

Приложение №__ к Техническому заданию "Изолированная система для безопасного исполнения файлов (Песочница/Sandbox)"

№ требования	Наименование требования/ технические характеристики	Участник		
		Наименование участника		
		Соответствие/ Не соответствие	Ссылка на описание (документ)	Комментарии
1	Решение должно относиться к классу Sandbox	Соответствие/ Не соответствие		
2	Развертывание Системы: On-Premise (программно-аппаратный комплекс).	Соответствие/ Не соответствие		
3	ПО в составе АПК должно поставляться сроком на 3 года (по типу подписки, включая тех.поддержку)	Соответствие/ Не соответствие		
4	Решение поддерживает следующие методы анализа угрозы: • возможность идентификации в режиме реального времени фишинговых сайтов нулевого дня, включая спам и сайты, содержащие вредоносное ПО; • поддержка обнаружения сетевых угроз в режиме сниффера; • выявление деятельности ботнетов и сетевых атак, посещений вредоносных URL-адресов; • обеспечение проверки объектов посредством антивирусного сканирования.	Соответствие/ Не соответствие		
5	Обязательные типы расширения файлов: • исполняемые файлы Windows: .bat, .cab, .cmd, .dll, .exe, .js, .msi, .ps1, .vbs, .vbe, .wsf • microsoft Office: .doc, .docm, .docx, .dot, .dotm, .dotx, .ics, .iqy, .one, .pot, .potm, .potx, .ppt, .pptm, .pptx, .ppam, .pps, .ppsm, .ppsx, .pub, .rtf, .sldm, .sldx, .xlam, .xls, .xlsb, .xslm, .xlsx, .xlt, .xltn, .xltx • файлы документов и электронной почты: .eml, .pdf, .rl • файлы для Android: .apk • файлы Linux: .elf, .sh, ObjectFiles • файлы MacOS: .app, .dmg, Mach-O • веб-файлы: .asp, .hta, .htm, .html, .lnk, .js, .lnk, .url, WEblink • сжимайте файлы: .7z, .ace, .arj, .bz2, .gz, .iso, .jar, .kgb, .lzh, .rar, .swf, .tar, .tgz, .udf, .upx, .xz, .z, .zip	Соответствие/ Не соответствие		
6	Наличие поддержки следующих типов ОС для эмуляции: • Windows (несколько версий, включая актуальные); • Linux (Redhat, OEL, Ubuntu, CentOS); • поддержка 32/64-bit; • возможность кастомизации виртуальных образов.	Соответствие/ Не соответствие		
7	Система должна поддерживать интеграции с: • файрволами (NGFW); • шлюзом электронной почты (Email Gateway); • Web Gateway; • антивирусом (Endpoint Protection) • системой EDR / XDR • системой SIEM (в перспективе).	Соответствие/ Не соответствие		
8	Обмен данными должен поддерживать: • REST API; • стандарт STIX/; • Syslog.	Соответствие/ Не соответствие		
9	Интеграция Системы с endpoint решениями (антивирусом) • возможность автоматической передачи подозрительных файлов с endpoint-агентов антивируса. • возможность автоматического блокирования признаков компрометации на конечных точках. • поддержка автоматической изоляции хоста (при наличии интеграции).	Соответствие/ Не соответствие		
10	Производительность Системы: • производительность по числу локальных виртуальных машин на устройстве: не менее 14; • возможность расширения в облако до 80 виртуальных машин; • эффективная пропускная способность песочницы: не менее 10 000 файлов в час; • производительность проверки объектов посредством предварительной фильтрации (статический анализ): не менее 20 000 файлов в час; • производительность проверки объектов посредством эмуляции в виртуальной среде (динамический анализ): не менее 500 файлов в час; • производительность при интеграции с решением для защиты почты: 100 000 писем в час; • производительность проверки объектов посредством MTA Adapter 25 000 писем в час; • производительность в режиме сниффера: не менее 500 Мбит/с.	Соответствие/ Не соответствие		

11	Управление и администрирование Системы • WEB-интерфейс управления; • разграничение ролей (ролевая модель); • журналирование действий администраторов; • интеграция с AD/LDAP; • поддержка двухфакторной аутентификации для администраторов Системы.	Соответствие/ Не соответствие		
12	Решение предоставляет следующие отчеты: • подробный поведенческий отчет: - файловая активность, - изменения реестра, - сетевые соединения, - процессы, • визуализацию графического отображения этапов кибератаки от начала до цели, • формирование признаков компрометации (hash, IP, URL, domain), • экспорт отчетов в PDF.	Соответствие/ Не соответствие		
13	Лицензирование Системы • лицензия должна покрывать: - количество анализируемых объектов, - количество интегрируемых устройств, - обновления сигнатур и движков. • количество VM – не менее 4 шт. (с возможностью дальнейшего расширения, путем активации дополнительной лицензии); • срок подписки на ПО – 3 года; • срок технической поддержки – не менее 3 лет.	Соответствие/ Не соответствие		
14	Дополнительные требования • поддержка собственных исследовательских центров от производителя; • интеграция с платформами класса XDR	Соответствие/ Не соответствие		
15	В проект включены инсталляционные работы	Соответствие/ Не соответствие		
16	В проект включено проектирование	Соответствие/ Не соответствие		
17	В проект включено обучение 2 специалистов Заказчика	Соответствие/ Не соответствие		
18	В проект включена сертификация ПО/АПК в ЦКБ	Соответствие/ Не соответствие		
19	Язык интерфейса - русский/английский	Соответствие/ Не соответствие		
20	Наличие у Исполнителя МАФ	Соответствие/ Не соответствие		

* все пункты являются обязательными и блокирующими.

Дата:

дд/мм/гггг

Составил:

Начальник отдела ИБ

Должность

Р.А.Б.

Абдульваат Р.А.

ФИО

Согласовано:

Директор Департамента ДИБиР

Должность

Олматов

Олматов Б.А.

ФИО

