**SOAR**

**1. Введение**

**Определение SOAR в контексте кибербезопасности**

**SOAR (Security Orchestration, Automation and Response)** – это класс решений и платформ, позволяющих автоматизировать, координировать и унифицировать процессы обнаружения, расследования и реагирования на кибератаки. Основной фокус SOAR – объединить несколько инструментов информационной безопасности (SIEM, EDR, IDS/IPS и др.), а также стандартизировать, документировать и автоматизировать рутинные задачи реагирования.

По данным Gartner, SOAR-платформы обеспечивают организациям возможность систематизировать действия по обнаружению, классификации и предотвращению инцидентов, повышая эффективность работы специалистов по кибербезопасности. Кроме того, они способствуют сокращению затрат времени на поиск и анализ угроз за счёт автоматизации многих ручных процессов.

**Роль SOAR в обеспечении безопасности информационных систем**

1. **Оркестрация действий между инструментами безопасности**  
   SOAR связывает различные системы защиты (SIEM, системы сканирования уязвимостей и т.д.), позволяя автоматизировать весь цикл расследования инцидента.
2. **Автоматизация процессов реагирования**  
   В случае обнаружения угрозы SOAR запускает заранее настроенные сценарии реагирования (Playbooks), которые автоматически выполняют рутинные действия: закрытие портов, блокировку пользователей, уведомление ответственных лиц и т.д.
3. **Улучшение видимости инцидентов**  
   Все данные об инцидентах стекаются в центральную панель (консоль SOAR), что позволяет специалистам быстрее выявлять взаимосвязи между событиями и эффективнее определять приоритеты.
4. **Сокращение нагрузки на специалистов**  
   Автоматизация рутины даёт возможность экспертам сфокусироваться на более сложных задачах, требующих опыта, аналитических навыков и креативного подхода.
5. **Совместная работа в команде**  
   SOAR облегчает ведение документации и коллективную работу, позволяя различным отделам и специалистам совместно участвовать в процессе реагирования.

**2. Состояние технологии**

В последние годы SOAR-платформы стали неотъемлемой частью экосистем кибербезопасности. По оценкам Forrester, востребованность решений SOAR постоянно растёт, так как организации стремятся повысить эффективность работы SOC (Security Operations Center) и снизить время на устранение последствий атак.

**Текущие тенденции в использовании SOAR**

1. **Автоматизация анализа инцидентов**  
   Современные SOAR-инструменты могут собирать логи, данные SIEM и другие источники, чтобы формировать цельную картину инцидента и помогать экспертам быстрее принимать решения.
2. **Интеграция с SIEM, EDR и Threat Intelligence**  
   Большинство SOAR-решений имеют встроенные коннекторы к популярным платформам, таким как Splunk, IBM QRadar, Microsoft Sentinel, Palo Alto Networks Cortex XDR, что упрощает сбор и корреляцию данных (см. Palo Alto Networks Cortex XSOAR).
3. **Открытые стандарты и совместная разработка**  
   Набирают популярность сообщества, предлагающие готовые “плейбуки” (playbooks) и интеграции. Например, MITRE выпускает методологические рекомендации для автоматизации процесса реагирования на основе фреймворка MITRE ATT&CK™ (MITRE ATT&CK).
4. **Рост популярности облачных SOAR-решений**  
   Всё больше компаний переходят к облачным моделям — в формате SaaS — для упрощения развертывания и снижения затрат на поддержание собственной инфраструктуры.
5. **Использование искусственного интеллекта**  
   Встроенные механизмы ML/AI в SOAR позволяют улучшать анализ больших массивов данных и автоматически адаптировать сценарии реагирования под новые типы атак.

**3. Перспективы технологии**

SOAR-системы продолжают активно развиваться и занимать всё более значимую роль в защите информационных систем. Их возможности расширяются за счёт тесной интеграции с другими технологическими элементами кибербезопасности.

**Ожидаемые тренды в развитии SOAR**

* **Дополнительная автоматизация сложных сценариев**  
  С ростом объёмов данных будут востребованы более глубокие механизмы оркестрации и гибкие Playbooks, учитывающие контекст и динамику инцидентов.
* **Интеграция с решениями для облачных сред и IoT**  
  Расширение применения SOAR для защиты контейнерных платформ (Kubernetes, Docker) и устройств IoT за счёт появления специализированных коннекторов.

**Прогнозы роста и популярности**

* **Рост рынка SOAR**  
  По данным MarketsandMarkets, рынок SOAR будет демонстрировать высокие темпы роста в течение ближайших лет, благодаря увеличению числа кибератак и потребности в быстрой автоматизации процессов.
* **Расширение локальных внедрений**  
  В России и странах СНГ ожидается рост спроса на платформы SOAR, адаптированные под местное законодательство и инфраструктуру. Это связано с усилением требований к защите персональных данных и критической информационной инфраструктуры.

**Возможные вызовы и ограничения**

1. **Сложность интеграции**  
   Внедрение SOAR требует глубокой интеграции с имеющимися системами и правильной настройки Playbooks, что может быть сложно для организаций с устаревшей архитектурой.
2. **Обучение специалистов**  
   Для эффективной эксплуатации SOAR необходимы сотрудники, обладающие как техническими навыками (Python, YAML, JSON), так и пониманием угроз; их нехватка может затормозить внедрение.
3. **Высокая стоимость**  
   Полноценная реализация SOAR может потребовать значительных инвестиций на первоначальном этапе (лицензии, инфраструктура, обучение).

**4. Рыночная ниша**

**Целевая аудитория и сегментация рынка**

* **Средние и крупные компании**  
  Организации, у которых есть собственный SOC (Security Operations Center), заинтересованы в инструментах, способных сократить время на ручные операции и улучшить корреляцию данных.
* **Аутсорсинговые SOC-провайдеры (MSSP)**  
  Поставщики управляемых услуг (Managed Security Services Providers) внедряют SOAR для предоставления более быстрого и качественного сервиса клиентам.
* **Государственный сектор**  
  Госучреждения и критически важные отрасли (энергетика, транспорт, здравоохранение) нуждаются в централизованном управлении безопасностью, быстром реагировании и соблюдении регуляторных норм.

**Отрасли, использующие SOAR**

* **Финансовый сектор**  
  Банки и финтех-компании применяют SOAR для быстрого обнаружения мошенничества и соблюдения требований регуляторов (ЦБ РФ, PCI DSS и др.).
* **Телеком**  
  Телекоммуникационные операторы обрабатывают большие объёмы трафика, поэтому нуждаются в автоматизированных системах обнаружения и блокировки атак.
* **Промышленность и энергетика**  
  Для защиты SCADA/ICS-систем от киберинцидентов всё чаще внедряются SOAR-платформы.

**5. Производители**

На мировом рынке и в России существует ряд ключевых поставщиков SOAR-решений. Ниже представлены некоторые из них:

**Международные компании**

1. **Palo Alto Networks**  
   Их платформа **Cortex XSOAR** (ранее Demisto) обеспечивает сквозную оркестрацию и автоматизацию процессов, интеграцию с различными источниками Threat Intelligence и поддержку многопользовательской среды  
   *Подробнее*
2. **IBM**  
   **IBM Security SOAR** (ранее Resilient) – одно из популярных решений для автоматизации реагирования на инциденты, позволяющее формировать сценарии и плейбуки, поддерживающие MITRE ATT&CK и другие стандарты.  
   *Подробнее*
3. **Splunk**  
   **Splunk SOAR** (ранее Phantom) – система, обеспечивающая автоматизацию, оркестрацию и оперативную визуализацию инцидентов, включая широкий каталог готовых интеграций.  
   *Подробнее*
4. **Rapid7**  
   **InsightConnect** – решение для автоматизации инцидент-менеджмента и рутинных задач, упрощающее поиск и устранение угроз.  
   *Подробнее*

**Российские компании**

1. **Positive Technologies**  
   Разработчики SIEM- и SOC-решений, интегрирующие модули SOAR для автоматизации детектирования и реагирования на угрозы.  
   *Пример продукта MaxPatrol SIEM*
2. **Лаборатория Касперского**  
   Предоставляет платформу **Kaspersky Anti Targeted Attack** (KATA), которая включает элементы автоматизации процессов обнаружения и реагирования, а также легко встраивается в SOC.  
   *Подробнее*
3. **Group-IB**  
   Использует собственные наработки в области Threat Intelligence и внедряет автоматизацию реагирования в рамках своих решений для SOC.  
   [*Подробнее*](https://www.group-ib.com)

**6. Заказчики**

**Типичные профили заказчиков**

1. **Крупные корпорации**  
   Банки, ритейл и промышленные предприятия, которые имеют собственные SOC и нуждаются в повышении эффективности детектирования и реагирования.
2. **Государственные учреждения**  
   Органы власти и госкомпании, обрабатывающие критически важные данные, где нужна строгая регламентация и масштабирование инструментов безопасности.
3. **Аутсорс-провайдеры (MSSP)**  
   Предоставляющие услуги киберзащиты как сервис. Для них SOAR – ключ к ускорению реагирования и оптимизации внутренних процессов.

**Ожидания и потребности заказчиков**

* **Сокращение времени реагирования**  
  Автоматизация рутины и единая консоль для координации инцидентов.
* **Снижение затрат на безопасность**  
  Автоматизация рутинных операций уменьшает необходимость в большом количестве аналитиков.
* **Более глубокая аналитика**  
  Интеграция с платформами Threat Intelligence и ML-алгоритмами повышает точность обнаружения и помогает прогнозировать будущие атаки.

**Примеры внедрения SOAR**

1. **IBM SOAR в крупном банке**  
   Автоматизация плейбуков реагирования сократила время нейтрализации инцидентов с часов до минут и позволила снизить риски финансовых потерь.  
   *Источник: IBM Security Stories*
2. **Palo Alto Networks Cortex XSOAR в ретейле**  
   Компания автоматизировала проверку и блокировку потенциально скомпрометированных учётных записей, что уменьшило риск массовых утечек данных клиентов.
3. **Splunk Phantom в госсекторе**  
   Интеграция с SIEM и госреестрами уязвимостей ускорила реагирование на новые угрозы и повысила прозрачность процессов для регуляторов.

**7. Выводы**

SOAR-платформы (Security Orchestration, Automation and Response) вносят кардинальные изменения в организацию процессов кибербезопасности, предоставляя единый центр для автоматизации, координации и анализа действий по предотвращению атак и реагированию на них. Их применение даёт значительную экономию времени и ресурсов, позволяя сосредоточиться на стратегических аспектах защиты.

Основные преимущества SOAR:

* **Сокращение времени на реагирование**  
  Автоматизация рутинных задач и стандартизация плейбуков.
* **Повышение эффективности SOC**  
  Централизованное управление, улучшенная видимость и гибкая оркестрация действий.
* **Улучшенная аналитика и совместная работа**  
  Сбор метрик, удобные дашборды и инструменты коллаборации упрощают взаимодействие между аналитиками.

В то же время при внедрении SOAR важно учитывать сложность интеграции, потребность в квалифицированных кадрах и высокие требования к точности входных данных. Однако при грамотном планировании и настройке система SOAR становится одним из ключевых элементов современной кибербезопасности, способным значительно повысить общий уровень защиты организации.

**Ссылки на источники:**

1. Gartner: Market Guide for SOAR Solutions
2. Forrester: The Forrester Wave™: Security Analytics Platforms, Q4 2022
3. MITRE ATT&CK: https://attack.mitre.org/
4. MarketsandMarkets: Security Orchestration Automation and Response (SOAR) Market
5. IBM: IBM Security SOAR
6. Splunk: Splunk SOAR
7. Palo Alto Networks: Cortex XSOAR