ТЕХНИЧЕСКОЕ ЗАДАНИЕ К ТЕНДЕРУ № _____ «_____»

Закупка «Средство мониторинга и анализа поверхности атаки ASM (Attack Surface Management)»

1. Общие сведения

1.1. Полное наименование системы и ее условное обозначение

Полное наименование системы – Средство мониторинга и анализа поверхности атаки.

Условное обозначение системы – «Система».

1.2. Количество активов – 500 шт.

2. Цели создания Системы

2.1. Обнаружение всех учтенных и не учтенных активов компании доступных извне.

2.2. Выявления имеющихся или вероятных угроз, векторов атак и уязвимостей.

2.3. Обнаружение скомпрометированных данных в сети Интернет в том числе в «Darkweb».

3. Требования к системе

3.1. Требования к обнаружению и отображению инфраструктуры

3.1.1. Система должна иметь распределенную инфраструктуру сканирования и обеспечивать автоматическое обнаружение активов в режиме реального времени.

3.1.2. Система должна давать возможность исследования собственной инфраструктуры Заказчика извне, для выявления имеющихся или вероятных угроз путем построения графа связности исследуемого ресурса или узла с другими

3.1.3. Система должна иметь возможность фильтрации информации по времени в построенном графе и создания персонализированного цифрового отпечатка активов.

3.1.4. Система должна иметь возможность настраивать граф обнаруженной инфраструктуры.

3.1.5. Система должна позволять вручную настраивать белые списки доменов и IP-адресов.

127018, Россия, г. Москва,
Сущевский вал, дом 5, строение 3
Тел./факс: +7 495 7487954/94
www.migcredit.ru

3.1.6. Все данные должны предоставляться через единый интерфейс системы и отображаться в легко распознаваемом, фильтруемом и управляемом формате.

3.2. Технические требования к сбору информации

3.2.1. Система должна обеспечивать пассивное сканирование IPv4 пространства в режиме реального времени по всем активам инфраструктуры Заказчика.

3.2.2. Система должна выявлять IPv6 адреса, связанные с активами Заказчика.

3.2.3. Система должна обеспечивать обнаружение, анализ и построение связей между SSL/TLS инфраструктурой Заказчика.

3.2.3. Система должна обеспечивать многоуровневый подход к построению связей между доменами, IP-адресами и активами инфраструктуры на основе исторических данных WHOIS, DNS, и запущенных сервисов.

3.2.4. Система должна обеспечивать сбор данных о развернутом оборудовании и программном обеспечении Заказчика и сопоставлять с данными об уязвимостях.

3.2.5. Система должна предоставлять отображение полной инфраструктуры Заказчика с технической оценкой активов и уровня защищенности инфраструктуры в режиме реального времени.

3.3. Требования к выявлению технических проблем инфраструктуры

3.3.1. Система должна обеспечивать обнаружение и анализ уязвимостей конфигураций операционных систем, сервисов, приложений, программного и аппаратного обеспечения, в том числе программных библиотек в активах Заказчика.

3.3.2. Система должна обеспечивать поиск неточностей в конфигурации активов Заказчика таких как: общедоступные Базы данных, файловые хранилища или списки директорий сервисов.

3.3.3. Система должна обеспечивать обнаружение неточностей в конфигурации DNSSEC, SPF и DMARC в активах Заказчика.

3.3.4. Система должна обеспечивать уведомление о предстоящих изменениях состояния TLS инфраструктуры активов (окончание действия SSL-сертификатов).

3.3.5. Система должна обеспечивать обнаружение и анализ самоподписанных сертификатов, актуальных версий SSL/TLS и алгоритмов шифрования в активах Заказчика.

3.3.6. Система должна сканировать подсети Заказчика для определения открытых портов, служб и используемых веб-приложений. Сканирование не должно предполагать использование уязвимостей или загрузки какого-либо контента. Сканирование должно проводиться в “скрытом режиме”, подразумевающем отсутствие обнаружения факта сканирования со стороны СЗИ Заказчика. Сканирование должно выявлять открытые порты

служб удаленного администрирования (RDP, SSH, VPN и т.п.), порты баз данных, небезопасные заголовки служб, открытые прокси-серверы, запущенные узлы Tor, а также то, был ли актив целью DdoS-атаки.

3.3.7. Система должна выявлять факты похищения аутентификационных данных Заказчика связанных с обнаруженными активами с помощью ВПО или фишинга.

3.3.8. Система должна выявлять наличие аутентификационных данных Заказчика в опубликованных в общем доступе или на теневых площадках взломанных базах данных сторонних сервисов имеющих возможное отношение к обнаруженным активам Заказчика

3.3.9. Система должна обнаруживать факты взаимодействия ВПО, проанализированных в общедоступных решениях типа “песочница”, а также проанализированных в платформах детонации Исполнителя с активами Заказчика.

3.3.10. Система должна определять наличие работающего ВПО в выявленных активах Заказчика.

3.3.11. Система должна выявлять факты упоминания активов Заказчика на теневых площадках сети Интернет (Darkweb).

3.4. Требования к предоставлению данных о вредоносном программном обеспечении (ВПО).

3.4.1. Система должна сопоставлять информацию об образцах вредоносного ПО с инфраструктурой Заказчика и производить оповещение в случае, если вредоносная программа имеет файл настроек, где затрагиваются его IP-адреса, домены и другие активы.

3.4.2. Система должна предоставлять актуальную информацию о событиях фишинга, затрагивающих инфраструктуру Заказчика.

3.4.3. Система должна определять факт использования вредоносного кода типа JS-сниффера на доменах и страницах веб-сайтов Заказчика.

3.4.4. Система должна предоставлять информацию о принадлежности активов Заказчика к бот-сетям.

3.5. Требования к предоставлению данных из закрытых источников

3.5.1. Система должна производить поиск информации об активах Заказчика по различным скрытым информационным ресурсам и форумам (Darkweb).

3.5.2 Система должна определять:

- Упоминания IP или доменной информации;
- Адрес упоминания активов

- Тело сообщения об упоминании активов;

3.5.3. Система должна предоставлять следующие сведения, публикуемые на скрытых форумах и ресурсах:

- Дата и время выявления обнаружения сообщения;
- Наименование темы ветки сообщений на форуме, наименование форума, текст сообщения на форуме;
- Информация по профилю, опубликовавшему сообщение, никнейм;

3.5.4. Система должна предоставлять актуальную информацию о различных данных Заказчика, скомпрометированных при помощи форм грабберов, похитителей паролей, компьютерных троянов, RAT, фишинга, JS-Sniffers.

3.6. Требования по предоставлению рекомендаций по исправлению обнаруженных проблем в активах Заказчика

3.6.1. Система должна предоставлять информацию о возможности реализации атак через выявленную проблему в активе Заказчика

3.6.2. Система должна предоставлять описание необходимых исправлений выявленных проблем в активах Заказчика.

3.7. Требования к интерфейсу

3.7.1. Система должна предоставлять возможность отображения инфраструктуры компании Заказчика

3.7.2. Система должна предоставлять возможность добавления и удаления активов для расширения или сужения параметров сканирования.

3.7.3. Система должна предоставлять возможность добавления, удаления, фиксирования проблем безопасности.

4. Дополнительные преимущества

4.1. Дополнительным преимуществом будет являться, если Система позволяет обеспечить:

- возможность добавления нескольких учетных записей для работы с системой
- отображать данные о глобальной инфраструктуре на географической карте.
- возможность ручного экспорта данных, предоставленных в решении.