УДК 004.056

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ПРИ ЗАЩИТЕ КОНЕЧНЫХ УСТРОЙСТВ

Калугина А.С. (Университет ИТМО),
Научный руководитель – доктор технических наук, профессор практики Лившиц И.И.
(Университет ИТМО)

Введение. В настоящие время методы атак на информационные системы стремительно развиваются. Злоумышленники находят новые методы обхода известных систем защиты информации, которые в большом количестве внедрены в инфраструктуру крупных предприятий. Известно, что 80% источников данных в Mitre att&ck являются конечными хостами. Существующие классы систем защиты информации выявляют нарушения информационной безопасности с помощью статически задаваемых правил, основанных на рекомендациях вендоров, репутационных баз, данных из отрытой разведки, а также по общедоступным методикам kill-chain. Традиционные инструменты безопасности могут быть эффективны против известных угроз, аналитика поведения пользователей и сущностей необходима для выявления неизвестных и внутренних угроз [1]. Для формирования шаблона поведения пользователя используются алгоритмы машинного обучения, которые формируют аналитику по каждому пользователю за заданный период обучения и выявляют нетипичные действия проставляя скоринг событиям информационной безопасности.

Основная часть. В докладе рассматриваются различные подходы к формированию шаблона поведения пользователей с помощью известных алгоритмов машинного обучения:

1. Обучение с учителем [2];
2. С частичным привлечением учителя [3];
3. Без учителя.

Выявлены недостатки и проблемы, возникающие при формировании шаблона поведения пользователей в зависимости от используемого алгоритма, например, отсутствие меток нормального и аномального поведения, поиск оптимального периода обучения, длительность обучения и другие. Также рассмотрены параметры пользователей, по которым формируются шаблоны поведения пользователей и выявлены параметры, для которых необходимо формировать шаблоны поведения.

Выводы. В работе представлен результат анализа перспектив применения алгоритмов машинного обучения при защите конечных устройств. Выявлены недостатки и выбраны наиболее перспективные направления для дальнейшего исследования. На основе выполненного обзора в дальнейшем будет разрабатываться алгоритм формирования шаблонов поведения пользователей.

Список использованных источников:

1. Joyatee Datta, Rohini Dasgupta, Sayantan Dasgupta, Karmuru Rohit Reddy. Real-Time Threat Detection in UEBA using Unsupervised Learning Algorithms [Электронный ресурс]. – URL: https://ieeexplore.ieee.org/abstract/document/9614848, свободный. Яз. англ. (дата обращения 10.02.2023).
2. Yuan F., Cao Y., Shang Y., Liu Y., Tan J., Fang B. Insider threat detection with deep neural network [Электронный ресурс]. – URL:https://www.semanticscholar.org/paper/Insider-Threat-Detection-with-Deep-Neural-Network-Yuan-Cao/558767fab1845a63e94edc54dc0e9e7f89918469, свободный. Яз. англ. (дата обращения: 13.02.2023).
3. Zheng G., Srikumar V. DeepLog: anomaly detection and diagnosis from system logs through deep learning [Электронный ресурс]. – URL: https://www.cs.utah.edu/~lifeifei/papers/deeplog.pdf, свободный. Яз. англ. (дата обращения: 13.02.2023)

Калугина А.С. (автор) Подпись

Лившиц И.И. (научный руководитель) Подпись