Next-Gen SIEM від CrowdStrike: нове слово у переході до AI-driven безпеки

Андрій ЛЕВЧЕНКО, BDM в iIT Distribution, — про можливості новітнього продукту Next-Gen SIEM.

Злочинці діють дедалі спритніше. Впоратися з сучасними загрозами може тільки штучний інтелект.

Кібербезпека давно стала важливою частиною сучасного світу. Нещодавня масштабна кібератака на державні реєстри України вчергове підкреслює необхідність впровадження сучасних технологій захисту та забезпечення безпеки цифрових активів.

Зловмисники та зокрема російські хакери стають все більш винахідливими в своєму інструментарії та досягають своїх цілей швидше. За даними «Звіту про глобальні загрози 2024» від CrowdStrike, найкоротший час прориву злочинів був зафіксований у 2023 році і становив лише 2 хвилини і 7 секунд. Це підкреслює необхідність забезпечення аналітиків з безпеки сучасними інструментами, які вирівнюють умови гри і дозволяють їм працювати більш ефективно і результативно.

Сучасні аналітики потребують нового покоління технологій управління інформацією та подіями безпеки (SIEM), здатних масштабуватися для управління петабайтами даних. Водночас постає питання: чи можуть сучасні SIEM відповідати вимогам часу?

Давайте розглянемо основні переваги та можливості новітнього продукту Next-Gen SIEM від CrowdStrike. Чи це справді те, що можна назвати ***«next-gen»***? Чи просто черговий маркетинговий слоган? І де та межа, після якої ми готові сказати: ось він — продукт майбутнього?

Що таке Next-Gen SIEM?

Next-Gen SIEM — це не просто інструмент для збору та обробки логів, а повноцінна екосистема для забезпечення безпеки в сучасних умовах кіберзагроз. Така система поєднує кілька ключових характеристик, які роблять її незамінною:

- масштабується без обмежень у хмарі, що дозволяє забезпечувати безперервну роботу навіть для найскладніших інфраструктур;
- відповідає на запити в петабайтах даних **менш ніж за 2 секунди**, що значно скорочує час реакції на інциденти;
- має **автоматизовані можливості AI**, які дозволяють команді SOC сфокусуватися на ключових завданнях, а не на рутині;
- забезпечує **інтерактивний воркбенч**, що дозволяє проводити розслідування з максимальним комфортом.

В результаті маємо характеристики майже автономної системи, що здатна самостійно виконувати як прості, так і складні завдання, надавати повну інформацію про інциденти, генерувати аналітику та дашборди, а також забезпечувати швидке реагування навіть на найбільш непередбачувані загрози. Це рішення ідеально підходить для сучасних організацій, які прагнуть бути на крок попереду прогресивних кіберзлочинців.

Витоки Next-Gen SIEM

Аби зрозуміти, як CrowdStrike прийшов до створення власної SIEM, повернімося до 2021 року. У час, коли світ переживав пандемію COVID-19 та посилення політичної нестабільності, **CrowdStrike купує компанію-стартап Humio** з річним доходом в $19 млн, заплативши $400 млн. Революційна безіндексна архітектура Humio, яка стане основою для створення майбутнього CrowdStrike SIEM, забезпечує феноменальну **швидкість запитів і стиснення даних до 25х і більше**. Ці характеристики дали CrowdStrike надійний технологічний фундамент для побудови SIEM-рішення нового покоління.

Чи вийшло у CrowdStrike?

Коротка відповідь – так.

CrowdStrike Next-Gen SIEM повністю відповідає вимогам сучасного SOC-ком'юніті. Продукт пропонує всі функції, що зазначені у попередніх розділах, і навіть більше

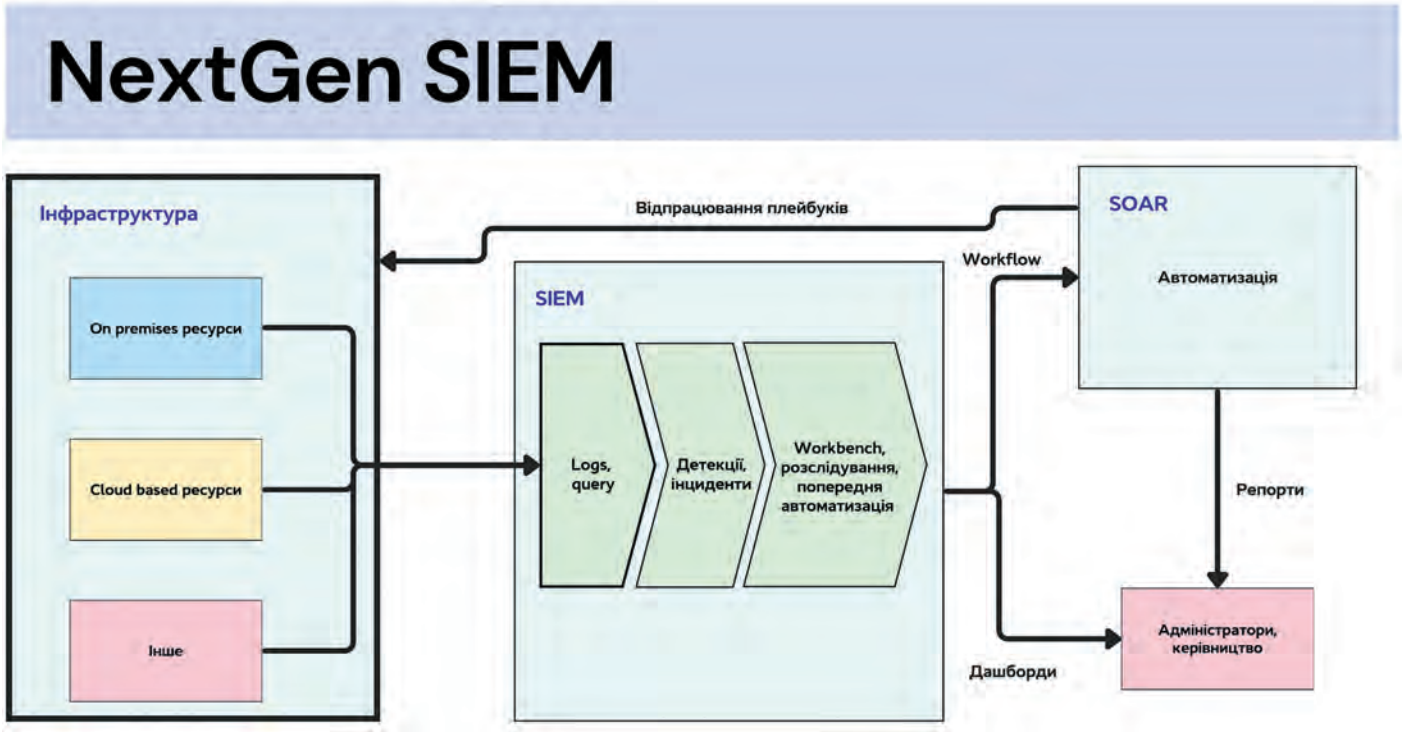

Рис. CrowdStrike Next-Gen SIEM

(**рис.**). CrowdStrike створив одну із найпотужніших платформ, здатну значно спростити роботу аналітиків безпеки та підвищити ефективність SOC. Можливості CrowdStrike SIEM.

Універсальна інтеграція логів: підключення джерел даних з хмари, on-prem, мережевих пристроїв і навіть спеціалізованих платформ, як-от Cribl, виконується легко і швидко.

Автоматизація з SOAR (CrowdStrike Fusion): завдяки інтеграції з SOAR-платформою автоматизуються рутинні завдання, як-от реагування на інциденти або попереднє сортування логів, що дозволяє зосередитися на стратегічних задачах.

Безкоштовне зберігання логів з кінцевих пристроїв: це значно знижує витрати на інфраструктуру, дозволяючи зберігати критичні дані без додаткових фінансових витрат.

Глибока інтеграція з AI: CrowdStrike використовує штучний інтелект, який аналізує логи, автоматично виявляє аномалії, пропонує інсайти та забезпечує високий рівень деталізації даних.

Ефективна візуалізація: інтуїтивна платформа надає широкі можливості для аналітики, кастомізації дашбордів і створення звітів. Це дозволяє легко інтерпретувати дані і приймати оперативні рішення.

На додачу CrowdStrike абсолютно безкоштовно пропонує 10 ГБ зовнішніх логів щодня. Це означає, що навіть невеликі компанії, які не мають значних бюджетів, можуть скористатися всіма перевагами системи і підключити додаткові джерела даних без зайвих витрат.

Чому це важливо?

Застарілі інструменти не встигають за сучасними загрозами. Обтяжуючи команди безпеки нескінченними ручними процесами та надзвичайно низькою швидкістю пошуку, вони затримують розслідування та реагування і тим самим збільшують ризик зламу. Командам потрібна технологія SIEM наступного покоління, створена для масштабування та продуктивності, на основі автоматизації та ШІ.

Для SOC-аналітика час — головний ресурс. Якщо SIEM працює повільно або неефективно, команда замість аналізу інцидентів витрачає час на пошук даних. **CrowdStrike вирішує цю проблему** завдяки швидкості, автоматизації та інтеграції.

CrowdStrike створила продукт, який відповідає всім вимогам next-gen SIEM: масштабування, швидкість, AI, автоматизація. Це не просто крок вперед — це повноцінна революція в тому, як SOC-команди працюють з логами. Next-gen SIEM від CrowdStrike — це про зручність, ефективність та майбутнє кібербезпеки.

Вибір ефективних продуктів безпеки — це завжди непросте завдання. Рішення CrowdStrike функціонують як комплексна екосистема, що надає не лише передові технології кіберзахисту, але й доступ до світового рівня професійних знань та досвіду.

Отримати детальну інформацію про рішення від ***CrowdStrike*** *ви можете в офіційного дистриб'ютора на території України, компанії* ***iIT Distribution****:*
cs@iitd.io; www.iitd.ua