Falcon Guardian

Виявлення та реагування на загрози для ШІ-середовищ

ШІ-агенти змінюють підхід до роботи. ШІ вже не лише створює контент: агенти можуть аналізувати інформацію, отримувати доступ до корпоративних ресурсів і самостійно виконувати дії. Кількість таких агентів швидко зростає, тому компанії часто не знають, де вони працюють, хто ними користується, до яких ресурсів вони мають доступ і які ризики створюють.
Водночас уже відомі проблеми безпеки ШІ нікуди не зникли. Працівники додають ШІ-інструменти та ресурси швидше, ніж команди безпеки встигають їх виявляти, контролювати й захищати. Під час взаємодії з неврахованими ШІ-сервісами можуть передаватися конфіденційні дані. А ШІ-агенти та робочі навантаження, які створюють інженерні команди, стикаються з новими загрозами, зокрема атаками типу prompt injection.
Для безпечного впровадження ШІ компаніям потрібно контролювати його використання та захищати дії автономних агентів під час виконання.

Захист ШІ під час роботи

CrowdStrike Falcon® Guardian — флагманське AIDR-рішення CrowdStrike. Рішення забезпечує єдину видимість і контроль використання ШІ, захист під час роботи, розслідування та реагування.
Модуль виявляє ШІ-агентів, показує їхні дії та пов’язує активність ШІ з процесами на кінцевих пристроях. Це допомагає простежити весь ланцюг — від промпту до впливу на систему, оцінити масштаб інциденту та швидко відреагувати.
Falcon Guardian виявляє Shadow AI, захищає чутливі дані й протидіє атакам на ШІ-системи.

Безпечне впровадження та розробка ШІ-агентів

ШІ змінює роботу працівників, виконання завдань автономними агентами та розробку власних ШІ-рішень. Falcon Guardian об’єднує видимість, контроль, захист даних і протидію загрозам у середовищах кінцевих пристроїв, хмарних платформ і SaaS.

Безпечне використання ШІ працівниками
Виявлення Shadow AI, застосовування детальних політик доступу та захист чутливих даних. Контроль автономних ШІ-агентів, які працюють на кінцевих пристроях.

Безпечна розробка ШІ
Захист власих ШІ-застосунки, агентів і робочих навантажень під час їх роботи. Falcon Guardian блокує загрози, запобігає витоку даних і надає інформацію для розслідувань та контролю відповідності вимогам.

Ключові переваги

- **Виявлення Shadow AI**
  Постійна видимість дозволених і невідомих ШІ-агентів, місць їхньої роботи, відповідальних за розгортання та зон зосередження основних ризиків.
- **Контроль дотримання політик ШІ**
  Перетворення політик керування ШІ на технічні засоби контролю, управління дозволеними сценаріями використання ШІ та захист чутливих даних відповідно до встановлених вимог із запобіганням ненавмисним витокам.
- **Захист агентів під час роботи**
  Блокування prompt injection та інших атак на сторонніх агентів, установлених на кінцевих пристроях, і корпоративних агентів, розгорнутих у хмарі.
- **Швидше розслідування та локалізація загроз**
  Виявлення специфічних для ШІ загроз, відновлення послідовності дій агента, оцінка масштабу інциденту та своєчасне реагування для запобігання поширенню загрози на інші системи.

Ключові можливості

Виявлення ШІ та оцінка ризиків

- **Виявлення shadow AI та агентів:** Контроль використання ШІ в підтримуваних середовищах і постійне виявлення відомих та раніше невідомих ШІ-агентів.
- **Оцінка ризиків на кінцевих пристроях:** Інформація про те, де працюють агенти, хто ними користується, наскільки вони захищені та які дії потребують уваги.
- **Мапування зв'язків:** Поєднання даних про користувачів, облікові записи, моделі, агентів, інструменти та кінцеві пристрої для оцінки активності й ризиків.

Керування використанням ШІ та контроль доступу

- **Детальні політики безпеки:** Застосування контекстних правил до користувачів, агентів, моделей і взаємодій із ШІ.
- **Контроль агентів на кінцевих пристроях:** Дозвіл роботи затверджених типів агентів і блокування несанкціонованих.
- **Захист чутливих даних:** Виявлення та блокування конфіденційної інформації, персональних даних, облікових даних, секретів і вихідного коду.

Захист корпоративних ШІ-рішень

- **Захист під час роботи:** Виявлення та блокування загроз для корпоративних ШІ-застосунків, агентів і робочих навантажень.
- **Інтеграція із процесом розробки:** Підключення Falcon Guardian через SDK, хмарні інтеграції, ШІ-шлюзи або MCP-проксі.
- **Контроль дотримання політик:** Захист даних і застосування корпоративних правил до промптів, відповідей, моделей та інших взаємодій із ШІ.

Виявлення та блокування загроз

- **Протидія prompt injection і маніпуляціям:** Виявлення прямих і непрямих атак за понад 200 техніками, а також jailbreak і спроб маніпуляції моделями.
- **Виявлення шкідливої активності:** Пошук індикаторів загроз, ознак компрометації агентів та інших атак на основі даних про взаємодію з ШІ й активність кінцевих пристроїв.
- **Захист MCP-взаємодій:** Моніторинг MCP-комунікацій для виявлення шкідливої або несанкціонованої активності.

Розслідування та зупинення атак на ШІ

- **Відстеження впливу промптів:** Відновлення ланцюга подій від взаємодії з агентом до подальших дій у системі.
- **Ізоляція ШІ-агентів:** Автоматичне блокування небезпечних дій агентів та ізоляція скомпрометованих активів.
- **Журнали активності:** Збереження даних про роботу ШІ та спрацювання політик для розслідувань, безперервного моніторингу й контролю відповідності вимогам.

Побудовано на платформі Falcon

Falcon Guardian поширює перевірену архітектуру захисту CrowdStrike на рівень автономних ШІ-агентів. Глибока видимість кінцевих пристроїв дає змогу простежити зв'язок між промптом і діями агента та захищати ШІ під час роботи. Для цього не потрібен окремий стек безпеки: один сенсор, одна консоль і одна платформа.

Єдині операції захисту ШІ з Falcon Next-Gen SIEM

Телеметрія Falcon Guardian надходить безпосередньо до CrowdStrike Falcon® Next-Gen SIEM і не потребує додаткового опрацювання. Дані про активність ШІ можна зіставляти з інформацією про кінцеві пристрої, облікові записи, хмарні та SaaS-середовища. Це спрощує розслідування комплексних загроз і зменшує витрати на передавання даних до сторонніх SIEM.

Експертний захист Falcon Guardian

CrowdStrike Falcon® Complete for Guardian і CrowdStrike Falcon® Adversary OverWatch™ for Guardian доповнюють платформу керованим виявленням та реагуванням і проактивним пошуком загроз. Експерти CrowdStrike допомагають розслідувати й зупиняти атаки на ШІ-застосунки та автономних агентів.

Про iiTD

iiTD — офіційний Value Added дистриб'ютор рішень у сфері кібербезпеки та IT. Компанія працює за channel-first моделлю та реалізує комплексні проєкти через партнерську мережу.

www.iitd.ua
sales.ua@iitd.ua