ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ

УДК 004.89 Обзорная статья
DOI: 10.35330/1991-6639-2024-26-4-62-70
EDN: MJSYHZ

Разработка программных средств для автоматизации процесса мониторинга и анализа данных, поступающих в мониторинговый центр оператора системы безопасности

О. А. Ширко[1], И. С. Османов[2]

[1]Российский экономический университет им. Г. В. Плеханова
117997, Россия, Москва, Стремянный переулок, 36
[2]Московский государственный технический университет им. Н. Э. Баумана
105005, Россия, Москва, 2-я Бауманская улица, 5

Аннотация. Статья посвящена исследованию программных средств для автоматизации процесса мониторинга и анализа данных, поступающих в мониторинговый центр оператора системы безопасности. Обоснованы актуальность и значимость темы исследования. Дается краткое обоснование роли процесса мониторинга и анализа данных, которые поступают в центр системы безопасности. Методы исследования основаны на использовании данных анализа мониторинга, получаемых от систем сбора информации в самых различных областях. В настоящее время накоплен достаточно широкий спектр программных средств для автоматизации процесса мониторинга, обеспечивающих обслуживаемость и своевременное реагирование на определенные события. В работе автором доказано, что автоматизация позволяет специалистам работать быстрее, гибче и продуктивнее – от повышения безопасности системы до улучшения взаимодействия с клиентами. Сделан вывод, что внедрение облачной системы автоматизации является необходимым условием для реализации современных систем обеспечения безопасности. Внедрение подобных систем позволит значительно снизить риски возникновения опасных ситуаций и время реагирования на них без необходимости повышения расходов на безопасность организации в целом.

Ключевые слова: система мониторинга, системы безопасности, анализ данных, мониторинговый центр, оператор системы, автоматизация безопасности, разработка программных средств, угрозы

Поступила 10.04.2024, одобрена после рецензирования 28.05.2024, принята к публикации 10.07.2024

Для цитирования. Ширко О. А., Османов И. С. Разработка программных средств для автоматизации процесса мониторинга и анализа данных, поступающих в мониторинговый центр оператора системы безопасности // Известия Кабардино-Балкарского научного центра РАН. 2024. Т. 26. № 4. С. 62–70. DOI: 10.35330/1991-6639-2024-26-4-62-70

MSC: 00A72 Review article

Development of software tools for automating the process of data monitoring and analyzing received by the monitoring center of the security system operator

O.A. Shirko[1], I.S. Osmanov[2]

[1]Plekhanov Russian University of Economics
117997, Russia, Moscow, 36 Stremyannyy lane
[2]Moscow State Technical University named after N.E. Bauman
105005, Russia, Moscow, 5, 2nd Baumanskaya street

Abstract. The article is devoted to the study of software tools for automatizing the process of data monitoring and analyzing received by the monitoring center of the security system operator. The relevance and significance of the research topic is substantiated. A brief justification is given for the role of the process of data monitoring and analyzing that is received by the security system center. The research methods are based on the use of monitoring analysis methods obtained from information collection systems in a wide variety of fields. Currently, a fairly wide range of software tools has been accumulated to automate the monitoring process, ensuring serviceability and timely response to certain events. In the work, the author proves that automation allows specialists to work faster, more flexibly and more productively – from improving system security to improving customer interaction. It is concluded that the introduction of a cloud automation system is a prerequisite for the implementation of modern security systems. The introduction of such systems will significantly reduce the risks of dangerous situations and the response time to them without the need to increase the cost of security of the organization as a whole.

Keywords: monitoring system, security systems, data analysis, monitoring center, system operator, security automation, software development, threats

Submitted 10.04.2024, approved after reviewing 28.05.2024, accepted for publication 10.07.2024

For citation. Shirko O.A., Osmanov I.S. Development of software tools for automating the process of data monitoring and analyzing received by the monitoring center of the security system operator. *News of the Kabardino-Balkarian Scientific Center of RAS.* 2024. Vol. 26. No. 4. Pp. 62–70. DOI: 10.35330/1991-6639-2024-26-4-62-70

Введение

Организации всегда стремились обеспечить надежную, безопасную и эффективную работу своей ИТ-инфраструктуры. Разрушительные последствия успешных нарушений безопасности, которые наблюдались в последнее время, заставили все больше и больше предприятий по разработке программного обеспечения сместить свое внимание на создание программных продуктов с высокой степенью безопасности (т. е. без уязвимостей) с нуля. Для создания безопасных программных приложений требуются соответствующие механизмы, позволяющие руководителям проектов и разработчикам отслеживать уровень безопасности своих продуктов во время их разработки, а также выявлять и устранять уязвимости до их выпуска.

В свою очередь, как очень точно указывают Ю. Лиу и Т. Жи, внедрение автоматизированных процедур безопасности стало необходимостью для предприятий, выполняющих крупномасштабное развертывание программного обеспечения в облаке. Лучшее понимание этого явления помогает принимать более обоснованные решения в области обеспечения безопасности на всех уровнях [1].

Более того, автоматизация безопасности позволяет выявлять входящие угрозы, сортировать и расставлять приоритеты предупреждений по мере их появления, а также выполнять автоматическое реагирование на инциденты.

Основная часть

В современную цифровую эпоху роль операторов службы безопасности как никогда важна. Будь то мониторинг камер наблюдения, управление системами контроля доступа или реагирование на сигналы тревоги, их задачи многогранны и часто требуют быстрого и точного принятия решений. Однако ландшафт операций по обеспечению безопасности быстро развивается благодаря автоматизации. Рассмотрим три важных способа, которыми автоматизация меняет методы работы операторов безопасности:

- Расширенное наблюдение и снижение количества ручных задач.
- Унифицированные процессы.
- Эффективная обработка сигналов тревоги и своевременное реагирование на инциденты.

Применение систем автоматизации позволяет заметно повысить эффективность работы операторов [2]. Представим систему безопасности, которая никогда не спит, неустанно следит за помещениями и мгновенно выявляет потенциальные угрозы, – так автоматизация наблюдения и обнаружения угроз революционизирует индустрию безопасности. Традиционно перед операторами службы безопасности стояла сложная задача ручного мониторинга множества камер наблюдения, что не только требовало больших ресурсов, но и чревато человеческими ошибками. Автоматизация же использует возможности искусственного интеллекта (ИИ) и машинного обучения для анализа видеопотоков в режиме реального времени.

Алгоритмы распознавания образов на основе систем ИИ могут достаточно быстро обнаружить аномалии, такие как несанкционированный доступ, необычное поведение или даже брошенные предметы с точностью, превышающей эффективность работы оператора [3]. При обнаружении таких аномалий система немедленно оповещает оператора службы безопасности, обеспечивая быстрое реагирование. Более того, в современной научно-исследовательской литературе обнаруживаются доказательства, для анализа событий ИИ использует различные стратегии для сокращения времени реагирования, включая следующие: интеллектуальный анализ данных об инцидентах безопасности; присвоение оценок рисков; кластеризация по общим признакам; дифференциация и приоритизация отдельных классов рисков; сортировка уведомлений аналитикам-людям; рекомендации по реагированию или мерам устранения; автоматизация задач сдерживания – все это примеры мероприятий по сдерживанию. Кроме того, автоматизация может выходить за рамки простого обнаружения аномалий путем анализа поведения человека [4]. Например, она может выявлять людей, находящихся в непосредственной близости в зонах ограниченного доступа или хаотично перемещающихся, помогая операторам сосредоточиться на потенциальных угрозах, а не просматривать многочасовой отснятый материал.

В постоянно меняющемся ландшафте физической безопасности операционные центры безопасности играют ключевую роль в защите организаций от угроз. Сотрудники операционного центра безопасности сталкиваются с постоянным потоком тревог и инцидентов, требующих быстрого и точного реагирования. Автоматизация становится все более необходимой в этой области, поскольку она упрощает операции и обеспечивает соблюдение стандартизированных процессов, предлагая надежное решение проблем, с которыми сталкиваются профессионалы в области безопасности.

Вышесказанное позволяет заключить, что одним из основных преимуществ разработки программных средств для автоматизации процесса мониторинга и анализа данных, поступающих в мониторинговый центр оператора системы безопасности, является ее способность применять стандартизированные процедуры для обеспечения согласованности при обработке сигналов тревоги. Независимо от источника тревоги или местоположения автоматизация гарантирует, что каждое предупреждение обрабатывается единообразно в соответствии с заранее установленными протоколами. Такая согласованность предотвращает ошибки или оплошности при срабатывании сигнализации, особенно в ситуациях с высокими ставками.

Современные системы автоматического обеспечения безопасности предполагают последовательное выполнение установленного плана реагирования при обнаружении ка-

кого-либо из описанных инцидентов [6]. В этом случае срабатывает одно и то же систематическое, хорошо продуманное реагирование, будь то оповещение низкого уровня или потенциально критическое нарушение. Это сводит к минимуму риск человеческой ошибки и гарантирует, что каждый инцидент устраняется быстро и эффективно.

Так, к примеру, разработка программных средств для автоматизации процесса мониторинга и анализа данных, поступающих в мониторинговый центр оператора системы безопасности с помощью IBM Instana Observability, предоставляет автоматизированные возможности мониторинга, оповещения и исправления на базе ИИ, обеспечивающие беспрецедентный доступ к сложным распределенным приложениям, службам и компонентам инфраструктуры в режиме реального времени. Сюда входят серверы, контейнеры, базы данных и многое другое, поэтому у команд есть все данные и контекст, необходимые для предотвращения простоев, оптимизации использования ресурсов и повышения общей производительности и удобства работы пользователей.

В быстро развивающемся мире мониторинга облачной инфраструктуры постоянно разрабатываются новые инструменты. Программа должна иметь возможность собирать данные из различных источников, таких как видеокамеры, датчики движения, датчики дыма и т. д. Затем она должна анализировать эти данные, определять потенциальные угрозы и предупреждать операторов о возможных проблемах. Кроме того, программа должна иметь функцию хранения и архивирования данных для последующего анализа и использования в расследованиях инцидентов. Такая программа позволит операторам системы безопасности быстро реагировать на потенциальные угрозы и повысит эффективность работы мониторингового центра.

Так, программы для автоматизации процесса мониторинга обычно разрабатываются с использованием специальных инструментов и технологий, таких как мониторинг производительности приложений (APM), мониторинг инфраструктуры, управление событиями и т. д. Разработка таких программ включает в себя определение требований, анализ процессов мониторинга, проектирование архитектуры, программирование, тестирование и внедрение.

Обсуждение

В настоящее время на рынке представлено множество инструментов мониторинга облачной инфраструктуры, каждый из которых обладает уникальным набором функций, поэтому важно понимать конкретные потребности (например, Instana, Dynatrace, Azure Monitor, Amazon CloudWatch, Elastic Observability, Pre Crimes, Лавина, Human Risk).

Остановимся более подробно на Instana – это платформа для мониторинга и анализа производительности приложений, которая работает на основе ИИ и автоматически обнаруживает проблемы производительности. Instana играет важную роль в автоматизации процесса мониторинга, так как позволяет быстро выявлять и устранять проблемы, улучшать производительность приложений и обеспечивать надежную работу IT-инфраструктуры. С помощью Instana можно отслеживать метрики производительности, а также получать уведомления о возможных проблемах для оперативного реагирования.

Карта инфраструктуры Instana предоставляет обзор всех контролируемых систем, что позволяет легко визуализировать каждый аспект инфраструктуры приложения. Каждый блок в столбцах представляет программные компоненты, работающие в этой системе, и меняет цвет в зависимости от любых инцидентов, событий или изменений (рис. 1).

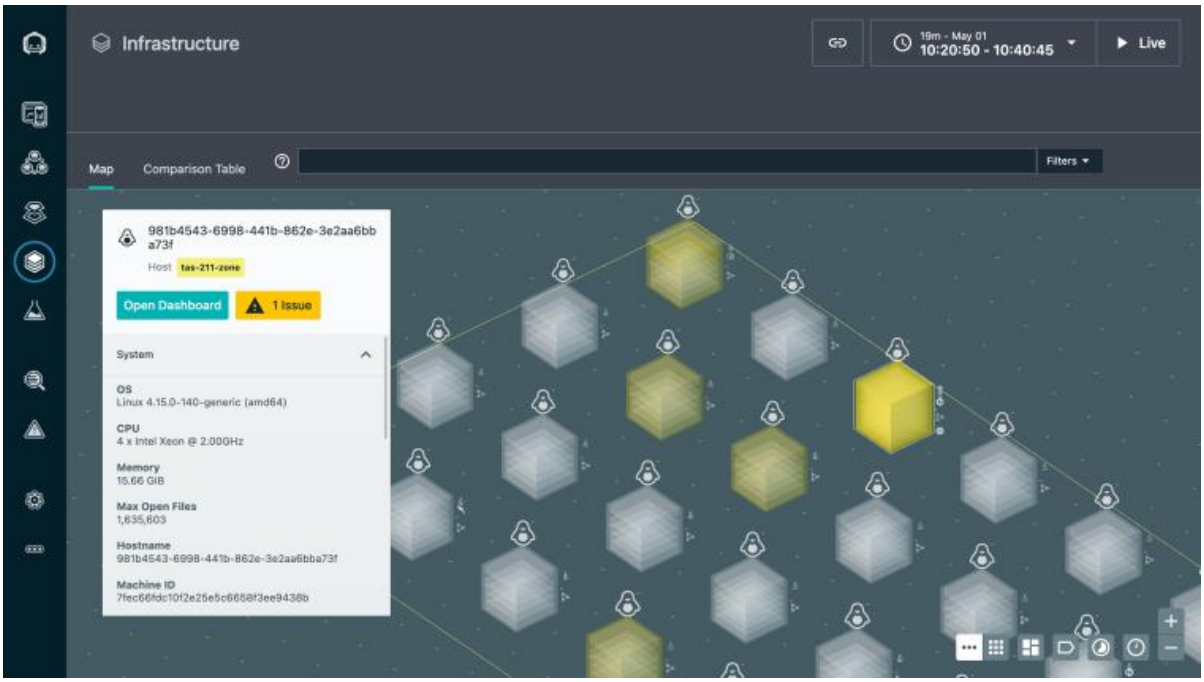

Рис. 1. *Карта инфраструктуры Instana [5]*

Fig. 1. *Infrastructure map Instana [5]*

Сравнительная таблица позволяет легко и быстро определить компоненты приложения, которые имеют решающее значение для производительности приложения или службы. Можно сортировать по таким показателям, как использование ЦП или потребление памяти, и сравнивать показатели с течением времени, чтобы легко определить, улучшают или ухудшают производительность новые изменения или развертывания (рис. 2).

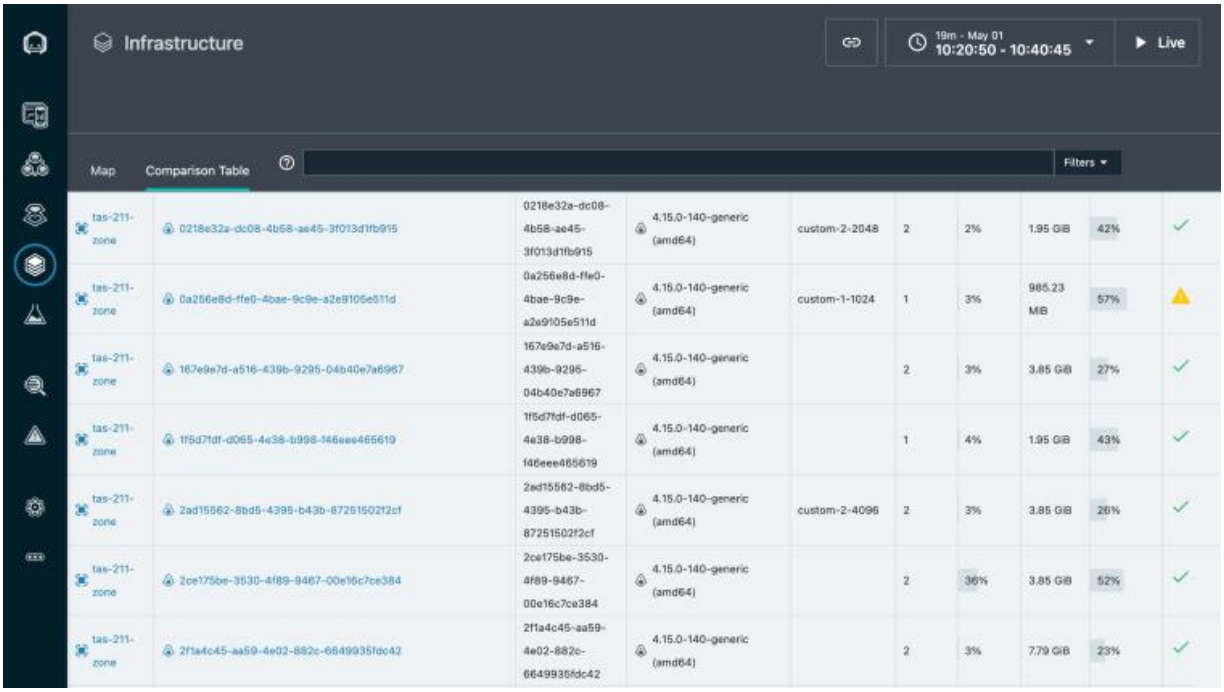

Рис. 2. *Сравнительная таблица [5]*

Fig. 2. *Comparative table [5]*

Панель контекстного руководства Instana отображает все взаимозависимости между облаком, инфраструктурой и компонентами приложения. Это помогает сразу понять восходящие и нисходящие зависимости всякий раз, когда в приложении или компоненте возникает проблема (рис. 3).

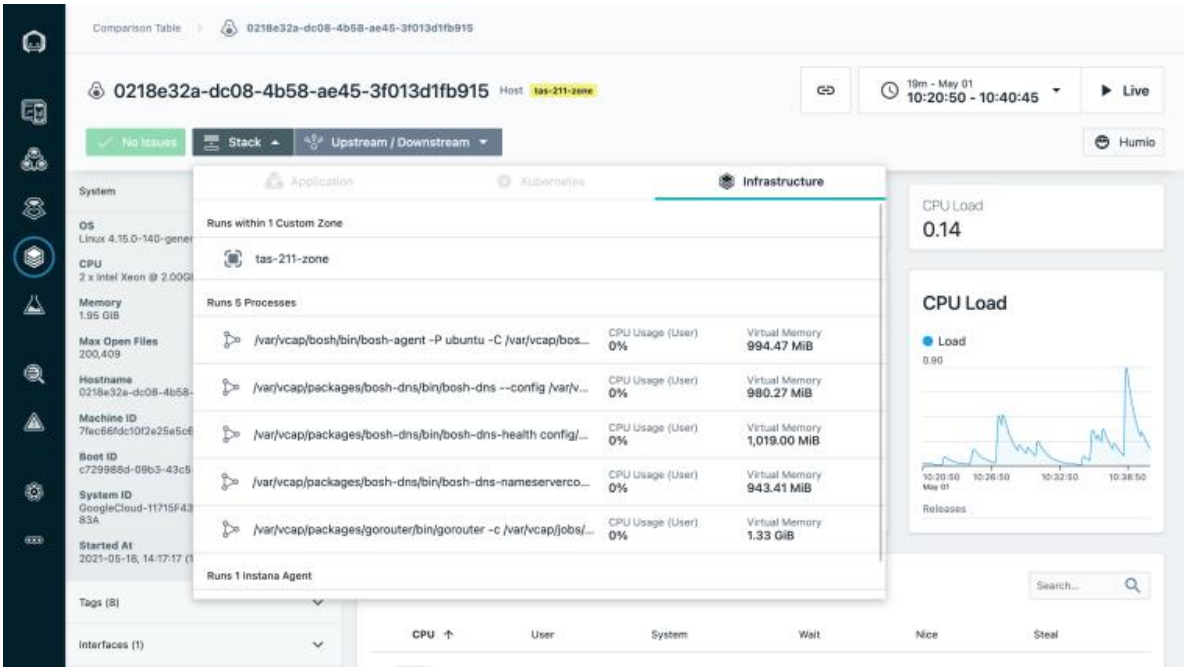

Рис. 3. *Панель контекстного руководства Instana [5]*

Fig. 3. *Contextual Guide Panel Instana [5]*

Разработка программного средства должна предоставлять инструменты для мониторинга и контроля состояния безопасности нескольких процессов управления и выполнять сбор и агрегацию данных из различных смежных систем. Карта инфраструктуры Instana предоставляет обзор всех отслеживаемых систем, что позволяет легко визуализировать каждый аспект инфраструктуры приложения. Каждый блок в компонентах pillars представляет программные компоненты, работающие в данной системе, и будет менять цвет для отражения любых инцидентов, событий или изменений. Облачный мониторинг представлен на рис. 4.

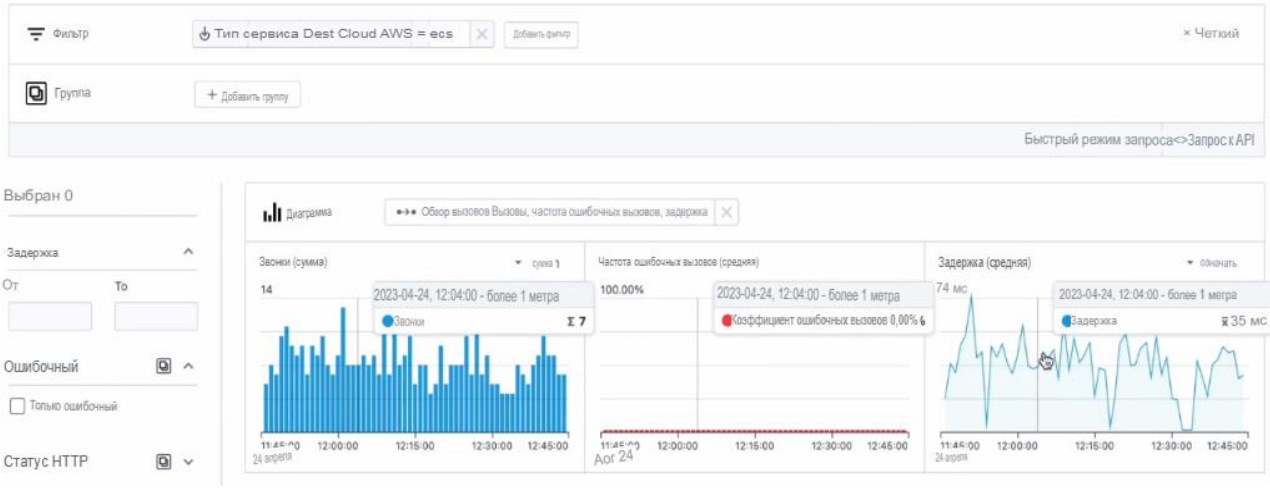

Рис. 4. *Облачный мониторинг инфраструктуры Instana [5]*

Fig. 4. *Cloud monitoring of Instana infrastructure [5]*

Отметим, что Instana обеспечивает автоматизированный мониторинг инфраструктуры в режиме реального времени с детализацией показателей за 1 секунду в нескольких облаках и локальных средах для обеспечения точности полного стека в любое время. От администратора или пользователя не требуется специальных знаний, сложной настройки или написания программного кода. Эта программа разработана для упрощения работы специалистов по безопасности. Ее цель – автоматизировать процессы и облегчить задачи команды. Основная трудность при подготовке операторов связана с устоявшимся мнением, что приобретение аппаратуры и программного обеспечения не требует дополнительных вложений, связанных с обучением специалистов. При этом стоит учитывать, что достаточно специфическая система мониторинга все же требует некоторой дополнительной подготовки. Тем более, в отличие от базовых навыков работы на ПК навыки согласованного поведения в критических ситуациях приобретаются лишь в ходе оперативного решения подобных ситуаций.

Результаты

Современные системы в своей автоматизации зашли так далеко, что в состоянии самостоятельно выполнять большинство функций. К примеру, кроме рассматриваемой Instana, такие системы, как Pre Crimes, «Лавина» или Human Risk, тоже успели хорошо себя зарекомендовать.

Стоит сказать, что Checkmk, так же, как и Instana, – это надежный инструмент, специализирующийся на комплексном мониторинге ИТ-инфраструктуры. Он охватывает не только серверы и приложения, но также распространяется на сети, контейнеры, облака и среды Интернета вещей, что оправдывает его «лучшее качество» для комплексного мониторинга ИТ-инфраструктуры. Функция автоматического обнаружения Checkmk особенно ценна, поскольку она автоматически идентифицирует и отслеживает новые компоненты в инфраструктуре. Кроме того, консоль событий эффективно управляет оповещениями и сопоставляет их, позволяя быстрее решать проблемы. Что касается интеграции, Checkmk поддерживает широкий спектр технологий, в том числе технологии AWS, Microsoft Azure, Google Cloud, Kubernetes, Docker и другие [6].

К плюсам работы с современными автоматизированными системами видеоанализа можно отнести то, что операторы не устают, у них не притупляется внимание, они не отвлекаются, четко работают по заданным алгоритмам, не отступая от них ни на шаг и не проявляя инициативы и самодеятельности. Стоит сказать, что на данном этапе даже самые совершенные системы являются всего лишь помощниками операторов. Кроме того, необходимость анализа информации, быстрого принятия оперативных решений, руководства оперативными подразделениями, в том числе в экстремальных ситуациях – все эти задачи по-прежнему лежат на человеке. А автоматизированные системы всего лишь позволяют снять с оператора часть нагрузки. Последнее, правда, не означает, что взамен снятой нагрузки оператора можно и нужно озадачить какой-либо другой работой. В таком случае особенности человеческой психики просто не позволят ему сразу включиться в выполнение своей основной задачи.

Следует заметить, что преимущества стандартизированных процессов, которым способствует автоматизация, выходят за рамки реагирования на инциденты и упрощения обучения и адаптации. Они также значительно упрощают обучение и адаптацию нового персонала мониторингового центра оператора системы безопасности. Когда процедуры согласованы и автоматизированы, новым сотрудникам команды легче понять, как эффективно управлять сигнализациями. Сокращается время обучения, и каждый может быстро освоить лучшие практики. Благодаря автоматизации процесса мониторинга и анализу данных новые сотрудники получают хорошо структурированную автоматизированную

систему, которая помогает им на каждом этапе реагирования на инциденты. Они могут учиться на практике, следуя установленным протоколам, не упуская важных деталей. Это повышает их квалификацию и гарантирует, что они с первого дня будут придерживаться установленных стандартов безопасности.

Автоматизация увеличивает возможности процесса мониторинга и анализа данных, поступающих в мониторинговый центр оператора системы безопасности, позволяя ему достигать большего с помощью имеющихся ресурсов. Это дает возможность аналитикам безопасности сосредоточиться на критических задачах, требующих вмешательства человека, таких как принятие сложных решений и адаптация к новым угрозам. Напротив, рутинные и повторяющиеся задачи автоматизированы до совершенства.

Разработка программных средств для автоматизации процесса мониторинга и анализа данных сокращает количество ложных срабатываний, которые операторы должны расследовать. Автоматизация также играет решающую роль в эскалации инцидентов. Автоматизация может выполнить заранее определенный набор действий в ответ на подтвержденный сигнал тревоги, включая анализ и интерпретацию информационных источников об угрозах, обновление запросов, отправку уведомлений по электронной почте, расследование инцидентов собиранием и анализом журналов, а также устранение предупреждений. Более того, автоматизация идет рука об руку с оптимизацией ресурсов. Это помогает организациям наиболее эффективно использовать свои ресурсы за счет сокращения числа ложных срабатываний, автоматизации рутинных задач и предоставления возможностей оперативного обслуживания. Это позволяет персоналу сосредоточиться на более сложных задачах с добавленной стоимостью, экономя время и деньги при максимальном повышении эффективности групп управления сигнализацией.

Вышесказанное позволяет сделать объективное заключение о том, что роль операторов службы безопасности растет вместе с технологическими достижениями в области автоматизации. Эти три существенных изменения – улучшенное наблюдение и обнаружение угроз, унифицированные процессы за счет централизации в облаке и эффективная обработка сигналов тревоги – демонстрируют, как автоматизация упрощает их задачи и повышает общую безопасность. По мере развития технологий мы можем ожидать, что операции по обеспечению безопасности станут еще более эффективными и будут чутко реагировать на возникающие угрозы. Эти технологии предоставляют операторам инструменты, позволяющие опережать развивающиеся угрозы, оптимизировать управление данными и улучшить сотрудничество.

Заключение

Таким образом, внедрение автоматизации в службы безопасности позволяет обеспечить защиту физических активов и открыть новые возможности в области безопасности. Облачная централизация и автоматизация становятся неотъемлемой частью современных операций по обеспечению безопасности. Футурология в области безопасности предполагает, что будущее этой отрасли связано с автоматизацией, которая позволит повысить уровень безопасности.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

1. *Лиу Ю., Жи Т.* Система мониторинга и анализа данных DNS-сервера в режиме реального времени. Международный журнал инновационных компьютерных технологий и менеджмента. Том 13. № 4. 2017. С. 1425–1432.

Liu Y., Zhi T. Real-time DNS server data monitoring and analysis system. *Mezhdunarodnyy zhurnal innovatsionnykh komp'yuternykh tekhnologiy i menedzhmenta* [International Journal of Innovative Computer Technology and Management]. Vol. 13. No. 4. 2017. Pp. 1425–1432. (In Russian)

2. *Метени М.* Непрерывный мониторинг с использованием автоматизации. ScienceDirect, 2017. 287 с.

Metheny M. *Nepreryvnyy monitoring s ispol'zovaniyem avtomatizatsii* [Continuous monitoring using automation]. ScienceDirect, 2017. 287 p. (In Russian)

3. *Нгуен П., Грэм А.* Повышение безопасности с помощью автоматизации. Serious Edge. 2015. 320 с.

Nguyen P., Graham A. *Povysheniye bezopasnosti s pomoshch'yu avtomatizatsii* [Improving security with automation]. Serious Edge. 2015. 320 p. (In Russian)

4. *Панос К.* Автоматизация сбора информации об угрозах безопасности. “Options”, IEEE Security & Privacy. № 12. 2014. С. 42–51.

Panos K. Automating security threat intelligence collection. *“Options”, IEEE Security & Privacy*. No. 12. 2014. Pp. 42–51. (In Russian)

5. Карта инфраструктуры Instana // https://www.ibm.com/products (Дата обращения 29.05.2024).

Karta infrastruktury Instana [Instana instruction cards]. https://www.ibm.com/products (Accessed 05/29/2024). (In Russian)

6. 27 инструментов мониторинга облачной инфраструктуры, которые стоит изучить в 2024 году // https://thectoclub.com/ (Дата обращения 29.05.2024).

27 instrumentov monitoringa oblachnoy infrastruktury, kotoryye stoit izuchit' v 2024 godu [27 Cloud Infrastructure Monitoring Tools Worth Learning in 2024]. https://thectoclub.com / (Accessed 05/29/2024). (In Russian)

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts of interests.

Финансирование. Исследование проведено без спонсорской поддержки.

Funding. The study was performed without external funding.

Информация об авторах

Ширко Олег Анатольевич, аспирант, Российский экономический университет им. Г. В. Плеханова;
117997, Россия, Москва, Стремянный переулок, 36;
oleg.shirko@gmail.com
Османов Ислам Суадинович, студент, Московский государственный технический университет им. Н. Э. Баумана;
105005, Россия, Москва, 2-я Бауманская улица, 5;
destufnd@gmail.com

Information about the authors

Oleg A. Shirko, Post-graduate Student, Plekhanov Russian University of Economics;
117997, Russia, Moscow, 36 Stremyannyy lane;
oleg.shirko@gmail.com
Islam S. Osmanov, Student, Bauman Moscow State Technical University;
105005, Russia, Moscow, 5, 2nd Baumanskaya street;
destufnd@gmail.com