ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056.5, 004.89

ИССЛЕДОВАНИЕ АДАПТИВНЫХ ПРАВИЛ БЕЗОПАСНОСТИ НА ОСНОВЕ ИИ ДЛЯ ОПЕРАТИВНОГО РЕАГИРОВАНИЯ НА КИБЕРУГРОЗЫ

Петров Никита Эдуардович,
Студент магистратуры, 2 курс, 10.04.01 «Информационная безопасность», МИРЭА - Российский технологический университет (РТУ МИРЭА), г. Москва
neket20021@mail

Аннотация

В работе рассматриваются основные аспекты адаптивного подхода: использовании алгоритмов искусственного интеллекта (ИИ) для формирования динамических правил блокировки и временных TSR-правил. В целях проверки возможностей защиты было выполнено практическое исследование на экспериментальном стенде PNETLab с использованием Suricata, Snort и AI-IPS. На основе анализа результатов систем выявлены различия между классическими IPS и адаптивным модулем IPS – AI-IPS.

Ключевые слова: атаки, Suricata, Snort, AI, IPS, IDS, временные правила.

RESEARCH OF AI-BASED ADAPTIVE SECURITY RULES FOR RAPID RESPONSE TO CYBER THREATS

Petrov Nikita Eduardovich,
Master's student, 2st year
MIREA - Russian Technological University (RTU MIREA), Moscow

ABSTRACT

The paper discusses the main aspects of the adaptive approach: the use of artificial intelligence (AI) algorithms to generate dynamic blocking rules and temporary TSR rules. In order to test the protection capabilities, a practical study was performed on the PNETLab experimental stand using Suricata, Snort, and AI-IPS. Based on the analysis of the system results, the differences between classic IPS and the adaptive IPS module, AI-IPS, were identified.

Keywords: attacks, Suricata, Snort, AI, IPS, IDS, temporary rules.

Современные киберугрозы обладают высокой степенью вариативности, используют нестандартные векторы атаки, подмену протоколов, полиморфизм и тактики обхода традиционных средств защиты.[1] Особенно критично это для промышленных систем

(ICS/SCADA), где атаки на Modbus, Siemens S7, ARP-спуфинг и MITM способны вызвать изменение технологических параметров, аварии или вывод оборудования из строя.

Классические IDS/IPS-системы – Suricata, Snort – опираются на статические сигнатуры, что хорошо работает против известных угроз. [3] Однако они плохо выявляют новые атаки, требуют регулярного обновления правил и часто дают ложные срабатывания при интенсивном трафике. [2]

Использование методов искусственного интеллекта позволяет перейти от реактивного реагирования (по известным IOC) к проактивному [4], выявляя отклонения от нормального поведения без необходимости заранее знать сигнатуру угрозы.

Обзор традиционных методов обнаружения и предотвращения вторжений:

1. Сигнатурный анализ является основным механизмом работы классических IDS/IPS (Suricata, Snort). Принцип сигнатурного анализа заключается в следующем: поступает сетевой пакет, выполняется поиск совпадений по базе правил, при наличии совпадений генерируется предупреждение или блокировка.

Преимущества:

- высокая точность при известных угрозах;
- минимальный процент ложных срабатываний.

Недостатки:

- невозможность обнаружения новых атак;
- привязка к частоте обновления правил ET Open, SSLBL и др.;
- чувствительность к обфускации и нестандартной нагрузке.

2. Эвристический и поведенческий анализ анализируют: частоту запросов, аномалии в последовательности команд, отклонения в структуре протоколов.

Хотя это и помогает частично компенсировать недостатки сигнатурного подхода, системы по-прежнему основываются на заранее заданных правилах и не способны адаптироваться.

3. Суть адаптивного подхода на основе ИИ заключается в том, что в отличие от статической IPS, ИИ-подход строит модель нормального поведения:

- сбор «чистого» трафика;
- обучение модели на нормальном трафике;
- запуск мониторинга;
- все отклонения считаются потенциально вредоносными.

После выявления аномалий ИИ автоматически генерирует AI-IPS временные правила, которые:

- не полностью останавливают систему;
- дают аналитикам время проверить инцидент;
- минимизируют простои при блокировке.
- Преимущества адаптивных правил:
- обнаружение неизвестных атак;
- устойчивость к модификациям нагрузки;
- минимизация ручного сопровождения;

– автоматическая реакция в реальном времени.

Ограничение: ИИ не гарантирует детерминированности, поэтому требуется TSR-подход и гибридные методы.

Для проведения практического исследования был использован экспериментальный стенд следующей конфигурации:

1. PLC – контроллер;
2. HMI – человеко-машинный интерфейс;
3. Attacker – злоумышленник;
4. AI-IPS – маршрутизатор + IPS;
5. Net0 – внешний доступ при необходимости.

В целях получения результатов защиты анализируемых IPS были проведены три атаки: Modbus Write (злоумышленник сканирует сеть на порт 502, затем запускает скрипт, отправляющий Modbus write в PLC, меняя уставки); ARP-spoofing MITM (злоумышленник запускает ARP-спуфинг HMI и PLC, становится посредником, подменяет ответы Modbus/S7); S7 неавторизованная запись (скрипт посылает команды на запись или большие пакеты загрузки).

Для IDS/IPS Suricata первым этапом была проведена проверка возможности обмена пакетами PLC и HMI. Следующим шагом проведены атаки, по завершению которых были получены следующие результаты:

– нормальный трафик между PLC и HMI проходит;
– атака Modbus частично проходит;
– S7 успешно блокируется;
– ARP-spoofing проходит.

По аналогичному методу были проведены атаки на IDS/IPS Snort/pfSense. Ниже представлены итоги реализованных атак:

1. Modbus – частичное срабатывание (2 из 5 регистров изменены);
2. ARP-spoofing – атакующий не увидел трафика;
3. S7 – полная блокировка.

Для обучения модели AI-IPS был собран трафик взаимодействия сетевых устройств без проведения атаки. Первоначально в AI-IPS нет блокировок трафика. Подобно двум предыдущим экспериментам была проверена корректность настройки путём анализа трафика PLC и HMI. Были запущены три атаки, которые успешно были нейтрализованы. Можно отметить, что нормальный трафик проходит стабильно, модель не дает ложных срабатываний, временные правила остаются пустыми до появления угроз.

	Без защиты	Suricata	Snort	AI
Modbus	+	+/-	+/-	-
Arp-spoofing	+	+	-	-
S7	+	-	-	-

Исходя из результатов практического исследования можно сделать следующие выводы:

– традиционные IPS эффективны лишь против известных угроз;

- Suricata и Snort частично пропускают предоставленные атаки;
- AI-IPS блокирует все атаки и действует без явно заданных сигнатур;
- TSR-подход блокирует не весь трафик.

Таким образом, AI не обладает способностью всегда выдавать при одинаковых входных данных одинаковый результат, как и весь ИИ, что критично в кибербезопасности. [5] На выход приходят статические правила в IPS, куда мы заносим конкретно какие IoC надо блокировать. Всё меняется, когда идёт речь о новых угрозах, на которые не успели появиться IoC – тут AI находится в выигрыше. Но для того, чтобы минимизировать цену ошибки, в случае легитимного трафика, вводится понятие TSR (временное правило), которое позволяет дать дополнительное время на анализ администраторам безопасности, не пропустить атаку, но не сильно тормозить процессы. Лучшим решением будет комбинированный метод, когда статические правила IPS используются с временными правилами.

Список литературы:

1. Козлова Н. Ш., Довгаль В. А. Анализ применения искусственного интеллекта и машинного обучения в кибербезопасности. // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2023. – №3 (326). – С. 65-70.
2. Намиот Д.Е., Ильюшин Е.А., Чижов И.В. Искусственный интеллект и кибербезопасность. // International Journal of Open Information Technologies. – 2022. – № 10(9). – С. 135.
3. Саматов М. А. Анализ эффективности IDS/IPS-систем на базе Suricata в обеспечении сетевой кибербезопасности. // Вестник науки. – 2024. – №12 (81). – С. 1352-1360.
4. Шабанов, А. Применение технологий искусственного интеллекта в информационной безопасности / А. Шабанов // AM Live. – 2022 [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/primenenie-sistem-iskusstvennogo-intellekta-v-zaschite-informatsii/viewer. – Дата доступа: 21.10.2025
5. Admass W. S., Munaye Y. Y., Diro A. A. Cyber security: State of the art, challenges and future directions. // Cyber Security and Applications, 2024. – № 2. – 7 p.

References:

1. Kozlova N. S., Dovgal V. A. Analysis of the use of artificial intelligence and machine learning in cybersecurity. // Bulletin of the Adygea State University. Series 4: Natural, mathematical and technical sciences. – 2023. – №3 (326). – Pp. 65-70.
2. Namiot D.E., Ilyushin E.A., Chizhov I.V. Artificial intelligence and cybersecurity. // International Journal of Open Information Technologies. – 2022. – № 10(9). – P. 135.
3. Samatov M. A. Analysis of the effectiveness of IDS/IPS systems based on Suricata in ensuring network cybersecurity. // Bulletin of Science. – 2024. – №12 (81). – Pp. 1352-1360.
4. Shabanov, A. Application of artificial intelligence technologies in information security / A. Shabanov // AM Live. – 2022 [Electronic resource]. – Access mode: https://cyberleninka.ru/article/n/primenenie-sistem-iskusstvennogo-intellekta-v-zaschite-informatsii/viewer. – Access date: 21.10.2025

5. Admass W. S., Munaye Y. Y., Diro A. A. Cyber security: State of the art, challenges and future directions. // Cyber Security and Applications, 2024. – № 2. – 7 p.