СУБЛИЦЕНЗИОННЫЙ ДОГОВОР №

г. Минск ___.____ 2023

_____, именуемое в дальнейшем «Сублицензиат», в лице _____, действующего на основании _____, с одной стороны, и открытое акционерное общество «Белорусский межбанковский расчетный центр», именуемое в дальнейшем «Сублицензиар», в лице _____, действующего на основании _____, с другой стороны, вместе именуемые Стороны, заключили настоящий Сублицензионный Договор о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1 В соответствии с условиями настоящего Сублицензионного Договора (далее – Договор) Сублицензиат передает Сублицензиару неисключительные имущественные права на систему мониторинга состояния кибербезопасности, которая указана в Спецификации (Приложение № 1 к Настоящему Договору), ограниченное правом инсталляции, копирования и запуска компьютерных программ (далее – права на компьютерные программы), сроком пользования в течении 24 месяцев с даты их передачи Сублицензиару. В течение указанного периода Сублицензиат предоставляет Сублицензиару техническую поддержку.

Требования, предъявляемые к компьютерным программам, указаны в Приложении № 2 к настоящему Договору.

Условия использования прав на компьютерные программы определяются составленными обладателями исключительных прав лицензионными соглашениями (далее по тексту – «Лицензионное соглашение»). Территория действия прав на компьютерные программы – Республика Беларусь.

1.2 Сублицензиат гарантирует, что он действует в пределах прав и полномочий, предоставленных ему правообладателем компьютерных программ, и на момент предоставления (передачи) Сублицензиару права на использование компьютерных программ не заложены, не арестованы, не являются предметом исков третьих лиц и являются лицензионным продуктом.

1.3 За предоставленные Сублицензиару права на компьютерные программы Сублицензиар обязан произвести оплату в соответствии с условиями настоящего Договора. Сублицензиар не вправе отказаться полностью или в части от заказанных прав на компьютерные программы (Приложение №1 к Сублицензионному Договору), в том числе отказаться от их получения.

2. СТОИМОСТЬ ПРАВ НА КОМПЬЮТЕРНЫЕ ПРОГРАММЫ И ПОРЯДОК ОПЛАТЫ

2.1 Общая стоимость прав на компьютерные программы включает в себя техническую поддержку, указана в Спецификации (Приложение № 1 к настоящему Договору) и составляет _____ (_____) белорусский рубль ___ копеек, в том числе НДС _____ (_____) белорусских рублей ___ копеек. Общая стоимость прав включает в себя техническую поддержку на 24 месяца, а также стоимость диска с дистрибутивами.

2.2 Оплата суммы, прав на компьютерные программы осуществляется по факту передачи прав не позднее 5 (пяти) банковских дней с даты подписания обеими Сторонами акта приема-передачи прав на компьютерные программы.

2.3 Оплата осуществляется в безналичном порядке в белорусских рублях путем перечисления денежных средств на расчетный счет Сублицензиата.

3. СРОКИ И УСЛОВИЯ ПЕРЕДАЧИ ПРАВ НА КОМПЬЮТЕРНЫЕ ПРОГРАММЫ. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

3.1 Передача прав на компьютерные программы Сублицензиару осуществляется в срок 7 (семь) банковских дней с момента подписания настоящего Договора и передачи Сублицензиату всех необходимых документов, в том числе подписанного Договора.

3.2 Передача ключевых файлов и (или) буквенно-цифровых кодов, предназначенных для активации (приведения в работоспособное полнофункциональное состояние) компьютерных программ осуществляется по электронным каналам связи одновременно с передачей прав на компьютерные программы. Дистрибутивы компьютерных программ загружаются с официального сайта производителя _____ (*указывается сайт производителя)*, а также передаются на диске по товарно-транспортной накладной.

3.3 Приемка прав на компьютерные программы осуществляется подписанием сторонами акта приема-передачи прав на компьютерные программы.

3.4 Датой передачи прав на компьютерные программы считается дата подписания обеими Сторонами акта приема-передачи прав на компьютерные программы.. Сублицензиар в течение 5 (пяти) рабочих дней с момента получения акта приема-передачи прав на компьютерные программы обязан подписать его и вернуть Сублицензиату или в тот же срок в письменном виде предоставить Сублицензиату мотивированный отказ от приемки прав на компьютерные программы, в противном случае права на компьютерные программы считаются принятыми надлежащим образом. Мотивированный отказ представляется в письменном виде с обоснованием причин.

3.5. Сублицензиат обязуется обеспечить Сублицензиару на постоянной основе, в рамках установленного п.1.1 Договора срока пользования правами на компьютерные программы техническую поддержку на следующих условиях:

Техническая поддержка осуществляется в объеме:

− предоставление информационной поддержки: оказание консультаций по функциональным возможностям программного обеспечения (далее – ПО), ошибкам его функционирования, некорректной работой функций;

− устранение ошибок функционирования ПО и его восстановления после критических ошибок;

− уведомление о выходе новых версий и исправлений (патчей);

− своевременное предоставление исправлений (патчей), новых версий (обновлений);

− обучение персонала Сублицензиара работе с ПО;

− проведение вебинаров, тренингов (по предварительному согласованию Сторон).

Прием заявок на техническую поддержку осуществляется по контактному телефону _____ (*указывается номер телефона*) в рабочие дни с понедельника по четверг с 08:30 до 17:30, в пятницу – с 08:30 до 16:15 и/или по электронному адресу Сублицензиата _____ (*указывается электронный адрес*) круглосуточно. Обработка поступивших заявок осуществляется в рабочие дни с понедельника по четверг с 08:30 до 17:30, в пятницу – с 08:30 до 16:15. Заявки, поступившие вне указанного времени, обрабатываются на следующий рабочий день.

Время реакции Сублицензиата на поступившую заявку – не более 60 минут.

Время предоставления Сублицензиатом рекомендаций/решений по заявке Сублицензиара не более 3 рабочих дней.

4. ОТВЕТСТВЕННОСТЬ СТОРОН

4.1 В случае неисполнения или ненадлежащего исполнения своих обязательств по-настоящему Договору стороны несут ответственность в соответствии с законодательством Республики Беларусь и настоящим Договором.

4.2 Сублицензиару известны важнейшие функциональные свойства компьютерных программ, в отношении которых предоставляются права на использование, а также условия лицензионного соглашения для конечных пользователей; Сублицензиар несет риск

соответствия компьютерных программ его желаниям и потребностям, а также риск соответствия условий и объема предоставляемых прав своим желаниям и потребностям. Сублицензиат не несет ответственность за какие-либо убытки, ущерб, не зависимо от причин его возникновения, (включая, но не ограничиваясь этим, особый, случайный или косвенный ущерб, убытки, связанные с недополученной прибылью, прерыванием коммерческой или производственной деятельности, утратой деловой информации, небрежностью, или какие-либо иные убытки), возникшие вследствие использования или невозможности использования компьютерных программ.

4.3 За необеспечение Сублицензиатом установленного в п.3.1 Договора срока передачи права на компьютерные программы, Сублицензиат уплачивает Сублицензиару неустойку в виде пени в размере 0,15 % от суммы вознаграждения, определенной в п.2.1. Договора, за каждый день просрочки.

4.4. Сублицензиат обязуется возместить Сублицензиару все убытки, включая упущенную выгоду, причиненные Сублицензиару в связи с предъявлением правообладателем и/или иными третьими лицами претензий в отношении правомерности использования компьютерных программ и прав на них.

4.5. За нарушение срока оплаты неисключительного имущественного права, установленного п.2.1 Договора Сублицензиар уплачивает Сублицензиату неустойку в виде пени в размере 0,15 % от суммы вознаграждения, определенной в п.2.1. Договора за каждый день просрочки.

5. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ

5.1 Стороны, по-настоящему Договору, освобождаются от ответственности за полное или частичное неисполнение своих обязательств в случае, если такое неисполнение явилось следствием обстоятельств непреодолимой силы, то есть событий, которые нельзя было предвидеть или предотвратить. К таким событиям относятся: стихийные бедствия, военные действия, принятие государственными органами или органами местного самоуправления нормативных правовых актов и иные действия, препятствующие сторонам выполнению своих обязательств.

5.2 При наступлении обстоятельств, указанных в пункте 5.1 настоящего Договора, каждая Сторона должна не позднее 5 (пяти) дней с момента наступления таких обстоятельств известить о них в письменном виде другую Сторону. Извещение должно содержать данные о характере обстоятельств, оценку их влияния на возможность исполнения Стороной своих обязательств по данному Договору, а также предполагаемые сроки их действия.

5.3 В случае наступления обстоятельств, предусмотренных пунктом 5.1 настоящего Договора, срок выполнения Стороной обязательств по-настоящему Договору отодвигается соразмерно времени, в течение которого действуют эти обстоятельства и их последствия.

5.4 Если действие обстоятельств непреодолимой силы продолжается свыше одного месяца, Стороны проводят дополнительные переговоры для выявления приемлемых альтернативных способов исполнения настоящего Договора либо настоящий Договор подлежит расторжению в установленном порядке.

6. ДЕЙСТВИЕ ДОГОВОРА. ИНЫЕ УСЛОВИЯ

6.1 Настоящий Договор вступает в силу с момента его подписания обеими Сторонами и действует до полного исполнения обязательств Сторонами.

6.2 Все изменения и дополнения к настоящему Договору действительны только в случае, если они составлены в письменной форме и подписаны уполномоченными на, то представителями Сторон.

6.3 Настоящий Договор, протоколы разногласий, дополнительные соглашения к нему могут быть заключены путем обмена посредством факсимильной связи, позволяющей достоверно определить, что документ исходит от стороны по Договору. В этом случае оригиналы документов должны быть переданы почтой. До получения оригиналов Стороны признают юридическую силу факсимильной копии документа.

6.4 Все приложения к настоящему Договору являются его неотъемлемой частью.

6.5 Сторона, чьи права или законные интересы нарушены, с целью непосредственного урегулирования спора обязана предъявить другой стороне претензию (письменное предложение о добровольном урегулировании спора). Сторона, получившая претензию, в десятидневный срок со дня ее получения письменно уведомляет заявителя претензии о результатах ее рассмотрения. В случае недостижения Сторонами компромисса в результате досудебного урегулирования спора, все споры и разногласия по заключению, исполнению, изменению, расторжению настоящего Сублицензионного Договора рассматриваются в порядке, предусмотренном законодательством Республики Беларусь.

6.6 Настоящий Договор составлен в двух экземплярах, имеющих равную юридическую силу, по одному для каждой из Сторон.

6.7 В случае изменения реквизитов одной из Сторон по Договору, Стороны обязуются уведомить друг друга о произошедших изменениях в письменном виде в течение 5 (пяти) рабочих дней с момента изменений, в противном случае, обязательства по Договору будут считаться исполненными не уведомленной Стороной надлежащим образом. Заключение дополнительного соглашения в данном случае не требуется.

6.8 К настоящему Договору прилагается и является его неотъемлемой частью:

Приложение 1: Спецификация

Приложение 2: Требования, предъявляемые к компьютерным программам

7. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН:

СУБЛИЦЕНЗИАТ:

_____ /

м.п.

СУБЛИЦЕНЗИАР:

ОАО «БМРЦ»,
ул. Кальварийская, 7, 220048, г. Минск, Республика Беларусь
тел. +375 17 259 14 85, факс +375 17 375 34 03
официальный сайт: www.bisc.by; e-mail: agreement@bisc.by; СМДО: Org10841
ответственное подразделение – Управление защиты информации в АИС - тел. 259 14 20;
правовые вопросы – тел. +375 17 259 14 09, факс +375 17 373 91 66;
финансовые вопросы – тел. +375 17 259 14 04.
УНП 193002449, ОКПО 501297625000
IBAN BY09 MMBN 3012 0717 8001 0000 0000
в ОАО «Банк Дабрабыт»,
ул. Коммунистическая, 49, пом.1, 220002, г. Минск, Республика Беларусь
BIC MMBNBY22

_____ /

м.п.

Приложение № 1
к Сублицензионному Договору
№ _____ от ____.___.2023

Спецификация

№	Неисключительные имущественные права	Кол.	Стоимость за ед. бел. руб.	Цена без НДС, бел. руб.	Стоимость без НДС, бел. руб.	Сумма НДС, бел. руб.	Всего с НДС, бел. руб.
1.	Лицензия на использование программы Система мониторинга состояния кибербезопасности с предоставлением технической поддержки **на 24 месяца**						
ИТОГО:							

Общая стоимость составляет: _____ (_____) белорусский рубль ___ копеек, в том числе НДС _____ (_____) белорусских рублей ___ копеек

От Сублицензиата

_____/
м.п.
«___» _____ 2023 г.

От Сублицензиара

_____/
м.п.
«___» _____ 2023г.

Приложение № 2
к Сублицензионному Договору
№ _____ от ____.___.2023

ТРЕБОВАНИЯ,
предъявляемые к компьютерным программам

Система должна включать в себя следующие подсистемы и компоненты:

подсистема сбора и обработки событий информационной безопасности (SIEM);

подсистема сбора и анализа индикаторов компрометации и киберугроз (Threat Intelligence Platform);

компонент динамического анализа вредоносных файлов (Sandbox).

Лицензирование платформы должно обеспечивать возможность использования ее с целью оказания услуг на коммерческой основе.

Срок действия лицензий с предоставлением технической поддержки – 24 (двадцать четыре) месяца.

Требования, предъявляемые к подсистеме сбора и обработки событий информационной безопасности

Подсистема должна иметь сертификат соответствия требованиям ТР 2013/027/BY, СТБ 34.101.74-2017 (пункт 7.3.).

Требование к оборудованию

Компоненты подсистемы должны поддерживать установку как на физических, так и на виртуальных машинах.

Основные компоненты (модули, отвечающие за сбор событий, корреляцию, хранение событий) должны поддерживать установку на операционных системах семейства Linux:

Astra Linux Special Edition 1.7 и выше;

Oracle Linux версии 8.4 и выше;

Debian версий 10.3 - 10.13.

Подсистема должна обеспечивать высокую производительность и поддерживать прием и обработку потока в размере от 10 000 событий в секунду (EPS).

Требования к архитектуре подсистемы

Подсистема должна поддерживать горизонтальное масштабирование ключевых ее компонентов: коллектора, коррелятора и хранилища событий.

Компоненты подсистемы должны поддерживать установку в распределённых и изолированных сетях без необходимости доступа к сети Интернет.

Подсистема должна обеспечивать централизованное управление посредством веб-консоли без установки дополнительного ПО на АРМ администратора.

Подсистема должна поддерживать разделение ресурсов и сервисов на логические сущности («тенанты»), позволяя в рамках единой инсталляции предоставлять возможность разграничения прав доступа пользователей подсистемы к событиям, инцидентам, правилам корреляции, нормализации, а также определенным настройкам подсистемы.

Подсистема должна обеспечивать возможность централизованного обновления конфигурации или перезапуска компонентов, в том числе принудительного. Подсистема должна поддерживать возможность добавления сторонних компонентов в процесс обработки событий. Подсистема должна обеспечивать режим работы отказоустойчивого кластера для всех основных компонентов с «горячим» переключением (High Availability).

Подсистема должна поддерживать работу с несколькими независимыми кластерами хранилища событий для возможности организации гибких схем географически распределенных подсистем.

Архитектура решения должна обеспечивать возможность развертывания в географически распределенной инфраструктуре.

Подсистема должна поддерживать поиск по событиям в удалённых офисах из центрального узла подсистемы.

Требования к сбору, анализу и хранению событий

Подсистема должна обеспечивать как активный, так и пассивный сбор событий с источников данных.

Подсистема должна осуществлять поиск (инвентаризацию) активов или поддерживать импорт активов из сторонних источников.

Подсистема должна поддерживать возможность сохранения исходного события.

Подсистема должна поддерживать возможность добавления пользовательских типов источников событий и соответствующей настройки правил разбора и нормализации.

Подсистема должна обеспечивать создание пользовательских нормализаторов на основе поддерживаемых форматов и протоколов сбора данных.

Подсистема должна обеспечивать возможность мониторинга поступления событий от источников с отслеживанием количества событий в указанный промежуток времени и автоматическим оповещением на электронную почту в случае отклонения от заданных параметров мониторинга для каждого из источников в частности.

Подсистема должна поддерживать импорт/экспорт контента и ресурсов: правил корреляции, парсеров, коннекторов и т.д.

Требования к функциям обогащения событий

Подсистема должна поддерживать обогащение событий с помощью Threat Intelligence (сведения об индикаторах компрометации и соответствующем контексте: хэши файлов, URL-адреса, внешние IP-адреса), DNS, служба каталогов Active Directory, геоданные.

Требования к функциям корреляции событий, работы с инцидентами

Подсистема должна обеспечивать потоковую корреляция событий для выявления инцидентов и событий ИБ на основе правил корреляции в режиме близком к режиму реального времени.

Подсистема должна поставляться с набором предустановленных правил корреляции, созданных на основе исследований актуальных угроз и способов атак, разработанных на базе матрицы MITRE ATTACK.

Подсистема должна обеспечивать возможность многоуровневой корреляции с передачей результатов работы одного правила корреляции на вход другим правилам корреляции.

Подсистема должна обеспечивать возможность использования в правилах обогащения и корреляции табличных списков.

Подсистема должна поддерживать возможность тестирования правил корреляции на исторических данных.

Подсистема должна иметь возможность приоритизации выявленных угроз ИБ как с учётом уровня критичности правила корреляции, так и с учетом критичности и количества затронутых информационных активов.

Подсистема должна поддерживать автоматическое объединение скоррелированных событий, являющихся результатом работы одного и того же правила корреляции, в карточку инцидента.

Подсистема должна обеспечивать управление карточками инцидентов, включая: ручное добавление или удаление карточки инцидента, или изменение данных карточки; возможность вручную связать инцидент с событиями и активами; возможность создания задач для

пользователей подсистемы по расследованию, сбору доказательств и восстановлению работоспособности информационной систем; возможность сохранения проведенных мероприятий и их комментирование; хранение истории изменений карточки инцидента и выполнения поставленных задач.

Подсистема должна обеспечивать поддержку механизмов фильтрации и сортировки инцидентов. Подсистема должна обеспечивать автоматическую ассоциацию активов с событиями и/или инцидентами.

Требования к управлению сведениями об активах

Подсистема должна поддерживать создание пользовательских групп (категорий) активов.

Подсистема должна обеспечивать возможность ручной и автоматической категоризации активов на основе одного или комбинации признаков.

При задании условий автоматической категоризации активов подсистема должна обеспечивать возможность тестирования заданных условий по имеющейся базе информационных активов.

Подсистема должна поддерживать возможности поиска по активам, сохраненных во встроенной базе данных.

Требования к функциям работы с инцидентами

Подсистема должна обеспечить автоматическое формирование карточек инцидентов по результатам срабатывания правил корреляции.

В подсистеме должна быть реализована возможность ручной привязки дополнительной информации к инциденту – по пользователям, активам, событиям корреляции с возможности классификации инцидента.

Требования к визуализации и отчётности

Подсистема должна предоставлять инструменты визуализации и отчётности.

Подсистема должна поставляться с предустановленным набором графических панелей и отчётов.

Подсистема должна поддерживать возможность создания пользовательских дашбордов и шаблонов отчетов.

Подсистема должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов.

Подсистема должна обеспечивать построение отчетов по инцидентам.

Подсистема должна обеспечивать возможность отправки отчетов по почте.

Подсистема должна поддерживать рассылку отчетов по настраиваемому расписанию.

Требования к мониторингу производительности

Подсистема должна обеспечивать сбор и хранение метрик производительности всех компонентов подсистемы.

Метрики производительности должны отображаться в графическом интерфейсе подсистемы.

Подсистема должна поддерживать передачу метрик производительности во внешние системы мониторинга.

Требования к безопасности

Подсистема должна обеспечивать разграничение прав доступа к функционалу на основе ролевой модели.

Подсистема должна регистрировать события доступа и значимых изменений конфигурации.

Подсистема должна поддерживать аутентификацию и авторизацию с использованием следующих механизмов:

локальная база учётных данным (по логину-паролю) пользователей;

Active Directory.

Подсистема должна иметь встроенные механизмы противодействия попыткам подбора пароля.

Требования, предъявляемые к подсистеме сбора и анализа индикаторов компрометации и киберугроз

Подсистема должна обеспечивать доступ пользователей через графический веб-интерфейс (далее также — пользовательский интерфейс).

Должна обеспечиваться реализация ролевой модели управления доступом пользователей к функциям подсистемы.

Должна обеспечиваться возможность создания локальных учетных записей пользователей в интерфейсе подсистемы.

Должна обеспечиваться возможность просмотра через пользовательский интерфейс индикаторов компрометации.

Должна обеспечиваться возможность задания уровня доверия к источнику информации об угрозах через пользовательский интерфейс.

Подсистема должна поддерживать возможность получения индикаторов компрометации из различных источников.

Подсистема должна обеспечивать возможность добавлять и просматривать источники информации об угрозах через пользовательский интерфейс.

Должен предоставляться API для загрузки в подсистему индикаторов компрометации.

Подсистема должна обеспечивать возможность автоматического обогащения поступающих в нее индикаторов компрометации.

Подсистема должна обеспечивать возможность обогащения информации в составе индикаторов компрометации пользователями подсистемы.

Подсистема должна обеспечивать возможность использования правил обогащения, созданных пользователями.

Должно обеспечиваться хранение и экспорт настроек подсистемы.

Подсистема должна обеспечивать возможность создания и выгрузки наборов индикаторов компрометации, предназначенных для экспорта в смежные и сторонние системы (далее также – фидов).

Подсистема должна обеспечивать возможность настройки создания фидов:

– периодичность автоматического создания фидов;

– критерии попадания индикаторов компрометации в фид;

– глубина выборки индикаторов компрометации для попадания в фид.

Подсистема должна обеспечивать возможность выгрузки файлов фидов в форматах STIX 2.0 и JSON.

Подсистема должна обеспечивать возможность выгрузки файлов фидов через API.

В комплекте поставки подсистемы должны быть фиды, содержащие информацию о вредоносных хеш-данных, данные об IP-репутации, данные фишинговых URLадресов, в т.ч релевантных белорусскому сегменту глобальной сети Интернет (коммерческие версии).

Требования, предъявляемые к компоненту динамического анализа вредоносных файлов

Компонент должен иметь сертификат соответствия требованиям ТР 2013/027/BY.

Компонент должен поддерживать следующие операционные системы для анализа файлов в изолированной среде:

CentOS;

Microsoft Windows 7 x64/x86;

Microsoft Windows 10 x64;

Компонент должен поддерживать кастомизацию образов операционных систем для разворачивания в изолированной среде.

Компонент должен автоматически масштабировать количество виртуальных машин для анализа файлов в зависимости от выделенных ресурсов на этапе развертывания.

Компонент должен анализировать на основе заданных правил поведения следующие действия: создание файлов; запуск процессов; выполнение интернет-запросов; изменения в системном реестре.

Компонент должен иметь возможность ручной загрузки объектов на проверку через веб-интерфейс.

Компонент должен выстраивать граф поведения образцов файлов в изолированной среде после проведения поведенческого анализа и отображать его в графическом интерфейсе.

Компонент должен обеспечивать запуск и анализ поведения в изолированной среде файлов следующих форматов:

PE (исполняемые);

скрипты (vbs, bat, ps);

Microsoft Office (rtf, doc/docx, xls/xlsx, ppt/pptx);

Adobe Acrobat (pdf);

архивы (rar, 7z, zip).

Компонент должен уметь извлекать файлы из архивов, в том числе, защищенных паролем (при его наличии).

Компонент должен иметь встроенный механизм AntiEvasion для защиты от техник обхода песочниц.

Компонент должен иметь возможность доступа к сети Интернет для проведения более глубокого анализа поведения анализируемых объектов.

Компонент должен обеспечивать возможность выгрузки анализируемого контекста:

копия сетевого трафика;

созданные артефакты/сэмплы файлов;

лог активности объекта в изолированной среде.

От Сублицензиата	**От Сублицензиара**
_____/	_____/
м.п.	м.п.
«___» _____ 2023 г.	«___» _____ 2023г.