Яндекс Браузер | для организаций

Как Яндекс Браузер для организаций усиливает ИБ-экосистему компании

Экосистема кибербезопасности организации может включать множество различных элементов: от базовой защиты от вредоносных файлов, фишинга, защиты от утечек данных, до комплексных систем мониторинга и реагирования на киберугрозы, противодействия DDoS-атакам, контроля доступа к данным, управления правами и учётными записями, и других систем.

Обычно браузер в этой экосистеме является источником различных рисков для ИТ-инфраструктуры организации и «слепым пятном» для службы информационной безопасности. Ведь у большинства корпоративных защитных систем нет эффективных инструментов для контроля за кодом, который исполняется в браузере, и за информацией (в том числе конфиденциальной), которая в нём обрабатывается. Существующие решения в этой области обычно имеют высокую цену и требуют дорогостоящей экспертизы, которую может себе позволить далеко не каждая организация. В результате исполнение вредоносного кода в веб-приложениях остаётся незамеченным ИБ-специалистами неделями или даже месяцами, и организации получают ощутимый ущерб от кибератак.

При этом значительную часть рабочего времени сотрудники проводят именно в браузере: заходят на внутренние и внешние веб-ресурсы, пользуются веб-приложениями и расширениями. Все эти сценарии использования браузера несут потенциальные угрозы вредоносных атак или утечки конфиденциальных данных.

Яндекс Браузер для организаций учитывает главные корпоративные ИБ-риски, повышает защищённость ИТ-инфраструктуры и расширяет возможности существующей в организации ИБ-экосистемы.

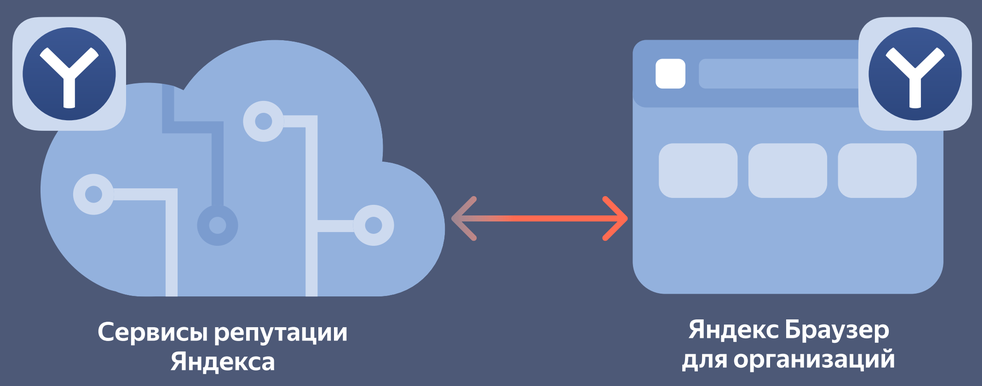
Расскажем подробнее, какую роль Яндекс Браузер для организаций играет в обеспечении корпоративной безопасности.

1. Усиление защиты с помощью вспомогательных систем

Для обеспечения высокого уровня безопасности корпоративных данных Браузер использует как ряд встроенных технологии для защиты от киберугроз, так и вспомогательные системы.

- **Проверка угроз с помощью сервиса репутации Яндекса**

  При открытии сайтов и загрузке файлов Браузер использует вспомогательные сервисы репутации. Он оценивает файлы или адреса веб-страниц, с которыми взаимодействует в процессе работы сотрудник, ориентируясь на информацию из сервиса репутации Яндекса. Это обеспечивает организации дополнительную защиту от большого количества угроз, включая новейшие и редкие.



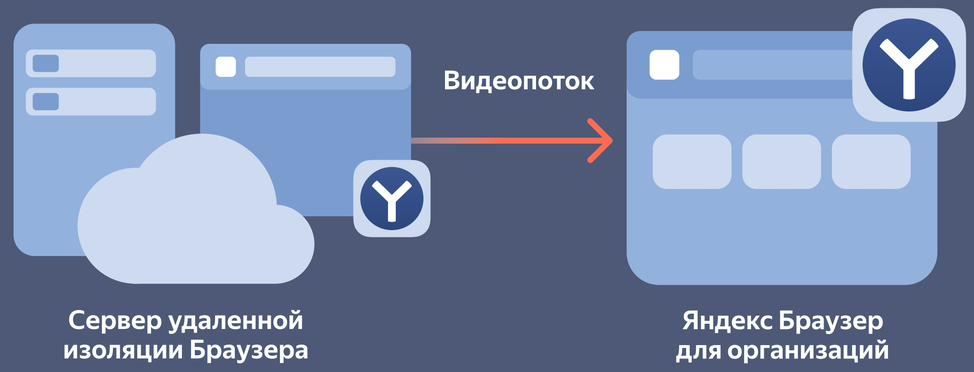
- **Интеграция с внешней DLP-системой**

  У Браузера есть набор собственных технологий для защиты от утечки данных, но если в организации используется отдельная DLP-система, он может выступить как её агент (режим DLP-агента) и стать ценным дополнением для такой системы на настольных и мобильных платформах.

  Благодаря тому, что Браузер доступен на всех популярных ОС, включая Android и iOS, служба безопасности может контролировать все потоки данных, проходящих через Браузер, на всех корпоративных устройствах, а также на личных устройствах сотрудников, если они используются для работы. Кроме того, Яндекс Браузер для организаций в режиме DLP-агента делает процесс защиты от утечек более производительным, ведь на сканирование в DLP-систему из Браузера отправляются только защищаемые объекты, а не весь трафик.

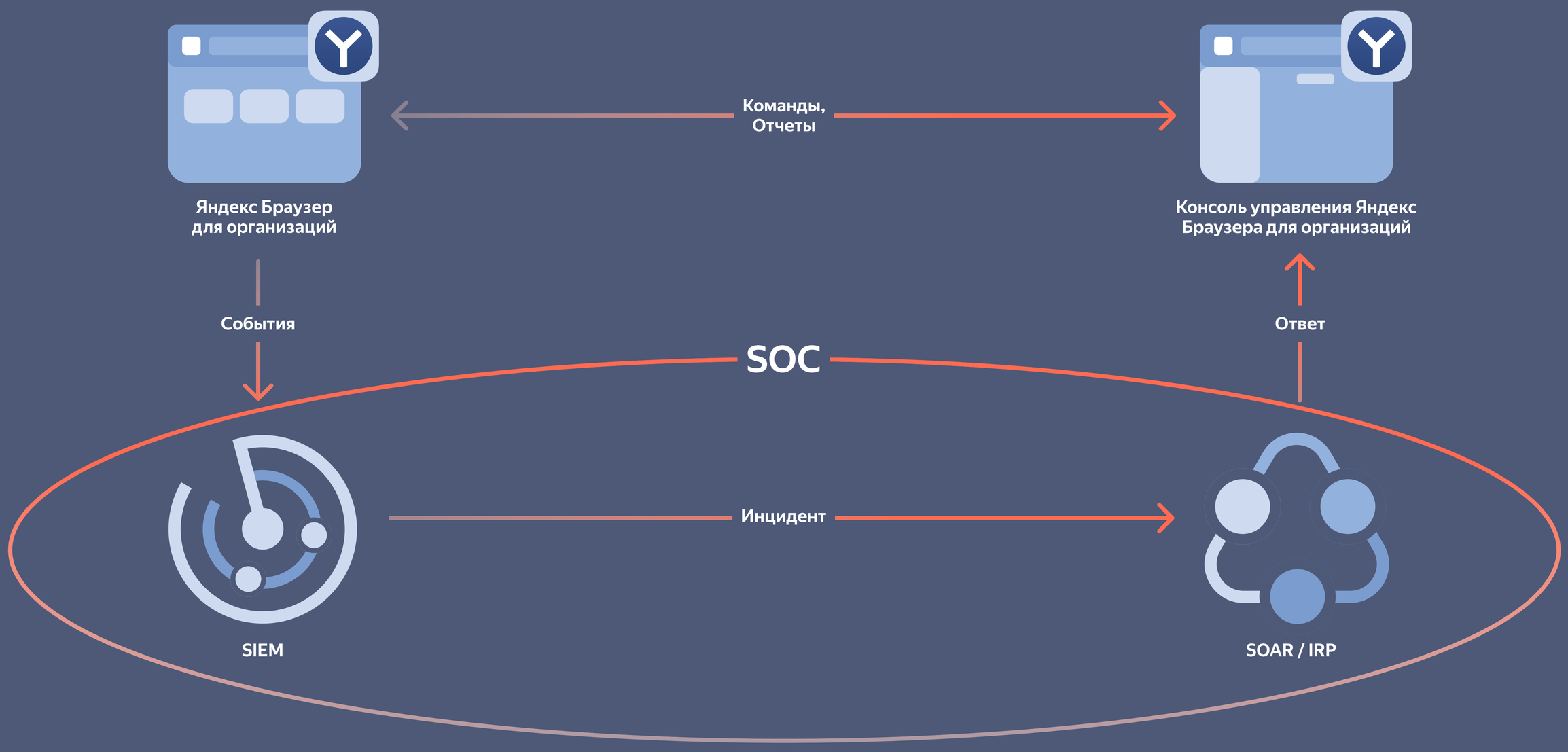
- **Режим удалённой изоляции**

  Браузер может работать в режиме удалённой изоляции. Он предполагает, что само веб-приложение или сайт запускаются и работают в изолированном контейнере на удалённом сервере, а во вкладку браузера на компьютере пользователя транслируется безопасный видеопоток. Даже если в браузере будет открыт вредоносный сайт или будет проэксплуатирована уязвимость нулевого дня, локальная рабочая станция и данные на ней не пострадают, так как атака в реальности произойдёт в изолированном контейнере на удалённом сервере и не покинет пределы её контура.



2. Интеграция в существующую экосистему безопасности

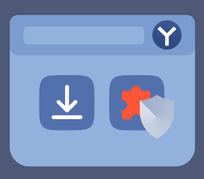
У расширенной версии Яндекс Браузера для организаций есть Консоль управления. Это продвинутая веб-консоль для управления парком браузеров и взаимодействия с другими системами. Вместе Браузер и Консоль могут быть частью экосистемы безопасности в связке с другими системами информационной безопасности.



При интеграции с системами мониторинга событий безопасности (SIEM) браузер становится дополнительным источником данных, значимых для службы информационной безопасности. В частности, сотрудники SOC могут получать данные о браузерной сессии в режиме реального времени, а также инициировать ответные меры по запросу сотрудников, отвечающих за реагирование на инциденты. Кроме того, эти сведения могут быть использованы не только для более эффективного расследования уже случившихся инцидентов, но и для отражения атак в режиме реального времени — Браузер может работать в связке с платформами реагирования на инциденты (SOAR/IRP). Это позволяет автоматизировать взаимодействие и организовать автоматическую обработку инцидентов безопасности или ответ на них в автоматическом режиме.

Вот как это работает на примере инцидента с детектированием вредоносного кода внутри браузерного расширения.

Сотрудник скачивает расширение на свой Яндекс Браузер для организаций, чтобы автоматически исправлять орфографию в документах, с которыми работает. Первое время расширение выполняет заявленные функции, но спустя несколько недель злоумышленник отправляет расширению обновление с вредоносными функциями.



Собственные защитные системы Браузера фиксируют попытку исполнения вредоносного JavaScript-кода, оповещают об этом систему мониторинга событий безопасности и блокируют исполнение кода.

Система мониторинга событий создаёт инцидент информационной безопасности и оповещает систему оркестрации, автоматизации и реагирования на инциденты безопасности или платформу реагирования на инциденты. Та, в свою очередь, отправляет управляющее воздействие в Консоль управления Яндекс Браузера для организаций, используя API Консоли.

Получив управляющую команду, Консоль моментально и автоматически отправляет команду блокировки исходного расширения для всех управляемых Браузеров, предотвращая таким образом возможные атаки на других сотрудников.

Таким образом, Браузер, взаимодействуя через Консоль управления с другими системами, может помочь предотвратить атаку, которая может оставаться невидимой для стандартного набора защитных решений. И это лишь один из примеров возможной интеграции.

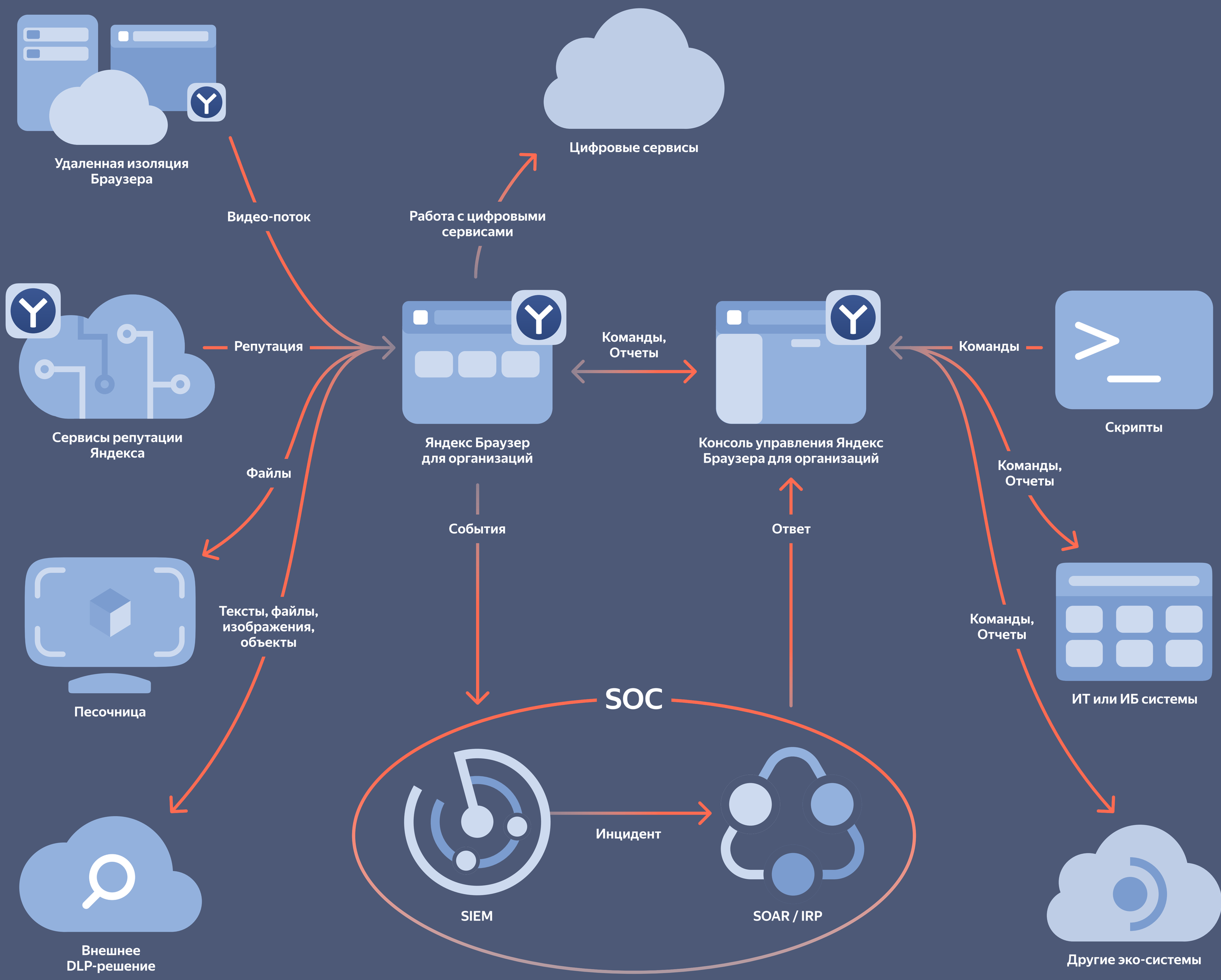
- ## Безопасный Браузер интегрированный в ИТ-инфраструктуру организации

  API Консоли управления позволяет реализовать широкий круг дополнительных сценариев взаимодействия с внешними системами, чтобы гармонично встроиться в существующую экосистему информационной безопасности организации.

  IT-администраторы и сотрудники службы ИБ могут автоматизировать процессы, связанные с управлением парком браузеров и реагированием на инциденты, и организовать взаимодействие с другими внешними экосистемами безопасности и управления, которые используются в организации.

  Яндекс Браузер для организаций — это не просто браузер, но настраиваемый корпоративный инструмент, способный помочь автоматизировать цикл обработки инцидентов безопасности и существенно повысить уровень прозрачности событий, связанных с активностью сотрудников на внутренних и внешних веб-ресурсах.

Безопасный Браузер интегрированный в ИТ-инфраструктуру организации



Яндекс Браузер | для организаций |

Наш сайт: browser.yandex.ru/corp

Telegram
Дзен
YouTube
ВК Видео

Связаться с нами: