виявлення загроз.

Logsign Unified SO Platform:

Logsign Unified SO Platform – це вдосконалена платформа для управління безпекою, збагачена такими функціями, як керування логами, кореляція, обробка даних та виявлення подій, аналіз загроз, управління інцидентами, автоматизація та розширені звіти. Вона використовує розширену аналітику для аналізу даних про безпеку з різних джерел, зокрема з мережевих пристроїв, серверів, програм і кінцевих точок. Logsign USO Platform інтегрує SIEM нового покоління, аналітику загроз, UEBA та SOAR і дає змогу організаціям оптимізувати та впорядкувати свої операції з кібербезпеки.

Крім того, платформа пропонує можливості безперешкодної інтеграції, що дозволяє без зусиль інтегрувати існуючі рішення для безпеки і використовувати велику бібліотеку інтеграції, розширюючи функціональність Logsign USO Platform і забезпечуючи комплексний підхід до управління безпекою. Завдяки цим широким можливостям, вона дозволяє організаціям покращити свій стан безпеки та забезпечити відповідність нормам і стандартам.

Діаграма рішень для SIEM, SOAR, XDR та Logsign Unified SO Platform

Рішення	Ключовий функціонал	Основні функції	Сценаріїї використання
SIEM	Збирає та агрегує події безпеки з різних джерел, аналізує події для виявлення загроз безпеці, генерує сповіщення для розслідування	Централізоване керування подіями безпеки	Виявлення потенційних інцидентів безпеки, забезпечення централізованого огляду подій безпеки, моніторинг відповідності нормативним вимогам
SOAR	Автоматизує реагування на інциденти за допомогою правил кореляції, правил сповіщення (alert rules) та правил дії (action rules)	Оркестрація й автоматизація операцій з безпеки	Автоматизація розслідування та виправлення інцидентів безпеки, скорочення часу реагування, покращення узгодженості заходів реагування
XDR	Забезпечує комплексне виявлення загроз та реагування на них у різних доменах	Кросдоменне виявлення та реагування на загрози	Кореляція та аналіз подій безпеки з різних джерел, виявлення просунутих загроз на кінцевих точках, у мережі та хмарі
SO Platform Logsign Unified	Забезпечує комплексну уніфіковану платформу для управління безпекою, виявлення загроз та реагування на інциденти для підприємств будь-якого розміру	Керування безпекою на інтегрованій платформі	Збір, кореляція та аналіз даних з різних джерел, забезпечення комплексної видимості, розсліду-вання, ефективне виявлення потенційних загроз, швидке автоматичне реагування на інциденти для їх виправлення та зменшення наслідків

Примітка: Певні функції вказаних технологій можуть варіюватися залежно від вендора. Тут розглянуті загальні можливості.

Порівняльна таблиця для SIEM, SOAR, XDR та Logsign Unified SO Platform

Рішення	SIEM	SOAR	XDR	Logsign Unified SO Platform
Керування логами	✓	✗	✗	✓
Моніторинг у реальному часі	✓	✓	✓	✓
Деталізоване розслідування	✗	✓	✓	✓
Аналіз даних	✓	✗	✗	✓
Звітування про комплаєнс	✓	✗	✗	✓
Керування кейсами та інцидентами	✗	✓	✓	✓
Виявлення загроз та реагування на них	✗	✓	✓	✓
Підтримка Mitre ATT&CK Mapping	✗	✓	✓	✓
Виявлення аномалій	✗	✓	✓	✓
Наявність специфічних знань у спеціалістів	✓	✗	✗	✗
Автоматизоване реагування	✗	✓	✓	✓
Автоматизація та оркестрація	✗	✓	✓	✓
Дослідження загроз	✗	✓	✓	✓
UEBA (Аналітика поведінки користувачів та суб'єктів)	✗	✗	✗	✓

Примітка: Певні фунції та кейси використання згаданих технологій можуть варіюватися залежно від вендора. Тут розглянуті загальні можливості.

Висновки

Logsign Unified SO Platform забезпечує всі функції, згадані в діаграмах вище, на єдиній платформі в інтегрованому вигляді, щоб допомогти організаціям підвищити рівень безпеки і знизити ризик кібератак, надаючи їм інтегровану і ефективну платформу управління безпекою, яка містить всі можливості SIEM, SOAR, XDR і багато іншого. За допомогою Logsign USO Platform організації зможуть централізувати свої операції з безпеки, у такий спосіб досягаючи підвищеної ефективності з точки зору часу і людських ресурсів на додаток до значно покращеного рівня безпеки.

Logsign

Logsign — це міжнародний постачальник, який спеціалізується на наданні комплексних рішень з кібербезпеки, що дозволяють організаціям підвищити свою кіберстійкість, знизити ризики та оптимізувати процеси безпеки, водночас зменшивши хаос в HR- та операційному відділах. Logsign незмінно пропонує ефективну, зручну та бездоганну платформу і використовує новітні технології для створення безпечних, стійких і сумісних середовищ, надаючи організаціям комплексну видимість своєї IT-інфраструктури, розширюючи можливості виявлення загроз і оптимізуючи зусилля з реагування на них. У сучасному складному ландшафті загроз Logsign гарантує, що компанії мають відмінний процес кібербезпеки, проактивно захищаючи свої системи, дані та цифрові активи. Компанія Logsign представлена на чотирьох континентах, її клієнтська база налічує понад 600 підприємств і державних установ, уже два роки поспіль компанія згадується в магічному квадранті Gartner SIEM. Крім того, Logsign має високі рейтинги на сайтах Gartner Peer Insight і G2.

bakotech

BAKOTECH — міжнародна компанія, яка займає лідируючі 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 до- та постпродажну, маркетингову, технічну підтримку для партнерів та кінцевих замовників.

logsign.bakotech.com

logsign@bakotech.com