АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ
AUTOMATION AND CONTROL

УДК 004.056, 004.77 **DOI: 10.18413/2518-1092-2024-9-4-0-2**

Лазарев С.А.
Рубцов К.А.

О ПОВЕДЕНЧЕСКОЙ АНАЛИТИКЕ ДЛЯ СИСТЕМЫ ЗАЩИТЫ ОТ ЦЕЛЕНАПРАВЛЕННЫХ АТАК И ЕЕ ПРИМЕНЕНИЕ ДЛЯ ОПЕРАЦИОННЫХ СИСТЕМ СЕМЕЙСТВА ASTRA LINUX

Белгородский государственный национальный исследовательский университет,
ул. Победы, 85, г. Белгород, 308015, Россия

e-mail: lazarev_s@bsu.edu.ru

Аннотация
В статье рассмотрена задача разработки подсистемы поведенческой аналитики для системы защиты от целенаправленных атак и применение ее работы на операционных системах семейства Astra Linux. Произведен обзор возможных видов целенаправленных атак и типовых действий, подлежащих оценке при построении системы защиты от целенаправленных атак. Рассмотрены различные виды систем безопасности и их ранжирование по технологиям защиты. Предложено использование многомерной модели распределения Гаусса (GMM) для анализа поведения объектов информационного взаимодействия совместно с отечественной системой защиты от целенаправленных атак AVSOFT ATHENA под управлением операционной системы Astra Linux, осуществляющей анализ сетевой активности, анализ использования ресурсов.
Ключевые слова: системы защиты от целенаправленных атак; поведенческая аналитика; отечественные операционные системы; многомерная модель распределения Гаусса
Для цитирования: Лазарев С.А., Рубцов К.А. О поведенческой аналитике для системы защиты от целенаправленных атак и ее применение для операционных систем семейства Astra Linux // Научный результат. Информационные технологии. – Т.9, №4, 2024. – С. 11-20. DOI: 10.18413/2518-1092-2024-9-4-0-2

Lazarev S.A.
Rubtsov K.A.

ABOUT BEHAVIORAL ANALYTICS FOR THE SYSTEM FOR PROTECTION AGAINST TARGETED ATTACKS AND ITS APPLICATION FOR OPERATING SYSTEMS OF THE ASTRA LINUX FAMILY

Belgorod State National Research University,
85 Pobedy St., Belgorod, 308015, Russia

e-mail: lazarev_s@bsu.edu.ru

Abstract
The article discusses the task of developing a behavioral analytics subsystem for a system of protection against targeted attacks and the application of its work on operating systems of the Astra Linux family. A review of possible types of targeted attacks and typical actions to be assessed when building a protection system against targeted attacks is provided. Various types of security systems and their ranking according to protection technologies are considered. It is proposed to use a multidimensional Gaussian distribution model (GMM) to analyze the behavior of objects of information interaction together with the domestic system of protection against targeted attacks

AVSOFT ATHENA running the Astra Linux operating system, which analyzes network activity and analyzes the use of resources.
Keywords: protection systems against targeted attacks; behavioral analytics; domestic operating systems; multivariate Gaussian distribution model
For citation: Lazarev S.A., Rubtsov K.A. About behavioral analytics for a system of protection against targeted attacks and its application for operating systems of the Astra Linux family // Research result. Information technologies. – T.9, №4, 2024. – P. 11-20. DOI: 10.18413/2518-1092-2024-9-4-0-2

ВВЕДЕНИЕ

Разработка подсистемы поведенческой аналитики подразумевает использование алгоритмов анализа и классификации типов атак на систему информационной безопасности. Раннее компьютерные атаки использовались для нанесения ущерба путём внедрения вирусного кода, удаления важной информации, атаки на сайты с целью подмены содержимого WEB-ресурса, и другие виды информационного воздействия [1]. В настоящее время типичны атаки преследующие цели: получение выгоды финансового характера, решение задач борьбы с конкурентами, выполнение разведывательных действий, дискредитация и т.п. [2].

При проведении целенаправленных атак используются все доступные злоумышленниками средства – специально разработанные вредоносные программы, атаки на веб-серверы и сетевую инфраструктуру, социальная инженерия, использование инсайдеров. Рассматривая целенаправленные атаки, следует учитывать угрозы APT (Advanced Persistent Threat). APT это довольно сложные целевые атаки, которые осуществляются в течении продолжительного времени. Основной задачей таких атак, является получение контроля над инфраструктурой организации и, как следствие, доступ к устройствам пользователей. Получение доступа к устройствам пользователей может повлечь потерю конфиденциальной информации организации. APT осуществляются обычно адаптивными алгоритмами с учетом применяемых средств защиты в организации. Особое внимание злоумышленники уделяют незаметности проникновения, что дает возможность осуществлять контроль над взломанной системой максимально длительное время. Необходимость использования злоумышленниками APT в целенаправленных атаках на защищенные системы обусловлено невозможностью применения простых методов вторжения и задачей максимально скрыть факт несанкционированного доступа. Для защиты от APT используется подход с обеспечением защиты на всех уровнях. Важным моментом является минимизация человеческого фактора, снижающего уровень защиты системы. Для этого необходимы мероприятия по систематическому обучению и проверке персонала. Для противодействия целенаправленным атакам необходимо применение специализированных программно-аппаратные средств, реализующих различные уровни защиты. Такие средства, должны своевременно обнаруживать атаки по косвенным признакам, выявлять различные отклонения в работе пользователей и сетевой инфраструктуры, т.е. осуществлять анализ поведения пользователей и объектов информационного взаимодействия на основе сущностей с помощью программных модулей поведенческой аналитики DLP-систем (Data Leak Prevention Systems) [3, 4].

ОСНОВНАЯ ЧАСТЬ

Системы защиты от целенаправленных используют различные средства противодействия и защитные механизмы. Основные методы и технологии по защите информации были описаны американской исследовательской и консалтинговой компанией Gartner Research (Gartner), которая специализируется на рынке информационных технологий. В настоящее время предложенные компанией Gartner методы защиты информации используются во всех современных программных продуктах защиты. Некоторые производители средств защиты от целенаправленных атак осуществляют детальную проработку одного из методов, другие пытаются представить большее количество программ, как клиентских, так и для серверов под управлением ОС Windows, с целью

охватить как можно больше областей, предложить заказчикам комплексные и самодостаточные решения по защите информации. Имеются также производители средств защиты от целенаправленных атак, которые создают программное обеспечение на базе существующих продуктов.

Согласно данным компании Gartner полноценное детектирование и осуществление противодействия целенаправленным атакам, а также защите от угроз APT необходимо одновременно использовать как минимум пять основных методов и технологий защиты [5]:

1) Проведение в реальном времени анализа сетевого трафика, построение нормальной модели объектов сетевого взаимодействия компании, анализ аномальных ситуаций и отклонений от типичного процесса сетевого взаимодействия на предмет обнаружения атаки и осуществление блокирования подозрительного по результатам анализа сетевого трафика

2) Мониторинг сетевого трафика без моментального реагирования, накопление статистики для дальнейшего поиска аномалий при проведении поведенческого анализа на большом объеме данных за длительный период. Этот метод применяется для обнаружения атак и последующего расследования инцидентов.

3) Использование средств виртуализации, то есть технологии «песочниц». Применение изолированной виртуальной среды для запуска программ и скриптов проходящих в сетевом трафике инициированным пользовательской ЭВМ, позволяет выполнить анализ их поведения, осуществить контроль требуемых основных аппаратных ресурсов: загрузка процессорных ядер, потребление оперативной памяти, интенсивность использования внешней (дисковой) памяти и сетевой доступ.

4) Проведение поведенческого анализа активности пользовательских ЭВМ. Этот метод защиты предполагает перехват системных функций и доступа к ресурсам пользовательской ЭВМ с одновременным поиском аномалий в работе приложений и операционной системы. Метод предполагает использование активных способов защиты, как блокирование потенциально опасных приложений и операций.

5) Сбор и хранение данных об активности пользователя, выполняемых приложений и операционной системы на пользовательской ЭВМ. Накопленный массив используется для поведенческого анализа на большом массиве данных активности пользовательской ЭВМ в течении длительного времени.

Из приведенных выше пяти основных методов и технологий защиты, предложенных компанией Gartner, можно выделить три главных технологии для обнаружения целенаправленных атак:

1) анализ сетевого трафика;

2) поведенческий анализ пользовательской ЭВМ, то есть анализ приложений и работы операционной системы;

3) применение технологии «песочницы».

Следует отметить, что целенаправленные атаки и APT это распределенные во времени процессы, которые используют различные точки вторжения. Для их своевременного обнаружения и предотвращения ущерба необходимо использовать как можно больше различных средств и методов защиты.

Для подсистемы поведенческой аналитики для системы защиты от целенаправленных атак можно выделить российские продукты: Kaspersky Anti Targeted Attack Platform имеющая возможности анализа сетевого трафика и телеметрии с пользовательских ЭВМ, а также выполнять эмуляцию угроз с помощью песочницы и набора современных детектирующих технологий. InfoWatch Targeted Attack Detector обеспечивает детальный контроль состояния пользовательских ЭВМ, сбор информации об активности пользователей и приложений в облачном сервисе с последующим анализом, основанным на работе с большими данными. Также на российском рынке представлены системы от Ростелеком семейства Solar для крупных компаний и государственного сектора, Falcongaze с системой SecureTower для крупных и средних компаний, Infowatch с целой линейкой продуктов предоставляющих услуги защиты и анализа информации, Athena от компании «АВ Софт» обеспечивающей систему класса «песочниц», в которых каждый файл проходит

многоуровневую проверку статическим и динамическим методами анализа с использованием технологии искусственного интеллекта. Среди западных продуктов защиты от целенаправленных атак следует выделить специализированные решения: Arbor Spectrum, Check Point SandBlast и другие. Стоит отметить, что решения каждой компании имеют свою специфику применения, так решения от Infowatch имеют системную архитектуру компонентов, работающих на разных платформах (Windows и Linux), а решения от российской компании SearchInform представляет собой большое количество программ как для клиентов, так и для серверов, причем все компоненты системы работают на ОС Windows [6].

Акцентируя внимание на поведенческом анализе приложений и ОС пользователей можно отметить, что важным моментов в системе безопасности также является человеческий фактор, без учета которого повышаются риски целенаправленных атак и несанкционированного доступа к информационной системе компании. В этом случае целесообразно применение систем анализа поведения пользователей и сущностей (UEBA), в которых используется поиск и выявление аномалий в поведении пользователей и различных систем. Данный тип поведенческого анализа особенно важен в случае, если компания использует различные системы сбора данных. Использование множества различных систем информационной безопасности и большой объем информации приводит к перегруженности сотрудников, отвечающих за безопасность, что приводит к снижению оперативного реагирования на инциденты нарушения безопасности. Использование систем UEBA позволяет повысить эффективность работы сотрудников службы безопасности за счет использования настраиваемых профилей реагирования системы на инциденты с потенциальной утечкой данных. Систем анализа поведения пользователей и сущностей являются продолжением систем поведенческого анализа пользователей (UBA). Главным отличием систем UEBA от UBA является наличие профилей для анализа сущностей, то есть анализ на информационную безопасность серверов, приложений на пользовательских ЭВМ, сетевого трафика и хранимых данных как локально, так и на NAS. Использование систем UEBA в компаниях позволяет не только обнаружить внутренние утечки информации, но и выявить внешние целенаправленные атаки. При применении системы UEBA создаются профили для объектов информационной безопасности. В качестве таких объектов могут быть пользователи сетевой инфраструктуры компании, а также различные сущности. Такой единый подход к различным объектам контроля позволяет своевременно реагировать в случае компрометации данных или объектов информационной инфраструктуры. Для систем UBA типична практическая реализация как отдельные решения под конкретные задачи, которые не требуют интеграции с другими системами и могут работать самостоятельно. Системы UEBA разрабатываются с возможностью анализа данных других систем и поставляются в рамках платформы [7].

Внедрение в систему компонентов анализа поведения сущностей позволяет значительно расширить возможности по обнаружению сетевых атак за счет использования моделей поведения.

В настоящее время имеется тенденция совместного использования систем поведенческого анализа с решениями DLP, EDR, SIEM для обеспечения сотрудников информационной безопасности точными данными как о сотрудниках, так и их активности, а также активности различных устройств инфраструктуры компании [8].

Можно выделить несколько типовых угроз, приводящих к негативным последствиям. Согласно «Методике оценки угроз безопасности информации» [9] и ГОСТ [10, 11] предлагается выделить 3 уровня рисков, обозначенных как У1, У2 и У3:

1) У1, ущерб, причинённый физическому лицу;

2) У2, ущерб, причинённый юридическому лицу, индивидуальному предпринимателю, нарушения хозяйственной деятельности;

3) У3, ущерб государству в области обеспечения обороны страны, безопасности государства и правопорядка, а также в социальной, экономической, политической и экологической сферах деятельности.

Соответственно действия нарушителей сопоставляются с целями их действий и возможным риском нанесения ущерба. Для классификации нарушителей предлагается использовать 4 категории от Н1 до Н4.

Авторы предлагают для оценки уровней опасности экспертную оценку с линейными числовыми показателями опасности для шести уровней угроз: отсутствие угрозы – 0; низкий – 0,2; базовый – 0,4; базовый повышенный – 0,6; средний – 0,8; высокий – 1.

Была осуществлена экспертная оценка уровня опасности угроз для 21 различной цели и от 1 до 7 видов для каждой цели нарушителей при атаке на систему безопасности. Был получен средний уровень угроз 0,66, что без учета вероятности каждого вида угроз превышает базовый повышенный уровень, т.е. система общего назначения (широкого применения) информационной безопасности должна соответствовать и уметь обрабатывать не менее среднего уровня возможных угроз атаки. Это подтверждает целесообразность использования комплексных систем защиты в организации.

Одним из важных компонентов систем защиты является подсистема поведенческой аналитики. Такая система в расширенном понимании может использоваться для анализа действий различных объектов информационного взаимодействия. Под объектами информационного взаимодействия можно рассматривать действия программного кода, отдельных приложений, рабочих станций пользователей и поведение самих пользователей. При таком рассмотрении минимизируется влияние человеческого фактора в системе безопасности.

Подсистема поведенческой аналитики системы защиты от целенаправленных атак может быть построена как автономное или встроенное решения (рисунок).

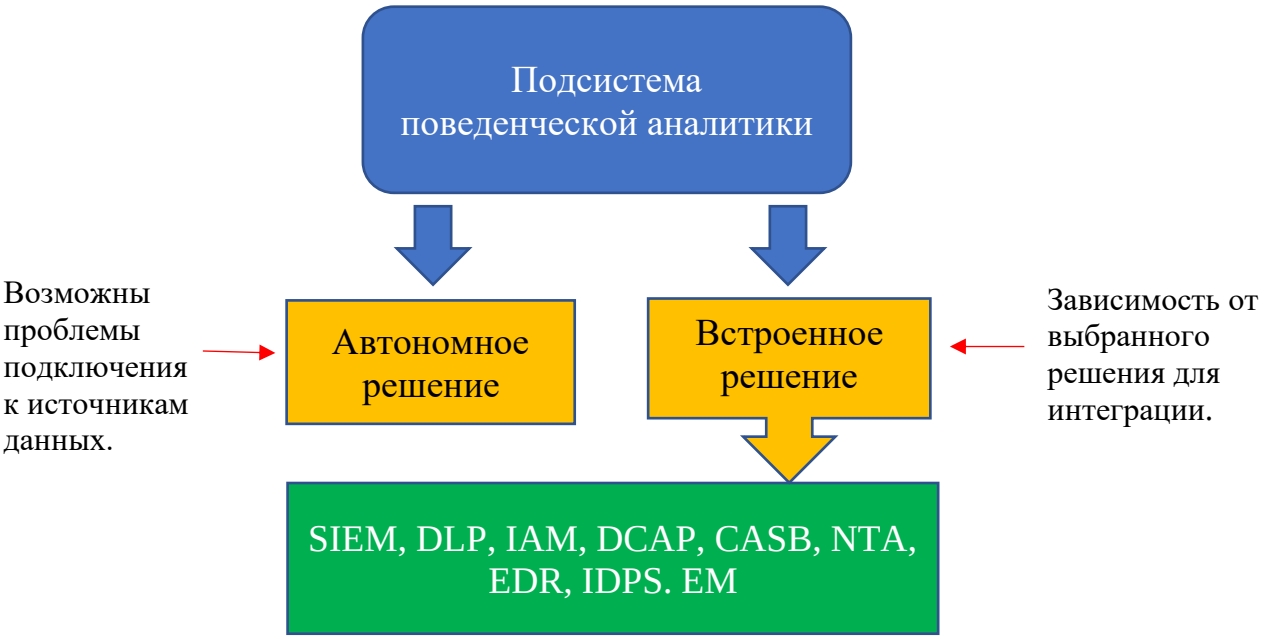

Рис. Структура подсистемы поведенческой аналитики системы защиты от целенаправленных атак в случае автономного и встроенного решения

Fig. Structure of the behavioral analytics subsystem of the system for protecting against targeted attacks in the case of a stand-alone and built-in solution

По состоянию на 2023 год представленные решения на рынке в системах безопасности как UBA имеют равное разделение между встроенными и автономными. Для встроенных решений характерна интеграция в состав систем других классов, которые специализируются на смежных задачах [12-17].

Автономное решение имеет две критические проблемы:

1) интеграция в существующую ИТ-инфраструктуру;

2) получение актуальных данных в достаточном количестве.

Внедрение автономного решения целесообразно проводить в средней или крупной компании. Полнофункциональное развертывание автономного решения является весьма дорогостоящим проектом и требуется детальная его проработка на стадии проектирования и оценка окупаемости проекта. Такое решение эффективно, когда в компании имеется единая база данных, где накоплены данные для проведения поведенческого анализа.

В имеющихся отечественных решениях InfoWatch, SearchInform и Zecurion, поведенческий анализ осуществляется отдельными компонентами DLP-систем или может производится на основе данных из других DLP-систем.

Авторами был выбран продукт AVSOFT ATHENA, который имеет внутри два класса современных систем безопасности: виртуальную среду типа «песочница» и антивирусный мультисканер. Система ATHENA позволяет выполнять анализ на предмет безопасности файлов и ссылок из различных источников, включая данные, передаваемые от собственной системы агентов установленных на рабочих местах пользовательских ЭВМ. Важным моментом данной системы является то, что ATHENA универсальна по отношению к источнику данных. Например, в качестве источника может быть файловое хранилище, другая система интегрированная по API, антиспам система, межсетевой экран, различные виды трафика: сетевой, почтовый или веб-трафик.

Авторы использовали API AVSOFT ATHENA для расширения поведенческой аналитики и проверили работоспособность компонента под операционной системой Astra Linux.

Для решения задачи расширения поведенческой аналитики, поведение объектов информационного взаимодействия рассматривалось как случайный процесс с разверткой во времени. При этом анализировалась информация по различным критериям согласно требуемому функционалу. Для каждого объекта информационного взаимодействия формируется многомерная случайная величина размерности равной количеству анализируемых критериев.

Для упрощения модели каждый объект информационного взаимодействия рассматривался как незначительно зависящий от других объектов и процессов при длительном интервале наблюдения. Такие процессы описываются нормальным распределением Гаусса [18]:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}},$$

где μ −математическое ожидание (среднее значение), медиана распределения, σ −среднеквадратическое отклонение, σ^2 −дисперсия распределения.

Для анализа поведения объектов информационного взаимодействия используется многомерная модель распределения Гаусса (GMM). Это позволяет выполнить моделирование распределения согласно критериям набора функций типичного поведения объектов информационного взаимодействия и осуществить независимое измерение нормальности их поведения. Использование такой модели поведенческой аналитики предпочтительнее дискриминационного метода, например, на основе опорных векторов (SVM). Модель на основе опорных векторов оптимизируется для разделения нескольких классов, причём второй класс должен быть указан явно. Такую модель затруднительно применить в случае многоклассовой среды (например, пытаясь отличить поведение произвольного программного кода при динамическом анализе от другого кода). Из-за отсутствия описания класса кода нарушителя до проведения атаки, такую модель довольно трудно оптимизировать. Факт вероятной атаки можно обнаружить как выявление аномалий в поведении объектов информационного взаимодействия при динамическом анализе.

Выбранная авторами генеративная вероятностная модель дает возможность производить обучение (формирование) по массиву данных самостоятельно. Считается, что GMM в генеративном классе моделей является одной из самых надежных и доступных. Частным случаем GMM является алгоритм K-Means, где ковариационные матрицы гауссовых подмоделей ограничены диагональю (идеально сферической). В GMM ковариационные матрицы не имеют ограничений, кроме полного ранга. Это означает, что со временем изменяются не только оценки средних значений модели, но и форма овалов, которые концептуально представляют собой ковариационные матрицы. Для

подсистемы поведенческой аналитики системы защиты от целенаправленных атак использовалась стандартная многомерная гауссовская модель:

$$p(\mathbf{x}|\boldsymbol{\theta}) = \frac{1}{(2\pi)^{d/2}\sqrt{|\boldsymbol{\Sigma}|}} \exp\left(-\frac{1}{2}(\mathbf{x}-\boldsymbol{\mu})\boldsymbol{\Sigma}^{-1}(\mathbf{x}-\boldsymbol{\mu})^{\top}\right),$$

$$q(\mathbf{x}|\boldsymbol{\Theta}) = \sum_{i=1}^{k} \pi_i p(\mathbf{x}|\boldsymbol{\theta}_i),$$

где $\boldsymbol{\theta}_i = \{\mu_i, \Sigma_i\}$ и π_i коэффициент смешивания, а $q(\mathbf{x}|\boldsymbol{\theta}_i)$ необходимо для представления функции правдоподобия GMM.

Вычисление параметров Θ осуществлялось с помощью оптимизации вышеуказанных формул с применением алгоритма максимизации ожидания. В состав этого алгоритма включено определение $q(\mathbf{x}|\boldsymbol{\theta}_i)$, то есть ожидаемого значения по всем данным поведенческой аналитики и вычисление производной этой функции по параметрам Θ = {μ, Σ, π} с инициализацией нулевым значением этой функции. В результате вычислений можно получить направление градиента функции. Далее меняются параметры так, что они позволяют осуществлять движение в направлении этого градиента. Процесс повторяется до тех пор, пока не будет достигнут предел улучшения. Для оценки параметров использовалась стандартная методика максимизации ожиданий. В программной реализации алгоритма использованы правила обновления подмоделей GMM.

Если $\tau_{n,k}^{(t)}$ это вероятность, что *k*-й подмодели GMM принадлежит выборка $\mathbf{x}_n$, то при оценке времени *t* правила для обновления параметров GMM будут следующие:

$$\tau_{n,i}^{(t)} = \frac{\pi_i N\left(\left(\mathbf{x}_n \middle| \boldsymbol{\mu}_i^{(t)}\right), \boldsymbol{\Sigma}_i^{(t)}\right)}{\sum_j \pi_j N\left(\left(\mathbf{x}_n \middle| \boldsymbol{\mu}_j^{(t)}\right), \boldsymbol{\Sigma}_j^{(t)}\right)},$$

$$\pi_i^{(t+1)} = \frac{\sum_n \tau_{n,i}^{(t)}}{N}, \quad \boldsymbol{\mu}_i^{(t+1)} = \frac{\sum_n \tau_{n,i}^{(t)} \mathbf{x}_n}{\sum_n \tau_{n,i}^{(t)}},$$

$$\boldsymbol{\Sigma}_i^{(t+1)} = \frac{\sum_n \tau_{n,i}^{(t)} \left(\mathbf{x}_n - \boldsymbol{\mu}_i^{(t+1)}\right)\left(\mathbf{x}_n - \boldsymbol{\mu}_i^{(t+1)}\right)^{\top}}{\sum_n \tau_{n,i}^{(t)}}.$$

Эти параметры являются итеративными и обновляются с использованием приведенных выше уравнений до тех пор, пока не исчезнет улучшение распределения $\{\boldsymbol{\mu}_1, \boldsymbol{\mu}_2, \ldots, \boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2, \ldots, \pi_1, \ldots\}$ правдоподобия $q(\mathbf{x}|\boldsymbol{\theta}_i)$.

Несмотря на то, что алгоритм GMM изначально не создавался для использования в поведенческой аналитике и не оптимизировался для разделения объектов информационного взаимодействия на несколько классов, он хорошо работает в сравнении с альтернативами на основе SVM, использующих разделение на два класса. Приведенный алгоритм показал свою работоспособность для решения проблемы моделирования поведения различных объектов информационного взаимодействия.

Для вынесения вердикта об опасности объекта информационного взаимодействия использовалась стандартная для AVSOFT ATHENA 10-ти бальная шкала баллов для вынесения вердиктов (таблица).

Таблица

Соответствие вердикта количеству баллов

Table

Correspondence of the verdict to the number of points

Баллы	Вердикт	Правило соответствия
1–3	Безопасный	Минимальный вес индикатора, который показывает самый низкий уровень опасности, равен 1 баллу. Максимальный вес индикатора, который показывает самый высокий уровень опасности, равен 10 баллам.
4–7	Подозрительный	
8–10	Вредоносный	

Таким образом формируются 3 вида вердиктов для объектов информационного взаимодействия:

1) Безопасный. В поведении обнаружены только безопасные индикаторы, без признаков присутствия подозрительных или вредоносных индикаторов.

2) Подозрительный. В поведении обнаружены подозрительные индикаторы, и объект не может считаться безопасным.

3) Вредоносный. В поведении обнаружены индикаторы, которые явно указывают на вредоносные действия объекта.

Предлагаемый авторами алгоритм поведенческой аналитики для системы защиты от целенаправленных атак реализован с применением API программной платформы «Система защиты от целенаправленных атак AVSOFT ATHENA» в среде операционных системы Astra Linux Special Edition «Воронеж».

ЗАКЛЮЧЕНИЕ

Проведенные авторами исследования показали целесообразность применения комплексных методов к защите информации информационной инфраструктуры компании с необходимостью учета как объектов информационного взаимодействиях, так и учета человеческого фактора. Важным компонентом современных систем безопасности является поведенческая аналитика, которая может быть применена к различным объектам информационного взаимодействия. Авторы предлагают для системы защиты от целенаправленных атак при анализе поведения объектов информационного взаимодействия использовать многомерную модель распределения Гаусса (GMM). Ее применение позволило осуществить моделирование распределения согласно критериям набора функций типичного для поведения объектов информационного взаимодействия и осуществить измерение по десятибалльной шкале нормальности их поведения в системе защиты от целенаправленных атак AVSOFT ATHENA под управлением Astra Linux Special Edition «Воронеж».

Список литературы

1. Осипов В.Ю., Юсупов Р.М. Информационный вандализм, криминал и терроризм как современные угрозы обществу // Тр. СПИИРАН, 8 (2009). – С. 34-45.

2. Фалеев М.И., Черных Г.С. Угрозы национальной безопасности государства в информационной сфере. – 2014. – Т. 4. – № 1(6). – URL: https://iee.unn.ru/wp-content/uploads/sites/9/2018/02/2.Inf.ugrozy-vred.programmykomp.prestupleniya.pdf (дата обращения: 10.07.2024).

3. Семененко В.А. Информационная безопасность // М.: МГИУ, 2011. – 277 с.

4. Шаньгин В.Ф. Информационная безопасность и защита информации // М.: ДМК, 2014. – 702 с.

5. Five styles of advanced threat defense. – Gartner Research, 2013. URL: https://www.gartner.com/en/documents/2576720 (дата обращения: 04.07.2024).

6. Системы поведенческой аналитики пользователей и сущностей (UEBA). URL: https://www.anti-malware.ru/security/user-and-entity-behavior-analytics (дата обращения: 06.02.2024).

7. Как системы безопасности анализируют поведение пользователей: «подводные камни» и специфика решений UBA. – Tadviser, 2019. URL:

https://www.tadviser.ru/index.php/Статья:UBA_(User_Behavior_Analytics,_Анализ_поведения_в_сфере_систем_обеспечения_безопасности) (дата обращения: 12.02.2024).

8. Обзор рынка систем поведенческого анализа – User and Entity Behavioral Analytics (UBA/UEBA). – Anti-Malware, 2017. URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba (дата обращения: 19.07.2024).
9. Методический документ. Методика оценки угроз безопасности информации. – М.: ФСТЭК России, 2021. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (дата обращения: 03.07.2024).
10. ГОСТ Р 50922-96. Защита информации. Основные термины и определения. – М.: Госстандарт России, 1996. URL: https://docs.cntd.ru/document/1200004674 (дата обращения: 22.07.2024)
11. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. URL: https://docs.cntd.ru/document/1200084141 (дата обращения: 22.07.2024)
12. Prokhorenkova L., Gusev G., Vorobev A., Dorogush A.V., Gulin A. CatBoost: unbiased boosting with categorical features. Yandex, Moscow, 2019.
13. Siris V.A., Papagalou F. Application of anomaly detection algorithms for detecting SYN flooding attacks. Computer Communications. – 2006. – 29.
14. Ahmed T., Oreshkin B., Coates M. Machine Learning Approaches to Network Anomaly Detection. Second Workshop on Tackling Computer Systems Problems with Machine Learning Techniques. 2007, Cambridge
15. Shabtai A., Kanonov U., Elovici Yu., Glezer Ch., Weiss Ya. Andromaly: a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems, 2010.
16. Kou Yu., Lu Ch.-T., Sinvongwattana S., Huang Yo.-P. Survey of Fraud Detection Techniques. International Conference on Networking, 2004.
17. Mishra A., Nadkarni K., Patcha A. Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications, 2004.
18. Song Y., Salem M.B., Hershkop S. System Level User Behavior Biometrics using Fisher Features and Gaussian Mixture Models // IEEE Security and Privacy Workshops. - New York, USA: IEEE, 2013. – P. 52-59.

References

1. Osipov V.Yu., Yusupov R.M. Information vandalism, crime and terrorism as modern threats to society // Tr. SPIIRAN, 8 (2009). – pp. 34-45.
2. Faleev M.I., Chernykh G.S. Threats to the national security of the state in the information sphere. – 2014. – Volume 4. – No. 1(6). – URL: https://iee.unn.ru/wp-content/uploads/sites/9/2018/02/2.Inf.ugrozy-vred.programmykomp. prestupleniya.pdf (access date: 10.07.2024).
3. Semenenko V.A. Information security // M.: MGIU, 2011. – 277 p.
4. Shangin V.F. Information security and information protection // M.: DMK, 2014. – 702 p.
5. Five styles of advanced threat defense. – Gartner Research, 2013. URL: https://www.gartner.com/en/documents/2576720 (access date: 04.07.2024).
6. User and Entity Behavioral Analytics (UEBA) systems. URL: https://www.anti-malware.ru/security/user-and-entity-behavior-analytics (access date: 06.02.2024).
7. How security systems analyze user behavior: pitfalls and specifics of UBA solutions. – Tadviser, 2019. URL: https://www.tadviser.ru/index.php/Статья:UBA_(User_Behavior _Analytics,_Анализ_поведения_в_сфере _систем_обеспечения_безопасности) (access date: 12.02.2024).
8. Market overview of behavioral analysis systems – User and Entity Behavioral Analytics (UBA/UEBA). – Anti-Malware, 2017. URL: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba (access date: 19.07.2024).
9. Methodological document. Methodology for assessing threats to information security. – M.: FSTEC of Russia, 2021. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/metodicheskij-dokument-ot-5-fevralya-2021-g (access date: 03.07.2024).
10. GOST R 50922-96. Data protection. Basic terms and definitions. – M.: Gosstandart of Russia, 1996. URL: https://docs.cntd.ru/document/1200004674 (access date: 22.07.2024)
11. GOST R ISO/IEC 27005-2010. Information technology. Methods and means of ensuring security. Information security risk management. URL: https://docs.cntd.ru/document/1200084141 (access date: 22.07.2024)
12. Prokhorenkova L., Gusev G., Vorobev A., Dorogush A.V., Gulin A. CatBoost: unbiased boosting with categorical features. Yandex, Moscow, 2019.

13. Siris V.A., Papagalou F. Application of anomaly detection algorithms for detecting SYN flooding attacks. Computer Communications. – 2006. – 29.

14. Ahmed T., Oreshkin B., Coates M. Machine Learning Approaches to Network Anomaly Detection. Second Workshop on Tackling Computer Systems Problems with Machine Learning Techniques. 2007, Cambridge

15. Shabtai A., Kanonov U., Elovici Yu., Glezer Ch., Weiss Ya. Andromaly: a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems, 2010.

16. Kou Yu., Lu Ch.-T., Sinvongwattana S., Huang Yo.-P. Survey of Fraud Detection Techniques. International Conference on Networking, 2004.

17. Mishra A., Nadkarni K., Patcha A. Intrusion detection in wireless ad hoc networks. IEEE Wireless Communications, 2004.

18. Song Y., Salem M.B., Hershkop S. System Level User Behavior Biometrics using Fisher Features and Gaussian Mixture Models // IEEE Security and Privacy Workshops. – New York, USA: IEEE, 2013. – P. 52-59.

Лазарев Сергей Александрович, кандидат экономических наук, доцент, заведующий лабораторией прикладного системного анализа и информационных технологий
Рубцов Константин Анатольевич, кандидат технических наук, заведующий учебно-научной лаборатории информационно-измерительных и управляющих комплексов и систем

Lazarev Sergey Alexandrovich, Candidate of Economic Sciences, Assistant professor, Head of the Laboratory of Applied System Analysis and Information Technologies
Rubtsov Konstantin Anatolievich, Candidate of Technical Sciences, Head of the Educational and Scientific Laboratory of Information, Measuring and Control Complexes and Systems