УДК 004.056.53:004.75:004.67

ПРИМЕНЕНИЕ BIG DATA ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ

М.В. Романюк
И.о. начальника отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры информатики, магистрант кафедры ПИКС
romanuk@bsuir.by

Е.А. Лещенко
Инженер-программист отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры информатики, магистрант кафедры ПИКС
e.leshchenko@bsuir.by

С.С. Марковский
Инженер-программист отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР
s.markovskij@bsuir.by

М.В. Романюк
Окончил Белорусский государственный университет информатики и радиоэлектроники. Инженер-программист, и.о. начальника отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры информатики БГУИР, магистрант кафедры проектирования информационно-компьютерных систем БГУИР.

Е.А. Лещенко
Окончил Белорусский государственный университет информатики и радиоэлектроники. Инженер-программист отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР, ассистент кафедры информатики БГУИР, магистрант кафедры проектирования информационно-компьютерных систем БГУИР.

С.С. Марковский
Окончил Белорусский государственный университет информатики и радиоэлектроники. Инженер-программист отдела сетевых технологий Центра информатизации и инновационных разработок БГУИР.

Аннотация. Выполнен обзор применимости технологий Big Data для анализа нормального функционирования информационных систем и компьютерных сетей и защиты данных этих систем и сетей от нежелательных воздействий киберугроз.

Рассмотрен пример применения технологий *Big Data* в *SIEM*-системах и сделаны выводы о полезности применения *Big Data*, т.к. это позволяет эффективно анализировать миллиарды событий в день и не допускать возникновение инцидентов информационной безопасности.

Ключевые слова: защита компьютерных сетей, *SIEM*, прогнозирование угроз, информационная безопасность

Введение. В современном мире, где предприятия и организации в своей деятельности повсеместно используют компьютерные сети, обеспечение безопасности этих сетей имеет первостепенное значение. В связи с экспоненциальным ростом объема данных, генерируемых и передаваемых по этим сетям, традиционные меры безопасности стали недостаточными для борьбы с более сложными киберугрозами, которые появляются ежедневно.

Справляться с современными киберугрозами помогают технологии *Big Data*, предлагающие расширенные возможности обработки и анализа больших объемов данных для обнаружения и устранения угроз безопасности в режиме реального времени. В этой статье рассматривается применение больших данных для повышения безопасности компьютерных сетей, их преимущества, проблемы и будущие перспективы.

Сбор и агрегирование данных. Аналитика *Big Data* начинается со сбора и агрегирования данных из различных источников в сети. Сюда входят сетевые журналы, пакеты, системные события и журналы действий пользователей. Собирая данные из различных источников, платформы *Big Data* создают комплексное представление о деятельности сети, позволяя специалистам информационной безопасности выявлять нехарактерные паттерны и потенциальные угрозы**.**

Мониторинг и обнаружение в режиме реального времени. Одним из ключевых преимуществ Больших Данных в области сетевой безопасности является возможность мониторинга и анализа сетевого трафика в режиме реального времени. Передовые алгоритмы аналитики могут обнаруживать аномалии, такие как необычные скачки трафика, попытки несанкционированного доступа или подозрительные модели поведения, немедленно информируя специалистов информационной безопасности о потенциальных угрозах. Такой подход позволяет быстро реагировать на угрозы и устранять их последствия, сводя к минимуму влияние инцидентов безопасности [1].

Поведенческий анализ и обнаружение аномалий. Аналитика больших данных позволяет применять методы машинного обучения и искусственного интеллекта для поведенческого анализа и обнаружения аномалий. Создавая базовые профили поведения пользователей, устройств и приложений эти системы могут выявлять отклонения от нормальных моделей, свидетельствующие о нарушениях безопасности или внутренних угрозах. Такой подход к обеспечению безопасности позволяет организациям обнаруживать угрозы и реагировать на них до того, как они перерастут в серьезные инциденты информационной безопасности.

Прогнозирующая аналитика и анализ угроз. Платформы Big Data могут использовать исторические данные и информацию об угрозах для прогнозирования и предотвращения будущих инцидентов безопасности. Анализируя прошлые атаки и тенденции, эти системы могут предвидеть возникающие угрозы и уязвимости, позволяя организациям принимать упреждающие меры для обеспечения безопасности. Кроме того, интеграция внешних источников информации об угрозах обеспечивает ценный контекст для понимания развивающегося спектра угроз, позволяя специалистам информационной безопасности действовать на опережение злоумышленников.

Масштабируемость и гибкость. Технологии *Big Data* обеспечивают масштабируемость и гибкость, позволяя организациям адаптироваться к динамичному характеру сетевых сред. Будь то крупномасштабные распределенные сети или облачные инфраструктуры, платформы *Big Data* могут легко справляться с объемом, скоростью и разнообразием генерируемых данных, обеспечивая непрерывный мониторинг и анализ без снижения производительности.

Примеры применения *Big Data* в защите компьютерных сетей. Хорошим примером использования технологий *Big Data* для повышения безопасности в компьютерных сетях предприятий и организаций являются *SIEM*-системы.

Security Information and Event Management (*SIEM*) – это программные комплексы для обеспечения компьютерной безопасности, которые сочетают в себе мониторинг ИТ-инфраструктуры в режиме реального времени на предмет угроз безопасности со сбором и анализом данных журналов и событий с различных компонентов *IT*-среды.

Появление больших объемов быстро меняющихся неструктурированных данных, таких как данные, генерируемые веб-приложениями, электронной почтой и социальными

сетями, создает проблему для *SIEM* с точки зрения способности находить корреляции и другую важную информацию о текущем состоянии безопасности. Такая информация может быть важна для обеспечения информационной безопасности, но старые типы *SIEM*-систем могут быть не приспособлены для работы с ней.

Сила технологии больших данных такова, что теперь доступны распределенные вычислительные среды и фреймворки, такие как *Hadoop*, позволяющие легко хранить и анализировать огромные объемы неструктурированных данных. Аналитика больших данных позволяет расширить возможности *SIEM*-систем в обнаружении угроз, предоставляя доступ к корреляции между пулами данных, которая ранее была недоступна. Эти большие данные могут включать в себя файлы журналов и события из внутренних систем, а также внешние источники, такие как данные разведки угроз, базы данных уязвимостей и данные социальных обогатителей [2].

Объем данных о событиях безопасности настолько велик, что специалисты информационной безопасности крупнейших современных предприятий могут анализировать миллиарды событий в день. Решения *SIEM*, интегрированные с инфраструктурой больших данных, позволяют организациям избежать сложностей, связанных с обработкой всех данных и событий, необходимых для обнаружения угроз информационной безопасности, при отсутствии в организации сложной инфраструктуры и больших человеческих ресурсов для анализа всей информации и поиска таких нарушений.

Заключение. Таким образом, применение *Big Data* для обеспечения информационной безопасности компьютерных сетей представляет собой значительный сдвиг в парадигме обнаружения и устранения угроз. Используя возможности передовой аналитики, машинного обучения и мониторинга в режиме реального времени, технологии *Big Data* позволяют специалистам информационной безопасности опережать развивающиеся киберугрозы и защищать критически важные активы. Однако эффективность решений по обеспечению безопасности на основе *Big Data* зависит не только от технологий, но и от квалифицированного персонала и надежных стратегий кибербезопасности. По мере того, как организации будут продолжать цифровые преобразования, интеграция аналитики *Big Data* в их системы безопасности будет иметь решающее значение для поддержания устойчивости к постоянно меняющемуся спектру угроз.

Список литературы

[1] Leveraging Big Data Analytics with SIEM: Extracting Actionable Insights for Proactive Security: [Электронный ресурс]. URL: https://www.linkedin.com/pulse/leveraging-big-data-analytics-siem-extracting-aravind-raghunathan. (Дата обращения: 09.02.2024).

[2] What is SIEM and How Does it Relate to Big Data and Machine Learning? [Электронный ресурс]. URL: https://datafloq.com/read/siem-how-does-relate-big-data-machine-learning/. (Дата обращения: 11.02.2024).

Авторский вклад

Авторы внесли равноценны вклад.

APPLYING BIG DATA TO PROTECT COMPUTER NETWORKS

M.V. Romaniuk
Acting Head of the Network Technologies Department of the Center of Informatization and Innovation Elaborations, Assistant of the Department of Computer Science of BSUIR, Master's student of the Department of ICSD of BSUIR

E.A. Leshchenko
Software Engineer of the Network Technology Department of the Center of Informatization and Innovation Elaborations, Assistant of the Department of Computer Science of BSUIR, Master's student of the Department of ICSD of BSUIR

S.S. Markovskii
Software Engineer of the Network Technology Department of the Center of Informatization and Innovation Elaborations

Abstract. The review of the applicability of Big Data technologies for analyzing the normal functioning of information systems and computer networks and protecting the data of these systems and networks from the undesirable effects of cyber threats is carried out.

An example of the use of Big Data technologies in SIEM systems is considered and conclusions are drawn about the usefulness of using Big Data, since it allows you to effectively analyze billions of events per day and prevent the occurrence of information security incidents.

Keywords: protection of computer networks, SIEM, threat prediction, information security