the open Net

sine qua non

Зачем нам еще один стандарт (и каким он должен быть)

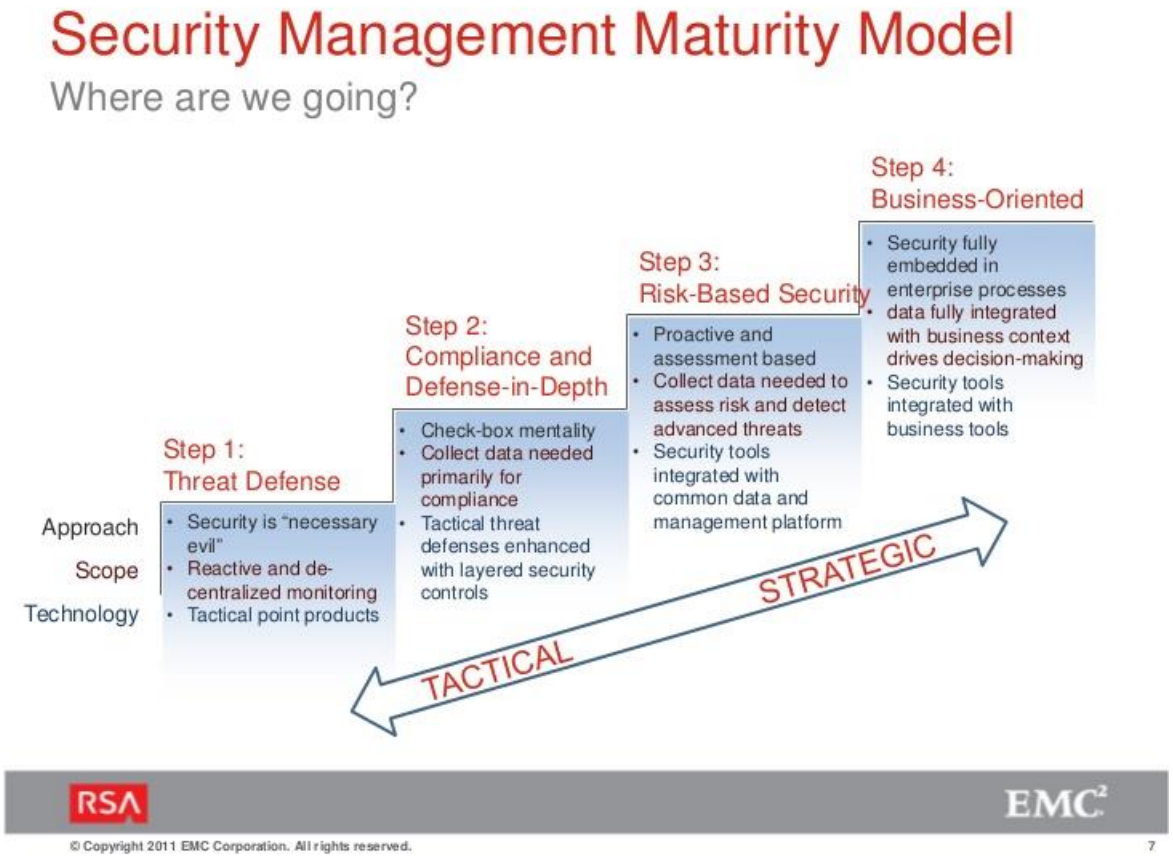
arkenoi@gmail.com

RUSCRYPTO 2017

Ассоциация “Открытая Сеть”

- “измерение качества интернета” (в том числе метрик безопасности)
- техническая экспертиза
- коммуникации и обучение

Чем занимается ИБ по мнению вендоров GRC (и почему GRC плохое слово и не нужно его употреблять лишний раз)



Чем занимается ИБ на самом деле?

- Только рисками
- Если ИБ занимается чем-то, что не считается рисками, или кто-то неправильно понял, или кто-то не умеет объяснять

Бедность и шизофрения

- Для безопасности нужно одно, говорится о другом, а делается третье (а все потому что не знаем рисков, а интересы участников конфликтуют)
- Отсюда бедность — на такую чушь не дают денег!

Ловушка поставщиков решений

- С топовых компаний снимают сливки
- Они оплачивают разработку новых технологий, ML/AI/так далее
- Остальные получают жмых и объедки (“черта бедности”) и вынуждены ждать, пока технология из “высокого искусства” станет ремеслом
- Производители не заинтересованы ускорять этот процесс.

Печальный итог

- 60% компаний оценивают информированность руководства о рисках ИБ от “никакой” до “небольшой”.

(NopSec 2016 Outlook: Vulnerability Risk Management and Remediation Trends)

Does it blend?

- А давайте просто следовать лучшим практикам! Выделим фиксированный процент IT-бюджета на безопасность и постараемся его разумно потратить.

Клинический случай: межсетевые экраны

- “Шлюзы приложений” старой школы: давайте определим безопасное подмножество протоколов и будем с ним работать, а приложения будем учить писать правильно
- (что-то пошло не так, “firewall friendly”)
- ~~к чорту все, буду проституткой~~ все бегает по http[s], фильтруем пакетики как умеем
- Давайте хоть что-то будем разбирать в трафике

Does not blend

- “взять процент от IT-бюджета и следовать лучшим практикам не работает”

  без понимания рисков бюджет урежут, а один размерчик всем не подойдет, лучшие практики это миф

Дай миллион

- Тебе зачем?
- На безопасность!
- Зачем нужна твоя безопасность?
- Три опции: ответить “это ты мне скажи” (я тебя нанимал не делать проблемы а решать), врать и запугивать и “на комплаенс”

Проблема уязвимостей

- “Лучшие практики” предполагают хорошо работающий патч-менеджмент, подтверждаемый проверками эффективности
- Рекомендации по “периодическому сканированию” основаны именно на этом предположении.
- Все это, как правило, не работает.

Что такое риск

- Насколько плохо
- Как часто

Риски уязвимостей

- Ценность актива (asset management), определяющая параметры ущерба
- Факторы окружения, определяющие частоту контакта с угрожающим агентом
- Это тоже на 80% сводится к простым эвристикам, но сейчас нет времени объяснять
- Поэтому речь пойдет о третьем факторе — возможностях атакующего

Приоритизация уязвимостей

- Сканирование (дешево)
- Непрерывное управление (дорого)
- Black magic (очень дорого)
- Добавим GRC для гламура

Приоритизация уязвимостей

- Способы поместить уязвимости в контекст “для бедных” и компромиссы
- Критичные системы
- Торчит в интернет
- Остальное “как-нибудь потом” — в итоге атакующий может с легкостью поддерживать присутствие в сети организации

Почему не CVSS

Спросите пентестера! (или хакера)

- Эксплуатируема ли уязвимость в конкретной системе?
- Есть ли **готовый** эксплоит?
- Что он дает?

- If you know that, you get part of the equation solved. The other parts are the asset value, protection countermeasures and you chances to be attacked.

Winshock: страшно аж жуть

- Winshock (MS14-066)

- Удаленное исполнение кода в TLS-библиотеке SChannels
- “Есть доступные эксплоиты” (CVSS=10)
- На самом деле только отказ в обслуживании

Фреймворки и стандарты TI

- SIEM is the king
- короля делает свита (CybOX,STIX,TAXII)
- Что не про события и сигнатуры, то для оценки соответствия (OVAL, XCCDF)
- Что не для оценки соответствия — то не для машин, а для людей (CVRF)
- Главный вывод: у вас дыра в безопасности (нет стандартов определяющих реальные последствия эксплуатации)

Как мы дошли до жизни такой

- Что нужно, чтобы стандарт был живой
- keep it simple
- живые продукты
- ~~поддержка Department of Homeland Security~~

Посмертное вскрытие: VEDEF

- Пять лет заседали
- Попытались объять необъятное
- не опубликовали даже драфта

Посмертное вскрытие: ССЕ

- Начали за здравие
- Какое-то время поддерживали
- Все умерло
- Обещают реанимацию

На аппарате жизнеобеспечения: CPE

- “Вроде поддерживается”
- Вендоры не хотят
- Ограниченное использование (де факто только ОС и веб-серверы)
- SCAP, OVAL вместо

А может, ну его?

- ad hoc formats
- Вендоры не хотят (привет, Vulners!)
- Ограниченное использование (де факто только ОС и веб-серверы)
- SCAP, OVAL — тесты вместо формального описания окружения

Требования

- Простота
- Формат для машин, а не для людей
- НЕ формат для уведомлений безопасности
- НЕ формат сигнатур для сканеров
- Интегрируемость с существующими фреймворками

Трудности

- “Основной ключ” идентификации уязвимости: оказывается, в CVE есть не все
- CPE невозможно получить с живой системы
- CCE мертв, конфигурацию описать нельзя никак
- Специализированные тесты — плохо, мы не сканер пишем.

Ищем компромиссы

- CVE основа, но возможны альтернативные пространства имен
- CPE используем как умеем для описания платформы, а для поиска достаточно привязки к CVE
- конфигурацию огрубляем (работает всегда; по умолчанию; в специальных случаях)
- все остальное — в расширения

ECDML и EACVSS

- Exploit Capability Definition Markup Language – описываем возможности эксплоитов через CVE, CPE и опциональную дополнительную информацию (CCE бы помогла, но умерла так умерла)
- EACVSS – Exploit Adjusted CVSS — скоринг с поправкой на возможности конкретного эксплоита

Попробуйте это прочитать

```
<exploit>
<configuration>
<cpe-lang:logical-test operator="OR" negate="false">
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_8.1:-:-:~-~-~-~x64~"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_8.1:-:-:~-~-~-~x86~"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:-:gold"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:r2:-:~-~datacenter~~~
"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:r2:-:~-~essentials~~~
"/>
        <cpe-lang:fact-ref name="cpe:/o:microsoft:windows_server_2012:r2:-:~-~standard~~~~"/
>
</cpe-lang:logical-test>
</configuration>
<eacvss>
  <cvssv2:base-score>8.5</cvssv2:base-score>
  <cvssv2:access-vector>NETWORK</cvssv2:access-vector>
  <cvssv2:access-complexity>LOW</cvssv2:access-complexity>
  <cvssv2:authentication>NONE</cvssv2:authentication>
  <cvssv2:confidentiality-impact>PARTIAL</cvssv2:confidentiality-impact>
  <cvssv2:integrity-impact>NONE</cvssv2:integrity-impact>
  <cvssv2:availability-impact>COMPLETE</cvssv2:availability-impact>
  <cvssv3:base-score>8.2</cvssv3:base-score>
  <configuration-constraints>DEFAULT</configuration-constraints>
  <availability>PUBLIC</availability>
  <malware>false</malware>
  <worms>false</worms>
</eacvss>
<exploit_frameworks>metasploit</exploit_frameworks>
<exploit-quality>NORMAL</exploit-quality>
<metasploit_module_path>auxiliary/scanner/http/ms15_034_http_sys_memory_dump.rb</metasploit_module_path>
<publication_date>15-Apr-2015</publication_date>
<last_updated>15-Apr-2015</last_updated>
</exploit>
```

Что дальше

- Рабочая группа, если будут желающие
- Наполнение базы
- Разработка инструментария
- Совершенствование методологии с учетом других факторов (+FAIR)
- Контекст Threat Intelligence от операторов связи

Вопросы?

Пишите мне! arkenoi@gmail.com