МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра интеллектуальных систем

Аннотация к дипломной работе

ОБНАРУЖЕНИЕ ВТОРЖЕНИЙ НА ОСНОВЕ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Машкарева Наталья Дмитриевна

Научный руководитель: Соболь А.М., начальник отдела кибербезопасности ЦИТ БГУ

Минск, 2025

РЕФЕРАТ

Дипломная работа содержит 73 с., 16 рис., 15 табл., 12 источн., 2 прил.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, SIEM-СИСТЕМЫ, ЖУРНАЛЫ СОБЫТИЙ, МАШИННОЕ ОБУЧЕНИЕ, ЛАТЕРАЛЬНОЕ ПЕРЕМЕЩЕНИЕ, HADOOP, KAFKA, ELASTIC SEARCH, СИСТЕМЫ ЛОГИРОВАНИЯ.

Цель работы – разработка архитектуры SIEM-системы и построение модели машинного обучения для обнаружения атак латерального перемещения на основе анализа системных событий в ОС. Объектом исследования являются события информационной безопасности операционных систем.

В работе проанализированы особенности существующих SIEM-решений, таких как KUMA, R-Vision и MaxPatrol SIEM. Проведено сравнение их архитектур, функциональных возможностей и методов нормализации и корреляции. На основе анализа сформулированы требования к собственной архитектуре.

Разработана архитектура системы сбора и анализа событий с распределённым хранилищем на базе Hadoop, системы потоковой передачи данных Apache Kafka и полнотекстового поиска Elastic Search. Выполнена нормализация логов различных источников в единую структуру данных. Разработана и обучена модель XGBoost для выявления латерального перемещения злоумышленника внутри сети. Проведена оценка точности модели. Матрица ошибок и метрики показали высокую точность и сбалансированное качество классификации. Построена ROC-кривая для оценки AUC.

Разработанное решение протестировано и адаптировано под инфраструктуру информационной безопасности Белорусского государственного университета. Практическая значимость заключается в возможности интеграции системы в корпоративные сегменты с целью повышения эффективности мониторинга и реагирования на инциденты.

РЭФЕРАТ

Дыпломная праца змяшчае 73 с., 16 рыс., 15 табл., 12 крыніц, 2 прыкладанні.

ІНФАРМАЦЫЙНАЯ БЯСПЕКА, SIEM-СІСТЭМЫ, ЖУРНАЛЫ ПАДЗЕЯЎ, МАШЫННАЕ НАВУЧЭННЕ, ЛАТЭРАЛЬНАЕ ПЕРАМЯШЧЭННЕ, HADOOP, KAFKA, ELASTICSEARCH, СІСТЭМЫ ЛАГАВАННЯ.

Мэта працы – распрацоўка архітэктуры SIEM-сістэмы і стварэнне мадэлі машыннага навучання для выяўлення атак латэральнага перамяшчэння на аснове аналізу сістэмных падзей у АС. Аб’ектам даследавання з’яўляюцца падзеі інфармацыйнай бяспекі аперацыйных сістэм.

У працы прааналізаваны асаблівасці існуючых SIEM-рашэнняў, такіх як KUMA, R-Vision і MaxPatrol SIEM. Праведзена параўнанне іх архітэктур, функцыянальных магчымасцей і метадаў нармалізацыі і карэляцыі. На аснове аналізу сфармуляваны патрабаванні да ўласнай архітэктуры.

Распрацавана архітэктура сістэмы збору і аналізу падзей з размеркаваным сховішчам на базе Hadoop, сістэмай струменевай перадачы даных Apache Kafka і поўнатэкставага пошуку Elasticsearch. Здзейснена нармалізацыя лагаў розных крыніц у адзіную структуру даных. Распрацавана і навучана мадэль XGBoost для выяўлення латэральнага перамяшчэння зламысніка ўнутры сеткі. Праведзена ацэнка дакладнасці мадэлі. Матрыца памылак і метрыкі паказалі высокую дакладнасць і збалансаваную якасць класіфікацыі. Пабудавана ROC-крывая для ацэнкі AUC.

Распрацаванае рашэнне пратэставана і адаптавана пад інфраструктуру інфармацыйнай бяспекі Беларускага дзяржаўнага ўніверсітэта. Практычная значнасць заключаецца ў магчымасці інтэграцыі сістэмы ў карпаратыўныя сегменты з мэтай павышэння эфектыўнасці маніторынгу і рэагавання на інцыдэнты.

ABSTRACT

The thesis contains 73 pages, 16 figures, 15 tables, 12 sources, 2 appendixes.

INFORMATION SECURITY, SIEM SYSTEMS, EVENT LOGS, MACHINE LEARNING, LATERAL MOVEMENT, HADOOP, KAFKA, ELASTICSEARCH, LOGGING SYSTEMS.

The objective of this work is to develop a SIEM system architecture and build a machine learning model for detecting lateral movement attacks based on the analysis of operating system (OS) events. The research focuses on information security events in operating systems.

The study examines the features of existing SIEM solutions, such as KUMA, R-Vision, and MaxPatrol SIEM, comparing their architectures, functionalities, and methods of normalization and correlation. Based on this analysis, requirements for a custom architecture were formulated.

A distributed event collection and analysis system architecture was developed, utilizing Hadoop for storage, Apache Kafka for data streaming, and Elasticsearch for full-text search. Logs from various sources were normalized into a unified data structure. An XGBoost model was developed and trained to detect lateral movement within a network. The model's accuracy was evaluated, with the confusion matrix and metrics demonstrating high precision and balanced classification quality. An ROC curve was plotted to assess the AUC.

The developed solution was tested and adapted for the Belarusian State University's information security infrastructure. The practical significance lies in the system's potential integration into corporate segments to enhance monitoring efficiency and incident response.