SOC – Кому и зачем?

Денис Поршин
Руководитель отдела кибербезопасности в СФО

Софтлайн сегодня и завтра

Softline – лидирующий глобальный поставщик ИТ-решений и сервисов, работающий на рынках восточной Европы, центральной Азии, Америки, Индии и Юго-Восточной Азии.

1 миллиард $
оборот в FY2016

3800+
сотрудников в группе компаний

3000+
реализованных проектов

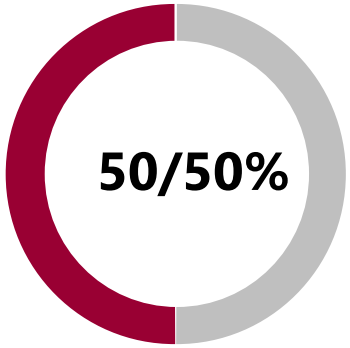
+39%
среднегодовой темп роста
за последние 10 лет в рублях

25 лет
на IT-рынке

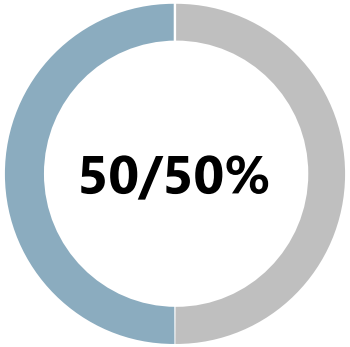
Представительства в
30 странах
80 городах

500+
инженеров и разработчиков

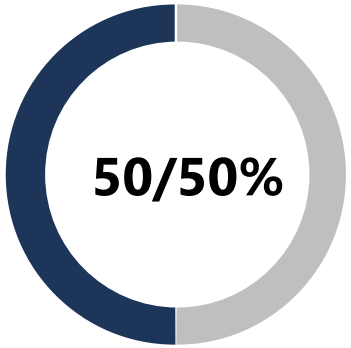
Стратегия 2017-2019



Россия – вне России



Сервисы – Поставки



Облака – не облака

Наши заказчики

Глобальные компании

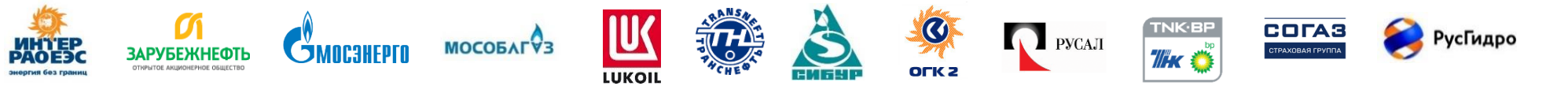
Крупные корпоративные клиенты

Средний и малый бизнес

Госорганизации

Образование и Здравоохранение

Промышленность



Экспертиза в кибербезопасности

Структура

- SL Solution - интеграция
- Axsoft - дистрибуция
- Учебный Центр (№1 в корп. обучении)
- Аттестационная лаборатория
- Разработка средств защиты (бренды Стахановец - OEM модуль в InfoWatch, PhishMan)
- SOC worldwide

Сервисы

- консалтинг и аудит
- проектирование
- внедрение
- соответствие требованиям
- поддержка 24*7*365
- обучение
- безопасность как сервис

Факты

- Топ 2 рейтинга CnewsSecurity 2013-2017
- 9% - интеллектуальная составляющая
- 150+ специалистов
- Сильнейшие компетенции:
  - CheckPoint
  - Лаборатория Касперского
  - Инфотекс
  - Код Безопасности
  - Solar Security
  - InfoWatch
  - Positive Tech.

- Защита онлайн-сервисов
- Защита веб и почты
- Защита инфраструктуры
- Управление доступом
- Защита от мошенничества
- Защита от направленных атак
- Безопасность промышленных систем
- Защита данных
- Защита сети
- Импортозамещение
- Обеспечение соответствия требованиям
- Центры реагирования ИБ (SOC)

СТАТИСТИКА

Чем раньше будет выявлена угроза, тем меньше будут затраты на ликвидацию ее последствий.

По данным Kaspersky Lab и Positive Technologies, угрозу обнаруживают почти сразу только в 8,19% случаев. Обычно на это требуются сутки (20,58%), несколько дней (28,64%) или даже недель (19,08%).

Зачем нужен SOC

SOC

Центр мониторинга и реагирования на инциденты информационной безопасности

сложный комплекс технических средств, выстроенных процессов и профильных специалистов

Цели

- Снижение рисков хищения данных и денежных средств, прерываний в деятельности бизнеса
- Снижение тяжести последствий инцидентов

Задачи

- Контроль состояния IT-инфраструктуры
- Проактивное предотвращение инцидентов
- Автоматизация процессов управления инцидентами
- Расследование инцидентов

Преимущество аутсорсинга SOC

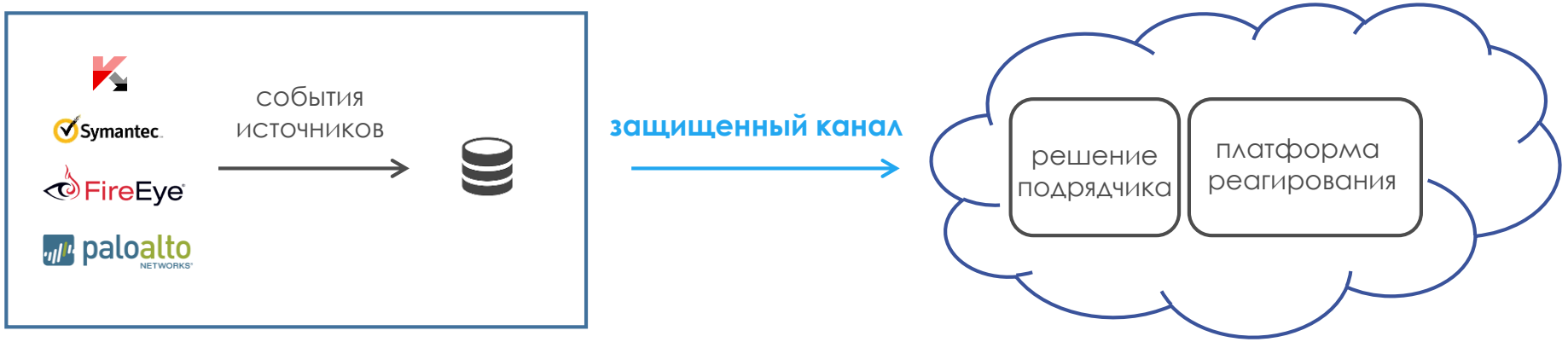
- Предсказуемые затраты и сроки на внедрение
- Нет необходимости в собственной дорогостоящей инфраструктуре для управления инцидентами
- Решение кадровых проблем
- Перенос ответственности за качество сервиса
- Автоматизация рутинных действий по обеспечению ИБ
- Получение своевременных сведений об угрозах и уязвимостях

Сервис SOC

- Мониторинг и реагирование 24/7
- Более 25 экспертов в команде SOC
- Выявление инцидентов с помощью настраиваемых механизмов анализа событий
- Автоматическое реагирование на типовые инциденты
- Регулярная отчетность

Варианты реализации

Облачная

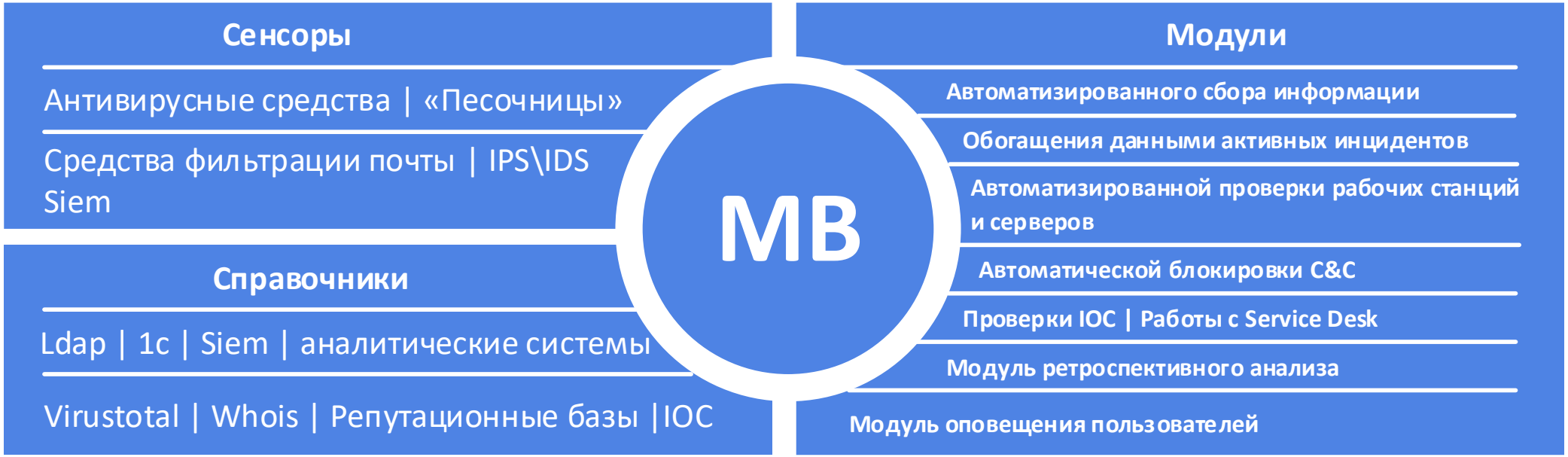


Смешанная

Сравнение SOC Infosecurity

СЕРВИСЫ	INFOSECURITY	Другие SOC
Мониторинг событий ИБ	V	V
Выявление инцидентов ИБ	V	V
Реагирование на инциденты ИБ	V	Только оповещение
Автоматическое блокирование угроз	V	X
Компьютерная криминалистика	V	Только аналитика, без сбора юридически значимых доказательств

Автоматизация. Messila Bot



Пример инцидента

Фильтр: Заблокирован запуск потенциально опасного ПО

IP компьютера	10.10.10.10
FQDN комьютера	COMPUTER.DOMAIN.RU
Домен	DOMAIN.RU
Время обнаружения инцидента	2017-06-26T16:31:17
Фактическое время блокировки	2017-06-26T00:00:00
Исполняемый файл	c:\klpd\klpd.exe
MD5 сумма	c9a5d0ae656a3d970eb29dda7dc969f2
SHA256 сумма	c112ab629fb3ab68ea1977ed40590fa0588c6fc479beb9448e2f5c1fafdc2e0d
Вердикт VT	13
Описание от сенсора	Зафиксированны не заблокированные SRP подозрительные объекты.

Инфо по пользователям

IP адрес	10.10.10.10
Имя пользователя	Иванов Иван Иванович
Аккаунт	ivanov_ii
Email	ivanov@domain.ru
Департамент	Финансовый отдел
Номер телефона	12-3456

Процедура реагирования

Мониторинг :

- Установить назначение ПО, письмо пользователю из этой заявки (шаблон письма: На вашем ПК был заблокирован запуск потенциально опасного ПО. Прошу предоставить информацию о [имя_файла] и уточнить было ли согласовано его использование.)
- Выкачать образец с хоста и положить в папку для отправки в антивирусные лаборатории
- Перевести в очередь SOC

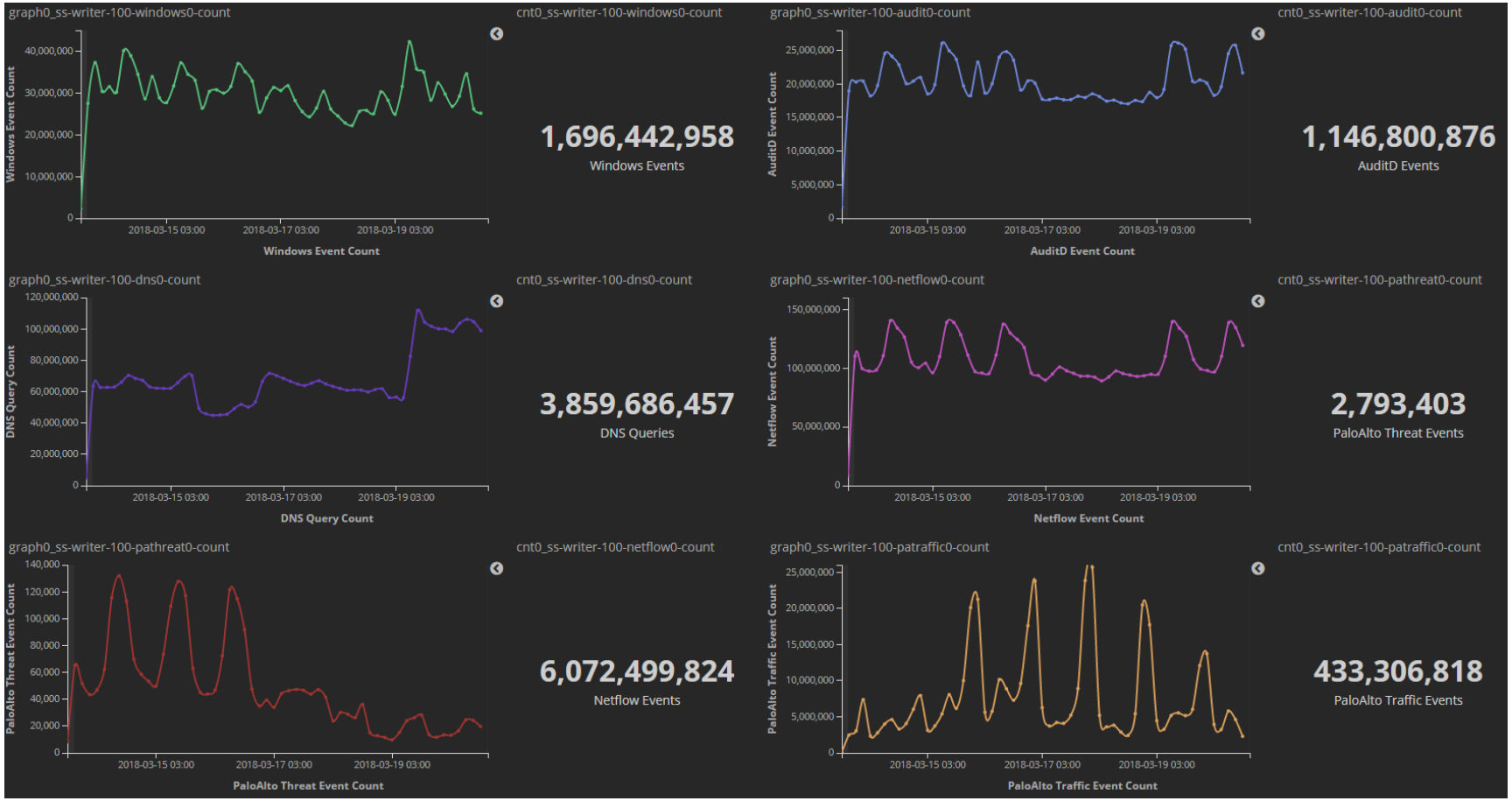
SOC :

- Принять решение об опасности для инфраструктуры

В случае опасности

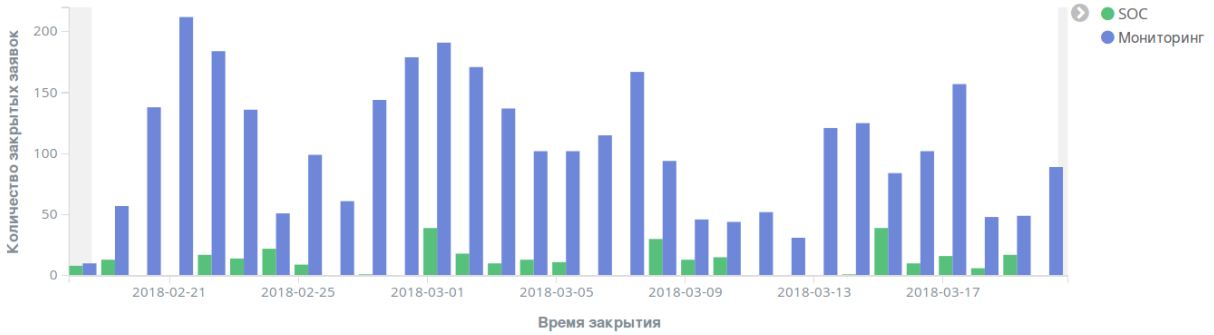
- Удалить указанный образец
- Выявить путь проникновения на рабочую станцию
- Оценить последствия запуска вредоноса
- Выполнить внеплановое сканирование

СРЕДСТВА КОНТРОЛЯ



КОНТРОЛЬ МЕТРИК

otrs-mon-soc-bar



otrs-mon-soc-metric

filters	Количество закрытых заявок
SOC	322
Мониторинг	3,303
	3,625

otrs-mon-soc-services

SOC: filters

Имя сервиса	Количество заявок	Затраченное время (мин)
Разбор инцидентов ИБ	238	4,201
SOC::Контроль сетевого доступа	45	824
SOC::Анализ malware. KES	20	438
SOC::Анализ угроз (TDS)	19	1,337
SOC::Анализ угроз (FireEye NX)	15	337
SOC::Мониторинг инфраструктуры SOC	15	245
SOC::Анализ malware (FireEye EX)	12	336
SOC::Анализ malware.SEP	6	124

Мониторинг: filters

Имя сервиса	Количество заявок	Затраченное время (мин)
Антивирусная защита (AV)	1,030	7,870
SOC::Контроль целостности на серверах (Tripwire)	819	5,489
SIEM (Arcsight/Kibana/Bot-Trek)	305	3,175
SOC::Контроль доступа на сервера (AcrSight)	265	1,973
Управление политиками на АТМ	189	2,883
Контроль изменений::Tripwire	136	1,125
SOC::Мониторинг инфраструктуры SOC	131	1,534
SOC::Контроль операций в прикладных системах (AcrSight)	120	690

Пилот

КЕЙСЫ

Обнаружить несанкционированное повышение привилегий

Обнаружить невылеченный вредоносный код

Обнаружить malware-эпидемию

ПРОДЕМОНСТРИРУЕМ

Дашборды по логам и инцидентам

Оперативное оповещение об инциденте

Отчет по разбору инцидента

Аналитические запросы

Работу MessilaBot

ОТ КЛИЕНТА НУЖНО

1. Заполнить анкету по инфраструктуре
2. Вместе с нами настроить VPN-канал
3. Предоставить сетевые доступы и аппаратные мощности
4. Настроить инфраструктуру и прикладную часть серверов
5. Предоставить данные для мониторинга
6. Сгенерировать тестовые события

СРОК: 7-8 НЕДЕЛЬ

GO GLOBAL

GO CLOUD

GO INNOVATIVE