SOLAR

W: RT-SOLAR.RU

ЧЕК-ЛИСТ

НА ЧТО ОБРАТИТЬ ВНИМАНИЕ ПРИ ВЫБОРЕ РЕШЕНИЯ ПО МОНИТОРИНГУ ВНЕШНИХ ЦИФРОВЫХ УГРОЗ

Список требований

Пройдите по всем пунктам документа, чтобы сформулировать и структурировать требования к решению и к внутренним процедурам, необходимым для его эксплуатации

[01]

Факторы рисков

[02]

Архитектура решения

[03]

Зоны ответственности

[04]

Интеграционные возможности

[05]

Особенности поставщика

[06]

Стоимость

01. Факторы рисков

Определите ключевые факторы рисков, актуальных для вашей компании

Необходимо учесть: факторы рисков, актуальных для смежных отделов — служб IT и ИБ, PR-департамента, службы экономической безопасности, отдела поддержки тендеров и т. д.

ИНФОРМАЦИОННЫЕ РИСКИ

- [ ] Теневое IT
- [ ] Фишинговые атаки на сотрудников компании
- [ ] Атаки на IT-инфраструктуру
- [ ] Продажа доступов/чувствительных данных на закрытых площадках
- [ ] Атаки через партнеров

РЕПУТАЦИОННЫЕ РИСКИ

- [ ] Публикация чувствительных данных в открытых источниках
- [ ] Негативные информационные кампании, направленные на дискредитацию бренда
- [ ] Использование бренда компании в противоправных целях
- [ ] Использование личного бренда ключевых лиц компании в противоправных целях
- [ ] Фишинговые атаки на клиентов и партнеров

ЭКОНОМИЧЕСКИЕ РИСКИ

- [ ] Противоправное использование платежных инструментов
- [ ] Продажа запрещенных товаров/услуг на маркетплейсах
- [ ] Подложное партнерство

02. Архитектура решения

Определите предпочтительную архитектуру решения

◉ СЕРВИСНАЯ МОДЕЛЬ

Платформа и интерфейс пользователя предоставляются сервис-провайдером

Необходимо учесть:

- SLA на доступность внешней платформы

○ ГИБРИДНАЯ МОДЕЛЬ

Сервис-провайдер предоставляет платформу, интерфейс пользователя размещается на собственных ресурсах

Необходимо учесть:

- SLA на доступность внешней платформы
- Поддержание работоспособности ресурса, на котором будет размещен интерфейс пользователя

○ IN-HOUSE

Платформа и интерфейс пользователя размещаются на собственных ресурсах, сервис-провайдер предоставляет обновление источников данных

Необходимо учесть:

- Наличие мощностей для хранения и обработки данных
- Поддержание работоспособности ресурсов, на которых будут размещены платформа и интерфейс пользователя
- Наличие квалифицированных кадров для анализа событий

03. Зоны ответственности

Определите зоны ответственности при обработке событий

○ Выявление угроз, аналитика, работы по блокированию факторов рисков ведутся сервис-провайдером

Необходимо учесть:

- Категории выявляемых исполнителем событий
- Категории организаций, с которыми взаимодействует исполнитель в рамках блокировки
- SLA по реагированию на выявленный фактор риска

○ Выявление и аналитика угроз ведутся сервис-провайдером, работы по блокированию факторов рисков — собственными силами

Необходимо учесть:

- Категории выявляемых исполнителем событий
- Наличие каналов взаимодействия с организациями, участвующими в блокировании факторов рисков
- Наличие ресурсов на взаимодействие с этими организациями

◉ Сервис-провайдер предоставляет только сырые данные о выявленных угрозах, аналитика и работы по блокированию факторов рисков ведутся собственными силами

Необходимо учесть:

- Категории выявляемых исполнителем событий
- Наличие квалифицированных кадров для анализа полученных событий
- Наличие каналов взаимодействия с организациями, участвующими в блокировании факторов рисков
- Наличие ресурсов на взаимодействие с этими организациями

04. Интеграционные возможности

Определите необходимый функционал платформы

- [ ] Автоматическая передача данных о выявленных событиях в смежные системы (SIEM, CMDB, GRC и т. д.) через API или нативную интеграцию
- [ ] Возможность выгрузки данных в читаемые форматы: xml, json, csv

05. Особенности поставщика

Определите необходимые критерии для выбора поставщика

ОПЫТ И РЕСУРСЫ

- [ ] Наличие опыта оказания услуг компаниям отрасли
- [ ] Наличие опыта оказания услуг компаниям схожего масштаба
- [ ] Наличие специалистов, выделенных непосредственно на оказание услуги
- [ ] Наличие возможности проведения пилотных проектов

РЕЖИМ ОКАЗАНИЯ СЕРВИСА

- ( ) 8x5
- (•) 24x7

06. Стоимость

Дополнительно обсудите с поставщиком следующие детали:

- Гибкость тарификации (модульность, влияющие на тарифы факторы, сроки оплаты)
- Итоговую стоимость предложения