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

Аннотация к дипломной работе

РАЗРАБОТКА КОРРЕЛЯЦИОННЫХ ПРАВИЛ В SIEM-СИСТЕМЕ ARCSIGHT В БАНКОВСКОЙ СФЕРЕ

СЕНЬКЕВИЧ Елизавета Михайловна

Научный руководитель – старший преподаватель,
А.Л. Труханович

Минск, 2025

РЕФЕРАТ

Дипломная работа: 70 с., 32 рис., 4 табл., 23 источника

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, SIEM-СИСТЕМА, ARCSIGHT, КОРРЕЛЯЦИОННЫЕ ПРАВИЛА, APT-АТАКИ, ИНЦИДЕНТЫ БЕЗОПАСНОСТИ, УГРОЗЫ, УЯЗВИМОСТИ, ПОВЕДЕНЧЕСКИЙ АНАЛИЗ, БАНКОВСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА

Объект исследования – процессы выявления и анализа инцидентов информационной безопасности в автоматизированных банковских системах на основе средств корреляции событий в SIEM-системе ArcSight.

Цель работы – разработать и внедрить правила корреляции в SIEM-системе ArcSight для повышения эффективности обнаружения угроз в банковском секторе.

Разработана методика создания и внедрения корреляционных правил в SIEM-системе ArcSight с учётом специфики информационной безопасности в банковской сфере. Проведён анализ угроз и уязвимостей, построена модель нарушителя, выполнена оценка базового уровня защищённости информационной системы. Сравнены современные SIEM-решения

Исследованы основные принципы функционирования SIEM-систем, рассмотрены архитектура и возможности ArcSight. Написаны правило мониторинга, помогающее отследить внедрение и функционирование вредоносных программ на объектах информационной инфраструктуры, связанное с переходом пользователей на ресурсы злоумышленников, правило мониторинга помогающее отследить несанкционированный доступ к объектам информационной инфраструктуры с использованием информационно-коммуникационных технологий, правило мониторинга помогающее отследить сканирование объектов информационной инфраструктуры в целях поиска уязвимостей на периметре локальной сети организации.

РЭФЕРАТ

Дыпломная праца: 70 с., 32 мал., 4 табл., 23 крыніцы

ІНФАРМАЦЫЙНАЯ БЯСПЕКА, SIEM-СІСТЭМА, ARCSIGHT, КАРЭЛЯЦЫЙНЫЯ ПРАВІЛЫ, АРТ-АТАКІ, ІНЦЫДЭНТЫ БЯСПЕКІ, ПАГРОЗЫ, УЯЗВІМАСЦІ, ПАВОДЗІНСКІ АНАЛІЗ, БАНКАЎСКАЯ ІНФАРМАЦЫЙНАЯ СІСТЭМА

Аб'ект даследавання – працэсы выяўлення і аналізу інцыдэнтаў інфармацыйнай бяспекі ў аўтаматызаваных банкаўскіх сістэмах на аснове сродкаў карэляцыі падзей у SIEM-сістэме ArcSight

Мэта працы – распрацаваць і ўкараняць правілы карэляцыі ў SIEM-сістэме ArcSight для павышэння эфектыўнасці выяўлення пагроз у банкаўскім сектары.

Распрацавана методыка стварэння і ўкаранення карэляцыйных правіл у SIEM-сістэме ArcSight з улікам спецыфікі інфармацыйнай бяспекі ў банкаўскай сферы. Праведзены аналіз пагроз і уязвімасцяў, пабудавана мадэль парушальніка, выканана ацэнка базавага ўзроўню абароненасці інфармацыйнай сістэмы. Праведзена параўнанне сучасных SIEM-рашэнняў.

Даследаваны асноўныя прынцыпы функцыянавання SIEM-сістэм, разгледжаны архітэктура і магчымасці ArcSight. Напісана правіла маніторынгу, якое дапамагае адсочваць укараненне і функцыянаванне шкоднасных праграм на аб’ектах інфармацыйнай інфраструктуры, звязанае з пераходам карыстальнікаў на рэсурсы зламыснікаў; правіла маніторынгу, якое дапамагае адсочваць несанкцыянаваны доступ да аб’ектаў інфармацыйнай інфраструктуры з выкарыстаннем інфармацыйна-камунікацыйных тэхналогій; правіла маніторынгу, якое дапамагае адсочваць сканаванне аб’ектаў інфармацыйнай інфраструктуры з мэтай пошуку ўязвімасцяў на перыметры лакальнай сеткі арганізацыі.

ABSTRACT

The diploma work: 70 p., 32 fig., 4 tabl., 23 sources

INFORMATION SECURITY, SIEM SYSTEM, ARCSIGHT, CORRELATION RULES, APT ATTACKS, SECURITY INCIDENTS, THREATS, VULNERABILITIES, BEHAVIORAL ANALYSIS, BANKING INFORMATION SYSTEM

The object of the study is the processes of identifying and analyzing information security incidents in automated banking systems based on event correlation tools in the ArcSight SIEM system.

The goal of the work is to develop and implement correlation rules in the ArcSight SIEM system to improve the effectiveness of threat detection in the banking sector.

A methodology for creating and implementing correlation rules in the ArcSight SIEM system was developed, taking into account the specifics of information security in the banking sector. Threats and vulnerabilities were analyzed, a threat actor model was built, and a baseline assessment of the information system’s security level was carried out. A comparison of modern SIEM solutions was conducted.

The fundamental principles of SIEM system operation were studied, and the architecture and capabilities of ArcSight were examined. A monitoring rule was written to track the introduction and functioning of malware within the information infrastructure objects related to user transitions to malicious resources; a monitoring rule to detect unauthorized access to information infrastructure objects using information and communication technologies; and a monitoring rule to detect scanning of information infrastructure objects to find vulnerabilities on the organization’s local network perimeter.