ANGARA

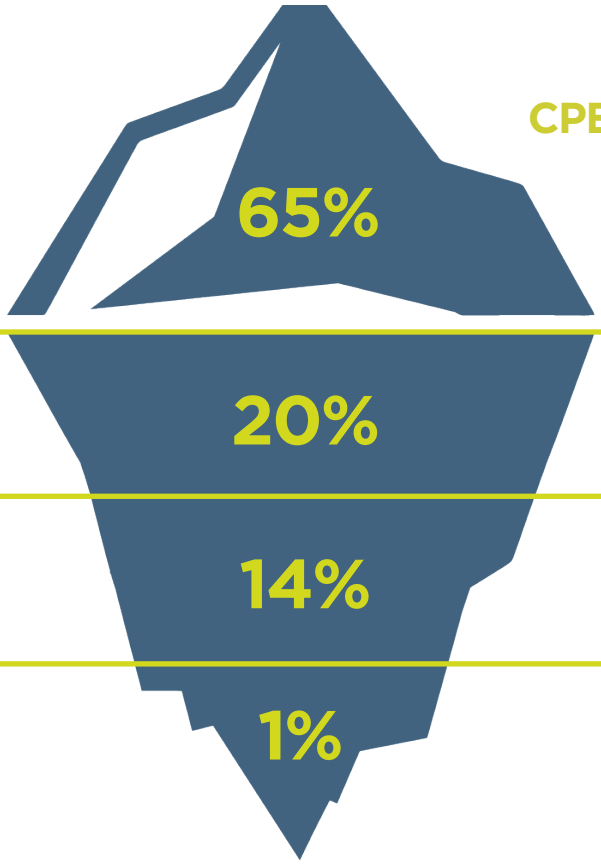
professional assistance

СЕРВИСЫ ЗАЩИТЫ ОТ APT, ВЫЯВЛЕНИЯ И РЕАГИРОВАНИЯ НА СЛОЖНЫЕ УГРОЗЫ

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

WWW.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 одного пользователя — решения рассчитаны на крупные инфраструктуры. Если нужна защита только критичных 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 критичных 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 Центра киберустойчивости Angara Cyber Resilience Center (SOC ACRC) осуществляют удаленный мониторинг, выявление и реагирование на инциденты информационной безопасности на критичных хостах.

Инфраструктура **ПО** **Аналитики** **Поддержка** **Сервис**

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:

60 инц. в месяц выявляют специалисты мониторинга при наличии средств активной защиты: хостовый антивирус, потоковый антивирус веб- и почтового трафика, системы фильтрации от спама.

1500 файлов **13000 ссылок** проходят репутационную проверку ежедневно при использовании доступа в интернет через браузер.

1,3 мбит/с полосы интернета составляет потребление всех агентов KEDR.

150 файлов **1500 ссылок** в электронных письмах проходит поведенческий и репутационный анализ ежедневно.

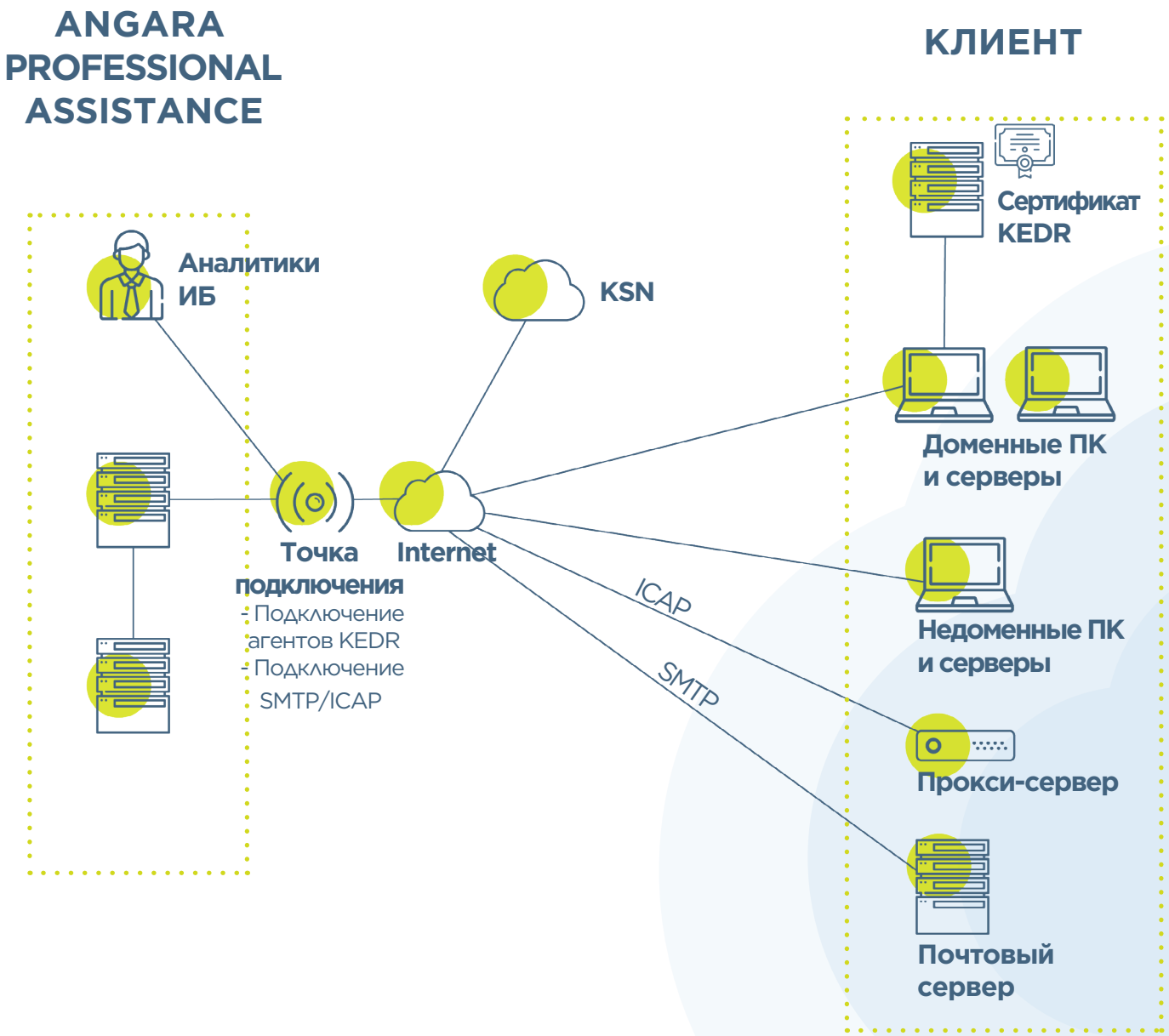
ЧТО ВЫ ПОЛУЧАЕТЕ

- 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 SOC (требует подключения дополнительных источников и развертывания коллектора логов на площадке заказчика).

КАКИЕ ОБЪЕКТЫ ЗАЩИЩАЮТСЯ

- Рабочие места и серверы с ОС Windows
- Рабочие места и серверы с ОС Linux
- Почтовые ящики пользователей на управляемом (неарендуемом) почтовом сервере.
- Любые устройства, подключенные к сети интернет через управляемый (неарендуемый) прокси-сервер.

АРХИТЕКТУРА СЕРВИСА



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 KATA	97% в квартал, едино-временный простой не более 4 часов
Время обнаружения инцидента	Максимальное время от выявления до регистрации подозрения на инцидент и начала расследования инцидента	30 минут
Время подтверждения инцидента	Максимальное время с момента регистрации подозрения на инцидент до отправки уведомления о подтверждении инцидента	1 час
Время расследования и реагирования	Максимальное время от момента подтверждения инцидента до отправки уведомления о расследовании инцидента или запуска задачи реагирования в KATA	4 часа
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.

О ГРУППЕ КОМПАНИЙ ANGARA

Группа компаний Angara, представленная системным интегратором 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 и программными разработками для анализа больших данных.

Группа компаний Angara входит в:

- **ТОП-20 крупнейших компаний информационной безопасности;**
- **ТОП-50 крупнейших поставщиков ИТ для финансового сектора;**
- **ТОП-50 крупнейших поставщиков ИТ-решений для госсектора;**
- **ТОП-50 крупнейших поставщиков ИТ-услуг;**
- **ТОП-100 крупнейших ИТ-компаний России.**

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»	Оказание 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 финансового, государственного, телекоммуникационного, промышленного секторов и ТЭК. 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 кибербезопасности ACRC за II полугодие 2020 года

ANGARA

professional assistance

Контакты

121096, г. Москва, ул. Василисы Кожиной,
д.1, к.1. БЦ «Парк Победы»
Телефон/факс: +7 (495) 269 26 07
E-mail: info@angarapro.ru

WWW.ANGARAPRO.RU