Этапы построения центра мониторинга и реагирования на инциденты ИБ

Прозоров Андрей, CISM
Руководитель экспертного направления
Компания Solar Security

Мой блог: 80na20.blogspot.com
Мой твиттер: twitter.com/3dwave

2017-02

О чем эта презентация?

I. Немного вводной информации про SOC
II. SOC по ФСТЭК России
III. Рекомендации про построение центра мониторинга и реагирования на инциденты ИБ

Базовый термин

Мониторинг: *Систематическое или непрерывное* ***наблюдение*** *за объектом с обеспечением контроля и/или* ***измерения его параметров****, а также* ***проведение анализа*** *с целью предсказания изменчивости параметров и принятия решения о необходимости и составе корректирующих и предупреждающих действий.*

ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»

Мониторинг

SOC

- Измерение ИБ (общее)
- …

- Анализ угроз и рисков
- Анализ уязвимостей ИС
- Анализ кода приложений
- Анализ прав доступа
- Управление событиями ИБ
- Тестирование на проникновение
- Контроль устранения ранее выявленных уязвимостей
- Контроль выполнения требований (тех.аудит)
- …

- Администрирование СЗИ
- Обучение и повышение осведомленности
- **Управление инцидентами**
- …

Отчеты по инцидентам ИБ

JSOC Security flash report Q3 2016

Отчет содержит информацию о выявленных инцидентах, разбитую по категориям, в зависимости от того, кто, как, в какое время и с использованием каких технологий реализовывал угрозы. Отчет содержит данные за третий квартал 2016 года.

Скачать

JSOC Security flash report Q2 2016

Отчет содержит информацию о выявленных инцидентах, разбитую по категориям, в зависимости от того, кто, как, в какое время и с использованием каких технологий реализовывал угрозы. Отчет содержит данные за второй квартал 2016 года.

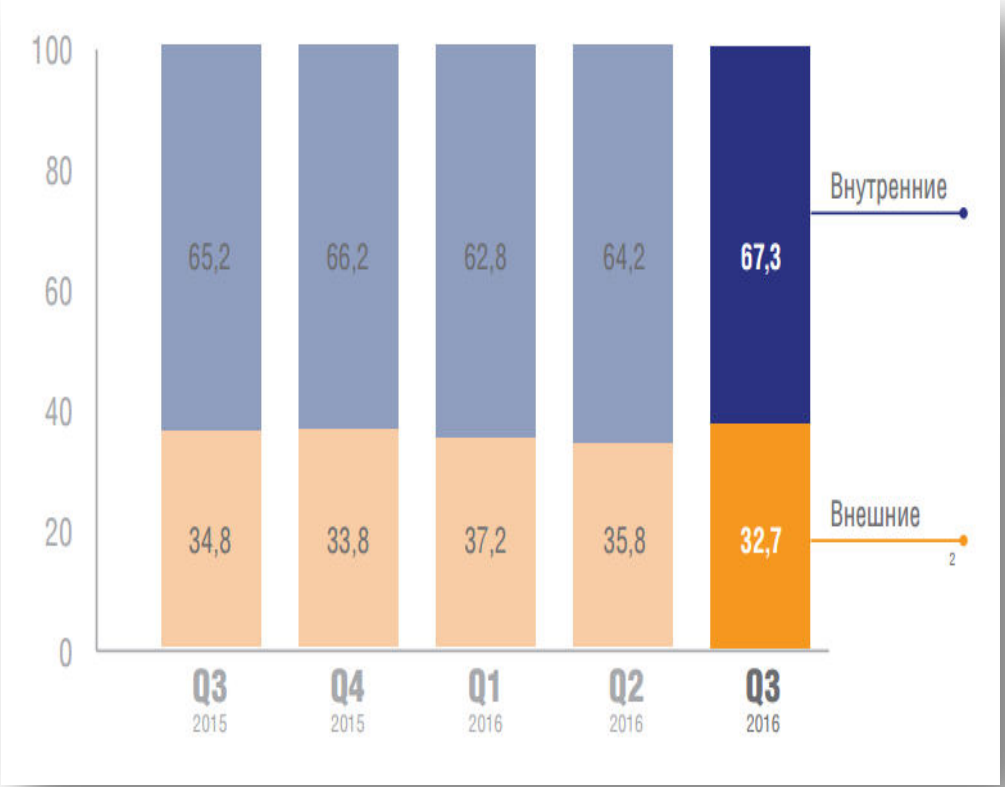
Скачать

JSOC Security flash report Q1 2016

Отчет содержит информацию о выявленных инцидентах, разбитую по категориям, в зависимости от того, кто, как, в какое время и с использованием каких технологий реализовывал угрозы. Отчет содержит данные за первый квартал 2016 года.

Скачать

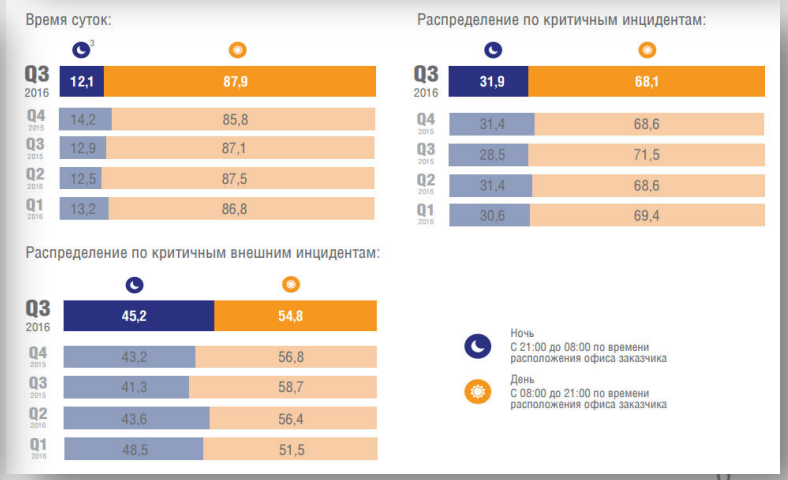
http://solarsecurity.ru/analytics/reports/


100
80
60
40
20
0
65,2
66,2
62,8
64,2
67,3
34,8
33,8
37,2
35,8
32,7
Внутренние
Внешние
Q3 2015
Q4 2015
Q1 2016
Q2 2016
Q3 2016


Направления атак
Прочие внешние атаки: атаки на сетевой стек, уязвимости DNS, нарушение защищенного периметра, уязвимости управляющих протоколов, фишинг
DDoS
Атаки на управляющие протоколы систем
Компрометация административных учетных записей
Атаки на веб-приложения
Brute-force и компрометация учетных данных внешних сервисов клиента
17,2
3,6
6,2
3,7
39,2
30,1
Q3
2016


Направления атак
Утечки конфиденциальных данных
Несанкционированные активности в рамках удаленного доступа, в том числе построение цепочки сессий до запрещенного сервера, выгрузка данных на внешний компьютер
Нелегитимные работы под привилегированными учетными записями: внутренние пользователи
Нелегитимные изменения в ИТ-системах: деятельность аутсорсеров и подрядчиков, в том числе несогласованные работы, приводящие к простою критичных бизнес-систем
Нарушение политик доступа в интернет, в том числе использование TOR-клиентов, анонимайзеров и посещение хакерских форумов
Вирусные атаки, включая массовые вирусные заражения, действия ransomware и поведенческое выявление zero-day
Прочее
Компрометация внутренних учетных записей
0,6
4,2
5,2
3,7
9,3
21,2
20,4
35,4
Q3
2016


Аутсорсеры, контрагенты, подрядчики
Внутренние штатные администраторы
Прочие внутренние пользователи
Q3 2016 8,9 24,7 66,4
Q4 2015 9,2 24,8 66
Q3 2015 11,3 23,6 65,1
Q2 2016 9,3 25,2 65,5
Q1 2016 10,4 22,2 67,4


Время суток:
Q3 2016 12,1 87,9
Q4 2015 14,2 85,8
Q3 2015 12,9 87,1
Q2 2016 12,5 87,5
Q1 2016 13,2 86,8
Распределение по критичным инцидентам:
Q3 2016 31,9 68,1
Q4 2015 31,4 68,6
Q3 2015 28,5 71,5
Q2 2016 31,4 68,6
Q1 2016 30,6 69,4
Распределение по критичным внешним инцидентам:
Q3 2016 45,2 54,8
Q4 2015 43,2 56,8
Q3 2015 41,3 58,7
Q2 2016 43,6 56,4
Q1 2016 48,5 51,5
Ночь
С 21:00 до 08:00 по времени расположения офиса заказчика
День
С 08:00 до 21:00 по времени расположения офиса заказчика

Типовые инциденты* (ежедневно)

- Использование TOR на хосте (нарушение правил работы или вредоносное ПО)
- Проблемы с учетными записями (критичные привилегии и группы, кратковременное превышение привилегий, создание во внерабочее время и пр.)
- Обнаружение невылеченных вредоносных объектов на рабочих станциях
- Модификация критичных веток реестра
- Большое количество обнаруженных и невылеченных объектов категории not-a-virus (могут «докачивать» исполняемые файлы)
- Обнаружение индикаторов компрометации Threat Intelligence
- Использование средств удаленного администрирования (teamviewer, ammyy admin)
- Успешные попытки подключения из различных стран в корпоративную сеть
- Подозрительная активность в ночное время, выходные и праздники
- Значительные объемы трафика на различные облачные хранилища и сторонние почтовые серверы
- Очистка журналов аудита
- …

*Из отчетов по инцидентам ИБ, выявленным Solar JSOC, в органах гос. власти и гос.компаниях

Для ИБ важно своевременно:

- обнаруживать **«слабости»** ИБ
- обнаруживать **инциденты** ИБ
- **реагировать** на них

Решение - SOC

- 1я линия (обнаружение)
- 2я линия (расследование и реагирование)
- 3я линия (экспертная поддержка, руководство, юр.вопросы)

Технологии, обеспечивающие:

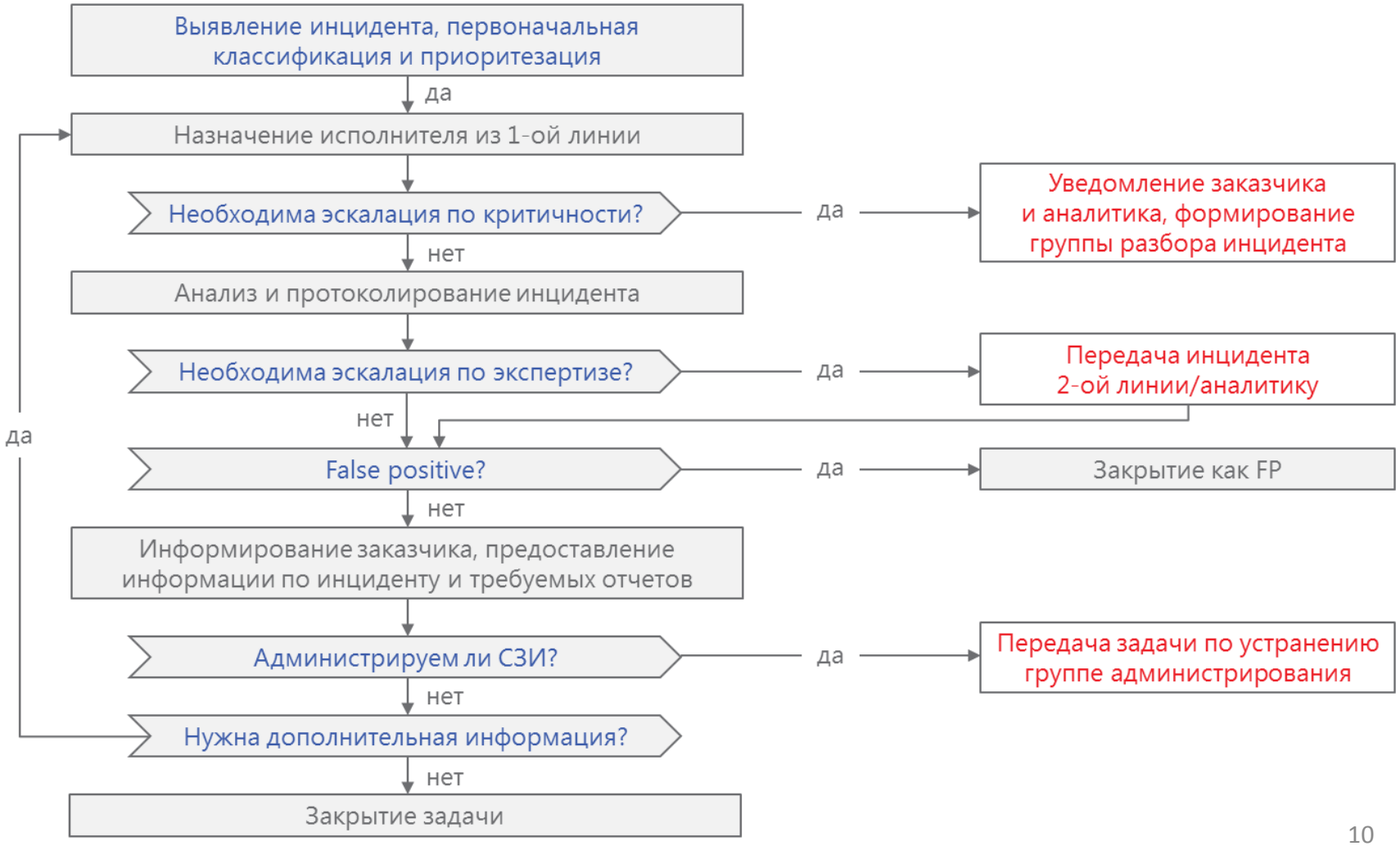
- Взаимодействие персонала
- Инвентаризацию ИС и контроль конфигурации
- Выявление уязвимостей
- Анализ событий ИБ
- Учет и обработку инцидентов
- Управления знаниями

- Анализ кода (прикладное ПО, вредоносное ПО)
- Сбор цифровых доказательств

- СЗИ (МСЭ, IPS, DLP, Sandbox, и пр.)
- …

- Инвентаризация
- Анализ угроз / рисков
- Выявление уязвимостей
- Тестирование на проникновение
- Контроль устранения ранее выявленных уязвимостей
- Контроль выполнения требований (аудит)
- Анализ кода приложений
- Обучение и повышение осведомленности
- Управление событиями ИБ
- Управление инцидентами
- …

Процесс обнаружения и реагирования на инциденты ИБ



SOC в Приказ 17/21/31

V. Регистрация событий безопасности (РСБ)

VII. Обнаружение вторжений (СОВ)

VIII. Контроль (анализ) защищенности информации (АНЗ)

XIV. Обеспечение безопасной разработки прикладного (специального) ПО разработчиком (ОБР)

XVIII. Информирование и обучение персонала (ИПО)

XIX.Анализ угроз безопасности информации и рисков от их реализации (УБИ)

XX. Выявление инцидентов и реагирование на них (ИНЦ)

XXI. Управление конфигурацией автоматизированной системы управления и ее системы защиты (УКФ)

II

Лицензия на ТЗКИ

ПП РФ N 79 «О лицензировании деятельности по технической защите конфиденциальной информации» (с 17.06.2017):

4. При осуществлении лицензируемого вида деятельности лицензированию подлежат:

в) услуги по **мониторингу** информационной безопасности средств и систем информатизации.

По сути, это **новый вид** лицензируемой деятельности…

Оборудование SOC (по ФСТЭК)

- Программное средство контроля целостности программ и программных комплексов
- Система контроля (анализа) защищенности ИС
- Средства, предназначенные для осуществления тестирования на проникновение
- Межсетевой экран уровня веб-сервера
- Межсетевой экран уровня сети
- Средство (средства) антивирусной защиты, предназначенное (предназначенные) для применения на серверах и автоматизированных рабочих местах ИС и средство (средства) их централизованного администрирования
- Система обнаружения вторжений
- Средство автоматизированного реагирования на инциденты ИБ
- Замкнутая система (среда) предварительного выполнения программ (обращения к объектам файловой системы)
- Система управления информацией об угрозах безопасности информации
- Система управления событиями безопасности информации
- Система управления инцидентами ИБ
- Средство (средства) защиты каналов передачи данных

- Информационная система, предназначенная для мониторинга ИБ

Необходима сертификация СЗИ

Необходимо выполнить требования Приказа №17

Типовые проблемы построения SOC

Ресурсные	Организационные
• Нет бюджета • Нет кадров • Отсутствие методологий (рекомендаций) • Отсутствие курсов повышения квалификации • …	• Ориентир на «бумажную безопасность» (compliance) • Слабое взаимодействие с регулятором • Низкий уровень зрелости процессов ИБ (СЗИ закуплены, но практически не используются) • Отсутствие поддержки руководства • Надо срочно… • Не понятно с чего начинать • …

III

Модели SOC

- Тип I: Внутренний (собственный) SOC
- Тип II: Общий (ведомственный) SOC
- Тип III: Внешний SOC (аутсорсинг)

Сравнение моделей SOC

	Тип I	Тип II	Тип III
Причина выбора	Наличие ресурсов и желание все делать самостоятельно	Требование материнской компании / регулятора	Желание оптимизировать ресурсы / их нехватка
Затраты	CAPEX + OPEX, часть затрат может быть скрытым	OPEX (но может быть бесплатно), предсказуемые	OPEX, предсказуемые
Кол-во персонала (Заказчик)	Большое подразделение (3 линии SOC)	1 сервис менеджер	1 сервис менеджер
Скорость запуска	Медленно, надо построить SOC	Быстро, надо подключить услуги	Быстро, надо подключить услуги
Понимание контекста	Высокое	Среднее	Низкое
Режим работы	Обычно 8x5 или 12x5	Обычно 24x7	Обычно 24x7
Доступ к ИС и СЗИ	Внутренний	Внешний	Внешний
Возможности по реагированию и гибкость	Полные	Расширенные	В рамках SLA
Лицензия на ТЗКИ (мониторинг)	Нет	Да	Да

Этапы внедрения SOC

Тип I	Тип II	Тип III
Обоснование бюджета	Обоснование бюджета	Обоснование бюджета
Инвентаризация и аудит	Выбор сервисов	Выбор провайдера и сервисов
Проектирование решения	Согласование требований (SLA) и плана интеграции	Согласование требований (SLA) и плана интеграции
Закупка, внедрение, настройка, обучение персонала. Опытная эксплуатация	Пилотное внедрение	Пилотное внедрение
Перевод в промышленную эксплуатацию	Перевод в промышленную эксплуатацию	Перевод в промышленную эксплуатацию
Оценка и планирование совершенствования	Оценка и планирование совершенствования	Оценка и планирование совершенствования

Важно понимать про SOC

- SOC – это люди, процессы и технологии
- Важно понимать цели и задачи SOC (мониторинг, реагирование, единый центр компетенций или др.)
- Невозможно совмещать процессы SOC с другой деятельностью
- Основа SOC – аналитики. Нужны квалифицированные и мотивированные кадры!
- Начинать стоит с режима работы 8x5, но задать целью 24x7
- Каждый инцидент – повод для развития системы ИБ
- Важно обеспечить взаимодействие с другими SOC / CERT / Гос.организациями, ответственными за ИБ. Клуб «SOC в России» - http://soc-club.ru

Простые рекомендации

На следующую неделю

- Перечитайте Приказ №17 и Методические рекомендации к нему…
- Оцените зрелость процессов, необходимых для SOC

На 3 месяца

- Поймите и примите необходимость управления инцидентами и донесите эту мысль до руководства
- Актуализируйте перечень важных информационных ресурсов
- Определите уместный тип SOC (I, II, III)
- Определите необходимые ресурсы (люди, процессы, технологии)
- Решите с лицензией на ТЗКИ
- Подготовьте верхнеуровневый план работ

На год

- Запустите процессы: Управление уязвимостями, Управление событиями ИБ и Управление инцидентами

Спасибо за внимание!

Прозоров Андрей, CISM

Мой блог: 80na20.blogspot.com
Мой твиттер: twitter.com/3dwave
Моя почта: a.prozorov@solarsecurity.ru