ПРИЛОЖЕНИЕ 1

Технические требования

Система должна включать в себя следующие подсистемы и компоненты:

подсистема сбора и обработки событий информационной безопасности (SIEM);

подсистема сбора и анализа индикаторов компрометации и киберугроз (Threat Intelligence Platform);

компонент динамического анализа вредоносных файлов (Sandbox).

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

Срок действия лицензий с предоставлением технической поддержки – 24 (двадцать четыре) месяца.

Требования, предъявляемые к подсистеме сбора и обработки событий информационной безопасности

Подсистема должна иметь сертификат соответствия требованиям ТР 2013/027/BY, СТБ 34.101.74-2017 (пункт 7.3.).

Требование к оборудованию

Компоненты подсистемы должны поддерживать установку как на физических, так и на виртуальных машинах.

Основные компоненты (модули, отвечающие за сбор событий, корреляцию, хранение событий) должны поддерживать установку на операционных системах семейства Linux:

Astra Linux Special Edition 1.7 и выше;

Oracle Linux версии 8.4 и выше;

Debian версий 10.3 - 10.13.

Подсистема должна обеспечивать высокую производительность и поддерживать прием и обработку потока в размере от 10 000 событий в секунду (EPS).

Требования к архитектуре подсистемы

Подсистема должна поддерживать горизонтальное масштабирование ключевых ее компонентов: коллектора, коррелятора и хранилища событий.

Компоненты подсистемы должны поддерживать установку в распределённых и изолированных сетях без необходимости доступа к сети Интернет.

Подсистема должна обеспечивать централизованное управление посредством веб-консоли без установки дополнительного ПО на АРМ администратора.

Подсистема должна поддерживать разделение ресурсов и сервисов на логические сущности («тенанты»), позволяя в рамках единой инсталляции предоставлять возможность разграничения прав доступа пользователей подсистемы к событиям, инцидентам, правилам корреляции, нормализации, а также определенным настройкам подсистемы.

Подсистема должна обеспечивать возможность централизованного обновления конфигурации или перезапуска компонентов, в том числе принудительного. Подсистема должна поддерживать возможность добавления сторонних компонентов в процесс обработки событий. Подсистема должна обеспечивать режим работы отказоустойчивого кластера для всех основных компонентов с «горячим» переключением (High Availability).

Подсистема должна поддерживать работу с несколькими независимыми кластерами хранилища событий для возможности организации гибких схем географически распределенных подсистем.

Архитектура решения должна обеспечивать возможность развертывания в географически распределенной инфраструктуре.

Подсистема должна поддерживать поиск по событиям в удалённых офисах из центрального узла подсистемы.

Требования к сбору, анализу и хранению событий

Подсистема должна обеспечивать как активный, так и пассивный сбор событий с источников данных.

Подсистема должна осуществлять поиск (инвентаризацию) активов или поддерживать импорт активов из сторонних источников.

Подсистема должна поддерживать возможность сохранения исходного события.

Подсистема должна поддерживать возможность добавления пользовательских типов источников событий и соответствующей настройки правил разбора и нормализации.

Подсистема должна обеспечивать создание пользовательских нормализаторов на основе поддерживаемых форматов и протоколов сбора данных.

Подсистема должна обеспечивать возможность мониторинга поступления событий от источников с отслеживанием количества событий в указанный промежуток времени и автоматическим оповещением на электронную почту в случае отклонения от заданных параметров мониторинга для каждого из источников в частности.

Подсистема должна поддерживать импорт/экспорт контента и ресурсов: правил корреляции, парсеров, коннекторов и т.д.

Требования к функциям обогащения событий

Подсистема должна поддерживать обогащение событий с помощью Threat Intelligence (сведения об индикаторах компрометации и соответствующем контексте: хэши файлов, URL-адреса, внешние IP-адреса), DNS, служба каталогов Active Directory, геоданные.

Требования к функциям корреляции событий, работы с инцидентами

Подсистема должна обеспечивать потоковую корреляция событий для выявления инцидентов и событий ИБ на основе правил корреляции в режиме близком к режиму реального времени.

Подсистема должна поставляться с набором предустановленных правил корреляции, созданных на основе исследований актуальных угроз и способов атак, разработанных на базе матрицы MITRE ATTACK.

Подсистема должна обеспечивать возможность многоуровневой корреляции с передачей результатов работы одного правила корреляции на вход другим правилам корреляции.

Подсистема должна обеспечивать возможность использования в правилах обогащения и корреляции табличных списков.

Подсистема должна поддерживать возможность тестирования правил корреляции на исторических данных.

Подсистема должна иметь возможность приоритизации выявленных угроз ИБ как с учётом уровня критичности правила корреляции, так и с учетом критичности и количества затронутых информационных активов.

Подсистема должна поддерживать автоматическое объединение скоррелированных событий, являющихся результатом работы одного и того же правила корреляции, в карточку инцидента.

Подсистема должна обеспечивать управление карточками инцидентов, включая: ручное добавление или удаление карточки инцидента, или изменение данных карточки; возможность вручную связать инцидент с событиями и активами; возможность создания задач для пользователей подсистемы по расследованию, сбору доказательств и восстановлению работоспособности информационной систем; возможность сохранения проведенных мероприятий и их комментирование; хранение истории изменений карточки инцидента и выполнения поставленных задач.

Подсистема должна обеспечивать поддержку механизмов фильтрации и сортировки инцидентов. Подсистема должна обеспечивать автоматическую ассоциацию активов с событиями и/или инцидентами.

Требования к управлению сведениями об активах

Подсистема должна поддерживать создание пользовательских групп (категорий) активов.

Подсистема должна обеспечивать возможность ручной и автоматической категоризации активов на основе одного или комбинации признаков.

При задании условий автоматической категоризации активов подсистема должна обеспечивать возможность тестирования заданных условий по имеющейся базе информационных активов.

Подсистема должна поддерживать возможности поиска по активам, сохраненных во встроенной базе данных.

Требования к функциям работы с инцидентами

Подсистема должна обеспечить автоматическое формирование карточек инцидентов по результатам срабатывания правил корреляции.

В подсистеме должна быть реализована возможность ручной привязки дополнительной информации к инциденту – по пользователям, активам, событиям корреляции с возможности классификации инцидента.

Требования к визуализации и отчётности

Подсистема должна предоставлять инструменты визуализации и отчётности.

Подсистема должна поставляться с предустановленным набором графических панелей и отчётов.

Подсистема должна поддерживать возможность создания пользовательских дашбордов и шаблонов отчетов.

Подсистема должна обеспечивать возможность формирования отчетов из состава имеющихся шаблонов.

Подсистема должна обеспечивать построение отчетов по инцидентам.

Подсистема должна обеспечивать возможность отправки отчетов по почте.

Подсистема должна поддерживать рассылку отчетов по настраиваемому расписанию.

Требования к мониторингу производительности

Подсистема должна обеспечивать сбор и хранение метрик производительности всех компонентов подсистемы.

Метрики производительности должны отображаться в графическом интерфейсе подсистемы.

Подсистема должна поддерживать передачу метрик производительности во внешние системы мониторинга.

Требования к безопасности

Подсистема должна обеспечивать разграничение прав доступа к функционалу на основе ролевой модели.

Подсистема должна регистрировать события доступа и значимых изменений конфигурации.

Подсистема должна поддерживать аутентификацию и авторизацию с использованием следующих механизмов:

локальная база учётных данным (по логину-паролю) пользователей;

Active Directory.

Подсистема должна иметь встроенные механизмы противодействия попыткам подбора пароля.

Требования, предъявляемые к подсистеме сбора и анализа индикаторов компрометации и киберугроз

Подсистема должна обеспечивать доступ пользователей через графический веб-интерфейс (далее также — пользовательский интерфейс).

Должна обеспечиваться реализация ролевой модели управления доступом пользователей к функциям подсистемы.

Должна обеспечиваться возможность создания локальных учетных записей пользователей в интерфейсе подсистемы.

Должна обеспечиваться возможность просмотра через пользовательский интерфейс индикаторов компрометации.

Должна обеспечиваться возможность задания уровня доверия к источнику информации об угрозах через пользовательский интерфейс.

Подсистема должна поддерживать возможность получения индикаторов компрометации из различных источников.

Подсистема должна обеспечивать возможность добавлять и просматривать источники информации об угрозах через пользовательский интерфейс.

Должен предоставляться API для загрузки в подсистему индикаторов компрометации.

Подсистема должна обеспечивать возможность автоматического обогащения поступающих в нее индикаторов компрометации.

Подсистема должна обеспечивать возможность обогащения информации в составе индикаторов компрометации пользователями подсистемы.

Подсистема должна обеспечивать возможность использования правил обогащения, созданных пользователями.

Должно обеспечиваться хранение и экспорт настроек подсистемы.

Подсистема должна обеспечивать возможность создания и выгрузки наборов индикаторов компрометации, предназначенных для экспорта в смежные и сторонние системы (далее также – фидов).

Подсистема должна обеспечивать возможность настройки создания фидов:

– периодичность автоматического создания фидов;

– критерии попадания индикаторов компрометации в фид;

– глубина выборки индикаторов компрометации для попадания в фид.

Подсистема должна обеспечивать возможность выгрузки файлов фидов в форматах STIX 2.0 и JSON.

Подсистема должна обеспечивать возможность выгрузки файлов фидов через API.

В комплекте поставки подсистемы должны быть фиды, содержащие информацию о вредоносных хеш-данных, данные об IP-репутации, данные фишинговых URLадресов, в т.ч релевантных белорусскому сегменту глобальной сети Интернет (коммерческие версии).

Требования, предъявляемые к компоненту динамического анализа вредоносных файлов

Компонент должен иметь сертификат соответствия требованиям ТР 2013/027/BY.

Компонент должен поддерживать следующие операционные системы для анализа файлов в изолированной среде:

CentOS;

Microsoft Windows 7 x64/x86;

Microsoft Windows 10 x64;

Компонент должен поддерживать кастомизацию образов операционных систем для разворачивания в изолированной среде.

Компонент должен автоматически масштабировать количество виртуальных машин для анализа файлов в зависимости от выделенных ресурсов на этапе развертывания.

Компонент должен анализировать на основе заданных правил поведения следующие действия: создание файлов; запуск процессов; выполнение интернет-запросов; изменения в системном реестре.

Компонент должен иметь возможность ручной загрузки объектов на проверку через веб-интерфейс.

Компонент должен выстраивать граф поведения образцов файлов в изолированной среде после проведения поведенческого анализа и отображать его в графическом интерфейсе.

Компонент должен обеспечивать запуск и анализ поведения в изолированной среде файлов следующих форматов:

PE (исполняемые);

скрипты (vbs, bat, ps);

Microsoft Office (rtf, doc/docx, xls/xlsx, ppt/pptx);

Adobe Acrobat (pdf);

архивы (rar, 7z, zip).

Компонент должен уметь извлекать файлы из архивов, в том числе, защищенных паролем (при его наличии).

Компонент должен иметь встроенный механизм AntiEvasion для защиты от техник обхода песочниц.

Компонент должен иметь возможность доступа к сети Интернет для проведения более глубокого анализа поведения анализируемых объектов.

Компонент должен обеспечивать возможность выгрузки анализируемого контекста:

копия сетевого трафика;

созданные артефакты/сэмплы файлов;

лог активности объекта в изолированной среде.