Professional Services

Managed SIEM

Сервис по удаленному сопровождению SIEM и управлению инцидентами информационной безопасности

СОДЕРЖАНИЕ

1. Краткое описание услуги

Сервис управления системой анализа и корреляции событий информационной безопасности (далее – **SIEM**) представляет собой комплексный набор услуг профессионального сопровождения SIEM на уровне первой, второй и третьей линии управления инцидентами, контентного наполнения SIEM правилами выявления инцидентов (**корреляционные правила**) и реакциями на них (**playbooks**).

Полный набор услуг сгруппирован на трех уровнях по следующему принципу:

[1] **Услуги уровня Lite** – необходимый и достаточной набор для «быстрого старта» и запуска SIEM в эксплуатацию.
[2] **Услуги уровня Base** – набор услуг, позволяющий обеспечить полноценное сопровождение SIEM и расширить сферу контроля инцидентов и управления активами.
[3] **Услуги уровня Advanced** – расширяют возможности SIEM, предоставляют инструменты для более глубокой аналитики, в том числе процессов функционирования самого SIEM-решения.

2. Регламент оказания услуги

Услуга Managed SIEM оказывается в режиме 8x5 и 24x7. Для более подробного описания см. раздел «Типовой регламент ».

2.1. Условия оказания услуги Managed SIEM в режиме 8x5

- **Регистрация запроса на оказание услуги:** в течение 2 (двух) часов в рабочие дни с 9:00 до 17:30 (МСК).
- **Время реакции:** в соответствии с SLA на оказание услуг. Описание типового SLA приведено в разделе 7.3.

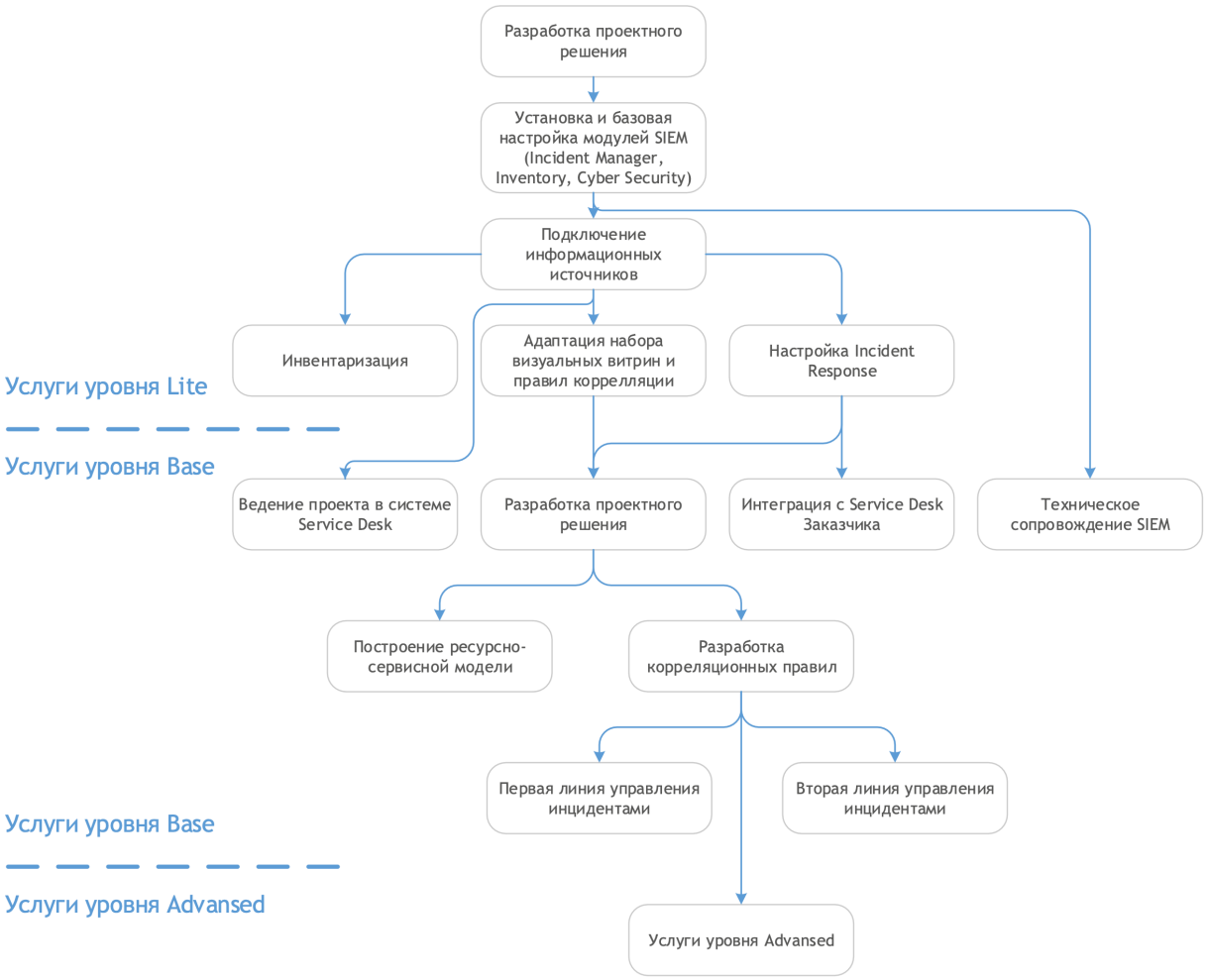
2.2. Условия оказания услуги Managed SIEM в режиме 24x7

- **Регистрация запроса на оказание услуги:** в течение 2 (двух) часов.
- **Время реакции:** в соответствии с SLA на оказание услуг. Описание типового SLA приведено в разделе 7.3.

3. Уровни оказания услуги

На схеме ниже показаны три уровня оказания услуги Managed SIEM: от минимального к расширенному.

> В рамках соглашения о присоединении к сервису управления SIEM **индивидуально согласовывается необходимый и достаточный для Клиента** состав услуг.



4. Услуги уровня Lite

4.1. Организационно-методологические сервисы

4.1.1. Разработка проектного решения

Прорабатываются и согласуются технические и организационные решения для дальнейшего внедрения SIEM. Технические и организационные решения оформляются в виде комплекта документации, включающей в себя:

— **Требования к вычислительным мощностям и правилам их масштабирования:**
- перечень источников с оценкой потока данных от каждого источника и требуемыми сроками хранения информации в SIEM;
- перечень серверов с требованиями по аппаратному обеспечению и операционным системам;
- порядок масштабирования вычислительных мощностей при увеличении потока данных или изменении состава источников;

— **Архитектура решения, включая схему комплекса технических средств:**
- состав модулей SIEM и распределение их по серверам;
- карта потока данных между компонентами SIEM;
- описание схемы интеграции с источниками данных;
- описание схемы хранения данных;
- базовые настройки модулей SIEM;
- решение по аутентификации и авторизации пользователей;
- схема комплекса технических средств SIEM с указанием их размещения на объектах Заказчика.

— **Ролевая модель доступа к данным и управления в системе SIEM:**
- перечень и описание ролей SIEM;
- матрица доступа;
- порядок внесения изменений в состав ролей и прав доступа;

— **Политика реагирования на инциденты ИБ:**
- SLA по реагированию на инциденты для каждой категории инцидентов;
- перечень участников процесса реагирования;
- список ресурсов и инструментов, необходимых для реагирования на инцидент ИБ;
- форма карточки инцидента;
- описание типового процесс реагирования на инцидент ИБ с указанием сценариев действий для каждого участника процесса реагирования.

— **Положение о классификации инцидентов ИБ:**
- категории инцидентов ИБ;
- уровни критичности инцидентов ИБ;
- порядок определения для инцидента ИБ уровня критичности и категории;
- перечень классифицированных инцидентов ИБ;
- описание формализованных правил для автоматизированной идентификации инцидентов ИБ;
- перечень условий для неавтоматизированной идентификации инцидентов ИБ.

— **Эскалация инцидентов и проблем:**
- матрица эскалации с указанием условий, адресатов эскалации, временных SLA и канала оповещения (исходя их уровня критичности инцидента);

Исходные данные для расчета стоимости оказания услуги:

— количество источников (с распределением по типам и оценкой объема поступающих данных от каждого);

— количество инцидентов;

— наличие требований к отказоустойчивости SIEM;

— количество площадок развертывания компонент SIEM.

4.2. Технические сервисы

4.2.1. Установка и базовая настройка модулей SIEM

Установка и настройка модулей Smart Monitor:

— Core:
- инсталляция компонент модуля на предоставленном серверном оборудовании;
- настройка выбранного хранилища данных;
- установка лицензии;
- создание необходимых ролей и учетных записей пользователей;
- настройка менеджера управления агентами;
- настройка Job Scheduler;
- настройка Dashboard Framework;
- настройка Smart Monitor Engine;
- настройка компонента ресурсно-сервисная модель.

— Incident Manager:
- инсталляция компонент модуля на предоставленном серверном оборудовании;
- настройка прав доступа пользователей к модулю;
- заведение необходимых уровней критичности инцидентов;

— Inventory:
- инсталляция компонент модуля на предоставленном серверном оборудовании;
- подключение инвентарных источников данных;
- формирование карточек активов;
- настройка правил агрегации активов из разных источников.

— Cyber Security:
- инсталляция компонент модуля на предоставленном серверном оборудовании;
- установка включенных в модуль правил и дашбордов

Исходные данные для расчета стоимости оказания услуги:

— наличие требований к отказоустойчивости SIEM;

— количество площадок развертывания компонент SIEM;

— поток данных от источников в ГБ/день;

— срок хранения информации от источников данных;

— имеются ли предпочтения по использованию хранилищ (Elasticsearch, Hadoop, ClickHouse).

4.2.2. Подключение информационных источников

Подключение информационных источников по согласованному на этапе формирования проектного решения списку:

— для агентской схемы подключения источников - подготовка и предоставление Заказчику агентов для установки их на источники данных. Консультационное сопровождение процесса установки агентов;

— для безагентской схемы подключения источников - настройка необходимых протоколов и сервисов для подключения к источникам, получение служебных учетных записей и проверка прав доступа к источникам;

— тестирование и отладка процесса получения данных;

— настройка справочников и структуры хранилища данных для каждого источника;

— нормализация поступающих от источников данных.

Исходные данные для расчета стоимости оказания услуги:

— количество источников (с распределением по типам и оценкой объема поступающих данных от каждого).

4.2.3. Настройка Incident Response

Настройка оповещений и реакций на выявленные инциденты информационной безопасности:

— настройка согласованного процесса реагирования на инциденты в Incident Manager;

— адаптация стандартной карточки инцидента к согласованной в рамках проектного решения;

- реализация правил автоматизированной идентификации инцидентов в соответствии с проектным решением;
- настройка оповещений об инцидентах в соответствии с проектным решением;
- настройка процедур эскалации в соответствии с проектным решением;
- обновление схемы реагирования на инциденты и правил идентификации (при необходимости).

Исходные данные для расчета стоимости оказания услуги:

- количество корреляционных правил.

4.2.4. Адаптация/разработка набора дашбордов

Адаптация/разработка набора визуальных витрин (функциональных дашбордов), покрывающих базовый набор информационных источников, включая:
- согласование оформления дашбордов;
- определение состава информационных панелей и отображаемых на них данных (диаграммы, графики, таблицы и проч.);
- определение источников данных для дашбордов, правил расчета значений, выводимых на дашборды и условий изменения цветовой идентификации информационных панелей.

Исходные данные для расчета стоимости оказания услуги:

- количество визуальных витрин (функциональных дашбордов);

4.2.5. Адаптация набора корреляционных правил

Адаптация набора корреляционных правил, покрывающих базовый набор информационных источников, включая:
- определение состава корреляционных правил;
- определение критичности инцидентов, выявляемых корреляционными правилами;
- настройка исключений;
- настройка уведомлений.

Исходные данные для расчета стоимости оказания услуги:

- количество корреляционных правил.

4.2.6. Инвентаризация активов

Категоризация информационных активов клиента с точки зрения кибербезопасности:
- формирование списка информационных активов;
- согласование схемы категоризации информационных активов с точки зрения кибербезопасности и проведение категоризации;
- определение перечня данных, получаемых от каждого актива;
- определение способа подключения к активу и получения от него данных;
- определение/адаптация правил агрегации данных из различных активов;
- актуализация типовой карточки активов;
- проработка правил разрешения конфликтов при получении различных значений одних и тех же полей от разных источников;

Исходные данные для расчета стоимости оказания услуги:

- количество типов активов.

5. Услуги уровня Base

5.1. Организационно-методологические сервисы

5.1.1. Разработка проектного решения

- Отчетность по итогам деятельности SIEM.
- Управление источниками событий для системы сбора и корреляции логов.
- Регламент подключения новых источников.
- Контроль актуальности списков источников сбора информации.
- Инструкция по развертыванию и настройке агентов сбора информации на конечных системах.

5.2. Технические сервисы

5.2.1. Разработка корреляционных правил

Услуга включает в себя мероприятия по разработке необходимых корреляционных правил:
- расширение комплекта корреляционных правил из модуля Cyber Security дополнительными правилами для покрытия нетиповых сценариев;
- разработка комплекта правил по согласованному ТЗ при отсутствии в спецификации SIEM модуля Cyber Security.

Исходные данные для расчета стоимости оказания услуги:

- требуемое количество корреляционных правил.

5.2.2. Построение ресурсно-сервисной модели

Построение ресурсно-сервисной модели (РСМ) объектов мониторинга для оперативной диагностики здоровья компонентов инфраструктуры и выявлением причинно-следственных связей инцидентов информационной безопасности:
- определение состава метрик для РСМ, правил их расчета и условий отнесения к одному из уровней критичностей (тревога, предупреждение, норма);
- определение состава индикаторов для всех уровней РСМ, зависимостей индикаторов более высоких уровней от индикаторов низких уровней и от метрик;
- реализация РСМ в виде дерева в SIEM;
- реализация возможности перехода по выбранной метрике к соответствующему функциональному дашборду.

Исходные данные для расчета стоимости оказания услуги:

- количество метрик (контролируемых показателей) для нижнего уровня РСМ.

5.2.3. Техническое сопровождение SIEM

Регламентное обслуживание SIEM в части администрирования её компонент, обновления общесистемного и прикладного программного обеспечения, составляющего основу SIEM-платформы (режим оказания услуги – 8x5).
В рамках подготовки к оказанию услуги выполняется:
- определение ответственных со стороны Заказчика и Исполнителя;
- определение канал взаимодействия для согласования непосредственных действий по сопровождению;
- уточнение конкретного перечня мероприятий по сопровождению и уровня их критичности (с указанием SLA);
- создание необходимых учетных записей и настройка прав доступа для специалистов Исполнителя;
- согласование матрицы эскалации;
- согласование порядка выполнения мероприятий по сопровождению, не входящих в оговоренный набор услуг.

Исходные данные для расчета стоимости оказания услуги:

- срок оказания услуги (мес.).

5.2.4. Ведение проекта в системе Service Desk

Заведение всех задач проекта в систему Service Desk на стороне исполнителя, отслеживание статуса открытых заявок, просмотр сводной информации о выполнении задач и ходе ведения проекта (режим оказания услуги - 8x5).
В рамках подготовки к оказанию услуги выполняется:
- определение формата заявок;
- определение ответственных со стороны Заказчика и Исполнителя;
- определение канал взаимодействия для согласования непосредственных действий по выполнению заявок;
- согласование SLA выполнения заявок;
- определение категорий заявок и уровней их критичности;
- согласование матрицы эскалации;
- создание необходимых учетных записей и настройка прав доступа для специалистов Исполнителя;
- согласование порядка выполнения заявок, не входящих в оговоренный набор услуг.

Исходные данные для расчета стоимости оказания услуги:

- срок оказания услуги (мес.).

5.2.5. Интеграция с Service Desk Заказчика

Настройка интеграции с имеющимися у клиента автоматизированными средствами управления заявками на управление ИТ/ИБ инфраструктурой (Help Desk, Service Desk).
В рамках подготовки к оказанию услуги выполняется:
- согласование и реализация схемы интеграции SIEM со средствами управления заявками;
- определение формата заявок;
- согласование SLA на заведение заявок;
- определение категорий заявок и уровней их критичности;
- определение ответственных со стороны Заказчика и Исполнителя;
- согласование матрицы эскалации;
- создание необходимых учетных записей и настройка прав доступа для специалистов Исполнителя.

Исходные данные для расчета стоимости оказания услуги:

- срок оказания услуги (мес.);
- режим оказания услуги (8x5 или 24x7).

5.2.6. Первая линия управления инцидентами

Первая линия реагирования на инциденты информационной безопасности:
- выявление инцидентов;
- регистрация, категорирование и первичный анализ инцидентов;
- запуск автоматизированного или ручного сценария реагирования;
- внесение предложений по изменению регламента работы первой линии, правил выявления инцидентов, порядка реагирования на инцидент.

В рамках подготовки к оказанию услуги выполняется:
- согласование SLA работы первой линии;
- определение ответственных со стороны Заказчика и Исполнителя;
- формирование состава и графика смен сотрудников первой линии;
- согласование матрицы эскалации.

Исходные данные для расчета стоимости оказания услуги:

- срок оказания услуги (мес.);
- режим оказания услуги (8x5 или 24x7).

5.2.7. Вторая линия управления инцидентами

Вторая линия реагирования на инциденты информационной безопасности:
- обогащение информации об инцидентах с дополнительных источников;

— расследование инцидентов с выявлением причин его возникновения и формированием отчёта;
— формирование новых сценариев выявления инцидентов.

В рамках подготовки к оказанию услуги выполняется:
— согласование SLA работы второй линии;
— определение ответственных со стороны Заказчика и Исполнителя;
— формирование состава и графика смен сотрудников второй линии;
— согласование матрицы эскалации.

Исходные данные для расчета стоимости оказания услуги:

— срок оказания услуги (мес.);

— режим оказания услуги (8x5 или 24x7).

6. Услуги уровня Advanced

6.1. Организационно-методологические сервисы

6.1.1. Разработка проектного решения

— Администрирование системы SIEM.
— Управление уровнем сервиса.
— Обеспечение безопасности и сохранности данных.
— Резервное копирование данных.
— Управление непрерывностью функционирования SIEM.
— Управление мощностями SIEM.
— Обеспечение масштабируемости.
— Управление изменениями системы SIEM.
— Мониторинг системы SIEM.
— Улучшение процедур SIEM.
— Регламент взаимодействия со сторонними организациями при информировании о инцидентах ИБ.
— Управление знаниями.

6.1.2. Разработка сценариев реагирования (playbooks)

Формирование сценариев реагирования на инциденты информационной безопасности (playbooks).

Описание каждого из playbook включает в себя:
— назначение playbook;
— описание процедуры первичного анализа инцидента;
— описание процедуры сдерживания, недопущения распространения;
— описание процедуры устранения вредоносной активности;
— описание процедуры восстановления после инцидента;
— описание процедуры оценки потерь от реализации инцидента;
— описание процедуры сбора и анализа ключевых событий развития и устранения инцидента, обновление внутренней базы знаний.

Исходные данные для расчета стоимости оказания услуги:

— количество playbooks.

6.1.3. Формирование ежемесячных отчетов о работе SIEM

Формирование ежемесячных отчетов о работе SIEM со сводной информацией о выявленных и отработанных инцидентах, а также плановых/фактических мерах повышения уровня информационной безопасности, реализуемых в ходе эксплуатации SIEM, в том числе:

- статистика по количеству новых, закрытых, в работе инцидентов всех уровней критичности и категорий;
- уровень защищенности активов Заказчика:
  - степень защищенности хостов от вредоносного ПО;
  - степень уязвимости хостов;
  - эффективность работы операторов по устранению инцидентов ИБ;
  - степень соблюдения трудовой дисциплины;
  - уровень соответствия требованиям ИБ;
  - объем спама;
  - управление правами доступа;
  - количество инцидентов, связанных с защищенными каналами связи.
- уровень соответствия требованиям ИБ:
  - защищенность хостов от вредоносного ПО;
  - процент хостов, на которых установлен DLP;
  - количество нарушений требований SLA по закрытию инцидентов;
  - количество нарушений требований SLA по регулярному сканированию хостов и обработке найденных уязвимостей;
  - нарушения требований по регулярному резервному копированию;
  - процент хостов с установленным запрещенным ПО;
  - количество нарушений политик ИБ (парольные политики, регистрация пользователей, нарушения с учетными записями и т.п.).
- уровень соблюдения требований ИБ пользователями;
  - активность пользователей в сети Интернет;
  - использование запрещенного ПО;
  - соблюдение режима работы.

Исходные данные для расчета стоимости оказания услуги:

- количество отчетов.

6.1.4. Оценка эффективности работы SIEM

Методология оценки эффективности SIEM в целом и отдельных сервисов в частности на базе KPI/SLA и описание влияния на бизнес-показатели внутреннего и внешнего бизнес-потребителя. Качественная и/или количественная оценка результатов деятельности SIEM для потребителей. В рамках данного сервиса критически важно установление бизнес-подразделений, которые формируют и согласовывают требования к оказываемым SIEM услугам.

В рамках оказания услуги могут быть применены, в том числе, следующие метрики оценки эффективности:

- временные SLA параметры обработки инцидента;
- эффективность эскалации инцидентов;
- число ложных срабатываний;
- текущая загруженность линий технической поддержки;
- динамика детектирования инцидентов;
- интегральная оценка соответствия нормативным требованиям;
- эффективность информационного обмена;
- профессиональная подготовка сотрудников ASOC;
- эффективность автоматизированных реакций на инциденты;
- воздействие инцидентов на объект мониторинга;
- финансовые затраты на расследование инцидентов;
- соотношение понесенных и предотвращенных потерь.

Исходные данные для расчета стоимости оказания услуги:

- количество метрик оценки эффективности работы SIEM.

6.2. Технические сервисы

6.2.1. Ведение базы знаний по кибербезопасности

Внедрение модуля Knowledge Center (если внедрение не было произведено ранее), организация структурированного хранения информации о правилах выявления инцидентов, сценариях реагирования, эксплуатационной документации и пр. Формирование связей на имеющиеся объекты знаний.

Исходные данные для расчета стоимости оказания услуги:

— количество объектов знаний.

6.2.2. Тестирование на проникновение

Периодическое осуществление инструментального тестирования на проникновение по модели black box, white box.

Цель:

— проверка степени защищенности Заказчика и/или реализация нормативных требований.

Решаемые задачи:

— проверка возможность получения доступа к информации ограниченного доступа сотрудником Заказчика;
— выявление уязвимости информационно-телекоммуникационной инфраструктуры Заказчика и вариантов их использования
— проверка возможность повышения своих привилегий рядовым сотрудником Заказчика;
— разработка рекомендаций по нейтрализации обнаруженных уязвимостей;
— проверка возможности проникновения в локальную сеть извне.

Применяемые инструменты:

— универсальные сканеры уязвимостей (например, xSpider);
— ручное тестирование, когда проводятся попытки преодолеть защиту через адресную строку веб-браузера, уязвимости в ОС, АО, СПО, ПО и т.п.;
— специализированное ПО (например, утилиты из дистрибутива ОС Kali Linux и т.п.)

Этапы оказания услуги:

— внешний анализ защищенности – модель black box. работы проводятся удаленно через сеть Интернет: организуются ряд согласованных атак через публичные ресурсы Заказчика;
— внутренний анализ защищенности – модель grey box или white box. Заказчик предоставляет удаленный доступ к своей локальной сети. Атаки моделируются от имени рядового сотрудника;
— подготовка отчета о тестировании на проникновение.

Результат оказания услуги:

— отчет, с описанием методологии тестирования, объектов воздействия, выявленных уязвимостей, уровней их критичности, а также набором рекомендации по устранению выявленных проблем.

Исходные данные для расчета стоимости оказания услуги:

— модель тестирования (black box, grey box, white box);

— перечень ресурсов для тестирования.

6.2.3. Третья линия управления инцидентами

Третья линия реагирования на инциденты информационной безопасности:

— углубленная форензика по массиву данных;
— применение специализированных инструментов анализа инфраструктуры, подверженной атаки;
— формирование отчета с описанием контрмер, направленных на предотвращение повторного появления инцидентов и дополнительных корреляционных правил его раннего детектирования;
— поиск признаков компрометации и поиск актуальных угроз

В рамках подготовки к оказанию услуги выполняется:

— согласование SLA работы третьей линии;
— определение ответственных со стороны Заказчика и Исполнителя;
— формирование состава и графика смен сотрудников третьей линии;
— согласование матрицы эскалации.

Исходные данные для расчета стоимости оказания услуги:

- срок оказания услуги (мес.);
- режим оказания услуги (8x5 или 24x7).

6.2.4. DevSecOps

Интеграция с процессами безопасной разработки Security Development Lifecycle (SDL).

6.2.5. Выявление аномалий в бизнес-процессах

Аналитика транзакций от прикладных бизнес-систем с построением корреляционных правил по выявлению аномалий в бизнес-процессах.

6.2.6. Модель управления рисками и оценки потерь от инцидентов

Формирование карты рисков информационной безопасности и их влияния на бизнес. Измерение ключевых показателей рисков кибербезопасности. Оценка потенциального ущерба от реализации киберугроз и их влияния на бизнес. Подбор компенсирующих мер и составление дорожной карты их внедрения.

6.2.7. Противодействие мошенничеству

Разработка правил противодействия внутреннему и внешнему фроду (антифрод) на основе прикладных логов и анализа действий пользователей/клиентов Заказчика.

6.2.8. Настройка средств защиты информации

Конфигурация СЗИ по результатам анализа текущих:
- аудит текущего состояния защищенности ИТ-инфраструктуры, информационных систем, бизнес-процессов;
- анализ достаточности имеющихся СЗИ и корректности их настроек, определение необходимости дозакупки СЗИ;
- формирование дорожной карты по приведению конфигураций СЗИ в необходимое состояние;
- настройка СЗИ;

Исходные данные для расчета стоимости оказания услуги:

- требования по ИБ, которым должны соответствовать настройки СЗИ;
- масштаб объекта защиты (количество офисов, АРМ, серверов);
- состав и количество имеющихся СЗИ.

6.2.9. Thread Intelligence

Thread Intelligence (далее TI) с подключением платных и бесплатных TI источников, настройкой обогащения сущностей SIEM информацией с этих источников, выводом на визуальные панели статистики по имеющимся индикаторам и инцидентам, связанным с IoC.
В рамках подготовки к оказанию услуги выполняется:
- согласование используемых типов источников IoC, форматов исходных данных, состава источников TI (платных и бесплатных);
- выбор варианта подключения источников IoC и выполнение подключения источников;
- реализация логики формирования сводного перечня IoC с учетом выбранных источников и форматов данных;

Исходные данные для расчета стоимости оказания услуги:

- необходимость использования платных источников TI (CTT Threat Feed, AM TIP, другое);
- требования/пожелания по конкретным источникам TI.

6.2.10. MITRE ATT@CK

Внедрение базы тактик и техника MITRE ATT@CK с обеспечением регулярного анализа покрытия актуальных векторов атак компенсирующими контрмерами и механизмами обнаружения злонамеренной активности внешних хакеров и внутренних нарушителей (инсайдеров).

Выполнение услуги предусматривает:

- автоматическое обновление информации об объектах (техниках, тактиках, группах, программном обеспечении) в соответствии с обновлением версий в базе знаний MITRE ATT&CK;
- реализацию базового набора корреляционных правил для детектирования потенциального применения техник базы знаний MITRE ATT&CK (а также на основе анализа риск-баллов объектов), применительно к инфраструктуре Заказчика;
- создание инцидента при детектировании использования техники базы знаний MITRE ATT&CK;
- реализацию механизмов увеличения риск-балла при детектировании события использования техник базы знаний MITRE ATT&CK для связанного объекта;
- предоставление визуальных инструментов для проведения процесса приоритезации техник, используемых злоумышленниками, по нескольким категориям актуальности/применимости в инфраструктуре Заказчика;
- предоставление визуальных инструментов для отображения и статистического анализа событий обнаружения использования техник MITRE ATT&CK;
- предоставление визуальных инструментов для статистического анализа риск скоринга в разрезе конкретных объектов/групп объектов: учетные записи пользователей, рабочие станции, сервера.

6.2.11. User Behavior Analytics

Внедрение модуля поведенческой аналитики (User Behavior Analytic) пользователей и механизмов оценки операционной эффективности сотрудников:

- определение объектов для профилирования;
- определение категорий расчета скоринга;
- разработка и адаптация имеющихся политик профилирования;
- настройка правил выявление отклонений;
- настройка визуальных витрин для анализа отклонений.

6.2.12. Резервное копирование и восстановление

Механизмы репликации данных. Восстановление dataset в случае технологических аварий.

6.2.13. Управление уязвимостями

Контроль уязвимостей компонент инфраструктуры Заказчика:

- приоритизация уязвимостей;
- регулярное обновление базы уязвимостей;
- периодические сканирования на поиск уязвимостей;
- анализ и корреляция обнаруженных уязвимостей с другими источниками;
- постановка задач по устранению уязвимостей специалистам Заказчика;
- оповещение выделенных сотрудников об обнаружении уязвимостей.
- создание инцидентов по выявленным уязвимостям.
- формирование отчета о статусе уязвимостей (обнаружено/устранено).

В рамках подготовки к оказанию услуги выполняется:

- согласование условий поиска уязвимостей (определение перечня сканируемых узлов, периодичности сканирования, места хранения результатов сканирования, визуального представления результатов сканирования, ответственных со стороны Заказчика).
- участие в выполнении необходимых настроек на стороне сканера уязвимостей.
- выполнение необходимых настроек на стороне SIEM (подключение источника – сканера уязвимостей, разработка дашбордов и отчетов, настройка правил срабатывания инцидентов, настройка оповещений, настройка автоматического направления запросов в ИТ/ИБ службы при обнаружении уязвимостей).

Исходные данные для расчета стоимости оказания услуги:

— срок оказания услуги (мес.);

— модель и версия сканера уязвимостей (при наличии);

— количество сканируемых узлов;

— платформа установки сканер – виртуальная/физическая?

6.2.14. Управление угрозами ИБ

— Выявление новых угроз.
— Разработка мероприятий по предотвращению появления новых угроз и устранения последствий реализации угроз.
— Анализ киберугроз на основе данных от внешних источников.

6.2.15. Подключение дополнительных источников

Подключение дополнительных источников, целесообразность которых обнаружена на этапе опытной и промышленной эксплуатации:
— для агентской схемы подключения источников - подготовка и предоставление Заказчику агентов для установки их на источники данных. Консультационное сопровождение процесса установки агентов;
— для безагентской схемы подключения источников - настройка необходимых протоколов и сервисов для подключения к источникам, получение служебных учетных записей и проверка прав доступа к источникам;
— тестирование и отладка процесса получения данных;
— настройка справочников и структуры хранилища данных для каждого источника;
— нормализация поступающих от источников данных.

Исходные данные для расчета стоимости оказания услуги:

— количество дополнительных источников (с распределением по типам и оценкой объема поступающих данных от каждого).

6.2.16. Разработка новых корреляционных правил

Разработка новых корреляционных правил, предварительно не заявленных на этапе внедрения SIEM.

Исходные данные для расчета стоимости оказания услуги:

— требуемое количество корреляционных правил;

6.2.17. Разработка новых визуальных витрин и отчетов

Разработка новых визуальных витрин и отчетов (функциональных дашбордов), обеспечивающих оперативный мониторинг средств защиты, инфраструктурных и прикладных объектов мониторинга:
— согласование оформления дашбордов;
— определение состава информационных панелей и отображаемых на них данных (диаграммы, графики, таблицы и проч.);
— определение источников данных для дашбордов, правил расчета значений, выводимых на дашборды и условий изменения цветовой идентификации информационных панелей.

Исходные данные для расчета стоимости оказания услуги:

— количество новых визуальных витрин (функциональных дашбордов);

7. Типовой регламент сопровождения

7.1. Область действия

Настоящий Типовой регламент сопровождения Smart Monitor (далее - Регламент) описывает порядок оказания услуг профессионального сопровождения.

7.2. Термины и определения

Исполнитель – представитель правообладателя программного обеспечения Smart Monitor, уполномоченный для оказания услуг сопровождения Конечному пользователю.

Рабочий День – период времени с 9.00 до 18.00 по московскому времени за исключением выходных и праздничных дней, установленных законодательством Российской Федерации.

Рабочий Час – астрономический час в пределах Рабочего дня.

Режим – диапазон часов/дней, в которые осуществляется оказание услуг сопровождения:

- Режим 8x5 – прием и решение Инцидентов Конечного пользователя в Рабочие дни и Рабочие часы;
- Режим 24x7 – прием и решение Инцидентов Конечного пользователя в Рабочие, выходные и праздничные дни, Рабочие и нерабочие часы.

Услуга по сопровождению – формализованное описание выполняемых действий, объединенных единой задачей функционирования Smart Monitor

SLA – временные рамки, заданные для регистрации, решения, расследования Инцидентов каждого из Уровней критичности на каждой из Линий сопровождения.

False Positive – ложное срабатывание, не являющееся реальной угрозой.

Линии сопровождения – группы специалистов Исполнителя, осуществляющие решение Инцидентов по следующему принципу:

- Первая линия сопровождения – решение типовых Инцидентов, не требующих дополнительного анализа/расследования;
- Вторая линия – решение нетиповых Инцидентов, требующих дополнительного анализа, обогащения данных, доработки корреляционной логики набора правил для снижения количества False Positive;
- Третья линия сопровождения – решение Инцидентов, требующих доработок (изменения логики функционирования) Smart Monitor

Сертификат сопровождения – электронный или бумажный документ, выданный Исполнителем на имя Конечного пользователя, содержащий, но не ограничивающийся, следующую информацию:

- ключ сопровождения;
- дату начала и окончания сопровождения;
- перечень услуг по сопровождению;
- режим, SLA приема и решения Инцидентов.

Инцидент – это событие или серия событий, которые указывают на нарушение или потенциальную угрозу безопасности информации, инфраструктуры или бизнес-процессов Конечного пользователя, устранение или предоставление рекомендаций по которым должны осуществить специалисты Исполнителя.

Корреляционное правило – логика в Smart Monitor для выявления Инцидентов.

Ключ сопровождения – переданная в электронном или бумажном виде Конечному пользователю последовательность букв и цифр, определяющая возможность получения Конечным пользователем оговоренных услуг сопровождения, режим приема и решения Инцидентов и сроки предоставления услуги сопровождения.

Конечный пользователь – юридическое или физическое лицо, которому переданы неисключительные права на программное обеспечение Smart Monitor.

Уровень критичности (Инцидента) – один из уровней:

- Критический:
  - доступность ресурсов (защищаемых приложений) нарушено или происходит резкое снижение производительности и защиты, что оказывает критическое влияние на бизнес-операции Заказчика (критически важные бизнес-процессы недоступны);
  - постоянное или практически постоянное прерывание услуг;
  - альтернативного решения для восстановления работоспособности не существует;
- Высокий:
  - функционирование системы частично остановлено, что оказывает серьёзное негативное влияние на бизнес-операции Заказчика;
  - имеет место периодический кратковременный перерыв в предоставлении услуг;
  - устойчиво работающего временного решения для восстановления работоспособности не существует;
- Средний
  - функционирование системы нестабильно, оказывается незначительное влияние на бизнес-операции Заказчика;
  - выполнение большинства повседневных задач производится в режиме, близком к обычному;
  - нарушен штатный режим работы одного пользователя;
- Низкий - консультационный запрос или запрос на проведение регламентных работ (обновление продукта, сигнатур, иное).

7.3. Типовой SLA

В настоящем регламенте предусмотрен следующий типовой SLA (если в Сертификате сопровождения не указано иное):

- **регистрация** Инцидента должна быть проведена в течение 2 Рабочих Часов для Режима 8x5 либо в течение 2 астрономических часов для Режима 24x7 (с момента фиксации инцидента и получения уведомления по адресу электронной почты SMSUP@volgablob.ru);
- **реакция** линий управления Инцидентами в рамках решения инцидента должна быть проведена в следующих условиях:

Время реакции (часов) [1] / **Уровень критичности**	**Первая линия**	**Вторая линия**	**Третья линия**
Критический	2	2	4
Высокий	4	8	16
Средний	8	16	-

[1] Если данное условие оговорено в Сертификате сопровождения - для каждого Инцидента время реакции и трудоемкость решения определяется и согласуется Исполнителем и Конечным пользователем (Клиентом) отдельно в переписке по электронной почте. При согласовании Исполнитель объявляет Клиенту примерное количество часов, требующихся для решения Инцидента. Исполнитель обязан принять часы, подтвердив их в переписке по электронной почте.

Время реакции (часов) [1] / Уровень критичности	Первая линия	Вторая линия	Третья линия
Низкий	16	-	-

Примечание: *для Режима 8x5 SLA приведен в рабочих Часах, для Режима 24x7 – в астрономических часах.*

7.4. Права и обязанности исполнителя

7.4.1. Исполнитель обязуется:

7.4.1.1. Обеспечивать мониторинг инцидентов ИБ в соответствии с режимом работы.

7.4.1.2. Оказывать Конечному пользователю услуги профессионального сопровождения на основании зафиксированных Инцидентов.

7.4.1.3. Соблюдать конфиденциальность при работе с информацией, полученной от Конечного пользователя напрямую или косвенно в процессе решения Инцидентов.

7.4.1.4. Оказывать услуги сопровождения в соответствии с оговоренным в Сертификате сопровождения Режимом.

7.4.1.5. Соблюдать порядок оказания услуг сопровождения, определенные в Разделе 7.3.

7.5. Исполнитель вправе:

7.5.1.1. Требовать от Конечного пользователя предоставления действующего Ключа сопровождения, выданного Конечному пользователю.

7.5.1.2. Запрашивать у Конечного пользователя информацию, необходимую для выполнения своих обязательств по настоящему Регламенту.

7.5.1.3. Не начинать или приостановить реагирование на Инцидент и уведомить его по телефону и/или электронной почте, в случае:

7.5.1.3.1. отказа Конечного пользователя предоставить дополнительную информацию, по мнению Исполнителя требующуюся для решения Инцидента (включая серийные номера, лицензионные, конфигурационные файлы и т.п.);

7.5.1.3.2. отказа или невозможности Конечного пользователя предоставить действующий Ключ сопровождения.

7.5.1.4. Выполнение возобновляется после устранения описанных причин приостановки.

7.6. Права и обязанности конечного пользователя

7.6.1. Конечный пользователь обязуется:

7.6.1.1. Предоставлять Исполнителю всю необходимую информацию для решения Инцидента, своевременно реагировать на запросы Исполнителя, касающиеся решения Инцидента.

7.6.2. Конечный пользователь вправе:

7.6.2.1. При наличии действующего Сертификата сопровождения запрашивать у Исполнителя и получать актуальные обновления модулей программного продукта Smart Monitor, на которые Конечному пользователю предоставлены неисключительные права.

7.6.2.2. При наличии действующего Сертификата сопровождения запрашивать у Исполнителя исправления обнаруженных ошибок в работе модулей программного продукта Smart Monitor, на которые Конечному пользователю предоставлены неисключительные права.

7.7. Порядок и сроки оказания услуг сопровождения

Настоящий регламент не предусматривает выезд инженера Исполнителя на площадку Конечного пользователя. Все работы Исполнитель выполняет удаленно.

Стоимость и сроки выезда инженера Исполнителя на площадку Конечного пользователя оговариваются отдельными договорами.

При возникновении необходимости, представитель Конечного пользователя направляет запрос с Инцидентом по электронной почте по адресу SMSUP@volgablob.ru и дублирует запрос в системе Service Desk. В запросе представитель Конечного пользователя обязан указать действующий Ключ сопровождения, выданный на имя Конечного пользователя.

Первая линия сопровождения Исполнителя обязана взять Инцидент в работу в соответствии с SLA (см. Раздел 7.3).

Реагирование на инцидент должно быть выполнено в соответствии с SLA (см. Раздел 7.3) Первой линией сопровождения, либо передан на Вторую линию сопровождения.

При поступлении Инцидента на Вторую линию сопровождения, реагирование должно быть выполнено в соответствии с SLA (см. Раздел 7.3), либо Инцидент должен быть передан на Третью линию сопровождения.

При поступлении Инцидента на Третью линию сопровождения, реагирование должно быть выполнено в соответствии с SLA (см. Раздел 7.3).

В соответствии с п.7.5.1.2, срок реагирования на Инцидент может быть увеличен или сокращен.

7.8. Конфиденциальность

Исполнитель не вправе, без письменного согласия Конечного пользователя, сообщать третьим лицам, за исключением работников Исполнителя, информацию, связанную или полученную в связи с оказанием услуг сопровождения (включая информацию о результатах оказания услуг сопровождения, оригиналы или копии документов), и использовать ее для каких-либо целей, кроме связанных с выполнением обязательств по Сертификату сопровождения (далее – конфиденциальная информация). Письменным согласием считается, помимо бумажной копии, электронное письмо, отправленное представителем Конечного пользователя в адрес Исполнителя.

Исполнитель обязуется обеспечить соблюдение его работниками и привлекаемыми к выполнению Работ третьими лицами требований конфиденциальности.

Исполнитель имеет право раскрывать конфиденциальную информацию государственным органам, уполномоченным запрашивать такую информацию в соответствии с законодательством Российской Федерации, на основании должным образом оформленного запроса на предоставление такой информации. При этом, Исполнитель обязан незамедлительно уведомить Конечного пользователя о поступившем запросе и предпринять все необходимые и допустимые законом действия для предотвращения раскрытия конфиденциальной информации.

7.9. Обстоятельства непреодолимой силы

Исполнитель не несет ответственность в случае несвоевременного или ненадлежащего исполнения каких-либо своих обязательств по настоящему Регламенту, если такое неисполнение обусловлено исключительно наступлением или действием обстоятельств непреодолимой силы, а именно: наводнение, землетрясение и другие природные стихийные бедствия, объявленные или фактические военные действия, гражданские волнения, а также издание актов государственных органов.