ANGARA
professional assistance

Отчет Центра киберустойчивости AngaraCyber Resilience Center (SOC ACRC) за II 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

Содержание

1 Общие сведения

Настоящий документ представляет собой отчет, основанный на статистике, собираемой ООО «Ангара ассистанс» в рамках предоставления услуг по мониторингу и управлению инцидентами информационной безопасности (ИБ) на базе Центра киберустойчивости AngaraCyber Resilience Center (далее – «Центр ACRC», «Центр киберустойчивости»).

Отчетный период с 01 июля по 31 декабря 2019 года.

В отчете представлены основные изменения в работе Центра мониторинга ACRC и новые возможности сервиса.

Данные статистики отражают производительность и текущую загрузку платформы ACRC. Представлены сведения по статистике зарегистрированных атак и подтвержденных инцидентов ИБ, выявленных аналитиками Центра. На основе этих данный выявлены основные тренды, сделаны прогнозы в сфере защиты данных от киберугроз и выделены основные задачи для ИБ подразделений.

2 Термины и определения

EPS (Events per Second)	Количество событий в секунду
Событие ИБ	Любое событие, связанное с изменением состояния системы (изменение конфигурации, появление новых пользователей или компьютеров, запуск программных процессов, установка сетевых соединений и т.п.)
Источник события	Программные средства или программно-аппаратные средства, генерирующие события
Подозрение на инцидент	Непредвиденное или нежелательное событие, которое может быть признаком Инцидента ИБ
Инцидент ИБ	Непредвиденное или нежелательное событие, негативное влияние которого на деятельность информационных систем достоверно установлено
Скоринг	Уровень опасности Инцидента ИБ

В рамках услуг Центром киберустойчивости обеспечивается автоматизированная обработка принимаемых Событий ИБ с целью их агрегирования и ранжирования, с последующей экспертной оценкой аналитиками ACRC.

Мониторинг Событий ИБ осуществляется по двум основным сценариям: Alerting и Hunting.

Alerting – метод, при котором поиск признаков различных атак осуществляется по разработанным правилам. Основную работу выполняет платформа ACRC, позволяющая автоматизировано обрабатывать большой поток данных и выявлять потенциальные Инциденты ИБ. Данные события требуют «ручного» анализа аналитиками ACRC с целью подтверждения или опровержения конкретного события.

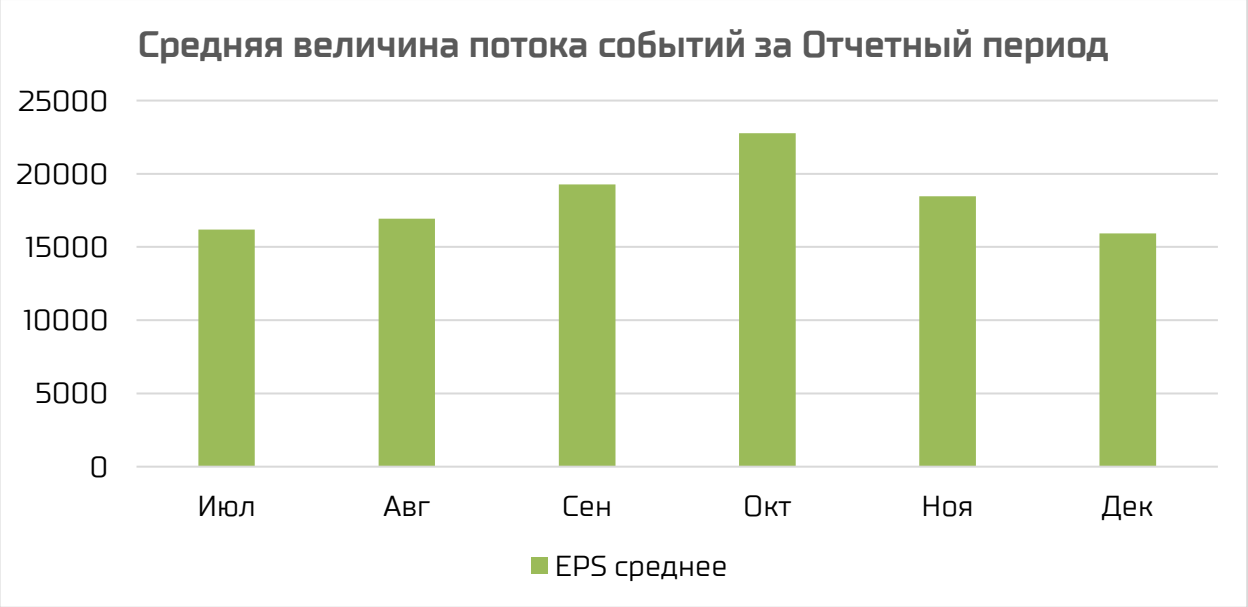
Hunting – метод анализа событий путем выявления нетипичной активности в работе определенных информационных систем (ИС), сетевом трафике и прочих событиях, обрабатываемых при мониторинге. Данный метод реализуется преимущественно «вручную» наиболее опытными аналитиками ACRC. Используются различные средства визуализации событий (диаграммы, графики) и системы эвристического анализа с применением техник искусственного интеллекта. При выявлении различных аномалий собирается дополнительная информация для подтверждения Инцидента ИБ. Новые способы выявления различных угроз впоследствии автоматизируются, составляются новые правила для платформы ACRC.

3 Статистика по данным

За II полугодие 2019 года средний поток принимаемых Центром ACRC событий не опускался ниже 15 000 EPS, а в октябре среднее значение EPS достигло своего максимума – 22 778 событий. Увеличение среднего потока событий обусловлено подключением новых Заказчиков. После подключения проводится ряд мероприятий по анализу и оптимизации потока входящих данных. В ходе данных работ исключаются события, не несущие полезной нагрузки, и устраняются различные ошибки конфигурации ИС, приводящие к генерации большого количества событий. После проведения этих работ наблюдается нормализация потока событий от источников, с чем связано уменьшение среднего EPS к концу отчетного периода.

При подсчете статистических данных не учитывается поток событий NetFlow, так как в подавляющем большинстве случаев такие события используются для обогащения информации при расследовании Инцидентов ИБ.

Если говорить о пиковых значениях до фильтрации входящих событий, то совокупное их количество от всех клиентов в текущем отчетном периоде кратковременно превышало отметку в 100 000 EPS.



Во втором полугодии 2019 года к мониторингу была подключена облачная платформа для управления конечными устройствами. Мобильные устройства давно используются в корпоративной среде, а соблюдение требований к безопасности и конфиденциальности данных – одна из важнейших задач наших Заказчиков. Подключение облачной платформы позволило обеспечить прозрачность и контроль за устройствами, выявлять Инциденты ИБ и отслеживать изменения в критичной для бизнеса системе. аналитиками ACRC отслеживаются события множественных ошибок аутентификации, сброса пароля для устройства, события удаленного управления устройствами, обращения к запрещенным ресурсам.

4 Статистика по подозрениям на Инциденты ИБ

При мониторинге Событий ИБ используется собственная модель «Cyber-Kill Chain», которая является упрощенной моделью MITRE, адаптированной на основе нашего опыта для организаций на территории РФ. Процессы мониторинга выстроены таким образом, чтобы максимально повысить вероятность выявления Инцидентов ИБ на ранних стадиях атак. На основе собственной матрицы признаков атак фиксируется каждое срабатывание правил автоматизированного выявления событий, которые могут сигнализировать об потенциальном инциденте ИБ и формируется Подозрение на инцидент с последующим расследованием для его подтверждения или опровержения.

Согласно нашей статистике, за II полугодие 2019 года было зафиксировано 4042 подозрения на атаку стадии «Заражение»: «Заражение ВПО», что почти в 7 раз превышает следующую по количеству подозрений атаку стадии «Разведка»: «Брутфорс». Под данным типом атаки подразумеваются многочисленные неуспешные попытки аутентификации на корпоративные сервисы Заказчика в следствии перебора учетных данных пользователей. Для внутренних сервисов данная активность часто связана с различными ошибками конфигурации. Сервисы доступные для пользователей сети Интернет так же подвергаются атакам. Согласно нашей статистике постоянно осуществляется сканирование, перебор учетных данных пользователей и попытки эксплуатации уязвимостей. Большая часть подобных атак отражается средствами защиты и не представляют серьезной угрозы.

В отличие от первого полугодия в топ потенциальных инцидентов ИБ поднимается «Установление связи с CNC». Данная активность вызвана усилением внимания к сетевым соединениям от подозрительных процессов и проверкой адресов назначения по различным репутационным базам. После установления подозрительного процесса, устанавливающего сетевые соединения к внешним адресам с «плохой» репутацией, проводится ряд дополнительных проверок по анализу поведения с целью выявления дополнительной активности, характерной для работы ВПО. По нашей статистике большинство срабатываний являются ложными и сильно зависят от качества TI фидов.

Для повышения наглядности графика, атаки «Заражение ВПО» исключены из статистики.

С увеличением потока входящих событий ожидаемо возросло количество ложноположительных срабатываний. Для повышения эффективности работы аналитиков и снижения числа ложноположительных срабатываний был доработан корреляционный модуль автоматизированного выявления Инцидентов ИБ.

Доработанный модуль позволяет выстраивать цепочки событий, и выявлять подозрения на основе превышения расчетного значения показателя опасности, настраиваемого для каждого правила.

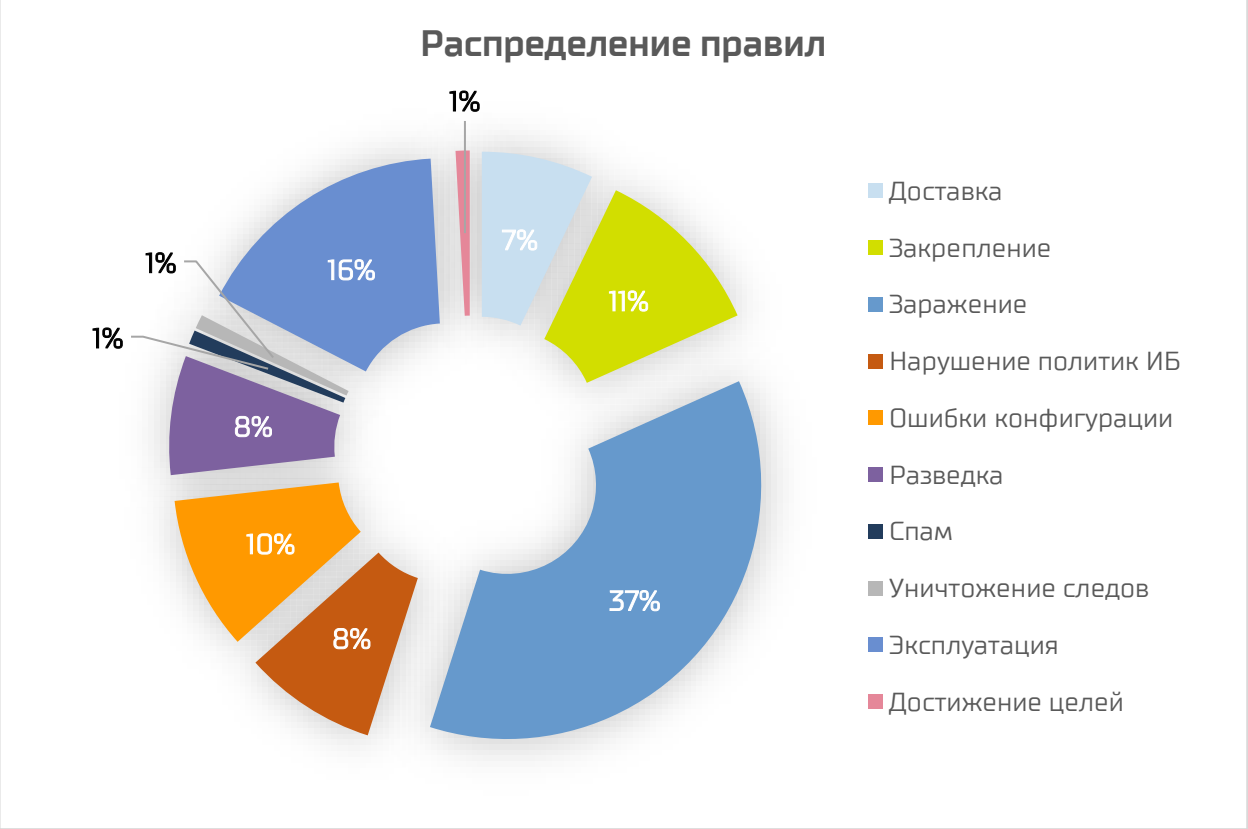
В первом полугодии 2019 года мы фиксировали большое количество срабатываний различных правил стадии «Доставка»: «Доставка ВПО через Email». По каждому срабатыванию правила, аналитики ACRC проводили ряд проверок для подтверждения инцидента ИБ. Новый функционал позволил автоматически сравнивать подозрения на инцидент с реакцией различных СЗИ тем самым снижая количество ложноположительных срабатываний и время реакции на Инцидент ИБ.

Вместе с доработкой модуля корреляции были модернизированы правила выявления инцидентов ИБ. На данный момент в нашей системе более 200 правил, часть из них теперь работают в связке друг с другом: результат срабатывания правила выявления является фактором, повышающим достоверность или необходимым аргументом для работы другого правила. Для наглядности приводится их распределение по стадиям атак. Согласно представленной

диаграмме, порядка 50% правил касается стадий «Заражение» и «Эксплуатация», и это – не случайность. Стадии «Разведка» и «Доставка» традиционно относятся к начальным свидетельствам проникновения злоумышленника в систему, но и процент ложноположительных срабатываний на них выше. Именно поэтому аналитики уделяют особое внимание на срабатывание правил, характерных для стадий «Заражение» и «Эксплуатация», – на этих стадиях достоверность атаки выше, т.к. предполагает успешно пройденную злоумышленником предварительную стадию «разведка», или свидетельствует о допущенных ошибках конфигурации и нарушении политик ИБ. Например, инцидент выявления и последующего блокирования вредоносного ПО антивирусом, свидетельствует о том, что превентивные СЗИ недостаточно качественно настроены, допуская проникновение ВПО в периметр. Также возможно допущены нарушения локальных политик, запрещающих доступ к ресурсам Интернет или использование съемных носителей: Если пользовательский ПК изолирован от Интернет на сетевом уровне, возможно использовался неправомерный доступ в Интернет с использованием USB-модемов или иного хоста в качестве прокси. Таким образом инцидент заражения ВПО, который не повлек ущерба на самом деле может являться последствием иного инцидента, чаще относящегося к несоблюдению принятых у клиентов политик и правил ИБ.

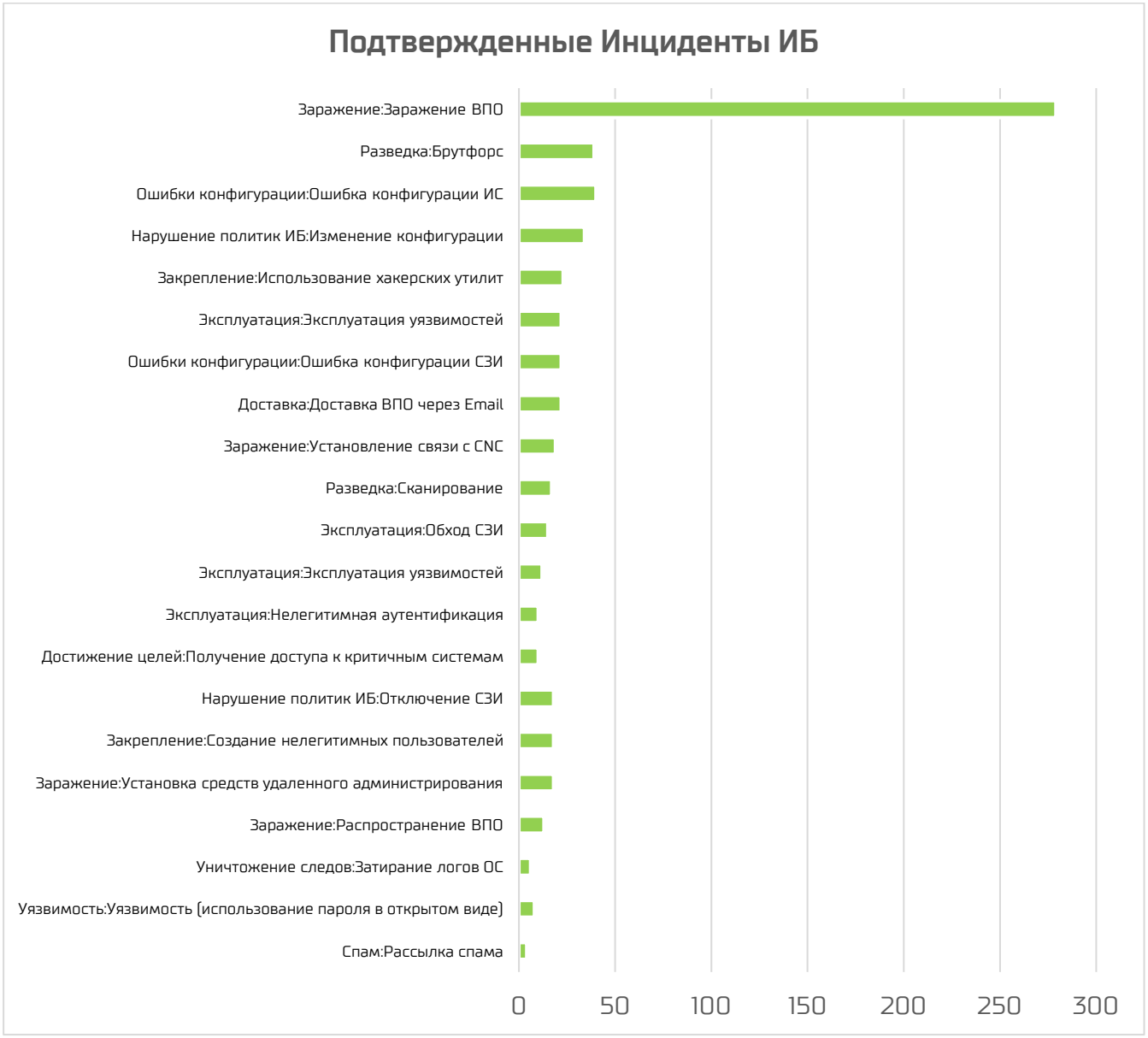
Кроме того, новый корреляционный модуль позволяет вычислять скоринг Инцидента ИБ в зависимости от критичности связанного с ним актива и положения сработавшего правила в цепочке событий. Информация о критичности актива или целой подсети заносится в систему совместно с Заказчиком, что позволяет одному и тому же правилу иметь различный скоринг, если оно сработало, например, на сервере или рабочей станции пользователя. Чем дальше стадия атаки в цепочке, тем выше ее скоринг и, тем меньше соответствующее правило имеет ложноположительных срабатываний (параметры, влияющие на скоринг устанавливаются аналитиками на основе статистики и экспертного опыта). Чем более критичен актив, тем выше будет итоговый скоринг сработавшего правила, а значит выше вероятность Инцидента ИБ. Например, одно и тоже правило будет иметь скоринг выше, если оно сработало на боевом сервере и ниже, если на тестовом.

Применение скоринга позволило снизить процент ложноположительных срабатываний за счет установки границы «белого шума» для правил: значения скоринга, ниже которого подозрение на инцидент не фиксируется в учетной системе. Значение границы «белого шума» различно для каждого клиента, и устанавливается на основе анализа двухнедельной статистики работы правил автоматизированного выявления и рассчитываемых значений скоринга. Кроме того, скоринг помогает аналитикам и команде реагирования прозрачнее оценивать срочность необходимых контрдействий: критичность активов и другие параметры являются отражением реальной ИТ-инфраструктуры клиента, а не универсальной модели «важно-срочно».



5 Статистика подтвержденных Инцидентов ИБ

Среди подтвержденных Инцидентов ИБ на первом месте по-прежнему наблюдаются инциденты стадии «Заражение»: «Заражение ВПО». Это связано с большим количеством поступающих фишинговых писем, активностью пользователей в сети Интернет, использованием некорпоративных внешних носителей информации. Отдельно стоит отметить, что в данную статистику не включаются события успешного удаления вирусов антивирусными средствами. Помимо срабатываний штатных средств антивирусной защиты, аналитики ACRC обогащают различные события по таким параметрам, как IP-адрес ресурса, URL, хэш-сумма файлов и т.д. В ходе обогащения информация проверяется по разным базам индикаторов компрометации, что позволяет выявлять вредоносное программное обеспечение, не детектируемое штатными средствами антивирусной защиты.



6 Статистика по работе аналитиков Центра ACRC

Усовершенствование системы автоматизированного выявления инцидентов ИБ наглядно проявляется в уменьшении количества ложноположительных срабатываний в условиях увеличения обрабатываемых в Центре ACRC событий. Если говорить о подтвержденных Инцидентах ИБ, то их количество возросло в ~4 раза, по сравнению с началом отчётного периода.

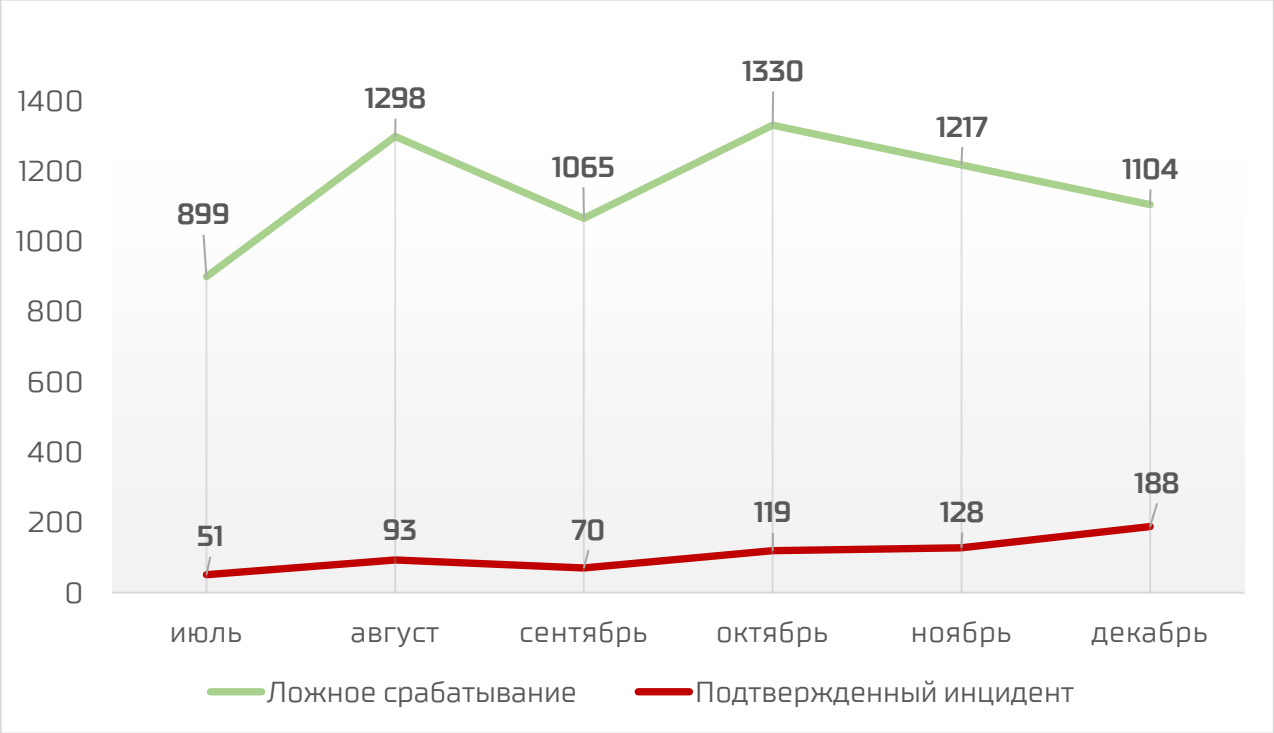


График отражает общее количество обработанных аналитиками ACRC ложноположительных срабатываний по отношению к подтвержденным инцидентам ИБ. Заказчик, в свою очередь, получает уведомление только в том случае, если аналитик считает, что возможен Инцидент ИБ. На графике видно, что % подтвержденных инцидентов значительно вырос при отсутствии роста общего кол-ва ложноположительных срабатываний, что свидетельствует о повышении эффективности выявления: SOC – это прежде всего люди, подверженные серьезной когнитивной нагрузке. Большой % ложноположительных срабатываний «замыливает глаз» и существенно снижает эффективность выявления, руководители SOC просто обязаны снижать долю времени, которая затрачивается на расследование ложноположительных срабатываний, т.к. эффективный SOC – это SOC не допускающий незамеченных инцидентов.

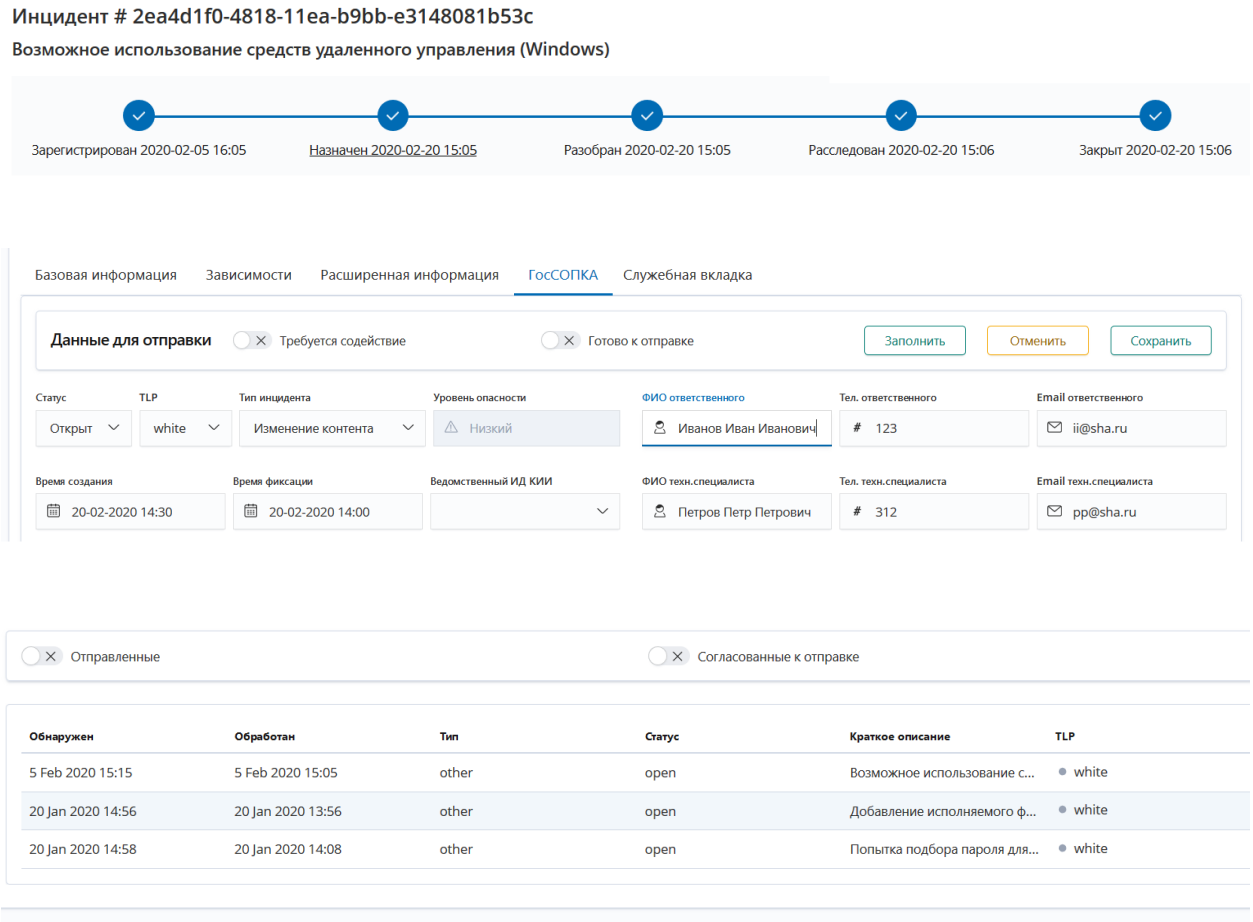
Решение об отнесении к ложноположительному срабатыванию может быть принято автоматически на основе логики фильтрации, согласовываемой с Заказчиком, или на основе экспертного опыта аналитика и обратной связи от Заказчика. Совершенствование работы фильтров производиться непрерывно в постоянном взаимодействии с Заказчиком.

7 Взаимодействие с Национальным координационным центром по компьютерным инцидентам (НКЦКИ)

Во втором полугодии 2019 года «Ангара ассистанс» подписала соглашение о взаимодействии с НКЦКИ. «Ангара ассистанс» является центром ГосСОПКА класса А и может выполнить все задачи, стоящие перед субъектами КИИ по обнаружению, предупреждению и ликвидации последствий атак, а также имеет необходимую техническую инфраструктуру для обмена информацией об Инцидентах ИБ с НКЦКИ.

Для осуществления данного взаимодействия был разработан специальный веб-интерфейс ГосСОПКА, который позволяет отображать информацию об инцидентах КИИ и осуществлять автоматизированную передачу данных об Инциденте ИБ в НКЦКИ с использованием API личного кабинета ГосСОПКА. Заказчики, использующие услугу ГосСОПКА от Центра ACRC, могут в любой момент просмотреть Инциденты ИБ и отправленные в ГосСОПКА уведомления, а также увидеть полный цикл обработки Инцидентов ИБ аналитиками ACRC.

Ниже представлены примеры веб-интерфейса для отправки Инцидентов ИБ в ГосСОПКА.



8 Заключение

Во втором полугодии 2019 года к Центру мониторинга была подключена облачная платформа для управления конечными устройствами. Подключение облачной платформы позволяет обеспечивать прозрачность и контроль за мобильными устройствами, выявлять Инциденты ИБ и отслеживать изменения в критичной для бизнеса экосистеме мобильных устройств – это позволяет аналитикам ACRC расширить границы мониторинга и горизонта событий ИБ клиента, повышая качество услуг.

За II полугодие 2019 года средний поток принимаемых Центром ACRC событий не опускался ниже 15 000 EPS, и достиг своего максимума в октябре – 22 778 событий. При этом согласно нашей статистике, за II полугодие 2019 года было зафиксировано 4042 подозрения на атаку стадии «Заражение»: «Заражение ВПО», что почти в 7 раз превышает следующую по количеству подозрений атаку стадии «Разведка»: «Брутфорс». В отличие от первого полугодия в топ потенциальных инцидентов ИБ поднимается «Установление связи с CNC».

С увеличением потока входящих событий ожидаемо возросло количество ложноположительных срабатываний – "установление связи с CNC", "Доставка ВПО через Email". Для повышения эффективности работы и снижения числа ложноположительных срабатываний аналитиками ACRC был доработан корреляционный модуль автоматизированного выявления Инцидентов ИБ, правила выявления инцидентов ИБ и механизм скорринга.

Среди подтвержденных Инцидентов ИБ на первом месте по-прежнему наблюдаются инциденты стадии «Заражение»: «Заражение ВПО». Это связано с большим количеством поступающих фишинговых писем, активностью пользователей в сети Интернет, использованием некорпоративных внешних носителей информации. Предположительно это тренд сохранится, и поэтому вопросы обучения сотрудников цифровой гигиене и грамотности остается приоритетной задачей для экспертов ИБ компании.

О группе компаний Angara

Группа компаний Angara, представленная головной организацией Angara Technologies Group и сервис-провайдером Angara Professional Assistance, предоставляет 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-10 самых быстрорастущих ИТ-компаний России (7 место, CNews);
- ТОП-20 крупнейших компаний информационной безопасности (13 место, TAdviser);
- ТОП-30 крупнейших поставщиков для банков (26 место, TAdviser);
- ТОП-50 крупнейших поставщиков ИТ-услуг (23 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).

Истории успеха

Компания	Проект
ПАО «Банк «Санкт-Петербург»	Трансформация центра мониторинга ИБ (SOC)
ООО «Инбанк»	Оказание услуг по мониторингу ИБ (SOC)
АО КБ «Юнистрим»	Оказанию услуг по выявлению и реагированию на инциденты ИБ
АО «ЭР-Телеком Холдинг»	Создание системы сбора и визуализации событий ИБ
СПАО «Ингосстрах»	Создание центра мониторинга ИБ (SOC)

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 (CEH, CISA, ITIL Expert).