МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра телекоммуникаций и информационных технологий

Аннотация к дипломной работе

РАЗРАБОТКА ПРАВИЛ КОРРЕЛЯЦИИ СОБЫТИЙ ДЛЯ KASPERSKY UNIFIED MONITORING AND ANALYSIS PLATFORM

СОБОЛЕВСКИЙ Павел Александрович

Научный руководитель – старший преподаватель,
И.А. Шалатонин

Минск, 2025

РЕФЕРАТ

Дипломная работа: 62 с., 50 рис., 18 источников

ПРАВИЛА КОРРЕЛЯЦИИ, АЛЕРТ, SIEM, KASPERSKY UNIFIED MONITORING AND ANALYSIS PLATFORM, KASPERSKY ANTI TARGETTED ATTACK PLATFORM, KASPERSKY SECURITY CENTER

Цель работы – разработка и внедрение правил корреляции событий для SIEM-платформы Kaspersky Unified Monitoring and Analysis Platform с учетом интеграции с Kaspersky Anti Targetted Attack Platform и Kaspersky Security Center, направленных на повышение эффективности обнаружения инцидентов информационной безопасности в телекоммуникационной компании.

Исследована архитектура, функциональные возможности и принцип работы SIEM-системы Kaspersky Unified Monitoring and Analysis Platform. Рассмотрены решения для защиты информации, представленные Лабораторией Касперского. Проанализированы существующие методы сбора и обработки событий в SIEM-системе. Реализована интеграция Kaspersky Unified Monitoring and Analysis Platform с Kaspersky Anti Targetted Attack Platform и Kaspersky Security Center в тестовой среде. На основании особенностей информационных технологий телекоммуникационной компании разработаны и протестированы правила корреляции, а также показана их эффективность при работе с событиями информационной безопасности.

Полученные результаты могут быть использованы для дальнейшего расширения набора правил корреляции, адаптации под другие источники событий и построения более сложных сценариев обнаружения инцидентов.

РЭФЕРАТ

Дыпломная праца: 62 с., 50 мал., 18 крыніц

ПРАВІЛЫ КАРЭЛЯЦЫІ, АЛЕРТ, SIEM, KASPERSKY UNIFIED MONITORING AND ANALYSIS PLATFORM, KASPERSKY ANTI TARGETTED ATTACK PLATFORM, KASPERSKY SECURITY CENTER

Мэта працы – распрацоўка і ўкараненне правілаў карэляцыі падзей для SIEM-платформы Kaspersky Unified Monitoring and Analysis Platform з улікам інтэграцыі з Kaspersky Anti Targetted Attack Platform і Kaspersky Security Center, накіраваных на павышэнне эфектыўнасці выяўлення інцыдэнтаў інфармацыйнай бяспекі тэлекамунікацыйнай кампаніі.

Даследавана Архітэктура, функцыянальныя магчымасці і прынцып работы SIEM-сістэмы Kaspersky Unified Monitoring and Analysis Platform. Разгледжаны рашэнні для абароны інфармацыі, прадстаўленыя Лабараторыяй Касперскага. Прааналізаваны Існуючыя метады збору і апрацоўкі падзей у SIEM-сістэме. Рэалізаваная інтэграцыя Kaspersky Unified Monitoring and Analysis Platform з Kaspersky Anti Targetted Attack Platform і Kaspersky Security Center ў тэставай асяроддзі. На падставе асаблівасцяў інфармацыйных тэхналогій тэлекамунікацыйнай кампаніі распрацаваны і пратэставаны правілы карэляцыі, а таксама паказана іх эфектыўнасць пры працы з падзеямі інфармацыйнай бяспекі.

Атрыманыя вынікі могуць быць выкарыстаны для далейшага пашырэння набору правілаў карэляцыі, адаптацыі пад іншыя крыніцы сабыццяў і пабудовы больш складаных сцэнарыяў выяўлення інцыдэнтаў.

ABSTRACT

The thesis contains 62 pag., 50 fig., 18 sources

CORRELATION RULES, ALERT, SIEM, KASPERSKY UNIFIED MONITORING AND ANALYSIS PLATFORM, KASPERSKY ANTI TARGETED ATTACK PLATFORM, KASPERSKY SECURITY CENTER

The aim of the work is to develop and implement event correlation rules for the Kaspersky Unified Monitoring and Analysis Platform SIEM platform, taking into account integration with the Kaspersky Anti Targeted Attack Platform and Kaspersky Security Center, aimed at improving the detection of information security incidents of the telecommunication company.

The architecture, functionality, and operating principle of the Kaspersky Unified Monitoring and Analysis Platform SIEM system are investigated. The information security solutions presented by Kaspersky Lab are reviewed. The existing methods of event collection and processing in the SIEM system are analyzed. Kaspersky Unified Monitoring and Analysis Platform is integrated with Kaspersky Anti Targeted Attack Platform and Kaspersky Security Center in a test environment. Based on the specifics of the telecommunication company's information technologies, correlation rules have been developed and tested, and their effectiveness in dealing with information security events has been demonstrated.

The results obtained can be used to further expand the set of correlation rules, adapt to other event sources, and build more complex incident detection scenarios.