УДК *004.056.5*

ОРГАНИЗАЦИЯ ЦЕНТРАЛИЗОВАННОГО СБОРА СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В SIEM-СИСТЕМАХ С УЧЕТОМ НОРМАТИВНЫХ ТРЕБОВАНИЙ

Г.С. Смотрук[1], Т.А. Пулко[2]

[1]ООО «СофтЛайн Директ», г. Минск, Республика Беларусь

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

Аннотация. Рассмотрены принципы формирование централизованного контура сбора и обработки событий информационной безопасности на базе SIEM-систем с учетом требований нормативного регулирования. Особое внимание уделено реализации архитектуры сбора событий в соответствии с Приказом ОАЦ № 130, определяющим обязательный перечень регистрируемых событий. Описаны подходы к интеграции различных источников данных, включая операционные системы, базы данных, средства защиты информации и сетевое оборудование.

Ключевые слова: информационная безопасность; SIEM-систем; правила корреляции; события информационной безопасности; приказ ОАЦ №130.

IMPLEMENTATION OF CENTRALIZED COLLECTION OF INFORMATION SECURITY EVENTS IN SIEM SYSTEMS SUBJECT TO REGULATORY REQUIREMENTS

H.S. Smatruk[1], T.A. Pulko[2]

[1]SoftLine Direct LLC, Minsk, Republic of Belarus

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

Abstract. The principles of forming a centralized circuit for collecting and processing information security events based on SIEM systems, taking into account the requirements of regulatory regulation, are considered. Special attention is paid to the implementation of the event collection architecture in accordance with OAC Order No. 130, which defines the mandatory list of recorded events. Approaches to the integration of various data sources, including operating systems, databases, information security tools, and network equipment, are described.

Keywords: information security; SIEM systems; correlation rules; information security events; OAC Order No. 130.

Введение

Для формирования целостной картины состояния информационной безопасности используются системы класса SIEM (Security Information and Event Management), обеспечивающие централизованный сбор, нормализацию, хранение и анализ событий информационной безопасности от различных источников. Принятие приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» установило обязательный перечень типов и записей событий информационной безопасности, подлежащих регистрации, консолидации и хранению. Данный перечень фактически определяет минимально необходимый набор наблюдаемых событий для мониторинга состояния информационной безопасности и создает нормативную основу для построения процессов выявления и расследования инцидентов.

Средства защиты информации, включая антивирусные решения, системы обнаружения и предотвращения вторжений, системы предотвращения утечек данных, средства управления привилегированным доступом, сканеры уязвимостей, системы динамического анализа и изоляции подозрительных объектов, платформы автоматизации реагирования и оркестрации безопасности, а также системы мониторинга, формируют отдельный поток событий, имеющий критическое значение для мониторинга состояния безопасности. Как правило, журналы таких систем концентрируются на сервере администрирования, откуда передаются в SIEM по протоколу Syslog либо через специализированные агентские модули. Регистрируемые события включают обнаружение и блокирование вредоносных объектов, выявление уязвимостей и результатов сканирования, изменение конфигурации средств защиты, запуск и остановку сервисов, выполнение автоматизированных сценариев реагирования, а также действия администраторов. Контроль этих событий позволяет не только выявлять атаки, но и отслеживать корректность функционирования самих средств защиты и факты их возможного обхода или отключения. Интеграция прикладного программного обеспечения и средств защиты информации в SIEM-систему реализуется с использованием комбинации агентского сбора, парсинга файлов журналов и подключения через программные интерфейсы. Такой подход обеспечивает полноту охвата событий, соответствие нормативным требованиям и формирует единое информационное пространство для последующей корреляции и выявления инцидентов информационной безопасности.

Основная часть

Для организации вышеописанного решения реализован комплексный и нормативно обоснованный контур сбора событий информационной безопасности, охватывающий все основные классы источников, определенные требованиями Приказа ОАЦ при Президенте Республики Беларусь от 25.07.2023 № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40». Архитектура сбора включает централизованную пересылку событий операционных систем Windows с использованием серверов Windows Event Collector, прямое агентское подключение для критически значимых серверов, а также применение встроенных механизмов аудита и системных журналов в операционных системах Linux с маршрутизацией данных через syslog-транспорт.

Аудит систем управления базами данных организован посредством специализированных коннекторов, обеспечивающих извлечение событий непосредственно из системных таблиц и представлений аудита, что позволяет фиксировать контроль сессий, действия пользователей с административными привилегиями и операции управления правами доступа. Для телекоммуникационного оборудования, межсетевых экранов, прикладного программного обеспечения и средств защиты информации используется унифицированный механизм передачи событий по протоколу Syslog либо через агентские модули с последующей нормализацией и классификацией в SIEM-системе.

Ключевым техническим аспектом такого решения является обеспечение гарантированной доставки событий. Это достигается за счет локальной буферизации на агентах, использования очередей сообщений и дисковых очередей syslog-сервисов, а также применения промежуточных коллекторов, что минимизирует риск потери данных при пиковых нагрузках и временных отказах каналов связи. Такой подход обеспечивает формирование устойчивого, воспроизводимого и полноформатного потока событий информационной безопасности, соответствующего нормативным требованиям и особенностям инфраструктуры организации. Данная база событий служит основой для разработки и апробации правил корреляции, направленных на выявление инцидентов и угроз информационной безопасности.

Практическая значимость реализации указанного подхода заключается в возможности использования разработанного набора правил корреляции при внедрении и эксплуатации систем мониторинга информационной безопасности в организациях, обязанных выполнять требования Приказа ОАЦ № 130, а также при модернизации существующих систем централизованного сбора и анализа событий информационной безопасности.

Заключение

Продемонстрирован комплексный подход к построению контура централизованного сбора событий информационной безопасности, ориентированный на соответствие требованиям нормативного регулирования и практическим задачам мониторинга. В качестве методологической основы использованы положения Приказа ОАЦ № 130, определяющего минимально необходимый набор регистрируемых событий и тем самым задающего формализованную модель наблюдаемости информационной инфраструктуры. Показано, что сформированный контур является основой для последующей корреляции и выявления инцидентов, а также соответствует требованиям к построению систем мониторинга безопасности.

Сведения об авторах

Смотрук Г.С., инженер-системотехник, ООО «СофтЛайн Директ», smotrukgerman@gmail.com.

Пулко Т.А., канд. техн. наук, доц., доц. каф. защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», pulko@bsuir.by

Information about the authors

Smatruk H.S., system engineer, SoftLine Direct LLC, smotrukgerman@gmail.com.

Pulko T.A., Cand. of Sci., Associate Professor, Associate Professor of the Information Security Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", pulko@bsuir.by.