

Информационная безопасность. Потенциальные риски, ставшие реальностью

Родион Сергеевич Нестеров

Менеджер группы развития решений информационной безопасности в ЮФО.

Что происходит?

Угрозы кибербезопасности

Статистика на территории Российской Федерации

Кратный рост числа направленных атак:

- Государственные организации
- Банки
- Сайты СМИ
- Коммерческие структуры
- Производство



Векторы атак:
RUS, PUC, POC, .ru, .рф
и др.



Вызовы Нового Времени

Массовый взлом сайтов 2023

XGIN	PASSWORD	CHECKWORD	ACTIVE	NAME	LAST_NAME	EMAIL	LAST_LOGIN
greensight.ru	\$6\$0VzasAoLxqv0R9580cy	Гринсайт	**	Гринсайт	Гринсайт	greensight.ru	2023-05-23
@rosaski.com	gJnFFq5600CkKk5T3iaaY	Контент-менеджер	**	***	***	rt@rosaski.com	2019-11-11
mut	***	***	**	***	***	***	2018-09-13
aski@rosaski.com	df1F0pbN2530wEbmc4t150Y	***	**	***	***	ask@rosaski.com	2018-09-12
aski_1@rosaski.ru	tnwCz0F499TEhh8jH680Y	***	**	***	***	aski_1@rosaski.ru	2018-09-13
greensight.ru	"3J\t4nR,e6Bdxk3Az927N	Рона	**	Гринсайт	Гринсайт	greensight.ru	2019-10-23
greensight.ru	fdxR2217647ZnutlNezn43cy	Отельер TL	**	***	***	greensight.ru	2021-12-15

@dataleak

Утечки информации

Продолжается "слив" данных из крупных компаний. Хакер уже "слил" данные [book24.ru](#), [askona.ru](#), [gloria-jeans.ru](#), «Ашан», «Твой Дом», «Буквоед», «Едим Дома», «Леруа Мерлен» и «ТВОЕ».

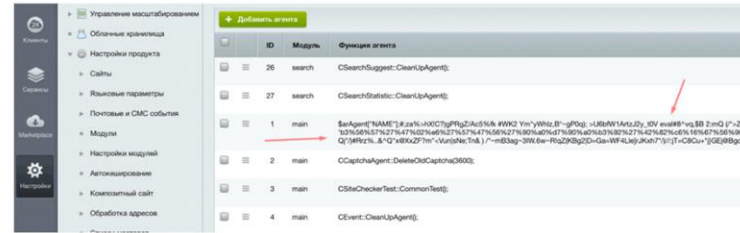
Сейчас были выложены в свободный доступ частичные дампы с информацией клиентов/пользователей предположительно: книжных интернет-магазинов «Читай-город» и «Эксмо», сайтов издательства «АСТ» и горного курорта «Роза Хутор».

Массовый дефейс веб-сайтов .RF

Средний 7 мин 50К

Блог компании RUVDS.com, CMS*, Информационная безопасность*, Разработка веб-сайтов*, 1С-Битрикс*

Кейс



26 мая 2023 года произошёл массовый дефейс веб-серверов национального сегмента сети интернет .RF. В качестве цели атаки выступила CMS «Битрикс».

Утечки информации

Вчера в открытый доступ были выложены фрагменты SQL-дампа из CMS «Bitrix» предположительно интернет-аптеки «Вита» ([vitaexpress.ru](#)).

В двух файлах находится частичная информация из таблиц заказов и зарегистрированных пользователей.

В свободно доступных фрагментах: 666,944 записи пользователей (645 тыс. уникальных адресов эл. почты и 654 тыс. уникальных номеров телефонов) за период с 29.08.2015 по 23.03.2023 и 351,708 заказов (933 и 943 уникальных адреса и номера

Инсайдер поневоле

- Авторизованные пользователи внутри сети намеренно или по незнанию могут стать орудием в руках опытных хакеров
- >50% кейсов вокруг ИБ связаны с действиями, осуществляемые от лица авторизованных внутри периметра учётных записей
- Контроль и повышение осведомлённости, как ключевые инструменты устранения рисков



Регуляторная политика

- Усиление контроля за обработкой и хранением персональных данных(152ФЗ)
- Изменения в 187ФЗ(250 Указ). Персональная ответственность за состояние информационной безопасности в организации
- Ужесточение наказания за нарушение 152ФЗ/187ФЗ. Обратные штрафы
- Переход от декларированной безопасности к реальной, через аудит и разработку дорожной карты

Тренды информационной безопасности РФ



Практическая ИБ

От бумажной безопасности и аттестации раз в три года к проверке реализуемости недопустимых событий, регулярными оценками защищенности и киберучениям



Минцифры

Усиление роли Минцифры в качестве регулятора по вопросам информационной безопасности (повышение осведомленности, НУЦ, оценка защищенности и т.п.)



Импортозамещение

Полный запрет на использование иностранных программных решений и средств защиты на всех объектах КИ и иных «критических» организациях



250-й указ

Усиление роли ИБ на предприятии через включение ответственного за ИБ в исполнительный орган предприятия и фокус на недопустимые события



КИИ

Изменение законодательства в области безопасности критической инфраструктуры, изменение правил категорирования и использования средств и ПО в КИИ



Персональные данные

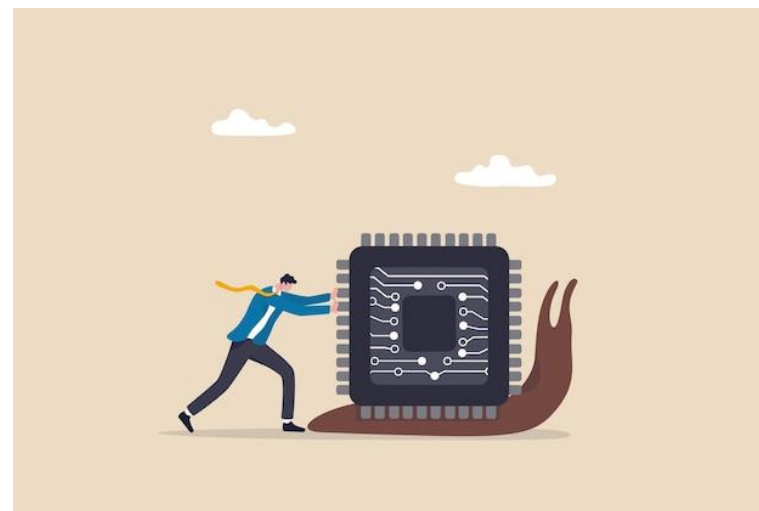
Усиление ответственности за утечки персональных данных в виде обратных штрафов и новых статей в Уголовный кодекс

Актуальные штрафы за нарушения

Статья	Характер нарушения	Минимум	Максимум
13.11 ч.1	Нарушения при обработке ПДн	60 000	100 000
13.11 ч.1.1	Повторное нарушение	100 000	300 000
13.11 ч.2	Обработка без письменного согласия субъекта	30 000	150 000
13.11. ч.2.1	Повторное нарушение	300 000	500 000
13.11. ч.5	Невыполнение требований субъекта об уточнении, блокировании или уничтожении ПДн в установленный срок	50 000	90 000
13.11. ч5.1	Повторное нарушение	300 000	500 000
13.11. ч.8	Нарушения при локализации баз данных на территории РФ	1 000 000	6 000 000
13.11.ч.8.1	Повторное нарушение	6 000 000	18 000 000

Рынок ПАК и ПО

Необходимо заместить уходящих с рынка игроков
Проблемы с обновлением и поддержкой импортных решений



- Срок поставки аппаратных решений до 6-9 месяцев
- Дополнительная нагрузка на бюджет

Что делать?

Российская безопасность

- Предложения Российских вендоров покрывают 90 процентов всех классов решений в области Информационной Безопасности(ИБ)
- Российские решения соответствуют стандартам мирового уровня
- Компетенции интеграторов, подтверждённые международными сертификатами
- Наличие собственных регуляторов, нормативных актов и стандартов в области Информационной Безопасности
- Многолетняя практика соответствие нормативным актам и требованиям регуляторов в области Информационной Безопасности
- Информационная безопасность как сервис



Защита сети

МЕЖСЕТЕВЫЕ
ЭКРАНЫ

 **UserGate**

 SANGFOR



SMART-SOFT



КОД
безопасности



CHECK POINT™

СИСТЕМЫ
АНАЛИЗА
ТРАФИКА



POSITIVE
TECHNOLOGIES

kaspersky

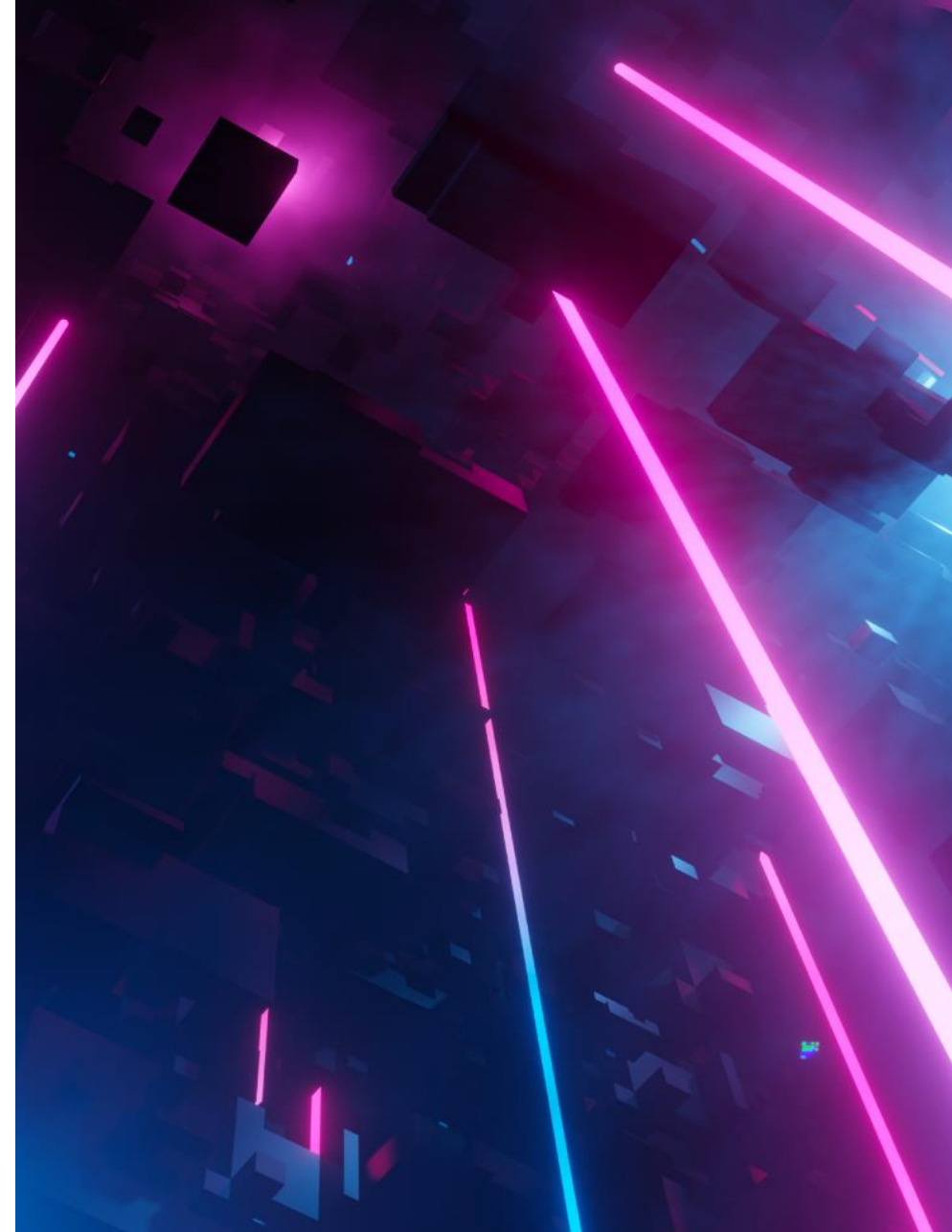


ГАРДА
ТЕХНОЛОГИИ

F.A.C.C.T.

Защита конечных точек

АНТИВИРУСЫ	  
EDR	   



Двухфакторная аутентификация

СИСТЕМЫ ДВУХФАКТОРНОЙ
АУТЕНТИФИКАЦИИ

Avanpost

Identity Blitz

Аладдин

MULTIFACTOR

СКБ Контур

INDEED ID

Защита от утечек\контроль пользователей

**СИСТЕМЫ ЗАЩИТЫ ОТ УТЕЧЕК
ИНФОРМАЦИИ**

INFOWATCH

Стахановец
система контроля сотрудников

SEARCHINFORM
INFORMATION SECURITY

SOLAR SECURITY
software&services

staffcop

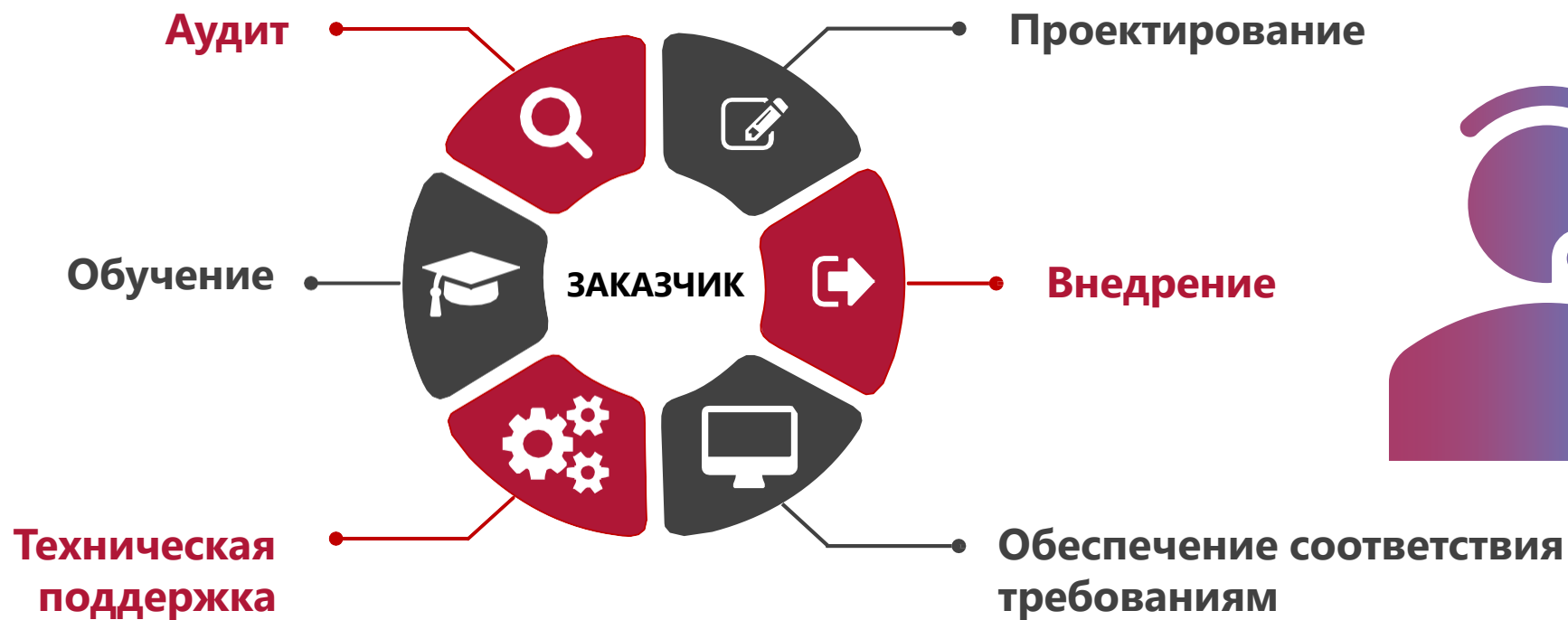
ZECURION


Реагирование на события ИБ


СИСТЕМЫ СБОРА И КОРРЕЛЯЦИИ СОБЫТИЙ	 POSITIVE TECHNOLOGIES   RUSIEM Всё под контролем  SEARCHINFORM INFORMATION SECURITY  kaspersky
СИСТЕМЫ АВТОМАТИЗАЦИИ РЕАГИРОВАНИЯ	 Security Vision  R-Vision

ЧЕМ МОЖЕТ ПОМОЧЬ SOFTLINE

Безопасность на всех этапах жизненного цикла систем



 **Топ 2 рейтинга**
CnewsSecurity 2013-2016

 **380 специалистов**
по направлению ИБ

Кибербезопасность

Инфраструктура

- Безопасное рабочее место
- Сетевая безопасность (NGFW, IPS, ATP)
- Облачная безопасность (CASB)
- Защищенные каналы связи (VPN)
- Аудит изменений
- Безопасная совместная работа с контентом
- Защита баз данных (DAM)
- Безопасная мобильность (MDM, EMM)
- Контроль целостности
- Безопасность почтового и веб трафика

Защита данных

- Тренинги/проверки сотрудников (awareness)
- Защита данных (DLP)
- Управление доступом (IDM, PAM, PIM, 2FA)
- Шифрование данных

Безопасность приложений

- Анализ кода
- Безопасность приложений (WAF)
- Управление конфигурациями
- Тесты на проникновение (pentest)

- Управление инцидентами (SIEM, IRP)
- Security Operation Center (SOC)
- Индустриальные стандарты
- Управление рисками
- Соответствие законам (152ФЗ, GDPR, СТОБР, 382П. 683-684П. 187ФЗ)
- Авторские продукты (ETHIC)
- КИИ

НАШИ СЕРВИСЫ:



Проектирование



Пилотирование



Внедрение



Техподдержка



Управляемые сервисы

Повышение осведомлённости пользователей

Оценка текущего состояния осведомлённости сотрудников, профессиональных компетенций



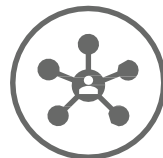
тестирование сотрудников заказчика

Платформы класса Awareness



PHISHMAN, ASAP, Антифишинг, СтопФиш, Secure-T

Сервис повышения осведомлённости



- Платформа в облаке
- Платформа в облаке+сервис
- Эл.курсы по подписке
- Фишинг по подписке

Коробочные электронные учебные курсы для СДО заказчика



Более 30+ курсов по разным темам ИБ

Разработка материалов для заказчика



- Электронные курсы и тесты
- Видеоролики
- Плакаты, скринсейверы
- Дайджесты
- Комиксы
- Игры
- День по ИБ
- Вебинары

Разработка стандарта повышения осведомлённости работников в области ИБ



- По направлениям
- По ролям

Экспресс-аудит

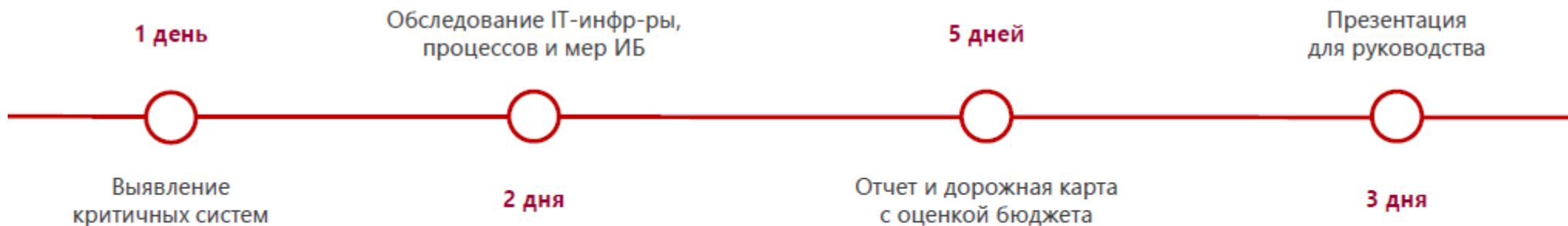


Верхнеуровневая оценка
состояния ИБ

Основывается на экспертизе.

Быстро делается и не отнимает
много времени у заказчика

Разработка рекомендаций по
совершенствованию уровня
обеспечения ИБ



10-15 рабочих дней на проект

Экспресс анализ защищенности инфраструктуры

Pentest

Как проводится экспресс анализ защищенности внешней инфраструктуры

- 1** Подготовительная стадия
 - Согласование границ работ.
 - Согласование протоколов взаимодействия.
- 2** Проведение работ
 - Анализ защищенности внешнего сетевого периметра (до 10 IP).
 - Анализ защищенности веб-приложения (до 1 шт., за исключением сложных веб-ресурсов)*.
- 3** Подведение итогов
 - Подготовка отчета с описанием работ и выводами.
 - Анализ результатов и подготовка рекомендаций.

Быстрый результат при небольших ресурсных и временных затратах.

- По результатам проекта вы получаете оценку текущей защищенности области исследования.
- Рекомендации, позволяющие устранить выявленные недостатки в существующей области исследования.

СРОК РЕАЛИЗАЦИИ:
2 недели

СТОИМОСТЬ:
350 тыс. руб.

Сервис SOC

Что это

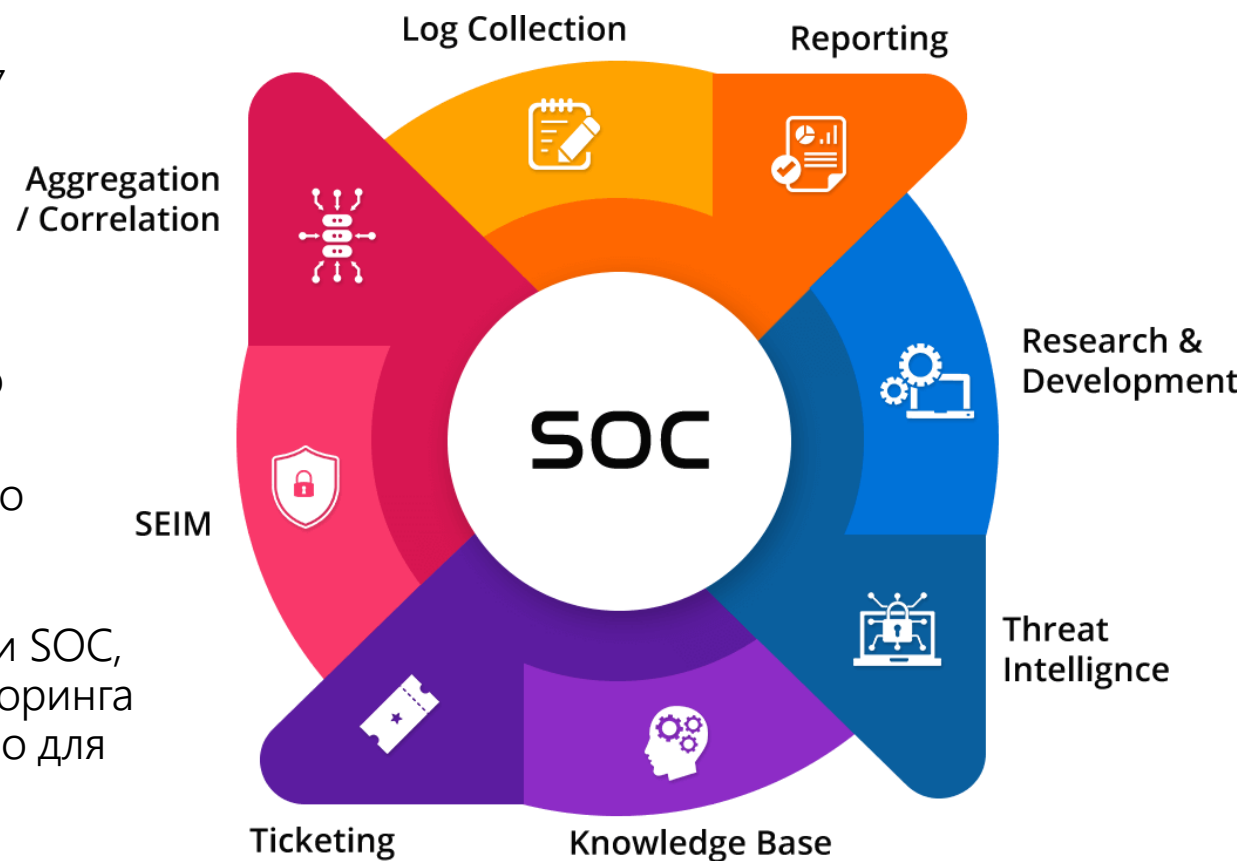
- Мониторинг состояния ИБ в режиме 24x7
- Выявление кибератак на ранних стадиях
- Минимизация потерь за счет оперативного разбора инцидентов

Зачем нужно клиенту

- Возможность оперативно и сравнительно недорого запустить SOC
- Уникальные компетенции, которые сложно найти и еще сложнее удержать

Варианты реализации

- Basic – базово необходимые возможности SOC, позволяющие запустить процессы мониторинга в круглосуточном режиме. Рекомендовано для средних компаний (1000 – 1500 ПК)
- Extended – расширенные возможности, включающие автоматизированную реакцию и углубленный разбор инцидентов ИБ



Соответствие требованиям



Соответствие требованиям

- Приведение в соответствие 187-ФЗ;
- Приведение в соответствие 152-ФЗ (17 и 21 приказа ФСТЭК);
- Приведение в соответствие ГОСТ57580
- Специальные проверки и специальные исследования
- Аттестация объектов автоматизации





Цифровая Трансформация.
Успешная. Эффективная.

Родион Нестеров

Менеджер группы развития решений
информационной безопасности в ЮФО.

Отдел территориальной экспертизы.

Мобильный: +7 (928) 882 87 77

Тел: +7 (861) 992-47-08 ext. 3093

Rodion.Nesterov@softline.com