SIEM, SOAR, XDR:
від журналу журналів до агентів

Людство створило безліч інструментів кібербезпеки, які в різній мірі перекривають одні одних. Це стосується і платформ автоматизації. Але генеративний ШІ добрався і до них.

Системи управління інформацією і подіями безпеки (SIEM) створювались для впорядкування і кореляції даних, які надходили від різних інструментів, виявлення загроз і централізованого моніторингу безпеки. Поступово функції SIEM доповнювались і розширювались. Сучасні системи базуються в хмарі, підтримують аналітику з використанням штучного інтелекту, інтегруються з іншими інструментами або й включають у себе їхню функціональність. Наприклад, SOAR, який автоматизує рутинні операції реагування. Рішення класу XDR також забезпечують збирання інформації про інциденти і автоматизоване реагування.

«МтБ» спробував дослідити, у яких напрямках рухаються ці системи і чи потрібні вони всі одночасно.

SIEM: як зробити дешевше

Gartner у своєму звіті Magic Quadrant for Security Information and Event Management, який вийшов на початку жовтня, визначає SIEM як налаштовувану систему обліку, яка збирає, агрегує і аналізує дані щодо безпекових подій з локальних і хмарних середовищ.

Згідно з визначенням, SIEM повинна обов'язково вміти отримувати дані з широкого кола систем; мати гнучкі опції щодо тривалого зберігання найважливіших даних та/або їх доступності для архівного пошуку; дозволяти користувачам самостійно розробляти або змінювати сценарії виявлення загроз на основі кореляційних, аналітичних і сигнатурних методів; підтримувати вендорський контент для виявлення і реагування на загрози та мати можливості для створення й налаштування власного контенту; забезпечувати генерацію звітів для власних цілей підприємства, виконання вимог законодавства (комплаєнсу) й аудиту; мати можливості для кастомного покращення робочих процесів у частині реагування і звітування; а також забезпечувати розслідування, представлення доказів і створення звітів на базі сповіщень, які генеруються при виявленні загроз.

Також Gartner наводить цілий список інших поширених функцій SIEM, серед яких: різні варіанти розміщення (локально, хостинг у хмарі, cloud native і SaaS); взаємодія з XDR, що включає EDR, NDR та інші функції розширеного збирання телеметрії та реагування; інтеграції зі сторонніми платформами накопичення різнотипних даних (data lake)

для їх там зберігання пошуку; децентралізований пошук за межами вендорського репозиторію і доручення додаткової інформації з зовнішніх джерел; функції платформи розвідки загроз (TIP) і маркетплейс, який дозволяє підписуватись на сторонній контент та інтегрувати технології інших вендорів; можливості покращення робочих процесів за допомогою автоматизації, оркестрації рутинних завдань і використання штучного інтелекту; тощо.

Gartner оцінював виробників SIEM впродовж 2024 року і по лютий 2025-го. В актуальному звіті до квадранту лідерів зараховано компанії Splunk, Microsoft, Securonix, Exabeam і Gurucul. Претендентами є Rapid 7, Palo Alto Networks і Fortinet, візіонерами — CrowdStrike та Elastic.

Gartner зазначає, що ринок SIEM не лише зростає, а й еволюціонує. Замовники продовжують купувати SIEM насамперед для операцій з виявлення загроз, розслідування і реагування (TDIR), а також для комплаєнсу і звітності. Друга причина пов'язана з розвитком SIEM: покупцям потрібні платформи, які простіші в експлуатації, забезпечують кращі можливості для управління даними і краще підтримують хмарні середовища.

Щоб зменшити вартість рішень SIEM, деякі вендори, як-от Microsoft, Palo Alto Network і CrowdStrike, включили SIEM до складу ширших хмарних рішень з пакетними ліцензіями. Інші виробники пропонують градацію обсягів вхідних даних, які часто називають причиною роздування вартості SIEM. У цьому варіанті замовники можуть обирати, які дані спрямовуються в SIEM для більш преміальних операцій, а які — для менш преміальних (наприклад, зберігання і пошук). Деякі вендори вбачають шлях зменшення складності SIEM у їх комбінуванні з іншими безпековими продуктами, такими як XDR та платформи розвідки загроз і оцінювання загальної вразливості (exposure assessment). Щоправда, хоча моновендорний підхід дозволяє скоротити експлуатаційні витрати, він може обмежувати SOC у виборі інструментів.

Інший підхід полягає у впровадженні автоматизації і штучного інтелекту. ШІ використовується для збирання інформації з журналів, виявлення загроз, збагачення інформації і покращення робочих процесів. Замовники очікують від виробників, що SIEM підтримуватиме запити природною мовою, пропонуватиме дії з нейтралізації загроз і виявлятиме тренди.

SOAR мертвий?

Прикметно, що Gartner у визначеннях функцій, які підтримує або з якими інтегрується SIEM, не згадав SOAR (Security Orchestration, Automation and Response). Це тому, що Gartner вважає SOAR вже не таким корисним і ефективним, як раніше. У своєму звіті «Цикл гайпу програм управління IT-сервісами (ITSM)» Gartner помістив SOAR на самому дні «жолоба розчарування», що означає, що «інновація не виправдовує завищених очікувань» (**рис. 1**)

Як зазначає компанія BlinkOps, яка спеціалізується на автоматизації кібербезпеки за допомогою агентів, термін SOAR з'явився у 2017 році на позначення інструмента, покликаного покращити ефективність реагування на кіберзагрози. «Оркестрація» означає інтеграцію різних систем та інструментів безпеки для створення механізму автоматичного

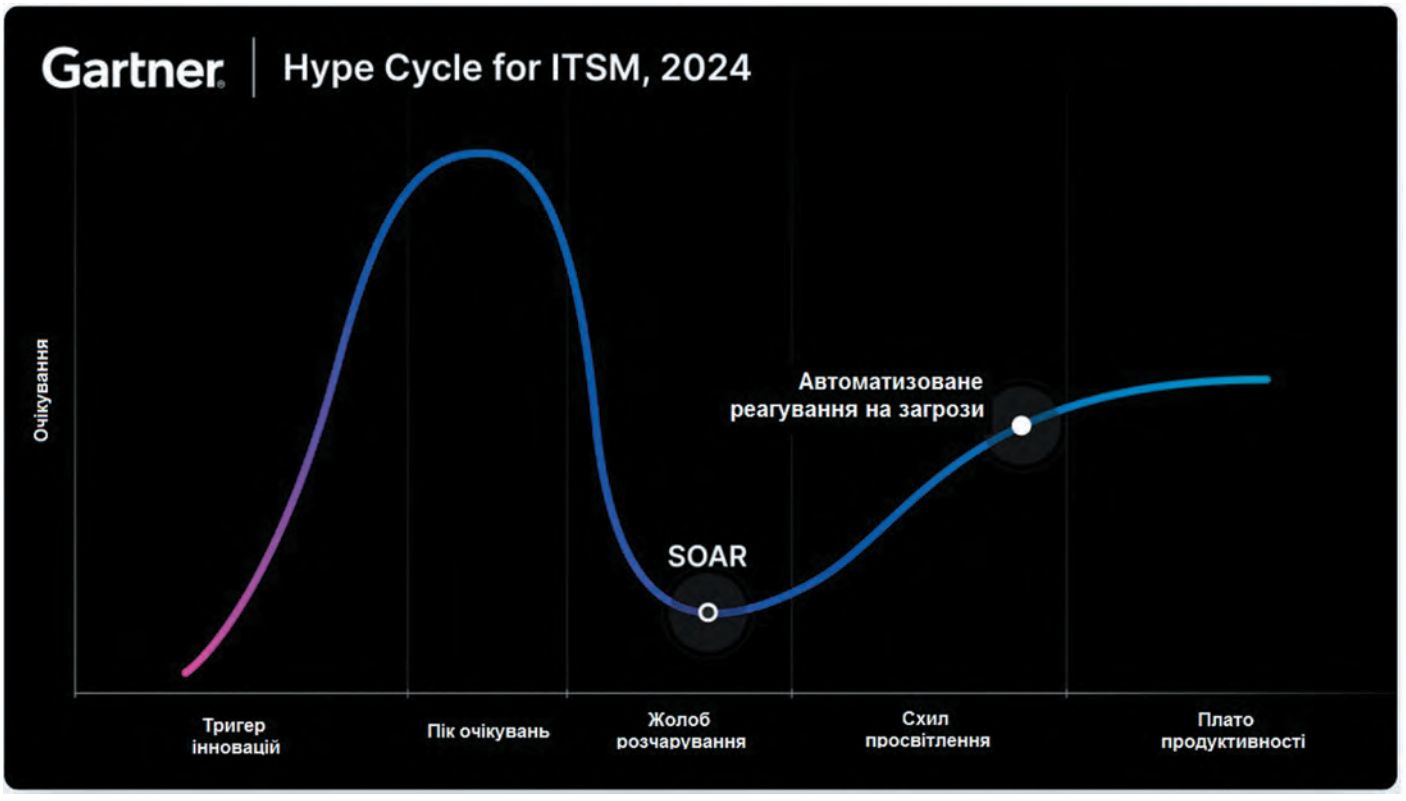

Рис. 1. SOAR на кривій гайпу Gartner (джерело: Torq)

реагування і забезпечення уніфікованого підходу до виявлення і знешкодження загроз. «Автоматизація» охоплює різні рутинні завдання, такі як сканування на вразливості, аналіз логів і створення тікетів, що вивільняє персонал для більш комплексної роботи. «Реагування» відбувається за допомогою наперед визначених плейбуків, які забезпечують автоматичні і напівавтоматичні дії залежно від характеру загрози — наприклад, такі як ізоляція заражених систем, блокування небезпечних IP-адрес або сповіщення клієнта. Метою всього цього є скорочення середнього часу виявлення і реагування (MTTD/MTTR) і відповідно мінімізація можливих збитків.

В ранні роки, йдеться облозі компанії D3 Security, інвестори й аналітики прогнозували швидке поширення SOAR. У 2019 році той же Gartner передбачав, що до 2021-го число компаній, які впровадили в себе цю технологію, зросте в 14 разів. Ще у 2023 році Gartner розташовував SOAR у тому самому «жолобі розчарування», який сам по собі не є вироком, оскільки веде до «схилу просвітлення», де очікування стають більш реалістичними, і характеризував технологію як таку, що знаходиться на початку етапу своєї зрілості з рівнем поширення у 20–50% і 5–10 роками до плато. Але щось пішло не так.

Попри потенціал, SOAR-рішення зіткнулись з проблемами, які зрештою призвели до їхнього занепаду. Впровадження SOAR вимагає значних коштів, а його налаштування під конкретні потреби може бути складним і витратним процесом. Платформу потрібно постійно оновлювати і підлаштовувати відповідно до нових загроз, що збільшує сукупну вартість володіння. Для роботи з SOAR потрібні фахівці з солідними навичками програмування і знанням розмаїтих інструментів безпеки, що означає залежність від кваліфікованого персоналу. Хоча SOAR розрахований на інтеграцію з різнорідними системами захисту, на практиці це може бути складно, що обмежує ефективність платформи. Врешті-решт SOAR не в змозі автоматизувати кожен можливий сценарій і вимагає людського втручання у разі комплексних і новітніх загроз. Розрив між очікуваннями і реальністю викликає розчарування у користувачів.

SOAR все ще потрібен

Журналіст Роберт Лімос у своєму матеріалі на Dark Reading, характеризує ситуацію словами: «Gartner дав, Gartner і взяв», зазначаючи, що це не перша технологія, визнана застарілою: наприклад, у 2010 році така доля спіткала інтернет по електропроводці, а у 2022-му — технологію Data Mesh. Передчасне застарівання стається зазвичай через появу конкуруючої технології.

Інші фахівці вважають, що не все так однозначно. Заява, що SOAR мертвий, «це найтупіше, що я чув, абсолютно безглуздо, — так висловився Джеймс Брір, CEO компанії Swimlane, яка спеціалізується на автоматизації кібербезпеки. — Якщо прибрати термін SOAR і вставити термін «автоматизація», то це твердження звучатиме абсурдно. Все одно що сказати, ніби ШІ відходить».

Роберт Лімос зазначає, що не всі виробники взагалі готові відмовитись від SOAR. Наприклад, Palo Alto Networks, навпаки, ще більше вкладається в автоматизацію. Компанія має власний SOC, який обробляє 36 млрд подій щодня — обсяг інформації складає 75 ТБ — силами усього лише 10 фахівців. Компанія стверджує, що її рішення Cortex XSOAR автоматизує роботу 16 аналітиків і забезпечує до 90% скорочення часу на ручні операції для замовників. «Хоча багато окремих продуктів з кібербезпеки надалі інтегруватимуть певний рівень автоматизації, рішення SOAR забезпечують більш надійні можливості для оркестрації й автоматизації розмаїтих дій в технологічному стеку організації», — прокоментував у цьому зв'язку Гонен Фінк, старший віце-президент PAN з продуктів Cortex і Prisma Cloud.

Аналітична компанія Omdia вважає, що виокремлена платформа SOAR залишається геть не застарілим, а цілком потрібним і виправданим підходом для багатьох компаній. Проте користувачі бажають рішень, які є простими в використанні, потребують мінімального навчання і легко інтегруються з іншими продуктами, тож виробники мусять надалі адаптувати свої платформи і розширювати сумісність з іншими вендорами і рішеннями.

Swimlane на своєму сайті публікує власні тренди ймовірного подальшого розвитку SOAR. По-перше, платформи розширять свою функціональність за межі традиційних сценаріїв виявлення загроз і реагування на інциденти: ймовірно, з'являться функції моніторингу в цілях комплаєнсу, оцінювання ризиків тощо. По-друге, стане більше гнучкості і можливостей налаштування, щоб організації могли підганяти SOAR-платформу під свої потреби і завдання. По-третє, оскільки організації активно переводять свою IT-інфраструктуру до хмари, необхідна інтеграція з хмарними інструментами і технологіями захисту. А щоб подолати дефіцит кваліфікованих працівників в умовах швидкозмінного ландшафту загроз, команди SOC дедалі більше надають перевагу рішенням з мінімальними потребами в програмуванні (low-code), які спрощують користування продуктом і водночас забезпечують досить потужні можливості.

Зрештою, певний аналог квадранта Gartner для SOAR існує: звіт QKS Group SPARK Matrix for Security Orchestration, Automation & Response (**рис. 2**).

XDR як SOAR

А все ж, які технології здатні замінити SOAR? По-перше, є версія (з застереженнями), що нішу SOAR можуть зайняти інші продукти. Наприклад, SIEM і XDR. D3 Security, однак, пише, що XDR з'явився на ринку не на заміну SOAR, а разом з ним. У 2024 році Gartner у своєму звіті Hype Cycle for Security Operations помістив XDR так само у «жолоб розчарування» одразу за SOAR і записав до технологій, які не встигають за мінливими вимогами компаній-замовників. У власному дослідженні, яке D3 Security проводила у 2024 році серед провайдерів керованої безпеки (MSSP), респонденти найчастіше називали головним інструментом автоматизації саме SOAR, тоді як XDR опинився на третьому місці (**рис. 3**).

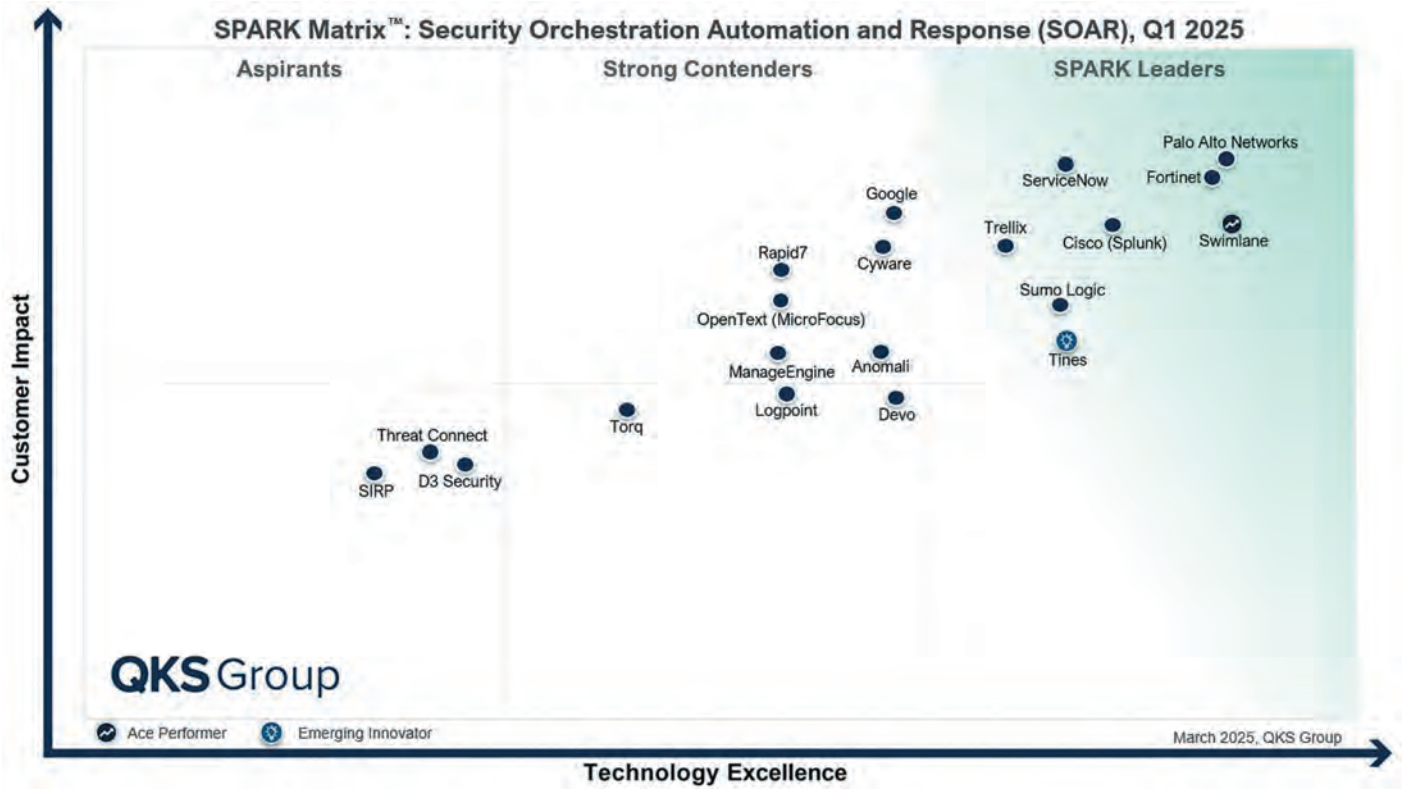

Рис. 2. «Матриця» SOAR QKS Group (2025 рік)

Хоча можливості цих інструментів частково збігаються, XDR розглядають радше як альтернативу SIEM, ніж SOAR. Серед великих організацій багато хто використовує і XDR, і SOAR: перший для виявлення загроз і предиктивних інсайтів, другий — для сортування подій і оркестрації. Сайт цитує слова Стівена Таллента, керівника MSSP High Wire Networks, який зазначив: якщо придивитись до різних платформ, які забезпечують функціональність XDR, то їм бракує можливостей, що їх надає повноцінний SOAR: сортування подій, зменшення ризиків, скорочення часу реагування і підвищення ефективності персоналу.

Агенти замість інструментів

Тим не менше йдеться у матеріалі Роберта Лімоса, хоча головні сценарії використання SOAR ніде не поділися,

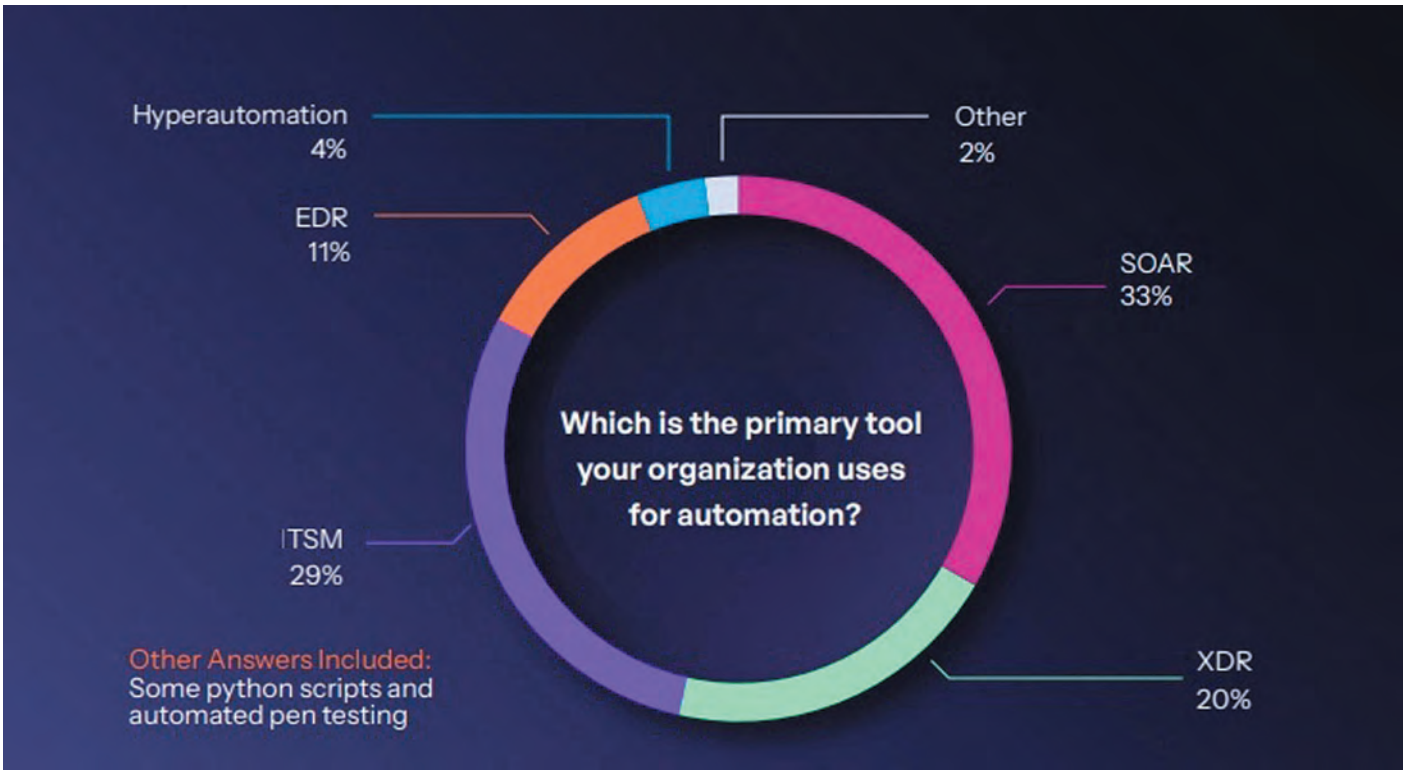

Рис. 3. Головний інструмент автоматизації (джерело: D3 Security)

Табл. Як сучасні ШІ-рішення можуть подолати проблеми, з якими стикається SOAR (джерело: BlinkOps)

Аспект	Традиційний SOAR	Рішення на базі генеративного ШІ
Можливості автоматизації	Автоматизує рутинні завдання	Автоматизує складні завдання, адаптується до нових загроз
Інтеграція	Часто ускладнена, вимагає спеціалізованих конекторів	Проста інтеграція за допомогою передових API і ML-алгоритмів
Фінансова ефективність	Високі стартова вартість і експлуатаційні витрати	Більш фінансово ефективне в довгостроковій перспективі, менше людського втручання
Взаємодія з людиною	Потребує висококваліфікованих аналітиків	Доповнює аналітиків, фокусує їхню увагу на стратегічних завданнях
Необхідні навички	Вимагає спеціалізованих навичок програмування	Дружнє до користувача, часто з низькими або нульовими вимогами щодо програмування
Доступність	Лише для фахівців з технічними знаннями	Демократизує доступ до просунутої автоматизації
Очікування	Часто вважається «срібною кулею»	Створене, щоб доповнювати людину, а не замінити її

поєднання автоматизації, ШІ та низки наявних вже продуктів з кібербезпеки може привести до появи платформи, яка перейме ринкову нішу у нинішніх SOAR: наприклад, SIEM нового покоління на базі ШІ-агентів. Він цитує Еріка Парізо, провідного аналітика Omdia, який вказує: людей, котрі приймають рішення в SOC, цікавлять не так оркестрація й автоматизація, як швидший і ефективніший цикл TDIR з кращими і стабільнішими результатами.

А Чес Клоусон, CTO компанії Sumo Logic, яка спеціалізується на платформах автоматизації безпеки, в коментарі зазначив, що хоча ШІ-агенти у галузі кібербезпеки все ще знаходяться у зародковому стані, індустрія з певністю рухається в цьому напрямку. ШІ-агент може програмувати, має доступ до API і всієї документації, з ним можна взаємодіяти як з людиною, тож «якщо ви маєте в своєму розпорядженні такого агента, який може зробити все, що ви захочете, це розмиває цінність SOAR», — зазначив він.

Вже згадана компанія BlinkOps, яка сама пропонує платформу автоматизації кібербезпеки на базі агентів, також вважає, що майбутнє пов'язане не з SOAR, а з рішеннями на базі генеративного ШІ. У таблиці, представленій BlinkOps, показано переваги таких рішень, хоча треба усвідомлювати, що лише час покаже, чи є це справді проривом, чи повторенням хайпу.

А як щодо SIEM? Джек Нальєрі, засновник компанії Panther Labs, у своєму блозі на Substack пояснює: тоді як SOAR допомагає з відомими і повторюваними шляхами, ШІ-агенти здатні динамічно оцінювати і обирати найефективніші способи вирішення проблеми. «Я завжди був такої думки, що SOAR як рішення, яке перевіряє сповіщення SIEM, є антипатерном. Якщо вам доводиться весь час повторювати одні й ті самі дії, то SIEM повинен мати ці функції у себе, а SOAR — використовуватись для усунення наслідків», — пише він.

ШІ-агенти можуть працювати як досвідчені аналітики, використовуючи потрібні їм інструменти, замість діяти відповідно до прописаних шаблонів, отримують відповіді динамічно. Якщо агент успішно виконує завдання, алгоритм може бути збережений для використання в майбутньому і прискорення аналізу.

Наприклад, у разі надходження сповіщення про підозрілий вхід в систему агент не дотримується статичного списку перевірок (чеклиста), а вибудовує динамічний шлях розслідування. Він може розпочати з даних про користувача, але, виявивши нещодавню зміну ролі, переходить до аналізу поведінкових патернів у групі подібних. Якщо він помітить встановлення на пристрій незвичного застосунку, то окремо розгляне історію пристрою. Цей гнучкий підхід відображає те, як мислить вмілий аналітик — керуючись зачіпками, а не процедурами.

Окрім того, різниця не лише в тому, що автоматизація стає більш «розумною» — важливо, як агенти розуміють і запам'ятовують контекст. Традиційні безпекові інструменти обробляють кожне сповіщення окремо, натомість агенти знають усю історію подій в корпоративному середовищі. Інциденти безпеки розгортаються як взаємопов'язані історії, створюючи контекстну «павутину», підтримувати яку для людської пам'яті не під силу.

При цьому агенти виступають у ролі помічників, а не замінників людини. Вони складають докладні резюме, пропонують наступні кроки на основі історичних патернів і знаходять подібні інциденти у минулому. Важливо, що вони не вимикаються під час перезмінки, тож контекст довготривалих інцидентів не буде втрачено.

Партнерство між аналітиками і ШІ-агентами відображає фундаментальний зсув у розвитку кібербезпеки: не автоматизація всього, а інтелектуальне доповнення людських можливостей, пише Джек Нальєрі. Найуспішнішими будуть ті інструменти безпеки, які ретельно підтримуватимуть баланс між можливостями агента і людським наглядом, фокусуючись не на заміні людського судження, а на покращенні результатів. У міру того, як агенти ставатимуть більш досконалими, аналітики переходитимуть до розбудови стратегії, пошуку загроз і реагування на інциденти — до тих областей, де людські інтуїція і креативність залишаються незамінними.

Агентні системи SIEM вже є на ринку. У серпні компанія Trend Micro анонсувала цю технологію в рамках своєї платформи Vision One. За повідомленням, Agentic SIEM створили з нуля для подолання таких проблем, як висока вартість, складність і перевантаження сповіщеннями. «Те, що раніше потребувало багатотижневих налаштувань,тепер автоматизовано за допомогою Agentic AI — він вчиться, створює мапи і в процесі оптимізує дані», — стверджується в анонсі. Сценарії використання — виявлення інцидентів і реагування, комплаєнс і розслідування.

Тож платформи автоматизації на базі ШІ вже тут. Цікаво буде поглянути за кілька років, що буде в «квадрантах» і на «кривих гайпу».

Василь ТКАЧЕНКО, **МтБ**