УДК 004.8-049.5

АРХИТЕКТУРА МОДУЛЯ ИИ-АГЕНТА ДЛЯ SIEM-СИСТЕМ НОВОГО ПОКОЛЕНИЯ

Е.И. Юнчиц, П.Б. Гусаков

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В статье рассматривается проблема перегрузки операторов безопасности ложными срабатываниями в традиционных системах SIEM. Предложена архитектура автономного ИИ-агента, внедряемого в средство защиты как функциональный элемент. Агент использует методы машинного обучения для анализа событий и автоматического реагирования на инциденты. Результаты моделирования показывают снижение нагрузки на аналитиков до 40%.

Ключевые слова: Искуственный интеллект; SIEM; машинное обучение; SOC; информационная безопасность; логи; инциденты; SOAR; аналитика; SHAP.

AI-AGENT MODULE ARCHITECTURE FOR NEXT-GENERATION SIEM SYSTEMS

E.I. Yunchits, P.B. Gusakov

Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. This article examines the problem of security operator overload with false positives in traditional SIEM systems. We propose the architecture of an autonomous AI agent, which can be embedded into the security solution as a functional element. The agent uses machine learning methods to analyze events and automatically respond to incidents. Simulation results show a reduction in analyst workload of up to 40%.

Keywords: Artificial intelligence; SIEM; machine learning; SOC; information security; logs; incidents; SOAR; analytics; SHAP.

Введение

SIEM-системы – центральный компонент мониторинга ИТ-инфраструктур. Рост объема логов и сложности атак увеличивает количество ложных срабатываний, отвлекающих SOC на неопасные инциденты. Это снижает эффективность и повышает риск пропуска реальных угроз. Внедрение ИИ-агентов позволит моментально реагировать на события кибербезопасности и заранее выявлять подозрительные действия злоумышленников.

Основная часть

ИИ-агент – программный модуль с понятными интерфейсами, встраиваемый в инфраструктуру. Архитектура включает три уровня: сбор данных, анализ угроз и ответные действия, повторяя схему современных SIEM (прием событий, аналитика, реагирование). Это обеспечивает легкую интеграцию.

На первом уровне выполняется нормализация логов по стандарту CIM (Common Information Model). Разнородные сообщения приводятся к единому формату. Без обработки алгоритмы работают нестабильно, а именно: события теряются, картина искажается. Качество данных определяет до 80% успеха внедрения ИИ[1].

Второй уровень представляет собой само ядро ИИ-агента. Здесь используются модели машинного обучения без учителя. Модели запоминают поведение пользователей и различных систем, фиксируют паттерны этого поведения и сообщают об отклонениях, снижая этим количество ложных срабатываний. Также увеличивается скорость обнаружения сложных атак [2].

Третий уровень обеспечивает взаимодействие с SOAR [3] и автоматизированные действия. При срабатывании агент изолирует хост, блокирует учетную запись и уведомляет смену без ручных команд. Сотрудники получают готовые инциденты, что разгружает команду для работы со нестандартными ситуациями.

Для оценки эффективности выполнено сравнение с существующими продуктами[4]. В таблице 1 приведены различия между SIEM-системами без ИИ-агента и SIEM-системами с ИИ-агентом.

Сравнительный анализ традиционных SIEM и систем с ИИ-агентом
на основе реальных продуктов
Comparative analysis of traditional SIEM and AI-agent-based systems using real products

Критерий	SIEM-системы без ИИ-агента	SIEM-системы с ИИ-агентом
Примеры продуктов	IBM QRadar, ArcSight, LogRhythm	Microsoft Sentinel + AI agents, Exabeam Fusion, Splunk ES + ML Toolkit
Уровень ложных срабатываний	60–90% от общего числа алертов	Снижение на 60–80% благодаря поведенческому анализу
Среднее время обнаружения атак	2–6 часов (ручная корреляция)	5–20 минут (автоматическая приоритизация)
Взаимодействие с SOAR	Требует отдельной настройки	Нативная интеграция

Как видно из таблицы выше, добавление ИИ-агентов в современные SIEM(Microsoft Sentinel, Exabeam Fusion, Splunk ES) сильно влияет на основные показатели их работы. По данным из отчетов о внедрении ИИ-агента, можно увидеть, что удается снизить количество ложных срабатываний примерно на 60-90%. Это позволяет уменьшить нагрузку на аналитиков и дает им больше времени на рассмотрение действительно критичных инцидентов. Также, одновременно с этим сокращается среднее время обнаружения угроз.

Заключение

Ключевая проблема – прозрачность моделей («черный ящик»). Система принимает решение, но не объясняет почему. Для решения в ИИ-агента внедряется компонент интерпретации на основе SHAP, формирующий пояснение о влияющих особенностях поведения.

Вопрос защищенности самого ИИ-агента также важен. Агент должен работать в изолированной среде, иметь ограниченные права и не получать прямого доступа к критичным системам. Обмен данными с SIEM должен проходить через защищенные API-интерфейсы.

Список использованных источников

1. Чувакин А. А., Шмидт К., Филлипс К. Логирование и управление журналами: авторитетное руководство по пониманию концепций логирования и управления журналами. Уолтем: Syngress, 2012. 480 с.

2. Алескер Э. В. (ред.) Технологии машинного обучения в кибербезопасности: учебное пособие. М.: Интернет-университет информационных технологий, 2023. 280 с.

3. Дэрил К., Граймс Дж. Оркестрация безопасности, автоматизация и реагирование для аналитиков безопасности. Бирмингем: Packt Publishing, 2023. 356 с.

4. Европейские платформы SIEM 2026: независимый сравнительный отчет. Tekpon, 2026.

References

1. Chuvakin A., Schmidt K., Phillips C. Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Waltham: Syngress, 2012. 480 pages.

2. Alesker E. V. (ed.) Machine Learning Technologies in Cybersecurity: Textbook. Moscow: Internet University of Information Technologies, 2023. 280 pages.

3. Daryl K., Grimes J. Security Orchestration, Automation, and Response for Security Analysts. Birmingham: Packt Publishing, 2023. 356 pages.

4. European SIEM Platforms 2026: Independent Comparison Report. Tekpon, 2026

Сведения об авторах

Юнчиц Е.И., курсант, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», egorynchic2007@gmail.com.

Гусаков П.Б., магистр**,** начальник цикла, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», p.gusakov@bsuir.by.

Information about the authors

Yunchits E.I., cadet, Educational Institution "Belarusian State University of Informatics and Radioelectronics", egorynchic2007@gmail.com.

Gusakov P.B., Master, Head of the Cycle, Educational Institution "Belarusian State University of Informatics and Radioelectronics", p.gusakov@bsuir.by.