

СОГЛАШЕНИЕ ОБ УРОВНЕ ПРЕДОСТАВЛЕНИЯ УСЛУГИ «THREAT DETECTION AND RESPONSE» («TDR»)

1. ПРЕДМЕТ СОГЛАШЕНИЯ

- 1.1. Настоящее Соглашение об уровне предоставления услуг (далее – Соглашение) является документом, фиксирующим Доступность Услуги, а также целевые количественные и качественные характеристики предоставления Услуги.
- 1.2. Услуга предоставляется в сотрудничестве с ООО «Безопасная информационная среда» (ООО «БИЗон», далее – «Партнер»).
- 1.3. Взаимодействие центра мониторинга Партнера (BI.ZONE SOC) и Исполнителя включает в себя регистрацию заявок о несоответствии предоставляемых услуг требуемым параметрам качества, организацию процесса восстановления сервиса, взаимное информирование ответственных руководителей компаний о ходе решения вопросов, связанных с восстановлением требуемого качества сервиса.

2. ПРОЦЕДУРА ВЗАИМОДЕЙСТВИЯ СТОРОН ПРИ ВЫЯВЛЕНИИ ИНЦИДЕНТОВ ИБ

- 2.1. Под реагированием на инцидент ИБ подразумевается структурированная совокупность действий Сторон, направленная на установление деталей инцидента, минимизацию ущерба от инцидента и предотвращение повторения подобного инцидента ИБ в будущем.
- 2.2. Действия по выявлению инцидентов ИБ и реагированию на них, а также их очередность представлены в Таблице 1:

Табл.1. Процедура реагирования на Инцидент ИБ

№	Задачи	Ответственный	Время реакции
1	Мониторинг и анализ событий ИБ		
1.1	В рамках мониторинга и анализа событий ИБ производится анализ срабатываний правил автоматического выявления угроз, выделение на базе них потенциальных инцидентов ИБ и их первичная оценка на предмет ложноположительных срабатываний. Инциденты могут быть охарактеризованы как: <ul style="list-style-type: none"> • FP (ложное срабатывание); • TP (подтвержденный инцидент ИБ). В ходе работы характер инцидента может быть изменен как на основании информации от Заказчика, так и на основании экспертного мнения Партнера.	Аналитик линий 1–2 BI.ZONE SOC	Согласно Таблице 3
2	Анализ инцидентов ИБ		
2.1	Анализ потенциальных инцидентов ИБ, оценка их приоритетов и выработка рекомендаций по первичному реагированию	Аналитик линий 1–2 BI.ZONE SOC	Согласно Таблице 3
3	Оповещение Заказчика об инциденте ИБ		
3.1	Фиксация инцидента ИБ в учетной системе Партнера путем заполнения карточки инцидента. Уведомление Заказчика об инциденте может быть осуществлено одним из следующих способом коммуникации: <u>Почтовое уведомление:</u> 1. В теме письма содержатся следующие значения: <ul style="list-style-type: none"> • Идентификатор информационной системы, в отношении которой был зафиксирован инцидент. • Номер инцидента, присвоенный учетной системой исполнителя: • Приоритет. • Название инцидента. 2. В теле письма, в карточке инцидента могут содержаться следующие данные: <u>Общая информация об инциденте ИБ:</u> <ul style="list-style-type: none"> • время регистрации в формате UTC; • приоритет; • текущий статус и комментарий к нему. <u>Сводная информация:</u>	Аналитик линий 1–3 BI.ZONE SOC	Согласно Таблице 3

	<ul style="list-style-type: none"> • список затронутых хостов и активных учетных записей в них на момент инцидента (при условии доступности этой информации); • список обнаруженных индикаторов компрометации (например, хеш-сумма файла, имя файла, адрес С&С-сервера, ассоциированные доменные имена и др.); • релевантные инциденту техники и тактики MITRE ATT&CK; • сработавшие правила автоматического выявления угроз, на базе которых обнаружен инцидент; • ссылки на дополнительные файлы, прикладываемые к инциденту. <p><u>Подробная информация:</u></p> <ul style="list-style-type: none"> • описание инцидента; • timeline инцидента; • обзор текущего и потенциального влияния инцидента на инфраструктуру Заказчика; • прочая информация. <p><u>Рекомендации:</u></p> <p>Первоочередные действия, которые подразумевают подтверждение легитимности/нелегитимности инцидентов ИБ. Также рекомендации, которые необходимо предпринять для предотвращения инцидента ИБ или минимизации его последствий, и которые не могут быть выполнены Исполнителем самостоятельно в рамках активного реагирования. Запрос дополнительной информации, которая требуется от Заказчика для проведения Исполнителем дальнейшего анализа инцидента ИБ, и которая не может быть получена Исполнителем самостоятельно в рамках активного реагирования.</p> <p>Карточка инцидента на BI.ZONE SOC Portal</p> <p>Карточка инцидента доступна в личном кабинете Заказчика.</p>		
4	Предоставление Заказчиком обратной связи по инциденту ИБ		
4.1	<p>После получения письма сотрудник Заказчика берет данный инцидент в работу и, по итогам работы с инцидентом, предоставляет обратную связь, а именно – подтверждает легитимность/нелегитимность данного инцидента, а также выполняет согласование сформированного Исполнителем плана активного реагирования (если это согласование необходимо). В случае нелегитимности описывает результаты выполнения рекомендаций и своё решение в отношении предлагаемого плана активного реагирования Партнера в ответном письме или комментарием в SOC Portal.</p>	Исполнитель	Согласно Таблице 3

2.3. Для каждого Инцидента ИБ назначается приоритет согласно Таблице 2 и категория согласно Таблице 4. Реагирование на Инциденты ИБ осуществляется в соответствии с временными характеристиками, определёнными в Таблице 1.

Табл.2. Приоритеты инцидента ИБ

Приоритет	Описание приоритета инцидента ИБ	Пример
Критический	инцидент, приводящий к компрометации большого количества защищаемых ресурсов в результате чего Заказчику может быть нанесен существенный ущерб, или же инцидент носит таргетированный характер	Таргетированная атака, в рамках которой была скомпрометирована учетная запись администратора домена
Высокий	инцидент, приводящий к возможности или созданию условий для компрометации защищаемых ресурсов Заказчика. Злонамеренная активность не была заблокирована превентивными СЗИ.	Активность вредоносного программного обеспечения, не детектируемого используемыми средствами антивирусной защиты
Средний	инцидент, который в данный момент не приводит к недоступности защищаемых ресурсов Заказчика, но в будущем с высокой степенью вероятности может вызвать инцидент с более высоким приоритетом. Злонамеренная активность была локализована и заблокирована превентивными СЗИ	Успешная эксплуатация уязвимости браузера с последующей попыткой заражения хоста вредоносным программным обеспечением, заблокированная средствами антивирусной защиты
Низкий	инцидент, в рамках которого Заказчику не было нанесено какого-либо ущерба. Осуществлялся сбор информации о системе в рамках имеющихся прав доступа	Идентифицированные потенциальные нежелательные программы – Adware, Riskware, not-a-virus и т. д

Табл. 3. Целевые показатели уровня предоставления услуги «Мониторинг инцидентов ИБ»

№	Показатель	Приоритет	Время выполнения показателя*	Табель	Время реакции Заказчика на запросы Партнера
1.	Обнаружение инцидента ИБ, регистрация инцидента ИБ	1 – Критический	До 15 минут	24×7	Не применимо
		2 – Высокий	До 15 минут	24×7	Не применимо
		3 – Средний	До 15 минут	24×7	Не применимо
		4 – Низкий	До 60 минут	24×7	Не применимо
2.	После регистрации инцидента ИБ Партнер проводит проверку ложного срабатывания и категорирование инцидента, уведомляет Заказчика об инциденте ИБ	1 – Критический	До 60 минут	24×7	Не применимо
		2 – Высокий	До 60 минут	24×7	Не применимо
		3 – Средний	До 180 минут	24×7	Не применимо
		4 – Низкий	До 280 минут	24×7	Не применимо
3.	Предоставление первичных рекомендаций по инциденту ИБ Заказчику	1 – Критический	3 часа с момента регистрации	24×7	До 60 минут
		2 – Высокий	8 часов с момента регистрации	24×7	Не применимо
		3 – Средний	16 часов с момента регистрации	24×7	Не применимо
		4 – Низкий	30 часа с момента регистрации	24×7	Не применимо
4.	Время на расследование инцидента ИБ и анализа журналов событий, предоставленных Заказчиком Партнеру	1 – Критический	Не применимо	24×7	Не применимо
		2 – Высокий	Не применимо	24×7	Не применимо
		3 – Средний	Не применимо	8×5	Не применимо
		4 – Низкий	Не применимо	8×5	Не применимо
5.	Инциденты отсутствия событий**	3 – Средний	Не применимо	8×5	8×5
6.	SLA на исполнение показателей (пп. 1-5)***	99%			

* Срок фактического восстановления и решения Инцидента ИБ отсчитывается с момента получения запроса Заказчиком увеличивается, в случаях, когда для восстановления и/или устранения Инцидента ИБ требуется формирование запроса в техническую поддержку производителя программного обеспечения, если при оказании Услуги используется программное обеспечение третьих лиц, (третья линия технической поддержки) и/или требуется дополнительная информация от Заказчика. В данном случае Инцидент ИБ переводится в статус «Ожидание» до момента решения запроса третьей линией технической поддержки и/или Исполнителем.

** Реакция предполагается для источников событий, согласованных по почте с уполномоченным представителем Заказчика.

*** 99% заявок будет выполнено в соответствии с временными показателями, 1% может быть решен с увеличенным временем реакции Партнера.

Табл.4. Категория инцидента ИБ

Unauthorized Access/Compromised
Инциденты, связанные с неавторизованным получением физического/логического доступ к защищаемой сети/системе/приложению/данным).
Scans/Probes/Attempted Access

Инциденты, связанные с активностью, направленной на получение сведений о доступных хостах, открытых портах, уязвимостях, установленном ПО или иных сведений о целевом объекте, которые могут быть использованы нарушителем для дальнейшего планирования и развития атаки.
Brute Force
Инциденты, связанные с успешными и неуспешными попытками подбора паролей в защищаемые системы.
Vulnerability
Инциденты, связанные с успешной эксплуатацией уязвимостей, а также выявлением (с использованием сканеров, анализ кода, Bug Bounty и т.п.) критичных уязвимостей (уязвимостей реализации), эксплуатация которых может привести к реализации угроз информационной безопасности (несанкционированный доступ, утечка конфиденциальной информации, несанкционированные денежные переводы и т.д.).
Defacement/Data Manipulation
Инциденты, связанные с нелегитимным изменением содержимого защищаемого ресурса (WEB-сайт, файлы, базы данных).
Data Leak
Инциденты, связанные с потенциальными утечками защищаемой информации (копирование файлов на подключаемые носители, выгрузка внутренних баз данных или баз знаний, отправка конфиденциальной информации по электронной почте и т. п.).
Malware
Инциденты, связанные с активностью вредоносного программного обеспечения (например, запуск шифровальщика, прописывание в автозагрузку трояна и т. п.).
Malware C&C Communication
Инциденты, связанные с выявлением взаимодействия хостов защищаемой инфраструктуры с известными командными центрами ботнет сетей.
Malicious Host
Инциденты, связанные с доступом к ресурсам, выполняющим распространение вредоносного ПО (исключая известные командные центры ботнет сетей), либо связанные непосредственно с размещением в сети Интернет таковых ресурсов.
Phishing
Инциденты, связанные с информацией, вводящей пользователей защищаемых информационных систем в заблуждение относительно принадлежности информации, распространяемой посредством сети Интернет/электронной почты, вследствие сходства доменных имен, оформления или содержания.
Spam
Инциденты, связанные с распространением незапрашиваемой электронной почты, носящей информативный/рекламный характер.
Prohibited Content
Инциденты, связанные с размещением в сети Интернет запрещенного контента; использованием нелегитимного ПО, применением средств обхода лицензионных ограничений.
Social Engineering
Инциденты, связанные с побуждением пользователей защищаемой информационной системы к совершению действий (путём обмана или злоупотребления доверием), направленных на достижение целей нарушителя (осуществление операций по переводу денежных средств, переход по вредоносной ссылке, разглашение парольной информации и т. п.).
Improper Usage
Инциденты, связанные с нарушениями требований политик/регламентов/инструкций ИБ (например, доступ в Интернет в обход прокси, использование TOR, подключение к публичным Wi-Fi сетям, использование УЗ доменного администратора на запрещённом хосте и т. п.).
Traffic Hijacking
Инциденты, связанные с атаками, направленными на изменение маршрутно-адресной информации (BGP Hijacking, Route Injection и т. п.).
Misconfiguration
Инциденты, связанные с ошибками в работе и настройке средств защиты информации, компонентов инфраструктуры.
Suspicious Process Activity
Инциденты, связанные с подозрительной активностью легитимных процессов операционной системы.

2.4. Заказчику предоставляется возможность отправлять запросы согласно показателям, указанным в Таблице 5. Для этого Исполнитель должен отправить запрос на электронный адрес soc@bi.zone с указанием идентификатора в теме письма в формате или завести заявку в BI.ZONE SOC Portal:

- тема письма: Идентификатор (предоставит сервис-менеджер Партнера), краткая суть запроса;
- тело письма: Подробное описание запроса, приоритет запроса.

Табл. 5. Целевые показатели проведения изменений в месяц

№	Показатель		Кол-во обращений
1.	Запрос на изменение	Заявки, связанные с изменением конфигурации Услуги (добавление/удаление источника событий ИБ, адаптация сценария, выдача УЗ в SOC Portal)	не более 8
2.	Информационный запрос	Заявки, связанные с консультационными вопросами, по Услуги (вопросы по работе с SOC Portal, вопросы по договору и т. п.)	не более 4

№	Показатель		Кол-во обращений
3.	Подозрение на Инцидент ИБ	Заявка, связанная с подозрением Заказчика на Инцидент ИБ. Изначально данному обращению присваивается «низкий» приоритет. При необходимости Заказчик может повысить приоритет. Работа по данному типу запроса ведется в соответствии с Таблицей 1.	Не ограничено

Табл.6. Целевые показатели уровня предоставления Услуг

№ п/п	Показатель	Время реакции Партнера*	Время реакции Исполнителя на запросы Партнера
1.	Реагирование на запрос на изменение	Не более 10 рабочих часов	не применимо
2.	Выполнение запросов на изменение	Не более 90 рабочих часов	не применимо
3.	Реагирование на информационный запрос	Не более 10 рабочих часов	не применимо
4.	Выполнение информационных запросов	Не более 90 рабочих часов	не применимо

* Учет времени выполнения запроса приостанавливается, если обстоятельства, влияющие на это время, находятся вне зоны ответственности Партнера.

2.5. После получения ответа на обращение Заказчик проверяет качество исполнения и подтверждает решение. В случае, если Заказчик не подтвердил решение в течение 21 (Двадцати одного) рабочего дня, обращение считается выполненным и автоматически закрывается.

2.6. Жизненный цикл инцидентов и обращений.
В процессе своего жизненного цикла инцидент и обращение они могут находиться в следующих, статусах, актуальность которых можно отследить в ЛК SOC Portal и/или уточнить аналитиков 1-й линии.

Табл.7. Статус инцидентов и обращений

Статус	Описание статуса
Waiting for support (Назначен)	– инцидент находится в работе у Партнера.
Waiting customer/Pending (В ожидании)	– решение Инцидента приостановлено по одной из следующих причин: <ul style="list-style-type: none"> • для решения требуется дополнительная информация от Заказчика; • зарегистрирован запрос в службу технической поддержки производителя оборудования, участвующего в оказании Услуги; • возникли другие обстоятельства, которые находятся вне зоны ответственности Партнера. Учет времени решения Инцидента на данном этапе приостанавливается.
Completed (Решен)	– по зарегистрированному инциденту или обращению: <ul style="list-style-type: none"> • выработаны необходимые меры по решению; • предоставлены рекомендации по нейтрализации угрозы ИБ, послужившей причиной инцидента; • установлено, что эксплуатационные характеристики Услуги соответствуют гарантированным параметрам. Если Заказчик отказывается подтвердить решение, инцидент может быть открыт заново путем отправки соответствующего уведомления Партнеру. При отсутствии уведомления от Заказчика в течение 3 (трех) рабочих дней решение считается подтвержденным, инцидент подлежит закрытию.
Customer completed	– инцидент переведен в статус «решен Заказчиком», проводится проверка Партнером.
DFIRMA (На расследовании)	– статус инцидентов ИБ, которые требуют проведения подробного расследования, с использованием методов компьютерной криминалистики и анализа вредоносного ПО, при этом требуемые в рамках расследования действия не ограничиваются предоставляемыми возможностями агента BI.ZONE Sensors по активному реагированию. На данном статусе учет времени устранения инцидента не учитывается.
Closed (Закрыт)	– решение инцидента подтверждено Заказчиком в установленный срок, либо инцидент автоматически закрыт ввиду отсутствия обратной связи от

	Заказчика в течение 21 (двадцати одного) рабочего дня. В данном статусе Инцидент не подлежит переоткрытию.
--	--

3. ПРОВЕДЕНИЕ РЕГЛАМЕНТНЫХ И/ИЛИ СРОЧНЫХ РАБОТ TDR

3.1. Условия проведения Регламентных работ и/или Срочных работ TDR, приведены в Таблице 8:

Табл.8. Условия проведения Регламентных и/или Срочных работ

Наименование работ	Продолжительность и интервалы между перерывами	Уведомление Заказчика	Дополнительные условия
Регламентные работы TDR (плановое техническое обслуживание, модернизация или усовершенствование подсистем, на базе которых оказывается Услуга). Проводятся Партнером	проводятся в интервале времени от 21.00 до 06.00 (Московское время) или по согласованному с Заказчиком периоду времени прерывания предоставления Услуги.	Партнер должен уведомить Заказчика о проведении работ минимум за 2 (два) дня до начала работ.	Исключением являются случаи, когда работы выполняются по запросу Заказчика, а также в случаях, когда Партнер не может соблюсти указанный срок в связи с тем, что плановые ремонтные работы на сети Партнера проводятся по требованию Российских государственных органов или компетентных органов отрасли телекоммуникаций России.
Срочные работы TDR (аварийные ремонтные работы подсистем, на базе которых оказывается Услуга; проводятся, когда отмечаются периодически возникающие прерывания в оказании Услуги или существенные ухудшения параметров качества, которые могут в дальнейшем привести к состоянию аварии). Проводятся Партнером	Время перерыва указывается в уведомлении о проведении работ	Партнер должен уведомить Заказчика о проведении работ не менее чем за 4 (четыре) часа до начала работ.	-

3.2. Заказчик при необходимости направляет предложения по корректировке сроков проведения работ, которые учитываются по технической возможности Партнером. В уведомлении, направленном Партнером, указываются:

- время проведения плановых ремонтных работ;
- дата проведения плановых ремонтных работ;
- продолжительность проведения плановых ремонтных работ;
- контактные данные лица, ответственного за предоставление информации о проводимых работах;
- информация о необходимости участия сотрудников Заказчика в плановых ремонтных работах, например, для проведения проверок работоспособности информационной системы Заказчика.

3.3. Заказчик должен выделить ответственных сотрудников для участия в работах. В случае невозможности привлечения сотрудника к работам на указанную дату, Заказчик направляет предложения по корректировке сроков проведения работ.

3.4. Заказчик должен уведомить Исполнителя о проведении любых плановых работ на своем оборудовании, которые могут привести к временной недоступности защищаемых ресурсов Заказчика и, как следствие, к перерыву в оказании Услуги, минимум за 2 (двое) суток до начала работ. В уведомлении должно быть указано: время, дата, продолжительность проведения плановых работ, контактные данные лица, ответственного за предоставление информации о проводимых работах. При изменении сроков проведения плановых работ Заказчик оповещает Исполнителя в кратчайшие сроки после принятия решения, но не менее, чем за 1 (одни сутки) до начала проведения работ. При отмене плановых работ Заказчик оповещает Исполнителя в кратчайшие сроки после принятия решения.

3.5. Заказчика должен уведомить Партнера о проведении любых аварийных ремонтных работ на своем оборудовании, которые могут привести к временной недоступности защищаемых ресурсов Заказчика и, как следствие, к перерыву в оказании Услуги, минимум за 2 (два) часа до начала работ. Уведомление должно быть направлено на электронный адрес уполномоченного представителя Исполнителя.

В уведомлении должны быть указаны:

- время, дата и продолжительность аварийных ремонтных работ;
- контактные данные лица ответственного за предоставление информации о проводимых работах;
- информация о необходимости участия сотрудников Заказчика в аварийных ремонтных работах (только при проведении работ Партнером).

3.6. Все уведомления Партнера, Заказчика и Исполнителя должны направляться на электронный адрес уполномоченных представителей Сторон.

4. ЗОНЫ ОТВЕТСТВЕННОСТИ НА ПЕРИОД ОКАЗАНИЯ УСЛУГИ

4.1. В рамках оказания Услуги зоны ответственности распределяются в соответствии с Таблицей 9. Партнер не несет ответственность за Компоненты Услуги, размещенные в ИТ-инфраструктуре Заказчика, в соответствии с Таблицей 9:

Табл.9. Зоны ответственности

Параметр		BI.ZONE SOC Portal	Компоненты Услуги, размещенных в ИТ-Инфраструктуре Заказчика
Уровень приложения	Мониторинг инцидентов ИБ	Партнер	Партнер
	Обеспечение работоспособности	Партнер	Партнер
	Восстановление работоспособности	Партнер	Партнер
Уровень ОС	Мониторинг	Партнер	Партнер
	Обеспечение работоспособности	Партнер	Партнер
	Восстановление работоспособности	Партнер	Партнер
Уровень виртуальной среды	Мониторинг	Партнер	Заказчик
	Обеспечение работоспособности	Партнер	Заказчик
	Восстановление работоспособности	Партнер	Заказчик
Уровень оборудования	Мониторинг	Партнер	Заказчик
	Обеспечение работоспособности	Партнер	Заказчик
	Восстановление работоспособности	Партнер	Заказчик