Falcon Guardian

Безопасное внедрение ИИ с обнаружением угроз и реагированием на них в ИИ-средах.

ИИ-агенты меняют подход к выполнению рабочих задач, превращая искусственный интеллект из инструмента генерации контента в автономные системы, способные анализировать информацию, получать доступ к корпоративным ресурсам и выполнять действия. По мере их распространения организации не всегда знают, где работают ИИ-агенты, кто их использует, к каким ресурсам они имеют доступ и какие риски создают. При этом проблемы безопасности ИИ остаются актуальными. Сотрудники внедряют ИИ-инструменты быстрее, чем команды информационной безопасности успевают их выявлять, контролировать и защищать. Конфиденциальные данные передаются через неконтролируемые взаимодействия с теневым ИИ (Shadow AI), а разработчики создают ИИ-агентов и рабочие нагрузки, подверженные новым угрозам, включая инъекции промптов. Безопасное внедрение ИИ требует контроля его использования и защиты действий автономных агентов во время выполнения задач.

Защита ИИ в процессе работы

CrowdStrike Falcon® Guardian — флагманское AIDR-решение CrowdStrike для обнаружения угроз и реагирования на них в ИИ-средах. Решение обеспечивает единую видимость и контроль использования ИИ, защиту в процессе работы, расследование инцидентов и реагирование на угрозы.
Falcon Guardian обнаруживает ИИ-агентов, отслеживает их действия и связывает активность ИИ с процессами на конечных устройствах. Это позволяет проследить всю цепочку — от промпта до воздействия на систему, оценить масштаб инцидента и оперативно отреагировать на угрозы.
Falcon Guardian выявляет Shadow AI, защищает конфиденциальные данные и противодействует атакам на ИИ-системы.

Безопасное внедрение и разработка ИИ-агентов

ИИ меняет подход к работе сотрудников, выполнению задач автономными агентами и разработке собственных ИИ-решений. Falcon Guardian объединяет видимость, контроль, защиту данных и противодействие угрозам на конечных устройствах, в облачных средах и SaaS.

Безопасное использование ИИ сотрудниками

Обнаружение Shadow AI, применение детализированных политик доступа и защита конфиденциальных данных. Контроль автономных ИИ-агентов, работающих на конечных устройствах.

Безопасная разработка ИИ

Защита корпоративных ИИ-приложений, агентов и рабочих нагрузок в процессе работы. Falcon Guardian блокирует угрозы, предотвращает утечки данных и предоставляет информацию для расследования инцидентов и контроля соблюдения требований безопасности.

Ключевые преимущества

- **Обнаружение Shadow AI**
Непрерывная видимость разрешённых и неизвестных ИИ-агентов, сред их выполнения, ответственных за развёртывание и областей наибольшего риска.

- **Контроль соблюдения политик ИИ**
Применение технических механизмов контроля для обеспечения соблюдения политик использования ИИ, управления разрешёнными сценариями и защиты конфиденциальных данных от непреднамеренных утечек.

- **Защита ИИ-агентов в процессе работы**
Блокирование атак типа Prompt Injection и других угроз, направленных на сторонних ИИ-агентов, установленных на конечных устройствах, и корпоративных ИИ-агентов, развёрнутых в облаке.

- **Ускоренное расследование и локализация угроз**
Выявление специфических для ИИ угроз, восстановление последовательности действий агента, оценка масштаба инцидента и оперативное реагирование для предотвращения распространения угроз на другие системы.

Ключевые возможности

Обнаружение ИИ и оценка рисков

- **Обнаружение Shadow AI и ИИ-агентов:** Мониторинг использования ИИ в поддерживаемых средах и непрерывное выявление известных и ранее неизвестных ИИ-агентов.
- **Оценка рисков на конечных устройствах:** Информация о том, где работают агенты, кто их использует, насколько они защищены и какие действия требуют внимания.
- **Анализ взаимосвязей:** Объединение данных о пользователях, учётных записях, моделях, агентах, инструментах и конечных устройствах для оценки активности и рисков.

Управление использованием ИИ и контроль доступа

- **Детализированные политики безопасности:** Применение контекстных правил к пользователям, агентам, моделям и взаимодействиям с ИИ.
- **Контроль агентов на конечных устройствах:** Разрешение работы утверждённых типов агентов и блокирование несанкционированных.
- **Защита конфиденциальных данных:** Выявление и блокирование передачи конфиденциальной информации, персональных данных, учётных данных, секретов и исходного кода.

Защита корпоративных ИИ-решений

- **Защита в процессе работы:** Обнаружение и блокирование угроз для корпоративных ИИ-приложений, агентов и рабочих нагрузок.
- **Интеграция с процессом разработки:** Подключение Falcon Guardian через SDK, облачные интеграции, ИИ-шлюзы или MCP-прокси.
- **Контроль соблюдения политик:** Защита данных и применение корпоративных правил к промптам, ответам, моделям и другим взаимодействиям с ИИ.

Обнаружение и блокирование угроз

- **Защита от Prompt Injection и манипуляций:** Обнаружение прямых и косвенных атак с использованием более 200 техник, а также попыток обхода ограничений и манипулирования моделями.
- **Выявление вредоносной активности:** Обнаружение индикаторов угроз, признаков компрометации агентов и других атак на основе данных о взаимодействиях с ИИ и активности конечных устройств.
- **Защита MCP-взаимодействий:** Мониторинг MCP-коммуникаций для выявления вредоносной или несанкционированной активности.

Расследование и предотвращение атак на ИИ

- **Отслеживание последствий промптов:** Восстановление цепочки событий от взаимодействия с агентом до последующих действий в системе.
- **Изоляция ИИ-агентов:** Автоматическое блокирование опасных действий агентов и изоляция скомпрометированных активов.
- **Журналы активности:** Сохранение данных о работе ИИ и срабатывании политик для расследования инцидентов, непрерывного мониторинга и контроля соблюдения требований.

На базе платформы Falcon

Falcon Guardian расширяет проверенную архитектуру защиты CrowdStrike на уровень автономных ИИ-агентов. Глубокая видимость конечных устройств позволяет проследить связь между промптом и действиями агента, обеспечивая защиту ИИ в процессе работы. При этом не требуется отдельная инфраструктура безопасности: один сенсор, одна консоль и одна платформа.

Единое управление безопасностью ИИ с Falcon Next-Gen SIEM

Телеметрия Falcon Guardian поступает непосредственно в CrowdStrike Falcon® Next-Gen SIEM без дополнительной обработки. Данные об активности ИИ можно сопоставлять с информацией о конечных устройствах, учётных записях, облачных и SaaS-средах. Это упрощает расследование сложных угроз и снижает затраты на передачу данных в сторонние SIEM-системы.

Экспертная защита Falcon Guardian

CrowdStrike Falcon® Complete for Guardian и CrowdStrike Falcon® Adversary OverWatch™ for Guardian дополняют платформу услугами управляемого обнаружения и реагирования на угрозы, а также проактивного поиска угроз. Эксперты CrowdStrike помогают расследовать и останавливать атаки на ИИ-приложения и автономных агентов.

Об iiTD

iiTD — официальный Value Added дистрибьютор решений в сфере кибербезопасности и ИТ. Компания работает по модели channel-first и реализует комплексные проекты через партнерскую сеть.

Для получения дополнительной информации, пожалуйста, свяжитесь с нами:

sales.kz@iit-d.kz | www.iit-d.kz sales@iitd.uz | www.iitd.uz