ASBIS®
SUCCESS THROUGH FOCUS

AI и ML в IT и ИБ

Ухов Денис, PLSM

Что такое AI?

AI (Искусственный Интеллект) — область компьютерных наук, направленная на создание систем, способных выполнять задачи, требующие человеческого интеллекта.

Что такое ML?

ML (Машинное Обучение) — подраздел искусственного интеллекта, фокусирующийся на разработке алгоритмов, которые могут учиться и делать прогнозы или решения на основе данных.

Преимущества AI и ML

Автоматизация рутинных задач: анализ логов, мониторинг событий безопасности

Преимущества AI и ML

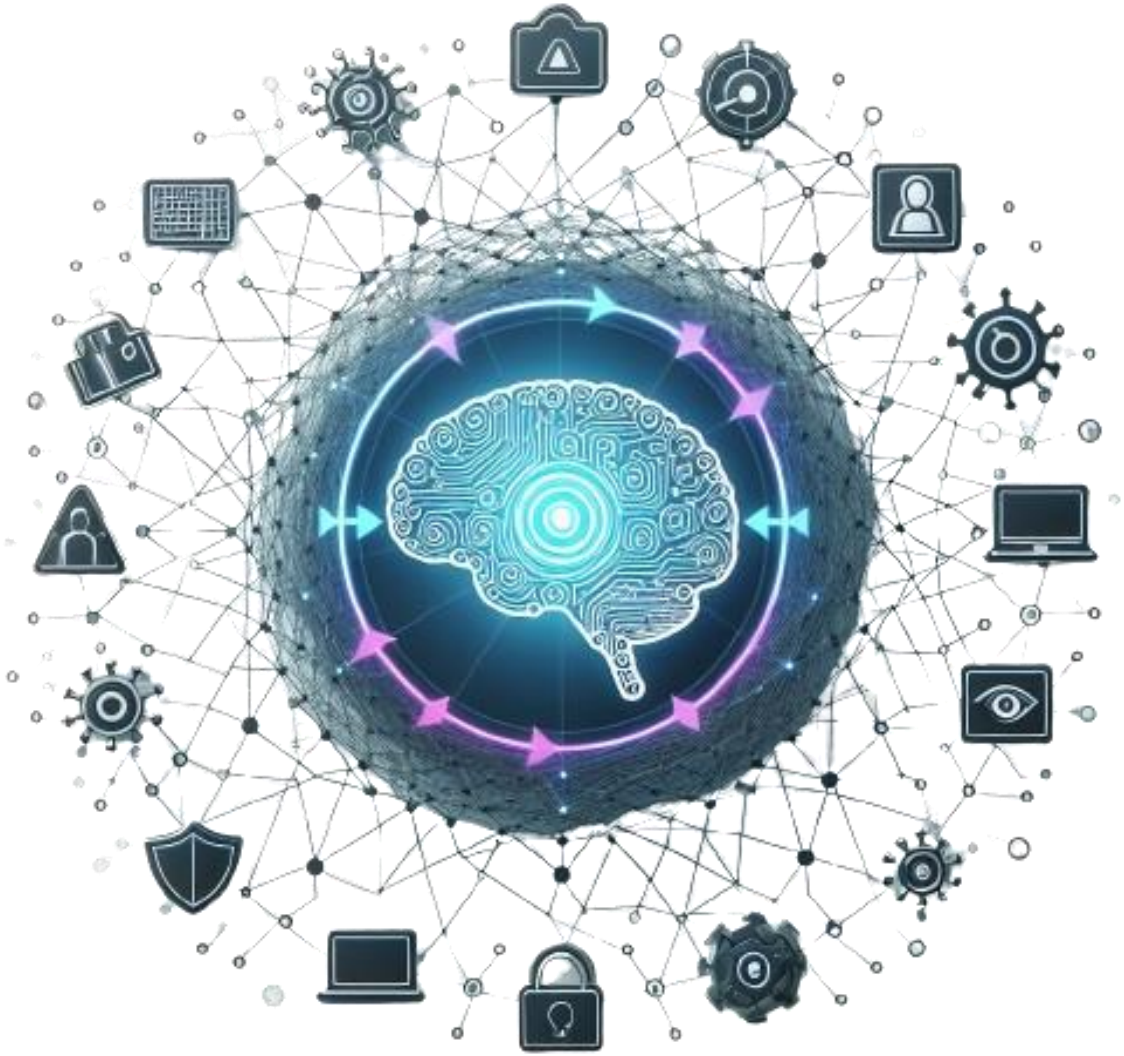
Масштабируемость: способность анализировать огромные объемы данных

Преимущества AI и ML

Выявление аномалий и отклонений в сетевом трафике, поведении пользователей

Преимущества AI и ML

Непрерывное самообучение и адаптация к новым киберугрозам



Преимущества AI и ML

Повышение эффективности аналитиков кибербезопасности

Немного статистики

- Ожидается, что мировой рынок ИИ в сфере кибербезопасности достигнет **38,2 миллиарда долларов** к **2025** году и **60,6 миллиарда долларов** к **2028** году при **темпах роста в 21,9%.**
- **45% организаций уже внедрили** ИИ/МЛ в свои системы кибербезопасности, а еще **35% планируют это сделать.**
- **88% профессионалов** в области кибербезопасности считают, что **искусственный интеллект необходим** для более эффективного выполнения задач
- **44% организаций** сообщили об **успешности использования** инструментов кибербезопасности на основе искусственного интеллекта

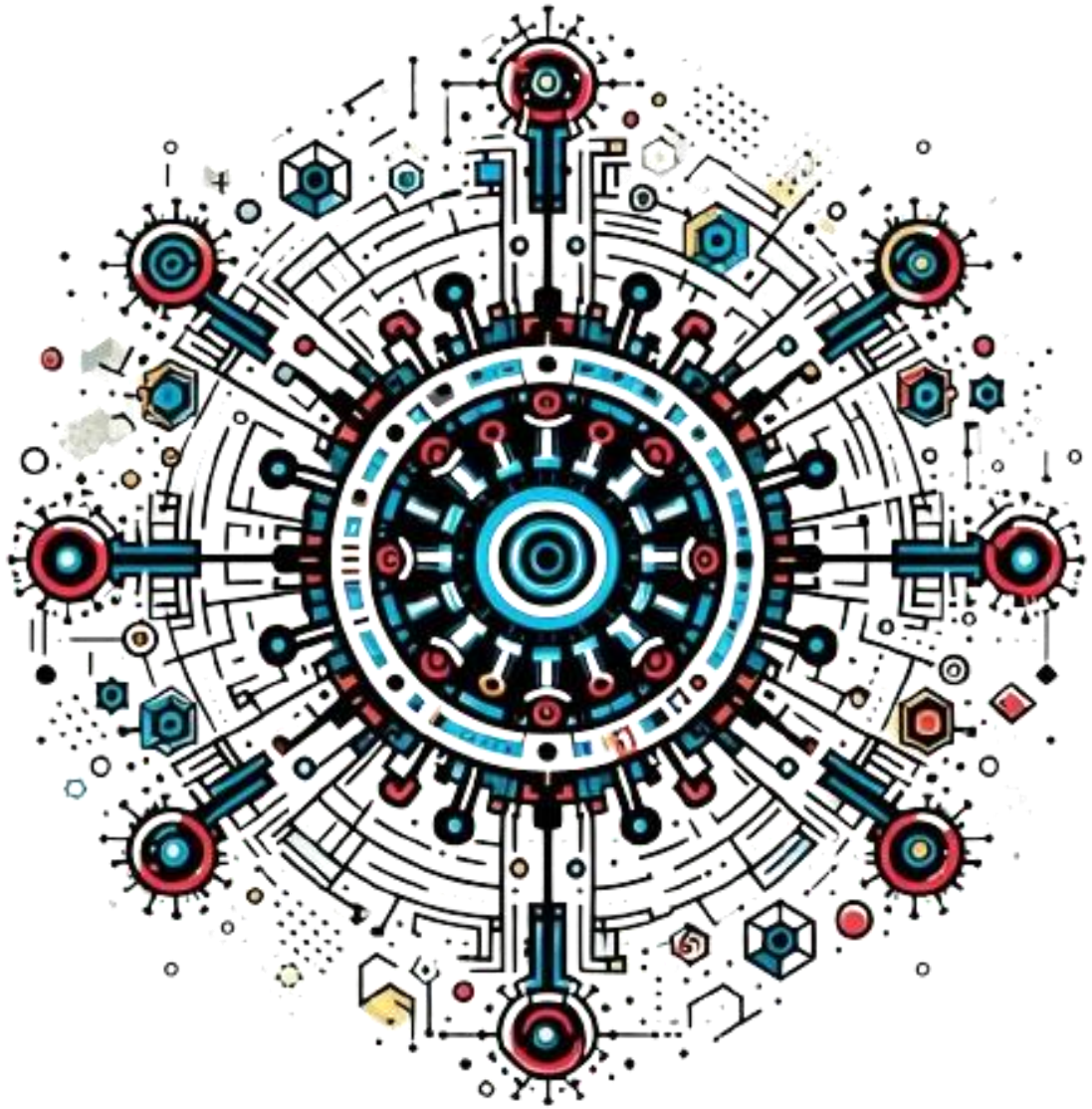
Что с другой стороны?

Автоматизация спам-атак, фишинга, DDoS атак

Что с другой стороны?

Изощренные методы социальной инженерии и вывода из строя систем

Что с другой стороны?



Обход систем обнаружения генерациями новых вариаций вредоносного ПО

Что с другой стороны?

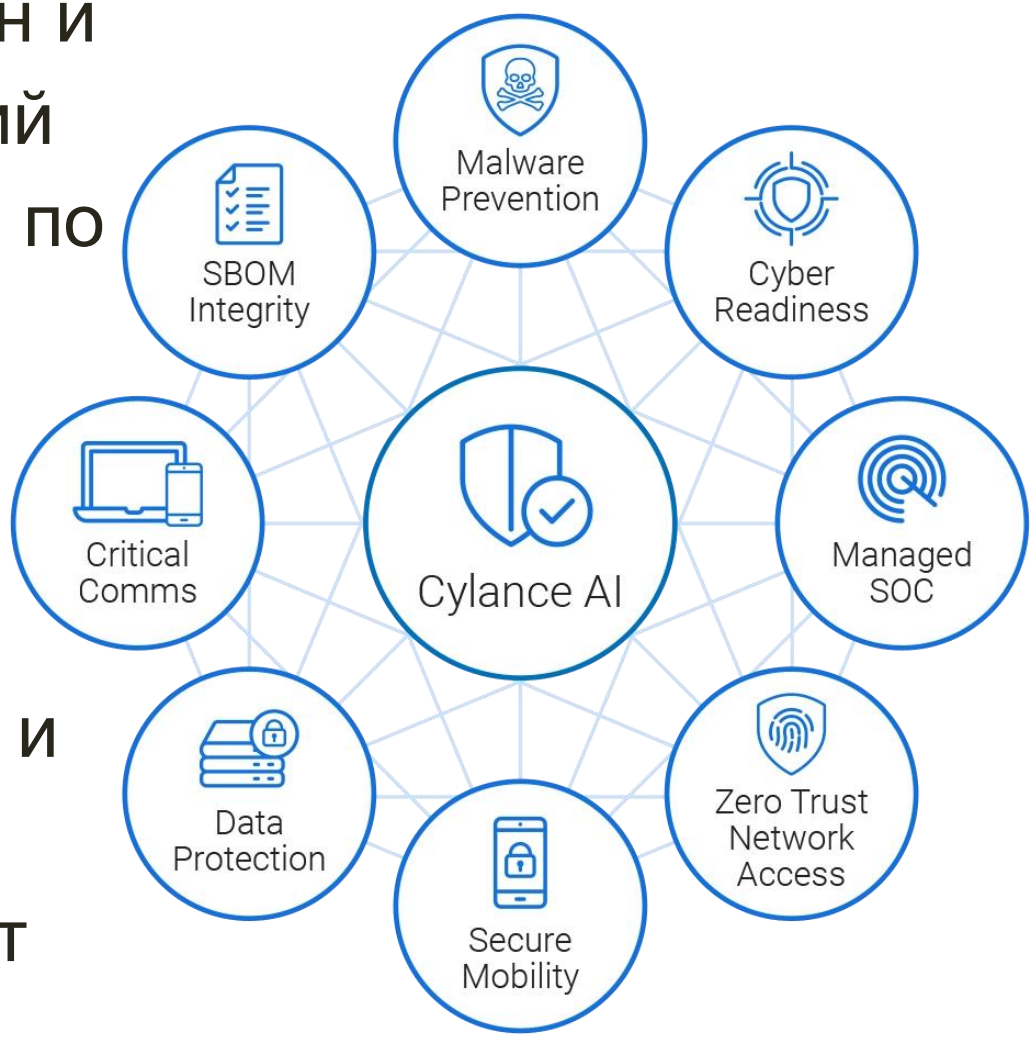
Оперативный
анализ
уязвимостей
и потенциальных
целей атак

CylanceAI от BlackBerry

- 98,9 процента обнаружения на онлайн и офлайн устройствах и лучший средний показатель блокировки 36,8 процента по сравнению с конкурентами.

- Легковесный агент, около 6% CPU.

- Сокращение времени расследования и восстановления после инцидентов безопасности на 30 %, а "усталости от оповещений" - на 90 %.



ThunderTPS от A10

- Zero-Day Attack Pattern Recognition (ZAPR) - динамическое распознавание шаблонов атак с помощью алгоритма машинного обучения и блокировка генерации сигнатур.
- Zero-Day Behavior Anomaly Recognition (ZBAR) - эвристический анализ поведения для динамического выявления аномального поведения и блокирования атакующих агентов.
- Реактивный режим, проактивный режим, Out-of-Band / TAP.

AirThink AI от Scalefusion

- Генерация скриптов: Powershell, Shell, Bash, Python
- Валидация имеющихся скриптов
- Инсайты инвентаризации
- Рекомендации по решению проблем с устройствами

AIOps в OpsB от opentext™

- Предотвращение проблем до того, как они затронут клиентов, благодаря обнаружению аномалий.
- Точное определение проблемы или сокращение числа элементов, на которые операторы должны обратить внимание.
- Более точная корреляция между изменениями и производительностью.
- Ускоренное среднее время обнаружения проблем (MTTD) и устранения проблем (MTTR).

ASBIS®
SUCCESS THROUGH FOCUS

Спасибо за внимание!

Denis Uhov
Product Line Sales Manager

Phone: +7 727 390 46 06
Mobile: +7 705 912 94 07
E-mail: Denis.Uhov@asbis.kz