КСБ-СОФТ

SOC RAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

БЕСПЛАТНОЕ ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

SOC RAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ КОМПАНИИ КСБ-СОФТ

НЕПРЕРЫВНАЯ ЗАЩИТА ОРГАНИЗАЦИЙ
ОТ УГРОЗ БЕЗОПАСНОСТИ

Мониторинг инцидентов ИБ в режиме 24/7

Вариативность при подключении

Высокий SLA – моментальное реагирование на инциденты

Индивидуальный подход к потребностям компании
и особенностям ее инфраструктуры

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

Вы можете бесплатно оценить качество предоставляемых услуг SOCRAT

Что входит в пилотное подключение?

- мониторинг 8x5 в ручном режиме
- время реакции на инцидент – до 24 часов с момента обнаружения (без учета выходных и праздничных дней)
- состав контролируемых узлов – до 10 узлов (АРМ/серверы) и/или 1 система обнаружения вторжений уровня сети
- длительность пилота – один календарный месяц

ЭТАПЫ ПИЛОТНОГО ПОДКЛЮЧЕНИЯ

ПРЕДВАРИТЕЛЬНЫЕ РАБОТЫ

- Подписываем соглашение между SOCRAT и организацией
- Организация назначает ответственное лицо за инциденты ИБ
- Организация заполняет анкету с указанием объектов мониторинга и канала взаимодействия

ЭТАПЫ ПИЛОТНОГО ПОДКЛЮЧЕНИЯ

ПОДКЛЮЧЕНИЕ К SOCRAT

- Устанавливаем и настраиваем компоненты системы мониторинга

- Устанавливаем и настраиваем защищенный канал связи между SOCRAT и организацией

ИЛИ

- Интегрируем имеющиеся в организации системы сбора информации с SOCRAT

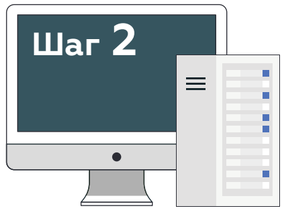
КАК SOCRAT РЕАГИРУЕТ НА ИНЦИДЕНТЫ

1 SOC-специалисты
просматривают события безопасности

НЕТ

Событие оказалось потенциально опасным?

ДА



2 SOC-специалисты
проводят первичный анализ событий безопасности

НЕТ

SOC-специалисты заподозрили наличие инцидента?

ДА

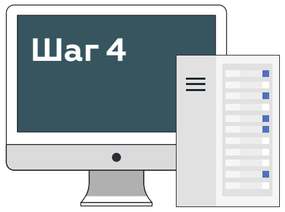
3 SOC-специалисты
создают карточку инцидента
уведомляют ответственное лицо в организации об инциденте

Организация подтвердила инцидент?

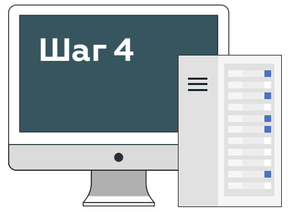
НЕТ

ДА

4 SOC-специалисты
делают отметку, что инцидент ложнопозитивный
закрывают инцидент



SOC-специалисты возвращаются к просмотру событий безопасности



4 Ответственное лицо в организации
выполняет рекомендации Центра мониторинга

SOC-специалисты
закрывают инцидент
усиливают контроль за угрозами безопасности

SOC-специалисты возвращаются к просмотру событий безопасности

История о том, как работает SOC

ПИЛОТНОЕ ПОДКЛЮЧЕНИЕ

ЧТО В ИТОГЕ

По итогам пилотирования специалисты SOCRAT предоставят отчет, содержащий

Карточки всех выявленных инцидентов ИБ

Следы вредоносного ПО (при обнаружении)

Статистику по выявленным событиям и инцидентам ИБ

Нелегитимные действия пользователей (при обнаружении)

Выявленные ошибки конфигураций (при обнаружении)

Рекомендации по повышению уровня безопасности в организации

КТО МЫ

Компания КСБ-СОФТ – системный интегратор в сфере информационной безопасности и импортозамещения информационных технологий

- Анализ уязвимостей и тестирование на проникновение
- Мониторинг и реагирование на инциденты ИБ
- Консалтинг по безопас-ной разработке и сертификации СЗИ
- Аудит информационной безопасности
- Обеспечение безопасности КИИ и АСУ ТП
- Защита информации в ГИС и ИСПДн

Наш вклад в кибербезопасность

Разработанные командой КСБ-СОФТ специализированные утилиты и скрипты для тестирования безопасности ИТ-инфраструктуры организаций

Созданный в соответствии с передовыми практиками цикл безопасной разработки

Активная деятельность в российском комьюнити безопасной разработки

Наши клиенты – государственные и коммерческие организации в 80 регионах России

На сегодня в портфолио компании 4000 проектов разной степени сложности, полученный опыт в которых помогает нам подбирать эффективные решения для защиты информационных ресурсов наших клиентов

SOC
RAT

SECURITY
OPERATION
CENTER
RUSSIAN
ANALYTICS
TEAM

SOCRAT – ЦЕНТР ПРОТИВОДЕЙСТВИЯ АТАКАМ

КСБ-СОФТ

8 800 3333-872

+7 (8352) 322-322

info@ksb-soft.ru

КАНАЛ
«МНЕНИЕ ИНТЕГРАТОРА»

ПОДКАСТ
«SOCRAT ЗА СТЕКЛОМ»

САЙТ
КОМПАНИИ