ПРИЛОЖЕНИЕ 2

Технические требования

Требования, предъявляемые к платформе реагирования на киберинциденты.

Платформа должна иметь сертификат соответствия требованиям ТР 2013/027/BY. Платформа должна иметь возможность развертывания на следующих операционных системах:

– CentOS;

– RedHat Enterprise Linux;

– Oracle Linux;

– Ubuntu;

– Debian;

– Astra Linux.

Доступ к функционалу платформы должен осуществляться через веб-интерфейс на русском и английском языках с возможностями изменения темы оформления (цветовой схемы).

Разграничение доступа в платформе должно основываться на ролевой модели. Роли должны быть как преднастроенные, так и кастомизируемые.

Платформа должна иметь функционал резервирования в режимах Active-Passive или Active-Active.

В платформе должно быть реализовано журналирование изменений объектов, исходящих как от пользователей, так и от платформы.

В платформе должна быть реализована поддержка работы в режиме мультиарендности.

В платформе должна быть реализована возможность экспорта следующих данных: сведения об активах, данных об уязвимостях, данных об инцидентах, сведений по задачам.

Платформа должна осуществлять логирование событий (возникающих в процессе работы) и хранить эти записи в журнале аудита.

Платформа должна иметь возможность взаимодействия не менее чем с 4 внешними информационными системами.

Платформа должна иметь возможность интеграции с системами класса SIEM, TIP.

Платформа должна иметь возможность настройки сценариев реагирования для каждого этапа цепочки действий при осуществлении кибератаки.

Функционалом платформы должно быть предусмотрено:

- наличие предустановленных скриптов, реализующих технические действия. визуализация сценария реагирования
- поддержка динамических сценариев реагирования с логическими операторами
- возможность запуска нескольких сценариев для одного инцидента
- возможность запуска сценариев из сценариев
- возможность автоматического объединения инцидентов в группы
- поддержка ретроспективного анализа

В функционале платформы должно быть реализовано:

- наличие готовых отчетов и дашборды;
- API для выгрузки в стороннюю систему;
- 1 отчеты по конкретному объекту;
- конструктор отчетов и графиков;
- экспорт информации по активам, инцидентам и другим элементам системы.

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

Срок действия лицензий с предоставлением технической поддержки – не менее 24 (двадцати четырёх) месяцев.

Требования к функциям модуля управления инцидентами

Модуль управления инцидентами должен обеспечивать реализацию следующих функций:

- сбор, регистрация и обогащение информации по инцидентам ИБ в единой системе;
- ведение карточек инцидентов, содержащих сведения по инцидентам, прикрепленные файлы и дополнительную информацию;
- возможность создавать инцидент как автоматически из внешних источников, так и вручную;
- классификация инцидентов по категориям и типам с возможностью изменения категорий и типов любых инцидентов;
- возможность назначения инциденту уровня критичности; возможность прикрепления к инциденту файлов;

- возможность связывания инцидента с другими объектами системы;
- возможность создания настраиваемых сценариев для реагирования на инциденты; механизм выявления признаков цепочки действий при осуществлении кибератаки (kill-chain.