3/5 правил жизни SOC

Антон Юдаков
Head of Operations - Solar JSOC

На одном слайде про Solar JSOC

39 крупных коммерческих клиентов	**60** специалистов по ИБ в штате	**5** лет оказания услуг
99,4% общая доступность сервиса	**10 мин** Время реакции на инцидент	**30 мин** Время анализа/ противодействия

МТС Банк

НСПК
НАЦИОНАЛЬНАЯ СИСТЕМА ПЛАТЕЖНЫХ КАРТ

БАНК САНКТ-ПЕТЕРБУРГ

Уральский Банк реконструкции и развития

media

Тинькофф

ПОЧТА БАНК

Что такое SOC?

Хабрахабр Публикации Пользователи Хабы Компании Песочница

193,25
Рейтинг

Solar Security
Безопасность по имени Солнце

SolarSecurity 15 ноября в 12:38

Собери свой Security Operation Center из 5 элементов

Управление проектами, Информационная безопасность, Занимательные задачки, SaaS / S+S, Блог компании Solar Security

Привет, Хабр!

Мы тут часто пишем о том, что работа центра мониторинга и противодействия кибератакам невозможна без определенных процессов (мониторинг, реагирование, расследование инцидентов и т.д.) и, конечно, без систем защиты (AV, WAF, IPS и т.д.).

То же самое мы объясняем заказчикам, но они, быстро пересчитывая деньги в кармане, иногда в ответ спрашивают: "А можно нам SOC в базовой комплектации?"

Предлагаем вам представить себя на месте такого заказчика. Под катом 26 аббревиатур и терминов. Проверьте, насколько вы понимаете принципы мониторинга и противодействия кибератакам и выберите всего 5 буквосочетаний, которые смогут надежно защитить компанию.

https://habrahabr.ru/company/solarsecurity/blog/342386/

Что такое SOC?

Хабрахабр Публикации Пользователи Хабы

193,25
Рейтинг

Solar Security
Безопасность по имени Солнце

SolarSecurity 15 ноября в 12:38

Собери свой Security Operati элементов

Управление проектами, Информационная безопасность, Занимательн

Привет, Хабр!

Мы тут часто пишем о том, что работа центра мониторинг невозможна без определенных процессов (мониторинг, ре т.д.) и, конечно, без систем защиты (AV, WAF, IPS и т.д.).

То же самое мы объясняем заказчикам, но они, быстро пе спрашивают: "А можно нам SOC в базовой комплектации?

Предлагаем вам представить себя на месте такого заказч Проверьте, насколько вы понимаете принципы мониторин выберите всего 5 буквосочетаний, которые смогут надежн

Пн 20.11.2017 14:10

Лезина Наталья

Опрос "Собери свой SOC из 5 элементов"

Привет, коллеги.

Ниже результаты нашего опроса. Всего проголосовало 114 человек.

Варианты	Количество проголосовавших	%
SIEM (Security information and event management)	85	74,6
IPS/IDS (Intrusion Prevention System/ Intrusion Detection System)	72	63,2
AV (Antivirus)	57	50,0
WAF (Web Application Firewall)	41	36,0
DLP (Data Leakage Prevention)	35	30,7
LM (Log Management)	35	30,7
CSIRT (Cyber Security Incident Response Team)	28	24,6
ADDoS (Anti DDoS)	26	22,8
EDR (Endpoint Detection and Response)	22	19,3
RVM (Risk & Vulnerability Management)	21	18,4
IR (Incident Response)	21	18,4
Pentest (Penetration test)	17	14,9
UEBA (User Behavior & Entity Analysis)	15	13,2
CCM (Change & Configuration Management)	14	12,3
TI (Threat Intelligence)	14	12,3
CERT (Computer Emergency Response Team)	12	10,5
MA (Malware Analysis)	11	9,6
AM (Asset Management)	8	7,0
BI/SI (Business Intelligence/Security Intelligence)	7	6,1

SOC – общая модель

Правила жизни SOC – о чем пойдет речь

- Сложность и сроки построения/подключения SOC
- Работа с контентом – какими должны быть инциденты
- Работа с TI (Threat Intelligence)

Сложность построения/подключения SOC

- **Задача – ~~завтра, сегодня,~~ вчера нужен SOC (быстрый старт):**
  - Типовой ответ интегратора – консалтинговый проект, построение SOC за… 3-5 лет.
  - Типовые опасения Заказчика – долго, дорого, сложно, готовы двигаться, но, похоже, потребуется повторное согласование с руководством.
  - Типовой результат – у нас нет SOC, ни своего, ни внешнего :(

Сложность построения/подключения SOC

- **Задача – ~~завтра, сегодня,~~ вчера нужен SOC (быстрый старт):**
  - Типовой ответ интегратора – консалтинговый проект, построение SOC за… 3-5 лет.
  - Типовые опасения Заказчика – долго, дорого, сложно, готовы двигаться, но, похоже, потребуется повторное согласование с руководством.
  - Типовой результат – у нас нет SOC, ни своего, ни внешнего :(

- **Подключаем внешний SOC? Опасения со стороны Заказчика:**
  - Честно, мы не знаем всего, что у нас есть и чего мы сейчас хотим.
  - SOC ничего про нас не знает, наверное, мы хотим очень аккуратно запускаться…
  - Сейчас придет SOC, запустит свои 250+ сценариев и… нам конец.

Сложность построения/подключения SOC

- **Как решить – запускаем параллельно:**

  1. Краткое обследование-инвентаризацию в формате бизнес-интервью, чтобы понять, как выглядит инфраструктура Заказчика «в крупную клетку», что реально «болит», где хранится самое важное, где возможны проблемы и т.д.

  На выходе: понимание инфраструктуры, какие сценарии нужны, какие подсистемы кроме базовых нужно подключать -> Roadmap.

  2. Подключение базовых подсистем с целью увидеть пусть и не полную, но целую картину. Накладываем карту сети.

  На выходе: немного структурировали хаос, уже что-то видим.

  3. Профилирование. Включаем сценарии для накопления статистики, смотрим неделю-две-месяц, согласовываем выборки с Заказчиком.

  На выходе: начинаем видеть только то, что хотим выявлять.

Длительность построения/подключения

- **Сколько времени нужно на запуск?**
  - На практике бутылочное горлышко – сам Заказчик.
  - Вернее, Заказчик и всё, что рядом (подрядчики, вендоры и т.д.).
- **На практике:**
  - В среднем подключение занимает 1-2 мес., далее – Roadmap.
  - Рекорд – 3 дня, но это был особый подвиг :)
  - В среднем по Roadmap 3 слой (бизнес-приложения) – через 5-6 мес.

- **Советы:**
  - Понимайте, что вы защищаете:
    - Идентифицируйте, что «главное» и где «болит».
    - Поймите, как защитить.
    - Следите максимально внимательно.
  - Выстраивайте взаимодействие с бизнесом.

Продолжаем…

- Сложность и сроки построения/подключения SOC
- Работа с контентом – какими должны быть инциденты
- Работа с TI (Threat Intelligence)

Работа с контентом

- Правила «из коробки» работают в «сферической» инфраструктуре.

- Необходимо группирование и унифицирование сценариев:
  - Логика инцидентов и их разбора одинакова – brute-force всегда brute-force вне зависимости от того, Windows/Unix/VPN/Application.
  - Одна атомарная атака = 1 инцидент (30,40,50 попыток эксплуатации уязвимости должны быть собраны и сопоставлены).

- Длинные цепочки корреляции низкоэффективны.
- Короткие цепочки генерят очень много FP, необходимо эффективно фильтровать.

См. 17:40 – 18:00 Жевнерев Максим, Сессия 8, Свой SOC, шаг за шагом.
Тема: Архитектура и методология разработки сценариев в SOC. **Зал 2.**

Работа с контентом: от подозрения к инциденту

Базовые сценарии (косвенные признаки)	Потенциальный инцидент
Входящее письмо от неизвестного отправителя	Почти 100% заражение хоста Вероятный целенаправленный взлом хоста
Запуск нелегитимного ПО (процесса) на рабочей станции	
Исходящая активность Remote Access Tools\TOR\Feeds	
Создание локального администратора на системе	
Модификация реестра по снятию ограничений RDP на хосте	
Большое кол-во неуспешных подключений во внешнюю сеть	Вероятные ботнеты\неизвестные вирусы
Доступ в интернет к известным опасным хостам (Feeds) \ подозрительные категории на прокси	
Исходящая попытка установить соединение удаленного администрирования	
Доступ к критичной информации (файл\база\etc)	Утечка информации
Использование учетных записей отсутствующих сотрудников	
Обнаружение передачи архива с паролем (DLP)\Отправка большого объема данных через веб-почту	
Обнаружение нового хоста во внешнем периметре	Успешный взлом внешнего сервиса
Внешнее сканирование портов	
Успешная аутентификация с не разрешенного сегмента сети (на сервис ***)	
Исходящая сетевая активность от критичного сервера к не доверенным хостам	

Работа с контентом

- **Советы:**
  - Не игнорируйте заблокированные инциденты:
    - Заблокированная активность – признак действий нарушителя.
    - Не получилось сразу – злоумышленник будет искать другой путь.
  - Не игнорируйте повторяемые инциденты:
    - Практически у каждого из них есть Root Cause, очень часто процессного характера.
  - Определитесь с форматом уведомлений:
    - Если риск FP минимален и сбор дополнительной информации возможен в автоматизированном режиме, нужна ли 1 линия?
    - Если, кроме того, информация по типу инцидента обрабатывается «пачкой», нужна ли 1 линия?

Продолжаем…

- Сложность и сроки построения/подключения SOC
- Работа с контентом – какими должны быть инциденты
- Работа с TI (Threat Intelligence)

Несколько слов о кооперации

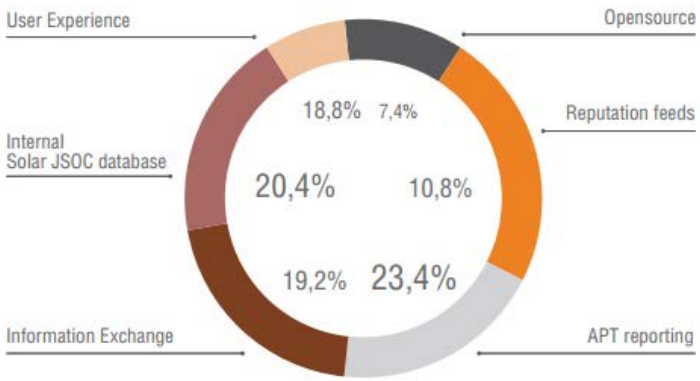
- **Кто владеет информацией?**
  - Перечень центров управления ботсетями вирусов-шифровальщиков.
  - Индикаторы компрометации нового или модифицированного вредоносного ПО, еще не выявляемого АВПО.
  - Сводка о последних атаках на отрасль – какие векторы и ПО используются?
  - Топ уязвимостей, эксплоитов и легитимного ПО, используемых хакерами.

- **Советы:**
  - Копите знания об атаках:
    - Новости по угрозам/ресерчам, сценариям/векторам атак.
    - Обмен с коллегами, CERT-ами и ведомствами.
    - Платные подписки.

Threat Intelligence кажется простым…

- **TI – источники:**
  - Платные широковещательные – антивирусные, сетевые и другие вендоры.
  - Платные узконаправленные – центры противодействия и расследования инцидентов, коммерческие CERT, исследовательские лаборатории.
  - Информационные обмены – CERT России (ФинЦЕРТ, GOV-CERT), клубы по интересам.
  - Собственные исследования – если есть возможность.
  - Бесценные – обращения пользователей :)

Статистика по использованию разных типов Intelligence в детектировании инцидентов



… но это не так

- **Советы:**
  - Не используйте в SOC все существующие фиды и IoC, анализируйте их «качество».
  - При анализе основное внимание обращайте на контекст (наличие расширенной информации по угрозам).
  - Работайте с фидами и IoC правильно:
    - Анализируйте релевантность индикаторов.
    - Проверенное добавляйте в real-time мониторинг.
    - Проводите ретроспективный поиск.
    - Критичное и однозначно опасное блокируйте превентивно.
    - Недоступное для мониторинга ставьте на периодический контроль.

    - Проверяйте на себе и своем контенте, если есть возможность.

Советы в заключение

- Когда SOC запущен:
  - Оценивайте его работу:
    - Количество инцидентов сейчас и месяц назад. Почему, с чем это связано?
    - Насколько быстро мы выявляем и блокируем атаку?
  - Планируйте движение по стратегии ИБ, осуществляйте эффективное бюджетирование систем:
    - На защиту какой бизнес-системы нужно направить свое внимание?
    - В инфраструктуре появляются 0-day вирусы. Нужно купить sandbox, заняться vulnerability management или security awareness?
- Выстраивайте взаимодействие с бизнесом.
- Подключайте к борьбе сильных союзников.

Спасибо за внимание!

Антон Юдаков,
CISSP, CISM

Head of Operations - Solar JSOC