FURTINET

Модернизируйте операции SOC при помощи решения Virtual Security Analyst на базе ИИ

Технология искусственного интеллекта (ИИ) способна выявлять закономерности, анализируя огромные объемы данных. За счет этого она обнаруживает тенденции и классифицирует угрозы значительно быстрее специалистов-людей. Виртуальный аналитик центра операций безопасности (SOC) на базе ИИ, использующий технологии глубокого обучения, к примеру глубинные нейросети, может компенсировать нехватку квалифицированных кадров, а также ускорить выявление инцидентов безопасности и реагирование на них.

74% специалистов по безопасности утверждают, что нехватка квалифицированных кадров отрицательно сказалась на их организации.[1]

Эту проблему можно решить при помощи виртуального аналитика SOC на базе глубинных нейросетей, который обеспечивает выполнение рутинных задач и оказывает поддержку специалистам, которые могут заняться более сложными вопросами.

Эффективная система ИИ должна обладать определенными характеристиками.

Средство Virtual Security Analyst на базе ИИ должно быть самообучающимся

Говоря о широко используемых алгоритмах **машинного обучения**, решение Virtual Security Analyst на базе глубинных нейросетей, способное работать в неуправляемом режиме без предварительного обучения в локальной среде и адаптироваться к быстрому усложнению угроз, послужит большим подспорьем малочисленным отделам SOC.

Машинное обучение		Глубокое обучение
Управляемое	**Модель обучения**	Неконтролируемое
Управляемый поставщиком домен	**Размещение ИИ**	В любом месте, в том числе в локальной среде клиента
Требует облачных обновлений	**Развитость ИИ (Непрерывное обучение)**	Самообучение. Возможно потребление данных глобальной сети
Недели	**Обучение в локальной среде**	Работоспособность с первого дня благодаря предварительному обучению

Технология ИИ должна взаимодействовать с персоналом организации, процессами и технологиями

Подобное взаимодействие улучшает масштабируемость групп сотрудников, автоматизирует рутинные задачи и обеспечивает своевременную защиту от изощренных угроз.

Адаптация ИИ для масштабирования SOC и решения проблемы нехватки кадров

Использование ИИ для своевременного выполнения трудоемких процедур выявления, анализа и реагирования на угрозы

Применение ИИ в целях повышения эффективности и оперативности обнаружения изощренных угроз

Скорость машины ИИ должна способствовать ускоренному выявлению, анализу и реагированию на угрозы

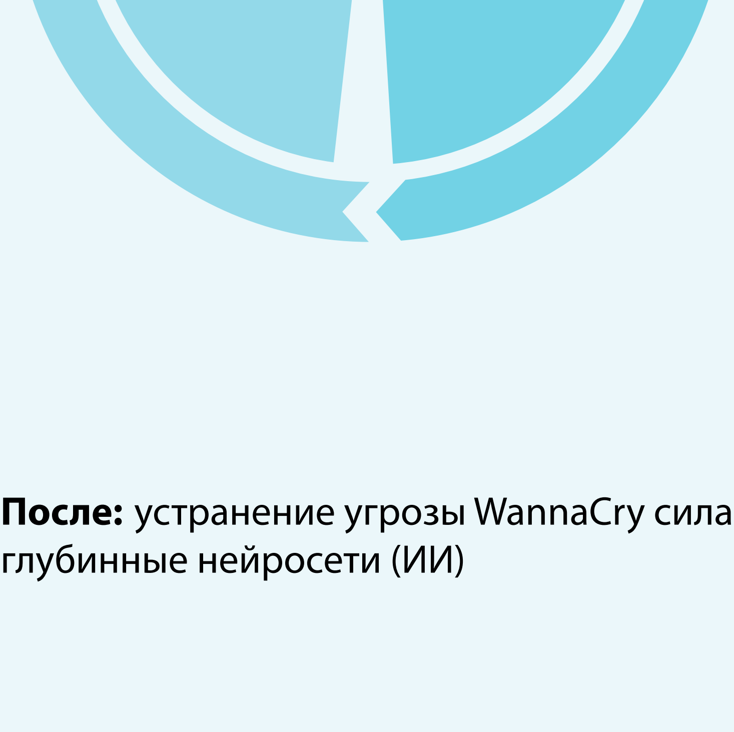
В среднем центр SOC ежедневно получает **10 000 оповещений**, однако численности персонала и количества ресурсов хватает на обработку лишь части оповещений.[2] Две трети специалистов по безопасности успевают исследовать менее 30 оповещений в день,[3] при этом половина из них с большой вероятностью оказывается ложной.[4]

Решение Virtual Security Analyst на базе ИИ способно ускорить выявление и классификацию потенциальных атак, принятие необходимых мер по анализу и идентификации источника угрозы и пораженных машин, а также реализацию плана устранения.

Это значительно снижает нагрузку на отдел безопасности и сокращает расходы на устранение инцидентов.

Пример жизненного цикла реагирования на угрозу

До: традиционный подход к устранению угрозы WannaCry только при участии аналитиков SecOps

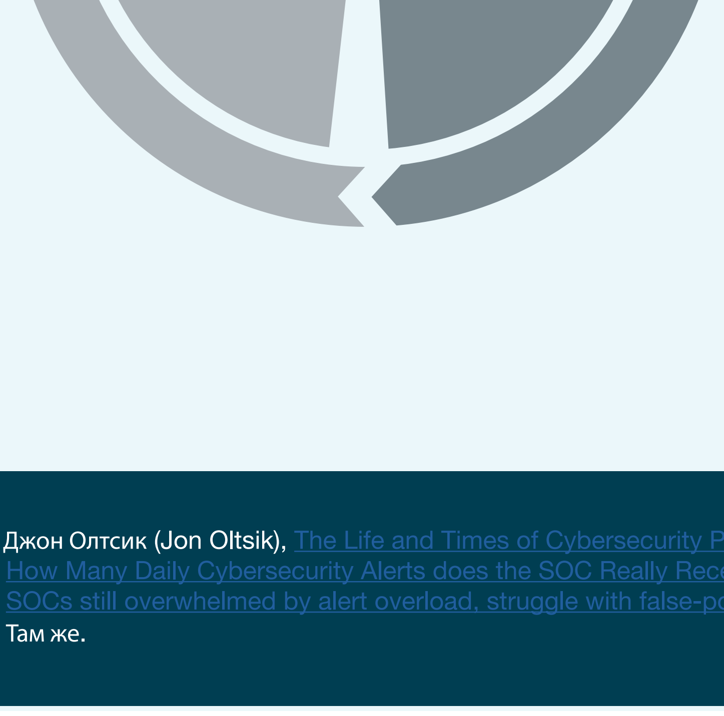


Выявление (более 1 часа)
- Допустим, что из 100–1000 оповещений об угрозах на панели мониторинга SOC выбрана программа вымогатель, либо
- Пострадавший пользователь напрямую сообщил об угрозе

Анализ (более 4 часов)
- Вход в продукты безопасности
- Анализ журналов/оповещений
- Обнаружение программ-вымогателей при помощи внешних и встроенных инструментов
- Выполнение внешних исследований
- Вход в продукты безопасности для отслеживания внутренних перемещений WannaCry
- Разработка плана по устранению угрозы

Реагирование (более 2 часов)
- Помещение устройств на карантин, сетевой сегмент
- Устранение угроз на устройствах/восстановление при помощи резервной копии
- Исправление уязвимостей
- Закрытие заявки

После: устранение угрозы WannaCry силами аналитиков SecOps, использующих глубинные нейросети (ИИ)



Выявление (менее 1 с)
- ИИ: обнаружение программ-вымогателей за доли секунды
- ИИ: самообучение новым особенностям программ-вымогателей

Анализ (менее 5 мин)
- ИИ: определение цепочки внедрения WannaCry при помощи контекстного исследования угроз
- ИИ: выявление первого объекта поражения WannaCry и внутренних перемещений угрозы
- SecOps: разработка плана по устранению угрозы

Реагирование (менее 30 мин)
- Технология ИИ, интегрированная с элементами управления безопасностью:
  - Помещение устройств на карантин, сетевой сегмент
- Дальнейшие действия SecOps:
  - Устранение угроз на устройствах/восстановление при помощи резервной копии
  - Исправление уязвимостей
- Закрытие заявки

---

[1] Джон Олтсик (Jon Oltsik), The Life and Times of Cybersecurity Professionals 2018, ESG & ISSA, апрель 2019 г.
[2] How Many Daily Cybersecurity Alerts does the SOC Really Receive?, Bricata, 2 октября 2019 г.
[3] SOCs still overwhelmed by alert overload, struggle with false-positives, Help Net Security, 29 августа 2019 г.
[4] Там же.

Узнайте больше о FortiAI

Ознакомьтесь с обзором решения FortiAI