Как ИИ формирует гонку вооружений в области кибербезопасности

Средний бизнес получает 10 000 оповещений каждый день от различных программных средств, которые он использует для мониторинга злоумышленников, вредоносных программ и других угроз. Сотрудники службы кибербезопасности часто оказываются завалены данными, которые им необходимо отсортировать, чтобы управлять своей киберзащитой.

Ставки высоки. Кибератаки растут и влияют тысячи организаций и миллионы людей только в США.

Эти проблемы подчеркивают необходимость более эффективных способов остановить волну кибератак. Искусственный интеллект особенно хорошо подходит для поиска закономерностей в огромных объемах данных. Как исследователь, который исследования ИИ и кибербезопасности Я считаю, что ИИ становится крайне необходимым инструментом в инструментарии кибербезопасности.

Помощь людям

Есть два основных способа, с помощью которых ИИ укрепляет кибербезопасность. Во-первых, ИИ может помочь автоматизировать многие задачи, с которыми человек-аналитик часто справлялся бы вручную. К ним относятся автоматическое обнаружение неизвестных рабочих станций, серверов, хранилищ кода и другого оборудования и программного обеспечения в сети. Он также может определить, как наилучшим образом распределить средства защиты. Это задачи, требующие больших объемов данных, и ИИ обладает потенциалом для обработки терабайт данных гораздо эффективнее и эффективнее, чем это когда-либо мог сделать человек.

Во-вторых, ИИ может помочь обнаружить закономерности в больших объемах данных, которые не могут видеть аналитики-люди. Например, ИИ может обнаруживать ключевые лингвистические шаблоны хакеров, публикующих новые угрозы в темная паутина и предупредите аналитиков.

В частности, аналитика с поддержкой ИИ может помочь распознать жаргон и кодовые слова, которые хакеры используют для обозначения своих новых инструментов, методов и процедур. Одним из примеров является использование имени Mirai для обозначения ботнета. Хакеры разработали этот термин, чтобы скрыть тему ботнета от правоохранительных органов и специалистов по киберугрозам.

ИИ уже добился некоторых первых успехов в области кибербезопасности. Все чаще такие компании, как FireEye, Microsoft и Google, разрабатывают инновационные подходы ИИ для обнаружения вредоносных программ, противодействия фишинговым кампаниям и мониторинга распространения дезинформации. Одним из заметных успехов является Киберсигналы Microsoft программа, которая использует ИИ для анализа 24 триллионов сигналов безопасности, 40 национальных государственных групп и 140 хакерских групп для получения информации о киберугрозах для руководителей высшего звена.

Федеральные финансирующие агентства, такие как Министерство обороны и Национальный научный фонд, признают потенциал ИИ для обеспечения кибербезопасности и инвестировали десятки миллионов долларов в разработку передовых инструментов ИИ для извлечения информации из данных, полученных из темной сети, и программных платформ с открытым исходным кодом, таких как GitHub глобальное хранилище кода для разработки программного обеспечения, где хакеры тоже могут делиться кодом.

Недостатки ИИ

Несмотря на значительные преимущества ИИ для кибербезопасности, у специалистов по кибербезопасности есть вопросы и опасения по поводу роли ИИ. Компании могут подумать о замене своих человеческих аналитиков системами ИИ, но могут быть обеспокоены тем, насколько они могут доверять автоматизированным системам. Также неясно, является ли и как хорошо документированный ИИ проблемы предвзятости, справедливости, прозрачности и этики появится в системах кибербезопасности на основе ИИ.

Кроме того, ИИ полезен не только специалистам по кибербезопасности, пытающимся переломить ситуацию в борьбе с кибератаками, но и злоумышленникам. Хакеры. Злоумышленники используют такие методы, как обучение с подкреплением и порождающие состязательные сети, которые генерируют новый контент или программное обеспечение на основе ограниченных примеров, для создания новых типов кибератак, которые могут обойти киберзащиту.

Исследователи и специалисты по кибербезопасности все еще изучают все способы использования ИИ злоумышленниками.

Предстоящий путь

Заглядывая в будущее, можно сказать, что у ИИ есть значительные возможности для роста в области кибербезопасности. В частности, прогнозы, которые системы ИИ делают на основе выявленных ими закономерностей, помогут аналитикам реагировать на возникающие угрозы. ИИ - это интригующий инструмент, который может помочь остановить волну кибератак и, при тщательном совершенствовании, может стать необходимым инструментом для следующего поколения специалистов по кибербезопасности.

Однако нынешние темпы инноваций в ИИ указывают на то, что полностью автоматизированные кибернетические сражения между атакующими ИИ и защитниками ИИ, вероятно, пройдут годы.