УДК 004.056.53

Лященко Зоя Владимировна, доцент кафедры Вычислительная техника и автоматизированные системы управления, Ростовский государственный университет путей сообщения, г. Ростов-на-Дону

Савелинко Артем Николаевич, студент, Ростовский государственный университет путей сообщения, г. Ростов-на-Дону

РОЛЬ И ВОЗМОЖНОСТИ ЖУРНАЛОВ СОБЫТИЙ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

Журналы событий бывают разных типов, каждый из которых дает уникальное представление о действиях, происходящих в цифровой среде. Например, системные журналы регистрируют события, связанные с работой операционной системы, в то время как журналы приложений фокусируются на работе конкретного программного обеспечения. Сетевые журналы фиксируют данные о трафике, проходящем через сеть, а журналы безопасности отслеживают события, связанные с безопасностью, например попытки входа в систему или изменения прав доступа пользователей. Типы событий и уровни потенциальных проблемных точек помогают классифицировать и определять приоритетность различных событий. Коды ошибок и сообщения о состоянии дают представление о состоянии системы и возможных проблемах. В случае инцидентов отклонения возможно найти информацию о доступе к файлам, выполненных командах или использованных ресурсах.

Annotation

Event logs come in different types, each of which provides a unique insight into the activities taking place in the digital environment. For example, system logs log events related to the operation of the operating system, while application logs focus on the operation of specific software. Network logs capture data about traffic passing

through the network, and security logs track security-related events, such as login attempts or user access rights changes. The types of events and le.vels of potential problem points help classify and prioritize various events. Error codes and status messages give an idea of the system status and possible problems. In case of rejection incidents, it is possible to find information about file access, commands executed, or resources used.

Ключевые слова: журналы событий, информационная безопасность, несанкционированный доступ, коды ошибок.

Keywords: event logs, information security, unauthorized access, error codes.

Когда речь заходит о форматах журналов, универсального подхода не существует. Различные системы и приложения часто по-своему структурируют данные журнала. Однако появились некоторые общие форматы, которые помогают стандартизировать эту информацию. Например, Syslog – это широко используемый протокол для регистрации сообщений, популярный в средах Unix и Linux. Журналы событий Windows имеют свою собственную структуру, предназначенную для систем Microsoft. Многие приложения используют простые текстовые журналы, в то время как другие могут использовать более структурированные форматы, такие как JSON или XML, для более удобного разбора и анализа.

Прежде чем погрузиться в тонкости анализа журналов, важно правильно подготовить базу.

Создание системы управления журналами. Речь идет не только о выборе программного обеспечения, но и о создании централизованного узла для всех данных журнала. Хорошая система управления журналами будет автоматически собирать журналы из различных источников в сети, надежно хранить их и предоставлять инструменты для удобного поиска и анализа. При выборе системы стоит учитывать такие факторы, как масштабируемость, простота использования и возможности интеграции с существующей инфраструктурой.

Создание политик сбора и хранения журналов. Эти политики определяют, какие типы журналов необходимо собирать, как долго требуется их хранить и

каким образом они будут храниться. Здесь нужно соблюдать баланс: если собирать слишком мало, можно упустить важную информацию; если собирать слишком много, можно утонуть в данных. Политика хранения должна соответствовать операционным потребностям, так и нормативным требованиям. Во многих случаях журналы могут стать основным доказательством в случае инцидента нарушения технологического процесса, поэтому необходима уверенность, что хранение их обеспечено достаточно долго, чтобы они были полезны.

Обеспечение целостности журналов и поддержание цепочки хранения. Это, пожалуй, самый важный аспект подготовки журналов. Журналы ценны только в том случае, если им можно доверять. Важно применять меры по предотвращению фальсификации, например, использование хранилища с функцией «запись-выдача» или цифровых подписей. Необходимо установить строгий контроль доступа, чтобы ограничить круг лиц, которые могут просматривать или изменять данные журнала. И создать четкую цепочку хранения – документировать, кто, когда и почему получает доступ к журналам.

Нормализация журналов. Различные системы часто создают журналы в разных форматах, что может затруднить их анализ. Нормализация журналов – преобразование их в стандартный формат – может значительно упростить процесс анализа в дальнейшем.

Тестирование. Необходимо регулярно проверять, работает ли коллекция журналов так, как ожидалось.

Основные инструменты для анализа журналов

Наличие правильных инструментов может иметь огромное значение. Это похоже на хорошо оборудованную мастерскую – каждый инструмент служит определенной цели, а при совместном использовании они могут помочь обнаружить сведения, которые в противном случае могли бы остаться скрытыми.

В основе многих операций по анализу журналов лежит система SIEM (Security Information and Event Management).

Инструменты SIEM – это системы, которые собирают, агрегируют и анализируют данные журналов из различных источников в сети. Они обеспечивают мониторинг в режиме реального времени, оповещение и часто включают встроенные аналитические возможности. SIEM особенно ценны своей способностью коррелировать события из разных источников, помогая обнаружить закономерности, которые могут указывать на угрозу безопасности.

Инструменты для разбора журналов помогают разбить сложные записи журнала на более удобные структурированные данные. Они могут извлекать из журналов определенные поля, отфильтровывать ненужную информацию и преобразовывать журналы в форматы, удобные для анализа. Среди популярных инструментов для разбора журналов – Logstash, Fluentd и Graylog. Эти инструменты необходимы для работы с огромным объемом и разнообразием данных журналов, которые генерируют современные системы.

Инструменты визуализации оживляют данные журнала. Они преобразуют необработанные данные в графики, диаграммы и информационные панели, с помощью которых легче обнаружить тенденции и аномалии. Такие инструменты, как Kibana, Grafana и функции визуализации Splunk, позволяют создавать пользовательские панели, давая возможность сразу же получить представление о состоянии системы и ее безопасности. Хорошая визуализация может превратить часы изучения файлов журналов в мгновения ясности, помогая быстро выявить области, требующие внимания.

Новейшими дополнениями к набору инструментов для анализа журналов являются средства машинного обучения и анализа с помощью искусственного интеллекта. Эти передовые инструменты могут просеивать огромные объемы данных журналов, изучая нормальную работу системы и отмечая необычные действия. Они особенно хороши в обнаружении тонких аномалий, которые могут ускользнуть от внимания человека. Некоторые инструменты используют искусственный интеллект для прогнозирования возможных будущих проблем на основе исторических данных журнала. Хотя эти инструменты очень мощные, их лучше использовать в сочетании с человеческим опытом, а не вместо него.

У каждого из этих инструментов есть свои сильные стороны, и наиболее эффективные стратегии анализа журналов часто предполагают их использование в комбинации. Например, можно использовать SIEM для сбора и корреляции журналов, инструменты синтаксического анализа для структурирования данных, инструменты визуализации для создания удобных для восприятия панелей, а также инструменты с поддержкой искусственного интеллекта для более глубокого изучения аномалий.

Ключевые методы, которые помогут повысить уровень анализа журналов.

Установление базовой линии – основа эффективного анализа журналов. Оно включает в себя понимание того, как выглядит «норма» в данной среде. Установив базовые показатели типичного поведения системы, действий пользователей и создается точка отсчета, по которой можно оценивать аномалии. Этот процесс требует времени и терпения, поскольку необходимо наблюдать за системами в течение длительного времени, чтобы учесть регулярные колебания, такие как повышенная активность в рабочее время или ежемесячные циклы обслуживания.

Корреляционный анализ – позволяет продвинуться дальше в распознавании закономерностей, соединяя точки между различными источниками журналов. Одно подозрительное событие в одном журнале может не вызвать подозрений, но, если соотнести его с событиями из других журналов, можно обнаружить системную проблему.

Обнаружение аномалий – это выявление необычного среди обычного. Этот метод в значительной степени опирается на установленные базовые показатели и навыки распознавания образов. Хотя многие инструменты предлагают автоматическое обнаружение аномалий, человеческая интуиция часто играет решающую роль в различении между доброкачественными аномалиями и потенциальными угрозами.

Поиск угроз с помощью журналов – это проактивный подход к безопасности. Это может включать в себя создание гипотез о потенциальных сценариях сбоев и последующее погружение в журналы, чтобы доказать или

опровергнуть эти гипотезы. Эффективная охота за угрозами требует глубокого понимания как среды, так и текущего ландшафта угроз.

Эти методы не являются взаимоисключающими; лучше всего они работают в сочетании друг с другом. При анализе журналов можно начать со сравнения базовых показателей, выявить закономерности, соотнести события в журналах, определить аномалии, а затем приступить к целенаправленному поиску угроз, основываясь на полученных результатах

Литература

1. Гаврилова, Т. А. Базы знаний интеллектуальных систем / Т. А. Гаврилова, В. Ф. Хорошевский. СПб.: Питер, 2000. - 384 с.

2. Тулупъев, А. Л. Алгебраические байесовские сети. Логико-вероятностный подход к моделированию баз знаний с неопределенностью / А. Л. Тулупьев. СПб.: СПИИРАН, 2000. - 292 с.

3. Фогелъсон, Ю. Б. Сокращение перебора при построении разделяющих признаков / Ю. Б. Фогельсон // Описание и распознавание объектов в системах искусственного интеллекта. — М.: Наука, 1980. С. 892.

4. Цибульский, Г. М. Модели обучения автоматизированных обучающих систем / Цибульский Г. М., Герасимова Е. И., Ерошин В. В. // Системотехника: сетевой электронный журнал. — 2004. № 2.

5. Городецкий, В. И. Оптимизация описания классов ситуаций в задаче распознавания по неполному множеству признаков / В. И. Городецкий // Кибернетика. 1987. - № 4. - С. 127-128.

Literature

1. Gavrilova, T. A. Knowledge bases of intelligent systems / T. A. Gavrilova, V. F. Khoroshevsky. St. Petersburg: Peter, 2000. - 384 p.

2. Tulupyev, A. JI. Algebraic Bayesian networks. A logical-probabilistic approach to modeling knowledge bases with uncertainty / A. L. Tulupyev. St. Petersburg: SPIIRAN, 2000. - 292 p.

3. Fogelson, Yu. B. Reduction of enumeration in the construction of dividing features / Yu. B. Fogelson // Description and recognition of objects in artificial intelligence systems. — M.: Nauka, 1980. p. 892.

4. Cybulsky, G. M. Models of learning automated learning systems / Cybulsky G. M., Gerasimova E. I., Eroshin V. V. // System Engineering: online electronic journal. — 2004. № 2.

5. Gorodetsky, V. I. Optimization of the description of classes of situations in the problem of recognition by incomplete set of signs / V. I. Gorodetsky // Cybernetics. 1987. - No. 4. - pp. 127-128.