e-mail: info@uzairways.com
e-xat: airways@exat.uz
tel: +998 (78) 140-46-23
www.uzairways.com

O'zbekiston, Toshkent,
Amir Temur shohko'chasi, 41
GSP-100060

Uzbekistan, Tashkent,
41, Amir Temur avenue
GSP-100060

UZBEKISTAN AIRWAYS

Joint-Stock Company | Aksiyadorlik jamiyati

УТВЕРЖДАЮ:
Вр.и.о. Первого Заместителя
Председателя Правления
АО «Uzbekistan Airways»

Musanov U.A.
«__» _____ 2026 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на приобретение услуги доступа к платформе Threat Intelligence для АО «Uzbekistan Airways»

РАСШИРЕННАЯ СПЕЦИФИКАЦИЯ ТЕХНИЧЕСКИХ ТРЕБОВАНИЙ

Платформа Threat Intelligence

1. Общие требования к платформе Threat Intelligence

№ треб.	Описание требования
1.1	Производитель предлагаемого решения должен входить в квадрант лидеров (Leaders Quadrant) актуального на дату подачи предложения исследования Gartner Magic Quadrant for Cyberthreat Intelligence Technologies.
1.2	Решение должно представлять собой единую платформу Threat Intelligence, предназначенную для централизованного сбора, хранения, обработки, анализа, обогащения и распространения информации о киберугрозах.
1.3	Решение должно обеспечивать централизованное управление индикаторами компрометации (IOC) и связанным с ними аналитическим контекстом.
1.4	Платформа должна обеспечивать использование Threat Intelligence в процессах мониторинга, обнаружения, расследования и реагирования на инциденты информационной безопасности.
1.5	Решение должно обеспечивать автоматизацию основных процессов работы с Threat Intelligence, включая обработку, анализ, обогащение и распространение информации о киберугрозах.
1.6	Платформа должна обеспечивать оценку актуальности, достоверности и релевантности Threat Intelligence для целей обеспечения информационной безопасности Заказчика.
1.7	Решение должно обеспечивать централизованное представление и взаимосвязь различных объектов Threat Intelligence, включая индикаторы компрометации, угрозы, вредоносное программное обеспечение, киберкампании и субъектов угроз.

2. Требования к источникам Threat Intelligence

№ треб.	Описание требования
2.1	Платформа должна обеспечивать автоматизированное получение Threat Intelligence из множества внешних источников.
2.2	Решение должно поддерживать подключение коммерческих и открытых источников Threat Intelligence.
2.3	Платформа должна обеспечивать возможность получения данных от CERT, CSIRT, отраслевых и иных доверенных источников.
2.4	Решение должно поддерживать подключение пользовательских источников Threat Intelligence.
2.5	Для каждого источника должна обеспечиваться настройка параметров подключения и периодичности обновления.

2.6	Платформа должна осуществлять контроль доступности и актуальности подключенных источников.
2.7	Решение должно формировать уведомления при прекращении или сбое получения данных от источника.
2.8	Платформа должна обеспечивать создание и ведение внутренних источников Threat Intelligence Заказчика.

3. Требования к Dark Web Monitoring

№ треб.	Описание требования
3.1	Платформа должна обеспечивать мониторинг доступных источников внешней Threat Intelligence, включая источники Dark Web и Deep Web, в целях выявления угроз, потенциально связанных с Заказчиком.
3.2	Решение должно обеспечивать выявление упоминаний наименования Заказчика, его брендов, доменных имен и иных определяемых Заказчиком объектов мониторинга.
3.3	Платформа должна обеспечивать мониторинг информации о потенциальных утечках учетных данных и данных, связанных с Заказчиком.
3.4	Решение должно обеспечивать выявление информации о публикации, продаже или распространении данных, предположительно относящихся к Заказчику.
3.5	Платформа должна обеспечивать выявление информации о деятельности Threat Actors и киберпреступных группировок, представляющих потенциальную угрозу для Заказчика.
3.6	Решение должно поддерживать мониторинг информации, связанной с ransomware-группировками и иной киберпреступной активностью.
3.7	Платформа должна обеспечивать возможность настройки объектов мониторинга и формирования уведомлений при обнаружении новой релевантной информации.
3.8	Платформа должна обеспечивать возможность связывания выявленной информации с соответствующими объектами Threat Intelligence, включая Threat Actors, Campaigns, Malware и IOC.

4. Требование к управлению индикаторами компрометации (IOC)

№ треб.	Описание требования
4.1	Платформа должна поддерживать основные типы индикаторов компрометации, включая IPv4-адреса, IPv6-адреса, доменные имена, URL, файловые хеш-суммы, адреса электронной почты, сетевые диапазоны и TLS/SSL-сертификаты.
4.2	Решение должно поддерживать возможность создания пользовательских типов индикаторов.

4.3	Платформа должна обеспечивать автоматическое определение типа индикатора при наличии достаточной информации.
4.4	Для каждого IOC должна поддерживаться информация об источнике происхождения.
4.5	Для IOC должны поддерживаться уровень достоверности, критичность и оценка риска.
4.6	Платформа должна поддерживать информацию о времени первого и последнего обнаружения индикатора.
4.7	Для IOC должна поддерживаться возможность добавления тегов и аналитических комментариев.
4.8	Платформа должна обеспечивать автоматическое выявление и объединение дублирующихся индикаторов с сохранением информации обо всех источниках.

5. Требование к нормализации и обогащению Threat Intelligence

№ треб.	**Описание требования**
5.1	Платформа должна обеспечивать нормализацию данных Threat Intelligence, поступающих из различных источников.
5.2	Решение должно приводить идентичные типы Threat Intelligence к единому формату представления.
5.3	При обработке и нормализации должна сохраняться информация об исходном источнике данных.
5.4	Платформа должна обеспечивать автоматическое обогащение Threat Intelligence дополнительной аналитической информацией.
5.5	Решение должно поддерживать получение информации о географическом расположении, ASN, DNS и репутации сетевых индикаторов при наличии соответствующих источников.
5.6	Платформа должна поддерживать обогащение доменов, IP-адресов, URL и файловых хешей.
5.7	Платформа должна обеспечивать возможность подключения дополнительных внешних и внутренних источников обогащения.
5.8	Результаты обогащения должны сохраняться в контексте соответствующего объекта Threat Intelligence.

6. Требования к аналитическому контексту Threat Intelligence

№ треб.	**Описание требования**
6.1	Платформа должна поддерживать ведение информации о Threat Actors.
6.2	Решение должно поддерживать ведение информации о вредоносном программном обеспечении и его семействах.

6.3	Платформа должна поддерживать ведение информации о кампаниях киберугроз.
6.4	Платформа должна обеспечивать связывание IOC с Threat Actors, Malware и Campaigns.
6.5	Платформа должна поддерживать визуализацию взаимосвязей между объектами Threat Intelligence.
6.6	Решение должно обеспечивать хранение аналитического описания и дополнительного контекста для объектов Threat Intelligence.

7. Требования к MITRE ATT&CK и TTP

№ треб.	Описание требования
7.1	Платформа должна поддерживать сопоставление Threat Intelligence с MITRE ATT&CK.
7.2	Решение должно поддерживать связь Threat Actors, Malware и Campaigns с тактиками и техниками MITRE ATT&CK.
7.3	Платформа должна обеспечивать визуализацию TTP, связанных с объектами Threat Intelligence.
7.4	Решение должно обеспечивать возможность поиска Threat Intelligence по тактикам и техникам MITRE ATT&CK.
7.5	Платформа должна обеспечивать актуализацию используемой базы знаний MITRE ATT&CK.

8. Требование к Vulnerability Intelligence

№ треб.	Описание требования
8.1	Платформа должна обеспечивать получение, обработку и анализ информации об известных уязвимостях, включая идентификаторы CVE.
8.2	Для каждой уязвимости должна обеспечиваться возможность получения дополнительного Threat Intelligence контекста.
8.3	Платформа должна предоставлять информацию о наличии публично доступного Proof of Concept (PoC) или exploit для соответствующей уязвимости при наличии таких сведений в используемых источниках Threat Intelligence.
8.4	Платформа должна предоставлять информацию о фактах активной эксплуатации уязвимости злоумышленниками при наличии соответствующих сведений.
8.5	Решение должно обеспечивать выявление информации о связи уязвимости с известными Threat Actors, вредоносным программным обеспечением, киберкампаниями и ransomware-активностью.

8.6	Решение должно обеспечивать возможность мониторинга появления новой информации, связанной с ранее выявленными уязвимостями.
8.7	Платформа должна поддерживать уведомление о появлении информации о новых критических уязвимостях, представляющих потенциальную угрозу для Заказчика.

9. Требования к интеграции

№ треб.	Описание требования
9.1	Платформа должна обеспечивать интеграцию с SIEM системой посредством поддерживаемого приложения, коннектора, API или иных документированных механизмов интеграции.
9.2	Интеграция должна обеспечивать передачу индикаторов компрометации и связанного Threat Intelligence контекста.
9.3	Решение должно поддерживать передачу информации о Threat Actors, Malware, Campaigns и уязвимостях при наличии соответствующей интеграционной возможности.
9.4	Должна обеспечиваться возможность автоматического обновления передаваемой Threat Intelligence.
9.5	Должна обеспечиваться возможность отзыва или прекращения использования IOC, утративших актуальность.
9.6	Платформа должна обеспечивать возможность обогащения событий информационной безопасности в Splunk данными Threat Intelligence.
9.7	При совпадении событий с IOC должна обеспечиваться возможность получения дополнительного контекста об угрозе.
9.8	Для совпавших IOC должны поддерживаться сведения об уровне риска, достоверности и источнике Threat Intelligence.
9.9	Должна обеспечиваться возможность использования Threat Intelligence при корреляции событий безопасности и выявлении инцидентов.
9.10	Решение должно обеспечивать возможность передачи результатов Risk-Based Vulnerability Prioritization.

10. Требования к форматам данных и API

№ треб.	Описание требования
10.1	Платформа должна поддерживать импорт и экспорт данных в распространенных машиночитаемых форматах, включая JSON и CSV.
10.2	Платформа должна обеспечивать возможность предоставления Threat Intelligence внешним системам через API и стандартизированные механизмы обмена.

10.3	Платформа должна поддерживать настройку правил обработки и преобразования данных, получаемых из пользовательских источников.
10.4	Платформа должна предоставлять документированный программный интерфейс API.
10.5	API должен обеспечивать доступ к основным функциям и объектам Threat Intelligence в соответствии с правами пользователя.
10.6	Решение должно поддерживать защищенные механизмы аутентификации и авторизации при использовании API.
10.7	Платформа должна поддерживать автоматизированную интеграцию с внешними информационными системами.
10.8	Операции, выполняемые через API, должны поддерживать журналирование.

11. Требование к поиску и аналитике

№ треб.	**Описание требования**
11.1	Платформа должна обеспечивать поиск по основным объектам Threat Intelligence.
11.2	Решение должно поддерживать поиск по IOC, Threat Actors, Malware, Campaigns, CVE и MITRE ATT&CK.
11.3	Платформа должна обеспечивать расширенную фильтрацию результатов поиска.
11.4	Решение должно поддерживать визуализацию связей между объектами Threat Intelligence.
11.5	Платформа должна обеспечивать возможность анализа инфраструктуры и взаимосвязей, связанных с угрозами.

12. Требование к дашбордам и отчетности

№ треб.	**Описание требования**
12.1	Платформа должна предоставлять настраиваемые дашборды для отображения актуальной Threat Intelligence.
12.2	Дашборды должны обеспечивать отображение новых и наиболее критичных угроз, IOC, Threat Actors, Campaigns и уязвимостей.
12.3	Решение должно поддерживать визуализацию совпадений Threat Intelligence с инфраструктурой Заказчика.
12.4	Платформа должна обеспечивать формирование аналитических отчетов.
12.5	Решение должно поддерживать автоматическое формирование отчетов по расписанию.
12.6	Решение должно поддерживать экспорт результатов в распространенные форматы.

13. Требование к уведомлениям

№ треб.	Описание требования
13.1	Платформа должна поддерживать формирование уведомлений о появлении новых критичных Threat Intelligence объектов.
13.2	Решение должно поддерживать уведомления при обнаружении совпадений Threat Intelligence с инфраструктурой Заказчика.
13.3	Платформа должна поддерживать уведомления при появлении информации о значимых активных угрозах и уязвимостях.
13.4	Платформа должна поддерживать уведомления о выявлении потенциальных утечек учетных данных и данных, связанных с Заказчиком.
13.5	Должна поддерживаться передача уведомлений посредством электронной почты, API или иных интеграционных механизмов.
13.6	Платформа должна поддерживать формирование уведомлений о появлении новых критичных Threat Intelligence объектов.

14. Требование к доступности и уровень сервиса (SLA)

№ треб.	Описание требования
14.1	Производитель и/или Поставщик должен обеспечивать доступность предоставляемой Платформы в соответствии с условиями соглашения об уровне сервиса (SLA).
14.2	Доступность Платформы должна составлять не менее **99,9 %** в течение календарного месяца, за исключением согласованных периодов плановых технических работ.
14.3	Условия SLA должны определять порядок регистрации, классификации и обработки обращений, связанных с недоступностью или нарушением функционирования Платформы.
14.4	Производитель и/или Поставщик должен обеспечивать техническую поддержку Платформы в течение срока действия подписки или технической поддержки.
14.5	Должна обеспечиваться возможность получения информации о состоянии доступности Платформы и проводимых плановых технических работах.

15. Требование к технической поддержке

№ треб.	Описание требования
15.1	Производитель и/или Поставщик должен обеспечивать доступность предоставляемой Платформы в соответствии с условиями соглашения об уровне сервиса (SLA).

15.2	Доступность Платформы должна составлять не менее **99,9 %** в течение календарного месяца, за исключением согласованных периодов плановых технических работ.
15.3	Условия SLA должны определять порядок регистрации, классификации и обработки обращений, связанных с недоступностью или нарушением функционирования Платформы.
15.4	Производитель и/или Поставщик должен обеспечивать техническую поддержку Платформы в течение срока действия подписки или технической поддержки.
15.5	Должна обеспечиваться возможность получения информации о состоянии доступности Платформы и проводимых плановых технических работах.

16. Требования к лицензированию

№ треб.	Описание требования
16.1	Срок лицензирования или подписки - не менее 1 года или 3 лет с момента активации (требуется официальное письмо с указанием срока предоставления лицензий и технической поддержки).
16.2	Требования к новизне - закупаемые лицензии/подписка должны быть новыми, ранее не использованными и не активированными.
16.3	Условия оплаты - 100% оплата в течение 10 дней с момента подписания сторонами акта выполненных работ/приема-передачи и подтверждения счета-фактуры.
16.4	Закупаемые лицензии/подписка должны быть оформлены на АО «Uzbekistan Airways» без права третьих лиц на поставляемые лицензии/подписку.

17. Требования, предъявляемые к участникам отбора

№ треб.	Описание требования
17.1	Техническая поддержка - гарантийное письмо о технической поддержке в режиме 24/7 в течение 1 года или 3 лет с момента активации лицензий или подписики и подписания акта приема-передачи.
17.2	Сроки поставки лицензии и оказания услуг - в течение 30 рабочих дней после подписания договора.

РАЗРАБОТАНО:

Врио директора департамента
ИТ инфраструктуры, цифровизации
и кибербезопасности **Kirillov A.A.**

С О Г Л А С О В А Н О:

Врио Первого заместителя Председателя правления по вопросам трансформации, финансов и приватизации **Sattarov A.A.**