Разработка концепции центра мониторинга ИБ

Услуги по SOC Консалтингу

kaspersky АКТИВИРУЙ БУДУЩЕЕ

SOC

Центры мониторинга и оперативного реагирования для борьбы с продвинутыми киберугрозами.

Их задача — оперативно выявлять инциденты информационной безопасности и принимать ответные меры, минимизируя ущерб.

Введение

Количество и масштаб кибератак, а также ущерб от них продолжают расти. Профессиональные киберпреступные организации, политические «хактивисты» и группы, имеющие государственную поддержку, значительно продвинулись в технологическом плане — часто они превосходят ИБ-службы как по уровню подготовки, так и по ресурсам.

Организация собственного SOC — ответственный и долгосрочный проект, который сложно реализовать без экспертной поддержки. «Лаборатория Касперского» предоставляет клиентам услуги консалтинга по построению SOC, которые опираются на собственный практический опыт, проверенные решения и методики.

Цель и задачи проведения работ

Целью проведения работ является разработка концепции центра мониторинга ИБ (SOC), которая учитывает задачи и инфраструктуру клиента, а также обеспечивает эффективную эксплуатацию и развитие SOC.

В рамках работ решаются задачи:

Разработка технической архитектуры SOC

Разработка организационно-штатной структуры SOC

Разработка операционной модели SOC

Определение ролей, обязанностей и требований для сотрудников SOC

Разработка процессов и сервисов SOC, а также соответствующих процедур для их реализации

Разработка специфичных сценариев реализации угроз ИБ (Use-cases)

Разработка сценариев реагирования на инциденты ИБ (Playbooks)

Разработка метрик и KPI для контроля эффективности деятельности SOC

Разработка стратегии и плана развития SOC, постпроектная поддержка и консультирование

Этапы работ

Мы разрабатываем рекомендации по всем аспектам работы SOC, включая работу с командой, процессами и технологиями.

Подход «Лаборатории Касперского» к организации SOC основан в первую очередь на нашем практическом опыте — эксплуатации собственного SOC, предоставлении аутсорсинговых услуг нашим клиентам, расследовании APT-кампаний и инцидентов заказчиков, а также ежедневном анализе около 380 тысяч новых образцов вредоносного ПО. Помимо собственного опыта, эксперты «Лаборатории Касперского» также используют общепризнанные «лучшие практики» в части SOC — такие как методики MITRE, NIST, SANS Institute, ENISA, FIRST и других экспертных сообществ.

Услуга консультирования по построению SOC включает этапы:

Сбор информации

Производится сбор исходных данных, необходимых для выполнения последующих этапов проекта. Сбор данных производится методом интервьюирования и анкетирования специалистов заказчика.

Проектирование

Разработка комплексной концепции SOC, адаптированной под инфраструктуру, требования и задачи клиента.

Разработка архитектуры технической платформы SOC (как с использованием продуктовой линейки «Лаборатории Касперского», так и сторонних решений).

Разработка структуры команды, ролей, обязанностей.

Разработка процессов SOC для операционных задач, задач управления и технического сопровождения.

При необходимости оказывается помощь с проведением интервью при найме новых сотрудников.

Сопровождение внедрения

Консультационная поддержка процессов внедрения и развертывания технических средств в рамках разработанной проектной документации SOC.

Развертывание и конфигурирование решений «Лаборатории Касперского» могут осуществляться силами партнера-интегратора или в рамках профессиональных сервисов «Лаборатории Касперского».

Развертывание и конфигурирование решений сторонних поставщиков могут осуществляться силами партнера-интегратора либо самостоятельно специалистами заказчика.

Комплексная поддержка

Поддержка и консультирование заказчика в течение оговоренного времени после введения SOC в эксплуатацию. Возможны различные варианты постпроектной поддержки, включая:

- предоставление сервисов безопасности (аутсорсинг) — опционально доступные сервисы для решения наиболее сложных задач, таких как обнаружение и реагирование на инциденты, цифровая криминалистика, анализ вредоносных программ и анализ защищенности;
- консультационная поддержка в рамках разработанной концепции SOC. Предоставляется заранее оговоренное количество часов консультационной поддержки;
- техническая поддержка решений «Лаборатории Касперского»;
- киберучения с участием Red Team;
- оценка уровня зрелости SOC в рамках реализации концепции непрерывного развития;
- проведение учений по симуляции атак.

Поэтапный подход

Проект построения SOC обычно является долгосрочным и комплексным проектом. Кроме того, процессы совершенствования и оптимизации процессов SOC, модернизации технологического стека и повышения квалификации персонала по своей сути являются постоянными и регулярными. С учетом опыта ведения таких проектов «Лаборатория Касперского» рекомендует применять итеративный подход — определять значимые уровни зрелости и достигать их в отдельных этапах или последовательных проектах по построению SOC. В качестве базовых предлагается рассмотреть уровни зрелости, указанные ниже. Данный перечень является предварительным и подлежит уточнению в рамках предпроектного планирования с учетом специфики и требований заказчика.

Уровень	Инструментарий	Функции	Персонал
Начальный	• SIEM • Сканнер защищенности • IRP/Ticketing • Потоки данных об • угрозах (фиды) • База знаний • Система IT-мониторинга SOC	• Мониторинг ИБ • Анализ защищенности инструментальными средствами • Реагирование на инциденты ИБ	• Аналитики первой, второй линии • Инженеры SOC
Расширенный	• EDR • NTA • Аналитические отчеты Threat Intelligence • Автоматизированные средства анализа ВПО (Research Sandbox) • Подсистема отчетности	• Анализ защищенности вручную (тестирование на проникновение) • Анализ готовой аналитической информации Threat Intelligence • Базовый Threat Hunting • Автоматизированный анализ ВПО • Базовая автоматизация рутинных действий	• Исследователи угроз
Целевой	• Решение для атрибуции угроз • Решение для поддержки процессов Threat Hunting • Решение класса Breach and Attack Simulation • Платформа Threat Intelligence (TIP) • Специализированное программное обеспечение для анализа ВПО	• Проактивный поиск угроз (Threat Hunting) • Атрибуция угроз • Киберучения (red teaming) • Подготовка собственных аналитических данных Threat Intelligence • Реверс-инжиниринг вредоносного ПО • Автоматизация	• Аналитики Threat Intelligence/ Threat Hunting • Персонал по анализу угроз (реверс-инжиниринг, атрибуция, форензика) • Команда оценки защищенности

Результаты

Услуга консалтинга по построению SOC от «Лаборатории Касперского» обеспечит клиенту следующее:

Разработка детального дизайна SOC

Разработка согласованной адаптированной концепции, покрывающей все аспекты создания, эксплуатации и развития SOC на основе опыта «Лаборатории Касперского» и «лучших практик»

Обучение

Обучение специалистов SOC клиента и передача знаний

Поддержка и постпроект

Поддержка процессов найма персонала — помощь с проведением интервью потенциальных кандидатов на роль персонала SOC. Постпроектная поддержка и консультирование

Результаты услуги в рамках проектной документации

Документация	Описание
Концепция SOC	**Основной документ, описывающий ключевые положения создания, эксплуатации и развития SOC** **Назначение, миссия, цели и задачи SOC** 1. **Стратегия SOC** — определяет SOC чартер, включая подробное описание миссии SOC и основных задач и целей SOC, его полномочий и места в структуре организации. 2. **Сервисный каталог SOC** — описание сервисов, предоставляемых SOC, в том числе внутренним заказчикам. 3. **Дорожная карта SOC** — описание основных этапов развития SOC (если применяется поэтапный подход) и дальнейшие векторы развития SOC на горизонте 1-3 года. 4. **Архитектура SOC** — описание технической архитектуры SOC, используемых решений, источников данных, потоков данных и схем интеграции. 5. **Оргштатная структура SOC:** • роли, обязанности и требования к квалификации сотрудников SOC; • текущая и целевая оргштатная структура SOC; • матрица ответственности (Responsbile, Accountable, Consulted, Informed, RACI); • рекомендованная программа обучения и сертификации; • процедуры onboarding персонала SOC; • расписание смен для 24x7 и других нестандартных режимов работы. **Ключевые показатели эффективности (КПЭ) SOC** В документе описываются метрики процессов и сервисов SOC. При этом метрики включают в себя как уровни оказания сервисов (SLA), так и внутренние ключевые показатели эффективности (KPI), информационные и технологические показатели.
Отчетность SOC	**Документ описывает типы, содержание и шаблоны отчетности** • процесс управления отчетностью; • перечень отчетов; • шаблоны и примеры отчетов.

Документация	Описание
Процессы и процедуры SOC	**Детализированное описание процессов и процедур SOC:** Карта процессов SOC **Описание процесса и процедур, включая**: • диаграмму процесса; • описание шагов в рамках процесса/процедуры; • связанные процедуры; • вход/выход процесса. **Описание групп и подгрупп процессов:** (пример) **Мониторинг и управление инцидентами** • мониторинг событий ИБ; • управление инцидентами. **Исследования и анализ угроз** • управление данными об угрозах (Threat Intelligence); • управления сценариями обнаружения (use cases management); • управление сценариями реагирования на инциденты ИБ (playbooks management); • активный поиск угроз (Threat Hunting); • анализ вредоносного ПО. **Управление** • управление знаниями; • управление сервисами; • управление эффективностью; • управление персоналом. **Сопровождение** • сопровождение технических средств; • управление изменениями; • управление потоками данных. **Уязвимости инфраструктуры** • анализ защищенности; • управление уязвимостями; • инвентаризация.
Управление сценариями обнаружения (use-cases) и реагирования (playbooks) в SOC	**Документ описывает систему управления жизненным циклом сценариев обнаружения (use-cases) и реагирования (playbooks) в рамках SOC, содержит следующие разделы:** • таксономия сценариев обнаружения и реагирования; • процесс управления сценариями обнаружения и реагирования; • процессы создания, пересмотра, тестирования, включения и вывод из эксплуатации сценариев обнаружения и реагирования; • перечень сценариев обнаружения (use-cases), релевантных для заказчика; • перечень сценариев реагирования (playbooks), актуальных для заказчика; • перечень пошаговых инструкций (runbooks) по выполнению сценария реагирования (разработка данного документа возможна только для продуктов «Лаборатории Касперского»).
Объект SOC	**Документ охватывает:** • **вопросы физической планировки SOC;** • **требования:** - к техническосу оснащению рабочих мест SOC; - зонированию SOC; - мебели, зонам отдыха.

Перечень документации является предварительным и требует согласования на этапе предпроектного планирования.

Также рекомендуем

Kaspersky Threat Intelligence

Быстрый доступ к техническим, тактическим, операционным и стратегическим данным об угрозах

Подробнее

Kaspersky Security Assessment

Анализ защищенности вашей организации

Подробнее

Kaspersky Incident Response

Ликвидация последствий инцидентов безопасности

Подробнее

«Лаборатория Касперского» задействует аналитику продвинутых угроз, цифровую криминалистику и расследования, чтобы помочь корпоративным клиентам защитить онлайн-сервисы и репутацию.

Подробнее

О «Лаборатории Касперского»

Технологии и решения «Лаборатории Касперского» защищают более 400 миллионов пользователей почти в 200 странах и регионах мира. «Лаборатория Касперского» — крупнейшая в мире частная компания, поставляющая решения для защиты рабочих мест. Компания входит в список четырех лидирующих мировых поставщиков решений для обеспечения безопасности рабочих мест. На протяжении своей 20-летней истории «Лаборатория Касперского» постоянно внедряет новые разработки в сфере IT-безопасности и предлагает эффективные решения для обеспечения компьютерной безопасности крупным предприятиям, малым компаниям и частным пользователям.

Несомненно, самый ценный актив компании — богатый многолетний опыт борьбы с крупными киберугрозами, изучения уязвимостей и вредоносного ПО, нейтрализации потенциально опасных приложений, фильтрации трафика и многих других практик. Благодаря этому мы на шаг впереди конкурентов — наша компания предлагает пользователям надежную защиту от атак новых типов.

Kaspersky SOC Consulting

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее