1 УДК 004.056.5

С. П. Киргизбаев [1], В. П. Киргизбаев [1], А. А. Бутин [1]

[1] Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

ПРИМЕНЕНИЕ SOAR-РЕШЕНИЙ ДЛЯ АВТОМАТИЗАЦИИ ПРОЦЕССОВ ВЫЯВЛЕНИЯ, АНАЛИЗА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ В КОРПОРАТИВНОЙ СЕТИ

Аннотация. В статье рассматриваются современные угрозы для цифровых активов бизнеса, включая кибератаки, внутренние угрозы и уязвимости программного обеспечения. В качестве решения этих проблем предлагается внедрение SOAR-платформ, предназначенных для автоматизации процессов выявления, анализа и реагирования на инциденты. Описываются ключевые функции SOAR-решений, такие как автоматизация рутинных задач, интеграция с системами безопасности, например, SIEM, а также стандартизация процессов реагирования. Приведён анализ как международных SOAR-решений (Palo Alto Cortex XSOAR, IBM Security QRadar SOAR, Fortinet FortiSOAR), так и отечественных (R-Vision SOAR, Security Vision SOAR, ePlat4m Orchestra). Отмечается, что автоматизация позволяет существенно сократить время реакции на инциденты, снизить риски, связанные с человеческим фактором, и улучшить координацию действий внутри компании. Интеграция с различными системами безопасности обеспечивает комплексный подход к защите цифровых активов. Кроме того, внедрение SOAR-решений способствует улучшению мониторинга и управления угрозами, предоставляя аналитические данные для прогнозирования возможных атак и повышения общей осведомленности о текущих рисках. Такие платформы обеспечивают централизованное управление инцидентами и позволяют проводить более эффективный анализ событий. В заключение подчёркивается значимость внедрения SOAR-платформ для повышения киберустойчивости организаций в условиях увеличения числа и сложности кибератак, а также необходимость постоянного совершенствования процессов кибербезопасности и адаптации к меняющимся угрозам.

Ключевые слова: информационная безопасность, SOAR-решение, цифровые активы, кибербезопасность, анализ киберинцидентов, автоматизация рутинных задач, интеграция.

S. P. Kirgizbaev [1], V. P. Kirgizbaev [1], A. A. Butin [1]

[1] Irkutsk State Transport University, Irkutsk, Russian Federation

APPLICATION OF SOAR SOLUTIONS FOR AUTOMATION OF INCIDENT DETECTION, ANALYSIS, AND RESPONSE PROCESSES IN A CORPORATE NETWORK

Abstract. The article discusses modern threats to digital business assets, including cyberattacks, internal threats, and software vulnerabilities. To address these challenges, the implementation of SOAR platforms is suggested to automate incident detection, analysis, and response. Key features of SOAR solutions include automation of routine tasks, integration with security systems like SIEM, and standardization of response processes. Both international SOAR solutions (Palo Alto Cortex XSOAR, IBM Security QRadar SOAR, Fortinet FortiSOAR) and domestic ones (R-Vision SOAR, Security Vision SOAR, ePlat4m Orchestra) are analyzed. Automation significantly reduces incident response time, minimizes human-related risks, and improves coordination within the company. Integration with various security systems provides a comprehensive approach to protecting digital assets. The adoption of SOAR solutions also enhances threat monitoring and management, providing data to predict potential attacks and increasing awareness of current risks. Such platforms offer centralized incident management and more efficient event analysis. In conclusion, the importance of implementing SOAR platforms to improve cyber resilience in the face of increasing and complex cyberattacks is highlighted, along with the need for continuous improvement of cybersecurity processes and adaptation to evolving threats.

Keywords: information security, SOAR solutions, digital assets, cybersecurity, cyber incident analysis, automation of routine tasks, integration.

Введение

Современный бизнес сталкивается с множеством угроз для своих цифровых активов. Одной из основных угроз являются кибератаки, которые могут включать вирусы, трояны, фишинг и атаки типа «отказ в обслуживании» (DDoS). Эти атаки могут привести к потере конфиденциальной информации, нарушению работы систем и значительным финансовым убыткам. Другой серьезной угрозой является внутренняя угроза. Сотрудники компании, имея доступ к важной информации, могут непреднамеренно или намеренно вызвать утечку данных.

Это может происходить из-за небрежности, недостатка знаний или злонамеренных действий. Внутренние угрозы особенно опасны, так как их сложнее выявить и предотвратить.

Кроме угроз своим цифровым активам бизнес должен учитывать риски, связанные с уязвимостями в программном обеспечении. Многие компании используют сторонние приложения и платформы, которые могут содержать уязвимости. Эти уязвимости могут быть использованы злоумышленниками для получения несанкционированного доступа к системам компании. Также стоит учитывать риски, связанные с использованием облачных сервисов. Несмотря на все преимущества, облачные технологии могут подвергаться различным видам атак, включая взлом учётных записей и перехват данных. Кроме того, компании могут сталкиваться с проблемами при обеспечении безопасности данных, хранящихся в облаке.

Для эффективного управления этими угрозами и рисками необходимо внедрение современных технологий и стратегий защиты. Одним из наиболее эффективных решений является использование SOAR-платформ, которые позволяют автоматизировать процессы выявления, анализа и реагирования на инциденты, обеспечивая таким образом надежную защиту цифровых активов [1]. SOAR, или Security Orchestration, Automation, and Response, представляет собой комплексный подход к управлению инцидентами информационной безопасности. Он объединяет в себе инструменты и процессы, направленные на автоматизацию реагирования на угрозы, что позволяет существенно ускорить и оптимизировать работу специалистов по кибербезопасности. Основные элементы SOAR-решения изображены на рисунке 1.

Рис. 1. Основные элементы SOAR-решения

Важным преимуществом SOAR-решений является их способность сокращать время между обнаружением инцидента и реагированием на него. Это достигается за счёт автоматизации рутинных задач, таких как сбор информации, анализ инцидентов и применение стандартных процедур реагирования [2]. Кроме того, SOAR позволяет интегрировать различные инструменты безопасности в единую платформу, что облегчает координацию действий и обмен информацией между разными системами и командами. SOAR-платформы также обеспечивают стандартизацию процессов реагирования. Благодаря заранее настроенным сценариям реагирования, компании могут быстро и эффективно справляться с инцидентами, минимизируя возможный ущерб. Стандартизация процессов помогает избежать ошибок и обеспечить соблюдение всех необходимых процедур. Кроме того, SOAR-решения способствуют улучшению взаимодействия между различными подразделениями. Платформа централизует управление инцидентами и обеспечивает доступ к информации для всех заинтересованных сторон. Это способствует более слаженной и координированной работе специалистов информационной безопасности.

Интеграция с существующими системами безопасности является одной из важнейших функциональных возможностей SOAR-решений. Эти платформы обеспечивают комплексное

взаимодействие с разнообразными инструментами и технологиями, уже используемыми в компании [3]. Одним из ключевых аспектов интеграции является совместимость SOAR-решений с системами управления событиями и информацией о безопасности (SIEM). SIEM собирает и анализирует данные о событиях безопасности в реальном времени. SOAR-решения дополняют этот процесс, автоматизируя реагирование на выявленные угрозы и координируя действия между различными системами. SOAR-платформы могут интегрироваться с антивирусными программами, системами обнаружения и предотвращения вторжений (IDS/IPS), а также с системами управления уязвимостями. Это позволяет создать единую экосистему безопасности, где все компоненты работают согласованно и эффективно. Интеграция обеспечивает быстрое и точное обнаружение угроз и их нейтрализацию.

Еще одним важным аспектом интеграции является взаимодействие с облачными сервисами и решениями для защиты данных. Современные компании часто используют облачные платформы для хранения и обработки информации. SOAR-решения могут интегрироваться с этими платформами, обеспечивая защиту данных как в локальной инфраструктуре, так и в облаке [4]. Это особенно важно в условиях растущего числа кибератак, нацеленных на облачные среды. Интеграция SOAR-решений с существующими системами безопасности также включает в себя поддержку различных протоколов и стандартов. Это позволяет обеспечить совместимость с широким спектром устройств и приложений, что упрощает процесс внедрения и эксплуатации.

Управление и анализ киберинцидентов являются ключевыми функциями SOAR-решений. Эти платформы обеспечивают систематический подход к обработке инцидентов, что позволяет значительно повысить эффективность и точность реагирования на угрозы. Одной из главных задач SOAR-решений является автоматизация процессов управления инцидентами. Платформы используют заранее настроенные сценарии для классификации и приоритизации инцидентов. Это позволяет быстро определить уровень угрозы и выбрать соответствующие меры реагирования. Автоматизация снижает риск человеческих ошибок и ускоряет процесс принятия решений.

SOAR-решения также играют важную роль в анализе киберинцидентов. Платформы собирают и коррелируют данные из различных источников, таких как системы мониторинга, сетевые устройства и журналы событий [5]. Это позволяет создать полную картину инцидента и понять его происхождение и возможные последствия. Глубокий анализ помогает выявить слабые места в системе безопасности и разработать меры для их устранения.

SOAR-решения обеспечивают эффективное управление инцидентами на всех этапах их жизненного цикла. Платформы поддерживают документирование всех действий и решений, принятых в процессе реагирования на инцидент. Это обеспечивает прозрачность и позволяет проводить последующий анализ для улучшения процедур безопасности. Еще одним важным аспектом является интеграция с системами отчетности и аналитики. SOAR-решения предоставляют инструменты для создания отчетов и визуализации данных, что помогает руководству компании принимать обоснованные решения по улучшению кибербезопасности. Регулярные отчеты помогают отслеживать динамику инцидентов и оценивать эффективность принимаемых мер.

В последние годы всё чаще выходят публикации, посвящённые исследованию SOAR-решений. Например, в статье [6] обосновывается необходимость применения систем класса SOAR для автоматизации управления инцидентами информационной безопасности. Основные функции SOAR включают оркестровку защиты данных и автоматизацию реагирования на инциденты. В ней рассматриваются функциональная архитектура таких систем, особенности их внедрения и преимущества в управлении информационной безопасностью, включая снижение нагрузки на персонал и повышение эффективности мер защиты.

Также в статье [7] проводится анализ применения SOAR-решений для управления инцидентами информационной безопасности. Авторы данной статьи рассматривают основные компоненты и функции SOAR, включая оркестрацию, автоматизацию и отчётность. Обсуждаются архитектурные особенности и интеграции с другими системами безопасности. Результаты

данного исследования демонстрируют преимущества SOAR в автоматизации реагирования на инциденты и повышении эффективности информационной безопасности.

Кроме того, в статье [8] сравниваются SOAR-решения и SIEM-системы для обеспечения информационной безопасности. Обсуждаются основные различия, преимущества и недостатки каждого подхода, а также их влияние на работу команд SecOps. SOAR повышает эффективность реагирования на инциденты за счёт автоматизации и интеграции процессов, тогда как SIEM требует большего участия специалистов для анализа данных и управления инцидентами.

Научная новизна статьи состоит в том, что до этого в российской научной литературе не проводился сравнительный анализ зарубежных и отечественных SOAR-решений для автоматизации реагирования на киберинциденты. Работа раскрывает преимущества и возможности интеграции этих платформ с различными системами безопасности, а также их значимость для повышения киберустойчивости отечественных организаций. Особенно актуально исследование в контексте импортозамещения, так как оно акцентирует внимание на локальных решениях, соответствующих российским стандартам безопасности.

Зарубежные решения

Для автоматизации процессов выявления, анализа и реагирования на инциденты в цифровых активах организации на международном рынке представлены различные SOAR-решения [9].

Palo Alto Cortex XSOAR

Palo Alto Cortex XSOAR – это одна из ведущих платформ в области автоматизации кибербезопасности, созданная для эффективного управления инцидентами. Продукт появился на рынке после приобретения компании Demisto в 2019 году компанией Palo Alto Networks. Demisto, основанная в 2015 году, специализировалась на разработке SOAR-решений, и интеграция её технологий в продуктовую линейку Palo Alto Networks привела к созданию Cortex XSOAR – комплексного решения для автоматизации операций по кибербезопасности. Основной целью Cortex XSOAR является предоставление организациям возможности автоматизировать рутинные задачи по реагированию на инциденты и повышать скорость и точность их решения [10]. Это позволяет сократить количество ложных срабатываний, уменьшить нагрузку на специалистов по кибербезопасности и ускорить процесс реагирования на реальные угрозы.

Ключевыми функциями Cortex XSOAR являются:

1. Автоматизация процессов реагирования на инциденты – платформа позволяет автоматизировать сотни процессов реагирования, что ускоряет реакцию на угрозы и снижает необходимость ручного вмешательства.

2. Оркестрация – интеграция с множеством сторонних инструментов, таких как системы мониторинга информационной безопасности, сканеры уязвимостей и платформы киберразведки, позволяет централизовать управление различными аспектами безопасности.

3. Рабочие процессы – Cortex XSOAR предоставляет готовые сценарии реагирования и позволяет создавать настраиваемые рабочие процессы под конкретные задачи или инциденты.

4. Объединение данных – платформа собирает и анализирует данные с различных источников, предоставляя аналитикам полную картину инцидента в реальном времени.

5. Машинное обучение – система использует элементы машинного обучения для оптимизации процессов и более точного прогнозирования рисков.

Особенность Cortex XSOAR – его гибкость и возможность масштабирования в зависимости от потребностей организации, будь то небольшая компания или крупное предприятие. Продукт активно развивается и остаётся одной из самых востребованных платформ в сфере автоматизации кибербезопасности [11]. Главное окно Palo Alto Cortex XSOAR представлено на рисунке 2.

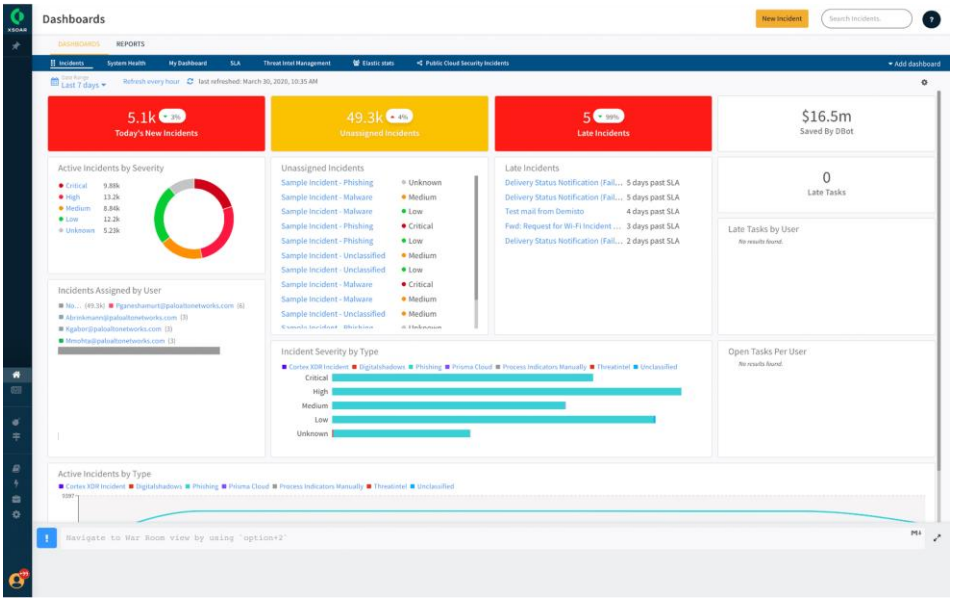

Рис. 2. Главное окно Palo Alto Cortex XSOAR

IBM Security QRadar SOAR

IBM Security QRadar SOAR – это комплексное решение, разработанное для автоматизации и управления процессами реагирования на инциденты в области кибербезопасности. Продукт является частью экосистемы IBM Security QRadar, которая включает инструменты для мониторинга и анализа угроз. QRadar SOAR был представлен в рамках развития решений IBM в области кибербезопасности и получил признание как один из ключевых продуктов для обеспечения защиты корпоративных сетей [12]. История продукта берёт своё начало с приобретения IBM компании Resilient Systems в 2016 году. Resilient Systems специализировалась на разработке решений для управления инцидентами и автоматизации реагирования. После приобретения технологии Resilient были интегрированы в QRadar, что позволило создать IBM Security QRadar SOAR, сочетающий в себе возможности оркестрации и автоматизации кибербезопасности.

Ключевыми функциями QRadar SOAR являются:

1. Автоматизация реагирования на инциденты – платформа предоставляет возможность автоматизации типичных процессов реагирования на инциденты, таких как сбор данных, анализ и реагирование. Это снижает человеческий фактор и ускоряет процесс устранения угроз.

2. Оркестрация – QRadar SOAR интегрируется с различными сторонними системами, включая системы управления событиями безопасности (SIEM), сканеры уязвимостей, платформы кибер разведки и другие инструменты, что позволяет централизованно управлять всеми аспектами кибербезопасности.

3. Управление инцидентами – платформа позволяет аналитикам кибербезопасности отслеживать инциденты в реальном времени, назначать задачи, контролировать выполнение процессов и вести расследования. QRadar SOAR предлагает интерактивные панели и подробные отчёты по инцидентам.

4. Гибкие рабочие процессы – пользователи могут настраивать рабочие процессы под конкретные потребности компании, что позволяет адаптировать систему под различные бизнес-процессы и типы угроз.

5. Совместная работа – QRadar SOAR поддерживает совместное взаимодействие между командами и специалистами по безопасности, упрощая обмен информацией и координацию действий при инцидентах.

Особенностью QRadar SOAR является тесная интеграция с другими продуктами IBM Security, что обеспечивает комплексный подход к управлению угрозами и инцидентами [13]. Решение позволяет ускорить процесс реагирования, улучшить качество расследований и

снизить нагрузку на специалистов. Главное окно IBM Security QRadar SOAR представлено на рисунке 3.

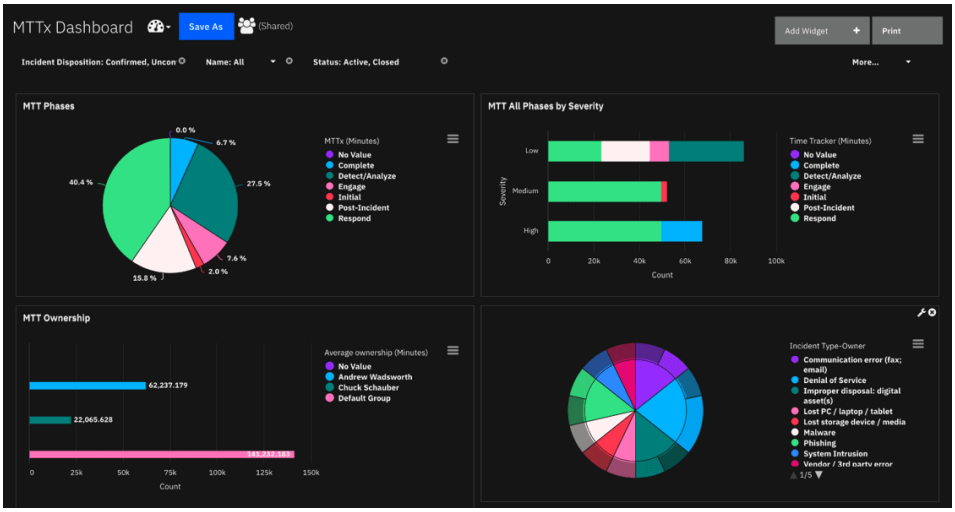

Рис. 3. Главное окно IBM Security QRadar SOAR

Fortinet FortiSOAR

Fortinet FortiSOAR – это платформа для оркестрации, автоматизации и реагирования на инциденты в области кибербезопасности, разработанная для повышения эффективности и ускорения процессов реагирования на угрозы. FortiSOAR входит в экосистему решений Fortinet Security Fabric и предоставляет возможность централизованного управления инцидентами и комплексного анализа угроз [14]. История FortiSOAR началась с того, что Fortinet активно расширяла свои решения в области автоматизации кибербезопасности. В 2019 году компания приобрела CyberSponse – ведущего разработчика решений SOAR. Технологии CyberSponse были интегрированы в продуктовую линейку Fortinet, что позволило создать FortiSOAR – мощное решение, сочетающее передовые технологии автоматизации и оркестрации безопасности.

Ключевыми функциями FortiSOAR являются:

1. Автоматизация реагирования на инциденты – FortiSOAR позволяет автоматизировать рутинные задачи по реагированию на инциденты, такие как сбор данных, анализ и принятие решений. Это помогает сократить время на устранение угроз и снизить нагрузку на специалистов по информационной безопасности.

2. Оркестрация безопасности – FortiSOAR интегрируется с более чем 300 сторонними приложениями и инструментами, такими как SIEM, системы управления уязвимостями и платформы киберразведки. Это обеспечивает гибкость и позволяет централизованно управлять всеми аспектами безопасности.

3. Рабочие процессы и сценарии – FortiSOAR предоставляет широкий набор готовых сценариев реагирования, которые можно адаптировать под конкретные потребности организации. Это позволяет улучшить эффективность реагирования и настроить рабочие процессы под бизнес-процессы компании.

4. Мониторинг и управление инцидентами в реальном времени – платформа поддерживает мониторинг инцидентов в реальном времени с использованием удобных панелей управления. Это обеспечивает аналитикам доступ к актуальной информации и помогает оперативно реагировать на новые угрозы.

5. Аналитика и отчеты – FortiSOAR предоставляет мощные инструменты для анализа инцидентов и создания отчетов, что позволяет организациям оценивать свою готовность к угрозам и улучшать стратегию киберзащиты.

Особенностью FortiSOAR является его глубокая интеграция с другими решениями Fortinet, что делает его частью единой системы кибербезопасности, покрывающей широкий спектр задач – от мониторинга и анализа угроз до их устранения [15]. FortiSOAR позволяет

организациям повысить свою киберустойчивость за счёт автоматизации и гибкого управления процессами. Главное окно Fortinet FortiSOAR представлено на рисунке 4.

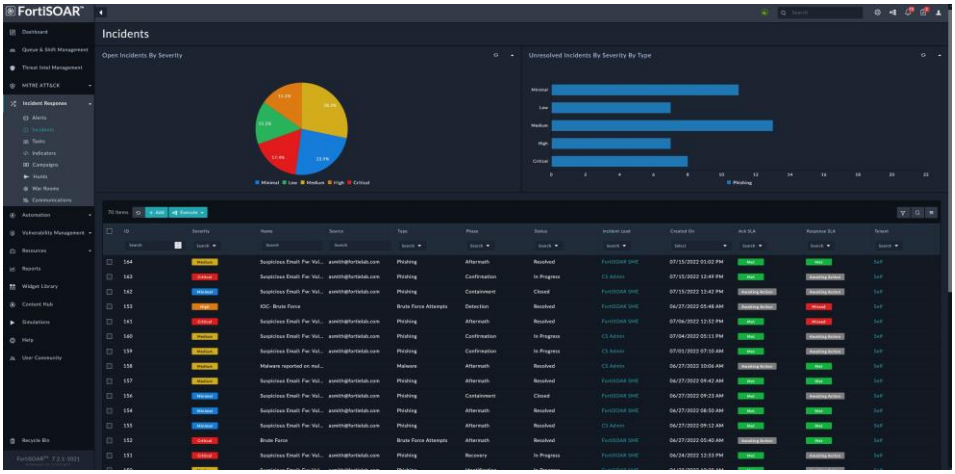

Рис. 4. Главное окно Fortinet FortiSOAR

Отечественные решения

Для автоматизации процессов выявления, анализа и реагирования на инциденты в цифровых активах организации на российском рынке представлены различные SOAR-решения.

R-Vision SOAR

R-Vision SOAR – это отечественная платформа для автоматизации, оркестрации и управления инцидентами кибербезопасности. Она разрабатывается компанией R-Vision, которая специализируется на создании решений для обеспечения информационной безопасности [16]. Платформа помогает организациям в управлении сложными инцидентами киберугроз, снижении времени реагирования и повышении эффективности работы аналитиков безопасности.

История R-Vision SOAR началась в ответ на растущие потребности бизнеса и государственных структур в современных средствах для автоматизации процессов киберзащиты. R-Vision, обладая многолетним опытом в создании решений для управления инцидентами и управления уязвимостями, разработала R-Vision SOAR как компонент своей экосистемы для кибербезопасности. Платформа стала важной частью продуктов компании, призванной помогать клиентам решать задачи в условиях возрастающей сложности кибератак и нагрузки на аналитиков SOC. R-Vision SOAR имеет сертификат ФСТЭК России №4782 от 5 марта 2024 года по 4 уровню доверия и входит в реестр российского программного обеспечения (запись в реестре №1954 от 23.09.2016).

Основные функции R-Vision SOAR включают:

1. Автоматизация реагирования на инциденты – платформа позволяет автоматизировать рутинные задачи и процессы реагирования на инциденты, такие как сбор данных, анализ и принятие решений. Это значительно ускоряет процесс реагирования и снижает риск ошибок.

2. Оркестрация – R-Vision SOAR интегрируется с множеством других систем безопасности, таких как SIEM, системы анализа уязвимостей и средства мониторинга сетей. Это позволяет централизовать управление безопасностью и координировать действия всех систем.

3. Гибкие рабочие процессы – пользователи могут настраивать рабочие процессы под конкретные бизнес-процессы и типы угроз. Система предоставляет возможность создавать настраиваемые сценарии реагирования в зависимости от политики безопасности компании.

4. Интеграция с SOC – R-Vision SOAR поддерживает интеграцию с центрами мониторинга безопасности, позволяя централизовать управление инцидентами и проводить их всесторонний анализ в реальном времени.

5. Расследование инцидентов – платформа предоставляет мощные инструменты для расследования и анализа инцидентов, включая сбор и обработку доказательств, возможность создания отчётов и ведения журнала действий.

Особенностью R-Vision SOAR является его локализация под российские стандарты и требования в области кибербезопасности, что делает его востребованным решением для организаций, работающих в условиях регулирования и высоких требований к защите информации [16]. Платформа также отличается простотой в настройке и использовании, что позволяет компаниям быстро адаптировать её под свои нужды и эффективно справляться с угрозами. Главное окно R-Vision SOAR представлено на рисунке 5.

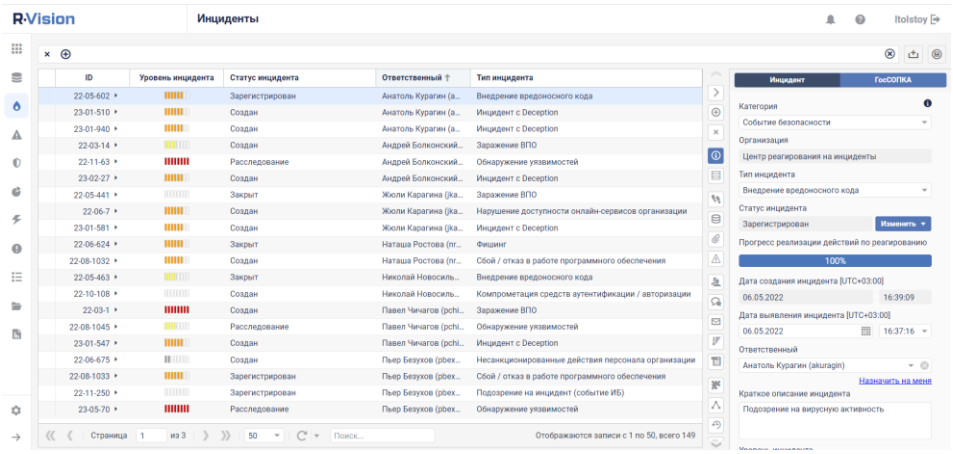

Рис. 5. Главное окно R-Vision SOAR

Security Vision SOAR

Security Vision SOAR – это платформа, предназначенная для автоматизации, оркестрации и управления процессами реагирования на инциденты кибербезопасности. Продукт разработан компанией Security Vision, которая специализируется на создании решений для защиты информации и управления безопасностью. Платформа ориентирована на поддержку служб информационной безопасности и упрощение процессов управления инцидентами [17].

История Security Vision SOAR началась с понимания того, что современные организации нуждаются в автоматизированных решениях для эффективного противодействия растущему числу кибератак и усложняющихся угроз. Компания Security Vision уже имела обширный опыт в области создания систем управления событиями и инцидентами безопасности, что позволило ей разработать SOAR-решение для автоматизации этих процессов. Этот продукт был выпущен на рынок для того, чтобы обеспечить отечественные компании и государственные структуры мощным инструментом для защиты данных. Security Vision SOAR имеет сертификат ФСТЭК России №4574 от 2 сентября 2022 года по 4 уровню доверия и входит в реестр российского программного обеспечения (запись в реестре №17600 от 17.05.2023).

Ключевые функции Security Vision SOAR включают:

1. Автоматизация реагирования на инциденты – платформа предоставляет мощные возможности для автоматизации всех этапов реагирования на киберинциденты, начиная от обнаружения угрозы и заканчивая её устранением. Это позволяет значительно ускорить процесс реагирования и снизить нагрузку на сотрудников SOC.

2. Оркестрация безопасности – Security Vision SOAR интегрируется с множеством сторонних решений для кибербезопасности, включая SIEM, системы мониторинга уязвимостей, сканеры сетевого трафика и другие средства защиты. Это даёт возможность централизованного управления и контроля над всеми процессами безопасности.

3. Гибкие сценарии реагирования – платформа поддерживает настройку сценариев реагирования в зависимости от политики безопасности организации. Пользователи могут создавать и настраивать процессы под конкретные типы инцидентов, что позволяет адаптировать SOAR-решение под уникальные потребности компании.

4. Поддержка совместной работы – Security Vision SOAR позволяет координировать действия между различными отделами и командами безопасности, что улучшает эффективность взаимодействия и ускоряет процесс реагирования на инциденты.

5. Анализ и отчётность – платформа предоставляет инструменты для подробного анализа инцидентов, построения отчётов и ведения истории расследований. Это помогает оценить эффективность мер безопасности и выявить слабые места в системе.

Особенностью Security Vision SOAR является её соответствие требованиям российских стандартов информационной безопасности, что делает её особенно привлекательной для государственных организаций и крупных компаний, работающих в условиях строгого регулирования [17]. Платформа также позволяет организациям повышать уровень готовности к угрозам за счёт гибкой настройки и интеграции с существующей инфраструктурой безопасности. Главное окно Security Vision SOAR представлено на рисунке 6.

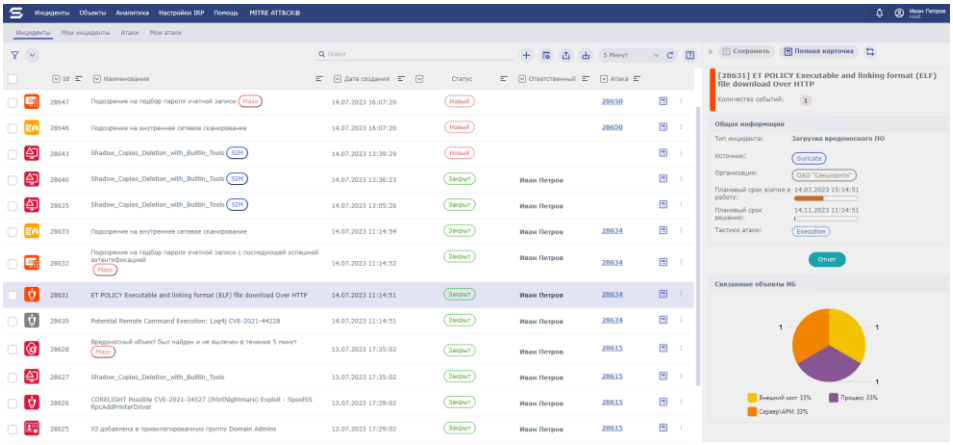

Рис. 6. Главное окно Security Vision SOAR

ePlat4m Orchestra

ePlat4m Orchestra – это платформа для оркестрации, автоматизации и реагирования на инциденты кибербезопасности, разработанная компанией «КИТ». Продукт создан для того, чтобы помочь организациям управлять инцидентами в области информационной безопасности и автоматизировать процессы реагирования, тем самым снижая нагрузку на аналитиков и ускоряя время реакции на угрозы.

История ePlat4m Orchestra началась с потребности в локализованном решении для российских организаций, которое бы соответствовало отечественным стандартам информационной безопасности. ООО «КИТ» разработал платформу для автоматизации работы служб безопасности и центров мониторинга информационной безопасности. Основной акцент был сделан на простоту интеграции с существующими системами и возможностях гибкой настройки для удовлетворения конкретных потребностей клиентов [18]. ePlat4m Orchestra имеет сертификат ФСТЭК России №4433 от 29 июля 2021 года по 6 уровню доверия и входит в реестр российского программного обеспечения (запись в реестре №8394 от 30.12.2020).

Ключевые функции ePlat4m Orchestra включают:

1. Автоматизация реагирования на инциденты – платформа позволяет автоматизировать большое количество рутинных задач по реагированию на инциденты. Это снижает вероятность человеческой ошибки, ускоряет решение инцидентов и позволяет сосредоточить ресурсы на более сложных задачах.

2. Оркестрация процессов безопасности – ePlat4m Orchestra поддерживает интеграцию с множеством сторонних решений, включая системы мониторинга, системы управления уязвимостями, антивирусное ПО и другие инструменты защиты. Это обеспечивает централизованное управление кибербезопасностью.

3. Гибкие рабочие процессы – платформа предоставляет возможность настраивать рабочие процессы реагирования в зависимости от требований организации. Она позволяет создавать уникальные сценарии автоматизированных действий, основанные на типах угроз и инцидентов.

4. Аналитика и отчёты – ePlat4m Orchestra поддерживает сбор и анализ данных по инцидентам, что помогает организациям лучше понимать свои слабые стороны и улучшать свои

процессы безопасности. Платформа также предоставляет инструменты для создания отчётов, которые можно использовать для последующего анализа или аудита.

5. Поддержка совместной работы – ePlat4m Orchestra способствует координации работы между различными подразделениями и командами по безопасности, что ускоряет процесс реагирования и улучшает взаимодействие.

Особенностью ePlat4m Orchestra является её адаптация под российские стандарты кибербезопасности и соответствие требованиям регуляторов. Платформа также активно используется в государственных структурах и крупных компаниях, где необходимо соответствие строгим требованиям в области защиты информации [18]. Интеграция с отечественными решениями и гибкость в настройке делают ePlat4m Orchestra важным инструментом для обеспечения комплексной защиты и автоматизации реагирования на инциденты кибербезопасности. Главное окно ePlat4m Orchestra представлено на рисунке 7.

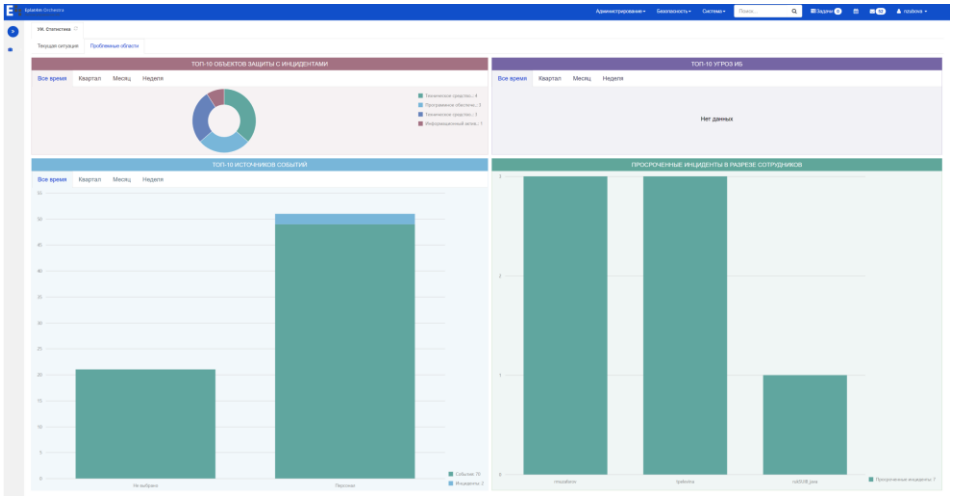

Рис. 7. Главное окно ePlat4m Orchestra

Сравнение зарубежных и отечественных решений

В таблицах 1 и 2 приведено сравнение SOAR-решений по важным для бизнеса характеристикам.

Таблица 1.

Сравнение зарубежных SOAR-решений

Параметр	Palo Alto Cortex XSOAR	IBM Security QRadar SOAR	Fortinet FortiSOAR
Основная функция	Автоматизация и оркестрация инцидентов безопасности	Автоматизация процессов реагирования на инциденты	Интеграция и оркестрация безопасности
Интеграции	900+ интеграций с различными системами и сервисами	Интеграция с IBM QRadar и другими SIEM	Интеграция с Fortinet Security Fabric и сторонними решениями
Поддержка SIEM	Да, поддерживает интеграцию с различными SIEM	Да, полная интеграция с QRadar SIEM	Да, интеграция с FortiSIEM и другими
Ориентированность	Большая гибкость в автоматизации, поддержка Playbooks	Глубокая интеграция с экосистемой IBM	Хорошо подходит для крупных корпоративных сред
Модульность и настраиваемость	Поддержка low-code для настройки процессов	Средняя гибкость, более направлена на использование в	Высокая модульность, возможность настройки и автоматизации

Параметр	Palo Alto Cortex XSOAR	IBM Security QRadar SOAR	Fortinet FortiSOAR
		рамках решений IBM	
Масштабируемость	Высокая, подходит для крупных предприятий	Высокая, идеально для интеграции в IBM экосистему	Масштабируется под крупные и средние компании
Интерфейс	Интуитивно понятный, с поддержкой drag-and-drop	Традиционный интерфейс, тесно связанный с QRadar	Гибкий интерфейс с поддержкой графических моделей
Целевой рынок	Средний и крупный бизнес	Крупные предприятия, использующие IBM решения	Средний и крупный бизнес
Облачная поддержка	Облачное, гибридное и локальное развертывание		
Особенности	Интеграция с большим числом сторонних систем, активное сообщество и поддержка	Отличная интеграция с экосистемой IBM	Глубокая интеграция с продуктами Fortinet, высокая скорость работы

Таблица 2.

Сравнение отечественных SOAR-решений

Параметр	R-Vision SOAR	Security Vision SOAR	ePlat4m Orchestra
Основная функция	Автоматизация процессов реагирования на инциденты, управление инцидентами	Автоматизация реагирования, управление инцидентами, соответствие требованиям регуляторов	Автоматизация и оркестрация безопасности, управление инцидентами
Интеграции	Интеграция с SIEM, системами управления ИБ и сторонними решениями	Широкие возможности интеграции с различными системами безопасности	Поддержка интеграций с системами ИБ, SIEM
Поддержка SIEM	Интеграция с различными SIEM, включая отечественные решения	Интеграция с большинством популярных SIEM, в том числе сторонними	Поддержка интеграции с различными SIEM, включая российские и международные решения
Ориентированность	Российские компании, крупный и средний бизнес	Крупные предприятия и госструктуры	Российские предприятия среднего и крупного масштаба
Модульность и настраиваемость	Высокий уровень настраиваемости, гибкая настройка Playbooks	Высокий уровень настраиваемости для специфических требований компаний	Хорошие возможности настраиваемости процессов и создания сценариев
Масштабируемость	Высокая, для предприятий среднего и крупного масштаба	Масштабируется под нужды крупных организаций и государственных структур	Масштабируемая платформа для компаний различного уровня
Интерфейс	Удобный пользовательский интерфейс с поддержкой графических инструментов	Интуитивный интерфейс, разработан для пользователей	Удобный и гибкий интерфейс с функцией drag-and-drop

Параметр	R-Vision SOAR	Security Vision SOAR	ePlat4m Orchestra
		разного уровня подготовки	
Целевой рынок	Российский рынок, средний и крупный бизнес	Крупные предприятия и государственные организации	Российский рынок, предприятия среднего и крупного масштаба
Облачная поддержка	Облачное, гибридное и локальное развертывание		
Особенности	Глубокая интеграция с российскими системами ИБ и SIEM, поддержка национальных стандартов	Поддержка выполнения требований законодательства, возможность работы с большими данными	Мощная система оркестрации с широкой интеграцией в ИБ-ландшафт

Из сравнения видно, что Palo Alto Cortex XSOAR, IBM Security QRadar SOAR и Fortinet FortiSOAR ориентированы на глобальный рынок и предлагают масштабируемость, широкую интеграцию с SIEM и сторонними системами, а также гибкость в настройке и автоматизации процессов. Напротив, R-Vision SOAR, Security Vision SOAR и ePlat4m Orchestra ориентированы на российский и международный рынки с акцентом на соответствие местным стандартам и потребностям государственных организаций. Они предлагают высокую настраиваемость и интеграции с российскими продуктами. В целом, каждая платформа адаптирована под свои целевые рынки и обладает преимуществами в зависимости от области применения.

Заключение

Авторами данной статьи был проведён анализ существующих на международном и отечественном рынках SOAR-решений, позволяющих автоматизировать процессы выявления, анализа и реагирования на киберинциденты. Такие решения, как Palo Alto Cortex XSOAR, IBM Security QRadar SOAR, Fortinet FortiSOAR и отечественные продукты, как R-Vision SOAR, Security Vision SOAR и ePlat4m Orchestra, демонстрируют свою эффективность в оркестрации, автоматизации, реагировании и обеспечении интеграции с разнообразными системами безопасности. Ключевыми результатами стали следующие выводы. Во-первых, автоматизация рутинных задач с помощью SOAR-платформ позволяет значительно сократить время реагирования на инциденты и уменьшить количество ошибок, вызванных человеческим фактором. Во-вторых, возможность интеграции с различными инструментами безопасности, такими как SIEM-системы и системы обнаружения и предотвращения вторжений, обеспечивает комплексный подход к защите цифровых активов. В-третьих, стандартизация процессов реагирования на инциденты, поддерживаемая SOAR-решениями, помогает повысить уровень согласованности действий между подразделениями и улучшить взаимодействие внутри компании. Таким образом, внедрение SOAR-решений представляет собой важный шаг в повышении киберустойчивости организаций, что особенно актуально в условиях растущего числа и сложности кибератак.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Что такое SOAR? [Электронный ресурс]. – Режим доступа: URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-soar (дата обращения: 05.10.2024).

2. SOAR (Security Orchestration, Automation and Response) [Электронный ресурс]. – Режим доступа: URL: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/ (дата обращения: 05.10.2024).

3. SOAR: что это такое и зачем нужно в кибербезопасности [Электронный ресурс]. – Режим доступа: URL: https://www.securitylab.ru/analytics/538804.php (дата обращения: 05.10.2024).

4. SOAR-системы [Электронный ресурс]. – Режим доступа: URL: https://www.securityvision.ru/blog/soar-sistemy/ (дата обращения: 05.10.2024).

5. SOAR: автоматизация реагирования [Электронный ресурс]. – Режим доступа: URL: http://itsec.ru/articles2/Oborandteh/soar-avtomatizatsiya-reagirovaniya (дата обращения: 05.10.2024).

6. Богданов В.В., Домуховский Н.А., Савин М.В. SOAR: автоматизация работы с инцидентами информационной безопасности // Защита информации. Инсайд. – Санкт-Петербург, 2021. – № 3(99). – С. 13-17.

7. Шамагулов А.А., Пономарева О.А. Анализ систем автоматизированного управления инцидентами SOAR // МСИ: 10 лет подготовки кадров для международной системы ПОД/ФТ: Материалы IX Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ, Москва, 22-24 ноября 2023 года. – Москва, 2023. – С. 86-97.

8. Егоров, Ю.В. Решения класса SOAR как этап развития систем SIEM // Collegium Linguisticum-2023: Сборник статей Ежегодной конференции Студенческого научного общества МГЛУ, Москва, 15–17 марта 2023 года. – Москва, 2023. – С. 715-719.

9. Обзор решений класса Security Orchestration, Automation and Response (SOAR) [Электронный ресурс]. – Режим доступа: URL: https://www.anti-malware.ru/analytics/Market_Analysis/Security-Orchestration-Automation-and-Response-SOAR-Solution-Overview (дата обращения: 05.10.2024).

10. Palo Alto Cortex XSOAR [Электронный ресурс]. – Режим доступа: URL: https://www.paloaltonetworks.com/cortex/cortex-xsoar (дата обращения: 05.10.2024).

11. Palo Alto Cortex XSOAR datasheet [Электронный ресурс]. – Режим доступа: URL: https://www.paloaltonetworks.com/resources/datasheets/cortex-xsoar (дата обращения: 05.10.2024).

12. IBM Security QRadar SOAR (Security Orchestration, Automation and Response) [Электронный ресурс]. – Режим доступа: URL: https://www.ibm.com/products/qradar-soar (дата обращения: 05.10.2024).

13. IBM Security QRadar SOAR overview [Электронный ресурс]. – Режим доступа: URL: https://www.ibm.com/docs/en/security-qradar/security-qradar-soar/saas?topic=solution-overview (дата обращения: 05.10.2024).

14. Fortinet FortiSOAR [Электронный ресурс]. – Режим доступа: URL: https://www.fortinet.com/products/fortisoar (дата обращения: 05.10.2024).

15. Fortinet FortiSOAR datasheet [Электронный ресурс]. – Режим доступа: URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisoar.pdf (дата обращения: 05.10.2024).

16. R-Vision SOAR [Электронный ресурс]. – Режим доступа: URL: https://rvision.ru/products/soar (дата обращения: 05.10.2024).

17. Security Vision SOAR [Электронный ресурс]. – Режим доступа: URL: https://www.securityvision.ru/products/soar/ (дата обращения: 05.10.2024).

18. ePlat4m Orchestra [Электронный ресурс]. – Режим доступа: URL: https://eplat4m.ru/products/eplat4m-orchestra/ (дата обращения: 05.10.2024).

REFERENCES

1. What is SOAR? [Electronic resource]. – Access mode: URL: https://www.microsoft.com/ru-ru/security/business/security-101/what-is-soar (date of access: 10/05/2024).

2. SOAR (Security Orchestration, Automation and Response) [Electronic resource]. – Access mode: URL: https://encyclopedia.kaspersky.ru/glossary/security-orchestration-automation-and-response-soar/ (date of access: 10/05/2024).

3. SOAR: What is it and why is it needed in cybersecurity [Electronic resource]. – Access mode: URL: https://www.securitylab.ru/analytics/538804.php (date of access: 10/05/2024).

4. SOAR systems [Electronic resource]. – Access mode: URL: https://www.securityvision.ru/blog/soar-sistemy/ (date of access: 10/05/2024).

5. SOAR: Automated Response [Electronic resource]. – Access mode: URL: http://itsec.ru/articles2/Oborandteh/soar-avtomatizatsiya-reagirovaniya (date of access: 10/05/2024).

6. Bogdanov V.V., Domukhovsky N.A., Savin M.V. SOAR: automation of work with information security incidents // Information protection. Inside. – Saint Petersburg, 2021. – № 3(99). – pp. 13-17.

7. Shamagulov A.A., Ponomareva O.A. Analysis of automated incident management systems SOAR // ISI: 10 years of training for the international AML/CFT system: Proceedings of the IX International Scientific and Practical Conference of the International Network Institute in the field of AML/CFT, Moscow, November 22-24, 2023. – Moscow, 2023. – pp. 86-97.

8. Egorov, Yu.V. SOAR class solutions as a stage in the development of SIEM systems // Collegium Linguisticum-2023: Collection of articles of the Annual Conference of the MGLU Student Scientific Society, Moscow, March 15-17, 2023. – Moscow, 2023. – pp. 715-719.

9. Overview of Security Orchestration, Automation and Response (SOAR) solutions [Electronic resource]. – Access mode: URL: https://www.anti-malware.ru/analytics/Market_Analysis/Security-Orchestration-Automation-and-Response-SOAR-Solution-Overview (date of access: 10/05/2024).

10. Palo Alto Cortex XSOAR [Electronic resource]. – Access mode: URL: https://www.paloaltonetworks.com/cortex/cortex-xsoar (date of access: 10/05/2024).

11. Palo Alto Cortex XSOAR datasheet [Electronic resource]. – Access mode: URL: https://www.paloaltonetworks.com/resources/datasheets/cortex-xsoar (date of access: 10/05/2024).

12. IBM Security QRadar SOAR [Electronic resource]. – Access mode: URL: https://www.ibm.com/products/qradar-soar (date of access: 10/05/2024).

13. IBM Security QRadar SOAR overview [Electronic resource]. – Access mode: URL: https://www.ibm.com/docs/en/security-qradar/security-qradar-soar/saas?topic=solution-overview (date of access: 10/05/2024).

14. Fortinet FortiSOAR [Electronic resource]. – Access mode: URL: https://www.fortinet.com/products/fortisoar (date of access: 10/05/2024).

15. Fortinet FortiSOAR datasheet [Electronic resource]. – Access mode: URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortisoar.pdf (date of access: 10/05/2024).

16. R-Vision SOAR [Electronic resource]. – Access mode: URL: https://rvision.ru/products/soar (date of access: 10/05/2024).

17. Security Vision SOAR [Electronic resource]. – Access mode: URL: https://www.securityvision.ru/products/soar/ (date of access: 10/05/2024).

18. ePlat4m Orchestra [Electronic resource]. – Access mode: URL: https://eplat4m.ru/products/eplat4m-orchestra/ (date of access: 10/05/2024).

Информация об авторах

Станислав Павлович Киргизбаев – студент, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: s.p.kirgizbaev@gmail.com

Владислав Павлович Киргизбаев – аспирант, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: v.p.kirgizbaev@gmail.com

Александр Алексеевич Бутин – к.ф.-м.н., доцент кафедры «Информационные системы и защита информации», Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: butin_aa@mail.ru

Authors

Kirgizbaev Stanislav Pavlovich – student, Irkutsk State Transport University, Irkutsk, e-mail: s.p.kirgizbaev@gmail.com

Kirgizbaev Vladislav Pavlovich – post-graduate student, Irkutsk State Transport University, Irkutsk, e-mail: v.p.kirgizbaev@gmail.com

Alexander Alekseevich Butin – Cand. Sc. (Physics and Mathematics), Associate Professor of the Department of Information Systems and Information Security, Irkutsk State Transport University, Irkutsk, e-mail: butin_aa@mail.ru

Для цитирования

С. П. Киргизбаев, В. П. Киргизбаев, А. А. Бутин. Применение SOAR-решений для автоматизации процессов выявления, анализа и реагирования на инциденты в корпоративной сети // «Информационные технологии и математическое моделирование в управлении сложными системами»: электрон. науч. журн. – 2024. – №3. – С. 29-44 – Режим доступа: https://ismm.irgups.ru/toma/323-2024, свободный. – Загл. с экрана. – Яз. рус., англ.

For citations

S. P. Kirgizbaev, V. P. Kirgizbaev, A. A. Butin. Application of SOAR solutions for automation of incident detection, analysis, and response processes in a corporate network // Informacionnye tehnologii i matematicheskoe modelirovanie v upravlenii slozhnymi sistemami: ehlektronnyj nauchnyj zhurnal [Information technology and mathematical modeling in the management of complex systems: electronic scientific journal], 2024. No. 3. P. 29-44.