Уведомление о проведении закупочной процедуры

АО «ОХК «УРАЛХИМ» (далее - «Организатор») настоящим объявляет о проведении закупочной процедуры в форме запроса предложений (далее – «процедура») на поставку программного обеспечения в рамках проекта «21_059_Внедрение защиты веб-приложений».

Для участия в процедуре юридическим лицам (далее – «Участник») необходимо зарегистрироваться в Ariba Network или войти в свою существующую учетную запись воспользовавшись ссылкой и следуя инструкциям http://www.uralchem.ru/purchase/tenders_Ariba/

После прохождения регистрации необходимо проинформировать организатора конкурентной процедуры для добавления Вашей компании в список участников.
Мосиенко Роман Борисович
по телефону: +7 (495) 721-89-89 (доб.12029) или
по электронной почте: roman.mosienko@uralchem.com.

Настоящее уведомление о проведении конкурентной процедуры в форме запроса предложений не является извещением о проведении конкурса (публичного конкурса) и не регулируется статьями 447—449, 1057—1061 Гражданского кодекса РФ.

Участник самостоятельно несет все расходы, связанные с подготовкой и подачей Предложения. Организатор не несет перед Участниками обязательств по компенсации понесенных расходов и по заключению договора по результатам проведения запроса предложений.

Для участия в закупочных процедурах, проводимых предприятием Группы «УРАЛХИМ» на портале SAP Ariba, Ваша компания соглашается с положениями и условиями «Соглашения участника», размещённого в Ariba Network.

Дата и время окончания приема Предложений: до 15.09.2021 г., 18-00 МСК.
Предложения, полученные позже установленного выше срока, будут отклонены Организатором процедуры без рассмотрения по существу, независимо от причин нарушения срока.
При необходимости Организатор, с уведомлением всех Участников, имеет право продлить срок окончания приема Предложений или изменить условия проведения конкурентной процедуры.

Сроки поставки: 01.10.2021.

По всем дополнительным вопросам по проекту, просьба обращаться
Файзуллин Александр Игоревич – Руководитель управления информационной безопасности
по телефону: +7 (495) 721-89-89 (доб. 12060) или
по электронной почте: Alexander.Faizullin@uralchem.com

Артемьев Никита Григорьевич
по телефону:+7-495-721-89-89 (доб.12031) или
по электронной почте: nikita.artemev@uralchem.com

Приложения:
Техническое задание на закупку программного обеспечения, предназначенного для защиты WEB приложений (WAF)

Техническое задание
на закупку программного обеспечения, предназначенного для защиты WEB приложений (WAF)

АО «ОХК «УРАЛХИМ»

г. Москва 2021 г.

Содержание

1. Список терминов и сокращений

API	Application Programming Interface
AD	Active Directory
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
CLI	Command Line Interface
DDoS	Distributed Denial of Service
FTP	File Transfer Protocol
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
HTTP(S)	HyperText Transfer Protocol (Secure)
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
OWA	Outlook Web Access
OWASP	Open Web Application Security Project
REST	Representational State Transfer
SAML	Security Assertion Markup Language
SIEM	Security Information Management
SNI	Server Name Indication
SQL	Structured Query Language
SSL	Secure Sockets Layer
SYSLOG	System log
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
WAF	Web Application Firewall
XML	eXtensible Markup Language
XSS	Cross-Site Scripting
ИБ	Информационная безопасность
ПО	Программное обеспечение

2. Общие сведения

2.1. Введение

Настоящий документ содержит технические требования на предоставление прав простой (неисключительной) лицензии на использование Системы, предназначенной для защиты WEB-сервисов (Далее — WAF). Данные требования необходимо использовать при подготовке конкурсных предложений для разработки соответствующих разделов документации.

2.2. Сведения о Заказчике

Акционерное общество «Объединенная химическая компания «УРАЛХИМ» (АО «ОХК «УРАЛХИМ» (далее — Общество). Юридический адрес: 123112, Россия, г. Москва, наб. Пресненская, д. 6, стр. 2.

2.3. Плановые сроки поставки: 01.10.2021 г.

3. Назначение и цели использования Системы

WAF должен реализовывать функции защиты WEB-сервисов, автоматизированную проверки HTTP/HTTPS трафика с целью выявления различных атак на уровне приложений.

Основное предназначение WAF — обеспечение безопасной и бесперебойной работы WEB приложений.

Цели использования WAF:

- своевременное обнаружение и блокирование сетевых атак, нацеленных на WEB-сервисы Общества;
- возможность проведения расследований инцидентов ИБ;
- повышение общего уровня защищённости корпоративных WEB-сервисов, опубликованных в сети Интернет.

WAF должен решать следующие задачи:

- защита Общества от убытков, связанных с утечками информации, отнесённой к защищаемой, путём противодействия попыткам взлома WEB-сервисов;
- защита Общества от убытков, связанных с нарушением работы WE-сервисов;
- предотвращение и информирование об инцидентах ИБ, проведение расследований инцидентов, связанных с WEB-сервисами.

4. Постановка задачи

4.1. Исходные данные и общая техническая информация:

- Общее количество опубликованных в сети Интернет WEB-сервисов – до 15.
- Расположение хостинга WEB-сервисов – территориально распределённое.
- Пропускная способность канала передачи данных между защищаемыми WEB-сервисами и сетью Интернет – до 1 Гбит/с.
- Использование среды виртуализации на базе Microsoft Hyper-V.
- Внедрена служба каталогов Active Directory.
- Почтовая WEB служба на основе Microsoft Exchange 2016.

5. Технические требования к ПО

WAF должен обладать следующими параметрами (включая, но не ограничиваясь).

1.	Архитектура и опции развертывания
1.1.	WAF должен поставляться в виде двух виртуальных машин
1.2.	WAF должен иметь возможность работать на гипервизорах Microsoft Hyper-V
1.3.	Количество поддерживаемых WAF WEB-сервисов: не менее 15.
1.4.	Пропускная способность WAF в режиме инспекции трафика: не менее 1 Гбит/с
1.5.	WAF должен поддерживать работу в режиме высокой доступности - кластеризации по схеме Active/Active, Active/Passive, а также иметь возможность работы нескольких устройств с синхронизацией всех объектов и политик WAF, кроме сетевых настроек
1.6.	WAF должен поддерживать работу с VLAN Tagging (802.1q)
2.	Защитные механизмы
2.1.	WAF должен обеспечивать возможность создания политик безопасности с помощью графического интерфейса
2.2.	WAF должен иметь встроенный сканер уязвимостей либо иметь возможность интеграции со сторонними сканерами уязвимостей
2.3.	WAF должен иметь встроенный антивирус для проверки загружаемых на защищаемые WEB порталы файлов, либо иметь возможность интеграции с внешними антивирусными системами, при этом поставка должна включать все необходимые для реализации данной функции лицензии
2.4.	WAF должен иметь функцию построения шаблона нормальной работы защищаемого WEB приложения (формирование позитивной модели), при этом должна быть предусмотрена возможность изменения (коррекции) профиля вручную администратором
2.5.	WAF должен иметь функцию защиты WEB форм аутентификации от подбора паролей (Brute Force)
2.6.	WAF должен иметь функцию подстановки CAPTCHA
2.7.	WAF должен иметь функцию защиты от DoS атак на уровне L7 (HTTP)
2.8.	WAF должен иметь функции проверки IP-репутации посетителей защищаемых WEB порталов (с целью определения и блокирования клиентов, посещающих WEB порталы из TOR сетей и анонимных прокси)
2.9.	WAF должен поддерживать функцию определения ботов и формирование перечня разрешенных ботов
2.10.	WAF должен иметь механизм блокировки IP клиента исходя из определенного геопозиции
2.11.	WAF должен иметь функцию защиты от использования ранее скомпрометированных УЗ

2.12.	WAF должен иметь механизм исключения IP из политик безопасности (добавление IP в белый список)
2.13.	WAF должен иметь функцию включения IP клиента в черный список для ограничения доступа к защищаемым WEB порталам
2.14.	WAF должен иметь функцию ограничения доступа к определенным разделам WEB портала на основании IP-адреса клиента
2.15.	WAF должен иметь функцию проверки протокола HTTP на соответствие стандарту, при этом должна быть возможность задавать различные ограничения по используемым параметрам протокола
2.16.	WAF должен иметь функции подписи и шифрования cookies
2.17.	WAF должен иметь функцию проверки JSON на соответствие схеме
2.18.	WAF должен иметь функцию защиты от атак, специфичных для XML
2.19.	WAF должен иметь предустановленные профили защиты для WEB приложений: Microsoft Exchange (OWA), Microsoft SharePoint
2.20.	WAF должен иметь функцию автоматического обновления антивирусных баз (при наличии встроенного антивирусного модуля), сигнатур атак, репутационной базы IP адресов
2.21.	WAF должен иметь функцию анализа протокола FTP
2.22.	WAF должен обеспечивать защиту программных интерфейсов API
2.23.	WAF должен иметь функцию перезаписи URL
2.24.	WAF должен противодействовать атакам и уязвимостям из актуального перечня OWASP Top 10: - Инъекционные атаки или внедрения - Недостатки аутентификации - Разглашение конфиденциальных данных - Внешние сущности XML - Недостатки контроля доступа - Некорректная настройка параметров безопасности - Межсайтовое выполнение сценариев - Небезопасная десериализация - Использование компонентов с известными уязвимостями - Недостатки журналирования и мониторинга
2.25.	WAF должен иметь функцию защиты от атак типа «человек по середине»
2.26.	WAF должен иметь функцию защиты от атак типа «Межсайтовая подделка запроса»
2.27.	WAF должен поддерживать функцию защиты технологии Cross-Origin Resource Sharing (CORS)
3.	Журналирование и отчеты
3.1.	WAF должен иметь функцию журналирования и построения отчетов с хранением данных на устройстве

3.2.	WAF должен иметь функцию отправки событий в сторонние системы (например, SIEM) по протоколу Syslog
3.3.	WAF должен иметь функцию создания и построения отчетов по различным параметрам (времени, IP клиентов, ID сигнатур, политикам т.п.)
3.4.	WAF должен предоставлять возможность журналировать и экспортировать взаимодействие пользователя с защищаемым ресурсом на уровне содержимого HTTP-сообщений или подробнее
4.	Управление
4.1.	WAF должен иметь функцию создания резервной копии конфигурации и её восстановления из графического интерфейса
4.2.	WAF должен иметь функцию работы с событиями безопасности с фильтрацией по таким параметрам как: время события, IP-адрес клиента, ID события блокировки, реакция на событие и т.п.
4.3.	WAF должен иметь функцию администрирования на основе ролевой модели
4.4.	WAF должен иметь функцию обновления встроенного ПО через графический интерфейс
4.5.	WAF должен иметь возможность графического представления по мониторингу сетевого трафика, состоянию системы и обнаружению угроз в интерактивном режиме (наличие dashboards)
4.6.	WAF должен иметь функцию отправки уведомлений по электронной почте о выявленных угрозах
5.	Аутентификация
5.1.	WAF должен поддерживать интеграцию с AD для аутентификации администраторов устройства
5.2.	WAF должен поддерживать интеграцию с AD для аутентификации пользователей, посещающих защищаемые WEB-ресурсы
5.3.	WAF должен поддерживать возможность редактирования формы, предназначенной для аутентификации пользователей
6.	Иные функции
6.1.	WAF должен иметь функцию балансировки трафика между защищаемыми WEB-ресурсами
6.2.	WAF должен поддерживать работу с протоколом TLS 1.3 как между WAF и клиентом, так и между WAF и защищаемыми WEB-ресурсами
6.3.	WAF должен иметь функцию SSL Offload (терминирование HTTPS соединений для разгрузки WEB приложения)
6.4.	WAF должен иметь возможность работы с протоколом WebSocket
6.5.	WAF должен иметь возможность работы с расширением протокола TLS - SNI
6.6.	WAF должен поддерживать работу с протоколом HTTP 1.2. и HTTP/2.0

6. Требования к технической поддержке

Поставляемое ПО должно обеспечиваться услугами по технической поддержке. Техническая поддержка должна включать в себя:

- консультирование специалистов Общества по поиску и диагностике неисправностей, а также по вопросам установки, настройки и эксплуатации ПО;
- уведомления о выходе обновлений ПО и о бюллетенях информационной безопасности;
- доступ к обновлениям ПО.

Режим оказания технической поддержки – 8x5 (в рабочие дни).

7. Дополнительные требования

Поставка ПО должна включать в себя все необходимые для полнофункциональной работы WAF (в соответствии с указанными техническими требованиями) лицензии и подписки, в том числе (включая, но не ограничиваясь):

- бессрочные основные лицензии на ПО;
- лицензии на обновления антивирусных баз (при наличии встроенного антивирусного модуля), сигнатур атак, репутационной базы IP адресов, а также иных модулей безопасности сроком на 2 года;
- техническую поддержку сроком на 2 года.