SOLIDLAB SOC

# ЦЕНТР МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

## СЦЕНАРИИ ИСПОЛЬЗОВАНИЯ

- Построение SOC с нуля под ключ
- Усиление внутренних команд заказчика
- Увеличение покрытия объектов мониторинга
- Мониторинг критической инфраструктуры
- Экспресс-аудит текущего уровня обеспечения ИБ
- Выделенный внешний SOC для мониторинга 24/7

## УСЛУГИ И СЕРВИСЫ

- Построение SOC с нуля: создание центра кибериндидентов с архитектурой, решениями, процессами и обучением
- Облачный или гибридный мониторинг 24/7/365, адаптированный под ваши потребности
- Оценка зрелости вашего SOC: анализ эффективности, выявление зон развития и создание дорожной карты
- Purple Team: объединение атакующих и защитных подходов с анализом реакции на атаки (Red Team vs Blue Team)
- Консалтинг по защите информации: оптимизация ИБ, разработка политик и рекомендаций для защиты данных

## ПРЕИМУЩЕСТВА

- Технологическая независимость: минимизация санкционных рисков и проблем лицензирования
- Глубокая интеграция: собственные продукты обеспечивают бесшовную работу компонентов SOC
- Экспертная аналитика: команда специалистов обеспечивает понимание угроз и точное детектирование атак
- Тесное взаимодействие команд Vulnerability Management+Red Team
- Вариативность выбора необходимых функций SOC

**Эксперты из разных областей ИБ**

**< 1 месяц доступ к SOC**

**< 13 мин время обработки инцидента**

**> 60 000 средний поток данных**

# ВАРИАНТЫ ВНЕДРЕНИЯ

## SOC as a Service

### T1 Базовый

- Мониторинг журналов событий
- Уведомления об инцидентах
- Пакет экспертизы «Базовый»
- Круглосуточный мониторинг (24/7)
- Первичный анализ инцидентов
- Автоматизированный мониторинг

### T2 Стандарт

- Все условия T1 включены
- Выделенная команда
- Поиск недостатков в конфигурациях
- Пакет экспертизы «Расширенный»
- Индивидуальные правила корреляции
- Подключение нетиповых источников
- Мониторинг актуальных типов угроз (TH/TI)
- Рекомендации по улучшению защиты

## SOC in-house

### T3 Кастомный

- Все условия T2 включены
- Разработка архитектуры SOC
- Внедрение и сопровождение партнерских решений
- Адаптация правил под потребности заказчика
- Обучение сотрудников заказчика
- Выстраивание индивидуальных процессов реагирования
- Прогнозирование угроз

# НАШ ПОДХОД

### Сбор событий

- Фиды
- Виртуальные машины
- Приложения
- Базы данных
- СЗИ
- Пользовательские хосты

### Проактивное реагирование

- Личный кабинет
- Расследование и форензика
- Purple Team
- Оповещение
- Повышение осведомленности
- Контроль инцидентов

### Анализ

- Быстрое подключение
- Анализ защищенности
- Сканер уязвимостей
- Детекты
- Threat Hunting
- Оптимизация SIEM

# ПОЧЕМУ МЫ?

- ✓ Полный цикл мониторинга и реагирования
- ✓ Команда с реальным опытом расследования сложных инцидентов
- ✓ Поддержка всех линий – L1, L2, L3
- ✓ Работа с любыми вендорами
- ✓ Адаптация под различные инфраструктуры
- ✓ Соответствие стандартам – ГОСТ 57580, 187-ФЗ
- ✓ Включение в процессы заказчика через API, CMDB, тикет-систему

125040, г. Москва, ул. Вавилова, д. 47А

+7 (499) 705-76-57

info@solidlab.ru

Группа компаний SolidLab работает в области информационной безопасности более 10 лет, защищая организации от киберугроз, предупреждая атаки, минимизируя риски финансовых и репутационных потерь. SolidLab предлагает полный комплекс услуг: от пентестов до защиты приложений, реагирования на инциденты и организации процессов SDLC.