Splunk Enterprise Security: сучасне дата-центричне SIEM-рішення

splunk> a cisco company

Число кіберзагроз невпинно зростає, збільшуючи навантаження на персонал центрів управління кіберзахистом (SOC). Щоб SOC міг ефективно працювати, потрібні технічні рішення, які ефективно фільтрують сповіщення і автоматизують реагування. Саме такі пропонує Splunk.

Сьогоднішній ландшафт загроз створює чимало проблем для фахівців з кіберзахисту, адже їм доводиться обробляти величезну кількість даних, що надходять з різноманітних джерел, аби мати видимість усього гетерогенного хмарно-локального середовища. Згідно з опитуванням, проведеним серед SOC організацією SANS Institute у 2023 році, головною перешкодою для успішної роботи SOC є брак контексту для безпекових подій. Через величезну кількість сповіщень, на які потрібно реагувати, аналітикам важко без контексту визначити, які з них є пріоритетними. Окрім того, 41% сповіщень взагалі ігноруються, бо персонал фізично не в змозі їх обробити.

За даними Splunk, працівники команд безпеки мають справу в середньому з понад 25 інструментами, які відповідають за виявлення інцидентів, розслідування і реагування на них. В результаті аналітики витрачають на розслідування інциденту в середньому три години.

Традиційні SIEM-системи, які використовуються в SOC, мають кілька серйозних недоліків. По-перше, вони не дають централізованої видимості, тобто не можуть забезпечити автоматичне приймання, нормалізацію і аналіз даних з будь-якого джерела. Окрім того, сам процес внесення даних може бути або дуже трудомістким, або дуже дорогим. Усе це збільшує час виявлення загроз і реагування на них.

Також традиційні SIEM не спроможні зменшити обсяг сповіщень, які мусять обробляти аналітики. Часто вони, навпаки, генерують ще більше сповіщень і хибних тривог, що збільшує навантаження і втому персоналу, створює додатковий шум і ускладнює виявлення високопріоритетних загроз. Ці SIEM часто не можуть інтегруватися зі сторонніми інструментами, через що користувачі змушені послуговуватися тими можливостями, які включені в SIEM, або витрачати додаткові кошти на додаткові розробки чи професійні послуги.

SIEM нового типу

Splunk є провідним виробником SIEM і рішень для безпекової аналітики. У 2024 році компанію вже вдесяте визнано лідером у звіті Gartner Magic Quadrant for Security Information and Event Management, також вона стала лідером у дослідженнях Forrester і IDC – єдина, яка отримала цю відзнаку від усіх трьох.

Splunk має низку ключових переваг, серед яких – потужна аналітика в реальному часі, гнучкість у зборі даних з будь-яких джерел, вбудовані AI-алгоритми для виявлення загроз та автоматизація реагування (SOAR). Рішення дозволяє обробляти великі обсяги інформації, зменшує кількість хибних спрацювань і надає зручні дашборди для централізованого керування безпекою.

Splunk Enterprise Security – це платформа, якій довіряють SOC'и всього світу. Це SIEM нового типу, завдяки якій аналітики мають усе, що їм потрібно, на одному робочому столі без необхідності перемикатися між різними інструментами. Платформа підтримує понад 1400 правил виявлення загроз (детекцій) «з коробки» і понад 100 за допомогою хмари. Ці детекції відповідають галузевим стандартам, таким як MITRE ATT&CK, NIST CS F 2.0 та Cyber Kill Chain. Окрім того, Splunk пропонує інструмент машинного навчання (Machine Learning Toolkit – MLTK) для швидшої детекції загроз шляхом виявлення аномалій. Група з дослідження кіберзагроз – Splunk Threat Research Team – надає найновішу інформацію щодо загроз і методів їх виявлення.

Серед подібних рішень Splunk Enterprise Security вирізняє дата-центричний підхід до безпеки, покладений в основу цієї SIEM.

- **Будь-які дані, будь-які джерела:** розрізнені дані стають доступними у вигляді, придатному для пошуку і подальших дій на їхній основі.
- **Швидкі, гнучкі розслідування:** забезпечує стовідсотковий комплаєнс і вп'ятеро прискорює розслідування безпекових інцидентів.
- **Доведена масштабованість:** рішення здатне приймати терабайти даних за день і здійснювати понад мільйон пошуків за тиждень.
- **Відкрита екосистема:** понад 2800 інтеграцій забезпечують підтримку будь-якого стеку технологій, наявного у користувача.
- **Підтримка будь-яких сценаріїв розгортання:** забезпечується ефективний моніторинг і захист мультихмарних та гібридних середовищ.

SIEM НОВОГО ПОКОЛІННЯ – КЛЮЧОВИЙ ЕЛЕМЕНТ СУЧАСНОЇ КІБЕРБЕЗПЕКИ

Сучасні кіберзагрози стають дедалі складнішими, а традиційні методи їх виявлення вже не справляються. SIEM нового типу – це еволюція систем інформаційної безпеки, яка поєднує потужну аналітику, автоматизацію та штучний інтелект. Завдяки такому підходу загрози виявляються в режимі реального часу, а реагування на них відбувається автоматично, без затримок і людського фактора. Це означає, що компанії отримують миттєвий захист, а їхні IT-фахівці можуть зосередитися на стратегічних завданнях, а не на ручному аналізі загроз.

Володимир Дубей,
Директор Winncom Technologies

SIEM нового покоління – це не просто моніторинг, а проактивна безпека, яка випереджає атаки ще до того, як вони стануть проблемою. Саме тому Winncom Technologies вважає такі рішення ключовим елементом сучасної кібербезпеки.

Сповіщення на основі ризиків

Унікальна технологія **Risk-Based Alerting (RBA)** здатна суттєво скоротити кількість сповіщень, які отримує персонал. RBA використовує метод кореляційного пошуку, який зводить безпекові події в єдиний індекс ризиків. Механізм детектування виявляє подію, доповнює її метаданими на кшталт джерела тривоги, атакувальної техніки згідно з MITRE ATT&CK і оцінки ризику, після чого динамічно оновлює цю оцінку залежно від атрибутів відстежуваного об'єкта: наприклад, чи причетний до інциденту користувач з привілеями доступу або сервер з виходом в Інтернет.

Аналітик отримує сповіщення (Risk Notable) лише тоді, коли задоволено задані критерії (зафіксовано достатньо подій, пов'язаних з об'єктом). В середньому RBA зменшує число сповіщень на 50–90%, а ті, що залишаються, мають високу достовірність, і їх можна розслідувати простіше й швидше.

Водночас кореляція кількох подій з присвоєнням їм оцінок (наприклад, відправлення листа на домен конкурентів, активність у незвичні години, копіювання файлів на USB-носій) дозволяє генерувати сповіщення у випадках, коли ці події поодинці лишились би непоміченими. Також RBA виявляє комплексну зловмисну поведінку протягом визначених проміжків часу (**рис. 1**). Завдяки цьому всьому аналітики бачать загрози, які традиційні SIEM можуть пропустити.

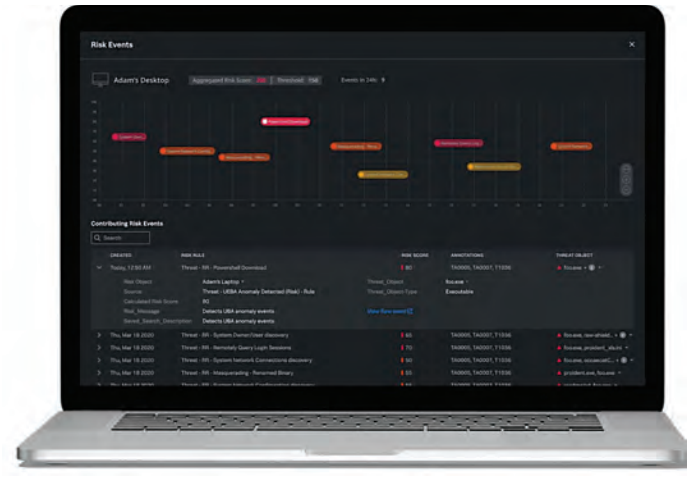

Рис. 1. Виявлення підозрілої поведінки з накопиченням оцінки ризику протягом доби

Швидко зрозуміти масштаб інциденту для точного реагування допомагає технологія візуалізації технології загрози – **Threat Topology Visualization** (**рис. 2**). Вона дає змогу визначити серйозність події та ідентифікувати інші об'єкти, зачеплені інцидентом, без необхідності написання жодного рядка пошукового коду. А технологія **MITRE ATT&CK Framework Matrix Visualization** показує використані злочинцями техніки і тактики у виявлених загрозах.

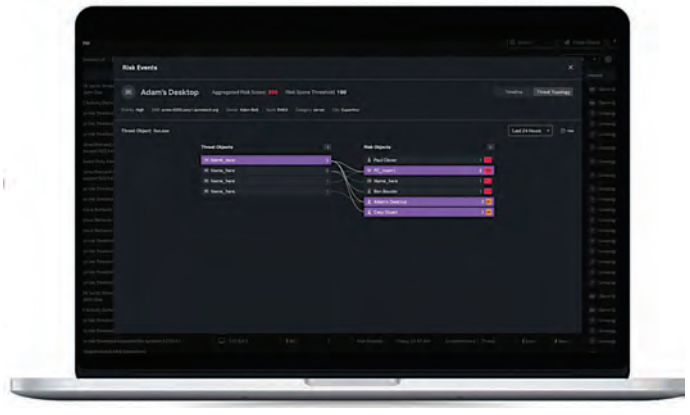

Рис. 2. Візуалізація топології атаки в Splunk

ПРО КОМПАНІЮ

Winncom Technologies – міжнародний системний інтегратор. Понад 25 років ми реалізуємо комплексні IT-рішення для різноманітних сфер бізнесу. Розвинена інфраструктура компанії, що включає офіси в Україні та Європі, дає змогу глибоко розуміти специфіку бізнесу на місцях. Тому наші клієнти отримують рішення та послуги, що враховують потреби конкретного ринку та водночас відповідають світовим стандартам і новітнім тенденціям.

Компанія Winncom Technologies є офіційним партнером Splunk зі статусом Associate Sell у трьох регіонах: Україні, Узбекистані та Казахстані. Наша команда включає 5 сертифікованих інженерів та сейлз-підрозділ, що спеціалізується на побудові та впровадженні рішень на базі Splunk. Ми зосереджені на реалізації проєктів у банківській, фінтех-сфері та державному секторі, допомагаючи клієнтам посилювати кібербезпеку, оптимізувати IT-інфраструктуру та отримувати цінні аналітичні інсайти з даних.

Winncom Technologies активно розвиває напрям SIEM-рішень, щоб допомогти бізнесу ефективно захищати дані, відповідати вимогам регуляторів та швидко реагувати на загрози.

Інтеграція з кіберрозвідкою і SOAR

Щоб мати об'єктивне розуміння безпекових подій, а також ризиків, які вони становлять, SOC потребує доступу до даних розвідки кіберзагроз (Threat Intelligence). Інтеграція кіберрозвідки у процеси SOC зменшує середній час виявлення загроз (MTTD) і середній час реагування (MTTR).

Функція **Threat Intelligence Management** дає змогу аналітикам розслідувати безпекові інциденти, отримуючи інформацію безпосередньо в SIEM без звертання до інших інструментів безпеки. Аналітики можуть створювати списки індикаторів компрометації (IOC) для отримання сповіщень, які відповідають специфічним для підприємства сценаріям. Відфільтровуючи дані про кіберзагрози, які не стосуються конкретної організації, Threat Intelligence Management скорочує число сповіщень, щоб аналітики могли зосередитись на потрібних їм сценаріях. А інтеграція з RBA допомагає з розслідуванням критичних подій.

Також Splunk Enterprise Security нативно інтегрується зі Splunk SOAR. **Mission Control**, функція пакета SIEM, об'єднує усі робочі процеси, пов'язані з виявленням, реагуванням і розслідування і забезпечує інтеграцію з SOAR на рівні автоматизованих сценаріїв реагування (плейбуків), посилених даними кіберрозвідки. В результаті отримуємо повністю інтегровані процеси управління сценаріями, сортування сповіщень, розслідування інцидентів та реагування на них, і все це в рамках Splunk Enterprise Security. Аналітик може за лічені хвилини і в кілька кліків ізолювати і заблокувати загрозу. Інтуїтивно зрозуміла бічна панель надає додаткову інформацію (подія, що спричинила тривогу, виявлені атакувальні техніки, плейбуки, що їх автоматично згенерував SOAR тощо). А плани реагування, які зберігаються в SIEM, дають можливість аналітикам запускати відповідні процеси для поширених безпекових сценаріїв.

Splunk дотримується вендорно-нейтрального підходу, даючи можливість користувачам створювати власні застосунки для своїх сценаріїв або обирати потрібні з Splunkbase – бібліотеки, що налічує понад 2800 застосунків від більш ніж 2200 партнерів для збирання, пошуку, моніторингу і аналізу даних.

Детальніше: +38 (044) 594–98–24,
sales.ua@winncom.ua, https://winncom.ua