Анатомия SOC

Дрюков Владимир
Руководитель Solar JSOC

SOC – модель для исследования

Несколько слов о мониторинге

- Гибко – блокировать можно не всегда:
  - Нельзя отобрать права локального админа у ИТ – а контролировать их надо усиленно
  - Удаленный доступ из-за границы бывает – но только в редких командировках
- Необходимо – одной активной блокировки недостаточно:
  - NGFW заблокировал бота на ноутбуке пользователя – он придет домой, там нет NGFW
  - Антивирус не дал поставить mimikatz злоумышленнику – он запустит аналог на powershell
- Прозрачно – понимание взаимосвязей систем и активности пользователей
  - Админы вывели новый хост на периметр – а обсудить с ИБ забыли
  - Учетная запись в ОС и запущенном приложении от разных пользователей – повышение полномочий с возможным мощенничеством

Задачи со звездочкой к мониторингу

- Условия - внешний сайт компании, актуальность патчей - неизвестна.
  «Китайские» сканеры создают 3000 срабатываний IDS в секунду.

Вопрос - На какие реагировать, как определить фактическую атаку?

- Условия - ИТ-администраторы за вчерашний день запустили 15 новых серверов инфраструктуры. Антивирус установлен на 3.

Вопрос - Как детектировать до первого инцидента?

- Условия - ИТ вместе с бухгалтерией придумали «удобный способ» передачи платежных документов из ERP в банк-клиент – через папку файлового сервера.

Вопрос - Как про это узнать, пока не стало поздно?

Контроль защищенности

Задача – понимать ключевые «болевые точки» инфраструктуры:

- Уязвимости;
- Покрытие инфраструктуры СЗИ;
- Корректность настроенных политик;
- Отлаженность процесса реагирования на инциденты;
- Защищенность ключевых бизнес-процессов;

Инструменты:

- Сканеры;
- Network policy management;
- Отчеты SIEM и СЗИ;
- Пентесты;
- Коммуникация с бизнесом, ИТ и работа с рисками

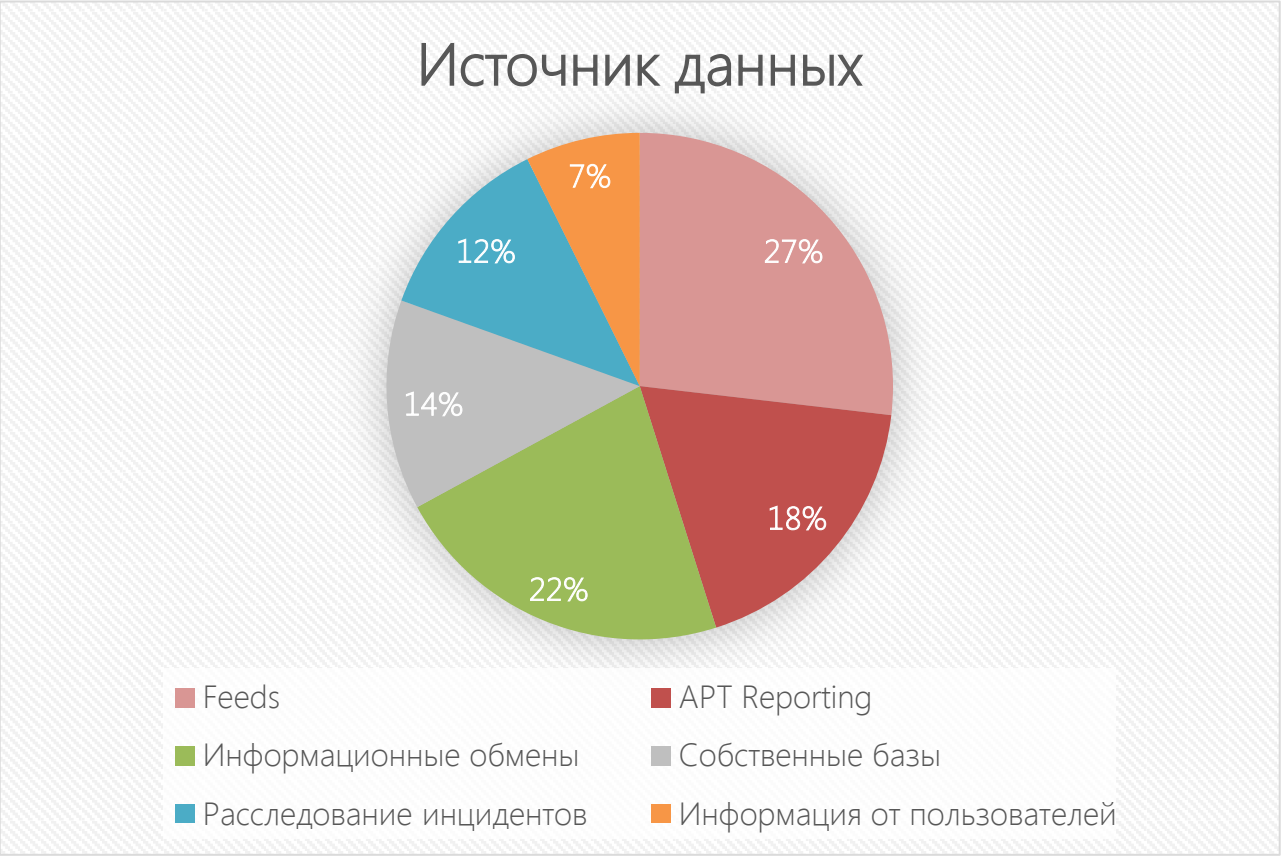
Кто владеет информацией…

- Перечень центров управления ботсетями вирусов-шифровальщиков
- Индикаторы нового вредоносного ПО, еще не выявляемое антивирусами
- Сводка о последних атаках на отрасль – какие векторы и ПО используются?
- Список скомпрометированных и продаваемых в сети учетных записей компании
- Топ уязвимостей и exploit, которые скачивают и изучают хакеры

Threat Intelligence

- Источники:
  - Платные широковещательные – антивирусные, сетевые и многие другие вендоры
  - Платные узконаправленные – центры противодействия и расследования инцидентов, коммерческие CERT, исследовательские лаборатории
  - Информационные обмены – CERT России (Fin-Cert, Gov-Cert), клубы по интересам
  - Собственные исследования – если есть возможность
  - Бесценные – обращения пользователей ☺
- Задача:
  - Критичное и однозначно опасное – заблокировать превентивно;
  - Широковещательное – мониторить;
  - Недоступное для мониторинга – поставить на периодический контроль

Threat Intelligence – статистика JSOC



SOC запущен. Как оценивать работу?

Возникающие вопросы:

- Инцидентов стало больше/меньше, чем месяц назад. Почему, с чем это связано?
- Много нарушений политик ИБ. Каких именно, какое подразделение наиболее подвержено?
- В инфраструктуре появляются 0day вирусы. Нужно купить sandbox или заняться awareness?
- На защиту какой бизнес-системы нужно направить свое внимание?
- Насколько быстро мы выявляем и блокируем атаку?

Цели:

- Планирование стратегии ИБ и эффективное бюджетирование систем
- Обоснование внесенных в SOC инвестиций
- Защищенность ключевых бизнес-процессов
- Оперативный контроль состояния ИБ

Советы «собратьям по оружию»

- Копите знания об атаках:
  - Обмен с коллегами
  - CERT-ы и ведомства
  - Платные подписки
- Не игнорируйте заблокированные инциденты:
  - Заблокированная активность – признак действий нарушителя
  - Не получилось сразу – будет искать другой путь
  - «Найти и обезвредить»
- Понимайте, что вы защищаете:
  - Идентифицируйте, где «болит»
  - Поймите, как защитить
  - Следите максимально внимательно
- Выстраивайте взаимодействие с бизнесом
- Создавайте красивые и правдивые отчеты ☺
- Подключайте к борьбе сильных союзников

Ваши вопросы?

Инцидент 1

Фиксация инцидента:

- Обнаружено обращение к ip C&C с АРМ сотрудника расчётного центра
- АРМ имеет доступ к работе с отчетностью МЦИ – инцидент высокой критичности
- Эвристика по АРМ установленным антивирусом результата не дала
- Проверка альтернативным антивирусом выдала вердикт – Обнаружен PDM:Trojan.Win32.Generic
- Приступили к исследованию машины и вредоноса

Итоги разбора:

- Вредоносное ПО, маскирующееся под системный процесс sys.exe
- Установлен при запуске файла skazki_dlya_bolshih_i_malenkih.pdf.exe
- Функционал
  - Снимки экрана каждые 5 минут
  - Запись клавиатурных вводов
  - Отправка всех данных через прокси на центр управления (не активирована)
- Компрометация
  - Все учетные данные пользователя
  - Учетная запись руководителя
  - Три учетные записи администраторов

Инцидент 2

Фиксация инцидента:

- Обнаружен запуск процесса procdump.exe на машине сотрудника службы взыскания
- ProcDump is a command-line utility whose primary purpose is monitoring an application for CPU spikes and generating crash dumps during a spike that an administrator or developer can use to determine the cause of the spike
- А еще используется киберпреступниками для компрометации паролей пользователей
- Пользователь ПО не запускал

Итоги разбора:

- Проникновение – через 0day-вложение
- Первое закрепление, получение прав локального администратора
- Попытка компрометации пароля help desk через запуск procdump
- Дальнейшие действия
  - Анализ 0day-вируса, выявление индикаторов компрометации
  - Проверка инфраструктуры на следы похожего вредоносного ПО (сеть и хосты)
  - Выявлено еще две скомпрометированные машины, проведена очистка сети

Инцидент 3

Фиксация инцидента:

- Зафиксировано подключение к Windows серверу СУБД АБС под учетной записью ИТ-специалиста поддержки
- Учетная запись с доступом на все хосты, но специалист поддержки отвечает за UNIX
- Пользователь не подтвердил попытку доступа
- Вывод – учетная запись скомпрометирована

Итоги разбора:

- Локализация атаки показала:
  - Найдена машина не в домене
  - На машине нет антивируса
  - Располагается на месте одного из сотрудников поддержки
- Внутренний злоумышленник
- Личный ноутбук с хакерскими утилитами, подключение к сети через подмену MAC
- Скомпрометированы:
  - Учетная запись системы мониторинга
  - 4 учетные записи администраторов
  - Около 20 хостов в инфраструктуре