ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ / Система мониторинга и управления событиями информационной безопасности «СёрчИнформ SIEM»

ЭКОНОМИКА

Дополнительная информация по кейсу

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ БИЗНЕСА

КРАТКОЕ ОПИСАНИЕ РЕШЕНИЯ

Решение представляет собой систему мониторинга и управления событиями информационной безопасности в режиме реального времени. Аккумулирует данные из различных источников, анализирует их, фиксирует уязвимости, ИБ-инциденты и оповещает о них службу безопасности. Сопоставляет внешне не связанные события и по их совокупности обнаруживает угрозы. Как SIEM помогает бизнесу:

- собирает и анализирует потенциально опасные события от всех устройств и ПО;
- выявляет инциденты ИБ: взломы, вирусные заражения, опасную активность пользователей, устройств и ПО;
- сообщает об угрозах в реальном времени, позволяет проактивно реагировать на инциденты.
- помогает управлять расследованиями инцидентов и отчитываться регулятору

SEARCHINFORM
INFORMATION SECURITY

УСЛОВИЯ РЕАЛИЗАЦИИ И ИСПОЛЬЗУЕМЫЕ ДАННЫЕ

Для внедрения требуется: серверное оборудование (за исключением внедрения в облаке); лицензии серверных ОС и СУБД.

В помощь заказчикам вендор предоставляет техническое задание к закупке необходимых компонентов.

Финансово-экономическая модель: Для госзаказчиков доступна закупка по 44-ФЗ и 223-ФЗ, для коммерческих компаний – на общих условиях. Основная модель – приобретение бессрочных лицензий и ежегодной технической поддержки (техническое обслуживание, обновления, доработки, обучение работе с ПО, консультации). Доступно внедрение по сервисной модели: в облаке, по подписке на период, в формате аутсорсинга.

Данные: данные заказчика, предоставляемые в рамках реализации проекта.

ПРОБЛЕМНАЯ СИТУАЦИЯ

- Подбор паролей, попытки нелегитимного доступа к сети или ее сегментам; изменение конфигураций и настроек, ошибки и превышение полномочий привилегированными пользователями
- Вирусные заражения и эпидемии, взломы, DDoS- и другие кибератаки
- Сбои и ошибки в работе ПО, перегрев оборудования и т.д.
- Уязвимости в корпоративных системах, грозящие взломами и заражениями
- Поздняя реакция на угрозы и инциденты информационной безопасности, несвоевременная отчетность регулятору

СТОИМОСТЬ И СРОКИ

От 6 часов

От 25 тыс. рублей
(за 1 бессрочную лицензию для контроля 1 пользователя (узла)

РЕЗУЛЬТАТЫ ЦИФРОВИЗАЦИИ

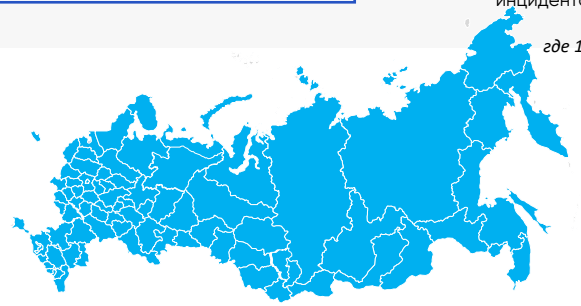
- Фиксируемые попытки нарушения сотрудниками норм ИБ, нерегламентированных изменений прав доступа, конфигурации и настроек корпоративных систем (в т.ч. со стороны привилегированных пользователей): на **95%*** реже
- Количество свершившихся (непредотвращенных) кибератак: на **95%** меньше (за счет раннего обнаружения угроз)
- Количество ошибок конфигурации, эксплуатации, обновления IT-оборудования и ПО: на **70%** меньше (за счет раннего выявления проблем и своевременной профилактики)
- Раннее выявление уязвимостей и сопутствующих угроз (благодаря встроенному сканеру уязвимостей), устранение проблем до наступления инцидента: на **80%** чаще
- Снижение трудовых и временных затрат на пресечение (благодаря функционалу активного реагирования), расследование (благодаря функционалу таск-менеджмента) и фиксацию (в т.ч. в форме отчетов в SOC и ГосСОПКА) выявленных инцидентов ИБ: **75%**

**субъективные оценки клиентов «СёрчИнформ», где 100% - среднее суммарное количество инцидентов ИБ, зафиксированных системой*

Сергей Ожегов

Генеральный директор
ООО «СёрчИнформ»

order@searchinform.ru



ОПЫТ РЕАЛИЗАЦИИ

Решения «СёрчИнформ» внедрены во всех регионах РФ.