

## ОПИСАНИЕ И УСЛОВИЯ ПРЕДОСТАВЛЕНИЯ УСЛУГИ «THREAT DETECTION AND RESPONSE» («TDR»)

### 1. ОБЩАЯ ИНФОРМАЦИЯ И ОПИСАНИЕ УСЛУГИ

- 1.1. Услуга TDR обеспечивает круглосуточный мониторинг информационной безопасности (ИБ) облачной инфраструктуры, оперативную реакцию на инциденты ИБ, проведение расследований при обнаружении продвинутых атак и консультирование по повышению защищенности инфраструктуры.
- 1.2. Оказание Услуги направлено на достижение следующих конечных целей:
- повышение уровня защищенности ИТ-инфраструктуры Заказчика от современных киберугроз и создание условий для предотвращения ущерба от инцидентов ИБ;
  - организация и осуществление мониторинга событий и обработки инцидентов ИБ (далее – «Организация мониторинга инцидентов ИБ»).
- 1.3. В рамках оказания Услуги могут быть решены следующие задачи:
- круглосуточный мониторинг информационной безопасности (ИБ) облачной инфраструктуры;
  - оперативная реакция на инциденты ИБ;
  - предоставление отчетов по текущему состоянию информационной безопасности (ИБ) инфраструктуры Заказчика;
  - проведение расследования по обнаруженным инцидентам;
  - подготовку рекомендаций по реагированию и предотвращению подобных инцидентов в будущем.
- 1.4. Услуга предоставляется Исполнителем в сотрудничестве с ООО «Безопасная информационная среда» (ООО «БИЗон», далее – Партнер) в варианте Horizon. Заказчик является конечным пользователем оказываемой Услуги. Описание варианта Horizon доступно на сайте Партнера по ссылке: <https://bi.zone/ru/catalog/services/threat-detection-and-response/>.

### 2. СОСТАВ, УСЛОВИЯ И ПОРЯДОК ОКАЗАНИЯ УСЛУГИ

- 2.1. На основании опросного листа, предоставленного Партнером и заполненного со стороны Заказчика, Исполнитель без выезда на площадку проводит анализ (обследование) ИТ-инфраструктуры Заказчика и определяет необходимый уровень Услуги. В зависимости от уровня состав Услуги может отличаться. В Таблице 1 приведена информация по их составу:

Табл.1. Состав Услуги TDR Horizon

TDR Horizon	
Состав услуг Партнера на I этапе	
1.	выдача рекомендаций по составу и приоритизации подключаемых на мониторинг источников событий ИБ. Типизация источников на типовые и нетиповые
2.	выработка организационно-технических решений по: - целевой архитектуре предоставления услуги; - техническим характеристикам и требованиям к вычислительным ресурсам; - порядку и организации межсетевому взаимодействию компонентов Услуги и BI.ZONE SOC (Центр мониторинга и реагирования на киберугрозы Партнера).
3.	определение потребностей Заказчика в части подключения существующих и разработки новых сценариев выявления атак, путем направления Исполнителю аналитического опросного листа для дальнейшего заполнения Заказчиком.
4.	предоставление доступа в BI.ZONE SOC Portal.
5.	в случае необходимости - предоставление Заказчику требования к вычислительным ресурсам, подсистеме (-ам) хранения и рекомендации по конфигурированию для установки дополнительных компонентов Услуги.
6.	выполняется конфигурирование и профилирование SIEM-системы под ИТ-инфраструктуру Заказчика, на основании предоставленного Исполнителем аналитического опросного листа (данные работы гарантируют работоспособность use-cases).
7.	направить инструкции по подключению источников к Услуге.
8.	разработка индивидуальных адаптеров для нетиповых источников.
9.	разработка новых сценариев выявления атак, а именно расширение категорий инцидентов и правил корреляции на основании специфичных запросов Заказчика.
Состав работ Заказчика на I этапе	
10.	настроить источники событий, согласно предоставленным инструкциям.

11.	ознакомиться с базой use-cases Исполнителя в BI.ZONE SOC Portal, согласовать режим активации правила: - режим активации автоматический – режим по умолчанию для большинства разрабатываемых правил, означает что правило доступно автоматически при наличии требуемых источников событий; - режим активации ручной – правило по умолчанию отключено, для его включения необходима заявка Исполнителю от Заказчика.
12.	предоставить Партнеру список сотрудников, которым необходимо направлять информацию по инцидентам ИБ.
<b>Состав услуг Партнера на II этапе</b>	
13.	анализ срабатываний правил автоматического выявления угроз в режиме 24x7 силами аналитиков 1-й линии Партнера. Аналитики 1-й линии должны обеспечивать обработку срабатываний правил автоматического выявления угроз, проверку ложных срабатываний, проведение первичной аналитики и выделение инцидентов ИБ на основе категорий инцидентов и правил, регистрацию и последующее сопровождение инцидента ИБ в соответствии со стандартами ITIL (категорирование, приоритизация, SLA и т.д.).
14.	обработка инцидентов ИБ силами аналитиков 2-й линии Партнера в режиме 8x5, проведение углубленной аналитики при решении инцидентов ИБ с использованием различных специализированных инструментов; адаптацию правил корреляции в соответствии с изменениями в ИТ-инфраструктуре Заказчика; добавление исключений в правила корреляции по требованию Заказчика.
15.	проведение углубленной аналитики, ретроспективного анализа событий, которые привели к инциденту ИБ, силами 3-й экспертной линии Партнера. Проведение первичного расследования без выезда на площадку Заказчика.
16.	отправка обнаруженных инцидентов ИБ в систему управления инцидентами Заказчика посредством направления карточки инцидента по электронной почте или за счет интеграции с API BI.ZONE SOC Portal (интеграция не подразумевает доработок Партнера и осуществляется Заказчиком самостоятельно на основании предоставленной документации на API).

- 2.2. После заполнения опросного листа и определения уровня состава Услуги Исполнитель и Заказчик согласуют Спецификацию по форме, указанной в Приложении № 1.CRS.2.2.A. к Договору, посредством электронной почты по адресам уполномоченных представителей Сторон. Границы оказания Услуги определяются индивидуально для каждого Заказчика и указываются Сторонами в соответствующей Спецификации.
- 2.3. Стоимость Услуги указывается в бланке Заказа. В стоимость Услуг включена стоимость лицензионных прав на программное обеспечение BI.ZONE SOC Portal (простая неисключительная лицензия).
- 2.4. По запросу Заказчика Партнер разрабатывает новые сценарии реагирования, количество новых сценариев не превышает значения, указанного в Спецификации. Для разработки сценария Исполнитель обеспечивает предоставление Партнеру Заказчиком следующей информации:
- заполненный опросный лист. Столбец «Значение» согласно примеру, указанному в Таблице 2; для заполнения данной таблицы могут быть привлечены сотрудники Партнера:

Табл.2. Опросный лист для разработки сценария

Название параметра	Значение
Предлагаемое название сценария	Multiple Failed Logon Attempts
Описание сценария, какую активность данный сценарий должен выявлять (чем подробнее описание, тем лучше)	Выявление множественных неуспешных попыток входа одного и того же пользователя (более 20 неуспешных входов за 1 минуту)
Риски, которые закрывает (выявляет) сценарий	Перебор паролей для учетных записей пользователей
Для каких источников событий данный сценарий (какие логи нужны)	Oracle DB, Apache (access logs)
Дополнительные требования к сценарию (конкретные устройства, учетные записи, группы учетных записей и т. д.)	Только для учетных записей группы CRM_Admin в AD и только для серверов prod_crm_1, prod_crm_2, prod_crm_db.
Исключения для сценария	исключить учетные записи вида tech_***, и входы по ссылке <a href="http://example.com/test_ent***">http://example.com/test_ent***</a>
Есть ли возможность сгенерировать подобную активность (Да/Нет)	Да

Название параметра	Значение
Ответственный со стороны Заказчика (к кому обращаться для уточнения деталей, генерации активности)	Иванов И. И. (i.i.ivanov@example.com; +7 (123) 456 -78-90)
Критичность сценария (для приоритизации инцидента)	High
Дополнительная полезная информация (комментарии, уточнения, пример событий)	-

После того, как Партнер получил заполненную таблицу, Партнер сообщает срок выполнения данной задачи. Источники событий, для которых разрабатываются сценарии, должны быть подключены к Услуге с должным уровнем логирования, то есть присутствует вся необходимая информация для обеспечения работоспособности сценария.

- 2.5. Архитектура Услуги состоит из следующих функциональных компонентов (Компоненты Услуги):
- **IBM QRadar SIEM Event Collector** – компонент сбора событий. Используется при подключении источников, для которых не требуется специальная обработка событий.
  - **Log Broker** – используется как брокер событий от источников требующих предварительной обработки событий. В первую очередь используется для агрегирования событий от источников типа – сетевое оборудование, обогащения событий и форматирования.
- 2.6. Партнером должно быть осуществлено размещение компонентов Услуги в виртуальной среде, построенной на базе гипервизора в ИТ-инфраструктуре Заказчика. Исполнитель должен обеспечить выделение Заказчиком следующих ресурсов:

Наименование компонента Услуги	Конфигурационные требования (на каждый сервер)	Кол-во
IBM QRadar Event Collector	в соответствии со Спецификацией	в соответствии со Спецификацией
Log Broker	в соответствии со Спецификацией	в соответствии со Спецификацией

- 2.7. Для централизованного сбора событий от источников Windows Исполнитель обеспечивает, что Заказчик должен использовать Windows Event Collector. По запросу Партнера Заказчик устанавливает на Windows Event Collector дополнительного агента для сбора событий.
- 2.8. После формирования требований по Услуге TDR Заказчик в срок не более, чем за 14 (четырнадцать) рабочих дней должен:
- предоставить Ресурсы, запрашиваемые в Таблице 2 настоящего Приложения.
  - организовал сетевую связность между компонентами, необходимыми для оказания Услуги.

### 3. ТАРИФИКАЦИЯ УСЛУГИ

- 3.1. Стоимость оказываемых Услуг согласовывается индивидуально Сторонами в Заказах Услуг. Стоимость Услуги указывается за Отчётный период. Величина ежемесячного платежа за пользование Услугой определяется в соответствии с составом запрошенной Услуги.

### 4. ОБЯЗАТЕЛЬСТВА СТОРОН

- 4.1. Заказчик обязуется:
- 4.1.1. Проводить взаимодействие по вопросам в рамках Услуги по электронным адресам, приведенным в Приложении № 4. к Договору.
- 4.2. Исполнитель обязуется:
- 4.2.1. Оказать Услуги с надлежащим качеством, в объеме и в сроки, согласованные Сторонами.
- 4.3. Исполнитель вправе:
- 4.3.1. Требовать от Заказчика предоставления ему информации и документов, необходимых для своевременного оказания Услуги;
- 4.3.2. Использовать полученную в ходе оказания Услуги по настоящему Договору статистическую информацию, формирующую правила о способах, методах, средствах реализации Услуги Исполнителем, для формирования собственной базы данных, в том числе составляющую элементы объектов интеллектуальной собственности Исполнителя.
- 4.4. У Заказчика имеется понимание, что Исполнитель оказывает Услуги в соответствии с действующим на момент оказания Услуг законодательством Российской Федерации, поэтому Заказчик не будет

требовать оказания Услуги в нарушение законодательства Российской Федерации или вне пределов действительных возможностей Исполнителя.

- 4.5. Исполнитель не несет ответственности перед Заказчиком за все последствия, вызванные непредставлением/несвоевременным предоставлением Заказчиком надлежащих доступов, информации, сведений (документов), предоставлением некомплектной документации или если эти последствия вызваны виновным действием (бездействием) самого Заказчика, либо третьих лиц со стороны Заказчика.
- 4.6. Исполнитель не несет ответственности за инциденты и другие обстоятельства, повлекшие за собой перерывы в предоставлении Услуги, вызванные любой из перечисленных ниже причин:
- проведение Партнером плановых и аварийных ремонтных работ на оборудовании, участвующем в оказании Услуги, с уведомлением Заказчика и Исполнителя;
  - проведение работ на оборудовании, участвующем в оказании Услуг, проводимые или Заказчиком или Партнером по запросу Заказчика;
  - тестовое предоставление Услуги по запросу Заказчика в случае, когда не было выявлено никаких инцидентов;
  - отказ или неспособность Заказчика обеспечить содействие Партнеру в установлении и устранении инцидентов в срок, определенный соглашением об уровне предоставления Услуги;
  - отказ или неспособность Заказчика предоставить необходимые данные для настройки программного обеспечения или оборудования в рамках предоставления Услуги в срок до 5 (пять) рабочих дней;
  - проведение работ Заказчиком по внесению изменений в состав и конфигурацию защищаемых ресурсов без уведомления Исполнителя и Партнера, которые могут привести к их временной недоступности и, как следствие, к перерыву в оказании Услуги;
  - неработоспособность или несовместимость программного и/или программно-аппаратного обеспечения Заказчика с Услугой;
  - в случае обстоятельств непреодолимой силы.

## **5. ОТЧЕТНОСТЬ**

- 5.1. Заказчик имеет возможность получать отчетность по каждому выявленному инциденту ИБ через личный кабинет SOC Portal, доступный по адресу: <https://soc.bi.zone/>, который позволяет:
- непрерывно отслеживать работу команды Партнера по выявлению и реагированию на инциденты ИБ;
  - просматривать статистику о произошедших инцидентах ИБ;
  - получать доступные отчеты и уведомления от Партнера;
  - регистрировать обращения и следить за их статусом в режиме реального времени;
  - получать визуально представленную информацию о параметрах оказания Услуги;
  - предоставление карточки инцидента по каждому выявленному инциденту ИБ по одному из каналов связи: электронная почта и SOC Portal.

## **6. ИНЫЕ УСЛОВИЯ, ПРИМЕНИМЫЕ К УСЛУГЕ**

- 6.1. Возможные виды подключения / изменения / отключения Услуг:
- 6.1.1. Посредством подписания бланка Заказа.
- 6.2. Возможный порядок расчетов по Услугам:
- 6.2.1. Постоплата.
- 6.3. Возможные способы оплаты / порядок пополнения Баланса:
- 6.3.1. Оплата в безналичном порядке на основании выставленного Исполнителем счёта.