



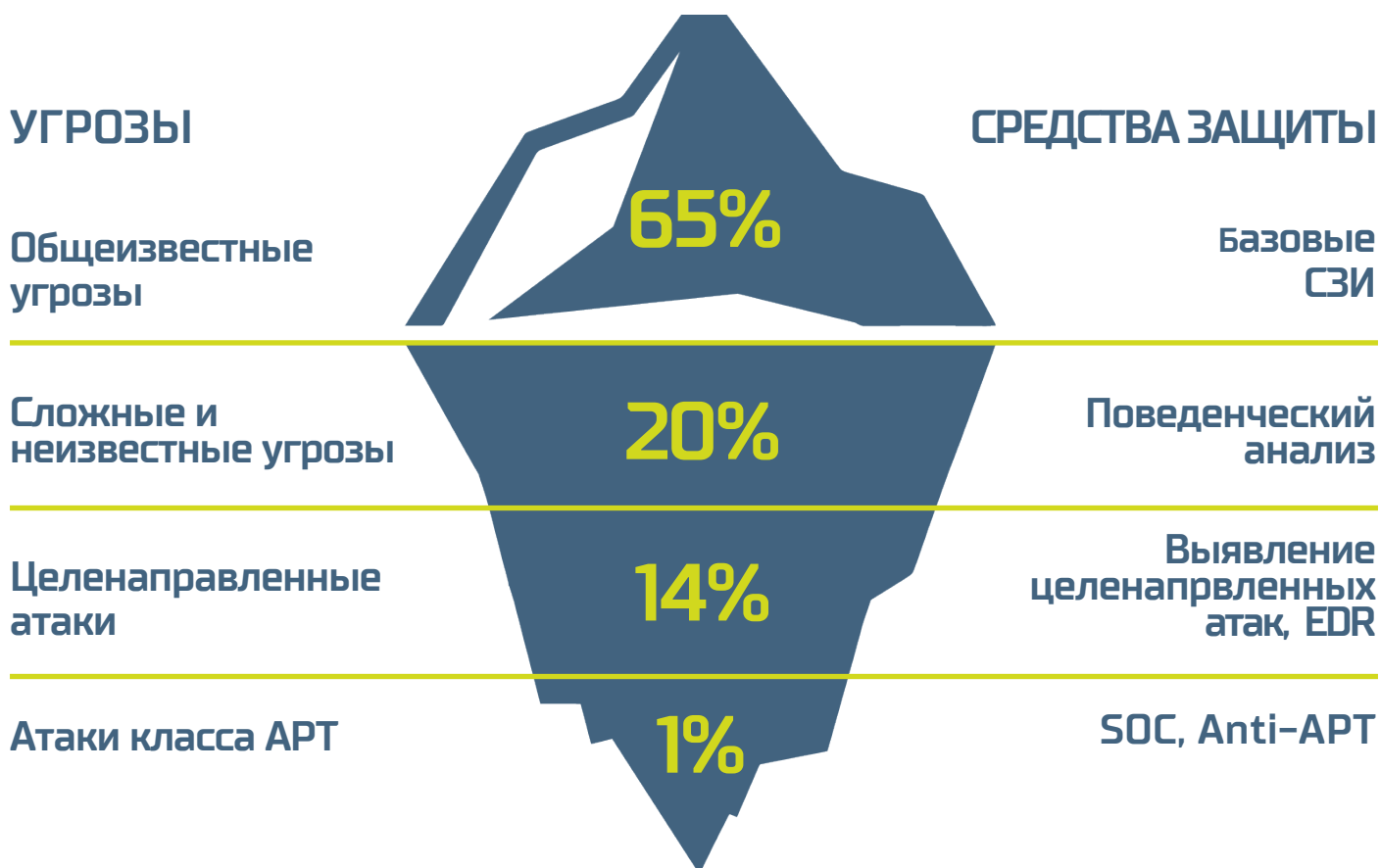
СЕРВИСЫ ЗАЩИТЫ ОТ АРТ, ВЫЯВЛЕНИЯ И РЕАГИРОВАНИЯ НА СЛОЖНЫЕ УГРОЗЫ

- ACR SERVICE EDR
- ACR SERVICE APT HUNTING
- ACR SERVICE APT LIQUIDATION

КОНТАКТЫ

121096, г. Москва,
ул. Василисы Кожиной, д. 1, к. 1
БЦ «Парк Победы»
Телефон: +7(495) 269-26-06
E-mail: info@angarapro.ru

В ТЕОРИИ



НА ПРАКТИКЕ

ДОРОГО Высокая стоимость владения Anti-APT и SOC

ДОЛГО Внедрение Anti-APT и SOC требует изменения инфраструктуры и занимает много времени

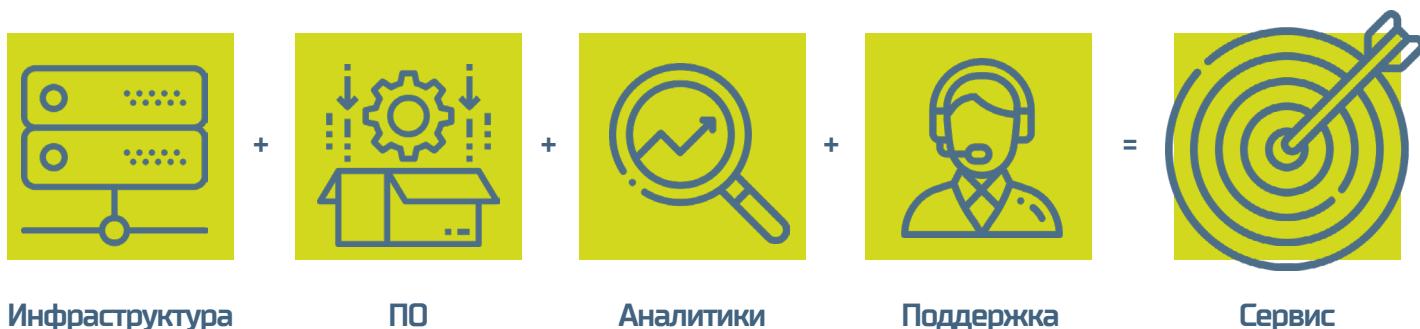
ТЯЖЕЛО Стоимость защиты сильно вариативна в пересчете на 1 пользователя — решения рассчитаны на крупные инфраструктуры. Если нужна защита только критических хостов, срок окупаемости существенно увеличится.

БОЛЬШОЙ РАЗРЫВ Между базовой защитой и защитой от сложных и таргетированных атак под управлением SOC (инвестиции, зрелость процессов, компетенции) нет промежуточного решения, фокусного для критических хостов и пользователей.

РЕШЕНИЕ – ACR SERVICE

Angara Professional Assistance предлагает сервис, построенный на базе продуктов «Лаборатории Касперского» — KATA и KEDR. Использование подписочной модели с понятными параметрами тарификации позволяет защищать и гибко управлять подключенными к сервису пользователями и хостами.

В рамках услуги аналитики-эксперты Angara Cyber Resilience Center (SOC ACRC) осуществляют удаленный мониторинг, выявление и реагирование на инциденты информационной безопасности на критичных хостах.



За инвестиции, приблизительно равные стоимости коробочных лицензий, вы получаете сервис, включающий инфраструктуру с гарантированной доступностью, непрерывный анализ событий квалифицированными специалистами с четким SLA.

СТАТИСТИКА

На каждые 100 пользователей организации:



ЧТО ВЫ ПОЛУЧАЕТЕ

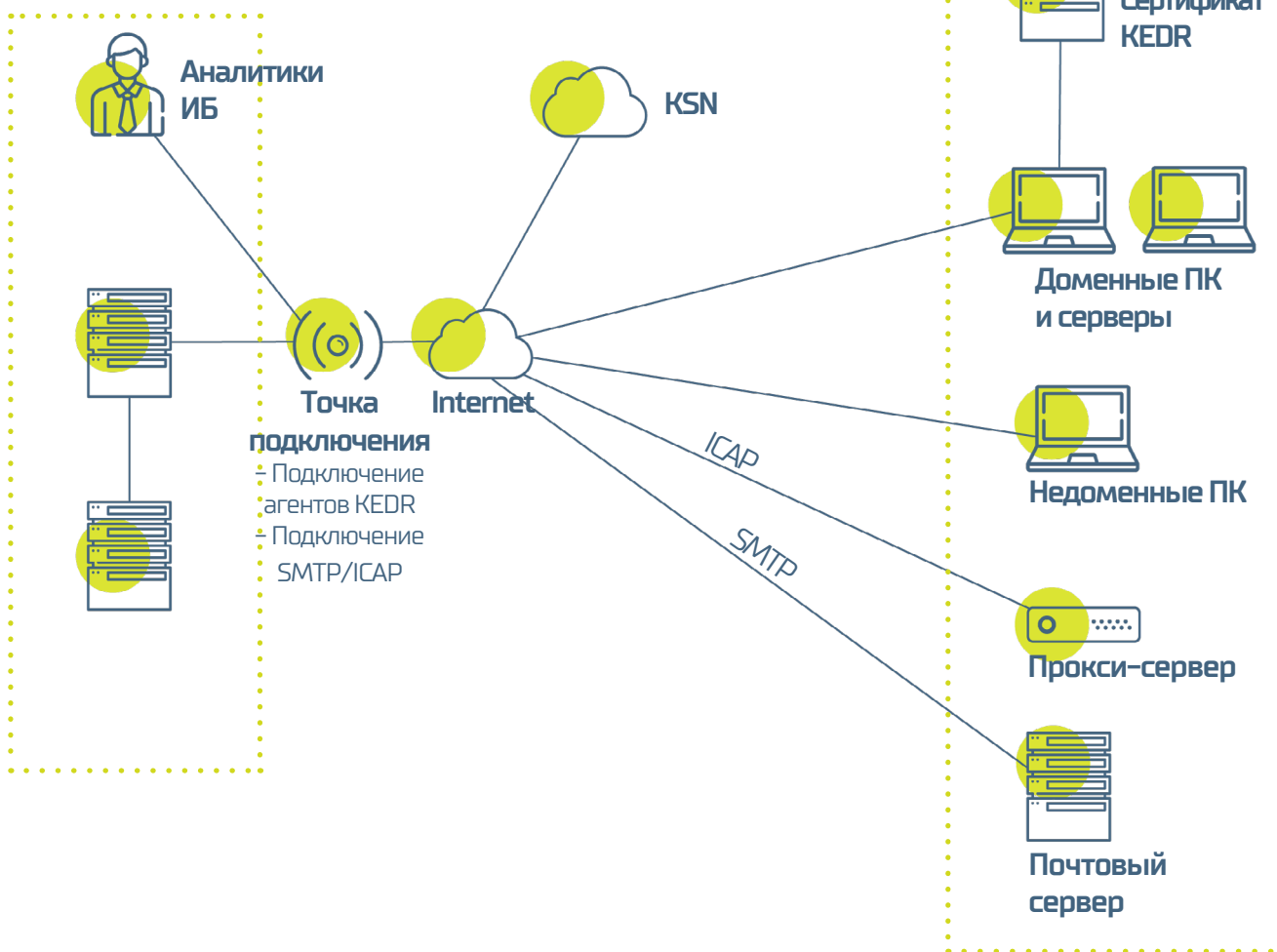
- Защиту от сложных целенаправленных угроз критичных хостов и пользователей на базе эффективных технологий всемирно известного производителя средств защиты;
- Своевременную реакцию на критичные инциденты (заблокировать запуск файла, поместить в карантин на всех хостах, извлечь экземпляр вредоносного ПО);
- Гарантированный уровень сервиса, подкрепленный финансовой ответственностью;
- Инструмент для оперативного и ретроспективного поиска по IOC и фактов выполнения или скачивания любых файлов (по правилам YARA);
- Аналитику и расследование выявляемых инцидентов экспертами SOC;
- Наглядные отчеты, прозрачно раскрывающие эффективность услуги на основе статистики;
- Оптимизацию расходов — стоимость сервиса, сопоставима со стоимостью лицензий и оборудования на защищаемую единицу;
- Возможность бесшовно повысить уровень сервиса до полноценных услуг ACRC SOC (требуется подключения дополнительных источников и развертывания коллектора логов на площадке заказчика).

КАКИЕ ОБЪЕКТЫ ЗАЩИЩАЮТСЯ

- Рабочие места с ОС Windows, входящие в доменную структуру на базе MS AD;
- Серверы с ОС Windows, входящие в доменную структуру на базе MS AD;
- Почтовые ящики пользователей на управляемом (не арендуемом) почтовом сервере;
- Любые устройства, подключённые к сети интернет через управляемый (не арендуемый) прокси-сервер.

АРХИТЕКТУРА СЕРВИСА

ANGARA PROFESSIONAL ASSISTANCE



ПАРАМЕТРЫ КАЧЕСТВА УСЛУГИ

ПАРАМЕТР	ОПИСАНИЕ	ЗНАЧЕНИЕ
Режим услуги	Временной интервал и график оказания услуги для обнаружения, оповещения и реагирования	9x5 или 24x7
Доступность услуги	% отношения длительности непрерывной работы сенсора КАТА	97% в квартал, единовременный простой не более 4 часов
Время обнаружения инцидента	Максимальное время от выявления до начала расследования инцидента	Не более 15 минут
Время оповещения об инциденте	Среднее время от выявления до момента отправки уведомления по итогам проведенного расследования	45 минут
Время реагирования на инцидент	Среднее время от выявления до момента запуска задачи реагирования в КАТА	60 минут
Время решения заявок на техническое сопровождение	Максимальное время решения заявок по техническому сопровождению (без учета времени работ в зоне ответственности производителя или клиента)	Не более 4 часов

КАК ПОДКЛЮЧИТЬСЯ

Подключение клиента производится в 3 этапа:

- 1 Фиксируем сведения о критичных хостах и пользователях, формируем сертификаты защищенного обмена
- 2 Подключаем копию почтового трафика, прокси сервер и устанавливаем агенты KEDR
- 3 Проверяем корректность работы, фиксируем параметры реагирования

Прогнозируемая длительность подключения — до 2х недель на 100 хостов/пользователей

О ГРУППЕ КОМПАНИЙ ANGARA

Группа компаний Angara, представленная головной организацией Angara Technologies Group и сервис-провайдером Angara Professional Assistance, предлагает полный спектр услуг по информационной безопасности, начиная с поставки и внедрения оборудования и ПО, заканчивая комплексом мероприятий по сопровождению ИТ- и ИБ-систем клиентов.

Группа компаний входит в:

ТОП-20 крупнейших компаний информационной безопасности (13 место, TAdviser);

ТОП-20 крупнейших поставщиков для банков (19 место, TAdviser);

ТОП-50 крупнейших поставщиков ИТ услуг (19 место, TAdviser)

ТОП-100 крупнейших ИТ-компаний России по версии CNews и TAdviser.

Angara Technologies Group специализируется на проектировании, внедрении и сопровождении систем и решений в области информационной безопасности, помогая совершенствовать процессы и повышать устойчивость информационных и технологических инфраструктур.

Angara Professional Assistance — это высокотехнологичный сервис-провайдер широкого набора тиражируемых услуг кибербезопасности (MSSP).

ИСТОРИЯ УСПЕХА

КОМПАНИЯ

ПРОЕКТ

Банк «Санкт-Петербург»

[Трансформация центра мониторинга ИБ \(SOC\)](#)

ООО «ИНБАНК»

[Оказание услуг по мониторингу ИБ \(SOC\)](#)

Банк «Юнистрим»

[Оказанию услуг по выявлению и реагированию на инциденты ИБ](#)

АО «ЭР-Телеком Холдинг»

[Создание системы сбора и визуализации событий ИБ](#)

Команда Angara Professional Assistance насчитывает более 50 экспертов в области поддержки и мониторинга информационных инфраструктур с опытом оказания услуг для крупнейших компаний нефтегазового, финансового и государственного секторов. Квалификация экспертов подтверждена сертификатами авторитетных международных организаций.

В фокусе компании: сервисы по модели Security as a service, аутсорсинг информационной безопасности, услуги по сопровождению и поддержке работоспособности ИТ- и ИБ-систем клиентов, повышению эффективности их работы и обеспечению непрерывности выполняемых функций.

[Отчет Центра киберустойчивости Angara Cyber ResilienceCenter \(ACRC\) за I полугодие 2019 года.](#)



КОНТАКТЫ

121096, г. Москва,
ул. Василисы Кожиной, д. 1, к. 1
БЦ «Парк Победы»
Телефон: +7(495) 269-26-06
E-mail: info@angarapro.ru