kaspersky

ИИ для SOC: эффективность без выгорания

Как ИИ трансформирует работу SOC

kaspersky.ru

SANS Institute комментирует по этому поводу:

«Мы видим, что компаниям приходится постоянно искать новых сотрудников, а потом пытаться их удержать, поскольку многие аналитики SOC не выдерживают нагрузки и решают сменить работу или даже сферу деятельности»

Выгорание специалистов SOC становится одной из главных угроз кибербезопасности

При этом Osterman Research в своём отчёте за 2024 год сообщает, что центрам мониторинга и реагирования (SOC) ежедневно приходится проверять всё больше оповещений — 97% организаций отметили, что их число растёт из года в год.

Выгорание специалистов SOC становится одной из главных угроз кибербезопасности. Но, к счастью, есть решение. Технологии на базе искусственного интеллекта автоматизируют выполнение рутинных задач, отсеивают ложные срабатывания и выполняют другие функции, снижая риски выгорания и повышая общую эффективность SOC.

Причины выгорания аналитиков SOC

С ростом количества оповещений растет и нагрузка на аналитиков. Они просто не успевают все классифицировать и проверять, и в результате очередь необработанных оповещений растет, а инциденты остаются незамеченными. В отчете говорится, что постоянное накопление нерешенных задач безопасности становится проблемой для 89,6% компаний, и чем интенсивнее поток оповещений, тем больше стресса испытывают специалисты SOC. Ресурсов хватает в среднем на обработку лишь 19% оповещений, и незавершенная работа превращается для аналитиков в порочный круг.

Неудивительно, что SANS Institute приходит к следующему выводу:

«Постоянная текучесть персонала в сфере ИБ приводит к серьезным проблемам, которые касаются не только ИБ-специалистов. Высокий уровень текучести неизменно приводит к нарушению рабочих процессов в SOC. В результате эффективность SOC снижается, и компания сталкивается с повышенными рисками безопасности. Если SOC не сможет удержать процессы на должном уровне, киберпреступники обязательно воспользуются появившейся лазейкой. Кажется, что из этого круга не вырваться. Но мы должны. Мы обязаны это сделать».

Возникает закономерный вопрос: что реально можно сделать для решения этой проблемы?

Владислав Тушканов

Руководитель группы исследования технологий машинного обучения

Снижение риска выгорания и повышение эффективности SOC

«Самый очевидный способ снизить риск выгорания специалистов SOC — это снижение нагрузки на них за счет автоматизации рутинной работы, например классификации и проверки оповещений.

Большое количество аналитиков тратят слишком много времени на решение повторяющихся задач, которые можно без труда автоматизировать. Скука тоже может стать причиной выгорания: утонув в рутинных процессах, специалисты не уделяют должного внимания более важным задачам, оставляя организацию уязвимой».

С этим мнением солидарны и эксперты компании KPMG:

«ИИ — эффективный инструмент для автоматизации множества задач, которые сейчас приходится выполнять вручную. Он высвобождает время специалистов, повышая их продуктивность. Алгоритмы машинного обучения находят закономерности и выявляют аномалии гораздо быстрее, чем люди. Таким образом повышается коэффициент обнаружения вредоносной активности и угроз для сетевой инфраструктуры и конфиденциальных данных предприятия. ИИ повышает эффективность реагирования на угрозы, сводя к минимуму прерывание бизнес-операций, и защищает активы компании от злоумышленников, которые охотятся за конфиденциальной информацией, например за номерами банковских карт или личных документов».

Многие SOC пытаются снизить нагрузку на аналитиков с помощью машинного обучения: эта технология выводит автоматизацию на новый уровень, отсеивая ложные срабатывания из массы оповещений и повышая эффективность их классификации.

Эффективный способ добиться этого — внедрение AI-«автоаналитика»: контролируемой модели машинного обучения, которая обучается на алертах, уже обработанных командой SOC, а затем самостоятельно воспроизводит их логику принятия решений. Она обрабатывает часто появляющиеся, типичные оповещения, высвобождая человеческие ресурсы. В результате специалистам SOC приходится проверять меньше оповещений, и они могут сосредоточиться на более интересных задачах, требующих внимания человека.

Чем может помочь «Лаборатория Касперского»

«Лаборатория Касперского» активно внедряет технологии искусственного интеллекта и машинного обучения в свои решения, а один из пяти экспертных центров компании — Kaspersky AI Technology Research — непрерывно совершенствует их.

Центр экспертизы Kaspersky AI Technology Research занимается разработкой решений и инструментов на базе ИИ для обнаружения угроз и других задач, а также исследованиями в области кибербезопасности и генеративного ИИ.

У нас широкий пул задач: мы применяем методы Data Science и алгоритмы ИИ для выявления киберугроз, таких как вредоносное ПО, спам, фишинг и целевые атаки. Кроме того, мы занимаемся оценкой рисков с использованием ИИ, которая позволяет выявлять подозрительное поведение хостов на основе корреляции данных в таких продуктах, как XDR и SIEM.

Разработка идет по нескольким направлениям. Мы активно внедряем генеративный ИИ, в частности большие языковые модели, в системы безопасности; работаем над инструментами поведенческого анализа и обнаружения аномалий на базе ИИ для информационно-промышленных сред; разрабатываем безопасные решения, методологии и подходы к использованию ИИ, которые помогут нашим партнерам и клиентам решать актуальные проблемы.

Владислав Тушканов

Руководитель группы исследования технологий машинного обучения

О «Лаборатории Касперского»

«Лаборатория Касперского» — международная компания, работающая в сфере информационной безопасности и защиты конфиденциальности данных с 1997 года.

Наши технологии обеспечивают защиту самых важных аспектов бизнеса более 200 тысяч корпоративных клиентов.

Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты рабочих мест, а также ряд специализированных решений и сервисов для борьбы с комплексными и постоянно эволюционирующими киберугрозами, в том числе кибериммунные системы.

Глубокие экспертные знания и многолетний опыт компании лежат в основе защитных решений и сервисов нового поколения, которые обеспечивают безопасность бизнеса, критически важных инфраструктур, государственных учреждений и рядовых пользователей, защищая более миллиарда устройств от новейших угроз и целевых атак.

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее